AN EFFICIENT FRAMEWORK OF IDENTITY-BASED CONDITIONAL PRIVACY-PRESERVING AUTHENTICATION FOR VEHICULAR AD HOC NETWORKS

MAHMOOD ARIF LAFTA AL SHAREEDA

UNIVERSITI SAINS MALAYSIA

2022

AN EFFICIENT FRAMEWORK OF IDENTITY-BASED CONDITIONAL PRIVACY-PRESERVING AUTHENTICATION FOR VEHICULAR AD HOC NETWORKS

by

MAHMOOD ARIF LAFTA AL SHAREEDA

**Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosphy**

April 2022

ACKNOWLEDGEMENT

With the name of Allah, Most Gracious, Most Merciful. Before anything, I give thanks to “Allah” for protection and the ability to do this research, which I will not be able to achieve that without his blessings. I would like to give deep thanks to the collegemates and lecturers at librarians, the National Advanced IPv6 Center, and other employer of the Center for their type support during my Ph.D. journey.

I would like to express my thanks to my research supervisor, Dr. Mohammed Anbar, and co-supervisors Associate Professor Dr. Selvakumar Manickam for their supervision, help suggestions, patience and precious comments. Without their help in every step throughout the process, this work would have never been achieved. I would like to thank you very much for your understanding and support over these past three years.

In this situation, I never forget life-coach "My Father" Arif Lafta, for his great encouragement, support, patience for me to complete my Ph.D. journey, without you, DAD, I am literally nothing. I would like also to thanks "My Mother", I really do not have any word to explain my thanks for your assistance to make me where I am now. And lastly, thanks to my two brothers Mohmmed Arif and Yousif Arif and my lovely three sisters.

Finally, my special and heartily thanks to the unknown soldier who helps me without notice. May the Almighty God richly bless all of you. I dedicate this research to all of these people.

Mahmood A. Al-Shareeda, Penang Malaysia, 2022.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

VANET	Vehicular Ad-Hoc Network
ITS	Intelligent Transportation System
GDP	Gross Domestic Product
MANET	Mobile Ad-Hoc Network
DSRC	Dedicated Short-Range Communication
WAVE	Wireless Access in Vehicle Environment
TA	Trusted Authority
RSU	Road-Side Unit
OBU	On-Bboard Unit
OSI	Open Systems Interconnection
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
TA	Trusted Authority
GUI	Graphical User Interface
TPD	Tamper Proof Device
CPPA	Conditional Privacy-Preserving Authentication
CRL	Certificate Revocation List
ECC	Elliptic Curve Cryptography
CPPA	Conditional Privacy-Preserving Authentication

PKI-CPPA	Public Key Infrastructure-Based Conditional Privacy-Preserving Authentication
GS-CPPA	Group Signatures-Based Conditional Privacy-preserving Authentication
ID-CPPA	Identity-Based Conditional Privacy-Preserving Authentication
EID-CPPA	Efficient Identity Based Conditional Privacy-Preserving Authentication
AES-CCM	Advanced Encryption Standard-Counter with Cipher Block Chaining Message
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDHP	Elliptic Curve Diffe-Hellman Problem

KERANGKA CEKAP PENYAHIHAN MENGEKALKAN-PRIVASI BERSYARAT BERASASKAN IDENTITI UNTUK RANGKAIAN KENDERAAN AD HOC

ABSTRAK

Rangkaian ad hoc kenderaan (VANET) telah menjadi semakin lazim sejak beberapa tahun kebelakangan ini disebabkan peranan kritikalnya dalam bidang pengangkutan pintar dengan menyokong komunikasi Kenderaan-ke-Kenderaan dan Kenderaan-ke-Infrastruktur. Keselamatan dan privasi VANET adalah amat penting kerana ia menggunakan medium komunikasi wayarles terbuka di mana mesej ditukar dalam teks biasa yang membolehkan penyerang memintas, mengusik, memainkan semula dan memadamnya. Untuk menangani isu ini, beberapa penyelidik telah mencadangkan beberapa skema dalam VANET. Taksonomi skema sedia ada adalah seperti berikut. Pengesahan pemeliharaan privasi bersyarat (PKI-CPPA) berasaskan infrastruktur kunci awam, pengesahan pemeliharaan privasi bersyarat (GS-CPPA) berasaskan tandatangan kumpulan dan skim pengesahan pengekalan privasi bersyarat (ID-CPPA) berasaskan identiti. Tesis ini mencadangkan satu kerangka pengesahan pengekalan privasi bersyarat berasaskan identiti yang cekap (EID-CPPA) berdasarkan kriptografi lengkung eliptik untuk menjamin keselamatan komunikasi dalam VANET. Kerangka EID-CPPA yang dicadangkan terdiri daripada empat fasa utama iaitu Pememulaan Sistem, Penggabungan, Penyiaran Mesej dan Kemas Kini Parameter. Tujuan utama di sebalik empat fasa yang digunakan adalah seperti berikut. Fasa pertama ialah Pememulaan Sistem, iaitu Autoriti Terpercaya (TA) bertanggungjawab menjana dan pramuat kunci awam dan peribadi ke dalam setiap Unit Tepi Jalan (RSU) yang terletak pada domain tunggal untuk mengurangkan saiz Senarai Pembatalan Sijil (CRL). Fasa kedua ialah Penggabungan, iaitu RSU bertanggungjawab menjana dan pramuat senarai ID samaran dan kunci tandatangan yang sepadan pada setiap kenderaan berdaftar untuk mencapai keperluan nyahpaut yang cekap. Fasa ketiga ialah Penyiaran Mesej, yang melibatkan menandatangani dan mengesahkan mesej. Fasa keempat ialah Kemas Kini Parameter, bertujuan menahan serangan saluran sisi yang digunakan untuk memperolehi maklumat sensitif yang disimpan pada Peranti Kalis-Gangguan (TPD) kenderaan. Untuk mengesahkan dan menentusahkan kerangka EID-CPPA yang dicadangkan, analisis keselamatan terperinci (logik Burrows–Abadi–Needham (BAN), model Oracle rawak, keselamatan bukti, dan atribut keselamatan) telah dinilai pada kerangka EID-CPPA yang dicadangkan. Keputusan analisis menunjukkan bahawa kerangka EID-CPPA yang dicadangkan adalah selamat. Sementara itu, dibandingkan dengan skim sedia ada, hasil simulasi kerangka EID-CPPA yang dicadangkan mengurangkan kos pemprosesan untuk menandatangani mesej, pengesahan tunggal dan pengesahan kumpulan masing-masing sebanyak 0.15%, 66.50%, dan 74.36%. Manakala kerangka EID-CPPA yang dicadangkan mengurangkan kos komunikasi mesej sebanyak 13.89%.

AN EFFICIENT FRAMEWORK OF IDENTITY-BASED CONDITIONAL PRIVACY-PRESERVING AUTHENTICATION FOR VEHICULAR AD HOC NETWORKS

ABSTRACT

Vehicular ad hoc networks (VANETs) have become increasingly common in recent years due to their critical role in the field of intelligent transportation by supporting Vehicle-to-Vehicle and Vehicle-to-Infrastructure communications. The security and privacy of VANET are of the utmost importance due to the use of an open wireless communication medium where messages are exchanged in the plain text allowing attackers to intercept, tamper, replay, and delete them. To address these issues, several researcher have been proposed schemes in VANET. The taxonomy of existing schemes is as follows. Public key infrastructure-based conditional privacy-preserving authentication (PKI-CPPA), group signatures-based conditional privacy-preserving authentication (GS-CPPA), and identity-based conditional privacy-preserving authentication (ID-CPPA) schemes. This thesis aims to propose an efficient framework identity-based conditional privacy-preserving authentication (EID-CPPA) based on elliptic curve cryptography to secure communication in VANETs. The proposed EID-CPPA framework comprises four main phases namely System Initialization, Joining, Broadcasting Massages and Updated Parameter. The first phase is System Initialization, where the Trusted Authority (TA) is responsible to generate and preload the public and private keys into each Road-Side Unit (RSU) located on single domain to reduce the size of Certificate Revocation List (CRL). The second phase is Joining, where the RSU is responsible to generate and preload lists of pseudonym-IDs and the corresponding signatures keys into each registered vehicle to achieve efficient unlinkability requirements. The third phase is Broadcasting Massages, which involves signing and verifying messages. The fourth phase is Updated Parameter, which aims to resist side-channel attacks to obtain the sensitive information stored on the Tamper-Proof Device (TPD) on the vehicle. To validate and verify the proposed EID-CPPA framework, a detailed security analysis (Burrows–Abadi–Needham (BAN) logic, random Oracle model, security of proof, and security attributes) are evaluated in the proposed EID-CPPA framework. Therefore, the analysis has shown that the proposed EID-CPPA framework is secure. In addition, compared with the existing schemes, the simulation result of the proposed EID-CPPA framework reduces the computation costs of signing the message, single verifying and batch verifying the messages by 0.15%, 66.50% and 74.36% respectively. While the proposed EID-CPPA framework reduces the communication costs of the message size by 13.89%.

CHAPTER ONE

INTRODUCTION

This chapter introduces the research behind this thesis. It discusses the security and privacy issues in the communication of the Vehicular Ad-Hoc Network (VANET). The chapter comprises sections on research overview, research background, problem statement, research objectives, and research scope and limitations in Sections 1.1, 1.2, 1.3, 1.4 and 1.5, respectively. Section 1.6 presents the research contribution in securing VANET communication through several steps in Section 1.7. Finally, Section 1.8 summarizes the thesis organization.

1.1 Overview

Annually, almost 1.3 million people are affected by road accidents. Road traffic injuries are the ninth leading cause of death globally and incur a loss of around 3% or USD 1 trillion of the world's Gross Domestic Product (GDP). Road accident is projected to be the fifth leading cause of death by 2030. Additionally, traffic congestions also waste an enormous amount of time and fuel.

Intelligent Transportation System (ITS) plays a crucial role in the mobility of modern human life in today's digital world. The value of global demand for connected vehicles was $63,026 million in 2017 and is forecasted to increase to $225,158 million by 2025, with a 17.1% compound annual growth rate between 2018 and 2025, as shown in Figure 1.1.

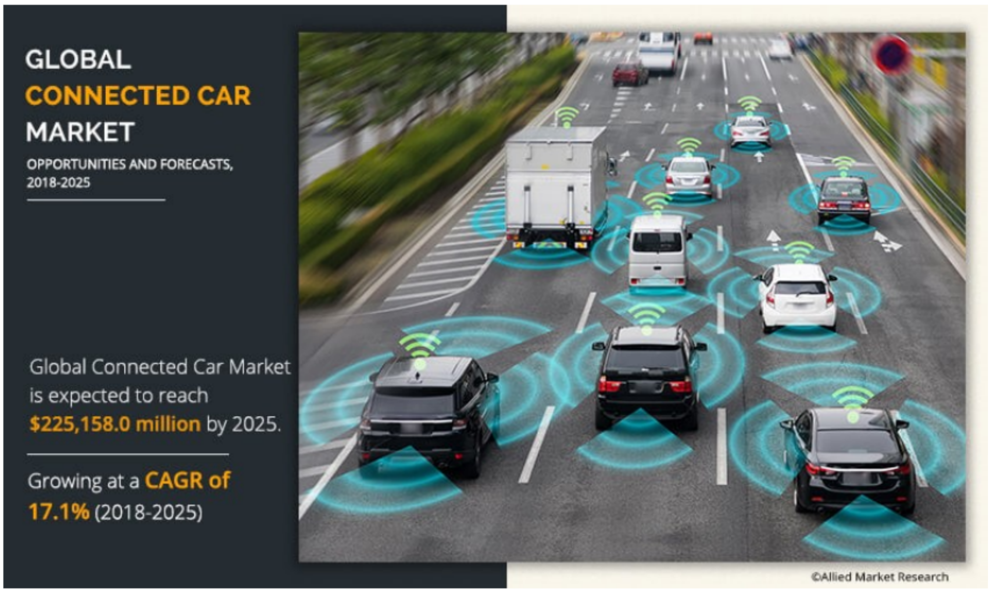
GLOBAL
CONNECTED CAR
MARKET
OPPORTUNITIES AND FORECASTS, 2018-2025
Global Connected Car Market is expected to reach $225,158.0 million by 2025.
Growing at a CAGR of 17.1% (2018-2025)
©Allied Market Research

Figure 1.1: Compound Annual Growth Rate of Global Demand for Connected Vehicles (2018–2025) Singh and Katare (2020).

It is being introduced to build intelligent vehicles through the rapid growth of wireless communication technology (Ali et al., 2017). Modern vehicle manufacturers and telcos have accepted that wireless communication will be an integral feature of every vehicle, enabling it to communicate with other vehicles and road infrastructures (C. Zhang et al., 2010). These vehicles form a particular type of ad hoc network, where the vehicles are the network nodes. This network is known as VANET, and it is becoming one of the most promising research areas for ITS with the above characteristics (Manivannan & Zeadally, 2020; Sheikh et al., 2019).

1.2 Background

This section first describes the VANET introduction; this is followed by a demonstration of the VANET components and lastly, the security and privacy issues for VANET are explained.

1.2.1 VANET Introduction

Vehicles have become synonym with human mobility nowadays. Consequently, much works and research have been done to improve vehicular technology. Recently, extensive research and massive development of VANETs have attracted industry, academia, and even the government's interest to get involved (Wang et al., 2020) (Wang et al., 2020). VANET is a subclass of Mobile Ad-Hoc Network (MANET) that uses mobile technologies as the network nodes for vehicle communication (Ali et al., 2017). The Wireless Access in Vehicle Environment (WAVE) was renamed to Dedicated Short-Range Communication (DSRC) (Jiang et al., 2006) standard using IEEE 802.11p standard for wireless communication. In the following subsection, VANET components and VANET's security and privacy issues are briefly presented.

1.2.2 VANET Components

In general, the architecture of a VANET system comprises three components: Trusted Authority (TA), Road-Side Unit (RSU), and On-Bboard Unit (OBU),as illustrated in Figure 1.2. TA is a third-party entity that is responsible for managing and generating the public system parameters on behalf of the other two entities. RSU is a fixed infrastructure typically deployed along the roadside, which acts as a proxy for communication between the vehicles and the TA via a wireless channel and wired channel, respectively. The OBU is equipped on every VANET-enabled vehicle, which allows the vehicle to process, receive, and broadcast safety-related messages for road traffic management. Each OBU is equipped with a Tamper Proof Device (TPD) to keep personally identifiable information safe and secure. RSU's computing power and storage capacity are higher than those of OBU.

Figure 1.2: The Three Components for VANET.

1.2.3 VANET's Security and Privacy Issues

In VANETs, security is a critical requirement. Due to the inherent characteristics of VANETs, it is vulnerable to different security attacks. Malicious actors can easily launch many attacks on broadcasted messages, even to the extent of taking control of the communication channels. Cui et al. (2019) demonstrated several attack processes, such as (i) replay antecedently acquired broadcasted message to recipients, (ii) modify the broadcasted message and transmit to other users in VANETs, (iii) fake authentic node and send messages to other users, (iv) intercept the broadcasted message, manipulate data, and perform sniffing, and (v) retrieve sensitive information that stored on OBU via side-channel attacks. A wrong message could lead the VANETs node to make incorrect judgments that cause serious road incidents. Therefore, the recipient (vehicles or RSUs) must check the validity of the received message before making any decisions or taking further actions (Wazid et al., 2019). Security issues will explain in Subsection 2.3.3(a)

In addition, the TA is responsible to revoke malicious vehicles from VANET resources used. When a report is received, TA adds pseudonym-ID to Certificate Revocation List (CRL) on each RSU during the revocation process. Therefore, when a malicious vehicle sends authenticated request to TA, RSU will revoke it after checking on CRL. Since the VANET system has the shared CRL for each RSU, the growth of

CRL is increased on a RSU. For instance, if there are 1000 revoked vehicles on CRL, RSU should be checked and matches pseudonym-ID before the authentication process continues during a long period times. Therefore, resulting in a very time-consuming CRL checking process.

Privacy issues are equally significant in VANETs (Ali et al., 2019; Qu et al., 2015). Malicious users can threaten user privacy during communication, such as acquiring a vehicle's original identity or determining its travel paths from examining the captured messages and cross-matching two or more broadcasted messages from the same source (linkability issue). Therefore, attackers can misuse the driver's private information for crimes like kidnapping, theft, and robbery (Abu Talib et al., 2018; Kumari et al., 2016). The consequence of drivers' information exposure is that vehicle users will be reluctant to embrace VANETs technology. Therefore, communication anonymity is a requirement for vehicle privacy preservation. Privacy issues will be more explained in Subsection 2.3.3(b).

1.3 Problem Statement

VANETs aim to improve road safety and make transportation more efficient. The security and privacy of VANET are of the utmost importance due to the use of an open wireless communication medium where messages are exchanged in plain text, which allows attackers to intercept, tamper, replay, delete and even trace driver's route. Hence, there is a high probability that the safety of a VANET-Based intelligent transportation system could be compromised. Therefore, security and privacy have become more significant and should be carefully addressed before deploying VANETs applications. Nowadays, securing and safeguarding VANETs message exchange is the focus of many security research teams, as reflected by the number of Conditional Privacy-Preserving Authentication (CPPA) schemes.

Several researchers proposed CPPA schemes to cope with security and privacy issues for the widespread deployment of VANETs to ensure secure communication. Generally, these types of schemes fall into three categories:Public Key Infrastructure-Based Conditional Privacy-Preserving Authentication (PKI-CPPA), Group Signatures-Based Conditional Privacy-preserving Authentication (GS-CPPA), and Identity-Based Conditional Privacy-Preserving Authentication (ID-CPPA). The major limitation of PKI-CPPA and GS-CPPA schemes are addressed by proposing ID-CPPA schemes that usually use two security cryptographies: Bilinear pairing and Elliptic Curve Cryptography (ECC). The schemes use bilinear pairing operations in signing and verifying messages during the broadcast process. However, these operations are one of the most complex cryptography operations and are very time-consuming. Therefore, these operations add considerable costs in computation overhead during the broadcasting process to verify the recipient. Due to the limitation of bilinear pairing, He et al. (2015) introduced ID-CPPA to provide authentication and protect the privacy of VANET nodes using a three-point multiplication of ECC operations during message signing and verifying. These operations are more efficient than bilinear pairing operations.

However, the four main limitations arising in many schemes based on the ID-CPPA category are as follows. (i) Growing CRL size, (ii) efficient unlinkability, (iii) performance efficiency and (iv) side-channel attacks (They will be discussed in Subsection 2.7.2 in details). The reasoning behind this claim is as follows. Firstly, when a malicious vehicle that broadcasted false messages is reported, the TA revokes the malicious vehicle's certificate and updates large number of revoked vehicles stored in the CRLs on RSUs, causing the workload management of CRLs. Consequently, the RSU incurs additional computation cost since it must first check the vehicle authenticity in the CRL list before it can authenticate itself with the system, which leads to reduced broadcasting performance in terms of message signing and verifying such as schemes proposed by (Alazzawi et al., 2019; Alshudukhi et al., 2021; Bayat et al., 2020; Pournaghi et al., 2018). Secondly, a vehicle computes new pseudonym-IDs for each message during the message signing process to satisfy unlinkability privacy requirements that prevent attackers from linking two or more messages to the same signer. However, the VANET system suffers from high computational costs generated by the signer to achieve unlinkability privacy requirements such as schemes proposed by (Alshudukhi et al., 2021; He et al., 2015; Pournaghi et al., 2018). Thirdly, to address high computation and communication costs caused by bilinear pairing operations and Map-To-Point function, Alazzawi et al. (2019); Alshudukhi et al. (2021) proposed a scheme using ECC and general hash function. However, many multiplication operations use ECC for message signing and verifying. Finally, the vehicle's OBU is vulnerable to side-channel attacks that could obtain sensitive information stored in the OBU's TPD through physical access. The disclosed sensitive information in the hand of malicious attackers can compromise the security of the VANETs system. A malicious attacker could use the information to send false messages, which leads to increased computation and communication costs during broadcasting such as schemes proposed by (Bayat et al., 2015; Jianhong et al., 2014).

Given the disadvantages mentioned earlier, this research's problem statement is the existing ID-CPPA schemes in the VANETs system have a considerable computation and communication overhead in signing and verifying messages. The reasons for the overheads are as follows:

1. The existing identity-based schemes suffer from growing CRL size during the mutual authentication process, resulting in a very time-consuming CRL checking process.
2. The existing identity-based schemes are unable to satisfy efficient unlinkability privacy-preserving requirements.
3. The existing identity-based schemes suffer from using a large number of multiplication point operations based on ECC.
4. The existing identity-based schemes are vulnerable to side-channel attacks, where attackers can broadcast false messages in the VANETs system.

1.4 Research Objectives

The goal of the thesis is focused primarily on proposing an efficient identity-based conditional privacy-preserving authentication (EID-CPPA) scheme to address the considerable computation and communication overhead costs in VANETs. There are four objectives defined to accomplish the thesis's primary goal, as follows:

1. To adopt a scheme to divide geographical areas of VANETs system into several domains by generating and preloading public/private keys for reducing the size of CRL.

2. To propose an efficient scheme that provides a signer (OBU) with the list of parameters from RSU during authentication process for satisfying an efficient unlinkability.

3. To propose an ECC scheme that a signer has the ability to compute part of the verifier's equation for reducing a large number of operations.

4. To propose a scheme that updates sensitive information by online and offline mode for resisting side-channel attack.

1.5 Research Scope and Limitations

In this research, the research scope is limited to proposing an EID-CPPA scheme to improve the CPPA in the VANETs system. Table 2.1 illustrates the research scope and evaluation considerations used.

Table 1.1: Summary of Research Scope and Limitations.

Item	**Scope of Research**
Environment	Vehicular Ad Hoc Network (VANET)
Cryptographic algorithm	Elliptic Curve Cryptography (ECC)
VANET protocol	DSRC, WAVE, and IEEE 802.11p
TA	Fully Trusted
RSU	Has Higher Racecourses Than OBU
Evaluation Metrics	Computation Cost, Communication Costs, Formal and Informal Security Analysis

1.6 Research Contributions

This research contributes an efficient scheme to reduce the system's overhead in computation and communication costs. The key contributions of this research are summarized as follows:

1. A division geographical areas by providing public and private keys into each domain. Several RSUs located in a domain has a shared CRL for revoking malicious vehicle, resulting in CRL checking process being reduced.

2. An efficient scheme by generating the list of parameters including pseudonym-IDs and signature keys during the mutual authentication process. Then RSU preloads these parameters into the corresponding registered vehicle.

3. A scheme has the ability to compute part of verifier's equation, which is utilized to mitigate the verification cost for the recipients (OBU or RSU).

4. A scheme that updates sensitive information by offline mode after time is expired for resisting side-channel attacks.

1.7 Research Steps

This section presents the research steps to achieve the research objectives. Figure 1.3 illustrates the research steps.

Step 01: Literature Review covers the background of VANET and its application followed by a detailed analysis of the VANET weakness and threats. Also, the existing schemes to secure communication of VANET are presented.

Step 02: Literature analysis discusses and analyses the significant schemes used to secure VANET communication and identifies each scheme's advantages and limitations. Hence, this step provides a better understanding of current schemes' limitations, research problems, and scope, which form the basis of the proposed framework.

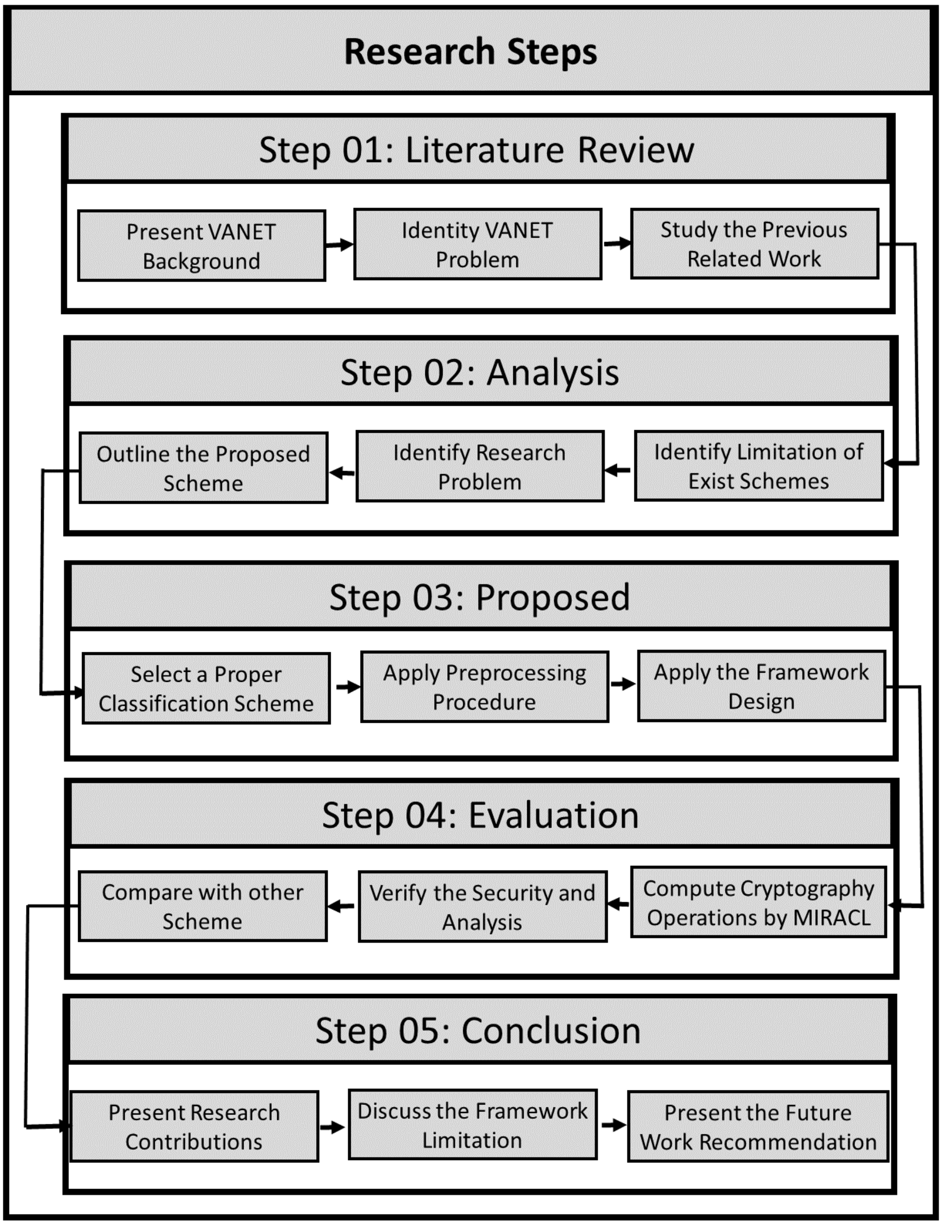
Research Steps
Step 01: Literature Review
Present VANET Background
Identity VANET Problem
Study the Previous Related Work
Step 02: Analysis
Outline the Proposed Scheme
Identify Research Problem
Identify Limitation of Exist Schemes
Step 03: Proposed
Select a Proper Classification Scheme
Apply Preprocessing Procedure
Apply the Framework Design
Step 04: Evaluation
Compare with other Scheme
Verify the Security and Analysis
Compute Cryptography Operations by MIRACL
Step 05: Conclusion
Present Research Contributions
Discuss the Framework Limitation
Present the Future Work Recommendation

Figure 1.3: Research Steps.

Step 03: Scheme Proposal presents and discusses the proposed framework design by selecting a proper classification in CPPA for vehicular communication. The proposed framework aims to meet all security and privacy requirements of VANET.

Step 04: Evaluation analyses and evaluates the efficiency of the proposed framework. The proposed framework's computation and communication costs are compared with the existing schemes for validation.

Step 05: Conclusion summarizes the research work, presents the contributions, highlights the limitations, and suggests future work.

1.8 Thesis Organization

This thesis has six chapters. Chapter 1 introduces the research topic. The rest of the chapters are as follows:

Chapter 2: critically reviews the background of the CPPA scheme in VANET. In addition, this chapter presents the essential concepts related to this research, the corresponding studies, and the weaknesses of each existing scheme.

Chapter 3: explains the research methodology of the proposed EID-CPPA framework and elaborates its requirements.

Chapter 4: explains the structural design and implementation of the proposed framework.

Chapter 5: presents a detailed performance evaluation of the proposed framework and the comparison with several existing schemes.

Chapter 6: concludes this thesis and provides the direction for future research.

CHAPTER TWO

LITERATURE REVIEW

Chapter 1 introduced the research in this thesis and outlined the chapters. This chapter presents the VANET background and literature review of VANET security and privacy schemes. The visual outline of Chapter 2 structure is in Figure 2.1. Section 2.1 explains the ITSs and MANET, while Section 2.2 provides VANET's background including, communication, architecture, standard, characteristics, and applications. The discussion of the VANET's security and privacy requirements, attacker classification, and security attack are in Section 2.3. Section 2.4 illustrates the type of cryptography algorithms used in VANET. Section 2.5 introduces three taxonomies of conditional privacy-preserving authentication schemes in the VANET system. Section 2.6 provides the analyses and critical review of related work within this taxonomy. Section 2.7 discusses the research gab based on the related work. Finally, Section 2.8 summarizes of this chapter.

2.1 Introduction

In this section, prior the VANET system is explaining in details in this chapter, Intelligent Transportation System (ITS) and Mobile Ad-Hoc Network (MANET) are briefly presented as follows.

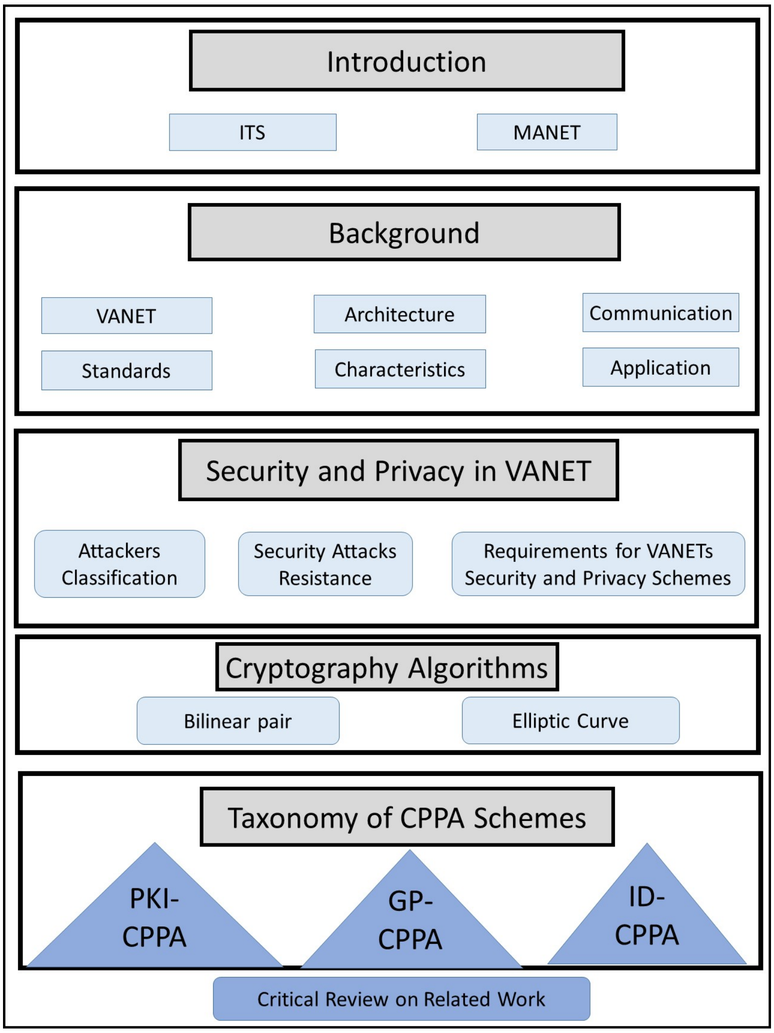

Figure 2.1: Chapter Two Structure.

2.1.1 Intelligent Transportation System

The ITS utilizes networking techniques to cope with various problems in transportation. ITSs are sophisticated applications that provide inventive transport and traffic management services and provide better information for many users and make transportation networks safer, more coordinated, and smarter (Shladover, 2018; Yang et al., 2019). VANET is already well-established vehicle traffic monitoring and control using the Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication concepts. It sends critical real-time messages in both directions that enable vehicles to take alternative paths to avoid traffic congestion.

The primary goal of ITS are: (i) environmental protection and safety; (ii) improving traffic safety; (iii) increasing effectiveness in transportation areas; (iv) reducing travel time; and (v) reducing travel costs.

2.1.2 Mobile Ad-Hoc Network

MANET is a technology widely used in mobile communication with many autonomous nodes. For a specific purpose, MANET can organize itself in different ways via wireless links. The MANET can be easily implemented and reconfigured when a problem occurs. The use of MANET has been increasing steadily in recent years compared to the wired network.

There are broad applications of MANETs. The following are some examples: (i) distribution of information in meetings and seminars; (ii) Internet hotspots in public transport; (iii) advertising for local shops and businesses; and (iv) rescue operations and military activities.

The application of some MANET concepts in the transportation environment could provide safety and convenience for users. Thus, ITS borrowed some ideas from MANET, such as in-vehicle communication, and is called VANET. Therefore, MANET is the superclass of VANET that can be specified.

2.2 Background

In this section, Vehicular Ad Hoc Network (VANET) is deeply explained in the following subsections.

2.2.1 Vehicular Ad Hoc Network

A VANET comprises a group of vehicles, moving or stationary, connected through a wireless network. The original purpose of VANETs was to provide safety and comfort for drivers and passengers in vehicular environments. This perspective is changing, as VANETs are now being positioned as an infrastructure for intelligent transport systems that support autonomous vehicles and any activity that requires Internet access in a smart city ecosystem. VANETs also enable onboard computers with minimum Internet infrastructure support, mainly in stationary vehicles, such as those at airport car parks, to serve as mobile computing cloud resources. The content produced and consumed by the vehicles is relevant only in a local context in terms of time, space, and the agents: the producer and the consumer. The information generated by the vehicles is only valid locally, has a limited spatial extent, exact life span, limited temporal extent, and has a local interest. For example, it is only relevant to the specific segment of the road at a particular time and for vehicles not too far from the approaching area of a highway.

2.2.2 VANET Architecture

Three main components in VANET architecture are Trusted Authority (TA), Roadside Unit (RSU), and On-Board Unit (OBU), as shown in Figure 2.2. The detail of the three main VANET components are as follows:

- Trusted Authority (TA) is a trusted third-party entity with high computing resources responsible for registering other components in VANETs. It can also be connected semi securely to RSUs via wired networks. Before joining a VANET network, all RSUs and vehicles in the system must first register with the TA.

- Road-Side Unit (RSU) is located on the roadside and responsible for managing vehicles within its communication range. RSUs either process received messages from vehicles locally or send them to the TA for validation and authentication.
- On-Board Unit (OBU) is installed on a vehicle that allows the vehicle to communicate with other vehicles or RSU using DSRC Protocol. There is a TPD in every OBU to protect the information from being exposed or leaked.

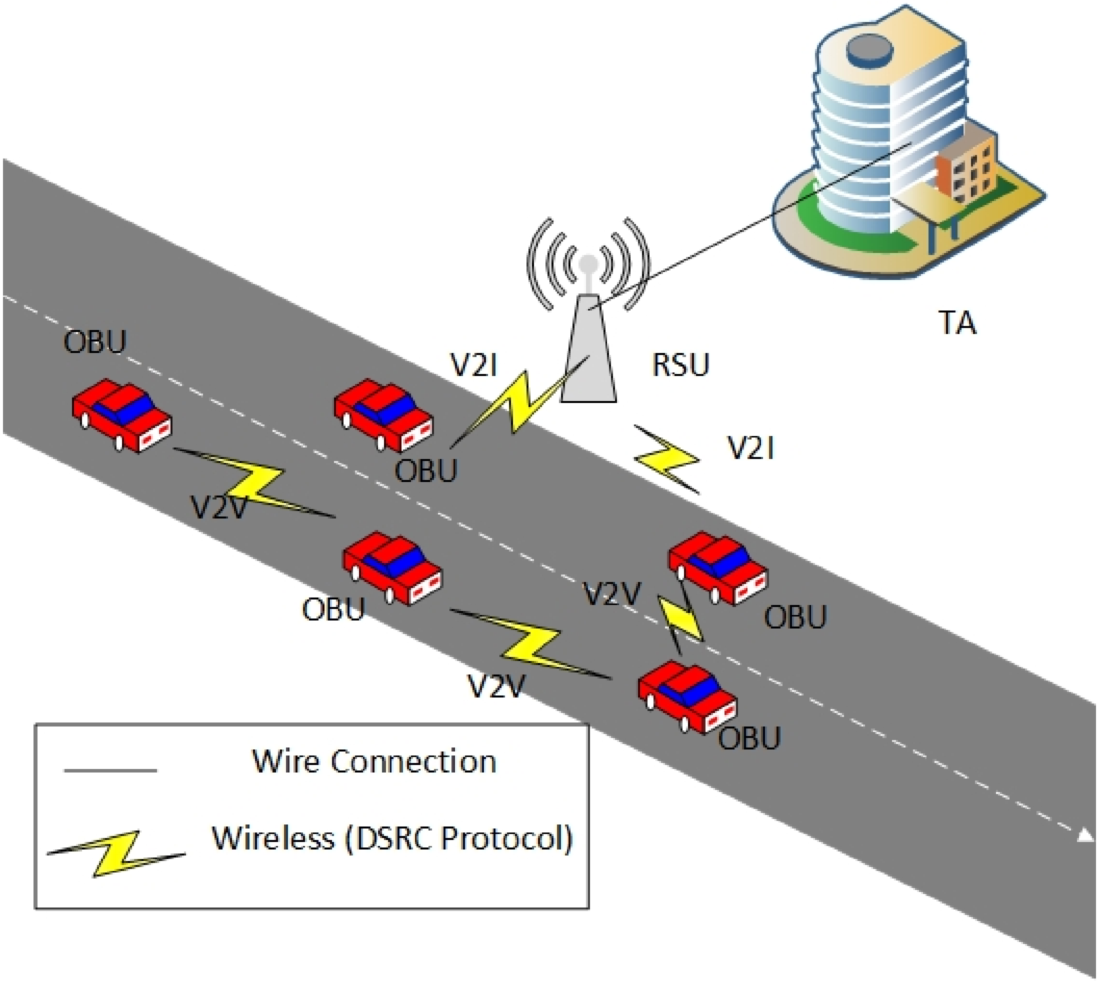

Figure 2.2: A Typical Structure of The VANETs Environment.

2.2.3 VANET Communications

To enhance the roads' flow, safety, and congestion, the ITS systematically offers communication security using various modern techniques such as VANETs. VANETs communication has two types: Vehicle-To-Vehicle (V2V) communication and Vehicle-To-Infrastructure (V2I) communication (Ali & Li, 2020).

- Vehicle-to-Vehicle (V2V): Vehicles use V2V communication to exchange information about traffic conditions with neighboring vehicles in regular intervals between 100 to 300 ms using the 5.9-GHz DSRC protocol (Lu et al., 2018).
- Vehicle-to-Infrastructure (V2I): Through its Graphical User Interface (GUI), the TA provides useful infotainment services and other traffic information to passengers and drivers using V2I communication. Based on the message received, vehicles can easily change their route to avoid unpleasant conditions such as traffic congestion and road accidents. In addition, RSUs transmit messages to ensure better safety and management of traffic within their communication range.

2.2.4 VANET Standards

VANET standardization is similar to the Open Systems Interconnection (OSI) model, with some changes on several layers and some addition to the management layer (Chehri et al., 2020; Khan & Lee, 2019). The standard protocols used to support communication for VANETs are the DSRC, WAVE, and IEEE 802.11p.

- DSRC is a short to medium-range wireless communication technology specifically designed for vehicles to communicate with each other using the frequency band between 5.850 to 5.925 GHz, with a 75 MHz spectrum (Chehri et al., 2020; Commission et al., 2002). The 75 MHz DSRC-band spectrum is divided into seven channels, as shown in Figure 2.3. Table 2.1 describes the various channel allocation in DSRC protocol (Commission et al., 2002).

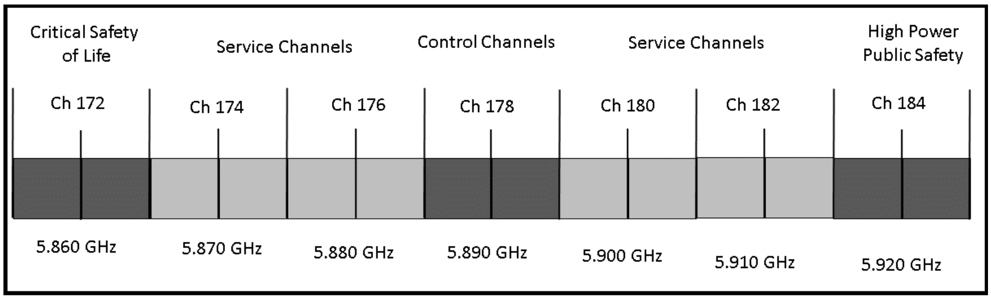

Figure 2.3: Channel Diagram of Dedicated Short Range Communication (DSRC).

Table 2.1: Current DSRC Channel Allocation.

Channel	Usage
178	The safety power applications
172, 174, 176, 180, 182, and 184	The service channel (SCH)
172 and 184	High power and public safety messages
Other channels	Traffic-related messages.

- WAVE is the IEEE published materials (ITS, 2018) for VANETs security with detailed documentation, including the latest ITS standards. The 1609 IEEE/WAVE standard specifies the architecture, method, protocols, and interface utilized to secure V2V and V2I communication on the VANET. The different WAVE standards as well as its integration with the OSI model is shown in Figure 2.4.

- IEEE 802.11p complies with the DSRC band. The IEEE adds the 802.11p to the IEEE 802.11 family to facilitate the vehicular communication network (Mejri et al., 2014).

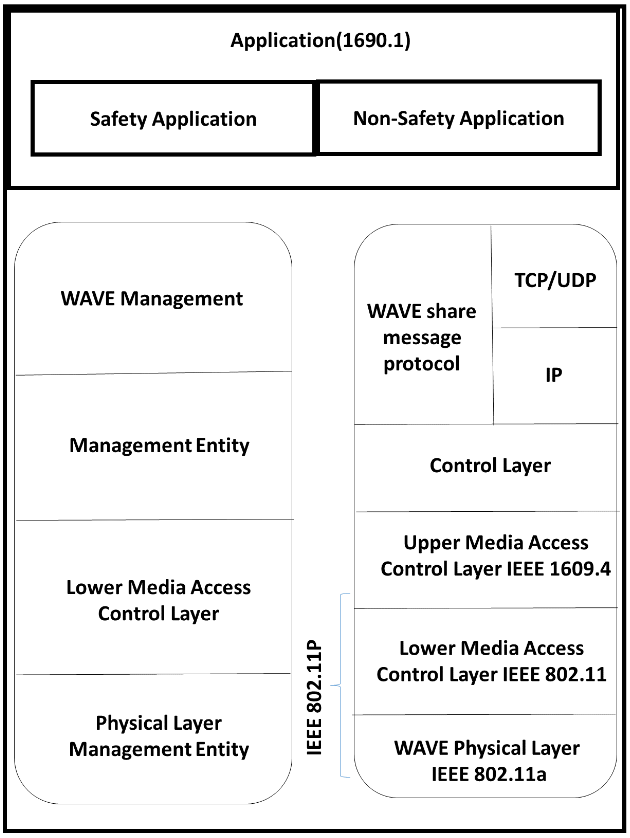
Application(1690.1)
Safety Application
Non-Safety Application
WAVE Management
Management Entity
Lower Media Access Control Layer
Physical Layer Management Entity
IEEE 802.11P
WAVE share message protocol
TCP/UDP
IP
Control Layer
Upper Media Access Control Layer IEEE 1609.4
Lower Media Access Control Layer IEEE 802.11
WAVE Physical Layer IEEE 802.11a

Figure 2.4: Wireless Access in Vehicular Environments (WAVE) Architecture.

2.2.5 VANET Characteristics

Compared to MANETs, VANETs have unique and essential characteristics in the security and privacy aspects. The following are the discussion regarding these VANET characteristics.

- High Mobility: The principal feature of VANETs is the high mobility of nodes. VANETs supports a large number of nodes with a wide range of mobility compared to MANETs. Since the nodes in VANET can move in random directions, VANET has become a different type of ad hoc network. It is not easy to estimate the node location and network topology because the node is the vehicle in VANET, which is constrained to the road and traffic lights. Many researchers have studied this unique feature (Blum et al., 2004; Jakubiak & Koucheryavy, 2008; Toor et al., 2008).

- Limitation of Transmission Power: WAVE is limited in transmission power, ranging from 0 to 28.8 dBm, restricting VANETs coverage range to a distance of only up to 1 kilometer (Morgan, 2010).
- Large Network: VANETs require extensive network area coverage. The network must cover the urban areas, highways, and the entry and exit point of the city (Toor et al., 2008; Yousefi et al., 2006).
- Driver Safety: VANET communication can provide the drivers and passengers with various advanced applications. Thus, VANET allows some applications to directly communicate between nodes (OBUs) and other networks (RSUs).
- Network Strength: The network strength in VANETs relies on the street traffic flow. It is very high during traffic congestion and very low when there is less or no traffic.
- Wireless Communication: The nodes in VANET exchange data and connect with other nodes via a wireless medium. Therefore, secure communication during transmission is a must (Hasrouny et al., 2017).
- Dynamic Network Topology: Due to the high mobility of nodes, the VANETs topology is rapidly changing. Thus, VANETs are more vulnerable to attacks and very difficult to identify malicious vehicles.

2.2.6 VANET Applications

VANET provides drivers and passengers with various advanced applications and offers unprecedented non-safety information and safety services. Information received by the vehicle, whether via V2V and V2I, increase the driver's and passenger's awareness of the road situation, which improves driving experience and passenger comfort (Jabbarpour et al., 2018; Yang et al., 2019). VANET applications are categorized into two: (i) non-safety applications and (ii) safety applications.

2.2.6(a) Non-Safety Applications

The non-safety applications of VANETs are for comfort services to improve driving experiences and passenger luxury. Examples of non-safety applications are as follows (Sheikh et al., 2019):

- Climate information update,
- Internet access,
- Communication between vehicles,
- Provide detailed hotel location, and
- Search nearby restaurants and petrol stations.

2.2.6(b) Safety Applications

The main objective of the safety applications in VANETs is to keep the road users, whether drivers or passengers, safe from harm. Examples of safety applications are as follows (Sheikh et al., 2019):

- Improve traffic and road safety,
- Broadcast lane changing warning,
- Provide emergency video streaming, and
- Avoid collisions and accidents.

2.3 Security and Privacy in VANET

Being a subclass of MANET, VANET inherits some vulnerabilities to security attacks (Engoulou et al., 2014). However, the security aspect gets far less attention due to its unique characteristics, such as highly dense and dynamic network topology. However, VANET's security is critical since VANETs components are exchanging vital and sensitive traffic-related messages. Therefore a VANET security scheme must ensure that attackers cannot modify traffic-related messages (Lin et al., 2008).

2.3.1 Attackers Classification

Researchers classify attackers according to their behavior in the network. An adversary node is any entity that injects or alters messages and disrupts the network. The attackers' primary aim is to cause problems in the network for personal benefit. According to Maxim Raya and Amer Aijaz, the attacks on VANETs are commonly classified into three types (Aijaz et al., 2006; Raya & Hubaux, 2007).

- Internal vs. External Attacks.

  Internal attacks are generally perpetrated from within the network by authenticated users familiar with the network configuration details. Internal attacks are extremely dangerous and more damaging compared to external attacks. External attacks typically come from unauthenticated users from outside the network, and it is usually less severe and not as damaging, as illustrated in Figure 2.5.

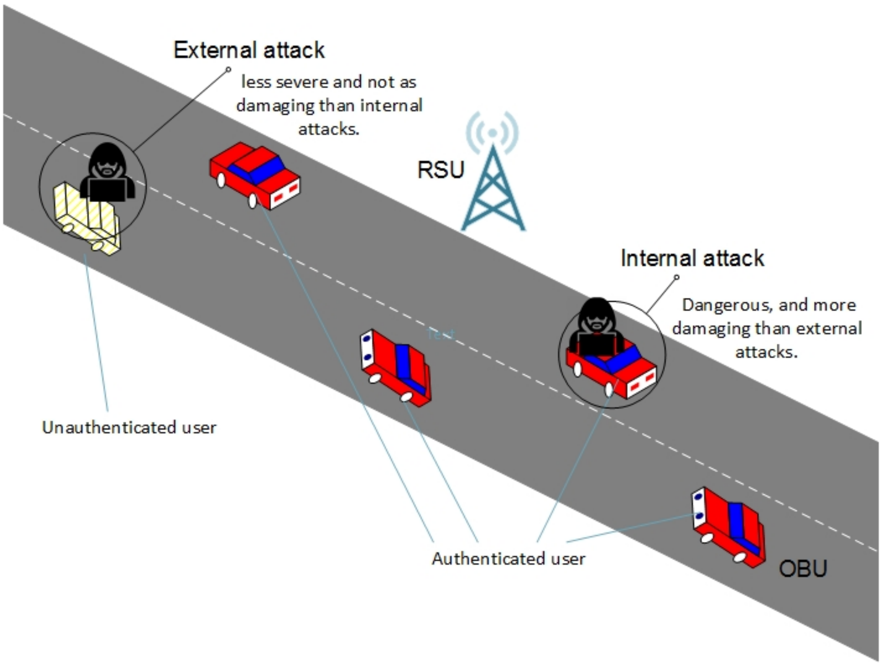
External attack
less severe and not as damaging than internal attacks.
RSU
Internal attack
Dangerous, and more damaging than external attacks.
Unauthenticated user
Authenticated user
OBU

Figure 2.5: Internal vs. External Attacks.

- Active vs. Passive Attacks.

  Passive attacks do not involve injecting or tampering with messages in the network. A passive attacker connects to the wireless network to learn about the pattern and frequency of the data transfer, possibly for use in the future. On the contrary, an active attacker alters information it received, generates false signals, drops received packets, or changes the data stream to disrupt network efficiency or obtain unauthorized access to services, as illustrated in Figure 2.6.

- Malicious vs. Rational Attacks.

  Not all attacks are perpetrated for personal gain; some attacks aim to disrupt network performance or create a hurdle for targeted victims in the network. On