A Design and Evaluation of a Secure Neighborhood Awareness Framework for Vehicular Ad-Hoc Networks

by

Osama Abumansoor

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements
for the Doctorate in Philosophy degree in
Electrical and Computer Engineering

Ottawa-Carleton Institute for Electrical and Computer Engineering
Faculty of Graduate and Postgraduate Studies
University of Ottawa

Abstract

Vehicular ad-hoc networks (VANETs) are envisioned to provide many road and safety applications that will improve drivers' awareness and enhance the driving experience. Many of proposed applications are location-based that depend on sharing the location information of vehicles and events among neighboring nodes. The location-based applications should provide vehicle operators with knowledge of the current surrounding conditions to help them make appropriate traveling decisions, such as avoiding traffic congestion. Drivers expect to receive accurate and reliable information from other vehicles. Therefore, securing localization service integrity is important to support a VANET's overall system reliability. In this thesis, we study the exchanged location information in VANETs and designed a framework to prevent potential security threats that will violate users' privacy and overcome limitations that can impact the exchanged data integrity and reliability. The solution developed a secure neighborhood awareness service and shared localization information management protocol in a VANET. The proposed framework is constructed through several components: (i) a location verification protocol that will secure location information by providing a non-line-of-sight (NLOS) verification protocol to overcome moving obstacle effects; (ii) privacy-preserving location information management to detect data inconsistency and provide a recovery process while preventing attackers from tracking individual vehicles; (iii) a trust model evaluation mechanism based on neighborhood awareness; (iv) an adaptive beacon protocol that will reduce the number of messages and provide quality of service(QoS) control for network managers and authorities. We also propose a security evaluation model that quantifies the security attributes for the localization service in a VANET. The model will help evaluate an integrated security measures that are provided by different components of the network services.

Acknowledgements

This work would not have been possible without the support of many people. I offer special thanks to my supervisor, Prof. Azzedine Boukerche. His guidance, encouragement, and trust in my abilities have helped me to overcome many obstacles that I have encountered during my studies. It was an honor to work under his supervision.

It was a pleasure to work among a supportive team and friends at the PARADISE Research Lab at the University of Ottawa.

I would like to acknowledge the financial support of the Saudi Arabian Ministry of Higher Education, the King Abdullah Scholarship Program, and the Natural Sciences and Engineering Research Council of Canada (NSERC) Developing Next Generation Intelligent Vehicular Networks and Applications (DIVA) Network.

I would like to thank all my family and friends back home for their support and encouragement. I thank my brothers and sisters for their help, love, and support. I would like to dedicate my work to my parents, Hayat Felemban and Dr. Sabri Abumansoor, for their prayers, continuous support, and endless love. I would like to express my love and gratitude to my wife, Nesreen Abourokbah, for her endless support, encouragement, and understanding during my studies. Finally, I offer a special dedication to my children, Yazan and Rimas, for adding sweet spice to my life.

Related Publications

The following publications by the author are relevant to this thesis:

Journals :

1. O. Abumansoor and A. Boukerche, "A Secure Cooperative Approach for Non Line-of-Sight Location Verification in VANET," *IEEE Transactions on Vehicular Technology,* vol. 61, no. 1, pp. 275–285, Jan. 2012.
2. O. Abumansoor and A. Boukerche, "A Privacy-Preserving Location Information Exchange Framework for Vehicular Ad-Hoc Networks," submitted to *Ad Hoc Networks Journal.*

Conferences :

1. O. Abumansoor and A. Boukerche, "A cooperative multi-hop location verification for Non Line Of Sight (NLOS) in VANET", in *Proceeding IEEE Wireless Communications and Networking Conference (WCNC)*, Cancune, Mexico, Mar. 2011, pp. 773–778.
2. O. Abumansoor, A. Boukerche, B. Landfeldt, and S. Samarah, "Privacy preserving neighborhood awareness in vehicular ad hoc networks," in *Proceedings of the 7th ACM symposium on QoS and security for wireless and mobile networks (Q2SWinet),* Miami, Florida, Oct. 2011, pp. 17-20.
3. O. Abumansoor and A. Boukerche, "Towards a Secure Trust Model for Vehicular Ad Hoc Networks Services," in *Proceeding IEEE Global Telecommunications Conference (GLOBECOM),* Houston, Texas, Dec. 2011, pp. 1–5.
4. O. Abumansoor and A. Boukerche, "Preventing a DoS Threat in Vehicular Ad-Hoc Networks Using Adaptive Group Beaconing," in *Proceeding of the 8th ACM symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet),* Paphos, Cyprus, Oct. 2012, pp. 1–8.

Contents

List of Tables

List of Figures

Glossary of Terms

AoA Angle of Arrival.

AGB Adaptive Group Beaconing.

BAM Building Attenuation Model.

BDAM Building and Distance Attenuation Model.

CA Certificate Authority.

CH Cluster Head.

CEDAR Core Extraction Distributed Ad Hoc Routing.

CMLVP Cooperative Multi-hop Location Verification Protocol.

CSMA Carrier Sense Multiple Access.

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance.

CVIS Cooperative Vehicle Infrastructure Systems.

DAM Distance Attenuation Model.

DCR Dynamic Channel Reservation.

DGPS Differential Global Positioning System.

DLP Density-based Location Privacy.

DTMC Discrete-Time Markov Chain.

ECDSA Elliptic Curve Digital Signature Algorithm.

ECIST European Commission Information Society Technologies.

EGNOS European Geostationary Navigation Overlay Service.

FRB Fixed Rate Beaconing.

GFM Greedy Filtering Matrix.

GIS Geographic Information System.

GloMoSim Global Mobile Information System Simulator.

GPS Global Positioning System.

IDS Intrusion Detection System.

LAD Location Anomaly Detection Protocol.

LOS Line-Of-Sight.

MAC Media Access Control.

MANET Mobile Ad-Hoc Network.

MBS Mobile Base Station.

MTTSF Mean Time to Security Failure.

NLOS Non-Line-Of-Sight.

NS-2 The Network Simulator, version 2.

OBU On-Board Unit.

OC-MAC Optimal Congestion and Medium Access Control

ODAM Optimized Dissimilation of Alert Messages.

PKI Public Key Infrastructure.

POMA Positioning, Mapping and Location Referencing.

QoS Quality of Service.

QVANO QoS for Highly Dynamic Vehicle Ad-Hoc Network.

ROPE Robust Position Estimation Protocol.

RSSI Radio Signal Strength Index.

RSU Road Side Unit.

SAR Sequential Assignment Routing.

SMP Semi-Markov Process.

SNR Signal to Noise Ratio.

TDMA Time Division Multiple Access.

TDoA Time Difference of Arrival.

ToA Time of Arrival.

ToF Time of Flight.

V2I Vehicle-to-Infrastructure communication.

V2V Vehicle-to-Vehicle communication.

VANET Vehicular Ad-Hoc Networks.

WAAS Wide Area Augmentation System.

WiFi Wireless Fidelity.

WSN Wireless Sensor Networks.

Z-MAC Zebra - Medium Access Control.

Chapter 1

Introduction

1.1 Background

Vehicular ad-hoc networks (VANETs) are envisioned to provide on-demand wireless communication infrastructure among vehicles and with the network authorities. The network will have two types of nodes: vehicles that will be equipped with sensors and communication devices that are consolidated in an on-board unit (OBU) and road-side units (RSUs) that present the fixed infrastructure that is linked to a management network and authorities, such as traffic police. Communication among vehicles is referred to as vehicle-to-vehicle communication (V2V) while vehicle to RSU communication is referred to as vehicle-to-infrastructure (V2I). Both communication links use a dedicated short-range communications (DSRC) spectrum and the 802.11p Wireless Access in Vehicular Environment (WAVE) operation stack [28, 33]. In the US, a 75MHz spectrum in the 5.9GHz band has been allocated by the Federal Communication Commission (FCC) for the use of intelligent transportation systems (ITS). In Europe, a 30MHz spectrum at 5.9GHz was allocated by the European Telecommunication Standard Institute (ETSI) for the same system.

The infrastructure setup will allow vehicles to cooperate with each other and with authority units to disseminate and exchange various road applications' messages. For example, warning messages and traffic management instructions can be broadcasted to increase drivers' awareness of potential travel hazards, allowing them to respond earlier to avoid traffic congestion and collisions or to clear the way for in-bound emergency response units (Figure 1.1). Researchers have envisioned more applications to be used in VANET such as [9, 27, 34, 39]:

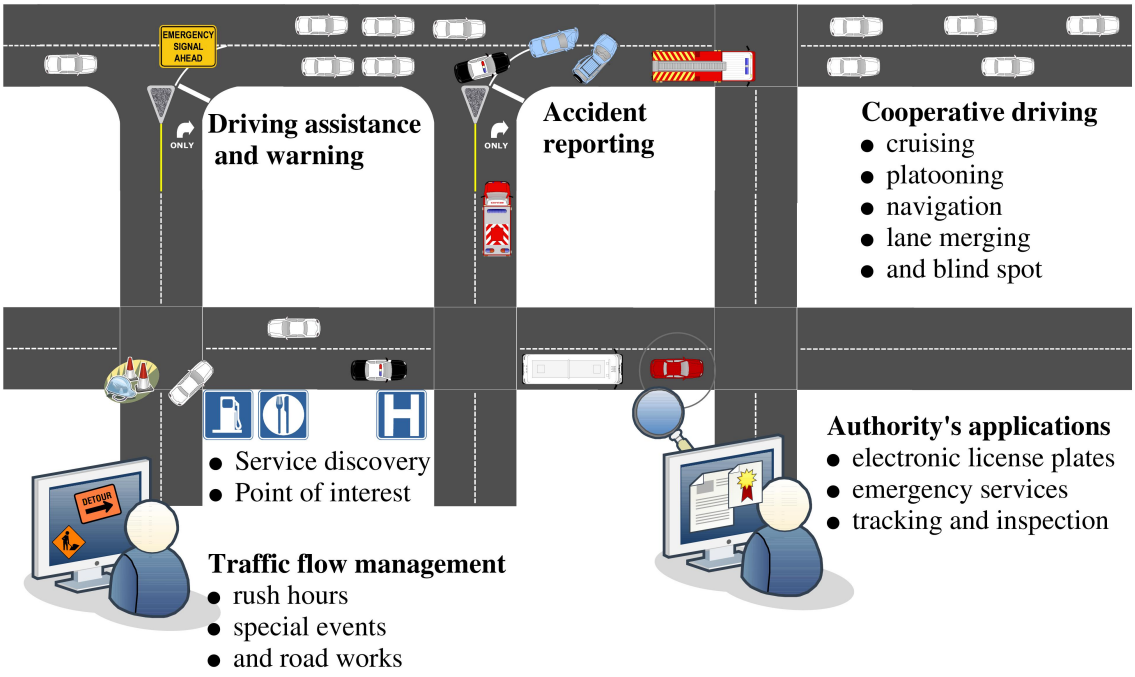


Figure 1.1: Multiple applications are envisioned for VANET.

- Cooperative driving assistance and warning
- Authorities' applications, such as electronic license plates (ELPs), emergency response services, accident data recording, vehicle tracking, and inspection
- Traffic flow management under different road conditions and events, such as rush hour, emergency operations, and road work
- Vehicle navigation, cruising, and platooning
- Passenger entertainment and comfort, such as instant messaging, Internet access, or a guide to points of interest
- Commercial applications, such as sales vehicle tracking, rentals, cargos, and advertisement content distribution.

Many of these promising applications require the knowledge of current event and neighboring vehicles' location information. A vehicle can determine its location using existing technologies such as global positioning systems (GPS) [35], map matching [9],

dead reckoning [9], cellular localization [94], image and video processing [10], and relative positioning [5].

Position information is exchanged among neighboring vehicles through frequent messaging such as beacons, group updates, or peer-to-peer messages. Such a communication method is subject to interference caused by obstacles or security threats that introduce false data. To secure VANET services and applications, researchers have proposed solutions to protect the network from security attacks and vulnerabilities. Researchers have identified attacks such as Sybil attacks, reply attacks, and wormhole attacks, and proposed several solutions and security frameworks to protect the network from such attempts [51, 64, 74, 81]. Other studies have presented solutions to handle localization errors and false data acquisitions [63]. A data fusion model was presented to combine diffident techniques to compute an accurate estimation of a vehicle's location to improve security measures and computation accuracy [9].

Each ad-hoc network has its own security requirements and service objectives. In wireless sensor networks (WSN), for example, secure localization and location verification were discussed to detect and isolate nodes that failed to estimate their own positions or were a source of false data [8]. In VANETs, vehicle operators will change their driving behavior based on received service information. Therefore, accurate and consistent data about surrounding vehicles' location is essential. Thus, a secure neighborhood awareness service VANET will help to meet such requirements and provide vehicles with verified information rather than ignoring the existence of a vehicle.

An example of such a demand can be described for a tracking application for authority vehicles (Figure 1.2). In the case where a law enforcement vehicles (E1 and E2) are pursuing a subject vehicle (A), with obstacles such as trucks and busses, authority vehicles may not receive constant updates from the subject vehicle. It will be very helpful for an authority to be able to track their subjects and determine whether it followed its predicted path or made a sudden change. With such information, the authority will have advantage over a run-away vehicle and help them to position themselves to reduce the time needed to stop and control the subject vehicle.

1.2 Study Motivation

Enabling each vehicle to determine its location is necessary in VANET, but they also need to have the information about the events of their surroundings and proximal vehicles. It is important to improve and maintain drivers' neighborhood awareness and to

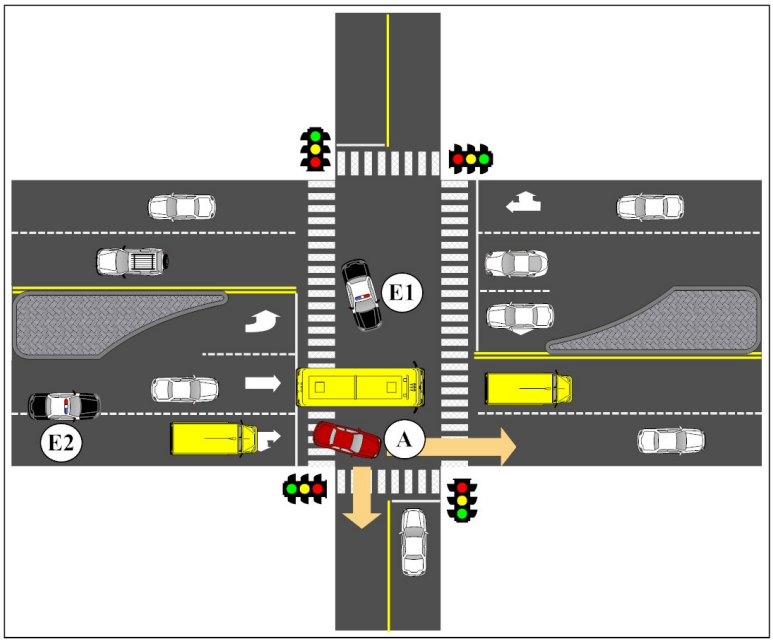


Figure 1.2: Secure neighborhood awareness provides VANET applications with helpful information by acquiring the current location state and overcoming data inconsistency.

develop reliable and secure localization information sharing protocols. However, such a goal faces a number of challenges. In addition to the challenges raised by the nature of the network (e.g., mobility, radio propagation, obstacles, etc.) that the researchers must deal with to develop an accurate and reliable localization system, it can be the target of security attacks that can compromise and disturb applications functionality. For example, an attacker may broadcast false location information to convince his neighbors that his vehicle is the best relay point for their messages, therefore hijacking their messages and collecting their information. Such an attempt can affect routing protocols, causing delays, packet drops, and loops [47].

Many location-based services and applications in a VANET rely on vehicles' current positions, which make it a target for attackers and malicious nodes. Attackers will keep investigating for system flaws, limitations, and security breaches, and with a wide-spread network and the neighborhood awareness-range that exceeds the human natural capabilities, attackers may use position information in their favor. In this thesis, we identified several potential threats that will affect localization services and the availability of exchanged location information among vehicles, thus risking the reliability and integrity of VANET-delivered applications. The study will focus on the following issues:

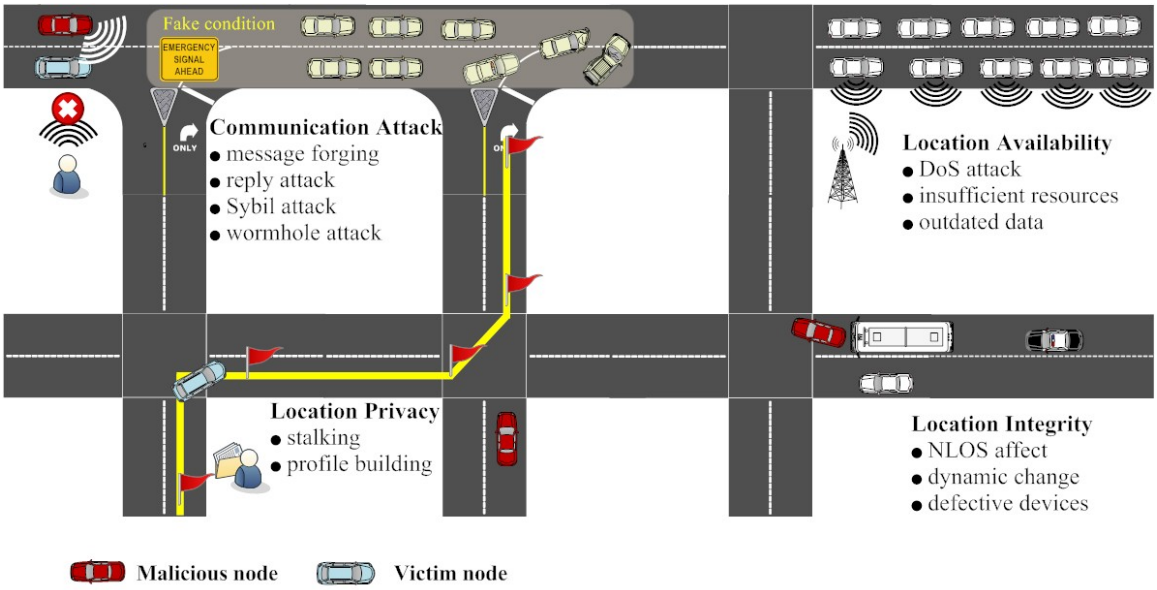


Figure 1.3: Security threats that can affect location-based applications in VANET.

- *Location verification under non-line-of-sight (NLOS)*: In VANETs, many objects such as buildings, trees, and other constructions that exists on roadsides can interfere or block radio signals [85]. Moreover, moving objects on the roads can also cause signal block. As vehicles come in different shapes and sizes, they can become an obstacle between neighbors that are in the same region of communication (Figure 1.4). Unlike buildings and fixed structures where interference and signal quality factors can be measured in the field and be taken into consideration, it is difficult to measure and average the signal errors because of vehicle shapes (e.g, trucks and buses), mobility, formation, and density. Several verification protocols for secure localization rely on direct communication between a vehicle and the node being verified. We propose a novel protocol that verifies a vehicle-announced location using a multi-hop cooperative approach when direct verification and communication is not possible.

- *Trust evaluation of neighboring nodes*: Current solutions depend on evaluating the trustworthiness of a neighboring node by its behavior toward a certain event or its participation in message forwarding. In both cases, the results depend on how often events occur or message routing is required. Moreover, in an obstructed environment, a NLOS condition may give the impression that a neighbor is a malicious node, as it will fail to respond to message forwarding or event reporting. This will

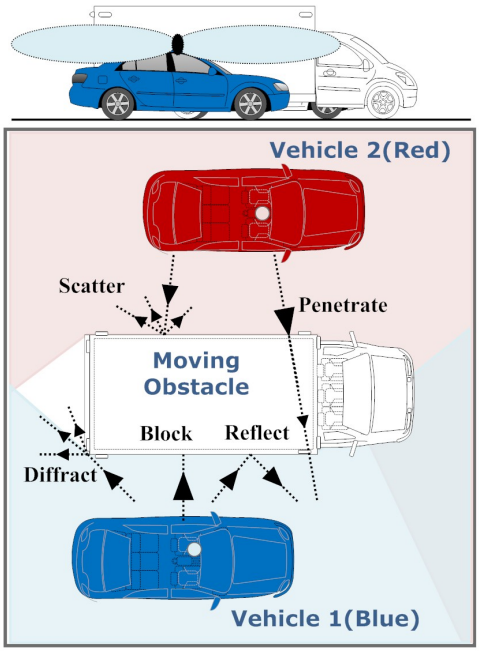


Figure 1.4: Moving obstacles can prevent from establishing direct communication among neighboring vehicles.

lead vehicles to evaluate the trustworthiness of others unfairly. Our objective is to increase security measurements, system integrity, and awareness by developing a trust model and introducing an evaluation attributes that allows vehicles to be aware of their neighbors' availability and reliability under NLOS conditions. With such a model, many applications and services can predict a node's behavior in response to various events.

- *QoS provisioning*: With the increased number of vehicles on the roads and expanding road network, authorities will require control of broadcasts to secure network resources for safety and warning messages. Current QoS solutions focus on providing routing protocols to guarantee resources for message senders or providing MAC layer scheduling and adaptive rate control to avoid packet collision. Therefore, each node adjusts its transmission behavior based on its preset detection mechanism that does not allow external control from an authority. Our objective is to improve QoS provisioning by improving the availability of exchange location information using adaptive group beaconing (AGB) and allowing authorities to gain control of the beacon rate of vehicles and offering access to network resources for critical applications.

- *Vehicles' privacy*: Current security frameworks apply digital signatures to secure exchanged messages and enable message receivers to authenticate the sender. In these frameworks, the users' identities are protected through the use of pseudonym keys that are frequently changed to avoid linking a group of messages to a single sender. This approach will protect the privacy of users during message exchange. However, once the sender is authenticated, the message data is available and an attacker can gain access to them using a compromised node, for example, by accessing his own vehicle's OBU. The vehicle ID, such as an electronic license plate (ELP), is a unique identifier. Frequent broadcasts of such information make it easier for a stalker to detect and follow a targeted vehicle. For example, an attacker depends on his visual abilities to detect, track, and stalk a subject vehicle. With the implementation of a VANET, an attacker will attempt to use the technology's features in his favor. With a successful attack, the stalker will be able to detect, track, and record a subject vehicle within its communication range that, by far, exceeds his visual range and individual abilities. To enhance privacy protection when exchanging location information, it is necessary to protect the beacon context itself, making the collected data useful for building awareness of neighboring vehicles but useless for building a travel profile. Our objective is to provide a solution and develop a privacy-preserving protocol to exchange and handle location information without revealing the identity of a vehicle. However, this will be difficult to manage because a vehicle will then receive many beacon messages without being able to identify the sender because listing neighboring vehicles in a table format will make it difficult to segregate them from each other. Moreover, a vehicle cannot determine whether the newly received beacon is an update of current information or a new vehicle record.

- *Secure neighborhood awareness service*: Many VANET applications are location-based and require a secure single source of neighboring vehicles and their location information. Consolidating the related components in a single service is essential for a VANET. The service will receive and handle location information and provide secure and reliable position and mobility data for safety applications and services such as routing protocols. Securing a single service will help future development and eliminate security breaches caused by multiple developments for multiple applications. Our objective is to consolidate all proposed solutions in a service model and provide a guideline for future development paths.

- *Security Evaluation Model*: VANET will be developed using many services and protocols. Each service will have its own deliverable and security countermeasures. Many of the proposed solutions discuss their security aspects as a qualitative value. The evaluation of many security countermeasure is based on common sense and previous encounter of similar problems in familiar technologies and networks. It is important to have an analytical approach to quantify the security attributes that the proposed system and its components can deliver. Such a model will help evaluate and estimate the optimal security measures the solution can provide.

1.3 Research Challenges

Securing applications and services in a VANET faces many challenges that need to be addressed. To develop a secure neighborhood awareness, it is important to overcome challenges that are brought by the characteristics of the network and human behavior such as:

1. *Moving obstacles and NLOS:* In addition to radio signal fading and interference that affects wireless communications, moving obstacles such as trucks can impact communication among vehicles. Since vehicles come in different shapes and sizes, they can act as obstacles between neighbors in the same communication range. Moving obstacles with different shapes, speeds, composition, and density can create a NLOS state that changes on an unpredictable temporo-spatial basis and could prevent a vehicle from receiving consistent updates and location information from its neighbors.

2. *No centralized security management system:* Since vehicles travel with unlimited geographic boundaries in traveling from one city to another, they do not have access to security management servers at all times. Each vehicle has to depend on itself and the help of neighboring vehicles to evaluate its data and local system integrity. Moreover, a centralized approach to verifying all messages will overload the authenticating servers and exhaust network resources.

3. *Privacy protection:* Preserving vehicle privacy is a major requirement. Private property vehicles will be equipped with communication devices. Future users will demand the protection of their identity, location, and activity. With the number of messages exchanged among vehicles, it is essential to prevent anyone from linking

messages to a specific user or use collected data to build a traveling profile of a targeted vehicle. The success of VANET implementation and all its applications can be jeopardized if user privacy is violated.

4. *Vehicles' mobility:* A VANET differs from other wireless and ad-hoc networks by its node speed and mobility, which are influenced by driver behaviors and strict movement that are limited by road boundaries and traffic rules. Moreover, vehicle movement is affected by events, weather, and time conditions, which keep the network topology in state of continuous change. In a wireless environment, mobility makes it difficult not only to track vehicles but also to access and maintain network resources.

5. *Modeling and simulations:* Simulation is an important stage of the evaluation process. Realistic modeling of a VANET environment is desired to present practical solutions for future implementations. Current network communication simulators (such as NS-2) supports three types of radio propagation models: free space, two-ray ground reflection, and shadowing propagation. These propagation models do not fulfill our requirements to simulate our protocol because they are used for line-of-sight (LOS) communication between wireless nodes. For our work, we need to simulate obstacles that present road vehicles with their own mobility and object dimensions.

6. *Nodes evaluation and trustworthiness:* Vehicles need to evaluate the trustworthiness of their neighboring nodes. However, the rapid change of network nodes makes it difficult to differentiate between misbehaving node and a node disconnected by obstacle interference or a sudden change in position and direction.

7. *Human nature to look for flaws:* Future end users will eventually discover additional technological limitations through practical encounters with inconsistencies and failures. Human behavior can be observed in its interaction with previous technology implementations. For example, the effects of human-system interactions is notable in wireless LAN and cellular phone network growth, such as when people notice communication limitations or signal interference issues in areas where public services are provided.

1.4 Thesis Contributions

Securing VANETs' applications and recovery from false data is important to improve the network deliverables and application liability. To meet such a requirement, secure neighborhood awareness service will not only validate the location of nodes but also provide the application with the current location status of neighboring vehicles, which will improve location-based application performance as well.

Our study objective is to identify potential threats that can affect the credibility and integrity of shared localization information and provide neighborhood awareness in a VANET while maintaining vehicle privacy. Moreover, we will integrate the proposed protocols and build a secure neighborhood awareness service for vehicles. The proposed solutions provide a secure source of information for location-based applications thus supporting a secure infrastructure for VANET services operating at the network layer. The main contributions of this thesis are as follows:

1. *Cooperative multi-hop location verification protocol (CMLVP):* We discuss the importance of location information and define an adversary model that will affect location-based applications. Current verification protocols require direct communication with subject vehicles. A NLOS condition prevents existing protocol from being executed. Our proposed location verification protocols is a cooperative approach that enables a vehicle to request assistance from its neighbors to verify a questioned vehicle to overcome the NLOS condition and the failure of direct verification. To evaluate the proposed solution, we developed an obstacle model to simulate obstacle interference in direct communication between two vehicles. Current solutions do not support moving obstacle signal propagation and interference. The model was implemented on the network simulator NS-2.

2. *Adaptive group beaconing (AGB) protocol:* Frequent message broadcasting of location information will result in high bandwidth consumption, especially in dense areas. In this thesis, we developed an adaptive group beaconing protocol that utilizes neighborhood awareness and cooperating nodes to adjust the beacon rate and other content of the beacon messages. The protocol evaluates neighboring nodes' trustworthiness to request the forwarding of location data for neighbors under NLOS conditions. Through the adaptive group beaconing solution, authorities and network service providers can provide critical applications and users with a level of QoS by allowing the controlled periodic message rate and content to reduce

the number of outgoing messages. In dense areas, emergency vehicles can request that vehicles change to an adaptive mode and reduce network resource utilization to guarantee enough resources for potential safety and emergency applications, thus allowing critical applications to access network resources.

3. *Neighborhood awareness service:* To enhance security measures, we introduce a consolidation of the proposed protocols in a single service model. The service model will handle received location information from neighboring nodes and provide position data for location-based applications and services. Future developed applications can obtain location information from the secure neighborhood awareness services. The service includes a trust model that considers the vehicles' location and communication status.

4. *Privacy preserving data management:* To protect the privacy of vehicles. We discuss the fact that the use of a vehicle identifier in beacon messages should be eliminated. Current studies assume the trustworthiness and safety of exchanging vehicle identification among the network members. Such an assumption is no longer acceptable due to privacy threats. We propose location information handling by vehicles using a grid map and indicating cell occupancy. The solution does not require node identifiers to be attached to location data.

5. *Trust evaluation model:* Current trust evaluation models for VANETs are based on evaluating the received messages and the behavior of nodes toward the assigned message relay [110, 115]. With NLOS conditions, message may not be received as expected. Therefore, a fair evaluation of a neighboring node may not be possible. In this thesis, we developed a trust evaluation model that takes into consideration NLOS conditions and location verification results to provide practical and fair trust evaluation of neighbors.

6. *Quantified Security Evaluation Model:* We developed a security analysis and evaluation model that will present the system's security attributes as quantified values. The model is based on a semi-Markov Process (SMP) to compute the confidentiality, integrity and availability security attributes. The model will help evaluate the system security measures and find the optimal solution the system can provide using different service components.

1.5 Thesis Structure

The remainder of this thesis is organized as follows:

- *Chapter 2*: Discusses related studies and proposed solutions for securing and handling location information. The literature review includes a discussion about localization techniques, security frameworks, location verification techniques, and privacy issues.
- *Chapter 3*: Presents the location verification protocol proposed to allow vehicles to verify a questioned node that cannot be reached through direct communication.
- *Chapter 4*: Presents a QoS provisioning using an adaptive group beaconing method that utilizes neighborhood awareness service data to adjust the beacon rate and content.
- *Chapter 5*: Presents the neighborhood awareness service and model. The privacy and security of location information exchange will be discussed, and a solution will be presented for a privacy-preserving awareness and data management and trust evaluation model that takes into consideration NLOS conditions.
- *Chapter 6*: Presents a security analysis model which defines and quantifies the security attributes for the location-information sharing process.
- *Chapter 7*: Presents the conclusion of the study and discusses future work that can be conducted to improve and apply the secure neighborhood awareness service to support VANET applications and its security measures.

Chapter 2

Literature Review

Vehicular ad-hoc networks (VANETs) are evolving due to its promising applications that will increase road safety and improve the driving experience. Securing the network services and application was the focus of many research activities. In this chapter, we will discuss related studies and proposed solutions to secure location information exchanged among vehicles. The discussion will be divided into several sections that focus on location data acquisition and location security aspects and how it can affect location information exchange in VANETs as well as development issues.

2.1 Localization Techniques

The first step to secure location information is to understand the source of location data and how a vehicle can determine its position. Several technologies are used to determine the position of an object in a wireless environment. Most of them proposed localization algorithms for mobile ad-hoc and wireless sensor networks. Furthermore, they are also used to develop localization systems for VANETs. However, each technique has advantages and disadvantages that should be taken into consideration in application design. Moreover, security concerns are also present and have to be evaluated. In this section, we will briefly discuss various localization techniques that are suggested for VANETs and highlight their security risks and concerns (Figure 2.1).

2.1.1 Global Positioning System (GPS)

Nowadays, GPS devices are handy and popular. GPS devices can calculate their position based on satellite signal information. Around 24 satellites are orbiting the earth

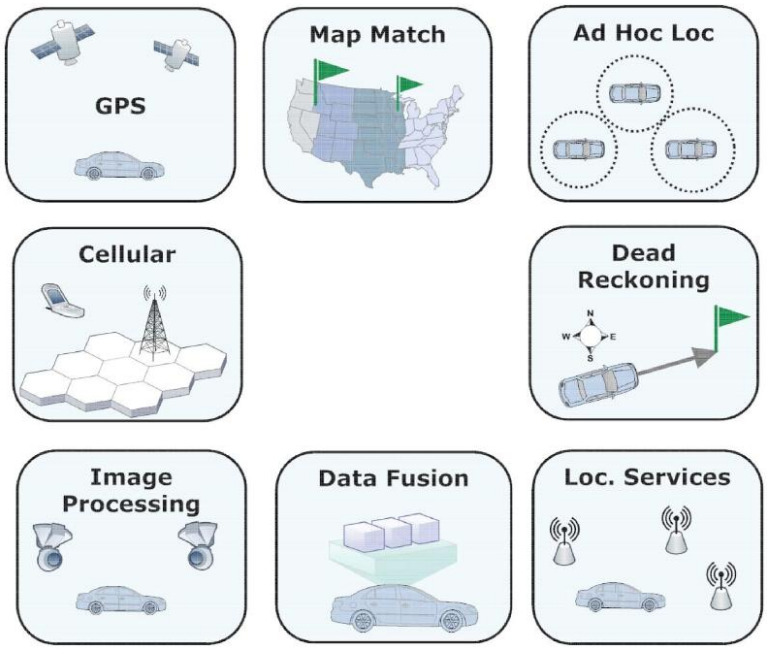


Figure 2.1: Localization techniques used in VANETs.

such that any region can receive signals from at least four satellites. GPS devices determine their physical position coordinates (i.e. latitude, longitude, and altitude) based on time-of-arrival (ToA) technique and multilateration computation [9, 83, 35].

Localization errors in GPS receivers can reach 10 to 30m. Nearby GPS devices tend to have the same calculated error as they all receive the same signal. There are a couple of solutions to resolve this problem. Using differential GPS (DGPS) may reduce the errors to a couple of meters. Fixed landmarks with predetermined localization information are equipped with GPS devices to compute their position based on satellite signals. The landmarks will then compute the difference between the calculated and the actual position. The calculated difference will then be distributed as an error correction to nearby devices. To implement DGPS, landmarks should be installed in various locations so that GPS devices can receive their signals at all times, which will add a significant cost to the infrastructure implementation.

Another solution to reduce GPS errors is to use an augmentation system such as wide area augmentation system (WAAS) and the European Geostationary Navigation Overlay Service (EGNOS), where correction values are being sent to GPS satellites from earth monitoring stations. The satellites augment the error correction information with

GPS information. GPS devices that support augmented data can extract the correction information and calculate their position with fewer errors, reaching sub-meters [9, 35, 83].

One of the major limitations of GPS is that devices depend on continuous receiving of satellite signals. The device needs to be able to receive signals from at least four satellites to calculate its position in a three-dimensional space. Although the satellites are orbiting the earth so that any site can receive signals from four to 11 different satellites, some conditions and obstacles may block the signals from reaching the receivers. Traveling through tunnels, canyons, valleys, and even urban areas with high-rise buildings may block the signal.

Localization system in VANETs should provide continuous knowledge of vehicle position. Loss of signal can affect the availability and integrity of the system. Moreover, indoor and closed areas, such as parking lots, cannot receive satellite signals. However, based on the fact that GPS devices are most popular among drivers and many vehicles are already equipped or being manufactured with pre-equipped devices, many proposed solutions for localization in VANETs have suggested the use of GPS systems or collaboration with vehicles equipped with GPS devices to estimate their position[5]. Such a solution can be acceptable for certain applications. However, the accuracy of a calculated position and the reliability of signal availability may not be suitable for most critical applications.

2.1.2 Map Matching

Map matching is not considered a localization system by itself, but is commonly used to correct and verify calculated position information from other techniques such as GPS. It compares road map data with the computed position and adjusts the position values to match the road coordinates where the vehicle is traveling.

Map data are collected and stored in devices using geographic information systems (GIS). The stored data includes road coordinates, landmark locations, zip codes, and other parameters that can be added through GIS. It became possible to store city maps and even world maps on simple portable devices. Map matching and map knowledge can also be used to plan trips by creating a trajectory from several points over time and comparing it with map information to find a traveling path geometry that matches the estimated trajectory [9, 83].

2.1.3 Dead Reckoning

Using this technique, a node can calculate its current position based on a previous known position and its mobility. The last known position can be determined by other techniques such as GPS or a position relative to a landmark. Mobility parameters such as speed, acceleration, time, direction, and distance can be obtained from attached sensors such as digital compasses and odometers. With the gathered information, the current position can be calculated and a predicted trajectory location can be estimated.

Dead reckoning can be used in VANETs for a short period of time when a GPS signal is unavailable or along with map matching [9]. Due to accumulating errors, it cannot be used for a long period of time. For example, in 30sec, a vehicle traveling in 100km/h can reach an error of 20m. Dead reckoning is used with GPS to calculate the position during a signal outage for a short period of time.

2.1.4 Cellular Localization

Cellular phone networks are widespread in many regions. Base stations are installed to cover a geographic area (cell) and provide communication to cell phones in their coverage area. The phone connects to the nearest base station based on the signal strength. During mobility, the phone communication changes from one station to another (handover) when it receives a stronger signal [9, 69, 105].

The cellular infrastructure can keep track of cell phone locations. Several methods are used to estimate their location. One method is using the received signal strength indicator (RSSI) to estimate the distance to the base station [69]. Another method is calculating the signal traveling time from a phone to the base station, known as time-of-arrival (ToA), or the time difference between the signal received from multiple stations, known as time-difference-of-arrival (TDoA) [69]. Position calculation is then done using multilateration computation. To use a signal traveling time method, an accurate time synchronization between nodes is required. Other methods are also used, such as angle-of-arrival (AoA) using directed antenna [69] and radio signal fingerprinting [9, 13].

Although tracking and localization in cellular networks are available[94], they are not suitable for all VANET applications. As discussed in [9], the average localization error is between 90–250m in an outdoor environment. However, localization information from cellular networks along with information from other techniques such as dead reckoning and map matching can be useful for calculation verification and correction.

2.1.5 Image and Video Processing

Image and video processing can be used to analyze objects and provide data for localization systems. Images from surveillance camera in parking areas, for example, can be used to determine vehicle location and help guide vehicles to find a parking spot[9]. On the other hand, vehicles equipped with camera sensors can analyze certain landmarks to calculate vehicle position with reference to these landmarks.

Chapuis et al.[11] proposed an algorithm to detect and recognize street-lane sides and highway marks captured from an on-board camera. The algorithm can calculate the vehicle position relative to the lane sides and also compute the lane width and street angle and curvature. Challita et al.[10] also proposed a localization protocol that combines GPS readings with a vision system. During a GPS outage, using a mounted camera, the vision system calculates the distance from the front car. By using a previous GPS reading, trajectory information, particle filtering, and vision system data, the vehicle can compute its current position. Fang et al.[19] proposed another localization system using video processing. Their image data consisted of ground texture information processed from a camera installed under the vehicle. Ferreira et al.[20] used image processing to detect and recognize the license plates of other vehicles to help locate the position of vehicles sought by the authorities.

Although image and video processing techniques can be reliable in some cases as it deals with recent data, it could be vulnerable to many environmental effects such as smoke, light illumination, and weather conditions. Moreover, a training phase is required to teach the system about different objects that may be recognized in the image when a new environment or artifacts are introduced.

2.1.6 Localization Services

Localization services can be provided through a separate infrastructure where terminals with wireless access units can broadcast localization information to neighboring nodes. Several localization algorithms were proposed as a solution to provide position information using known infrastructure such as the Cricket localization-support system[70], RADAR[3], ultra-wideband localization[44], and WiFi localization[14, 101]. The main approach for most solutions is to compute position based on signal characteristics such as strength[66], ToA[9], TDoA[94], and AoA[69].

Another envisioned approach to provide a localization service for VANETs is the use of wireless sensor networks (WSN)[9]. In addition to providing localization information

to vehicles, WSN can add value to different applications utilizing monitoring and sensing features such as temperature, motion, noise, and visibility, which will help to improve localization system accuracy and system performance. For example, based on traffic flow sensing, message broadcasting can be reduced during low traffic, as discussed by Schlingelhof et al. [83].

2.1.7 Relative Distributed Ad-Hoc Localization

Nodes can construct their own map and positioning estimations based on their relative position to its neighbors and nearby landmarks. Nodes exchange their maps to multi-hop neighbors to help each other build their own maps. Although this technique has been used for ad-hoc and wireless sensor networks, it is also proposed for VANET localization systems [9].

Binslimane et al. [5], proposed a distributed localization algorithm to determine the position of vehicles that are not equipped with GPS to determine their location by sending a request to its one-hop neighbors. Vehicles with GPS reply to the request by replying with their location information. With the information received and the distance obtained by applying the optimized dissemination of alert messages (ODAM) protocol, the vehicle can calculate its position. The vehicle requires a reply from three neighbors to do so. If the vehicle has fewer then three neighbors, the algorithm can estimate a relative position along with driving direction based on several possible scenarios.

Vehicles can obtain their relative position through the use of several technologies such as radio[65], and ultrasound sensors [9]. Parker et al. [65] introduced a distributed localization algorithm. Vehicles measure their distance to their neighbors using radio ranging technology (e.g., RSSI), and build a matrix of measured distance, and exchange the information with their neighbors. Using this along with GPS information, a rough estimation can be built. A refinement algorithm is then applied so that errors are reduced.

Several other algorithms have been developed for ad-hoc and wireless sensors networks. However, not all of them can be applied to VANETs due to mobility behaviors, speed, and distance. The use of this technique requires the cooperation of neighboring nodes. The emergence of a malicious node that provides false position data will affect the integrity of the whole system, which will produce false position calculations.

2.1.8 Data Fusion

Data fusion is the method of combining data from several techniques that we discussed previously. The objective of data fusion in localization is to improve the computation results in terms of accuracy and availability [9]. In addition to collected data from local sensors and devices, statistical methods are applied to improve prediction results. In WSN, Kalman filters [62], particle filters [10], and belief theory [63] were used to improve the estimated position calculation. Kalman filters have been also discussed for vehicular localization[62]. A generic model for data fusion for localization in VANETs [9] can be as shown in Figure 2.2.

Several localization systems have been developed to utilize data from different sources. Safespot[87] is a project initiated to develop road safety applications. The project started in 2006, co-founded by European Commission Information Society Technologies (ECIST). One of its objectives is to develop a relative localization algorithm with an accuracy of sub-meters. Its approach is to use data fusion algorithms that use information from multiple sources to calculate vehicle position and provide reliability information for the applications to decide whether the position accuracy can be used or not. POMA (Positioning, Mapping, and location referencing)[78] is a sub-project of the Cooperative Vehicle Infrastructure Systems (CVIS) was called for by the European Commission with the target of developing a new localization method combining different technologies. Data fusion algorithms are used to calculate vehicle position and verify its integrity. Vehicles will use GPS and EGNOS receivers to initially determine their position from GPS satellites and their augmented information. Position information will then be fused with infrastructure-based localization services and dead reckoning to estimate future positions. Moreover, the calculated position is verified with a map matching approach containing updated map data.

2.2 Beaconing and Message Exchange

After the understanding of how a vehicle can determine its position, we discuss in this section the location sharing among neighboring nodes and focusing on the performance issues and the security aspects. VANET application requires the exchange of event and vehicle position information. Moreover, to deliver accurate and reliable service, they require recent status and continuous updates. A great amount of data transmission is expected to fulfil the application requirements. Vehicles will exchange and share data

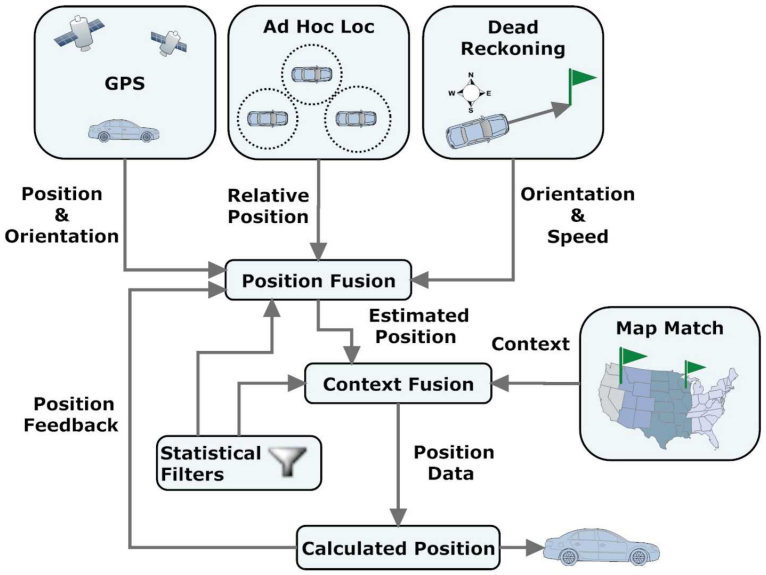


Figure 2.2: A data fusion model for vehicle localization in a VANET.

through periodic beacons, group updates, or direct peer-to-peer messages. Since vehicle mobility changes frequently (e.g., changing lanes, direction, speed, or acceleration), beacon messages will contain the current location and mobility information.

Periodic messages has an impact on the network performance of VANETs. Tian et al.[102] studied the performance of beacon messages in VANETs and showed that, in a density of 100 vehicles, the average rate of beacon lost can reach up to 40% due to collisions and radio interference. The following section we will discuss several studies that have been presented to control the message load on the communication channels and to maintain the network's quality of service (QoS) in VANETs.

2.2.1 Adaptive Beaconing and Control

An approach to control outgoing beacon messages is to use adaptive beaconing where the rate of message generation is adjusted according to defined metrics. Schmidt et al. [84] discussed general approaches to implement adaptive beaconing in VANETs. A vehicle can adjust its beacon rate based on its local state movement. By considering vehicle velocity, acceleration, yaw rate, and vehicle type (e.g., emergency vehicles), the vehicle can predict its situation and surrounding conditions. For example, low velocity can indicate that the vehicle is in a dense area, which means that the beacon rate should

Table 2.1: Summary of Adaptive Beaconing Solutions in VANETs.

Authors	Layer	Detection	Control
Zhou et al. [124]	*Cross layer*	*Link persistence probability*	*Message flow*
Lidstrom et al. [50]	*Application*	*App. requirement (range & delay)*	*Data scale & compression*
Mohandas et al. [60]	*Transport*	*Queue length at RSU*	*Data transmission rate*
Subramaniam et al. [97]	*Network*	*App. requirement (BW, delay, loss)*	*Route selection*
Yan et al. [118]	*Network*	*Link stability (radio & dist.)*	*Primary & backup route selection*
Bouassida et al. [7]	*MAC*	–	*Static and dynamic priority*
Schmidt et al. [84]	*MAC*	*Local state and environment*	*Beacon rate*
Sommer et al. [93]	*MAC*	*Channel quality, message utility*	*Transmission rate*
Lam et al. [40]	*MAC*	–	*Time slot reservation per vehicle*
Le et al. [43]	*MAC*	*Channel busy time*	*Rate, power, rate + power*

be reduced to maintain the offered bandwidth load. Sudden changes in acceleration and yaw rate can indicate the existence of a dangerous situation, which requires a higher beacon rate to update the condition. An active emergency vehicle also must increase its beacon rate to update its location and send its messages to surrounding vehicles to clear the way for it. Therefore, beacon rates are adjusted individually based on their own movements. Another approach is to adjust the rate according to the surrounding environment, such as vehicle density and movements. The authors discussed the trade-off between accuracy and the offered load. Reducing the beacon rate may free network resources, but, on the other hand, the status of the surrounding vehicles might not be properly updated to support application accuracy.

Sommer et al. [93] used adaptive beaconing to disseminate non-safety traffic messages. The adaptive traffic beacon service adjusts its message transmission rate based on channel quality and message utility. Channel quality is monitored and evaluated based on signal to noise ratio (SNR) measurements, the number of neighboring vehicles, and the last evaluated status. The message utility is determined based on the vehicle's distance to the event and message age.

Table 2.1 summarizes the related studies of adaptive beacon solutions proposed for VANETs. Current solutions control the beacon rate of individual vehicles to reduce the number of sent messages.

2.2.2 QoS Provisioning

In wireless and ad-hoc networks, QoS provisioning was discussed to improve network performance, secure application availability, and guarantee resource allocation. Martinez et al. [57] surveyed QoS provisioning in WSN; solutions have been developed in the network layer and the MAC layer to detect and control resource utilization. In the network

layer, several protocols have been proposed to reduce the amount of redundant information sent from sensor nodes to the sink node. This will reduce message transmission and saves node energy resources. For example, the directed diffusion protocol is a data-centric approach that allows the aggregation of sensor node data to a single destination by removing redundant information to reduce the amount of message transmission. In the sequential assignment routing (SAR) protocol, the route decisions are made based on energy resources, planned QoS, and traffic type. The multi-path tree is constructed between the source node and the sink, avoiding intermediate nodes with low energy. On the other hand, MAC layer protocols were developed to avoid collisions and prioritize the channel occupation. For example, Zebra MAC (Z-MAC) is a hybrid scheme that combines carrier sense multiple access (CSMA) and time division multiple access (TDMA) to schedule time slot assignments. Therefore, under low rate contention, it uses CSMA, and under high contention, it has a TDMA behavior.

In MANET, Marwaha et al.[58] discussed several proposed solutions. For routing protocols, solutions were proposed to overcome mobility challenges and maintain routing paths and available resources. For example, core extraction distributed ad hoc routing (CEDAR) uses bandwidth availability criteria for route selection. Core nodes are selected dynamically and collect bandwidth information from other nodes. Routes are then calculated from the source to the destination such that the closest core node to the destination is considered a source for the destination domain. Another protocol is QoS over AODV (QAODV), in which the source sends its QoS requirements with the route request. Every intermediate node should check to determine whether it can support the requested QoS. In the MAC layer, solutions have been developed to provide high-priority access to real-time applications by using priority queues such as in IEEE 802.11e.

In VANETs, similar approaches have been followed to present solutions with QoS provisioning. However, the network topology changes, and the distributed nature of VANETs pose challenges that require the development of new protocols. Therefore, various approaches have been considered by researchers to provide and support QoS in different network layers for both periodic and non-periodic messages. Solutions for routing protocols have been proposed to find a route from source to destination that fits the QoS requirements of the applications.

Subramaniam et al.[97] proposed a receiver-based routing protocol called QoS for highly dynamic vehicular ad-hoc networks (QVANO). The QoS requirements (bandwidth, delay, and packet loss) are negotiated based on the application requirements. During route discovery, the sender will request a route with its resource requirements,

and the intermediate nodes will forward the request and participate in the route if they can meet the application requirements. The destination node will send a reply to the sender if the requirements are met. This process will guarantee that the path from the sender to the receiver will provide the required resources before sending the application data. Yan et al.[118] proposed a routing protocol where the routing path and a backup path are selected based on their stability (radio and distance), cost, and delay.

Another approach is to handle QoS in the lower layers of the network by controlling the transmission rate or power to provide access priority to a communication medium and schedule the outgoing messages. One approach to avoid message collisions and overloading the network is to schedule the sent messages. Zhou et al. [124] proposed to improving the network throughput using an optimal congestion and medium access control (OC-MAC) algorithm to control the flow of messages in the transport layer according to link persistence probability, a factor of the current flow rate with respect to link capacity and the user's effect on the current link. The data rate on the links is adjusted in the medium access layer (MAC) by reducing the rate on links to less than the maximum probability and increasing the rate on links with maximum persistence probability. Based on the adjusted link rate, the flow rate on the transport layer is adjusted jointly. Bouassida et al.[7] proposed scheduling the transmitted messages using static and dynamic priority settings. Static priorities are set based on application and message type. The author categorized five message priority types: emergency priority (for single-hop emergency messages), VANET priority (for network layer beacon messages), high priority (for high-priority safety applications), medium priority (for normal safety applications), and low priority (for low-safety applications). The dynamic priority is determined based on the node speed, message utility (based on rebroadcasting and range factor), and validity of the message (maximum message duration). Messages are scheduled based on their assigned priority queues and reordered based on their dynamic factors. To improve the network throughput and avoid congestion, the authors also suggested controlled utilization of the control channel when the service channels are congested. Moreover, an equal share of the available bandwidth among neighboring vehicles and the proper selection of the next hop forwarder will provide cooperative message transmission and reduce the load on the network resources, allowing the transmission of high-priority messages without delay.

Lam et al.[40] proposed a dynamic channel reservation protocol where time slots in frames are assigned to a vehicle rather than packets. Each receiver will monitor the received frame, detect collisions that occurred in the received channels, and piggyback

the bitmap of the collisions to their transmission. When a sender collects collision information of its transmission from its neighbor, which indicates a collision in transmission, it will select another channel slot based on the availability bitmap. Mohandas et al. [60], proposed a solution for vehicle to RSU communication using an adaptive PI rate controller to control the transmission rate from the source. The rate from the source is adjusted based on the monitored receiving queue at RSU. Congestion is considered to occur when the instantaneous queue length is greater than the maximum. Lidström et al. [50] discussed providing QoS by allowing applications to specify their requirements using spatial-temporal parameters such as required range and delay time. This will also allow application to change their data scale to meet the requirements, such as setting the compression ratio of a video stream.

2.3 Security Threats in VANETs

With applications that deal with real-time events and provide critical information for vehicle operators, it is important to provide a secure and reliable application infrastructure for VANETs. Security in VANETs has been a major topic of concern for researchers [8, 34, 64, 76, 77]. They have identified several security threats and vulnerabilities and proposed solutions to resolve them. As in any wired or wireless communication network, it is essential to secure and protect its data and assets. In VANETs, sensors and equipment are deployed in a public environment, and vehicles use wireless communication to exchange messages while traveling at high speed. With such a topology, VANET systems and services are vulnerable to various risks and attacks. While some risks are caused by the nature of the network, e.g., a route link can be broken during message transmission because a vehicle changed its mobility, or by an intention act to serve an individual's goal; e.g., an attacker can compromise network equipment and send false warning messages to redirect vehicles to a different road path. Many researchers have discussed different security risks in VANETs [8, 34, 64, 76, 77]. These attacks include:

- *Physical attacks*: An attacker can gain physical access to the on-board-unit (OBU) and manipulate the sensors, wires, and antennas, causing the OBU to misread local information or send false messages. It may also cause signal jamming, which is also considered an attack and can affect system availability. Vandalizing the OBU can affect the integrity of localization system if the unit participates in distributing its location to proximate vehicles. For example, it can cause false position calcula-

tion by manipulating the antenna power and tricking nearby vehicles about signal strength measurements, creating what is known as distance reduction or enlargement effect. Physical attacks have been discussed in various studies [51, 73, 74]. The basic approach to resist such physical attack is to install OBU as a tamper-proof device that can be accessed only by authorized personnel, making it difficult for attackers to vandalize and manipulate the device components and protecting stored vehicle data such as identity and security keys.

- *Message forging*: An attacker may disseminate false or fake messages to all its surrounding neighbors such as claiming to be a beacon so that other nodes calculate their positions based on its existence or consider it their best route hop. A Sybil attack (Figure 2.3a) is one type of message forging attack where a node claims to be multiple nodes with different locations. The attacker (car B) may convince the application and another vehicle (car A) that congestion is building up (cars C, D, and E) so that approaching vehicles will avoid taking the same road, which will favor the attacker's traveling plans.

- *Message tampering*: Taking advantage of cooperative communication, an attack can be conducted by manipulating relayed message data (Figure 2.3b). For example, when a compromised node receives a beacon massage containing position information, it modifies it before relaying the message to other vehicles. False information will result in the incorrect calculation of node position or determining the best route path.

- *Reply attacks*: The attacker stores a previously forwarded message that originated from an eligible node and re-forwards the same message again later. Such an attack can cause other nodes to miscalculate their positions and misidentify their location as illustrated in (Figure 2.3c).

- *Wormhole attack*: An attacker may compromise two nodes in different physical locations and create a communication tunnel between them where messages received by one node are rebroadcasted by the other node. Nodes that are listening to the messages think that they are in another geographical location and calculate their positions based on data that do not represent their actual locations (Figure 2.3d). Wormhole attacks affect the integrity and reliability of localization systems.

- *Privacy invasion*: In all wireless networks, user privacy is a major issue. Protecting user identity and traveling information is an essential requirement. An attacker

can stalk a vehicle by building a travel profile of position history and predicting its next position. To do so, the attacker can collect the exchanged position information and match them with a source. Moreover, the attacker may try to compromise the localization system and gain access to the position information of its victim.

- *Availability and reliability vulnerability*: Attacks can also target the system's availability by preventing network entities from acquiring the proper services. Signal jamming, for example, is one way that an attacker can use to interrupt any wireless network, and results in what is known as a denial-of-service (DOS) attack. Another form of threat in VANET wireless communication is its vulnerability to interference and obstruction. Vehicles travel in different environment conditions. Despite weather conditions that can have an effect on wireless communication, objects and construction on the roadside can prevent proper communication due to reflection, diffraction, or obstruction. For example, buildings, bridges, tunnels, trees, and area topography can interfere with radio signals. Moreover, moving objects on the road, such as trucks, can also interfere with communication between vehicles. Such interruptions can affect VANET availability and reliability, especially for safety-related applications.

2.4 Security Requirements for VANETs

By identifying security threats and attacks, studies have listed general requirements to guide developers on how to secure VANET applications [34, 64, 76, 77]:

- *Secure message exchange*: Securing communication channels has been a subject of discussion for many researchers[12, 24, 34, 41, 51, 81]. The main objective was to secure the network against possible threats and attacks. The main goal is to prevent malicious nodes from sending false messages or tampering with exchanged messages. Moreover, it is necessary to authenticate the message sender to guarantee that the message was sent by an eligible node. The main resolution was to use a digital signature to sign outgoing messages, such as the frameworks proposed in [74, 73, 51].

- *Misbehavior detection and isolation*: Data mining and evaluating the validity of data over a period of time can help in detecting misbehaving nodes and data inconsistency by utilizing various statistical models and setting threshold values to

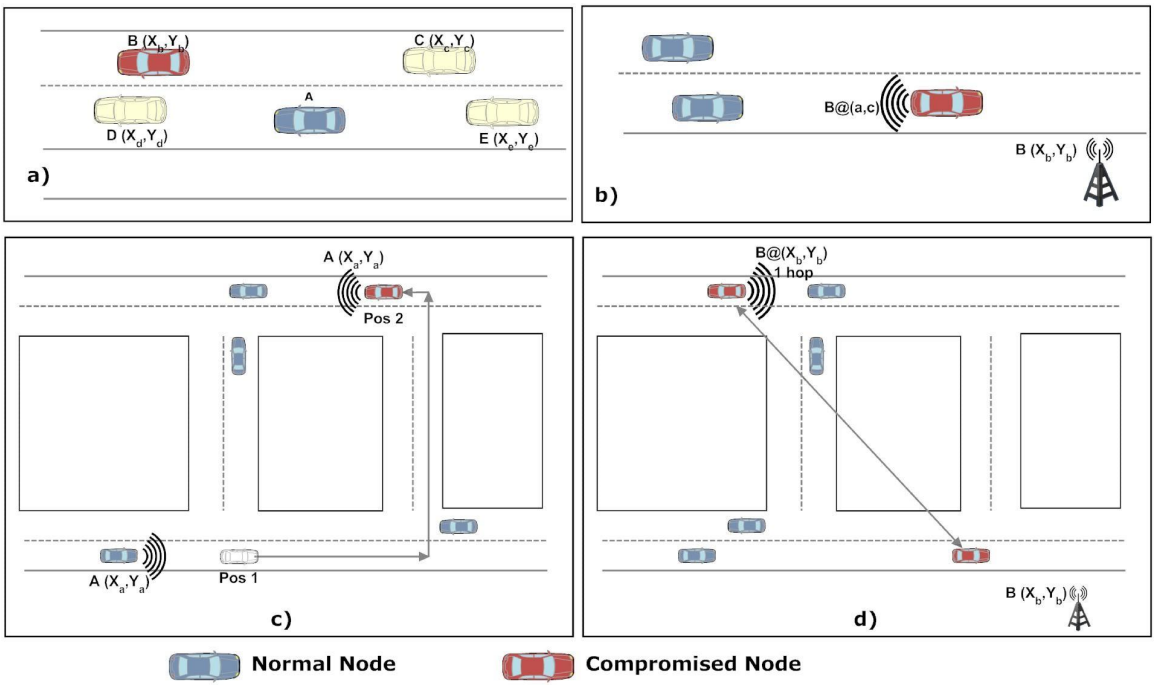


Figure 2.3: Communication attacks in a VANET: a) Sybil attack, b) message tampering, c) reply attack, and d) wormhole attack

determine abnormal activities[9]. However, for statistical models to produce better results, a sufficient number of data samples along with a longer period of time is recommended. Applying such an approach in VANETs will require historic data of monitored nodes such as vehicle mobility, location information, and vehicle density in a defined area. Tracking such information in VANETs can be a challenge due to rapid mobility and environmental changes over a short period of time. Collecting enough data and processing them under a suitable and sufficient statistical model for VANETs is an area of study[62].

- *Privacy*: Protecting user privacy is important in VANETs. Since VANET equipment and communication devices will be installed on private property, owners will have concerns for their privacy. Researchers have identified security threats that can invade vehicle privacy [12, 24, 34, 41, 51, 81]. Signing sent messages using certificates that uniquely identify a vehicle carries the potential to link messages to a sender and track a target vehicle. To protect user privacy from such a threat, researchers have proposed using pseudonym keys to provide anonymity when signing an outgoing message [74, 73, 51].

- *Secure localization*: Vehicle and event location information is essential in VANETs. In [9], authors discussed whether using existing localization techniques in VANETs, e.g., global positioning systems (GPS), relative distance computation, and dead reckoning are suitable for VANETs and proposed using a data fusion model to enable vehicles to compute their locations. Individual or cooperative localization computation must be secured to enable accurate and reliable positioning for application use. Securing individual computation can be achieved by improving local measurement technologies and data fusion models. In cooperative computation, securing exchanged information will help secure communication channels among vehicles. Other studies have used robust localization algorithms [8], distance verification measurement [45], and node misbehavior detection and isolation [22] to propose secure localization solutions.

2.5 Security Frameworks

In VANETs, fast and light security algorithms are highly desired. An article by Schaub et al.[81] summarized the security requirements for VANET communications. A proposed security framework should provide:

1. *Authentication:* By providing a process to verify received information trustworthiness. This process should include sender authentication to verify that a sender is a network member and allow message integrity checks to ensure that the message was not changed during transit.

2. *Accountability:* Authorities should be able to hold a vehicle accountable for sent messages while maintaining its anonymity from other vehicles. A user cannot deny sending a message before authorities (also known as non-repudiation).

3. *Restricted credential usage:* Security tokens should have limited time and parallel usage and cannot be reused to prevent malicious behavior such as a Sybil attack.

4. *Credential revocation:* Authorities should be able to revoke a vehicle's credentials and deny further access.

Many researchers [12, 24, 34, 41, 51, 52, 55, 64, 73, 74, 77, 82, 98, 99, 121, 122] have agreed that secure communication for exchanged messages can be achieved by using digital signatures as building blocks to verify the message integrity and authenticate

the senders without the ability to track and reveal their identity. However, for non-repudiation reasons, only authorities are able to track senders.

To summarize the digital signature process [74], a sender node will have a secret and a public key to sign an outgoing message. The message (MSG) will be constructed as follows:

$$MSG = \{M, T, MD, Cert\}$$

where M is the message data, T is the time stamp when the message was created. $Cert$ is the public key used to sign the message, and MD is the message digest (signature) that is generated from applying the signature algorithm to the message data and time stamp and using the secret key. The message receiver will first validate the certificate to determine whether it was revoked or not. Once the certificate has been validated, the receiver will be able to check the validity and integrity of the message by applying the signature algorithm to the message data (M) and time stamp (T) and comparing the result with the attached signature (MD). If the message was healthy and was not tampered with, both values will match. The secret and public keys are to be issued, managed, and revoked by an authorized certificate authority.

Several studies [34, 51, 52, 55] have evaluated the performance of digital signatures in VANETs and concluded that using a digital signature for message authentication with the Elliptic Curve Digital Signature Algorithm (ECDSA) as a cryptography mechanism is currently the most suitable method for VANETs. To prevent attackers from identifying the senders from their public keys and signatures, researchers have proposed providing anonymity using various signature key types such as symmetric keys[71] and asymmetric keys[82]. They have also proposed various key generation methods such as group signatures[12, 24], ID-based keys[99, 121, 122], and pseudonym keys[74, 77].

Table 2.2 summarizes studies in secure communication for VANETs and their approaches. Moreover, the IEEE1609.2 standard [29] was released that governs security services and communication for VANET applications. The standard covers methods and message format to secure communication channels against certain attacks. We will not discuss the proposed framework in more detail. However, during our study, we will assume that the communication channels among vehicles are secure by applying the IEEE1609.2 standard.

With secure communication, a localization system can guarantee that position information was sent from an eligible nodes. This prevents outside attackers and non-member vehicles from injecting false data into the network. Moreover, the receiver can verify the integrity of the message, making sure that the data was not changed during transmission.

Table 2.2: Summary of secure communication approaches proposed for VANET.

Authors	Digital Signature	Privacy	Key Revocation
Raya et al. [74]	*Elliptic curve*	*Pseudonym*	*Preloaded keys*
Sampigethaya et al. [77]	*Yes*	*Pseudonym and silent period*	–
Manvi et al. [55]	*Elliptic curve*	–	–
Papadimitratos et al. [64]	*Yes*	*Pseudonym*	*Certificate revoc. list*
Polossi et al. [68]	*Hybrid keys*	*Pseudonym*	*PKI*
Scheuer et al. [82]	*asymetric cryptography*	*Pseudonym*	*PKI*
Zhang et al. [122, 121]	*ID-based*	*Yes*	–
Chaurasia et al. [12]	*Group signature*	*Pseudonym*	*Regional authorities*
Lin et al. [52]	*Group sig. and ID-based*	*Yes*	*Revocation list*
Kim et al. [36]	*bilinear pair*	*anonymity*	–
Rabadi et al. [71]	*Symmetric key, DES*	*Group signature*	*Over the air rekeying*
Guo et al. [24]	*Yes*	*Group signature*	*Revocation list*
Laurendeau et al. [41]	*Hybrid keys*	*anonymity*	*expiry and CRL*
Sun et al. [99]	*Bilinear pairing*	*ID-based pseudonym*	*Preloaded and revoc. list*

However, inside attacks are still possible, where attackers try to compromise an authorized node to be able to send false position messages. Thus, securing communication alone is not enough to secure the localization services. Future development should also discuss securing location information availability and integrity against environmental and malicious effects.

2.6 Protecting Location Privacy

In a wireless communication network, privacy protection is a concern for both users and researchers [12, 24, 34, 41, 51, 81]. Studies have discussed the protection of location-based services (LBS) in wireless and mobile networks [6, 26, 61, 89]. A survey by Shin et al.[89] discussed two main issues with users' privacy, query and location privacy. The LBS system architecture for mobile network requires the user device to send query messages to the LBS servers. With addition to the location information, the query message may include additional information that may reveals the user's identity and interests. The challenging threat in such architecture is that the attacker can compromise and access the LBS servers and access the queries and location information of users. Various solutions were proposed to protect users' privacy in wireless and mobile networks. Server-based approaches, such as the k-anonymity[61], mix-zones[6], and path confusion[26] were proposed to protect the LBS server queries and users' location information. Users can also have the option, using their mobile devices, to unsubscribe to LBS, disable location sharing, and set its k-anonymity value to guarantee an acceptable privacy level.

The distributed nature of VANETs makes the vehicles a collecting node for users'

location information. Moreover, users have limited access to device settings, especially when driving, to change the settings of a vehicle's devices. Therefore, further investigation is required to protect users' information. Researchers [12, 24, 34, 41, 51, 81] have discussed privacy issues in VANETs and proposed several security frameworks to protect vehicle identities. Schaub et al. [81] discussed privacy requirements for VANETs. Security frameworks should provide authentication, accountability, restricted credential usage, and credential revocation mechanism. In addition, it should protect vehicle privacy and maintain minimum disclosure of location and activities and provide users anonymity and unlinkability of message sources.

As discussed in the previous section, several researchers [73, 74, 51] have focused on securing communication channels among vehicles with the ability to authenticate the message sender. With the use of digital signatures to secure messages, various solutions have been proposed to provide anonymity through various pseudonym approaches [74, 77], group signatures [12, 24], ID-based signatures [99, 121, 122] and key management [71, 82].

In [74], the authors initially proposed the use of pre-loaded pseudonym keys to sign outgoing messages, protecting users' identities from being revealed and traced by changing the signature keys. However, preloaded key raises issues of storage and key management. Other authors have proposed improving the anonymity of senders using group signatures [12, 24, 52]. Groups are constructed based on similarity parameters such as speed, direction, or regional position. A group leader will be elected to generate a group signature that will be used by all members as long as the group formation is maintained . Using group signatures will prevent attackers that manage to gather transmitted messages from distinguishing a single member from the group. Additional studies have aimed to improve network performance by allowing the use of ID-based signatures for low-risk nodes such as RSUs [99, 122].

The methodology of changing pseudonym keys was a focus of several studies to protect the privacy of vehicles [76, 77, 82, 96]. In [77], Sampigethaya et al. proposed the CARAVAN protocol that uses a grouping of vehicles where the group leader communicates with the RSU while the remaining group members remain in a silent period and stop broadcasting messages. The silent periods will reduce the load on the network by reducing the redundant broadcast of messages and preventing attackers from collecting data from an individual member. The other expanded their study in [76] and presented a protocol called AMOEBA and considered applying CARAVAN to V2V communication by using an application address range for vehicles requesting location-based services.

Moreover, the group leader will act as a mixer for forwarded requests by encrypting and reordering requests to prevent attackers from linking messages to requests and targeted vehicles.

Scheuer et al. [82] proposed managing pseudonym keys for vehicles where the key will change in mixed-zone areas such as road intersections. Therefore, tracing a vehicle can be prevented as the vehicle changes its key and may change its direction. In [96], Song et al. presented a scheme called density-based location privacy (DLP). The pseudonym key is changed based on the number of neighboring vehicles and traffic flow. The main focus was on securing signature keys and prevent attackers from tracing and linking messages to a specific vehicle.
Privacy issues were discussed by researchers [12, 24, 34, 41, 51, 81] within a security framework (Section 2.5) with the assumption that network members are trustworthy. However, up to our knowledge, no studies have discussed securing the message contents in VANETs and the impact of compromising a trusted node.

2.7 Securing and Verifying Location Information

Due to VANET limitations and the importance of position information, securing localization is a challenging area of research in VANETs [45]. A secure localization can be achieved with the following approaches [46, 8]:

1. *Secure communication*: Secure communication channels by enabling receivers to authenticate the sender while maintaining their privacy and checking message integrity. Some researchers have suggested securing VANET communications to authenticate the sender and check message integrity using digital signatures [51, 64]. In fact, IEEE1609.2 was released as a standard to secure messages in VANETs [29].

2. *Misbehavior detection and isolation*: Detect malicious nodes by evaluating the context of messages and the behavior of the sending nodes [22].

3. *Robust localization algorithm*: Develop computation algorithms that accept and deal with errors and false position information [8].

4. *Location verification*: Enable nodes to verify received location information and validate its integrity [117].

Researchers have discussed securing position information using location verification protocols [8, 45, 46]. Each network has its own characteristics, requirements, and objectives.

Thus, security objectives are different. Different location verification protocols were proposed for wireless and ad-hoc networks.

A survey in [8] discussed secure localization algorithms that were proposed for WSN. The objective of location verification in WSN is to evaluate whether the node has correctly computed a location. The Robust Position Estimation Protocol (ROPE) allows beacon nodes to use the radio signal physical parameters to verify the distance of a sender [42]. Another protocol, Location Anomaly Detection (LAD), detects network anomalies by comparing the received data to the deployment information of sensors and the expected behavior of their observations [17]. The Echo protocol performs an in-region check to verify a node position with the help of a selected neighbor node using radio signal parameters and ultrasound signals to compute distance[79]. Wei et al. [111] proposed using a verification center to collect the network nodes location observation data and detect anomaly nodes using the greedy filtering by matrix (GFM) algorithm.

Čapkun et al. [106] proposed verifying location estimations using a hidden mobile base station (MBS). The MBS sends a verification request to a node and receives a reply through radio and ultrasonic messages. MBS will compute the time difference between the two messages and calculate its distance to the node. Some authors, such as Singelee et al. [91], have proposed using distance bounding protocols to verify a node location. Specifically, they proposed using the time of flight measurements of electromagnetic signals.

Proposed solutions for wireless sensor networks and ad-hoc networks cannot be applied directly to VANETs because the security and application requirements are different. Hubaux et al.[27] described a verifiable multilateration protocol in which four base stations take turns computing the time of flight of a message sent to the questioned vehicle. Using the distance bounding approach, an accurate measure of a vehicle's position can be calculated. Golle et al.[22] have proposed a general approach model to detect malicious nodes. When data inconsistency is detected, an adversarial model is initiated to evaluate and explain the cause of the errors and correct them based on their explanations and analysis.

Xiao et al.[114] proposed a security scheme to detect and localize Sybil nodes by measuring the sender signal strength. The list of nodes and measured signal strength are shared among neighbors. Each node will run the enhanced verification algorithm based on the radio strength measurement to verify whether the node and its claimed position are correct. If a node recognizes the existence of a malicious node, it will run a statistical model algorithm to classify the malicious node and detect all Sybil nodes.

Table 2.3: Summary of secure localization and position verification proposed for VANET.

Authors	Cryptography	Verification	Detection	Filtering	Infrastructure
Golle et al. [22]	–	*Model to process data*	*Explaining errors*	–	*No*
Xiao et al. [114]	*Digital signature*	*Signal analysis*	*Statistic model*	–	*Yes*
Leinmuller et al. [45]	–	*Trust model using sensors*	–	–	*No*
Yan et al. [117]	–	*Radar*	*Movement history*	–	*No*
Song et al. [95]	*Symmetric keys*	*Signal analysis*	*Distance enlargment*	–	*No*
Ren et al. [75]	–	*Directional antenna*	–	–	*No*
Yan et al. [116]	–	*Filterd data*	–	*Grid map*	*No*

Leinmuller et al.[45] proposed a trust model that will enable a vehicle to evaluate its neighbors' trustworthiness. Each vehicle is equipped with multiple sensors, and a weight value is given for each sensor based on its reliability and known performance. Sensors' threshold values evaluate the neighboring nodes as acceptors or rejectors.

Yan et al.[117] proposed a solution to secure localization by verifying the announced position of neighboring vehicles using radars that read the physical parameters of nearby cars. The solution has a number of challenges such as the fact that a line-of-sight is required between two vehicles. Obstacles such as trucks can block the signal, causing the misclassification of neighbors.

Song et al.[95] proposed an infrastructure-less cooperative protocol to detect false position announcements by measuring the time-of-flight (ToF) to evaluate the claimer against distance reduction. Using another neighbor, the vehicle can then verify the location of a node for distance enlargement using ellipse computation with foci located at the vehicle and its assisting neighbor position. The position of the assisting neighbor with respect to the verifier and questioned node has an impact on the computation results.

Ren et al.[75] used two directional antennas to process a position verification algorithm that computes relative position with neighbors. The node constructs front and back group bit vectors and periodically sends group information to its neighbors. Yan et al.[116] proposed a filtering method to provide position integrity using box counting over a grid plane. By plotting the gathered position information, the grid with the largest amount of information is selected and used to compute the position.

Table 2.3 summarizes studies that have been conducted in this area. In most proposed solutions, verification protocols rely on a signal strength measurement between nodes that have a direct line-of-sight established between them. A state of non-line-of-sight (NLOS) may result in either dropping a record from a neighbor list or prevent nodes from establishing a proper communication channel to verify a questioned node.

2.8 Trust Evaluation

Several security and reputation trust models have been discussed for wireless networks, as reviewed in a survey by Yu et al.[119]. The authors categorized the trust and reputation management systems into individual- and system-level trust models. Individual-level trust models enable their agents to evaluate their neighbors based on first-hand experience. Each node will share its opinions with others and decide whether it should interact or not with a subject node. On the other hand, system-level models focus on applying a punishment and reward mechanism to encourage nodes to participate in the network services. The authors also listed open issues in trust models for wireless communications. Some of these issues included monitoring accuracy and framework design for specific networks.

Also, Wex et al. [112] surveyed possible trust establishment models for VANETs and categorized them into infrastructure-based and self-organized models. Infrastructure-based trust establishment provides global trust evaluation and knowledge using a centralized system such as certificate authority (CA). The trustworthiness of a vehicle is attached to the vehicle identifiers such as security certificates and assigned pseudonym keys. This type of model is inspired by previous wireless and ad-hoc networks and public key infrastructure (PKI). Self-organized trust establishment allows nodes to evaluate the trustworthiness of other nodes through direct communication and interaction or indirectly using shared information among vehicles. Due to the absence of a centralized reference, global knowledge of trust is not available. However, due to the dynamics of vehicles, self-organized trust establishment will be more suitable for VANET.

Zhang et al.[123] in their survey discussed the requirements for trust management. The proposed models for VANETs should support:

1. *Decentralization:* to adapt to the mobility and distributed environment of VANET.
2. *Sparsity:* to have the ability to evaluate indirect interactions.
3. *Dynamics:* to adapt to changes that occur in road conditions.
4. *Scalability:* to support high-density vehicle traffic flow.
5. *Confidence:* to capture and handle uncertainty.
6. *Security:* to support authentication and integrity check.
7. *Privacy:* to preserve user identities and activities.

8. *Robustness:* to protect the system from possible attacks such as Sybil attack.

Studies have presented several trust evaluation methods for VANET [110, 115]. Wang et al.[110] proposed secure routing by allowing the source to select the routing path based on maximum trust values of the link's node. The forwarding nodes keep track of the behavior of the next hop node. If the next hop node fails to forward, the message sender will decrease the trust value of the next hop node.

Other researchers [15, 16, 100] have focused on evaluating the trust of event messages through reputation propagation. Tajeddine et al.[100] proposed a framework that assigns each vehicle to a group and provides the vehicle with a signature key that corresponds to the group. When a vehicle detects an event, it sends an event message along with its trust values and signs it with the group key. The message receivers evaluate the signature keys and the group trustworthiness based on received messages. To preserve vehicle privacy, trust evaluation is based on groups rather than individuals. In [15], Ding et al. divided the roles of vehicles into event reported (ER), event observer (EO), and event participator (EP). In a case of an event, an ER detects it through its local sensors and sends a message informing its neighbors about the event, including its evaluation of event reputation. EOs are one-hop neighbors that monitor the behavior of the ERs. They also evaluate the reputation of events based on the received messages from ERs and forward the event messages to EPs. EPs are vehicles that are beyond 1-hop from an ER. They evaluate the message based on the reputation evaluation of all ERs and EOs. Dötzer et al.[16] presented an opinion decision method to evaluate and propagate the trust of event messages. The nodes' opinion decisions are piggybacked on forwarded event messages. A vehicle will evaluate an event based three factors, on first-hand experience with the event, indirect trust through sender trustworthiness, and partial opinions using the message-attached opinions. The final opinion is generated by weighting and combining the three factors.

Table 2.4 summarize related work showing that current trust and reputation systems require direct communication among neighbors. NLOS conditions can prevent fair trust evaluation. Moreover, most trust systems evaluate either the trust of incoming messages of events or the behavior of vehicles and participation in routing and message relaying.

Table 2.4: A summary of trust and reputation systems proposed for VANETs.

Authors	Targeted Service	Subject	Attribute
Xue et al. [115]	*Routing*	*Neighboring nodes*	*Direct distance verification*
Wang et al. [110]	*Routing*	*Next hop node*	*Attribute similarity (speed, brand)*
Li et al. [48]	*Group access*	*New member*	*Mobile trust module*
Tajeddine et al. [100]	*Event messages*	*Events*	*Group reputation, sensor quality, etc.*
Ding et al. [15]	*Event messages*	*Events*	*Reporter behaivior*
Dotzer et al. [16]	*Trust propagation*	*Events*	*Propagated opinions info.*

2.9 Simulation Environments

Several simulators and frameworks have been developed to simulate realistic wireless communication environments that were used to simulate WiFi, cellular, mobile ad-hoc, and wireless sensor networks, and some of them are also suitable for VANETs. Harri et al. [25] had conducted an intensive survey on mobility models and simulators that can be used for VANET. Although the focus was on realistic mobility models, the survey showed that few of these simulators take obstacles into consideration. For example, the network simulator NS-2 (available at http://www.isi.edu/nsnam/ns), a well-known network communication simulator that is used by many researchers, supports three types of propagation models: free space, two-ray ground reflection, and shadowing. QualNet [80] supports signal propagation and has a library of models that takes building structures and canyons into consideration. The Global Mobile Information Systems Simulation Library (GloMoSim)[120] supports free space and two-ray Ground.

Researchers [1, 21, 31, 37, 56, 80, 86, 108, 120] have developed mobility models to make simulations more realistic, and some have already considered propagation models. In the Obstacle Mobility Project [31], the model considers buildings as obstacles and takes them into consideration for mobility routes and radio propagation. Based on the distance between nodes, signal loss is calculated using tow-ray ground or the Friss model. UDel models [1] generate mobility and propagation trace files to be used with network simulators. The model generates a propagation matrix of a city map and calculates signal loss between two positions taking buildings into consideration. AutoMesh [108], a VANET simulation framework, gathers building 3D information from a geographic database and calculates propagation through shadowing. Moreover, it uses a log-normal shadowing model to calculate signal loss caused by moving vehicles passing between two communicating nodes. MobiReal [37] considers mobility obstacles to determine routes and uses shadowing to calculate signal propagations. CARISMA [86], a traffic simulator, takes into consideration that buildings exist on the roadsides and have an effect on

Table 2.5: Summary of simulation models with signal propagation proposed for VANETs.

Model/Simulator	Model Type	Obstacle (Buildings)	Obstacle Vehicles	Signal Loss Model
NS-2	*Network sim.*	*Yes*	–	*Free space, two-ray ground, shadowing*
QualNet [80]	*Network sim.*	*Yes*	*No*	*Free space*
GloMoSim [120]	*Network sim.*	–	–	*Free space, two ray ground*
AutoMesh [108]	*Framework*	*Yes*	*Yes*	*Shadowing, Log normal shadowing(vehicles)*
Obstacle [31]	*Traffic sim.*	*Yes*	*No*	*Two-ray ground and friis*
UDel Models [1]	*Traffic sim.*	*Yes*	*No*	–
MobiReal [37]	*Traffic sim.*	*Yes*	*No*	*Shadowing*
CARISMA [86]	*Traffic sim.*	*Yes*	*No*	*Shadowing*
BDAM [56]	*Propagation*	*Yes*	*No*	*Shadowing*
CORNER[21]	*Propagation*	*Yes*	*No*	*Corner*

signal propagation. BDAM[56] was proposed by its authors for a realistic propagation model for VANETs that consists of two components: the Distance Attenuation Model (DAM) and the Building Attenuation Model (BAM). DAM calculates signal fading based on distance, while BAM assumes that buildings block the line-of-sight. CORNER[21] predicts propagation between two vehicles that are in a line-of-sight and crossing a corner of a building. The prediction model is based on actual measurement readings where site measurements were recorded and fitted to a mathematical function to present the interference behavior.

Table 2.5 summarizes the models and frameworks that have considered obstacles in wireless simulations. As shown, fixed obstacles such as buildings have been discussed and modeled using the shadowing model to simulates the propagation affect on the signal. However, to our knowledge, none have discussed modeling moving obstacle in VANET simulations.

2.10 Security Analysis and Evaluation Models

Dependability and security models have been discussed in the field of computer science in their relation to system reliability. In [104], Trivedi et al. classified the dependability and security model types. They defined the relation between different focused attributes; availability, integrity, confidentiality, performance, reliability, survivability, safety, and maintainability. Based on the studied system, the evaluation may focus on one attribute or a composed set of attributes. The authors surveyed and classified different models that have been implemented for computer networks. As each network has its own requirements and deliverables, different models were presented to quantify the dependability and security of the studied system.

In [23], the authors proposed the following three different approaches to quantify security attributes for a intrusion detection software system: a generic state-space approach, a discrete event dynamic system approach, and a Markov-decision problem approach. The state-space approach can be solve as a semi-Markov problem (SMP) to obtain the probability of reaching security fail state and calculate the mean time to security failure (MTTSF). The discrete event dynamic system approach defines the system's safety properties based on controlled discrete events of sub-languages. The language presents policies that can be enforced. The Markov-decision problem approach associates cost with transition and therefore help obtain the optimal security policy for the system. Madan et al. [54] presented a model to quantify the security attribute for an intrusion-tolerant system. The model used a semi-Markov approach to calculate the MTTSF.

Researchers [4, 49, 109] also studied network resilience against security threats and proposed realtime evaluation to help detect security attacks. Li et al. [49] proposed a realtime method to evaluate and quantify a network-security measure against possible threats. The proposed solution is based on a hidden Markov Model. The security threats are defined by the implemented policies and categorized based on their severity on the network. The model will collect and analyze network traffic according to a knowledge library of intrusion attacks. The system threat level and reliability are calculated to trigger a security alarm if the values falls within a specified threshold value.

Baumann et al. [4] proposed a Markovian model to analyze the network behavior under flooding denial-of-service (DoS) attacks. The model is solved by continuous-time Markov chain. The model incorporate the network operational environment and applies a random dropping policy as a defence mechanism. Wang et al.[109] used an advanced semi-Markov process to model and analyze the performance of the MAC protocol in wireless LANs.

In VANETs, Ma et al. [53] proposed a location-privacy metric that will be undergone by taking a virtual snapshot of the system and measuring the user's information uncertainty. The metric will indicate the level of privacy the user will have against tracking attempts and linking trips to individuals. And, Shokri et al. [90] developed a framework to evaluate location privacy protection mechanisms against defined attacks.

In order to secure the localization service in VANETs, a quantified security analysis and evaluation model is desirable. With many network protocols proposed for VANETs, the model will help the system integrators to stack the protocols to provide the location services while securing the position information.

2.11 Summary

Numerous publications [12, 24, 34, 41, 51, 52, 55, 64, 73, 74, 77, 82, 98, 99, 121, 122] have reported solutions to secure VANET applications and user information. As a VANET is an ad-hoc network, it inherited the general features and limitations of wireless and distributed network as well as their threats and security vulnerability. Researchers have been inspired by previous work in MANET and WSN to apply the same solutions and protocols to VANETs [8, 9, 27]. However, VANET has its own challenges and requirements. In this chapter, we have reviewed studies proposed for wireless ad-hoc networks and VANETs that are related to our study. The objective of our work is to ensure the integrity and availability of exchanged localization information for VANET applications. The developments are to fill the technical gap in the state-of-the-art reported reported the literatures.
The conclusion of this chapter is summarized as follows:

1. Many studies have presented frameworks to secure communication channels to protect exchanged messages among vehicles from possible attacks [74, 73, 51]. The frameworks suggested the use of digital signatures to enable the receivers to authenticate the senders and validate message integrity. Sender identity and privacy are protected by using pseudonym keys and key management solutions, which will prevent attackers from identifying the message senders and linking messages to a targeted sender. However, with such a framework, the transmitted data are still in the reach of an attacker. By collecting exchange data, an attacker can extract the clear text data and ignore the signatures to obtain valuable data such as location information from periodic beacons. The lack of research in this area may be due to the assumption that every application should handle the security of its own data. This cannot be true for beacon service and information.

2. Exchanging location information among vehicles is critical for VANET applications. The delivered services should provide accurate information about the surrounding vehicles. For example, during lane merging, VANET applications should alert the driver about a vehicle that may exist in his blind spot. Ignoring the existence of a vehicle just because a beacon was not received from that vehicle may cause an accident due to poor decision-making and lead users to question their trust in and the reliability of such technology. Therefore, it is necessary to verify the location of vehicles and increase vehicles' awareness about their surroundings. Non-line-of-

sight (NLOS) conditions may prevent the proper exchange of location information among vehicles; therefore, further investigation must be conducted to tackle this challenge.

3. Although location information is important for many applications, we could not find a study that discussed a network service that could supply location information for a vehicle application. Allowing each application to develop its own location information handling will create redundant work and result in security flaws. The need for a unique service to secure and manage collected information services is essential.

4. With the envisioned applications for VANETs, the number of transmitted messages will increase. Current scheduling and rate control mechanisms allow nodes to change their transmission behavior based on the local detection of signal properties and collision probabilities or setting higher queueing priority for critical applications and their messages. However, in VANETs, authorities and network managers will need to have control over network resources in critical conditions and special events, providing QoS for applications by instructing vehicles to change their transmission behavior based on the event.

5. Simulation is an important part of evaluating proposed solutions for VANETs. The work in this thesis has been evaluated using NS-2. We chose this tool because it is a well-known tool and its simulation results are accepted among researchers in the field. To simulate moving obstacles, we need to develop an obstacle model that simulates NLOS conditions among vehicles.

6. Security analysis models is an important topic that need to be investigated for VANETs. With many solutions proposed for VANET and each of them addressing a different security aspect, it is important to quantify the security measures that a combined solution can provide. Current studies evaluate security measures using qualitative method. Quantified attributes are limited and focused on users privacy and information uncertainty.

Chapter 3

A Cooperative Multi-hop Location Verification Protocol

3.1 Introduction

Vehicular ad-hoc networks (VANETs) are being developed to provide on-demand wireless communication infrastructure among vehicles and authorities. Such an infrastructure is expected to deliver multiple road safety and driving assistance applications. Vehicles will be equipped with sensors and communication devices that will allow them to cooperate with each other and with authority units to disseminate and exchange various road applications' messages. For example, warning messages and traffic management instructions can be broadcast to increase drivers' awareness of potential travel hazards, allowing them to respond earlier to avoid traffic congestion and collisions or to clear the way for inbound emergency response units. Other applications pertain to passenger comfort and convenience, such as locating points of interest, exchanging multimedia assets with other users in the network, or receiving location-based commercial advertisements.

Many of these promising applications require knowledge of real-time events and neighboring vehicles' location specifications. A vehicle can determine its location using existing technologies such as global positioning systems (GPS), map matching, dead reckoning, cellular localization, image and video processing, and relative positioning. In [9], the authors have discussed integrating several techniques with statistical filters in a method called data fusion. Each technique has its advantages as well as security concerns, which must be taken into consideration during application development.

Enabling each vehicle to determine its location is necessary in VANET, however re-

porting GPS coordinates is not efficient for the receiver to trust the sender. Vehicles also need to have information about events in their surroundings and proximal vehicles. This type of information can be exchanged between network members using beaconing, direct messaging, or group updates. To secure received location information and validate its correctness in a non-line-of-sight condition, we will discuss in this chapter a cooperative multi-hop location verification protocol for VANET.

3.1.1 Motivation and Challenges

Security threats can compromise and disturb applications' functionality and may increase the chances of road accidents. Researchers [34, 64, 76, 77] have discussed various security risks and attacks, including physical attacks on network devices and communication attacks such as message forging, message tampering, reply attacks, wormhole attacks, and privacy invasion. There is another type of threat that can affect localization service integrity, reliability, and availability. Vehicle communications are vulnerable to signal interference as they travel in different environmental conditions. Physical objects and construction on the sides of the road (i.e., buildings, trees, and area topography) can interfere with radio signals and prevent proper communication. Moving objects such as trucks can also interfere with communication between vehicles and could block a driver's visual and communication line-of-sight (LOS), creating a non-line-of-sight (NLOS) state, which can lead drivers to make poor judgments when changing lanes or merging onto a highway.

In Figure 3.1, we illustrate what can happen if an obstacle blocks communication signals. Vehicle A detects an event, E, which is an emergency vehicle approaching. In response, A sends a warning message to its neighbors behind it to encourage their operators to slow down and allow the emergency vehicle to pass, a sequence of events that could prevent vehicle operators from needing to brake suddenly or swerve. However, vehicle B might not receive the warning due to the position of the bus, C. The bus does not forward the message, assuming that B is within A's communication range. If A has the knowledge that B is still within communication range but obstacle C is blocking direct communication with it, the application should decide to allow C to forward the message to ensure message delivery.

In VANETs, objects such as buildings, trees, and other features that exist on roadsides can interfere with or block radio signals [85]. In general, the higher the radio signal

frequency is, the more vulnerable it is to interference. One particular study showed the vulnerability of high-frequency radio signals to interference [18]. For example, at a frequency of 5.85GHz, a signal loss of 14dB is caused by home penetration and a loss of 11–16dB is due to tree shadowing, while a signal loss of 7.7dB is caused by penetrating a building at a frequency of 912MHz. In the U.S., the 5.9GHz frequency is assigned for VANET communication.

In a VANET environment, consideration should be given not only to fixed obstacles and buildings but to moving objects on the road that can cause signal block. Since vehicles come in different shapes and sizes, they can serve as obstacles between neighbors that are in the same communication range. Unlike with buildings and fixed structures for which interference and signal quality factors can be measured in the field and be taken into consideration while traveling in a given area, moving obstacles with different shapes, speed, composition, and density can create an NLOS state that changes on an unpredictable temporospatial basis and could prevent a vehicle from receiving consistent updates and location information from its neighbors.

3.1.2 Objective and Contributions

Improving and maintaining drivers' neighborhood awareness is important in VANETs. It is also important in developing a reliable and secure localization service capable of overcoming obstacles' effects on communication transmissions. We believe that vehicles should have better knowledge about their surroundings to support upper-level applications and services, which do not perform well in NLOS conditions. Our objective in this chapter is to improve vehicles' awareness of their neighbors in a NLOS condition in which direct verification was not possible to verify a subject node. In this chapter, we present a novel protocol that verifies a vehicle's announced location using a multi-hop cooperative approach whenever direct verification and communication is not possible. With such a solution, a vehicle's awareness of its neighbors increases, improving the reliability and availability of many safety, travel, and traffic management applications and services. We propose a cooperative location verification protocol in an NLOS condition. Unlike other verification protocols proposed for VANETs, the NLOS triggers the verification process rather than accepting the error. As part of the protocol evaluation, we also present an obstacle model that was used to simulate the NLOS condition. Current network simulators, such as NS-2, does not support moving obstacle that affects direct communication

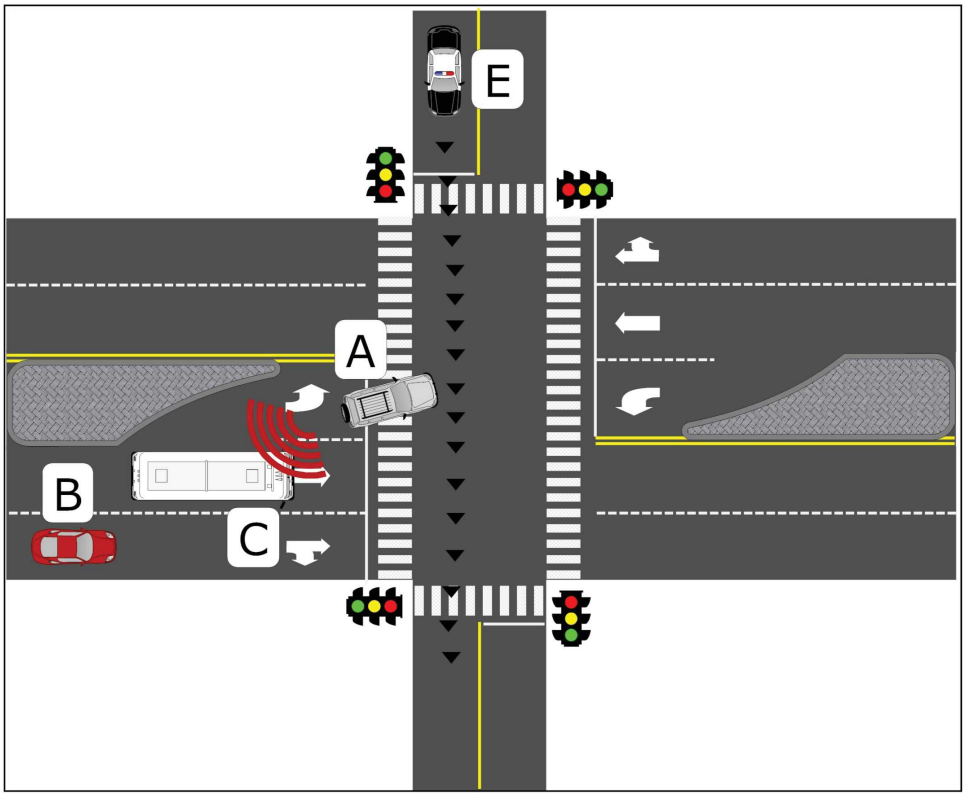


Figure 3.1: Vehicle awareness can improve applications that are affected by moving obstacles.

between vehicles.

The remainder of this chapter is organized as follows: In section 3.2, we identify the adversary model that can threat location based applications followed by the system's security requirements in section 3.3. In section 3.4, we will present the proposed solution for the CMLVP. In Section 3.5 we discuss the simulation results. Section 3.6 will include a discussion of related aspects and subjects of the protocol. Finally, we end the chapter with a summary.

3.2 Adversary Model

NLOS conditions are created naturally by the environment due to the mobility and physical characteristics of different objects surrounding a vehicle. Researchers and en-

gineers recognize such technological limitations even in the current phase of VANET development [18, 52, 85]. Future end-users will eventually discover additional technological limitations through practical encounters with inconsistencies and failures. The nuances of human behavior can be observed in previous technology implementations. For example, the effects of human-system interactions is notable in wireless LAN and cellular phone network growth, such as when people notice communication limitations or signal interference issues in areas where public services are provided.

In this chapter, we focus on system reliability and location information integrity. We consider two types of attacks: unintentional and intentional. Unintentional attacks on network reliability can occur on roads where large vehicles travel, such as industrial areas. These are locations where safety applications for hazards such as blind spots can help to reduce the number of accidents but where NLOS occurrences might prevent the desired reliability of those applications.

On the other hand, by knowing the limitations of wireless communication signals and possible methods of system exploitation, an adversary could use this technology in his or her favor. For example, a driver might try to avoid being tracked by police by traveling near large vehicles in an attempt to create a barrier.

3.3 Security Requirements

Since beacons and updates are received from different vehicles, context integrity and data consistency are important. The NLOS conditions can affect the integrity of exchanged location information about neighboring vehicles. In this section, we outline the security specifications that are required for the proposed solution that will lead to a secure neighborhood localization information network and validate the integrity of its data. The proposed solution should:

1. Increase neighborhood awareness and vehicles' knowledge about surrounding nodes under NLOS conditions.

2. Monitor localization information, detect data inconsistencies, and validate data integrity.

3. Ensure that a vehicle avoids total dependency on periodic incoming beacons and update messages.

4. Maintain confidentiality and employ message or sender authentication.

5. Validate processed information and eliminate false data before processing.

6. Support availability in a large-scale environment.

3.4 Cooperative Multi-hop Location Verification Protocol (CMLVP)

3.4.1 Assumptions

The protocol presented in this chapter is based on the following general assumptions:

1. All vehicle are capable of determining their own position and mobility information using a data fusion model of existing technologies such as GPS, map matching, a digital compass, and accelerator meters. By using improved GPS technologies such as differential GPS or augmented GPS, accurate position estimation can be achieved (error < 1 *meter*). Position errors tend to affect the position accuracy of all vehicles in the same area [9, 83]. Hence, relative position computations using GPS coordinates are acceptable. The scope of this protocol does not evaluate the correction and accuracy of the location estimation technologies.

2. Vehicles are able to verify direct neighbors with direct LOS using the received radio strength signal (RSS) and calculating the sender's relative distance [66].

3. Communication channels between vehicles are secure. Exchanged messages are digitally signed and vehicles are able to authenticate the message sender [64, 51, 29]. We assume that an outsider will not be able to inject false information. All protocol messages are sent by legitimate nodes and carry their true position and mobility information. With such an assumption, we focus our work on securing the integrity of the collected position information.

4. Energy consumption and computation resources are not a major concern in VANETs.

3.4.2 Vehicle Awareness Model

In this section, describe the basic role of a network member. Each vehicle sends its location and mobility information in a beacon message that is transmitted at a fixed rate, e.g. 10Hz. The receivers will validate the beacon message and store the data

of the sender and its location information in a local database. The validation in this step is the message integrity and sender authentication process. The collective data will build the vehicle's awareness of neighboring location information. To maintain accurate information, each record is monitored to check for any inconsistency. For example, if the record was not updated by a beacon message for two consecutive beacon times the record will be obsolete and the vehicle is considered as to be not existing. In the proposed solution, prior to deleting the record, the location verification process will be triggered to check whether the beacon was not received because of a NLOS or a if the vehicle actually moved away from the monitored range of communication.

3.4.3 Position Verification Computation

The position computation for the proposed protocol is based on triangulation calculations. In Figure 3.2, node A wants to verify node C's location; however, direct communication is not possible due to the existence of an obstacle. While node B can communicate directly with both A and C, each node knows its GPS position (x, y) in a two-dimensional plane. Node A sends a request to node B to verify location C with its announced position (x_c, y_c) and mobility vector. B can verify C's location by determining its distance (d_{bc}) using radio measurements, such as RSSI, and comparing the announced (D_{bc}) and measured values. If both values (D_{bc} and d_{bc}) are a match, B will send a response back to A containing the distance d_{bc} and verifying the location of C. Once received, A verifies d_{ab} (using the radio measurement) and calculates the angle θ between the normalized vectors $\overrightarrow{BA}$ and $\overrightarrow{BC}$ where:

$$\theta = \arccos(\overrightarrow{BA} \cdot \overrightarrow{BC}) \tag{3.1}$$

A will then calculate its distance d_{ac} from C using the calculated values d_{bc}, d_{ab}, and θ as follows:

$$d_{ac} = \sqrt{d_{bc}^2 + d_{ab}^2 - 2d_{bc}d_{ab}\cos\theta} \tag{3.2}$$

Node A now has the distance to C using RSS computation (d_{ac}) and the information from the last record update (D_{ac}). However, due to mobility, the actual position has changed since the information was received. To make a fair comparison of both values, both distances, d_{ac} and D_{ac}, must be adjusted to reflect the change using acquired mobility information from both the verification and the last record update, respectively. The

new estimated location of C is calculated such that:

$$\acute{x_c} = x_c + \Delta x \tag{3.3}$$

$$\acute{y_c} = y_c + \Delta y \tag{3.4}$$

where Δx and Δy are the changes in C's location caused by mobility, and $\acute{x_c}$ and $\acute{y_c}$ are the estimated new coordinates of C's location.
The distance to C's new location with respect to both source of data is then computed as follows:

$$\acute{d_{ac}} = \sqrt{(x - \acute{x_c})^2 + (y - \acute{y_c})^2} \tag{3.5}$$

$$\acute{D_{ac}} = \sqrt{(x - \acute{x_c})^2 + (y - \acute{y_c})^2} \tag{3.6}$$

With two sources of information for the distance to C, both values ($\acute{D_{ac}}$ and $\acute{d_{ac}}$) are compared and C is verified when both values match or fall within an error range, $\Delta v\ \Delta t$, where Δv is the change in C's speed and Δt is the time difference between the last record update and the time the reply message was received through the verification process; the records will be updated accordingly.

3.4.4 Position Verification Algorithm

Based on the aforementioned computation method, we built our protocol algorithm using the notation in Table 3.1. The steps for verifying the location information are as follows:

1. Each vehicle maintains a database of its neighbors' information, which is initially gathered and updated by received beacons or group messages. Location and mobility information are monitored to detect inconsistencies, such as unpredicted changes in a node location, mismatches in received information, or expired records. In any such event, the system will trigger the verification process.

2. When an inconsistency is detected, node V is triggered to verify a questioned neighbor C from its list. If V cannot verify C using direct communication or interference is causing calculation errors, the node will send a verification request, Req, to its direct neighbors. The Req message contains $\{Req_{id}, G_{id}, ID_c, Loc_c, M_c, ID_v, Loc_v, M_v\}$, [Alg. 3.1].

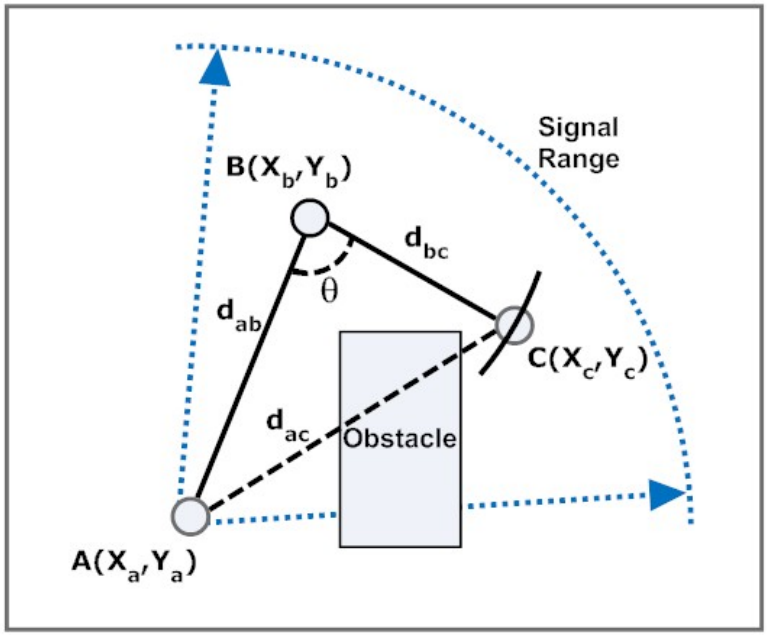


Figure 3.2: Estimating distance between two nodes (A and C) using a third common neighbor node (B).

3. If a node, N_i, receives the request, it will first verify the sender by checking its existence in its neighborhood list. It will then check to determine whether it has a direct communication with C. If it also does not have a direct communication with C, it will mark C in its table as a node to be verified and forwards the message to C. Before forwarding the message, node N_i listens to its neighbors and checks to determine whether any of them has forwarded the same message. If it has been forwarded, the node will ignore the forwarding process and wait for a reply. If it was not forwarded and a maximum number of hops were not reached, it will forward the message. The forwarded message contains the original request, adds (piggybacks) its information as a sender, and updates the hop count. If a reply is not received after a certain time, the message will be discarded and the record for C will be deleted [Alg.3.2].

4. If the request reaches a node, N_i, with direct communication, it will measure its distance (d_c) from C by measuring the received signal strength (RSS). Once measured, N_i compares the measured distance with the distance calculated from the announced position information. If both distances are equal, N_i sends a reply

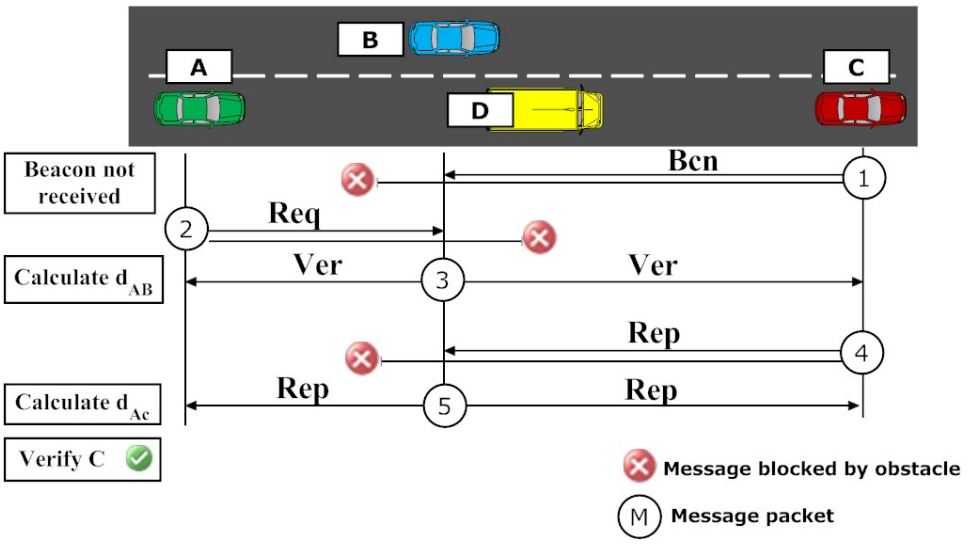


Figure 3.3: CMLVP message exchange process.

(*Rep*) to V with a message containing $\{Req_{id}, G_{id}, N_{id}, Loc_n, M_n, d_{nc}, C_{id}, Loc_c, M_c, Hop_{vc}\}$ [Alg.3.3].

5. When a node, N_i, receives a reply message, it will verify the sender and determine whether it processed the related request. If the request was processed, it will compute and verify the distance to the sender from the received signal and then compute its distance from C. If the distance matches the information in the table, it will mark the record as updated and adds a flag that the node has an NLOS. If the node, N_i, is not the request originator, V, it will forward the reply to V and update the value of d_c with its own. A node may receive replies from different neighbors, which increases the distance computation confidence. If the distance does not match or is not within the acceptable range criteria (within physical communication range and road limits), it will ignore the message and delete the record for C [Alg.3.4].

3.5 Simulations

In order to evaluate the proposed protocol we used NS-2 (Network Simulator-2) ver. 2.34, which is an open source network communication simulator that have been widely

Algorithm 3.1 Request for verification

```
1: while (neighborList.empty() = false) do
2:     for (∀ node ∈ neighborList()) do
3:         if (dataInconsistency(node) = true) then
4:             ▷ Triggers direct communication location verification
5:             VerifyLoc(C)
6:             if (NLOS(C) = true) then
7:                 msg ← Req_c
8:                 Send(msg) to one-hop neighbors
9:                 StartWaitTimer(ReqID)
10:                if (WaitTimeExpire(ReqID) = true) then
11:                    DeleteRecord(C), node is not verified
12:                end if
13:            end if
14:        end if
15:    end for
16: end while
```

Algorithm 3.2 Received a request message

```
1: input: receive(Req)
2: if (verifySender(Req) = true) then
3:     ▷ The sender is authenticated, process the request
4:     if (Group = G_id) then
5:         ▷ the message is for my group
6:         if (NLOS(C) = true) then
7:             ▷ no direct LOS with C
8:             markUpdate(C), marks node C for update
9:             Update(Req_c), update the request message
10:            msg ← Req_c
11:            Forward(msg), forward request to one-hop neighbors
12:        else
13:            ▷ Direct verification is available
14:            if (VerifyLoc(C)) then, verify the location of C (Alg. 3.3)
15:                msg ← Rep_c
16:                Send(msg)
17:            end if
18:        end if
19:    end if
20: end if
```

Algorithm 3.3 Verify claimed position

1: **if** (NLOS(C) = false) **then**
2: ▷ direct communication is available
3: $Measure\ RSS_c$
4: $Compute\ d_c$, from RSS
5: $Compute\ d_{nc} + d_{mob}$, from previously announced data
6: **if** $(d_c\ =\ d_{nc} + d_{mob})$ **then**
7: $return(True, d_c)$, node C is verified
8: **end if**
9: **else**
10: ▷ Multi-hop verification
11: **if** $(Hop_{nc}\ >\ 1)$ **then**
12: $Compute\ \theta$
13: $Compute\ distanc\ to\ sender$
14: $Compute\ d_c$ from RSS
15: $Compute\ d_{nc} + d_{mob}$ from announced data
16: **if** $(d_c\ =\ d_{nc} + d_{mob})$ **then**
17: $return(true, d_c)$
18: **end if**
19: **end if**
20: **end if**

Algorithm 3.4 Received a verification reply

1: input: $receive(Rep_v)$
2: **if** $(verifySender(Rep))$ **then**
3: ▷ The sender is authenticated
4: **if** $(Group = G_{id})$ **then**
5: ▷ The message is for my group
6: **if** $(verifyLoc(C)\ =\ true)$ **then**
7: ▷ The location of C was verified (Alg. 3.3)
8: $neighborList.update(C)$, to update local data
9: **if** $(replyDistination(Rep)\ !=\ me)$ **then**
10: ▷ I am not the request originator
11: $Update(Rep_v, d_c)$, update the reply message
12: $msg \leftarrow Rep_v$
13: $Send(msg)$, forward reply message to one-hop neighbors
14: **end if**
15: **end if**
16: **end if**
17: **end if**

Table 3.1: CMLVP Algorithm Notations

Variable	Description
C	*Claimer (questioned) vehicle*
d_c	*Relative distance to C*
d_{mob}	*Distance traveled by mobility*
G_{id}	*Group ID*
Hop_{vc}	*Hop counter between V and C*
ID_i	*Vehicel i ID*
Loc_i	*Location of node i*
M_i	*Mobility vector for node i*
N_i	*Vehicle N_i*
Req_{id}	*Verification request info*
Rep_{id}	*Verification reply info*
V	*Verifier vehicle*

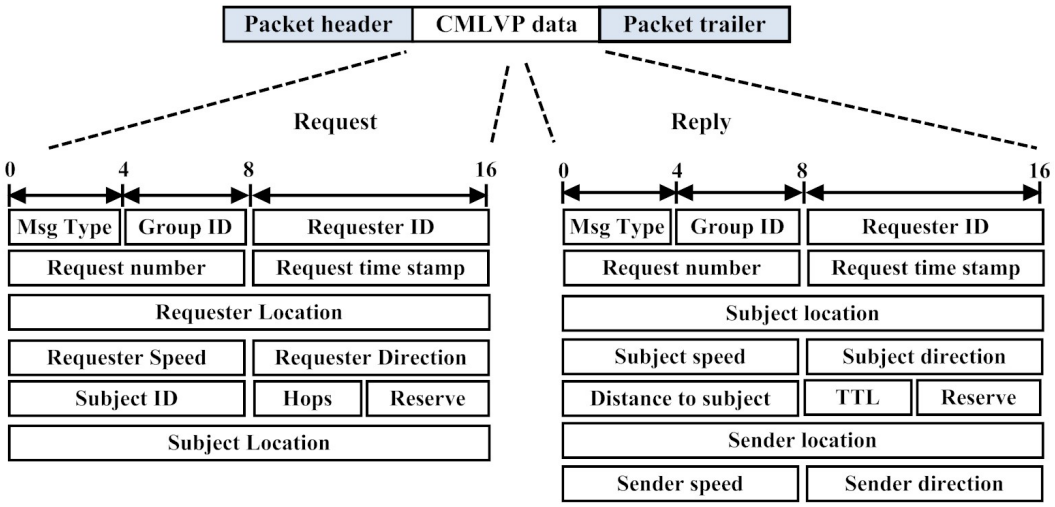


Figure 3.4: The cooperative multi-hop location verification protocol (CMLVP) packet format.

used and accepted in the research area. In this section we will discuss our simulation environment setup, parameters and experiment methodology.

3.5.1 Obstacle and Mobility Model

One of the main challenges in VANET simulation is realistic mobility and propagation with obstacle effects [85, 18]. In NS-2, there are three types of propagation models:

free space, two-ray ground reflection, and shadowing propagation. These propagation models do not fulfill our requirements to simulate our protocol because they are used for LOS communication between wireless nodes. As we have discussed in the literature review (Section 2.8), there are no mathematical models that presents the signal propagation affected by moving obstacles. For our work, we need to simulate obstacles that present road vehicles with their own mobility and object dimensions. To overcome this limitation, we have developed our own obstacle model.

To determine whether a LOS is obstructed by an object or not, we need to determine whether the obstacle lies between the sender and receiver. To do so, as shown in Figure 3.5, we present the object as a line segment (L_o) from its front end (x_3, y_3) to its back end (x_4, y_4). We also present the LOS between the sender (x_1, y_1) and receiver (x_2, y_2) as another line segment (L_c). The lines can be presented as follows:

$$L_c: \quad A_1\ x + B_1\ y = C_1 \tag{3.7}$$

$$where, \quad A_1 = y_2 - y_1$$

$$B_1 = x_1 - x_2$$

$$C_1 = A_1\ x_1\ +\ B_1\ y_1$$

$$L_o: \quad A_2\ x + B_2\ y = C_2 \tag{3.8}$$

$$where, \quad A_2 = y_4 - y_3$$

$$B_2 = x_3 - x_4$$

$$C_2 = A_2\ x_3\ +\ B_2\ y_3$$

A NLOS condition occurs where the two line segments intersect. To find an intersection point (x, y) we solve Eq.3.7 and Eq. 3.8 such that:

$$det = \begin{vmatrix} A_1 B_1 \\ A_2 B_2 \end{vmatrix} \tag{3.9}$$

If $(det \neq 0)$ then L_c and L_o intersect at point (x,y) such that:

$$x = (B_2\ C_1 - B_1\ C_2)/det \tag{3.10}$$

$$y = (A_1\ C_2 - A_2\ C_1)/det \tag{3.11}$$

If the point exists, it must satisfy the following conditions in order to consider an obstacle affect:

$$min(x_1, x_2) \leq x \leq max(x_1, x_2)$$

$$min(y_1, y_2) \leq y \leq max(y_1, y_2)$$

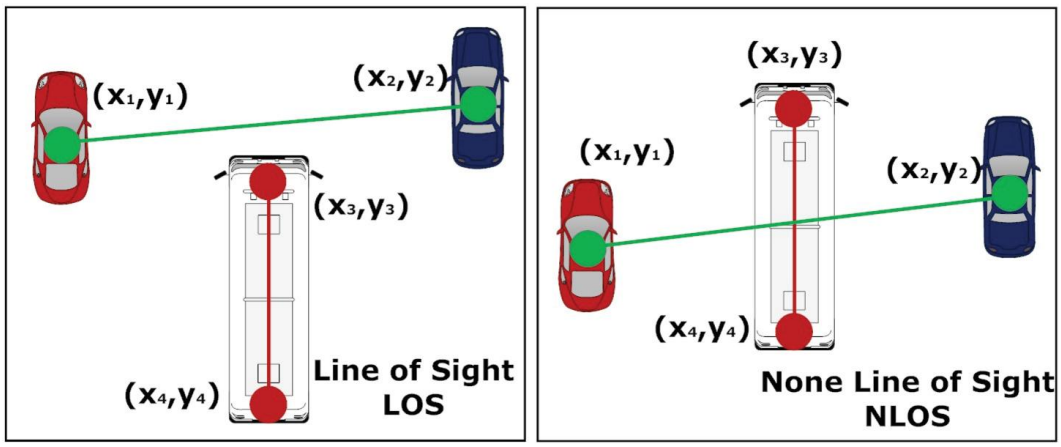


Figure 3.5: An obstacle (bus) blocking the line of sight of two cars

To maintain obstacle mobility, the obstacle's front-end (x_3, y_3) is attached to a vehicle node that is marked as an obstacle, such as a truck. The back-end of the obstacle is calculated based on the vehicle location, moving direction, and length of the obstacle. In our simulation, we used an obstacle length of 10-15m. In our experiments, we consider an NLOS condition to be a total signal block that results in a message drop as described in (Alg 3.5).

Algorithm 3.5 Moving obstacles interference

```
1: input : Received Msg
2: comLine(Sender,Receiver)
3: ▷ compute the line segment (L_c) between the sender and receiver
4: msgDrop = false
5: NLOS = false
6: ▷ direct communication is the default state
7: for (∀ node ∈ Obstcles) do
8:     ▷ check if L_c intersect with any L_o
9:     obstacleLine()
10:    ▷ compute the obstacle line segment (L_o)
11:    if (intersection(L_c, L_o) = true) then
12:        ▷ L_c and L_o intersect
13:        NLOS = true
14:        ▷ NLOS exists between the sender and receiver
15:    end if
16: end for
17: if (NLOS = true) then
18:    msgDrop = probNLOS()
19:    ▷ the probability of message delivery under NLOS
20: end if
21: return msgDrop
```

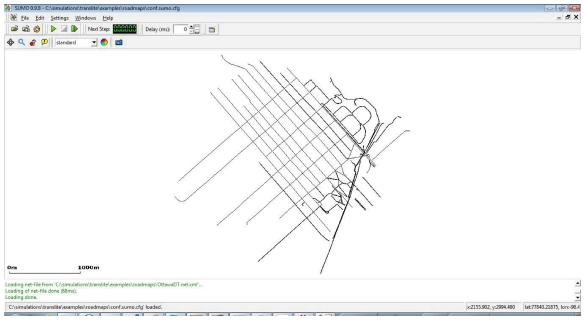
As for mobility, we used the traffic and network simulation environment ($TraNs$)[67] to generate realistic mobility traces for NS-2. $TraNs$ parses traffic simulation movement from simulation of urban mobility ($SUMO$) and generates a trace file that can be easily imported to NS-2. The generated traffic supports realistic VANET characteristics, including collision-free movement; lane changes; maintaining distance between vehicles; and the right-of-way rule, which includes traffic lights. Using the $TraNs$ map importing features, we used maps of highway 417 in Ottawa, Canada, to simulate a representative highway environment and down town area to represent an urban city environment (Fig. 3.6). Table 3.2 summarizes the parameters used in these simulations.

3.5.2 Performance Evaluation Aspects

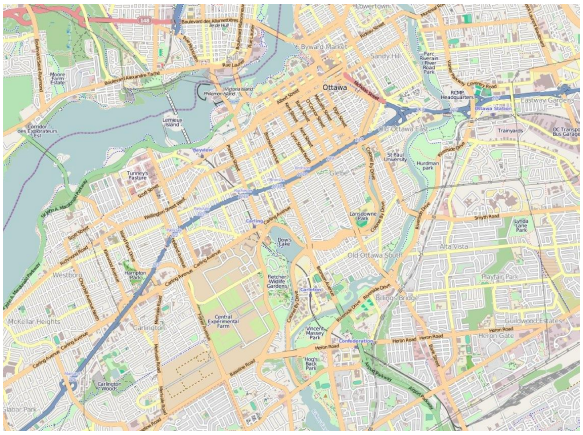
In order to evaluate the proposed solution, we focus our attention on the aspects that will secure the location verification process and leads to reach the planned objectives. The following aspects were considered to evaluate the performance of the proposed protocol:

1. *Neighborhood awareness and location verification*: The main objective of the pro-

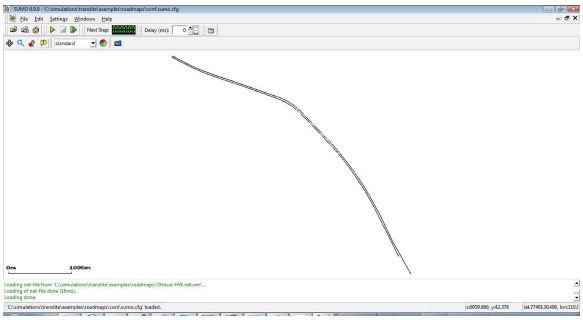
(a) The city of Ottawa



(b) Simulation city map by SUMO



(c) Highway-417 from the city of Ottawa



(d) Simulation highway map by SUMO

Figure 3.6: Simulation map for the city and the highway environment.

Table 3.2: CMLVP Simulation Environment Parameters

Parameter	**Value Setting(s)**
Radio Propagation	*Two-ray ground, Nakagami*
Antenna Type	*Omni antenna*
MAC Layer	802.11*p*
Radio Range	300*m*
Beacon Freq	1 *Hz*
Max Hop	4
Data Rate	6 *Mbps*
Packet Payload	152 *byte*
Number of Vehicles	100–1000
Speed Limits (*Highway*)	0–100*km/h*
Road length (*Highway*)	20*km*
Speed Limits (*Urban*)	0–50*km/h*
Road Area (*Urban*)	3*km* x 4*km*
Simulation Time	15–30*Min*

tocol is to allow the vehicles to have better knowledge about their surroundings. We want to examine the awareness rate under NLOS conditions and evaluate the protocol's effect on a vehicle's information about surrounding neighbors and their locations. By studying this aspect, we examine the number of vehicles the node had detected through beacon message and compare it with the actual number of proximate vehicles. An ideal awareness rate is achieved if the number of detected neighbors matches the actual number of surrounding vehicles within the communication range.

2. *Channel capacity utilization*: The proposed protocol generate request and reply messages to verify the location of a questioned node. It is important to evaluate the protocol's consumption of network resources. Evaluating the channel capacity utilization will help examine the number of messages generated by the protocol and how much channel capacity they consume. This aspect will also examine the protocol's scalability and discuss the factors that support or limit scalability.

3. *Message delivery success rate*: The NLOS condition between two vehicles will affect the message delivery between them. The CMLVP should allow vehicles to verify the location of a node that is blocked by NLOS and determine its communication link state. To show the improvement that the proposed protocol provided, we use

the message delivery success rate as an evaluation point. This aspect will examine the success rate of message delivery among vehicles within the same range of communication using single-hop messaging. With the effect of NLOS, we study the impact of location verification feedback on the selection of the message delivery method (using single-hop or multi-hop) for nodes that are in the same communication range.

4. *Response time*: The location verification protocol allows vehicles to determine the current state of the questioned node. A vehicle should be able to determine whether the node is in its announced position or has moved away and its record needs to be deleted. By examining the response time, we compute the time for a request to successfully verify a questioned node.

5. *Security counter measures*: The CMLVP was developed to secure the location information of vehicles. However, examining the protocol against possible threats we help understand the protocol's features and limitations. Through this aspect, we will discuss the protocol's security countermeasures and evaluate the system's resilience to possible security threats.

3.5.3 Results and Findings

In this section, we discuss the results on using an extensive set of simulation experiments we carried out to evaluate the performance of the proposed scheme.

Neighborhood awareness and location verification: The main objective for the proposed scheme is to increase the neighborhood awareness rate for vehicles in NLOS conditions. We can observe in Figure 3.7 that obstacles had a negative impact on the neighborhood awareness rate. In a highway scenario of 200 vehicles with 25% obstacle inclusion, the average awareness rate dropped to 30% using single-hop beaconing to update position information. On the other hand, multi-hop beaconing did improve awareness, but the data were inconsistent; the updates depended on receiving forwarded beacons, which were interrupted by the obstacles. Moreover, multi-hop beaconing has network performance issues that may limit its usage [59]. By using CMLVP, the average awareness rate increased to more than 80% when using the approach of verifying requests whenever a neighbor's record was inconsistent. Moreover, whenever a verification reply was received, the node recognized that an NLOS situation existed with the questioned

neighbor and did not expect a direct update from it. The node sent a request to determine whether the marked neighbor still existed before deleting a record from the list. Such a scheme allowed vehicle to be more aware about the position of their neighbors.

In Figure 3.8, the graph shows the average awareness rate for different vehicle densities with 25% obstacle inclusion in a urban city environment. We can observe the improvement in the neighborhood awareness rate using the CMLVP. For example, in a 400-vehicle scenario the average awareness rate was 42%. By activating the CMLVP, the neighborhood awareness rate improved reaching an average of 75%. The average neighborhood awareness rate of different scenarios, with 95% confidence interval, are presented in Table 3.3 and plotted in Figure 3.9. The results show the impact of obstacles on awareness and the improvement achieved using our proposed approach. As the density increases the awareness level drops because of the impact of packet collisions.

To study the vehicle's neighborhood awareness, we examined its knowledge of vehicles with respect to their distance. In Figure 3.10 and Figure 3.11, the graph shows the average awareness rate of a vehicle in relation to its distance in a urban city and a highway environment, respectively. The vehicle has less awareness of farther nodes because of the impact of hidden terminal problem in a wireless environment. For example, in a 400-vehicle city environment scenario, the average awareness rate for vehicles within 50m is 90% while the awareness rate about vehicles at 300m is 30%. The CMLVP improved the awareness increasing the rate about vehicles at 300m to an average of 50%. On the other hand, in a 400-vehicle highway environment scenario, the awareness rate for vehicles at 50m is at 95% and for vehicle at 300m the average was at 40%. Using CMLVP, the average awareness rate about vehicles at 300m improved reaching to an average of 92%. The decrease in the neighborhood awareness rate in the highway scenarios is less than the downtown scenarios because of the distribution of vehicles along a highway road is sparse, while in a downtown area the vehicle are more closer. Making the communication channel more vulnerable to packet collision and the affect of the hidden terminal problem.

Figure 3.12 shows the affect of vehicle density within the communication range on neighborhood awareness in a city environment. The awareness of surrounding vehicles drops as the density of vehicles increases. The close distances between group of vehicles impact the transmission on each other as transmissions from one group can impact the neighboring group. While in a highway environment, vehicles are farther from each other which reduces the impact of signal interference, as shown in Figure 3.13.

As we can see from the simulation results, the CMLVP improved the neighborhood

Table 3.3: The average neighborhood awareness rate in a city environment with 95% confidence interval.

	FRB-10Hz		with CMLVP	
Density	Low	High	Low	High
200	0.4235	0.5165	0.8038	0.8489
400	0.4091	0.4436	0.7369	0.7595
600	0.3863	0.4319	0.6908	0.7529
800	0.2313	0.3105	0.6714	0.7341

awareness rate for the vehicles that are affected by NLOS. Such an improvement will lead to the improvement of VANETs location-based application.

Channel Capacity Utilization: The protocol uses a cooperative approach, which requires an exchange of messages among neighboring vehicles. Therefore, we want to examine the protocol's network resource consumption. We monitored the volume of messages exchanged among vehicles and how much the scheme uses a wireless communication channel. We used a packet payload size of 152 bytes, which included request information and location information about a questioned node. Figure 3.14 shows the average channel utilization of 6Mbps channel capacity. The results showed an average of less than 20% channel capacity with different vehicle densities which includes the CMLVP messages and periodic beacon messages. Using the cooperative approach and enabling vehicles to update their records based on other requests helped to reduce the number of messages generated. Table 3.4, illustrated in Figure 3.18, shows the average consumption of a 6Mbps bandwidth under different scenarios with a 95% confidence of interval.

In Figure 3.15, the graph shows the protocol consumption of bandwidth in a highway scenario. The protocol's messages consumed 5–7% additional resources. Figure 3.16 shows the consumption rate in an urban environment which also shows that the CMLVP used additional resources. Although it shows that it has less messages than the highway scenario, the accessible resources limits the number of messages in a urban environment because of the higher density.

Allowing the vehicles to utilize the information in cooperative manner helped reduce the number of messages generated by the CMLVP. In Figure 3.17, the graph shows that the channel bandwidth can be saturated if cooperative updates are not allowed and each

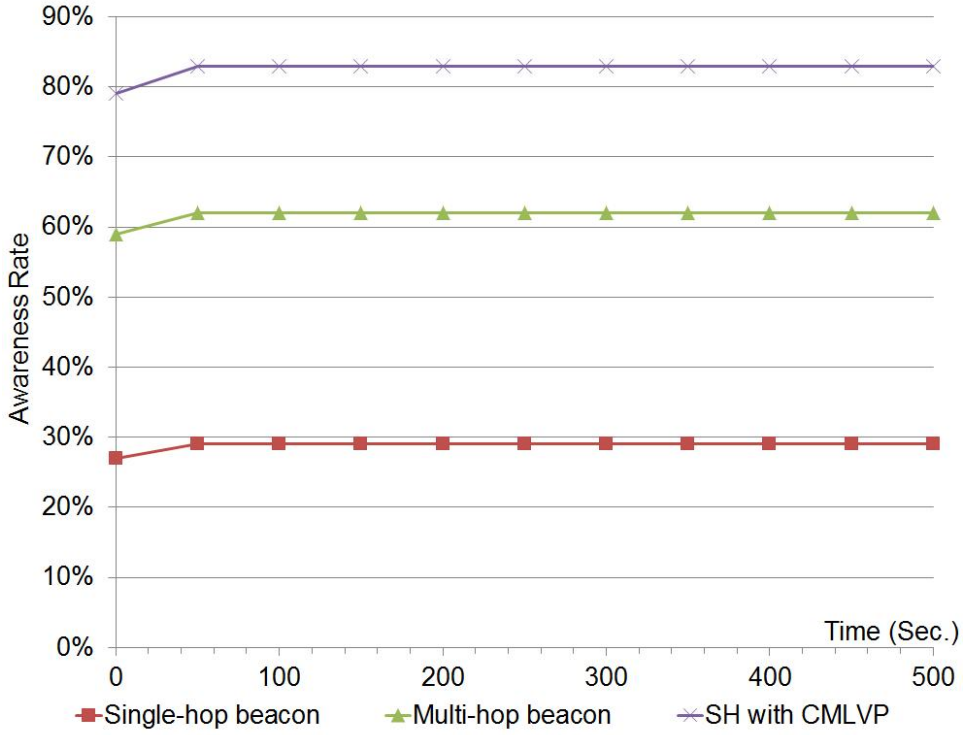


Figure 3.7: Average awareness rate comparison between single hop, multi-hop beaconing and CMLVP in a 200-vehicle with 25% obstacle simulation in a highway scenario.

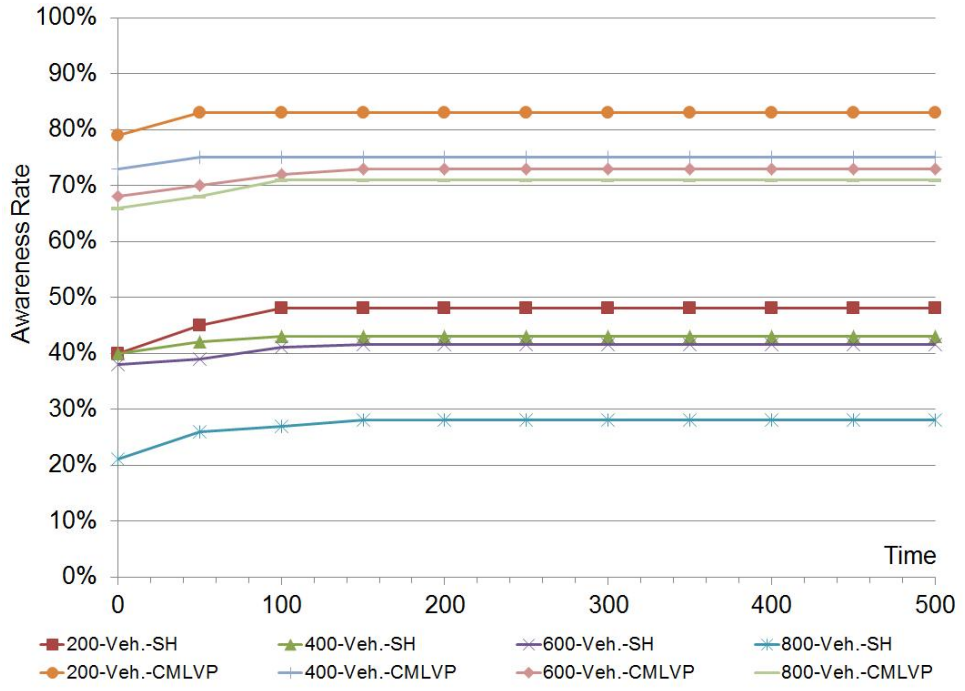


Figure 3.8: Average awareness rate for different vehicle density with 25% obstacles in an urban city environment.

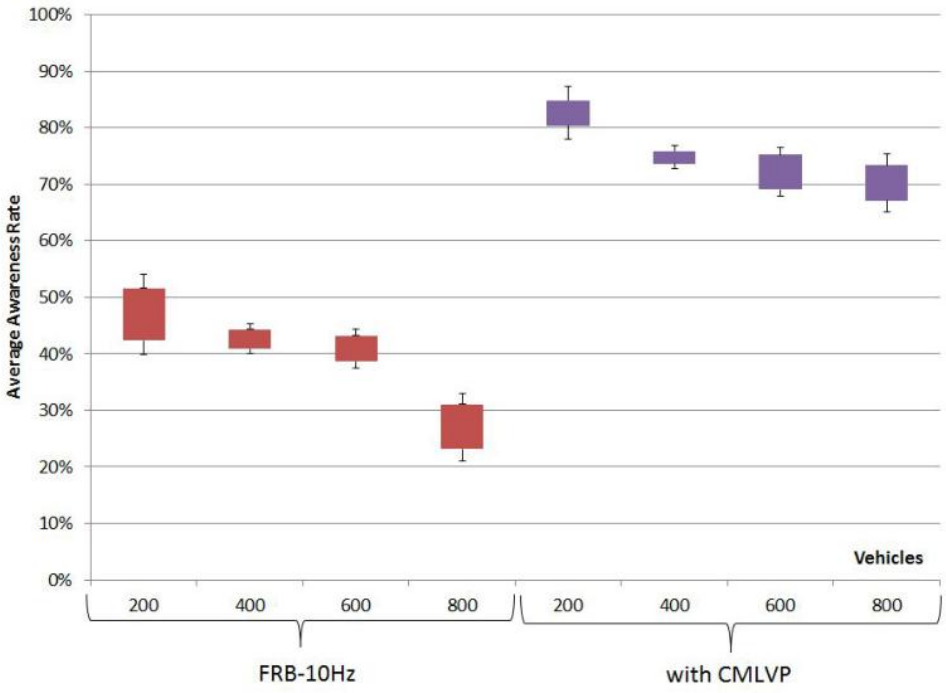


Figure 3.9: The average neighborhood awareness rate in a city environment with 95% confidence interval.

node has to generate its own verification requests, especially in a higher-density neighborhood.

Communication Complexity: To study number of messages generated by the CMLVP and its network resource consumption, we will discuss the communication complexity. with CMLVP, the vehicle will generate a request message if it requires to verify the location of a neighboring node. There for the total number of request messages ($ReqMsg_{total}$) can be expressed as:

$$ReqMsg_{total} = \sum_{i=1}^{n}((p_{nlos} \times NList_i) - (p_{req} \times NList_i)) \tag{3.12}$$

Where, n is the total number of vehicles, p_{nlos} is the probability of NLOS condition, $NList_i$ is the neighborhood list size for node i, and p_{req} is the probability of receiving a request message from a neighboring node.

The number of forwarded messages $FwdMsg_{total}$ is calculated by:

$$FwdMsg_{total} = \sum_{i=1}^{n}(p_{req} \times NList_i) + \sum_{i=1}^{n}(p_{rep} \times NList_i) \tag{3.13}$$

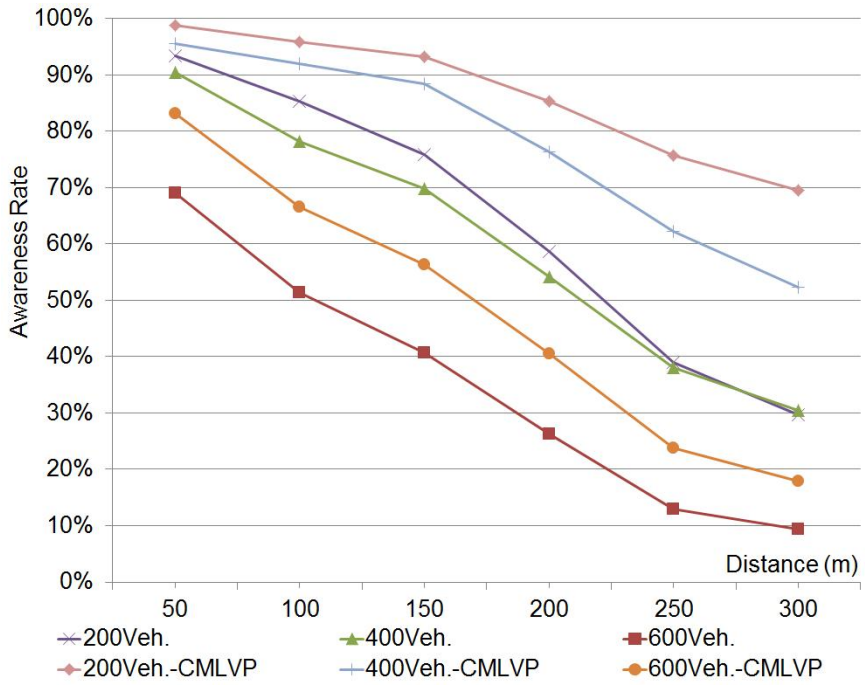


Figure 3.10: Average awareness rate vs. distance for different vehicle density with 25% obstacles in an urban city environment.

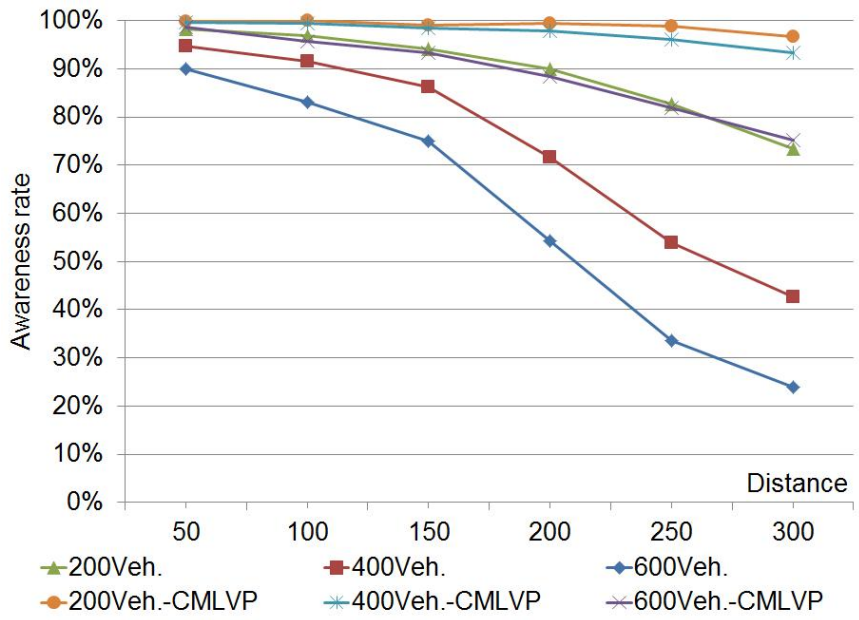


Figure 3.11: Average awareness rate for different vehicle density with 25% obstacles in a highway environment.

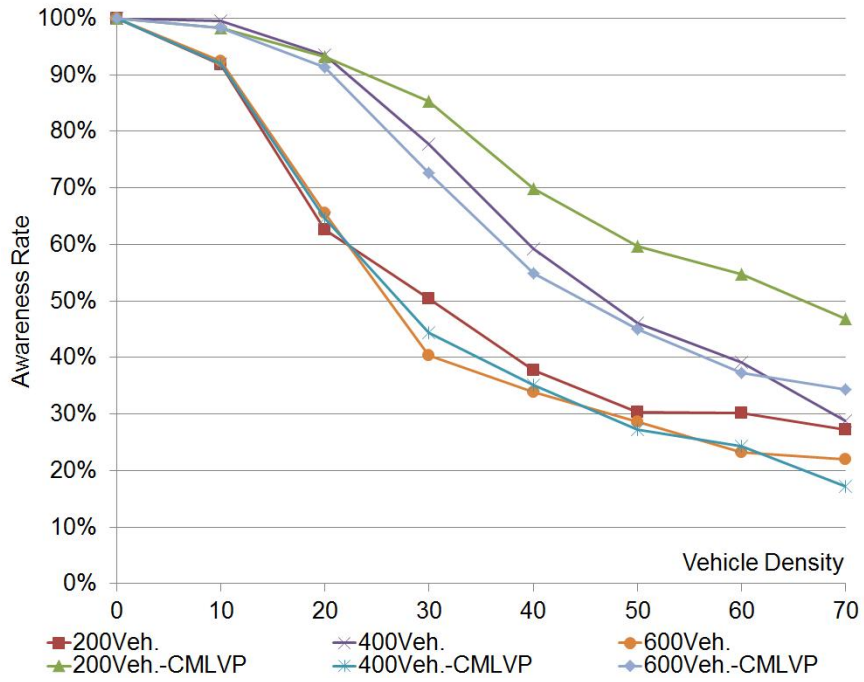


Figure 3.12: Average awareness rate for different vehicle density with 25% obstacles in an urban city environment.

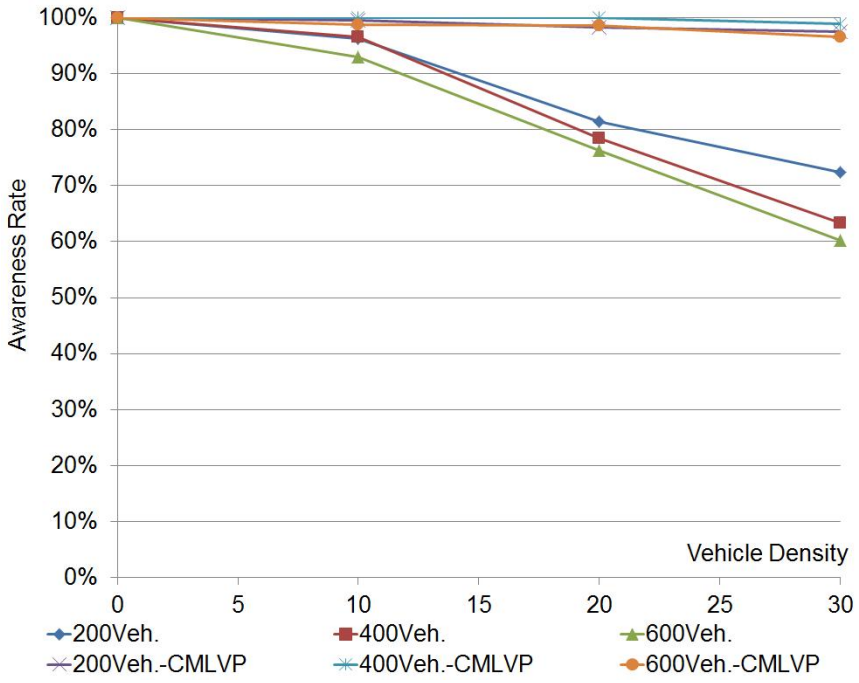


Figure 3.13: Average awareness rate for different vehicle density with 25% obstacles in a highway environment.

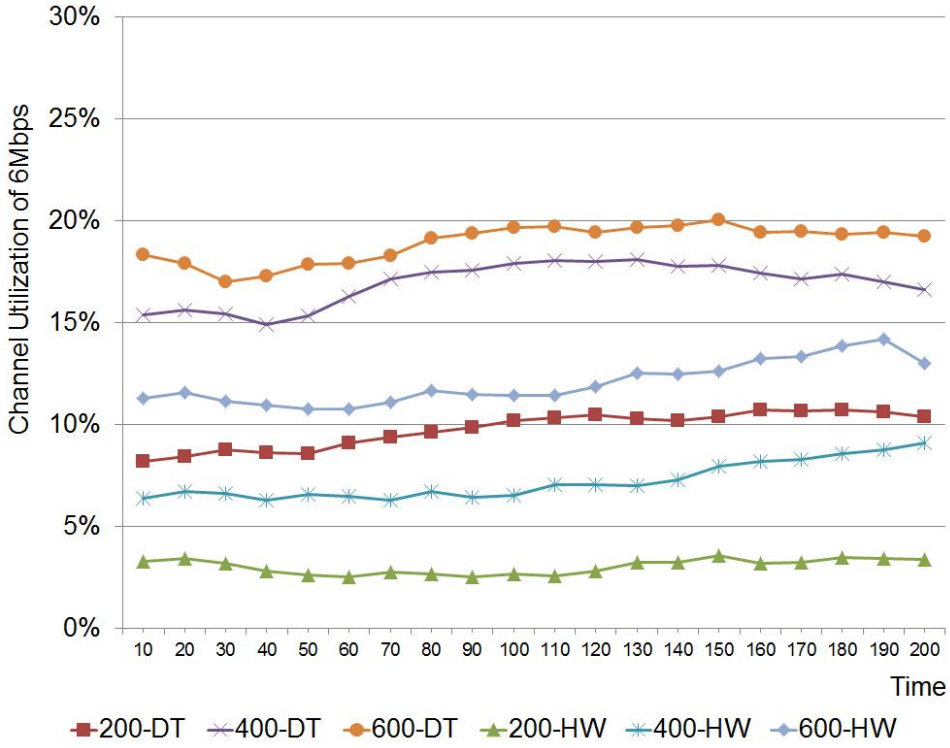


Figure 3.14: Average channel capacity utilization of 6Mbps for different density with 25% obstacles, in a downtown (DT) and highway (HW) environment.

The number of reply messages can be calculated:

$$RepMsg_{total} = \sum_{i=1}^{n} (p_{req} \times (1 - p_{nlos}) \times NList_i) \tag{3.14}$$

Therefore, the complexity is of order $O(n)$ where n is the vehicle density.

Message Delivery Success Rate: Using CMLVP should help vehicle to be aware of the communication link state with its neighbors. The vehicle will know which node has a direct communication link with and which is affected with a NLOS condition. We examined the message delivery success rate among vehicles within the same communication range to study the effect of obstacle and the improvement achieved by the CMLVP. In Figure 3.19, we compared a direct single-hop approach delivery to an approach that used CMLVP and NLOS condition information to deliver a message in a city environment. The vehicle will randomly select one of its neighbors and send a message to it.

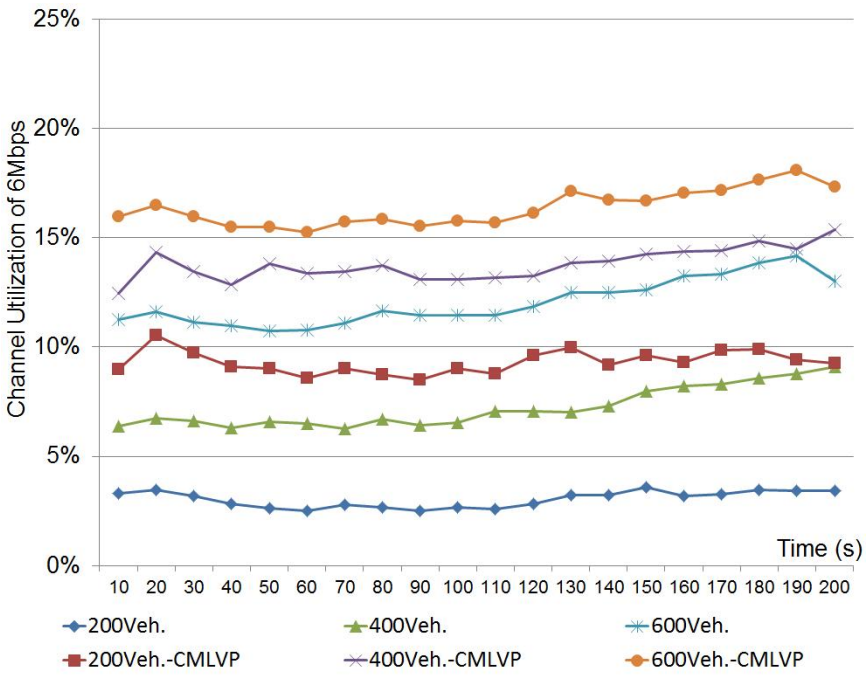


Figure 3.15: Average channel capacity utilization of 6Mbps for different density with 25% obstacles in a highway scenario.

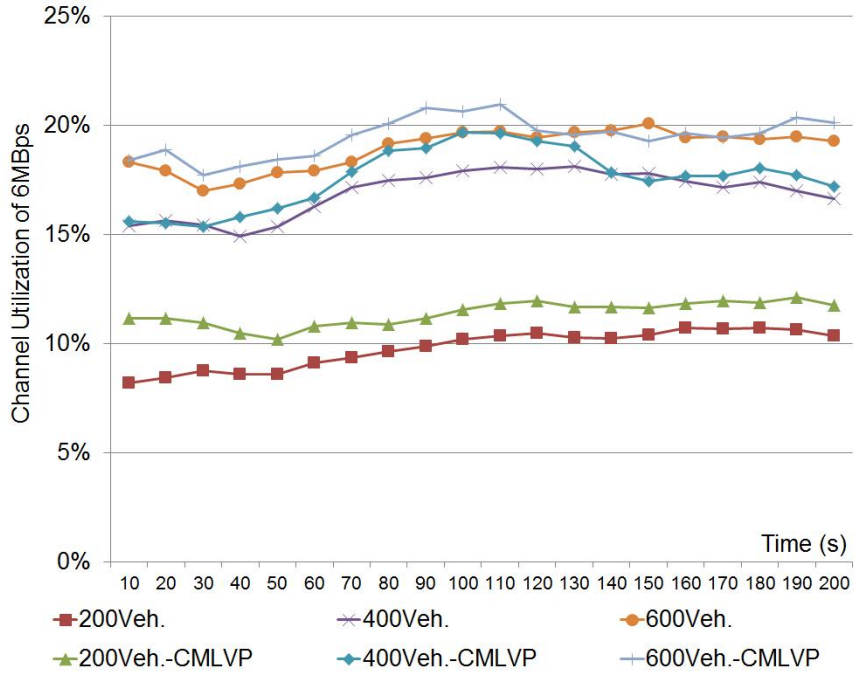


Figure 3.16: Average channel capacity utilization of 6Mbps for different density with 25% obstacles in a city scenario.

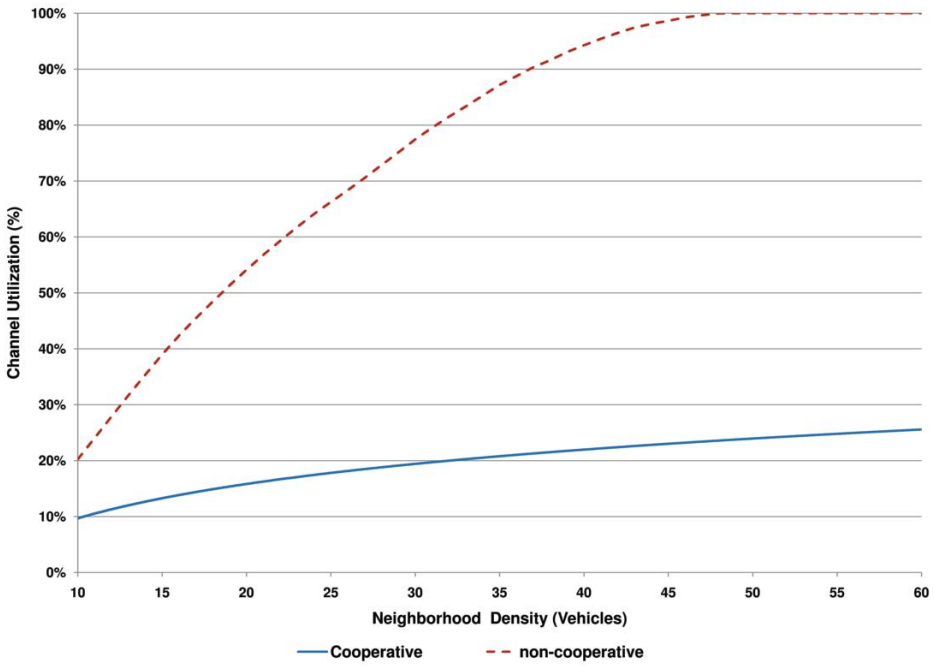


Figure 3.17: Average channel utilization using cooperative and non-cooperative updates. As the neighborhood density increases the amount of requests increases. Cooperative updates help reduce the amount of generated messages.

By determining the destination node, the sender determines whether it can forward the message directly or has to forward it with the assistance of other nodes. The results show an improvement in the delivery success rate and the impact of moving obstacles on direct messaging. For example, in a 200-vehicle scenario, the message delivery success rate improved about 10%. Such results may affect network applications and service, for example, routing protocols rely on a single-hop communication approach for vehicles within the same physical range of communication.

Process Time: Vehicles will use CMLVP to verify a node and determine whether it should keep the node's record or delete it. We examined the average processing time that a request takes from generation until a verification reply is received. Figure 3.20 shows that the average processing time increases slightly as the density increases due to the increase in the number of processed and queued messages. With different vehicle densities, the average processing time for a verification request is less than 200ms.

Table 3.4: Average bandwidth consumption of 6Mbps with 95% confidence interval.

		FRB-10Hz		with CMLVP	
Vehicles	Scenario	Low	High	Low	High
200	Downtown	0.0812	0.1144	0.1034	0.1241
400	Downtown	0.1491	0.1893	0.1493	0.2025
600	Downtown	0.1718	0.2066	0.1776	0.2119
200	Highway	0.0234	0.0311	0.0830	0.0940
400	Highway	0.0547	0.0739	0.1238	0.1391
600	Highway	0.1003	0.1224	0.1479	0.1651

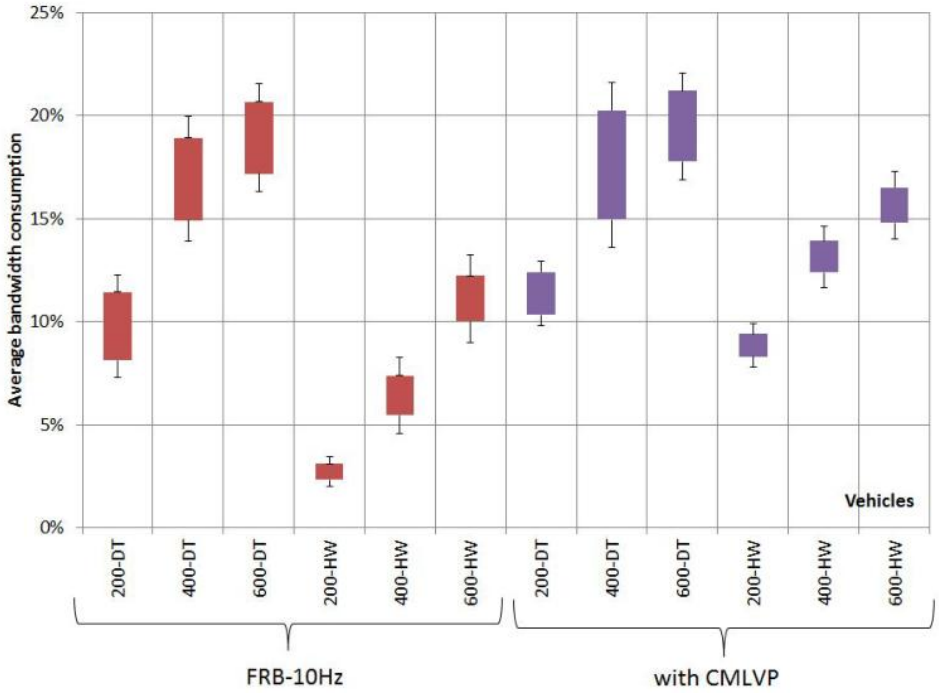


Figure 3.18: Average bandwidth consumption of 6Mbps with 95% confidence interval.

Security Attack Resilience: To evaluate the protocol's security measures, we included malicious nodes in our simulations. The malicious nodes executed different attacks that might affect the protocol. Attack options such as message forgery, reply attacks, false requests, reply message generation, and selfish nodes were made available to the malicious nodes. The results (shown in Figure 3.21) indicated the protocol's resilience to such identified attacks. The number of malicious nodes ranged between 25% and 75%. The awareness of a typical node did not change significantly with the increase in malicious

Table 3.5: Message delivery success rate with 95% confidence interval

	FRB-10Hz		with CMLVP	
Density	Low	High	Low	High
200	0.4027	0.4419	0.5352	0.5560
400	0.1195	0.1533	0.1822	0.2062

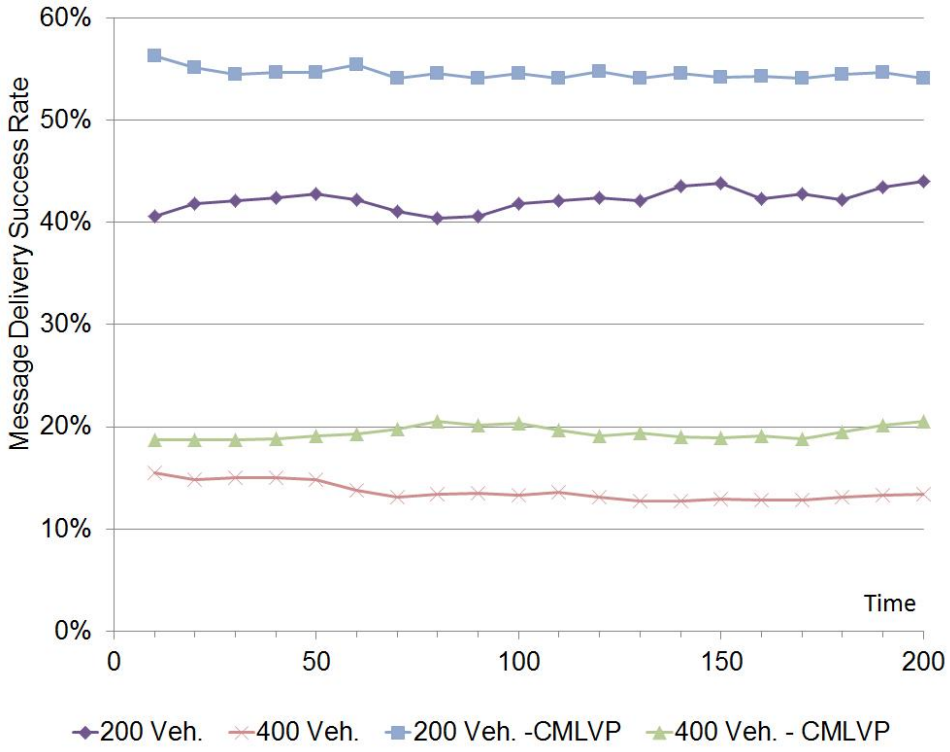


Figure 3.19: Average message delivery success rate for vehicles within the same range of physical communication using single hop vs. utilizing location verification information

nodes. This result occurred because we took into consideration security measurements in our protocol, including verification of the sender, tracking exchange requests, and setting a lifetime for requests. These measures helped to secure our protocol from most of the identified threats. Due to the protocol's cooperative approach, selfish and uncooperative nodes are the greatest threat to its functionality.

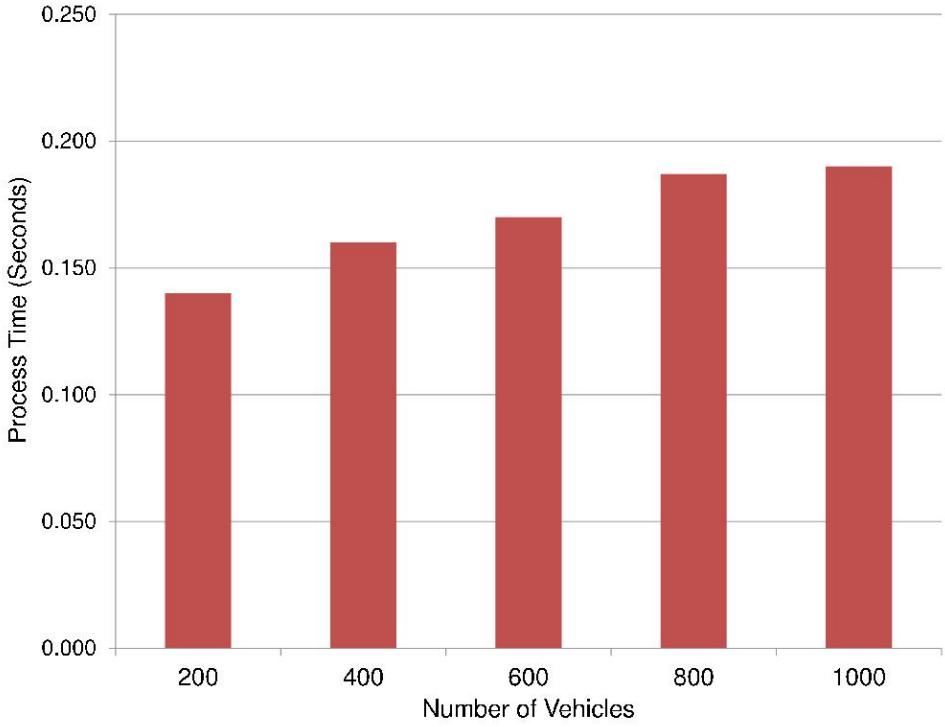


Figure 3.20: Average process time for a successful verification requests.

3.6 Solution Aspects and Security Measures

To help us develop the proposed scheme, we discussed, in section 3.3, the security requirements for a proposed location verification protocol. In this section, we discuss the security measures and related aspects of our proposed protocol:

1. *The proposed solution should increase neighborhood awareness and vehicles' knowledge about surrounding nodes under NLOS conditions*: Each vehicle maintains a database containing information about nearby neighbors. However, obstacles can prevent messages from reaching their destinations. When this occurs, a vehicle will not be able to directly verify one of its neighbors. The proposed cooperative multi-hop approach validates the location of a questioned node and recovers from the NLOS condition by trying to reach the destination through available proximal nodes. The simulation results showed awareness improvement, which will help to secure the integrity of neighborhood awareness and location information.

2. *Monitor localization information, detect data inconsistencies, and validate integrity*: Neighborhood awareness is continuously checked in the proposed system. Mobility

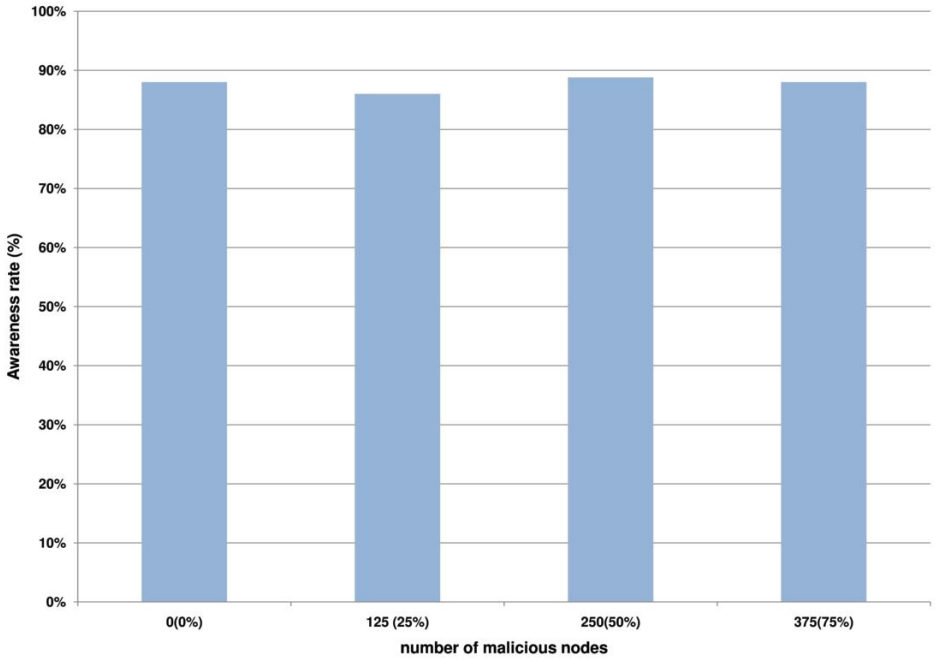


Figure 3.21: Average awareness rate of security attacks using a different number of malicious nodes in a 500-vehicle simulation.

and changes in driving behavior will result in changes in the data. Once an inconsistency is detected, such as a failed update or current information not matching a received update, the vehicle sends a verification request to validate the questioned node in order update its information.

3. *The vehicle should avoid total dependency on periodic incoming beacons and update messages*: Vehicles update their information using in-bound beacons and group updates transmitted through direct communication. The requesting node that detects inconsistencies in its database initiates location verification. The ability to question a node's location eliminates the total dependency on received beacon messages. Moreover, enabling a vehicle to request verification will enable the detection and reduce the effect of false position information sent by malicious nodes.

4. *Maintain confidentiality and message authentication*: As we stated in our assumptions, communication channels are secure and vehicles are able to validate sender and message integrity using digital signatures. Solutions such as the IEEE 1609.2 standard prevent unauthorized vehicles from injecting false messages. In addition, the system provides the ability to authenticate the sender while preserving

its anonymity.

5. *Validate processed information*: Each receiving node verifies the request or reply message forwarding node. If the sender is within the receiver's range and exists in its neighbor list, it will accept the message for processing. This verification process occurs for every message hop. Each request has a lifetime; once it expires, any related message is ignored. This security measure will eliminate the chance of processing false requests or replies that can be injected into the network.

6. *Support availability in a large-scale environment*: The verification process is the component that generates request messages. Every neighbor listening to the propagated message marks the claimed vehicle for verification. Once the reply is received, the nodes that marked their records will update their information once verified. This will reduce the number of generated messages used to verify a single node by using multiple requests at the same time. The protocol controls the number of hops through which a message can be forwarded by setting a maximum hop size. As shown in Figure 3.17, the cooperative approach reduces the utilization of channel capacity.

7. *The cooperative multi-hop location verification protocol (CMLVP) can help to secure localization services*: CMLVP helps vehicles to verify their neighbors when direct communication between the verifier and claimer is blocked. Neighbors cooperatively verify the claimer position and forward updated information to the verifier. If the direct verification fails, such as when using RSS measurement, the vehicle triggers the CMLVP protocol and checks the existence of the questioned vehicle before removing it from its neighbor list. This will secure the data integrity of neighborhood awareness and secure localization information when exchanged with neighboring nodes.

8. *CMLVP can help prevent misguiding localization services due to drivers' behavior*: As we described in the adversary model, drivers' experiences with technology can result in individuals using system limitations to achieve their own goals, such as avoiding being tracked by authorities. CMLVP helps to track vehicle location information and leverage other vehicles' updates. Vehicles that try to hide behind large vehicles to avoid direct communication with a certain vehicle can still be tracked using the cooperative approach.

9. *Protocol limitations*: Our proposed protocol is based on a cooperative approach. The protocol assumes that there is at least one shared neighbor that has a direct communication between the requester and the questioned vehicle. Without a shared neighbor, the requester will fail to receive a verification reply and drop the vehicle record from its database.

3.7 Summary

Obstacles can have a negative effect on drivers real-time traffic hazard awareness, which will effect some critical safety transactions such as merging with traffic, responding to sudden traffic pattern changes, and blind spot awareness. A state of non-line-of-sight (NLOS) between two vehicles may result in ignoring each other's existence while they are just a few meters apart. We believe that neighborhood awareness is essential to supporting reliability and integrity in VANET applications. Current VANET location verification solutions assume that direct communication among vehicles is available. In this chapter, we developed a collaborative protocol to verify an announced position when a direct communication between the questioned node and verifier is not possible. In addition to verifying a node location in a multi-hop cooperative approach, several security measures were included to improve message integrity, such as monitoring outgoing requests and reply messages. In addition, we presented an obstacle simulation model to simulate the affect of moving obstacles on the communication between two neighboring nodes. The simulation results showed that the proposed cooperative multi-hop location verification protocol (CMLVP) increased vehicles rate of neighborhood awareness under the effect of simulated obstacles. The exchanged messages helped to update neighboring vehicles records and increased awareness for other nodes that cooperatively forwarded requests and replies. A solution such as the one we propose will help to maintain the localization service's integrity and reliability, providing reliable position information for upper-level applications.

Chapter 4

Adaptive Group Beaconing and QoS Provisioning

4.1 Introduction

Many of vehicular ad-hoc network (VANET) applications are envisioned to be location-based, which requires the position and current status of surrounding vehicles and events. The reliability of the delivered services depends on the accuracy and availability of received location information. Location and mobility information can be exchanged among neighboring vehicles using periodic beacons. In a dense area, periodic beacon messages may cause communication channel congestion that will increase the probability of packet collision and cause delays in message delivery. A study by Tian et al.[102] showed that, in a road segment with 100 vehicles, beacon message delivery can suffer a packet loss that reaches up to 40%. High packet losses in neighborhood information will affect the reliability and integrity of safety and location-based applications, and they will also initiate the security risk of a denial-of-service (DoS) attack caused by legitimate periodic messages.

QoS provisioning is important in a communication network with multiple delivered applications and serving different users. In a wireless and distributed environments, QoS provisioning is a challenge where network resources are consumed by exchanged messages among nodes. With growing number of vehicles on the road and number of applications envisioned for VANETs, the network services providers and authorities will require the control on network resources. Which will also secure network and applications deliverables and guarantee their availability.

In section 2.2, we have reviewed studies that have evaluated and discussed performance issues caused by periodic message transmission. Solutions were proposed to avoid packet collisions in MAC layer by using different scheduling and congestion control mechanisms[7, 124]. Other researchers tackled the issue on higher level by reducing the beacon rate using an adaptive beaconing approach[84, 93]. Studies have also discussed DoS attacks in different layers of wireless ad-hoc networks and performance issues caused by periodic message transmission[30, 32].

4.1.1 Motivation and Challenges

With the increasing number of vehicles traveling in cities and limited expansion of paved roads, traffic congestions are highly expected. With VANET, safety and road assistant application will provide the vehicles' operators with knowledge of the current situation of the road they will drive through. This will help them decide whether to continue on the same path or divert to another route.

In VANETs, vehicles exchange their position information with their neighbors through periodic beacon messages. In dense areas, a massive amount of message may saturate the network and prevent critical application from acquiring the proper resources to exchange their messages. To resolve such potential threat, adaptive beaconing can adjust a vehicle's beacon rate based on defined criteria. In VANET, high mobility and rapid change in vehicles' location presents a challenge in detecting traffic congestion and providing secure and accurate position information.

The wireless and mobility nature of VANETs limits the amount of accessible resources which will increase the chances of packet collision and force nodes to delay or drop messages [92]. A denial-of-service (DoS) risk can be developed using legitimate periodic and event messages in dense areas which can impact the network performance by consuming communication channel resources. As the number of vehicles increases, the more channel bandwidth resources are required. Simple beacon messages are also affected by the increasing number of vehicles as shown by simulation in Figure 4.1 preventing their actual intent to update vehicle location. This will also apply to applications that want to send messages to other vehicle while they are struggling to send their beacon messages. Such phenomena will affect safety and location based applications' reliability and preventing them from delivering their service. This type of DoS threat does not require a malicious node to flood the network with false messages but can be used by an adversary to serve his goals. For example, seeking high density areas and traffic jams to avoid being de-

tected by authorities.

In addition to applications' requirements for accurate and secure position information, critical applications and high classified users, such as emergency and authority vehicles, requires priority acquisition to network resources to guarantee message delivery with minimum delay. Although current studies [7, 84, 93, 124] proposed scheduling and controlling the flow of outgoing messages to reduce network congestion and avoid packet collisions. Such solution depend on nodes self assessments and radio channel monitoring, for example monitoring signal to noise ratio (SNR) and packet collision probability. It does not allow network managers to control the provided services which may prevent critical applications from exchanging the proper messages. For example, when a group of vehicles are traveling and exchanging entertainment contents such as a video stream. It might consume the full bandwidth of the network within their communication range. If at the same time an emergency vehicle passing by and attempting to send emergency and safety messages it will need to schedule its outgoing messages so that it does not collide with the other applications. With multiple applications and service, periodic and non-periodic messages, it will make sense to provide the network administrators the ability to control and adjust the amount of generated message to prevent overloading the network and allow critical applications to have access to adequate bandwidth resources. Such capabilities will secure network and applications' availability and guarantee the QoS for authorities and critical users.

4.1.2 Objective and Contribution

To reduce the number of generated packets and free resources for critical applications' messages, studies have proposed a medium access control (MAC) layer scheduling and adaptive beacon to enable vehicles to control the flow of beacon messages where each node adjusts its transmission rate according to channel sensing and collision probability [7, 84, 93, 124]. Such an approach will schedule and prioritize outgoing messages for a node but does not control the channel utilization of the network resources. In order to secure the applications' deliverables and secure their availability, it is important to control the access to the network resources and maintain QoS for critical applications and emergency vehicles. For example, authorities will need their vehicles and roadside units (RSUs) to collaborate and manage the road traffic flow by disseminating instructions and safety messages during rush hours, or when an emergency vehicle may want to send a message instructing vehicles to clear the way for its arrival. Such messages should not

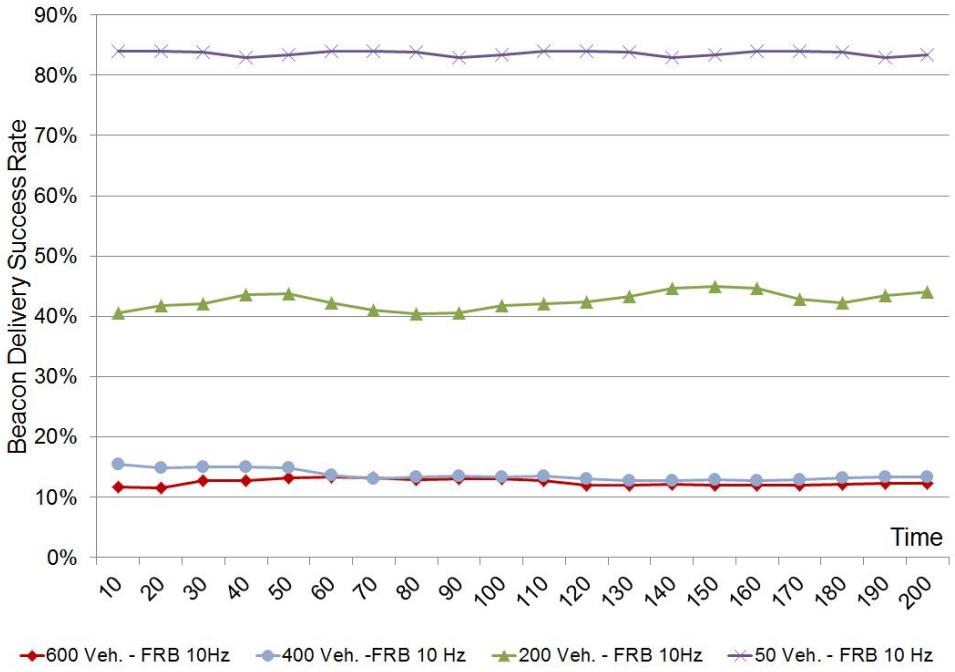


Figure 4.1: Beacon message delivery success rate decreases as number of vehicles increases.

be delayed and should be sent with high priority. However, in VANETs' wireless environment the probability of message collision and delay is high due to the large number of vehicles and huge number of periodic and multiple applications messages. Moreover, in highly dense areas, periodic application messages can create a denial-of-service attack to the network, preventing critical applications from exchanging messages.

In this chapter we discuss a DoS risk that is initiated by legitimate periodic messages and present a novel adaptive beaconing mechanism using neighborhood awareness information. The solution will reduce beacon message utilization of the channel capacity in dense areas and enable an authority to control overall beacon rates and provide bandwidth resources and quality-of-service (QoS) provisioning for critical applications, thus improving the availability of location services and network resources. The scheme also includes a trust evaluation model based on neighborhood awareness to maintain location data consistency during adaptive group beaconing (AGB) mode.

The remainder of this chapter is organized as follows: section 4.2 will present the adaptive group beacon scheme for VANET. The section will also discuss congestion de-

tection and trust evaluation model. In section 4.3, we will discuss the simulations and experiments that were conducted to evaluate the performance of the solution. Section 4.4 will discuss the solution's different aspects and related security measures. Finally we summarize this chapter with our conclusion and remarks.

4.2 Adaptive Group Beaconing (AGB)

The main objective for the proposed solution is to detect and control the beacon message dissemination among neighboring nodes. In this section, we will present the proposed scheme for adaptive group beacon (AGB). We will use the following terminologies to refer to different beaconing modes: In a *normal beacon*, which is the initial mode for a node, the vehicle sends its beacon messages at a fixed rate (e.g., 10 Hz) and the beacon message contains only the position and mobility information of the announcer. In a *group beacon*, which is the adaptive mode, the beacon message contains position information of other vehicles along with the sender's position information. A *cooperative beacon* involves proximate vehicles taking turns sending group beacons to reduce the number of sent messages.

4.2.1 Assumptions

The following assumptions are considered through out this chapter:

1. Each vehicle is capable of determining its own position and mobility information using a data fusion model of existing technologies such as GPS, map matching, a digital compass, and accelerator meters. By using improved GPS technologies such as differential GPS or augmented GPS, accurate position estimation can be achieved (error < 1 *meter*). Position errors tend to affect the position accuracy of all vehicles in the same area [9, 83]. Hence, relative position computations using GPS coordinates are acceptable. The scope of this thesis does not evaluate the correction and accuracy of the location estimation technologies.

2. Communication channels between vehicles are secure. Exchanged messages are digitally signed and vehicles are able to authenticate the message sender [64, 51]. We assume that an outsider will not be able to inject false information. All protocol messages are sent by legitimate nodes and carry their true position and mobility

information. With such an assumption, we focus our work on securing the integrity of the collected position information.

3. The proposed scheme allows the network operation managers and authorities to control the behavior of beacon message generation. The authorities can send their instructions through law enforcement vehicles, such as police cars, and roadside units. We assume that the authority's vehicles are identifiable and their communication are secure and trusted. Therefore, no adversary can imitate an authority vehicle. Authorities vehicles are identifiable, secure and trusted.

4. Energy consumption and computation resources are not a major concern in VANETs.

4.2.2 Vehicle Awareness Model

The initial state of a vehicle in the network is to broadcast its location information in as a normal beacon. Each vehicle sends its location and mobility information in a beacon message that is transmitted at a fixed rate, e.g. 10Hz. The receivers will evaluate the beacon message and store the data of the sender and its location information in a local database. The collective data will build the vehicle's awareness of neighboring location information. The vehicles data includes, current location, speed, acceleration, direction and the communication link state (LOS or NLOS). To maintain accurate information, each record is monitored to check for any inconsistency. For example, if the record was not updated by a beacon message for two consecutive beacon times the vehicle will attempt to verify the location and update the records. If the verification process fails (for LOS and NLOS), the record will be obsolete and the vehicle is considered to be not existing.

4.2.3 Congestion Detection

Road traffic congestion happens gradually as vehicles accumulate on a common path. Because vehicles have different travel paths and mobility behavior, several scenarios have to be considered when approaching a high-traffic area. The proposed AGB scheme will evaluate several attributes to detect the existence of high-density traffic and to determine the need to adjust beacon transmission rate and behavior based on the following:

1. *Number of vehicles:* The number of surrounding nodes within communication range of a vehicle (N_i)is the main factor that identifies congestion. If the number of

vehicles exceeds a maximum threshold ($N_i > N_{max}$) it will trigger a congestion state $C_{dens} = true$. The (N_{max}) value can be set by an authority based on traveling regions and time of day, and it can be redistributed based on special events and current conditions. Moreover, a vehicle would also determine the number of vehicles leading it (N_{front}) and the number of vehicles that are following it (N_{back}). A high density of leading vehicles indicates that there is traffic congestion coming ahead, while a high density following indicates that the vehicle is leaving traffic congestion. High traffic in both directions means that the vehicle is in the middle of the congestion.

2. *Mobility sudden change:* A sudden decrease of vehicle speed will influence surrounding vehicles to also reduce their speeds and continue with caution. Such behavior will accumulate traffic and increase the chances of traffic build-up. To identify a sudden break of a vehicle, we use $C_{mob} = true$, if the de-acceleration is larger than a defined threshold ($|\Delta a_t| > a_{th}$), where Δa_t is the change in the vehicle's acceleration.

3. *Receiving a group beacon message:* In a highly dense area, group beacons will be sent by vehicles instead of regular beacons. While approaching a congested area, a vehicle may receive a group beacon, or even a safety application message, from authorities or another leading vehicle. This attribute will be noted as $C_{gBcn} = true$, if a group beacon message were received.

4. *Channel congestion:* A vehicle may detect channel congestion due to high communication traffic or high signal interferences that limit the accessible channel resources. The media access control (MAC) services detects such conditions to help prevent packet collisions, which will help determine the need to adjust the beacon rate. This attribute will be noted as $C_{ch} = true$, if MAC services indicated high channel congestion probability.

5. *The presence of an authority nodes:* Authority nodes, such as police vehicles or RSUs, will be a source of safety and warning instructions to control traffic flow. QoS for authority nodes should be maintained to prioritize their messages. Once a vehicle detects the presence of an active authority node, it should reduce its utilization of network resources. The attribute will be noted as $C_{EV} = true$, if active emergency vehicle is present within range.

6. *Authority requests:* Authorities and network services managers can send instructions to vehicles to adjust their beacon rates and message transmissions to control overall bandwidth utilization. The request can be included within RSUs or an active emergency vehicle's beacon messages. Once a beacon is received, vehicles will adjust their network utilization to allow the exchange of critical application messages and reduce, or even stop, their beacon transmissions. This parameter will be indicated as $C_{Auth} = true$, if an instruction message were received.

Therefore, a congestion status will be determined by the logical expression:

$$CongDet() = C_{dens} + C_{mob} + C_{gBcn} + C_{ch} + C_{EV} + C_{Auth} \tag{4.1}$$

4.2.4 Trust Evaluation

The vehicles' movement are limited by paved roads and traffic regulations. In dense areas, vehicles share the path with others forming virtual groups that share the same interest such as destination and accessing the same road segments. Group communication between members is important to exchange updates for location and application data. However, the communication between members can be affected by different events and channel conditions. Therefore, evaluating the trustworthiness of neighboring nodes is important to secure the exchanged message delivery. The trust evaluation will allow the vehicle to determine which neighbor will be the best to perform an assigned task, such as message forwarding. In the AGB scheme, the trust values will help vehicles to determine which node will be included in its group beacon message and which node should be assigned to deliver the updates for it.

Each node maintains a record of every neighboring node. In addition to basic node information (mobility information, relative distance, group ID and a time stamp of the last update), nodes will evaluate and track the trustworthiness of neighboring vehicles based on neighborhood awareness. Individual trust evaluation is based on the following selected attributes:

1. *None-line-of-sight (NLOS) condition:* Nodes with direct communication are more reliable to deliver messages than are nodes that are behind obstacles. A vehicle can detect a NLOS condition with another vehicle by monitoring the beacon rate and data consistency of the subject node. Initiating a location verification process to evaluate the status of the node and determining if the communication link is affected by NLOS condition. If a NLOS condition is detected, the attribute for that

node can be noted as: $T_1 = \alpha_1(1 - NLOS)$, where (α_i) is a normalizing factor and NLOS = 1 or 0, indicating the link state for NLOS as true or false, respectively.

2. *Mobility similarity:* The relation among vehicles traveling in the same direction will last longer, which will allow more interaction and message exchange[2]. We are taking this into consideration as an attribute for the trust evaluation by evaluating the cosine similarity of the mobility vector of two nodes (M_i and M_j) will allow vehicles to determine direction similarity, such that:

$$cos(\theta) = \frac{M_i.M_j}{\parallel M_i \parallel \parallel M_j \parallel} \tag{4.2}$$

if $cos(\theta)$ is or is closer to (0), this means that the two vehicles are independent and traveling on the opposite direction. If the value is, or closer to (1), the two nodes are traveling in the same direction. This attribute will be noted as: $T_2 = \alpha_2(cos(\theta))$, where (α_2) is a normalizing factor.

3. *Distance and hop count:* Different applications may have different requirements with regard to node distance. A node that wants to send safety warning messages trusts further nodes to forward their messages in order to reach further distances, while other applications, such as lane merging, trust closer nodes. The distance to the node and the number of hops to reach it will help evaluate the state of the node's position. For example, To reach a node in a single hop is more reliable than a node with the same distance but requires more hops to reach. We take this into consideration and note the attribute as: $T_3 = \alpha_3(dist/hops)$, where (α_3) is a normalizing factor.

4. *Communication link stability:* With the dynamic nature of VANETs, the relative position among group of vehicles will change. Moving obstacles will also affect the communication link between two vehicles. Neighbors that maintained a stable link-state is more reliable than nodes that continuously switches from one state to another. To take that into consideration, we indicates the time the node remained in the same state (LOS or NLOS) as an attribute noted as: $T_4 = \alpha_4(t_s/t_{th})$, where (α_4) is a normalizing factor, t_s is the time since the last state change, and t_{th} is the minimum time threshold to consider the link as a stable link.

5. *Current trust score:* Tracking trust values for neighboring nodes will help detect sudden change in their behavior. We consider the last calculated trust value for a node and note it as: $T_5 = \alpha_5 Trust_0$, where (α_5) is a normalizing factor.

We will use a weighted average approach to compute the trust score for each node, where weights (w_i) are associated to the attribute values, such that:

$$Trust = \frac{w_1T_1 + w_2T_2 + w_3T_3 + w_4T_4 + w_5T_5}{w_1 + w_2 + w_3 + w_4 + w_5} \tag{4.3}$$

A vehicle will evaluate and maintain the trust values of neighboring nodes. In an adaptive group mode, a vehicle will request trusted nodes to forward, with along with their beacons, the location information of unreachable nodes that might be affected by NLOS conditions.

4.2.5 Adaptive Group Beaconing Process

After we have described the congestion detection methodology and the trust evaluation attributes, we will describe the steps for the proposed AGB process.

A vehicle will change its beaconing behavior from a normal mode to an adaptive mode once the congestion state is triggered—for example, by detecting a significant change in neighborhood density or other factors that were discussed in the previous section. When a vehicle detects that it is approaching congestion or near an emergency vehicle, it will adjust its beacon message content and rate to the adaptive mode. When it detects that it is leaving the congestion, it will set its beacon back to its normal mode. The following steps present the process of adaptive group beaconing:

1. Vehicles continuously receive beacon messages containing location information from their neighbors. Data are stored and monitored for inconsistency and congestion evaluation.

2. If a vehicle detects congestion (*CongStat()=true*)—for example, if it receives a group beacon message from one of its leading neighbors, or receives an instruction message from an active emergency node—it will understand that it is approaching congestion and it should change to adaptive mode by changing its beacon method and reducing its message rate. the Level 1 mode will allow the vehicle to determine the beacon rate based on the number of surrounding nodes, while the Level 2 mode will adjust the beacon rate and method based on authorities' instructions (Alg. 4.1).

3. The vehicle will send a request to trusted neighbors to forward the position information of less-trusted nodes. The request will guarantee that the update of

the vehicles that are under NLOS can receive one another's updates. If a vehicle receives an update forward request, it will mark its neighbor list according to the received list in the request message. When generating a group beacon, the node will check first for marked nodes to be attached to the group beacons (Alg. 4.2).

4. If the the beacon message is a group beacon, the data from the received group beacon will be extracted and recorded in the neighborhood awareness database. Once the group beacon is processed, the vehicle will check whether its data were included in the received beacon or not. If they were included, it will reset its beacon time based on the neighborhood list size and the type of authority request. If the node's information is not in the received group beacon, it will construct a group beacon message and send it to its neighbors (Alg. 4.3).

5. Neighboring vehicles cooperate and take turns in generating a group beacon message (Alg. 4.4). In a congested area, vehicles tend to have slower mobility and fewer changes. A group beacon message should satisfy the update requirements and prioritize forwarding the position information of nodes (with NLOS conditions) that were requested by neighbors, such that: groupSet=$\{Loc_i, M_i, List_{fwd}\}$. If a vehicle detects that its own updates were not included, it will interrupt and send a group beacon with its updates.

6. The vehicle will keep monitoring its status and surrounding conditions for any changes. For example, if a vehicle accelerates and its speed exceeds the average traffic flow speed, it will understand that it is moving out of the congestion area. Moreover, if there are no active authority instructions to maintain the adaptive mode, the vehicle will change back to its normal beacon mode (Alg. 4.5).

4.3 Simulations

Simulation experiments were conducted using the network simulator (NS-2), ver. 2.34, to evaluate the performance of our proposed solution. We simulated the city environment of downtown Ottawa, ON, Canada, using the parameters in Table 5.1. Vehicle mobility traces were generated by simulation of urban mobility (SUMO)[38]. We set the simulation experiment to initiate an adaptive group beacon when a vehicle detects ($N_{max} = 10$ vehicles) within its communication range. The beacon message will include

Table 4.1: AGB Algorithm Notations

Variable	**Description**
N_i	*Number of surrounding vehicle i*
N_{max}	*Threshold for Max. number of surrounding vehicles*
N_{front}	*Number of vehicles in front*
N_{back}	*Number of vehicles in back*
ΔV_t	*Change in speed*
V_{t-1}	*Last known speed*
V_{th}	*Change of speed threshold*
C_{dens}	*Density congestion attribute*
C_{mob}	*Mobility congestion attribute*
C_{gBcn}	*Group Beacon congestion attribute*
C_{ch}	*Channel congestion attribute*
C_{EV}	*Emergency vehicle congestion attribute*
C_{Auth}	*Authority message congestion attribute*
$ConDet()$	*Congestion detection trigger*
$NLOS$	*NLOS state with subject node*
C_{dens}	*Density base congestion attribute*
α_i	*notmalizing factor for attribute i*
T_i	*Trust attribute i*
w_i	*Associated weight for attribute i*
$dist$	*Distance to subject node*
$hops$	*Number of hops to reache a subject node*
$stab$	*Time of last changein link stability*
Loc_i	*Location information for node i*
M_i	*Mobility vector for node i*
$List_{fwd}$	*List of nodes to be forwarded*

a maximum of 10 nodes' information (512 byte). Vehicles also change to adaptive mode whenever an emergency vehicle request is detected.

4.3.1 Performance Evaluation Aspects

In order to evaluate the proposed solution, we focus our attention on the aspects that will evaluate the number of beacons and maintain the accuracy of neighborhood awareness. The following aspects were considered to evaluate the performance of the proposed scheme:

Algorithm 4.1 Monitoring Process in Normal Mode

```
1: while (adaptMode() = false) do
2:     if (C_EMS() = true) then
3:         ▷ received an authority's instruction
4:         Change to adaptiveMode(Level 2)
5:         ▷ level 2: follow authority instruction
6:     else congDetect() = true
7:         ▷ congestion is detected
8:         Change to adaptiveMode(Level 1)
9:         ▷ level 1: group beacon based on neighborhood
10:    end if
11: end while
12: construct List_fwd
13: ▷ get the list of nodes with NLOS condition
14: send forwardReq(List_fwd)
15: ▷ send list to trusted nodes
```

Table 4.2: AGB Simulation Environment Parameters

Parameter	**Value Setting(s)**
Radio Propagation	*Two Ray Ground, Nakagami*
Antenna Type	*OmniAntenna*
MAC Layer	802.11*p*
Radio Range	300*m*
Data Rate	6 *Mbps*
Packet Payload	$152 - 512$ *byte*
Number of Vehicles	$50 - 600$
Speed Limits	$0 - 50km/h$
City Area	$4km$ x $3km$
Simulation Time	$15 - 30Min$

1. *Channel capacity utilization:* The objective of AGB is to reduce the number of periodic messages to allow critical applications to use network resources. Therefore, it is important to examine the impact of periodic beacon messages on the network and the capacity offered by using the proposed AGB scheme. Through this aspect we will also evaluate the solution's scalability, and discuss the factors that support or limit scalability.

Algorithm 4.2 Update Forwarding Request

```
1: Process : Sending request
2: NLOSList() = getNLOSList()
3: ▷ get the list of nodes under NLOS
4: if (NLOSList() is not empty) then
5:     sendFwdReq(NLOSList(), trustNodes())
6:     ▷ broadcast list to trusted node
7: end if
8: while (adaptMode() = true) do
9:     if getNLOSList() != NLOSList() then
10:        ▷ NLOS list have been changed
11:        NLOSList() = getNLOSList()
12:        sendFwdReq(NLOSList(), trustNodes())
13:        ▷ broadcast list to trusted node
14:    end if
15: end while
16:
17: Process : Receiving request
18: input : Forward Request
19: if MsgType() = FwdRequest() then
20:    if (msgDist = me) then
21:        ▷ I am a distention node
22:        markBcnFwd(NLOSList())
23:        ▷ mark my neighbor list according to the received list
24:    end if
25: end if
```

Algorithm 4.3 Receiving a Beacon Message

```
1: input : beacon message
2: if (MsgType = groupBcn) then
3:     ▷ congestion is nearby
4:     Change to adaptiveMode(Level 1)
5:     ▷ level 1: group beacon based on neighborhood
6:     if (my info is included) then
7:         if (my info is correct) then
8:             ResetBcnTimer(list size,EV)
9:             ▷ reset beacon timer based on neighbor density and instructions
10:        else
11:            ▷ my location information is not correct
12:            SendBcnMessage()
13:            ▷ construct and send a group beacon message
14:        end if
15:    end if
16: end if
17: UpdateNeighborList()
18: ▷ update neighbor list with received beacon data
19: if (N_i > N_max) then
20:    ▷ congestion is being formed
21:    Change to adaptiveMode(Level 1)
22: end if
```

Algorithm 4.4 Sending Beacon Messages

```
1: input : Beacon Timer Expired
2: if (AdaptiveMode = true) then
3:     if (my info was not in last group beacon) then
4:         groupSet={Loc_i, M_i, List_fwd}
5:         sendGroupBcn(groupSet)
6:     end if
7:     ResetBeaconTimer()
8: else(Adaptive mode = false)
9:     sendBcn(Loc_i, Mob_i)
10:    ResetBeaconTimer()
11: end if
```

Algorithm 4.5 Monitoring Process in Adaptive Mode

```
1: while adaptiveMode = true do
2:     ▷ vehicle in adaptive mode
3:     if (C_EMS() = false) and (congDetect = false) then
4:         ▷ congestion trigger is off
5:         Change to normal mode
6:     end if
7: end while
```

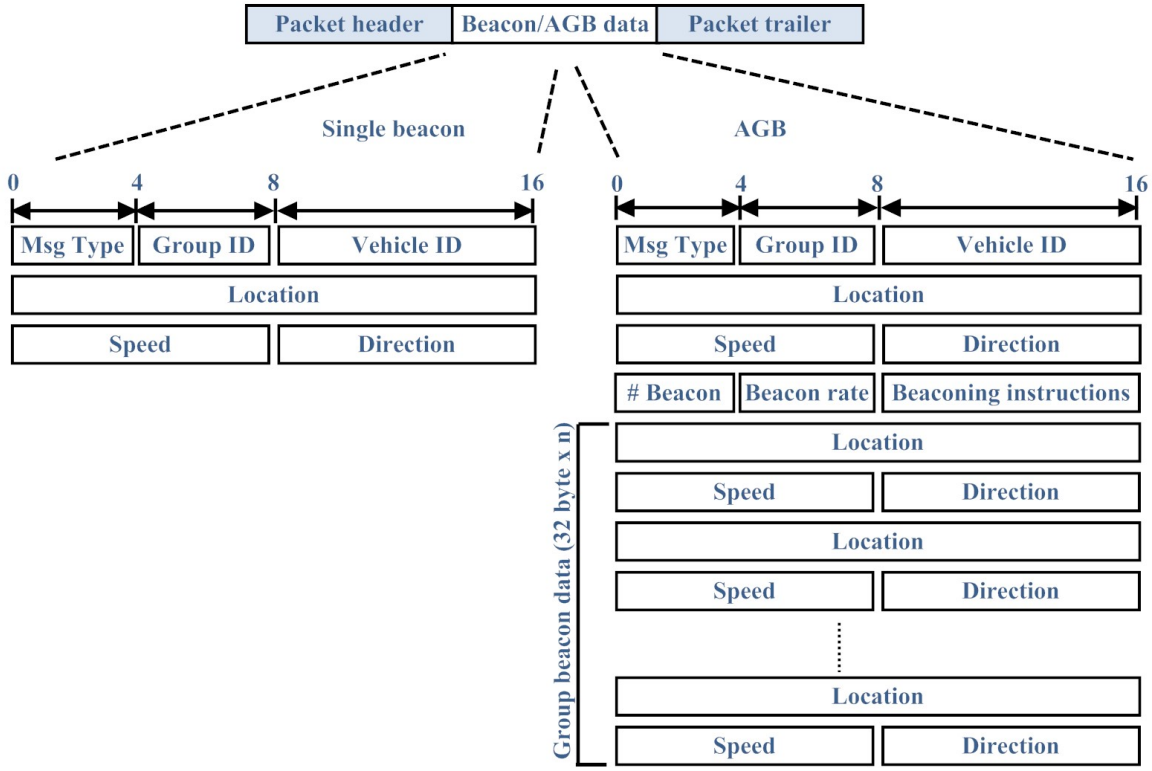


Figure 4.2: Beacon packet format.

2. *Neighborhood awareness accuracy:* Reducing the number of beacon messages using AGB will help reduce the utilization of the channel capacity. we want to examine the awareness rate achieved with the adaptive group beacon compared to the actual number of vehicles within a vehicle's communication range. The goal is to maintain a high awareness rate of the current number of surrounding vehicles and their positions in an instant.

3. *Message delivery success rate:* Critical application messages has a priority in VANETs. Using AGB, we want to evaluate the success rate of message delivery generated from emergency vehicles and evaluate the impact of periodic beacons and AGB on such messages.

4.3.2 Results and Finding

In this section, we discuss the results on using an extensive set of simulation experiments we carried out to evaluate the performance of the proposed scheme.

Channel capacity utilization: Theoretically, an increase in the number of vehicles within the same range of communication will increase the bandwidth utilization required to allow all members to send their beacons and will be limited by the available bandwidth. In Figure 4.3, fixed rate beacon (FRB) at 10 Hz requires more channel resources as the number of vehicles increases (within the communication range) and vehicles continue to transmit their information. However, packet collisions and signal interference will reduce the accessible channel resources for vehicles and limit the utilization to 50% of bandwidth as the density increases. AGB allows vehicles to use less channel resources (less than 30%) by combining multiple vehicle information in a single message. The cooperative approach reduced the amount of generated beacons and allowed other applications to utilize available resources. Table 4.3 shows the average consumption of beacon messages with 95% confidence interval.

To have a closer look at the number of generated beacon messages, we study the *communication complexity* of the system. The total number of beacon messages (Bcn_{total}) generated in the FRB mode is calculated as:

$$Bcn_{total} = \sum_{i=1}^{n} (R_i \times t) \tag{4.4}$$

Where, n is the total number of vehicles, R_i is the beacon rate for vehicle i and t is the calculated time interval. There for the communication complexity is of order $O(N)$.

Using the AGB mode the number of messages is calculated as:

$$Bcn_{total} = \sum_{i=1}^{n} (\frac{R_i}{G_i} \times t) \tag{4.5}$$

Where, n is the total number of vehicles, R_i is the beacon rate for vehicle i, G_i is the maximum attached beacon in a group beacon message, and t is the calculated time interval. There for the communication complexity is of order $O(N)$. The value of Bcn_{total}

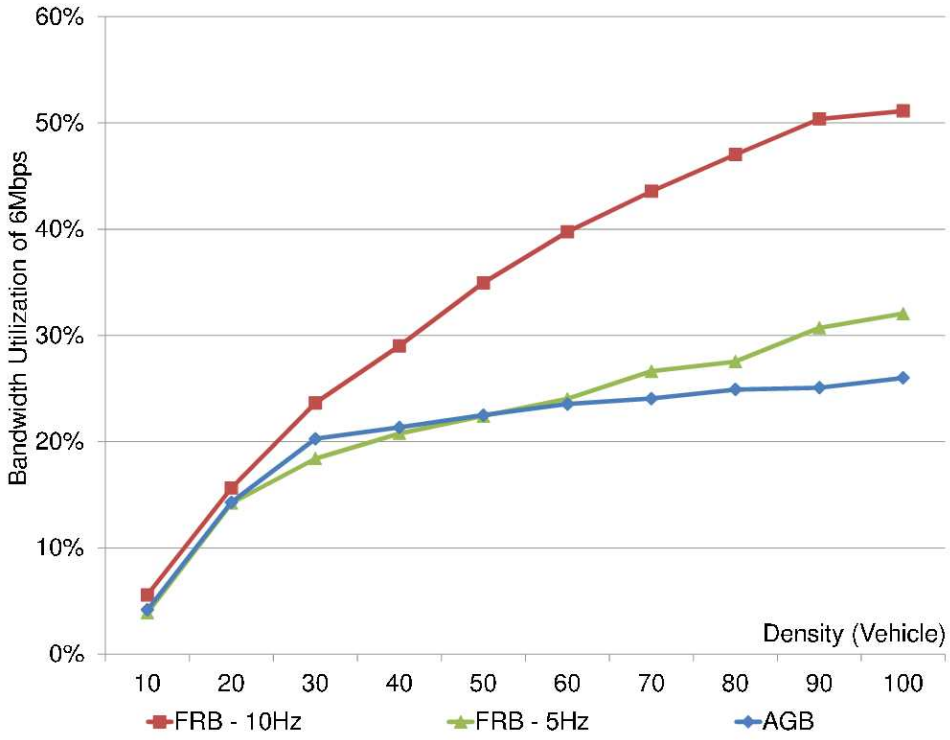


Figure 4.3: Channel bandwidth consumption by periodic beacon messages using fixed rate beacon (FRB) and adaptive group beacon (AGB).

Table 4.3: Beacon-message average utilization under different densities, with a 95% confidence interval.

Vehicle	FRB-10Hz		AGB-no trust		AGB	
Density	Low	High	Low	High	Low	High
10	0.0448	0.0666	0.0296	0.0540	0.0296	0.0540
20	0.1092	0.2037	0.3601	0.5660	0.0001	0.2060
30	0.1904	0.2828	0.1542	0.2513	0.1042	0.2013
40	0.2430	0.3375	0.1649	0.2619	0.1249	0.2219
50	0.3032	0.3956	0.1764	0.2735	0.1464	0.2435
60	0.3559	0.4391	0.1972	0.2735	0.1672	0.2435
70	0.3619	0.5094	0.1519	0.3292	0.1219	0.2992
80	0.4178	0.4828	0.2241	0.2741	0.1941	0.2441
90	0.3998	0.6078	0.2420	0.2598	0.2220	0.2398
100	0.4903	0.5324	0.2526	0.2675	0.2227	0.2376

in AGB is less because G_i is larger and R_i for a node in AGB is less than R_i in FRB.

Neighborhood awareness accuracy: Reducing the number of beacon messages using AGB will help reduce the utilization of the channel capacity. we want to examine the awareness rate achieved with the adaptive group beacon compared to the actual number of vehicles within a vehicle's communication range. Simulations of different vehicle densities were conducted over the same road segments and monitored over a period of time. As shown in Figure 4.4, the increasing number of vehicles within a communication range affected the awareness rate of vehicles' positions. Table 4.4 lists the average awareness rate with different densities in a city environment. In a scenario with 600 vehicles, the knowledge obtained from beacon messages and the awareness level of a vehicle was reduced to as low as 30% of the actual state. This is because of the impact of the high probability of packet collisions. Although the AGB provided more accurate information than did the FRB under different scenarios, it was still affected by high vehicle density. In Figure 4.6, we can observe that as the number of vehicles increased, the overall neighborhood awareness rate was reduced, which was caused by a high number of dropped packets. However, AGB provided higher awareness, as a single group beacon contained the information of more than one node. Although the AGB provided more information than did the FRB in highly dense areas, the high packet collision rate and hidden terminal problem affected the message delivery success rate.
In Figure 4.7, a comparison with other adaptive beaconing approaches, such as changing the beacon rate or transmission power. The AGB protocol provided a better awareness rate for its nodes. For example, for neighboring nodes that are at a distance of 100m, AGB provided an awareness rate of 80% while with an adaptive approach that adjust the transmission range to 100m and 10Hz beacon rate, the awareness rate was about 60%. We can also observe that the awareness rate for a node was reduced as relative distance increased. Table 4.5 lists the average awareness rate for a 400-vehicle scenario with different beaconing methods. The awareness rate is highly affected and reduced by only adjusting the power or transmission rate. The proposed AGB protocol delivers better awareness of surroundings. However, the awareness rates of far nodes are still affected by interference and the hidden terminal problem that appears at far nodes. The performance of AGB for the same road network under different scenarios is shown in Figure 4.8. The awareness rates of nodes are reduced due to channel congestion and packet collision. However, the awareness rates delivered are higher than those for the adaptive beacon using power and rate adjustments.

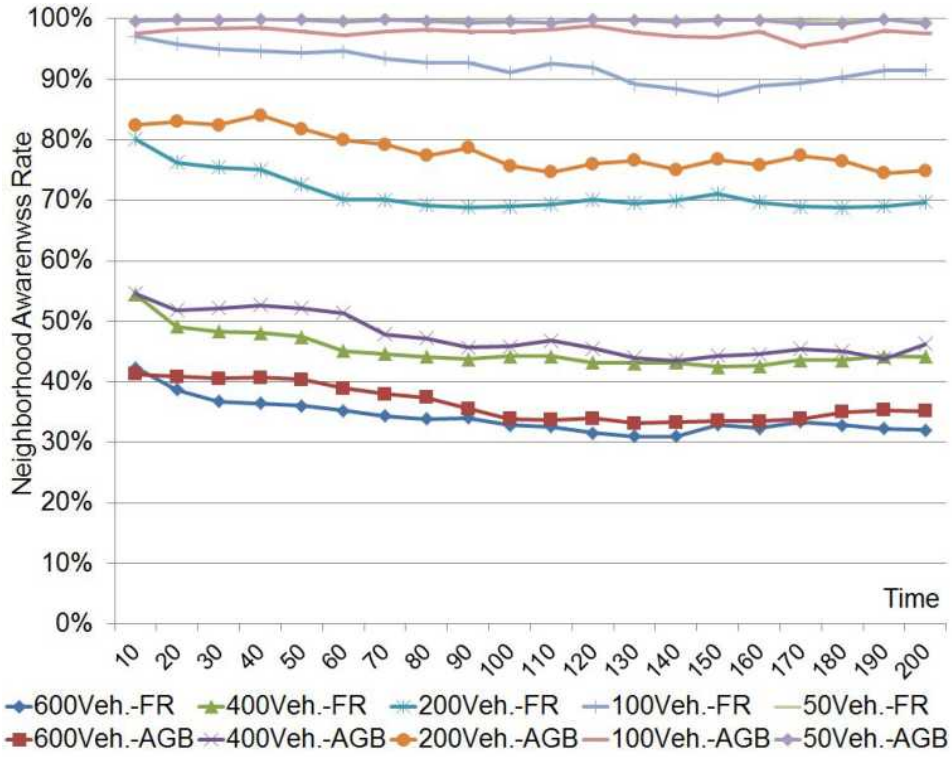


Figure 4.4: Neighborhood awareness accuracy obtained from beacon messages under different density scenarios.

Message delivery success rate: Critical application messages has a priority in VANETs. Using AGB, we aim to release network resources to allow high priority application and authority instructions to be delivered in order to secure VANETs services' availability. We examined the message delivery success rate generated from emergency vehicles and evaluate the impact of periodic beacons and AGB on such messages.

In Figure 4.9, we can observe the success rate for delivering beacon messages, which improved by using AGB under different densities. Once the number of surrounding vehicles increased, the success rate dropped to an average of 15% in a highly dense setting due to channel congestion and high probability of packet drop. By applying AGB, the network delivered a higher success rate than with FRB. This was achieved because vehicles were cooperating to generate beacon messages that not only contained their information but also the positions of other vehicles. Each vehicle scheduled its beacon based on its turn and its current state. Table 4.6 list the average delivery success rate for a single

Table 4.4: Neighborhood location awareness average rate in different density scenarios with 95% confidence intervals.

Vehicles	Beacon type	Range (0-50)		Range (50-100)		Range (100-150)		Range (150-200)		Range (200-250)		Range (250-300)	
		Low	High	Low	High	Low	High	Low	High	Low	High	Low	High
200	FRB-10Hz	0.9664	1.0000	0.9093	0.9991	0.8438	0.9715	0.7076	0.8929	0.5489	0.7483	0.4441	0.6450
200	AGB	0.9618	1.0000	0.9065	1.0000	0.8575	0.9849	0.7425	0.9334	0.6203	0.8538	0.5551	0.7903
400	FRB-10Hz	0.7356	0.8936	0.5740	0.7666	0.4525	0.6473	0.2664	0.4974	0.0946	0.3010	0.0466	0.2374
400	AGB	0.8859	0.9555	0.7543	0.8522	0.6576	0.7774	0.4961	0.6370	0.3004	0.4839	0.2262	0.4126
600	FRB-10Hz	0.6172	0.8194	0.4524	0.6638	0.3561	0.5430	0.1975	0.3758	0.0706	0.2122	0.0432	0.1614
600	AGB	0.7933	0.9302	0.6300	0.7697	0.5295	0.6690	0.3664	0.4965	0.1790	0.3297	0.1207	0.2544

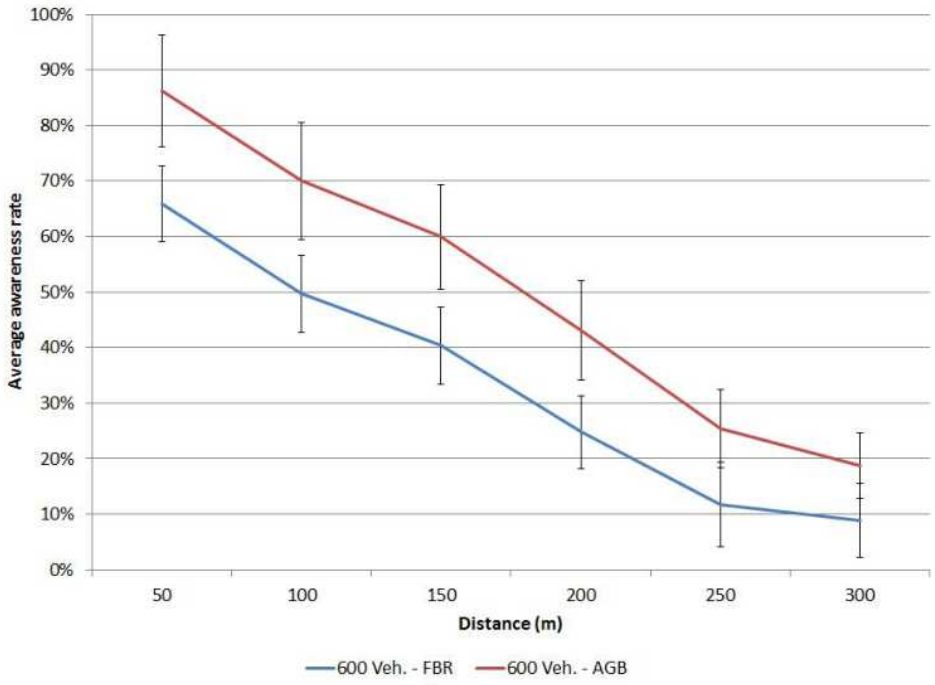


Figure 4.5: Neighborhood location awareness average rate for 600-vehicles scenarios with 95% confidence intervals.

hop beacon message with 95% confidence interval.

However, in a highly dense area, the probability for successfully delivering a message becomes low, which applies to emergency and safety messages. Figure 4.10 shows the delivery rate for a single hop message within a node's communication range. The delivery decreases as the distance between the sender and receiver increases. With the AGB, the delivery rate is higher than the rate in an FRB scenario because AGB utilizes fewer network resources, thus allowing other messages to utilize them. However, as density increases, the available network resources decrease for both beacon and application mes-

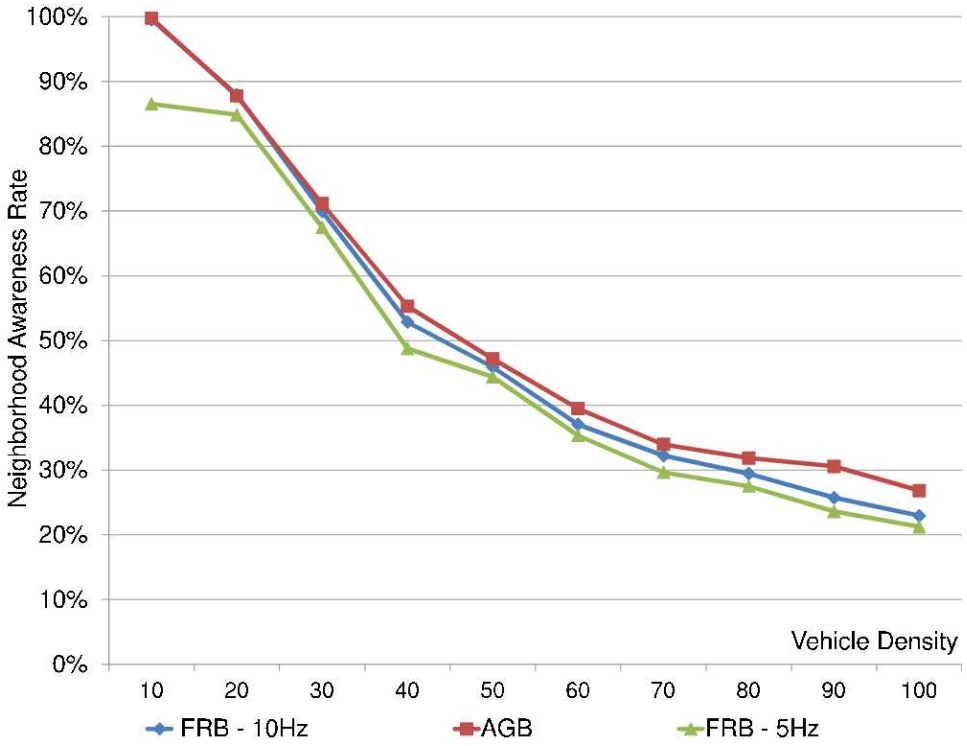


Figure 4.6: Neighborhood awareness accuracy obtained from AGB compared to actual state with FRB.

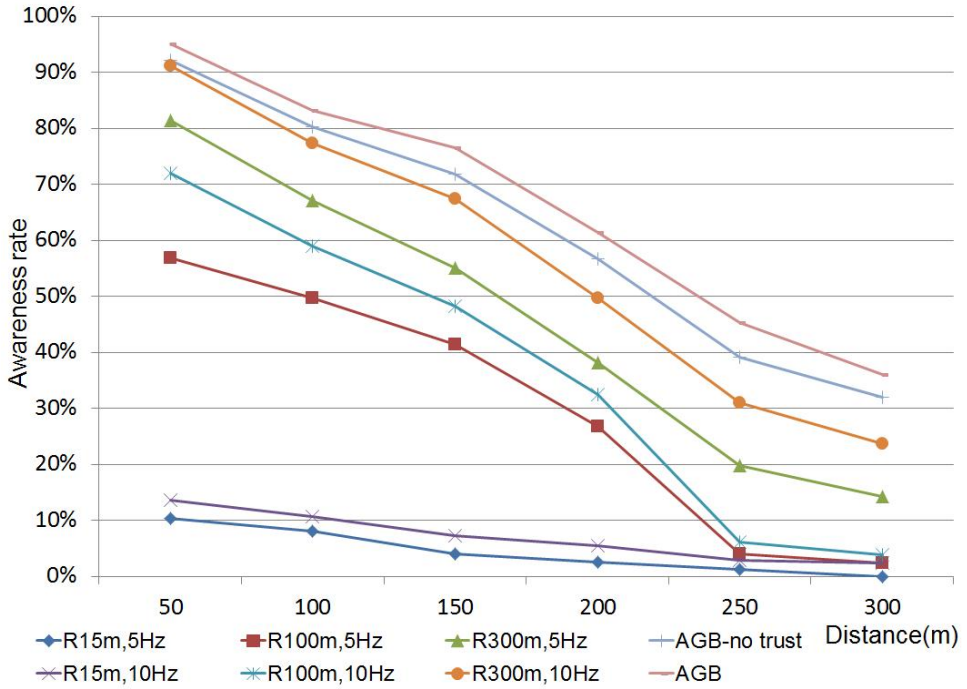


Figure 4.7: Awareness rate of AGB with comparison to other adaptive beaconing approaches in a 400-vehicle scenario.

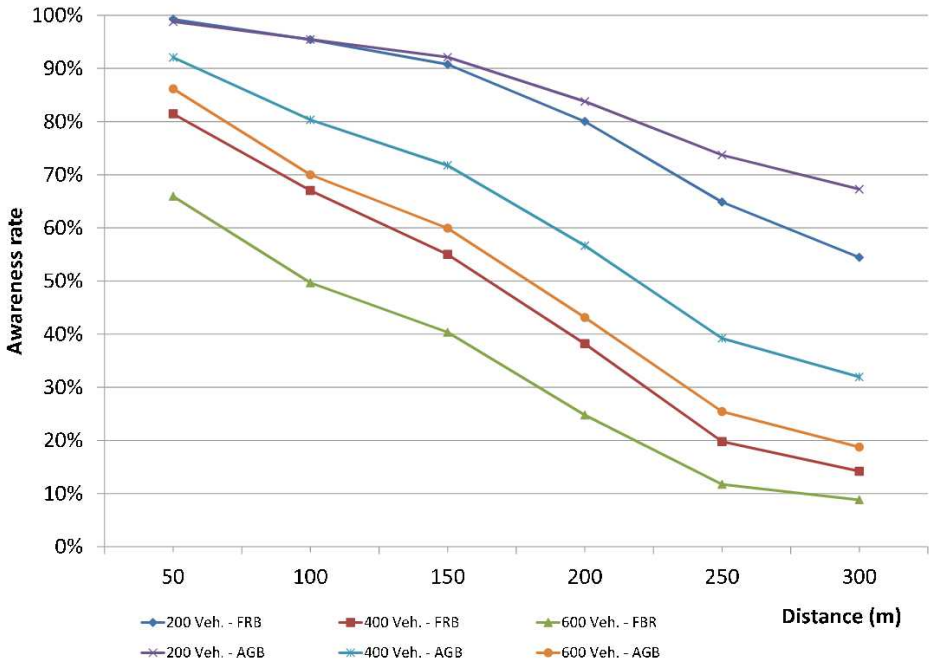


Figure 4.8: Average awareness rate based on distance to vehicle.

Table 4.5: The neighborhood location awareness average rate for a 400-vehicles scenario with 95% confidence intervals.

Trans. range (m)	Beacon Type	Range 0-50		Range 50-100		Range 100-150		Range 150-200		Range 200-250		Range 250-300	
		Low	High	Low	High	Low	High	Low	High	Low	High	Low	High
15	FRB-10Hz	0.0000	0.0023	0.0825	0.1757	0.0827	0.2334	0.0360	0.0952	0.0000	0.1074	0.0065	0.0346
100	FRB-10Hz	0.0380	0.3217	0.2097	0.9204	0.2100	0.7791	0.1350	0.6852	0.1190	0.4085	0.0071	0.0595
300	FRB-10Hz	0.2550	0.4415	0.7356	0.8936	0.5740	0.7666	0.4525	0.6473	0.2664	0.4974	0.0946	0.3010
15	FRB-5Hz	0.0000	0.0024	0.0825	0.1764	0.0827	0.2334	0.0360	0.0952	0.0000	0.1074	0.0065	0.0346
100	FRB-5Hz	0.2977	0.3505	0.8761	0.9616	0.7310	0.8491	0.6510	0.7697	0.3791	0.5006	0.0355	0.0729
300	FRB-5Hz	0.3898	0.5097	0.8705	0.9528	0.7147	0.8294	0.6144	0.7295	0.4221	0.5648	0.2328	0.3762
300	AGB	0.4461	0.5934	0.8859	0.9555	0.7543	0.8522	0.6576	0.7774	0.4961	0.6370	0.3004	0.4839

sages.

In Figure 4.11, the graph shows the result for the simulation of a scenario in which authority vehicles can force vehicles in a high-density area to reduce their beacon rates or even stop their beacon messages. At (t=100s), the vehicles started to receive an authority's instruction messages to adjust their beacon behavior, which resulted in improved message delivery. Enabling authorities to control the message rate of vehicles will help improve network performance and complying with QoS requirements of applications in highly dense areas.

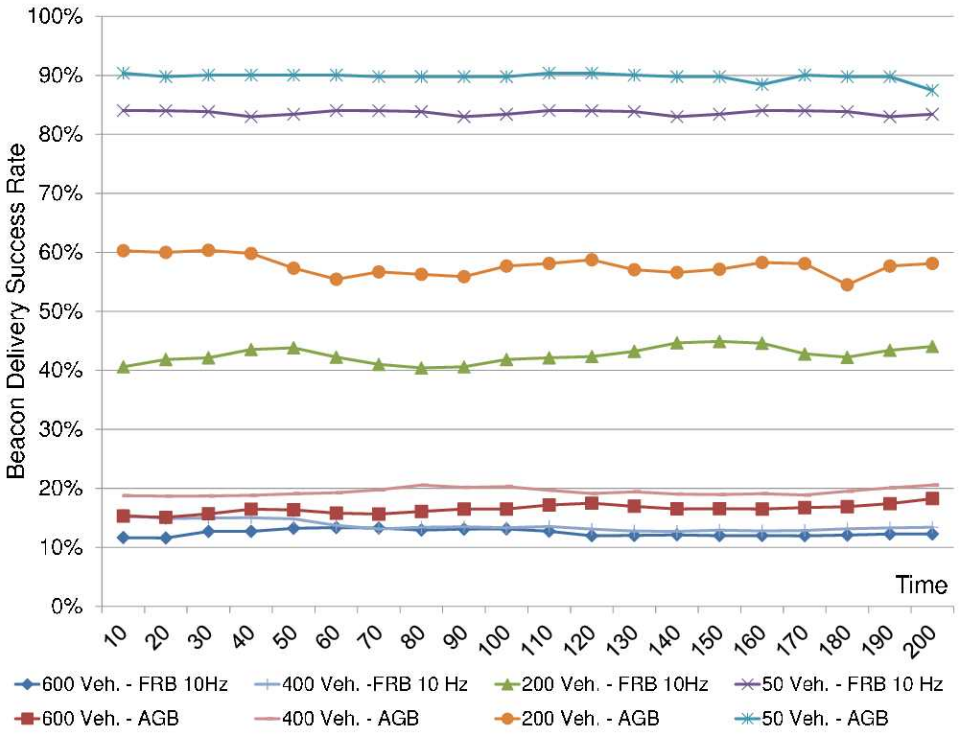


Figure 4.9: Message delivery success rates under different density scenarios.

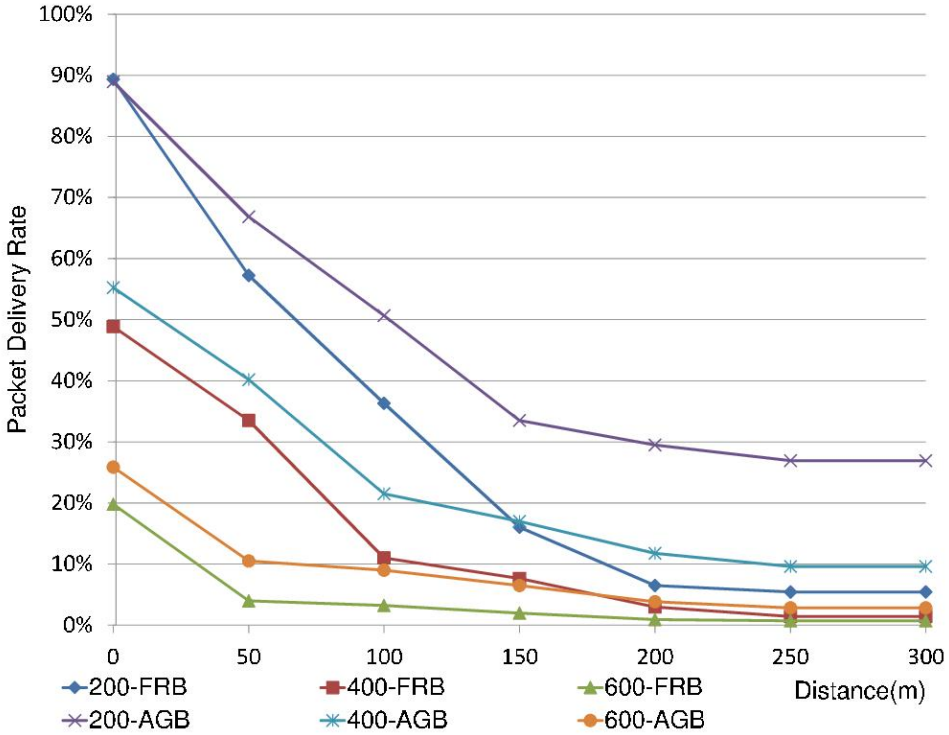


Figure 4.10: Message delivery success rates for a single hop message with respect to distance to node.

Table 4.6: The data packet delivery average rate with 95% confidence interval.

	Range (0-50)		Range (50-100)		Range (100-150)		Range (150-200)		Range (200-250)		Range (250-300)	
Scenario	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High
200-FRB	0.8737	0.9129	0.5529	0.5921	0.3395	0.3866	0.1405	0.1797	0.0453	0.0864	0.0309	0.0741
400-FRB	0.4691	0.5083	0.3155	0.3547	0.0865	0.1335	0.0568	0.0960	0.0101	0.0512	0.0000	0.0338
600-FRB	0.1782	0.2174	0.0201	0.0593	0.0088	0.0558	0.0002	0.0394	0.0000	0.0309	0.0000	0.0267
200-AGB	0.8696	0.9088	0.6486	0.6878	0.4831	0.5302	0.3156	0.3548	0.2752	0.3164	0.2456	0.2887
400-AGB	0.5328	0.5720	0.3820	0.4212	0.1917	0.2388	0.1504	0.1896	0.0980	0.1392	0.0723	0.1154
600-AGB	0.2389	0.2781	0.0854	0.1246	0.0664	0.1134	0.0451	0.0843	0.0186	0.0597	0.0046	0.0477

4.4 Solution Aspects and Security Measures

After we discussed the proposed adaptive group beaconing (AGB), we will discuss how can AGB support securing the availability and integrity of VANETs services. In this section, we will discuss several aspects related to the proposed AGB scheme.

1. *Neighborhood awareness:* VANETs will provide vehicles with information about their surroundings. The neighborhood awareness service is essential for providing accurate and reliable information. The proposed AGB is based on the knowledge of the neighboring vehicles' locations and movements. The adaptive mode will be triggered if a congestion is detected. One of the attributes that will trigger a congestion is the number of surrounding vehicles. Based on geographic location and time of the day, a threshold can be set for the number of vehicles (N_{max}) that are within the same communication range to trigger the adaptive beaconing mode. The threshold can be adjusted and redistributed by authorities' vehicles and RSUs to better manage the network resources.

2. *Safety applications:* With AGB, a vehicle can detect the existence of traffic congestion using neighborhood awareness and reception of a group beacon. For example, if a traffic accident occurred and traffic congestion were built up by a group of cars, an inbound vehicle may approach at a later time. If safety messages were disseminated before its arrival, it will have no knowledge about any previous instruction unless the messages are continuously generated in a beacon-message style. However, with the proposed solution, a vehicle detects the current state of leading vehicles and may send a request to them for the latest safety instructions. Such a feature will help reduce repeated safety messages and allow approaching vehicles to fetch the information in case they missed it.

3. *Scalability:* AGB supports scalability because it reduces the number of periodic beacon messages, as shown in the simulation results. Moreover, each beacon con-

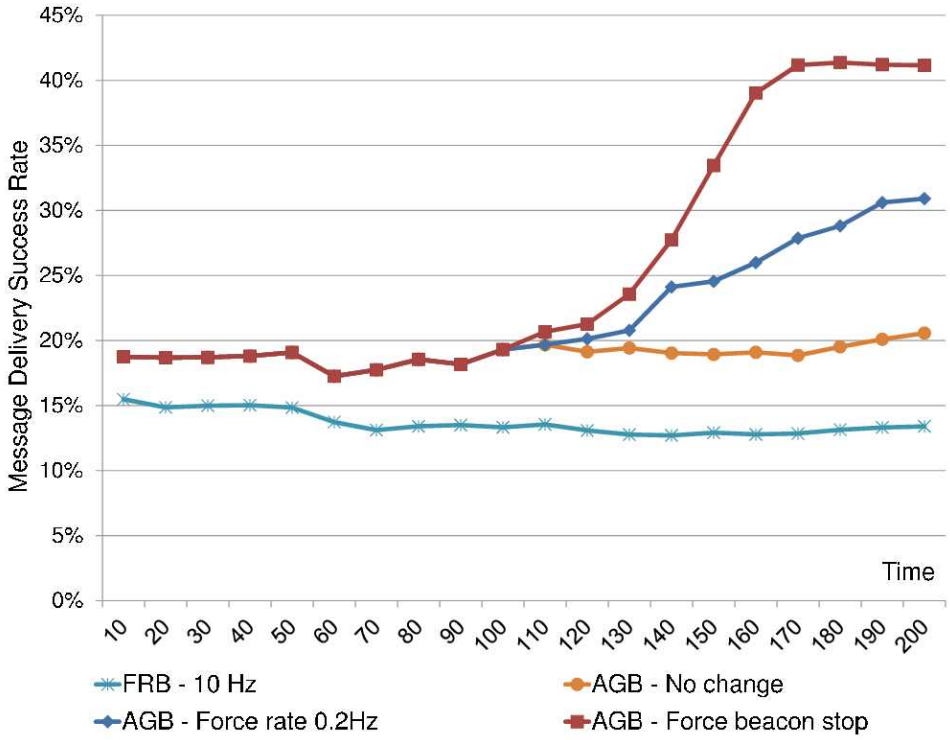


Figure 4.11: Message delivery success rates with different authorities' instructions to change beaconing behavior.

tains the information of a group of neighboring vehicles, and they take turns in generating the message to insure current status updates; the cooperative approach helps reduce the number of messages generated. However, in highly dense areas, the high probability of packet drops caused by collisions and signal interference can affect network scalability by preventing vehicles from sending beacon messages to their neighbors. In a highly dense area, an authority may prevent a potential DoS by instructing vehicles to reduce or stop beacon messages to support critical applications. However, scalability remains a challenge in VANETs because of the nature of wireless communication and mobility, signal interference, packet collision, and the hidden terminal problem.

4. *QoS provisioning:* In order to provide network QoS, the service provider should have control of network resources. The distributed wireless environment makes this a challenge. The periodic beacon messages that are needed to provide vehicles with updates on location and mobility information of their neighbors consume a lot of

channel resources and increase the probability of packet drops. In this chapter, we proposed an adaptive beacon methodology at the network service layer that will allow authorities' vehicles to control the beacon messages generated by vehicles to allow critical applications and messages to gain access to network resources during traffic congestion. Authorities' vehicles, such as police cars, can include in their beacons adaptation instructions for vehicles, such as normal and adaptive beacon rates and maximum vehicle density for congestion detection. Authorities can set QoS requirements and adaptation settings and provide this information to vehicles based on regional configuration through the vehicle registration process with the network.

5. *Trust evaluation:* Vehicles evaluate the trustworthiness of neighboring nodes based on neighborhood awareness. They evaluate whether direct communication with other nodes is stable and direct or if the communication is interrupted by obstacles which prevent direct communication. The purpose of the trust model for the solution is to allow vehicles to request trusted nodes to forward the location information of nodes that are under NLOS conditions to maintain vehicle awareness under the AGB mode.

6. *Securing location information:* Position information exchanged among vehicles will be authenticated and verified by digital signature frameworks. To avoid unauthorized utilization of adaptation requests, the receivers can verify the signatures associated with the message and authenticate its eligibility to make the request. Only authorities' nodes are eligible to send adaptation instructions to prevent malicious nodes from manipulating vehicles' beacon rates. Securing the availability of location information was improved by the proposed AGB solution with the location update forwarding requests to trusted neighbors, which maintained location information updates and reduced the effect of NLOS conditions.

4.5 Summary

In the VANET wireless environment, periodic beacon messages can consume a large amount of bandwidth resources and increase the chance of packet collisions, especially in dense areas. These legitimate messages may create a DoS risk by consuming the available network resources, which will affect the availability of exchanged location information, prevent acquiring the intended benefit of the periodic messages, and affect the

functionality of other critical applications. Adaptive beaconing can help reduce the load by adjusting the behavior and frequency of generated messages. Current studies have proposed adjusting transmission power and rate as well as scheduling message rate at the MAC layer to avoid packet collision. In this chapter, we discussed a potential DoS threat caused by traffic congestion that will affect the availability of location information used to build vehicles' awareness of their surrounding neighbors. We developed a novel approach for AGB in VANETs that involves authorities' vehicles and their QoS requirements. A vehicle adjusts its beacon rate and content based on the detection of congested areas and the requests from authorities' nodes. The adaptive mode generates group beacon messages, which not only provide the position and mobility information of an individual node but also contain information regarding other neighboring vehicles. Nodes can request trusted nodes to forward the location information of vehicles that are under NLOS conditions to maintain data consistency and guarantee the reachability of subject nodes. The group beacon will also help vehicles detect road traffic congestion and allow them to adjust their beaconing mechanism prior to entering the dense area. The cooperative approach for sending beacon messages reduces the number of generated messages and allows the authorities to control the rate or stop the transmission of beacon nodes. With such adaptation, network service providers and authorities will have control of the amount of resource utilization for beacon messages in dense areas. This will prevent the possible DoS threat that is caused by the network applications and services and will allow critical applications and messages to have higher priorities and network resource availability. The contribution of this work also includes a neighborhood awareness context-based trust model allowing vehicles to identify vehicles that might be under NLOS conditions due to obstacles. Simulation results showed that AGB had less impact on the network channel and improved message delivery success rates due to the smaller number of messages.

Chapter 5

A Secure Neighborhood Awareness Service

5.1 Introduction

Vehicular ad-hoc networks (VANETs) are envisioned to provide many road and safety applications. Vehicles will be able to communicate and exchange messages among themselves to provide awareness of neighboring nodes and events. One important type of vehicle information that will be shared is position and mobility data. Such information can be disseminated using periodic messages (beacons), group updates, or it can be attached (piggybacked) to applications' messages. The location information are used by many applications and network services. With location information of an event, such as a road accident, a driver can determine if he/she can take an alternate route. In addition, because it is aware of the location of other neighboring vehicles, a node can determine which neighbor will be the best next hop node to forward a message to its desired destination. Such dependency on position information will invite attackers to compromise the network by injecting false node and event positions or modifying exchanged data. Moreover, an attacker can track a vehicle by collecting its announced locations and can build a travel profile over time, which is a clear violation of privacy.

Securing the services and applications of VANETs against possible threats is a challenge. Network characteristics, such as vehicle mobility, driving behavior, and obstacles can affect the delivery of application messages reducing its reliability and credibility. Security frameworks and trust models were proposed to secure the network from identified security attacks[15, 16, 64, 76, 77]. However, application developers are left to

assess their security concerns with respect to location information. Without a centralized service, redundant work are produced to provide similar information for multiple applications. In this chapter, we present a secure neighborhood awareness service framework for VANET which will preserve vehicles' privacy and provide a secure and reliable location information for applications.

5.1.1 Motivation and Challenges

VANETs are valued by their delivered applications and services, such as safety and road condition's warnings. The drivers expect to receive reliable and consistent information. Non-line-of-sight (NLOS) conditions caused by moving obstacles can prevent proper communication among vehicles which effects critical services such as safety messages, routing and reputation exchange. For example, when evaluating the trustworthiness of a neighboring vehicle, many solutions [15, 16, 100, 110, 115] depend on evaluating the behavior of vehicles towards a certain event or its participation in message forwarding. In both cases, the results depends on how often events occur or message routing are required. Moreover, in an obstructed environment, a NLOS condition may give the impression that a neighbor is a malicious node, as it will fail to respond to message forwarding or event reporting. This will lead vehicles to evaluate the trustworthiness of others unfairly.

Securing VANETs' applications and preserving users privacy is a major task. With many applications depending on location information, application developers have to take into their consideration securing received data from other vehicles. With more applications beeing envisioned for VANET and the absence of a centralized network location service, redundant effort and process are conducted to secure location information for multiple applications. Moreover, the application that fails to secure the location service may risk and compromise the integrity of other applications.

Another challenge is protecting the vehicle's privacy. Communication devices are installed in private properties, and information are shared among other vehicles with no traveling boundaries. An attacker may use received position information to serve his/her goals. For example, an attacker could stalk a vehicle and collect its announced position to build a travel profile, or track the announced positions of authority vehicles to avoid encountering them on the road. Researchers have discussed possible security attacks and privacy concerns in VANET [34, 51, 64, 76, 77]. They have proposed solutions to protect the network from identified threats. However, it is still a challenge to secure VANET

because attackers continue to look for technical limitations and security flaws to reach their goals.

5.1.2 Objectives and Contributions

VANETs are envisioned to provide multiple applications for drivers, authorities and passengers. The network will not be limited to deliver a single or limited number of applications. For location-based applications, securing received information is important to secure their deliverables. Our objective is to provide vehicles with a secure location information service that will maintain received position information and provide the applications and other services with secure data. With such solution, securing location data can be focused on securing the proposed service. It will also reduce the risk of handling location security at application level and consolidating it in a single service.

In this chapter we developed a secure neighborhood location awareness service framework for VANET. The model consist of several components that adds security measures to the exchanged location information which will help to secure VANET applications and services. The service will allow vehicles to evaluate received position information from their neighbors and to maintain the integrity of the stored location data while preserving the vehicles' identity and activities. Another component in the framework is a secure trust evaluation model that allows vehicles to evaluate the trustworthiness of other nodes using the neighborhood awareness and location information. Moreover, the framework integrates the earlier proposed protocols in this thesis into the proposed service. The secure location verification protocol that allow the service to verify location information under NLOS conditions, and the AGB protocol which will support QoS to help authorities and network managers to control periodic message broadcast.

The remainder of this chapter is organized as follows: Section 5.2 will discuss the security vulnerabilities that will risk users privacy and location integrity followed by the security requirement for location information in section 5.3. In Section 5.4, we will present the secure neighborhood awareness service model and components. In Section 5.5 we describe the secure neighborhood awareness and group beaconing. Section 5.7 discuss the location verification components. In Section 5.8 we discuss the QoS management followed by a trust evaluation model in Section 5.6. Section 5.9 will discuss different aspects of the proposed solution. Finally, we end the chapter with a summary and remarks.

5.2 Adversary Model

Security is a broad term that involves many aspects and different point of views. To focus our work, we will discuss a security risk that involves the exchanged location information among vehicles. The objective of the proposed framework will countermeasure such risk and provide secure location data for location-based applications.

Location information is important for VANET applications. However, attackers may use it in their attempts to track vehicles. The attacker tries to collect position data of a specific vehicle(s) and builds a travel profile to fulfill his/her intentions such as stalking or avoiding law enforcement vehicles. To conduct such an attack, the attacker gathers periodic beacon data and updates. Since beacons' messages usually contain information of a vehicle identifier, location coordinates, and mobility information (such as direction and speed), it will be easy for an attacker to construct a table with collected information for a subject vehicle once he/she receives it.

In Figure 5.1, we illustrate the possible options for sending periodic location information. Sending the beacon message in clear text is, without any doubt, not acceptable in VANET. An attacker who is eavesdropping on the wireless network can easily collect the desired information. Using digital signatures for authentication purposes usually allows sending the data in clear text. A receiver will authenticate the message integrity using the certificate and message digest to decide whether to accept the message. However, the attacker does not need to validate message integrity. The attacker will collect as many messages as are related to a selected vehicle ID. Encrypted messages, on the other hand, do keep position data protected from outside attacks. However, a compromised node, which can be part of any group formation, can easily have access to decryption keys. An attacker can compromise an eligible vehicle that has a valid identity with the certificate authority and thus can collect the desired information from neighboring vehicles.

As we have discussed in section 2.8, current security frameworks [12, 24, 34, 41, 51] apply digital signatures to authenticate exchanged messages. This protects the user's identities through the use of pseudonym keys that are frequently changed to avoid linking a group of messages to the same sender. To enhance the protection of the privacy of vehicles, it is necessary to protect the beacon content itself. This makes it useless for building a travel profile but, at the same time, it is useful for building awareness of neighboring vehicles.

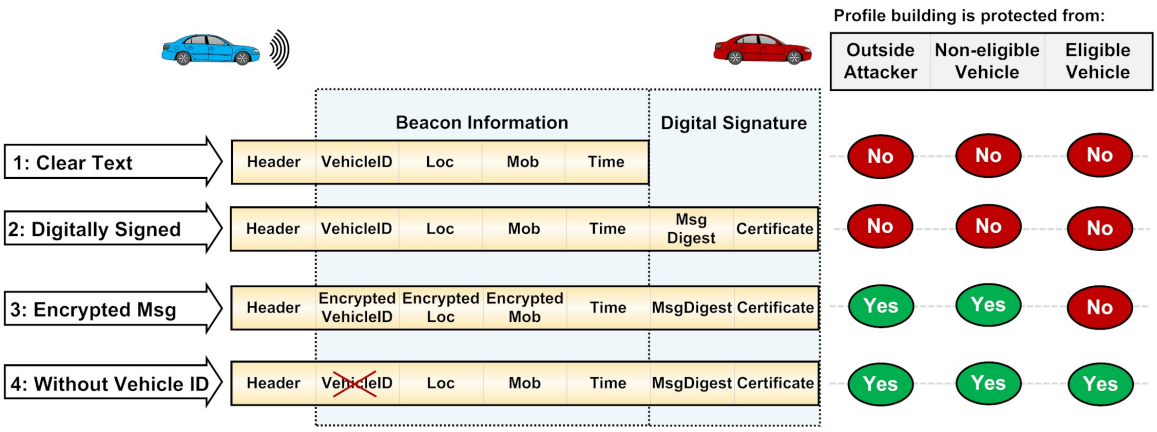


Figure 5.1: Security threats of profile building under different scenarios of beacon messages formats.

5.3 Security Requirements

With the security risk that have been identified, we need to set a list of security requirements to ensure that the proposed neighborhood awareness service framework will protect the location data. The following security requirements must be met to secure exchanged location information:

1. The proposed solution should enable the vehicle to evaluate the availability and trustworthiness of its neighbors while maintaining confidentiality and message authentication.

2. Evaluation process should not only depend on received incoming messages. The vehicle should initiate a validation process in a proactive and cooperative approach.

3. Data inconsistency and integrity should be monitored and validated and the proposed solution should increase neighborhood awareness and vehicle's knowledge about surrounding nodes under NLOS conditions.

4. Eliminate the use of Vehicle ID to reduce the chance of profile building

5. Preserve privacy in multiple processing levels.

5.4 Secure Neighborhood Awareness Service

5.4.1 Assumptions

To focus our work on developing a secure neighborhood awareness service framework and protect the network form the identified risk, we based the work on the following assumptions:

1. Each vehicle is capable of determine its own location in terms of GPS coordinates with high accuracy ($< 1m$ error) using a fusion of current technology such as global positioning system (GPS) [9];

2. Message receivers can determine the distance from the sender by measuring the physical parameters of the received radio signal strength (RSS) [66]; and

3. Message integrity can be verified and the sender can be authenticated by using digital signatures such as [29].

5.4.2 The Service Framework

To provide a secure neighborhood awareness in VANET, we proposed providing a secure service that works in the network layer (Figure 5.2). This way the service can pickup location information as soon as it passed by the MAC service and providing them to location based applications. Routing protocols that exists in the same layer can also obtain position information from the service outputs. The model will have the following components:

1. *Security module:* It works to secure communication channel among vehicles by providing secure key management and validation for message signatures and prevent unauthorized messages.

2. *Secure data warehousing framework:* It stores and maintains received location information of neighboring nodes. Secure access and users privacy should be maintained to prevent any attempt to build a traveling profile for a targeted vehicle.

3. *Monitoring process:* location information and mobility information should be monitored for consistency.

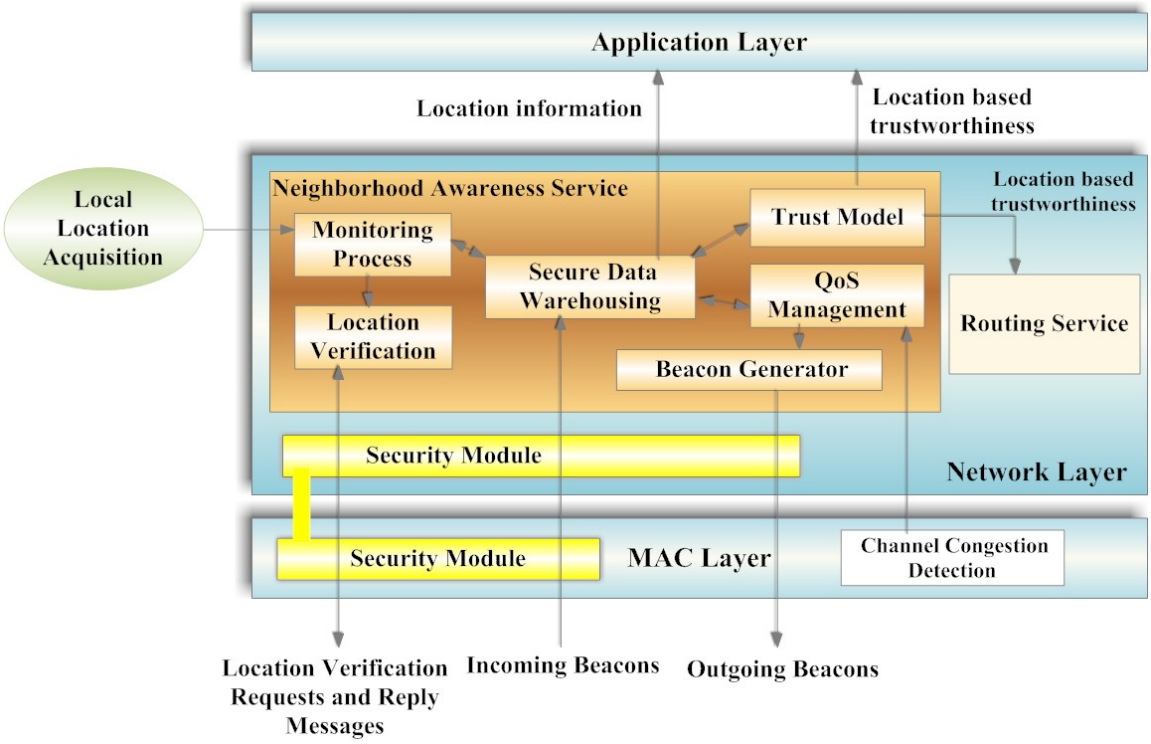


Figure 5.2: Neighborhood awareness service for VANET

4. *Location verification protocols:* The protocols evaluate and verify the location of a questioned node. If direct location verification cannot be established, indirect verification should be processed to validate the existence and location of the questioned vehicle.

5. *Trust evaluation model:* trust evaluation will help maintain neighborhood awareness of surrounding vehicles and their communication link reliability. Trust scores can be forwarded to VANET's applications and services to improve and secure their deliverables.

6. *QoS management and beacon generator:* This can be used to monitor transmission and communication conditions and adjust beacon rates and contents to support the required QoS of critical applications.

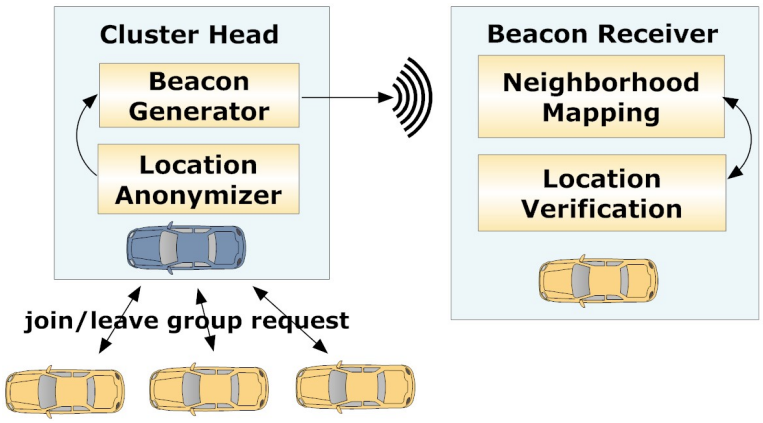


Figure 5.3: The framework architecture for secure location information exchange.

5.5 A Privacy Preserving Neighborhood Awareness and Group Beaconing

The privacy of information for vehicles and their users is a major concern in VANETs. Users will value the delivered applications but they want their privacy protection. Attackers may want to track a subject's location and expose their identity or traveling interests. To obtain the location information, the attacker have two sources of information, through beacon messages or by compromising the database of an active node. To protect the location information from such attempts, we present a novel location information exchange scheme. The proposed scheme consists of a cluster location anonymizer and the neighborhood mapping model (Figure 5.3). This scheme will be part of the neighborhood awareness service and describing the function of two of its components; the secure data warehousing and beacon generator.

5.5.1 Cluster Location Anonymizer

Vehicles travel on paved roads, and the traffic flow is controlled by sidelines and speed limits. Therefore, vehicles traveling on the same road segment form a group (cluster) of similarly behaving vehicles. A survey in [107] discussed articles that studied this behavior in VANET and that proposed algorithms to construct vehicle clusters. The main objective for vehicle clustering was to provide system scalability and to improve the network performance by reducing the message overhead. Another benefit from clustering

is to utilize the features of cluster groups to provide anonymity and secure message aggregation by using group signatures[72].

To focus our work on the privacy of the exchanged location information, we discuss the main characteristics of the clustering algorithm and the role of the cluster head (CH) to generate the group beacon. In this thesis, we assume a clustering algorithm is applied on the networking, taking into its consideration the mobility (speed and direction) similarity and stability, such as the one proposed in [113]. Vehicles traveling with the same speed and in the same direction are grouped, and a CH is elected to maintain group information. The CH will, or assigns a member to, generate a beacon message that includes the location information of the group. However, to maintain users' privacy, we propose that the CH collects the location information of group members through secure intra-group communication during the joining process and not periodic messages, which will also reduce the total number of generated messages. The CH will be responsible for generating the location updates of the group for all members. Each member will monitor its location, and the beacon message will be generated by the CH. If it detects any deviation from the broadcasted information, it will contact the CH to correct the member information.

In the proposed framework, the CH will anonymize its group members' location information by representing the location information as group area data. Therefore, the beacon information (Bcn) message sent by the CH will be constructed as $Bcn = \{G_{id}, Loc, Mob, N, L, W, T\}$, where G_{id} is the group ID, Loc is the center location of the group, Mob is the mobility information that includes the average speed and the direction of the group, N is the number of member nodes, L is the group length, W is the width of the group area, and T is the message time stamp. The CH will not include the exact location or reference ID of any of its group members. Doing so will prevents attackers from extracting the information of an individual vehicle. The location-based application is more concerned about location occupation and vehicles footprint, rather than who is at a location. For example, in a congestion detection application, the vehicle can detect a congestion if the number of vehicles on a road segment is higher than a threshold and the average speed is below a threshold.

The CH computes the group rectangular area information once it receives a joining request from a member. The center of the area Loc coordinates (X_{loc}, Y_{loc}) is given by (Figure 5.4):

$$(X_{loc}, Y_{loc}) \;=\; (\frac{min_x + max_x}{2}, \frac{min_y + max_y}{2}) \tag{5.1}$$

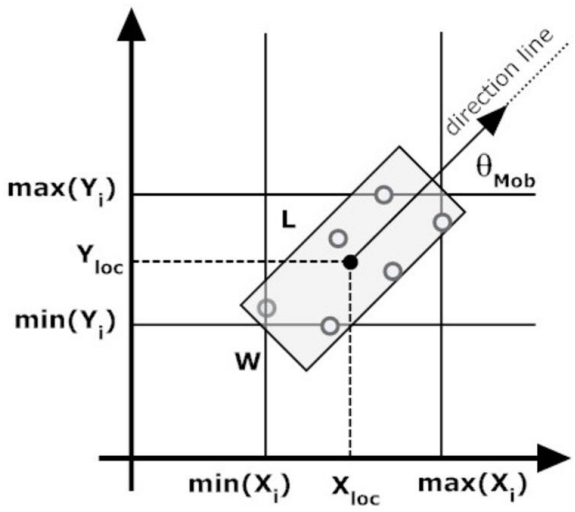


Figure 5.4: The cluster head computes the group area information.

Where min_x and max_x are the minimum and maximum values of all of the members x-coordinates, respectively. The min_y and max_y are the minimum and maximum values of all of the members y-coordinates, respectively. The length L is calculated as:

$$L = \frac{max_x - min_x}{\cos\theta} \tag{5.2}$$

Where $(\cos\theta \neq 0)$ and θ is the direction angle for the group. To calculate the width of the rectangle, the CH finds the maximum distance d_v of a member vehicle from the center direction line that is defined by:

$$y - y_{loc} = \tan\theta(x - x_{loc}) \tag{5.3}$$

And the distance d_v from the direction line $(ax_i + by_i + c = 0)$ is calculated as:

$$d_v = \frac{\|ax_i + by_i + c\|}{\sqrt{a^2 + b^2}} \tag{5.4}$$

The rectangle width L is calculated as $W = 2max_d$, where max_d is the maximum computed distance of all nodes.

5.5.2 The Neighborhood Map Model

Each vehicle monitors its surrounding area, which is divided into areas of 3 meters by 3 meters covering the physical communication range. We choose to use a 3-meter length

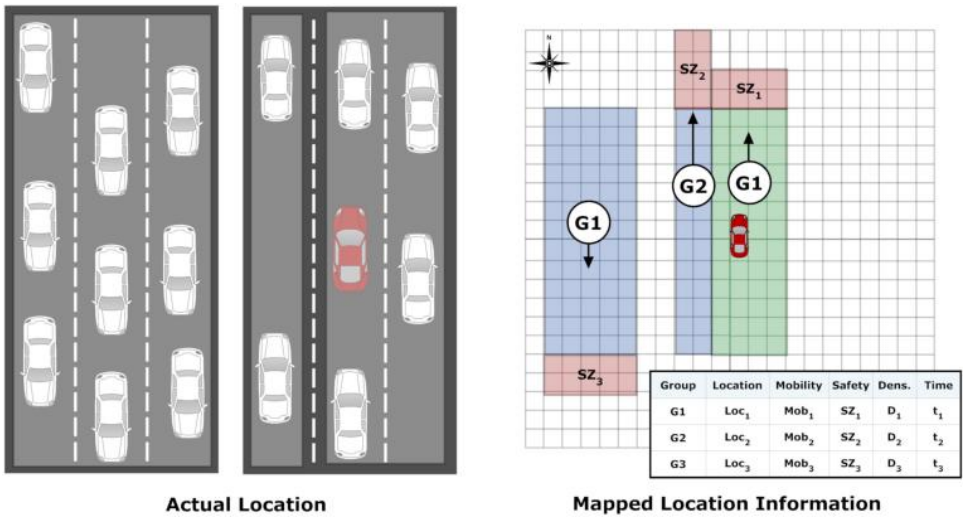


Figure 5.5: Mapping location information of neighboring vehicles.

based on the average width of a regular road lane. Once a vehicle receives a beacon message from its CH or other groups' CH, the announced location can be mapped by using the location information and converting the location coordinate to a relative area, as shown in Figure 5.5. The receiver will save the record of beacon information with its location in the map and time of update. A safety zone will also be added to the group information based on the group speed and direction. The safety zone will help vehicles to maintain awareness of their surroundings. For example, if a vehicle wants to pass another vehicle and move to the faster lane that is covered by a group area or a safety zone, it will alert the driver to stay in his position, as it is not safe to change lanes at this moment.

To maintain the integrity of stored group information, a location verification process will be initiated if the location in the map receives updates more or less frequently than expected (beacon interval time) and if the two group areas overlap. The CH of the questioned group will be challenged to verify the overlapped location area.

5.5.3 Secure Neighborhood Awareness Mapping Process

After describing the technique of the cluster anonymizer and the neighborhood map model, we will describe how they will work together as part of the framework process of exchanging the beacon information and maintaining the neighborhood awareness information. The process will take the following steps:

1. Each vehicle is running the cluster algorithm, in which vehicles with similar direction and speed are grouped. A cluster head (CH) is elected by the cluster algorithm, and group members securely communicate their location information to the CH. The CH will calculate and maintain the group location information as beacon information ($BcnInfo = \{Loc, Mob, N, L, W\}$). The group CH will send beacon messages (Bcn) about the group location every T_b. When T_b expires, the CH will construct and sign a beacon message, such as:
   $Bcn = \{G_{id}, Loc, Mob, N, L, W, T, MD, Cert\}$,
   where MD is the message digest of the signed message and $Cert$ is the certificate that will be used to authenticate the message integrity and sender.

2. When a vehicle receives a beacon message, it will authenticate the message sender and check the message integrity using the attached certificate. If the message was validated, it will extract the location information ($BcnInfo = \{Loc, Mob, N, L, W\}$). If the authentication fails, it will ignore the message.

3. The group location information will be mapped, and group information is stored. The ΔX will decide the North-South destination, and ΔY will determine the East-West position with respect to the receiver. If no group record is covering the allocated cell, a record will be added to the database containing the assigned area, location coordinates, mobility information, area size, and update time. If the group record is already assigned to the cell, it will compare the last update time with the current time to check for validity.

4. If the time is equal to the known beacon interval (T_b) and the updated information matches the predicted changes of the group, the record will be updated. If the time is different, this can indicate changes in the group CH or that an obstacle is blocking reception of beacon messages. To secure the integrity of group record, if the the time of the last update received was larger than (T_b), a location verification process will be triggered.

5. The stored data are continuously monitored to detect any data inconsistency. Events such as having two or more group area overlaps or inconsistent beacon time, as described in step 4, will trigger a location verification process that will send a request to a neighboring vehicle to obtain feedback about the subject location.

Algorithm 5.1 The computation and sending of group location information.

1: **process:** compute $BcnInfo$
2: **input:** $receiveMsg() = join/leave\ group$
3: Begin()
4: **if** (nodeType() = CH) **then**
5: ▷ Processed by CH
6: calculate $min_x, max_x, min_y, max_y$
7: calculate Loc_x, Loc_y
8: calculate L, W
9: BcnInfo = $\{G_{id}, Loc, N, L, W\}$
10: **end if**
11: End()
12:
13: **process:** send beacon
14: **input:** $timerExpire(T_b) = true$
15: Begin()
16: **if** (nodeType() = CH) **then**
17: ▷ Sent from CH
18: $Bcn = \{BcnInfo, T, MD, Cert\}$
19: sendMsg(Bcn)
20: **end if**
21: End()

Algorithm 5.2 Receiving group beacon information.

1: **Process:** *receive beacon information*
2: **Input:** $receiveMsg() = Bcn$
3: Begin()
4: **if** $(authMsg(Bcn) = true)$ **then**
5: ▷ message is verified
6: getBcnInfo($G_{id}, Loc, Mob, N, L, W, T$)
7: mapCells(BcnInfo)
8: **if** $(MyGroup() = G_{id})$ **then**
9: **if** (MyLocIn(BcnInfo) = false) **then**
10: send correction to CH
11: **end if**
12: **end if**
13: **if** (cellEmpty(BcnInfo) = true) **then**
14: ▷ the position is not occupied
15: addRecord(cellLabel,BcnInfo)
16: **else**
17: ▷ there is a record for this position
18: **if** $cellRecordGID = G_{id}$ **then**
19: updateRecord(BcnInfo)
20: **else**
21: verifyLoc(cellLabel)
22: ▷ trigger a location verification protocol
23: **end if**
24: **end if**
25: **end if**
26: End()

5.5.4 Privacy Evaluation Aspect

The main objective for the neighborhood awareness and group beacon scheme is to protect the privacy of the exchanged location information. To evaluate the performance of the scheme, we focus on the information entropy of the stored location information which was received through the group beacon messages.

The information entropy is used to evaluate the privacy of a set of data. It was first introduced by Shannon [88] in information theory and was then used as a metric to evaluate location privacy [89]. We will examine the location privacy of a vehicle using the information entropy of the stored beacon message. The information entropy (certainty) of a targeted vehicle location (H_v) obtained from a compromised vehicle neighborhood list is given by:

$$H_v \;=\; \sum_i \; p_i \;\log \frac{1}{p_i} \tag{5.5}$$

where p_i is the probability of successfully identifying the correct record, from list (i), that is linked to the target vehicle. To protect user privacy, the objective is to lower the entropy value. In this study, we compare the location privacy in three different beaconing approaches: exchanging location information with a vehicle ID, without an attached ID, and using group location mapping.

Using Vehicle ID: In a scenario with a vehicle ID registered in the list, the attacker who knows its target ID can search for the vehicle record in the neighborhood list. The probability of locating a target vehicle record will be ($p_v = 0.5$). Therefore, the information entropy will be $H(v) = 0.5$.

Without Vehicle ID: In the scenario where the vehicle ID is not used when storing vehicle information, the confusion is increased in which the probability of linking a record to a target is ($p_v \;=\; 1/n$), where n is the size of list. Therefore, the information entropy of a targeted vehicle is given by:

$$H_v(n) \;=\; -\; \sum \; \frac{1}{n} \;\log \frac{1}{n} \tag{5.6}$$

Group Location Mapping: Using group mapping to store the location information of surrounding vehicles, the probability of detecting the exact location of a targeted vehicle is a function of the number of groups (g) and the group area (A). The attacker will attempt to determine the location of the vehicle within the group specified area. As discussed previously, the group area is a function of the number of nodes (n) and the group average speed (s). The occupied area increases as the speed increases because

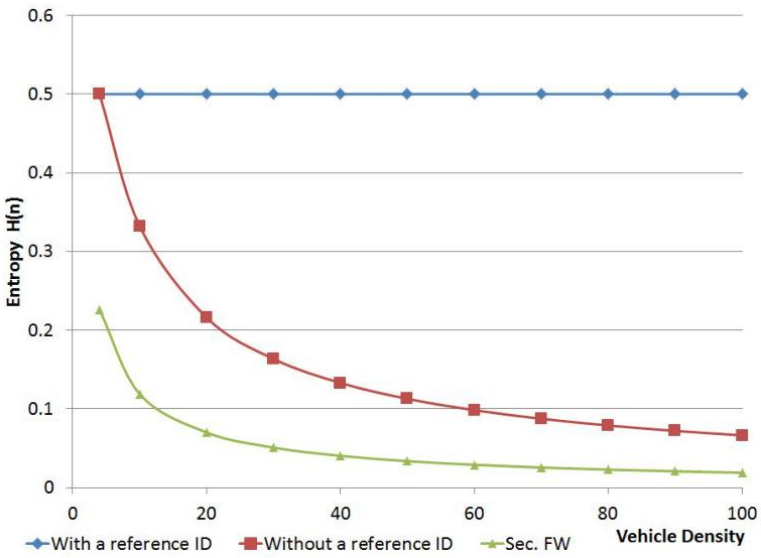


Figure 5.6: The entropy of detecting a vehicle from stored location information.

the distance between vehicles increase to maintain a safe distance. The probability of guessing the exact location within a group is $p_v = 1/A_g(n,s)$

$$H_v(n,s) = \sum_i \sum_{j=1}^{g} \frac{1}{A_j} \log A_j \tag{5.7}$$

As shown in Figure 5.6, we can observe that the group zone mapping have a better privacy protection for location information by reducing the certainty of detecting the location of the targeted vehicle. In Figure 5.7, the graph shows how the certainty decreases as speed and group density increases. Hence, group location mapping will preserve the privacy of vehicles location better than just eliminating the use of vehicle ID in the beacon messages.

5.5.5 Simulations and Privacy Evaluation

To evaluate the privacy of vehicle's location information, we conducted the simulation experiments using the network simulator (NS-2), ver. 2.34, using the parameters in Table 5.1. Vehicle mobility traces were generated by simulation of urban mobility (SUMO) for urban city and highway environments based on the road network of the city of Ottawa, Ontario, Canada. The simulation selects and tracks the movement of the targeted vehicle using collective information from neighboring nodes.

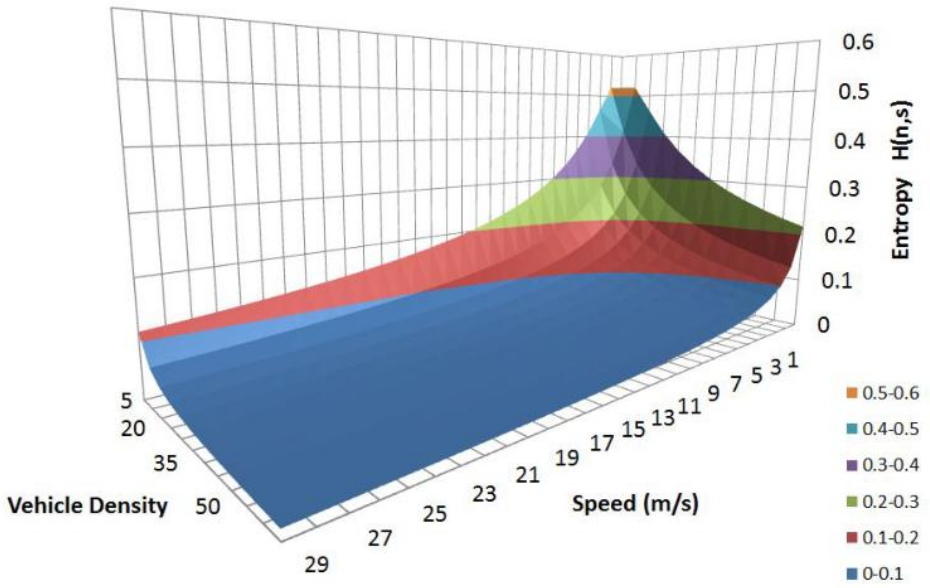


Figure 5.7: The entropy of detecting a vehicle of stored group information.

Table 5.1: Simulation Environment Parameters

Parameter	**Value Setting(s)**
Radio Propagation	*Two-ray ground, Nakagami*
Antenna Type	*Omni antenna*
MAC Layer	802.11*p*
Radio Range	300*m*
Beacon Freq	10 *Hz*
Data Rate	6 *Mbps*
Number of Vehicles	200–600
Speed Limits (Highway)	0–100*km/h*
Road length (Highway)	20*km*
Speed Limits (Urban)	0–50*km/h*
Road Area (Urban)	3*km* x 4*km*
Simulation Time	15–30*Min*

On the highway roads, vehicles' mobility (speed and direction) tends to be more stable than for vehicles in the city, where they stop for signals, take turns, change lanes, and come to total stops. Having each node send its beacon message will increase the probability of packet collision as the vehicle density increases. However, because distances between consecutive vehicles are required to be larger to maintain a safe distance, the dropped packet impact on the neighborhood list is less than it is in a city environment. In Figure 5.8, the elimination of vehicle's ID from the beacon messages reduced the certainty of the targeted vehicle's location. In a normal highway scenario and with different densities, distances among vehicles are maintained. Therefore the surrounding neighboring nodes are almost similar and the certainty of a tracked location data are the same. The consolidation of vehicles in the city environment (Figure 5.9) increases the probability of packet collisions, reducing the size of the detected neighborhood list, which will increase the entropy value of detecting a target vehicle.

The proposed solution of using group beacons has decreased the location information entropy. The attacker has to blindly guess the location and the group membership of a targeted vehicle within an announced area of groups. In a highway scenario (Figure 5.10), the distance between consecutive vehicles is larger, as drivers maintain a safe distance with the car in front. This behavior will result in giving a number of vehicles a larger group area than it will in a city environment for the same number of vehicles. Therefore, the certainty in a highway environment will be lower than in an urban environment (Figure 5.11). The proposed solution of group anonymizer and beaconing, as shown in Figure 5.10 and 5.11, had reduced the certainty value of information better than the certainty value of just eliminating the vehicle ID from beacon messages (Figure 5.8 and 5.9).

In Figure 5.12 we can observe the effect of speed on the information entropy in a highway environment. The safety distance between vehicles will increase the group size and decreases the information certainty of locating a targeted vehicle compared to in a city environment, as seen in Figure 5.13. When the density increases, the distance between vehicles will get smaller, and drivers tend to move more cautiously, which will reduce the size of the group area.

5.6 Trust Evaluation Model

The neighborhood awareness service in VANET should provide vehicles and applications with information of neighboring locations and their status. With the dynamic

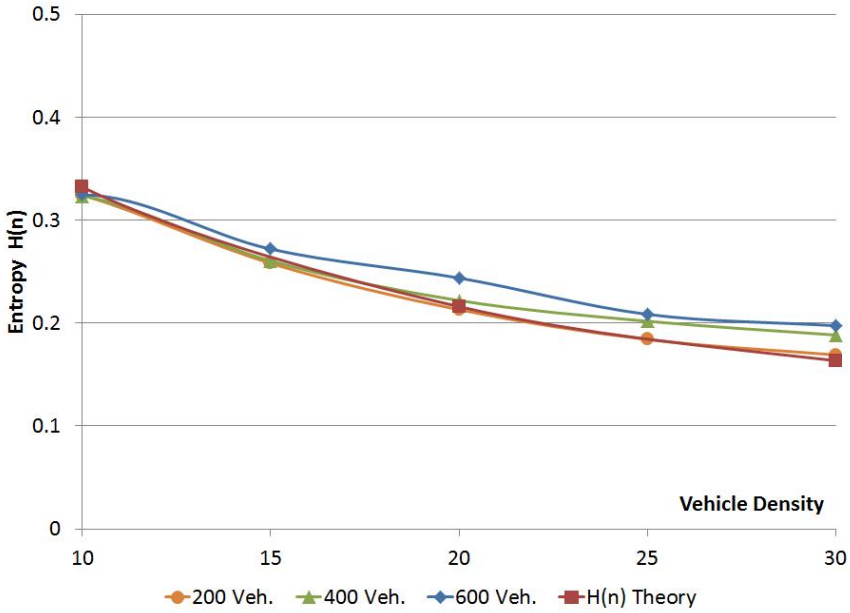


Figure 5.8: The information entropy of detecting a vehicle in a highway scenario with different densities by eliminating the use of vehicle ID.

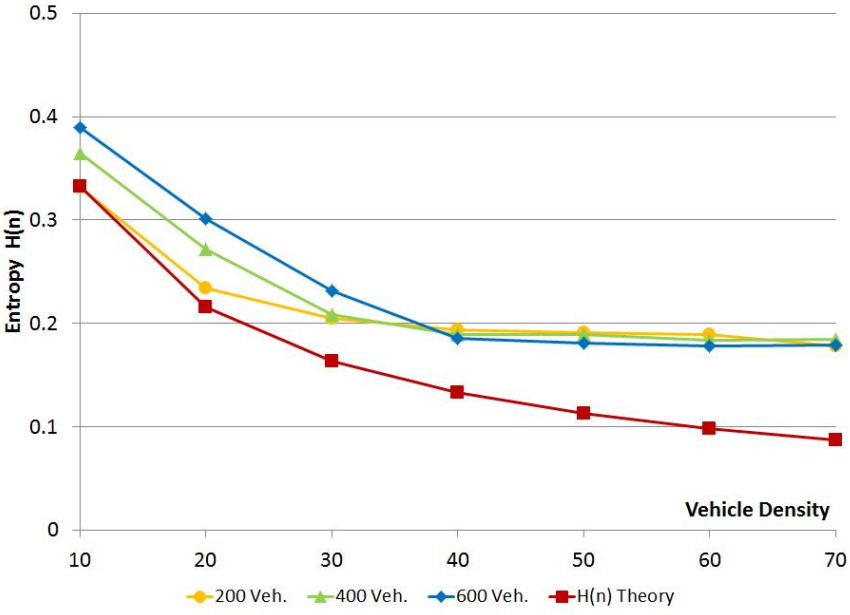


Figure 5.9: The information entropy of detecting a vehicle in an urban city environment scenario with different densities by eliminating the use of vehicle ID.

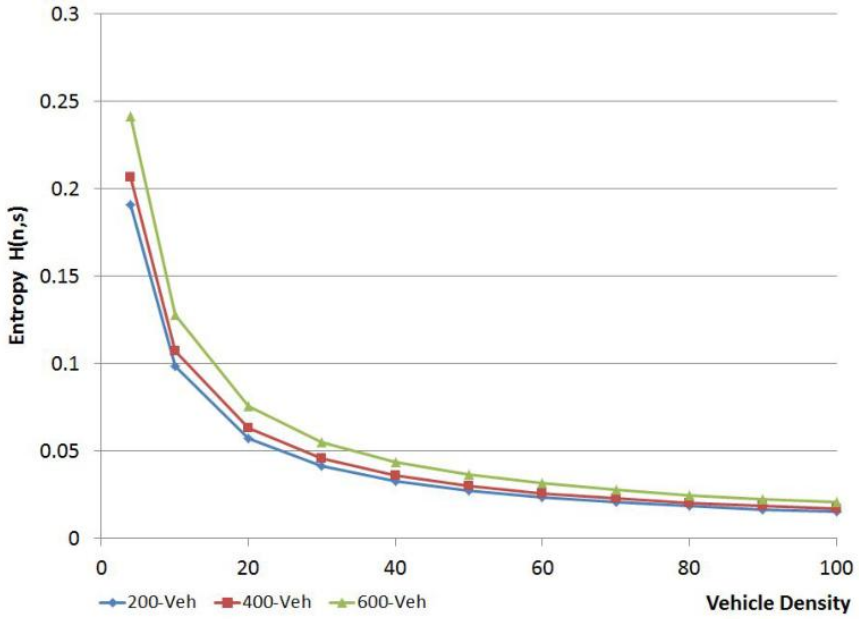


Figure 5.10: The information entropy using cluster group beacon in a highway environment with different densities.

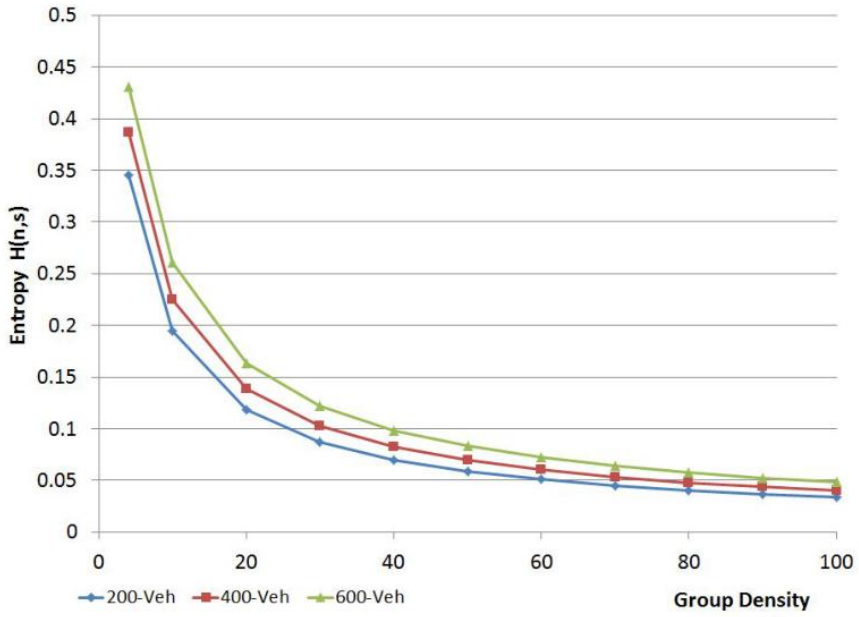


Figure 5.11: The information entropy using cluster group beacon in an urban city environment with different densities.

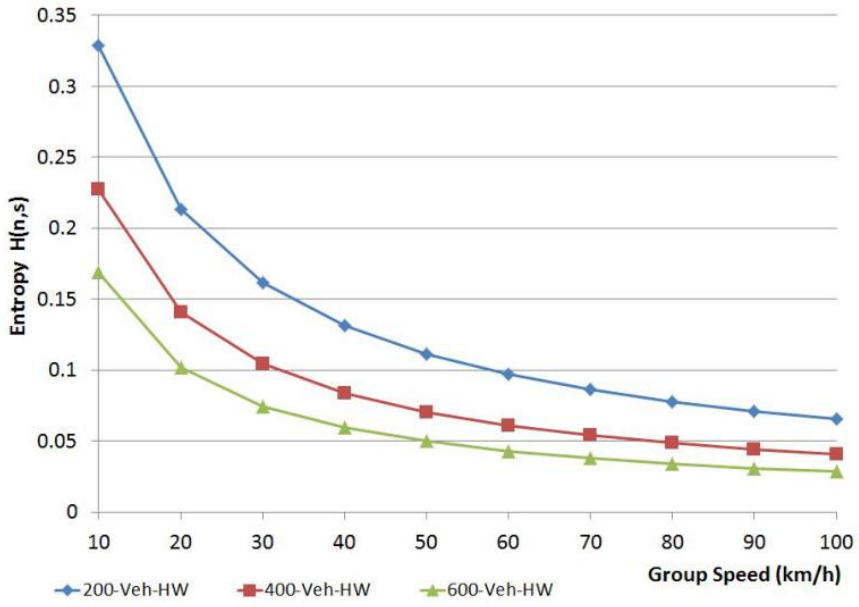


Figure 5.12: The average group speed affects the information entropy of group beacon as the area and relative speed between member vehicles increase when speed are increases in a highway environment.

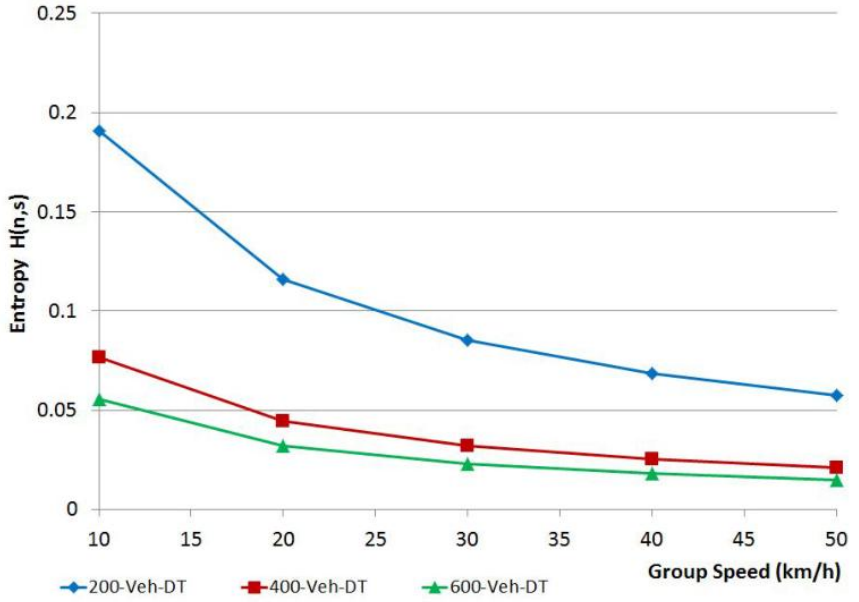


Figure 5.13: The average group speed affects the information entropy of group beacon as the area and relative speed between member vehicles increase when speed are increases in a city environment.

Table 5.2: The location information entropy (H) of individual beaconing and group area beaconing with 95% confidence interval.

		Individual		Group Area	
Density	Type	Min	Max	Min	Max
200	HW	0.168643648	0.336762021	0.00062061	0.06797668
200	DT	0.099530346	0.364405955	0.00283285	0.13752301
400	HW	0.134079802	0.271676987	0.0084781	0.04723322
400	DT	0.064545401	0.240108604	0.000959354	0.06821801
600	HW	0.12467065	0.243155961	0.00396332	0.10621859
600	DT	0.053895027	0.194336752	0.012322235	0.05092559

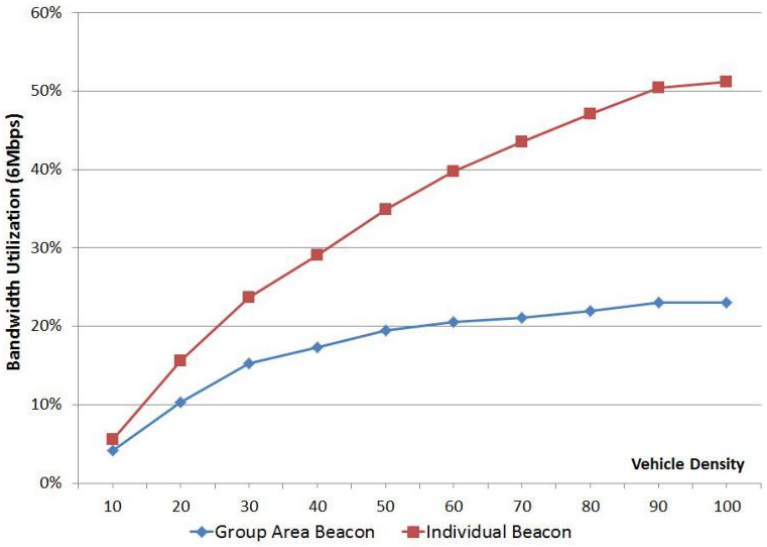


Figure 5.14: The group area beacon reduced the number of generated beacon messages in the network.

nature of the network, vehicles' relative position and communication status are subject to change. The trust model component will interpret the changes into trustworthiness value which will allow the vehicle to determine which neighbor will be the best to perform an assigned task, such as message forwarding. we discuss a trust evaluation method that will help vehicles maintain integrity information and reputation information of their neighbors.

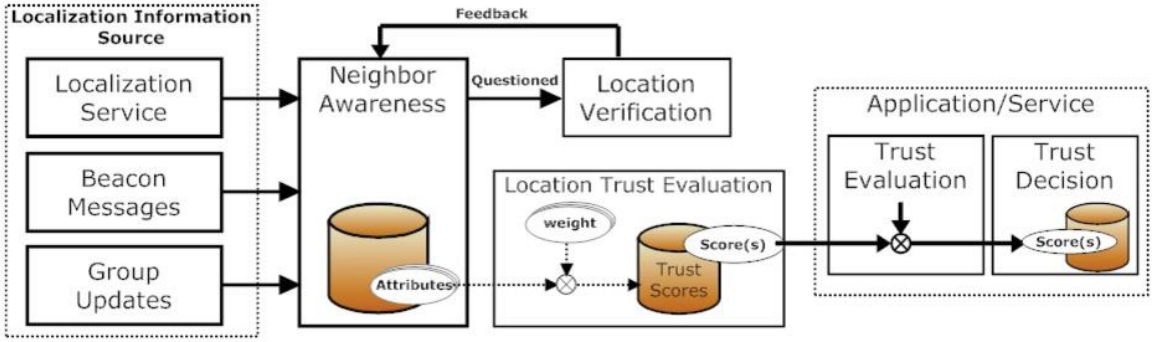


Figure 5.15: Secure trust model for VANET using location trust information.

5.6.1 Secure Trust Model

Secure messaging using cryptography, digital signatures and exchanged security keys were proposed to help build trust among vehicles allowing the receiver to accept or reject the message [12, 24, 34, 41, 51, 52, 55, 64]. However, compromised nodes can gain this level of trust once they are a member of the network. In addition, trust decisions are determined by evaluating exchanged security keys or by monitoring incoming messages and nodes' behavior towards events. In real life implementations, moving obstacles (e.g. trucks) can block exchanged messages and prevent proper exchange of critical information. For such reasons, it is necessary to enable the vehicle to further evaluate and compute trust level of its neighbors to maintain security measures. Several methods and approaches have been discussed and proposed for wireless communication [15, 16, 100, 110, 115]. However, there are raised issues that may prevent implementing proposed solutions in VANET[112]. In Figure 5.15, we illustrate the secure trust model components. The general process steps are as follows:

1. *Gathering Localization Information*: Each vehicle determines its own location information by its local localization service. It collects its neighbor information from received beacons and group updates.

2. *Maintain Neighborhood Awareness*: Each vehicle maintains a database of its current neighbors' location and their mobility information. The database is maintained and monitored continuously to check for any data inconsistency.

3. *Location Verification*: If the neighborhood awareness service detects any inconsistency in its data, it triggers the location verification process. The process validates claimed location of neighbors and updates the awareness database.

4. *Location Trust Evaluation*: This module calculates neighbor's trust based on location reachability and assigns a score to each node.

5. *Application Trust Evaluation*: Applications and services have different requirement and computation methods to compute trust of other nodes. Applications now have an additional attributes that tracks nodes' location and their reliability.

5.6.2 Trust Evaluation

Studies have presented trust evaluation methods for VANETs [15, 16, 100, 110, 115]. The evaluation are based on received messages of reported events and the nodes' responses to them. In our method, the evaluation attributes are based on location information and the surrounding network context. The vehicle should challenge a node and request for a verification to determine whether the communication link is affected by an obstacle or not. Therefore, a misbehavior of a node towards an event might be due to the affect of obstacle rather than an attempt to mislead. Moreover, a node with direct stable communication link is more trusted than a node affected by a non-line-of-sight (NLOS) condition.

Each node maintains a record of every neighboring node. In addition to basic node information (mobility information, relative distance, group id and a time stamp of last update), we add a NLOS flag indicator, number of hops and a trust score. The flag indicates whether the node information was received through direct communication or through a third party using the verification process. The number-of-hops value keeps track of number of hop to reach the subject node. The value is also computed through the location verification process. Individual trust evaluation is based on the following selected attributes:

1. *None-line-of-sight (NLOS) condition:* Nodes with direct communication are more reliable to deliver messages than are nodes that are behind obstacles. A vehicle can detect a NLOS condition with another vehicle by monitoring the beacon rate and data consistency of the subject node. Initiating a location verification process to evaluate the status of the node and determining if the communication link is affected by NLOS condition. If a NLOS condition is detected, the attribute for that node can be noted as: $T_1 = \alpha_1(1 - NLOS)$, where (α_i) is a normalizing factor and NLOS = 1 or 0, indicating the link state for NLOS as true or false, respectively.

2. *Mobility similarity:* The relation among vehicles traveling in the same direction

will last longer, which will allow more interaction and message exchange[2]. We are taking this into consideration as an attribute for the trust evaluation by evaluating the cosine similarity of the mobility vector of two nodes (M_i and M_j) will allow vehicles to determine direction similarity, such that:

$$cos(\theta) = \frac{M_i.M_j}{\parallel M_i \parallel \parallel M_j \parallel} \tag{5.8}$$

if $cos(\theta)$ is or is closer to (0), this means that the two vehicles are independent and traveling on the opposite direction. If the value is, or closer to (1), the two nodes are traveling in the same direction. This attribute will be noted as: $T_2 = \alpha_2(cos(\theta))$, where ($\alpha_2$) is a normalizing factor.

3. *Distance and hop count:* Different applications may have different requirements with regard to node distance. A node that wants to send safety warning messages trusts further nodes to forward their messages in order to reach further distances, while other applications, such as lane merging, trust closer nodes. The distance to the node and the number of hops to reach it will help evaluate the state of the node's position. For example, To reach a node in a single hop is more reliable than a node with the same distance but requires more hops to reach. We take this into consideration and note the attribute as: $T_3 = \alpha_3(dist/hops)$, where ($\alpha_3$) is a normalizing factor.

4. *Communication link stability:* With the dynamic nature of VANETs, the relative position among group of vehicles will change. Moving obstacles will also affect the communication link between two vehicles. Neighbors that maintained a stable link-state is more reliable than nodes that continuously switches from one state to another. To take that into consideration, we indicates the time the node remained in the same state (LOS or NLOS) as an attribute noted as: $T_4 = \alpha_4(t_s/t_{th})$, where ($\alpha_4$) is a normalizing factor, t_s is the time since the last state change, and t_{th} is the minimum time threshold to consider the link as a stable link.

5. *Current trust score:* Tracking trust values for neighboring nodes will help detect sudden change in their behavior. We consider the last calculated trust value for a node and note it as: $T_5 = \alpha_5 Trust_0$, where (α_5) is a normalizing factor.

We will use a weighted average approach to compute the trust score for each node, where weights (w_i) are associated to the attribute values, such that:

$$Trust = \frac{w_1T_1 + w_2T_2 + w_3T_3 + w_4T_4 + w_5T_5}{w_1 + w_2 + w_3 + w_4 + w_5} \tag{5.9}$$

A vehicle will evaluate and maintain the trust values of neighboring nodes. With nodes' reachability and reliability information, other applications and services can integrate this attribute and values to their own trust evaluation mechanism.

5.7 Location Verification

In VANET, each node maintains a neighbors' location database that is frequently updated by received beacon messages and group updates. While vehicles travel, the database starts to build up, creating neighborhood awareness for the vehicle. False information is expected to be received due to the nature of wireless communication or an adversary attempts to inject false data to the network. To secure the received information, the vehicle should be able to verify the correctness of the announced positions. In the proposed neighborhood awareness service, the main objective of the verification process is to verify the location of a node through methods other than received beacon messages. At first, the process will conduct a direct verification protocol, such as radio signal strength (RSS) measurements [66]. If direct verification fails, a location verification protocol under NLOS will be triggered to verify a node that might be blocked by an obstacle. In Chapter 3, we presented an efficient location verification process under NLOS conditions which can be used in such condition.

The location verification process is an important component that will help determine the communication state of neighboring nodes and increase the neighborhood awareness. For example, a vehicle can determine whether it has a direct communication link with one of its neighbors or if a NLOS condition exist between them.

5.8 QoS Management and Beacon Generator

Periodic messages are generated to update position and mobility status to neighboring nodes. With the increasing number of vehicles and multiple applications, the number of messages will increase and will effect the network performance. Critical applications may suffer to deliver their messages in dense area. Therefore, it is essential to provide QoS for

critical applications and allow authorities to dynamically change the QoS requirements based on current conditions and events.

The role of the QoS Management component is to monitor different attributes, such as the number of vehicles and authority's instructions, and change the rate and content of generated beacon messages. In Chapter 4, we proposed an adaptive group beaconing mechanism that will reduce the impact of beacon messages on the network.

5.9 Solution Aspects and Security Measures

The neighborhood awareness service should be a secure and reliable source of location information. Securing the exchanged location information among vehicles is a challenge due to the nature of the network and the continuous attempts by attackers to discover flaws and technical limitations. In this section, we briefly discuss additional aspects of the proposed secure neighborhood awareness service scheme and its security measures:

1. *The proposed solution should maintain confidentiality and messages authentication*: As we stated in our assumptions, communication channel are secured using digital signatures and vehicles are able to validate the sender and message integrity. Moreover, in our proposed location verification process, the request and reply messages receivers validate the sender and compare its location and previous request information prior processing or forwarding the messages. This step will eliminate the chance of processing false requests or reply that can be injected to the network.

2. *Data inconsistency and integrity should be monitored and validated*: The neighborhood awareness is continuously checked. Mobility and change of driving behavior will results in lots of changes in the data. Once an inconsistency is detected, the vehicle sends a verification request to validate the questioned node to update its information.

3. *The proposed solution should increase neighborhood awareness and vehicle's knowledge about surrounding nodes under NLOS conditions*: Each vehicle maintains a database that contains information about near neighbors. As we have mentioned, obstacles can prevent messages from reaching its destination. Vehicles would not receive proper beacons and are not able to directly verify one of its neighbors. With the proposed location verification process, we use a cooperative multihop approach to validate the location of a questioned node and recover from the NLOS by trying to reach it through others.

4. *The solution should not only depend on received incoming messages. The vehicle should initiate a validation process in a proactive and cooperative approach*: Vehicles update their information by received beacons and group updates through direct communication. The vehicle that detects inconsistency in its database initiates the location verification process. Enabling the vehicle to question certain node about their location will detect and reduce the effect of false position information sent by malicious nodes.

5. *The solution should support scalability*: The verification process is the model component that generates request messages. Every neighbor that listens to the propagated message marks the claimed vehicle for verification. Once a reply is received, nodes that marked their records will update their information. This will reduce the number of generated messages to verify a single node by multiple vehicles at the same time. Moreover, max hop count and controlled message dissemination are used to control message broadcast.

6. *The vehicle should be able to evaluate the availability and trust of its neighbors*: With a well maintained neighborhood awareness information, a vehicle can evaluate the trustworthiness factor of a neighbor by evaluating its reachability and how reliable is the line of sight between them. Once evaluated, other applications and services can utilize this information to evaluate their trust of other neighbors. For example, routing protocols can select a more reliable "next hop" that can be reached, or a safety application can still trust messages from a vehicle that is reporting an event but obstacle are preventing the messages from reaching their destination.

7. *Eliminate the use of Vehicle ID:* In our proposed solution, we stressed excluding the vehicle identifier in beacon messages. This will prevent the use of beacon information to track and build a profile for a target vehicle. However, excluding the ID from the beacons increases the challenge of managing received location information and making full use of the information received. In this chapter, we presented a solution that tackles such a challenge. The vehicle ID will be necessary for certain applications. Vehicles should exchange their IDs in a secure encrypted session provided by applications and not through periodic beacon messages.

8. *Preserve privacy in multiple processing levels:* By eliminating the use of vehicle IDs in beacon messages along with the security frameworks that use digital signatures

to provide message authentication and integrity checks, we can prevent attackers from tracking vehicle identities and linking announced positions to a sender using the content of the messages.

9. *Supporting non-repudiation:* Authorities must be able to track vehicles in certain conditions. This feature is supported by secure digital signatures and key management frameworks, as has been discussed by researchers such as [12, 34].

10. *Resist possible attacks on the system:* An attacker may attempt to inject false location information into the network. To protect the system from such an attack, multiple countermeasures are considered. Announced locations are compared with received radio strength measurement to calculate relative distance. Moreover, continuous monitoring to check for data inconsistency is performed. Records of post times are checked to detect missing or excessive updates. Group updates can also be used to update and locate mismatched allocations. Once an inconsistency is detected, a location verification process is carried out to evaluate the trustworthiness of the information and to retrieve updates from cooperative neighboring nodes.

11. *Detect and recover data inconsistency:* Data inconsistency may result from different events due to the nature of VANET, such as a vehicle changing its position in a formation by overtaking another vehicle, or due to a security attack. That is why continuous data monitoring of critical information, such as recording update times, will help detect any data inconsistency. Launching a verification process to validate a vehicle in a certain position will provide accurate feedback about the current state of the subject vehicle.

12. *Scalability support:* As we have observed in the simulation results, the proposed privacy preserving group beacon reduced the number of beacon messages generated. Each vehicle monitors its surrounding area (A) covered by its communication range (r), which is divided into an area cell of width (w). The max number of cell record in the database is given by $sizeNL() = A/w^2 = \pi r^2/w^2$. However, as shown by simulation, as the density of vehicles increases, the number of detected vehicles is less than the actual number of existing vehicles due to signal interference and packet collisions. Moreover, when vehicles are moving, minimum distance is maintained between vehicles in a single file. Such factors reduce the number of vehicles being monitored in a list. As shown in Figure 5.14, the beacon message generated by the group area approach consumed fewer bandwidth resources than

individual beaconing. The beacon messages are generated from the CHs only, and member vehicles will not send beacon messages, which will reduce the number of generated messages from (nR) messages to (gR), where n is the number of nodes, g is the number of surrounding groups, and R is the beacon rate.

5.10 Summary

Protecting VANET against possible security threats is essential. The nature of its implementation and characteristics introduces new challenges and concerns. Preserving a vehicle's privacy is a major concern for the researchers. It is important to identify and resolve any possible threat that can breach users' identities or their road activities. What adds to the challenge is that attackers will keep looking for system flaws to serve their goals.

With the number of provisioned applications in VANET, it is important to secure location information against possible attacks. To prevent redundant work and protect the applications from possible security flaws, it will require to consolidate location date under a single service that will insure its accuracy and validate its integrity.

In this chapter, we designed a secure neighborhood location awareness service for VANET that will validate and maintain received position information for neighboring nodes. The model consist of several components: a Secure data-warehousing, data inconsistency monitoring process, a location verification process, a trust evaluation model, and beacon generator management with QoS provisioning.

In addition, we discussed a security threat that an attacker can accomplish using a compromised vehicle. By collecting a vehicle information, a stalker can track a target vehicle, or a street racer can detect police cruisers and avoid them. We developed a secure neighborhood awareness process that exchanges secure beacon messages without the use of vehicle ID. The solution prevents attackers from collecting information and building a traveling profile for a targeted vehicle. Even if the attacker managed to compromise an eligible vehicle, it would be difficult to link collected position data to an individual vehicle. As discussed in the security analysis section, the solution should monitor and detect data inconsistency, which initiates a location verification process to verify a questionable vehicle location.

Moreover, current trust evaluation models depend on evaluating the behavior of nodes towards events and message forwarding results. NLOS conditions can make it difficult to differentiate between a miss behaving node and a node that is blocked by an obstacle.

In this chapter, we developed a trust model that uses location information as an evaluation attribute. This will overcome the effect of NLOS and increase vehicle's awareness of its neighbors. The model provides a source of information for other applications and services to determine the reliability and reachability of neighboring nodes based on their location, mobility and line of sight stability.

Chapter 6

A Quantified Security Evaluation Model

6.1 Introduction

Location information exchanged among neighboring vehicles is an essential process in vehicular ad-hoc networks (VANETs). Many applications are envisioned to enhance the driving experience by providing road conditions and services' information (e.g., road safety and warning messages). However, to provide reliable information, location-based applications depend on the current position of the vehicle and the location of neighboring nodes. Thus, neighboring vehicles will exchange their current mobility and location information through periodic beacon messages. Therefore, it is important to secure the exchanged location-information and users' data.

Researchers [34, 81, 27] have discussed security vulnerabilities and concerns, and have identified the requirements for a secure communication and message exchange in VANETs. They have also used a set of requirements as a guide-line for their studies. However, security requirements and compliance are discussed as a qualitative attribute categorized as system confidentiality, integrity, and availability. The discussion of quantified security attributes has focused on the concern of users' privacy and anonymity which occur in cases of data uncertainty and through k-anonymity evaluations.

The development of a quantified security analysis model for VANETs is becoming an important area of study. With many proposed solutions to secure different aspects of the network, a security analysis model will help macro-evaluation and determine the optimal security measures that a solution can provide. The secure neighborhood aware-

ness framework presented in this thesis is constructed from different components. Each component is evaluated individually and covers different aspect of security measure to protect location information. The next phase in such integrated solution is to be able to evaluate the security aspect in a quantified analytical approach. In this chapter, we present a security evaluation model that quantifies security attributes for exchanged location information processes.

6.1.1 Motivation

Researchers have discussed securing messages in VANETs with different methods [45, 46, 64, 74, 84, 123]. Some studies focused on securing the communication channel among network members using digital signatures and key management [64, 74]. Alternately, other studies presented solutions to secure network services such as secure message routing [45], secure localization [46], secure trust management [123], and the improving of network performance [84].

In the presented solutions, security is mainly discussed and evaluated as a qualitative attribute. The security issue being discussed, and its counter measures, are described based on common sense and similar approaches addressed in context of previously developed wireless technologies. To evaluate a proposed solution, studies support their discussions with a thorough evaluation of related and quantified metrics such as error rate, delivery rate, and scalability. Such an approach is acceptable when micro-evaluating individual protocols.

Security is a broad topic with many aspects to be considered and different opinions. Researchers within the network security community have different approaches for evaluating a security attribute[23, 54]. With the ongoing research in VANETs, more solutions and protocols will be presented. When integrating different solutions to provide a complete service, it will be difficult to evaluate the overall security attributes. An evaluation model with an analytical approach and quantified security attributes will help provide a tool to determine the optimal security measure, the system components can provide.

6.1.2 Objective and Contribution

The neighborhood awareness service is structured from multiple components that are integrated to provide a secure source for location information. It is important to secure position data through out all the processes. Our objective is to developed a security evaluation model to evaluate and quantify the overall security attributes (confidentiality,

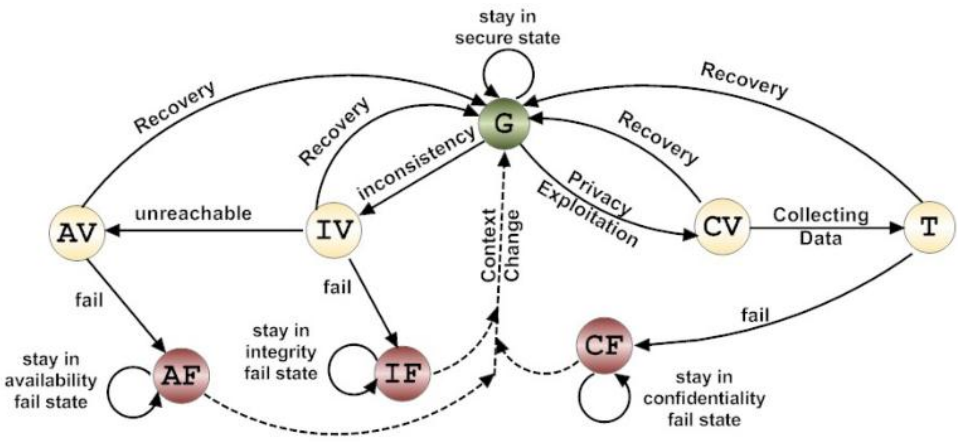


Figure 6.1: A state-space description for a secure location-information exchange.

integrity, and availability) for location-information exchange in VANETs. The model is solved using the semi-Markov process (SMP) and presents the security attributes for the exchanged location information as a quantified value. Moreover, to determine the system's security-resilience, the mean-time-to-security-failure (MTTSF) is defined for the proposed model.

6.2 Location-Sharing Security Evaluation Model

the objective of the neighborhood awareness service is to provide a secure location information of surrounding vehicles. The position and mobility data are handled by several components and processes that protect the information from being exploited. They provide a secure service for a vehicle which also changes their state to accommodate the dynamic of the network.

In this section, we present an evaluation model that describes the behavior of a vehicle with its neighbors. In this model, we focus our interest on the location information exchanged among neighboring nodes within the range of communication. We will use the state-space model approach inspired by the work in [54] to develop the system model for the localization service in VANETs.

6.2.1 State Transit Model

Location information is transmitted by vehicles through periodic beacon messages. A vehicle is concerned with the privacy of its outgoing messages, and with the integrity and

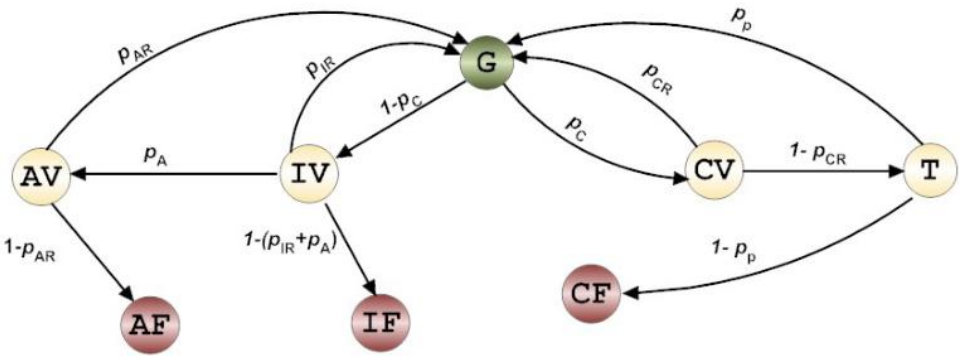


Figure 6.2: The embedded discrete-time-Markov-chain (DTMC) probabilities for a secure location-information exchange model.

correctness of the incoming messages. Figure 6.1 illustrates the state-transition space for the relation between a vehicle and its neighbors location information. The model states (S) and their transitions (τ) are described as follows:

- **Good state (G):** presents the desirably secure state. In this case, it is the state in which the vehicle's beacon information is accurate and the identities are secure. The received beacon messages are processed to present neighbors in the current status as best as possible. Proposed security protocols for VANETs should lead the system towards this state.

- **Confidentiality vulnerability (CV):** the state in which the privacy of the user is exploited, for example, the message signature's anonymity was exploited. In this state, the system is exposed for attackers to track vehicles and to link messages to a single sender. The system may recover from the status of CV state and upgrade to the G state by security measures such as key management [77] and key revocation[52].

- **Tracking attack (T):** in this state, the attacker conducts a data-collection process after discovering the exploited and tracked messages in an effort to identify and to link messages to a single vehicle. The recovery of such attacks provides the system with a countermeasure to make collected data ambiguous for the attackers [77], while remaining useful for the localization service.

- **Confidentiality failure (CF):** if the system was not able to recover from the CV state, for example, the information certainty is at a high level and the attacker was

able to extract targeted data. At this stage, the confidentiality of the system has been compromised and the model will mark the *confidentiality* security attribute as having failed.

- **Integrity vulnerability (IV):** the system transitions to this state when the neighborhood awareness service detects an inconsistency in data. Examples of this are if the beacon rate of a neighboring node was found to not be consistent or if false location information was received. The system may recover from such a vulnerability through message integrity and security measures[74], error detection and correction[9], location verification protocols[46], and Sybil-attack detection[22]. If the countermeasures and integrity-check protocols were unable to recover from this state, the system will attempt to connect to the neighboring node for verification. If the verification challenge fails, the model will transition to the IF state. But if the vehicle is unable to establish a connection with the subject neighbor, the system might have a network performance issue, in which case the system state will transition to the AV state.

- **Integrity failure (IF):** if the system was not able to recover from the IV state and the inconsistency verification was unsuccessful, the model will mark the integrity security attribute as a failure.

- **Availability vulnerability (AV):** if a vehicle cannot establish a communication link with a neighboring node, the network might be suffering from a lack of resource availability. In high density areas, such as an urban city environment, high consumption of network resources will prevent proper communication between neighboring nodes and the exchange of position updates. Quality of service (QoS) provisioning, service scalability, and adaptive beaconing can be part of the system-recovery process for this state. If the system was able to recover from such a state, the model will transit to state G. If not, the system will transit to the AF state.

- **Availability failure (AF):** if the system was not able to recover from the AV state, the system will not be able to secure resources for its application. An example of this is the recovery from a denial-of-service attack (DoS). In this case, the model will mark the availability security-attribute as a failure.

Because of the dynamic changes in VANETs, the surrounding context will change. This may result in changing states CF, IF, and AF to a G state. The clearing out of vehicles

from a congested area, an act allowing them to gain access to proper resources, is an example of a possible changing state.

6.2.2 Semi-Markov Process Analysis

The semi-Markov process (SMP) is a generalized Markov chain that includes time as a state specification. The transition to the next state depends on the current state and on the time spent (sojourn time) on the current state [103]. We will solve the proposed DTMC for the exchanged location information in VANETs using the SMP.

The stochastic process of the model is presented by $\{X(t) : t \geq 0\}$; and, the state space is donated by $X_s = \{G, CV, IV, AV, T, CF, IF, AV\}$. To analyze the SMP, we need to define the state's mean sojourn time (τ_i) where $i \in X_s$. The mean sojourn time refers to the time a state takes in comparison to the related protocol and the effort it requires to decide upon and recover from the security risk, in addition to its independence of the actual SMP state. The state probability (π) donates steady-state probability. The transition probability between different states is p_{ij} where $i, j \in X_s$.

6.2.3 System's Security Attributes

To quantify the security attributes, we focus our interest on the system's steady-state confidentiality (C), integrity (I), and availability (A). The system confidentiality is the the system's effort to protect the privacy of location information and preventing security exploits on the user's identification, travel activities, and traveling profile. System confidentiality is considered to be exploited and compromised in states CV, T, and CF. Thus, the system confidentiality is given by:

$$C = 1 - (\pi_{CV} + \pi_T + \pi_{CF}) \tag{6.1}$$

The system integrity is its ability to detect and recover from location data inconsistency and errors. The integrity of the system is at risk in states IV and IF. Therefore, the system integrity is denoted by:

$$I = 1 - (\pi_{IV} + \pi_{IF}) \tag{6.2}$$

The system availability is its resilience to resource limitation and its scalability which affect the proper exchange of location data among neighboring nodes. The location service availability is vulnerable in state AV and AF. The system availability is given

$$P = \begin{bmatrix} 0 & p_C & 0 & 0 & 1-p_{CR} & 0 & 0 & 0 \\ p_{CR} & 0 & 1-p_{CR} & 0 & 0 & 0 & 0 & 0 \\ p_p & 0 & 0 & 1-p_P & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_{IR} & 0 & 0 & 0 & 0 & 1-(p_{IR}+p_a) & p_a & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_{AR} & 0 & 0 & 0 & 0 & 0 & 0 & 1-p_{AR} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{6.7}$$

by:

$$A = 1 - (\pi_{AV} + \pi_{AF}) \tag{6.3}$$

To analyze the SMP corresponding to the state-transition model, we need to compute the steady-state probability (π) of each state of the model. The probability is described by the embedded discrete-time Markov chain (DTMC) steady state probability (k) and the state mean sojourn time (τ) such that:

$$\pi_i = \frac{k_i \tau_i}{\sum_j k_j \tau_j} \ , \ where \ i, j \ \in \ X_s \tag{6.4}$$

and:

$$\sum_i \ k_i \ = \ 1, \ i \in \ X_i \tag{6.5}$$

The DTMC steady-state probability (Figure 6.2) is computed as:

$$\overline{k} \ = \ \overline{k} \ \cdot \ P \tag{6.6}$$

where $\overline{k} \ = \ [k_G, k_{CV}, k_T, k_{CF}, k_{IV}, k_{IF}, k_{AV}, k_{AF}]$ and P is the embedded DTMC probability matrix for the model (Equation 6.7). Solving equations 6.6 and 6.5 will result in

the following:

$$k_G = \frac{1}{3-p_C p_{CR}} \tag{6.8}$$

$$k_{CV} = \frac{p_C}{3-p_C p_{CR}} \tag{6.9}$$

$$k_T = \frac{1-p_{CR}}{3-p_C p_{CR}} \tag{6.10}$$

$$k_{CF} = \frac{(1-p_P)(1-p_{CR})}{3-p_C p_{CR}} \tag{6.11}$$

$$k_{IV} = \frac{1-p_C}{3-p_C p_{CR}} \tag{6.12}$$

$$k_{IF} = \frac{1-p_{IR}-p_a}{3-p_C p_{CR}} \tag{6.13}$$

$$k_{AV} = \frac{p_a(1-p_C)}{3-p_C p_{CR}} \tag{6.14}$$

$$k_{AF} = \frac{p_a(1-p_C)(1-p_{AR})}{3-p_C p_{CR}} \tag{6.15}$$

Solving equation 6.16 with k values will compute the steady-state values (π) for the SMP model such that:

$$\begin{aligned} \pi_G &= h_G[h_G + p_c h_{CV} + (1-p_{CR})(h_T + h_{CF}(1-p_p)) \\ &\quad +(1-p_C)(h_{IV} + p_a(h_{AV} + (1-p_{AR})h_{AF})) \\ &\quad +h_{IF}(1-p_{IR}-p_a)]^{-1} \end{aligned} \tag{6.16}$$

$$\pi_{CV} = \frac{p_C h_{CV}}{\pi_G} \tag{6.17}$$

$$\pi_T = \frac{(1-p_{CR})h_T}{\pi_G} \tag{6.18}$$

$$\pi_{CF} = \frac{(1-p_P)(1-p_{CR})h_{CF}}{\pi_G} \tag{6.19}$$

$$\pi_{IV} = \frac{(1-p_C)h_{IV}}{\pi_G} \tag{6.20}$$

$$\pi_{IF} = \frac{(1-p_{IR}-p_a)h_{IF}}{\pi_G} \tag{6.21}$$

$$\pi_{AV} = \frac{p_a(1-p_C)h_{AV}}{\pi_G} \tag{6.22}$$

$$\pi_{AF} = \frac{p_a(1-p_C)(1-p_{AR})h_{AF}}{\pi_G} \tag{6.23}$$

Substituting equations 6.1, 6.2, and 6.3 with the values of (π_i) will give the values of C, I, and A, respectively.

6.2.4 Mean Time To Security Failure

The mean time to security failure (MTTSF) is the mean time for the system to reach one of its failure states. To compute the MTTSF for the proposed model, we analyzed the SMP with its absorbing states. With respect to the proposed SMP model for location exchange in VANETs, the absorbing states are denoted by $X_a = \{CF, IF, AF\}$, and the transition states are $X_t = \{G, CV, T, IV, AV\}$. The probability matrix has a general form[103]:

$$P = \begin{bmatrix} Q & | & B \\ - - - & | & - - - \\ 0 & | & 1 \end{bmatrix} \tag{6.24}$$

where Q is the probability matrix between the transit states (X_t), and B is the probability matrix between the transit state (X_t) and the absorbing states (X_a). The MTTSF of the model can then be given as:

$$MTTSF = \sum_{i \in X_t} K_i \tau_i \tag{6.25}$$

where K_i denotes the average number of times state i was visited before the DTMC process reaches one of the absorbing states, and τ_i is the mean sojourn time of state i. K_i can be computed using the formula:

$$K_i = q_i + \sum_{i \in X_t} K_i \tau_i \tag{6.26}$$

where q_i is the probability that the DTMC starts in state i. In this model, we assume that the initial state is always state G.

6.3 Solution Evaluation

To evaluate the proposed model, we want to examine the behavior of the system under different conditions. The literature did not provide us with experimental measurement and estimations of the probability of occurrence of security risk and the probability and average time the protocols recovering from such events. For our study, we will provide estimated values for the parameters. The assumptions are based on educated guesses used to illustrate the behavior of the model. In our future work, we will include experimental values.

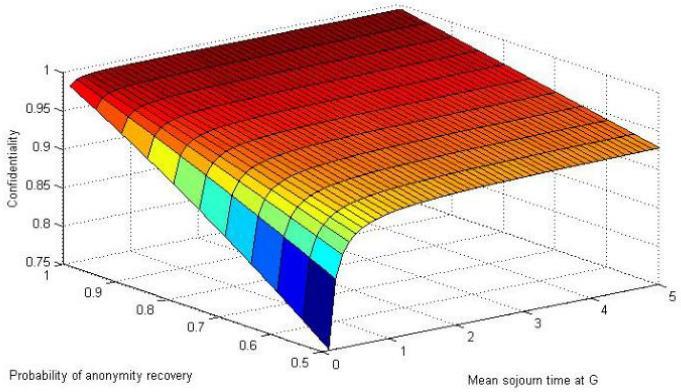


Figure 6.3: The security-confidentiality attribute with respect to mean sojourn time of state G and the probability of anonymity recovery.

The evaluation is based on assumptions for transition probabilities with given values of $P_C = 0.2,\ P_{CR} = 0.8,\ P_{IR} = 0.6,\ P_A = 0.2,\ P_{AR} = 0.6,\ and\ P_P = \ 0.4$. The mean sojourn time for the states is given the values $h_{cv} = 0.25,\ h_t = 0.25,\ h_{iv} = 0.25,\ h_{av} = 0.25,\ and\ h_t = 0.25$ of a time unit.

Figure 6.3 shows the relation of the confidentiality attribute C to the anonymity-recovery probability (P_{CR}) and the mean sojourn time (h_G). To improve the system confidentiality and to preserve user privacy, system development should increase the values of P_{CR} and P_p, and reduce the value of P_C. This can be achieved by improving user anonymity, such as ID protection, key management, and increased data uncertainty.

Figure 6.4 shows the relation of the integrity attribute (I) to the integrity-recovery probability (P_{IR}) and the mean sojourn time (h_G). The improvement of data-verification protocols, such as location verification protocols, error correction, and Sybil-node detection, will secure the integrity of shared location data by increasing the value of P_{IR}.

Figure 6.5 shows the relation of the availability attribute A with the availability recovery probability (P_{AR}). Improving the QoS and protocols' scalability will increase P_{AR}.

In Figure 6.6, the relation of the MTTSF to the probability of anonymity-recovery (P_{cr}) and mean sojourn time (h_G) is illustrated. This shows that the act of improving confidentiality alone will not be enough to score a high MTTSF. Improving the system-integrity and system-availability will increase the steady-state probability of state G.

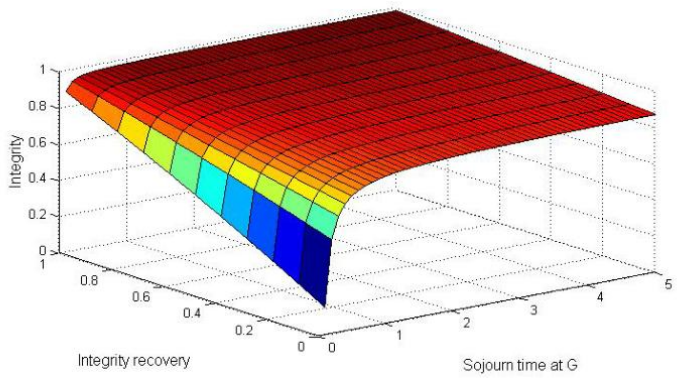


Figure 6.4: The security-integrity attribute with respect to mean sojourn time of state G and the probability of integrity recovery.

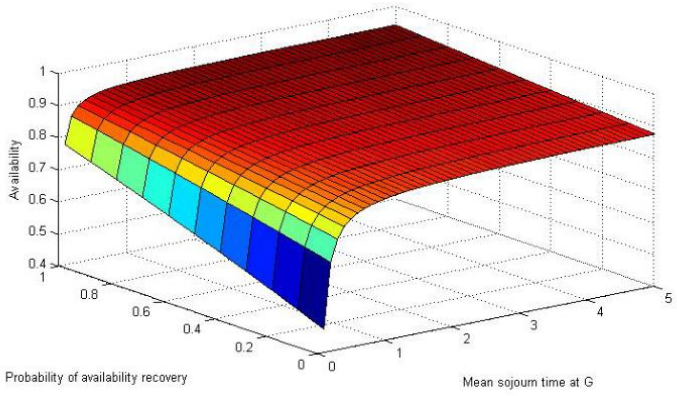


Figure 6.5: The security-availability attribute with respect to mean sojourn time of state G and the probability of availability recovery.

6.4 Summary

Sharing location information among neighboring vehicles is important for the providing of location-based applications in VANETs. Researchers [8, 34, 64, 76, 77] have discussed security vulnerabilities and risks that can affect the integrity and availability of delivered applications. Moreover, studies have discussed privacy issues and proposed solutions to protect users' privacy and secure exchanged location-information [12, 24, 34, 41, 51, 81]. Many of the studies have discussed security issues and have addressed the attaining of resolutions through qualitative values and common sense, while also discussing the presence of similar issues in previously developed technologies. Moreover, proposed solutions are compared with similar solutions to conduct a fair eval-

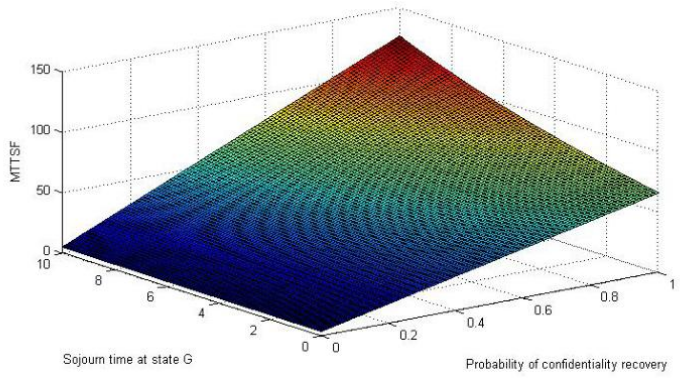


Figure 6.6: The mean time to security failure (MTTSF) attribute with respect to mean sojourn time of state G and the probability of confidentiality recovery.

uation. With so many solutions and approaches to resolving identified security threats, it is necessary to develop an analytical model to study the behavior of the network and quantify security attributes in VANETs.

In this chapter, we developed an analytical model to evaluate the overall security measures for the location information service in VANETs. The model is developed by solving a semi-Markov process problem, and resulted in quantifying the *confidentiality, integrity*, and *availability* of exchanged location information in the system. Moreover, the *mean-time-to-security-failure* (MTTSF) was also defined by computing the mean time for the system to reach a (failure) state of absorption for the SMP model. The proposed model will help evaluate the security measures provided by system components, and to help determine the optimal security measures the system can provide.

Chapter 7

Conclusion

Sharing position information among neighboring vehicles will improve various location-based applications. It is important for vehicles to have current and accurate information about their surroundings. However, such information can be affected by various factors due to the nature and characteristic of the VANET and security attacks. The dynamic nature of the network introduces a challenge as moving obstacles interferes the wireless communication channel and prevent proper exchange of information among vehicles. On the other hand, adversaries will use the network's features and limitations to serve their interest.

In the information security domain, the discussion on the security aspects of a system has different point-of-views and different opinions. In this thesis, we focus on the security aspects for VANETs and on its location-based applications. We discuss the risks that may impact their performance and functionality. Our objective for this thesis is to identify security vulnerabilities and challenges that may impact the exchanged location information and develop a solution and security countermeasures for the identified threats.

The cooperative multi-hop location verification protocol (CMLVP) is an efficient cooperative approach to verify an announced position when direct communication between the questioned node and verifier is not possible. Besides verifying a node location in a multi-hop cooperative approach, several security measures were taken to secure message integrity. The simulation results showed that the protocol increased the vehicle's average neighborhood awareness rate under the effect of obstacles. Moreover, the exchanged messages helped update neighbors' records and increase the awareness of other nodes that are cooperatively forwarding requests and replies. To evaluate the proposed pro-

tocol, we developed the obstacle model that was used to simulate the non-line-of-sight (NLOS) condition which resolved the limitation of current network simulators, such as NS-2, that do not support moving obstacles and their affect on direct communication between vehicles.

The frequent message broadcast of location information will result in high bandwidth consumption, especially in dense areas. In this thesis, we developed an adaptive group beaconing (AGB) method that utilizes the proposed location information service. Based on the density of the neighborhood and mobility information, the vehicles will change beacon message frequency and context to reduce the number of outgoing messages. Through the adaptive group beaconing solution, authorities and network service providers can provide critical applications and users a level of QoS by allowing the control periodic message rate and content to reduce the number of outgoing messages. In dense areas, emergency vehicles can request vehicles to change to adaptive mode and reduce network resource utilization to guarantee enough resources for potential safety and emergency applications.

To protect the privacy of vehicles, we discussed the fact that the use of a vehicle identifier in beacon messages should be eliminated. The assumption that all member nodes of the network are trustworthy and that it is safe to exchanging vehicle identification among the network members is no longer acceptable due to privacy threats. To resolve this issue, we developed a location information group mapping using a grid map and indicating cell occupancy. The location information for a group are anonymized and cluster head will broadcast the the information as group beacon. The location information of an individual vehicle can not be extracted from group information, therefore protecting users' privacy and preventing attackers from linking gathered position data to a target vehicle.

We developed a trust evaluation model that take into consideration NLOS conditions and location verification results. The trust model can help verify the location of a node to increase vehicle awareness. The model provides a source of information for other applications and services to determine the reliability and connectivity of neighboring nodes based on their location, mobility, and line-of-sight stability. Simulations showed improvement in the delivery success rate by helping the service to change the decision regarding the "next hop" node to forward a message to its destination.

A consolidation of the developed protocols into a single service model was designed to enhance security measures. Future developed applications can obtain location information from the secure neighborhood awareness services. By securing the inter-process

of the service the framework will provide a secure source of position information for location-based applications and services.

We developed an analytical model to evaluate the overall security measures for the location information service in a VANET. The model was developed by solving a semi-Markov process problem and resulted in quantifying the confidentiality, integrity, and availability security attributes of the exchanged location information process in the system. Moreover, the mean-time-to-security-failure (MTTSF) was also defined by computing the mean time for the system to reach an absorbing (failure) state for the SMP model. The proposed model will help evaluate the security measures provided by system component and find the optimal security measures that the system can provide.

The work in this thesis was done after conducting a thorough literature review of different security aspects that affects location information in VANETs. This was done to make sure that the contributions in this thesis are novel and opens directions for future research and development. Based on the simulation results and discussions in this thesis, we believe that we have extended the knowledge in the security domain of VANETs and its location-based applications.

7.1 Summary of Contributions

The focus of this thesis was to identify security vulnerabilities that will impact vehicles' location information and develop solutions that will protect the data integrity and users' privacy. The work presented in this thesis makes the following contributions:

1. The development of a cooperative multi-hop location verification protocol (CM-LVP); an efficient protocol to verify a nodes' location under NLOS conditions.

2. The development of an adaptive group beaconing (AGB) technique with quality of service provisioning; an efficient mechanism to improve the system's availability for location sharing.

3. The development of a privacy preserving group mapping; to protect the privacy of vehicle's location and prevent profile building.

4. The development of a secure trust evaluation model; to evaluate the trustworthiness of neighboring nodes based on their position and line-of-sight conditions.

5. The development of a neighborhood location awareness service framework; integrating location processing sub-services to provide a secure and reliable source of location data for location-based applications and services.

6. The development of a security evaluation model for location sharing; to help evaluate the security attributes for an integrated solution of location processing sub-services and protocols.

7.2 Future Work

Several future research direction can be realized by extending the work in this thesis, including

1. Securing the exchanged location information among vehicles is an important task in VANETs. As we have discussed in the thesis, securing its availability and reliability is essential to improving the availability and reliability of location-based applications. Due to the dynamic nature of the network, obstacle's positions and NLOS conditions are also changing. The investigation of the behavior of the system with moving obstacles, such as predicting a NLOS condition, can improve the system integrity and neighborhood awareness service.

2. The proposed obstacle model can be improved by conducting field measurement of moving obstacles' affect on messages and location information availability and presenting the measured data in mathematical models for different scenarios and driving conditions. With such data in hand, it will be possible to evaluate the proposed solutions for location verification in VANETs through proposed external hardware and measurements such as radar and ultrawideband signal measurements.

3. Evaluating the performance of the neighborhood awareness service and protocols on a real test-bed.

4. Different dynamic group construction and management can be studied and evaluated to improve the AGB protocol and increase the average awareness rate based on QoS requirements.

5. Further evaluation should be conducted of the security analysis model. Parameters for different components of the location awareness services should be measured to provide the model with the proper values to compute the system security attributes.

A full evaluation with different integrated components, and true values, should be investigated.

6. Studies should continue to identify potential security threats that will compromise the confidentiality, integrity, and availability of exchange location information. With the multiple useful and important applications that will be delivered through VANETs to improve drivers' safety and awareness on roads, attackers will be eager to use technologies' features and limitations in their favor.

Bibliography

[1] The UDel Models - MANET Mobility and Path Loss in an Urban/Suburban Environment. Technical Report, 2004, Available: http://www.udelmodels.eecis.udel.edu.

[2] B. Ali, N. Pissinou, and K. Makki. Identification and Validation of Spatio-Temporal Associations in Wireless Sensor Networks. In *3rd International Conference in Sensor Technologies and Applications*, pages 496–501, 2009.

[3] P. Bahl and V.N. Padmanabhan. Radar: An in-building rf-based user location and tracking system. In *Proceedings of the IEEE Infocom 2000, vol. 2, IEEE, Tel Aviv, Israel*, page 775784, 2000.

[4] H. Baumann and W. Sandmann. Markovian Modeling and Security Measure Analysis for Networks Under Flooding DoS Attacks. In *20th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, pages 298–302, 2012.

[5] A. Benslimane. Localization in Vehicular Ad-Hoc networks. In *2005 Systems Communications, ICW '05*, 2005.

[6] A. Beresford and F.Stajano. Location Privacy in Pervasive Computing. *IEEE Pervasive Computing*, 2(1):46–55, 2003.

[7] M.S. Bouassida and M. Shawky. A Cooperative and Fully-Distributed Congestion Control Approach within VANETs. In *9th International Conference on Intelligent Transport Systems Telecommunications,(ITST)*, pages 526–531, 2009.

[8] A. Boukerche, H. Oliveira, E. Nakamura, and A. Loureiro. Secure Localization Algorithms for Wireless Sensor Networks. *IEEE wireless communications*, 46(4):96–101, 2008.

[9] A. Boukerche, H. Oliveira, E. Nakamura, and A. Loureiro. Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems. *Computer Communications*, 31(12):2838–2849, 2008.

[10] G. Challita, S. Mousset, F. Nashashibi, and A. Bensrhair. Particle Filters For An Accurate Localization of Communicant Vehicles. In *Fifth International Conference on Autonomic and Autonomous Systems, ICAS'09*, pages 195–199, April 2009.

[11] R. Chapuis, J. Laneurit, R. Aufrere, F. Chausse, and T. Chateau. Accurate Vision Based Road tracker. In *IEEE Intelligent Vehicle Symposium*, volume 2, page 666671, 2002.

[12] B. Chaurasia, S. Verma, and S. Bhasker. Message broadcast in VANETs using Group Signature. In *4th International Conference on Wireless Communication and Sensor Networks, WCSN*, pages 131–136, 2008.

[13] M. Chen, D. Haehnel, J. Hightower, T. Shon, A. LaMarca, I. Smith, D. Chmelev, J. Hughes, and F. Potter. Practical Metropolitan-Scale Positioning for GSM Phones. In *Proceeding of 8th Ubicomp, Orange County, California*, pages 225–242, 2006.

[14] Y.-C. Cheng, Y. Chawathe, A. LaMarca, and J. Krumm. Accuracy characterization for metropolitan-scale wi-fi localization. In *Proceedings of the 3rd International Conference on Mobile systems, Applications, and Services, Mobi-Sys05, ACM Press, New York, NY, USA*, page 233245, 2005.

[15] Q. Ding, M. Jiang, X. Li, and X. Zhou. Reputation-based Trust Model in Vehicular Ad Hoc Networks. In *International Conference on Wireless Communications and Signal Processing, WCSP*, pages 1–6, 2010.

[16] F. Dotzer, L. Fischer, and P. Magiera. VARS: A Vehicle Ad-Hoc Network Reputation System. In *6th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, WoWMoM*, pages 454–456, 2005.

[17] W. Du, L. Fang, and P. Ning. LAD: Localization Anomaly Detection for Wireless Sensor Networks. In *19th IEEE International Parallel and Distributed Processing Symposium*, page 41a, 2005.

[18] G. Durgin, T.S. Rappaport, and X. Hao. Measurements and models for radio path loss and penetration loss in and around homes and trees at 5.85 GHz. *IEEE Transactions on Communications*, 46(11):1484–1496, 1998.

[19] H. Fang, C. Wang, M. Yang, and R. Yang. Ground-Texture-Based Localization for Intelligent Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 10(3):463–468, September 2009.

[20] M. Ferreira, H. Conceicao, R. Fernandes, and R. Reis. Locating cars through a vision enabled VANET. In *IEEE Intelligent Vehicles Symposium*, pages 99–104, 2009.

[21] E. Giordano, R. Frank, G. Pau, and M. Gerla. CORNER: a realistic urban propagation model for VANET. In *7th International Conference on Wireless On-Demand Network Systems and Services, WONS'10*, pages 57–60, 2010.

[22] P. Golle, D. Greene, and J. Staddon. Detecting and Correcting Malicious Data in VANETs. In *Proceeding of the 1st ACM International Workshop on Vehicular ad hoc network, VANET '04*, October 2004.

[23] C. Griffin, B. Madan, and K. Trivedi. State Space Approach to Security Quantification. In *29th Annual Int. Computer Software and Applications Conference (COMPSAC)*, pages 83–88, 2005.

[24] J. Guo, J. Baugh, and S. Wang. A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework. In *2007 Mobile Networking for Vehicular Environments*, pages 103–108, 2007.

[25] J. Harri, F. Filali, and C. Bonnet. Mobiliyt Models for Vehicular Ad Hoc Networks: A Surevey and Taxonomy. *IEEE Communications Surveys and Tutorials*, 11(4):19–41, 2009.

[26] B. Hoh and M. Gruteser. Protecting Location Privacy Through Path Confusion. In *IEEE First Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks, SecureComm*, pages 194–205, 2005.

[27] J.P. Hubaux, S. Čapkun, and J. Luo. The security and privacy of smart vehicles. *IEEE Security & Privacy*, 2(3):49–55, May 2004.

[28] IEEE 802.11p. IEEE Standard for Information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments, IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007) . 2010.

[29] IEEE1609.2. *IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages*. IEEE, 2013.

[30] A.K. Jain and V. Tokekar. Classification of Denial of Service Attacks in Mobile Ad Hoc Networks. In *International Conference on Computational Intelligence and Communication Networks (CICN)*, pages 256–261, October 2011.

[31] Amit Jardosh, Elizabeth M. Belding-Royer, Kevin C. Almeroth, and Subhash Suri. Real world Environment Models for Mobile Ad hoc Networks. *IEEE Journal on Special Areas in Communications - Special Issue on Wireless Ad hoc Networks*, 2005.

[32] R.H. Jhaveri, S.J. Patel, and D.C. Jinwala. DoS Attacks in Mobile Ad Hoc Networks: A Survey . In *Second International Conference on Advanced Computing & Communication Technologies (ACCT)*, pages 535–541, January 2012.

[33] D. Jiang and L. Delgrossi. IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environment. In *IEEE Vehicular Technology Cenference, VTC 2008*, pages 2036–2040, 2008.

[34] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedershiem, T. Thong, G. Calandriello, A. Held, A. Kung, and J. Hubaux. Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges. *IEEE Communication Magazine*, 46(11):110–118, 2008.

[35] M. Kennedy. *Global Positioning System and GIS : An Introduction*. 2nd Ed., CRC Press, New York, NY, 2002.

[36] B. Kim, K. Choi, J. Lee, and D. Lee. Anonymous and Traceable Communication Using Tamper-Proof Device for Vehicular Ad Hoc Networks. In *International Conference Information Technology*, pages 681–686, November 2007.

[37] Kazuki Konishi, Kumiko Maeda, Kazuki Sato, Akiko Yamasaki, Hirozumi Yamaguchi, Keiichi Yasumoto, and Teruo Higashino. MobiREAL Simulator – Evaluating MANET Applications in Real Environments. In *13th Annual Meeting of the IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems(MASCOTS2005)*, 2005.

[38] Daniel Krajzewicz, Georg Hertkorn, Christian Rossel, and Peter Wagner. SUMO (Simulation of Urban MObility) An open-source traffic simulation. *Proceedings of the 4th Middle East Symposium on Simulation and Modelling (MESM2002), United Arab Emirates*, September 2002.

[39] R. Kroh, A. Kung, and F. Kargl. VANETS Security Requirements Final Version. In *Ver. 2.0, SeVeCom (Secure Vehicular Communication) Project, URL: http://www.sevecom.org/.*

[40] R. Lam and P. Kumar. Dynamic Channel Reservation to Enhance Channel Access by Exploiting Structure of Vehicular Networks. In *IEEE 71st Vehicular Technology Conference (VTC 2010-Spring)*, pages 1–5, May 2010.

[41] C. Laurendeau and M. Barbeau. Secure Anonymous Broadcasting in Vehicular Networks. In *32nd IEEE Conference on Local Computer Netwroks*, pages 661–668, 2007.

[42] L. Lazos, R. Poovendran, and S. Čapkun. ROPE: robust position estimation in wireless sensor networks. In *4th International Symposium on Information Processing in Sensor Networks*, pages 324–331, 2005.

[43] L. Le, R. Baldessari, P. Salvador, A. Festag, and W. Zhang. Performance Evaluation of Beacon Congestion Control Algorithms for VANETs. In *IEEE Global Telecommunications Conference, (GLOBECOM)*, pages 1–6, December 2011.

[44] J.-Y. Lee and R. Scholtz. Ranging in a dense multipath environment using an uwb radio link. *Selected Areas in Communications, IEEE Journal*, 20(9):16771683, 2002.

[45] T. Leinmuller, E. Schoch, and F. Kargl. Improved Security In Geographic Ad Hoc Routing Through Autonomous Position Verification. In *Proceedings of the 3rd international workshop on Vehicular ad hoc networks, VANET'06*, September 2006.

[46] T. Leinmuller, E. Schoch, and F. Kargl. Position Verification Approaches For Vehicular Ad Hoc Networks. *IEEE Wireless Communications*, 13(5):16–21, 2006.

[47] T. Leinmuller, E. Schoch, F. Kargl, and C. Maihofer. Influence of Falseified Position Data on Geographic Ad-Hoc Routing. In *2nd European Workshop on Security and Privacy in Ad hoc and Sensor Networks, Visegrad, Hungary*, July 2005.

[48] B. Li, J. Wang, T. Dong, and Y. Liu. An New Approach to Access VANETs. In *ISECS International Colloquium on Computing, Communication, Control, and Management*, pages 482–485, 2009.

[49] W. Li and Z. Guo. Hidden Markov Model Based Real Time Network Security Quantification Method. In *Int. Conf. on Networks Security, Wireless Communications and Trusted Computing, NSWCTC*, 2009.

[50] K. Lidström and T. Larsson. A spatial QoS requirements specification for V2V applications. In *IEEE Intelligent Vehicles Symposium (IV)*, pages 548–553, June 2010.

[51] X. Lin, R. Lu, C. Zhang, H. Zhu, P-H Ho, and X. Shen. Security in Vehicular Ad Hoc Networks. *IEEE Communications Magazine*, 46(4):88–95, 2008.

[52] X. Lin, X. Sun, P. Ho, and X. Shen. GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications. *IEEE Transaction on Vehicular Technology*, 56(6):3442–3456, November 2007.

[53] Z. Ma, F. Kargl, and M. Weber. A Location Privacy Metric for V2X Communication Systems. In *IEEE Sarnoff Symposium*, pages 1–6, 2009.

[54] B. Madan, K. Goševa-Popstojanova, K. Vaidyanathan, and K. Trivedi. A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant Systems. *Performance Evaluation*, 56:167–186, 2004.

[55] S.S. Manvi, M.S. Kakkasageri, and D.G. Adiga. Message Authentication in Vehicular Ad Hoc Networks: ECDSA Based Approach. In *International Conference on Future Computer and Communication, ICFCC*, pages 16–20, 2009.

[56] F. Martinez, C-K Toh, J-C Cano, C. Calafate, and P. Manzoni. Realistic Radio Propagation Models (RPMs) for VANET Simulations. In *IEEE Wireless Communication and Networking Conference, WCNC'09*, 2009.

[57] J.-F. Martinez, A.-B. Garc, I. Corredor, L. Lpez, V. Hernndez, and A. Dasilva. QoS in wireless sensor networks: survey and approach. In *Euro American conference on Telematics and information systems, EATIS*, May 2007.

[58] S. Marwaha, J. Indulska, and M. Portmann. Challenges and Recent Advances in QoS Provisioning, Signaling, Routing and MAC protocols for MANETs. In *Australasian Telecommunication Networks and Applications Conference, ATNAC*, pages 97–102, December 2008.

[59] J. Mittag, F. Thomas, J. Harri, and H. Hartenstein. A Comparison of Single- and Multi-hop Beaconing in VANETs. In *The Sixth ACM International Workshop on Vehicular Inter-Networking, VANET'09*, September 2009.

[60] B.K. Mohandas, O.W.W. Yang, and R. Liscano. Improving Data QoS in Vehicular Communication. In *First International Conference on Future Information Networks, ICFIN*, pages 161–166, October 2009.

[61] M. Mokbel, C.-Y. Chow, and W. Arif. The New Casper: Query Processing for Location Services Without Compromising Privacy. In *32nd International Conference on Very Large Data Bases, VLDB*, pages 763–774. ACM, Sep 1998.

[62] B. Mourllion, D. Gruyer, A Lambert, and S Glaser. Kalman filters predictive steps comparison for vehicle localization. In *IEEE/RSJ International Conference on Intelligent Robots and Systems, IROS 2005*, pages 565–571, August 2005.

[63] E. Nakamura, A. Loureiro, and A. Frery. Information fusion for Wireless sensor networks: Methods, models, and classifications. *ACM Computing Surveys*, 39(3), Sep 2007.

[64] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J-P. Hubaux. Secure Vehicular Communication Systems: Design and Architecture. *IEEE Communication Magazine*, 46(11):100–109, November 2008.

[65] R. Parker and S. Valaee. Vehicle Location in Vehicular Networks. In *IEEE 64th Vehicular Technology Conference, VTC 2006-Fall*, pages 1–5, 2006.

[66] R. Parker and S Valaee. Vehicular Node Localization Using Received-Signal-Strength Indicator. *IEEE Transactions on Vehicular Technology*, 56(6):3371–3380, 2007.

[67] M. Piorkowski, M. Raya, A. L. Lugo, P. Papadimitratos, M. Grossglauser, and J. P. Hubaux. TraNS: Realistic Joint Traffic and Network Simulator for VANETs. *ACM SIGMOBILE Mobile Computing and Communications Review*, 12(1), 2008.

[68] K. Plossi, T. Nowey, and C. Mletzko. Towards a Security Archetecture for Vehicular Ad Hoc Networks. In *Proceedings of the 1st International Conference on Availability, reliability and Security, ARES'06*, April 2006.

[69] I. Poole. *Cellular Communications Explained : From Basics to 3G*. 1st Ed., Newnes, Burlington, MA, 2006.

[70] N.B. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location-support system. In *Mobile Computing and Networking, Boston, MA, USA*, page 3243, 2000.

[71] M. Rabadi and S. Mahmud. Privacy Protection among Drivers in Vehicle-to-Vehicle Communication Networks. In *IEEE 4th Consumer Communications and Networking Conference, CCNC'07*, pages 281–286, 2007.

[72] M. Raya, A. Aziz, and J-P. Hubaux. Efficient Secure Aggregation in VANETs. In *Proceedings of the 3rd international workshop on Vehicular Ad Hoc Networks, VANET'06*, September 2006.

[73] M. Raya and J-P. Hubaux. The Security of Vehicular Ad Hoc Networks. In *Proceeding of 3rd ACM workshop on security of ad hoc and sensor network, ACM*, November 2005.

[74] M. Raya and J-P. Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security, IOS Press*, 15(1):39–68, 2007.

[75] Z. Ren, W. Li, and Q. Yang. Location Verification For VANETs Routing. In *IEEE International Conference On Wireless and Mobile Computing, WiMob'09*, pages 141 – 146, October 2009.

[76] K. Sampigethaya, L. Mingyan, L. Huang, and R. Poovendran. AMOEBA: Robust Location Privacy Scheme for VANET. *IEEE Journal on Selected Areas in Communications*, 25(8):1569–1589, October 2007.

[77] Krishna Sampigethaya, Leping Huang, Mingyan Li, Radha Poovendran, Kanta Matsuura, and Kaoru Sezaki. Caravan: Providing Location Privacy for VANET. In *Embedded Security in Cars (ESCAR), Berlin, Germany*, 2005.

[78] R. Sash, A. Wolisz, and J. Rabaey. On the performance of geographical routing in the presence of localization errors. In *IEEE International Conference on Communications, ICC, Vol. 5*, pages 2979–2985, 2005.

[79] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *2nd ACM Workshop on Wireless Security*, San Diego, CA.

[80] Inc SCALABLE Network Technologies. QualNet Developer. http://www.scalable-networks.com.

[81] F. Schaub, M. Zhendong, and F. Kargl. Privacy Requirements in Vehicular Communication Systems. In *International Conference on Computational Science and Engineering, CSE*, volume 3, pages 139–145, 2009.

[82] F. Scheuer, K. Plossl, and H. Federrath. Preventing Profile Generation in Vehicular Networks. In *IEEE International Conference on Wireless and Mobile Computing, WIMOB '08*, pages 520–525, October 2008.

[83] M. Schlingelhof, D. Betaille, P. Bonnifait, and K. Demaseure. Advanced positioning technologies for co-operative systems. *IET Intelligent Transport Systems*, 2(2):81–91, 2008.

[84] R. Schmidt, T. Leinmůller, E. Schoch, F. Kargl, and G. Schăfer. Exploration of Adaptive Beaconing for Efficient Intervehicle Safety Communication. *IEEE Network*, 24(1):14–19, Jan 2010.

[85] R. K. Schmidt, T. Kollmer, T. Leinmller, B. Boddeker, and G. Schafer. Degradation of Transmission Range in VANETs caused by Interference. *PIK - Praxis der Informationsverarbeitung und Kommunikation, Special Issue on Mobile Ad-hoc Networks*, 32(4):224–234, 2009.

[86] C. Schroth, F. Dotzer, T. Kosch, B. Ostermaier, and M. Strassberger. Simulating the traffic effects of vehicle-to-vehicle messaging systems. In *5th International Conference on ITS Telecommunications*, 2005.

[87] R. Schubert, M. Schlingelhof, H. Cramer, and G. Wanielik. Accurate Positioning for Vehicular Safety Applications - the Safespot Approach. In *IEEE 65th Vehicular Technology Conference, VTC2007-Spring*, pages 2506–2510, April 2007.

[88] C. E. Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[89] K. Shin, X. Ju, Z. Chen, and X. Hu. Privacy Protection for Users of Location-Based Services. *IEEE Wireless Communications*, 19(1):30–39, Feb 2012.

[90] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux. Quantifying Location Privacy. In *IEEE Symposium on Security & Privacy*, pages 247–262, 2011.

[91] D. Singelee and B. Preneel. Location verification using secure distance bounding protocols. In *IEEE International Conference in Mobile Adhoc and Sensor Systems*, pages 834–840, 2005.

[92] K. Sjoberg, E. Uhlemann, and E. Strom. How Severe is the Hidden Terminal Problem in VANETs When Using CSMA and STDMA? In *IEEE Vehicular Technology Conference, VTC-Fall*, pages 1–5, 2011.

[93] C. Sommer, O.K. Tonguz, and F. Dressler. Traffic Information Systems: Efficient Message Dissemination via Adaptive Beaconing. *IEEE Communication Magazine*, 49(5):173–179, May 2011.

[94] H-L. Song. Automatic Vehicle Location in Cellular Communications System. *IEEE Transactions on Vehicular Technology*, 43(4):902–908, November 1994.

[95] J-H Song, V.W.S. Wong, and V.C.M. Leung. Secure Location Verification for Vehicular Ad-Hoc Networks. In *IEEE Global Telecommunications Conference, GLOBECOM*, pages 1–5, 2008.

[96] J.-H. Song, V.W.S. Wong, and V.C.M. Leung. Wireless Location Privacy Protection in Vehicular Ad-Hoc Networks. In *IEEE International Conference on Communications,ICC*, pages 1–6, June 2009.

[97] P. Subramaniam, A. Thangavelu, and C. Venugopal. QoS for Highly Dynamic Vehicular Ad Hoc Network Optimality. In *11th International Conference on ITS Telecommunications, ITST*, pages 405–411, 2011.

[98] J. Sun, C. Zhang, and Y. Fang. An ID-Based Framework Achieving Privacy and Non-Repudiation in Vehicular Ad Hoc Networks. In *IEEE Military Communications Conference, MILCOM'07*, pages 1–7, October 2007.

[99] J. Sun, C. Zhang, Y. Zhang, and Y. Fang. An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks. *IEEE Transactions on Parallel and Distributed Systems*, 21(9):1227–1239, 2010.

[100] A. Tajeddine, A. Kayssi, and A. Chehab. A Privacy-Preserving Trust Model for VANETs. In *IEEE 10th International Conference on Computer and Information Technology, CIT*, pages 832–837, 2010.

[101] A. Thangavelu, K. Bhuvaneswan, K. Kumar, K. SenthilKumar, and S.N. Sivanandam. Location Identification and Vehicle Tracking using VANET (VETRAC). In *International Conference on Signal Processing, Communications and Networking, ICSCN'07*, pages 112–116, 2007.

[102] D. Tian, Y. Wang, and K. Ma. Perfromance Evaluation of Beaconing in Dense VANETs. In *IEEE Youth Conf. on information Computing and Telecommunications, YC-ICT*, pages 114–117, 2011.

[103] K. Trivedi. *Probability and Statistics with Reliability, Queuing, and Computer Science Applications*. New York, NY, John Wiley & Sons, second edition, 2002.

[104] K. Trivedi, D. S. Kim, A. Roy, and D. Medhi. Dependability and Security Models. In *7th Int. Workshop on the Design of Reliable Communication Networks*, pages 11–20, 2009.

[105] A. Varshavsky, M.Y. Chen, E. de Lara, J. Froehlich, D. Haehnel, J. Hightower, A. LaMarca, F. Potter, T. Sohn, K. Tang, and I. Smith. Are GSM phones THE solution for localization? In *Procceedings of 7th IEEE, Workshop on Mobile Computing Systems and Applications, WMCSA '06*, pages 20–28, 2006.

[106] S. Čapkun, K. B. Rasmussen, M. Cagalj, and M. Srivastava. Secure Location Verification with Hidden Mobile Base Station. *IEEE Trans. Mobile Computing*, 7(4):470–483, Apr 2008.

[107] S. Vodopivec, J. Bešter, and A. Kos. A Survey on Clustering Algorithms for Vehicular Ad-Hoc Networks. In *35th Int. Conf. on Telecommunications and Signal Processing (TSP)*, pages 52–56, July 2012.

[108] R. Vuyyuru and K. Oguchi. Vehicle-to- vehicle ad hoc communication protocol evaluation using realistic simulation framework. In *4th Annual Conference on Wireless on Demand Network Systems and Services, WONS'07*, pages 100–106, January 2007.

[109] H. Wang, G. Kang, and K. Huang. An Advanced Semi-Markov Process Model for Performance Analysis of Wireless LANs. In *IEEE Vehicular Technology Conference (VTC Fall)*, 2012.

[110] J. Wang, Y. Liu, X. Liu, and J. Zhang. A Trust Propagation Scheme in VANETs. In *IEEE Intelligent Vehicles Symposium*, pages 1067–1701, 2009.

[111] Y. Wei, Z. Yu, and Y. Guan. Location Verification Algorithms for Wireless Sensor Networks. In *27th International Conference in Distributed Computing Systems*, pages 70–77, 2007.

[112] P. Wex, J. Breuer, T. Leinmuller, and L. Delgrossi. Trust Issues for Vehicular Ad Hoc Networks. In *IEEE Vehicular Technology Conference*, pages 2800–2804, 2008.

[113] G. Wolny. Modified DMAC Clustering Algorithm for VANETs. In *3rd Int. Conf. on Systems and Networks Communications, ICSNC*, pages 268–273, 2008.

[114] B. Xiao, B. Yu, and C. Gao. Detection and Localization of Sybil Nodes in VANETs. In *Proceeding of the 2006 workshop on dependability issus in wireless ad hoc network and sensor networks, DIWANS'06*, September 2006.

[115] X. Xue, N. Lin, L. Ding, and Y. Ji. A Trusted Neighbor Table Based Location Verification for VANET Routing. In *IET 3rd International Conference on Wireless, Mobile and Multimedia Networks, ICWMNN*, 2010.

[116] G. Yan, X. Chen, and S. Olariu. Providing VANET Position Integrity through Filtering. In *Proceeding of the 12th International IEEE Conference on Intelligent Transportation System*, October 2009.

[117] G. Yan, S. Olariu, and M. Weigle. Providing VANET security through active position detection. *Computer Communications*, 31(12):2883 – 2897, 2008.

[118] G. Yan, D. Rawat, and B. Bista. Provisioning Vehicular Ad Hoc Networks with Quality of Service. In *International Conference on Broadband, Wireless Computing, Communication and Applications, (BWCCA)*, pages 102–107, November 2010.

[119] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato. A Survey of Trust and Reputation Management Systems in Wireless Communications. *Proceedings of the IEEE*, 98(10):1755–1772, 2010.

[120] Xiang Zeng, Rajive Bagrodia, and Mario Gerla. GloMoSim: a Library for Parallel Simulation of Large-scale Wireless Networks. In *12th Workshop on Parallel and Distributed Simulations – PADS '98, Banff, Alberta, Canada*, May 1998.

[121] C. Zhang, X. Lin, R. Lu, P-H Ho, and X. Shen. An Efficient Message Authentication Scheme for Vehicular Communications. *IEEE Transactions on Vehicular Technology*, 57(6), November 3357-3368.

[122] C. Zhang, R. Lu, X. Lin, P-H Ho, and X. Shen. An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks. In *The 27th Conference on Computer Communications, INFOCOM'08*, pages 246–250, 2008.

[123] J. Zhang. A Survey on Trust Management for VANETs. In *IEEE International Conference on Advanced Information Networking and Applications (AINA)*, pages 105–112, March 2011.

[124] L. Zhou, B. Geller, B. Zhengi, and J. Cui. Cross-layer design for scheduling in cooperative VANETs. In *9th International Conference on Intelligent Transport Systems Telecommunications,(ITST)*, pages 505–509, 2009.