

UNIVERSITY OF OTTAWA

PH.D. THESIS

Interactive Bias Injection Attacks Against Cyber-Physical Control Systems

Author:

Yuri Boiko

Supervisors:

Dr. Tet Yeap

Dr. Iluju Kiringa

A thesis submitted to the University of Ottawa in fulfillment of the
requirements for the degree of Doctor of Philosophy

in the

Smart IoT Lab

School of Electrical Engineering and Computer Science
Faculty of Engineering

© Yuri Boiko, Ottawa, Canada, 2026

List of Publications

Articles for Refereed Journals

(Published as preprint and/or under review)

1. Yuri Boiko, Iluju Kiringa, and Tet Yeap, "Linear Dynamic Predictor Based Defense Against Current Drainage Cyber Attack of BLDC Motor Control System", Authorea Preprints, 2024. [1]

Published Conference Papers

1. Yuri Boiko, Iluju Kiringa and Tet Yeap, "Current Drainage Attack Correction via Adjusting the Attacking Saw Function Asymmetry," in Proc. 17th Int. Conf. Cyber Resilience Systems and Cybersecurity (CRSC), Ottawa, ON, Canada, Dec. 2023, pp. 685–691. Published by WASET as Int. J. Comput. Inf. Eng., vol. 17, no. 12, Open Science Index 204. Available online: <https://publications.waset.org/10013400.pdf> [2]
2. Yuri Boiko, Iluju Kiringa, and Tet Yeap, "Extended Pulsation Attack Against Kalman Filter Driven BLDC Motor Control System", 2023 13th International Conference on Advanced Computer Information Technologies (ACIT), Wrocław, Poland, 2023, pp. 397-402. doi: 10.1109/ACIT58437.2023.10275446. [3]
3. Yuri Boiko, Iluju Kiringa and Tet Yeap, "Voltage hopping induced by bias injection attack against Kalman filter of BLDC motor", 2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC), Houston, TX, USA, 2023, pp. 1-5. doi: 10.1109/ICAIC57335.2023.10044123. [4]
4. Yuri Boiko, Iluju Kiringa and Tet Yeap, "Current drainage induced by bias injection attack against Kalman filter of BLDC motor", 2022 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2022, pp. 364-369. doi: 10.1109/CSR54599.2022.9850310. [5]

5. Yuri Boiko, Ci Lin, Iluju Kiringa, and Tet Yeap. "Performance of BLDC Motor under Kalman Filter Sensorless Drive", Conference: Control Systems and Automation, July 2021 in Ottawa, ON, Canada, World Academy of Science, International Journal of Electrical and Information Engineering 15, no. 7, pp.282-288 (2021).
<https://publications.waset.org/10012126.pdf> [6]
6. Yuri B. Boiko and Tet H. Yeap, "Self-similarity of the simulated internet traffic from the source with clustered fragmented periodic output", In: SummerSim 2013 conference proceedings, Toronto, ON, Canada, 2013, pp. 35-40.
<https://dl.acm.org/doi/10.5555/2557696.2557734> [7]

Papers Submitted for Conference Participation (currently under review)

1. Yuri Boiko, Iluju Kiringa and Tet Yeap, "Induced Pulsation Attack Against Kalman Filter Driven Brushless DC Motor Control System," in Proc. 17th Int. Conf. Cybersecurity, Cybercrime and Cyberthreats (ICCCC), Montreal, QC, Canada, May 2023. Accepted for publication in Int. J. Electr. Inf. Eng.;
Abstract available online: <https://publications.waset.org/abstracts/164883.pdf> [8]

Abstract

As industrial infrastructure increasingly relies on high-performance motion control, the security of feedback loops in Cyber-Physical Systems (CPS) has become a critical concern. This dissertation investigates cyber-attack vulnerabilities in closed-loop controlled Brushless DC (BLDC) motor systems, demonstrating that standard state estimation techniques like the Kalman Filter can be exploited to mask catastrophic physical damage. Through systematic modeling and simulation, this research establishes a taxonomy of six distinct bias injection attack modalities: Probing Mode attacks for reconnaissance; Current Drainage attacks exploiting saw-function modulation; Voltage Hopping attacks achieving high-frequency manipulation above circuit cutoff frequencies; and three pulsation-based attacks (Induced, Extended, and Hyper-Spiking) that exploit dynamic resonance and phase synchronization. This classification distinguishes between transient disruptions and more persistent threats, demonstrating that Extended Pulsation is a necessary condition for the manifestation of latent Hyper-Spiking phenomena.

Novel contributions include the discovery of the voltage hopping phenomenon, where voltage excursions of ± 500 V occur at 2.1875 kHz with minimal impact on observable state variables, and the hyper-spiking attack mechanism producing voltage spikes up to 6000 V through phase-tuned resonance. The “attack withdrawal syndrome” is identified and characterized, demonstrating that abrupt attack termination can produce transients exceeding attack peak values by factors of up to 3.8. A comprehensive taxonomy relating saw-function asymmetry parameter (K_S) to current drainage signatures reveals that symmetric profiles enhance stealth while asymmetric profiles maximize damage observability.

A Linear Defense Strategy using parallel linear-dynamic prediction is proposed to neutralize current drainage and induced pulsation attacks. By employing anticipatory compensation, the strategy also effectively mitigates attack withdrawal syndrome, as confirmed through experimental validation. The defense architecture operates within an asymmetric Stackelberg game framework, achieving real-time performance suitable for embedded controllers. By establishing

the theoretical foundations for securing feedback loops against resonance-based manipulation, this research provides the necessary framework for designing resilient next-generation industrial controllers.

Keywords: Industrial Control System Cybersecurity, ICS Cybersecurity, Cybersecurity, Cyber-Physical Systems, CPS, BLDC Motor Control, Sensorless Drive, Kalman Filter, Bias Injection Attack, Resonant Attacks, Resonant Bias Injection Attacks, Voltage Hopping, Induced Pulsation, Extended Pulsation, Hyper-Spiking, Current Drainage, Probing Attack, Attack Withdrawal Syndrome, Initial Impulse, Asymmetric Stackelberg Game, Linear Predictor-Based Defense, Pre-emptive Compensation Defense, State Estimation Resilience.

Acknowledgements

I would like to express my deepest gratitude to my supervisors, **Dr. Tet Yeap** and **Dr. Iluju Kiringa**, for their invaluable guidance, patience, and unwavering support throughout my doctoral research at the University of Ottawa. Their profound expertise in Smart IoT and Cyber-Physical Systems has been fundamental to the successful completion of this work.

I am also deeply grateful to my thesis committee members, **Dr. Azzedine Boukerche**, **Dr. Mohammad Zulkernine**, **Dr. Qi-Jun Zhang**, and **Dr. Ahmed Karmouch**, for their insightful suggestions and for challenging me to think critically. Your diverse perspectives have significantly enriched the depth and quality of this research. Furthermore, I would like to thank **Dr. Riadh Habash** and **Dr. Qi-Jun Zhang** for serving on my comprehensive examination committee and for their rigorous academic guidance.

I am indebted to the members of the **Smart IoT Lab** for fostering such a stimulating and collaborative environment. In particular, I wish to thank my colleagues **Dr. Ci Lin**, **Dr. Patrick Killeen**, **Dr. Kalonji Kalala**, **Futong Li**, and **Faezeh Halabian**. The discussions, camaraderie, and mutual support we shared made this long journey not only productive but also truly enjoyable.

I gratefully acknowledge the financial support provided by the **Ontario Research Fund** and the **University of Ottawa** admission scholarship, which enabled me to pursue my Ph.D. My growth as a scholar and educator was further enriched by my experiences as a research and teaching assistant. For providing these valuable opportunities to develop my pedagogical skills, I sincerely thank **Dr. Murat Simsek**, **Dr. Jochen Lang**, **Dr. Guy-Vincent Jourdan**, **Dr. Yongyi Mao**, **Dr. Gilbert Arbez**, **Dr. Nguyen Quyen**, and **Dr. Tet Yeap**.

Finally, my heartfelt thanks go to my family. Your unwavering encouragement and belief in me have been my greatest source of strength throughout this journey.

Table of Contents

List of Publications	ii
Abstract	iv
Acknowledgements	vi
List of Tables	xii
List of Figures	xiii
List of Code Snippets	xxiv
Nomenclature	xxv
1 Introduction	1
1.1 Motivation	1
1.2 Research Objectives	3
1.3 Thesis Statement	5
1.4 Research Framework	7
1.4.1 Baseline System Architecture	7
1.4.2 Control Loops and Attack Surface	8
1.4.3 Assumptions for Adversarial and Defensive Agents	9
1.4.4 Interactivity and Goals	10
1.5 Key Challenges	10
1.6 Novel Contributions	12

1.6.1	Systematic Attack Taxonomy and Characterization	12
1.6.2	Pulsation-Based Attack Family and Dynamic Resonance Exploitation . .	14
1.6.3	Defense Architecture and Countermeasure Development	15
1.6.4	Methodological Contributions	16
1.6.5	Practical Security Implications	17
1.6.6	Summary of Contributions	18
1.7	Significance of the Contributions	18
1.8	Thesis Organization	20
2	Literature Review	21
2.1	Integrity Attacks Against CPS	21
2.2	Communication layer security	25
2.3	Attacks via TCP/IP connection	26
2.4	Bias injection attack against state observers	28
2.5	DC motor as an object for attacks	32
2.5.1	BLDC motor as an object for attacks	32
2.5.2	Electric vehicle as an object for attacks	35
2.6	A machine learning approach for attacks design	38
2.7	Vulnerabilities and Defense Gaps in Industrial CPS	44
3	Problem Formulation and Methodology	47
3.1	Problem Formulation	47
3.2	Methodology	48
3.2.1	Driving BLDC motor with Kalman filter based drive	48
3.2.2	Cyber-attack construction	54
3.3	Predictive Cyber-defense design	60
4	Experimental Results	64
4.1	Position Sensorless Drive of BLDC Motor	64
4.1.1	Equal Angular Increments in Driving of BLDC Motor	65

4.1.2	Equal Time Increments in Driving of BLDC Motor	71
4.2	Probing Mode Cyber-attacks	75
4.2.1	Probing by double-step function bias injection	76
4.2.2	Probing by linear ramp bias with initial shallow drop	77
4.2.3	Saw Bias Probe Injection	78
4.3	Current Drainage Cyber-Attack	80
4.3.1	Attack Objectives and Manifestation	80
4.3.2	Deep-leveled, Large-amplitude Modulation Saw Teeth	82
4.3.3	Deep-leveled, Intermediate-amplitude Modulation Saw Teeth	84
4.3.4	Deep-leveled, Small-amplitude Modulation Saw Teeth	85
4.3.5	Adjusting Asymmetry in Saw Function	86
4.3.6	Summary of the Current Drainage Attack	94
4.4	Voltage Hopping Cyber-Attack	95
4.4.1	Selecting Model for the Bias Coefficient $\chi(t)$	96
4.4.2	Impact of Bias Coefficient $\chi(t)$ Modulation Frequency Fine Tuning	97
4.4.3	Summary on Voltage Hopping Attack	103
4.5	Pulsations Cyber-Attacks	103
4.5.1	Induced Pulsations Cyber-Attack	104
4.5.2	Extended Pulsations Cyber-Attack	115
4.5.3	Hyper-spiking Cyber-Attack	125
4.5.4	Summary and Conclusive Remarks on Pulsations Cyber-attacks	129
4.6	Linear Defense Implementation	131
4.6.1	Linear Defense Strategy	131
4.6.2	Experimental Problem Formulation for Defense	134
4.6.3	Predictor-based Defense Architecture	134
4.6.4	Current Drainage to be Negated	136
4.6.5	Attack Withdrawal Syndrome to be Negated	138
4.6.6	Predictor Based Defense Operation	140

4.6.7	Experimental Results of Defensive Actions	141
4.6.8	Current Drainage Negation	141
4.6.9	Start Impulse Issue	142
4.6.10	Attack Withdrawal Syndrome Negation	144
4.6.11	Induced Pulsation Negation	145
4.6.12	Discussion on the Defense Approaches	148
4.6.13	Summary on Linear Defense Implementation	148
4.6.14	Future Work Extension	149
5	Analysis and Discussion	150
5.1	Summary of Key Experimental Results	150
5.1.1	The Strategic Dual Nature of Initial Probing Attacks	151
5.1.2	The Identified Attacks Variations	151
5.1.3	The Strategic Edge of Unpredictability	155
5.1.4	The First Line of Defense: Reverse Feedback with Linear Extrapolator	156
5.1.5	The Second Line of Defense: Adaptive Predictors for Resonance Attacks	157
5.1.6	Game-Theoretic Applicability in Attacker–Defender Interaction	158
5.1.7	Asymmetric Stackelberg Game Interpretation	158
5.1.8	Applicability of Alternative Game-Theoretic Models	167
5.2	Comparison of Methodologies	170
5.2.1	Static vs. Interactive Dynamics: Evasion Philosophy	170
5.2.2	Historical Context: Comparison with Stuxnet	171
5.2.3	Attack Target: Beyond Static Bias and Network Protocols	171
5.2.4	Resource Model	172
5.2.5	Real-Time Identification vs. Computational Overhead	173
5.2.6	Integrity in Network Security	173
5.2.7	Estimation: Issue of Static Bias	174
5.2.8	Game Strategy	174
5.2.9	Compensation Technique	174

6	Conclusions and Future Work	177
6.1	Summary of Research and Contributions	177
6.2	Limitations of the Current Study	179
6.3	Future Work	179
6.3.1	False-Data Injection Attacks on Field-Oriented Control	180
6.3.2	Attacks on Sensorless AC Control Schemes	181
6.3.3	Security of Industrial Variable-Frequency Drives	181
6.3.4	Digital Twin–Based Experimental Platform	181
6.3.5	Model-Based Intrusion Detection Using Observer Residuals	182
6.3.6	Autonomous Defensive Agents and Malware Containment	182
	References	183

List of Tables

2.1	Summary of the selected attacks/defense strategies for CPSs.	23
2.2	Summary of the attacks with various levels of machine learning intelligence. . . .	40
4.1	Summary of Quantitative Defense Metrics for Pulsation Negation	147
5.1	Comparison of Game-Theoretic Models for Cyber–Physical Defense	169
5.2	Qualitative Comparison of Attack and Defense Methodologies (part 1)	172
5.3	Qualitative Comparison of Attack and Defense Methodologies (part 2)	176

List of Figures

2.1	Wireless system communication features and targeted attacks [22].	26
2.2	Block diagram of the benchmark platform for the verification of stealthy attack technology [26].	27
2.3	Luenberger Observer control scheme.	29
2.4	Transformation of the controller's signal to the plant by the attacker's induced distortion in Luenberger Observer control scheme.	29
2.5	A control scheme with Kalman filter as an optimal observer.	30
2.6	Transformation of the controller's signal to the plant with accommodation of the attacker's induced distortion in control scheme with Kalman filter as an optimal observer.	30
2.7	Motor Threat Model (MTM) attack tree templates for control, data exfiltration, and disrupt objectives. (Reproduced from ref. [27]).	33
2.8	Modified Motor Threat Model attack tree template for control objectives (see initial version in Figure 2.7, specifically, in its left top part) with inclusion of a state observer as potential target for attack. (Modified from ref. [27]).	33
2.9	The seven Motor Threat Model (MTM) layers of vulnerabilities for the attacks. (Reproduced from ref. [27]).	34
2.10	Modified layer structure of Motor Threat Model (MTM) to include a state observer as potential layer of vulnerability. (Modified from ref. [27]).	34
2.11	Overall scheme of the combined control strategy for EV. (Reproduced from Yousfi et al. (2011) [72]).	37
2.12	General block diagram of an ICS continuous feedback-loop indicating where cyber-attacks can target and compromise the system: (1) actuators, (2) sensors, or (3) controller. Here, altered data from the attack is highlighted in red which the physics-based detection intends to detect. [75].	39

2.13	Adding the observer to an ICS continuous feedback-loop, thus rendering additional point for the attack (point (4) observer) as compared to that of Figure 2.12.	39
2.14	Active System Identification attack with a MitM in the feedback link. It is reproduced from [91].	43
3.1	Schematic of the employed control system of BLDC motor with Kalman filter in the feedback loop. Kalman filter's inputs are operating voltages v_a, v_b and v_c for the motor's phases A, B and C, while outputs are estimated values of angular speed $\hat{\omega}$ and rotor's angular position $\hat{\theta}$.	49
3.2	Bias injection attack construction against Kalman filter as a driver in a feedback loop of PID controlled BLDC motor in position sensorless mode.	55
3.3	Architecture with position sensorless drive for BLDC motor as well as bias injection $\delta\omega$ access point. Kalman filter inputs are voltages in the respective winding, u_a, u_b, u_c , and load torque τ_L .	56
3.4	Model verification with sequential test (I) through (iv). The set of state variables is: i_a, i_b, i_c are currents in the respective winding, speed estimate $\hat{\omega}$ and position estimate $\hat{\theta}$ of the rotor. Values of the phase currents are in A (Amperes) (i_a, i_b, i_c), angular speed ω is in rad/s (radians per second), rotor position θ is in rad (radians), and phase voltage u_a is in V (Volts). The horizontal axis represents time in seconds (s).	58
3.5	Testing functions of distortion bias coefficient, χ : (a) positive rectangular pulse; (b) linearly increasing bias; (c) saw function (deep-leveled, low-modulation height saw); (d) saw function (deep-leveled, intermediate-modulation height saw).	59
3.6	The first scenario, illustrating the defense mechanism under Informed Counter-Bias. The figure depicts the state where the attack detector is active and has successfully measured the adversarial bias. This measured bias is used to initiate a predictor component, which estimates the expected bias for the subsequent sampling cycle. The calculated compensatory counter-bias signal is then prepared for injection into the control loop in the next step.	61
3.7	The defense mechanism block is idle in the scenario of Informed Counter-Bias. In this state, the block gives a nominal output value of "1" for the counter-bias signal, resulting in no active compensation.	62

3.8	Operation of the Blind Compensation scheme of predictive defense against bias injection attack. From the values of the output voltages (u_a, u_b, u_c) from the inverter and the torque value (τ_L), the defender estimates the expected effect of the attacker action for the next sampling cycle and injects the counter-bias to sustain the required angular speed ω . The figure illustrates the ideal case where the estimate $\hat{\chi}$ equals the true but unknown distortion χ	62
3.9	The idle state of the defense module in the Blind Compensation scheme. The attack detector is active and continuously monitoring the system, but the defense mechanism is functionally idle, providing a nominal output value of "1" for the counter-bias signal.	63
4.1	Operating voltages for the motor's phases A, B and C measured with respect to the ground (variables for parameters used in the program are: u_{AG}, u_{BG}, u_{CG}). Voltages are represented in relative units (proportional to variable $KV = 100$ scaling up factor (V)). Horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$	66
4.2	Test Case #1: Starting of BLDC motor from zero position (zero orientation angle $\theta = 0$, zero initial speed $\omega_0 = 0$, cycle number $M = 1$). Shown sequentially are the state variables (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). Vertical scales are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$	67
4.3	Test Case #2: Rotor acceleration stage (verification at the 11-th rotation cycle, $M = 11$). Shown sequentially are the state variables (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). Vertical scales are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$	68
4.4	Test Case #3: Saturation of acceleration and onset of torque ripples after approximately 100 rotations (verification at the 111-th rotation cycle, $M = 111$). Shown sequentially are the state variables (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). Vertical scales are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$	69

4.5	Test Case #4: Steady-state rotation achieved after approximately 500 rotations (verification at the 500-th rotation cycle, $M = 500$). Shown sequentially are the state variables (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). Vertical scales are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$	70
4.6	Open-loop control of BLDC motor using the Kalman Filter (KF) with an equal time increments drive. Shown are 10 consecutive frames, starting with frame number 101 and ending with frame number 111. The state variables are shown sequentially (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). Vertical scales are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$	72
4.7	Reduction of torque ripples via increased motor induction. The inductance values are doubled compared to Figure 4.6, reaching $L = 0.04$ H and mutual inductance $M = 0.02$ H. Shown sequentially are the state variables (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). Vertical scales are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$	73
4.8	Further reduction of torque ripples achieved by reducing the Kalman Filter (KF) sampling time $\Delta t = T$ from $20 \mu\text{sec}/\text{step}$ down to $15 \mu\text{sec}/\text{step}$. Other parameters remain the same as in Figure 4.6. Shown sequentially are the state variables (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). Vertical scales are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $15 \mu\text{sec}/\text{step}$	74
4.9	Probing mode attack with double-step function as bias distortion coefficient. Values of i_a are in Amps, values of $\omega = \hat{\omega}$ are in rad/sec.	76
4.10	Probing attack by linear ramp bias with initial shallow drop Values of i_a are in Amps, values of $\omega = \hat{\omega}$ are in rad/sec, time in sec (horizontal axis).	78

4.11	System response to the saw bias probe injection profile. The current surge is delayed during the first saw tooth and begins at the start of the second period when ω dropped by $\delta\omega = 59.52$ rad/s. Parameters: A probe rate $\chi' = 4.286 \times 10^{-5}$, $K_p = 10$, and attack start time $t = 1.5$ s. Current i_a is shown in Amperes (A), angular velocity ω (or $\hat{\omega}$) in rad/s, and time t in seconds (s).	79
4.12	Performance of the deep-leveled saw function with large-amplitude modulation saw profile in bias injection on system response – the current drainage effect is periodic, as the saw tooth sequence is. Saw tooth depth is initialized at $\delta\omega = 23.81$ rad/sec level, $\chi' = 0.00004286$, $K_p = 10$, attack starts at $t = 1.5$ sec. Values of i_a are in Amps, values of $\omega = \hat{\omega}$ are in rad/sec, time is in seconds (horizontal axis).	83
4.13	Performance of the deep-leveled, intermediate-amplitude modulation sawtooth function in bias injection on system response – the current drainage segments begin to overlap. Saw tooth depth is initialized at $\delta\omega = 11.9$ rad/sec level, $\chi' = 0.00004286$, $K_p = 10$, attack starts at $t = 1.5$ sec. Values of i_a are in Amps, values of $\omega = \hat{\omega}$ are in rad/sec, time is in seconds (horizontal axis).	84
4.14	Performance of the deep-leveled, small-amplitude modulation saw teeth profile in bias injection on system response – the current drainage segments strongly overlap. Saw tooth depth is initialized at $\delta\omega = 5.95$ rad/sec level, which is 2.38 percent of the level of initial speed of 250 rad/sec, $\chi' = 0.00004286$, $K_p = 10$, attack starts at $t = 1.5$ sec. Values of i_a are in Amps, values of $\omega = \hat{\omega}$ are in rad/sec, time is in seconds (horizontal axis).	86
4.15	The Tested Distortion Coefficient (χ) Profiles for Current Drainage Experiments: (a) Fully Asymmetric Sawtooth Wave; (b) Partially Asymmetric Sawtooth Wave; (c) Fully Symmetric Triangle Wave; (d) Attack Flow engaging the Fully Asymmetric Wave (a). The variation in χ asymmetry is used to adjust the current drainage effect.	88
4.16	Attack using saw function with fully asymmetric triangle as a tooth shape for the bias distortion coefficient χ ($K_S = 0$, right triangle case with $h = 0.1$, i.e., 10% of the attack depth on a χ -scale). Values of the phase currents are in A (Amperes) (i_a, i_b, i_c), angular speed ω is in rad/s (radians per second), rotor position θ is in rad (radians), and phase voltage u_a is in V (Volts). The horizontal axis represents time in seconds (s).	90

4.17	Attack using saw function with acute triangle tooth shape for the bias distortion coefficient χ , with symmetry $K_S = 0.0002$ and saw depth $h = 0.1$. Values of the phase currents are in A (Amperes) (i_a, i_b, i_c), angular speed ω is in rad/s (radians per second), rotor position θ is in rad (radians), and phase voltage u_a is in V (Volts). The horizontal axis represents time in seconds (s).	91
4.18	Attack with acute triangle saw function as bias distortion coefficient with symmetry $K_S = 0.0005$ and saw depth $h = 0.1$. Values of i_a, i_b, i_c are in Amps, ω are in rad/sec, θ are in radians, u_a are in Volts. Horizontal axis is time in seconds.	92
4.19	Attack using saw function with isosceles triangle tooth shape for the bias distortion coefficient χ , with symmetry $K_S = 1$ and saw depth $h = 0.1$, i.e., 10% of the attack depth on a χ -scale. Values of the phase currents are in A (Amperes) (i_a, i_b, i_c), angular speed ω is in rad/s (radians per second), rotor position θ is in rad (radians), and phase voltage u_a is in V (Volts). The horizontal axis represents time in seconds (s).	93
4.20	The high-frequency modulation of the distortion coefficient χ required to achieve the "voltage hopping" effect. The signal is a symmetric saw wave with a frequency of 17.5 kHz and an amplitude of $h = 1.3$. This profile produces interchanging sequences of $\chi > 1$ and $\chi < 1$ values necessary for the effect.	98
4.21	Voltage hopping attack (start point $t = 1.5$ s, end point $t = 2$ s, indicated by red arrow) with χ modulation at 17.5 kHz and amplitude of $h = 1.3$ (as in Figure 4.20). State variables shown are winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), and position (θ in rad (radians)). The signal u_a represents the phase voltage in winding "a" (in V (Volts)).	99
4.22	Reduction of χ modulation frequency to 3.5 kHz induces moderate deceleration in the voltage hopping attack (start $t = 1.5$ s, end $t = 2$ s, indicated by red arrow). State variables shown are winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), and position (θ in rad (radians)). The signal u_a represents the phase voltage in winding "a" (in V (Volts)).	100
4.23	Further reduction of χ modulation to 2.5 kHz improves the equilibrium between acceleration/deceleration in the voltage hopping attack (start $t = 1.5$ s, end $t = 2$ s, indicated by red arrow). State variables shown are winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), and position (θ in rad (radians)). The signal u_a represents the phase voltage in winding "a" (in V (Volts)).	101

- 4.24 Equilibrium state achieved at χ modulation frequency of 2.1875 kHz in the voltage hopping attack (start $t = 1.5$ s, end $t = 2$ s, indicated by red arrow). No visible steady-state effect is observed on state variables, but large voltage jumps persist. State variables shown are winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), and position (θ in rad (radians)). The signal u_a represents the phase voltage in winding “a” (in V (Volts)). 102
- 4.25 Tested linear distortion functions with constant gradient for the following values of $\nabla\chi$ in steps⁻¹ units: (a) 1.5×10^{-5} , (b) 3×10^{-5} , (c) 4.5×10^{-5} , (d) 6×10^{-5} , and (e) 15×10^{-5} . Attack window duration is fixed to be $\Delta t = 0.5$ s, but time allocation for each step is dynamically linked to the angular speed ω 105
- 4.26 Overall system performance, including acceleration for time interval $t = [0, 0.5)$ s, stabilization for $t = [0.5, 1.0)$ s, step function response for $t = [1.0, 1.5)$ s, attack window marked by red arrow at $t = [1.5, 2)$ s with gradient $\nabla\chi = 1.5 \times 10^{-5}$ steps⁻¹ as in Figure 4.25(a), and attack withdrawal syndrome for $t > 2$ s with post-attack stabilization. The figure shows five system variables: currents (i_a, i_b, i_c) in A (Amperes), angular speed (ω) in rad/s (radians per second), rotor angular position (θ) in rad (radians), and phase voltage (u_a) in V (Volts). 107
- 4.27 System response to the attack followed by attack withdrawal syndrome for gradient $\nabla\chi = 1.5 \times 10^{-5}$ steps⁻¹ as in Figure 4.25(a). The attack window is marked with a red arrow. State variables shown include: winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)). 108
- 4.28 System response to the attack followed by attack withdrawal syndrome for gradient $\nabla\chi = 3 \times 10^{-5}$ steps⁻¹ as in Figure 4.25(b). The attack window is marked with a red arrow. State variables shown include: winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)). 109
- 4.29 System response to the attack followed by negated attack withdrawal syndrome for gradient $\nabla\chi = 4.5 \times 10^{-5}$ steps⁻¹ as in Figure 4.25(c). The attack window is marked with a red arrow. State variables shown include: winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)). 110

4.30	System response to the attack followed by reappearing inverted attack withdrawal syndrome for gradient $\nabla\chi = 6 \times 10^{-5} \text{ steps}^{-1}$ as in Figure 4.25(d). The attack window is marked with a red arrow. State variables shown include: winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).	111
4.31	System response to the attack followed by inverted attack withdrawal syndrome for gradient $\nabla\chi = 15 \times 10^{-5} \text{ steps}^{-1}$ as in Figure 4.25(e). The attack window is marked with a red arrow. State variables shown include: winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).	112
4.32	Wide-range saw functions tested to verify the impact of interruptions in linear growth and modifications to the parameters of the resulting wide-range saw functions on system responses. The functions cover a range of frequencies (approx. 3.4 Hz to 14 Hz) and peak χ values (χ_{top}) (specifically, $\chi_{\text{top}} = 1.5$ and $\chi_{\text{top}} = 2.3$ r.u.).	117
4.33	Extended pulsations induced by synchronization between the system's response and the distorting activity of the attacker under engaging of a wide-range saw function (as shown in Figure 4.32(a)) with a repetition frequency of approximately 3.4 Hz and peak χ value of 1.5 r.u. (relative units). The attack is placed within the window $t = [1.5, 2.0]$ s. State variables shown include: winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).	118
4.34	Phase relations between system response and attacker manipulation. The system response is plotted against the distorting activity of the wide-range saw function (as shown in Figure 4.32(a)), which has a repetition frequency of approximately 3.4 Hz and a peak χ value of 1.5 r.u. (relative units). State variables shown include: winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).	119
4.35	Chaotic features in system response due to the de-synchronization effect in the extended pulsation attack at a frequency of approximately 14 Hz for the wide-range saw function χ , as shown in Figure 4.32(b). De-synchronization of the current and voltage response patterns from the fundamental frequency of the saw-function is observed. State variables shown include: winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).	121

4.36	Chaotic response features under periodic influence at a frequency of approximately 14 Hz of the wide-range saw function of distortion χ , as depicted in Figure 4.32(b). De-synchronization of the current and voltage patterns with respect to the fundamental harmonic of the saw function is observed. State variables shown include: winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).	122
4.37	Repetitive nature of the system response within the extended pulsation attack window of $t = [1.5, 3.0]$ s for the initiating wide-range saw function of χ as depicted in Figure 4.32(c). State variables shown include: winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).	123
4.38	Hyper-spikes occurrence within the extended pulsation attack at a saw-function modulation frequency of approximately 6 Hz. Attack window duration is fixed to $\Delta t = 1.5$ s, with time allocation for each sampling step dynamically linked to the angular speed ω . State variables shown include: winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).	126
4.39	Architecture with position sensorless drive for BLDC motor as well as bias injection $\delta\omega$ access point. Kalman filter inputs are voltages in the respective winding, u_a, u_b, u_c , and load torque τ_L	135
4.40	Introduction of defense circuit into control system feedback loop of Figure 4.39. Attack predictor inputs are (1) estimate of rotor angular speed $\hat{\omega}$ and (2) its modified by the attacker value of $\chi\hat{\omega}$ corrected by the prior cycle predicted distortion coefficient χ^-	136
4.41	Tested distortion functions χ for the attacker manipulation game: (a) negative rectangular pulse; (b) gradually increasing bias; (c) saw function (deep-leveled, low-modulation height saw); (d) saw function (deep-leveled, intermediate-modulation height saw).	137
4.42	The bottom part of the tested partially symmetric triangular shallow saw function, similar to that shown in Figure 4.41 (c), follows a specific saw pattern. The parameters of the triangular tooth $\triangle AOC$ are as follows: the ascending side AO is represented by 1000 sampling steps of AB, and the descending side OB is represented by 100 sampling steps of BC. The symmetry coefficient is defined as $\tan(\beta)/\tan(\alpha) = 0.01$, where α is the angle $\angle AOB$ and β is the angle $\angle BOC$ of $\triangle AOC$	138

4.43	Current drainage effect observed under attack using the partially symmetrical shallow triangular saw function χ from Figure 4.42, with the defense system in an idle state. The attack commences at $t=1.5$ s and concludes at $t=2$ s, with the final phase depicted in Figure 4.44.	139
4.44	The observed effect of the attack withdrawal syndrome at the conclusion of the current drainage attack in a simulation experiment using the partially symmetrical shallow triangular saw function χ from Figure 4.42. This observation is made with the defense system in an idle state. The initial phase of the attack is depicted in Figure 4.43.	139
4.45	Predicting values of χ^- with the linear-dynamic difference equation (4.7) based predictor within the architecture of Figure 4.40 and the attack engaging saw function from Figure 4.42. Points A and B of Figure 4.42 are projected to points A^- and B^- herewith following vertical red-dashed projection lines starting from Figure 4.42 and ending herewith.	142
4.46	Negation of the current drainage attack at time window $t=[1.5; 2]$ seconds with linear-dynamic predictor in architecture of Figure 4.40. The attacker employs deeply diving but shallow modulation height saw function from Figure . 4.42. The defender counteracts by anticipating it as that shown in Figure 4.45. The residual disturbance of the angular speed ω calculated as the area above its steady state value $\omega_{steady}=249$ rad/s is ca. 0.2% of area under otherwise undisturbed $\omega = \omega_{steady}$ within the disturbance window. The issue of initial spike at $t = 1.5$ seconds is seen.	143
4.47	Enlarged view of the initial spike observed at time point $t = 1.5$ seconds during the negation of the current drainage attack. This negation strategy is implemented using a linear-dynamic predictor within the architecture illustrated in Figure 4.40. The attacker employs a shallow saw function detailed in Figure 4.42, while the defender anticipates and counters it, as demonstrated in Figure 4.45. Notably, the issue of the initial spike at $t = 1.5$ seconds is evident in windings 'a' and 'c' for both current and voltage ('b' was idle on this cycle). . .	144
4.48	Negation of attack withdrawal syndrome by linear-dynamic predictor circuit on defense module. The attack ends at $t = 2$ seconds point.	145
4.49	Negation of induced pulsations during an Extended Pulsations Attack via a linear-dynamic predictor circuit on the defense module. The adversarial activity occurs between $t = 1.5$ and $t = 3$ seconds.	146

4.50	Detailed transient response at the onset of induced pulsation negation via the linear-dynamic predictor circuit. The adversarial activity is initiated at the $t = 1.5$ s mark.	147
5.1	Asymmetric Stackelberg game tree illustrating defender (leader) and attacker (follower) interaction in linear-dynamic prediction defense. Leaf nodes are annotated with mathematical outcome criteria according to (5.10) and (5.11).	163
5.2	Discrete-time sequence of attacker–defender actions illustrating temporal leadership structure.	165

List of Code Snippets

3.1	Base set of parameters in Matlab simulation program	54
3.2	The non-diagonal elements of the fourth column of the matrix $\mathbf{A}$	54
4.1	Code in MATLAB notations for relations between voltage variables used as Kalman filter inputs for the equal angular increments drive simulation.	65

Nomenclature

Abbreviations

AWS Attack Withdrawal Syndrome

BEMF Back Electromotive Force

BLDC Brushless Direct Current

CPS Cyber-Physical System

DoS Denial of Service

EPA Extended Pulsations Attack

EV Electric Vehicle

FDI False Data Injection

FOC Field-Oriented Control

ICS Industrial Control System

IPA Induced Pulsations Attack

KF Kalman Filter

MCKF Maximum Correntropy Kalman Filter

MitM Man-in-the-Middle

MTM Motor Threat Model

OTS-KF Optimal Two-Stage Kalman Filter

PID Proportional-Integral-Derivative

UAV Unmanned Aerial Vehicle

Nomenclature

System Parameters (BLDC Motor and Control)

R Phase resistance (Ω)

L Phase inductance (H)

M Mutual inductance (H)

i_a, i_b, i_c Phase currents in windings A, B, and C (A)

u_a, u_b, u_c Phase voltages measured with respect to neutral node (V)

u_{ab}, u_{bc}, u_{ca} Line-to-line operating voltages (V)

$U_{abca}, U_{bcab}, U_{cabc}$ Transformed voltage variables for KF input

ξ_a, ξ_b, ξ_c Phase back electromotive force (BEMF) voltages (V)

u_n Neutral node voltage (V)

ω Rotor electrical angular velocity (rad/s)

ω_{ref} Reference angular speed set-point (rad/s)

θ Rotor electrical angle/position (rad)

τ_L Applied mechanical torque load ($N \cdot m$)

K_ξ (K_{emf}) Back EMF constant ($V \cdot s/rad$)

J Rotor inertia ($kg \cdot m^2$)

B (B_d) Motor viscous damping friction coefficient ($N \cdot m \cdot s/rad$)

p Number of motor poles

$f(\theta)$ Normalized trapezoidal function for BEMF calculation

K_p Proportionality coefficient for P-controller

Δt (T) Sampling time interval (s)

K_V Voltage scaling/amplification coefficient

State-Space and Kalman Filter Variables

- x_k Discrete-time system state vector at index k
- u_k Control input vector
- y_k Measurement/observation output vector
- v_k, w_k Process and measurement noise vectors
- $\mathbf{A}, \mathbf{B}, \mathbf{C}$ System dynamics, input, and measurement matrices
- $\hat{x}_k$ Estimated system state vector (posterior)
- $\hat{x}_k^-$ Predicted system state vector (prior)
- $\mathbf{P}_k$ State error covariance matrix
- $\mathbf{Q}$ Process noise error covariance matrix
- $\mathbf{R}$ Measurement noise error covariance matrix
- $\mathbf{K}_k$ Kalman gain matrix
- z_k Measurement vector at index k
- $\mathbf{I}$ Identity matrix

Cyber-Attack and Defense Variables

- χ Malicious distortion coefficient injected by the attacker
- χ^- Predicted distortion coefficient estimated by the defender
- $\delta\omega$ Injected bias term for angular speed estimates (rad/s)
- K_S Symmetry coefficient of the triangular saw-function tooth
- α, β Angles defining the asymmetry of the triangular saw tooth
- $h (\Delta\chi_{saw})$ Depth or amplitude of the sawtooth modulation
- $\nabla\chi (\chi')$ Gradient or first derivative of the distortion coefficient
- $\chi_{top}, \chi_{bottom}$ Maximum and minimum values of the distortion coefficient

χ_0 Value of the distortion coefficient at the zero-crossing point

$E_I(\chi)$ Accumulated current stress (physical damage proxy)

$I_{max}(\chi)$ Peak current (overload indicator)

T_{det} Time-to-detection of the attack

$E_{\Delta}(\chi)$ Residual energy (diagnostic measure)

J_A Attacker's utility/payoff function in Stackelberg game

J_D Defender's cost function in Stackelberg game

K_D Tunable defense gain for compensatory feedback

u_{def} Corrective defense signal injected into the control loop

$O_{withdraw}$ Metric for Attack Withdrawal Syndrome (AWS) severity

Subscripts and Superscripts

k Time step/sampling index

s Attack commencement index

th Threshold value

$pred$ Predicted value

$meas$ Measured value

$*$ Modified/compensated value

Chapter 1

Introduction

Development of industrial infrastructure nowadays involves the expansion of industrial control systems (ICS) and their connection to cyberspace [9]. Maintaining the security of such systems is essential for the operation of ICS [10, 11]. On the other hand, this expansion also increases the potential for attacks, whether initiated from inside industrial facilities or from cyberspace [4–7, 9, 12].

1.1 Motivation

Rapid technological development in cyberspace has enabled extensive interconnection of physical infrastructure with communication networks. Industrial devices, energy systems, transportation platforms, and robotic systems increasingly operate as cyber–physical systems (CPS) in which sensing, computation, communication, and control are tightly integrated. This integration significantly improves efficiency, remote accessibility, and system-level coordination. At the same time, it introduces new vulnerabilities, as malicious actors may exploit imperfections in communication networks, software layers, or sensing infrastructure to influence the behavior of the underlying physical systems.

As a result, cybersecurity has become a critical component of modern control architectures. In recent years, significant research efforts have been directed

toward understanding and mitigating cyber attacks on feedback-controlled systems. One widely studied attack class is false data injection (FDI), where an adversary manipulates sensor measurements transmitted to the controller. Such attacks can degrade system performance or even destabilize the controlled process while remaining difficult to detect using standard residual-based monitoring methods [13–15]. Most existing studies model these attacks as additive disturbances applied to sensor signals.

However, in many practical systems the adversary may instead alter the scale or gain of the measurement signal, resulting in multiplicative distortion rather than additive corruption. For example, a distorted measurement of angular velocity may take the form

$$\tilde{\omega}_k = \chi_k \omega_k.$$

Such distortion is fundamentally different from additive injection because it modifies the effective feedback gain within the closed-loop system, potentially altering the system dynamics themselves. When the distortion varies over time, particularly in a periodic manner, it can introduce parametric excitation effects that may interact with the natural modes of the controlled system. In electromechanical systems such as BLDC motor drives, this interaction may lead to resonance-like amplification of mechanical stress even when the attack signal itself remains bounded.

Despite significant advances in CPS security and resilient observer design, relatively little attention has been devoted to parametric attack mechanisms in discrete-time sampled-data control systems, especially in electromechanical drives. Furthermore, most existing defensive strategies are primarily reactive, focusing on disturbance rejection or attack detection after the fact. In adversarial environments, however, defenders may benefit from anticipatory strategies that estimate potential attacker actions and proactively compensate for them.

Dynamic game theory offers a useful framework for modeling strategic interactions between attackers and defenders. Nevertheless, most game-theoretic

studies of CPS security focus on resource allocation, monitoring policies, or network-level interactions, rather than on how adversarial actions influence the physical dynamics of the controlled system itself.

The motivation of this thesis is therefore to investigate cyber–physical attacks that exploit parametric distortion of feedback signals and to develop anticipatory defensive mechanisms capable of mitigating their effects. In particular, the work aims to bridge three areas that have largely evolved independently:

- cyber–physical attack modeling,
- dynamic game-theoretic interaction,
- predictive compensation in sampled-data control systems.

By integrating these perspectives, the thesis seeks to better understand how adversarial signal distortion can influence the stability and performance of controlled electromechanical systems and how predictive countermeasures can reduce the resulting risks.

1.2 Research Objectives

Motivated by the vulnerabilities of cyber–physical control systems to adversarial manipulation of feedback signals, this thesis investigates the dynamic interaction between malicious signal distortion and defensive control strategies in electromechanical systems. In particular, the work focuses on discrete-time observer-based control architectures for brushless DC (BLDC) motor drives, where manipulation of measured signals may influence the closed-loop dynamics of the physical system.

The primary objective of this research is to analyze how adversarial distortions of feedback signals can affect the stability and physical behavior of controlled electromechanical systems and to develop defensive mechanisms capable

of mitigating these effects. To achieve this goal, the thesis pursues the following specific objectives.

First, the work investigates adversarial interaction in discrete-time observer-based BLDC control systems. The analysis focuses on how malicious manipulation of measured signals propagates through the observer and control loop and influences the resulting closed-loop system dynamics.

Second, the thesis analyzes the possibility of resonant excitation arising from sampled bias injection in discrete-time systems. Particular attention is given to periodic or structured distortions of measured angular velocity and their interaction with the natural modes of the electromechanical system.

Third, the relationship between innovation residual bounds and electromechanical stress is examined. While residual-based monitoring schemes are widely used for attack detection, bounded residual signals do not necessarily imply bounded physical stress or mechanical oscillations. The research therefore investigates how adversarial signal distortion may lead to amplified electromechanical responses even when estimation residuals remain within nominal limits.

Fourth, a predictor-based anticipatory compensation strategy is developed to mitigate the effects of adversarial distortion. The proposed approach estimates future attack signals and introduces compensatory actions intended to restore nominal closed-loop behavior.

Fifth, the interaction between attacker and defender strategies is formalized within an asymmetric Stackelberg game-type framework. In this formulation, the defender anticipates potential attacker actions and designs compensatory strategies accordingly, while the attacker attempts to influence the system through distortion of feedback measurements.

Finally, the theoretical developments are validated through discrete-time simulations of observer-based BLDC motor control systems. These simulations illustrate the dynamic effects of adversarial signal distortion and demonstrate the performance of the proposed anticipatory compensation strategy.

To summarize, the objectives of this research are as follows:

1. Investigate adversarial interaction in discrete-time observer-based BLDC control systems.
2. Analyze resonant excitation caused by sampled bias injection in feedback signals.
3. Examine the relationship between innovation residual bounds and electromechanical stress.
4. Develop a predictor-based anticipatory compensation strategy.
5. Formalize the interaction within an asymmetric Stackelberg game-type framework.
6. Validate the proposed concepts through discrete-time simulations.

1.3 Thesis Statement

This thesis addresses the problem of adversarial manipulation of feedback signals in discrete-time cyber–physical control systems and its potential impact on the dynamics of electromechanical processes. In particular, the work focuses on observer-based control architectures applied to brushless DC (BLDC) motor drives, where distortion of measured signals may alter the effective closed-loop dynamics of the system.

The central thesis of this work is that discrete-time observer-based cyber–physical systems possess a structural vulnerability to adversarial excitation when feedback signals are manipulated in a manner that interacts with the natural modes of the controlled process. Under certain conditions, structured distortions of sensor measurements may act as a form of parametric excitation capable of producing resonance-like amplification of electromechanical responses.

Such effects may arise even when the innovation residual of the observer remains bounded, thereby challenging the assumption that residual-based monitoring alone is sufficient to ensure safe system operation.

To address this vulnerability, the thesis proposes an anticipatory defense mechanism based on predictor-driven compensation of distorted measurements. By estimating potential adversarial actions and applying compensatory adjustments to the feedback signal, the defender can disrupt the dynamic coupling between adversarial excitation and the physical system dynamics. This unilateral anticipatory strategy reduces the effectiveness of resonant excitation mechanisms and helps restore the nominal behavior of the controlled system.

The interaction between attacker and defender strategies is further interpreted within a hierarchical strategic framework resembling an asymmetric Stackelberg game. In this formulation, the defender anticipates possible attacker actions and designs compensatory responses accordingly, while the attacker attempts to influence the system through distortion of feedback signals.

Through analytical development and discrete-time simulation studies of observer-based BLDC control systems, this thesis establishes both the theoretical foundations and practical evidence for the proposed anticipatory defense approach. The results contribute toward the development of more robust security architectures for cyber–physical systems, in which dynamic system behavior and strategic interaction between adversarial agents are explicitly taken into account.

In summary, the thesis demonstrates that adversarial signal distortion can induce resonance-like amplification in discrete-time observer-based cyber–physical systems and shows that anticipatory compensation strategies can effectively mitigate this vulnerability.

1.4 Research Framework

The proposed research effort is limited by simulation and modeling approaches due to the necessity of establishing and verifying operational principles of introducing interactivity into cyber-attack scenarios. While practical implementation in hardware is crucial for final deployment, the conceptual development of the interactivity approach between the adversarial agent and the Cyber-Physical System (CPS) under attack logically precedes actual hardware realization. The validity of the developed models is scrutinized in rigorous verification tests, designed to confirm the consistency of the model's operational responses to external disturbances and parameter variations.

1.4.1 Baseline System Architecture

As a CPS to be attacked, the Brushless Direct Current (BLDC) motor driven by a Kalman filter and controlled by a PID controller is selected as a baseline system. The reasons for this selection are:

- The highly dynamic nature of such a system, which allows speed variation in a wide range, thus providing feasible room for interactive activities from the attacker side.
- The potential possibility of connecting to cyberspace for operational needs (e.g., outside-activated speed control of a self-driving vehicle), which makes such scenarios practically viable.
- The extensive use of BLDC motors in robotics as well as industrial schemes (e.g., engines for centrifuges); this underlines the importance of potential attack schemes in the current industry.
- The appreciable level of existing mathematical descriptions of the control schemes (involving BLDC motor, PID controller, and state observer); this

allows us to rely on existing analytical tools for in-depth exploration of algorithmic manipulations within the attack.

Within this thesis, the operation of the BLDC motor is governed by a linear model described by linear state equations. All nonlinear effects are assumed to be negligible, and their possible consideration is left for future work.

1.4.2 Control Loops and Attack Surface

A Kalman filter is used as an optimal state observer for BLDC motor operation. The filter takes the winding's operating voltages and torque as inputs. Based on electromagnetic interactions, the motion of the rotor is calculated via state equations, yielding estimated state variables: the rotor's spatial position and its angular velocity.

The filter output feeds two distinct control loops:

- **Internal Control Loop (Motor Drive):** Estimated values of the rotor's angular position are directed to the inverter to facilitate timely polarity switching (commutation).
- **External Control Loop (Speed Control):** Estimated values of the rotor's angular velocity are directed to a PID controller to maintain the required speed via applied voltages and supplied currents. This loop constitutes the primary connection point for remote control centers via a cyber link.

The attacker is assumed to be able to connect to both feedback loops. However, due to the external feedback loop's connection to cyberspace for remote commands, it is considered the more readily accessible and, thus, the primary target for the attacks considered in this thesis. Access to the internal feedback loop, while feasible via existing back-doors or hardware/software Trojans, is considered a lower priority attack vector in this work.

1.4.3 Assumptions for Adversarial and Defensive Agents

A number of assumptions are adopted for the scenarios under consideration to be practically viable, covering both the attacker and the defender in this interactive cyber-physical setting.

Attacker Assumptions

For the attacker, the following capabilities are assumed:

- The attacker is able to enter the connection within the control feedback loop and fully control the data flow in it, including substitution of variable values and time stamps.
- The attacker is able to analyze the data and engage machine learning tools for sophisticated data manipulation.
- The attacker is able to turn the attack ON and OFF at any time moment, facilitating studies of transient effects.
- The attacker may have limited knowledge about the structural features of the system under attack but can gain the required knowledge by analyzing the system's responses to induced external disturbances.

Defender Assumptions

For the defender, the assumptions are as follows:

- The defender is fully aware of the attack as well as all the manipulations with the data and re-connections in the circuits made by the attacker.
- The defender is able to analyze all the data and engage machine learning tools to counter the data manipulation made by the attacker.

- The defender's objective is not to escape the attack but rather to negate its impact and provide system operational consistency under the attack conditions (i.e., a resiliency approach).
- The defender needs to gain knowledge about the attacker's potential, specifically estimating the attacker's capabilities in forecasting the defensive responses.

1.4.4 Interactivity and Goals

The issues of anomaly detection in this context become relevant in the frame of learning the opponent's capabilities rather than merely identifying their specific moves. The task for the defender is to develop higher accuracy in predicting steps to be taken by the attacker to negate those, thus providing operational functionality for the system under attack.

Overall, the potential benefits of interactivity via machine learning tools are sought within a three-way interconnection:

- **Attacker Goal:** Gaining control to guide the system into the desired state of increased vulnerability (e.g., instability or accelerated wear).
- **Defender Goal:** Negating the impact of the attack on-the-fly and maintaining system resiliency.
- **System Goal:** Automatically engaging relevant mechanisms of sustainable operation under adversarial conditions.

1.5 Key Challenges

The proposed framework introduces several theoretical and practical challenges associated with secure control of electric motor drives under adversarial manipulation. These challenges arise from the interaction between discrete-time control

dynamics, multiplicative signal distortion, and the strategic behavior of an intelligent attacker. The following issues define the central technical difficulties addressed in this work.

First, the implementation of discrete-time resonance conditions under multiplicative distortion presents a fundamental analytical challenge. Unlike classical disturbance models that assume additive perturbations, the considered adversarial mechanism alters the effective system parameters through multiplicative bias injection. This modification changes the closed-loop state transition matrix and may shift the eigenvalue spectrum toward instability. In the absence of a defensive mechanism, certain eigenvalues of the attacker-modified system matrix can satisfy resonance conditions that amplify oscillatory behavior and degrade system stability.

Second, maintaining reliable control performance under adversarial conditions is a key requirement for cyber-physical systems. Electric motor drives operate with strict timing constraints and tight stability margins. When an attacker introduces systematic bias into the control loop, the resulting distortion propagates through the discrete-time dynamics and may lead to degraded tracking performance, oscillations, or loss of controllability. Ensuring continued operation despite these disturbances requires the controller to actively detect and counteract dynamic distortions while preserving the original control objectives.

Third, achieving prediction-based divisional compensation introduces additional complexity in both modeling and implementation. The defender must estimate the distortion introduced by the attacker and generate a counter-injection signal that negates its effect at each sampling instant. Perfect compensation is achieved only when the defender accurately predicts the attacker's bias for every sampling cycle, which requires precise modeling of the attacker's influence on the system dynamics and minimal prediction error. Any mismatch between predicted and actual distortions may allow residual resonance effects to persist.

Finally, establishing an asymmetric interaction model between attacker and

defender is necessary to capture the strategic nature of this problem. Traditional security formulations often assume additive payoff structures or symmetric influence over system variables. In contrast, the present framework considers a divisional compensation mechanism in which the defender neutralizes multiplicative distortions introduced by the attacker. This leads to inherently asymmetric interactions between the two agents and requires new modeling approaches that depart from standard additive formulations commonly used in cyber-physical security literature.

Addressing these challenges is essential for enabling resilient control of electric motor drives subject to adversarial manipulation and for developing a systematic framework for counteracting parametric resonance induced by cyber attacks.

1.6 Novel Contributions

This dissertation presents a comprehensive investigation of cyber-attack vulnerabilities in closed-loop controlled Brushless DC (BLDC) motor systems operating as Cyber-Physical Systems (CPS), with a Kalman filter serving as the state estimator. The research establishes a systematic taxonomy of bias injection attacks and develops corresponding defense mechanisms. The principal novel contributions of this work, which constitute the foundation for thesis defense, are enumerated below:

1.6.1 Systematic Attack Taxonomy and Characterization

1. **Probing Mode Attack Framework:** Established a methodological framework for low-impact reconnaissance attacks that enable adversaries to gather system intelligence while maintaining stealth. Two specific probing variants were implemented and characterized: (i) double-step function bias injection, and (ii) linearly increasing bias injection. This framework provides

foundational understanding of adversarial information acquisition strategies in CPS environments.

2. **Current Drainage Attack Classification:** Developed and verified a comprehensive taxonomy of current drainage attacks based on saw-function modulation parameters, including:

- Characterization of damage mechanisms through both mechanical wear (via rotor speed ripples) and electrical stress (via prolonged high-current surge overlap)
- Identification of the relationship between modulation depth ($\Delta\chi_{\text{saw}}$) and damage mode: large-amplitude modulation maximizes mechanical wear, while small-amplitude modulation with deep-leveled saw functions maximizes electrical damage
- Discovery and quantification of the asymmetry parameter (K_S) effect on attack signatures, demonstrating that fully asymmetric triangular saw teeth ($K_S \approx 0$) produce proportional current drainage reproduction, while symmetric teeth ($K_S = 1$) generate harmonic-free, stealthier attack profiles

3. **Voltage Hopping Attack Discovery:** Identified and characterized a novel attack modality achieving high-frequency, high-amplitude voltage manipulation (± 500 V jumps) at frequencies exceeding the RL circuit cutoff frequency ($f > f_c$) with minimal effect on observable state variables (currents, speed, position). The critical innovation lies in demonstrating:

- Achievement of apparent system equilibrium despite severe voltage excursions
- Exploitation of impedance shift and transient stress mechanisms above cutoff frequency
- Equilibrium state occurrence at modulation frequency of 2.1875 kHz,

providing adversaries with enhanced stealth while maintaining destructive potential.

1.6.2 Pulsation-Based Attack Family and Dynamic Resonance Exploitation

1. **Discovery of Novel Resonant Attack Mechanisms:** Demonstrated and validated three novel Resonant Attack Mechanisms—Voltage Hopping, Induced Pulsation, and Hyper-Spiking—which exploit the system’s dynamic model by exciting its internal resonant frequencies. The critical innovation lies in:

- Establishing the continuum theory of pulsation-based threats progressing from transient resonant activation (Induced), through prolonged resonance locking (Extended), to phase-aligned burst amplification (with Hyper-spiking).
- Characterizing the variations, such as the Extended Pulsations version, which reveals synchronization patterns (fundamental and sub-harmonic) for improving covertness.
- Identifying voltage breakdown failure modes (up to 6000 V hyper-spikes) as primary threat vectors.

2. **Characterization of Novel Temporal Vulnerability Artifacts:** The analysis of the resonant attack mechanisms led to the identification and detailed characterization of three key temporal vulnerability artifacts that define the system’s transient response to adversarial manipulation:

- The **Initial Impulse Syndrome**, defining the large transient estimation error immediately following attack initiation.
- The **Attack Withdrawal Syndrome**, quantifying the system’s delayed and oscillatory recovery upon attack termination.

- **Attacks with Interruption/Resuming Sequences**, which exploit the combined and accumulating impact of the impulse and withdrawal syndromes to induce chronic instability.

1.6.3 Defense Architecture and Countermeasure Development

1. **Linear Defense Strategy Implementation:** Developed and validated first-layer defense mechanism using linear-dynamic predictor operating parallel to main control loop. Demonstrated capabilities include:

- Real-time reconstruction of expected plant dynamics under legitimate operating conditions.
- Achieved better than 95% stability retention for the highly specialized Current Drainage modality, specifically under conditions of deep-level low modulation depth sawtooth distortion through anticipatory compensation of angular speed estimate distortions.
- **Successful defense** against the **Induced Pulsations attack** modality, demonstrating better than 95% accuracy in attack detection and signal neutralization across varying interference frequencies.
- Successful mitigation of attack withdrawal syndrome through preemptive distortion compensation.
- Computational efficiency suitable for resource-constrained embedded controllers.

2. **Asymmetric Stackelberg Game Formulation:** Established defender advantage in asymmetric information game where defender adopts follower position with full transparency of attacker actions. Demonstrated:

- Defender capability to counteract saw-function modulation attacks across depth and frequency variations.

- Limitations in defending against attack initiation impulse, establishing requirement for dedicated anomaly detection algorithms.
 - Framework for systematic evaluation of defense effectiveness under various attack scenarios.
3. **Signature-Based Detection Framework:** Compiled comprehensive attack signature database enabling pattern recognition approaches to identify:
- Current drainage patterns as functions of saw-function asymmetry (K_S).
 - Voltage hopping characteristics at resonant frequencies.
 - Pulsation modulation harmonics and phase relationships.
 - Hyper-spiking temporal markers and amplitude distributions.

1.6.4 Methodological Contributions

1. **Comprehensive CPS Vulnerability Assessment Framework:** Established systematic methodology progressing from probing through full-scale exploitation, demonstrating:
 - Attacker decision-making trade-offs between stealth and information acquisition.
 - Vulnerability quantification through sustained current manipulation.
 - Dual-pathway destruction analysis (mechanical vs. electrical stress).
2. **Multi-Domain Attack Impact Analysis:** Developed integrated evaluation framework spanning temporal, frequency, and phase domains, enabling:
 - Simultaneous assessment of mechanical, electrical, and thermal damage pathways.
 - Quantification of stealth-effectiveness trade-offs across attack parameter spaces.

- Identification of critical frequency regimes (sub-harmonic, fundamental, super-harmonic, cutoff).
3. **Simulation-Based Validation Methodology:** Established comprehensive modeling and simulation framework for CPS security research, verified across:
- Open-loop and closed-loop control schemes.
 - P-controller and PID-controller configurations (with initial focus on P-controller to isolate integration/differentiation effects).
 - Position-sensorless BLDC motor operation under Kalman filter drive.

1.6.5 Practical Security Implications

The research establishes several critical insights for CPS security practitioners:

1. **Detection Strategy Guidance:** Identified need for integrated monitoring beyond static anomaly detection, including:
 - Continuous spectral analysis for harmonic detection.
 - Inter-spike interval variance monitoring.
 - Phase-coherence tracking within feedback loops.
 - Frequency-domain residual diagnostics for early resonance indicators.
2. **Mitigation Recommendations:** Established design principles for resilient controllers:
 - Adaptive damping mechanisms to prevent resonance build-up.
 - Phase randomization to interrupt synchronization attacks.
 - Dynamically adjustable threshold systems responsive to attack.

3. **Threat Model Refinement:** Demonstrated that CPS vulnerabilities extend beyond logical/parametric weaknesses into dynamic resonance and temporal coherence domains, requiring fundamental reconsideration of security architectures in feedback-regulated systems.

1.6.6 Summary of Contributions

This dissertation advances the state of knowledge in CPS security through: (1) systematic characterization of six distinct attack modalities against BLDC motor control systems; (2) discovery of three novel Resonant Attack Mechanisms and characterization of the resulting Temporal Vulnerability Artifacts; (3) development and validation of a linear defense architecture demonstrating better than 95% stability retention against Current Drainage and Induced Pulsations attacks; (4) establishment of signature-based detection framework; and (5) formulation of comprehensive threat model spanning mechanical, electrical, and control-theoretic damage pathways. These contributions provide both theoretical foundation and practical guidance for securing feedback-controlled cyber-physical systems against sophisticated adversarial manipulation.

1.7 Significance of the Contributions

The contributions of this research extend across theoretical, methodological, and practical dimensions of cyber-physical system security. By focusing on electric motor drives as a representative control-critical infrastructure, the work establishes new connections between control theory, cyber-physical security, and adversarial system modeling.

From a theoretical perspective, this work moves beyond the conventional assumption of additive false data injection disturbances. Instead, it introduces a multiplicative attack model in which the adversary alters the effective gain structure of the control loop. Such manipulation induces parametric excitation within

the closed-loop dynamics, potentially generating resonance effects that are not captured by traditional additive disturbance models. A central theoretical insight developed in this research is the existence of a stealth gap, where bounded residual signals in standard monitoring mechanisms do not necessarily imply bounded physical stress in the electromechanical system. This observation highlights a critical vulnerability in commonly used detection frameworks. To address this limitation, the proposed framework introduces a divisional prediction mechanism that mathematically reduces the effective distortion introduced by the attacker in real time through counter-injection.

From a methodological standpoint, the research establishes an interdisciplinary framework that integrates adversarial modeling with discrete-time control analysis. The interaction between the attacker and defender is modeled through an asymmetric Stackelberg formulation, in which the defender anticipates the strategy of the leader and implements a compensatory response. This formulation captures the realistic asymmetry present in cyber-physical systems where defensive mechanisms must react to strategic adversaries. In addition, the work develops a discrete-time bias modeling framework capable of representing multiplicative interference within the control loop. This approach enables the formulation of predictive defense mechanisms that combine principles from control theory with anticipatory responses to adversarial manipulation, thereby extending traditional reactive security paradigms.

From a practical perspective, the results of this work contribute directly to the protection of hardware systems based on brushless DC motor drives. Such drives form a fundamental component of modern cyber-physical infrastructure, including robotics platforms, electric vehicles, and industrial automation systems. By mitigating the effects of adversarial distortions in the control loop, the proposed defense mechanism reduces torque ripple and prevents long-term mechanical degradation such as bearing wear and structural fatigue. The experimental validation performed in this research demonstrates measurable reductions in cumulative electromechanical stress, illustrating the practical feasibility of the

approach and its relevance for improving the resilience of control-critical hardware systems.

1.8 Thesis Organization

The remainder of this thesis is organized as follows: Chapter 2 provides an introductory overview of various cyber-attacks against Cyber-Physical Systems (CPS). Chapter 3 formulates the research problem based on the literature reviewed in Chapter 2. The methodology proposed to address the formulated research questions is then presented. Specific models for simulations are suggested, based on the control schemes of a BLDC motor with a Kalman filter state estimator as a driver. Chapter 4 presents experimental results on various attack scenarios. The proposed Defense Architecture is verified in a simulation experiment at the Linear Defense Module level, serving as a first line of defense. In Chapter 5, an analysis of the results obtained in Chapter 4 is presented from a general perspective, as well as through the consideration of Game Theory. Finally, Chapter 6 concludes the manuscript with the formulated major conclusions. Furthermore, the Future Work directions are outlined.

Chapter 2

Literature Review

To contextualize the proposed research and establish a clear foundation for the contributions of this thesis, this chapter presents a comprehensive literature review. The review is strategically organized to first introduce the fundamental concepts of Cyber-Physical Systems (CPSs) and the specific operational domain of motor control. Subsequently, we conduct a detailed analysis of existing works concerning cyber-attack modeling against state estimators and control systems, concluding with a survey of contemporary defense and resilient control architectures. This structured analysis highlights current gaps in the literature that this thesis aims to address.

2.1 Integrity Attacks Against CPS

The widespread adoption of digital control systems in industrial settings has opened the door to digital security threats that can be harmful to industrial infrastructures. Recent systematic reviews of the field provide an updated taxonomy of threats and defenses, helping to classify the evolving landscape of CPS vulnerabilities and countermeasures [16]. To ensure the safe operation of industrial systems with digital control, a certain minimum level of security systems must be in place, of which cyber-security measures are an essential part.

From a control-theoretic viewpoint, designing for security and resilience in networked control systems involves a focus on formal methods that can provide theoretical guarantees for attack detection, resilient state estimation, and secure controller synthesis [17]. Attackers of ICS may seek to disrupt industrial processes, reduce efficiency, or take control of various parts of the system or of the system as a whole, thus jeopardizing the process itself as well as its operational safety, especially if the attacker drives the system into unstable or risky states [18]. As a defense against these threats, techniques such as intrusion detection [19], attack dissemination, and con-

trol regaining methods [20] are commonly used. The relevant literature on attacks against CPSs and related defensive strategies has been extensively reviewed and is summarized in Table 2.1.

Duo *et al.* (2022) presented a survey of state-of-the-art results on cyber attacks on CPS [21]. The authors distinguished between time-driven and event-driven systems. It is worth noting here that the integration of both time-driven and event-driven systems constitutes the concept of interactivity, which the current thesis suggests as an area of new exploration. In this context, the dynamics of the system and its responses to external perturbations may offer attackers possibilities to drive CPS into desired states of increased vulnerability. Defense strategies in this case need to account for those possibilities, and therefore, defensive development requires research and in-depth study of opportunities for such interactive attacks. Duo *et al.* (2022) distinguished three types of attacks: those on availability, integrity, and confidentiality of the system [21]. Within the perspective of the present thesis work, attacks on integrity are of particular relevance, as they target the correctness of the execution of physical processes. The flow of physical processes provides CPS operation according to system control theory, as CPS is a physical system controlled by industrial control technologies. Stemming from system control analysis, the study of cyber attacks has perspectives in two ways: for the attacking and defensive sides. The attacker's outlook is to identify weaknesses in CPS architecture and to formulate the attack approach. On the other hand, the defender's task is to design an early detection method to identify the attack and/or to develop efficient control methods to defy the attacks. The present thesis work adopts a similar approach, as it is currently a generally accepted way of conducting cybersecurity research. In the context of control theory, a cyber-physical system (CPS) can be modeled as a discrete-time system, where the state of the system at time k is denoted by x_k . In this setting, the behavior of the system can be captured by the following set of control equations:

$$\begin{cases} x_{k+1} = Ax_k + v_k \\ y_k = Cx_k + w_k \end{cases} \quad (2.1)$$

Here, A and C are matrices that describe the dynamics and measurements of the system, respectively. The vectors v_k and w_k represent process noise and measurement noise, respectively, and are assumed to be uncorrelated zero-mean Gaussian noises with covariances Σ_v and Σ_w , respectively [21].

Integrity attacks on cyber-physical systems (CPS) can target the sensor measurements data flow and/or control commands flow. Specifically, if we denote the attack vector at time k as a_k , then the actual measurement under attack is given by $y_k^a = y_k + a_k$, where $y_k^a \in \mathbf{R}^m$. Similarly, in the case of attacks on control commands flow, we have $u_k^a = u_k + a_k$, where u_k^a and u_k represent the control inputs when attacks are present and absent, respectively [31]. Moreover, when stochasticity is present in the system, a discrete-time stochastic model can be used to

Table 2.1: Summary of the selected attacks/defense strategies for CPSs.

Reference	Vulnerability	Attacks	Defenses
Kriaa <i>et al.</i> (2015) [18]	system instability	the attacker drives the system into unstable or risky states	intrusion detection [19], attacks dissemination as well as control regaining methods [20]
Duo <i>et al.</i> (2022) [21]	CPS	availability, integrity, and confidentiality of the system	(1) Attack detection; (2) Secure control;
Angueira <i>et al.</i> (2022) [22], Wu <i>et al.</i> (2018) [23]	wireless communication channels	false data injection attack via communication layer	maintain information integrity, relying on wiretap Gaussian/Fading model [24]; extra authentication and encryption tools [25]
Wang and Yang (2019) [26]	closed-loop Cyber Physical Systems (CPS) with reference signals	stealthy attack employing protocol/Internet protocol (TCP/IP) connections by injection of false sensor data	eavesdropping countermeasures, such as operating under stable conditions
Jablonski <i>et al.</i> (2019) [27]	TCP port of Raspberry PI controller	via TCP port of Raspberry PI controller switching input and output port connectivity, then substituting the reference speed for operated DC motor	restricting the pigpiod to only allow control from certain hosts on the local network
Mo <i>et al.</i> (2010) [28]	the integrity of the state estimator	hijacking data for selected subset of sensors and sending altered readings	observe full set of all the estimation biases
Keller and Darouach (1997) [29]	random bias influence	false data injection	Integrated type of approach: Optimal two-stage Kalman filter (OTS-KF)
Tummala and Inapakurthi (2022) [30]	security of power system	false data injection, data replay attack, denial of service (DoS), scaling, and ramp attacks	an optimal two-stage Kalman filter (OTS-KF) for simultaneous state and cyber-attack estimation [30]
Jablonski and Wijesekera (2019) [27]	(i) speed control, (ii) components, (iii) torque, (iv) over-rotation, (v) overheating, (vi) PWM	pin-control attacks disrupting PWM, denial of service (DoS), false data injections, sensor attacks, and/or attacks against operating controller's software	Engage Motor Threat Model (MTM) for (1) Identifying kill chains and then (2) design additional security controls to ensure the integrity, availability, and confidentiality

describe the system behavior [32]. This model takes the form:

$$\begin{cases} x_{k+1} = Ax_k + \chi_B(Z_k)Bu_k + v_{k+1} \\ y_k = Cx_k + w_{k+1}, \quad k = 0, 1, \dots, T-1 \end{cases} \quad (2.2)$$

Here, $x_k \in \mathbf{R}^m$ is the system's state, $u_k \in \mathbf{R}^m$ is the control input, $y_k \in \mathbf{R}^p$ is the observation output, $\chi_B(Z_k) \in [0, 1]$ is the DoS attack sequence that disrupts the control packets from reaching the actuator, while Z_k is related to the internal state of the attacker. In presenting the equations (2.2) here, the parameter $\chi(Z_k)$ of [32] has been replaced by $\chi_B(Z_k)$ to avoid overlap with the symbolic notation of χ for the distortion coefficient used in this thesis and our published and submitted materials. Otherwise, the notation of [32] is preserved. It is worth noting that the interpretation of the equations (2.2) by Befekadu *et al.* (2015) [32] is in the context of the availability attack, specifically the DoS attack, not the integrity attack. Mathematically, this is supported by the fact that the term $\chi_B(Z_k) \in [0, 1]$ takes the value of $\chi_B(Z_k) = 0$ when the control packets are disrupted from reaching the actuator (i.e., the attack is on), and the value of $\chi_B(Z_k) = 1$ when the packets reach the actuator (i.e., there is no attack present). The proposition of this thesis is that the attack presented by the equations (2.2) may be transformed into an integrity attack if the values of $\chi_B(Z_k) \in \mathbf{R}^r$, i.e., if those values are made to be real numbers. In this case, instead of disrupting the packet flow, we would obtain distortion of values in the packet flow, thus achieving false data injection mode, which amounts to an integrity attack against CPS.

Moreover, the proposition may be extended to include all parts of the equations (2.2) by distorting the term with state matrix A, as well as the term with measurement matrix C. Generalized form of such an integrity attack may be represented by the following system of equations:

$$\begin{cases} x_{k+1} = \vec{\chi}_A(Z_k, S_k)Ax_k + \vec{\chi}_B(Z_k, S_k)Bu_k + v_k \\ y_k = \vec{\chi}_C(Z_k, S_k)Cx_k + w_k, \quad k = 0, 1, \dots, k_{max} \end{cases} \quad (2.3)$$

where $\vec{\chi}_A(Z_k, S_k)$, $\vec{\chi}_B(Z_k, S_k)$ and $\vec{\chi}_C(Z_k, S_k)$ are the attacking distortion vectors against state A, actuator B and measurement C matrices, Z_k and S_k are the states of the attacker and that of the system at a time index k, k_{max} is maximum time index of observation. For implementing each of the attacking vector there is a need for ability of the attacker to make a respective connections and rewiring in the circuits. Apart from technical difficulties of implementing all of those, there is increased risk of detection by the defending party. Therefore, it may be advantageous to limit the attack's aspirations to a single target, having in mind the need to avoid detection and keeping the attack in stealthy mode. Having that, the aspiration of the present thesis is set to be limited to the integrity attack against the data flow of state variables estimations by the system's observer, assumed to be present in the system architecture. This aspiration is represented below by a simplified version of equations (2.3), as follows:

$$\begin{cases} x_{k+1} = \vec{\chi}_A(Z_k, S_k)Ax_k + Bu_k + v_k \\ y_k = Cx_k + w_k, \quad k = 0, 1, \dots, k_{max} \end{cases} \quad (2.4)$$

As it is seen, the vector $\vec{\chi}_A(Z_k, S_k)$ here depends not only on the state of the attacker Z_k , but also on the state of the system S_k . It means that the attacker is reflecting on the effects of the attack on the CPS and is adjusting the parameters of the attack accordingly. The ability of the attacker to adapt on-the-fly the parameters of the attack is equivalent to creating an additional feedback loop designed to guide the attacked CPS in some predefined state by attacker's choice. Such systems are of particular interest for investigating potential threats and developing appropriate countermeasures, which provides the justification for the research effort presented in this thesis.

2.2 Communication layer security

Security issues in the communication layer are addressed by various research groups focusing on wireless communication channels [22, 23]. This goes despite current domination of wired systems in factory environments for its robustness in noisy and complex conditions of operation. In addition to that, wired channels present a challenging barrier for determined attackers to overcome in the attempts of overtaking the control on the system and/or bringing down the communication system. Nevertheless, wired systems have their limitations, including difficult scalability, resource-consuming maintenance, and lack of flexibility in operation. In contrast to the above, wireless systems come in as a versatile solution in removing severe limitations of the wired architectures, however, this comes at a cost of sacrificing standards in reliability performance and operational security. The last issue becomes of particular importance within the frame of this thesis as wireless channels create additional opportunities for potential attackers to acquire control over the connected to the network CPS. A full range of security vulnerabilities in wireless communications is reproduced herewith in Figure 2.1 from survey of Angueira *et al.* (2022) [22].

Within the context of the present thesis topic a particularly important item in Figure 2.1 is the one associated with the icon "Integrity" and connected to it icon "Man-in-the-Middle" including elaboration note underneath. It signifies integrity attack based on the man-in-the-middle scenario, when the attacker manages to intercept the wireless node (the way to do it is circuit dependent and requires separate consideration in particular cases). As the note underneath the icon suggests, the attacker then gets the possibility of modifying the data and re-sending them

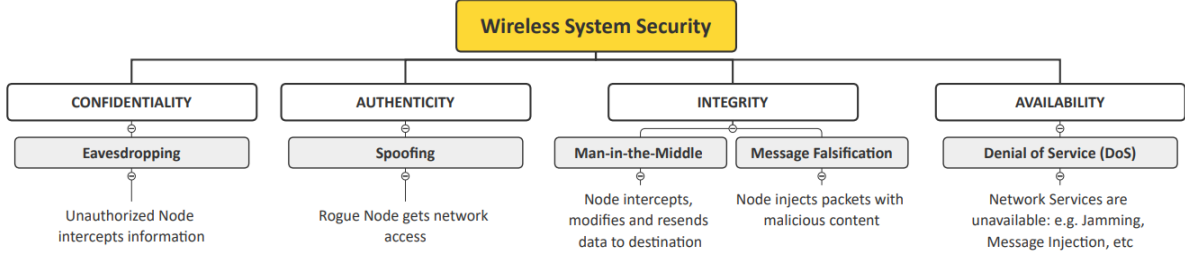


Figure 2.1: Wireless system communication features and targeted attacks [22].

to the destination, thus implementing a false data injection attack. For the present thesis important is the fact of qualifying such a possibility as a realistic one, because this allows to accept the assumption of such a possibility to be practically implementable to be valid and justify the research effort in how to use it with modeling and simulation tools for now, leaving specifics of hardware implementation to the future.

The integrity of CPS in part depends on the capacity of communication channels to provide the accuracy and reliability of the transmitted data. This, in turn, requires communication nodes to maintain legitimate status as being non-compromised by external interference. In the alternative, the nodes subjected to malicious intervention may be compromised [33] and become involved in data modification. Through a compromised node the attacker may alter the data flow integrity in the network as a result of successful malicious attacks.

Among the existing integrity attacks carried out through communication channels, the most relevant within the scope of this thesis is the Man-in-the-Middle attack [34] (also illustrated in Figure 2.1). Such an attack includes the possibility of messages modification, i.e. a compromised node intercepts original messages and modifies it. Generally speaking, a rogue node becomes a source of false messages destined to an authorized node and therefore it is considered to be a vulnerability of information integrity. Generally accepted known countermeasures to maintain information integrity, such as approaches relying on wiretap Gaussian/Fading model [24], as well as additional extra authentication and encryption tools [25], may not necessarily be applicable in case of control circuits of CPS operation, either conceptually or technically, i.e., for sufficiently high speed circuits operations. Therefore, this issue requires further research effort in developing an efficient defensive procedures, including those of attack detection and remedial steps.

2.3 Attacks via TCP/IP connection

Wang and Yang (2019) proposed a stealthy attack methodology against closed-loop Cyber-Physical Systems (CPS) with reference signals, utilizing Transmission Control Protocol/Internet

Protocol (TCP/IP) connections [26]. The paper removes the conservative assumption that the model parameters of CPS are known to attackers and that attackers can modify sensor measurements, making it an effective attack methodology against closed-loop CPS with reference signals. The CPS relies on TCP/IP-based networked control system. The paper also provides a practical functional benchmark platform (refer to Figure 2.2) to implement the proposed methodology for hardware setup and verify it for practically viable scenarios.

Figure 2.2: Block diagram of the benchmark platform for the verification of stealthy attack technology [26].

Among the specific components that may be a target for attacks are electrical motors, which are common in robotics, automation systems, and transportation vehicles. Jablonski *et al.* (2019) demonstrated a procedure in which the attacker connects via the TCP port of a Raspberry PI

controller to a DC motor and switches the input and output port connectivity via an externally initiated command, thus obtaining the possibility to substitute the reference speed for the operated DC motor and gain control over its operation [27]. This further contributes to proving the viability of attacking routes involving TCP/IP connectivity.

2.4 Bias injection attack against state observers

The security of state estimation is a critical sub-field of CPS security, as compromising the system's perceived state can completely undermine its control logic. Comprehensive surveys on this topic detail various attack models targeting sensing and estimation pipelines, including bias injection and replay attacks, as well as corresponding detection and defense strategies [35], with dedicated analyses demonstrating how such attacks can be formally characterized and countered at the estimator level [36].

Another type of attack may include attempts to compromise the integrity of the acting state estimator, for example by hijacking data for selected subset of sensors and sending altered readings [28]. As the Kalman filter gained popularity in a state estimator role, such an attack may be efficient if directed against the Kalman filter [37].

Overall, in the current literature the attacks against state observers are analyzed within Network Control System (NCS) paradigm where the system and the controller with state estimator are separated in space and the connection of two separated parts is implemented via network communication channels. For such architectural designs, the attacker uses network channels to set up Man-in-the-Middle connections and thus to control the data flow either from sensors to the state estimator or from the controller to the plant, or both.

However, NCSs form only part of the industrial infrastructure employing CPSs. Another part, such as self-driving vehicles, industrial robots need to localize sensors, controllers, and state observers at the same location, namely, on board the vehicles or robots, while having such system connected to the remote servers for data collection and monitoring their operational activity. In such settings, the control system operation is maintained with or without connection to the remote server and therefore connectivity to the network is not mandatory. However, advantages of remote data collection as well as the possibility of remote commands for changing the mode of CPS's operation (such as stop, increase or reduce the speed for the vehicles, or change the route or acquire new target for the robots) may still outweigh the risks associated with exposure to potential attacks via cyber space connectivity. Such systems, however, have not yet received adequate research attention.

More generally, the Luenberger Observer control scheme, such as the one shown in Figure

2.3, with a connection to the cloud for data collection is of interest in the above terms of identifying potential vulnerabilities for deceptive type of attacks, such as bias injection. In Figure 2.4 the expected transformation of the system is presented where the attacker's access to the control output line allows transformation of the operating equation into the one accommodating the attacker's induced distortion of the controller signal.

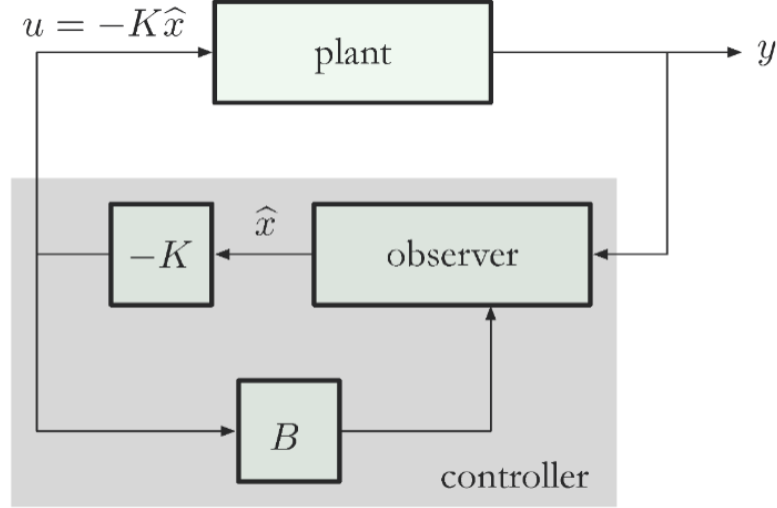


Figure 2.3: Luenberger Observer control scheme.

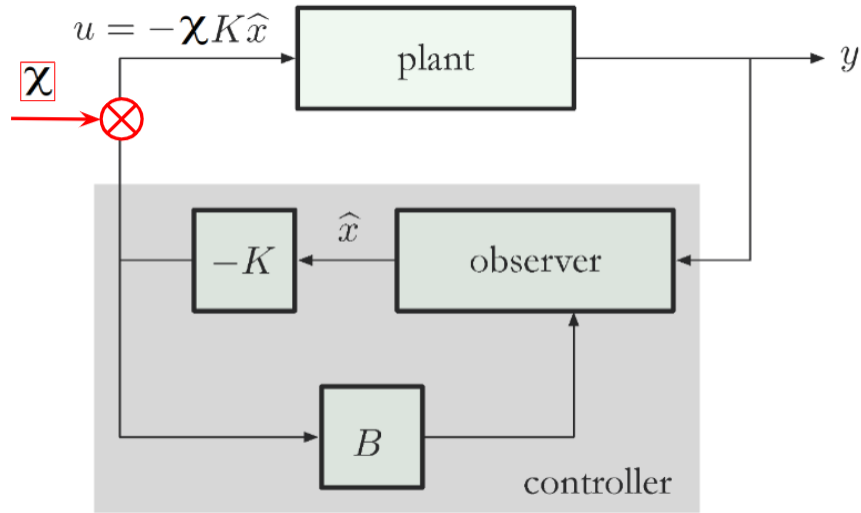


Figure 2.4: Transformation of the controller's signal to the plant by the attacker's induced distortion in Luenberger Observer control scheme.

Similarly, for the Kalman filter used as an optimal observer (see Figure 2.6), the access point to the controller's output line allows the attacker to modify the equation of the control operation

with distorted data as shown in Figure 2.6.

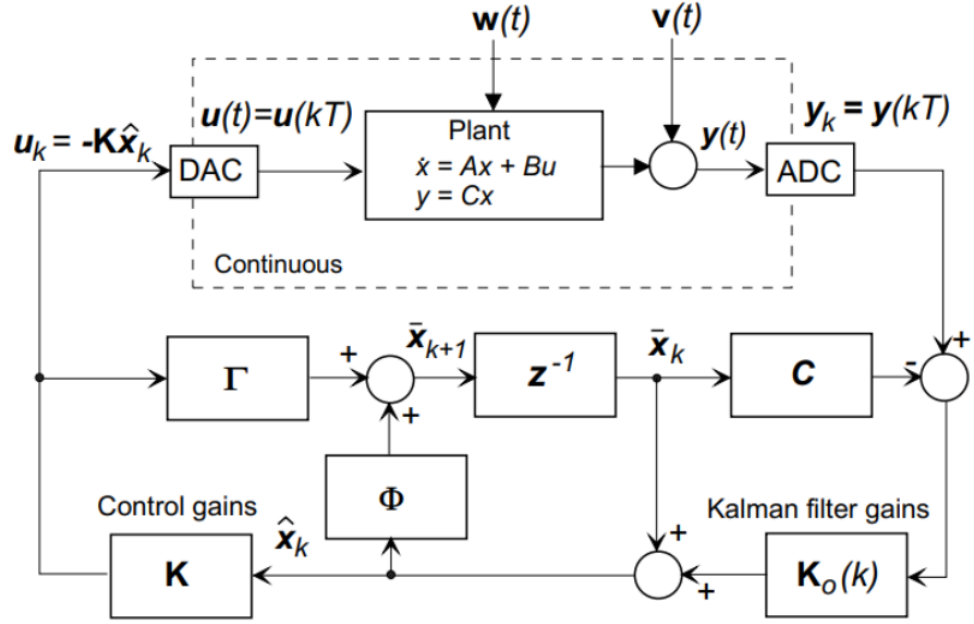


Figure 2.5: A control scheme with Kalman filter as an optimal observer.

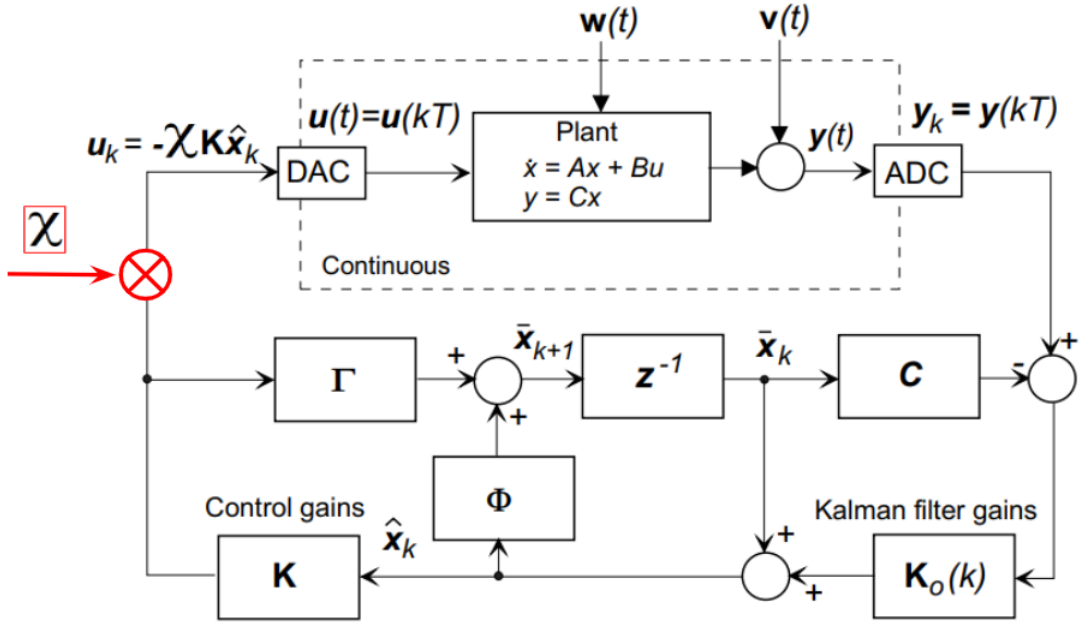


Figure 2.6: Transformation of the controller's signal to the plant with accommodation of the attacker's induced distortion in control scheme with Kalman filter as an optimal observer.

An integrated type of approach was suggested by Keller and Darouach (1997) to control

systems subjected to random bias influence. Their method assumed the possibility of splitting out in the state equation the contribution from the system without bias and the bias component itself. In this way, the possibility was explored to combine two functionalities in a single Kalman filter - one is to estimate the states of the system with no bias, and the second one is to estimate the bias itself [29]. The resulting outcome of such approach was achieving control of the system under random bias, which we may call to be “integrated” in a sense that it is achieved within a single device (Kalman filter), whose algorithm is appropriately modified, but still included three basic steps - initialization, prediction, and update. The newly designed Kalman filter was named the Optimal two-stage Kalman filter (OTS-KF) referring to optimal estimation of both – the system states as well as bias values within the same algorithmic procedure. In this respect, the OTS-KF was considered to be an extension to the Kalman filter where state estimation and bias estimation run in parallel. Moreover, because the bias term’s origin is irrelevant to the processing, and as an option, may have been of an artificial nature, i.e. being part of the false data injection or, in other words, the attack.

Practical application of OTS-KF for cybersecurity of power system was explored by Tumala and Inapakurthi (2022) in which attack detection and defense functionalities were made to be part of Kalman filter state estimation algorithm. For that the Kalman filter algorithm was modified to include an additional stage to result in a so-called optimal two-stage Kalman filter (OTS-KF) for simultaneous state and cyber-attack estimation [30].

In this approach, the biases/cyber-attacks were modeled as unknown inputs in the control system dynamics. Specifically, five types of cyber-attacks were verified: false data injection (FDI), data replay, denial of service (DoS), scaling, and ramp attacks. The synthesized attack data sets were injected into the measurements and estimated using the suggested OTS-KF. To account for possible load variations, the proposed OTS-KF was reformulated to estimate the states and outliers along with the related load variations. The proposed technique was validated on power system models, including two-, three-, and five-area benchmarks. The simulations demonstrated the viability of the proposed technique under various test conditions.

Despite the advantages of the OTS-KF, the efficacy of this approach remains to be verified for systems other than power system models. Anticipated problems for high-speed dynamic systems may include potential convergence issues in real-time operation.

Beyond the OTS-KF, other robust filtering techniques have been developed to address non-Gaussian disturbances characteristic of cyber-physical attack environments. The Maximum Correntropy Kalman Filter (MCKF) replaces the conventional minimum mean-square-error criterion with the maximum correntropy criterion, making it inherently resilient to the heavy-tailed, impulsive noise introduced by many cyber-attacks and thus providing an alternative defense for state estimation [38, 39]. Recent work has further extended this framework to handle specific

attack types such as replay attacks, demonstrating the adaptability of correntropy-based filters to structured adversarial threat models [40].

However, the primary limitation of any Maximum Correntropy Criterion (MCC) filter, including the MCKF, is its dependence on the critical tuning parameter: the kernel bandwidth (σ). This improved resilience comes at the cost of increased parameter tuning complexity and higher computational demands compared to the classical KF, which is a critical consideration in high-speed cyber-physical motor control applications.

2.5 DC motor as an object for attacks

Jablonski and Wijesekera (2019) introduced the Motor Threat Model (MTM) to assist with identifying hardware and software risks in electrical motor systems [27]. Authors analyzed various attack objectives against electrical motors based on system type and provided a set of examples of attack techniques that can achieve the selected objectives. Specific types of induced failures as a result of these attacks include the following: (i) loss of speed control, (ii) wearing down system components, (iii) limiting the produced torque, (iv) over-rotating servo motors, (v) overheating up to catching fire and (vi) disruption of the Pulse Width Modulation (PWM). These failures are achievable via attacks against hardware, such as pin-control attacks disrupting PWM, or via software, such as denial of service (DoS), false data injections, sensor attacks, and exploiting the lack of security controls in the controller's software libraries.

The above modeling classifications were summarized in schematics reproduced from ref. [27] in Figure 2.7 with Motor Threat Model (MTM) attack tree templates for control, data exfiltration, and disrupt objectives. Suggestion of this Thesis to include a state observer as potential vulnerability constitutes the expansion of the attack tree template for control, and it is presented in Figure 2.8.

Similarly, our suggestion is to extend a schematic 2.9 for Motor Threat Model to include the state observer (such as, for example, Kalman filter) to be a potential layer of vulnerability as shown in Figure 2.10.

2.5.1 BLDC motor as an object for attacks

DC motors attracted attention as dynamic systems suitable for cyber-attacks aiming at cyber-physical systems. Moreover, the sensorless drive of BLDC motor has been reported to deliver an efficient control of BLDC motor when employing various versions of Kalman filter for the

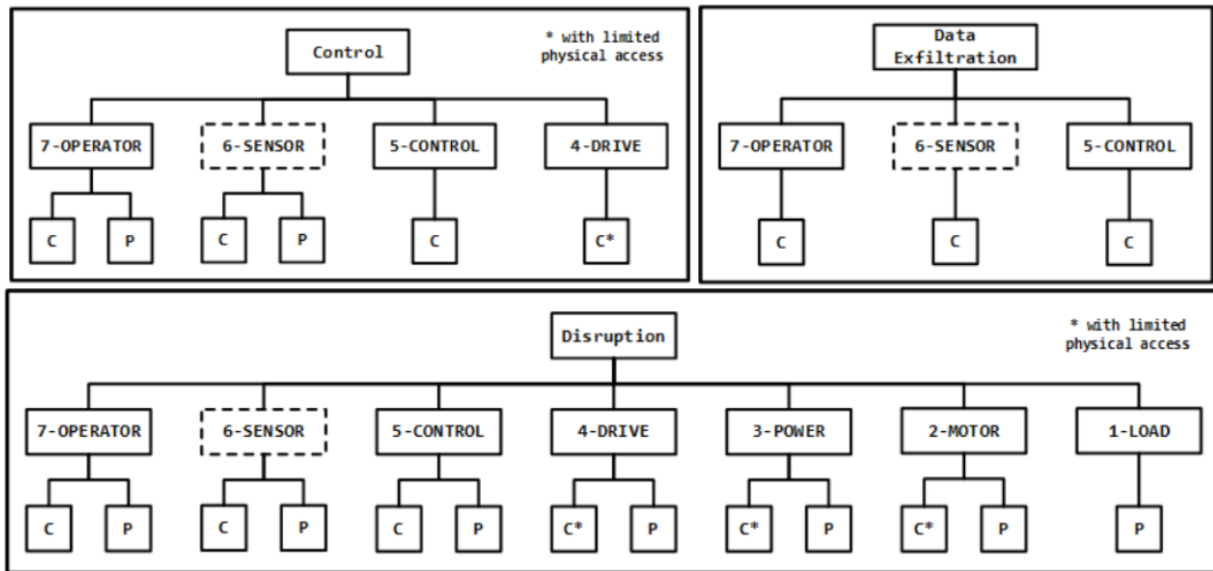


Figure 2.7: Motor Threat Model (MTM) attack tree templates for control, data exfiltration, and disrupt objectives. (Reproduced from ref. [27]).

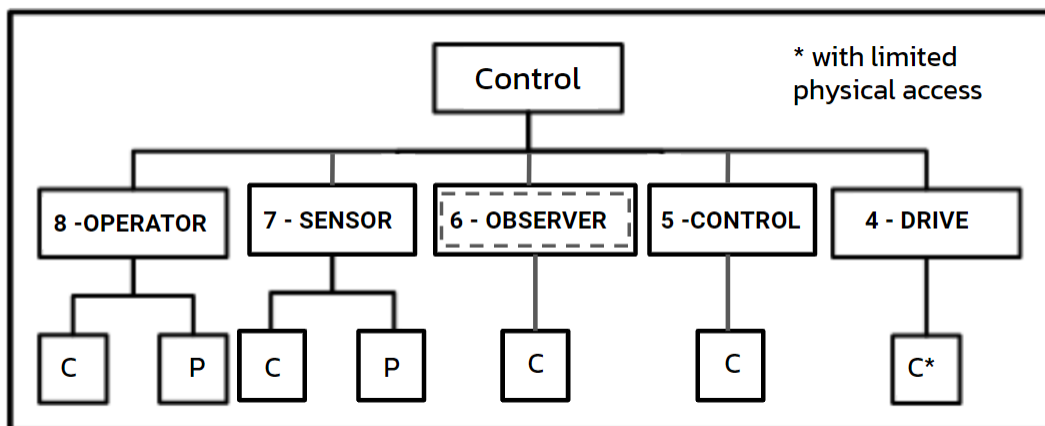


Figure 2.8: Modified Motor Threat Model attack tree template for control objectives (see initial version in Figure 2.7, specifically, in its left top part) with inclusion of a state observer as potential target for attack. (Modified from ref. [27]).

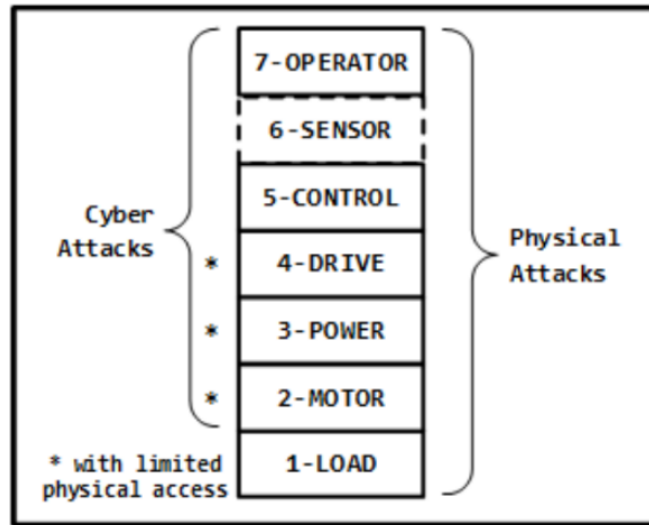


Figure 2.9: The seven Motor Threat Model (MTM) layers of vulnerabilities for the attacks. (Reproduced from ref. [27]).

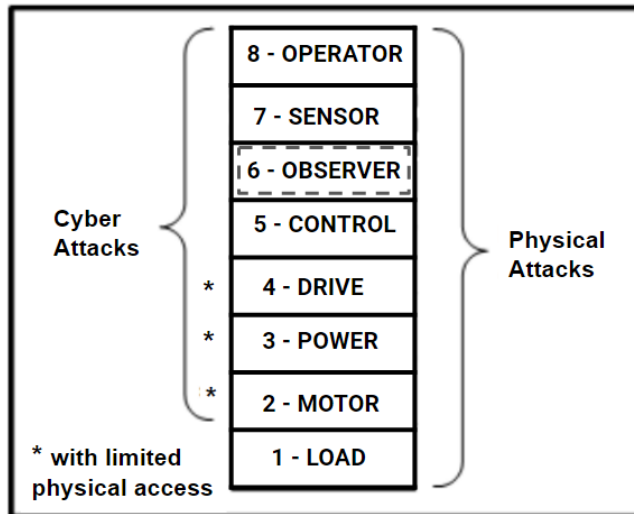


Figure 2.10: Modified layer structure of Motor Threat Model (MTM) to include a state observer as potential layer of vulnerability. (Modified from ref. [27]).

purpose of phase synchronization in the motor's windings [41]-[42]. Some advanced architectures have been reported to achieve intelligent operation of sensorless drive for BLDC motor. Specifically, Sabir et al. (2016) suggested a hybrid fuzzy/PI controller with improved efficiency [43], while disturbance observers have allowed for adaptive velocity estimations [44]. The implementation of the extended Kalman filter has enabled speed and rotor position estimation [45], and sliding mode control with a Kalman filter has also been verified [46]. Applications of BLDC motor control in the aerospace industry continue to be pursued [42]. However, the overall picture is still lacking in its coverage of the dependencies of sensorless control on internal motor parameters, external disturbances, and operating circuit parameters.

2.5.2 Electric vehicle as an object for attacks

The internal networks of modern vehicles are a primary target for attackers, with surveys highlighting ongoing challenges in securing in-vehicle communication protocols like the Controller Area Network (CAN) bus against sophisticated threats, including injection, replay, and masquerade attacks, as well as the countermeasures proposed to address them [47, 48]. Beyond the internal network, the broader attack surface of connected and autonomous vehicles — encompassing V2X communications and Electronic Control Unit (ECU) vulnerabilities — poses additional security risks that demand comprehensive threat analysis and defense frameworks [49].

Electric vehicles (EV) are becoming prevalent in the market in a wide range of applications in the air, on land, and on and under water. Unmanned Aerial Vehicles (UAV) operate in the air and include various types of copters and drones, allowing remote control and/or autonomous flying. Electrical trucks, cars, and bikes are filling the niche of ground transportation. The water domain is accepting models of on-surface and under-surface drones. Many of these vehicles require network connections, such as GPS for location, a link to a remote operator, or an internet connection for data exchange. Electrical motors are used in these vehicles as a source of mechanical force, generating rotational torque to drive the wheels or propellers. Attacking the electric motors of vehicles is therefore an attractive goal for seizing control during operation. Self-driving vehicles present a particular vulnerability, especially those with a permanent connection to networks for data exchange or remote commands.

The sophistication of attacks has also evolved to include coordinated cyber-physical attacks, which simultaneously target both data streams and physical components of an EV powertrain, spanning firmware, energy management systems, and motor drive controllers [50, 51]. Developing resilient control strategies capable of withstanding such multi-faceted attacks is a critical area of current research, with recent work proposing structured resilience frameworks that address the full attack lifecycle — from anticipation and resistance through detection, evaluation, and recovery [52].

Among the existing motors for electrical vehicles, brushless designs are the most popular, with the Permanent Magnet (PM) Brushless (BL) in-wheel motor regarded as advantageous because of its high efficiency. Integrating the motor into the wheel eliminates the need for a transmission and thus simplifies the mechanical design of a car while also eliminating transmission losses, contributing to overall efficiency. For EV applications, three types of Brushless (BL) motors remain most popular [53–66]. The Brushless DC (BLDC) motor is designed with concentrated windings to produce a trapezoidal Back-EMF waveform and an air gap magnetic flux distribution that is ideally trapezoidal. For efficient operation, the windings are powered with quasi-rectangular (or six-step) current pulses. Another type, the Permanent Magnet Synchronous Motor (PMSM), is designed with distributed windings to generate a sinusoidal Back-EMF and air gap flux distribution, and is therefore optimally powered by sinusoidal phase currents. Finally, the induction motor is characterized by its robustness, low cost, and ability to handle high momentary peak torque [67–71].

Overall, we note that the maturity and robustness of the induction motor (IM) technology has been successfully applied to electric vehicles (EVs) (e.g., early Tesla models). However, the Permanent Magnet (PM) motor solutions are generally preferred across electric mobility applications [71]. The suitability depends critically on the vehicle class, power requirement, and budget:

- The Permanent Magnet Synchronous Motor (PMSM) is most suitable for high-performance and high-range passenger EV applications due to its inherently higher power-to-volume ratio (torque density) and its lower energy consumption (higher peak efficiency) across a wide operating range. It is also the dominant technology for many high-power marine electric drives.
- The Brushless DC (BLDC) motor remains the optimal choice for systems where low cost and simple control are paramount. This includes all auxiliary systems (e.g., pumps, fans, compressors) in larger EVs, as well as the main propulsion unit for many ubiquitous small electric platforms, such as electric bicycles, scooters, Unmanned Aerial Vehicles (UAVs/-drones), unmanned ground vehicles (UGVs), and small electric boat drives.

While the IM is the most robust and cost-stable option, the superior energy conversion efficiency of PM motors is the decisive factor in most battery-powered applications. Given the BLDC motor’s ubiquity in mass-market electric mobility platforms (especially UAVs and low-cost small EVs) and its reliance on the computationally simpler but security-critical trapezoidal (six-step) control method, the BLDC motor presents a high-volume target for control system attacks. Therefore, the analysis of its controlled systems is a highly relevant focus for this thesis.

Of importance to our study is the issue of potential motor drives in an EV. Yousfi et al. (2011) suggested a combined control strategy [72] for an EV, as shown in Figure 2.11. The switch allows for selection between two drives: one based on Hall sensor measurements of the rotor position, and another, the position-sensorless drive.

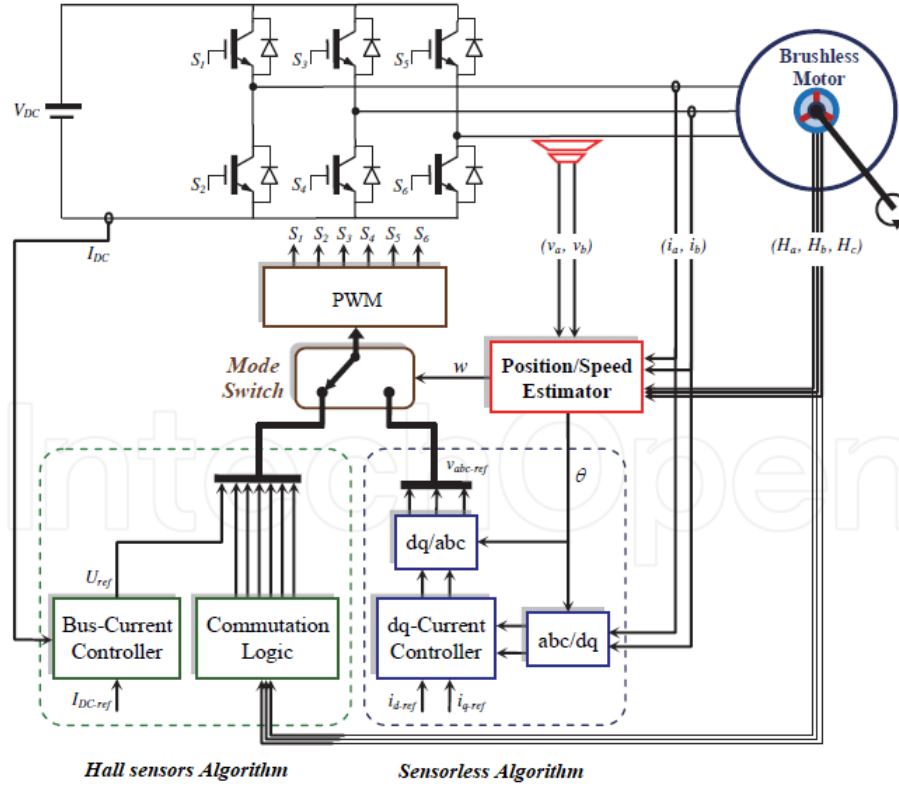


Figure 2.11: Overall scheme of the combined control strategy for EV. (Reproduced from Yousfi et al. (2011) [72]).

The three Hall sensors are positioned on the motor's stator to provide 60 electrical degrees of resolution for the rotor's position. Hence, in Hall sensor mode, the error of the rotor's position estimate is reset when the magnetic axes of the rotor enter a new 60° sector. Starting the motor requires meeting a low-speed/high-torque requirement, which is handled by the Hall sensor mode. After overcoming the vehicle's inertia, the speed becomes sufficiently high to estimate the rotor position via a combined Back-EMF/Hall sensor method. At a sufficiently high speed, operation is switched to the position-sensorless drive mode, which relies on the Back-EMF-based method of estimating the rotor's position.

From a cybersecurity viewpoint, it is important to analyze the impact of having both types of motor drives available on cyber-attack and defense approaches, and the differences in their efficiencies in particular.

Furthermore, the security of an electric vehicle cannot be considered in isolation, as it often connects to the larger power grid for charging. False data injection (FDI) attacks targeting the vehicle-to-grid (V2G) interface — including manipulation of charging station data markets and load-altering attack concealment — can have cascading effects, creating instability in the broader power system and highlighting the interconnected nature of cyber-physical threats [73, 74].

2.6 A machine learning approach for attacks design

In order to design an efficient defense structure, first the security threats need to be identified properly. Such an identification task, in turn, requires detailed structural analysis of the CPSs or their ICS analogs. For that reason, the attacker-side approach needs to be evaluated. Phillips *et al.* (2019) reviewed the reconnaissance effort necessary for the attacker to gather details of the system dynamics needed to design sophisticated attacks against ICSs. Specifically developed was a reconnaissance approach relying on the ICS's I/O data to infer the dynamic model of the system's operation [75]. Such a technique is based on a data-driven approach designed to retrieve features of the system's dynamics, and thus eventually infer its model via the so-called system identification process.

The authors went further by proposing a novel type of cyber-attack in which the controller's proportional, integral and derivative gain values were targeted and modified under the condition of having constant set-point in the control system [75]. Potential attack points reviewed by Phillips *et al.* (2019) are reproduced in Figure 2.12 and include (1) actuators, (2) sensors, or (3) controller. It is a suggestion of this thesis work to include into the scheme the observer, thus rendering an additional point for the attack (point (4), observer) as shown in Figure 2.13. The difference that inclusion of the observer brings in is a possibility to attack not just sensory data but the state variable values instead. The state variables are not necessarily measured with the existing tools and sensors but rather are estimated via state equations and accounting for the data supplied by sensors measuring the parameters of the process.

A practical potential of attacks against CPSs became obvious with the demonstration of Stuxnet worm [76]. A variety of potentially inflictible damages to CPS under attack triggered an interest of the research community to the security issues of networked control systems. Two queueing models were developed by Long *et al.* (2005) [80] to evaluate the effect of time delay in induced jitter and packet loss in the network on the attacked CPS. Within this scenario, the CPS's models remain unknown to the attacker and are considered to be irrelevant. For this, the attack is designed to be universal in nature and with no need to account for the specifics of both the controller and the physical plant under attack. Instead, the network is randomly flooded with the traffic by the attacker to induce jitter and packet loss and thus to affect the operation of CPS.

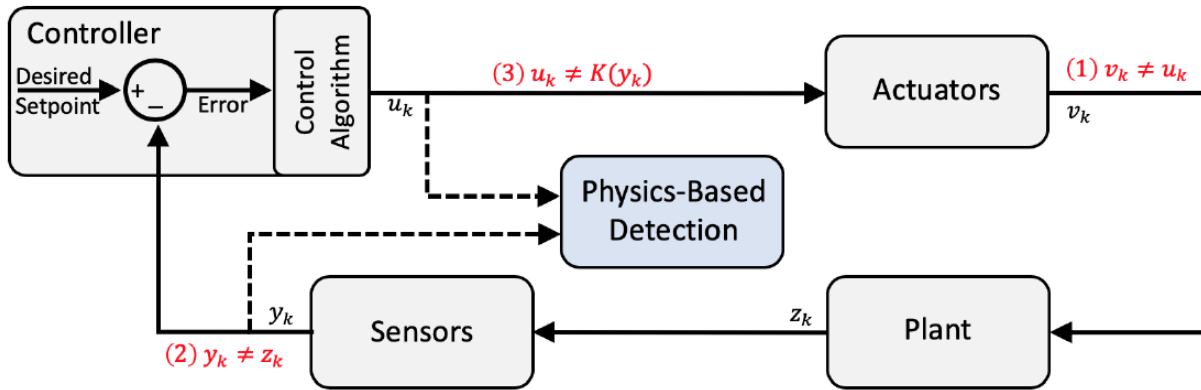


Figure 2.12: General block diagram of an ICS continuous feedback-loop indicating where cyber-attacks can target and compromise the system: (1) actuators, (2) sensors, or (3) controller. Here, altered data from the attack is highlighted in red which the physics-based detection intends to detect. [75].

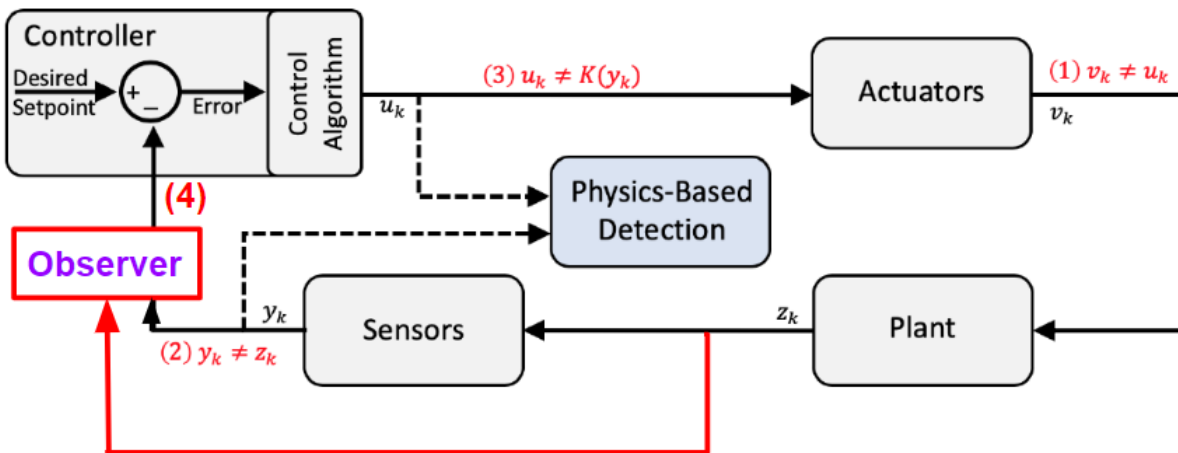


Figure 2.13: Adding the observer to an ICS continuous feedback-loop, thus rendering additional point for the attack (point (4) observer) as compared to that of Figure 2.12.

Table 2.2: Summary of the attacks with various levels of machine learning intelligence.

Reference	Attack	Model knowledge	How the knowledge is obtained	Counter measures
Stuxnet worm [76–78]	Modifications in the PLC code	Yes	Experiment in a real system	(1)Architectural design features [78]. (2)Moving target defense (MTD) approach [79]
Long <i>et al.</i> [80]	Inducing jitter and packet loss	None	N/A	(1)Packets differentiation based on "Type of Service" (TOS) header's field [80]. (2)Generate audit trails for <i>en route</i> traffic and then trace the origin of the attack packets [81–84]
Farooqui <i>et al.</i> [85]	Data injection	None	N/A.	Process control experiments within SCADA testbed environment
Smith [86, 87]	Data injection	Yes	Not described	Subject to future work
Teixeira [14]	Packet loss	None	N/A	Subject to future work
Teixeira [14]	Data injection	Yes	Not described	Subject to future work
Amin <i>et al.</i> [88, 89]	Data injection	Yes	Not described	A robust attack diagnostic scheme based on enhanced hydrodynamic models of canal pools
de Sa <i>et al.</i> [90]	Data injection	Yes	Passive system identification	Operating in stationary mode conditions
de Sa <i>et al.</i> [91]	Data injection	Yes	Active system identification	Reduction of the attack signal-to-noise ratio

Despite universality being a potentially advantageous feature, such an attack lacks covertness as the excessive traffic may be detected by monitoring systems and used to trigger the defensive mechanisms. In particular, packet differentiation based on "Type of Service" (TOS) header's field had been proposed and explored by Long *et al.* (2005) [80] to implement based on that packet filtering as an efficient countermeasure to isolate the attacking traffic within the network and thus negate its impact on CPS. An alternative defense approach was suggested by Snoeren *et al.* (2002) [81], which in essence included generation of audit trails for *en route* traffic followed by tracing the origin of the attack packets. This approach gained popularity due to the offered potential of blocking the malicious traffic at its very source. A number of research ef-

forts explored this concept lately [82–84]. Apart from the lack of covertness in the attack, an additional drawback of the universal type of the attack without accounting for the specifics of the CPS’s model is that the plant under attack may exhibit unpredictable behavior, which may not necessarily be the preferred outcome by the attacker. The cons for the attacker here would be that unpredictable system response may become too strong and therefore easily detectable by defense modules, while the attacker may prefer to remain undetected. As a stealthy type of attack remains a preferred option, the knowledge of the system model becomes desirable due to the potential to achieve the desirable effect with less activity but the one which relies on the knowledge of the system model and hence holds a promise of predicting system’s responses and designing the attack accordingly. Such an approach would bring in more intelligence into the attack thus making it more efficient and less detectable.

An ample effort towards intelligent type of attacks undertook Teixeira *et al.* (2015) [14] by building up a general type of a framework to analyse various kind of attacks over the networks. Their contribution included classification as well as formulating a set of prerequisites for the attack design to account for model knowledge and available resources, such as disclosure and disruption. It follows from their findings that covertness of the attack may be provided only with reliance on high level of awareness about the model of the targeted system. The experimental results provided by Smith *et al.* (2011 and 2015) [86, 87] are well in-line with provisions from Teixeira *et al.* (2015) [14]. Specifically, considered were man-in-the-middle (MitM) attacks, where knowledge of the attacked system model appears to be useful for the false data injection into the feed-forward and/or feedback streams in terms of providing stealthy mode for the attack. The closer the model operated by the attacker is to the actual one for the plant under attack, the better stealthiness of the attack is achieved, at least as it stands out from the analysis of the signals reaching the controller [86, 87]. Another demonstration of the stealthy attack was done by Amin *et al.* (2013), in which [88, 89] targeted were water resources of the Gignac canal of France. In this case the attacker was relying on the knowledge of the system’s model to generate the attack signal and inject it into the network of control system to redirect water streams and thus achieving the goal while remaining stealthy. There the knowledge of the model played a key role in both - the attack formulation as well as providing covertness of the endeavor.

It is worth noting that the above mentioned cases, namely referenced by [14, 86–89], the knowledge of the system’s model was assumed to be given in advance and thus was readily available to the attacker for usage in the attack design. Such favourable circumstances of the system’s model availability may not necessarily be present to the attacker. To attain such knowledge the attacker may need to undertake specific reconnaissance actions, which would constitute a specialized part of the attacker’s activity and which deserves separate consideration and be as well an attack itself with the purpose of gaining at least some knowledge about system’s model. Most stealthy version of such attack would be eavesdropping, where the attacker passively in-

tercepts external communications of the system and thus collects information about system's functionalities, modes of operation, behaviours, interactive responses. Such information may be then used to reconstruct approximation to the system's model via reverse engineering approach. Such a passive type of approach was demonstrated by de Sa et al. (2017) in their Passive System Identification attack [90] used to generate the data for the injection into the network to achieve system degradation effect via eventual Controlled Denial-of-Service (CDoS) attack. A high degree of covertness in the Passive System Identification approach as its apparent pros is at least partially out-weighted by its cons of dependence on the sequences of externally occurring events, which are outside of the attacker's influence but which determine meaningful part of the information gathered by the attacker for the system reverse engineering purposes. To overcome such deficiency, the active component from the attacker the attacker would be needed designed to provoke system to reveal it features via responses to attacker's induced testing signals. The success of such approach would be more dependent on the creativity and sophistication of the attacker's system identification algorithms rather than on the occurrence of events outside of the attacker's control. Such an active alternative was formulated by de Sa et al. (2017) as an Active System Identification attack [91], where the attacker's approach allows to avoid passive observation with waiting for meaningful events to occur but rather creates such events with pre-designed disturbances sent through the network.

Within the Active System Identification attack the attacker aims to determine the unknown coefficients of the CPS's transfer function $G(z)$ defined as

$$G(z) = C(z)P(z), \quad (2.5)$$

where $C(z)$ is the control function of the controller, while $P(z)$ is the transfer function for the plant, all the transfer functions being linear time-invariants. The architecture in question is shown in Figure 2.14. To perform the attack, the attacker is to connect as a Man-in-the-Middle (MitM) to one of the available branches - the forward branch or the feedback one (the last case is shown in Figure 2.14 for a certainty of consideration). After establishing the link, the attacker may inject false data by modifying the data of the stream flowing through the connecting node. The model estimation of the attacked CPS is made by the attacker measuring the response of the system on injected attacking signal $a(k)$.

The limitation of the Active System Identification attack is in the fact that the scope of the attack is limited by the task of approximating model of the system. The current thesis aims to supplement the Active System Identification stage with the follow up attack by engaging interaction with the system in order to guide the system into the prescribed state of increased vulnerability, which is derived from the identified system's model extracted from the results of the prior stage, the Active System Identification part.

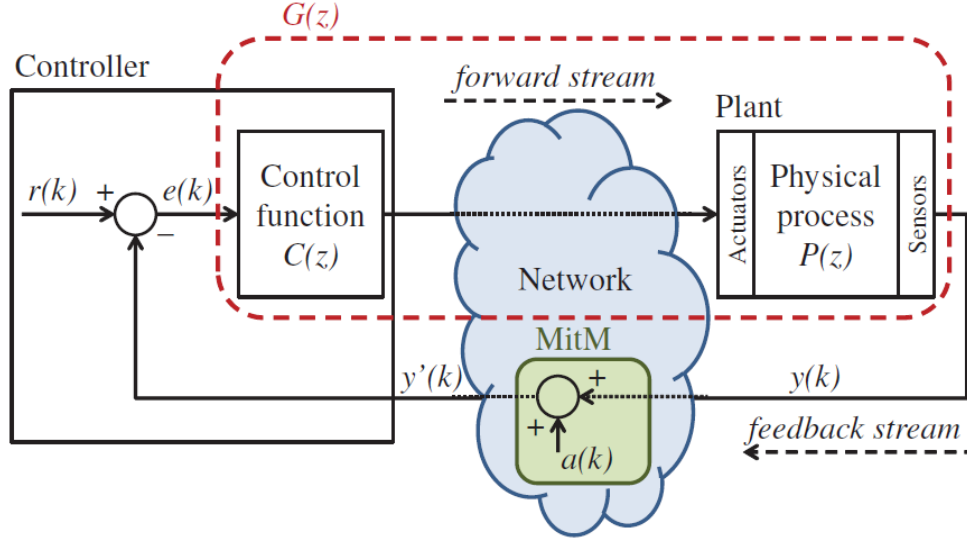


Figure 2.14: Active System Identification attack with a MitM in the feedback link. It is reproduced from [91].

The above literature classification is summarized in Table 2.2. The center point of the present thesis is the introduction of interactivity feature into the attack relying on the knowledge of the system's model. In this regard, the way the knowledge obtained about the system is relevant only in terms of reliability of gathered information and accuracy of the attained model to rely on by the attacker. After that the interactivity with the system follows the pattern of Active System Identification attack but with the goal of steering the system to the desired by attacker state. There is wide open field for the research of that kind for both sides - the attacker as well as the defender. In fact competition of the machine learning tools engaged into the interaction under attack would be deciding the winner, where the attacker may gain stealthy control over the system to manipulate it to desired states while the defender's success is in implementing stable operation of the system even under attack condition thus negating the attack itself rather than isolating the system from network connectivity.

Modern defensive strategies are also increasingly data-driven, enabling resilient control against sensor attacks even without precise knowledge of the system model. Such approaches learn the system dynamics and attack patterns from operational data — ranging from deep reinforcement learning-based passive resilient controllers that adapt to evolving attack strategies [92], to hybrid data-and-model observers that leverage deep learning predictors to rapidly locate attacked sensor channels [93] — offering a flexible and practical alternative to traditional model-based detection [94].

As a proactive defense, Moving Target Defense (MTD) has emerged as a promising paradigm for CPS security. By dynamically and strategically altering system parameters — such as net-

work configurations, operating environments, and communication channels — MTD complicates the reconnaissance and attack planning phases for an adversary, thereby increasing the system’s resilience [95]. Recent work has begun addressing the practical challenges of deploying MTD in resource-constrained IoT and CPS environments, where the overhead of continuous reconfiguration must be carefully managed [96, 97].

To better capture the complex, interconnected nature of CPS, advanced machine learning models are being developed for anomaly detection. For instance, Spatio-Temporal Graph Neural Networks (ST-GNNs) can model the system as a graph, learning the intricate spatial and temporal relationships between components to more effectively identify subtle deviations caused by an attack. Recent work has demonstrated this approach in reconfigurable CPS environments, where graph attention networks successfully detect threats by capturing the evolving topology of interconnected subsystems [98].

2.7 Vulnerabilities and Defense Gaps in Industrial CPS

The evolution of security in *Cyber-Physical Systems* (CPS) has established a robust theoretical foundation, yet significant gaps remain regarding the physical-electrical interplay in high-speed motor control. Early foundational models, most notably by Mo and Sinopoli [36], established the mathematical boundaries of stealthy integrity attacks. Their work focused on the statistical limits of innovation-based detectors, demonstrating that an attacker could remain invisible by constraining bias within the noise floor of the system’s residuals. While these models provide a rigorous baseline for *data-level* security, they primarily treat the system as a discrete-time linear abstraction, leaving the vulnerabilities of *high-frequency electrical resonances* largely unexplored.

The historical precedent of *Stuxnet* [99] highlighted the catastrophic potential of logic-level manipulation in industrial drives, where mechanical resonance was exploited to cause physical failure. However, *Stuxnet* targeted essentially undefended systems. In modern contexts where state estimators like the Kalman filter are standard, there is a critical need to investigate whether these very defenses can be exploited.

Current literature, including taxonomic frameworks by Teixeira et al. [14], categorizes attacks based on adversary knowledge and resources but lacks a detailed characterization of *inter-active* attacks that adapt to the feedback loop’s switching frequencies.

A significant and persistent hurdle in the contemporary literature on cyber-physical security is the inherent trade-off between detection accuracy and computational cost. Recent advancements in 2025 have seen the emergence of highly sophisticated identification techniques, such

as the *SAD-GAN* framework [100], which utilizes *Generative Adversarial Networks* for self-adaptive anomaly detection. While these frameworks achieve remarkable accuracy on standard *CPS* benchmark datasets, their reliance on deep learning architectures necessitates substantial memory and processing power. Similarly, modern adaptive detection methods, such as those proposed by Moriano et al. [101], seek to jointly optimize model adaptation and data processing to handle dynamic environments.

However, as highlighted by real-world cyber security demonstrations on networked electric drive systems [102], these high-performance algorithms often require computational resources that are simply not available on standard embedded motor controllers. This creates a critical disconnect between theoretical detection capability and practical edge deployment. Current research remains largely dominated by statistical and machine-learning approaches that demand extensive training data and significant inference overhead. There is, therefore, a clear and urgent need for a shift toward detection methodologies that leverage domain-specific physical signatures—specifically those appearing in the frequency and phase domains—to provide a computationally efficient, real-time security layer capable of operating within the strict deterministic constraints of high-speed motor control.

A parallel challenge exists at the network layer, where research has focused heavily on communication-layer vulnerabilities. Recent studies have provided detailed analyses of Man-in-the-Middle (MITM) and spoofing attacks within networked control and power-electronics systems — ranging from comprehensive reviews of attack vectors in microgrid CPS [103] to live testbed demonstrations of multi-stage MITM intrusions causing false data injection and false command injection in power system networks [104]. However, these investigations remain largely protocol-focused, centering on the detection of packet delays, unauthorized access, or frame manipulation. While these contributions are vital for securing the communication medium, they often overlook the control-loop integrity of high-speed plants — a gap made more acute by recent findings that adversaries can construct *perfect stealthy attacks* that satisfy residual-based detection thresholds while still corrupting system state [105]. There is thus a documented lack of research into how an adversary can stay within protocol-compliant bounds while still executing stealthy, high-frequency masking within the motor’s electrical bandwidth — a gap that necessitates a shift toward physics-aware network security.

A significant volume of recent research has focused on the vulnerability of state observers and estimation mechanisms to integrity attacks. Foundational contributions have rigorously analyzed how adversaries can manipulate Kalman Filters (KF) and Luenberger observers by injecting malicious data — both through stealthy attack strategies targeting distributed estimators [106] and through integrity attacks with varying data access that exploit the information boundary between the attacker and estimator [107], and reduced-order descriptor observer methods that address simultaneous FDI attacks and unknown disturbances [108]. Observer-based detection

frameworks have been proposed in response, leveraging adaptive residual thresholds to identify injected biases [109]. However, these 2024–2026 studies primarily address *static bias* or slowly varying offsets that shift the estimated state away from the true plant behaviour. While these models are effective for detecting long-term divergence, they lack the high-fidelity temporal resolution required to capture transient phenomena. Specifically, there is an unaddressed gap in the literature regarding how high-frequency excursions can remain undetected by traditional observers that are tuned to filter out high-frequency noise — a limitation that this research seeks to overcome.

The shift toward strategic resilience has led to the adoption of game-theoretic models to characterise the interactions between adversaries and defenders in CPS. Recent work has utilised Stackelberg hierarchies to address resource allocation under cyber-attacks — from data-driven secure control under hybrid DoS and FDI attacks modelled as a non-cooperative Stackelberg game [110], to Bayesian Stackelberg frameworks with incomplete information optimising node-level energy allocation during jamming and denial-of-service conditions [111]. Multi-agent reinforcement learning extensions of these hierarchical frameworks have further been proposed to handle the dynamic, multi-player nature of CPS resilience problems [112]. However, these 2024–2026 models are predominantly communication-centric, focusing on the availability of network nodes and the mitigation of packet loss or denial-of-service conditions. While effective for ensuring data throughput, these models often abstract away the internal physics of the plant, treating the control loop as a black box. Consequently, there is an unaddressed gap regarding the application of Stackelberg strategies to the high-frequency internal dynamics of embedded motor drives — a limitation that motivates the development of a physics-aware asymmetric game framework.

The development of resilient control laws has increasingly turned toward sophisticated adaptive mechanisms to counteract adversarial influence. Recent advancements have introduced Adaptive Neural Network (NN) architectures — including self-triggered resilient controllers using backstepping and Nussbaum-function-based compensation [113] and finite-time fuzzy adaptive output feedback schemes [114] — designed to maintain plant stability during active sensor and actuator signal manipulation. The most recent work has further extended these frameworks to handle unmodeled dynamics alongside FDI attacks simultaneously [115]. While these 2024–2025 frameworks provide robust convergence under a wide range of attack intensities, they encounter a fundamental *Stability vs. Stealth* trade-off. Specifically, high-gain compensation strategies often induce aggressive control efforts that can inadvertently expose the presence of a defender or trigger secondary instabilities. Furthermore, current literature lacks a systematic treatment of the transient disruption occurring immediately following the termination of an attack. This dissertation identifies this post-attack recovery phase as a critical vulnerability that existing adaptive baselines are not designed to compensate for.

Chapter 3

Problem Formulation and Methodology

In this chapter, the research problem is formulated based on the above analysis of the available literature information. Furthermore, the methodology to address the research issues at hand is outlined.

3.1 Problem Formulation

The goal of this project is the further development and verification of the principles for building a secure environment for Cyber-Physical System's (CPS's) operation. Specifically, this includes three stages/levels of security architecture design:

- (i) cyber attacks construction,
- (ii) attacks detection and identification, and
- (iii) defence creation.

In this regard, the first level (i) is the essential part of security awareness, when potential dangers are recognized in sufficient details, allowing the alignment of levels (ii) and (iii) in most appropriate way to accommodate the features of anticipated cyber threats.

The level (i) includes selection of the desirable purpose of the attack, identifying a suitable way of its implementation as well as algorithmic framework for its operation. The next level, (ii), i.e., attack detection and identification, stems from the level (i) in that based on the knowledge of the potentially efficient attack's features, the detection modules could be designed with a proper integration into the system and allowing both – the timely detection of the attack as well as its sufficient identification. As a means for attack detection the neural network-based anomaly detectors are seen as a potentially suitable tool. Similarly, neural associative memories may be

explored for recognition of specific signatures of the attacks. However, at the present stage when the attack is still in the theoretical stage of development, the scope of the present thesis should be limited to basic detection techniques relying on direct physical processes rather than sophisticated information processing techniques. This is because only after specific implementation of the attack in the hardware-made test-bed environment the issue of detection becomes relevant in terms of the need to overcome the stealth of the implemented attacking methods. Before that, if basic detection methods suffice for the development of the attack models, then more sophisticated approaches may be left for the future time when such development acquires practical relevance.

Once detected, the attack counteraction may be envisaged with neural predictors generating compensating biases that aim to nullify the attack's consequences. This would constitute level (iii) of cybersecurity aiming to allow safe operation of the system during the attack with minimal impact on the system thus defeating the attacker's aspirations.

3.2 Methodology

3.2.1 Driving BLDC motor with Kalman filter based drive

The methodology chosen herewith is simulation and modeling. The BLDC model relies on known electromagnetic interactions in the motor's winding in the rotating magnetic field of permanent magnets. The Kalman filter observes the current values in the motor's winding and estimates commutation instants for each winding, sending switching signals to the feedback line of the control scheme (Figure 3.1).

Two modes of data sampling for analyzing feedback output from the BLDC motor have been tested: (1) equal angular separation and (2) equal time intervals. In case (1), the data are collected via equal intervals $\Delta\theta$ of the rotor's sequential angular position θ_i , $i = 1, 2, 3, \dots$, i.e., keeping $\Delta\theta = \text{const}$. In case (2), the data collection time points t_i are separated by equal sampling time intervals $\Delta t = \text{const}$, thus ensuring constant sampling rate $r_s = 1/\Delta t$. In the equal angular separation mode, the motor supplied the sequence of operating voltages which according to the state model would lead to the desired values of the state variables. In the equal time intervals sampling mode, the sequence of operating voltages is affected by the estimates of the outgoing states of BLDC motor conducted by the Kalman filter (KF).

The Logic Controller in Figure 3.1 aims to reach the speed ω_{ref} . In our task, the need is to explore motor behavior within the full range of available speeds under a given set of system parameters. To achieve that, the value of ω_{ref} is to be chosen above the upper bound ω^{upper}

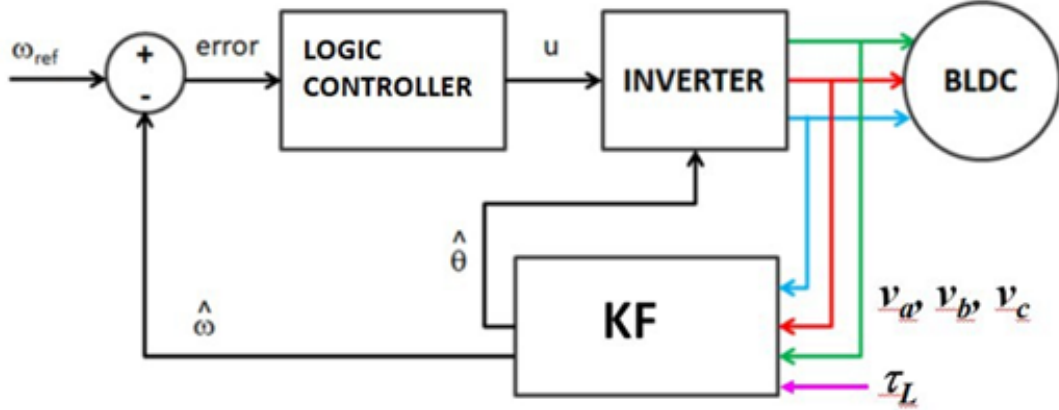


Figure 3.1: Schematic of the employed control system of BLDC motor with Kalman filter in the feedback loop. Kalman filter's inputs are operating voltages v_a, v_b and v_c for the motor's phases A, B and C, while outputs are estimated values of angular speed $\hat{\omega}$ and rotor's angular position $\hat{\theta}$.

of the observable speeds, otherwise it is scaled up and the experiment is repeated to ensure $\omega_{ref} > \omega^{upper}$.

BLDC Motor Model

The BLDC state space model is derived (see [6]) based on established electromagnetic interactions in the motor windings. It is to be used for the more complex speed estimation methods and will assume that the motor has a trapezoidal shaped back EMF. The motor is assumed to have three identical phases of which one can model only one phase and apply it to the rest of the phases. By using this consideration, the first equation for the phase becomes:

$$u_a = Ri_a + (L - M)\frac{di_a}{dt} + \xi_a + u_n, \quad (3.1)$$

where u_a is the phase voltage, R is the phase resistance, i_a is the phase current, L is the phase inductance, M is the mutual inductance, ξ_a is the phase back EMF voltage, u_n is the neutral node voltage. The back EMF is assumed to be trapezoidal, therefore the commutation scheme becomes such that only two phases are active at the same time. Then the neutral voltage can be presented as in the following:

$$u_n = \frac{1}{3}[(u_a + u_b + u_c) - (\xi_a + \xi_b + \xi_c)], \quad (3.2)$$

Combining the above equations brings about the following:

$$\frac{di_a}{dt} = \frac{u_{ab} - u_{ca}}{3(L - M)} - \frac{R}{(L - M)}i_a + \frac{\xi_b + \xi_c - 2\xi_a}{3(L - M)} \quad (3.3)$$

The back EMF can be expressed as a function of angular velocity rather than that of voltage. Now all three phases need to be accounted for, so that proper commutation maintains 120-degree shifts between the phases. In this case the back EMF components become:

$$\xi_a = K_\xi \omega f(\theta), \quad (3.4)$$

$$\xi_a = K_\xi \omega f\left(\theta - \frac{2\pi}{3}\right), \quad (3.5)$$

$$\xi_a = K_\xi \omega f\left(\theta + \frac{2\pi}{3}\right), \quad (3.6)$$

with function $f(\theta)$ being defined as:

$$f(\theta) = \begin{cases} \frac{6}{\pi} \cdot \theta & \text{if } 0 \leq \theta < \frac{\pi}{6} \\ 1 & \text{if } \frac{\pi}{6} \leq \theta < \frac{5\pi}{6} \\ \frac{-6}{\pi} \cdot (\theta - \pi) & \text{if } \frac{5\pi}{6} \leq \theta < \frac{7\pi}{6} \\ -1 & \text{if } \frac{7\pi}{6} \leq \theta < \frac{11\pi}{6} \\ \frac{6}{\pi} \cdot (\theta - 2\pi) & \text{if } \frac{11\pi}{6} \leq \theta < 2\pi \end{cases} \quad (3.7)$$

The function $f(\theta)$ has the trapezoidal shape for a 360-degree electrical cycle. The phase current equations thus can be expressed as follows:

$$\frac{di_a}{dt} = \frac{u_{ab} - u_{ca}}{3(L - M)} - \frac{R}{(L - M)}i_a + \frac{K_\xi \omega [f(\theta - \frac{2\pi}{3}) + f(\theta + \frac{2\pi}{3}) - 2f(\theta)]}{3(L - M)} \quad (3.8)$$

$$\frac{di_b}{dt} = \frac{u_{bc} - u_{ab}}{3(L - M)} - \frac{R}{(L - M)}i_b + \frac{K_\xi \omega [f(\theta) + f(\theta + \frac{2\pi}{3}) - 2f(\theta - \frac{2\pi}{3})]}{3(L - M)} \quad (3.9)$$

$$\frac{di_c}{dt} = \frac{u_{ca} - u_{bc}}{3(L - M)} - \frac{R}{(L - M)}i_c + \frac{K_\xi \omega [f(\theta) + f(\theta - \frac{2\pi}{3}) - 2f(\theta + \frac{2\pi}{3})]}{3(L - M)} \quad (3.10)$$

The equation for angular velocity can be obtained from the expression for electromagnetic torque in combination with the conversion of electrical degrees into mechanical ones and the expression for mechanical motion torque, resulting in:

$$\frac{d\omega}{dt} = \frac{p^2 K_\xi}{J} \left[f(\theta) i_a + f\left(\theta - \frac{2\pi}{3}\right) i_b + f\left(\theta + \frac{2\pi}{3}\right) i_c \right] - \frac{p\tau_L}{2J} - \frac{B\omega}{J} \quad (3.11)$$

Matrices of the state space equations from the above become:

$$A = \begin{bmatrix} \frac{-R}{(L-M)} & 0 & 0 & F_{14} & 0 \\ 0 & \frac{-R}{(L-M)} & 0 & F_{24} & 0 \\ 0 & 0 & \frac{-R}{(L-M)} & F_{34} & 0 \\ \frac{p^2 K_\xi}{J} f(\theta) & \frac{p^2 K_\xi}{J} f\left(\theta - \frac{2\pi}{3}\right) & \frac{p^2 K_\xi}{J} f\left(\theta + \frac{2\pi}{3}\right) & \frac{-B}{J} & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad (3.12)$$

$$B = \begin{bmatrix} \frac{1}{3(L-M)} & 0 & 0 & 0 \\ 0 & \frac{1}{3(L-M)} & 0 & 0 \\ 0 & 0 & \frac{1}{3(L-M)} & 0 \\ 0 & 0 & 0 & \frac{-p}{2J} \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad (3.13)$$

with a state vector that is

$$\vec{x} = \begin{bmatrix} i_a \\ i_b \\ i_c \\ \omega \\ \theta \end{bmatrix} \quad (3.14)$$

while the input vector that is

$$\vec{u} = \begin{bmatrix} u_{ab} - u_{ca} \\ u_{bc} - u_{ab} \\ u_{ca} - u_{bc} \\ \tau_L \end{bmatrix} \quad (3.15)$$

where elements F_{14} , F_{24} , and F_{34} , of the state matrix A are

$$F_{14} = \frac{K_\xi [f(\theta - \frac{2\pi}{3}) + f(\theta + \frac{2\pi}{3}) - 2f(\theta)]}{3(L - M)} \quad (3.16)$$

$$F_{24} = \frac{K_\xi [f(\theta) + f(\theta + \frac{2\pi}{3}) - 2f(\theta - \frac{2\pi}{3})]}{3(L - M)} \quad (3.17)$$

$$F_{34} = \frac{K_\xi [f(\theta) + f(\theta - \frac{2\pi}{3}) - 2f(\theta + \frac{2\pi}{3})]}{3(L - M)} \quad (3.18)$$

Here R is the phase resistance; L is the phase inductance; M is the mutual inductance; p is the number of poles; K_ξ is the back EMF constant; J is the rotor inertia; $f(\theta)$ is the normalized trapezoidal function; B is the motor viscous damping friction; i_a , i_b , i_c are the phase currents; $u_{ab} - u_{ca}$ is the applied phase A voltage; $u_{bc} - u_{ab}$ is the applied phase B voltage; $u_{ca} - u_{bc}$ is the applied phase C voltage; τ_L is the applied mechanical torque load; θ is the electrical angle; ω is the electrical angular velocity.

Kalman Filter Estimator for BLDC Motor

The Kalman filter is an estimator with statistical properties to estimate an output based on a mathematical model. The estimator considers the errors produced by process, estimation and measurement noise and under the assumption of all noise to be Gaussian distributed it estimates an output. The discrete Kalman estimator can be in two different states, the prediction step where the estimator tries to predict the current system state, and the correction step where the so-called Kalman gain is computed and the system state is estimated. The Kalman estimator can be described with the following equations:

Prediction step:

$$\hat{x}_k^- = A\hat{x}_{k-1}^- + B\vec{u}_k \quad (3.19)$$

$$\mathbf{P}_k^- = \mathbf{A}\mathbf{P}_{k-1}\mathbf{A}^T + \mathbf{Q} \quad (3.20)$$

Correction step:

$$\mathbf{K}_k = \mathbf{P}_k^- \mathbf{C}^T (\mathbf{C}\mathbf{P}_k^- \mathbf{C}^T + \mathbf{R}) \quad (3.21)$$

$$\hat{\mathbf{x}}_k = \hat{\mathbf{x}}_k^- + \mathbf{K}_k (\mathbf{z}_k - \mathbf{C}\hat{\mathbf{x}}_k^-) \quad (3.22)$$

$$\mathbf{P}_k = (\mathbf{I} - \mathbf{K}_k \mathbf{C}) \mathbf{P}_k^- \quad (3.23)$$

where $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ are the matrices of the state space equations; $\hat{\mathbf{x}}_k^-$ is the estimated state (prior); $\hat{\mathbf{x}}_{k-1}^-$ is the previous estimated state; $\hat{\mathbf{x}}_k$ is the estimated state output; $\mathbf{B}\vec{u}_k$ is the input vector; $\mathbf{P}_k$ is the state error covariance matrix; $\mathbf{Q}$ is the process noise error covariance matrix; $\mathbf{R}$ is the measurement error covariance matrix; $\mathbf{K}_k$ is the Kalman gain; $\mathbf{I}$ is the identity matrix; $\mathbf{z}_k$ is the measurement vector. Herewith the Kalman estimator is only used with a position-sensorless scheme; therefore, the current is the only sensor measurement. As the variance of the current is assumed to be 0.1A, the measurement noise error matrix $\mathbf{R}$ becomes:

$$\mathbf{R} = \begin{bmatrix} 0.1 & 0 & 0 \\ 0 & 0.1 & 0 \\ 0 & 0 & 0.1 \end{bmatrix} \quad (3.24)$$

The chosen variance values are: 0.02A for the currents, 50 rpm for the angular velocity and $\pi/36$ (or 5^0) for the position. Hence, the $\mathbf{Q}$ matrix assumes the form (3.25):

$$\mathbf{Q} = \begin{bmatrix} 0.02 & 0 & 0 & 0 & 0 \\ 0 & 0.02 & 0 & 0 & 0 \\ 0 & 0 & 0.02 & 0 & 0 \\ 0 & 0 & 0 & 50 & 0 \\ 0 & 0 & 0 & 0 & \frac{\pi}{36} \end{bmatrix} \quad (3.25)$$

In the MATLAB implementation of the Kalman filter for BLDC motor, the following initial set of parameters was employed in the program (we call it herewith as “base set”) and initialized as in Listing 3.1 (MATLAB notations):

Listing 3.1: Base set of parameters in Matlab simulation program

```
T = 0.000020; % seconds
L = 0.02; M = 0.01; % Henry
R = 1; % initialize resistance R;
Kemf = 1; % back-EMF coefficient
tauL = 1; % is the applied mechanical torque load
p = 4; %% number of poles
Bd = 1; % Bd is the motor viscous damping friction;
J = 1; % is the rotor inertia
```

The non-diagonal elements of the 4th column of the matrix A have been represented by the 2-D array F1234, which was defined (in MATLAB notations) as Listing 3.2:

Listing 3.2: The non-diagonal elements of the fourth column of the matrix A

```
F1234 = zeros(3,N);
for n = 1:N
    F1234(1,n) = [Kemf/(3*(L-M))] * (ftetaM(n)+ftetaP(n)-2*fteta(n));
    F1234(2,n) = [Kemf/(3*(L-M))] * (fteta(n)+ftetaP(n)-2*ftetaM(n));
    F1234(3,n) = [Kemf/(3*(L-M))] * (fteta(n)+ftetaP(n)-2*ftetaP(n));
end
```

3.2.2 Cyber-attack construction

Figure 3.2 illustrates the general architecture of the proposed bias injection attack targeting a Kalman filter-based observer used in a BLDC motor system with a PID controller.

Here the attacker aims to explore the effect of synchronizing the dynamics of injected false data and the dynamics of the system. Such synchronization is introduced via implementing periodic modulation of the values of the false data, thus linking time changes of the last ones with the reaction of the system to those changes. Creating such a link allows to explore the possibility of achieving synergistic effect between dynamics of the system and that of the injection attack itself. The example of such synergy would be the possibility for self-amplification of the attack, i.e., increasing the sensitivity of the system to the same level of attacking action.

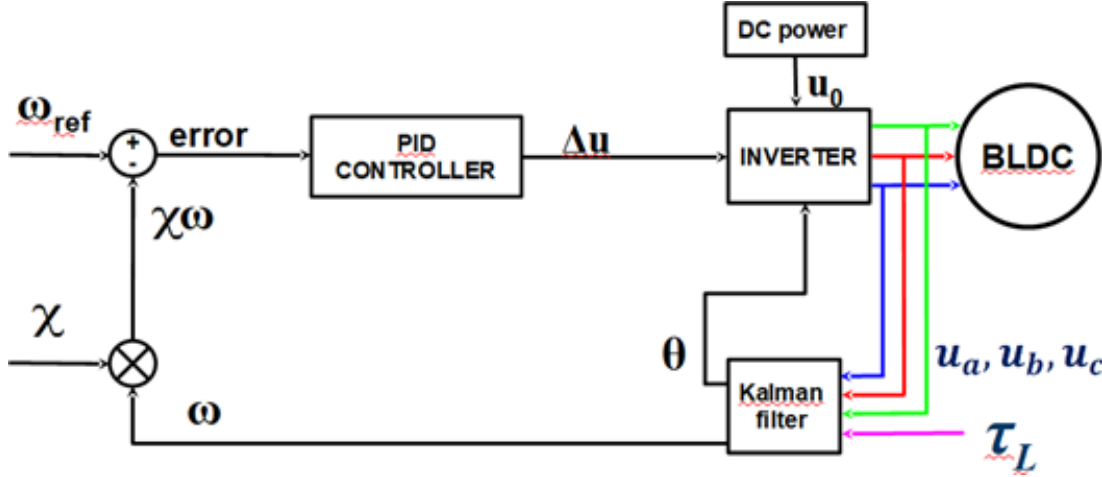


Figure 3.2: Bias injection attack construction against Kalman filter as a driver in a feedback loop of PID controlled BLDC motor in position sensorless mode.

More specifically, to achieve the goal, herewith we shall explore the potential of the data injection attack directed against Kalman filter used in the role of a driver for BLDC motor

Recently, a model was reported and tested for open loop control of BLDC motor, driven in position sensorless mode by Kalman filter state estimator (see [6]). Demonstrated was the ability of the Kalman filter to cause ripples in motor operation. Bearing in mind that induced instabilities may be used for attack purposes aiming to reduce the efficiency of the BLDC motor drive, the task here is formulated to explore the potential of introducing controlled bias into the Kalman filter's estimate of the angular velocity of the rotor with the purpose of achieving controllable disturbances in motor operation within the closed loop control system.

Mathematically, the problem formulation includes the following substitutions in the update stage of the state equation for the Kalman filter of BLDC motor [6]: (i) $\omega \rightarrow \chi\omega$, (ii) $u_a \rightarrow u_a + \Delta u/3$, (iii) $u_b \rightarrow u_b + \Delta u/3$, (iv) $u_c \rightarrow u_c + \Delta u/3$, where all variables are defined as in Figure 3.2. Quantitatively, substitution (i) from the attacker in the state equation is supposed to get balanced with substitutions (ii), (iii) and (iv) from the controller.

To verify the available potential for adversary attacking actions, an architecture employing a position sensorless drive for the BLDC motor has been selected (see Figure 3.3). An initial version of similar architecture is described in more details and operation of related model is subjected to various tests [6].

There is one distinctive difference in the system in Figure 3.3 from that described earlier [6] - the closed loop control here is locked up by proportional controller (P-controller) instead of so-called logical controller of ref. [6]. The logic of the controller in ref. [6] was set to ensure a prevalence of the reference speed over the one actually achieved. In practical terms it means

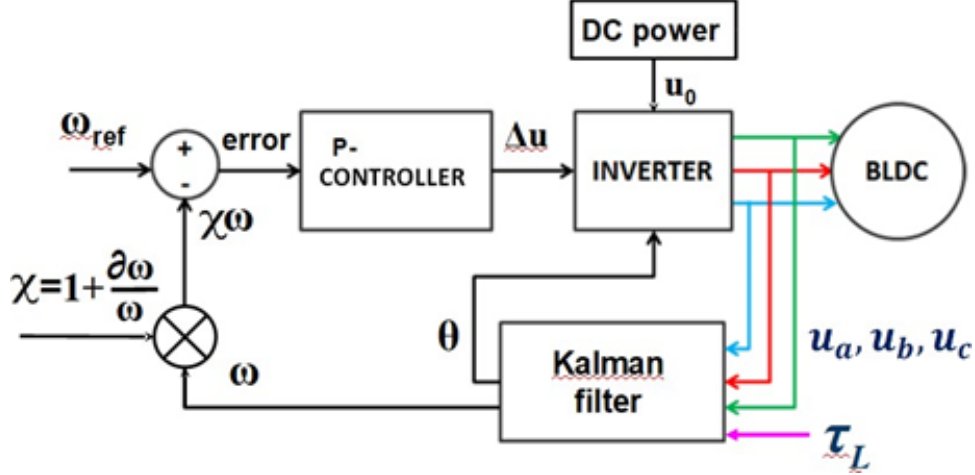


Figure 3.3: Architecture with position sensorless drive for BLDC motor as well as bias injection $\delta\omega$ access point. Kalman filter inputs are voltages in the respective winding, u_a, u_b, u_c , and load torque τ_L .

that the circuits in ref. [6] operated in open-loop control mode to verify maximum possible load operation for the given set of motor parameters in the model.

Another distinctive feature of the architecture in Figure 3.3 is the presence of the access point for the bias $\delta\omega$ injection where angular speed $\hat{\omega}$ estimate made by the Kalman filter is modified with the bias term $\delta\omega$ and thus is replaced with $\hat{\omega} + \delta\omega$ to be processed by the controller's comparator node to calculate the deviation of the $\hat{\omega} + \delta\omega$ from the reference value ω_{ref} , to produce an error term:

$$error = \omega_{ref} - (\hat{\omega} + \delta\omega), \quad (3.26)$$

which is for the controller to compensate.

Operation with no Bias Injection

Under regular conditions (i.e. with no bias, $\delta\omega = 0$) for stable motor operation at a reference speed ω_{ref} the following set of parameters hold: $error = 0$, $\hat{\omega} = \omega_{ref}$, the controller outputs $\Delta u = 0$ and thus inverter is fed only by input voltage u_0 from the power source. If an error deviates from 0, the controller outputs an addition of Δu to the DC power supplied to inverter totaling it to $u_{DC} = u_0 + \Delta u$, where for proportional controller the following holds:

$$\Delta u = K_p * error, \quad (3.27)$$

and where K_p is the proportionality coefficient for P-controller used as a controller's tuning

parameter for an error compensation.

Operation with Bias Injection

Bias injection occurs when the attacker sets $\delta\omega \neq 0$, either positive or negative, substituting the initial Kalman filter estimation $\hat{\omega}$ with modified value $(\hat{\omega} + \delta\omega)$. Equations (3.26) and (3.27) still apply, however, the resulting value of δu produced by the controller would account for the bias term as if it were part of the Kalman filter estimate. The created thus a mismatch between state estimate supplied to the controller and the actual one would constitute a condition for operation under attack. Calculation of $\delta\omega$ at each point in time has been carried out from the following equality:

$$\chi\hat{\omega} = \hat{\omega} + \delta\omega \quad (3.28)$$

with χ being a distortion coefficient desired by the attacker in transforming the estimation of $\hat{\omega}$ by the Kalman filter into modified values $\chi\hat{\omega}$.

Model verification

To ensure the developed model operates adequately, we have implemented verification of its operation under standard conditions, which include the following:

- (i) acceleration at $\hat{\omega} < \omega_{ref}$ with $\delta\omega = 0$ and $K_p = 0$ (it is equivalent to open loop operation);
- (ii) adjusting torque load to stabilize open loop operation at $\hat{\omega} = \omega_0$ (100 rad/sec) level with $\delta\omega = 0$ and $K_p = 0$ (last condition ensures equivalence to open loop);
- (iii) step-function response ($\omega_{ref} = \omega_0 + \Delta\omega$ with $\delta\omega = 0$ and $K_p > 0$) of the closed loop control;
- (iv) stable operation for $\hat{\omega} = \omega_{ref} = \omega_0 + \Delta\omega$ with $\delta\omega = 0$ and $K_p > 0$.

The result of such testing is shown in Figure 3.4 with $\omega_0 = 100$ rad/sec, $\Delta\omega = 150$ rad/sec, $K_p = 10$, and where time sections for tests are allocated as follows. Within time t from $t = 0$ to $t = 0.5$ sec the test (i) is run. Then until $t = 1.0$ sec the test (ii) is run, after which point ω_{ref} has

been modified to run test (iii) followed by test (iv). It is seen that the model works as expected, maintaining steady acceleration in part (i), keeping up with holding the required ω_0 in part (ii), then showing proper step-function response for part (iii), and finally showing stable closed loop operation for part (iv).

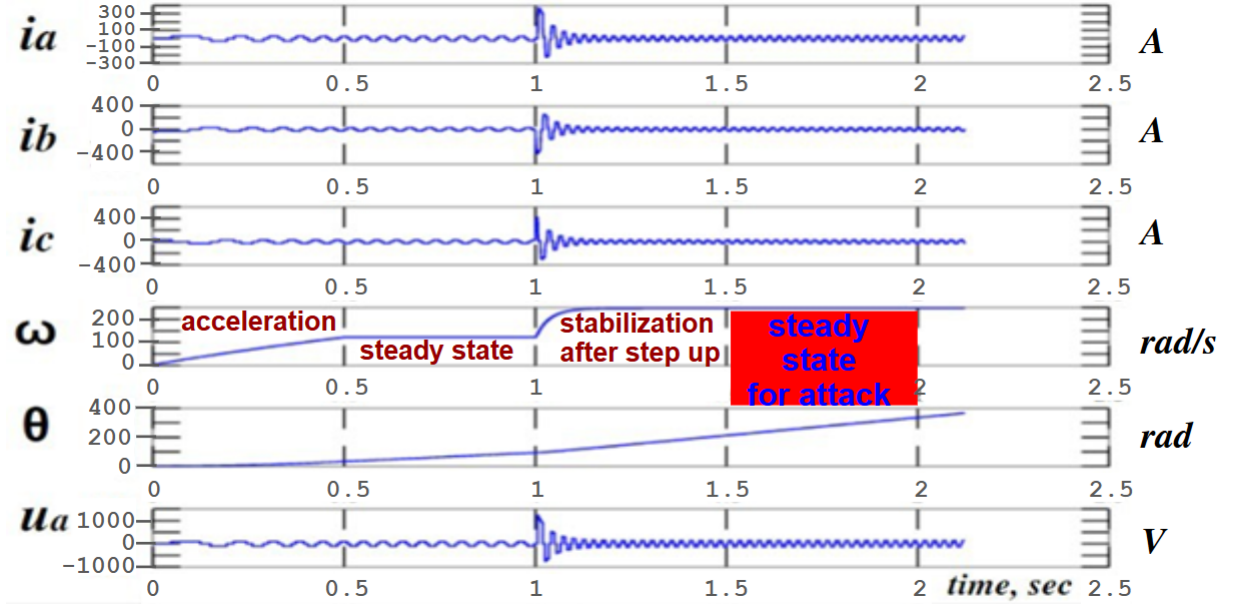


Figure 3.4: Model verification with sequential test (I) through (iv). The set of state variables is: i_a , i_b , i_c are currents in the respective winding, speed estimate $\hat{\omega}$ and position estimate $\hat{\theta}$ of the rotor. Values of the phase currents are in A (Amperes) (i_a , i_b , i_c), angular speed ω is in rad/s (radians per second), rotor position θ is in rad (radians), and phase voltage u_a is in V (Volts). The horizontal axis represents time in seconds (s).

Bias coefficient functions

Having verified the response of the system to step-function at the input and without bias in the feedback loop, we shall proceed to the introduction of the bias $\delta\omega$ into the feedback loop, which would constitute the attack against the Kalman filter estimates of the motor speed.

Constant bias coefficient (double-step function)

A double-step function shown in Figure 3.5,a represents a version of the attack with constant bias coefficient $\chi = \text{const.}$ One would expect the response of the system to be similar to that of a step-function in the input indicating appropriate change of the relation between ω_{ref} and estimated value of $\hat{\omega}$, except that in this case instead of $\hat{\omega}$ there will be its modified value $(\hat{\omega} + \delta\omega) = \chi\hat{\omega}$.

Linearly increasing bias coefficient

The obvious drawback of using a double-step function in the bias injection attack is its quick changes at both sides, the beginning and the end. Such quick changes may not go stealthy and are easily detectable. In this respect, it may be advantageous to use a function with gradually increasing bias, shown in Figure 3.5,b. A particular example presented in Figure 3.5,b has a bias function with linearly increasing χ , or, in other terms, with $\chi' = d\chi/dt = \text{const}$, i.e., constant bias coefficient derivative. Accumulated final bias of the same value as for the double-step function may be reached slowly but steadily with more chances to go undetectable.

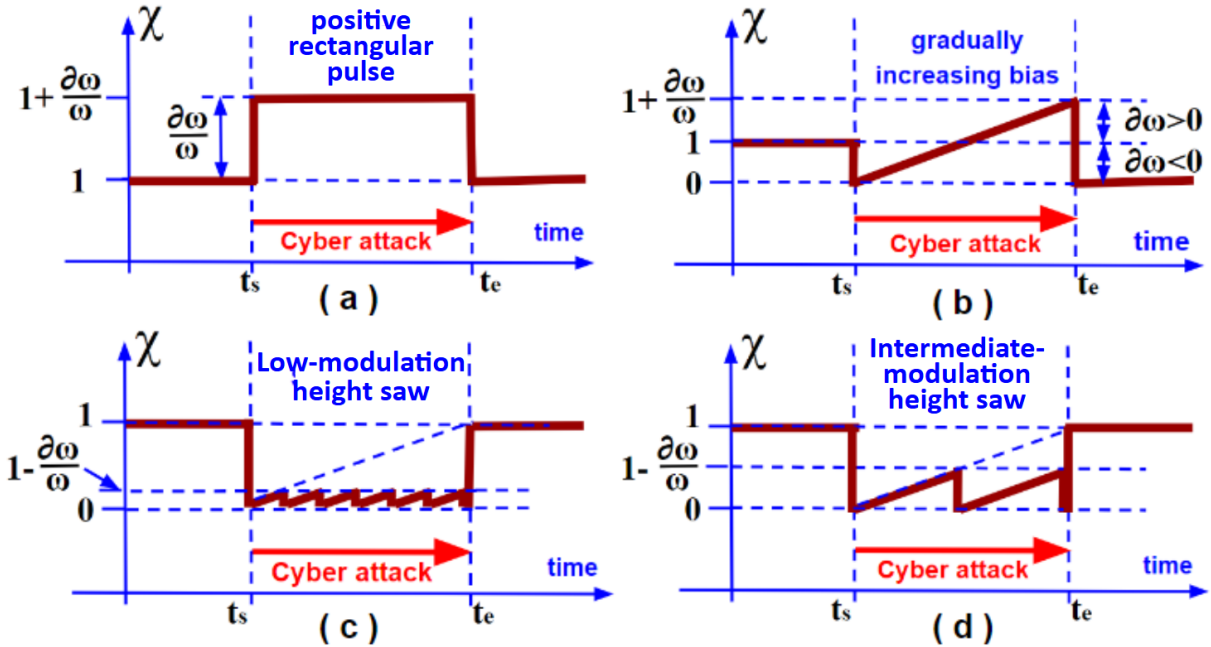


Figure 3.5: Testing functions of distortion bias coefficient, χ : (a) positive rectangular pulse; (b) linearly increasing bias; (c) saw function (deep-leveled, low-modulation height saw); (d) saw function (deep-leveled, intermediate-modulation height saw).

Bias Coefficient for the Sawtooth Function

To increase the stealthiness of the bias injection, the gradually increasing function for χ can be replaced by a sawtooth waveform with the same gradient, as illustrated in Figures 3.5,c and 3.5,d for the linear case where $f' = \frac{d\chi}{dt} = \text{const}$ within each tooth. This modification may allow the bias amplitude to remain below the noise level, thereby enhancing the stealthiness of the attack. Consequently, the depth of the sawtooth becomes a critical parameter to consider when selecting

the preferred attack strategy. In a sawtooth-shaped waveform with a right angle in its triangular form, only two of the three parameters — gradient, frequency, and modulation depth — are independent.

3.3 Predictive Cyber-defense design

In this thesis, a predictive architecture for control system defense is proposed, wherein the defender seeks to anticipate the attacker's next move in a discrete-time environment. Based on this prediction, the defender's strategy is to proactively neutralize the anticipated action from the attacker. An essential prerequisite for employing the defense is the detection of the attack itself, followed by the identification of its type.

Attacks detection and identification.

In general, an attack detector is required to ensure the timely activation of available defenses. The development of sophisticated detection mechanisms is particularly important for identifying unknown or previously unseen attacks. For the defense architecture, we consider two distinct scenarios based on the defender's awareness and capabilities:

1. **Informed Counter-Bias (Assumption of Known Attack):** In this scenario, the defender is fully aware of the attacker's bias injection (e.g., the specific bias magnitude and timing). The defender attempts to counteract the attack directly by injecting a measurable counter-bias signal into the control loop.
2. **Blind Compensation (Assumption of Unknown Attack):** In this scenario, the defender is not fully aware of the attacker's specific alterations. The primary objective is to maintain stable and continuous motor operation despite the impact of any disturbance. The defender's action is focused on compensating for the impact of the attacker's actions on the motor's state. This is achieved by correcting the estimated value of the angular speed ($\hat{\omega}$) using the inverse of the estimated distortion coefficient ($\hat{\chi}$) induced by the attacker. This compensation ultimately stabilizes the output voltages (u_a, u_b, u_c) from the inverter and the torque value (τ_L).

Defense creation

The first scenario, which involves Informed Counter-Bias, is illustrated in Figure 3.6, where the defender actively monitors the injected adversarial bias and prepares to inject a compensatory counter-bias signal into the feedback loop during the subsequent sampling cycle.

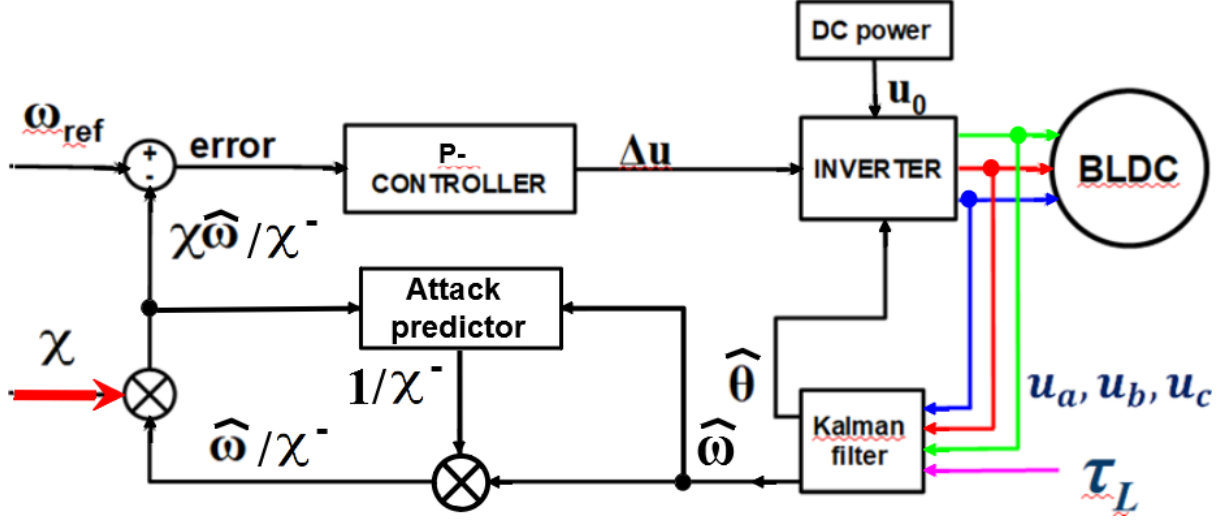


Figure 3.6: The first scenario, illustrating the defense mechanism under Informed Counter-Bias. The figure depicts the state where the attack detector is active and has successfully measured the adversarial bias. This measured bias is used to initiate a predictor component, which estimates the expected bias for the subsequent sampling cycle. The calculated compensatory **counter-bias signal** is then prepared for injection into the control loop in the next step.

The state when the defense is idle in the first scenario (Informed Counter-Bias) is illustrated in Figure 3.7. The output counter-bias signal in such a case is a nominal value of "1", resulting in zero compensation for the attacker's action, thereby offering no defense during this state.

The second scenario (the Blind Compensation) is illustrated in Figure 3.8, where the roles of the detector and defender are combined into a single functional block operating in parallel to the speed estimator. This combined functional block is capable of predicting the estimated distortion coefficient ($\hat{\chi}$). This estimate is then used to correct the estimated angular speed ($\hat{\omega}$), by applying a compensatory signal proportional to the inverse of the distortion ($\hat{\chi}$), thereby ensuring motor stability.

The idle state for the defense module in the second scenario (Blind Compensation) is illustrated in Figure 3.9. The module is turned off by setting the output of the counter-bias to a nominal value of "1". In this state, the defense block provides zero compensation; thus, any change in the observed output voltages (u_a, u_b, u_c) and torque (τ_L) results in a proportional change in the

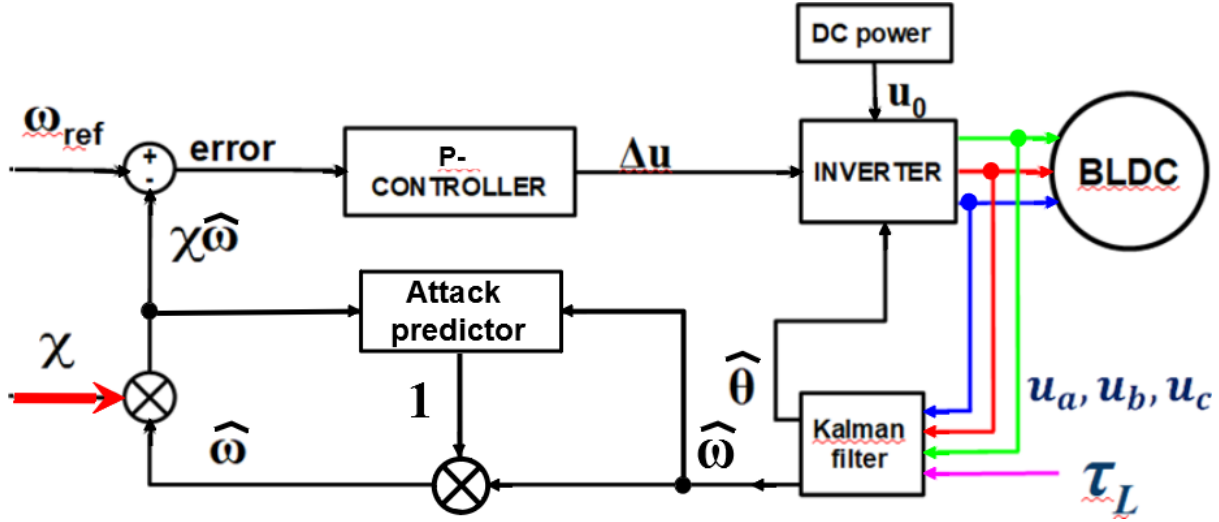


Figure 3.7: The defense mechanism block is **idle** in the scenario of Informed Counter-Bias. In this state, the block gives a nominal output value of "1" for the counter-bias signal, resulting in no active compensation.

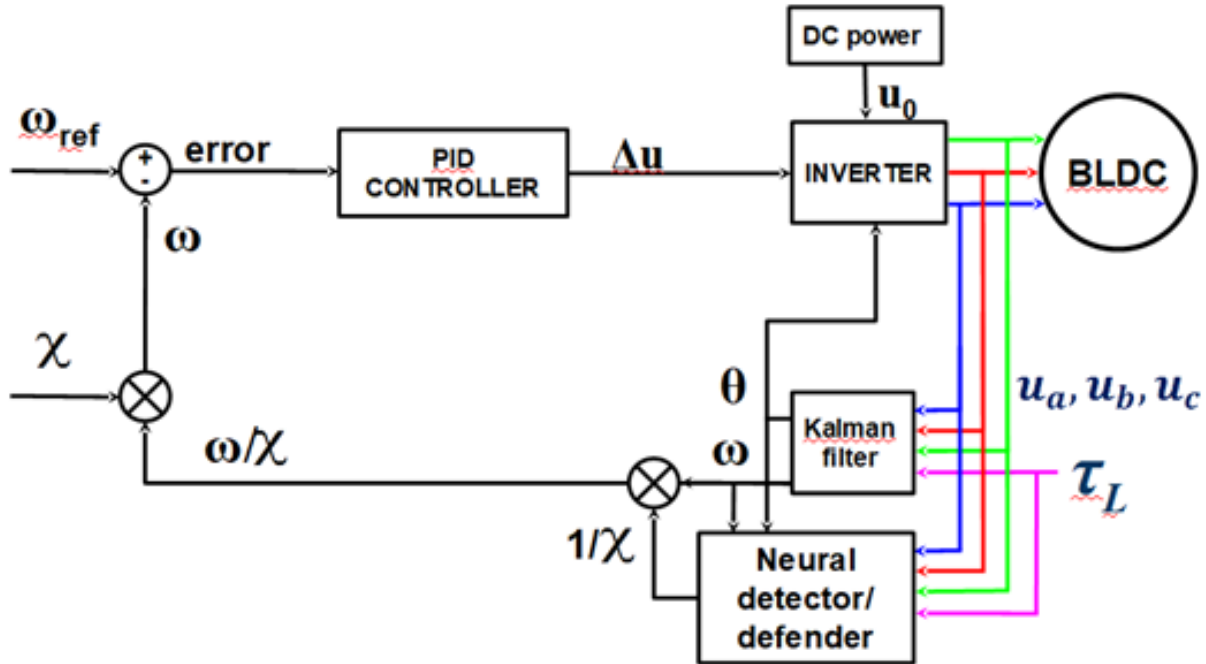


Figure 3.8: Operation of the Blind Compensation scheme of predictive defense against bias injection attack. From the values of the output voltages (u_a, u_b, u_c) from the inverter and the torque value (τ_L), the defender estimates the expected effect of the attacker action for the next sampling cycle and injects the counter-bias to sustain the required angular speed ω . The figure illustrates the ideal case where the estimate $\hat{\chi}$ equals the true but unknown distortion χ .

estimated angular speed ($\hat{\omega}$). The system treats these changes as legitimate deviations due to a change in the motor's operational mode rather than deviations caused by an attack.

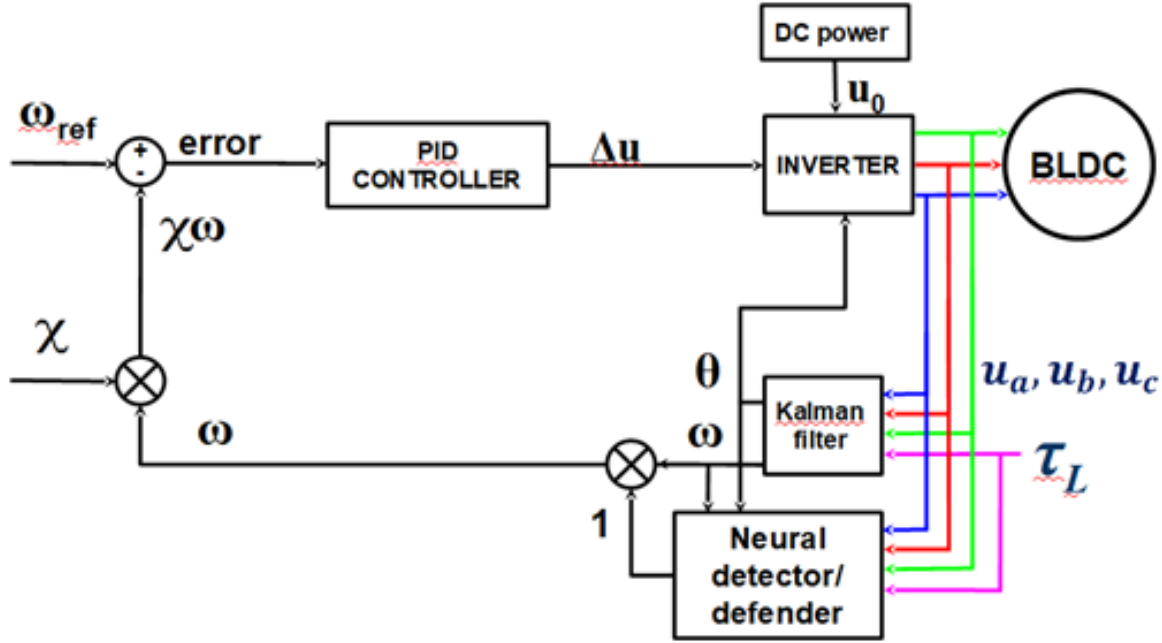


Figure 3.9: The idle state of the defense module in the Blind Compensation scheme. The attack detector is active and continuously monitoring the system, but the defense mechanism is functionally idle, providing a nominal output value of "1" for the counter-bias signal.

The scope of this thesis is deliberately limited to the first scenario (Informed Counter-Bias), where it is assumed that the general type of attack is known to the defender. This assumption is justified by the novelty and early theoretical stage of the proposed research, where the stealthiness of the attack is treated as a parameter still under investigation rather than a pre-fulfilled practical requirement. Accordingly, the functionality of attack detection and identification in this thesis is simplified, assuming timely and accurate recognition of the attack. This simplification allows any available defenses to be activated immediately, enabling the research to focus primarily on evaluating the efficiency of the defense strategies under development.

The concept of such defense relies on the potential ability of the predictor component to anticipate the attacking values of the distortion coefficient (χ) based on previous sampling steps. This enables the system to implement compensation in advance—specifically, one time step ahead of the actual system operation—to mitigate the attack's impact.

Chapter 4

Experimental Results

The foundational aspects of the proposed attack scheme were validated through simulation and modeling. The target system selected was a Brushless DC (BLDC) motor operating as a Cyber-Physical System (CPS), which uses a Kalman Filter as the state estimator to ensure timely commutation. Operation was verified under both open-loop and closed-loop control schemes.

To effectively isolate the dynamic effects of integration and differentiation on the system responses, the analysis initially focuses on a P-controller closed-loop scheme. Extending these scenarios to Proportional-Integral-Derivative (PID)-controlled circuits—which involves estimating the combined effects of the integral (I) and derivative (D) terms alongside the proportional (P) control structure—will require a separate, dedicated analysis.

4.1 Position Sensorless Drive of BLDC Motor

The control scheme shown in Figure 3.1 is simulated. A Kalman filter is employed in the feedback loop to realize the position sensorless drive of the BLDC motor. For analysis, the model's Kalman filter operates using two distinct data sampling modes when processing the motor's feedback output:

1. **Equal Angular Separation Mode:** Data is sampled based on estimated equal increments ($\Delta\theta$) of the rotor's angular position (θ_i). Thus, $\Delta\theta = \text{const}$, and the sampling rate varies inversely with the rotor's speed (ω).
2. **Equal Time Intervals Mode:** The time separation between data sampling points (t_i) is held constant. Thus, the sampling time interval $\Delta t = \text{const}$.

The results of the modeling and simulation, which focus on the effects of system parameters on the performance of the sensorless control scheme, are presented below.

4.1.1 Equal Angular Increments in Driving of BLDC Motor

For the simulation of the BLDC motor drive using the equal angular increments mode, the motor's phase voltages (u_A, u_B, u_C) are used to derive specific voltage variables required by the Kalman filter state estimator. These relations are detailed in Listing 4.1 using MATLAB notation.

The simulation first calculates the standard line-to-line voltages (u_{AB}, u_{AC}, u_{BC}). Subsequently, a set of transformed voltage variables ($U_{abca}, U_{bcab}, U_{cabc}$) are computed. These transformed variables, represented by the vector uk , are used as the observational inputs to the Kalman filter for estimating the rotor's angular position and speed.

Listing 4.1: Code in MATLAB notations for relations between voltage variables used as Kalman filter inputs for the equal angular increments drive simulation.

```
for n = 1:N
    uAB(n) = uA(n) - uB(n);
    uAC(n) = uA(n) - uC(n);
    uBC(n) = uB(n) - uC(n);
    Uabca(n) = uAB(n) + uAC(n);
    Ubcab(n) = uBC(n) - uAB(n);
    Ucabc(n) = -uAC(n) - uBC(n);
    uk(1,n) = Uabca(n);
    uk(2,n) = Ubcab(n);
    uk(3,n) = Ucabc(n);
end
```

Simulation Stages for Equal Angular Increments Drive

Four distinct operational stages were analyzed during the simulation of the BLDC motor drive utilizing the equal angular increments mode:

1. **Motor Start-up:** The initial phase, where the BLDC motor is driven from a standstill (zero angular position).
2. **Acceleration Phase:** The period immediately following start-up, characterized by increasing rotor speed.
3. **Acceleration Saturation:** The transition phase where the rate of acceleration decreases as the motor approaches the maximum speed permitted by the control voltage or load.

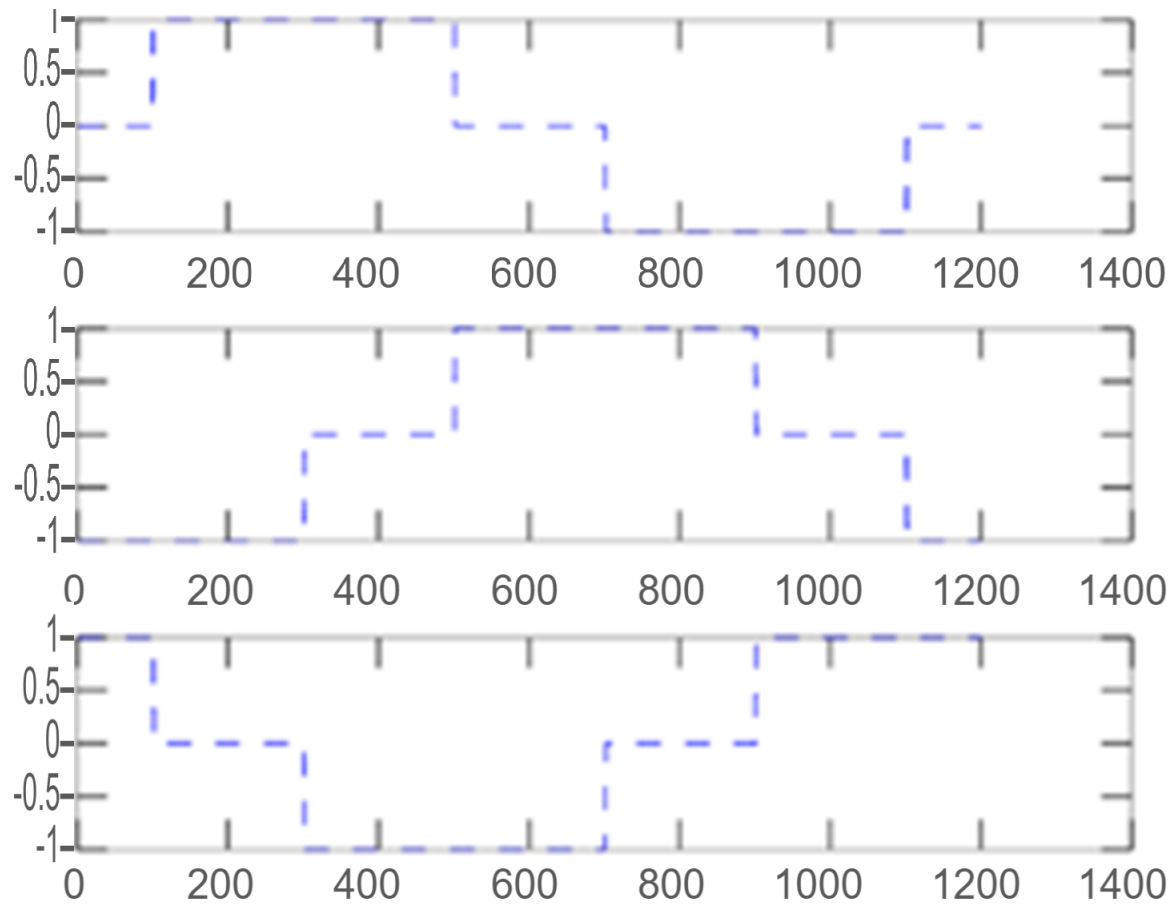


Figure 4.1: Operating voltages for the motor's phases A, B and C measured with respect to the ground (variables for parameters used in the program are: u_{AG} , u_{BG} , u_{CG}). Voltages are represented in relative units (proportional to variable $KV = 100$ scaling up factor (V)). Horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$.

4. **Steady-State Rotation:** The final phase, where the motor achieves and maintains a constant operational speed.

Test Case #1: Motor Start-up

Test case #1 analyzes the start-up of the BLDC motor from the initial condition: orientation angle $\theta = 0$ and initial speed $\omega_0 = 0$, with the rotation cycle number $M = 1$. The dynamic evolution of the state variables during this first driving cycle is presented in Figure 4.2. The figure demonstrates that the proper commutation of the winding currents results in rotor acceleration, which is notably higher in the first half of the very first cycle of rotation.

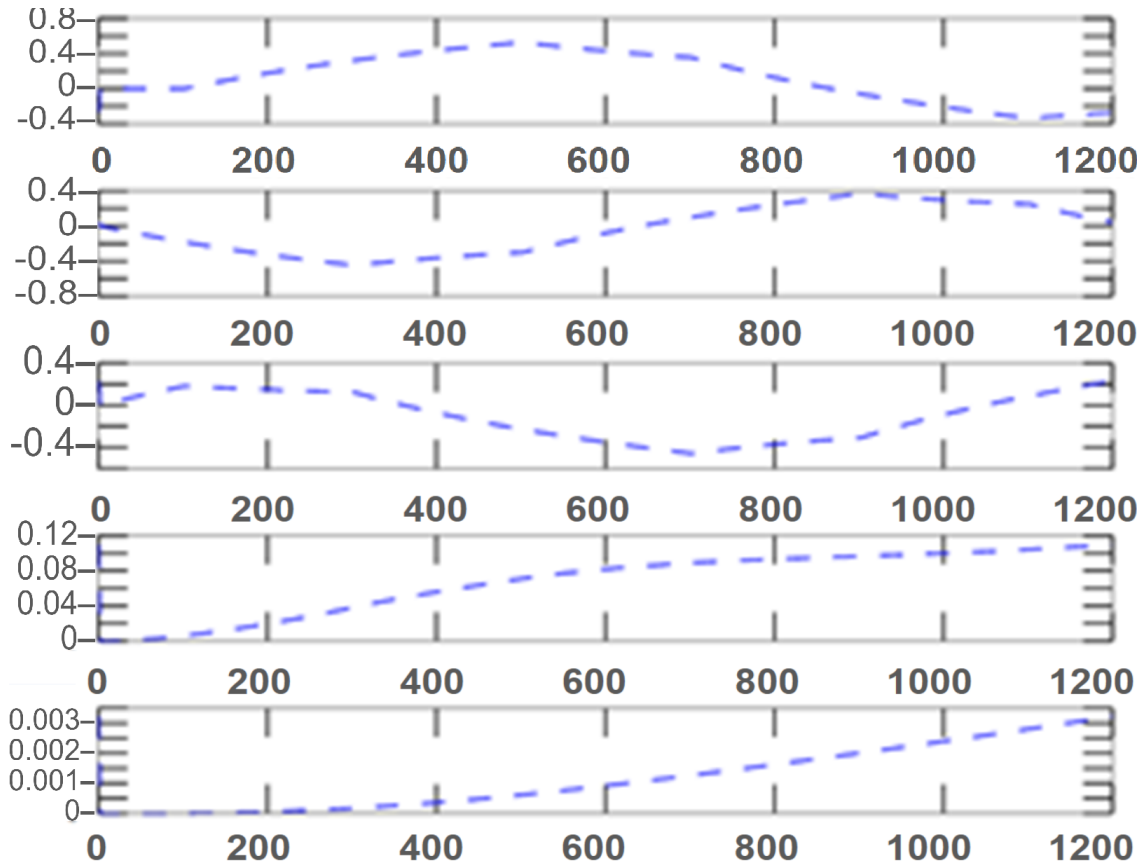


Figure 4.2: Test Case #1: Starting of BLDC motor from zero position (zero orientation angle $\theta = 0$, zero initial speed $\omega_0 = 0$, cycle number $M = 1$). Shown sequentially are the state variables (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). Vertical scales are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$.

Test Case #2: Acceleration Phase

The rotor's acceleration progressively increases with subsequent cycles, as Test Case #2 confirms in Figure 4.3 for the **11-th rotation cycle** (i.e., for $M = 11$).

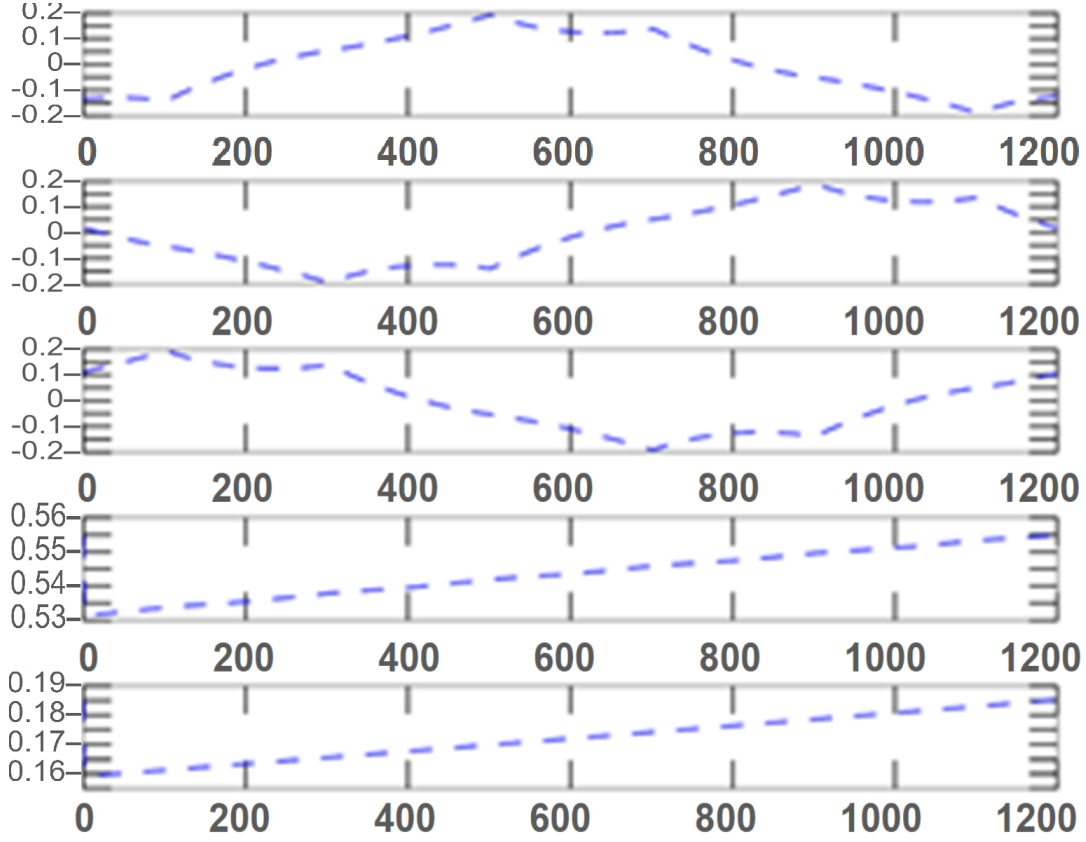


Figure 4.3: Test Case #2: Rotor acceleration stage (verification at the 11-th rotation cycle, $M = 11$). Shown sequentially are the state variables (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). Vertical scales are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$.

Test Case #3: Acceleration Saturation and Torque Ripples

The growth of acceleration eventually saturates, leading to the occurrence of torque ripples after approximately 100 rotations. This effect is demonstrated by Test Case #3 in Figure 4.4, which shows the system dynamics for the 111-th rotation cycle (i.e., for $M = 111$).

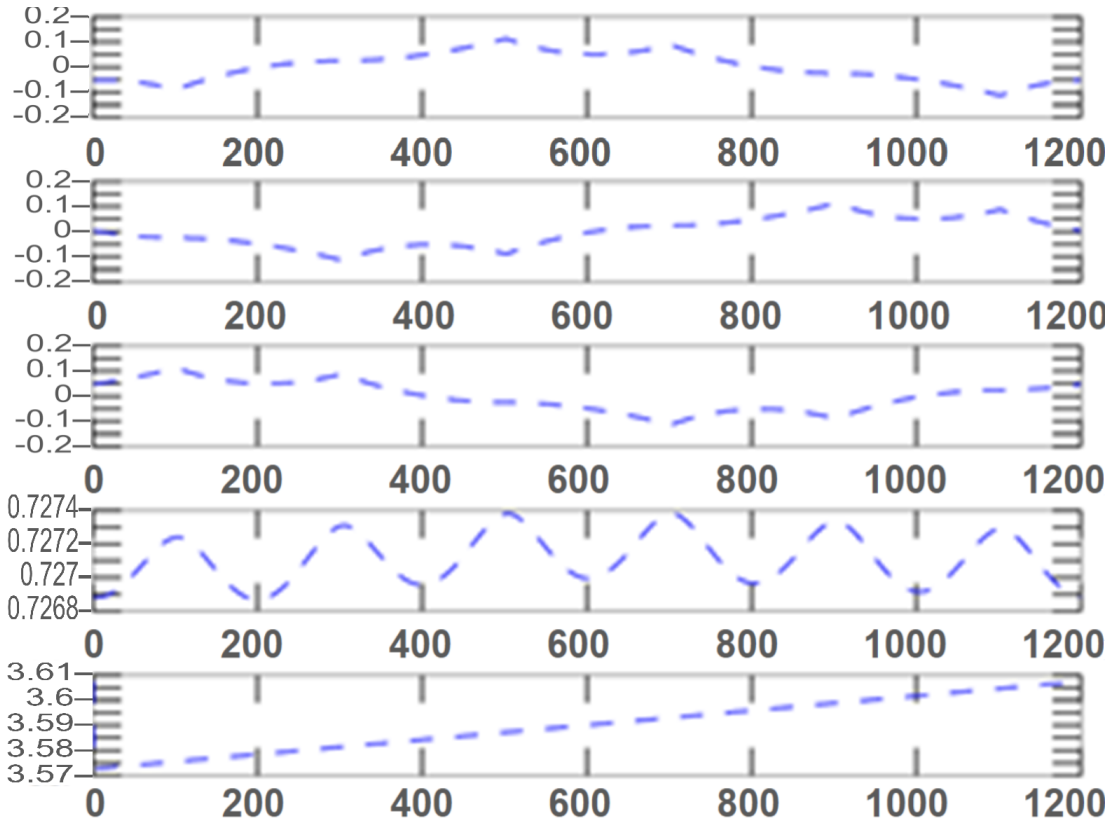


Figure 4.4: Test Case #3: Saturation of acceleration and onset of torque ripples after approximately 100 rotations (verification at the 111-th rotation cycle, $M = 111$). Shown sequentially are the state variables (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). Vertical scales are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$.

Test Case #4: Steady-State Rotation

This trend continues until steady-state rotation is reached after approximately 500 rotations. This final operating condition is verified by Test Case #4 in Figure 4.5, which shows the system dynamics for the 500-th rotation cycle (i.e., for $M = 500$).

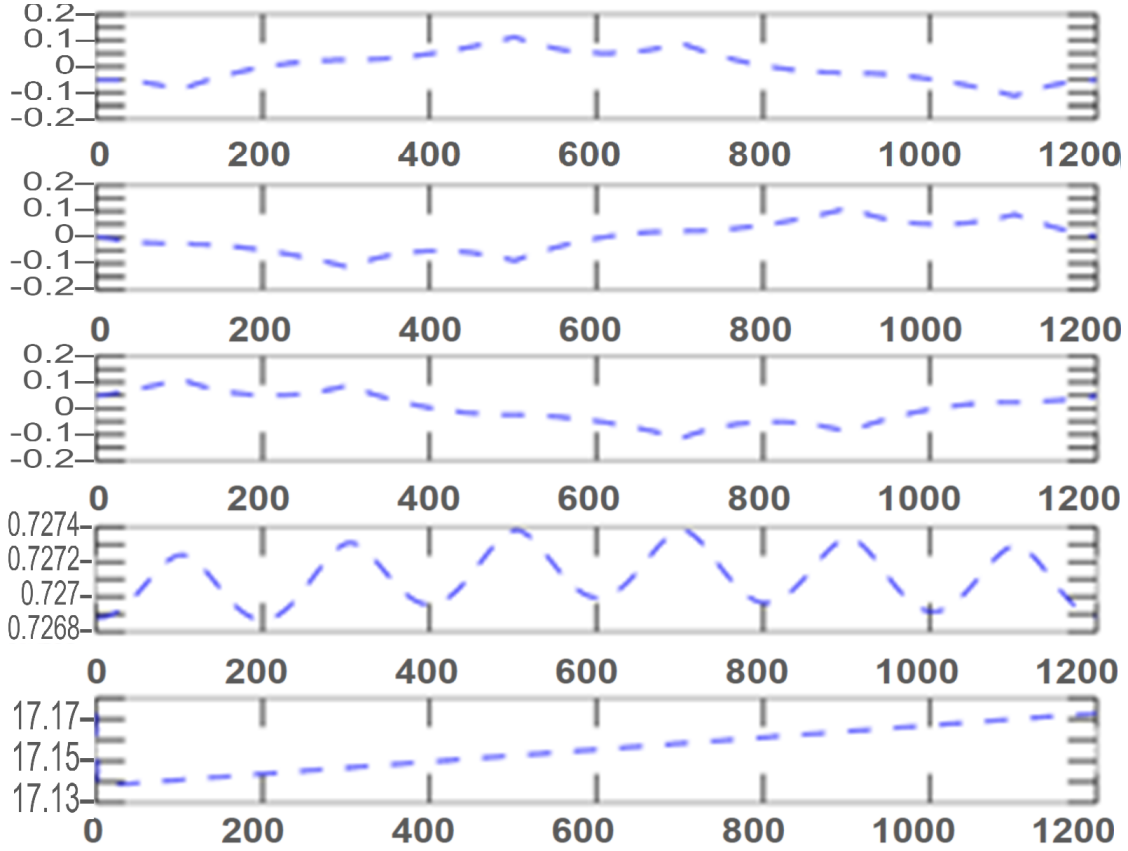


Figure 4.5: Test Case #4: Steady-state rotation achieved after approximately 500 rotations (verification at the 500-th rotation cycle, $M = 500$). Shown sequentially are the state variables (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). Vertical scales are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$.

Transition to Back-EMF Dependence

After the rotation speed reaches a certain level, the values of the generated back electromotive force (BEMF) become sufficiently large to sustain stable closed-loop sensorless control.

4.1.2 Equal Time Increments in Driving of BLDC Motor

The equal time increments drive of the BLDC motor is achieved by engaging the Kalman Filter (KF) estimator in the feedback loop with a constant sampling rate to estimate the commutation instances.

The initial angular speed for stable closed-loop sensorless control is established at approximately 1000 rotations/min (the entry level), from which the system evolves toward the upper speed limit.

The performance analysis for the equal time increments drive will therefore be conducted across a sequence of consecutive rotations, presented here as "frames" that illustrate the dynamic changes of the state variables.

The performance of the closed-loop BLDC motor control with the KF estimator is shown in Figure 4.6. The figure highlights the effect of torque ripple, which exhibits two distinct modulation frequencies: a lower frequency equal to the rotation speed, and a higher frequency that is six times the rotation speed.

The double increase in phase induction (to $L = 0.04$ H and mutual inductance $M = 0.02$ H) reduces the amplitude of the torque ripple proportionally, as shown in Figure 4.7.

Changing the sampling time (T) in the Kalman Filter (KF) estimator also affects the torque ripples. Specifically, reducing the sampling time T from $20 \mu\text{sec}$ (as used in Figure 4.7) to $15 \mu\text{sec}$ facilitates the reduction of the essential ripples, as shown in Figure 4.8.

The balance between the external torque load and the input voltage amplification coefficient (K_V) is illustrated in Figure 3.4 as a transient response beginning at $t = 0.5$ s.

The coefficient K_V (represented by the variable KV in the MATLAB code) serves as a scaling factor, converting the reference input voltages (shown in Figure 4.1) into the actual motor drive voltages.

In Figure 3.4, the external load changes abruptly at $t = 0.5$ s, increasing from 0 to $20 \mu\text{N}$. To counterbalance this load and maintain speed stability, the amplification coefficient is adjusted in the simulation from $K_V = 100$ to $K_V = 125$.

With this successful load balancing, the motor speed is first stabilized. We then proceed to induce a speed increase via a step-function input, followed by stabilization at a higher operational speed. This ensures the attack is initiated under stable, well-defined operating conditions.

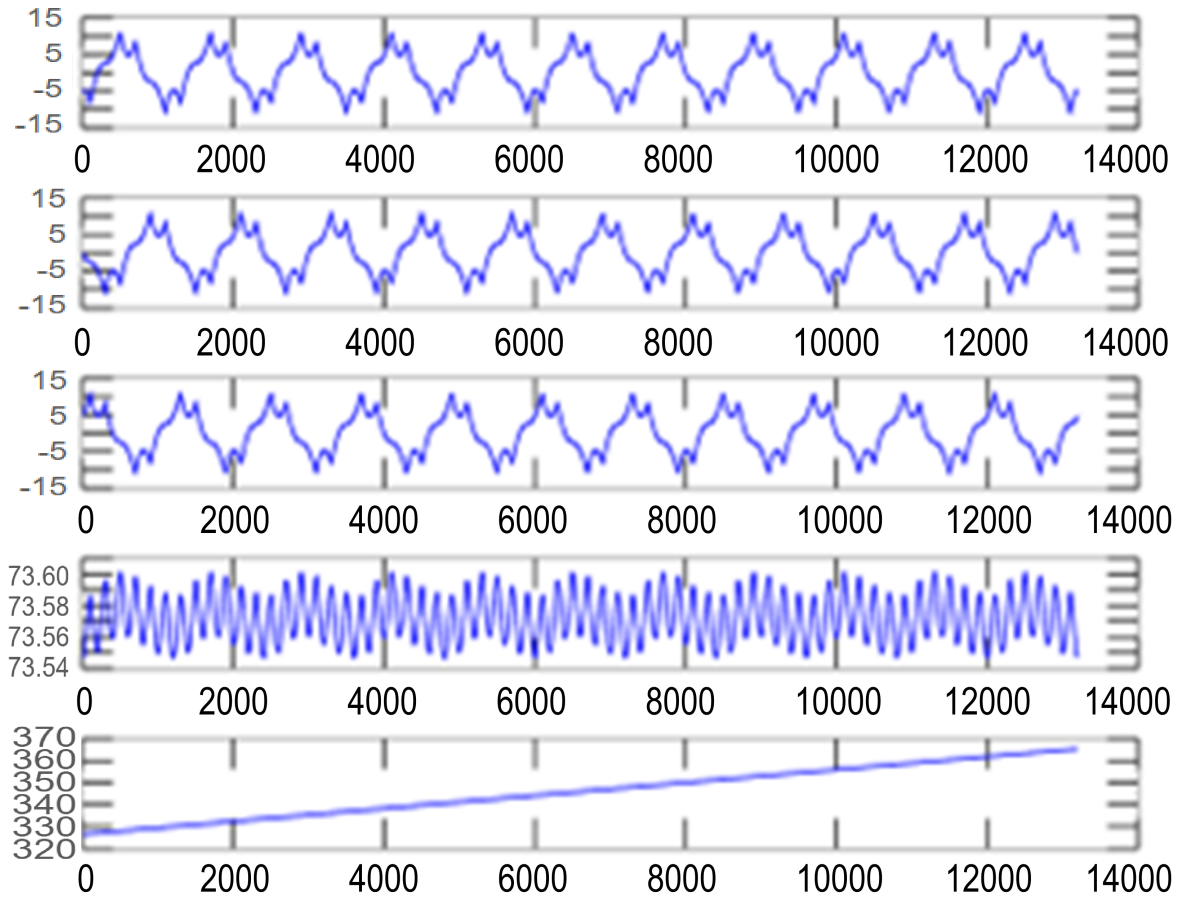


Figure 4.6: Open-loop control of BLDC motor using the Kalman Filter (KF) with an equal time increments drive. Shown are 10 consecutive frames, starting with frame number 101 and ending with frame number 111. The state variables are shown sequentially (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). **Vertical scales** are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$.

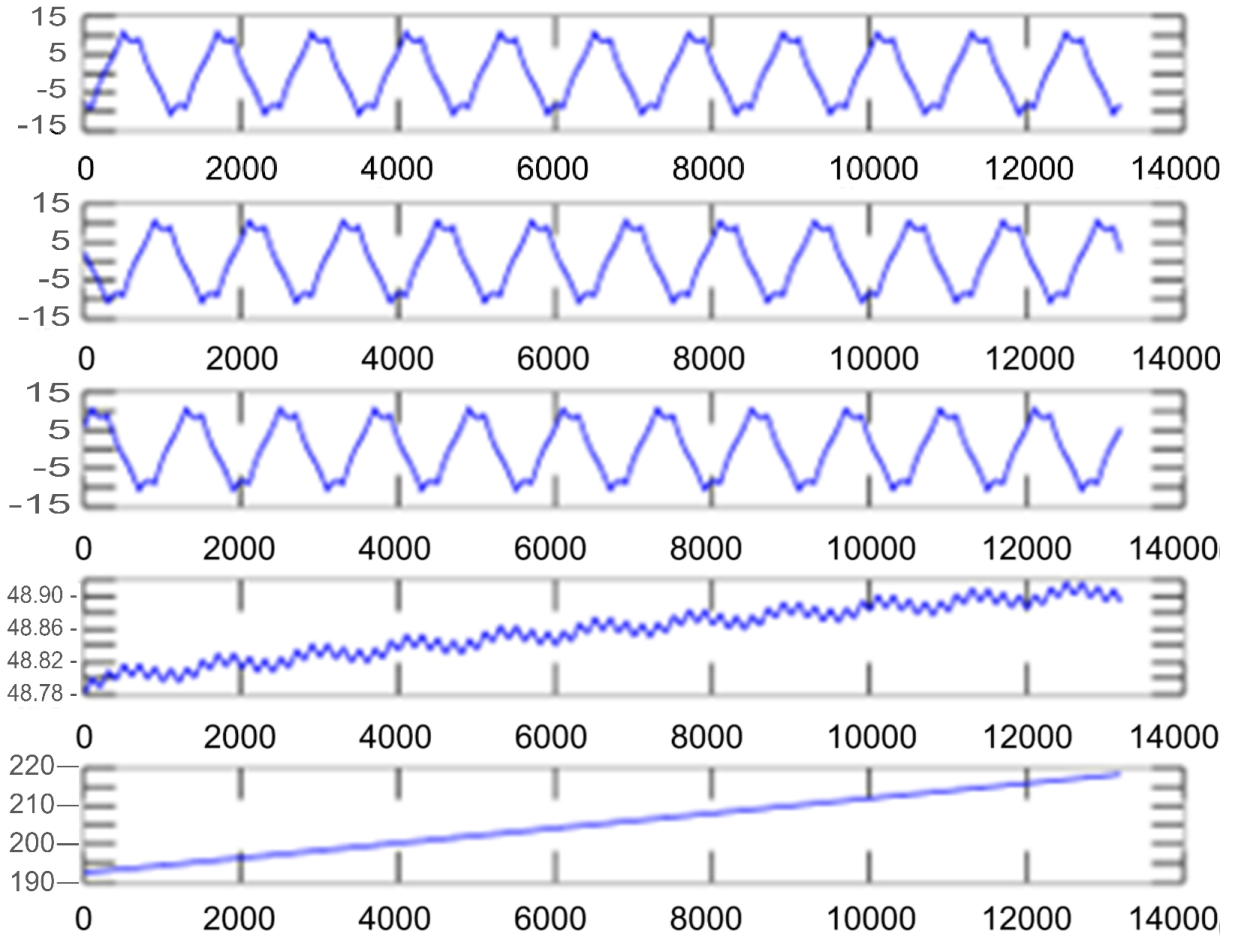


Figure 4.7: Reduction of torque ripples via increased motor induction. The inductance values are doubled compared to Figure 4.6, reaching $L = 0.04$ H and mutual inductance $M = 0.02$ H. Shown sequentially are the state variables (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). Vertical scales are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $20 \mu\text{sec}/\text{step}$.

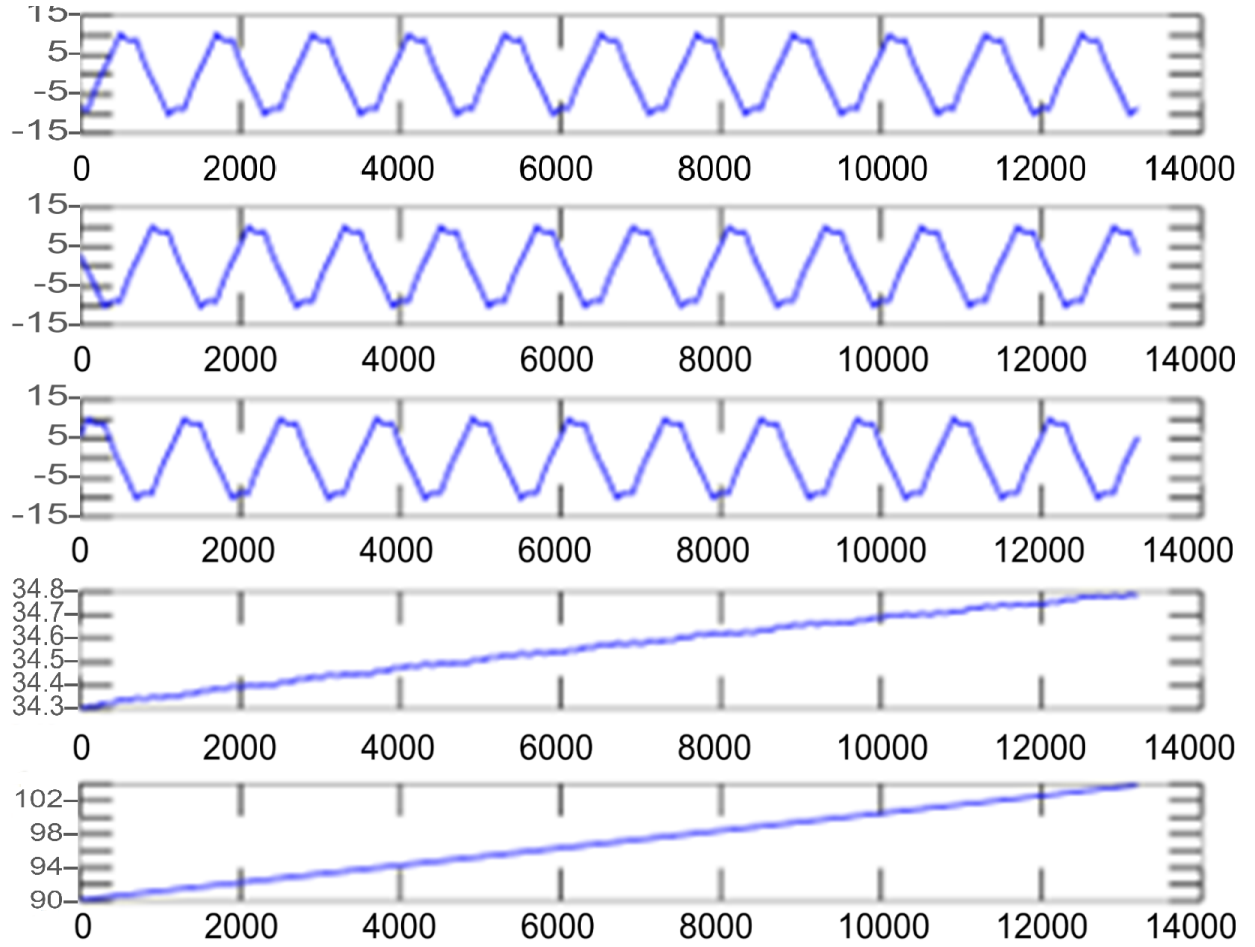


Figure 4.8: Further reduction of torque ripples achieved by reducing the Kalman Filter (KF) sampling time $\Delta t = T$ from $20 \mu\text{sec}/\text{step}$ down to $15 \mu\text{sec}/\text{step}$. Other parameters remain the same as in Figure 4.6. Shown sequentially are the state variables (from top to bottom): three phase currents, angular speed (ω), and electrical angle (θ). Vertical scales are in relative units and are sequentially as follows: proportional to Amperes for phase currents, rad/sec for angular speed, and rad for electrical angle. The horizontal scale is in relative step units, assuming to be scaled up by $15 \mu\text{sec}/\text{step}$.

4.2 Probing Mode Cyber-attacks

An attacker’s decision to perform low-impact probing prior to a full-scale assault reflects a deliberate trade-off between stealth and information acquisition. By conducting limited, cautious tests rather than immediately escalating to destructive actions, the attacker reduces the probability of rapid detection and response—thereby preserving access to the target environment for longer periods. At the same time, these measured probes provide critical empirical feedback: they reveal how the system processes unexpected inputs, how control logic and safety interlocks respond, and whether monitoring or anomaly-detection mechanisms trigger alerts. The knowledge gained enables the adversary to refine their selection of attack vectors, timing, and payloads to maximize effect while minimizing exposure. From the attacker’s perspective, this measured approach increases the likelihood of success because it converts uncertainty about the victim’s defenses into actionable intelligence, allowing prioritization of scenarios that offer the highest impact-per-risk ratio.

Ethically and practically, documenting this motivation is important for defenders: understanding why adversaries probe helps security teams prioritize sensitive detection points, instrument system responses to low-level anomalies, and design deception or canary mechanisms that convert reconnaissance into early warning. Framing probing behavior within a threat model therefore serves both to explain attacker incentives and to guide mitigation strategies that reduce the strategic advantage gained through stealthy reconnaissance.

Next, we consider the implementation of possible probing attack variants against the BLDC motor control system, where the attacker has gained control over the feedback loop data flow (as shown in Figure 3.3). For the attacker, ‘probing’ here means introducing a perturbation small enough to evade detection but large enough to be measured through a tangible parameter, allowing the attacker to scale up for prognostic escalation. The two variations of the attacks implemented in the probing mode explored below are:

- 1) the double-step function bias injection.
- 2) the linearly increasing bias injection.

In our simulations, the bias injection probing attack will commence at $t = 1.5$ sec and terminate at $t = 2.0$ sec, denoted by the time interval $\tau = [1.5, 2.0]$. This probing attack duration will be explicitly indicated on the respective plots using a red arrow along the timeline.

4.2.1 Probing by double-step function bias injection

First, we implement a probing attack by injecting a double-step bias function (illustrated in Figure 3.5, a), where the bias coefficient is set to a constant $\chi = 1.5$ during the attack and $\chi = 1$ otherwise.

The probing attack time range is $t = [1.5, 2.0]$ sec, and the resulting system behavior is displayed in Figure 4.9. The system response is fully consistent with the step-function test (ii) shown in Figure 3.4. Specifically, the injection of a positive bias ($\delta\omega > 0$) yields a negative control voltage ($\Delta u < 0$) because the P-controller attempts to suppress the perceived excess of estimated angular speed. After the probing attack concludes, the bias is removed, and the system recovers similarly but with the expected opposite sign in the generated Δu values.

In Figure 3.4, the bias distortion coefficient χ is set to 1.5 within the attack interval $t = [1.5, 2.0]$ and 1.0 otherwise, with a P-controller coefficient $K_p = 10$. The values for i_a are in Amps, and ω and $\hat{\omega}$ values are in rad/sec.

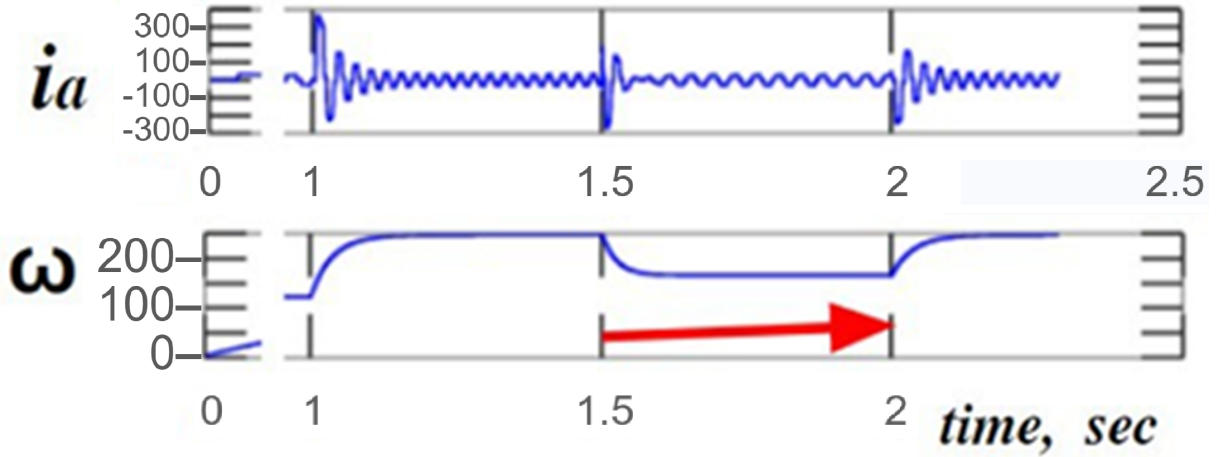


Figure 4.9: Probing mode attack with double-step function as bias distortion coefficient. Values of i_a are in Amps, values of $\omega = \hat{\omega}$ are in rad/sec.

This probing attack test allows the attacker to deduce the following critical system features:

1. The amplitude of the system response to the injected bias.
2. The sign of that response.

3. The system's inertia (i.e., the characteristic time constant for system response).

Furthermore, observing the system's response to the applied bias amplitude directly reveals the absence of effective defensive mechanisms designed to counter that level of injection.

These observations allow the attacker to better prepare for subsequent selection and variation of attacking strategies.

4.2.2 Probing by linear ramp bias with initial shallow drop

As the next step, we transition the bias function coefficient (χ) to the linearly increasing after initial shallow drop bias profile shown in Figure 3.5b, applied over the entire probing duration. We will also refer to this as the linear ramp after shallow drop bias. This mode first introduces a controllably limited initial drop in bias, followed by a gradual injection of bias that accumulates via small, incremental changes throughout the probing attack. This avoids the abrupt exposure caused by a full-scale step function.

The initial drop of χ constituted $\Delta\chi = 0.25$ from its equilibrium value of 1, reaching $\chi_{min} = 0.75$. This drop is relatively shallow. The linear increase of χ that followed reached the value of $\chi_{max} = 1.25$, thus rising above the equilibrium level by the same amount, $\Delta\chi = 0.25$. This profile therefore provides a total height of the bias ramp equal to $\chi_{max} - \chi_{min} = 0.5$, which matches the total height used for the double-step probe discussed in Subsection 4.2.1. Here χ_{max} and χ_{min} represent maximum and minimum of χ values in the probes.

Unlike the double-step probe, the injection with linearly accumulated increments requires the system to accommodate the distortion through a slower rate of change in the χ parameter. While the final parameter value (χ) is the same as in the previous probing attack test, the system experiences a series of small, rapidly-damped transient events that are negligible, allowing for smooth accommodation of the increasing bias across the discrete time steps. Such a gradual development of the probing injection attack also assists the attacker in keeping the probe stealthy.

The system response is shown in Figure 4.10, where the bias coefficient rate χ' is set to 0.00004286 within the attack range $t = [1.5, 2.0]$, and the P-controller coefficient is $K_p = 10$.

This probe reveals the system's response dynamics: first, the initial response to the bias drop, where the angular speed (ω) evolves towards higher values, followed by the gradual accumulation of impact during the ramp, causing ω to progressively decrease. Data gathered from this probe and the previous double-step bias probe allow the attacker to estimate the resulting current increase in the motor's windings and, consequently, the potential impact on the motor's electronic circuits.

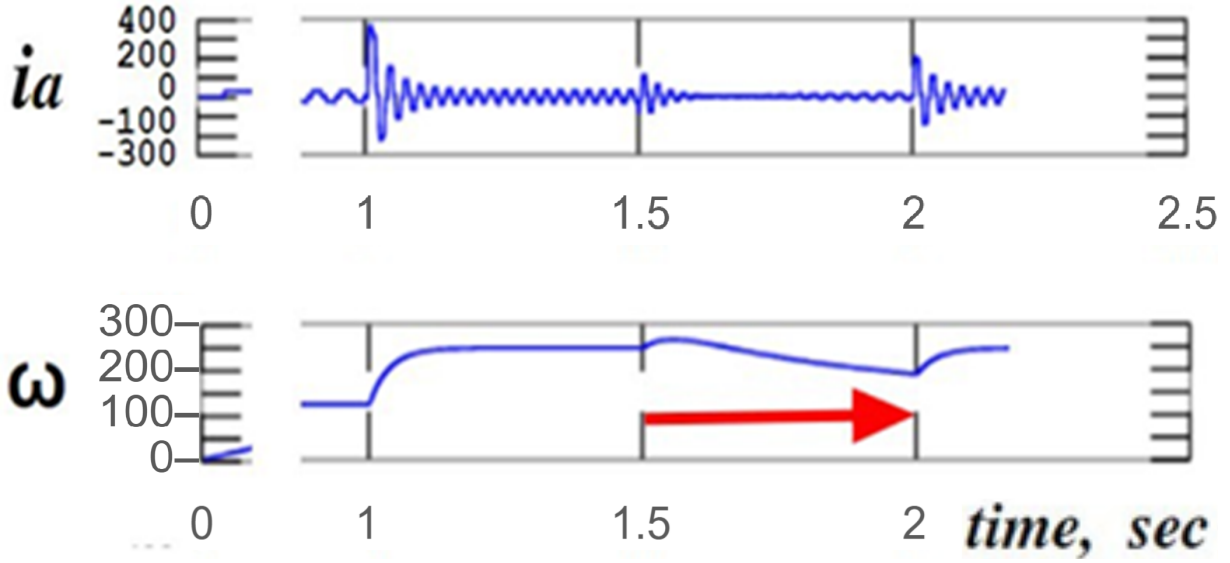


Figure 4.10: Probing attack by linear ramp bias with initial shallow drop Values of i_a are in Amps, values of $\omega = \hat{\omega}$ are in rad/sec, time in sec (horizontal axis).

Having observed the transient responses of the system on the above probes, the attacker may further expand variability of the probes via designing saw function probe considered in the next subsection.

4.2.3 Saw Bias Probe Injection

In constructing the saw function for the probing bias injection coefficient χ , the gradient was retained as the same constant slope used in the linearly increasing probe profile. This relationship is visually reflected in Figures 3.5c and 3.5d, where the triangles forming the saw teeth are scaled-down versions of the initial triangle of the ramp probe shown in Figure 3.5b.

The saw bias probe differs from the previously considered linear ramp bias probe with initial shallow drop (discussed in Subsection 4.2.2) in that the linear growth of χ is constrained, never exceeding the equilibrium level of $\chi = 1$. Consequently, χ resets to its bottom (i.e., χ_{min}) each time it reaches the equilibrium level. The justification for this sawtooth probe design anticipates that the system's response during the first sawtooth period—following the initial shallow drop of χ —should closely mirror the response observed in the linear ramp bias case (see Section 4.2.2). Any significant deviation from this trend is therefore expected only after the probe enters the second sawtooth period. This anticipation appears to be correct, as demonstrated by the actual results shown in Figure 4.11.

The key outcome observed from the saw bias probe injection is the ability to induce a sig-

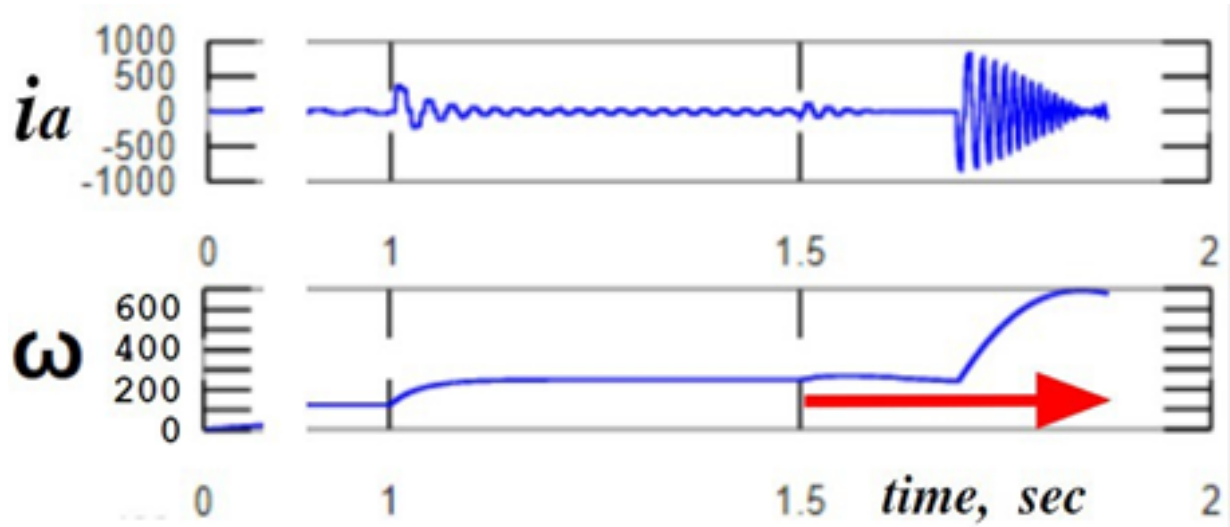


Figure 4.11: System response to the saw bias probe injection profile. The current surge is delayed during the first saw tooth and begins at the start of the second period when ω dropped by $\delta\omega = 59.52$ rad/s. **Parameters:** A probe rate $\chi' = 4.286 \times 10^{-5}$, $K_p = 10$, and attack start time $t = 1.5$ s. Current i_a is shown in Amperes (A), angular velocity ω (or $\hat{\omega}$) in rad/s, and time t in seconds (s).

nificant increase in rotor acceleration and angular velocity (ω) (of about triple value from about 200 rad/s up to about 600 rad/s). This increase effectively overrides the motor's control functionality as managed by the host system, which set up a potential target for the attacker.

Another byproduct of this probe is a high surge in the current values operating in the motor windings. While this current surge may fall outside the attacker's direct observation—as we assume control only over the feedback control loop data flow of ω —it is still a relevant threat. The surge is potentially well within the reach of the attacker to be inferred from the known host system operating relationships, where an increase in ω is necessarily connected to an increase in the motor's winding currents. Specific values experienced by the host system during this saw bias injection probe are approximately 750 Amps, as shown in Figure 4.11. Such high currents may be damaging to the motor's operating circuits, which is of potential interest to the attacker if their goals include inflicting electrical damage on the host system. Alternatively, the attacker may be interested in the possibility of inducing significant power losses by rendering the motor's operation inefficient.

Based on the results from the above probe injections, the attacker may now design a damage-inflicting attack, which we will next consider and call the **current drainage attack**.

4.3 Current Drainage Cyber-Attack

Now that the attacker has obtained basic information about the host system's responses to the probing attacks, the next logical step is to plan and execute a full-scale attack emphasizing the discovered vulnerabilities. Since prior tests established the system's susceptibility (i.e., confirmed the lack of countermeasures), the primary goal of this stage is to quantify the maximum damage that can be inflicted upon the system components through sustained current manipulation. Specifically, we estimate the physical damages resulting from maximizing the current drainage inherent in the highly distorted commutation sequences. The subsequent subsections will detail the attacker's methodology for exploiting the two primary pathways for such destruction: maximizing mechanical wear through aggressive speed oscillation and maximizing electrical stress through prolonged, high-current surge overlap.

4.3.1 Attack Objectives and Manifestation

The primary goal of this attack is to inflict a *severe current surge* in the motor windings via bias injection into the feedback control system for the *BLDC motor*. This is achieved by misleading the controller about the actual angular velocity (ω) to provoke an erroneous correction via *forced acceleration*. The major expected damage would be to the electrical circuits of the motor controls, possible **overheating** of the motor's windings, as well as *efficiency loss* due to induced energy loss. Therefore, the current drainage attack builds directly upon the observable effects of the saw bias probe, specifically targeting the motor's thermal and electrical limits, which the attacker infers from the observed ω data. The attack mechanism involve the controlled over-excitation within the host. Specifically, the core of the attack is exploiting the *inefficiency* or damage threshold of the motor's drive circuitry.

1. **Leveraging the Sawtooth:** The attacker uses the saw bias profile because it forces the controller into aggressive, repetitive corrective actions (high acceleration/deceleration cycles around the setpoint).
2. **Inference and Calibration:** As established, the attacker infers the ω change, which is necessarily linked to high current (i_a) draw. The attacker calibrates the frequency and amplitude of the saw function (using χ' and $\Delta\chi$) until the predicted current surge (like the 750 A observed previously) pushes the system close to its rated limits - but ideally just below the threshold that would trigger hardware protection mechanisms.
3. **Continuous Load:** Unlike a single-shot spike, the current drainage aspect implies a sustained, high-load operation. By keeping the controller misinformed via the periodic bias

injection, the motor is forced to operate continuously at a state where power consumption is high but output is inefficient or non-nominal.

This mechanism has two primary, intertwined objectives derived from forcing sustained, high-current operation:

1. Electrical Component Damage (Critical) The most severe outcome is immediate or long-term hardware failure.

- **Target:** The motor windings and the Motor Control Unit (MCU) power electronics (like MOSFETs or IGBTs).
- **Mechanism:** Sustained operation near or above the 750 A mark leads to Joule heating ($P = I^2 R$). This rapid, continuous generation of waste heat can cause insulation breakdown in the windings or thermal failure in the switching transistors.

2. Efficiency Loss and Thermal Degradation (Power Drainage) If immediate failure is avoided, the sustained inefficient operation leads to degradation.

- **Inefficiency:** The controller is constantly over-correcting or oscillating around the commanded state, leading to high reactive power or dissipated energy that does not contribute to the desired mechanical work. This is the "power loss" component.
- **Thermal Stress:** Even if currents stay below the critical failure point for a short period, prolonged exposure to elevated temperatures significantly reduces the lifespan of electronic components and motor insulation. This is a stealthier damage vector than outright burnout.

In short, the current drainage attack is a rate-limited, sustained overload attack masked as control oscillation, designed to trigger thermal runaway or electronic component aging.

The attacker can infer the success of their action by observing the increase in the angular velocity (ω), as this rise is directly related to the current surge the attack is designed to induce. This increase in (ω) can also be considered a secondary goal for the attacker, since its implementation simultaneously ceases host control over the motor operation. Consequently, if the motor controls other functionalities of the larger system, those functionalities become compromised as well. For example, this larger system could be an electric vehicle, an industrial centrifuge, or an electrical pump. In some scenarios, seizing control over the motor's operation may become the primary goal for an attacker aiming for higher consequences than mere efficiency disruption and/or circuit malfunctioning.

Constructing the attacking function for injecting distortion χ into the ω data stream involves two elements: 1) an initial drop of χ from the equilibrium level of 1, similar to the saw bias probe but executed to a greater depth (specifically, close to zero while keeping $\chi > 0$); and 2) sawtooth modulation upon the bottom level using a triangular shape, growing linearly from the lowest level $\chi = \chi_{\text{bottom}}$ up to the set sawtooth height $\chi = \chi_{\text{top}}$. Both parameters defining the sawtooth profile—the base level, $\chi = \chi_{\text{bottom}}$, and the height of the teeth, $\Delta\chi_{\text{saw}} = \chi_{\text{top}} - \chi_{\text{bottom}}$ —may be varied by the attacker across a range of values.

We classify the sawtooth function based on its base level: it is defined as deep-leveled if χ_{bottom} is close to zero in the positive domain, intermediate-leveled when in proximity to $\chi = 0.5$, and shallow-leveled when close to the equilibrium level of 1.

Furthermore, we distinguish several cases based on the modulation amplitude, defined by the tooth height $\Delta\chi_{\text{saw}}$: small modulation amplitude when $\Delta\chi_{\text{saw}} \approx 0.1$; intermediate modulation for $\Delta\chi_{\text{saw}} \approx 0.5$; large-amplitude sawtooth for $\Delta\chi_{\text{saw}} \approx 1$; and wide-range modulation for $1 < \Delta\chi_{\text{saw}} < 1.5$.

The attacker can infer from the probing attacks that the strongest rotor acceleration—and consequently the strongest current surge in the windings—is achievable using the deep-leveled distortion function (for our consideration of the sawtooth function the χ_{bottom} is to be taken close to zero). While the subsequent analysis focuses on refining this sawtooth profile, note that the attacker is not strictly limited to this function for general attack design. The next verification step required is the selection of the tooth height, $\Delta\chi_{\text{saw}} = \chi_{\text{top}} - \chi_{\text{bottom}}$, to optimize the attack's effectiveness within this specific sawtooth framework. We therefore consider three available options for the attacker: large modulation depth where $\Delta\chi_{\text{saw}} < 1$; intermediate modulation where $0.1 < \Delta\chi_{\text{saw}} < 0.5$ (approaching 0.5); and small modulation where $0.001 < \Delta\chi_{\text{saw}} < 0.1$ (approaching 0.1).

4.3.2 Deep-leveled, Large-amplitude Modulation Saw Teeth

First, we consider the deep-leveled saw function with large-amplitude modulation (Figure 4.12). The system responds with a strong attempt to compensate for the misleading signal, which suggests a drop in angular velocity (ω) from the stationary level of 250 rad/s down to a deceptive low value (e.g., 2.5 rad/s). This forces an accelerated growth in the operating angular speed, which saturates near 700 rad/s as the χ value linearly increases to χ_{top} . Following saturation close to $\chi = \chi_{\text{top}}$, the system response attempts to decelerate as χ continues its upward trajectory towards the equilibrium level, until the end of the tooth cycle when χ instantly drops back to χ_{bottom} in the next sampling iteration, thus restarting the aggressive acceleration phase.

The attacker infers that the rotor's acceleration is caused by the surge of current in the motor's

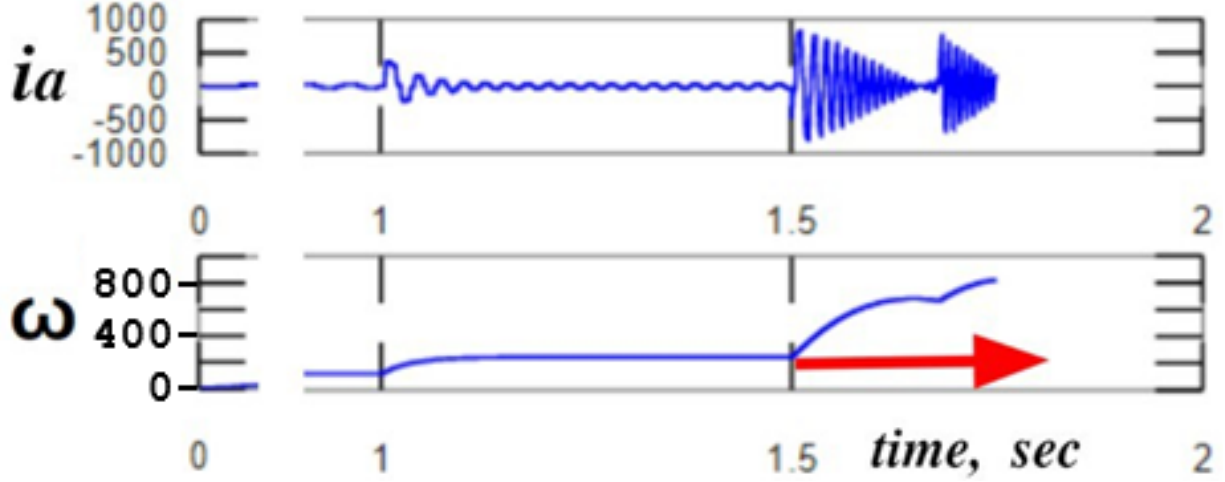


Figure 4.12: Performance of the deep-leveled saw function with **large-amplitude modulation** saw profile in bias injection on system response – the current drainage effect is periodic, as the saw tooth sequence is. Saw tooth depth is initialized at $\delta\omega = 23.81$ rad/sec level, $\chi' = 0.00004286$, $K_p = 10$, attack starts at $t = 1.5$ sec. Values of i_a are in Amps, values of $\omega = \hat{\omega}$ are in rad/sec, time is in seconds (horizontal axis).

windings. Figure 4.12 demonstrates this current surge specifically for winding "a" (i_a). The strongest current surge, reaching up to about 800 Amps, corresponds to the initial drop of χ to χ_{bottom} , which is immediately followed by the first upward sweep of the sawtooth.

The attacker achieved the following by employing the deep-leveled saw function with large-amplitude modulation (Figure 4.12):

1. **Mechanical Stress:** The system was tricked into a wasteful acceleration-deceleration sequence, imposing significant mechanical wear on the motor by tripling the rotor speed (ω) above its equilibrium level and periodically transient deceleration phases into overall accelerating trend.
2. **Electrical Stress and Inefficiency:** Periodical surges of electrical current were induced in the motor's windings, reaching peak values of approximately 800 Amps. These surges cause operational inefficiency due to energy losses and heat production.
3. **Control Override and Danger:** The extreme acceleration values effectively override the system's control over the host operation. Furthermore, the current surges drain energy from the system and pose a potential danger to the control circuits.

4.3.3 Deep-leveled, Intermediate-amplitude Modulation Saw Teeth

Next we consider a scenario in which the attacker keeps the saw function at the same deep level ($\chi_{\text{bottom}} \approx 0$), but reduces the modulation amplitude to the intermediate level. The teeth of the saw are still kept similar to those of the large-amplitude modulation saw, meaning the triangles retain the same shape but their size is reduced by approximately half. Maintaining this similarity requires keeping the value of the first derivative for χ constant; in our case, this rate is $\chi' = 4.286 \times 10^{-5}$.

The result of applying the deep-leveled, intermediate-amplitude modulation sawtooth function is shown in Figure 4.13. It can be seen that the areas of induced current surges now overlap for neighboring teeth, resulting in the elimination of deceleration stripes; only modulated acceleration stripes remain. The motor is continuously accelerating, but the rate of acceleration is not constant - it is modulated by the frequency and shape of the sawtooth, causing ripple in the torque/speed curve.

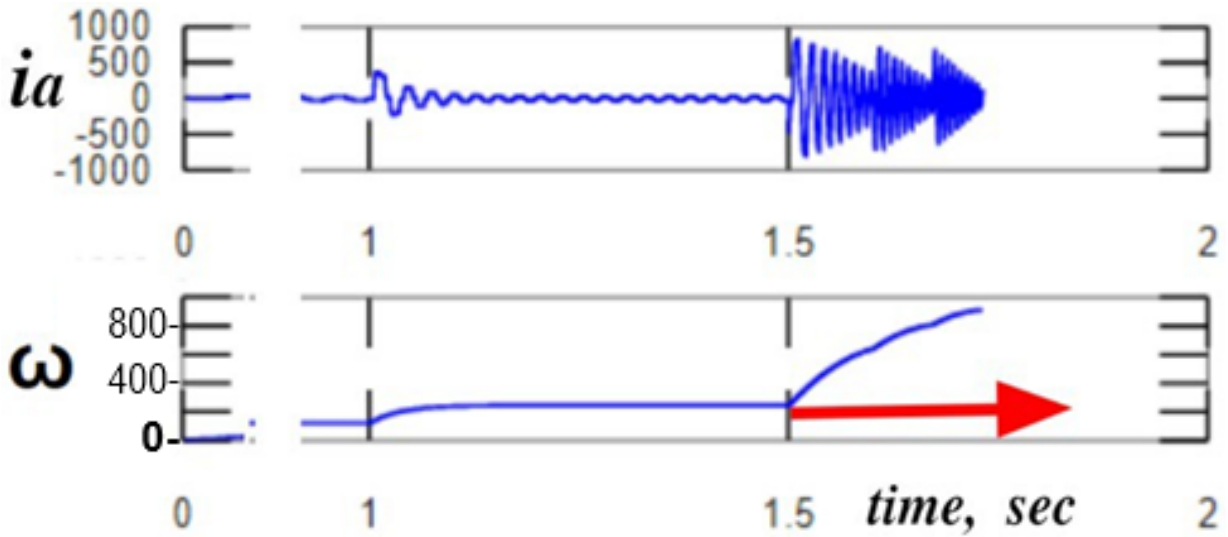


Figure 4.13: Performance of the deep-leveled, intermediate-amplitude modulation sawtooth function in bias injection on system response – the current drainage segments begin to overlap. Saw tooth depth is initialized at $\delta\omega = 11.9$ rad/sec level, $\chi' = 0.00004286$, $K_p = 10$, attack starts at $t = 1.5$ sec. Values of i_a are in Amps, values of $\omega = \hat{\omega}$ are in rad/sec, time is in seconds (horizontal axis).

The key observation is the elimination of deceleration phases. This makes perfect sense for the attacker:

- **Large Amplitude** ($\Delta\chi_{\text{saw}} \approx 1$): The saw swung from $\chi_{\text{bottom}} \approx 0$ all the way up to $\chi_{\text{top}} \approx 1$. When χ was close to 1 (equilibrium), the controller might have started pulling back (deceleration) before the cycle reset.

- **Intermediate Amplitude** ($\Delta\chi_{\text{saw}} \approx 0.5$): The saw now swings from $\chi_{\text{bottom}} \approx 0$ to $\chi_{\text{top}} \approx 0.5$. Because the natural recovery/control action of the motor takes over before χ reaches 1, the controller never gets a chance to command a deceleration before the reset to χ_{bottom} occurs, resulting in continuous acceleration segments (modulated only by the sawtooth frequency).

The observation that only acceleration stripes remain is a crucial finding for the attacker in characterizing this specific attack setting. From this, the attacker can infer a direct connection between the lack of deceleration and the overall increase in the integrated impact of the operating current surges, which is visually confirmed in Figure 4.13 via the overlapping stripes generated by individual saw teeth. The improved impact of the heat production in motor control power circuits and windings may constitute a potentially attractive target for further exploration by the attacker. Further reduction of the saw teeth modulation amplitude in the attack is considered the next step for this purpose.

4.3.4 Deep-leveled, Small-amplitude Modulation Saw Teeth

As a result of further reduction of modulation amplitude in attacking the χ function, we arrive at the deep-leveled, small-amplitude modulation saw teeth function, which has the impact on the system as shown in Figure 4.14. It is important to note that the saw triangles here are kept geometrically similar to the cases of large and intermediate modulation amplitude, so that reduction of the saw triangles height leads to proportional frequency increase for the saw function modulation. This is seen from the following analysis:

If we assume χ' (the slope) is constant (due to geometric similarity):

$$T = \frac{\Delta\chi_{\text{saw}}}{\chi'}$$

If $\Delta\chi_{\text{saw}}$ (the height/amplitude) is reduced, then T (the period) is reduced. If T is reduced, then f_{mod} increases.

As Figure 4.14 shows, the attacker can detect the smoothing effect on the motor ripples as system inertia provides continuous acceleration to above $\omega = 1000$ rad/s. This reduces the infliction of mechanical damages (not that the attacker wants this reduction), but more importantly, it allows the intrusion to avoid detection via vibration detectors, which strongly favors the attacker.

An important inference for the attacker is the increased intensity of the current drainage, where segments from neighboring saw teeth strongly overlap. This maximizes the impact of the inflicted power losses in the heating up of the circuits and windings, giving an edge to the attacker on the electrical damage objective.

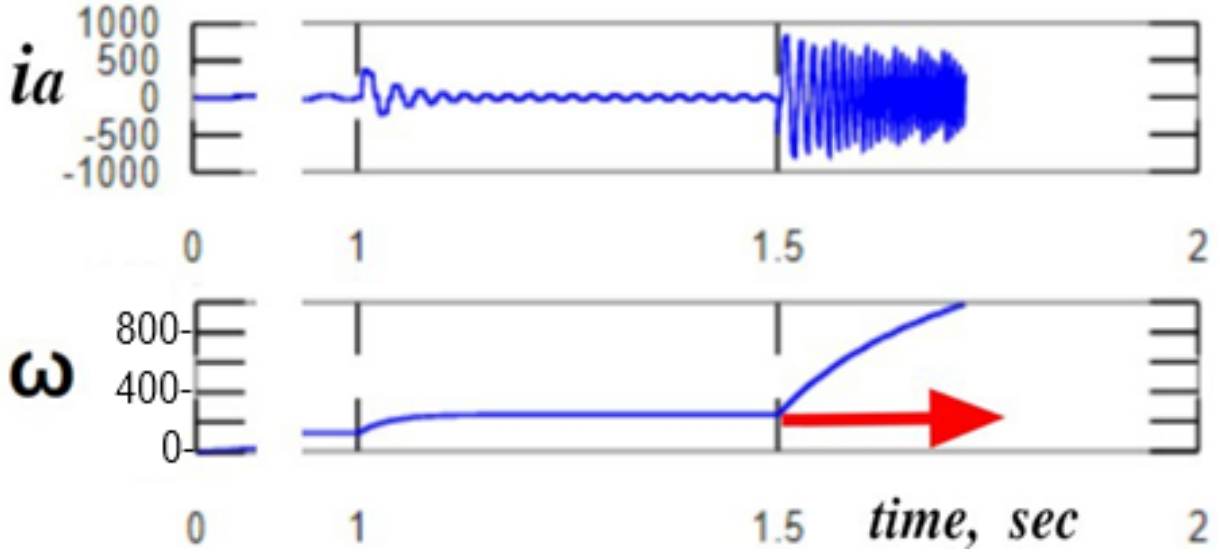


Figure 4.14: Performance of the deep-leveled, small-amplitude modulation saw teeth profile in bias injection on system response – the current drainage segments strongly overlap. Saw tooth depth is initialized at $\delta\omega = 5.95$ rad/sec level, which is 2.38 percent of the level of initial speed of 250 rad/sec, $\chi' = 0.00004286$, $K_p = 10$, attack starts at $t = 1.5$ sec. Values of i_a are in Amps, values of $\omega = \hat{\omega}$ are in rad/sec, time is in seconds (horizontal axis).

4.3.5 Adjusting Asymmetry in Saw Function

So far, we have considered the option of maximal asymmetry in the sawtooth function for the attacking bias injection. This strong asymmetry, characterized by the abrupt change of the parameter, was initially favored by the attacker for its capacity to inflict the strongest impact against the host system. However, such an abrupt change may also serve as a readily detectable feature within the defense infrastructure. Since sufficient stealth is a critical criterion for proper attack design, the attacker must account for the risks of early detectability. Consequently, the attacker needs to consider smoothing the saw profile by increasing the symmetry of the saw teeth triangles. The effect of this transformation on the attack outcome is considered next, building upon the initial framework.

In the previous consideration of the current drainage attack, the triangular saw function was employed as a distortion tool for the modification of the feedback data stream values of the angular velocity. Various depths of triangular saw function profiles were considered in terms of their effect on the current drainage flow. This effort yielded a set of specific signatures of the current drainage attack for future use via pattern recognition for attack detection purposes.

Consideration in these experiments, however, was limited to only a single type of triangular shape: specifically, the right-angled triangle. This type of triangle in the saw function exhibits the

highest possible asymmetry along the direction of time flow. In turn, this signifies, on one hand, the strongest possible change of disturbance with time, but on the other hand, it also corresponds to the least stealthy approach for the attack.

Therefore, in order to find a better balance between the strength of the attack and its stealthiness, alternative shapes for the tooth of the saw function need to be explored. The opposite to the right triangle in terms of asymmetry along the time axis would be the isosceles triangle shape, which provides maximal symmetry for the saw tooth in the time direction. Between these two opposites [maximal asymmetry (defined by the 90° angle at the base)/right triangle and maximal symmetry/isosceles], a set of various acute through obtuse triangle shapes of the tooth in the saw function would represent the partial asymmetry case.

Our next goal is therefore to verify the effect of the **asymmetry in triangular tooth shapes** of the attacking saw function on current drainage flow in terms of the attack strength, its stealthy implementation, as well as to determine attack signature features which are linked to the saw tooth asymmetry.

Asymmetry in Saw-Function

To quantitatively characterize the asymmetry of the triangular tooth in the attacking saw-function, we introduce a symmetry coefficient K_S defined as:

$$K_S = \frac{\tan(\beta)}{\tan(\alpha)} \quad (4.1)$$

and where angles α and β are shown in Figure 4.15, (a)–(c). Thus defined, $K_S = 0$ brings about fully asymmetric case of Figure 4.15 (a) (zero symmetry), $K_S = 1$ corresponds to fully symmetric tooth in saw-function shown in Figure 4.15 (c), whereas intermediate cases of $0 < K_S < 1$ in tooth asymmetry are represented in Figure 4.15 (b) (partial symmetry/asymmetry).

Bias Coefficient Functions Tested

In order to verify the extent to which asymmetry of the tooth in attacking saw-function may affect the flow of the current drainage attack of the kind, shown in Figure 4.15 (d), the range of shown in Figure 4.15 (a)–(c) tooth shapes for the bias coefficient saw-functions have been tested. Varied is also tooth height, which in turn is related to the modulation depth of the attacking distortion coefficient χ .

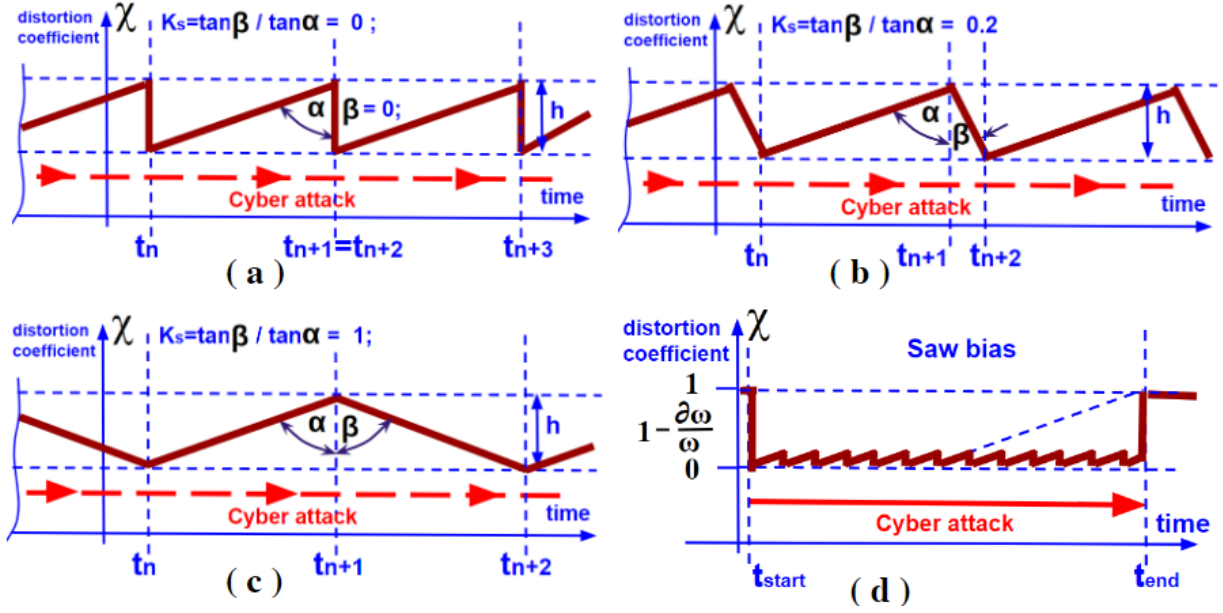


Figure 4.15: The Tested Distortion Coefficient (χ) Profiles for Current Drainage Experiments: (a) Fully Asymmetric Sawtooth Wave; (b) Partially Asymmetric Sawtooth Wave; (c) Fully Symmetric Triangle Wave; (d) Attack Flow engaging the Fully Asymmetric Wave (a). The variation in χ asymmetry is used to adjust the current drainage effect.

Procedures in Simulation Experiment

For comparative analysis, we adhere to a specific time schedule: the bias injection attack begins at $t = 1.5$ s and ends at $t = 2.0$ s. In the plots that follow, the attack interval is consistently marked by a red arrow along the time axis. The respective tests have been conducted prior to modeling and simulation experiments, specifically verification test of model operation under standard conditions, such as (i) acceleration and (ii) stabilization under open loop operation, followed by closed loop control tests, namely, (iii) step-function response and (iv) stabilization test.

Next, we shall see in the modeling and simulation experiment on how the change of the asymmetry of the tooth in saw-function of χ within the current drainage attack affects the flow of the attack itself. To do so we follow the sequence of experiments shown in Figure 4.15 (a)–(c) while implementing the attack based on sequence shown in Figure 4.15 (d). As Figure 4.15 (d) suggests, the attack is preceded by stable, a “no-attack” state with $\chi = 1$. Then the attack begins with χ dropping down to zero ($\chi = 0$) and initiating saw-function teeth sequence oscillating above zero level of χ , which is representing the attack window marked with red arrow on the plots. As a starting point for demonstrating the effect of saw-function tooth asymmetry on attack induced current drainage, the fully asymmetric tooth shape with $K_S = 0$ will be considered (i.e., the right triangle tooth shape). Then, the tooth shape will be modified to increase the

symmetry, rendering intermediate cases of $0 < K_S < 1$ in tooth asymmetry (i.e., various acute triangle shapes of the tooth in saw function representing partial asymmetry case will be scanned). Finally, isosceles triangle shape will be tested which provides best symmetry for saw tooth in time direction.

Injecting Fully Asymmetric Saw Bias

We now initiate the series of current drainage attack trials by varying the symmetry parameter, K_S , to explore its influence on the attack performance. The case where $K_S = 0$ (representing a fully asymmetric tooth function) is illustrated in Figure 4.16. For this trial, the system is run in the test-drive phase from $t = 0$ to $t = 1.5$ s, with the attack commencing immediately after stabilization at $t = 1.5$ s. The attack follows the schedule shown in Figure 4.15 (d) starting from $\chi = 1$ (i.e., from no distortion) and dropping down to $\chi = 0$ (i.e., maximum distortion with negative bias). Then the saw function of χ values sets in and oscillations above zero level of χ continue until the end of the attack ($t_{\text{end}} < 2$ sec), after which the value of returns back to $\chi = 1$ level of no attack state. In Figure 4.16 the periodic oscillation of the current has the same period as the saw function. Gradual linear decrease of the amplitude of current oscillations is linearly proportional to the respective increase of the saw tooth's cross-section height at the same time moment.

Next, we shall modify saw function by replacing right triangle tooth shape to the acute one.

Injecting Partially Asymmetric Saw Bias

When replacing the right triangle with acute one in saw function, the time of ascend to the triangle highest point was retained the same. It means that the period of oscillations for saw function with such acute triangles as tooth shapes was higher than that for the case of right triangles. This fact has implications in observed features of occurring system response shown in Figure 4.17 where the symmetry of the acute triangle shape of the tooth there is $K_S = 0.0002$.

Comparing periods of current modulation in the attack time window it is seen that the modulation frequency of the current drainage is increasing for the acute triangle shape case. This goes despite the fact that the period of acute triangle saw function is higher than that of the right triangle. Explanation of this may be in emergence of the higher harmonics for the case of acute triangle.

The result of further increase of the symmetry and connected to that increase in modulation frequency of the current drainage is shown in Figure 4.18. The symmetry of the acute triangle shape of the tooth there is increased to $K_S = 0.0005$, which is 2.5 times of that shown in

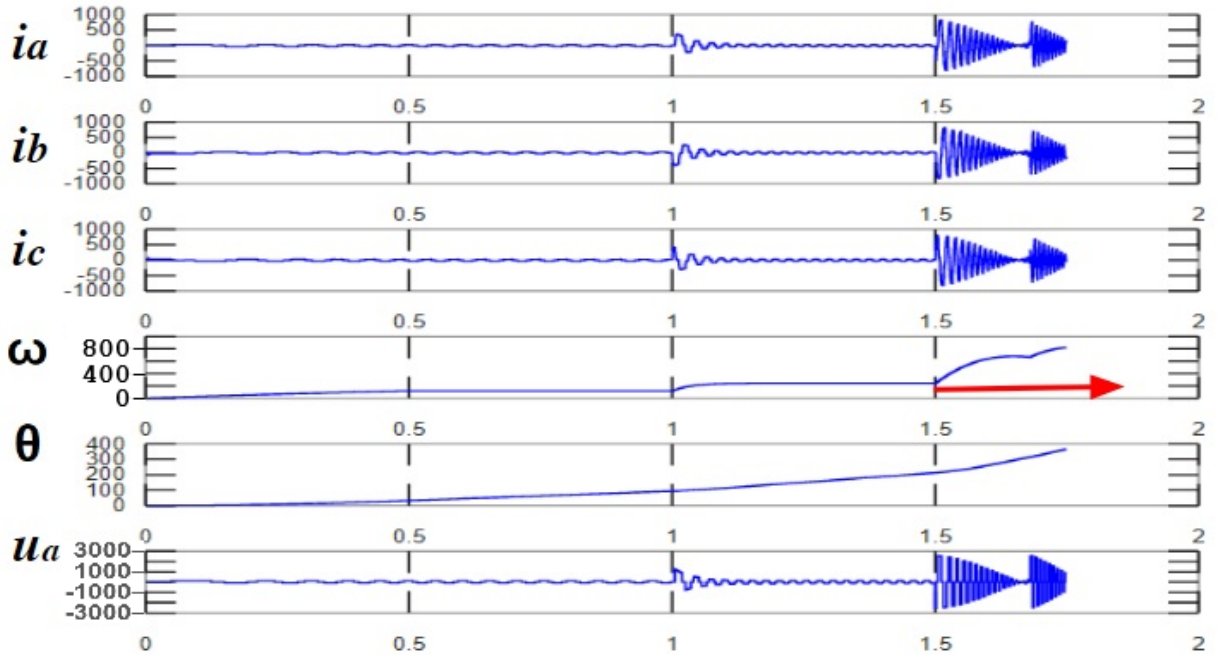


Figure 4.16: Attack using saw function with fully asymmetric triangle as a tooth shape for the bias distortion coefficient χ ($K_S = 0$, right triangle case with $h = 0.1$, i.e., 10% of the attack depth on a χ -scale). Values of the phase currents are in A (Amperes) (i_a, i_b, i_c), angular speed ω is in rad/s (radians per second), rotor position θ is in rad (radians), and phase voltage u_a is in V (Volts). The horizontal axis represents time in seconds (s).

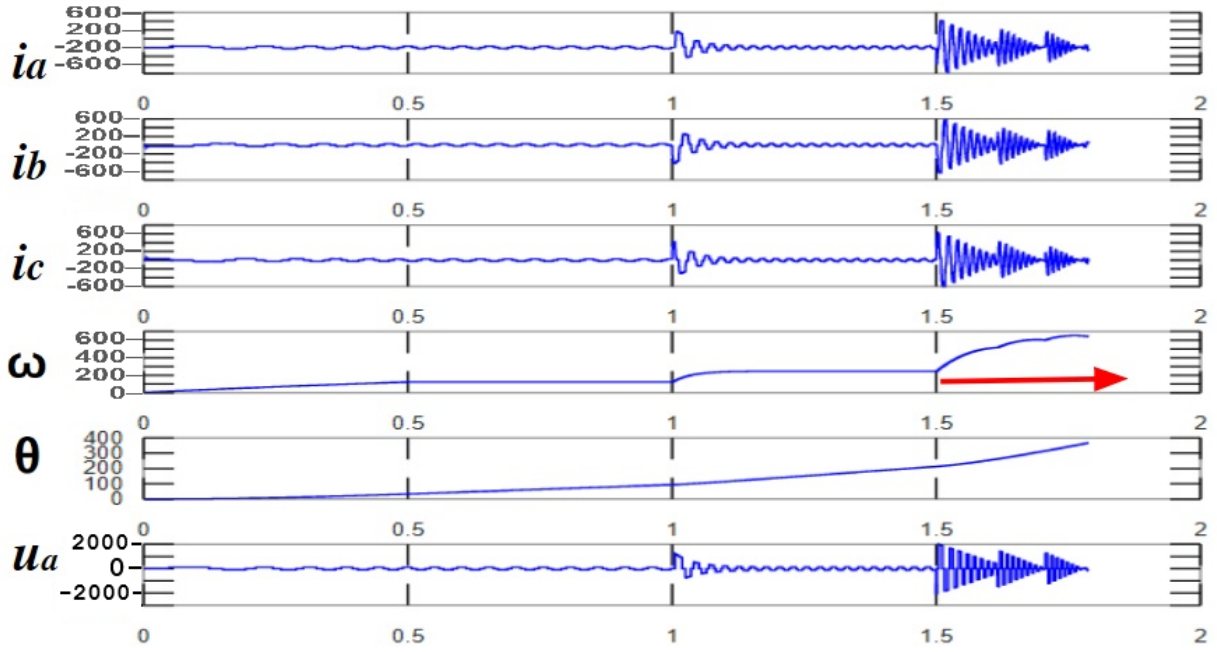


Figure 4.17: Attack using saw function with acute triangle tooth shape for the bias distortion coefficient χ , with symmetry $K_S = 0.0002$ and saw depth $h = 0.1$. Values of the phase currents are in A (Amperes) (i_a, i_b, i_c), angular speed ω is in rad/s (radians per second), rotor position θ is in rad (radians), and phase voltage u_a is in V (Volts). The horizontal axis represents time in seconds (s).

Figure 4.17. As a consequence, modulation frequency of the current drainage is increasing approximately 2.5 times as well, thus confirming inter-relation between saw tooth symmetry and current drainage modulation.

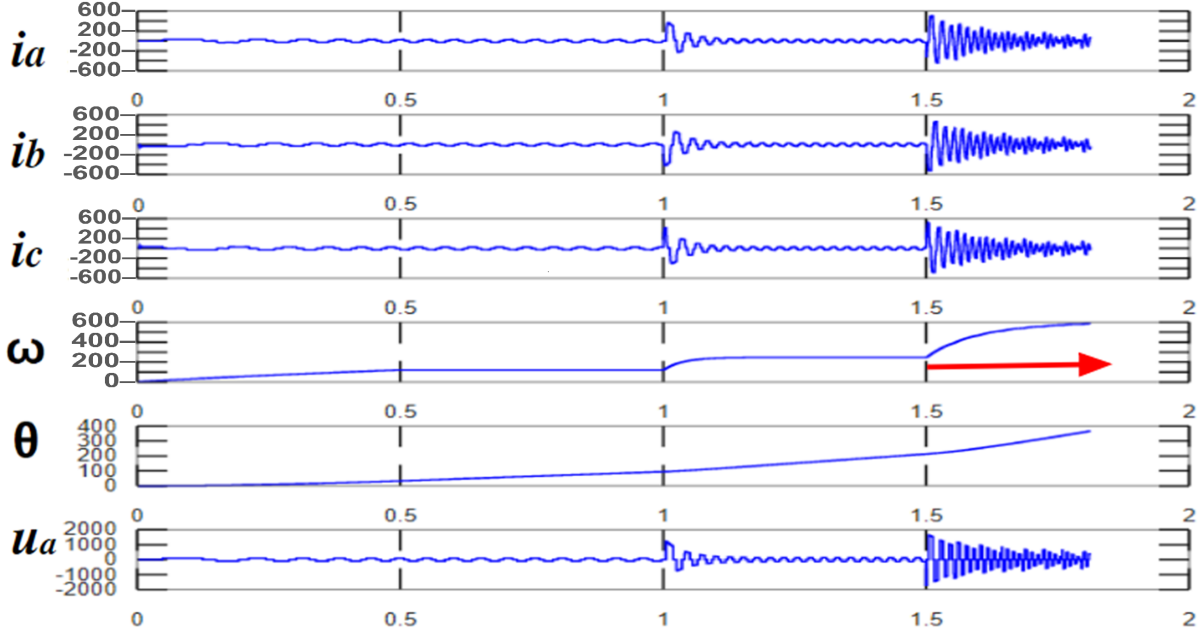


Figure 4.18: Attack with acute triangle saw function as bias distortion coefficient with symmetry $K_S = 0.0005$ and saw depth $h = 0.1$. Values of i_a , i_b , i_c are in Amps, ω are in rad/sec, θ are in radians, u_a are in Volts. Horizontal axis is time in seconds.

Having established the linear proportional relation between saw tooth symmetry and current drainage modulation frequency, it is logical to proceed to the case of strongest possible symmetry in the next subsection.

Injecting Fully Symmetric Saw Bias

The best symmetry for saw tooth in time direction is provided by the isosceles triangle shape, which has symmetry coefficient $K_S = 1$. Ascending time from the triangle left hand lowest point to its top in the middle becomes equal to the descending time from the top point to the right-hand side lowest point. The Figure 4.19 shows the result of engaging the isosceles triangle shape for the tooth in saw function for the attack.

It is seen that the smoothest change in current drainage is achieved for isosceles triangle shape of the tooth in saw function.

Next, we shall discuss implications of the observed dependencies.

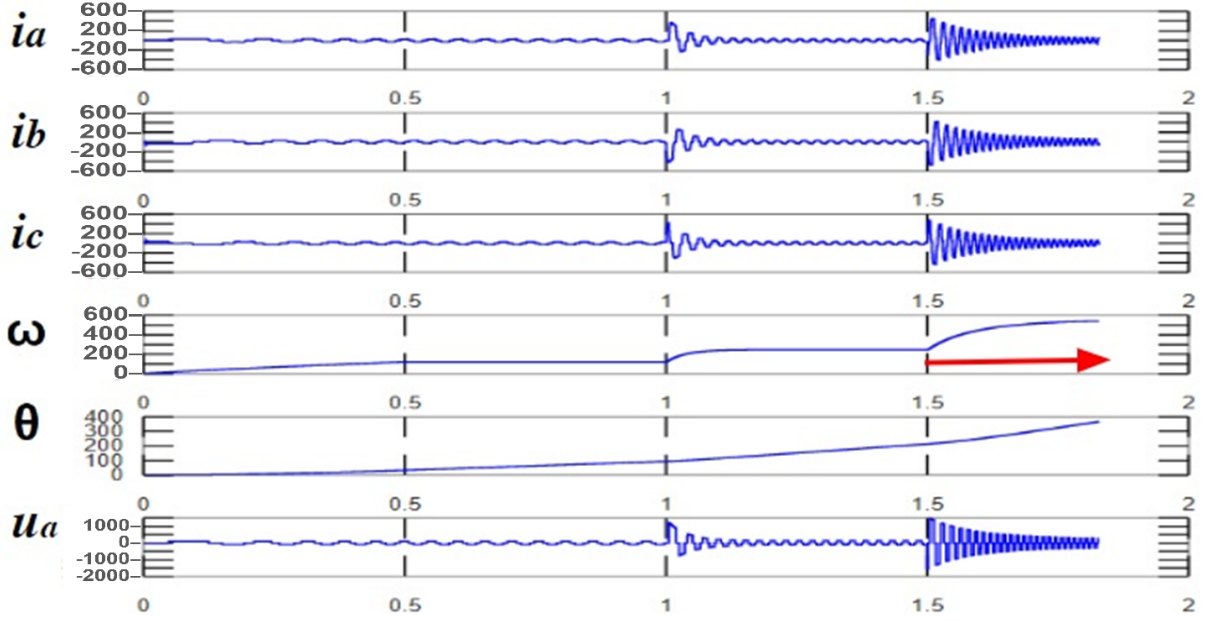


Figure 4.19: Attack using saw function with isosceles triangle tooth shape for the bias distortion coefficient χ , with symmetry $K_S = 1$ and saw depth $h = 0.1$, i.e., 10% of the attack depth on a χ -scale. Values of the phase currents are in A (Amperes) (i_a, i_b, i_c), angular speed ω is in rad/s (radians per second), rotor position θ is in rad (radians), and phase voltage u_a is in V (Volts). The horizontal axis represents time in seconds (s).

Summary on Asymmetry in Distortion Function

The above simulations reveal a way in which current drainage attack may be affected via change of symmetry in the triangular tooth shape of a saw function – such a change modifies modulation of the occurring current flow. The current modulation amplitude and its frequency appears to be a function of the symmetry of the tooth shape employed. An extreme case of the fully asymmetric tooth shape of the right triangle brings about proportional modulation when the current drain repeats the shape of the attacking saw function in its amplitude and frequency. Modulation frequency harmonics occur on the current profile when symmetric features are introduced into saw function. Their frequency increases with the extent of symmetry until its reaching switching frequency of the windings. For fully symmetric tooth shape harmonics vanish in current drainage modulation profile.

Detection of higher harmonics in the current drainage flow provides information on the attacking function parameters, such as symmetry of engaging triangular saw function. In turn, presence of harmonics in current drainage modulation offers distinguishing pattern of the attack, suitable for signature-based classification.

Moreover, the stealthy approach for the attack gives preference to the symmetric type of the saw function employed where current drainage modulation profile stays harmonics free. Signa-

ture of the attack becomes less expressive for identification which help the attack to stay undetected.

Conclusive Remarks on Asymmetry in Distortion Function

A new set of features is identified and verified via modeling and simulation in the current drainage attack against closed loop-controlled BLDC motor. Specifically, an asymmetry of triangular tooth shape in the employed saw function is found to affect the modulation frequency of the drained current.

The proportional reproduction of the saw function oscillations in the current drainage takes place for fully asymmetric triangular shape of the tooth in the saw function.

Higher frequency harmonics occur in modulation signal of the drained current for partially asymmetric tooth shapes in saw function. The frequency of the harmonic's modulation of the current increases with the increase of symmetry of the triangular tooth shape involved.

Ultimately, for fully symmetric triangular tooth shape in the attacking saw function the higher harmonics vanish in the current modulation profile thus rendering smoother current drainage flow.

Signatures of the current drainage patterns for varying asymmetry in the tooth shape of saw function engaged are gathered with potential to identify the attack and its parameters via pattern recognition approach.

4.3.6 Summary of the Current Drainage Attack

To summarize the experimental findings on the Current Drainage Attack against the controlled BLDC motor, the use of a deep-leveled saw function for attacking bias injection allows the adversary to inflict damage through two distinct but related mechanisms: mechanical wear and electrical damage.

- **Modulation Depth ($\Delta\chi_{\text{saw}}$) Effects:** The magnitude of the attack damage can be regulated by varying the modulation depth of the saw function.
 1. **Mechanical Wear:** This damage mode, induced via rotor speed ripples ($\Delta\omega$), is maximized for large-amplitude modulation and significantly reduced for small-amplitude modulation.
 2. **Electrical Damage:** Conversely, the impact of electrical damage to the circuits and windings increases for small-amplitude modulation, provided the deep-leveled saw function is maintained.

In either case, for the undefended host system, the attacker achieves the primary goal of overriding motor functionality, effectively nullifying the host operational ability under this attack scenario.

- **Asymmetry (K_S) Effects (Modulation Frequency Control):** A new set of features is identified and verified through modeling and simulation related to the tooth shape of the saw function. The asymmetry of the triangular tooth shape (controlled by K_S) is found to affect the modulation frequency of the drained current, providing a secondary layer of attack customization:

1. **Fully Asymmetric Triangle ($K_S \approx 0$):** A proportional reproduction of the saw function oscillations occurs in the current drainage, meaning the attack signature mirrors the injected signal.
2. **Partially Asymmetric Triangle ($0 < K_S < 1$):** Higher-frequency harmonics occur in the modulation signal of the drained current. The frequency of these harmonic modulations increases as the symmetry of the triangular tooth shape increases (i.e., K_S approaches 1).
3. **Fully Symmetric Triangle ($K_S = 1$):** The higher harmonics vanish in the current modulation profile, rendering a smoother current drainage flow.

These distinct current drainage patterns, dictated by varying the asymmetry in the tooth shape, yield gatherable signatures. These signatures provide the potential to identify the attack and its parameters via a pattern recognition approach, thereby enabling the construction of formidable defense structures.

4.4 Voltage Hopping Cyber-Attack

In the previous section, we considered the distortion function χ primarily containing dominant low-frequency components of saw functions and limited gradients of the parameter χ changes. This was done to address the potentially valid concern of the adversary regarding the need to maintain low detectability against a defending system, if one exists. However, the attacker may determine from probing attempts that the host system is insufficiently protected against cyber-intruders. This impression may serve as encouragement to exercise extreme scenarios for the attack in pursuit of the quickest results and maximizing inflicted damages. Under such circumstances, the attacker may engage higher frequencies and higher amplitudes of χ modulation. These options are to be considered next in order to evaluate the available destructive potential of the adversary against the given cyber-physical system. Of particular interest are the frequencies

that are higher than the cutoff frequency (f_c) of the operating RL circuits. Attacking at or above f_c is a strategy for maximizing damage, as it exploits two distinct destructive mechanisms:

1. **Impedance Shift:** While current amplitude may drop as the inductive impedance dominates, pushing the system into this high-frequency regime stresses the system's ability to maintain stable control, maximizing operational error.
2. **Transient Stress:** The power electronics (inverter switches/MOSFETs) are subjected to extremely rapid switching cycles. This results in high di/dt and dv/dt values, accelerating switching losses and causing transients that the circuitry is not designed to handle, leading to significant electrical damage.

The impact of the attacker on the relations between voltage and current changes in the control units, as well as its effects on the resulting rotor angular velocity (ω), is in the focus of this consideration.

4.4.1 Selecting Model for the Bias Coefficient $\chi(t)$

Engaging values $\chi > 1$ versus $\chi < 1$ has an opposite impact on the controller output. For $\chi > 1$, the controller receives over-estimates of the angular velocity and, therefore, generates a signal for deceleration. In the opposite case, for $\chi < 1$, under-estimated values of the angular velocity are reaching the controller, and an acceleration scenario is enforced. Logically, sequential transitions between values $\chi > 1$ and $\chi < 1$ should result in sequential switching between states of deceleration and acceleration, which in physical realization would impose increased mechanical strain onto the rotor, thus offering the attacker one extra venue for damage.

However, if the transitions are sufficiently quick, the system may not necessarily be able to implement the full cycles of deceleration/acceleration physically. Instead, it may experience significant overload from mutually contradictory sequences of commands. The resulting system overload may in itself be the desirable outcome for the attacker. To establish a basis for potential defense strategies, a simulation of such an extreme scenario is implemented herewith, with relevant parameter variations to grasp the presented spectrum of threats in full.

Contrasting previously explored one-sided (i.e., $\chi > 1$ or $\chi < 1$) values and low-frequency components of χ , the focus here shifts to double-sided, high-frequency changes of χ to achieve the anticipated modification of the attack. Technically, this means the attacker would oscillate the values of χ around the neutral level of $\chi = 1$ (the non-distorted, or “no-attack,” level) at a frequency significantly higher than the switching rate of the inverter between the motor windings. The potential interest in this extreme scenario stems from the possibility of balancing the

contradicting sequence of values ($\chi > 1$ and $\chi < 1$) at a rate faster than the system's inherent reaction speed.

An example of high frequency modulation of the distortion coefficient used herewith in simulation experiment is shown in Figure 4.20. It is seen there that the values of χ are sequentially changing between values of $\chi > 1$ and $\chi < 1$. In Figure 4.20 depicted is extreme case of transitions between $\chi = 0$ and $\chi = 1.3$ in one step followed by reverse transition in one simulation step back to $\chi \approx 0$. The modulation frequency f_{mod} of the distortion coefficient χ in Figure 4.20 is 17.5 kHz, which is the highest possible for the given set of the operating motor parameters.

Since the modulation frequency (17.5 kHz) equals the sampling rate (f_s), the period of the modulation (T_{mod}) must equal the sampling period (T_s).

$$T_{\text{mod}} = \frac{1}{17.5 \text{ kHz}} = T_s$$

Therefore, the upward transition ($\chi_{\text{bottom}} \rightarrow \chi_{\text{top}}$) takes one full sampling step (duration T_s), as well as the downward transition ($\chi_{\text{top}} \rightarrow \chi_{\text{bottom}}$) takes one full sampling step (duration T_s). Therefore, the total period of the waveform is two sampling steps ($2T_s$), making the modulation frequency half the sampling rate ($f_{\text{mod}} = f_s/2$). The sampling rate f_s of the control system is defined by the sampling rate of the Kalman filter-based driver. This rate is automatically selected based on the operating speed of the motor (ω) and is determined to be 35 kHz.

This timing forces the transition of χ from its lowest value $\chi = \chi_{\text{bottom}}$ to the highest one $\chi = \chi_{\text{top}}$ to occur in a single sampling step, and the reverse transition from χ_{top} to χ_{bottom} occurs within the subsequent sampling step. This rapid change significantly affects the interaction between the motor and controller due to the respective shift in the moments of highest and lowest values of χ with respect to the phase positions of the rotor. The attacker can achieve such a critical phase relation by tuning the frequency of the χ modulation, thereby positioning themselves to take advantage of this possibility for overriding motor control purposes. The resulting impact of manipulating the attacking function χ to engage this kind of phase-related interaction is considered next.

4.4.2 Impact of Bias Coefficient $\chi(t)$ Modulation Frequency Fine Tuning

The results of the simulation experiments are presented herewith in the order of decreasing frequency of the $\chi(t)$ modulation, utilizing alternating sequences of $\chi > 1$ and $\chi < 1$. To achieve the precise frequency tuning, the number of steps required to change χ from its lowest value ($\chi_{\text{bottom}} = 0$) to its maximum value ($\chi_{\text{top}} = 1.3$) is controlled. Only symmetrical saw-functions are used for modulation purposes; that is, an increase of χ is followed by its decrease at the same

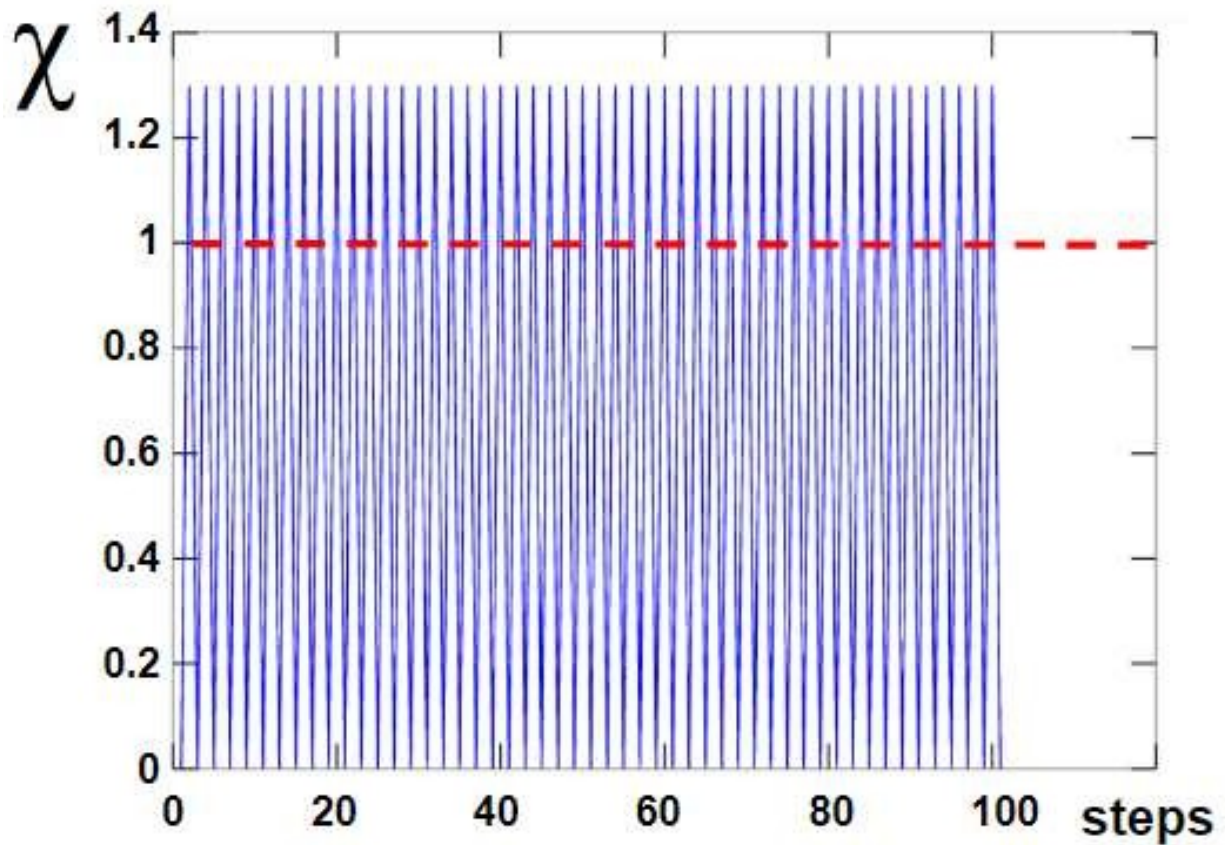


Figure 4.20: The high-frequency modulation of the distortion coefficient χ required to achieve the "voltage hopping" effect. The signal is a symmetric saw wave with a frequency of 17.5 kHz and an amplitude of $h = 1.3$. This profile produces interchanging sequences of $\chi > 1$ and $\chi < 1$ values necessary for the effect.

pace. In other words, the number of iteration steps for χ to ascend is the same as that required to descend back to the level $\chi = 0$.

The timing schedule for this bias injection attack starts at $t = 1.5$ sec and ends at $t = 2.0$ sec. The attack time windows are marked with a red arrow along the time axis on the plots. Prior to the simulation of the attack, respective validation tests were conducted under standard conditions: (i) acceleration, (ii) open-loop stabilization, followed by closed-loop control tests: (iii) step-function response, and (iv) stabilization test.

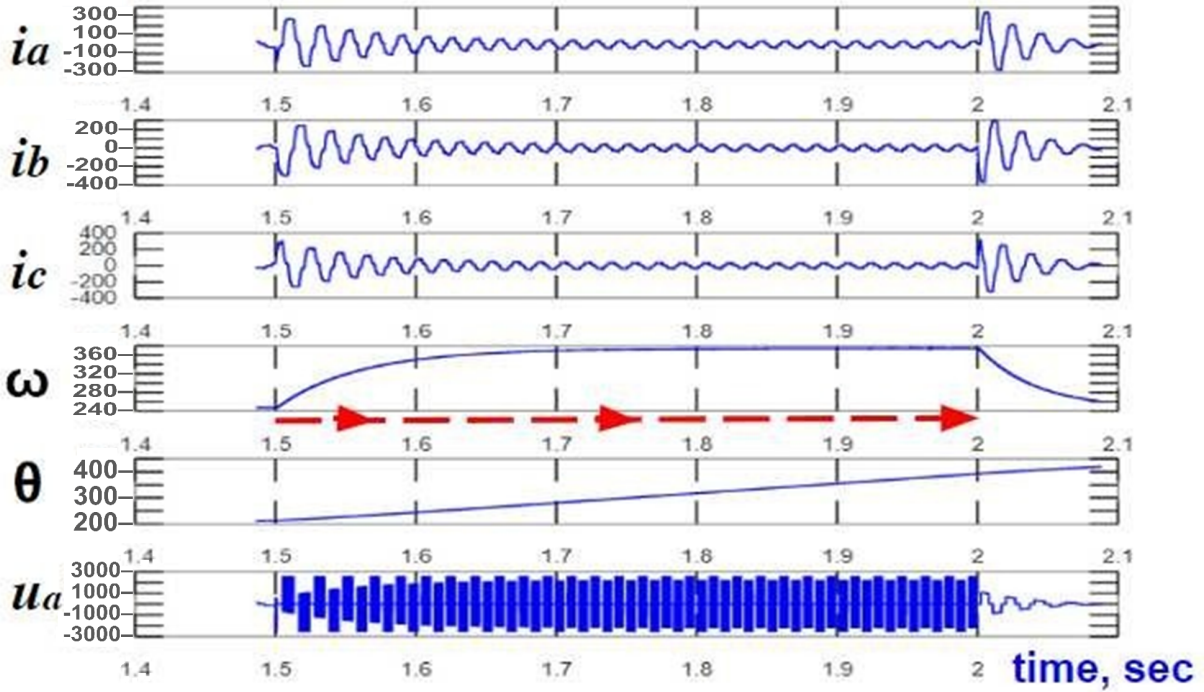


Figure 4.21: Voltage hopping attack (start point $t = 1.5$ s, end point $t = 2$ s, indicated by red arrow) with χ modulation at 17.5 kHz and amplitude of $h = 1.3$ (as in Figure 4.20). State variables shown are winding currents (i_a , i_b , i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), and position (θ in rad (radians)). The signal u_a represents the phase voltage in winding “a” (in V (Volts)).

The attack simulation at the highest frequency of χ modulation, 17.5 kHz, is shown in Figure 4.21. It is observed that the disproportionately high changes in operating voltage (± 3000 V for winding a , u_a is shown) do not cause a strong effect on the winding current. Only a slight increase in current is observed at the beginning of the attack; however, after the motor speed saturates following the initial acceleration, the voltage changes have no measurable effect on the current values, which gradually subside and stabilize at a regular operational level.

Next, the modulation frequency of χ is reduced by a factor of 5, down to 3.5 kHz. The result of this reduction is presented in Figure 4.22. It is observed that the voltage jumps are reduced

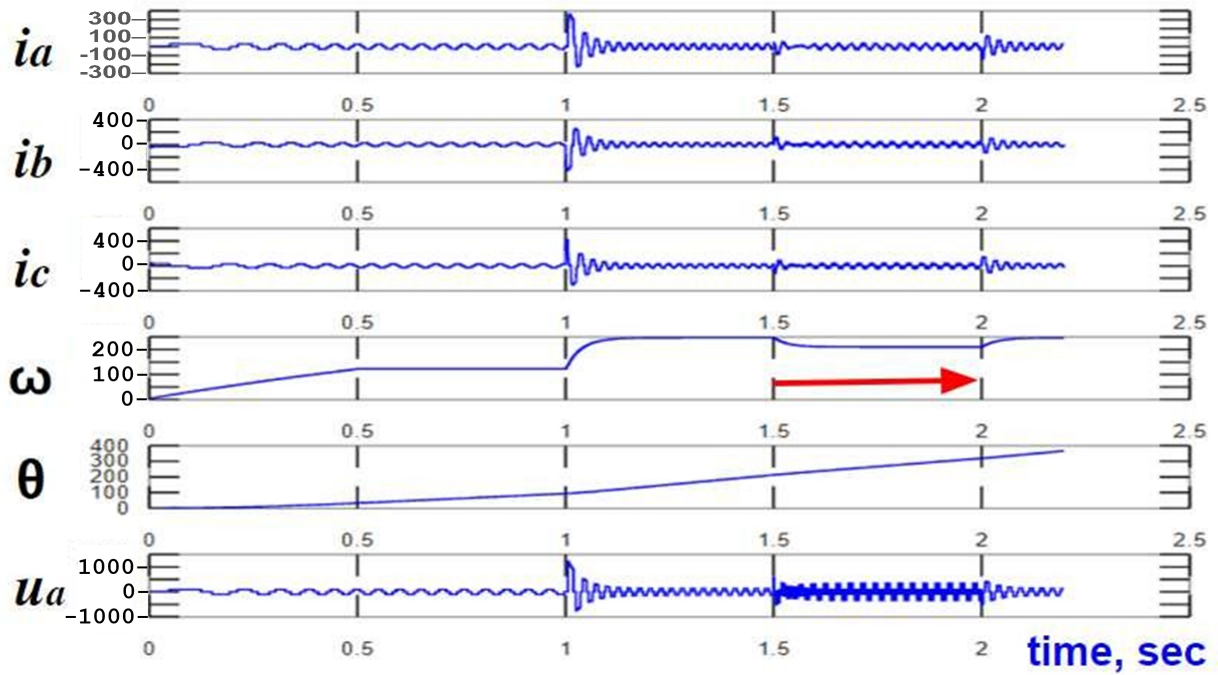


Figure 4.22: Reduction of χ modulation frequency to 3.5 kHz induces moderate deceleration in the voltage hopping attack (start $t = 1.5$ s, end $t = 2$ s, indicated by red arrow). State variables shown are winding currents (i_a , i_b , i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), and position (θ in rad (radians)). The signal u_a represents the phase voltage in winding “a” (in V (Volts)).

to moderate levels (± 500 V), the currents subside to almost regular operational conditions, and a moderate deceleration occurs. Interpretation of this shift may be sought in the change of the phase interaction between the controller's command impulses and the rotor's rotation.

A further reduction of the modulation frequency, down to 2.5 kHz, reveals a trend toward reduced deceleration due to the attack (see Figure 4.23).

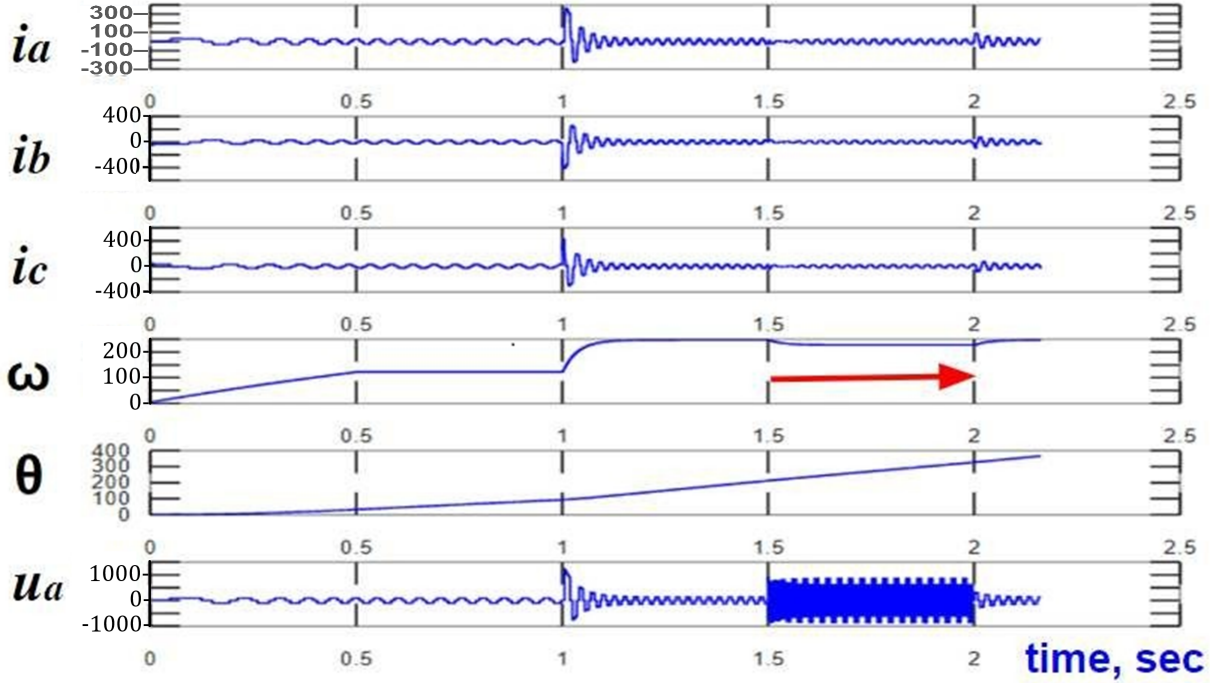


Figure 4.23: Further reduction of χ modulation to 2.5 kHz improves the equilibrium between acceleration/deceleration in the voltage hopping attack (start $t = 1.5$ s, end $t = 2$ s, indicated by red arrow). State variables shown are winding currents (i_a , i_b , i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), and position (θ in rad (radians)). The signal u_a represents the phase voltage in winding “a” (in V (Volts)).

Notably, the currents now remain low, trending toward normal operation, which is consistent with the reduced deceleration effect. The implication is that a state is approached where acceleration and deceleration perfectly cancel each other out, maintaining a stable speed despite sufficiently large jumps in the operational voltages defined by the controller.

Such a balanced equilibrium is achieved by fine-tuning the modulation frequency to 2.1875 kHz. This balanced state offers the attacker the advantage of stealth, as no detectable deviations in the winding currents are observed, and stable speed operation is maintained according to the required reference value. At the same time, the continuous voltage jumps with an amplitude of ± 500 V may present a viable threat to the circuits themselves. This scenario is referred to as the “voltage hopping attack” due to the described feature of avoiding related contributions to the state variables (currents, speed, acceleration, rotor's position) while stressing the voltage supply.

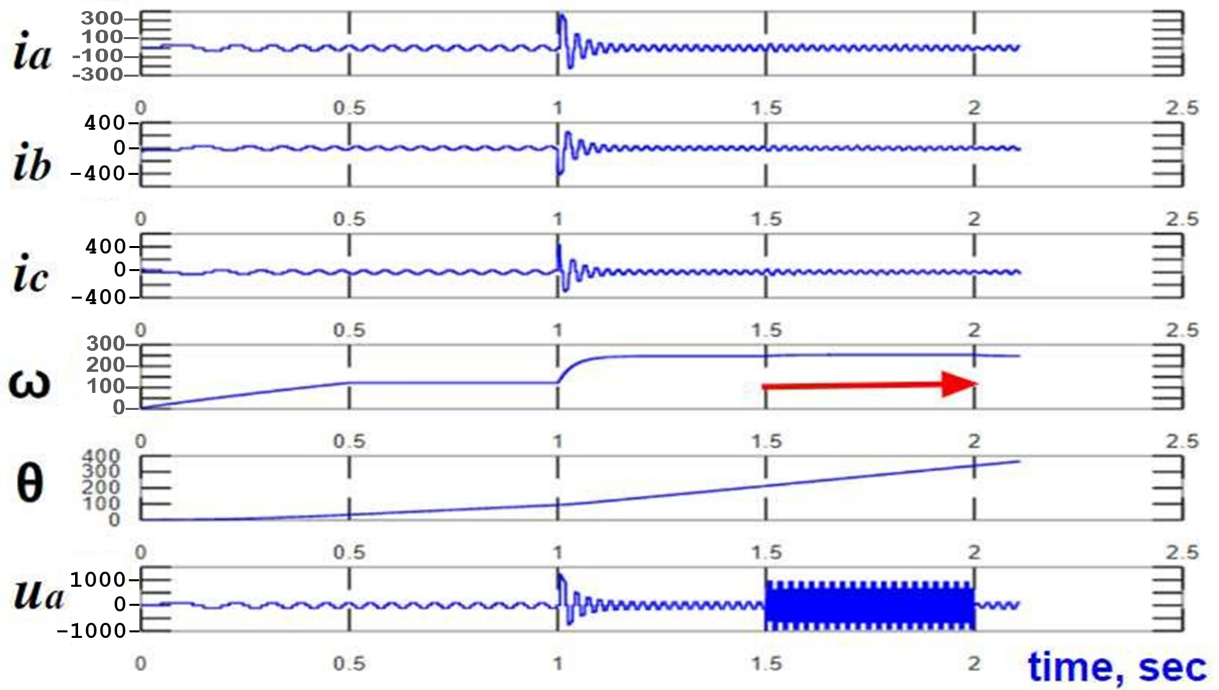


Figure 4.24: Equilibrium state achieved at χ modulation frequency of 2.1875 kHz in the voltage hopping attack (start $t = 1.5$ s, end $t = 2$ s, indicated by red arrow). No visible steady-state effect is observed on state variables, but large voltage jumps persist. State variables shown are winding currents (i_a , i_b , i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), and position (θ in rad (radians)). The signal u_a represents the phase voltage in winding “a” (in V (Volts)).

4.4.3 Summary on Voltage Hopping Attack

A new type of attack, the voltage hopping attack, is suggested and verified via modeling and simulation against a position sensorless drive for a BLDC motor. The main feature of this attack is its ability to induce significant, rapid jumps in the operating voltages, up to ± 500 V, with no visible effect on the primary state variables, such as winding currents, rotor speed (ω), and rotor position (θ). This allows the system to maintain a state of apparent equilibrium.

The attack is based on bias injection into the false estimates of angular velocity provided by the Kalman filter. The biases injected into the angular speed estimates are subjected to high-frequency, high-amplitude modulation. The specific transformation of initial data into false data relies on the multiplication of real data values by a distortion coefficient (χ). The values of this distortion coefficient are determined on-the-fly, accounting for the current rotor's position and the expected compensatory reaction of the controller to the deviation from the required system state. In essence, the voltage supplied by the controller to the circuits follows the path dictated by the false data and, consequently, does not correct the situation but rather exacerbates it.

The attacker in this situation is shown to have the advantage of being able to choose which path to lure the system into. To do so, the attacker must be capable of making correct predictions of the controller's response to the bias in the false data. The results of the simulation experiment demonstrate that high-frequency modulation of the distortion coefficient may lead to the voltage hopping effect, where rapid voltage changes are not mirrored by proportional current changes. This causes the actual voltage to significantly exceed normal operating values without triggering current overload.

An equilibrium state is shown to be achievable at a distortion coefficient modulation frequency of 2.1875 kHz. Due to the invisibility of the attack via standard state variables, this configuration offers the attacker the advantage of stealthiness while maintaining the destructive power of the induced high voltage jumps, a threat which the defender needs to be aware of.

Signatures of the voltage hopping patterns are collected to enable the potential timely identification of the attack for remedial measures implementation.

4.5 Pulsations Cyber-Attacks

Having explored various frequencies of the attacking function modulation, a noticeable difference was observed at the extreme high end. Specifically, matching the phase condition between the modulation frequency and the rotor movement gave the attacker a special mode of control, resulting in the voltage hopping effect. The opposite side of the modulation spectrum, however,

has not yet been considered in detail. Nevertheless, the attacker has already gained insight into low-frequency probing actions by applying a linearly increasing bias as a probe. The system's observed sensitivity to this manipulation gives the adversary incentive to explore the area of very low, even down to zero (*i.e.*, near or even straight DC, frequency manipulation modes within the motor's feedback loop. This scenario is to be considered next.

4.5.1 Induced Pulsations Cyber-Attack

The attacker's initial probe with a linearly increasing bias limited the exploration of χ variations to a narrow range of amplitude span and speed of χ changes. However, these two parameters are directly related to the interaction between the attacker and the system. By varying the depth of χ modulation and the speed of χ changes ($d\chi/dt$), the attacker gains the ability to manipulate the system's behavior and state to find vulnerabilities and cause operational damages. It is critical for the defender to be aware of these potential threats and take defensive measures. Therefore, the goal of this study is to verify the effects of varying the depth of χ modulation in the DC or nearly DC injection mode and its first derivative on dynamic system responses, behavior alterations, system efficiency, and potential threats to its vulnerability and reliability.

Bias Coefficients for Induced Pulsations Cyber-Attack

To address the defined goal of verifying the impact of the distortion coefficient χ 's amplitude and rate of change on the system response, the following functions for χ were employed, as shown in Figure 4.25. In the mathematical representation, using simulation steps (or attacker increments) as the independent variable on the x-axis, these functions demonstrate an initial drop from the "no-attack" value of $\chi = 1$ to a near-zero value. Following this, the χ values increase steadily, maintaining a constant first derivative ($d\chi/dt$).

If the attacker maintains a constant attack time window, the constant gradient of these linear functions directly defines the final modulation depth (amplitude) achieved for χ . Therefore, by comparing the system performance under the implementation of the χ functions shown in Figure 4.25 (a) through (e), it will be possible to address the research goal regarding the verification of varying χ values and its gradient on system behavior. The results of this simulation experiment are presented next.

Operation Under Attack

The confirmed model is employed in subsequent attack testing, with a designated attack time slot of $t=[1.5; 2.0)$ seconds during stationary operation without any ongoing attacks. At $t=1.5$

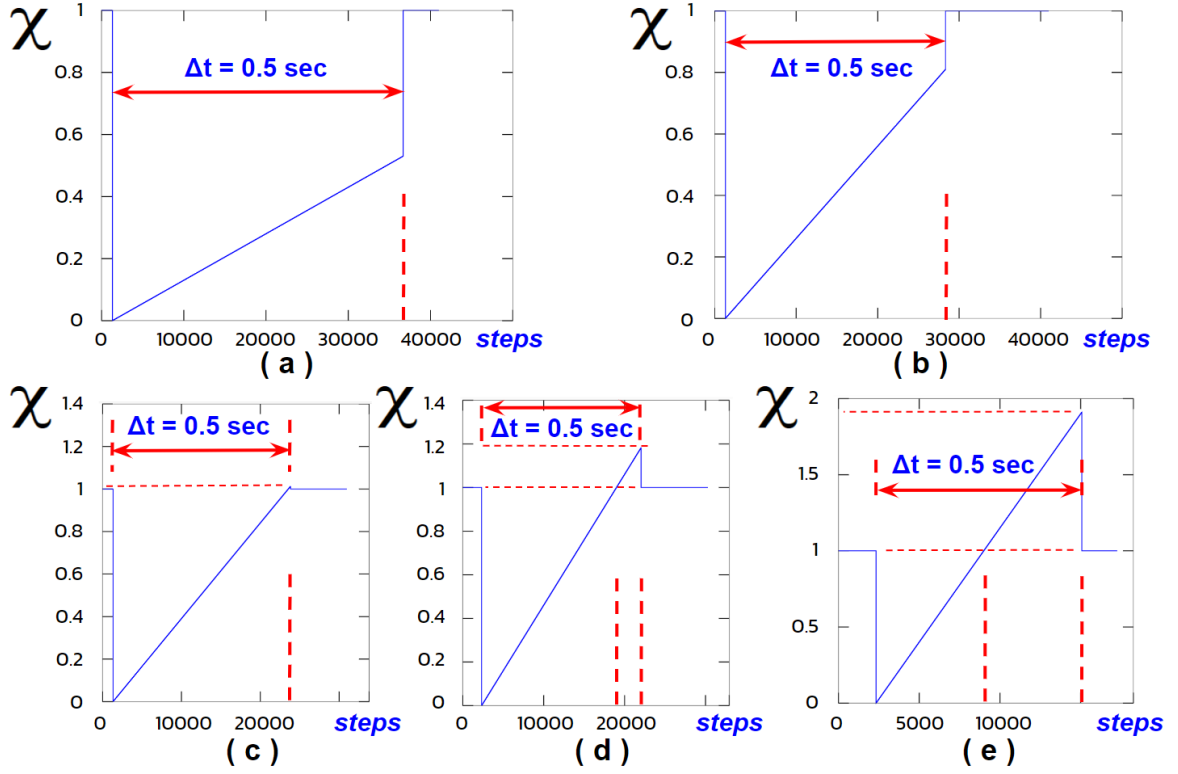


Figure 4.25: Tested linear distortion functions with constant gradient for the following values of $\nabla\chi$ in steps^{-1} units: (a) 1.5×10^{-5} , (b) 3×10^{-5} , (c) 4.5×10^{-5} , (d) 6×10^{-5} , and (e) 15×10^{-5} . Attack window duration is fixed to be $\Delta t = 0.5$ s, but time allocation for each step is dynamically linked to the angular speed ω .

seconds, the attack is initiated by activating $\chi \neq 1$, and it persists until $t=2.0$ seconds, at which point the distortion is eliminated by resetting $\chi = 1$, thereby eliminating the bias.

To inject bias, the attacker sets $\delta\omega \neq 0$ and replaces the Kalman filter's estimations of ω with altered values of $(\omega + \delta\omega)$. The controller then considers the bias term to generate the bias compensating voltage Δu , thereby treating the biased injected input as a legitimate estimate from the Kalman filter.

Simulation Results for Induced Pulsations Cyber-Attack

The results of the simulation experiments are presented herewith in the order of increasing linear gradient of the $\chi(t)$ modulation depth, corresponding to functions (a) through (e) shown in Figure 4.25. To change the linear function gradient, the number of χ increments at each step was modified from its lowest value (one) to its maximum value (ten). Each increment of χ amounted to 1.5×10^{-5} in relative units (denoted "r.u." herewith). Therefore, the minimal gradient applied in these experiments was $\nabla\chi = 1.5 \times 10^{-5} \text{ step}^{-1}$, as shown in Figure 4.25(a). The maxi-

imum gradient of χ amounted to $1.5 \times 10^{-4} \text{ step}^{-1}$, thus covering a total range of one order of magnitude change.

Variations of Linear Gradient Distortion Coefficient

The results of the simulation experiments are presented herewith in the order of increasing linear gradient of the $\chi(t)$ modulation depth, corresponding to functions (a) through (e) shown in Figure 4.25. To change the linear function gradient, the number of χ increments at each step was modified from its lowest value (one) to its maximum value (ten). Each increment of χ amounted to 1.5×10^{-5} in relative units (denoted "r.u." herewith). Therefore, the minimal gradient applied in these experiments was $\nabla\chi = 1.5 \times 10^{-5} \text{ step}^{-1}$, as shown in Figure 4.25(a). The maximum gradient of χ amounted to $1.5 \times 10^{-4} \text{ step}^{-1}$, thus covering a total range of one order of magnitude change.

The attack simulation for the lowest value of $\nabla\chi(t) = 1.5 \times 10^{-5} \text{ step}^{-1}$ is presented in Figure 4.26 at the time slot $t = [1.5, 2)$ seconds. The figure shows the evolution of five state variables (windings currents i_a , i_b , and i_c , angular speed ω , and angular position θ) and one of the input variables, voltage u_a of the winding 'a'. The model verification stages preceding the attack for the time window $t = [0, 1.5)$ seconds, described and seeing in Figure 3.5, are also shown, as well as the post-attack area for $t \geq 2$ seconds. Within the attack window of $t = [1.5, 2)$ seconds, the system response is represented by pulsations of the currents and voltage. It is important to note that the oscillatory behavior of the system variables is caused by a strictly monotonic change of the distortion coefficient with $\chi < 1$. The attack window of 0.5 seconds fits almost one full period of pulsation, consisting of two unequal parts with a modulation function resembling an asymmetric sine wave. Within this full period of pulsation, there is a 'zero crossing' point where the modulation functions for all currents and voltage reach a zero value. This event is reflected by the angular speed ω reaching saturation point in its growth. Here, the observed phase shift between the above 'zero crossing' point and saturation for ω is consistent with the rotor inertia. This low-frequency modulation of the angular speed ω may be seen as induced ripples and as such may serve as one of the goals for the attacker in an attempt to undermine the operational efficiency of the system. Having quite high amplitudes of currents and voltage pulsations, specifically about 1000 Amps for currents and of about 2500 Volts for voltage, another goal for the attacker is significant dissipation and waste of energy, as well as endangering the integrity of the electrical circuits of the system.

An additional feature seen here is the burst of the currents and voltage at the attack termination point, $t = 2$. The amplitude of current and voltage increases there even higher than that for the attack itself, thus presenting one more resource for the attacker in energy waste and circuit endangering. After $t = 2$, the peak values for the current outbursts reached 1000 Amps, and the

voltage outburst almost reached 4000 V. The last value is about twice as high as peak pulsation voltage. We suggest calling this resource for the attacker the attack withdrawal syndrome, indicating that under certain circumstances, the attack withdrawal may be as damaging as the attack itself.

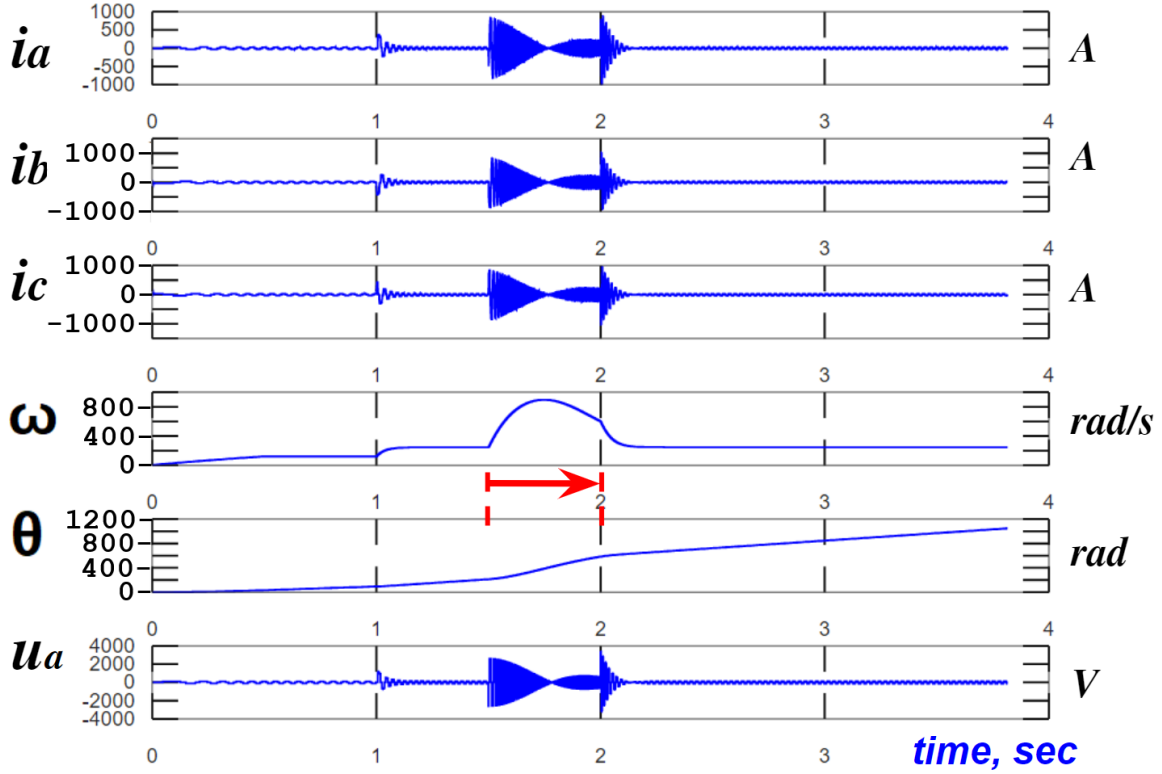


Figure 4.26: Overall system performance, including acceleration for time interval $t = [0, 0.5)$ s, stabilization for $t = [0.5, 1.0)$ s, step function response for $t = [1.0, 1.5)$ s, attack window marked by red arrow at $t = [1.5, 2)$ s with gradient $\nabla\chi = 1.5 \times 10^{-5}$ steps $^{-1}$ as in Figure 4.25(a), and attack withdrawal syndrome for $t > 2$ s with post-attack stabilization. The figure shows five system variables: currents (i_a , i_b , i_c) in A (Amperes), angular speed (ω) in rad/s (radians per second), rotor angular position (θ) in rad (radians), and phase voltage (u_a) in V (Volts).

The presentation of the above features in higher resolution and combined with the plot of χ evolution is made in Figure 4.27. It is seen that the linear gradient function of χ generated by the attacker algorithm within the coordinates of χ vs. quantization steps acquires nonlinear modifications in the time domain. The reason for that is that the attacker is linking quantization step values with the operating values of the angular speed ω in the system, thus maintaining an interactivity mode. Higher resolution in Figure 4.27 also allows us to see more clearly the phase relations between the 'zero crossing point' and the speed ω saturation point, where the latter follows the former with some inertial delay. The uncertainty remains with regard to the difference between the 'zero crossing' for currents and the same for voltage. Within the presented accuracy, there is no detectable phase shift between them. The separated dashed lines for them

in Figure 4.27 indicate margins of accuracy in localization rather than any phase differences. A numerical estimate of the χ value at the zero crossing point for the presented case is indicated by the horizontal dashed line to be about $\chi_0 = 0.3$.

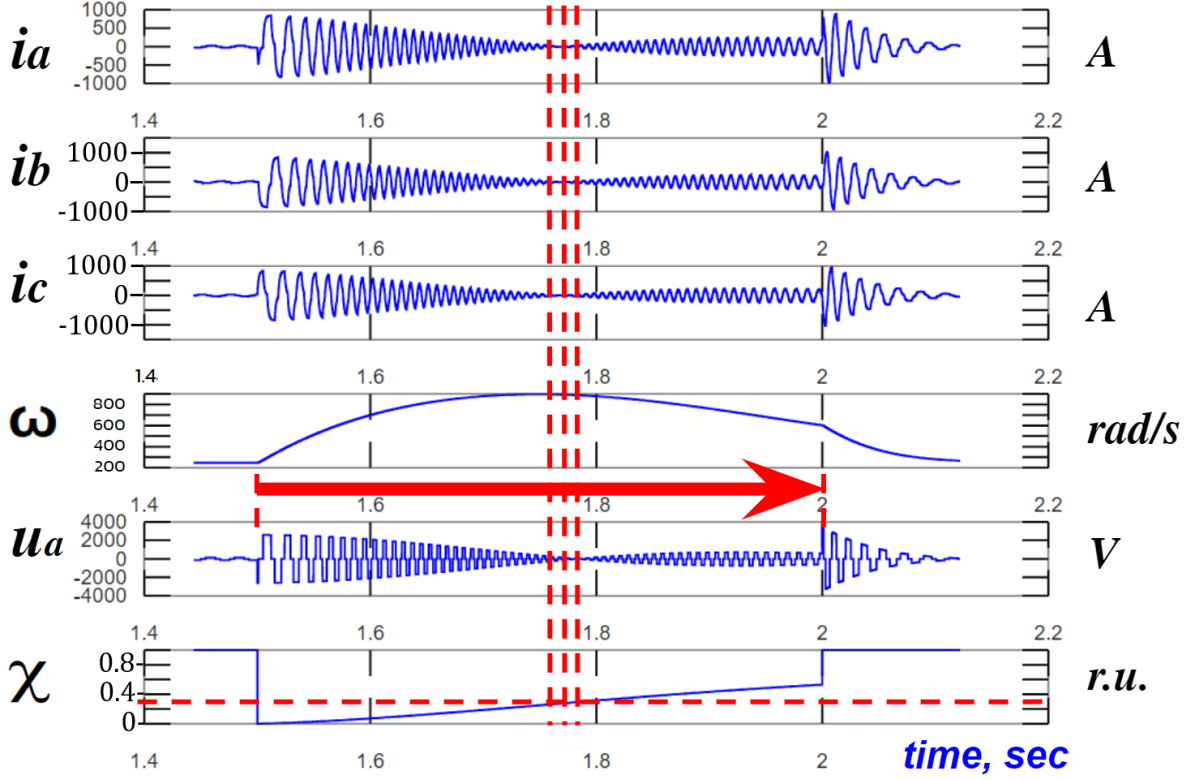


Figure 4.27: System response to the attack followed by attack withdrawal syndrome for gradient $\nabla\chi = 1.5 \times 10^{-5} \text{ steps}^{-1}$ as in Figure 4.25(a). The attack window is marked with a red arrow. State variables shown include: winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).

Raising the incremental increase of the χ value from one to two quantization units at each iteration step on the attacker side allows for doubling the gradient of the linearly increasing part of the χ function, making it $\nabla\chi(t) = 3 \times 10^{-5} \text{ steps}^{-1}$ as shown in Figure 4.25(b). As a result, the pulsation frequency experiences an increase, which is evidenced by comparing the positions of the first zero crossing point in Figure 4.28 to that in Figure 4.27. In the latter case, the zero crossing point is estimated to be in the range of 1.77 to 1.78 seconds, while in the upgraded case of Figure 4.28, the zero crossing point is clearly shifted to the left by more than 0.069 seconds, approaching the 1.70 seconds mark. This event occurs at the level of $\chi_0 = 0.34$ for the last case. As a result, a larger portion of the pulsation period fits into the attack window, causing a deeper reduction in the speed ω at the end of the attack, specifically at $t = 2$ sec. This brings the value of $\omega(t = 2)$ closer to the steady-state level of the attack-free condition, resulting in a smaller outburst associated with the attack withdrawal syndrome. The maximum values for this outburst

are under 500 Amps for the currents and under 1000 V for the voltage. Compared to the case presented in Figure 4.27, where the gradient of χ is $\nabla\chi(t) = 1.5 \times 10^{-5} \text{ steps}^{-1}$, the outburst of currents is reduced by about half, and the outburst of voltage is reduced by about four times in the case presented in Figure 4.28, where the gradient of χ is increased to $\nabla\chi(t) = 3 \times 10^{-5} \text{ steps}^{-1}$.

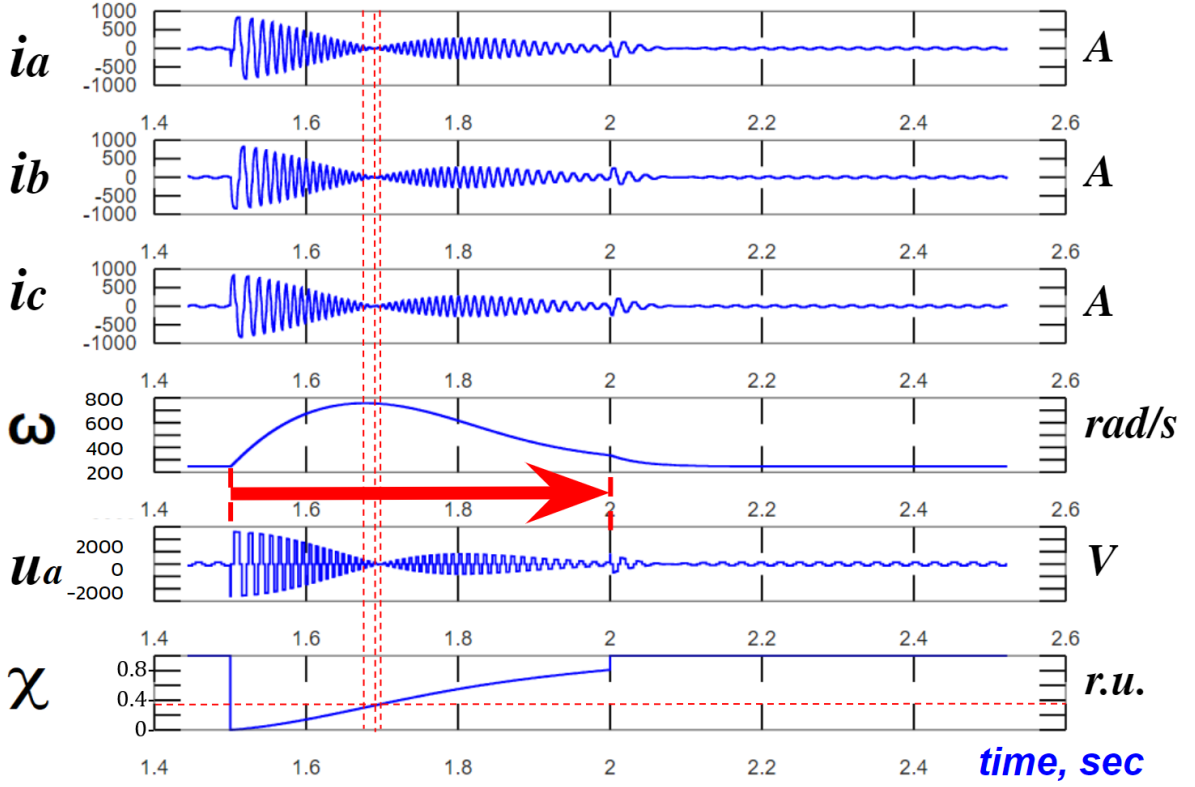


Figure 4.28: System response to the attack followed by attack withdrawal syndrome for gradient $\nabla\chi = 3 \times 10^{-5} \text{ steps}^{-1}$ as in Figure 4.25(b). The attack window is marked with a red arrow. State variables shown include: winding currents (i_a, i_b, i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).

The trends observed in previous cases continue for a larger gradient of χ as shown in Figure 4.29, where $\nabla\chi(t) = 4.5 \times 10^{-5} \text{ steps}^{-1}$ (as seen in Figure 4.25(c)). While all the tested functions for χ above approached the level of $\chi = 1$ from below and started from close to zero positive values, none of them actually reached the neutrality level of $\chi = 1$. In contrast, the case in Figure 4.25(c) not only reaches the level of $\chi = 1$, but also enters the semi-plane of $\chi > 1$, where the attacker attempts to slow the rotor below the equilibrium level of speed ω . This results in the full pulsation period fitting within the attack window of $t = [1.5, 2)$ seconds, causing the currents and voltage to reach zero level at the end of the attack at $t = 2$ seconds. The zero crossing point occurs earlier at around 1.66 seconds, and χ_0 is higher at 0.399 compared to previous cases where it was 0.3 for $\nabla\chi(t) = 1.5 \times 10^{-5} \text{ steps}^{-1}$ and 0.34 for $\nabla\chi(t) = 3 \times 10^{-5} \text{ steps}^{-1}$. At the same time, the speed ω reaches a stable operational level at which the system enters the

post-attack area of $t > 2$ seconds. As a result, the attack withdrawal syndrome disappears, which may improve the attacker's covertness.

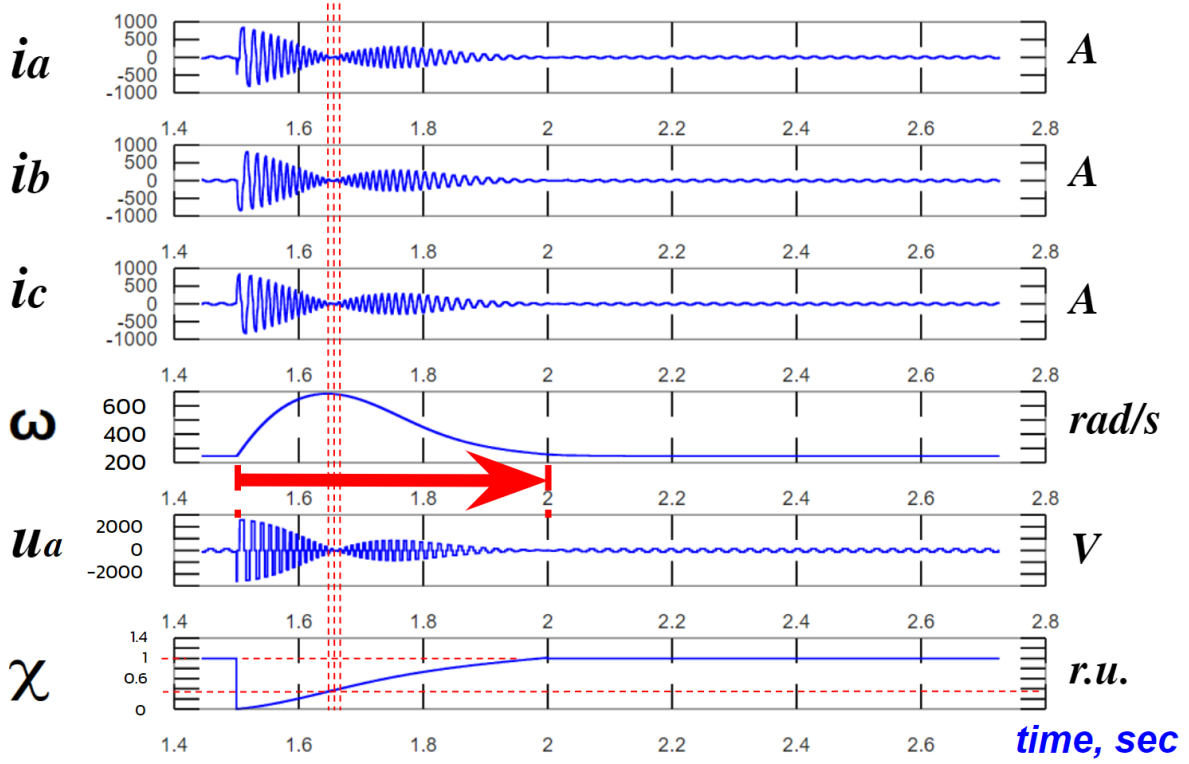


Figure 4.29: System response to the attack followed by negated attack withdrawal syndrome for gradient $\nabla\chi = 4.5 \times 10^{-5} \text{ steps}^{-1}$ as in Figure 4.25(c). The attack window is marked with a red arrow. State variables shown include: winding currents (i_a , i_b , i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).

Further increases in the gradient of the linear χ -function, as in the cases of Figures 4.25(d) and 4.25(e), strengthen the trends of shifting the zero-crossing point to an earlier time and slightly increasing the related values of χ_0 , as shown in Figures 4.30 and 4.31, respectively. Furthermore, the attack withdrawal syndrome returns in its inverted form of accelerating the rotor back to its no-attack equilibrium speed ω level. However, the generated levels of current and voltage remain within the regular operating limits of the BLDC motor and do not pose a threat to the system. These generated levels may serve as indicators of the attack, reducing its covert nature and making it undesirable for the attacker. This sets the upper limit for the prospective gradient values of linear gradient χ -function.

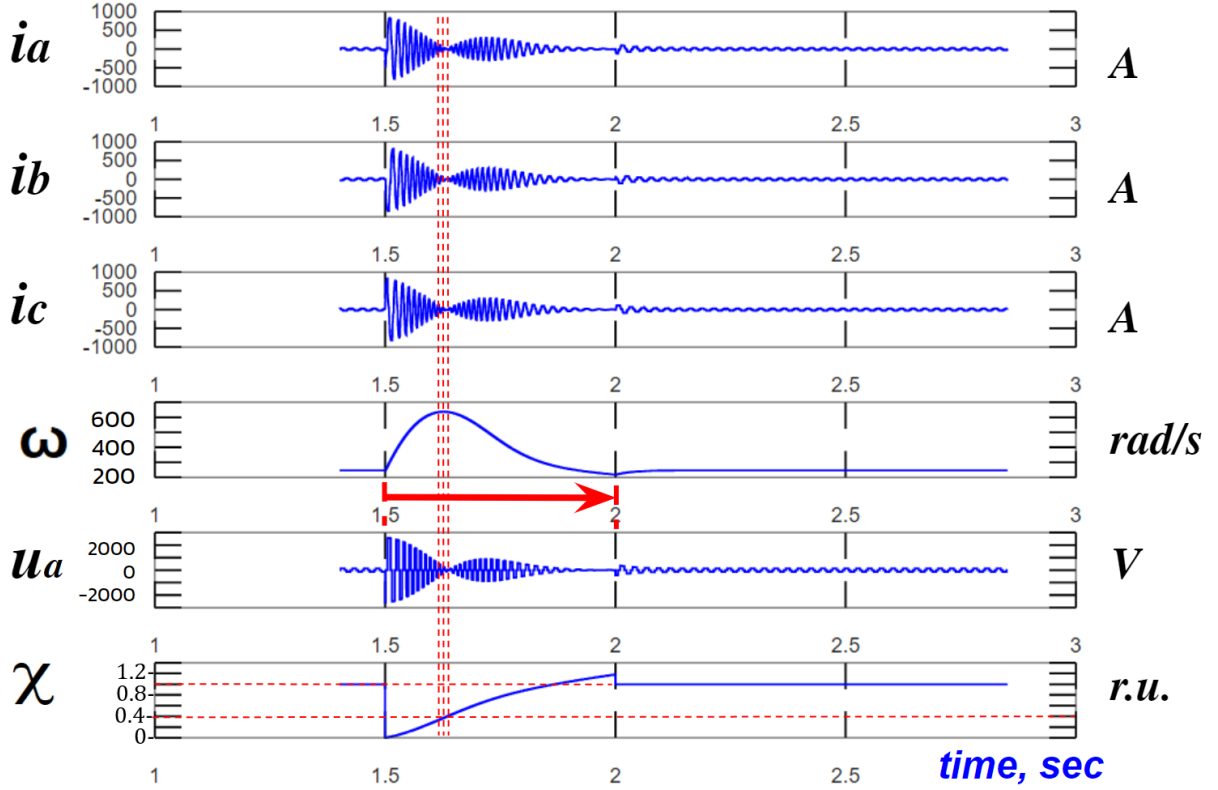


Figure 4.30: System response to the attack followed by reappearing inverted attack withdrawal syndrome for gradient $\nabla\chi = 6 \times 10^{-5} \text{ steps}^{-1}$ as in Figure 4.25(d). The attack window is marked with a red arrow. State variables shown include: winding currents (i_a , i_b , i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).

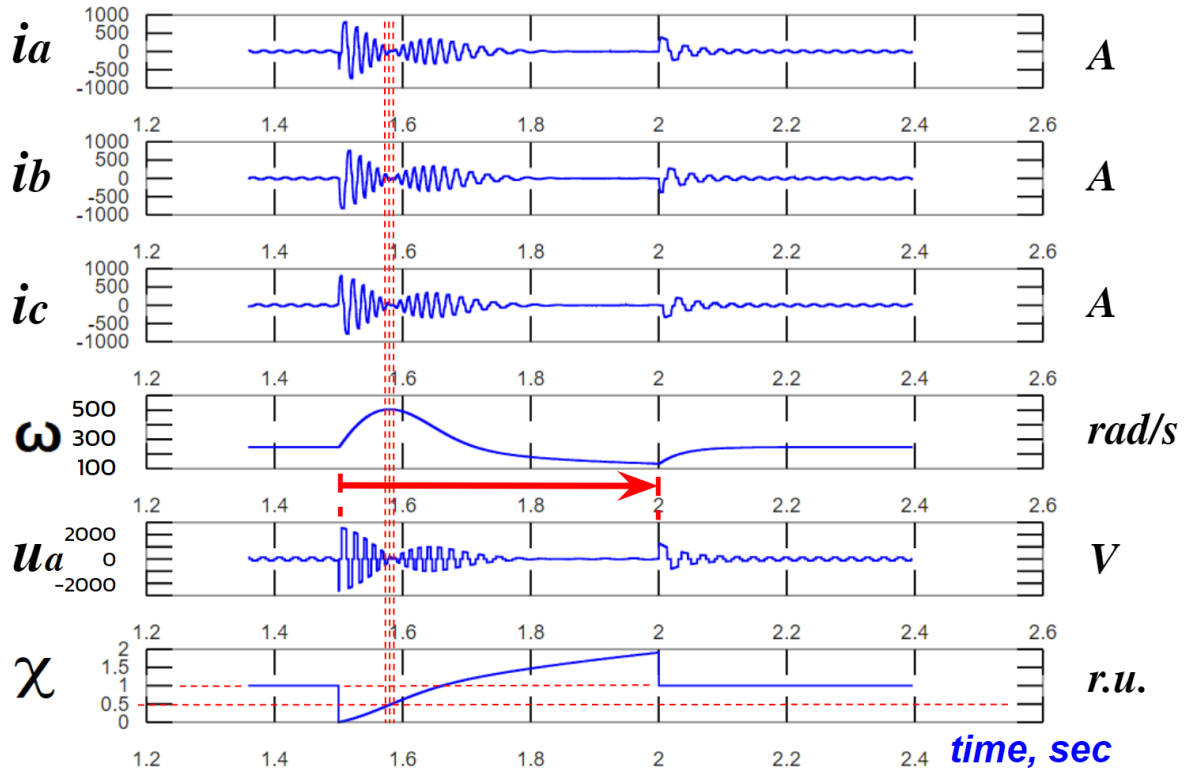


Figure 4.31: System response to the attack followed by inverted attack withdrawal syndrome for gradient $\nabla\chi = 15 \times 10^{-5} \text{ steps}^{-1}$ as in Figure 4.25(e). The attack window is marked with a red arrow. State variables shown include: winding currents (i_a , i_b , i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).

Induced Pulsations Attack: Analysis and Discussion

The simulation experiments presented above show that, within the bias injection paradigm, a linear gradient distortion function provides attackers with the opportunity to induce high-amplitude pulsations in both the current and voltage scales of the BLDC motor windings. Peak values of about 1000 A in current and 2500 V in voltage scales pose a significant threat to the integrity of hardware elements, and as such, may lead to circuit breakdowns. The damaging power of this induced pulsation attack can be increased by interrupting it before the end of the pulsation modulation period. For example, if the attack is interrupted in the middle of the second half of the asymmetric sine modulation wave, when the acquired rotation speed significantly supersedes that of the attack-free equilibrium level, additional and/or even stronger impact will be produced by the ensuing attack withdrawal syndrome effect.

On the other hand, if the attacker wants to avoid possible detection from defense devices, it is advantageous to prioritize the covert nature of the attack. In such cases, engaging the attack withdrawal syndrome may appear to be counterproductive as it can reveal features of the attack signature. The attacker has the option of eliminating the attack withdrawal component from the attack content by equalizing the attack duration to the full length of the pulsation modulation period of the asymmetric sine wave. In other words, terminating the attack at the end of the period of induced pulsation wave ensures the absence of the attack withdrawal syndrome and provides a smooth transition of the system from the state of being under attack to attack-free operation.

A similar dilemma arises when selecting the modulation depth of the distortion χ -function and its gradient for the attack. The attack's effect is more powerful when the modulation depth is deeper, resulting in a larger deviation from the $\chi = 1$ state, as well as when the gradient $\nabla\chi$ values are smaller, which prolong the deviation from the $\chi = 1$ state. Conversely, a larger gradient $\nabla\chi$ results in a faster approach to the neutrality level of $\chi = 1$, thus reducing the attack's impact. Therefore, for the sake of covertness, the attacker should prioritize a shallow depth of χ -modulation and a higher gradient of χ . However, the attack's impact is more substantial for deeper modulation of χ and lower $\nabla\chi$. The attacker may compromise by shortening the attack duration for higher $\nabla\chi$.

And last but not least, the observation is that crossing the neutrality level during an induced pulsation attack does not bring benefits to the attacker, neither in terms of attack strength nor in terms of covertness. The first reason is that the attack strength weakens in the vicinity of the neutrality level $\chi = 1$, so approaching to cross this level hinders the attack itself. For the second reason, reversing the proportionality of χ from $\chi < 1$ to $\chi > 1$ only changes the sign of the $\delta\omega$ term to be added to the equilibrium value of speed ω . This, in turn, reverses the sign of the attack withdrawal syndrome from slowing down to acceleration but it still serves as an identifier for the

attack detectors, thereby reducing covertness.

Summary of the Findings on Induced Pulsations Attack

In conclusion, the modeling and simulation of the bias injection of distorted values into the Kalman filter's estimations of the BLDC motor's angular speed, within the feedback loop of the control system, can force the system into an induced pulsation mode. An attacker can create this opportunity by employing a linear distortion function with a constant gradient, which initiates an interactive reaction of the system to the injected disturbances.

The following characteristics of this induced pulsation attack under a constant gradient of linear distortion function have been identified:

1. The duration of one full period of induced pulsation is determined by the duration of the evolution of the distortion coefficient χ from a value close to zero to the neutrality level of $\chi = 1$.
2. The induced pulsation takes the form of an asymmetric sine wave with a peak value of about 1000 A for current and 2500 V for voltage under the condition of equilibrium angular speed $\omega = 250$ rad/s.
3. The peak value of the induced pulsation is defined by the maximum depth of χ deviation from the neutrality level $\chi = 1$ towards zero. The gradient value of the engaged linear distortion function does not affect the peak value in pulsation.
4. The gradient of the linear distortion function defines the zero-crossing point for the pulsation modulation function of current and voltage in the windings, and it also has some influence on the depth value χ_0 at which zero crossing occurs. The measured values of χ_0 are 0.3, 0.34, 0.399, 0.41, and 0.5 relative units for the gradients of 1.5×10^{-5} , 3×10^{-5} , 4.5×10^{-5} , 6×10^{-5} , and 15×10^{-5} of the linear distortion function, respectively.
5. This technique also enables the control of the magnitude and sign of the system reaction to the interruption of the attack, which we call the 'attack withdrawal syndrome'. Specifically, interrupting the attack at $\chi < 1$ leads to current and voltage outbursts for decelerating the rotor, followed by an exponential decay. The demonstrated peak values of outbursts were 1000 A in current and 3800 V in voltage, which exceeded peak values for the attack itself. This allows using the attack withdrawal syndrome as an additional attack feature. Moreover, to prioritize the covertness of the attack, the attack withdrawal syndrome can be nullified by adjusting the attack termination moment to that of crossing the equilibrium line of $\chi = 1$.

Stemming from the findings of the induced pulsations attack based on the linear, uninterrupted recovery of initially shrunk values of the distortion parameter χ , the next exploration area for the adversary involves investigating interrupted linear distortion functions for χ , as these offer the potential advantage of periodical renewals in the attack pattern. This is the subject of the next subsection.

4.5.2 Extended Pulsations Cyber-Attack

A linear distortion function with a constant gradient ($\nabla\chi$) can cause induced pulsations in the values of winding current and voltage. To illustrate this result, we provide an example of a linear distortion function in Figure 4.32 and show its effect on the system's state variables, such as winding currents (i_a, i_b, i_c), angular speed (ω), and one of the control variables, winding "a" voltage (u_a). When the level χ reaches $\chi = 1$, which represents normal operating conditions, a secondary maximum in the induced pulsation for both current and voltage modulation is observed. However, if the linear trend of increasing χ continues beyond $\chi = 1$, the modulation amplitude for current and voltage decreases, and the rotor speed slows down. This may cause the angular speed to fall below its equilibrium value, which raises the issue of optimizing the interruption of the linear χ growth from the attacker's point of view. Interrupting the linear growth of χ allows the attacker to initiate the beginning of a new cycle of linear growth, which can extend the attack duration. This, combined with covertness, could inflict wear-and-tear damage to the motor and other system components. In an electric vehicle, for example, the mechanical strains caused by the attack could expand to transmission parts, increasing the wear potential.

Comparing this to the original linear distortion function, introducing interruptions in the linear up-trend for the distortion coefficient effectively converts the function from a simple ramp to a saw-like function. As a result of this transformation, new parameters emerge to govern the interaction process, such as the amplitude (associated with the height of the saw teeth) and the frequency of the saw-function (inversely proportional to the width of the saw teeth, i.e., its period).

Therefore, the purpose of this study is to identify the benefits an attacker may gain by manipulating the interruption of the linear growth of the distortion function. By doing so, the modulation depth (saw height) and frequency of the resulting saw-like χ -function can be varied, opening up an unexplored domain. This goal overlaps with that stated in the first report on attacks involving distortion in the feedback loop data channel, specifically the 'current drainage' attack. The difference in this study is that we approach the problem from a different angle: starting with the linear distortion function and seeking to optimize the transformation process to maximize benefits for the attacker in scanning and identifying vulnerability states in the system. This back-end

approach allows us to explore the full range of saw depth and saw frequency variations based on manipulations of the system responses. The initial version of the study only covered one-sided trends over a narrow range of depths and frequencies, which resulted in a limited and incomplete view. Expanding this coverage provides new insights into the process understanding and its practical implementation.

Exploring Interrupted Linear Distortion Functions

To verify the impact of interrupting the linear growth of the distortion function and varying the parameters of the resulting wide-range saw function for the distortion coefficient on system response, the following functions for χ have been used, as shown in Figure 4.32. In mathematical representation with coordinates of χ versus simulation steps (or increments used by the attacker, which are the actual sampling rates that the Kalman filter exercises based on the rotation speed), it can be observed that after the initial drop from the 'no attack value' of $\chi = 1$ to almost zero, the value of χ steadily increases while maintaining a constant first derivative until reaching the interruption point, $\chi_{\text{top}} > 1$. At the next iteration, the bias is reset to its bottom level value, χ_{bottom} , and a new cycle of growth begins. These cycles are repeated until the end of the attack window is reached, after which the χ coefficient is reset to one and the bias is dropped, allowing the system to evolve to its equilibrium state.

The selected wide-range saw functions for these tests cover a range of frequencies, from approximately 3.4 Hz to 14 Hz, including an intermediate point of around 6 Hz. The peak χ values (χ_{top}) reached in these functions vary from 1.5 to approximately 2.3 in its relative units (r.u.). The corresponding amplitude of the saw function is defined as $\Delta\chi = \chi_{\text{top}} - \chi_{\text{bottom}}$. On this scale, a value of one represents no distortion. Values close to zero indicate significant distortion, resulting in diminished estimates from the Kalman filter, while values above one indicate over-estimation, with estimates more than double the actual values. This selection of tests serves as a starting point for addressing the defined goal for the χ coefficient within the low-frequency range of the wide-range saw function. The effects of changing the frequency and the peak value (χ_{top}) of the employed wide-range saw function for χ within these defined parameter ranges are presented next.

Simulation Experiments with Extended Pulsation Attack

The results of the simulation experiments with the adversary engaging wide-range saw function for the attack are presented in the following order, as shown by Figure 4.32, for functions (a) to (c). The starting point for the wide-range saw function frequency, as indicated by Figure 4.32(a), is defined by the need to fit at least one saw-tooth into the attack window of a selected duration of

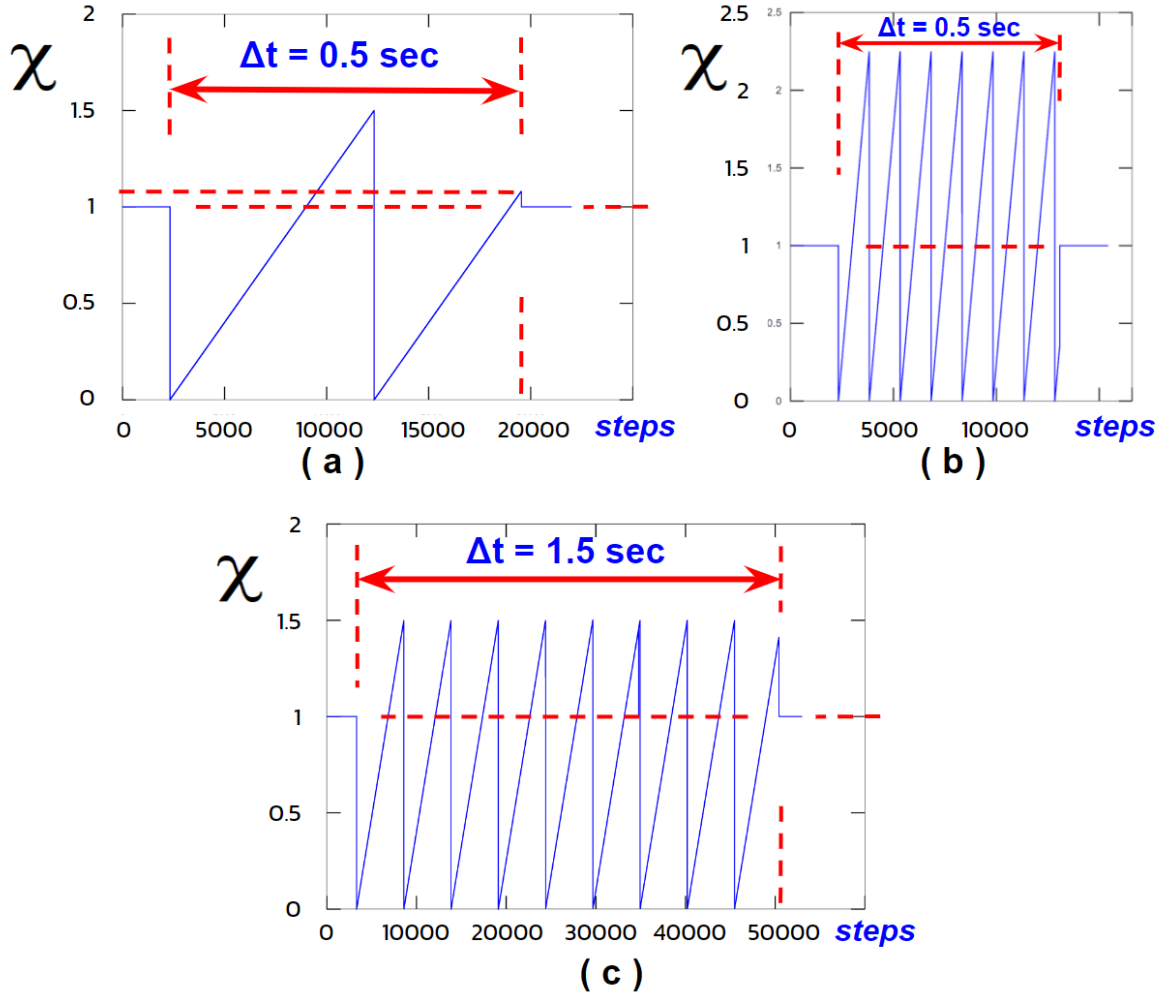


Figure 4.32: Wide-range saw functions tested to verify the impact of interruptions in linear growth and modifications to the parameters of the resulting wide-range saw functions on system responses. The functions cover a range of frequencies (approx. 3.4 Hz to 14 Hz) and peak χ values (χ_{top}) (specifically, $\chi_{\text{top}} = 1.5$ and $\chi_{\text{top}} = 2.3$ r.u.).

0.5 seconds. A frequency of approximately 3.4 Hz is chosen to fully fit one complete saw-tooth and a significant portion of the second tooth within the 0.5 sec attack interval. This allows for the observation of the impact of the connection between two consecutive teeth of the saw-function, as well as an interruption of the attack before the end of the second saw-tooth. The range of χ change in terms of the peak χ value (χ_{top}) covers values from almost zero ($\chi_{\text{bottom}} \approx 0$) to approximately 1.5, encompassing areas below and above the equilibrium level of one.

The overall result of connecting two teeth of a saw function to represent the distortion is presented in Figure 4.33. To confirm system model functionality and stable operation, the figure also includes preceding system tests (as detailed in Figure 3.4). The attack event is initiated after stabilization at $t = 1.5$ s, placed within the time window of $t = [1.5, 2.0]$ s, and is followed by the system's subsequent recovery and stabilization.

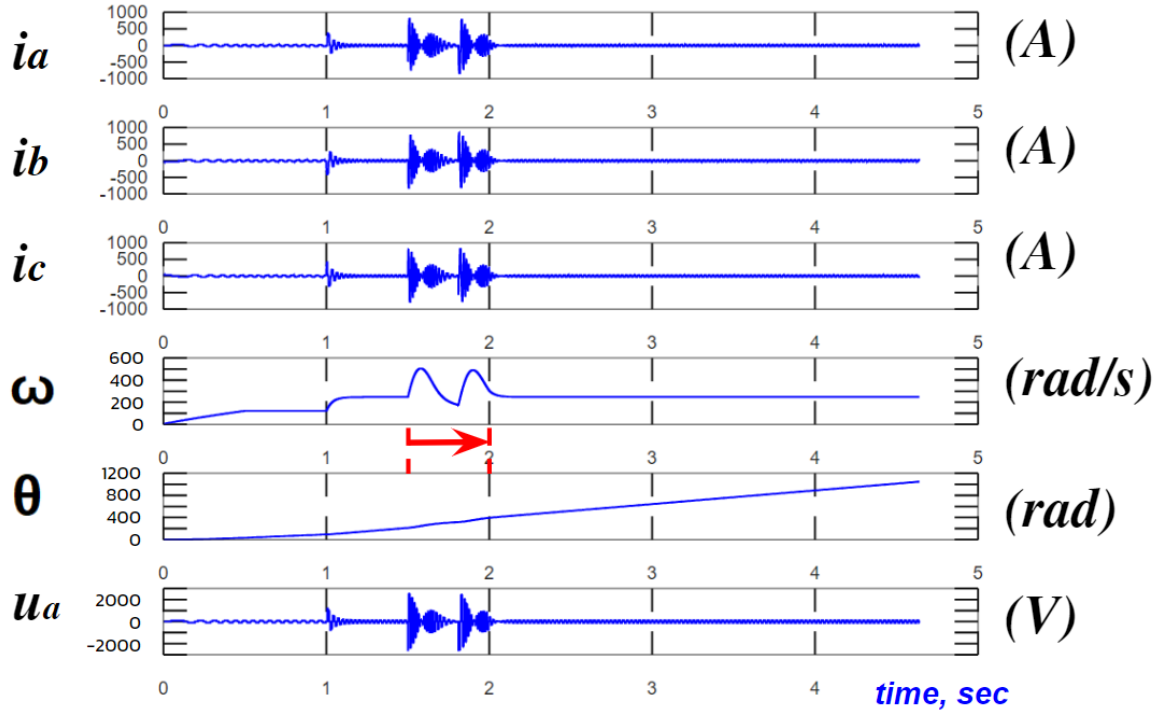


Figure 4.33: Extended pulsations induced by synchronization between the system's response and the distorting activity of the attacker under engaging of a wide-range saw function (as shown in Figure 4.32(a)) with a repetition frequency of approximately 3.4 Hz and peak χ value of 1.5 r.u. (relative units). The attack is placed within the window $t = [1.5, 2.0]$ s. State variables shown include: winding currents (i_a , i_b , i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).

The response for the second saw-tooth waveform closely resembles the pattern observed during the first one, indicating a direct synchronization between the system's response and the distorting activity of the attacker. This suggests a strong correlation between the system's behavior and the attacker's actions, as evidenced by the repeating pattern in the system response.

A more detailed presentation of the phase relations between the system response and attacker manipulation for the same case is shown in Figure 4.34. In comparison to Figure 4.33, Figure 4.34 includes the mapping of χ values to the time domain, deviating from the triangular shape initially taken by the attacker within the coordinates of iteration steps as presented in Figure 4.32. The reason for this deviation is the nonlinear changes to the term of angular speed ω in the equation used to achieve interaction with the system when the attacker is calculating the required value of χ for a specific time moment of bias injection:

$$\chi = 1 + \delta\omega/\omega, \quad (4.2)$$

where ω is the estimated value of rotor angular speed obtained from the Kalman filter, and $\delta\omega$ is the injected bias for the required distortion of it.

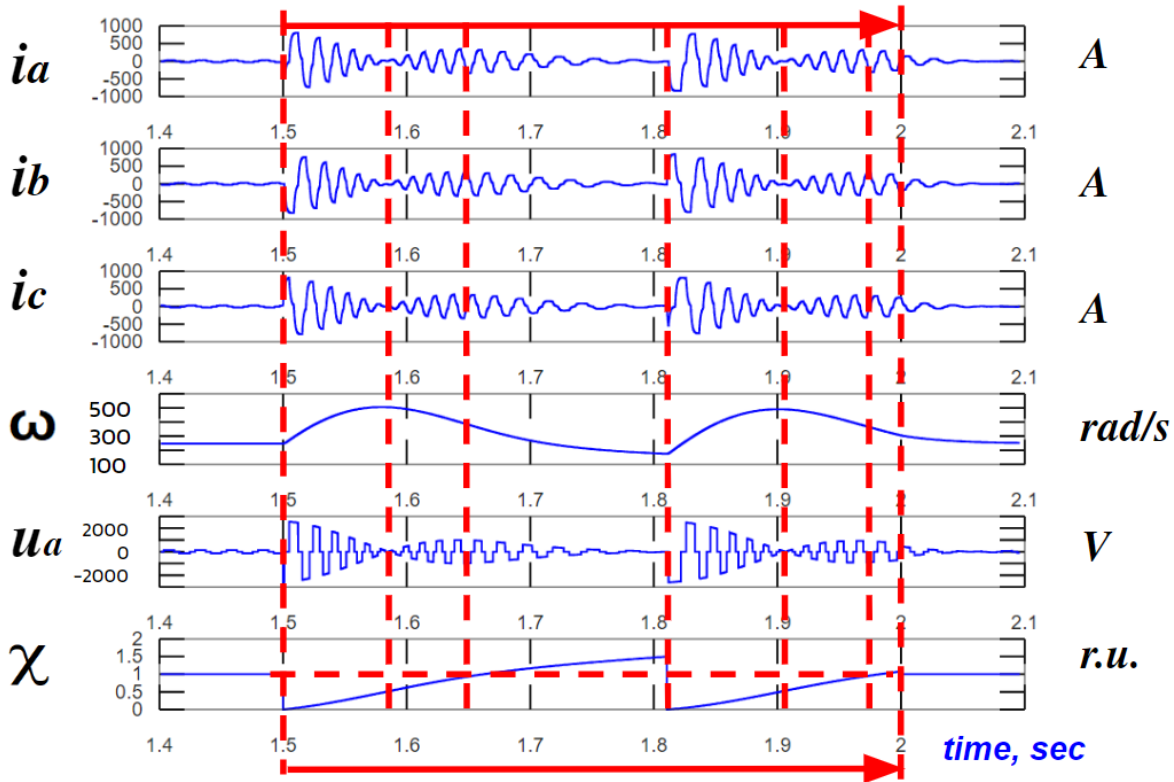


Figure 4.34: Phase relations between system response and attacker manipulation. The system response is plotted against the distorting activity of the wide-range saw function (as shown in Figure 4.32(a)), which has a repetition frequency of approximately 3.4 Hz and a peak χ value of 1.5 r.u. (relative units). State variables shown include: winding currents (i_a , i_b , i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).

The main phase relations here remain the same as in induced pulsation attack. Specifically, for each individual pulse response and each saw-tooth: (1) crossing the equilibrium level of

$\chi = 1$ corresponds to the peak value of the secondary modulation wave of the pulse, (2) the zero-crossing point between the primary and secondary peaks of the induced individual pulse corresponds to an intermediate level of $\chi < 1$, (3) values of $\chi > 1$ correspond to deceleration of the rotor below its equilibrium speed, and (4) the attack withdrawal syndrome phase and amplitude depend on the phase of the pulse at which interruption of the attack occurs. The case in Figure 4.34 illustrates the attack 'spill over' effect when the induced pulse continues beyond the point of attack termination due to the transition of the system from a disturbed state to the equilibrium one.

Tuning the frequency of the saw-function to approximately 14 Hz leads to a change in initially established synchronization between pulsations and saw-teeth, as Figures 4.35 and 4.36 illustrate. On the overall scale shown in Figure 4.35 with preceding system tests, the attack window appears to be filled with more chaotic pulse responses than that of one-to-one synchronization shown in Figure 4.34. Examination of the current and voltage patterns in the enlarged scale of Figure 4.36 reveals pattern repetition within each pair of consecutive teeth of the saw-function. Thus, synchronization between the saw-function and system response here is established for a first sub-harmonic of the saw-function. A higher level of the χ values up to about 2.3 r.u. allows for reaching deeper deceleration levels and, as a matter of consequence, higher modulation depth of the angular speed, which remains synchronized with the fundamental frequency of the saw-function.

The last simulation experiment is designed to illustrate the capability of extending the time window for the pulsation attack while maintaining the pattern throughout the entire extended period. The attacker chooses intermediate starting values for frequency and peak χ value of the saw-function, which are approximately 6 Hz and 1.5 r.u., respectively, as shown in Figure 4.32(c). The attack window is extended to cover the time window $t = [1.5, 3.0]$ seconds. The result of the simulation experiment is shown in Figure 4.37.

Comparing the χ -function initially chosen by the attacker, as shown in Figure 4.32(c) in mathematical form of simulation steps coordinates, with the resulting χ -function shown in the last row of Figure 4.37 in the time domain, some frequency tuning can be observed during the attack due to changes in the rotor speed. This affects the resulting frequency of χ to maintain interaction with the system, as per Equation 4.2. Due to the deceleration of the rotor and the overall average reduction in speed, the average frequency of the implemented χ is reduced to approximately 5 Hz in the time domain, from its initial value of approximately 6 Hz in the mathematical domain of simulation steps coordinates.

It can be observed from Figure 4.37 that the attack converges to repeating patterns in current, voltage, and angular speed modulation, and becomes sustainable for further extension.

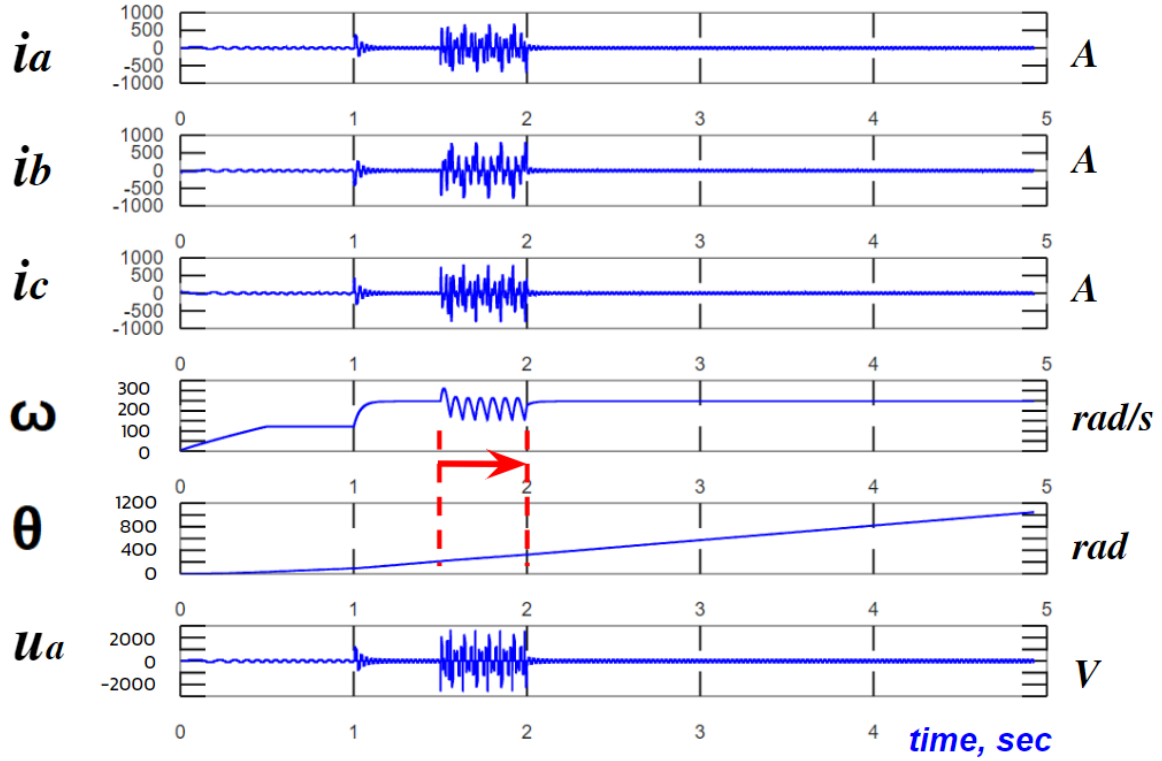


Figure 4.35: Chaotic features in system response due to the de-synchronization effect in the extended pulsation attack at a frequency of approximately 14 Hz for the wide-range saw function χ , as shown in Figure 4.32(b). De-synchronization of the current and voltage response patterns from the fundamental frequency of the saw-function is observed. State variables shown include: winding currents (i_a , i_b , i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).

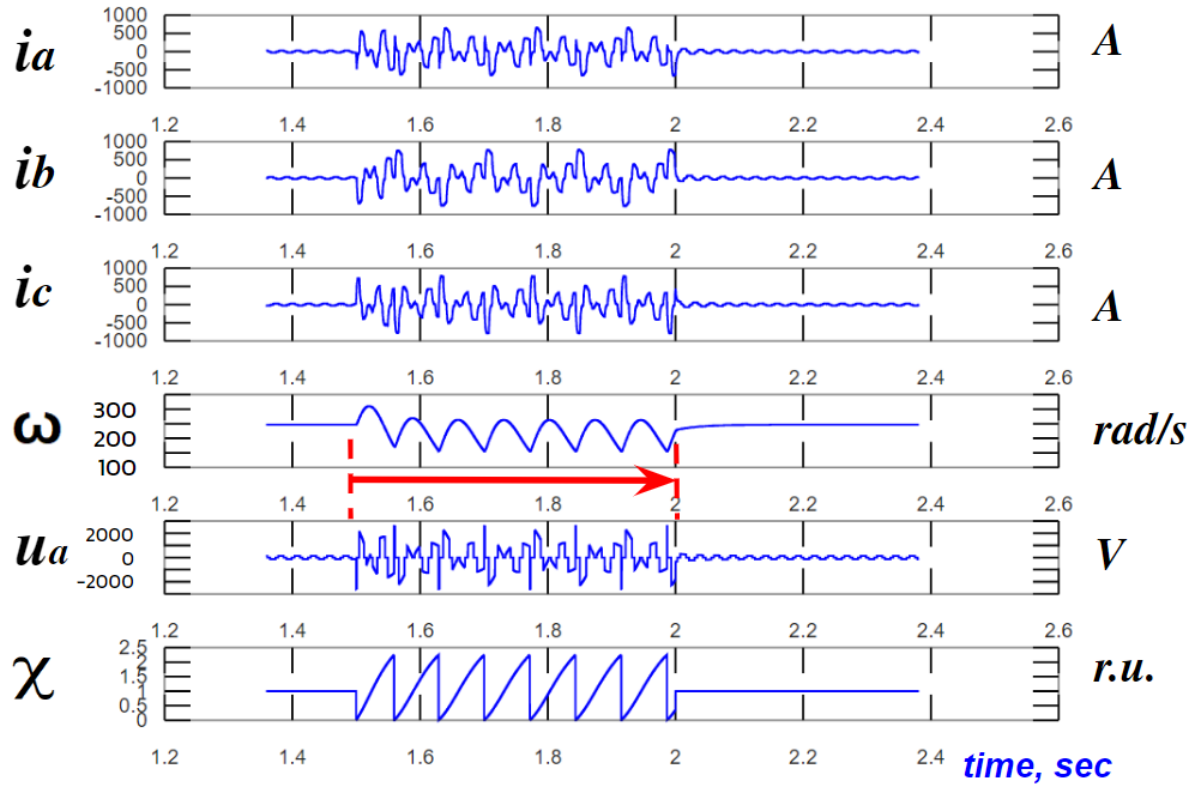


Figure 4.36: Chaotic response features under periodic influence at a frequency of approximately 14 Hz of the wide-range saw function of distortion χ , as depicted in Figure 4.32(b). De-synchronization of the current and voltage patterns with respect to the fundamental harmonic of the saw function is observed. State variables shown include: winding currents (i_a , i_b , i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).

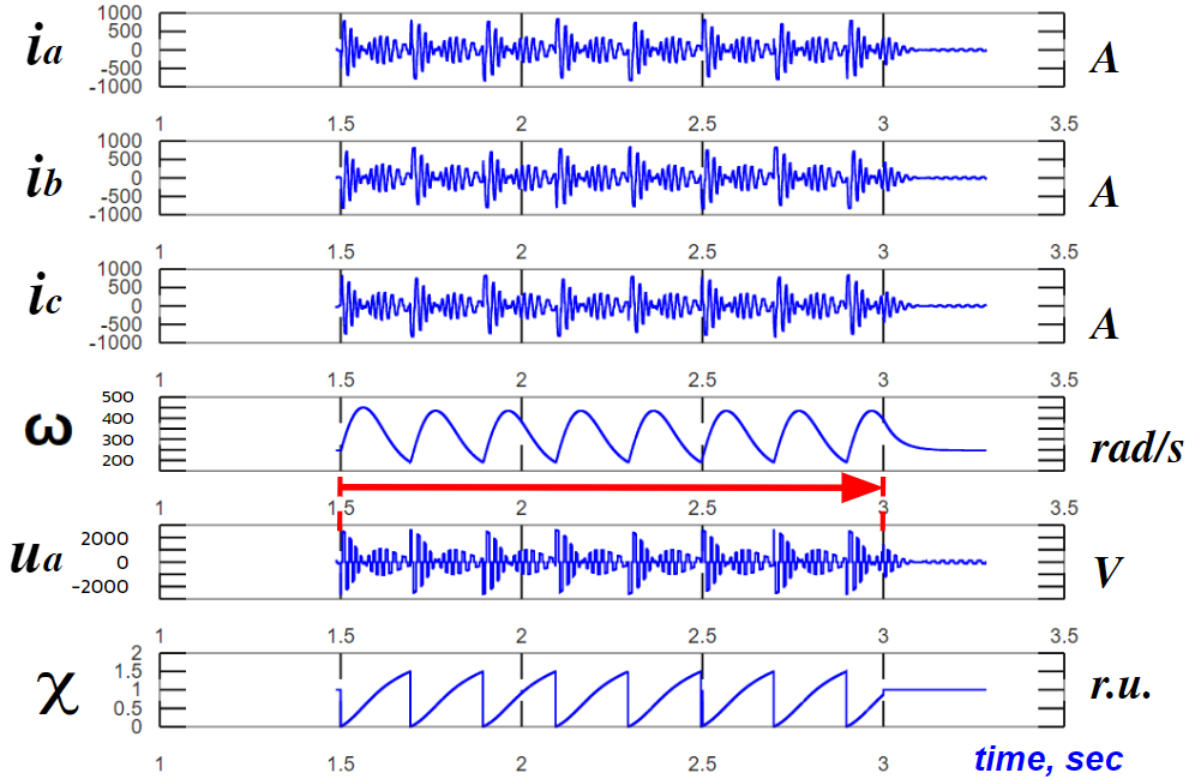


Figure 4.37: Repetitive nature of the system response within the extended pulsation attack window of $t = [1.5, 3.0]$ s for the initiating wide-range saw function of χ as depicted in Figure 4.32(c). State variables shown include: winding currents (i_a , i_b , i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).

Discussion of Extended Pulsation Attack Results

The above simulation experiments demonstrate that, when using the bias injection paradigm, introducing interruptions in the linear growth of the distortion coefficient and transforming the linear distortion function into a periodic wide-range saw function provides additional degrees of freedom for the attacker to manipulate the system responses interactively. This manipulation can be achieved through specific additional parameters such as the saw-function frequency and amplitude ($\Delta\chi$).

The results show that at least two modes of operation are accessible to the attacker. In the first mode, the current and voltage pulsation patterns are synchronized to the fundamental frequency of the saw-function, resulting in highly regularized modulation of pulses corresponding to the individual teeth of the distortion saw-function. This is accompanied by angular speed modulation of the rotor motion, with the average pulsation frequency being close to the fundamental frequency. The impact of this attack regime on the system is evident in the pronounced regular pulsations of the current and voltage in the circuits, as well as the mechanical part being affected by angular speed modulation.

However, it should be noted that the regularized pulsations of the first case can serve as revealing signatures of the attack and may be easily detected by attack detectors. A stealthier approach is observed when the current and voltage modulation patterns are synchronized to the first sub-harmonic of the distortion saw-function (the second mode). In this case, the pulsations acquire some irregularities, reducing their tractability due to their chaotic and noise-like appearance. Critically, the modulation of the angular speed remains synchronized with the fundamental frequency, resulting in comparable mechanical strains as in the first case of full synchronization to the fundamental frequency. This combination of added covertness with the same mechanical impact may be more attractive to the attacker in achieving their goals.

The demonstrated ability of the attack to extend with converging patterns of pulsations in current, voltage, and angular speed modulation has the potential for the attacker to target distributed in time accumulated damage. This would allow for improved covertness of the attack while still achieving the desired damages at the end of the procedure.

Summary of Findings on Extended Pulsations

In conclusion, the results of modeling and simulation experiments reveal that the induced pulsation attack converges to an extended pulsation attack pattern in the current, voltage, and angular speed of the rotor motion when a linear distortion function is transformed into a saw-function in the case of bias injection against Kalman filter-based estimates of the angular speed of a BLDC motor in a control system.

Two modes of synchronization patterns have been demonstrated for extended pulsation attack:

1. **Synchronization to the Fundamental Frequency:** The patterns in the current, voltage, and angular speed modulation repeat themselves at the pace of the fundamental frequency of the distortion saw-function.
2. **Synchronization to the First Sub-harmonic:** The patterns in the current and voltage are synchronized with the first sub-harmonic of the saw-function (a frequency that is twice as low as the fundamental one), while the angular speed modulation retains synchronization with the fundamental frequency.

The advantages of synchronization to the fundamental frequency are evident in the pronounced impact of the attack on circuits and mechanics, albeit sacrificing covertness. In the case of synchronization of the current and voltage patterns to the first sub-harmonic, covertness is improved by irregularities in pulsations, while still maintaining angular speed modulation at the fundamental frequency and therefore sustaining mechanical strains at the initial level.

The extended nature of the attack brings about the possibility for accumulated resulting impact under improved covertness of reduced levels of parameter modulation.

Having obtained the synchronization effects leading to extended pulsations for all state variables, the attacker would be more than inspired to further explore the domain of phase synchronization of the attack function modulation with the motor rotation motion. Some of the findings for the attacker on this route, which are of critical importance to the defender, are considered next.

4.5.3 Hyper-spiking Cyber-Attack

Previously, we presented simulation results demonstrating the "Extended Pulsation Attack" scenario, characterized by periodic asymmetric sine wave pulsations in both current and voltage of the circuit windings. Expanding on these findings, we present an extension of the attack that allows for tuning the phase shift of the attacking saw-function with respect to the rotor rotation phase. This adjustment enables the occurrence of periodic hyper-spikes in the voltage of the windings, with individual spikes reaching amplitudes of up to 6000 V, as Figure 4.38 attests. Consequently, this poses an increased threat to the physical integrity of the involved circuits.

We refer to the effect observed in Figure 4.38 as the hyper-spiking attack for its occurrence only in the voltage domain. All other variables, such as currents in the windings i_a , i_b , i_c , and the angular speed ω , exhibit behavior similar to that under the extended pulsation attack, to which the

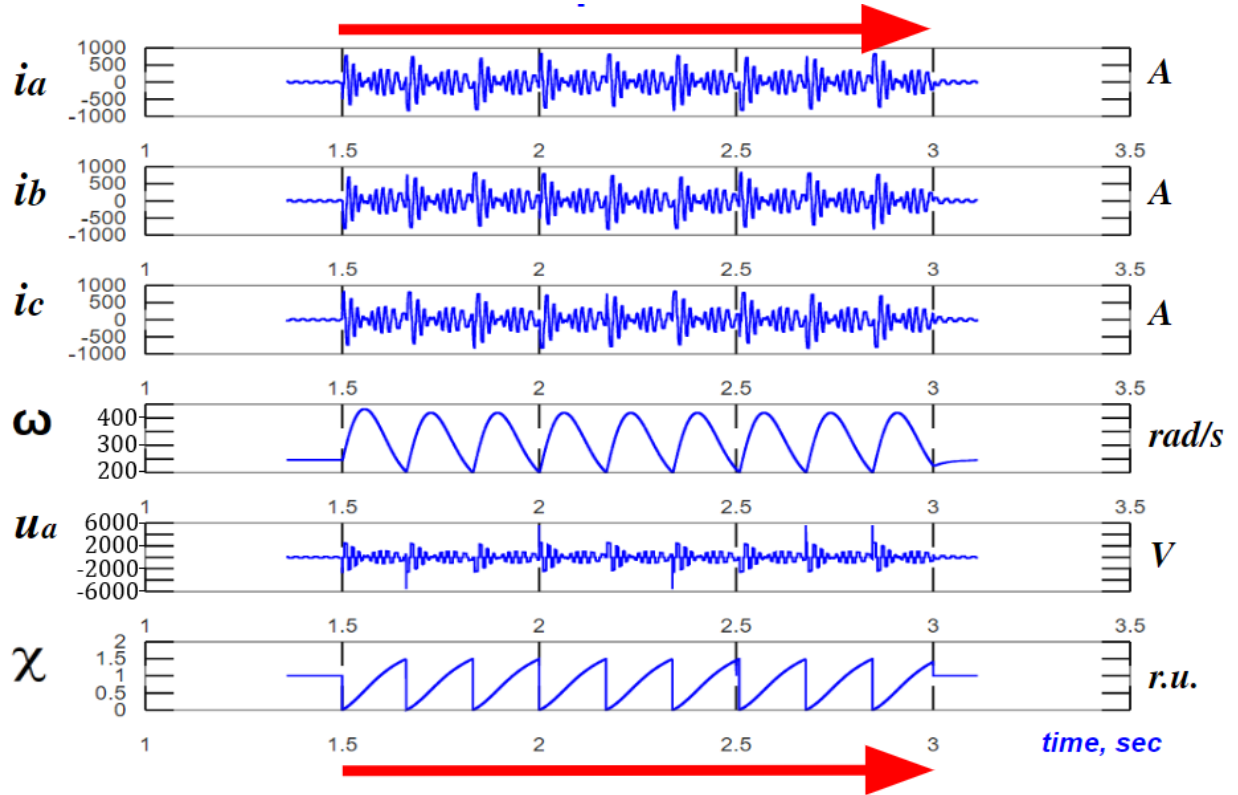


Figure 4.38: Hyper-spikes occurrence within the extended pulsation attack at a saw-function modulation frequency of approximately 6 Hz. Attack window duration is fixed to $\Delta t = 1.5$ s, with time allocation for each sampling step dynamically linked to the angular speed ω . State variables shown include: winding currents (i_a , i_b , i_c in A (Amperes)), rotor speed (ω in rad/s (radians per second)), rotor position (θ in rad (radians)), and phase voltage (u_a in V (Volts)).

hyper-spikes add on the top extras of electrical circuit's challenges. Specifically, from extended pulsation retained are the following features:

- 1) operating currents and voltages experience sine wave low-frequency modulation, and
- 2) the angular speed ω follows the current pulsations with the same frequency and high amplitude. The angular speed ripples in Figure 4.38 reach a maximum amplitude ($\Delta\omega$) of ± 150 rad/s at the no-attack base speed (ω_{base}) of 250 rad/s, or 60% of ω_{base} .

The maximum of induced sine wave pulsations are around 2000 V, while hyper-spikes exceed this value by about three times, with the peaks reaching 6000 V. This gives an edge to the attacker in the move to exceed the electrical break-through threshold in control circuits or windings.

There appear to be three essential conditions that must be satisfied for the hyper-spiking effect to occur.

1. **Abrupt Distortion Drop (χ Transition):** Hyper-spikes tend to emerge at moments of abrupt decreases in the distortion coefficient χ —that is, when χ suddenly and significantly deviates from its initial value. In Figure 4.38, such deviations occur when χ decreases from approximately 1.5 r.u. (well above equilibrium) to small positive values near zero (considerably below the equilibrium level of 1). This distortion forces the controller to switch from deceleration to strong acceleration. However, this condition alone appears to be *necessary but not sufficient* for a hyper-spike to be generated. For instance, during an extended pulsation attack, this transition occurs periodically yet does not produce hyper-spikes unless an additional, second condition is also fulfilled.
2. **Resonant Frequency Condition:** The occurrence of hyper-spikes requires a resonant relationship between the modulation frequency of χ (f_χ) and the frequency of rotor rotation (f_{rotor}), defined by the motor's angular velocity ω . This resonance manifests as the appearance of hyper-spikes only at specific modulation frequencies of χ corresponding to a given motor speed. In the simulation experiment presented in Figure 4.38, this resonant condition was achieved by fine-tuning the modulation frequency of χ , which in turn was controlled through subtle adjustments of χ' at fixed levels of χ_{bottom} and χ_{top} .
3. **Sufficient Attack Duration:** The attack duration must be sufficiently long for hyper-spikes to manifest. Specifically, the attack should exceed several of the longest inter-spike intervals so that at least two consecutive spikes fall within the attack window. If the attack duration is shorter than the longest inter-spike interval, then—even when the resonance-frequency phase condition is satisfied—no spikes may occur, or only a single spike may appear and be misinterpreted as an outlier. Consequently, a hyper-spiking attack may remain undetected.

It should be emphasized that even a single hyper-spike (on the order of 6000 V) may suffice to induce voltage breakdown failures, such as arc discharge, dielectric breakdown, or electro-burn within the control circuitry. For example, in Figure 4.38, five hyper-spikes are observed within the 1.5 s attack window (from $t = 1.5$ s to $t = 3$ s). The first four spikes are separated by approximately 0.333(3) s and are counter-phased, with each subsequent spike exhibiting an opposite polarity relative to its predecessor. The fifth spike, however, breaks this periodicity, occurring after only half that interval (0.166(6) s). Therefore, under the resonance-frequency condition illustrated in Figure 4.38, a 1.5 s attack duration is sufficient to guarantee the occurrence of hyper-spikes, whereas a substantially shorter attack (e.g., 0.15 s) may fail to include the expected hyper-spike within its temporal window.

Summary on Hyper-spiking Cyber-attack. This subsection introduces the *hyper-spiking* cyber-attack, an extension of the extended pulsation attack in which phase tuning of the attacking saw-function induces brief, large-amplitude voltage spikes in the motor windings (peaks up to ≈ 6000 V). The hyper-spiking attack (§4.5.3) represents a critical extension of the demonstrated extended pulsation attack, achieved by tuning the phase shift of the distortion saw-function relative to the rotor's rotation. This tuning successfully induces periodic hyper-spikes exclusively in the voltage domain (Figure 4.38), with individual peaks reaching up to 6000 V—a threefold increase over the voltage pulsations observed in the Extended Pulsation Attack—significantly escalating the threat of voltage breakdown failures (e.g., arc-discharge or electro-burn).

The underlying kinematic and electrical effects of the extended pulsation attack are retained, including low-frequency sine wave modulation of currents and voltages, and severe angular speed ripples (± 150 rad/s, or 60% of the 250 rad/s base speed). Although phase currents and rotor speed retain characteristic of the extended pulsation case (the low-frequency sine modulation and pronounced speed ripples), the hyper-spiking attack superimposes high-amplitude, short-duration voltage excursions that markedly increase the likelihood of physical damage to control electronics. Three necessary conditions for hyper-spiking are identified: (i) abrupt downward transitions in the distortion coefficient χ that trigger a switch from deceleration to strong acceleration; (ii) a resonant relation between the χ -modulation frequency and the rotor rotational frequency; and (iii) an attack duration sufficiently long to encompass multiple inter-spike intervals. Because even a single hyper-spike may cause voltage breakdown (e.g., arc discharge, dielectric failure, electro-burn), this attack provides the adversary with the means to achieve rapid physical damage, offering a high-impact, covert method for compromising the control system's integrity, thus presenting a significant threat to the host cyber-physical system.

4.5.4 Summary and Conclusive Remarks on Pulsations Cyber-attacks

The systematic exploration of Pulsations Cyber-attacks demonstrates that the vulnerability of cyber-physical systems extends beyond logical or parametric weaknesses into the domain of dynamic resonance and temporal coherence. Through progressively refined attack modalities—Induced, Extended, and Hyper-spiking—the study establishes how time-aligned, low-amplitude data injections can exploit the control-loop dynamics, leading to measurable distortions in current, torque, velocity, and feedback synchronization.

In the *Induced Pulsations Cyber-attack*, short-term injections with frequency components close to the natural oscillatory mode of the current or speed control loop triggered self-excited pulsations. Even when the injected magnitude remained below nominal sensing noise, resonance amplification produced sustained oscillations observable in motor current envelopes and control error trajectories. The effect was particularly pronounced when the attack frequency matched the system’s dominant eigenfrequency or when the phase shift between injected and feedback signals approached the resonant synchronization condition. This attack effectively converts minor cyber perturbations into persistent physical oscillations through dynamic feedback reinforcement.

The *Extended Pulsations Cyber-attack* elaborated on this mechanism by introducing longer-duration and amplitude-modulated injections designed to maintain phase-locking over extended intervals. Such attacks not only sustained oscillatory activity but also induced gradual drift in operating points and elevated root-mean-square (RMS) current, leading to thermal stress and degraded control accuracy. The extended temporal envelope allowed the oscillations to pass through the control loop filters, appearing as slow-varying quasi-stationary fluctuations rather than abrupt anomalies—thus complicating detection by conventional threshold-based monitors. Nonlinear coupling among harmonic components further generated sidebands observable in the frequency spectrum, evidencing energy transfer between the attack signal and the system’s inherent modes.

The *Hyper-spiking Cyber-attack* represented an extreme manifestation of resonance-based exploitation, where the injected sequence was synchronized with the inter-spike timing of system variables such as current ripples or switching events. When the attack duration exceeded several of the longest inter-spike intervals, a series of temporally aligned bursts (hyper-spikes) emerged, driving instantaneous current and torque deviations far above normal operational bounds. These bursts disrupted the regular spike-train structure, leading to phase desynchronization between control references and actual responses. The hyper-spiking regime exposed the system’s hypersensitivity to phase jitter and demonstrated that even minimal time-domain interference, if precisely timed, can cause disproportionate physical consequences.

Collectively, the three subclasses outline a continuum of pulsation-based threats: from transient resonant activation (Induced), to prolonged resonance locking (Extended), and finally to

phase-aligned burst amplification (Hyper-spiking). Across this continuum, the attack efficacy correlates with the degree of phase coherence and frequency matching between injected and system signals. The dynamic evolution observed—from low-amplitude periodic ripples to chaotic bursting—illustrates how cyber manipulation of temporal signal structure can progressively compromise system stability and safety margins.

From a defensive standpoint, these results underline the need for integrated monitoring strategies that extend beyond static anomaly detection. Countermeasures should include continuous spectral analysis, inter-spike interval variance monitoring, and phase-coherence tracking within control feedback loops. Incorporating adaptive damping or phase randomization in the controller design can mitigate resonance build-up and interrupt phase synchronization. Moreover, frequency-domain residual diagnostics can serve as early indicators of low-level resonant excitation before macroscopic instability arises.

In conclusion, the family of Pulsations Cyber-attacks reveals a distinct class of dynamic threats in which the adversary exploits temporal vulnerabilities inherent to feedback-regulated systems. By bridging the cyber and physical domains through frequency and phase manipulation, these attacks transform minor data injections into self-sustaining oscillations or hyper-spiking bursts. The obtained insights provide both a conceptual and analytical foundation for developing dynamic-resilience frameworks capable of predicting, detecting, and suppressing resonance-based intrusions in safety-critical cyber-physical infrastructures.

Consideration so far has covered scenarios of attacks against an unprotected host cyber-physical system with no protection against bias injection by the adversary. The attacker in such cases had full manipulative control of the data in the feedback loop. The main focus there was on the creativity of the attacker and the possibilities available to him to overtake control over host operation and efficient ways to either undermine system efficiency, or inflict various kinds of damages via mechanical dis-functionalities or electrical breakdowns. Such aggressive activities, however, are detectable by the sensors (which record the deviations) and subsequently analyzed by anomaly detectors designed to oversee the malfunctioning at early stages. If such malfunctioning is caused by the attack, then building defense structures within the operating host may potentially negate the consequences of the attack and, in the best case scenario, allow flawless operation under attack. More realistically, defense capabilities may partially block the most destructive attacking capabilities, reduce the adversary's efficiency, and gain time to locate the root cause of the security violations and eliminate the vulnerability without disrupting host operation. The implementation of the defense mechanism against bias injections is considered next.

4.6 Linear Defense Implementation

Following the discussion of system vulnerability under hyper-spiking and resonance-induced current drainage, the next step is to introduce an active defense mechanism capable of suppressing such attacks before they escalate to destructive or destabilizing amplitudes. The proposed *Linear Defense Strategy* represents the first layer of the defensive framework, aimed at restoring current predictability and re-establishing dynamic equilibrium under adversarial data injection. This subsection extends and generalizes the approach to originally formulated defense principle. Here, the method is reformulated within a broader cyber-physical context and linked directly to the defense taxonomy. Accordingly, this Linear Defense is treated as a baseline—yet analytically transparent—countermeasure, preceding the nonlinear and adaptive extensions as prospects for future work.

4.6.1 Linear Defense Strategy

The central concept of the Linear Defense Strategy lies in reconstructing the expected dynamic behavior of the plant using a *linear dynamic predictor* that operates parallel to the main control loop. This predictor continuously estimates the nominal current trajectory under legitimate operating conditions, providing a reference signal that can be compared to the actual feedback stream. Any deviation exceeding a dynamically adjustable threshold is interpreted as a potential manifestation of data injection or current distortion. By relying on linear dynamic modeling, the approach ensures computational simplicity and real-time implementability, which are essential for embedded control environments and resource-constrained industrial controllers.

Mathematically, the Linear Defense operates as an auxiliary observer built on a linearized representation of the system dynamics:

$$\hat{\mathbf{x}}(k+1) = \mathbf{A}_L \hat{\mathbf{x}}(k) + \mathbf{B}_L \mathbf{u}(k), \quad (4.3)$$

where $\hat{\mathbf{x}}(k)$ denotes the predicted state vector, $\mathbf{u}(k)$ is the input (typically voltage or command signal), and $\mathbf{A}_L$, $\mathbf{B}_L$ are the corresponding state-space matrices derived from the nominal linear model. The discrepancy between predicted and measured feedback currents,

$$\Delta i(k) = i_{\text{meas}}(k) - i_{\text{pred}}(k), \quad (4.4)$$

serves as the core diagnostic variable. Under normal operation, $\Delta i(k)$ remains bounded within the tolerance range determined by system noise and model uncertainty. During a cyber-attack, particularly one introducing malicious current perturbations synchronized with the system's nat-

ural oscillation frequency, $\Delta i(k)$ exhibits a distinct transient pattern that can be detected early enough to trigger corrective control or isolation measures.

The Linear Defense, therefore, acts as both an *anomaly detector* and an *active damping compensator*. Once abnormal residual behavior is detected, a proportional corrective signal is injected into the control loop:

$$u_{\text{def}}(k) = -K_D \Delta i(k), \quad (4.5)$$

where K_D is a tunable defense gain that determines the strength of the compensatory feedback. Selecting K_D involves balancing sensitivity and stability: a high gain enhances rapid suppression of injected disturbances but may amplify noise-induced oscillations, whereas a low gain improves robustness at the cost of slower mitigation response.

In this way, the Linear Defense forms a fundamental building block for hierarchical protection architecture. While its simplicity limits its ability to handle nonlinearly modulated or frequency-shifting attacks, it remains invaluable as a first response mechanism capable of stabilizing system current before higher-order defense layers—such as adaptive or nonlinear predictors—are engaged.

Implementation Narrative. The implementation of the Linear Defense predictor is intentionally designed to require minimal computational overhead and no modification to the main control algorithm. The predictor module operates in parallel with the motor control loop, receiving the same command input $\mathbf{u}(k)$ and plant feedback signals $i_{\text{meas}}(k)$, while maintaining an independent state estimate $\hat{\mathbf{x}}(k)$. This modular structure facilitates easy integration into existing controllers or digital signal processors (DSPs) without interrupting the primary real-time operations.

The predictor parameters $\mathbf{A}_L$ and $\mathbf{B}_L$ are derived from the linearized plant model around its nominal operating point, typically obtained from the small-signal analysis of the BLDC drive. This linearization captures the essential current-to-voltage dynamics relevant to fast anomaly detection, while omitting higher-order nonlinearities that would otherwise increase computational complexity. Because of the model's linear form, all predictor updates can be computed using a few matrix–vector multiplications per control cycle, which is well within the processing capabilities of typical embedded microcontrollers.

An adaptive calibration stage can be optionally included to account for slow parameter drifts, such as those caused by temperature variation or component aging. During benign operation intervals, the predictor gain matrices are periodically adjusted using a least-squares minimization of the residual $\Delta i(k)$ defined in (4.4). This continuous self-calibration helps maintain alignment between the predictor and the actual system, ensuring that residual deviations remain primarily attributable to external disturbances or malicious injections rather than modeling errors.

Dynamic Response of the Linear Defense. The temporal behavior of the Linear Defense under both normal and attack conditions can be understood by examining the closed-loop interaction between the defense feedback (4.5) and the plant dynamics. When no attack is present, the predictor output $i_{\text{pred}}(k)$ closely follows the measured current, producing a near-zero residual. Consequently, $u_{\text{def}}(k)$ remains negligible, and the defense has minimal influence on nominal operation. The system thus behaves as an almost transparent layer that continuously monitors without interference.

During a current-drainage or resonant hyper-spiking attack, however, the measured current deviates abruptly from the predicted trajectory. This deviation causes a sharp increase in $\Delta i(k)$, which in turn activates the corrective signal $u_{\text{def}}(k)$. Because $u_{\text{def}}(k)$ is proportional to $\Delta i(k)$, the defense introduces a counter-phase component that effectively damps the artificially induced oscillations. From a frequency-domain perspective, this action increases the effective damping ratio of the current control loop and shifts the resonance poles away from the imaginary axis, thereby suppressing the energy accumulation that characterizes the hyper-spiking phenomenon.

The reaction time of the defense is mainly governed by the control-cycle period and by the selected gain K_D . Empirical tuning has shown that setting K_D to approximately one-third of the nominal controller gain achieves an optimal balance between disturbance suppression and noise immunity for typical BLDC applications. This configuration ensures that the Linear Defense can react within a few sampling intervals—fast enough to prevent sustained current amplification while maintaining system stability.

Attack–Defense Interaction Examples. To illustrate the dynamic interaction between the Linear Defense and the adversarial inputs, several representative scenarios were simulated using the same baseline model as in Section 4.5.3. When subjected to a short probing attack of limited duration, the residual $\Delta i(k)$ exhibited a single pronounced peak corresponding to the injected pulse, followed by rapid decay due to the compensatory effect of (4.5). This behavior demonstrates that the defense can neutralize low-intensity intrusions without introducing noticeable control perturbations.

Under a sustained resonant attack tuned to the system’s natural oscillation frequency, the defense acted as a stabilizing damper that reduced current amplitude by more than an order of magnitude compared to the unprotected system. The measured current converged back to the nominal limit within a few milliseconds after the attack termination, confirming the capability of the linear predictor to recover nominal operation automatically.

However, the defense’s effectiveness diminishes when the attacker dynamically shifts the injection frequency or employs nonlinear modulation patterns that fall outside the predictor’s linear bandwidth. Such cases motivate the development of the *Nonlinear Defense* framework, which

extends the predictor concept to handle adaptive and broadband attack patterns. Nonetheless, the Linear Defense remains a crucial foundation, ensuring that the system can resist or at least delay destabilization long enough for higher-order defenses to be engaged.

Summary of Theoretical Consideration. The Linear Defense Strategy establishes the conceptual and practical baseline for protecting the system against data-injection and current-drainage attacks. Its formulation as a linear dynamic predictor provides a transparent analytical framework that can be fully characterized in both time and frequency domains, enabling rigorous verification and straightforward hardware implementation. Because of its computational efficiency and ease of calibration, the method is particularly well suited for real-time applications where embedded controllers must maintain low latency and deterministic execution.

4.6.2 Experimental Problem Formulation for Defense

The modeling and simulation of injecting biased estimations of rotor angular speed values into the feedback loop of the BLDC motor control system (see architecture in Figure 4.39) revealed the occurrence of a current drainage effect in the motor's windings. This effect is suggested to be a potential threat that cyber attackers could exploit to disrupt the normal operation of controlled motor systems. Such disruption could result in excessive energy losses, overheating, power disruptions, and even circuit damage.

The computational procedure used in our study has been verified as suitable for use by an attacker in a *manipulative* game against such systems. This procedure involves employing a distortion tool to modify the feedback data stream values of angular velocity through multiplication with a distortion coefficient, denoted as χ . As a logical extension of this consideration, there is a need to develop viable defense approaches capable of negating the impact of such an attack on the cyber-physical system in question. These approaches should aim to achieve safe operation even under continuing attack conditions. Therefore, the goal of the present study is the design and verification of architectural defense mechanisms capable of negating, on the fly, the damaging effects of the current drainage cyber-attack against the BLDC motor control system.

4.6.3 Predictor-based Defense Architecture

In the attack design, the attacker is assumed to gain access to the data stream of the Kalman filter's state parameter estimates. The attacker engages in a manipulation game with the system by modifying the data values for the rotor angular speed ω , thereby triggering a corrective response from the controller. We also assume that the attacker is capable of ensuring the delivery of the

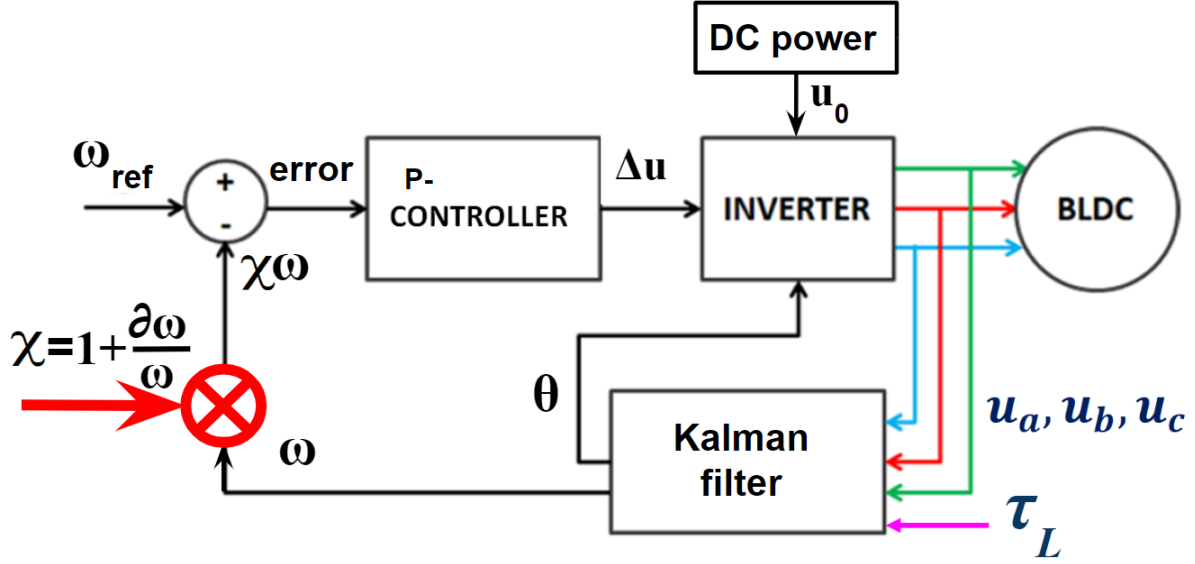


Figure 4.39: Architecture with position sensorless drive for BLDC motor as well as bias injection $\delta\omega$ access point. Kalman filter inputs are voltages in the respective winding, u_a, u_b, u_c , and load torque τ_L .

modified ω values to the error verification node (i.e., the comparator), making it challenging for the controller and defense measures to prevent this. Therefore, our goal is to design a defense strategy that leaves the feedback loop under the attacker's control while granting the defender observation privileges over the attacker's actions (i.e., the feedback loop) and control privileges over the Kalman filter (KF) outputs. As a defense measure, which adheres to these constraints, the current article suggests the introduction of a predictor into the control scheme, which makes one-step predictions of the distortion coefficient values that the attacker will use in subsequent iterations. Herewith, these predictions rely on a linear-dynamic predictor algorithm that takes into account the distortion coefficient value from the previous iterative time step, as well as its first and second derivatives.

The suggested defense circuit is illustrated in the Figure 4.40. It includes a predictor with inputs from both ends of the feedback loop where the attack occurs. By using inputs from the beginning of the feedback loop (i.e., the Kalman filter output) and its end (i.e., the comparator input), the predictor can estimate the injected bias (or calculate the value of the distortion coefficient employed by the attacker) and output a one-step prediction of the bias to be expected from the attacker, assuming inertia holds. In this context, inertia refers to the attacker retaining both the first and second derivatives of the distortion coefficient χ when changing the latter. For the sake of simplicity, we limit the accuracy of our consideration to the second derivative of χ . These assumptions enable the defender to engage in an asymmetric information game aimed at

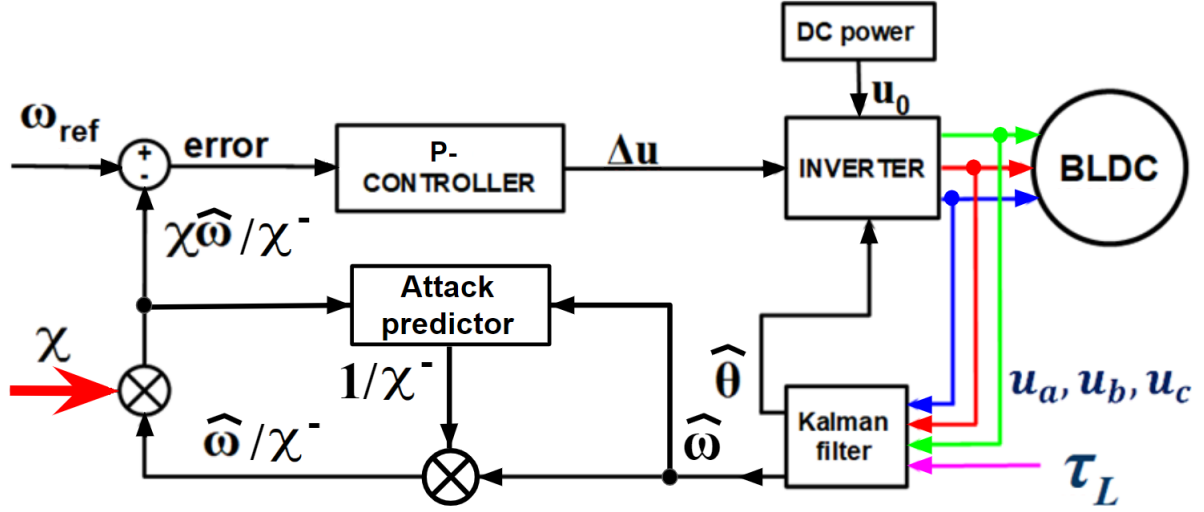


Figure 4.40: Introduction of defense circuit into control system feedback loop of Figure 4.39. Attack predictor inputs are (1) estimate of rotor angular speed $\hat{\omega}$ and (2) its modified by the attacker value of $\chi\hat{\omega}$ corrected by the prior cycle predicted distortion coefficient χ^- .

countering the attack. The defender can preemptively modify the KF's estimate of ω with the reverse value of the expected distortion coefficient χ^- , specifically designed to cancel out the expected distortion introduced by the attacker in the upcoming estimation cycle. If the predictor is idle, its output defaults to $\chi^- = 1$, and the attacker resumes the manipulation game with the system.

4.6.4 Current Drainage to be Negated

The effect of current drainage occurs in case of engaging distortion functions shown in Figure 4.41 (c) and (d). Some data on current drainage are already presented in reference [1] for saw functions with fully asymmetrical triangular tooth shape. Here we present additional current drainage case for the shallow saw function but with triangle tooth with increased symmetry shape. Symmetry of the saw tooth in the simulation program is defined by the number of sampling steps required to ascend from the base level to triangle highest point and the number of steps for descending back. Full asymmetry of triangular tooth shape for a given saw function modulation amplitude is corresponding to the case of descending from triangle top to its base level in one sampling step. Full symmetry here corresponds to the equal speeds of descend and ascend between triangle base and its top.

The cases of full asymmetry of triangle saw tooth functions are presented in reference [1] showing proportionality of the drained current values to the distortion coefficient χ . The triangle

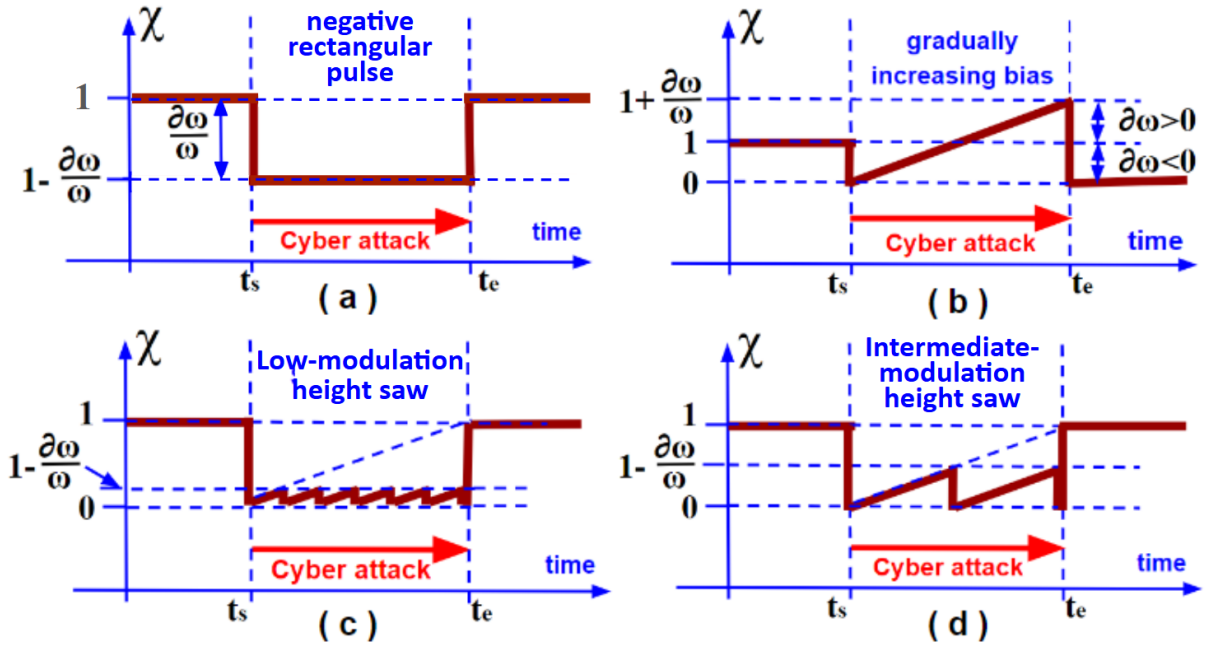


Figure 4.41: Tested distortion functions χ for the attacker manipulation game: (a) negative rectangular pulse; (b) gradually increasing bias; (c) saw function (deep-leveled, low-modulation height saw); (d) saw function (deep-leveled, intermediate-modulation height saw).

shape of saw function teeth there is also reproduced in the current modulation due to the above proportionality. Here we supplement those data with the partially symmetric triangle saw tooth shape. Partial symmetry is achieved by reducing the descend speed to the value of full height in hundred sampling steps instead of one step. The bottom of the shallow saw function for the resulting χ is presented here in Figure 4.42. The bottom part of the tested partially symmetric triangular shallow saw function, similar to that shown in Figure 4.41 (c), follows a specific saw pattern. The parameters of the triangular tooth $\triangle AOC$ are as follows: the ascending side AO is represented by (projected from) 1000 sampling steps of AB side, and the descending side OB is represented by (projected from) 100 sampling steps of BC side. The symmetry coefficient is defined as $\tan(\beta)/\tan(\alpha) = 0.01$, where α is the angle $\angle AOB$ and β is the angle $\angle BOC$ of $\triangle AOC$.

The current drainage effect, resulting from the attacker's use of the χ function from Figure 4.42 (i.e., the partially symmetrical shallow triangular saw function), under the condition of an idle defense, is depicted in Figure 4.43.

It is seen that at the attack starting point of $t=1.5$ s when the attacker drops (as in Figure 4.41, (c)) the values of distortion coefficient χ from its neutrality level of $\chi = 1$ to the level of $\chi \ll 1$ (of about 0.01484 relative units in Figure 4.42), the currents in the motor windings experience step-like increase due to compensatory voltage supply from the controller. Additional

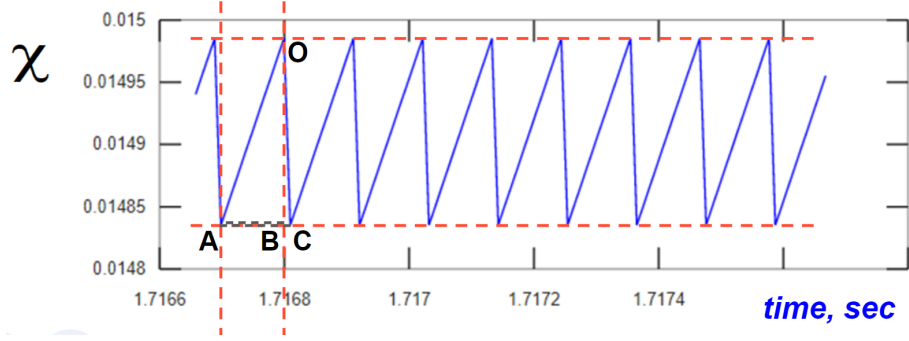


Figure 4.42: The bottom part of the tested partially symmetric triangular shallow saw function, similar to that shown in Figure 4.41 (c), follows a specific saw pattern. The parameters of the triangular tooth $\triangle AOC$ are as follows: the ascending side AO is represented by 1000 sampling steps of AB, and the descending side OB is represented by 100 sampling steps of BC. The symmetry coefficient is defined as $\tan(\beta)/\tan(\alpha) = 0.01$, where α is the angle $\angle AOB$ and β is the angle $\angle BOC$ of $\triangle AOC$.

voltage from controller is resulting in windings voltage increase first followed by respective increase of its currents. This, in turn, leads to gradual increase of the rotor angular rotation speed ω (forth strip in the plot Figure 4.43). For the given values of the χ modulation, the voltages modulation amplitude reaches 2000 Volts and respective currents reach 1000 Amps level (see Figure 4.43). Such current increase we call "current drainage" as it is caused by the attacker false data injection aiming to mislead the controller and waste the energy unnecessarily.

As in fully asymmetric case of shallow triangular saw function χ described earlier [1], the attack causes significant increase of windings currents, but symmetry in the teeth of saw function leads to smoother variations of the currents modulation. Potentially, this reduces amplitude of related ripples and increases stealthiness of the attack.

Essential here is accumulation of the attack energy in kinematics of the rotor rotation. This manifests itself in the increase of the angular speed ω . Such an accumulation of energy leads to an increased impact on the system when the attack activity is seized. We call such an impact "the attack withdrawal syndrome", which will be considered in the next section.

4.6.5 Attack Withdrawal Syndrome to be Negated

The attack withdrawal syndrome manifests as a sudden cessation of attack activity, resulting in the release of accumulated energy from the preceding attack. In Figure 4.44, this event corresponds to the termination of the attack at $t = 2$ seconds. In our specific case, this phenomenon arises due to a rapid signal change in the feedback loop, signaling the necessity to dissipate kinetic energy. To achieve this, the controller shifts the inverter into a deceleration mode to counteract the inertia of the rotor's rotation.

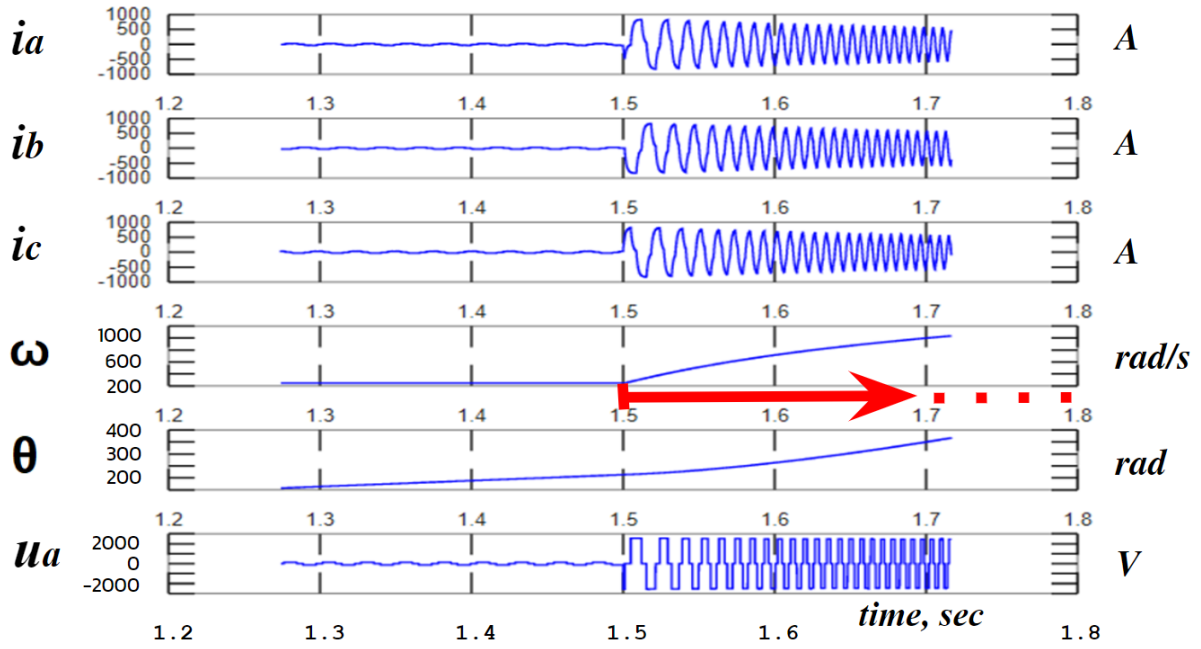


Figure 4.43: Current drainage effect observed under attack using the partially symmetrical shallow triangular saw function χ from Figure 4.42, with the defense system in an idle state. The attack commences at $t=1.5$ s and concludes at $t=2$ s, with the final phase depicted in Figure 4.44.

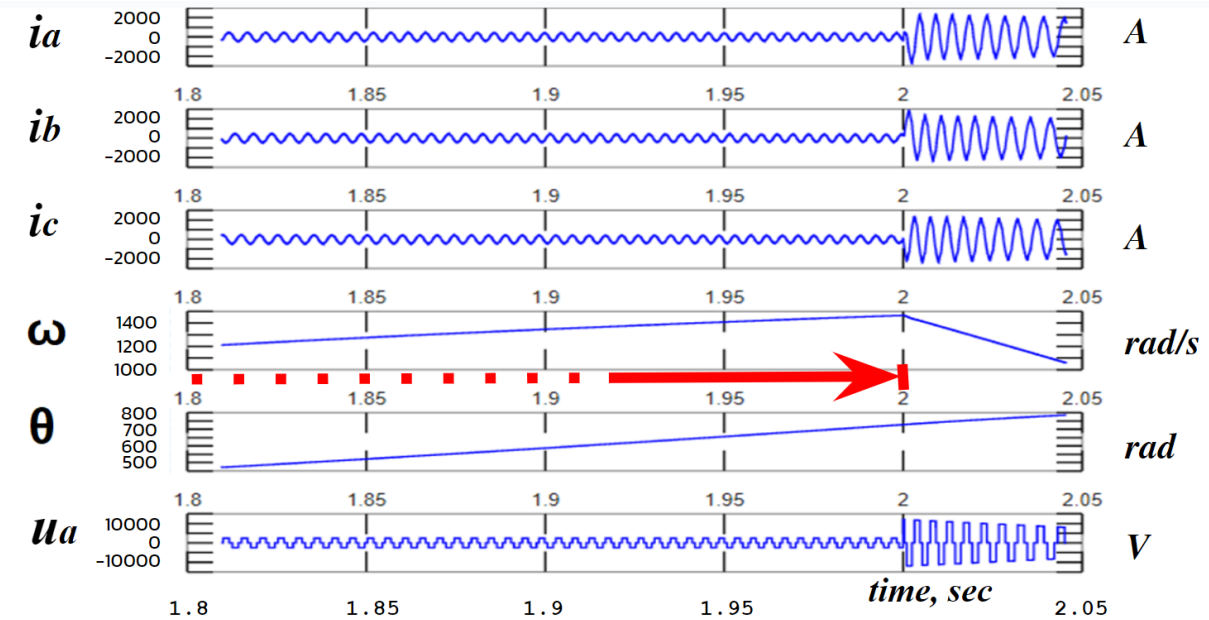


Figure 4.44: The observed effect of the attack withdrawal syndrome at the conclusion of the current drainage attack in a simulation experiment using the partially symmetrical shallow triangular saw function χ from Figure 4.42. This observation is made with the defense system in an idle state. The initial phase of the attack is depicted in Figure 4.43.

The "Attack Withdrawal Syndrome" effect is depicted in Figure 4.44 at the conclusion of the current drainage attack (at $t = 2$ seconds) in a simulation utilizing the partially symmetrical shallow triangular saw function χ referenced in Figure 4.42. Throughout this attack, the defense system remained inactive, resulting in a predicted χ -value of $\chi^- = 1$ for each subsequent iteration. The value $\chi^- = 1$, representing the inactive defense state, is reflected in both Figure 4.43 and Figure 4.44. Figure 4.43 illustrates the onset of the attack, while Figure 4.44 captures the conclusion of the attack followed by the system's post-attack relaxation. Both figures illustrate the operation of the architecture portrayed in Figure 4.40, where the value $\chi^- = 1$ persists. Upon comparing the amplitude changes in currents and voltages at the attack's onset ($t = 1.5$ seconds) and termination ($t = 2$ seconds), it is evident that the impact of the attack's cessation is notably more pronounced than that of its commencement. Specifically, the induced current upsurges within the windings fluctuate between +2000 and -2000 Amperes, while the voltage values vary between +10000 and -10000 Volts. Additionally, the rotor speed decelerates from 1400 radians per second to a static level of 250 radians per second.

4.6.6 Predictor Based Defense Operation

The defense approach explored here represents the initial steps a defender might take to sustain the proper operation of the system amid ongoing attacks. This assumes the defender has comprehensive insight into the attack activities. In our simulation experiment, this insight enables the utilization of signal distortions created by the attacker as input data for the defender module.

The defense architecture proposed here relies on the potential to forecast attacker actions based on past behavior. The schematic depicted in Figure 4.40 illustrates a defense approach built upon the defender's capability to predict the manipulations carried out by the attacker within the control system's feedback loop. The operation of this design is discussed further.

The defensive strategy outlined in Figure 4.40 is designed to ensure the normal operation of the system under continuous attack scenarios. Essentially, the defender observes the attacker's distortion action, $\chi_{(t)}$, at time t , and at that moment t predicts the next iteration's expected action, $\chi_{(t)}^-$, for the time $(t + 1)$ based on the attacker's historical distortion actions (e.g., at time points t , $(t - 1)$, $(t - 2)$, $(t - 3)$, etc.). Subsequently, at the next iteration $(t + 1)$, the defender adjusts the estimated parameter $\hat{\omega}_{(t+1)}$ derived by the Kalman Filter (KF) by multiplying it with the inverse of the predicted attacker action, $1/\chi_{(t)}^-$, resulting in an estimated value of $[1/\chi_{(t)}^-] * \hat{\omega}_{(t+1)}$. This proactive correction aims to counteract the anticipated distortion action by the attacker, ultimately yielding a modified value $\omega_{(t+1)}^*$ at the end of the feedback loop in Figure 4.40:

$$\omega_{(t+1)}^* = \chi_{(t+1)} * [1/\chi_{(t)}^-] * \hat{\omega}_{(t+1)} \quad (4.6)$$

According to equation 4.6, if the defender's predicted value $\chi_{(t)}^-$ closely aligns with the attacker's implemented value $\chi_{(t+1)}$, the feedback loop within the control system would yield an estimated value $\omega_{(t+1)}^*$. This estimated value, despite the attacker's distortion, closely approximates the actual value $\hat{\omega}_{(t+1)}$. Achieving this alignment allows the defender to ensure the correct operation of the Cyber-Physical System (CPS) even under cyber attack conditions, effectively nullifying the impact of the attack. Subsequently, we delve into experimental details aimed at nullifying specific attack modes, such as the current drainage attack, along with the associated challenges, including the attack's initiation impulse and withdrawal syndrome.

4.6.7 Experimental Results of Defensive Actions

Presented here are the results of simulation of the defense operation employing linear-dynamic based predictor. As shown in Figure 4.40, the predictor took as inputs two values of the estimated angular speed - one, $\hat{\omega}$ coming as immediate output from the KF, i.e. the beginning of the feedback loop, and another one, ω^* at the entry to the comparator, i.e. at the very end of the same feedback loop. If the attack starts at time $t = t_{(s)}$, then the attacker injects distortion coefficient $\chi_{(s)}$ at that moment and consequently builds up a time series of distortion coefficients for the attack operations at discrete time points $t_{(s+1)}$, $t_{(s+2)}$, $t_{(s+3)}$, ..., $t_{(s+k)}$, represented by values $\chi_{(s+1)}$, $\chi_{(s+2)}$, $\chi_{(s+3)}$, ..., $\chi_{(s+k)}$. Assumption of full transparency of the attack for the defender allows the predicting module of Figure 4.40 to derive the time series for $\chi_{(m)}^-$ employing the following linear-dynamic difference equation:

$$\chi_{(m)}^- = \chi_{(m)} + \frac{\chi_{(m-2)} - \chi_{(m-1)}}{t_{(m-2)} - t_{(m-1)}} \cdot [t_{(m)} - t_{(m-1)}] \quad (4.7)$$

where $m = 2, 3, 4, \dots$

In the conducted simulation experiments, the process of predicting χ^- values was performed using a linear-dynamic difference equation (4.7)-based predictor, as illustrated within the architecture depicted in Figure 4.40. This prediction was based on the engagement of the attack using the saw function detailed in Figure 4.42. Notably, the transition of points A and B from Figure 4.42 to the corresponding points A^- and B^- was achieved through the implementation of vertical red-dashed projection lines, enabling the establishment of their relationship within the analysis. The performance of the resulting defense scheme is presented below.

4.6.8 Current Drainage Negation

In the illustration of Figure 4.46, the scenario depicts the negation of a current drainage attack utilizing a linear-dynamic predictor within the architecture of Figure 4.40. The attacker's strategy

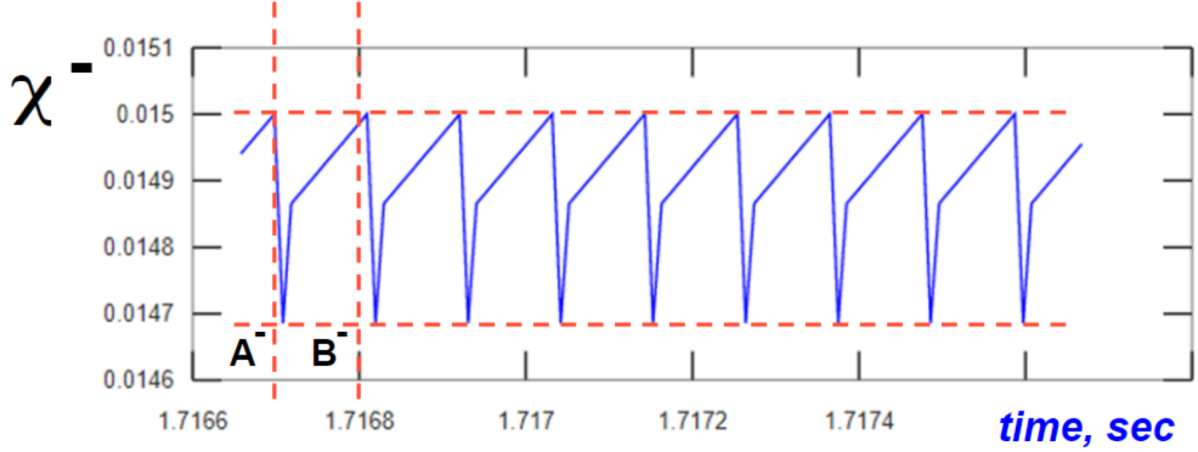


Figure 4.45: Predicting values of χ^- with the linear-dynamic difference equation (4.7) based predictor within the architecture of Figure 4.40 and the attack engaging saw function from Figure 4.42. Points A and B of Figure 4.42 are projected to points A^- and B^- herewith following vertical red-dashed projection lines starting from Figure 4.42 and ending herewith.

involves employing a shallow saw function from Figure 4.42, while the defender anticipates this action, as showcased in Figure 4.45. Notably, the visualization reveals the presence of an initial spike, highlighting a potential issue in the defense against such an attack.

The attack starts at $t = 1.5$ seconds and ends at $t = 2$ seconds. The defense module is turned on, effectively negating the attack except the remaining spike at $t=1.5$ sec, which is to be considered in the next subsection.

4.6.9 Start Impulse Issue

The initial impulse issue arises due to the unpredictability of the attack's commencement. The attack often occurs unexpectedly, and the predictor circuits depicted in Figure 4.40 lack the capability to anticipate this precise moment. The Figure 4.47 exhibits a critical phase during the initial stage (at $t = 1.5$ seconds) of neutralizing the current drainage attack using a linear-dynamic predictor within the architecture detailed in Figure 4.40. Employing a shallow saw function illustrated in Figure 4.42, the attacker instigates the attack, prompting the defender to anticipate and effectively counteract it, as demonstrated in Figure 4.45. This specific snapshot highlights the emergence of an initial spike issue in windings 'a' and 'c' for both current and voltage, warranting closer inspection and consideration in the defense strategy. Addressing the initial spike issue involves implementing a direct solution to prevent the defense module from excessively reacting to abrupt changes in the system state induced by the attack. In our scenario, this overreaction results in the generation of spikes, which pose a greater risk to the circuits than the attack itself. By introducing algorithmic restrictions, we can confine the defense system's

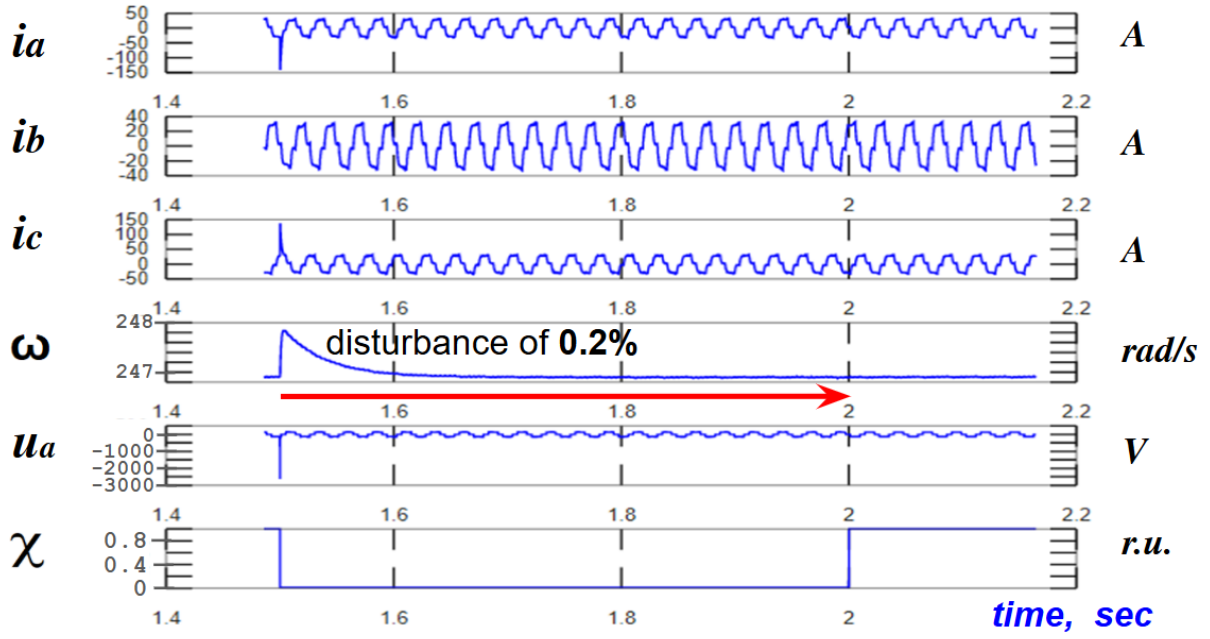


Figure 4.46: Negation of the current drainage attack at time window $t=[1.5; 2]$ seconds with linear-dynamic predictor in architecture of Figure 4.40. The attacker employs deeply diving but shallow modulation height saw function from Figure 4.42. The defender counteracts by anticipating it as that shown in Figure 4.45. The residual disturbance of the angular speed ω calculated as the area above its steady state value $\omega_{steady}=249$ rad/s is ca. 0.2% of area under otherwise undisturbed $\omega = \omega_{steady}$ within the disturbance window. The issue of initial spike at $t = 1.5$ seconds is seen.

response within safe bounds for the circuits. This limitation aims to mitigate the negative impact caused by the defense system's excessive response.

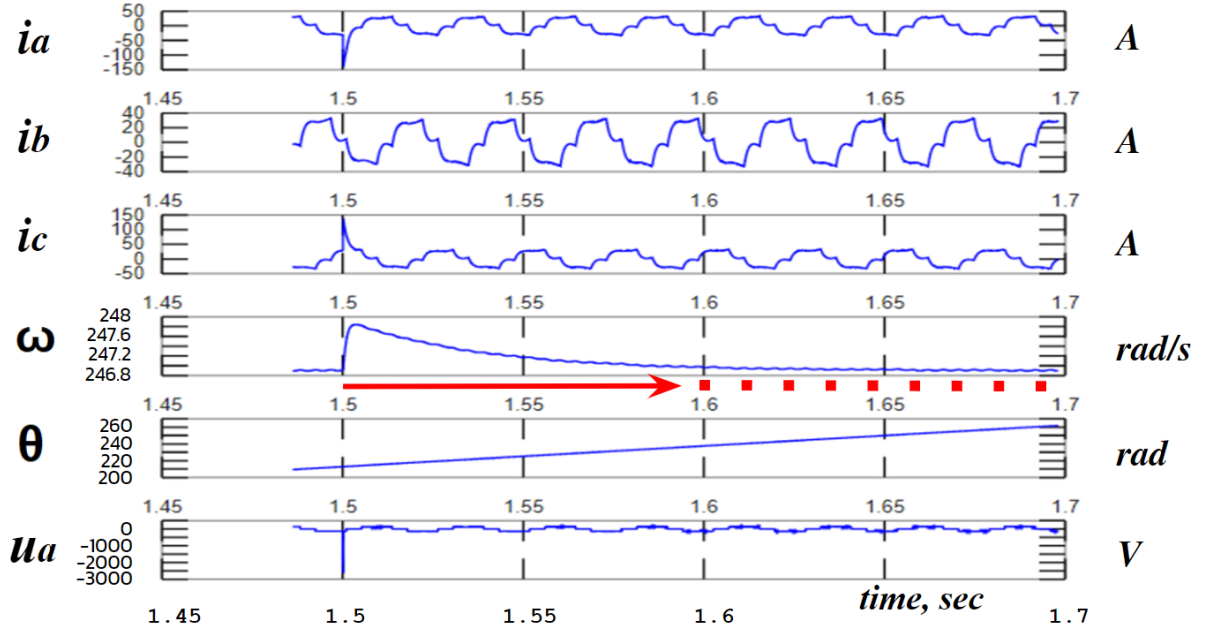


Figure 4.47: Enlarged view of the initial spike observed at time point $t = 1.5$ seconds during the negation of the current drainage attack. This negation strategy is implemented using a linear-dynamic predictor within the architecture illustrated in Figure 4.40. The attacker employs a shallow saw function detailed in Figure 4.42, while the defender anticipates and counters it, as demonstrated in Figure 4.45. Notably, the issue of the initial spike at $t = 1.5$ seconds is evident in windings 'a' and 'c' for both current and voltage ('b' was idle on this cycle).

Conversely, in the absence of the defense module, the attack termination led to the manifestation of attack withdrawal syndrome symptoms, as depicted earlier (refer to Figure 4.44). However, with the inclusion of the linear-dynamic predictor defense circuits depicted in Figure 4.40, a notably smoother withdrawal was observed, as elaborated in the subsequent analysis.

4.6.10 Attack Withdrawal Syndrome Negation

The linear-dynamic predictor module demonstrates not only efficient suppression of the current drainage attack, but as a matter of consequence facilitates a smooth transition through the attack's conclusion at the $t = 2$ seconds mark as depicted in Figure 4.48. This success can be attributed to the prevention of destructive energy accumulation within the system, a factor which we've identified as a leading cause of attack withdrawal syndrome due to the release of accumulated energy upon attack termination.

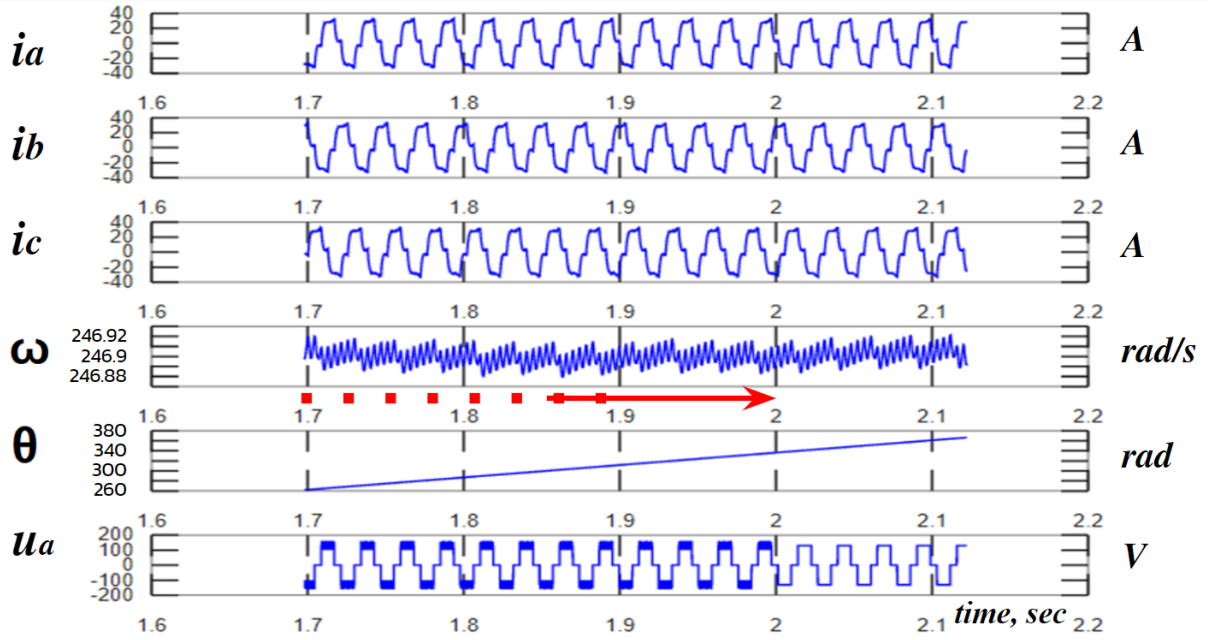


Figure 4.48: Negation of attack withdrawal syndrome by linear-dynamic predictor circuit on defense module. The attack ends at $t = 2$ seconds point.

4.6.11 Induced Pulsation Negation

The linear predictor-based defender demonstrates high efficiency in suppressing induced pulsation attacks. This capability is illustrated in Figure 4.49 for the *Extended Pulsations Attack* mode, where the attack duration is extended to allow for the emergence of hyper-spikes under specific resonance conditions.

Two critical features are observed: first, the induced pulsations are effectively suppressed; second, the hyper-spikes persist and bypass the defense mechanism. This highlights the dual nature of the linear predictor-based architecture. While it successfully mitigates standard Induced Pulsation Attacks, even in their extended forms, it exhibits a fundamental limitation in protecting against hyper-spikes. Consequently, an adversary can achieve attack success by tuning into the hyper-spiking mode to overcome the linear defense layer and inflict electrical damage.

Notably, the *Attack Withdrawal Syndrome* is also eliminated by the linear defender, validating the robustness of this architecture against post-termination transients. However, as shown in Figure 4.49, hyper-spikes remain a significant threat, appearing in both the current and voltage domains.

Furthermore, the initial starting impulse remains prominently high. As previously discussed, this impulse must be managed through anomaly-preventing hardware circuits, as its predictability remains an analytically intractable task within the current linear framework.

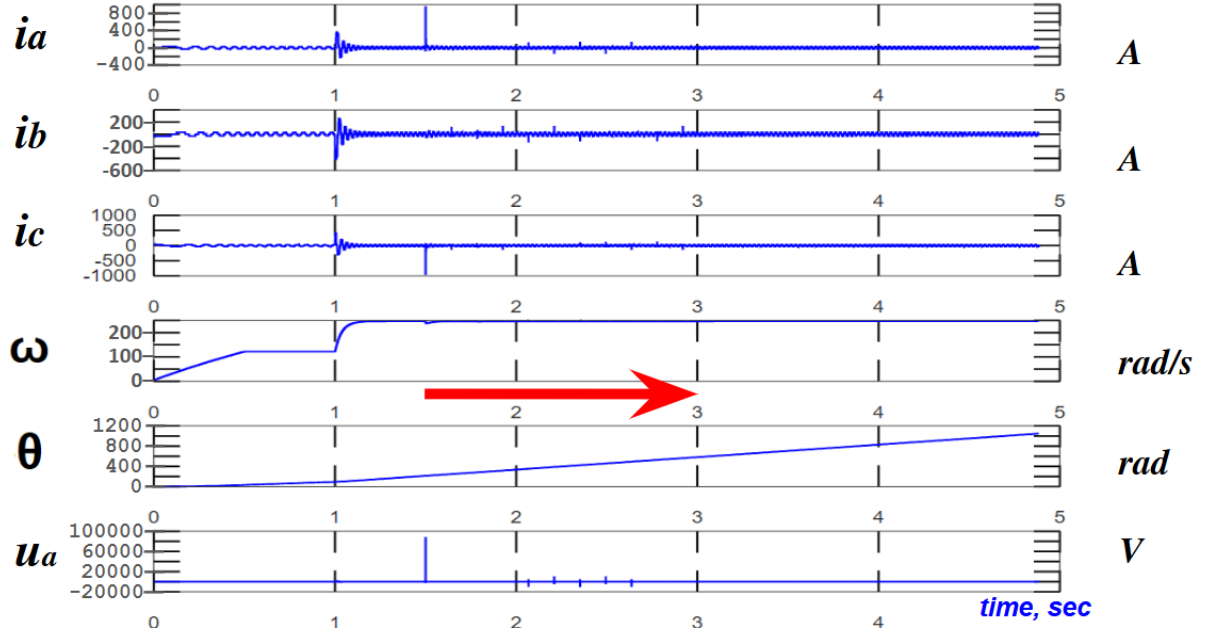


Figure 4.49: Negation of induced pulsations during an Extended Pulsations Attack via a linear-dynamic predictor circuit on the defense module. The adversarial activity occurs between $t = 1.5$ and $t = 3$ seconds.

Quantitative Analysis of Pulsation Negation

A detailed view of the *Induced Pulsations Attack* negation by the linear defender is provided in Figure 4.50, illustrating the quantitative residual impact on the rotor's angular velocity (ω) while the attack is suppressed.

Quantitative Performance Metrics of Pulsation Negation

The efficacy of the linear predictor-based defender is quantitatively evaluated by examining the residual impact of the suppressed *Induced Pulsation Attack* on the rotor's angular velocity (ω). As illustrated in Figure 4.50, the defense module demonstrates high precision in maintaining the control loop's integrity relative to the nominal operating speed of 247 rad/s.

During the initial 0.1 s transient phase of the attack, ω exhibits an initial reduction of 9 rad/s before recovering. This peak deviation constitutes approximately 3.6% ($9 \times 100/247$) of the nominal value. Utilizing the integral area under the time-plot of ω to assess energy displacement, the effective reduction is calculated at 1.8% ($4.5 \times 100/247$). These metrics indicate a defending efficiency exceeding 95% at the critical point of attack entry.

As the system transitions into the steady-state phase of the attack, it reaches an equilibrium characterized by residual ripples with an amplitude of 1.5 rad/s and a period of 0.15 s. In this

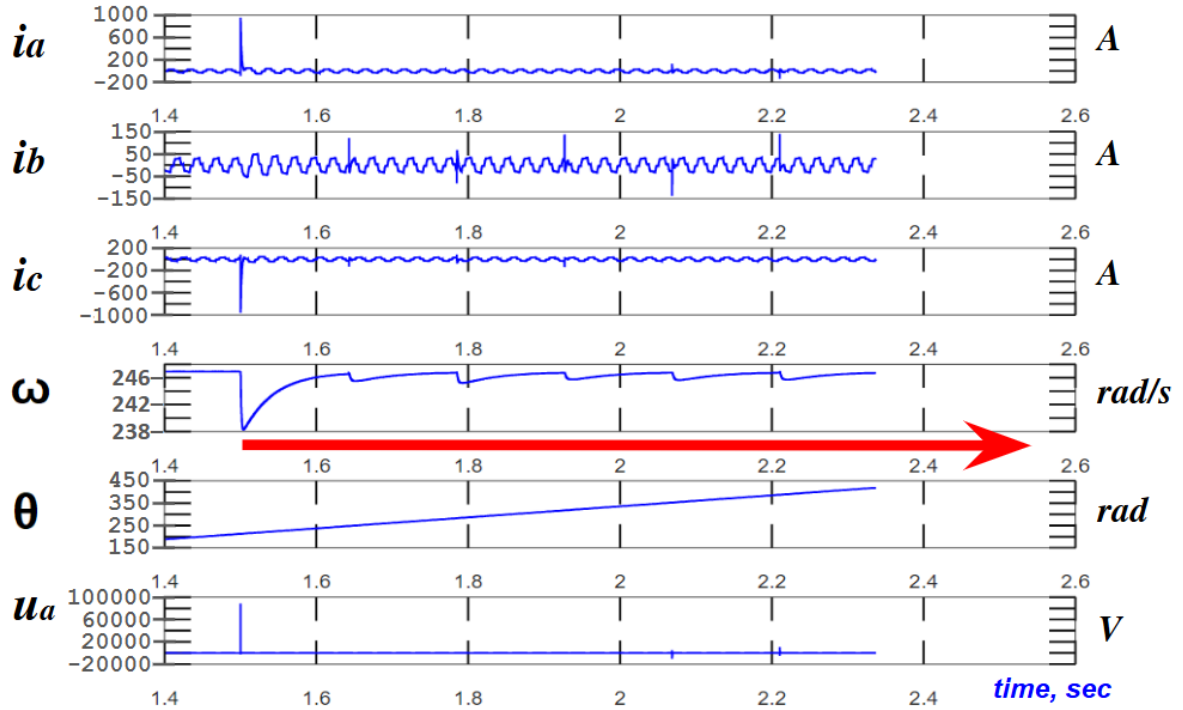


Figure 4.50: Detailed transient response at the onset of induced pulsation negation via the linear-dynamic predictor circuit. The adversarial activity is initiated at the $t = 1.5$ s mark.

regime, the maximum deviation from the designated ω level is restricted to approximately 0.6% ($1.5 \times 100/247$). From an integral perspective, these ripples represent less than 0.3% ($0.75 \times 100/247$) of total system instability. The aforementioned quantitative performance metrics are summarized in Table 4.1.

Table 4.1: Summary of Quantitative Defense Metrics for Pulsation Negation

Phase	Peak Deviation	Integral Instability	Defense Efficiency
Attack Entry (Transient)	3.6%	1.8%	98.2%
Steady-State (Ripples)	0.6%	0.3%	99.7%

Furthermore, the *Attack Withdrawal Syndrome* is observed to be effectively eliminated by the linear defender. This neutralization of post-termination transients is a significant metric of the architecture's robustness, ensuring that the system returns to its nominal state without secondary oscillation or settling-time delays.

4.6.12 Discussion on the Defense Approaches

As part of the discussion, comparing our suggested solution with existing approaches becomes pertinent. Notably, Lanotte et al.'s work (2020, 2022) focused on runtime enforcement for ensuring security in industrial control systems [13, 14]. They introduced a runtime enforcement approach aimed at ensuring compliance with specifications in networks of controllers. The system was rigorously validated through a non-trivial case study involving the domain of industrial water treatment systems. This study entailed injecting various types of malware into controllers, each designed with distinct malicious objectives.

Our contribution aims to broaden the scope of systems covered by runtime enforcement validation, thus augmenting the versatility of this approach. Moreover, integrating this method into high-speed (high-frequency) applications, such as control systems for electrical motors, would significantly elevate the value of the approach pioneered by R. Lanotte et al. (2022).

Additionally, the runtime enforcement methodology holds promise for integration with alternative defense mechanisms. Developing these complementary strategies could further bolster the reliability and effectiveness of collaborative defense architectures.

4.6.13 Summary on Linear Defense Implementation

The proposed defense module architecture demonstrated promising capabilities in effectively neutralizing the current drainage attack targeting the BLDC motor as a cyber-physical control system. Notably, the verified efficacy lies in the linear-dynamic predictor module's ability to anticipate and counter the attacker's malicious actions within the control system's feedback loop based on historical data.

Through the use of modeling and simulation tools, our study has showcased the efficacy of a fundamental predictor module employing linear-dynamic predicting algorithms in providing defense mechanisms against bias injection cyber-attacks aimed at closed-loop-controlled systems, such as Kalman filter-driven brushless DC (BLDC) motors.

The scenario focused on the current drainage attack, conducted with full transparency for the defender, demonstrated the defender's capability to counteract the manipulative tactics employed by the attacker. The attacker's manipulation, altering distortion coefficients that modify angular speed estimates, resulted in a notable increase in motor currents, generating an accumulative effect on the rotor's speed.

Notably, the abrupt termination of the attack induced an intensified increase in currents during the forced braking process, potentially leading to more damaging circuit overloads, a phenomenon identified as the 'attack withdrawal syndrome.' Employing an asymmetric Stackelberg

game and relying on a linear-dynamic predictor, the defender successfully outmaneuvered the attacker. This predictor enabled the defender to proactively counteract the distortion of angular speed estimates.

Our findings demonstrate the defender’s potential to effectively neutralize both the current drainage attack itself and its subsequent impact, including the attack withdrawal syndrome. However, the defender’s inability to preempt the damaging effects of the attack initiation impulse underscores the necessity for a dedicated algorithm equipped with a separate anomaly detector to mitigate its detrimental impact.

For the induced pulsation attack, as well as for its extended version the architecture maintains system stability with a defense efficiency exceeding 98% during the attack’s steady-state phase and over 96% during transient entry. However, the defender’s inherent limitation in preempting the attack initiation impulse underscores the necessity for supplementary hardware-level anomaly detectors. Ultimately, these findings confirm that while linear predictors are highly effective against induced pulsations and withdrawal transients, a comprehensive defense requires a multi-layered, physics-aware approach to mitigate the full spectrum of high-frequency adversarial impulses.

4.6.14 Future Work Extension

Despite its advantages, the Linear Defense is inherently limited by its reliance on a fixed linear model and constant-gain compensation. While this approach is sufficient to mitigate attacks operating within or near the linear region of the plant dynamics, its efficacy significantly degrades when adversaries exploit non-linearities, time-varying parameters, or frequency-hopping injection patterns. Under these circumstances, the predictor may gradually lose synchronization with the true system behavior, thereby enabling the attacker to re-establish resonance or inject undetectable bias. These limitations motivate the necessary extension of the defense architecture toward adaptive and nonlinear domains.

The next subsection therefore introduces the *Nonlinear Defense Strategy*, which generalizes the predictor concept to a nonlinear mapping framework capable of capturing higher-order interactions between state variables. By embedding the linear predictor as its initialization or low-order component, the nonlinear layer inherits the stability and interpretability of the Linear Defense while enhancing resilience against complex, time-varying, and broadband cyber-attack patterns. Together, these two defense stages form a hierarchical protective architecture in which the Linear Defense acts as the fast-response stabilizer and the Nonlinear Defense provides deeper adaptive immunity against sophisticated adversarial behaviors.

Chapter 5

Analysis and Discussion

While the preceding chapters analyzed the quantitative outcomes of individual experiments within their respective contexts, the accumulation and variety of the experimental data now necessitate a broader, more integrated analysis. This chapter moves beyond isolated findings to synthesize the results from a higher level of integration, assessing their collective significance for the design and security of cyber-physical systems. Specifically, the discussion interprets the empirical evidence concerning the BLDC motor's vulnerabilities and defense mechanisms through the strategic lenses of Game Theory and comparative robustness thereby establishing the practical and theoretical implications of this research.

5.1 Summary of Key Experimental Results

This section provides a synthesis of the key quantitative findings derived from the cyber-physical simulations focusing on the BLDC motor control system. The experiments were specifically designed to empirically validate the security hypotheses regarding the integration of IoT communication lines, which simultaneously introduce connectivity advantages and create pathways for adversarial intervention. As detailed below, the major result of this analysis is the identification of new vulnerabilities within the motor's critical feedback loop to bias injection attacks, achieved under the realistic assumption of the adversary's full control over data flow via communication lines or AI worm deployment. This summary establishes the foundation for the subsequent Game Theory and comparative robustness discussions by detailing the specific performance impacts of these cyber-physical compromises.

5.1.1 The Strategic Dual Nature of Initial Probing Attacks

Initial probing bias injections in the cyber-physical system (CPS) possess a critical dual nature: they function as both reconnaissance acts and system vulnerability confirmation mechanisms. This understanding is vital for accurately modeling the attacker's utility in the subsequent Game Theory analysis.

The attacker's actions are often not immediately aimed at causing catastrophic damage but rather at maximizing information gain before a full-scale assault. The primary goals during this phase include:

1. **System Identification and Response Confirmation:** Probing injections are used to characterize the system's dynamic response (transfer function, latency, and response to anomaly). Observing whether the controller output (e.g., motor command) smoothly follows the manipulation provides vital confirmation that the system is susceptible.
2. **Filter/Detector Resilience Test:** The injections test the system's defensive mechanisms. If small biases are assimilated without triggering protective measures, the attacker confirms the viability of the targeted feedback channel as a long-term vector for full-scale False Data Injection (FDI) attacks.

Conversely, the success of the probing attack confirms the viability of a full-scale assault. The moment the system's response indicates it is following the manipulation, the attacker has validated a core weakness and can escalate the attack by increasing the bias magnitude or frequency, thus conserving their resources and effort.

This dual nature has critical implications for the defender's optimal strategy, requiring a defense that focuses on disrupting the attacker's learning phase by maximizing the cost and uncertainty associated with initial reconnaissance attempts.

5.1.2 The Identified Attacks Variations

The first major finding of the experimental analysis is the identification of the Current Drainage Attack as a viable option for a full adversarial assault on the BLDC motor control system. This attack is realized through a targeted bias injection, represented by the difference $\delta\chi = \chi_{top} - \chi_{bottom}$. Crucially, the effectiveness of this assault can be finely tuned by the adversary across a wide operational range via the following key parameters: the amplitude of the implemented $\delta\chi$, the modulation frequency for χ , and the shape of the χ -function. For instance, the specific form of the attack can be customized by selecting the shape of the triangles in a sawtooth-like function used to represent χ .

Limitations of Conventional Sensory Identification

While the Current Drainage Attack is fundamentally identifiable by its effects on the system state variables, relying solely on regular sensory hardware and straightforward signature analysis is often insufficient against a sophisticated, tuned adversary. The effectiveness of the attack lies precisely in its ability to evade simple, threshold-based detection by exploiting the system's inherent physical characteristics.

1. **Stealth and Amplitude Tuning:** The adversary can precisely tune the bias injection's amplitude ($\delta\chi$) such that the resulting increase in measured current draw falls within the controller's established tolerance bands or the system's ambient operational noise floor. Conventional anomaly detectors are designed to ignore such marginal variations, flagging them as benign sensor drift.
2. **Physical Masking and Filtering:** The cyber-physical nature of the system—specifically the motor's large inertia and electrical time constants—acts as a natural low-pass filter. This physically masks the sharp transitions of the injected bias function, smoothing the attack signature before it reaches the sensory hardware. The straightforward, high-confidence signature is thus lost to the physics of the system.
3. **Need for Contextual Analysis:** Simple sensory hardware only provides raw data. Identifying the Current Drainage Attack with high confidence necessitates an analytical defense that models the expected behavior. Detection requires verifying if the observed current draw is disproportionate to the legitimate torque command issued by the controller, reliably extracting the small, malicious bias from the ambient system noise.

Therefore, the development of advanced analytical defenses, which forms the basis of the comparison in Section 5.1, is motivated by the failure of conventional sensory methods to reliably detect these stealth attacks.

The Stealth Variant: Long-Term Efficiency Degradation

Simulation experiments reveal that the Current Drainage Attack may be implemented in a soft, stealthy form, specifically tuned to deprive the host of efficiency only, rather than inflicting immediate physical damage or triggering high-amplitude alarms. This finding introduces a critical complication for the defense model:

- **Prolonged Manipulation:** By keeping the injected bias ($\delta\chi$) amplitude low and the modulation frequency outside critical detection ranges, the attack signature merges with ambient system noise. This allows the manipulation to be sustained over extended periods.

- **Long-Term Damage:** This stealthy variant becomes a preferred option for a sophisticated attacker, as the resulting long-term efficiency loss (e.g., increased energy consumption, premature wear, reduced operational lifespan) accumulates into significant damage without revealing the adversary's presence.
- **Shifting Defense Goal:** The defender's challenge shifts from detecting a sharp, transient anomaly to identifying a subtle, sustained drift in system performance metrics, necessitating the use of advanced prediction models (as discussed in Section 5.1) that can distinguish small, persistent bias from natural system aging or operational variances.

This potential for enduring, low-impact manipulation fundamentally challenges high-confidence detection systems, underscoring the necessity of robust, adaptive analytical defenses.

The Stealthiest Threat: The Voltage Hopping Attack

Among the identified bias injection attacks, the Voltage Hopping Attack presents the stealthiest and most sophisticated threat. Its design relies on a resonant infiltration technique that enables it to deliberately evade detection by the sensory environment by causing no immediate, measurable effect on major physical state variables.

- **Resonant Evasion Mechanism:** The attack is precisely tuned to operate at frequencies that do not significantly excite the system's dynamics, thus avoiding changes in the motor current (I) and speed (ω). This circumvention of the primary sensing channels renders straightforward detection by conventional sensory hardware ineffective.
- **Control Circuit Target:** The impact of the attack is designed to be directed against the control circuits themselves, inducing voltage jumps within the control system logic.
- **Covert Damage Escalation:** The central trick of this covert manipulation is that the undetected activity causes the control circuits to execute high-voltage jumps. These high-frequency high-amplitude voltage jumps pose a significant and direct risk of damaging the control circuits, representing a highly impactful, non-kinetic form of physical damage over time.

The Voltage Hopping Attack thus provides a compelling motivation for the development of adaptive analytical defenses that monitor control signals and internal model consistency, rather than solely relying on physical feedback data.

The Destructive Class: Pulsation Attacks

In stark contrast to the stealthy, low-amplitude manipulations, the Pulsation Attacks represent the least covert but most comprehensively damaging adversarial actions. This class of attacks engages resonance phenomena with the rotating rotor to induce severe electrical and mechanical pulsations throughout the system.

- **High Visibility, High Impact:** Pulsation Attacks abandon stealth for impact, generating large, easily identifiable signatures in the state variables. However, their high-amplitude nature means detection, while simple, may be too late to prevent damage.
- **Induced Pulsations Attack (IPA):** Within this class, the IPA is designed to be highly destructive. It actively self-shakens the motor, both electrically and mechanically, via carefully tuned injections that align with the system's resonant frequencies.
- **Goal of Destruction:** The primary objective of the IPA is to rapidly find the weakest link in the system (e.g., motor bearings, winding insulation, power electronics) and escalate the stress to reach a destructive stage. This represents the ultimate outcome in the attacker's utility function for immediate system incapacitation.

The existence of Pulsation Attacks underscores the necessity for defenses that offer both high-precision, low-magnitude detection (for stealth attacks) and extremely rapid, failsafe countermeasures (for destructive attacks like the IPA).

The Extended Pulsations Attack (EPA)

An escalation of the Induced Pulsations Attack (IPA) is the Extended Pulsations Attack (EPA), where the attack is sustained over a prolonged duration. This variant shifts the adversarial goal from immediate, transient destruction to accumulating damage in the fastest attainable way through persistent system stress.

- **Sustained Resonance:** Unlike the standard IPA, the EPA maintains the resonant excitation as long as the adversary is able (or until the defender intervenes). This ensures continuous engagement with the system's destructive frequencies.
- **Accumulated Stress:** The persistence of the attack is defined by the lasting sequence of high-amplitude mechanical ripples in the rotating rotor, accompanied by continuous current and voltage pulsations. This sustained energy transfer accelerates material fatigue, rapidly degrading mechanical components (e.g., bearings and shafts) and stressing electrical insulation.

- **Guaranteed Failure:** The EPA represents a strategy designed to ensure a high-confidence, long-term failure of the cyber-physical system, even if the initial pulsation does not immediately lead to a breakdown. The accumulation of stress guarantees a reduced operational life and an eventual catastrophic system failure.

The EPA necessitates the implementation of autonomous, immediate countermeasures that can detect and shut down large-amplitude oscillations within minimal tolerance time to mitigate the rapid accumulation of irreversible damage.

The Ultimate Threat: Resonance-Tuning Hyper-spiking Attack

The ultimate threat achievable within this attack class is the Hyper-spiking Attack, which serves as a resonant tuning twin to the Extended Pulsations Attack (EPA). This attack exploits non-linear electromagnetic interactions to achieve a rapid, amplified electrical danger that surpasses the damage potential of standard pulsations.

- **Resonant Escalation Mechanism:** The Hyper-spiking Attack relies on the attacker's ability to fine-tune the modulation frequency of χ within the framework of the EPA. This fine-tuning achieves a specific resonant interaction in the electromagnetic domain.
- **Periodically Occurring Hyper-spikes:** The result is the generation of voltage spikes that are regular, periodically occurring, and significantly higher in amplitude than the baseline pulsations.
- **Amplified Electrical Danger:** These hyper-spikes represent the most effective way for the adversary to induce an immediate and amplified electrical breakdown risk. They impose a critical danger to the circuit insulation and power electronics, providing a pathway to system incapacitation when the initial Pulsation Attack, even its Extended version, failed to meet the goal of rapid destruction.

The existence of the Hyper-spiking Attack underscores the necessity for defenses to not only damp low-frequency oscillations but also to maintain extremely tight control over the system's susceptibility to highly tuned, high-energy resonant events.

5.1.3 The Strategic Edge of Unpredictability

One of the strongest strategic advantages an adversary may exercise is unpredictability in timing and action. If the steps of the attacker are predictable, the defender is empowered to preemptively

take defensive measures and neutralize threats. However, the attacker maintains the intrinsic advantage of the first move, which can occur unexpectedly. The timing of critical adversarial acts—such as the beginning or interruption of the attack, or switching attacking mode—is always the prerogative of the attacker, providing a decisive edge.

Among the specific findings of this research, the impact of unpredictability is most notable in two phenomena:

1. **Initial Spike at the Beginning of the Current Drainage Attack:** The commencement of the Current Drainage Attack involves an abrupt, unexpected change in the distortion parameter χ . As observed in our simulations, this abrupt change most certainly produces an initial electrical spike in voltage. This spike poses an immediate danger to the operating circuits and must be addressed with hardware elements designed to block unexpectedly high changes in system parameters, as prevention may not be feasible due to the unpredictable timing.
2. **Attack Withdrawal Syndrome (AWS):** This effect poses a significant danger if, during the attack, kinematic energy was strongly accumulated (via persistent acceleration) or strongly dissipated (via triggered deceleration) by the rotor. In such cases, the unexpected interruption of the attack—the withdrawal—may have an effect stronger than the attack itself due to the abrupt release or reversal of the accumulated energy, as shown in our simulations.

In facing even formidable defenses, the attacker may always count on the possibility of surprising the defender with either the unexpected beginning of an attack or its unexpected, abrupt interruption. Our simulated experiments suggest that exploiting these moments of unpredictability can deliver the desired outcome for the attacker, even against highly robust defense mechanisms.

5.1.4 The First Line of Defense: Reverse Feedback with Linear Extrapolator

The research proposes a fundamental defense mechanism implemented as a reverse feedback loop designed to neutralize expected adversarial bias injections preemptively. The core component of this defense is a predictor designated to estimate the probable value of the attacking distortion coefficient, χ^- .

This estimated value is subsequently used for a preemptive modification of the ω values in the feedback loop data-stream. The objective is to cancel out the expected malicious modification to be introduced by the attacker in the coming sampling cycle.

- **Tactical Robustness through Simplicity:** Unlike more sophisticated adaptive and non-linear predictors, the linear predictor does not require any prior training and relies solely on the most recent set of data points. This characteristic offers strong robustness against unpredictable changes in the attacker's tactical moves, avoiding the instability often inherent in models relying on longer historical data or complex training.
- **Predictor Design:** The most straightforward technical solution for the predictor is implemented for this purpose: a linear extrapolator of the first order.
- **Demonstrated Efficiency:** Despite its simplicity, the linear extrapolator demonstrated notable efficiency against the Current Drainage Attack, particularly in scenarios involving deeply set and small modulation height sawtooth function attacking waves.
- **Mitigation of AWS:** Of particular importance is its demonstrated ability to negate the Attack Withdrawal Syndrome (AWS) for the implemented set of parameters. By maintaining a coherent model during the abrupt interruption, the predictor prevents the destabilizing energy release observed in the undefended system.

Because of this demonstrated effectiveness against stealthy, prevalent attacks and its ability to mitigate the dangerous AWS phenomenon, this solution may be considered to be an essential first line of defense against bias injection attacks within the cyber-physical control system.

5.1.5 The Second Line of Defense: Adaptive Predictors for Resonance Attacks

While the linear extrapolator provides strong initial robustness, more advanced predictor solutions involving adaptivity features are necessary to effectively fight off the highly sophisticated, resonant types of attacks (e.g., the Hyper-spiking Attack, Section 5.1.2). These advanced defenses are therefore strategically planned for the second line of defense.

- **Design Requirements:** Due to the high-speed environment of the cyber-physical system, efficiency requires these advanced predictors to utilize a combination of on-the-fly training and pre-trained modules with dedicated attack signature recognition features.
- **Priorities Shift:** For this second line, the highest priority shifts from general robustness to adaptivity and the ability to predict and model resonance-involving attack patterns over multiple sampling cycles.

- **Future Work Direction:** These complex solutions, with their inherent computational overhead and training requirements, constitute a clear and significant direction for future work developments, extending the scope of the defense beyond the initial protection offered by the linear predictor.

This tiered defensive approach ensures the host system is protected against common, easily implemented threats immediately, while reserving resource-intensive, adaptive countermeasures for the most sophisticated and damaging resonant attacks.

5.1.6 Game-Theoretic Applicability in Attacker–Defender Interaction

The interaction between the attacker and defender can be interpreted as a dynamic non-cooperative game. Each participant seeks to optimize a competing objective: the attacker aims to maximize system degradation while minimizing detectability and energy cost, whereas the defender aims to minimize degradation under resource and latency constraints.

The attacker–defender exchange may be modeled as a repeated game in which each side adapts its strategy in response to observed outcomes. Under this formulation, cyber-physical engagement evolves toward equilibrium points analogous to Nash equilibria, where neither party can unilaterally improve its payoff. Distinct attack regimes—Induced, Extended, and Hyper-spiking—correspond to different strategic zones ranging from stealth probing to aggressive exploitation.

The defender’s strategies include static linear control, adaptive estimation, and predictive or nonlinear countermeasures. Their effectiveness and resource expenditure define the payoff structure. A Stackelberg interpretation can further describe sequential adaptation, where the attacker acts as a leader probing the system response and the defender reacts to minimize subsequent exposure. This formulation provides a theoretical framework to analyze strategic escalation and defensive learning.

5.1.7 Asymmetric Stackelberg Game Interpretation

The interaction between the attacker and the linear predictor-based defender can be formally interpreted as an *asymmetric Stackelberg game*. In the general sense, a Stackelberg game represents a hierarchical optimization process involving two agents — a leader and a follower — whose objectives are mutually dependent but conflicting. The leader commits to a strategy first, while the follower reacts optimally to this decision within its own feasible space. This framework is particularly well suited to describe cyber–physical conflicts, in which one participant initiates

an adversarial action that the other must counteract dynamically under limited information and temporal constraints.

Asymmetry of Information and Capabilities. The term *asymmetric* in this context denotes the unequal access to system information and the imbalance of control authority between the two parties. The attacker, having the ability to manipulate the estimation channel, operates with direct knowledge of the injected bias or distortion signal. In contrast, the defender has access only to corrupted feedback data and thus must infer the attack indirectly. This asymmetry creates a natural hierarchical structure in which the attacker acts as the leader, choosing the manipulation strategy that maximizes disruption, while the defender acts as the follower, adapting its response through predictive estimation and compensation. The defender's objective, therefore, is to minimize deviation from the nominal system trajectory by counteracting the attack's effects before they propagate through the closed-loop dynamics.

Leadership and Follower Dynamics. In the described scenario, the attacker can be regarded as the *Stackelberg leader*, selecting its bias injection profile in advance or in real time to exploit the system's response characteristics. The defender, modeled as the *Stackelberg follower*, observes the outcomes of this manipulation and adjusts its predictive model accordingly. However, the linear-dynamic predictor introduces an additional nuance: it embeds an internal forward model that anticipates expected plant behavior, effectively allowing the defender to act in a semi-leader capacity within its own predictive domain. Hence, the hierarchy is twofold: the attacker leads in the disturbance space, while the defender partially leads in the prediction space. This layered relationship results in a dynamic interplay between manipulation and compensation, where both participants continuously adapt their strategies under constrained observability.

Defensive Mechanism as Predictive Compensation. The defender's linear predictor serves as a proactive mechanism to mitigate the impact of bias injection. Instead of reacting to measured deviations, the predictor estimates the nominal trajectory of the controlled variable (e.g., rotor angular speed) and adjusts the feedback control signal accordingly. In this manner, it neutralizes the attacker's manipulation before it manifests as a significant physical deviation in the plant. This predictive compensation transforms the defensive response into a model-based dynamic optimization problem: the defender seeks to minimize the expected deviation given the modeled statistics or patterns of the attacker's distortions. Consequently, the Stackelberg structure becomes an analytical framework for quantifying the efficiency and stability margins of the Linear Defense strategy.

Illustrative Dynamics of Attack–Defense Interaction. Simulation results presented earlier in this work demonstrate the sequence of actions that characterize the asymmetric Stackelberg interaction. The attacker initiates the game by injecting a bias into the angular speed estimation loop, thereby triggering an abnormal growth of motor currents and mechanical acceleration. When the defender’s predictor engages, it generates a compensating control action that suppresses this current growth, restoring stable operation despite the ongoing manipulation. Upon abrupt withdrawal of the attack — the so-called *attack withdrawal syndrome* — the predictor continues to stabilize the system by absorbing the transient overshoot in current, effectively mitigating the induced stress on power circuits. This closed-loop behavior confirms that the defender’s linear-dynamic strategy functions as a predictive follower, dynamically neutralizing the leader’s manipulative actions in real time.

Asymmetric Stackelberg Game: formal measures and win/lose criteria

To make the Stackelberg interpretation operational and measurable, we now introduce a compact mathematical description of the attacker–defender interaction, define scalar and functional measures of attack severity and defensive performance, and state formal win/lose criteria used in our analysis.

Compact dynamic model. Let the (discretized) physical plant state be $\mathbf{x}(k) \in \mathbb{R}^n$, with the nominal (no-attack) input $\mathbf{u}(k)$ and measured current $i_{\text{meas}}(k)$. The attacker injects a distortion sequence $\chi(k)$ into the estimation/measurement channel (for instance, biasing the angular-speed estimate), which—through the controller—produces an effective disturbance torque/voltage acting on the plant. For compactness we write the plant dynamics as

$$\mathbf{x}(k+1) = \mathbf{A}_p \mathbf{x}(k) + \mathbf{B}_p (\mathbf{u}(k) + \mathbf{u}_{\text{att}}(k)), \quad (5.1)$$

where $\mathbf{u}_{\text{att}}(k) = \mathcal{T}\{\chi(k)\}$ denotes the attack-induced input (a known linear mapping $\mathcal{T}$ may be used in the linearized model). The predictor (defender) runs in parallel:

$$\hat{\mathbf{x}}(k+1) = \mathbf{A}_L \hat{\mathbf{x}}(k) + \mathbf{B}_L \mathbf{u}(k). \quad (5.2)$$

Define the predicted current $i_{\text{pred}}(k) = \mathcal{C} \hat{\mathbf{x}}(k)$ and the residual

$$\Delta i(k) = i_{\text{meas}}(k) - i_{\text{pred}}(k). \quad (5.3)$$

The defender issues a corrective action (linear compensator)

$$u_{\text{def}}(k) = -K_D \Delta i(k), \quad (5.4)$$

which augments the nominal control input (i.e., $\mathbf{u}(k) \leftarrow \mathbf{u}(k) + u_{\text{def}}(k)$). Combining (5.1)–(5.4) yields a closed-loop input/output relation mapping the attack sequence $\{\chi(k)\}$ into the measurable residual $\{\Delta i(k)\}$ and into the plant current sequence $\{i_{\text{meas}}(k)\}$.

In the z -domain (or using the LTI-input assumption on the linearized model) this mapping can be compactly written as

$$\Delta I(z) = H_{\Delta}(z; K_D) \Delta(z), \quad I_{\text{meas}}(z) = H_I(z; K_D) \Delta(z) + H_u(z) U(z), \quad (5.5)$$

where H_{Δ} and H_I are transfer functions that depend explicitly on the defense gain K_D as well as on the plant and predictor matrices. These transfer functions are the primary object linking attacker actions to observable quantities.

Performance and damage measures. We adopt the following measures to quantify attack severity and defensive success.

- **Residual energy** (diagnostic measure)

$$E_{\Delta}(\chi) = \sum_{k=0}^T (\Delta i(k))^2 = \|\Delta i\|_2^2 \quad (5.6)$$

accumulated over a monitoring horizon T .

- **Accumulated current stress** (physical damage proxy)

$$E_I(\chi) = \sum_{k=0}^T (i_{\text{meas}}(k))^2 = \|i_{\text{meas}}\|_2^2. \quad (5.7)$$

- **Peak current** (overload indicator)

$$I_{\text{max}}(\chi) = \max_{0 \leq k \leq T} |i_{\text{meas}}(k)|. \quad (5.8)$$

- **Detection time** (time-to-detection)

$$T_{\text{det}}(\chi) = \min \{k : |\Delta i(k)| > \eta(k)\}, \quad (5.9)$$

where $\eta(k)$ is the (possibly time-varying) detection threshold.

All measures are implicitly functions of the attack sequence χ and of the chosen defense gain K_D via the closed-loop mapping (5.5).

Win / lose criteria. We define practical win/lose conditions that map physical and diagnostic measures into binary outcomes (see Figure 5.1).

Interpretation of Payoff Comparison. In the context of the Stackelberg bias–compensation game, let the attacker’s payoff under different defender responses be denoted by $U_A(\rho_1)$ and $U_A(\rho_2)$, where ρ_1 and ρ_2 represent two alternative defensive strategies. If

$$U_A(\rho_1) < U_A(\rho_2),$$

this inequality indicates that the attacker’s utility is lower when the defender employs strategy ρ_1 . Consequently, ρ_1 is considered a more effective defense, as it reduces the attacker’s success and thus minimizes the expected system loss. Formally, the defender seeks to minimize the attacker’s utility, expressed as

$$\rho^* = \arg \min_{\rho} U_A(\rho),$$

which is equivalent to maximizing the defender’s own payoff $U_D = -U_A$. Therefore, when $U_A(\rho_1) < U_A(\rho_2)$, it follows that $U_D(\rho_1) > U_D(\rho_2)$, signifying that the defender “wins” under ρ_1 by achieving a higher utility and more effective compensation of the injected bias.

- **Defender wins** if over the monitoring window:

$$E_I(\chi) \leq E_I^{(\text{th})}, \quad I_{\max}(\chi) \leq I_{\text{safe}}, \quad T_{\text{det}}(\chi) \leq T_{\text{allow}}, \quad (5.10)$$

i.e., the accumulated stress and peak currents remain below safety thresholds and the attack is detected within an acceptable delay T_{allow} .

- **Attacker wins** if any of the following occurs:

$$E_I(\chi) > E_I^{(\text{th})} \quad \text{or} \quad I_{\max}(\chi) > I_{\text{safe}} \quad \text{or} \quad T_{\text{det}}(\chi) > T_{\text{allow}}. \quad (5.11)$$

In particular, causing an overload ($I_{\max} > I_{\text{safe}}$) or producing large accumulated energy that can damage circuits are considered successful attacks.

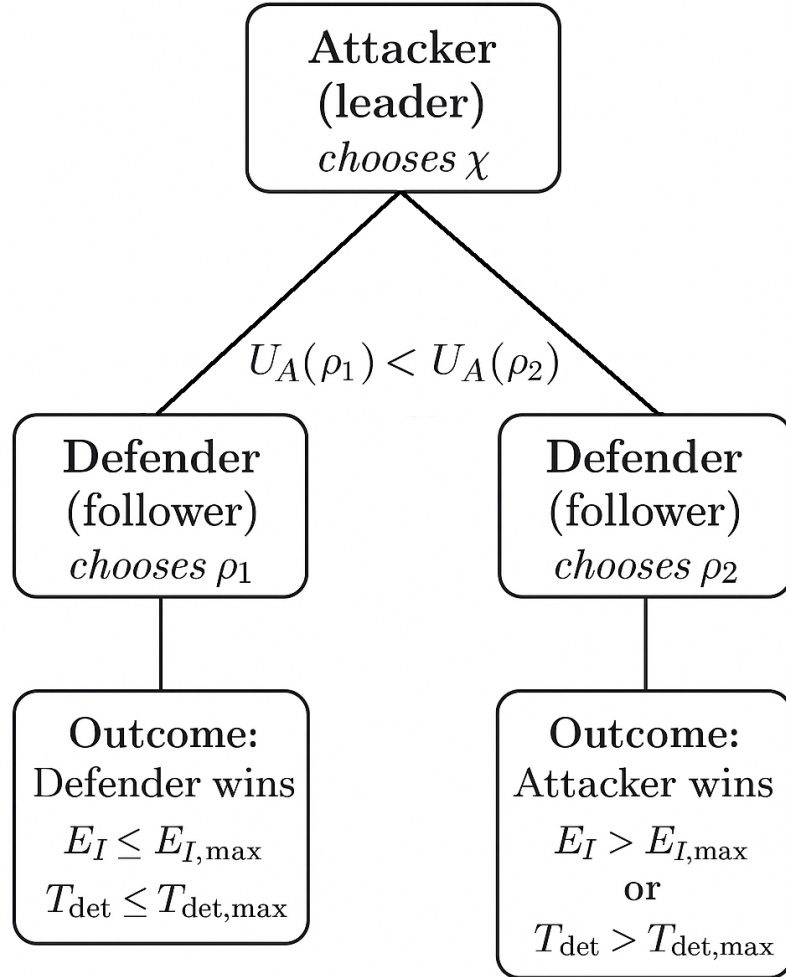


Figure 5.1: Asymmetric Stackelberg game tree illustrating defender (leader) and attacker (follower) interaction in linear-dynamic prediction defense. Leaf nodes are annotated with mathematical outcome criteria according to (5.10) and (5.11).

An additional specialized metric captures the *attack withdrawal syndrome*:

$$O_{\text{withdraw}}(\chi) = \max_{k \in [\tau_w, \tau_w + \Delta]} |i_{\text{meas}}(k)| - \max_{k < \tau_w} |i_{\text{meas}}(k)|, \quad (5.12)$$

where τ_w denotes attack termination time and Δ a short post-withdrawal window. If $O_{\text{withdraw}}(\chi) > O_{\text{th}}$, the withdrawal syndrome is considered damaging.

Temporal Leadership Structure in Discrete-Time Stackelberg Game

In the implemented cyber-physical defense framework, the interaction between the attacker and the defender unfolds in discrete time, constrained by the system's sampling rate. Each round of interaction corresponds to one sampling interval k , during which the attacker injects bias and the defender updates its compensatory strategy in the next cycle. This inherently defines a temporal asymmetry that determines leadership roles within the Stackelberg formulation.

Sequential decision flow. At each sampling round k :

1. The *attacker* selects and applies a bias distortion $\chi(k)$ to the system state or measurement channel.
2. The *defender* observes or estimates the resulting deviation, computes the compensatory response $\rho(k)$, and applies it in the following round $k + 1$.

At round $k + 1$, the new attack $\chi(k + 1)$ interacts multiplicatively with the previously prepared defense $\rho(k)$, producing an effective bias compensation term:

$$\chi(k + 1) \times \rho(k) \approx 1,$$

which ideally neutralizes the injected distortion.

Leader–follower interpretation. Since the attacker commits its action $\chi(k)$ before the defender's compensatory strategy $\rho(k)$ becomes active, the attacker possesses the *first-mover advantage* and therefore occupies the role of the Stackelberg *leader*. Conversely, the defender acts as the *follower*, optimizing its response given the prior attack observation:

$$\rho^*(\chi) = \arg \min_{\rho} U_D(\chi, \rho), \quad \chi^* = \arg \max_{\chi} U_A(\chi, \rho^*(\chi)).$$

This dynamic realizes a discrete-time Stackelberg game, where leadership is determined not by computational dominance but by the causal order of information flow within the sampling cycle.

Repeated interaction and predictive adaptation. Because the game repeats across time steps, the overall system constitutes a *repeated Stackelberg game*. Over successive rounds, the defender may exploit statistical or model-based predictions of $\chi(k)$ to preemptively adjust $\rho(k)$, thus gradually diminishing the attacker’s effective leadership advantage. In the limit of perfect prediction, the defender approaches quasi-leadership despite its temporal lag, representing the transition toward the anticipatory and adaptive defense regime .

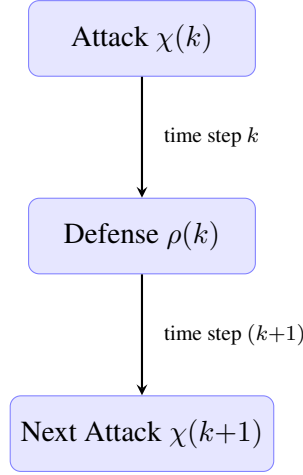


Figure 5.2: Discrete-time sequence of attacker–defender actions illustrating temporal leadership structure.

Stackelberg optimization statement. We formalize the hierarchical game as follows. The attacker (leader) selects an attack sequence χ to maximize its damage utility J_A , while the defender (follower) chooses the defense parameter K_D after observing (or anticipating) χ and seeks to minimize its cost J_D .

Representative utility / cost functions are:

$$J_A(\chi; K_D) = w_1 E_I(\chi; K_D) + w_2 I_{\max}(\chi; K_D) - w_3 g(T_{\det}(\chi; K_D)), \quad (5.13)$$

$$J_D(K_D; \chi) = c_1 E_I(\chi; K_D) + c_2 \|u_{\text{def}}(\cdot)\|_2^2 + c_3 \mathbb{I}\{T_{\det}(\chi; K_D) > T_{\text{allow}}\}, \quad (5.14)$$

where $w_i, c_i > 0$ are weighting coefficients, $g(\cdot)$ is a decreasing function penalizing early detection for the attacker (i.e., attacker prefers longer stealth), and $\mathbb{I}\{\cdot\}$ is the indicator function. Note the explicit dependence of the measures on K_D via the closed-loop mapping (5.5).

The Stackelberg equilibrium (attacker leader) is the solution of the bilevel optimization:

$$\chi^* = \arg \max_{\chi \in \mathcal{D}} J_A(\chi; K_D^*(\chi)), \quad \text{where} \quad K_D^*(\chi) = \arg \min_{K_D \in \mathcal{K}} J_D(K_D; \chi). \quad (5.15)$$

Here $\mathcal{D}$ denotes feasible attack sequences (e.g., energy-limited or amplitude-limited) and $\mathcal{K}$ feasible defense gains (stability-preserving gains).

Analytic bound and sufficient defender condition. Under linearity and for an L_2 attack energy budget $\|\chi\|_2$, relations (5.5) imply

$$\|\Delta i\|_2 \leq \|H_\Delta(\cdot; K_D)\|_2 \|\chi\|_2, \quad (5.16)$$

and similarly

$$\|i_{\text{meas}}\|_2 \leq \|H_I(\cdot; K_D)\|_2 \|\chi\|_2 + \|H_u\|_2 \|u\|_2. \quad (5.17)$$

A *sufficient* (conservative) condition for defender victory is therefore

$$\|\chi\|_2 \leq \min \left\{ \frac{\sqrt{E_I^{(\text{th})}} - \|H_u\|_2 \|u\|_2}{\|H_I(\cdot; K_D)\|_2}, \frac{\eta_{\min}}{\|H_\Delta(\cdot; K_D)\|_2} \right\}, \quad (5.18)$$

where $\eta_{\min}$ is the minimum residual amplitude that must be exceeded for timely detection and $\|H\|_2$ denotes the induced L_2 norm. This inequality shows that improving defender performance reduces the induced norms $\|H_I\|_2, \|H_\Delta\|_2$ (via appropriate choice of K_D), thereby enlarging the set of attack energies that the defender can safely handle.

Interpretation and guidance. The bilevel formulation (5.15) captures the asymmetric nature of the confrontation: the attacker optimizes its sequence with knowledge that the defender will react optimally (within feasible K_D). Important practical consequences follow:

1. *Trade-off for defender.* Increasing K_D typically reduces $\|H_I\|_2$ and $\|H_\Delta\|_2$ (helping satisfy (5.18)) but increases control effort $\|u_{\text{def}}\|_2^2$ and may endanger stability if chosen too large. Thus $K_D^*(\chi)$ in (5.15) reflects a sensitivity–stability trade-off.
2. *Attacker strategy.* The attacker may prefer waveform shapes (e.g., resonant tones, broadband pulses, or stealthy low-energy biases) that maximize J_A while minimizing immediate detection (large $g(T_{\text{det}})$). Frequency-selective attacks that excite modes weakly damped by the given K_D are particularly effective.
3. *Design implication.* From (5.18), reducing the predictor/defense-induced norms (through improved predictor fidelity, adaptive calibration, or multi-rate compensation) directly increases the defender’s tolerance to attack energy. This justifies hierarchical extension to nonlinear/adaptive defenses that shrink these norms across a wider range of operating points.

Concluding remark. The formal Stackelberg formulation thus provides a measurable and actionable framework to compare attacker and defender capabilities, to compute conservative bounds for safe operation, and to guide calibration of K_D and detection thresholds. In simulations reported earlier, the defender succeeds when (5.18) holds for the attack energies used; conversely, attacks that violate these bounds produce overloads or withdrawal overshoots and thereby achieve attacker objectives (cf. criteria (5.10)–(5.11)).

Summary. In summary, the asymmetric Stackelberg game interpretation provides a theoretical foundation for understanding how the linear-dynamic predictor operates as a rational, model-based follower in a hierarchical cyber–physical confrontation. The asymmetry originates from unequal information availability and from the fundamentally different objectives of the two agents: the attacker seeks to maximize deviation or current drain, whereas the defender seeks to minimize it under prediction uncertainty. By formalizing the defense within this game-theoretic framework, the Linear Defense Strategy gains interpretive clarity and mathematical generality, establishing a bridge toward more advanced adaptive and nonlinear defenses .

5.1.8 Applicability of Alternative Game-Theoretic Models

Although the linear-dynamic predictor defense is most naturally formulated as an asymmetric Stackelberg game, the general cyber–physical interaction between attacker and defender can, in principle, be represented within several related game-theoretic frameworks. The choice of the model depends on the timing of decisions, the information available to each player, and the nature of the system dynamics (continuous or discrete). In the present study, the Stackelberg structure remains the most faithful and analytically justified formulation; however, it is instructive to outline potential alternatives for completeness.

1) Stackelberg Game (Baseline Formulation). In the adopted framework, the attacker and defender act sequentially, with one side assigned the role of *leader* and the other as *follower*. The attacker, as the leader, selects the bias distortion χ_k first, attempting to maximize its own payoff U_A , while the defender responds with a compensatory prediction ρ_k to minimize U_D . This ordering reflects the real-world causality of the closed-loop system: the false data are injected first, and the defense predictor subsequently reacts. The discrete-time version of this sequential process is described by

$$\chi_k^* = \arg \max_{\chi_k} U_A(\chi_k, \rho_k^*), \quad \rho_k^* = \arg \min_{\rho_k} U_D(\chi_k, \rho_k), \quad (5.19)$$

where k indexes sampling instants of the control loop. This formulation captures both the informational asymmetry and the causality of attack–response dynamics, making it most appropriate for sampled-data systems such as Kalman filter-driven BLDC motor control.

2) Repeated Stackelberg Game. Since the system evolves discretely with period T_s , the same strategic interaction is replayed at each sampling instant, forming a *finite-horizon repeated game*. This allows the attacker and defender to update their strategies iteratively based on previous outcomes:

$$\rho_{k+1}^* = \mathcal{F}(\rho_k^*, \chi_k), \quad \chi_{k+1}^* = \mathcal{G}(\chi_k^*, \rho_k), \quad (5.20)$$

where $\mathcal{F}(\cdot)$ and $\mathcal{G}(\cdot)$ denote respective adaptive rules. This variant is especially relevant when the predictor incorporates learning or when the attacker attempts to refine its bias over multiple episodes.

3) Nash (Simultaneous-Move) Game. If both sides act within the same sampling step without knowledge of each other’s decisions, the problem degenerates to a simultaneous-move or *Nash* game. Each player selects its strategy assuming the other does the same:

$$\chi_k^*, \rho_k^* = \arg \max_{\chi_k} \arg \min_{\rho_k} \{U_A(\chi_k, \rho_k), U_D(\chi_k, \rho_k)\}. \quad (5.21)$$

Such a scenario may approximate situations where attack and defense algorithms operate on exactly synchronized time scales. However, it loses the hierarchical causality intrinsic to the actual cyber–physical process and thus provides less realistic modeling fidelity for the present system.

4) Bayesian Stackelberg Game. When either side operates with incomplete information about the other—for example, the defender is uncertain about the distribution of the bias amplitude χ_k , or the attacker does not know the predictor gain—the interaction may be cast as a *Bayesian Stackelberg game*. Expected payoffs are then optimized over unknown parameters:

$$\chi_k^* = \arg \max_{\chi_k} \mathbb{E}_\Theta[U_A(\chi_k, \rho_k, \Theta)], \quad \rho_k^* = \arg \min_{\rho_k} \mathbb{E}_\Theta[U_D(\chi_k, \rho_k, \Theta)], \quad (5.22)$$

where Θ represents the random information set. Although this formulation becomes relevant when modeling uncertainty in cyber-attack detection or stochastic sensor noise, it exceeds the deterministic scope of the present linear predictor study.

5) Differential Game (Continuous-Time Limit). In the limiting case of vanishing sampling period ($T_s \rightarrow 0$), the discrete Stackelberg process approaches a *continuous-time differential*

game:

$$\dot{x}(t) = f(x(t), \chi(t), \rho(t)), \quad J_A = \int_0^T U_A(x(t), \chi(t), \rho(t)) dt, \quad (5.23)$$

which is a standard formulation in control-theoretic adversarial modeling. While mathematically elegant, it is not computationally exact for digital control systems where all measurements and actuation are quantized by the sampling rate.

6) Comparative Summary. Table 5.1 summarizes the applicability of different game formulations to the linear-dynamic predictor defense.

Table 5.1: Comparison of Game-Theoretic Models for Cyber-Physical Defense

Game Type	Timing	Information	Domain	Applicability
Stackelberg (Discrete)	Sequential	Full	Discrete-time	Excellent — adopted here.
Repeated Stackelberg	Sequential	Full	Discrete-time	Strong variant allowing adaptation and learning over rounds.
Nash (Simultaneous)	Simultaneous	Full	Discrete-time	Limited realism due to absence of temporal hierarchy.
Bayesian Stackelberg	Sequential	Partial	Discrete-time	Effective for uncertain parameters or incomplete knowledge.
Differential (Continuous)	Sequential / Simultaneous	Full	Continuous-time	Represents a limiting continuous-time case.

7) Conclusion. Because the defense algorithm operates predictively in reaction to bias injections, and because all state and control variables are updated at discrete sampling intervals, the *discrete-time Stackelberg game* provides the most realistic and analytically consistent representation of the attacker-defender interaction. Nevertheless, the same interaction can evolve into repeated or Bayesian variants if adaptive learning or parameter uncertainty are incorporated in future extensions of the model.

5.2 Comparison of Methodologies

Although the attacks and defense strategies developed in this dissertation are validated through the specific lens of BLDC motor control, their significance is best understood when compared qualitatively to the broader landscape of Cyber-Physical System (CPS) security literature.

5.2.1 Static vs. Interactive Dynamics: Evasion Philosophy

Foundational work by Mo and Sinopoli [36] established the theoretical limits of “stealthy” attacks where an adversary adds a constant or slowly drifting bias to sensor measurements. While mathematically robust, these models often treat the system as a discrete-time linear abstraction. In contrast, the Voltage Hopping and Hyper-spiking attacks identified in this research are highly interactive; they exploit the high-frequency switching and phase-tuned resonances inherent in the power electronics.

The foundational framework established by Mo and Sinopoli [36] defines attack stealthiness through the lens of an innovation-based failure detector. In their model, the system is deemed under attack if the residual—the difference between the measured and estimated states—exceeds a statistical threshold (typically using a chi-squared test). They prove that a “stealthy” attacker must constrain the injected bias so that the *Kullback-Leibler (KL) divergence* between the healthy and compromised innovation distributions remains bounded. This traditionally limits the attacker to low-magnitude, static, or slow-drifting signals that mimic natural sensor noise.

Therefore, traditional stealth relies on staying within the statistical noise floor of a chi-squared detector. The methodology proposed here introduces “frequency-domain masking,” where the attack signal exists at frequencies deliberately chosen to be filtered out by the system’s own electrical cutoff characteristics, rendering it invisible to the estimator while causing physical stress.

Mo and Sinopoli [36] proved that for an attack to be stealthy, the bias must be small enough that the “Kullback-Leibler divergence” between healthy and attacked distributions stays below a threshold.

While Mo and Sinopoli [36] focused on the statistical limits of the residual, our work exploits the physical bandwidth of the BLDC inverter, allowing for high-magnitude voltage excursions that are naturally attenuated by the system’s low-pass characteristics before they reach the residual detector.

5.2.2 Historical Context: Comparison with Stuxnet

To understand the "significance" of our findings, it is useful to compare them to Stuxnet, the first widely recognized malware to target industrial PLC-controlled frequency drives.

First, consider the vulnerability target: Stuxnet targeted a completely undefended system by overwriting logic to manipulate motor speeds until mechanical failure (centrifuge resonance) occurred [99]. It relied on a lack of integrity checks.

Now compare the evolutionary step made: this dissertation assumes a defended system equipped with a predictor-based compensator thus upgrading defense to the modern standard for resilience. The "Voltage Hopping" and "Hyper-spikes" attacks are qualitatively more sophisticated than Stuxnet because they do not simply "break" the system; they fool the defense into believing the system is operating normally while the damage is being dealt. This demonstrates that state estimation, if not protected by the proposed Stackelberg-based defense, can actually become a liability by masking the attack.

These considerations on qualitative comparison of suggested in this dissertation techniques against theoretical baselines [36] and the historical Stuxnet [99] case are summarized in Table 5.2.

The comparative analysis summarized in Table 5.3 highlights the fundamental shift from data-centric security to a physics-aware interactive framework and is reviewed in the following subsections. While contemporary research has established a robust defense against network-layer threats, this dissertation addresses a critical gap in the physical-electrical coupling of high-performance motor drives.

5.2.3 Attack Target: Beyond Static Bias and Network Protocols

Existing work on cyber-physical security of networked DC drive systems has primarily addressed data-level threats — such as sensor bias injection and actuator signal manipulation — with control-theoretic countermeasures that assume a largely static adversary model [116, 117]. At the network and protocol level, comprehensive reviews of microgrid and power-electronics CPS have catalogued communication vulnerabilities and surveyed detection strategies across standard industrial protocols [103, 118, 119]. However, these approaches share a common limitation: they treat the adversary as a passive disturbance or a rule-violating intruder detectable through protocol anomalies, rather than as a strategic, interactive agent. For BLDC systems in particular, this assumption is fundamentally inadequate. The switching dynamics and phase resonances inherent to BLDC operation create an electrical bandwidth within which an adversary can execute

Table 5.2: Qualitative Comparison of Attack and Defense Methodologies (part 1)

Feature	Traditional Models (e.g., Mo, Sinopoli [36], Stuxnet [99])	Proposed Herewith In- teractive Framework
Attack Domain	Primarily <i>data-centric</i> (sensor bias) or <i>logic-centric</i> (Stuxnet).	<i>Physics-aware</i> and <i>resonance-tuned</i> (Voltage Hopping, Hyper-spiking).
System Awareness	Static or open-loop targeting of setpoints.	Closed-loop, interactive exploitation of feedback dynamics.
Stealth Mechanism	Statistical noise floor mimicry or lack of system monitoring.	<i>Frequency-domain masking</i> and hardware-based attenuation.
Defense Philosophy	Detection-focused (passive) or intrusive (<i>Physical Watermarking</i>).	Resilience-focused (proactive) via <i>Stackelberg</i> compensation.
Operational Cost	Potential control performance degradation (Watermarking).	Zero performance impact during nominal operation.
Critical Outcome	Focus on identification of integrity breach.	Neutralization of <i>Withdrawal Syndrome</i> and physical transients.

Voltage Hopping and *Hyper-spiking* — deliberately modulating adversarial signals to remain coherent with the plant’s natural frequency response, thereby evading both data-level detectors and protocol-layer monitors alike. The proposed framework addresses this gap by explicitly modelling the adversary as a rational agent within a game-theoretic structure, enabling detection and mitigation of stealthy attacks that existing static and protocol-focused baselines are not designed to handle.

5.2.4 Resource Model

In comparing our findings with the secure control framework of Teixeira et al. [14], we observe that the *Voltage Hopping* attack represents a physical bypass of the resource-limited constraints they theorized. While their model predicts attack success based on the adversary’s knowledge of

the system matrix, our work demonstrates that a “physics-aware” adversary can achieve disruption using significantly fewer resources by tuning into the system’s resonant frequencies. Furthermore, the *withdrawal syndrome* identified in this dissertation reveals a transient disruption phase that exists outside the steady-state framework defined in their *Automatica* study.

5.2.5 Real-Time Identification vs. Computational Overhead

A significant hurdle in current literature is the trade-off between detection accuracy and computational cost. Modern identification techniques — including GAN-based self-adaptive anomaly detection frameworks that achieve high accuracy on CPS benchmark datasets [100] and adaptive detection methods that address both model adaptation and data processing jointly [101] — provide strong detection performance but require substantial computational resources that may not be available on embedded motor controllers [102]. The signature-based detection introduced in this research leverages the frequency and phase domains to identify attacks in real-time. This provides a lightweight alternative that focuses on the physical signatures of *Hyper-spiking* and resonance, rather than general statistical anomalies that require extensive training data and inference overhead.

5.2.6 Integrity in Network Security

In the domain of network security, this dissertation departs from the protocol-centric baselines that dominate current literature. Comprehensive reviews of microgrid CPS attacks [103] and live testbed demonstrations of MITM intrusions in power system networks [104] exemplify methodologies that excel at identifying spoofing and unauthorized access through network-layer anomalies — packet delays, frame manipulation, and unauthorized session establishment. Even the most recent advances in stealthy attack detection [105] operate at the residual signal level, relying on statistical watermarking thresholds rather than the physical behavior of the plant itself. The proposed framework departs from this paradigm by shifting the security focus to the integrity of the control loop directly. By identifying that high-frequency masking via *Voltage Hopping* can occur entirely within valid, protocol-compliant traffic, this work provides a defense against a class of sophisticated excursions that network-layer monitors and residual-based detectors are structurally not designed to observe. Consequently, the proposed interactive framework reframes CPS security not merely as a question of *correct packets*, but of *correct physical behavior*.

5.2.7 Estimation: Issue of Static Bias

In the context of state estimation, this dissertation provides a critical extension to the integrity attack models established by Wang et al. [106], Wei et al. [107], and Sun and Yang [108]. While their respective works provide robust detection for “stealthy attack strategies” and “reduced-order descriptor observer” methods for simultaneous *FDI* and unknown disturbances, they primarily address the steady-state divergence caused by static bias or slowly varying offsets. Our findings demonstrate that by exploiting the “information boundary” between the attacker and the estimator, an adversary can execute *Voltage Hopping* and *Hyper-spiking* transients that reside at the edge of the sampling frequency. Unlike the adaptive residual thresholds or descriptor-based methods proposed in the literature [109], which are often tuned to filter out high-frequency noise as part of disturbance rejection, the proposed framework identifies these excursions as intentional adversarial signatures. By providing the “high-fidelity temporal resolution” that existing baselines lack, this research effectively overcomes the limitation of traditional observers in high-speed *BLDC* environments.

5.2.8 Game Strategy

In the domain of game strategy, this dissertation provides a departure from the communication-centric *Stackelberg* models established by Fei et al. [110], Bhattacharya et al. [112], and the *Bayesian* frameworks of 2024 [111]. While their methodologies excel at optimizing “node-level energy allocation” and addressing “hybrid *DoS* and *FDI* attacks” at the network layer, they fundamentally treat the control loop as a “black box.” Our findings demonstrate that an interactive adversary can bypass these network-layer defenses by exploiting the internal high-frequency dynamics of the plant. By implementing an *Asymmetric Stackelberg* structure directly within the embedded control loop, the proposed framework identifies *Voltage Hopping* and *Hyper-spiking*—signatures that communication-centric games are not designed to characterize. Consequently, this work effectively fills the unaddressed gap in the literature by shifting the strategic focus from data throughput to physics-aware control integrity.

5.2.9 Compensation Technique

In the area of attack compensation, the proposed interactive framework is compared against the adaptive *NN* and finite-time fuzzy feedback methods established by Fan et al. [114] and the recent non-strict feedback architectures [115]. While their methodologies—including *Nussbaum*-function-based compensation [113] — successfully maintain stability during the active phase of an attack and handle “unmodeled dynamics,” they remain prone to significant physical excursions

during the recovery phase. Our results demonstrate that the proposed framework effectively neutralizes the *Withdrawal Syndrome* through the use of anticipatory linear prediction—a capability absent in these contemporary adaptive baselines. By balancing the “Stability vs. Stealth” trade-off more effectively than high-gain or backstepping strategies, our approach ensures a seamless transition between the attack and post-attack states, preventing the secondary transients that characterize traditional adaptive responses.

Table 5.3: Qualitative Comparison of Attack and Defense Methodologies (part 2)

Feature	Contemporary Baselines and Issues	Proposed Framework
Attack Target	Sensor/actuator bias injection in networked DC systems [116, 117]. <i>Issue: Treats the plant as a linear channel, neglecting switching dynamics and phase resonances.</i>	<i>Physics-aware</i> exploitation of <i>BLDC</i> switching and phase resonance via <i>Voltage Hopping</i> .
Resource Model	Constraints based on <i>steady-state</i> disruption resources [14]. <i>Issue: Overlooks resonance-based efficiency.</i>	<i>Physics-aware</i> bypass: high-impact disruption with minimal resources.
Identification	GAN-based self-adaptive anomaly detection [100, 101]. <i>Issue: High computational cost for embedded motor controllers.</i>	Real-time signature-based detection across frequency and phase domains.
Network Security	MITM and spoofing detection in microgrid CPS [103–105]. <i>Issue: Blind to control-loop integrity within compliant traffic.</i>	Focus on <i>control-loop</i> integrity and high-frequency masking.
Estimation	Integrity attacks on <i>KF</i> exploiting unknown disturbances [106, 107]. <i>Issue: Focus on static bias or slowly varying offsets.</i>	Discovery of <i>Voltage Hopping</i> and <i>Hyper-spiking</i> transients.
Game Strategy	<i>Stackelberg</i> model for hybrid <i>DoS/FDI</i> and node-level energy allocation [110–112]. <i>Issue: Communication-centric/Black-box.</i>	<i>Asymmetric Stackelberg</i> framework for embedded <i>control-loop</i> integrity and high-frequency dynamics.
Compensation	Adaptive fuzzy, self-triggered, and backstepping resilient control for non-strict <i>CPS</i> [113–115]. <i>Issue: Stability vs. Stealth / termination transients.</i>	Neutralization of <i>Withdrawal Syndrome</i> via anticipatory linear prediction.

Chapter 6

Conclusions and Future Work

The proliferation of Brushless DC (BLDC) motors in safety-critical Cyber-Physical Systems (CPS) demands robust security research to address emerging vulnerabilities. BLDC motors have become the propulsion and actuation standard across high-volume, performance-critical applications, including medical robotics, autonomous vehicles, and the rapidly growing sector of Unmanned Aerial Vehicles (UAVs). This ubiquity stems from their inherent advantages: superior power-to-weight ratio, high efficiency, and low maintenance requirements.

However, the very features that make them essential—their precise, sensor-driven electronic control—also expose them to sophisticated cyberattacks. Unlike traditional mechanical systems, the performance and safety of a BLDC motor system are entirely dependent on the integrity of the data flowing through its digital control loop (current, voltage, and estimated speed signals). An adversary can exploit this dependency by injecting subtle, stealthy biases or spikes into the feedback signals, leading to dangerous consequences: from simple control degradation and efficiency loss, to catastrophic physical failure and loss of life in safety-critical applications.

Therefore, research into proactive defense architectures for BLDC motor control systems is no longer a theoretical exercise but a critical requirement for maintaining the stability and reliability of modern CPS infrastructure.

6.1 Summary of Research and Contributions

This dissertation addressed the critical and emerging security vulnerabilities within BLDC motor-driven Cyber-Physical Systems (CPS), which are increasingly deployed in safety-critical infrastructure, ranging from UAVs to medical devices. The primary aim was to move beyond simple attack identification toward the development and validation of proactive defense architectures.

The research yielded several significant contributions:

1. **Systematic Characterization of Attack Modalities:** A comprehensive classification detailing six distinct attack modalities was established, providing a foundational and exhaustive taxonomy for threats targeting the BLDC motor's control loop, spanning both stealthy data manipulation and disruptive high-power injection. The six identified adversarial modalities are classified by their impact pathway:
 - **Data Manipulation Attacks** (Targeting State Estimation): Probing and Current Drainage.
 - **Power Disruption Attacks** (Targeting Actuation): Voltage Hopping, Induced Pulsation, Extended Pulsation, and Hyper-Spiking.
2. **Discovery of Novel Attack Mechanisms Engaging Resonance Effects:** The research demonstrated and quantified the system's susceptibility to sophisticated, transient control-theoretic attacks through the discovery and validation of three novel Resonant Attack Mechanisms:
 - The Voltage Hopping, Induced Pulsation, and Hyper-Spiking mechanisms, which were shown to lead to destabilizing manipulation of the control signals by exciting the system's internal resonant frequencies. The analysis included characterization of the variations, such as the Extended Pulsations version of the Induced Pulsation mechanism.
3. **Characterization of Novel Temporal Vulnerability Artifacts:** The analysis of the adversarial attack mechanisms further led to the identification and detailed characterization of three key temporal vulnerability artifacts that define the system's transient response to adversarial manipulation:
 - The **Initial Impulse Syndrome**, defining the large transient estimation error immediately following attack initiation.
 - The **Attack Withdrawal Syndrome**, quantifying the system's delayed and oscillatory recovery upon attack termination.
 - **Attacks with Interruption/Resuming Sequences**, which exploit the combined and accumulating impact of the impulse and withdrawal syndromes to induce chronic instability.
4. **Development and Validation of a Linear Defense Architecture:** A robust defense architecture was developed and successfully *validated*, effectively neutralizing the impacts of specific bias injection attacks. Quantitative analysis confirms that this defense achieves

better than 95% *stability retention* for both the *Current Drainage* modality—under conditions of deep-level, low modulation depth sawtooth distortion—and the *Induced Pulsations* modality across a wide range of *attack frequencies*.

5. **Establishment of Detection Frameworks:** A signature-based detection framework was formulated, providing timely and accurate recognition of adversarial activity, which is crucial for enabling the Informed Counter-Bias defense strategy.
6. **Comprehensive Threat Models:** We formulated a comprehensive set of threat models spanning the mechanical, electrical, and control-theoretic pathways, offering a holistic view of CPS vulnerabilities.

These contributions provide both theoretical foundations for understanding temporal vulnerabilities in feedback systems and practical guidance for implementing robust security architectures in safety-critical cyber-physical infrastructures.

6.2 Limitations of the Current Study

The research presented is subject to several practical and theoretical limitations. The primary defense analysis was constrained to the Informed Counter-Bias scenario (Scenario 1), where the general attack type is assumed known. Further, the defense mechanism itself is restricted to a linear architecture, and all validation was performed within a simulation environment, without full real-time hardware implementation validation.

6.3 Future Work

Building upon the foundations established in this dissertation, future research directions should focus on extending the analysis across broader motor platforms and integrating advanced computational intelligence to enhance both adversarial and defensive capabilities:

- **Generalization to AC Motor Control Systems:** The current defense architecture, designed for the trapezoidal control of BLDC motors, should be extended to the control systems of general AC motors, such as Permanent Magnet Synchronous Motors (PMSMs) and Induction Motors (IMs). This extension necessitates investigating the effectiveness of the proposed defense strategies when applied to the complex, continuous vector control techniques (Field-Oriented Control, FOC) used by these motor types. This analysis will determine the generality of the temporal vulnerabilities discovered.

- **Integration of Advanced AI Agents for Attack and Defense:** Future work should explore the use of Artificial Intelligence (AI) agents to significantly advance the complexity of both sides of the security problem:
 - **AI-Driven Adversaries:** Developing intelligent attack agents (e.g., using Reinforcement Learning) capable of discovering and launching adaptive, stealth-optimized attacks in real-time. These agents would actively adjust their parameters to evade detection thresholds.
 - **Intelligent Defense Mechanisms:** Exploring the use of machine learning techniques (e.g., Neural Networks or Adaptive Kalman Filters) to create nonlinear and adaptive defense mechanisms capable of predicting and compensating for complex, time-varying adversarial inputs without explicit prior knowledge of the attack type.
- **Hardware and Multi-System Validation:** The theoretical models should be subjected to rigorous real-time hardware implementation validation to quantify practical latency, computational overhead, and effectiveness on physical motor drives and in multi-motor distributed systems (e.g., networked UAV swarms).

A natural direction for further research is the extension of these concepts to AC induction and synchronous motor drives, which are the predominant workhorses of industrial automation. Their nonlinear dynamics, estimator-based control structures, and inverter dependencies introduce distinct cyberattack surfaces that remain underexplored. The following research directions are proposed.

6.3.1 False-Data Injection Attacks on Field-Oriented Control

Field-oriented control (FOC) of induction and synchronous machines relies on accurate measurements or estimations of stator currents, rotor speed, and flux components. Theoretical foundations for false-data injection (FDI) attacks in feedback-driven systems have been rigorously developed in the control-security community [120, 121]. Applying these principles to AC motor control loops, future work may investigate how small coordinated biases injected into the i_d/i_q feedback channels, speed estimators, or flux observers influence torque production and stability margins.

Analytical objectives could include deriving FDI detectability conditions for AC FOC architectures and establishing parameter-space regions where classical threshold-based protections fail. Simulation studies may then demonstrate destabilizing effects, such as torque ripple amplification, erroneous flux weakening, or loss of synchronism.

6.3.2 Attacks on Sensorless AC Control Schemes

Sensorless AC motor drives depend on observers such as Model Reference Adaptive System (MRAS) estimators, extended Kalman filters (EKF/UKF), sliding-mode observers, and other hybrid variants. These algorithms are known to exhibit sensitivity to parameter mismatch and structured noise, and their vulnerabilities extend naturally to adversarial perturbations. Contemporary reviews and developments in sensorless control [122, 123] illustrate increasing reliance on estimator-driven feedback, which in turn broadens the corresponding attack surface.

Future research may examine how an attacker could exploit MRAS adaptation errors, sliding-surface switching dynamics, or the discrete-time covariance structure of EKF/UKF estimators to mislead rotor-speed or flux estimates. Complementary defensive work may focus on enhanced residual monitoring, adaptive thresholding, and robustified observer designs.

6.3.3 Security of Industrial Variable-Frequency Drives

Industrial deployments of variable-frequency drives (VFDs) have demonstrated configuration-, firmware-, and network-level vulnerabilities. Publicly documented cases show that insecure or poorly segmented VFD interfaces can allow adversaries to remotely modify critical operational parameters, including skip frequencies, acceleration ramps, or motor-nameplate constants [124, 125]. Such modifications can induce destructive mechanical resonance, excessive thermal loading, or accelerated fatigue of AC motors.

Future work may include developing a taxonomy of VFD-specific attack vectors, characterizing unsafe operating envelopes for common industrial loads, and designing integrity-checking strategies for configuration parameters. This includes anomaly detection based on cross-validation between commanded parameters, inferred motor states, and inverter switching behavior.

6.3.4 Digital Twin–Based Experimental Platform

To safely examine adversarial scenarios without risking physical equipment, a high-fidelity digital twin of an AC motor drive system can serve as an experimental backbone. Recent work on digital-twin frameworks for cyber–physical system verification [126] demonstrates the feasibility of integrating detailed machine models, inverter nonlinearities, and networked communication modules within virtual environments.

Such a platform would enable reproducible security experiments, reinforcement-learning–based attack exploration, and co-simulation of control logic and cyber-layer interactions. Hardware-in-the-loop (HIL) extensions can later validate digital-twin findings on real drives with reduced risk.

6.3.5 Model-Based Intrusion Detection Using Observer Residuals

Residual-based detection has proven effective for identifying faults in induction machines, particularly using EKF and UKF methods [127]. Future work may adapt these techniques to cybersecurity contexts by distinguishing adversarially induced anomalies from legitimate mechanical or electrical faults. This includes designing residual filters robust to intentional biasing, establishing dynamic thresholds that reduce false alarms, and integrating observer inconsistency metrics into real-time security monitors.

6.3.6 Autonomous Defensive Agents and Malware Containment

Historical analyses of industrial-targeted malware, most prominently the Stuxnet operation [128], illustrate the feasibility of coordinated, multi-stage cyber-attacks on drive systems. Building on this precedent, future research may explore autonomous defensive agents capable of performing integrity checks, detecting abnormal drive behavior, and initiating safe reconfiguration or isolation procedures.

Although such defensive agents must adhere to strict safety guarantees, they may offer an additional layer of resilience, especially in high-value industrial environments where response time is critical.

References

- [1] Y. Boiko, I. Kiringa, and T. Yeap, “Linear-dynamic predictor based defense against current drainage cyber attack of BLDC motor control system,” *Authorea Preprints*, 2024.
- [2] Y. Boiko, I. Kiringa, and T. Yeap, “Current drainage attack correction via adjusting the attacking saw function asymmetry,” in *Proc. 17th Int. Conf. Cyber Resilience Systems and Cybersecurity (CRSC)*, Published by WASET as *Int. J. Comput. Inf. Eng.*, vol. 17, no. 12, Open Science Index 204. Available online: <https://publications.waset.org/10013400.pdf>, Ottawa, ON, Canada, Dec. 2023, pp. 685–691.
- [3] Y. Boiko, I. Kiringa, and T. Yeap, “Extended pulsation attack against Kalman filter driven BLDC motor control system,” in *2023 13th International Conference on Advanced Computer Information Technologies (ACIT)*, IEEE, Wrocław, Poland, 2023, pp. 397–402. DOI: [10.1109/ACIT58437.2023.10275446](https://doi.org/10.1109/ACIT58437.2023.10275446)
- [4] Y. Boiko, I. Kiringa, and T. Yeap, “Voltage hopping induced by bias injection attack against Kalman filter of BLDC motor,” in *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)*, Houston, TX, USA, Feb. 2023, pp. 1–5. DOI: [10.1109/ICAIC57335.2023.10044123](https://doi.org/10.1109/ICAIC57335.2023.10044123)
- [5] Y. Boiko, I. Kiringa, and T. Yeap, “Current drainage induced by bias injection attack against Kalman filter of BLDC motor,” in *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, Rhodes, Greece, Jul. 2022, pp. 364–369. DOI: [10.1109/CSR54599.2022.9850310](https://doi.org/10.1109/CSR54599.2022.9850310)
- [6] Y. Boiko, C. Lin, I. Kiringa, and T. Yeap, “Performance of BLDC motor under Kalman filter sensorless drive,” in *International Journal of Electrical and Information Engineering*, vol. 15, Ottawa, ON, Canada, 2021, pp. 282–288. [Online]. Available: <https://publications.waset.org/10012126/performance-of-bldc-motor-under-kalman-filter-sensorless-drive>
- [7] Y. B. Boiko and T. H. Yeap, “Self-similarity of the simulated internet traffic from the source with clustered fragmented periodic output,” in *2013 SummerSim*, Toronto, ON,

- Canada, 2013, pp. 35–40. [Online]. Available: <https://dl.acm.org/doi/10.5555/2557696.2557734>
- [8] Y. Boiko, I. Kiringa, and T. Yeap, “Induced pulsation attack against Kalman filter driven brushless DC motor control system,” in *Proc. 17th Int. Conf. Cybersecurity, Cybercrime and Cyberthreats (ICCCC)*, Accepted for publication in *Int. J. Electr. Inf. Eng.*; Abstract available online: <https://publications.waset.org/abstracts/164883.pdf>, Montreal, QC, Canada, May 2023.
 - [9] A. W. Colombo, S. Karnouskos, O. Kaynak, Y. Shi, and S. Yin, “Industrial cyberphysical systems: A backbone of the fourth industrial revolution,” *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 6–16, Mar. 2017. DOI: [10.1109/MIE.2017.2648857](https://doi.org/10.1109/MIE.2017.2648857)
 - [10] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, “Ensuring safety, security, and sustainability of mission-critical cyber–physical systems,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 283–299, Jan. 2012. DOI: [10.1109/JPROC.2011.2165689](https://doi.org/10.1109/JPROC.2011.2165689)
 - [11] Y. Lakhdhar, S. Rekhis, and N. Boudriga, “Proactive security for safety and sustainability of mission critical systems,” *IEEE Transactions on Sustainable Computing*, vol. 6, no. 2, pp. 257–273, Apr. 2021. DOI: [10.1109/TSUSC.2018.2810092](https://doi.org/10.1109/TSUSC.2018.2810092)
 - [12] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits, “Taxonomy for description of cross-domain attacks on CPS,” in *Proceedings of the 2nd ACM international conference on High confidence networked systems*, Philadelphia, Pennsylvania, USA, 2013, pp. 135–142. DOI: [10.1145/2461446.2461465](https://doi.org/10.1145/2461446.2461465)
 - [13] F. Pasqualetti, F. Dörfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013. DOI: [10.1109/TAC.2013.2266831](https://doi.org/10.1109/TAC.2013.2266831)
 - [14] A. M. H. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, “A secure control framework for resource-limited adversaries,” *Automatica*, vol. 51, pp. 135–148, 2015. DOI: [10.1016/j.automatica.2014.10.067](https://doi.org/10.1016/j.automatica.2014.10.067)
 - [15] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure estimation and control for cyber-physical systems under adversarial attacks,” *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, 2014. DOI: [10.1109/TAC.2014.2303233](https://doi.org/10.1109/TAC.2014.2303233)
 - [16] H. Harkat, L. M. Camarinha-Matos, J. Goes, and H. F. Ahmed, “Cyber-physical systems security: A systematic review,” *Computers and Industrial Engineering*, vol. 188, p. 109891, 2024. DOI: [10.1016/j.cie.2024.109891](https://doi.org/10.1016/j.cie.2024.109891) [Online]. Available: [sciencedirect.com/science/article/pii/S0360835224000123](https://www.sciencedirect.com/science/article/pii/S0360835224000123)

- [17] H. Fawzi, P. Tabuada, and S. N. Diggavi, “Secure estimation and control for cyber-physical systems under adversarial attacks,” *IEEE Transactions on Automatic Control*, vol. 59, pp. 1454–1467, 2012. [Online]. Available: <https://api.semanticscholar.org/CorpusID:13501109>
- [18] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, “A survey of approaches combining safety and security for industrial control systems,” *Reliability Engineering & System Safety*, vol. 139, pp. 156–178, 2015. DOI: [10.1016/j.ress.2015.02.008](https://doi.org/10.1016/j.ress.2015.02.008) [Online]. Available: [sciencedirect.com/science/article/pii/S0951832015000538](https://www.sciencedirect.com/science/article/pii/S0951832015000538)
- [19] R. Mitchell and I.-R. Chen, “A survey of intrusion detection techniques for cyber-physical systems,” *ACM Computing Surveys (CSUR)*, vol. 46, no. 4, pp. 1–29, Mar. 2014, Art. 55. DOI: [10.1145/2542049](https://doi.org/10.1145/2542049)
- [20] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, “Attacks against process control systems: Risk assessment, detection, and response,” in *Proceedings of the 6th International Symposium on Information, Computer and Communications Security (ASIACCS 2011)*, Hong Kong, China, May 2011, pp. 355–366. DOI: [10.1145/1966913.1966959](https://doi.org/10.1145/1966913.1966959)
- [21] W. Duo, M. Zhou, and A. Abusorrah, “A survey of cyber attacks on cyber physical systems: Recent advances and challenges,” *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 5, pp. 784–800, May 2022. DOI: [10.1109/JAS.2022.105548](https://doi.org/10.1109/JAS.2022.105548)
- [22] P. Angueira, I. Val, J. Montalbán, Ó. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, and A. Arriola, “A survey of physical layer techniques for secure wireless communications in industry,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 810–838, 2022. DOI: [10.1109/COMST.2022.3148857](https://doi.org/10.1109/COMST.2022.3148857)
- [23] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, “A survey of physical layer security techniques for 5G wireless networks and challenges ahead,” *arXiv:1801.05227*, Jan. 2018. DOI: [10.48550/arXiv.1801.05227](https://doi.org/10.48550/arXiv.1801.05227)
- [24] M. Hayashi and Á. Vázquez-Castro, “Two-way physical layer security protocol for gaussian channels,” *IEEE Transactions on Communications*, vol. 68, no. 5, pp. 3068–3078, May 2020. DOI: [10.1109/TCOMM.2020.2973618](https://doi.org/10.1109/TCOMM.2020.2973618)
- [25] J. Thomas, S. Cherian, S. Chandran, and V. Pavithran, “Man in the middle attack mitigation in LoRaWAN,” in *2020 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, India, Feb. 2020, pp. 353–358. DOI: [10.1109/ICICT48043.2020.9112391](https://doi.org/10.1109/ICICT48043.2020.9112391)

- [26] J.-S. Wang and G.-H. Yang, "Data-driven methods for stealthy attacks on tcp/ip-based networked control systems equipped with attack detectors," *IEEE transactions on cybernetics*, vol. 49, no. 8, pp. 3020–3031, 2018. DOI: [10.1109/TCYB.2018.2837874](https://doi.org/10.1109/TCYB.2018.2837874)
- [27] M. Jablonski and D. Wijesekera, "Attacking electric motors for fun and profit," in *Proceedings of Black Hat USA 2019*, White paper and presentation available at <https://i.blackhat.com/USA-19/Wednesday/us-19-Jablonski-Attacking-Electric-Motors-For-Fun-And-Profit-wp.pdf>, Las Vegas, NV, USA, Aug. 2019.
- [28] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *49th IEEE Conference on Decision and Control (CDC)*, Atlanta, GA, USA, 2010, pp. 5967–5972. DOI: [10.1109/CDC.2010.5718158](https://doi.org/10.1109/CDC.2010.5718158)
- [29] J. Keller and M. Darouach, "Optimal two-stage Kalman filter in the presence of random bias," *Automatica*, vol. 33, no. 9, pp. 1745–1748, 1997. DOI: [10.1016/S0005-1098\(97\)00088-5](https://doi.org/10.1016/S0005-1098(97)00088-5) [Online]. Available: [sciencedirect.com/science/article/pii/S0005109897000885](https://www.sciencedirect.com/science/article/pii/S0005109897000885)
- [30] A. S. L. V. Tummala and R. K. Inapakurthi, "A two-stage Kalman filter for cyber-attack detection in automatic generation control system," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 1, pp. 50–59, Jan. 2022. DOI: [10.35833/MPCE.2019.000119](https://doi.org/10.35833/MPCE.2019.000119)
- [31] X. Ge, Q.-L. Han, M. Zhong, and X.-M. Zhang, "Distributed krein space-based attack detection over sensor networks under deception attacks," *Automatica*, vol. 109, p. 108557, 2019. DOI: [10.1016/j.automatica.2019.108557](https://doi.org/10.1016/j.automatica.2019.108557) [Online]. Available: [sciencedirect.com/science/article/pii/S0005109819304182](https://www.sciencedirect.com/science/article/pii/S0005109819304182)
- [32] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under markov modulated denial-of-service (dos) attack strategies," *IEEE Transactions on Automatic Control*, vol. 60, no. 12, pp. 3299–3304, Dec. 2015. DOI: [10.1109/TAC.2015.2416926](https://doi.org/10.1109/TAC.2015.2416926)
- [33] R. Acharya and K. Asha, "Data integrity and intrusion detection in wireless sensor networks," in *2008 16th IEEE International Conference on Networks*, New Delhi, India, Dec. 2008, pp. 1–5. DOI: [10.1109/ICON.2008.4772642](https://doi.org/10.1109/ICON.2008.4772642)
- [34] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016. DOI: [10.1109/COMST.2016.2548426](https://doi.org/10.1109/COMST.2016.2548426)

- [35] D. Zhang, Q.-G. Wang, G. Feng, Y. Shi, and A. V. Vasilakos, "A survey on attack detection, estimation and control of industrial cyber-physical systems," *ISA Transactions*, vol. 116, pp. 1–12, Oct. 2021. DOI: [10.1016/j.isatra.2021.01.036](https://doi.org/10.1016/j.isatra.2021.01.036)
- [36] Y. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," *IEEE Transactions on Automatic Control*, vol. 60, no. 4, pp. 1145–1151, Apr. 2015. DOI: [10.1109/TAC.2014.2350231](https://doi.org/10.1109/TAC.2014.2350231)
- [37] J. Lu and R. Niu, "False information injection attack on dynamic state estimation in multi-sensor systems," in *17th International Conference on Information Fusion (FUSION)*, Salamanca, Spain, Jul. 2014, pp. 1–8. [Online]. Available: http://confcats_isif.s3.amazonaws.com/web-files/event/proceedings/html/2014Proceedings/papers/fusion2014_submission_400/paper400.pdf
- [38] H. Song, D. Ding, H. Dong, and Q.-L. Han, "Distributed maximum correntropy filtering for stochastic nonlinear systems under deception attacks," *IEEE Transactions on Cybernetics*, vol. 52, no. 5, pp. 3733–3744, 2022. DOI: [10.1109/TCYB.2020.3016093](https://doi.org/10.1109/TCYB.2020.3016093)
- [39] B. Liu, B. Chen, H. Zhao, J. Qin, and J. Cao, "Distributed maximum correntropy unscented Kalman filter under hybrid attacks in non-Gaussian environment," *Asian Journal of Control*, 2024. DOI: [10.1002/asjc.3343](https://doi.org/10.1002/asjc.3343)
- [40] X. Xu, X. Kan, W. Wang, and J. Chu, "Distributed maximum correntropy Kalman filtering for stochastic discrete time system: A encoding-decoding-based approach," *Journal of the Franklin Institute*, vol. 363, no. 6, p. 108 498, 2026. DOI: [10.1016/j.jfranklin.2026.108498](https://doi.org/10.1016/j.jfranklin.2026.108498) [Online]. Available: [sciencedirect.com/science/article/pii/S0016003226000980](https://www.sciencedirect.com/science/article/pii/S0016003226000980)
- [41] A. Bello, I. M. Kilishi, M. M. Bari, and U. Abubakar, "Comparative review of PMSM and BLDCM based on direct torque control method," *International Journal of Scientific & Technology Research*, vol. 3, pp. 195–199, 2014. [Online]. Available: <https://api.semanticscholar.org/CorpusID:18900311>
- [42] M. Johansson, "Evaluation of sensor solutions & motor speed control methods for BLDCM/PMSM in aerospace application," M.S. thesis, Lulea University of Technology, Sweden, 2017. [Online]. Available: <https://ltu.diva-portal.org/smash/get/diva2:1065318/FULLTEXT01.pdf>
- [43] A. Sabir and M. Kassas, "A novel and simple hybrid fuzzy/pi controller for brushless DC motor drives," *Automatika*, vol. 56, no. 4, pp. 424–435, 2015. DOI: [10.1080/00051144.2015.11828656](https://doi.org/10.1080/00051144.2015.11828656)

- [44] M. Tomita, T. Senjyu, S. Doki, and S. Okuma, “New sensorless control for brushless DC motors using disturbance observers and adaptive velocity estimations,” *IEEE Transactions on Industrial Electronics*, vol. 45, no. 2, pp. 274–282, Apr. 1998. DOI: [10.1109/41.681226](https://doi.org/10.1109/41.681226)
- [45] B. Terzic and M. Jadric, “Design and implementation of the extended Kalman filter for the speed and rotor position estimation of brushless DC motor,” *IEEE Transactions on Industrial Electronics*, vol. 48, no. 6, pp. 1065–1073, Dec. 2001. DOI: [10.1109/41.969385](https://doi.org/10.1109/41.969385)
- [46] T. Shi, N. Lu, Q. Zhang, and C. Xia, “Brushless DC motor sliding mode control with Kalman filter,” in *2008 IEEE International Conference on Industrial Technology*, Apr. 2008, pp. 1–6. DOI: [10.1109/ICIT.2008.4608509](https://doi.org/10.1109/ICIT.2008.4608509)
- [47] N. Aliwa, O. Rana, C. Perera, and P. Burnap, “Cyberattacks and countermeasures for in-vehicle networks,” *ACM Computing Surveys*, vol. 54, no. 1, pp. 1–37, 2021. DOI: [10.1145/3431233](https://doi.org/10.1145/3431233)
- [48] B. Gul and F. Ertam, “In-vehicle communication cyber security,” *Vehicular Communications*, vol. 50, 2024, Art. 100846. DOI: [10.1016/j.vehcom.2024.100846](https://doi.org/10.1016/j.vehcom.2024.100846)
- [49] M. D. Mwanje, O. Kaiwartya, M. Aljaidi, Y. Cao, S. Kumar, D. N. Jha, A. Naser, and J. Lloret, “Cyber security analysis of connected vehicles,” *IET Intelligent Transport Systems*, vol. 18, pp. 1175–1195, 2024. DOI: [10.1049/itr2.12504](https://doi.org/10.1049/itr2.12504)
- [50] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, “Cyber–Physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4639–4657, Aug. 2021. DOI: [10.1109/JESTPE.2020.3045667](https://doi.org/10.1109/JESTPE.2020.3045667)
- [51] L. Guo and J. Ye, “Cyber-Physical security of electric vehicles with four motor drives,” *IEEE Transactions on Power Electronics*, vol. 36, no. 4, pp. 4463–4477, Apr. 2021. DOI: [10.1109/TPEL.2020.3025718](https://doi.org/10.1109/TPEL.2020.3025718)
- [52] C. Liu, J. Ye, G. Fang, D. Wang, L. Zhou, and A. Emadi, “Resilience framework for power electronic systems against cyber-physical attacks: A review,” *IEEE Open Journal of Power Electronics*, vol. 6, pp. 28–55, 2025. DOI: [10.1109/OJPPEL.2024.3512452](https://doi.org/10.1109/OJPPEL.2024.3512452)
- [53] J. F. Gieras, R.-J. Wang, and M. J. Kamper, *Axial Flux Permanent Magnet Brushless Machines*, 2nd ed. Dordrecht, Netherlands: Springer Science & Business Media, 2008. DOI: [10.1007/978-1-4020-8227-6](https://doi.org/10.1007/978-1-4020-8227-6)

- [54] D. C. Hanselman, *Brushless Permanent Magnet Motor Design*, 2nd ed. The Writers' Collective, 2003. [Online]. Available: <https://blog.avislab.com/uploads/2014/05/BrushlessPermanentMagnetMotorDesignVersion2.pdf>
- [55] R. Krishnan, *Permanent Magnet Synchronous and Brushless DC Motor Drives*. Boca Raton, FL: CRC Press, 2010. DOI: [10.1201/9781420014235](https://doi.org/10.1201/9781420014235)
- [56] C.-T. Liu, S.-C. Lin, J. Zamora, and T.-S. Chiang, "Optimal operational strategy design of a single-sided permanent magnet axial-flux motor for electrical vehicle application," in *38th IAS Annual Meeting on Conference Record of the Industry Applications Conference, 2003.*, vol. 3, Salt Lake City, Utah, USA, Oct. 2003, pp. 1677–1683. DOI: [10.1109/IAS.2003.1257781](https://doi.org/10.1109/IAS.2003.1257781)
- [57] A. D. Gerlando, G. Foglia, and C. Ricca, "Analytical design of a high torque density in-wheel YASA AFPM motor," in *2020 International Conference on Electrical Machines (ICEM)*, vol. 1, Gothenburg, Sweden, Aug. 2020, pp. 402–408. DOI: [10.1109/ICEM49940.2020.9270998](https://doi.org/10.1109/ICEM49940.2020.9270998)
- [58] A. Echle, Y. Gong, J. Terfurth, and N. Parspour, "Fea-based comparison of BLDC and BLAC modes for an axial flux motor with trapezoidal BEMF," in *IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society*, Singapore, Oct. 2020, pp. 2694–2701. DOI: [10.1109/IECON43393.2020.9255310](https://doi.org/10.1109/IECON43393.2020.9255310)
- [59] A. Chowdhury, S. Das, T. Tsuda, N. Saito, S. Saha, and Y. Sozer, "Design and comprehensive performance analysis of transverse flux and axial flux topologies for permanent magnet synchronous machines," in *2021 IEEE Energy Conversion Congress and Exposition (ECCE)*, Vancouver, Canada, Oct. 2021, pp. 3957–3962. DOI: [10.1109/ECCE47101.2021.9595076](https://doi.org/10.1109/ECCE47101.2021.9595076)
- [60] O. Dobzhanskyi, O. Duniev, E. Amiri, A. Yehorov, P. Gottipati, A. Masliennikov, and E. Mendrela, "Performance comparison of BLDC permanent magnet machines with different topologies," in *2021 IEEE 2nd KhPI Week on Advanced Technology (KhPI-Week)*, Kharkiv, Ukraine, Sep. 2021, pp. 346–350. DOI: [10.1109/KhPIWeek53812.2021.9569983](https://doi.org/10.1109/KhPIWeek53812.2021.9569983)
- [61] S. K. Chawrasia, C. Kumar Chanda, and S. Banerjee, "Design and analysis of in-wheel motor for an electric vehicle," in *2020 IEEE Calcutta Conference (CALCON)*, Calcutta, India, Feb. 2020, pp. 351–355. DOI: [10.1109/CALCON49167.2020.9106538](https://doi.org/10.1109/CALCON49167.2020.9106538)
- [62] A. Chinthala and S. Vuddanti, "Performance analysis of induction motor and PMSM for electrical vehicle traction application," in *2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, Ballari, India, Apr. 2022, pp. 1–6. DOI: [10.1109/ICDCECE53908.2022.9793305](https://doi.org/10.1109/ICDCECE53908.2022.9793305)

- [63] R. Kumar, P. Kumar, B. Kumar, P. Singh, R. Kumar, and A. Kumar, "Design and analysis of high performance of a BLDC motor for electric vehicle," in *2022 2nd International Conference on Emerging Frontiers in Electrical and Electronic Technologies (ICEFEET)*, Piscataway, New Jersey, USA, Jun. 2022, pp. 1–4. DOI: [10.1109/ICEFEET51821.2022.9848307](https://doi.org/10.1109/ICEFEET51821.2022.9848307)
- [64] P. H. Kumar and V. T. Somasekhar, "An enhanced fault-tolerant and autoreconfigurable BLDC motor drive for electric vehicle applications," *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, vol. 4, no. 1, pp. 368–380, Jan. 2023. DOI: [10.1109/JESTIE.2022.3196818](https://doi.org/10.1109/JESTIE.2022.3196818)
- [65] S. Chen, X. Hao, C. Gao, and Z. Jiang, "An effective nontransient active short-circuit method for PMSM in electric vehicles," *IEEE Transactions on Industrial Electronics*, vol. 70, no. 4, pp. 3571–3580, Apr. 2023. DOI: [10.1109/TIE.2022.3176315](https://doi.org/10.1109/TIE.2022.3176315)
- [66] A. M. EL-Refaie, "Electrical machines for traction and propulsion applications," in *Transportation Electrification: Breakthroughs in Electrified Vehicles, Aircraft, Rolling Stock, and Watercraft*, IEEE, 2023, pp. 1–26. DOI: [10.1002/9781119812357.ch1](https://doi.org/10.1002/9781119812357.ch1) [Online]. Available: ieeexplore-ieee-org.proxy.bib.uottawa.ca/document/9989495
- [67] G. Sieklucki, "An investigation into the induction motor of Tesla model S vehicle," in *2018 International Symposium on Electrical Machines (SME)*, Andrychów, Poland, Jun. 2018, pp. 1–6. DOI: [10.1109/ISEM.2018.8442648](https://doi.org/10.1109/ISEM.2018.8442648)
- [68] C. Shumei, L. Chen, and S. liwei, "Study on efficiency calculation model of induction motors for electric vehicles," in *2008 IEEE Vehicle Power and Propulsion Conference*, Harbin, China, Sep. 2008, pp. 1–5. DOI: [10.1109/VPFC.2008.4677791](https://doi.org/10.1109/VPFC.2008.4677791)
- [69] S. Bose, S. Chourey, and S. Sundaram, "An optimization based pid controller tuning approach for the induction motor employed in an electric vehicle," in *2022 Interdisciplinary Research in Technology and Management (IRTM)*, Kolkata, India, Feb. 2022, pp. 1–5. DOI: [10.1109/IRTM54583.2022.9791654](https://doi.org/10.1109/IRTM54583.2022.9791654)
- [70] J. West, "DC, induction, reluctance and PM motors for electric vehicles," in *IEE Colloquium on Motors and Drives for Battery Powered Propulsion*, London, UK, Apr. 1993, pp. 1/1–111. DOI: [10.1049/pe:19940203](https://doi.org/10.1049/pe:19940203)
- [71] N. Hashemnia and B. Asaei, "Comparative study of using different electric motors in the electric vehicles," in *2008 18th International Conference on Electrical Machines*, Vilamoura, Portugal, Sep. 2008, pp. 1–5. DOI: [10.1109/ICELMACH.2008.4800157](https://doi.org/10.1109/ICELMACH.2008.4800157)

- [72] D. Yousfi, A. Elbacha, and A. A. Ouahman, “Efficient sensorless PMSM drive for electric vehicle traction systems,” in *Electric Vehicles*, S. Soylu, Ed., Rijeka: IntechOpen, 2011, ch. 9. DOI: [10.5772/16600](https://doi.org/10.5772/16600)
- [73] S. Acharya, R. Mieth, R. Karri, and Y. Dvorkin, “False data injection attacks on data markets for electric vehicle charging stations,” *Advances in Applied Energy*, vol. 7, 2022, Art. 100098. DOI: [10.1016/j.adapen.2022.100098](https://doi.org/10.1016/j.adapen.2022.100098)
- [74] B. Raouf and S. Mousavian, “False data injection to conceal load-altering attacks via electric vehicles,” *Sustainable Energy, Grids and Networks*, vol. 42, 2025, Art. 101676. DOI: [10.1016/j.segan.2025.101640](https://doi.org/10.1016/j.segan.2025.101640) [Online]. Available: [sciencedirect.com/science/article/abs/pii/S2352467725000220](https://www.sciencedirect.com/science/article/abs/pii/S2352467725000220)
- [75] T. Phillips, H. Mehrpouyan, J. Gardner, and S. Reese, “A covert system identification attack on constant setpoint control systems,” in *2019 Seventh International Symposium on Computing and Networking Workshops (CANDARW)*, Nagasaki, Japan, Nov. 2019, pp. 367–373. DOI: [10.1109/CANDARW.2019.00070](https://doi.org/10.1109/CANDARW.2019.00070)
- [76] S. Al-Rabiaah, “The “Stuxnet” virus of 2010 as an example of a “APT” and its “recent” variances,” in *2018 21st Saudi Computer Society National Computer Conference (NCC)*, Riyadh, Saudi Arabia, Apr. 2018, pp. 1–5. DOI: [10.1109/NCG.2018.8593143](https://doi.org/10.1109/NCG.2018.8593143)
- [77] S. Kriaa, M. Bouissou, and L. Piètre-Cambacédès, “Modeling the stuxnet attack with bdmp: Towards more formal risk assessments,” in *2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, Cork, Ireland, Oct. 2012, pp. 1–8. DOI: [10.1109/CRISIS.2012.6378942](https://doi.org/10.1109/CRISIS.2012.6378942)
- [78] A. Nourian and S. Madnick, “A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet,” *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 1, pp. 2–13, Jan. 2018. DOI: [10.1109/TDSC.2015.2509994](https://doi.org/10.1109/TDSC.2015.2509994)
- [79] J. Tian, R. Tan, X. Guan, Z. Xu, and T. Liu, “Moving target defense approach to detecting Stuxnet-like attacks,” *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 291–300, Jan. 2020. DOI: [10.1109/TSG.2019.2921245](https://doi.org/10.1109/TSG.2019.2921245)
- [80] M. Long, C.-H. Wu, and J. Hung, “Denial of service attacks on network-based control systems: Impact and mitigation,” *IEEE Transactions on Industrial Informatics*, vol. 1, no. 2, pp. 85–96, May 2005. DOI: [10.1109/TII.2005.844422](https://doi.org/10.1109/TII.2005.844422)
- [81] A. Snoeren, C. Partridge, L. Sanchez, C. Jones, F. Tchakountio, B. Schwartz, S. Kent, and W. Strayer, “Single-packet ip traceback,” *IEEE/ACM Transactions on Networking*, vol. 10, no. 6, pp. 721–734, Dec. 2002. DOI: [10.1109/TNET.2002.804827](https://doi.org/10.1109/TNET.2002.804827)

- [82] R. C. Baishya and D. K. Bhattacharyya, "Singleton flow traceback (SFT) mechanism," in *2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP)*, Guwahati, Assam, India, Feb. 2020, pp. 139–148. DOI: [10.1109/ISEA-ISAP49340.2020.235012](https://doi.org/10.1109/ISEA-ISAP49340.2020.235012)
- [83] A. Y. Nur and M. E. Tozal, "Single packet as traceback against DoS attacks," in *2021 IEEE International Systems Conference (SysCon)*, Vancouver, BC, Canada, Apr. 2021, pp. 1–8. DOI: [10.1109/SysCon48628.2021.9447126](https://doi.org/10.1109/SysCon48628.2021.9447126)
- [84] M.-H. Yang, J.-N. Luo, M. Vijayalakshmi, and S. M. Shalinie, "Hybrid multilayer network traceback to the real sources of attack devices," *IEEE Access*, vol. 8, pp. 201 087–201 097, 2020. DOI: [10.1109/ACCESS.2020.3034226](https://doi.org/10.1109/ACCESS.2020.3034226)
- [85] A. A. Farooqui, S. S. H. Zaidi, A. Y. Memon, and S. Qazi, "Cyber security backdrop: A SCADA testbed," in *2014 IEEE Computers, Communications and IT Applications Conference*, Beijing, China, Oct. 2014, pp. 98–103. DOI: [10.1109/ComComAp.2014.7017178](https://doi.org/10.1109/ComComAp.2014.7017178)
- [86] R. S. Smith, "A decoupled feedback structure for covertly appropriating networked control systems," *IFAC Proceedings Volumes*, vol. 44, no. 1, pp. 90–95, 2011, 18th IFAC World Congress. DOI: [10.3182/20110828-6-IT-1002.01721](https://doi.org/10.3182/20110828-6-IT-1002.01721) [Online]. Available: [sciencedirect.com/science/article/pii/S1474667016435925](https://www.sciencedirect.com/science/article/pii/S1474667016435925)
- [87] R. S. Smith, "Covert misappropriation of networked control systems: Presenting a feedback structure," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 82–92, Feb. 2015. DOI: [10.1109/MCS.2014.2364723](https://doi.org/10.1109/MCS.2014.2364723)
- [88] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—part I: Analysis and experimentation of stealthy deception attacks," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 5, pp. 1963–1970, Sep. 2013. DOI: [10.1109/TCST.2012.2211873](https://doi.org/10.1109/TCST.2012.2211873)
- [89] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—part II: Attack detection using enhanced hydrodynamic models," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 5, pp. 1679–1693, Sep. 2013. DOI: [10.1109/TCST.2012.2211874](https://doi.org/10.1109/TCST.2012.2211874)
- [90] A. O. de Sá, L. F. R. d. C. Carmo, and R. C. S. Machado, "Covert attacks in cyber-physical control systems," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 4, pp. 1641–1651, Aug. 2017. DOI: [10.1109/TII.2017.2676005](https://doi.org/10.1109/TII.2017.2676005)
- [91] A. O. de Sa, L. F. R. da Costa Carmo, and R. C. S. Machado, "Bio-inspired active attack for identification of networked control systems," in *10th EAI International Conference on Bio-inspired Information and Communications Technologies (BICT, formerly BIO-*

- NETICS), Hoboken, New Jersey, USA: EAI, Mar. 2017. DOI: [10.4108/eai.22-3-2017.152407](https://doi.org/10.4108/eai.22-3-2017.152407)
- [92] L. Xin and Z.-Q. Long, “A learning-based passive resilient controller for cyber-physical systems: Countering stealthy deception attacks and complete loss of actuators control authority,” *IEEE/CAA Journal of Automatica Sinica*, vol. 12, no. 7, pp. 1368–1380, 2025. DOI: [10.1109/JAS.2024.124683](https://doi.org/10.1109/JAS.2024.124683)
 - [93] Q. Wang, Y. Qian, and A.-Y. Lu, “Data and model-based switching observer for cyber-physical systems against sparse sensor attacks,” *International Journal of Systems Science*, vol. 57, no. 1, pp. 1–13, 2025. DOI: [10.1080/00207721.2025.2486163](https://doi.org/10.1080/00207721.2025.2486163)
 - [94] W. Liu, J. Sun, G. Wang, F. Bullo, and J. Chen, “Data-driven resilient predictive control under denial-of-service,” *IEEE Transactions on Automatic Control*, vol. 68, no. 8, pp. 4722–4737, 2023. DOI: [10.1109/TAC.2022.3209399](https://doi.org/10.1109/TAC.2022.3209399)
 - [95] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, “A survey of moving target defenses for network security,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1909–1941, 2020. DOI: [10.1109/COMST.2020.2982955](https://doi.org/10.1109/COMST.2020.2982955)
 - [96] D. Gurung, M. Pradhan, and S. Gurung, “Towards understanding the applicability of runtime moving target defense for the Internet of Things and Cyber Physical Systems,” *Scientific Reports*, vol. 16, p. 5907, 2026, Article 5907. DOI: [10.1038/s41598-026-36797-4](https://doi.org/10.1038/s41598-026-36797-4) [Online]. Available: nature.com/articles/s41598-026-36797-4
 - [97] Swati, S. Roy, J. Singh, and J. Mathew, “Securing IIoT systems against DDoS attacks with adaptive moving target defense strategies,” *Scientific Reports*, vol. 15, no. 1, Mar. 2025, Art. no. 9558, Art. no. 9558. DOI: [10.1038/s41598-025-93138-7](https://doi.org/10.1038/s41598-025-93138-7)
 - [98] R. Canonico, F. Lista, A. Navarro, G. Sperli, and A. Vignali, “Threat detection in re-configurable cyber-Physical systems through spatio-temporal anomaly detection using graph attention network,” *Computers & Security*, vol. 156, 2025, Art. 104509. DOI: [10.1016/j.cose.2025.104509](https://doi.org/10.1016/j.cose.2025.104509)
 - [99] D. Kushner, “The real story of Stuxnet,” *IEEE Spectrum*, vol. 50, no. 3, pp. 48–53, Mar. 2013. DOI: [10.1109/MSPEC.2013.6471059](https://doi.org/10.1109/MSPEC.2013.6471059)
 - [100] M. Bhutani, S. Dalal, M. Alhussein, U. K. Lilhore, K. Aurangzeb, and A. Hussain, “SAD-GAN: A novel secure anomaly detection framework for enhancing the resilience of cyber-physical systems,” *Cognitive Computation*, vol. 17, p. 127, Jul. 2025, Article 127. DOI: [10.1007/s12559-025-10483-5](https://doi.org/10.1007/s12559-025-10483-5)

- [101] P. Moriano, S. C. Hespeler, M. Li, and M. Mahbub, “Adaptive anomaly detection for identifying attacks in cyber-physical systems: A systematic literature review,” *Artificial Intelligence Review*, vol. 58, p. 283, Jun. 2025, Article 283. DOI: [10.1007/s10462-025-11292-w](https://doi.org/10.1007/s10462-025-11292-w)
- [102] H. Yang, B. Yang, S. Coshatt, Q. Li, K. Hu, B. C. Hammond, J. Ye, R. Parasuraman, and W. Song, “Real-world cyber security demonstration for networked electric drives,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 13, no. 4, pp. 4659–4668, Aug. 2025. DOI: [10.1109/JESTPE.2025.3550830](https://doi.org/10.1109/JESTPE.2025.3550830)
- [103] S. Suprabhath Koduru, V. S. P. Machina, and S. Madichetty, “Cyber attacks in cyber-physical microgrid systems: A comprehensive review,” *Energies*, vol. 16, no. 12, 2023, Art. 4573. DOI: [10.3390/en16124573](https://doi.org/10.3390/en16124573)
- [104] P. Wlazlo, A. Sahu, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, “Man-in-the-Middle attacks and defence in a power system cyber-physical testbed,” *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 3, pp. 164–177, 2021. DOI: [10.1049/cps2.12014](https://doi.org/10.1049/cps2.12014)
- [105] Y.-A. WWang, Z. Wang, L. Zou, B. Shen, and H. Dong, “Detection of perfect stealthy attacks on cyber-physical systems subject to measurement quantizations: A watermark-based strategy,” *IEEE/CAA Journal of Automatica Sinica*, 2025. DOI: [10.1109/JAS.2024.124815](https://doi.org/10.1109/JAS.2024.124815)
- [106] J. Wang, Y. Liu, H. Yuan, and W. Yang, “Stealthy attack against distributed State Estimation for Cyber-Physical Systems,” *International Journal of Robust and Nonlinear Control*, vol. 35, no. 2, e7697, 2025. DOI: [10.1002/rnc.7697](https://doi.org/10.1002/rnc.7697)
- [107] J. Wei, J. Zhou, and T. Chen, “Integrity attacks on state estimation with varying data access: From visibility to full restriction,” *Automatica*, vol. 174, p. 112 162, 2025. DOI: [10.1016/j.automatica.2025.112162](https://doi.org/10.1016/j.automatica.2025.112162)
- [108] Q. Sun and G.-H. Yang, “Secure state estimation against fdi attacks and unknown disturbances: A descriptor reduced-order observer method,” *IEEE Internet of Things Journal*, vol. 12, no. 20, pp. 42 932–42 939, 2025. DOI: [10.1109/JIOT.2025.3595094](https://doi.org/10.1109/JIOT.2025.3595094)
- [109] X. Yu, C. Gao, Y. Du, B. Gao, D. Tian, and T. Hou, “Adaptive residual observer-based detection and isolation framework against false data injection attack in large-scale power systems,” *Scientific Reports*, vol. 15, no. 1, p. 4821, 2025. DOI: [10.1038/s41598-025-24992-8](https://doi.org/10.1038/s41598-025-24992-8)

- [110] C. Fei, J. Shen, H. Qiu, and Z. Zhang, “Data driven secure control for Cyber–Physical Systems under Hybrid Attacks: A Stackelberg game approach,” *Journal of the Franklin Institute*, vol. 361, no. 6, p. 106 715, 2024. DOI: [10.1016/j.jfranklin.2024.106715](https://doi.org/10.1016/j.jfranklin.2024.106715)
- [111] Y. Wang, W. Xing, J. Zhang, L. Liu, and X. Zhao, “Remote state estimation under dos attacks in cpss with arbitrary tree topology: A bayesian stackelberg game approach,” *IEEE Transactions on Signal and Information Processing over Networks*, vol. 10, pp. 527–538, 2024. DOI: [10.1109/TSIPN.2024.3394776](https://doi.org/10.1109/TSIPN.2024.3394776)
- [112] S. Krishna Niketh, S. Bhattacharya, A. Das, and S. Ray, *Game-theoretic resilience framework for Cyber-Physical microgrids using Multi-Agent Reinforcement Learning*, 2025. DOI: [10.48550/arXiv.2509.08310](https://doi.org/10.48550/arXiv.2509.08310) arXiv: [2509.08310](https://arxiv.org/abs/2509.08310) [eess.SY].
- [113] Z. Qin, H. Yu, Z. Yu, and S. Li, “Observer-based adaptive resilient control for nonlinear cyber-physical systems with unknown cyber-attacks: A self-triggered approach,” *International Journal of Robust and Nonlinear Control*, vol. 36, no. 3, pp. 1283–1298, 2025. DOI: [10.1002/rnc.70200](https://doi.org/10.1002/rnc.70200) [Online]. Available: <https://api.semanticscholar.org/CorpusID:281461287>
- [114] X. Fan, Y. Li, and S. Tong, “Finite-time fuzzy adaptive output feedback resilient control of nonlinear cyber-physical systems with sensor attacks and actuator faults,” *Journal of Systems Science and Complexity*, vol. 37, pp. 1545–1560, 2024. DOI: [10.1007/s11424-024-3401-z](https://doi.org/10.1007/s11424-024-3401-z)
- [115] A. Bali, M. Maaruf, U. P. Singh, A. Fekih, A. N. Abubakar, and M. Khalid, “Adaptive control of Nonstrict-Feedback Cyber-Physical Systems with unmodeled dynamics and False Data Injection attacks,” *International Journal of Control*, pp. 1–17, Oct. 2025. DOI: [10.1080/00207179.2025.2571931](https://doi.org/10.1080/00207179.2025.2571931)
- [116] Y. Chen, T. Li, Y. Long, and W. Bai, “Attacks detection and security control for cyber-physical systems under false data injection attacks,” *Journal of the Franklin Institute*, vol. 360, no. 14, pp. 10 476–10 498, 2023. DOI: [10.1016/j.jfranklin.2023.07.020](https://doi.org/10.1016/j.jfranklin.2023.07.020) [Online]. Available: [sciencedirect.com/science/article/pii/S0016003223004507](https://www.sciencedirect.com/science/article/pii/S0016003223004507)
- [117] D. Montoya-Acevedo, W. Gil-González, O. D. Montoya, C. Restrepo, and C. González-Castaño, “Adaptive speed control for a DC motor using DC/DC converters: An inverse optimal control approach,” *IEEE Access*, vol. 12, pp. 154 503–154 513, 2024. DOI: [10.1109/ACCESS.2024.3482982](https://doi.org/10.1109/ACCESS.2024.3482982)

- [118] E. D. Ayele, J. Ferreira Gonzalez, and W. B. Teeuw, “Enhancing cybersecurity in distributed microgrids: A review of communication protocols and standards,” *Sensors*, vol. 24, no. 3, 2024, Art. 854. DOI: [10.3390/s24030854](https://doi.org/10.3390/s24030854)
- [119] S. Tan, P. Xie, J. C. Vasquez, and J. M. Guerrero, “Developments, challenges and future opportunities in cybersecure microgrid control,” *Nature Reviews Electrical Engineering*, 2025. DOI: [10.1038/s44287-025-00189-z](https://doi.org/10.1038/s44287-025-00189-z)
- [120] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” in *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS)*, Chicago IL, USA, 2009, pp. 21–32. DOI: [10.1145/1653662.1653666](https://doi.org/10.1145/1653662.1653666)
- [121] Y. Mo and B. Sinopoli, “False data injection attacks in control systems,” in *Proceedings of the 1st Workshop on Secure Control Systems (SCS)*, ser. CPSWeek 2010, Held in conjunction with HSCC 2010, Stockholm, Sweden, Apr. 2010. DOI: [10.1109/CDC.2010.5718158](https://doi.org/10.1109/CDC.2010.5718158) [Online]. Available: <https://yilinmo.github.io/public/papers/scs2010.pdf>
- [122] R. Kumar and P. N. S. Prasad, “A review of mras-based speed estimation techniques for sensorless induction motor drives,” *IET Electric Power Applications*, vol. 9, no. 6, pp. 482–496, 2015. DOI: [10.1049/iet-epa.2014.0220](https://doi.org/10.1049/iet-epa.2014.0220)
- [123] L. Delorme, M. Ayala, O. González, J. Rodas, R. Gregor, and J. C. Hernández, “Speed sensorless control for a six-phase induction machine based on a sliding mode observer,” *Machines*, vol. 13, no. 8, p. 639, 2025. DOI: [10.3390/machines13080639](https://doi.org/10.3390/machines13080639) [Online]. Available: <https://www.mdpi.com/2075-1702/13/8/639>
- [124] R. Wightman, “An easy way for hackers to remotely burn industrial motors,” *Wired*, Jan. 2016, Journalistic report summarizing VFD parameter vulnerabilities discovered by security researchers (Digital Bond / Reid Wightman). [Online]. Available: <https://www.wired.com/2016/01/an-easy-way-for-hackers-to-remotely-burn-industrial-motors/>
- [125] M. G. Angle, S. Madnick, J. L. Kirtley, and S. Khan, “Identifying and anticipating cyberattacks that could cause physical damage to industrial control systems,” *IEEE Power and Energy Technology Systems Journal*, vol. 6, no. 4, pp. 172–182, 2019. DOI: [10.1109/JPETS.2019.2923970](https://doi.org/10.1109/JPETS.2019.2923970) [Online]. Available: web.mit.edu/smadnick/www/wp/2017-14.pdf

- [126] R. J. Somers, K. K. H. Leung, and A. J. R. B. P. Silva, “Digital-twin-based testing for cyber–physical systems: A review and research agenda,” *Information and Software Technology*, vol. 148, p. 107 022, 2023. DOI: [10.1016/j.infsof.2023.107022](https://doi.org/10.1016/j.infsof.2023.107022) [Online]. Available: sciencedirect.com/science/article/pii/S0950584922002543
- [127] F. Karami and J. Poshtan, “Detection of broken rotor bars in induction motors using an unscented Kalman filter,” *Mechanical Systems and Signal Processing*, vol. 24, no. 5, pp. 1748–1759, 2010. DOI: [10.1016/j.ymssp.2009.12.006](https://doi.org/10.1016/j.ymssp.2009.12.006) [Online]. Available: sciencedirect.com/science/article/pii/S0888327009004423
- [128] R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, May 2011. DOI: [10.1109/MSP.2011.67](https://doi.org/10.1109/MSP.2011.67)