# DETECTING ROGUE NODES IN VEHICULAR AD-HOC NETWORKS (DETER)

A Thesis Submitted to
City, University of London, School of Mathematics, Computer Science and Engineering.
In Fulfilment of the Requirements for the Degree
Doctor of Philosophy in
Information Engineering

By

**Syed Kamran Zaidi**

2016

# Acknowledgements

In the name of Allah, the most beneficent, the most merciful.

I would like to thank Prof. Muttukrishnan Rajarajan for his able guidance, support and help that enabled me to complete the PhD. His help in both academic and non-academic matters has been highly beneficial. His insight and experience has enabled me to understand and pursue research and then get good quality publications. Working with him has made me a better researcher and professional.

I would also like to thank Dr. Veselin Rakocevic for his very useful comments and guidance to improve the research results.

I would like to thank my family, my parents and especially my wife Ramza for supporting me during this testing period of my life. I would not have been able to embark on this journey let alone complete it without her help and support.

# Declaration

No portion of the work referred to in this thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning. I hereby grant powers of discretion to the University Librarian to allow this thesis to be copied in whole or in part without further reference to the author. This permission covers only single copies made for study purposes, subject to normal conditions of acknowledgement.

# Abstract

Vehicular ad hoc Networks (VANETs) are self-organizing networks of vehicles equipped with radios and processors. VANETs are very promising as they can make driving safer by improving road awareness through sharing of information from sensors. Vehicles communicate with each other wirelessly to exchange information and this exchange of information is susceptible to attacks of different kinds. There are some very important issues that need to be resolved before VANETs can be deployed on large scale. Security and privacy issues are undoubtedly the most important factors that need to be resolved.

Amongst various problems to be solved in VANETs is the issue of rogue nodes and their impact on the network. This thesis discusses the problems associated with the security and privacy of vehicular networks in the presence of rogue nodes. The rogue nodes can share / inject false data in the network which can cause serious harm. The techniques proposed make VANETs secure and prevent them from the harmful impact of rogue nodes. The proposed work makes the network safer by making it fault tolerant and resilient in the presence of rogue nodes that can be detected and reported. As VANETs are highly dynamic and fast moving so, a data centric scheme is proposed that can determine if a node is rogue or not just by analysing its data. The work then enhances the developed mechanism by applying hypothesis testing and other statistical techniques to detect intrusions in the network by rogue nodes. The technique is simulated using OMNET++, SUMO and VACAMobil and the results obtained have been presented, discussed and compared to previous works.

In order to prevent rogue nodes from becoming part of the VANETs this thesis also presents a novel framework for managing the digital identity in the vehicular networks. This framework authenticates the user and the vehicle separately from two authorities and allows him to communicate securely with the infrastructure using IBE (Identity Based Encryption). The proposed technique also preserves the privacy of the user. The proposed scheme allows traceability and revocation so that users can be held accountable and penalised. The results have been compared to previous works of similar nature. The thesis also discusses the Sybil attack and how to detect them using game theory in a VANET environment.

# List of Publications:

1. **Kamran Zaidi**, Yogachandran Rahulamathavan and Muttukrishnan Rajarajan. "DIVA-Digital Identity in VANETs: A multi-authority framework for VANETs," in *Networks (ICON), 2013 19th IEEE International Conference on*, pp. 1-6. IEEE, 2013.

2. **Kamran Zaidi**, Milos Milojevic, Veselin Rakocevic and Muttukrishnan Rajarajan. "Data Centric Rogue Node Detection in VANETs," in *IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom),* TrustCom 2014, Beijing, China.

3. **Kamran Zaidi**, Milos Milojevic, Veselin Rakocevic, Arumugum Nallanathan and Muttukrishnan Rajarajan. "Host Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection," in *IEEE Transactions on Vehicular Technology*. 2015

4. **Kamran Zaidi** and Muttukrishnan Rajarajan, "Vehicular Internet: Security & Privacy Challenges and Opportunities," in *Future Internet*, pp. 257-275, vol. 7, 2015.

**Submitted:**

5. **Kamran Zaidi** and Muttukrishnan Rajarajan, "Deception Games: Sybil Attack Detection in VANETs Using Game Theory," *Submitted to Computers & Security on* 14$^{th}$ Aug 2016.

## Table of Contents

# List of FIGURES

# List of TABLES

# Chapter 1 : Introduction

## 1.1 Background

Vehicular Ad-hoc Network (VANET) is an interconnection of vehicles with on-board Units (OBUs) that communicate with one another to form a wireless network. VANETs are considered imminent due to their huge potential in terms of road safety and other convenience applications. Vehicular networks are considered imminent due to the advancement and ease in wireless connectivity. It is just a matter of time before they become a reality. Vehicular networks are considered important due to their tremendous potential both in terms of safety and commercial applications.

Over the last three decades there have been a lot of innovation in vehicles in terms of fuel efficiency, navigation, comfort and making the general feel of driving more pleasant and enjoyable but there hasn’t been much change in terms of road safety. Road travel is still considered to be quite hazardous as the mistake of a single person can have catastrophic results especially at high speeds. Although, there has been a lot of automation in vehicles by incorporating sensors, cameras and radars but the full potential of this technology can only be realized if vehicles are equipped with radios and allowed to communicate with each other. This will lead to the deployment of VANETs.

The developments in the automotive industry in the last few decades have been impressive. Cars today are much more fuel-efficient than ever before. However, the advancements in automotive technology did not have the same impact on the safety of the roads. Vehicles today are still as vulnerable to accidents due to fog, ice, and other hazards on the road, but above all, they are vulnerable to human error. However, this is all set to change: the automotive industry has been working actively for years to put different sensors in cars and connect them to an on-board computer. With advancement in telecommunications, it is now possible to connect vehicles to each other through wireless technologies to enable them to communicate and cooperate. Now, not only is the automotive industry pursuing autonomous vehicles—they are being encouraged by the governments as well. The UK government announced in March 2015 that a £100 m funding for research into driver-less cars will bring in companies from not only the automotive industry but also from Information Technology (IT), telecommunications, and infrastructure [1]. In the US, car manufacturers like General Motors (GM) are already selling 4G Long Term Evolution (LTE)-connected cars in their 2015 fleet and they predict having fully connected cars by the end of this decade [2]. Moreover, IEEE believes that the need to get a driver's license might be eliminated by 2040 as autonomous cars would be ubiquitous [3].

Car manufacturers such as GM and Ford have opened up application development for their platforms by making their Application Program Interface (API) available to developers [4], [5]. They plan to follow the conventional business model, i.e., the developers submit their apps which are tested and approved before making them available for download. This LTE connectivity alone will serve to improve the in-vehicle infotainment services by providing access to high-speed internet, streaming movies, navigation, music, and live television, etc. The other aspect is commercial, i.e., offering location-based services and advertisements to the vehicle passengers. The LTE connectivity will not only bring internet to the vehicle but also make the vehicle a part of the internet, easing the way for the Vehicular Ad hoc NETworks (VANETs).

The true potential of the connected vehicle will be realized only when vehicles are interconnected to each other. This network, formed by the interconnection of vehicles, is referred to as VANET. This paradigm shift in vehicular technology will usher in a new era of innovation and will open a huge range of application areas that can help in improving road safety and reducing accidents on roads.

## 1.2 Problem Statement

The biggest challenge in the deployment of VANETs is that of Security and Privacy. The vehicles will share some messages with each other to make them aware of the traffic and road conditions. These messages are referred to as Cooperative Awareness Messages (CAMs) and will be shared at regular intervals. These messages consist of parameters like the position, speed etc. of the transmitting vehicle which are broadcasted to all vehicles in range. Therefore, security is crucial as drivers might make life critical decisions based on the information provided by other vehicles. Similarly, privacy of users is important as users don’t want to be tracked or identified all the time while at the same time we need accountability in the network so that users behave responsibly. The privacy and accountability of the user might look contradictory requirements but they are important and necessary in vehicular networks.

The OBUs possess reasonable computing power and memory but as the vehicles are travelling at high speeds, it is necessary that vehicles are able to authenticate the messages quickly. At the same time the messages have to be accurate (recent, relevant) and reliable (true) so that they can be acted upon by the recipient. This accuracy and reliability is provided by securing the communication in VANETs. Security can be achieved by using cryptographic techniques once the user has been authenticated. However, these cryptographic techniques should be suitable for the fast moving and quickly changing nature of VANETs.

Privacy is the ability to keep the identity of the user secret while allowing them to communicate and interact with other users while ensuring that the security of the communications is not violated.

## 1.3 Research Objectives

VANETs are dynamic and very fast moving and therefore, have special requirements. The most important requirement is for the vehicles to exchange credible, useful and accurate information about the traffic. However, as vehicles that come in contact with each other are mostly meeting for the first time, therefore, there is a need for some mechanisms to establish the identity of the vehicle and the credibility of the information being shared. VANETs can expand rapidly and may consist of thousands of nodes all communicating with one another. This raises the problem of the correctness of information that is being shared. As the information being shared can be used to take life saving decisions, it is imperative that the accuracy of the information is quickly ascertained and then auctioned upon. One answer to these issues is Cryptography albeit with some caveats. This means that only those vehicles are allowed to become part of VANETs that have been authenticated and then get the necessary keys. The ephemeral and fast changing nature of VANETs requires that the cryptographic techniques used should be scalable and efficient as otherwise there can be a bottleneck of messages. Also, the techniques used should preserve the privacy of the users.

However, a vehicle that has been authenticated and becomes part of the VANET can then inject false messages in the network and is very difficult to detect. It is therefore, essential that the information exchange in vehicular networks is secured against false data injection. Even if false data is injected in the network, the network should be resilient to such attacks and should have the ability to detect and correct the information to some extent. Therefore, the research question is:

**How to detect rogue (malicious) nodes in VANETs?**

The sub questions formulated are:

1. How to keep illegitimate / rogue nodes out of VANETs?
2. How to create and manage Identities in VANETs?
3. How to make VANETs resilient to false data injection attacks from nodes that turn rogue?
4. How to detect rogue nodes that are part of VANETs?
5. How to create a VANET model that can be used to determine normal or abnormal behaviour?

## 1.4 Research Method

In order to solve the above mentioned problem first, the literature review is carried out to identify the security and privacy requirements of vehicular networks. This set of requirements then help us determine as to how these can be achieved. Also, we identify the different types of attacks that can be launched in VANETs and how these attacks can be detected and prevented. We then develop a VANET model that can be used to predict their behaviour in normal or special conditions. This enables us to automate the detection of anomalies in VANETs using various techniques. The model is then validated with the help of simulations under different conditions. Different techniques are tested and the best method is selected to detect malicious behaviour in VANETs.

## 1.5 Contributions

Securing VANETs is a difficult task as the nodes are fast moving, connections are short lived and the topology of the network changes very quickly. There is a requirement for nodes to establish connections and trust each other for information exchange. This thesis also proposes and presents some solutions and techniques to help solve these issues. The research presented in this thesis has been published in [6], [7], [8] and [9]. This thesis makes the following original contributions:

i. **Application of a traffic model to VANETs to help detect rogue nodes and make them resilient to false data injection:**

This thesis presents and implements a VANET model through which vehicles share their own calculated parameters about the traffic which help others to determine the highway conditions. The vehicles which are close together will measure similar parameters and share them to develop a consensus about the road conditions. Each vehicle can compare the values being received from other vehicles and averages them to form a generalized picture of the road conditions ahead. Moreover, each vehicle will compare the values received with the VANET model and only accept them if they conform to it. In this way, inconsistent values can be detected and reported. If the parameters don’t conform to the VANET model and inconsistent values are being received from only one or few vehicles then they are flagged as rogue.

This thesis proposes that vehicles do not accept and re-broadcast an emergency message as soon as it is received but only do so if the parameters validate the emergency message. This means that the system works better as only vehicles that are in (or very close to) the incident region will send out the emergency message and other vehicles that are far away will only prompt other vehicles to slow down. Thus, the system will allow the information to be carried at large distances and at the same time a gradual reduction in speed is allowed.

ii. **Propose an Intrusion Detection System (IDS) for Vehicular Ad hoc Networks to detect and identify rogue nodes.**

This thesis proposes a host based IDS for VANETs that resides on each node (vehicle) that can detect intrusions in the network. The IDS uses statistical techniques to detect intrusions in the network and then identify the rogue nodes. The IDS is tested through simulations and results are presented and discussed. The results show that the proposed IDS works very well even in the presence of a high number (up to 40%) of rogue or malicious nodes.

### iii. Evaluating our proposed false data rejection and rogue node detection technique using OMNET++, SUMO and VACaMobil:

We evaluate our proposed technique that detects and rejects false data and detects rogue node sending the data using OMNET++, SUMO and VACAMOBIL. OMNET++ is a modular, component based C++ library and framework for the simulation of networks (wired and wireless). OMNET++ offers an eclipse based IDE and many useful data analysis tools. Simulation of Urban Mobility (SUMO) is a tool used to generate vehicular traffic and VACaMobil is a VANET Car Mobility manager for OMNET++ that uses SUMO to offer a comprehensive range of VANET simulations.

### iv. Propose a new method to create and use the Digital Identity in VANETs:

In order to keep the rogue nodes out of VANETs in the first place, it is necessary to devise a mechanism that properly authenticates the user before allowing him to become a part of the system. The thesis proposes a new way to form digital identities in VANETs so that the actual user of a vehicle can be held accountable for their actions and not the vehicle. As the vehicle usually has a one to many relationships with drivers, therefore, if the vehicle is identified and revoked then the driver can later on deny using the vehicle. Therefore, it is the driver who needs to be identified and penalised and not the vehicle. The OBUs use this digital identity to create their own Pseudonyms that are changed frequently but still be authenticated by the Trusted Authorities or Road Side Units. This will ensure that once the driver has been identified, he can be penalized for their actions.

Also, we propose a new multi-authority framework which splits the power to disclose the identity of a user to two authorities that have to work together to de-anonymize a user. This is done to provide an additional layer of security for the user as the existing works give this ability to either the RSU or a single TA which if compromised can completely reveal a user’s identity.

**v. Propose a Game Theoretic model to detect Sybil nodes in VANETs:**

Sybil attack is a serious threat to the working of VANETs. Sybil attack is directly related to the unfair use of the identity or identities in VANETs. Sybil attacks are difficult to detect in any network but increasingly so in the case of VANETs due to their inherent nature. In this thesis, a game theoretic framework for Sybil attack detection is proposed that models such a situation in VANETs as a game and is able to detect the malicious node and the Sybil nodes in most cases.

## 1.6 Assumptions and Scope

There are certain assumptions that have been made while formulating the research questions, proposing solutions for problems and while setting up and running simulations. These assumptions are discussed here:

**i. Not Dependent on Tamper Proof Device**

This research does not depend on and does not assume Tamper Proof Devices (TPD) or Trusted Platform Module (TPM) installed in vehicles. The primary reason for this is to keep the research and solutions as wide as possible and also because dependence on such hardware raises the cost of the vehicles and also limits the solutions. Moreover, it raises some other questions as well such as; what if a vehicle has not one but multiple devices connected to radios (thereby claiming multiple identities).

### ii. Interference in Communication:

Interference in Vehicle to Vehicle (V2V) communication and Vehicle to Infrastructure (V2I) has been ignored in this research. The reason for this is that this research work focuses on the security and privacy aspects of the communication and doesn't directly deal with the channel characteristics.

### iii. Bootstrapping Problem:

The proposed Intrusion Detection System (IDS) has the ability to get up and running quickly i.e. it has the ability to load up and start taking decisions quickly. The IDS can start taking correct decisions after just a few (seven) communication exchanges with other vehicles. This is acceptable as this can be done in as little as 700 ms (0.7 sec).

### iv. Rogue Nodes / Users:

The rogue node / user in this thesis is assumed to be either a malicious user who has the intention to disturb the network by sending out false information or a node with faulty sensors. The malicious user sends false information to other nodes in order to paint a false picture of the traffic up ahead for various reasons. This could be to indicate congestion up ahead so as to cause other vehicles behind it to change route or to claim a false identity such as that of an emergency vehicle in order to free up the road for themselves. Similarly, a node with faulty sensors can do similar damage without knowing and therefore, they are also considered rogue nodes in this thesis. The Greenshield's traffic model applied to VANETs and the averaging of the data received from all nodes in the vicinity enables the proposed IDS to be able to detect anomalies. Moreover, we are proposing that vehicles do not broadcast a received emergency message as is proposed in other works as this raises many problems for the bandwidth limited channel.

Consider as an example a vehicle that tries to send a **false** 'Emergency Braking' message to all vehicles behind it in order to cause chaos. Now, this rogue vehicle has to be a certain distance away from the targeted vehicles in order for them to **fall** for it as otherwise the vehicles would experience or not experience the braking event themselves as well. When the rogue node sends the false emergency message, then there can be other vehicles in its vicinity that should have also experienced the emergency event and would send similar emergency message. If such an emergency message is only coming from one vehicle then it will be suspicious. Also, if the rogue vehicle is sending such a false message from quite further up ahead the road then other vehicles in between should have experienced the effects of a real braking event and their parameter values should have gone down as well. If this is not the case then again the emergence message is false.

### v. Security of Vehicle Control Systems

This thesis does not deal with the security of vehicle control systems i.e. doesn’t address the security issues associated with the hacking of autonomous vehicles and is out of scope of this thesis. This thesis deals with security and privacy of the users and their communications only.

## 1.7 Thesis Outline

The thesis is structured as follows:

**Chapter 2** presents the introduction to VANETs, its applications, the possibilities and its architecture. The standards and proposed protocols are discussed in detail.

**Chapter 3** discusses the security and privacy issues in wireless ad hoc networks in general and VANETs in particular. It discusses different types of attacks and possible precautions. It also discusses the roles and responsibilities of different entities and the security and privacy requirements from different perspectives. The current and past work done in security and privacy for VANETs is also reviewed.

**Chapter 4** presents the proposed technique to make VANETs resilient against false data injection with the help of a data centric scheme. The chapter provides details on the applied VANET model and the data aggregation and dissemination techniques proposed. The details on the simulation parameters and the result obtained are presented and discussed in detail.

**Chapter 5** presents the proposed Intrusion Detection System (IDS) for VANETs. The IDS uses statistical techniques to detect rogue node in the network. The IDS is tested by simulations under different conditions and parameters and compared to other recent works.

**Chapter 6** presents the proposed framework for creating and managing digital identities in VANETs. It uses the Identity Based Encryption technique using the proposed digital identity to encrypt the Vehicle to Infrastructure communication (V2I). Also, Sybil attacks in VANETs which are linked to the identity management in VANETs are discussed and a game theoretic framework for their detection is presented.

**Chapter 7** summarizes the work done in this thesis, gives the conclusion and recommends the future work that needs to be done in order to take this work further.

# Chapter 2 : Background

## 2.1 Wireless Ad hoc Networks

Wireless ad hoc networks have been the subject of research for the last two decades now. They are decentralized networks that are connected wirelessly. They have been immensely popular both in the industry and military applications because of their ease of deployment, robustness, scalability, low cost and data acquisition capabilities. They do not require any infrastructure like routers in wired networks. Instead of routers, the network functions by allowing nodes to forward data to / for other nodes. Therefore, the nodes form a route dynamically based on the availability of the nodes. This means that efficient and dynamic routing protocols are very important for wireless ad hoc networks. In such a case, flooding can also be used to forward the data but this obviously results in congestion in the network. Ad hoc networks often refer to the IEEE 802.11 mode of wireless networks. Wireless ad hoc networks are limited in their capability due to the limited computing, storage and power requirements of the nodes.

## 2.2 Mobile Ad hoc Networks (MANETs)

Mobile Ad hoc network (MANET) is a type of wireless ad hoc network in which the nodes are allowed to move freely and independently in any direction. As all the nodes are moving, therefore, the topology of the network changes quickly and frequently. Similar to wireless ad hoc networks, MANETs are self-configuring and form dynamic links to other nodes to convey information in the network. The nodes can communicate with each other via multiple hops. The nodes are usually slow moving and have a range of a few meters.

## 2.3 Vehicular Ad hoc Networks (VANETs)

Vehicular Ad hoc networks (VANETs) are a type of MANETs in which vehicles form a network to communicate with each other via radios and sometimes with the help of road side infrastructure. VANETs have the potential to make our roads safer by allowing vehicles to communicate with other vehicles on the road and therefore, allow them to share any safety related information amongst themselves. Road safety is just one aspect of VANETs; there are numerous other applications which have been proposed by researchers and some have already started taking shape.

Vehicular Ad hoc Networks (VANETs) have received a lot of attention from the research community in the last few years primarily because they are being seen as not only necessary but imminent. The advancements in sensors and wireless technology in the last decade have been remarkable but they have not done much to improve the safety of the highways. Moreover, it's both obvious and logical that equipping vehicles with sensors and allowing them to communicate with each other can help in many hazardous situations like fog, slippery roads and accidents ahead on highways.

It is only a matter of time before vehicular networks become a reality. Recently, AT&T and GM have signed a deal to work on connected together. The vehicles will have 4G / LTE connectivity providing super-fast telematics services. AT&T believes it can be worth one billion dollars in revenue eventually [10]. This will provide the enabling technology for the interconnection of vehicles to form VANETs. With this imminent arrival of VANETs, it becomes necessary to ensure that the implementation of VANET is practical and provides some immediate benefit to all the stakeholders namely the users, service providers (i.e. insurance companies etc.) and the authorities.

### 2.3.1 VANET Applications:

Many different convenience and commercial applications have been proposed for VANETs by researchers in [11], [12], [13] and safety applications proposed by the Vehicle Safety Communications Consortium (VSC) of the Department of Transportation in [14]. Some of the applications that have been recommended and considered for VANETs are:

i. **Safety Applications:** Notifications for crashes, hazards on the roads (slippery or wet road conditions), traffic violation warning, curve speed warning, emergency electronics brake light, pre-crash sensing, co-operative forward collision warning etc.

ii. **Convenience Applications:** Navigation, Personal routing etc., Congestion advice, toll collection, parking availability info etc.

iii. **Commercial Applications:** includes entertainment and information exchange applications such as location based services.

### 2.3.2 Differences between VANETs and MANETs

VANETs can be classified as a sub class of Mobile ad hoc Networks (MANETs) but differ from them in the following ways:

i. In VANETs, nodes are fast moving and the topology of the network is changing very quickly.

ii. The nodes in VANETs are not constrained in terms of memory or processing power i.e. the OBUs have reasonable processing power.

iii. The nodes are equipped with on board batteries and therefore, are not constrained in terms of power.

### 2.3.3 VANET Architecture

The general architecture of a VANET is pretty much accepted as standard and consists of Road Side Units (RSUs) as part of the infrastructure, On Board Units (OBUs) which reside on the vehicles and a Trusted Authority (TA) which is responsible for Authentication. The OBUs are basically processors with reasonable amount of memory available. There is no problem of power for the OBU and the computing power available in OBU is assumed to be reasonable. The OBU and RSU enable the Vehicle to Infrastructure (V2I) or Vehicle to Roadside (V2R) communication and Vehicle to Vehicle (V2V) communication as shown in Figure 2-1.

#### *2.3.3.1 Road Side Unit (RSU):*

The RSUs are part of the infrastructure that communicate with the vehicles and are able to perform many supporting functions like authentication, information dissemination, revocation etc. The RSUs are at regular distance apart from each other and cover the whole length of the highway. The RSUs are connected to the TAs with the help of high speed links such as fibre optic cables. The RSUs have sufficient computing and storing capacity and power is also not an issue as they can be powered by solar cells.

#### *2.3.3.2 On Board Unit (OBU):*

The OBUs consist of a processor with reasonable computing power, sufficient memory and a radio to communicate with other OBUs and RSUs. Wireless Access in Vehicular Environment (WAVE) is based on IEEE 802.11p standard and provides the basic radio standard for Dedicated Short Range Communication (DSRC) in VANETs. DSRC is explained in detail below.

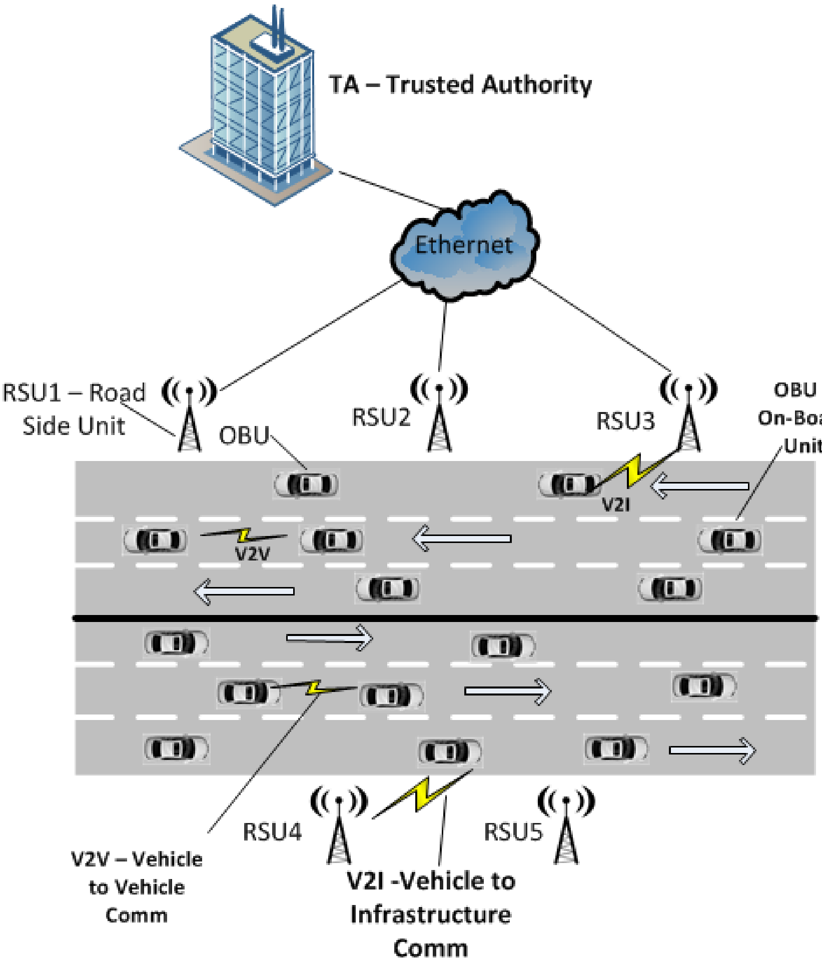


**Figure 2-1: VANET Architecture**

### *2.3.3.3 Trusted Authority (TA):*

The TA is the central authority that authenticates all vehicles. It keeps a record of all vehicles, drivers etc. and issues keys and certificates. There are no power, processing or memory limitations with the TA.

## 2.4 Communication Technologies for VANETs

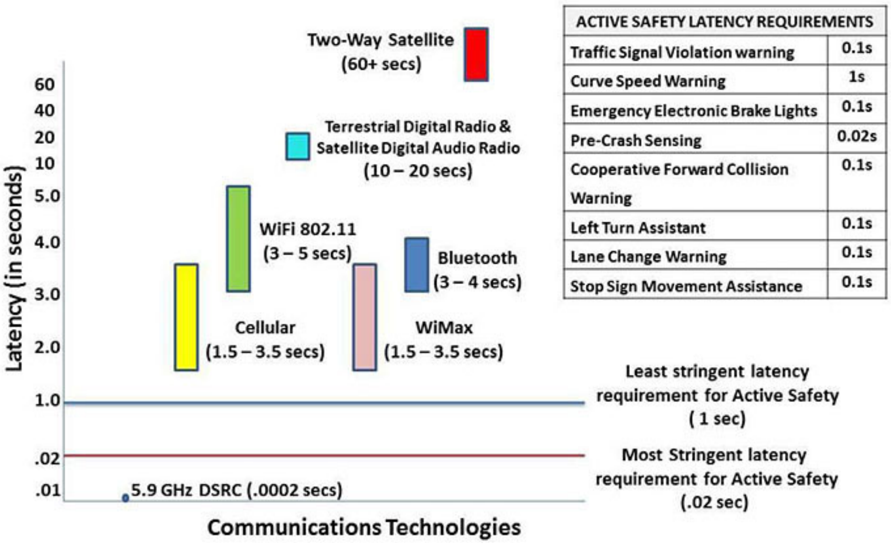
There are various wireless communication technologies that are available to be used in VANETs. These include Wi-Fi, WiMAX, 3G / 4G mobile technologies and Dedicated Short Range Communication (DSRC). We will look at DSRC in detail as it is specific to VANETs.

### 2.4.1 Dedicated Short Range Communication (DSRC)

Dedicated short range communication refers to two-way wireless communication channels specifically designed for automotive use based on the IEEE 802.11p standard. The 802.11p is the approved amended version of IEEE 802.11 for providing Wireless Access in Vehicular Environment (WAVE) to support Intelligent Transportation Systems (ITS). DSRC was designed specifically for the vehicular environment keeping in mind the stringent latency requirements of the safety applications. According to [15], DSRC is the only short range wireless technology that provides:

- Fast Network acquisition, low latency, high reliability communication link
- Can work with vehicles travelling at high speeds
- Prioritizing safety messages
- Tolerance to multipath interference
- Better performance in extreme weather conditions
- Protection of security and privacy

The latency requirement of different warning messages and the performance of DSRC in comparison with other communication technologies is shown below:



| ACTIVE SAFETY LATENCY REQUIREMENTS | |
|---|---|
| Traffic Signal Violation warning | 0.1s |
| Curve Speed Warning | 1s |
| Emergency Electronic Brake Lights | 0.1s |
| Pre-Crash Sensing | 0.02s |
| Cooperative Forward Collision Warning | 0.1s |
| Left Turn Assistant | 0.1s |
| Lane Change Warning | 0.1s |
| Stop Sign Movement Assistance | 0.1s |

**Figure 2-2: Latency Comparison of Communication Technologies [15]**

DSRC has been allocated 75 MHz in the 5.9 GHz band by the FCC in the US and a 30 MHz band has been allocated in the same band in Europe as well as shown in Table 2.1.

| S/No. | Region | Frequency (GHz) |
|---|---|---|
| 1. | North America | 5.85 - 5.925 |
| 2. | Europe | 5.795 - 5.815 |
| 3. | Japan | 5.770 - 5.850 |

**Table 2.1: DSRC Spectrum Allocation Worldwide**

Vehicles use DSRC radios to communicate with each other i.e. vehicle to vehicle (V2V) and with the infrastructure i.e. vehicle to infrastructure (V2I) communication. The communication range of DSRC is between 300 and 1000 meters. The DSRC spectrum is split into 7 channels of 10MHz each as shown in Figure 2-3 below.

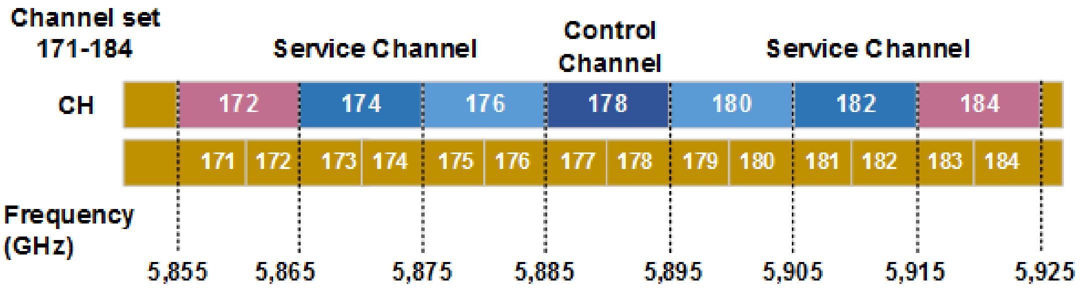


**Figure 2-3: Frequency Allocation in IEEE 802.11p [16]**

### 2.4.1.2 Wireless Access in Vehicular Environment (WAVE)

WAVE refers to the complete protocol stack of IEEE 802.11 and IEEE 1609 protocol family for vehicular environment as shown in Figure 2-4. A brief description of these standards is given below:

**IEEE 1609.1** is the resource manager and describes the key components of WAVE system architecture and the type of devices supported by OBUs.

**IEEE 1609.2** provides the security services for applications and management messages and defines secure messages formats and the circumstances in which they are used.

**IEEE 1609.3** defines network and transport layer services including addressing and routing. It also defines Wave Short Messages (WSM) that is an efficient alternative to IPv6.

**IEEE 1609.4** defines the enhancements to the 802.11 Medium Access Control (MAC) and Physical (PHY) layers to support multi-channel wireless communications.

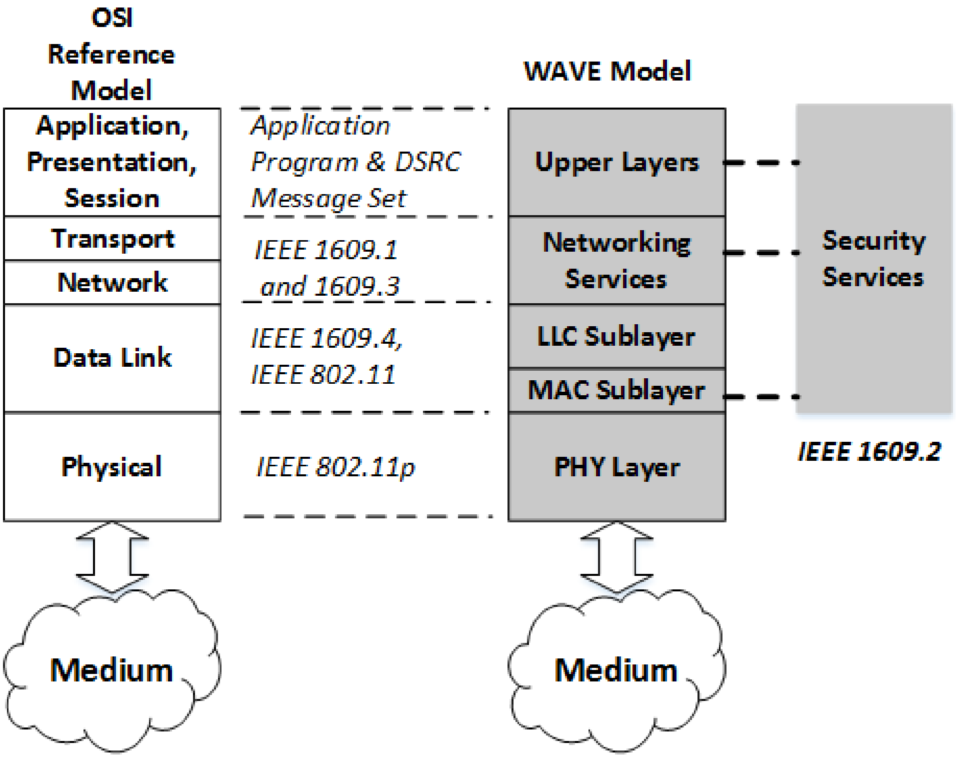


**Figure 2-4: OSI vs WAVE Protocol Stack [17]**

## 2.5 VANET Characteristics

VANETs have some unique characteristics that distinguish them from other wireless networks. These include:

### 2.5.1 High mobility

The vehicles in VANETs are highly mobile and moving at very high speeds. This mobility has serious implications for the working of VANETs. Some of the factors that must be taken into consideration due to high mobility are as follows:

#### 2.5.1.1 Low Latency

VANETs are dynamic and high speed networks where nodes rely on the information being exchanged to make suitable decisions. Due to the inherent nature of VANETs, it is necessary that the information being shared is acted upon quickly. Therefore, it is essential that processing times / latency is kept in mind in all aspects of planning so that it can be kept small so as to be effective in VANETs. The latency requirements in VANETs are in milliseconds which only DSRC can provide.

#### 2.5.1.2 Trust

In VANETs, vehicles come into contact for short periods of time and these interactions are short lived. Therefore, it is important that the data being shared is being received from trustworthy nodes. However, trust in VANETs can't be managed in the same way as it is done for other networks. The primary reason for this is that it is difficult to have an online central authority that keeps and manages the trust scores for all vehicles. Moreover, centralized solutions haven’t proved very efficient in other setups either.

#### 2.5.1.3 Reliability

Due to the short latency requirements in VANETs, it is important that the information being received is reliable, relevant and actionable.

### 2.5.2 Communication Range

The communication range in VANETs can be between 300m to 1000m depending on the transmission power selected. This range is quite big as compared to the other wireless networks and has some unique advantages and disadvantages associated with it that will be addressed in detail in the next chapter.

### 2.5.3 Storage and Computing Power

The storage and computing power are both abundant in OBUs in the vehicles. This abundance makes it possible to install applications of different types and enables a range of services in VANETs. However, these enhanced services also create security and privacy issues as each application has to follow a strict set of rules and procedures to ensure security and privacy of the user.

# Chapter 3：Security and Privacy

There has been a lot of research in the security and privacy of wireless networks and many different methods have been proposed. Most of the techniques presented are based on Public Key Infrastructure (PKI) i.e. the entity identifies and authenticates itself with a Certificate Authority (CA) / Trusted Authority (TA) and obtains keys which it uses to encrypt and decrypt messages.

## 3.1 Cryptographic Techniques

### 3.1.1 Symmetric Key Cryptography

The basic idea behind these algorithms is that there is a common shared secret between the sender and the receiver that is used to encrypt and decrypt the data. The shared key has to be transferred between the users via a secure channel and has to be kept secret from other users as anyone with the secret key is able to decrypt all data.

Symmetric key algorithms can be classified into stream ciphers and block ciphers. In stream cipher, a byte of data is encrypted at a time whereas in block ciphers a block (chunk) of data is encrypted in one go. The Advanced Encryption Standard (AES) currently uses 128 bit blocks.

Some of the popular Symmetric algorithms include Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4) and 3DES (Data Encryption Standard or Triple DES). AES replaced Data Encryption Standard (DES) in 2001 by National Institute of Standards and Technology (NIST) and approved by the National Security Agency (NSA) for top secret information. RC4 is a stream cipher that was fast and simple but various vulnerabilities lead to its prohibited use. The 3DES is a symmetric key block cipher that applies the DES three times to each cipher.

Symmetric algorithms are much faster than asymmetric algorithms but the shared secret keys need to be updated / changed regularly as the whole system is compromised if the key is leaked. Symmetric ciphers have in the past been susceptible to known-plaintext attacks, chosen plaintext attacks and cryptanalysis.

### 3.1.2 Asymmetric Key Cryptography

Asymmetric key cryptography, also referred to as Public key cryptography, uses two different keys (public and private keys) to encrypt and decrypt data. The two keys are mathematically related and form a pair. The idea is that the public key for each user is distributed to all other users with the help of which they can encrypt the data for the owner of the key and only the owner can decrypt it using his private key. The private key cannot be obtained from the public key. The private key can also be used to digitally sign messages which can be verified with the help of the public key of the user by the recipient. The asymmetric key cryptography relies on the difficulty of solving the mathematical problems that are inherent in elliptic curves, integer factorization and discrete logarithm relationships which are used to setup the shared key between the two users.

As mentioned before, the asymmetric key algorithms are slower than the symmetric key algorithms. The idea of asymmetric key cryptography was first published by Diffie and Hellman in 1976 [18].

RSA (Rivest, Shamir and Adleman) key exchange proposed in 1978 in [19] and DH (Diffie - Hellman) key exchange mechanisms solved the problem of exchanging symmetric keys securely i.e. they do not need a secure channel for the initial exchange of secret keys between the two parties. DH provides key distribution and secrecy, Digital Signature Algorithm (DSA) provides digital signatures and RSA provides both key distribution and secrecy. RSA is typically used in practice primarily because Verisign was a spin-off of RSA security which is the largest online Certificate Authority (CA). Verisign was acquired by Symantec in 2010.

### 3.1.3 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) [20] is another approach to implement PKI using the algebraic properties of elliptic curves. The main advantage of ECC, as compared to non-ECC schemes, is that it is able to provide the same level of security with a smaller key size. ECC algorithms can be used for encryption and digital signature generation.

Public Key Cryptography is based on the infeasibility of solving certain mathematical problems such as factorization of large prime numbers into its large prime factors. Similarly, in ECC it is assumed that finding the discrete logarithm of an elliptic curve given a publicly known base point is infeasible. This is known as the Elliptic Curve Discrete Logarithm Problem (ECDLP) [21].

The security of ECC depends on the feasibility of computing a point multiplication and the inability to find the multiplicand given the product points and original. This Point multiplication is defined as the operation of successively adding a point to itself repeatedly on an elliptic curve. E.g.

Given a curve $A = x^3 + cx + d$, point multiplication is defined as adding a point such as $P$ to itself repeatedly i.e. $nP = P + P + P + \ldots\ldots\ldots + P$

where $Q = nP$

and ECDLP is defined as the infeasibility to find $n$ given $Q$ and $P$.

The ECC has the ability to provide same level of security as RSA with a smaller key size. This reduces storage and transmission size and is also the main advantage to using ECC.

### 3.1.4 Identity Based Encryption

Identity Based Encryption (IBE) was first proposed by Shamir [22] in 1984 when he showed how a name or any identifier could be used as a public key. However, he was not able to give a practical demonstration of this. The first mathematical proof and practical demonstration was given by Boneh & Franklin in 2001 using bilinear maps [23]. Cocks, a mathematician in UK at GCHQ, had devised a similar scheme around the same time based on quadratic residues but it was kept classified. The working of IBE is explained below.

There are three entities in an IBE based system namely User1, User2 and a trusted third party known as the Private Key Generator (PKG). The PKG sets up the system parameters and the master public key but retains the private keys for the individual users. User1 (or anyone) can generate a public key for any identifier such as a name, telephone number, email id (belonging to User2) etc. using the published master key and encrypt the message using this key for User2. User2 can then authenticate itself to the PKG and obtain its private key to decrypt the message over a secure channel. This mechanism is shown in Figure 2.

IBE is a very useful crypto technique that is highly suitable for dynamic networks i.e. networks that are changing rapidly. It is also useful for forming dynamic coalitions i.e. networks that have to be setup quickly e.g. in an emergency where pre-distribution of keys is not possible. Other benefits of IBE include ease of use and management as public keys are derived from identifiers; there is no need of a public key infrastructure or distribution. Also, there is a possibility of sending an encrypted message with an expiry timestamp. This enables the sender to define a lifetime of the message sent to the recipient.

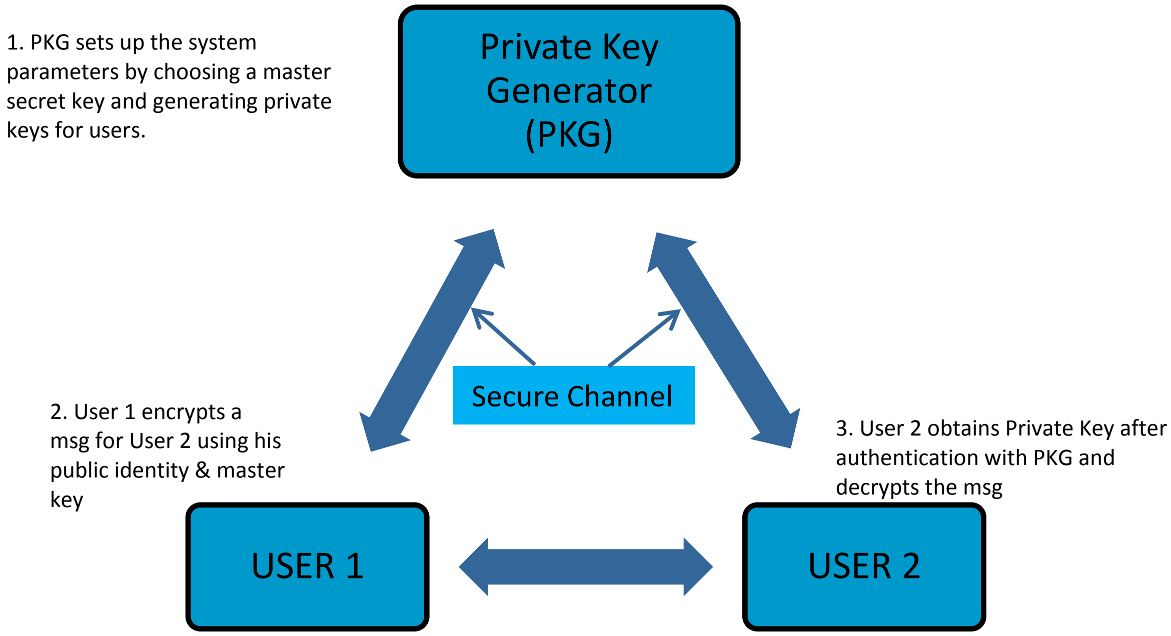

1. PKG sets up the system parameters by choosing a master secret key and generating private keys for users.
Private Key Generator (PKG)
Secure Channel
2. User 1 encrypts a msg for User 2 using his public identity & master key
3. User 2 obtains Private Key after authentication with PKG and decrypts the msg
USER 1
USER 2

**Figure 3-1: Identity Based Encryption (IBE) Working**

There are some drawbacks of IBE as well. First, if the PKG is compromised then all messages encrypted over the lifetime of the public / private key pair are also compromised. Also, a secure channel is required between the user and the PKG for transmitting the private key.

## 3.2 Security and Privacy in VANETs

Vehicles are exchanging information with each other so that they are informed of the road traffic conditions. In the applications discussed above, the vehicles are sharing information in V2V & V2I communications. This information includes their position as well as information about road conditions. Furthermore, in VANETS a driver may need to take lifesaving decisions based on the information received (e.g. emergency brake light, forward collision warning). It is therefore, necessary that the reliability, integrity and most importantly the timeliness of the messages are ensured so that action can be taken on the received information in a split second due to the speeds involved in case of vehicles.

The area of security and privacy in VANETs has received significant attention from researchers as it is considered to be the weakest link in the architecture. The VANET architecture consists of RSUs as part of the infrastructure and OBUs which reside on the vehicles and a Trusted Authority (TA) which is responsible for authentication.

There are many different convenience and commercial applications that have been proposed for VANETs by researchers in [11], [12] and [13] and safety applications proposed by the Vehicle Safety Communications Consortium (VSC) of the Department of Transportation USA in [14]. Some of the applications that have been recommended for VANETs include traffic violation warning, emergency electronics brake light, forward collision warning, road conditions, traffic updates, navigation, parking availability, vehicle diagnostics and different location based services.

Authentication and non-repudiation is achieved by digital signatures as described in [24], [25], and [26]. Many different schemes have been proposed including Public Key Infrastructure (PKI) in [27] , [28] and elliptic curve crypto system (ECC) based PKI in [29]. ECC is considered computationally efficient as compared to RSA and has a smaller key size [30]. Privacy is achieved by using Pseudonyms (PN) or anonymous public and private key pairs to sign messages or by using group signatures [31]. In group signatures only one member of a group communicates at a time on behalf of the group so the identity of all members of group remains safe. However, group signatures are considered to be quite expensive in terms of computation [26] and infeasible for OBU [32].

The PNs or public and private key pairs can only be used once which means the OBU has to store them in large numbers. This raises the question of how to replenish them in the OBU once they have been used up. Furthermore, revocation is a serious issue in using PNs and public / private key pairs e.g. if a vehicle is revoked then all the PNs or public and private key pairs have to be revoked [25], [26] and added to a Revocation List (RL). Therefore, if a single vehicle is revoked then there might be several thousand entries added to the list [33]. This growing RL can cause serious problems at the RSU when verifying hundreds or thousands of messages every 300ms (as dictated by VSC [14]).

## 3.3 Security and Privacy Requirements in VANETs

Security and privacy are serious issues in vehicular communications. A lot of research has gone into debating the requirements of security and privacy in VANETs. In [32], [25], [34]. [35], [36], [37] and [38] authors have identified various security and privacy requirements for VANETs. We further categorize and group the main security and privacy requirements and how they are achieved in VANET as shown in Figure 3-2 and explained below.

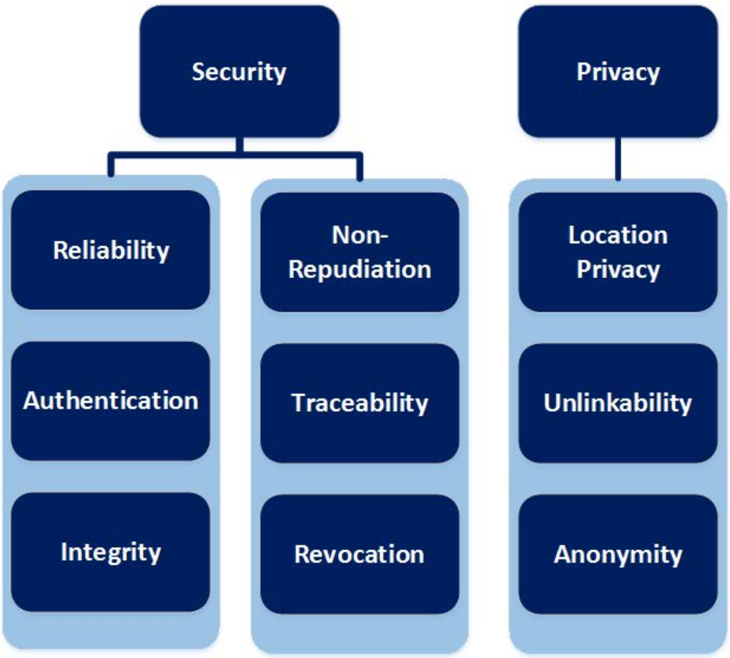


**Figure 3-2: Security and Privacy Requirements in VANETs**

### 3.3.1 Reliability:

Reliability is achieved through authentication by confirming the identity of the user and issuing them keys when they are authenticated. Authentication ensures that user is who he says he is and the message has not been tampered while in transit i.e. it ensures integrity of messages. Therefore, authentication ensures reliability. This means that if a user is authenticated as an emergency services vehicle e.g. ambulance, fire brigade, police etc. then they are indeed valid official vehicles and no one else can pose as such (an impersonation attack [28], [31]). Similarly, no private vehicle should be able to pose as anybody else. Furthermore, the contents of messages being sent out by any vehicle on the road can’t be changed without being noticed.

### 3.3.2 Location Privacy:

In [32], authors define linkability as the continuous or long term tracking of any user in a VANET by monitoring the transmissions or the information being exchanged in VANETs. This is undesirable in VANETs and is defined as breach of privacy. Nobody wants to be tracked or monitored so that their personal information or knowledge of their whereabouts could not be used for the wrong reasons. Therefore, preserving the location privacy of users is of fundamental importance in VANETs. This implies that the consecutive messages being sent by a user should not be linked to the same user. This is defined as unlinkability that helps achieve anonymity as shown in Figure 3-2. This means that a user should be able to send multiple messages anonymously. This anonymity is usually achieved by using PNs that are changed with every message or after some time. The anonymity is conditional rather than absolute meaning it can be revoked if the user is involved in a violation.

### 3.3.3 Non-Repudiation:

Non-repudiation means the sender of a message should not be able to deny sending it. Non-repudiation leads to traceability i.e. the ability of the authorities to trace a user involved in a violation. This traceability usually leads to revocation which means de-anonymizing the user and taking some action against the user. The violation may invoke revocation if it is a serious violation e.g. a vehicle sends out a malicious message to the vehicles on the same highway that there is a traffic jam on the road ahead with the intent to clear the road for him [28], [33], [39].

## 3.4 Attacks in VANETs

### 3.4.1 Sybil Attack

A Sybil attack is the ability of a single entity to claim multiple false or valid identities in a network without being detected. The attacker is then able to control a significant part of the network and can perform various malicious activities including out voting a valid / legitimate user and injecting false information in the network. Sybil attacks in VANETs have been discussed in [40], [41], [42], [43], [41] and [44]. The concept of valid identity in a network refers to distinct identities, which mean that one entity can be differentiated from the other. However, researchers have argued that it is impossible to present convincingly distinct identities for initially unknown elements in a distributed computing environment without the presence of a central certification authority [45]. Therefore, one approach to preventing such attacks is to have a trusted agency that certifies identities. However, having an online trusted authority that is accessible everywhere is not an easy task.

### 3.4.2 False Information Injection Attack

In VANETs, once nodes have been authenticated, they can share information with other nodes. However, once nodes are allowed to share information and a node becomes rogue then there is no quick way to detect or stop this node from injecting false information in the network. This kind of attack is the most serious and easiest to launch in VANETs and have been discussed in [46], [47], [48], [49] and [8]. In VANETs, there are some emergency messages, which are exchanged e.g. emergency braking, traffic light violation etc. that can cause other users to take drastic actions and may put lives in danger. Once the information is determined to be false then the sender can be penalised but a procedure is needed that allows the receivers to find out if false information has indeed been injected in the network and by whom.

### 3.4.3 Wormhole Attack

The wormhole attacks in VANETs have been discussed in [50] and [38]. In wormhole attack an attacker records a message that was received at one location, and retransmits it to another location. This makes other nodes believe that the original sender of the message is within their communication range and they might try to route their message through this node which will fail. This attack thus prevents discovery of other routes other than the wormhole as the nodes try to select the route with the fewest hops. Moreover, this can result in wrong information being shared in VANETs causing chaos.

### 3.4.4 Denial of Service (DoS) Attack

The DoS attack is considered very serious in any kind of network i.e. wired or wireless. However, it can have life threatening consequences in VANETs. DoS attack in VANETs are discussed in [51], [52], [53] and [54]. A DoS attack basically makes a network unavailable for legitimate users by broadcasting continuously and thus using up all the bandwidth. The main aim of the attacker is to consume the network resource (bandwidth) so that other users can't access the network services. In VANETs, the attacker can launch such an attack by continuously broadcasting using single or multiple radios so that access to the network can be denied in a particular area. As bandwidth is already limited in VANETs, such an attack can be devastating as vehicles keep themselves aware of their surroundings by exchanging Cooperative Awareness Messages (CAM).

## 3.5 Security and Privacy Preserving Schemes in VANETs

In order to cater for the transmission of location information: confidentiality of location of a user (Location Privacy) is essential for VANET security. This location information can be used by adversaries in tracking vehicles or routes. Different security schemes have been used to protect privacy or achieve anonymity and based on the underlying security mechanisms they use, these schemes can be classified as:

- Pseudonyms coupled with Public Key Infrastructure (PKI)
- Trust Based schemes
- Group signatures
- Identity based signature schemes.
- K-anonymity schemes.

There are various issues associated with each of these schemes which we will discuss in the next section.

### 3.5.1 Pseudonym coupled with PKI Based Schemes

In VANETs, the vehicles are transmitting their location info e.g. to warn other users of accidents. Researchers in [24] & [26] propose using pseudonyms to preserve privacy. The use of Pseudonyms (PNs) hides the real identity of the user and prevents the linking of real-ID of the user with the pseudonyms thereby providing Unlinkability. However, Trusted Authority (TA) which issues pseudonyms can reveal the real ID of the user if user commits an illegal act hence providing Traceability.

In all cases, the On Board Unit (OBU) is assumed to be a tamper-proof device which contains the unique Vehicle Identification Number or VIN. This VIN is tied to an identity certificate at the time of registration. From here on, the Trusted Authority (TA) (e.g., transport authority) is tasked with issuing new blocks of pseudonyms / certificates to the vehicles, to be used while communicating with the Road Side Units (RSUs). These certificates have a validity period and the vehicle switches its pseudonyms to ensure privacy. The authors in [32] suggest that short-term linkability should be allowed so that the receiver is able to verify that two or more messages in a short time frame have come from the same sender, as this might be required by applications. The recommended time after which the pseudonyms are switched also varies, e.g., every minute or every few minutes, with every message or every second [53]. However, the frequency of PN changes is directly proportional to the computation overhead at the RSU, which can slow down packet delivery. Also, the OBU is also supposed to store the public keys of all CA (Certificate Authority) / TA. Furthermore, different PKI-based techniques that use a CA/TA connected with the RSU have been suggested.

The downside of the pseudonym scheme is that the user (OBU) has to have hundreds or thousands of these pseudonyms stored on board and they need to be refreshed after some time (e.g., once a year). Different papers have explored this and proposed different methods of refreshing these, e.g., downloading new pseudonyms when the vehicles go in for service (once a year). It is also suggested that the pseudonyms are refilled at social spots [26]. In [54], a PN distribution scheme is proposed, which incorporates control channels and service channel intervals in communication between vehicle and RSU for PN refill. It is important to note that pseudonym schemes alone do not support authentication, integrity, and non-repudiation. Signing protocols have been proposed that provide integrity and authentication. In this, a large number of certified public-private key pairs are stored in the OBU. Each key pair is used for a short period of time and then discarded. Using PKI involves downloading and maintaining public key certificates, which results in heavy computational overhead that is not desirable in VANETs as the computing power of OBU is limited.

Anonymous certificates in PKI-based schemes can guarantee identity privacy but cannot guarantee location privacy. This is because an attacker can monitor the certificate change by a vehicle between two observation points while moving in the same lane with the same speed. Also, the TA/CA has the ability/capability to identify the real identity of a vehicle based on its anonymous certificate. In [6], a method has been proposed so that multiple authorities are required to de-anonymize a user to increase the security. In [55], authors propose that the users change their PNs only at predetermined locations (mix zones) where the density of vehicles is high and the speed and direction of vehicles changes often. However, the authors conclude that such a technique provides limited privacy due to the inherent lack of randomness in vehicle mobility.

A major drawback of using PN is maintaining the Certificate Revocation List (CRL), which keeps track of revoked certificates of misbehaving vehicles. This list then has to be checked to ensure whether a vehicle is revoked or not, which is both time- and resource-consuming. Authors in [53] propose a reduction in CRL size by limiting the list to regions, i.e., each RTA will maintain its own CRL, thereby reducing the size of each CRL.

### 3.5.2 Trust Based Schemes

Trust based security schemes have been proposed for VANETs by researchers in [56] and [57]. Trust based schemes involve attaching a trust score to each vehicle. The trust could either be central or self-organizing. Centralized trust means keeping and managing a centralized system that keeps a record of these trust scores. Self-organizing trust means assigning a score to users based on current or past interactions either directly or indirectly. Centralized trust management is problematic as it is difficult to maintain the list of all users and provide efficient and quick access to it. Another problem with trust schemes is that a new user would have to be given a default trust score. Also, once a group of vehicles form a network, it is then difficult to protect oneself from an insider. This is because an insider can transmit false information messages and emergency messages which will be accepted as it is a trusted node. To account for this, data-centric trust schemes have been suggested in [58], where a malicious node can be identified based on the data/information being exchanged. In [8], a data-centric mechanism is proposed that enables users to aggregate the data and then determine if a rogue is sending false data. The rogue node can then be reported and its data is ignored. Data Centric schemes are discussed in detail in the next chapter.

VANETs share many characteristics with Mobile *Ad-Hoc* Networks (MANETs). Trust-based routing schemes have been proposed for MANETs and the same idea of trust has also been applied to VANETs in [59], [57], [56]. However, apart from a lot of similarities between them, e.g., decentralized system, mobility, and openness, VANETs are different as they consist of a much larger number of nodes and their topology changes quickly as vehicles move fast [60]. Therefore, forming a network based on the trustworthiness of vehicles is quite challenging. In MANETs, the focus is on reliable packet delivery, whereas in VANETs the aim is to increase road safety and, therefore, the decision-making process has to be very fast due to the high speeds and limited time involved.

In [61], authors propose trust establishment through infrastructure or in a self-organizing manner. The former means to use a central authority or security infrastructure and the latter involves developing a trust score dynamically. In infrastructure-based trust establishment, there has to be a centralized authority, but it is very difficult to do that quickly in VANETs due to the size and time restrictions. In self-organizing trust establishment, the trust is based on the direct (self-interaction), indirect (receiving interaction information from other nodes), and hybrid approaches (combination of the two) as shown in Figure 3-3.

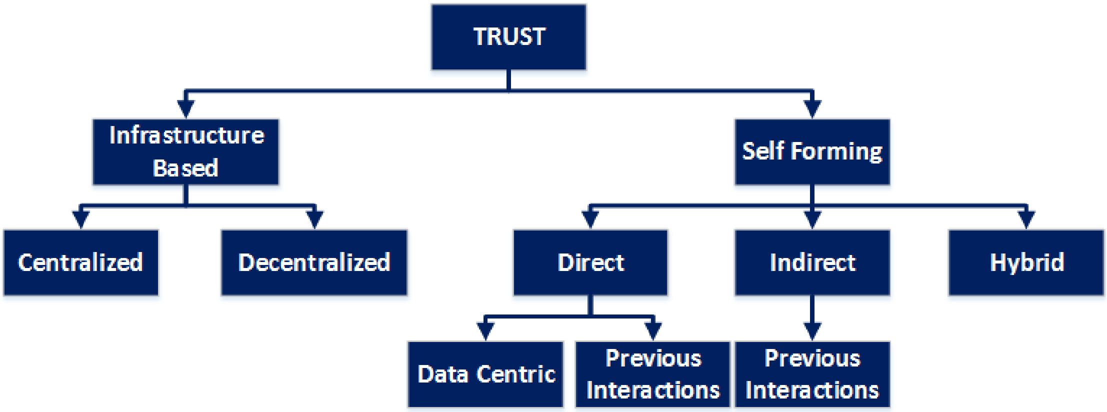


**Figure 3-3: Classification of trust establishment approaches**

### 3.5.3 Group Signatures

For VANETs, researchers have proposed grouping of vehicles travelling at the same speed and in the same direction. This allows group members to anonymously issue messages and signing them with the group signature on behalf of the group. This also allows extended silent periods for vehicles as only one vehicle in the network transmits at a time. By combining the vehicles into groups the authors proposed that a vehicle can reduce its V2I transmission which enhances the anonymity of vehicles. Group signatures allow distribution of a group public key associated with multiple group private keys. Therefore, an attacker will be able to detect that a message has been sent by a particular group but it won't be able to identify which vehicle sent the message [61].

In [32] a scheme based on group signatures and short lived keys is presented called temporary Anonymous Certified Keys (TACS) as an efficient way to fulfil the privacy & safety requirements. The scheme suggests a long term group key stored in the OBU provided by a Managing Authority which the OBU uses anonymously to prove to the RA that it is a valid OBU and get short term certified key which is only valid in that RA’s region. As soon as the OBU moves into a new region, it has to update its TACK by getting a new short lived certified key from the new RA. This ensures that OBUs update their keys after entering a new region. This ensures short-term linkability and Traceability in the long run as the Managing Authority can be queried by the RA for the real identity of the vehicle.

Group signatures provide a high level of privacy but revocation becomes a serious problem when the size of the group increases, thereby raising scalability issues. Furthermore, they can be computationally more expensive [62].

### 3.5.4 Identity Based Encryption Using Pseudonyms

Identity-based encryption (IBE) was first proposed in [22]. Identity-based cryptography allows the public key of an entity to be derived from its public identity information such as name, email address, or VIN, etc. Anybody who wants to send a message to a user can use the recipient’s identity to get their public key and encrypt the message using this key, which can only be decrypted by the private key of the intended recipient. A private key generator (PKG) is used to generate and distribute private keys for users (through a secure channel) and also to distribute the public key. IBE is highly suited to a dynamic ad hoc network like VANETs, as it allows nodes that have not met before to start communicating with each other quickly and safely.

The authors in [6], [63], [64] have used the idea of IBE in VANETs. The proposed architecture in [64] consists of four entities, two TAs which are trace authority (TRA), a PKG, an RSU at the roadside and mobile OBUs on vehicles. Privacy in IBE schemes is achieved by using pseudonyms that the user can request from the TRA. The TRA is responsible for registration of RSUs and OBUs, and can reveal the actual identity of the signing OBU. The PKG is responsible for generating and assigning private keys for OBUs and RSUs. Self-generating pseudonyms (PNs) are suggested for privacy preservation. For authentication, a pool of PNs is preloaded into a vehicle for different regional trusted authorities (RTAs). Users from different regions can authenticate each other via RTAs. RTAs are responsible for generating cryptographic key materials for the RSUs and the vehicles in the region and deliver them over secure channels. The users use their self-generated pseudonyms as identifiers instead of real-world identities. Similarly, the idea of IBE is used in [63] to improve the performance and reduce the processing time of RSU when it is verifying signatures for a large number of users.

Identity-based cryptography seems to be a good candidate for security and privacy in VANETs but has its own limitation and challenges, especially with revocation, which is still a major problem and is open for research. Secure channels for secret key distribution and heavy computation costs are other factors to consider. However, IBE is suited to a dynamic network such as VANET as there is no need for distribution and storage of certificates / keys to the users. Moreover, the master key can be changed regularly to keep revocations in check.

### 3.5.5 k-Anonymity Schemes

K-anonymity is a property of some anonymized data such that the individuals to whom the data belongs can't be identified. Researchers have proposed k-anonymity schemes for VANETs. In [65], a k-anonymity scheme has been proposed where k vehicles in a region are assigned the same PN for communicating with the RSU. This ensures that an attacker cannot associate a message with a specific vehicle. An attacker can only detect that a group of nodes are receiving the messages but cannot determine which one in particular. The source and destination anonymity cannot be guaranteed as VANETs are inherently changing all the time, therefore, it is difficult to identify the source and destination. In k-anonymity schemes, when a message has to be delivered to a vehicle, the region is flooded with the message to ensure that it reaches the destination vehicle.

K-anonymity schemes provide privacy preservation but in a multi-hop scheme (VANETs) there is a clear problem of the scarce bandwidth resource utilization. The network might be flooded by the same message, causing congestion which is highly undesirable in VANETs.

## 3.6 Performance Comparison

In order to compare the performance of different schemes discussed in this thesis, it is necessary to have complete details of the algorithms proposed for all the schemes. One parameter that can be used to judge the performance of networks is communication overhead, but in order to calculate this, it is necessary to know the exact type and size of data that the OBU will be handling. This can only be obtained after finalizing the type of applications that will be deployed in VANETs. Similarly, bandwidth utilization is another important parameter that has to be taken into account, but it is difficult to calculate it as the type of data and applications in VANETs have not been finalized. Therefore, we have compared the major performance characteristics of the discussed schemes by defining or modifying some parameters in Table 3.1 and we have discussed the major features and disadvantages of each scheme in Table 3.2. For comparison of the schemes discussed, we have used the rating system of HIGH, MED, and LOW in Table 3.1. The performance metrics used in Table 3.1 are described below:

### 3.6.1 Scalability

Scalability is a well-defined performance metric for network protocols and architectures and it means how well a system can cope with the expansion of the network while maintaining the performance standards. A LOW in this category means that the scheme is not suitable for a network in which the number of nodes can grow beyond a small number. A MED in this category means that the scheme can work well for a limited number of nodes but it should not exceed that limit. A HIGH means that the scheme is highly scalable and can work well for a very large number of nodes.

### 3.6.2 Computing cost

The computing cost i.e. the cost of running the protocol on the CPU has been chosen as a metric because it is always in demand and usually it is always less than what is desired. Furthermore, experience has shown that the appetite of programs and data eats up the computing power available very quickly. We have considered the computing cost in the CPU at both the RSU and OBU. This metric is especially important at the OBU end where we can have reasonable, but never excessive, computing power. A LOW here means that the computing resources (CPU) required are much less than available. HIGH means that computing resources available might fall short of what is required. Similarly, MED means that the computation resources are sufficient.

### 3.6.3 Privacy

This is the fundamental requirement of all schemes studied and has been rated according to the merits and demerits of each when viewed in its entirety, e.g., in the case of pseudonym cum PKI schemes, the privacy has been rated as MED as the PNs changing and their maintenance poses a serious challenge for the successful deployment in VANETs. HIGH means strong, MED means acceptable but risky, and LOW means unacceptable or no level of privacy.

### 3.6.4 Latency

This is another well-known parameter for networks that means delays which are experienced in a network due to any reason. A network with LOW latency is considered to be fast and vice versa.

### 3.6.5 Cost of deployment

This parameter indicates whether the infrastructure requirements make it easy to deploy in the practical world or not. A scheme with HIGH cost of deployment is high-cost and difficult to deploy, i.e., with many additions/changes to the existing network making it impractical. A scheme which gets a LOW in this metric will be low-cost to deploy and will require a few changes to the existing network to make it feasible. The high cost is due to the deployment of infrastructure such as RSUs which will add significant cost to the overall deployment.

**Table 3.1: Comparison Based on Performance Metrics**

| S/No. | Scheme | Scalability | Computing Cost | | Privacy | Latency | Deployment Cost |
|---|---|---|---|---|---|---|---|
| | | | RSU | OBU | | | |
| **1.** | **Pseudonym cum PKI** | HIGH | HIGH | HIGH | MED | MED | HIGH |
| **2.** | **Group Signatures** | LOW | MED | HIGH | HIGH | HIGH | HIGH |
| **3.** | **Trust Based Schemes** | LOW | HIGH | HIGH | LOW | HIGH | HIGH |
| **4.** | **K-anonymity** | LOW | MED | HIGH | HIGH | HIGH | MED |
| **5.** | **IBE with Pseudonyms** | HIGH | MED | HIGH | HIGH | HIGH | HIGH |

**Table 3.2: Qualitative Comparison of Security and Privacy Schemes in VANETs**

| S. No. | Schemes | Features | Disadvantages |
|---|---|---|---|
| 1 | Pseudonym cum PKI [24] & [26] | (a) User privacy is achieved by using pseudonym coupled with PKI;<br>(b) Certificates (public, private key pairs) are downloaded from trusted authority;<br>(c) Pseudonyms are changed continuously for preserving privacy. | (a) Thousands of certificates to be downloaded to OBU; (b) Certificates need to be replenished periodically; (c) CRL has to be maintained and it keeps on changing and is time- and resource-hungry; (d) The CA can link pseudonyms with vehicles, and therefore have to be secure. |
| 2 | Group Signatures [32], [61]. | (a) Privacy achieved by forming groups;<br>(b) Reduced transmission by ways of periodic broadcasts by a single member of group. | (a) TA can reveal the real identity of user<br>(b) CRL has to be maintained and checked and it increases with the size of the group. |
| 3 | Trust Based Schemes [56] & [57] | Information accepted based on trust.<br>Trust established based on previous record in a centralized authority or based on current and previous interactions with the user in the same session. | (a) No initial trust information available as centralized system would be too slow/too huge; (b) Protection against inside attackers is difficult; (c) Trust score has to be maintained and checked. |
| 4 | K-Anonymity Schemes [65] | (a) Messages are disseminated by ways of flooding it to neighbours; (b) Ensures privacy as long as size of group is adequate. | Flooding is used to disseminate messages which if not effective, can overwhelm the network and eat up bandwidth for the same message. Efficient and practical algorithm missing. |
| 4 | Identity Based Encryption (IBE) With Pseudonyms [6], [63], [64] | (a) User's public key is derived from his public identification such as VIN, etc., which eliminates the need for public key distribution (b) No need for certificate downloads and storage in OBUs (c) Additional information such as a time stamp can also be added. | (*a*) Secure channel needed for private key distribution; (*b*) PKG has to be highly secure; (*c*) TRA can reveal the real identity of the user, therefore must be secure; (*d*) Revocation is still an open problem. |

## 3.7 Intrusion Detection System (IDS)

An intrusion can be defined as an unauthorized activity or access in the network. Intrusion Detection System (IDS) can be described as hardware or software that detects intrusions into the network. The IDS differs from firewalls in that firewalls look outward i.e. try to block attackers from outside whereas IDS protects the network from both insiders and outsiders. IDS work by examining network traffic and data being exchanged and raise an alarm for any suspected intrusion. It means that there have to be well defined policies and procedures so that their violation can be flagged as an intrusion. IDS have been proposed for MANETs in [66], [67], [68] and for VANETs in [69], [70].

Intrusion detection is the most reliable approach to protect vehicular networks against threats as it has the ability to detect insider and external attacks with a high accuracy [71]. Some research has been done in the area of IDS / IPS for Mobile Ad-hoc Networks (MANETs) and VANETs in [72] and [73]. In [74], the authors propose an acknowledgement scheme to prevent packet dropping and false misbehaviour report generation by nodes for MANETs to report or convict a rogue node. In [75], the authors propose a watchdog for intrusion detection in VANETs. The watchdog works by monitoring all packets to decide if an attack is under progress. In [76], trust and position information is combined to determine if a vehicle is falsifying its position i.e. if the position claimed by one vehicle overlaps the position claimed by another in which case the vehicle with low trust value is flagged as an intruder. In [69], a method is proposed to detect intrusions through trust by assigning reputation scores to vehicles and the RSUs are used to compute these scores and the CA aggregates them. Similarly, in [72], rule based anomaly detection and reputation scores are used for the IDS in vehicular network. In [77], [78], intrusion prediction approaches have been discussed.

Depending on the type of detection mechanism used in IDS or where they are deployed they can be divided into the following three types:

## 3.7.1 Types of IDS based on Detection Mechanism

### *3.7.1.1 Signature Based IDS*

The IDS that use this detection mechanism have a database of signatures that are used to compare the network traffic against so as to check for known threats and malicious activities. However, a new attack or intrusion will not be detected as there will be no known signature to compare against and therefore, will go undetected. The benefits of signature based IDS include:

- They can identify known attacks very quickly
- They don’t generate many false alarms as they are programmed to detect known attacks.

The signature based IDS have the following limitations:

- They require updated signature libraries.

### *3.7.1.2 Anomaly Based IDS*

In anomaly based IDS the traffic patterns are compared against a threshold or baseline and anything above the threshold is categorized as an anomaly and is flagged as such. The threshold can be set based on the type of traffic and ports on which such traffic is being generated. The threshold policies have to set carefully or a lot of benign activities (false positives) can be classified as anomalies which then have to be dealt with by the security administrators. The benefits of anomaly detectors are as follows:

- They don’t need to rely on predefined attack signature files to identify attacks.
- They can help identify patterns which can then become signatures for misuse detectors.

The limitations of the anomaly detectors are as follows:

- They require more experienced systems administrators because the detector can only point out abnormalities.
- They may produce a lot of false positives / alarms.
- They require more human intervention.

#### *3.7.1.3 Hybrid IDS:*

A Hybrid IDS uses the combination of both signatures and anomalies to detect intrusion in the network. This combination of both mechanisms will result in better performance for intrusion detection.

### 3.7.2 Types of IDS based on Position of Deployment

#### *3.7.2.1 Network Intrusion Detection System (NIDS)*

A NIDS is deployed at a central and strategic position or positions in the network to monitor all traffic in and out of the network. This enables the NIDS to look at the traffic and highlight anomalies and raise alerts so that they can be dealt with by the security engineers. NIDS can do the following:

- Improve Overall Security:
- Protect Multiple Systems:
- Raise Alert for Incoming Attacks:
- Take Corrective Measures: by changing the configuration of a firewall for example.

The NIDS has the following limitations:

- Processing Speed: if overwhelmed then their performance can deteriorate
- Encryption: NIDS generally don’t decrypt packets therefore, attacks that are encrypted tend to go undetected by NIDS.
- False Positives: NIDS only reports what it is programmed to report and will generate false positives and true negatives.

Some examples of NIDS are:

1. Snort is a free open source NIDS.
2. NetProwler is a commercial NIDS available from Symantec.

### *3.7.2.2 Host Based Intrusion Detection System (HIDS)*

HIDS is deployed at each host or node that needs to be protected and it monitors all traffic in and out from it. It monitors the changes to key files or directories and reports any unusual or suspicious activity to the administrator. The host based IDS is more suitable for distributed networks where the nodes have sufficient computing power and storage capabilities. HIDS is installed on individual computers to protect those systems. HIDS typically utilize OS audit trails and system logs. Also, HIDS can check the integrity of system files to ensure that they are not tampered with. Some benefits of HIDS are:

- They are better than NIDS at monitoring and securing systems.
- They are not helpless against encryption as they can read transmitted packets before they are encrypted and received packets after they are decrypted.
- They can detect file modifications and Trojans etc.

One of the main concerns for HIDS is that they use up the host resources.

### 3.7.3 Response Types

The IDS can generate a response to an attack once it has been identified. This response can be either Active or Passive.

#### 3.7.3.1 Active Response

The active response is something that is automatic and might be something as generating an alert, creating logs, increasing data collection or reconfiguring the firewall or other devices. On the other hand the active response might also include automatic counter-attacks to bring down the attacker’s system, network or find out more about the attacker.

#### 3.7.3.2 Passive Response

This method means putting everything in the hands of the administrator by issuing an alert in the form of an email or a message to tell them that an attack might be in progress. The administrator can then determine the best course of action.

### 3.7.4 Evasion Methods for IDS

**Obfuscation:** This is a technique used by intruders where they manipulate the data so that signatures do not match and avoid detection due to it.

**Fragmentation:** Using this technique an attack is broken down into multiple attacks to avoid detection by staying invisible to anomaly detection systems.

# Chapter 4 : Data Centric Rogue Node Detection

## 4.1 Introduction

In VANETs vehicles communicate by different types of beacon messages to inform each other of their position and speed to give them a sense of traffic around them. Vehicles can also send emergency messages in case of accidents or other hazards. The very fast moving nodes have to act quickly based on these emergency messages. However, a rogue node which sends false emergency messages can wreak havoc in the network that may even result in fatalities. In this chapter we present and simulate a technique to detect a rogue node that is sending false emergency messages in VANETs by cooperative exchange of data without the need of any infrastructure or revocation list. Also, the proposed mechanism will make VANETs fault tolerant and resilient against injection of false data.

The vehicles exchange messages with each other periodically called beacon messages and can also send emergency messages. As nodes in VANETs are vehicles moving at very high speeds, it is imperative that messages received are correct and give a true picture of the road conditions.

Existing mechanism for authenticating messages in VANETs involves the use of cryptography and trust. Cryptographic techniques involve paired keys and overhead in terms of computing cost, storage and time. Time is of the essence in VANETs especially in case of emergency messages when critical decisions have to be taken quickly. Even if emergency messages are kept unencrypted for faster processing, a false emergency message can cause severe damage. Emergency messages include emergency braking, accident, black ice on road and sudden lane changes. These messages are to be transmitted automatically to the vehicles behind so that effective safety measures can be taken. The emergency messages for cases like accidents or emergency braking are time critical and require immediate action and therefore, it is recommended to transmit these unencrypted.

However, a false emergency message can cause severe problems on the highways and can even result in fatalities. The condition is exacerbated when an emergency message is broadcast to be relayed by vehicles to others behind them in a multi hop fashion to convey the information as far back as possible. This raises the problem of broadcast storm in an already bandwidth limited channel when density of vehicles is high. Also, questions such as how far the emergency message should travel and when should vehicles stop transmitting it has been the focus of discussion for many years now. Furthermore, if messages are being relayed then the messages could be tampered with and would be impossible to detect.

A lot of research has been done in the past to secure VANETs by encrypting messages with the help of paired keys. The vehicles authenticate themselves with the TA and then RSU and obtain keys or certificates that they can use within the region of the RSU to exchange messages with other vehicles. Other vehicles do the same and therefore, whoever has obtained valid keys / certificates after authentication is assumed to be a trusted user and its messages are assumed to be correct as long as the credentials are valid. However, if a valid user turns rogue or transmits false data due to a faulty sensor then he cannot be stopped and this can result in serious damage. Therefore, there is a need for developing security mechanisms for VANETs that are data centric rather than identity centric.

## 4.2 Greenshields's Traffic Model

Greenshields's model **[79]** is considered to be a reasonable model in traffic engineering for estimating and modelling traffic when it is uninterrupted (without traffic signals etc.). Greenshields's model uses standard parameters such as flow (vehicles per hour) and density (vehicles per km). The model describes the relationship between speed (*v*) and density (*k*) of vehicles as being negatively correlated with density increasing with the decrease in speed as shown in Figure 4-1c. In the figure $k_m$ and $v_m$ are the optimal density and speed respectively which allows the traffic to progress at the optimum rate of flow - $q_m$ as shown in Figure 4-1 (a), (b) & (c)**.**

**Speed (*v*)** is the speed of the vehicles in km / hr and **density (*k*)** is the number of vehicles per km. The relationship between v and $k$ is expressed in the form of a graph in Figure 4-1. In the figure $v_f$ is the free flow speed when density is zero i.e. vehicles can choose to move freely as there are no or very few vehicles on the road. As the density of vehicles increases the speed decreases till density reaches the maximum which is referred to as jam density or $k_j$ at which point the speed becomes zero and vehicles are stuck in a jam. From Fig. 4.1 the relationship between speed and density is given as:

$$v = v_f - \frac{k}{k_j} v_f \tag{4.1}$$

The relationship between speed, density and flow is as follows:

**Flow (*q*)** is defined as the number of vehicles going through a section per hour and is given as:

$$q = k \times v \tag{4.2}$$

From eqs. 4.1 & 4.2 the relationship between speed and density can be found to be:

$$q = v_f k - \frac{k^2}{k_j} v_f \tag{4.3}$$

The relationship between the three parameters i.e. speeds, density and flow is given in Figure 4-1a, b & c below:

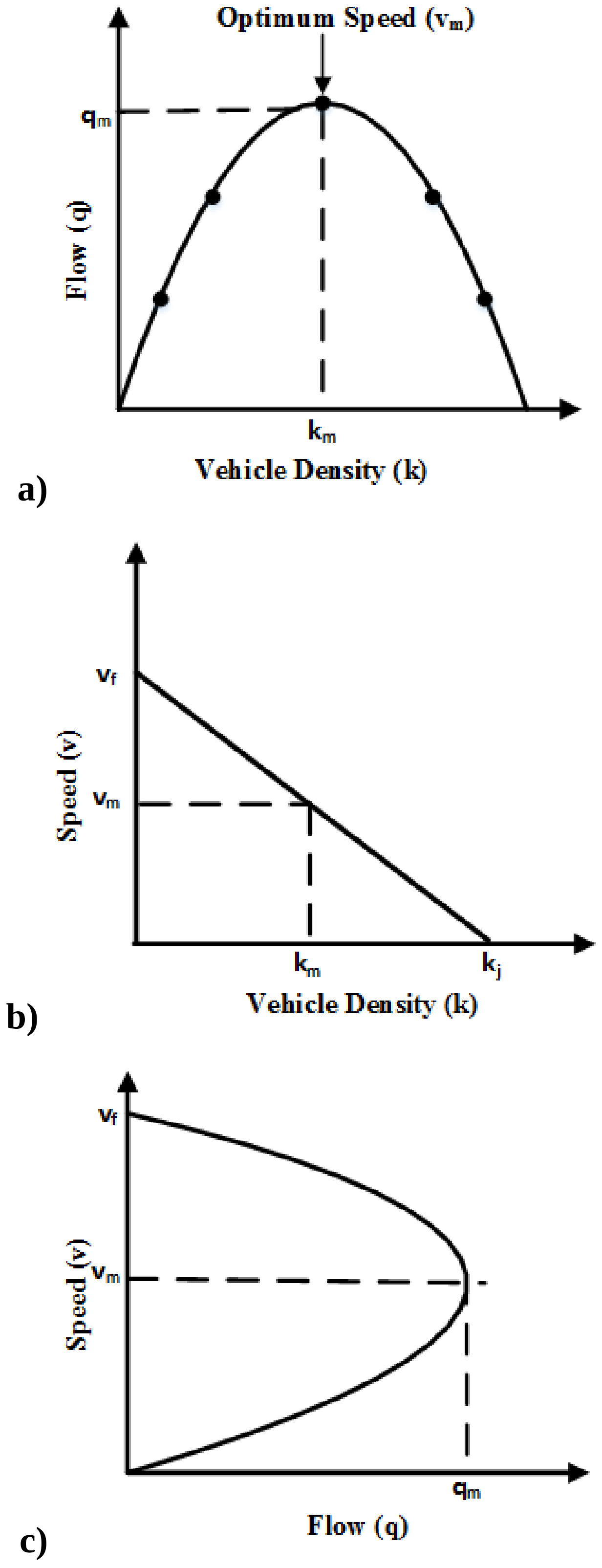


**Figure 4-1: Greenshields's Fundamental Diagrams: (a) Flow vs Density, (b) Speed vs Density, (c) Speed vs Flow**

### 4.2.1 Explanation of the Greenshields's Fundamental Diagrams:

Figure 4-1 (a, b & c) represent the Greenshields's fundamental diagrams. Fig. 4.1a shows the relationship between Flow and Density when the average speed of vehicles starts increasing where the speed is zero at the origin. The average speed increases until it reaches the optimum speed $v_m$ at which point the flow and density are also at their optimum levels i.e. $q_m$ and $k_m$ respectively. After this peak, if the average speed of vehicles increases any further then it will result in an increase in the density but a decrease in the flow of the vehicles.

Figure 4-1b shows the linear relationship between the speed and density of vehicles. The vehicles can move with free flow speed $v_f$ when the density of vehicles is near zero. However, the average speed of vehicles decreases when the density of vehicles increases and reduces to zero when the density of vehicles reaches jam density $k_{j.}$

Figure 4-1c shows the relationship between the average speed and flow of vehicles with varying density of vehicles. As the density increases from zero, the graph moves from $v_f$ to the origin at which point the Flow and average speed become zero and the density reaches the maximum i.e. jam density $k_{j.}$

.

## 4.3 Scheme Overview

We present a scheme, Cooperative Detection And Correction (C-DAC), in which all vehicles calculate their own values of flow. Vehicles send their speed, flow, density and location information to other vehicles and each vehicle can calculate their own value of flow which gives them a very good model of the traffic in their vicinity and up ahead as well. Each vehicle can predict the density of vehicles on the highway by the number of messages it receives from other vehicles by checking their IDs from messages. This enables each vehicle to calculate the density quite accurately in a moving window around itself as shown in Figure 4-2. The size of this density window is equal to the transmission and reception range of a vehicle (500 meters). This means that a vehicle can receive messages from a vehicle which is up to 500m ahead of it and 500m behind it. Therefore, each vehicle has a communication window of 1000m around it that it can use to calculate the density ($Density_{calc}$). Also, each vehicle can calculate the average speed of vehicles ($Speed_{AVG}$) within its communication window. In C-DAC scheme each vehicle transmits not only its location and speed but the calculated value of flow as well. Therefore, the vehicles calculate the traffic flow parameter using density and average speed of other vehicles through Greenshields's model. The flow serves as a global parameter which each vehicle calculates on its own and should be very similar for vehicles that are close to each other in the same traffic conditions.

The idea is that in case of an actual emergency situation, a vehicle will generate a message that has a very small value of flow that indicates that the flow of vehicles on that stretch of road has suddenly reduced. This will be confirmed by other vehicles as well which calculate a similar small value of flow on their own and generate messages.

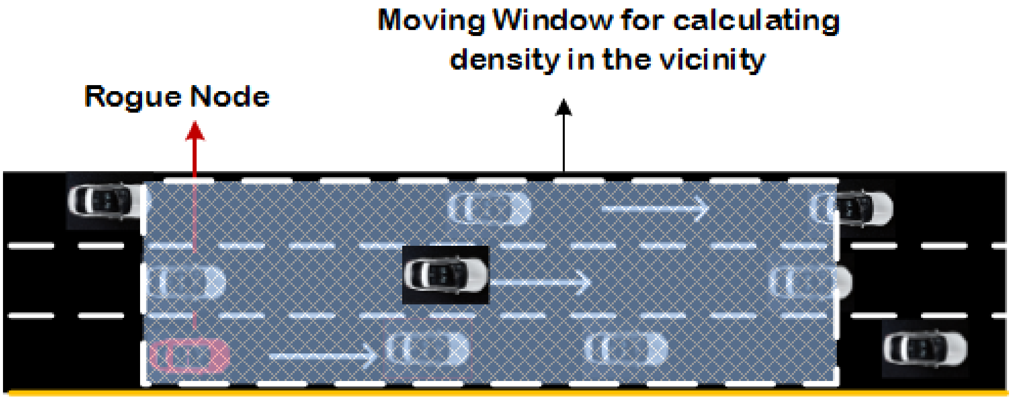


**Figure 4-2: Estimating density of vehicles in VANETs**

However, if a node generates a false message indicating a small value of flow either with malicious intent or due to some fault then it would be the only vehicle that generates such a value and can be singled out. The vehicle’s speed has been used by some researchers [80] to estimate density but it does not give good results as the assumption is that given the opportunity the vehicle will try to achieve the maximum speed possible which is not true in real life.

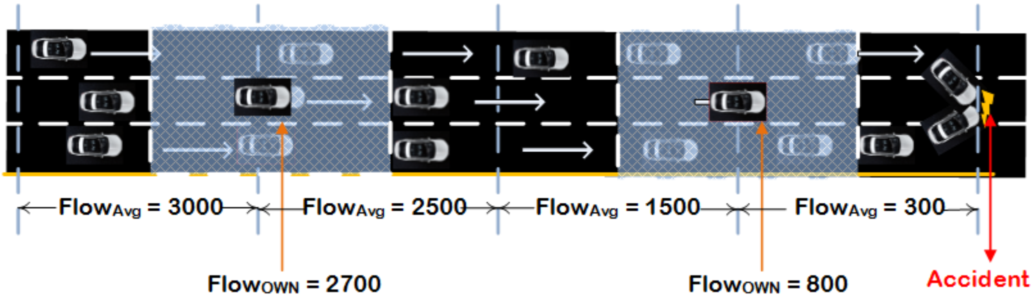


**Figure 4-3: Varying value of flow in an Accident scenario**

Each vehicle transmits its $Flow_{OWN}$ which becomes $Flow_{Rcvd}$ for other vehicles. If a vehicle receives a value of Flow from another vehicle that does not agree with the VANET model then the data is rejected and vehicles' ID is noted and reported. If the data agrees with the model then the receiving node checks the data with its own calculated values to confirm if values are indeed correct (shown in Figure 4-4). If the values do not agree with the node's own calculated parameters of Flow, Speed and density then the values are discarded and the sender ID is reported. The two values of flow are calculated as follows:

$$FLOW_{OWN} = Speed_{AVG} \times Density_{Calc} \qquad (4.4)$$

$$FLOW_{AVG} = \sum_{i=1}^{n} \frac{FLOW_{Rcvd_i}}{n} \qquad (4.5)$$

However, in case of an actual accident the low value should be reported by all vehicles and it should propagate throughout the highway efficiently and gradually as shown in Figure 4-3. Moreover, in case of actual accident the speed of the vehicle that is receiving the messages will come down as well as it can detect obstacles with the help of on-board radar etc.  Therefore, the main assumption is that the vehicle will be able to trust its own calculated values even if it can't trust anyone else. As, vehicle's own speed comes down then from eq. (4-4) the $Flow_{OWN}$ should come down as well which is then sent to other vehicles. If the received data doesn't conform to the VANET model, own calculated values or both then the data will be discarded and the node will be reported.

**Conformance to VANET model and producing an attack:**

Conformance to the VANET model means that the parameters of the traffic that the vehicle exchanges with other vehicles have to follow the model, if a vehicle is conforming to the model then it can't produce an attack. Conversely, it can be said that if a vehicle is producing an attack then it is non-conformant to the VANET model. If a conformant vehicle sends out a false emergency braking message then it will be contradicting itself. Moreover, if a vehicle sends out an emergency message then other vehicles in that region should also experience the same event and send out a similar emergency message. If this is not the case then the single emergency message can be easily classified as false. The flow chart for our scheme C-DAC is shown in Figure 4-4.

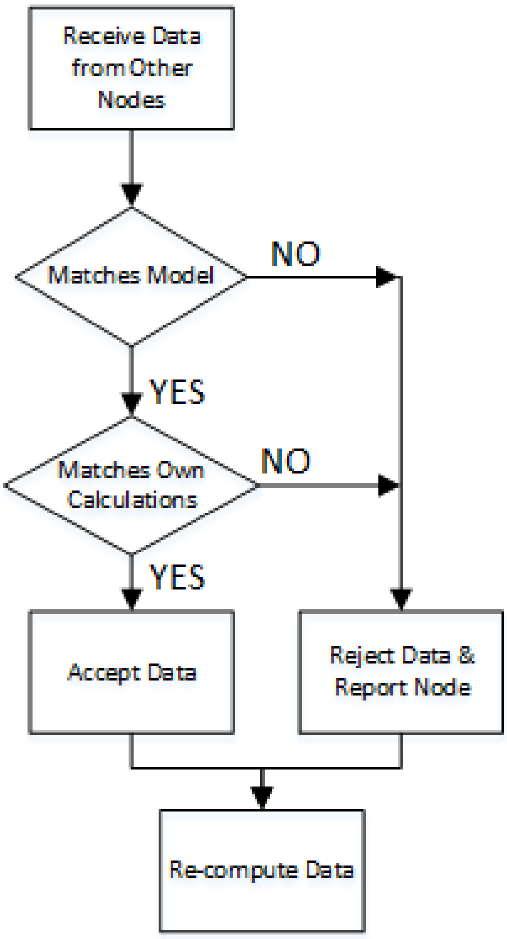


**Figure 4-4: Overview of Cooperative Detection and Correction scheme (C-DAC)**

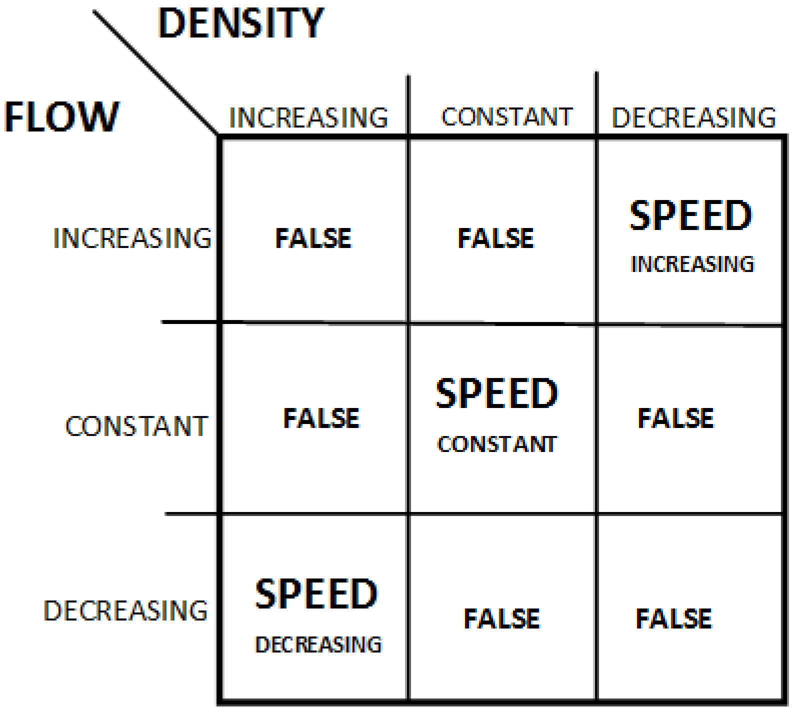
### 4.3.1 Rogue Node Model

A node is termed as rogue if it starts to inject false data in the network either on purpose with malicious intent or due to faulty sensors. Moreover, the rogue node can start sending false data at any time and can falsify values of their own speed and their calculated values of flow and density either in beacon message or emergency message. However, a rogue node can’t modify values of other nodes in the network. In case of a false emergency message the rogue node will start sending a low value of Flow or sudden decrease in speed or both to indicate an accident or emergency braking.

### 4.3.2 Data Centric Rogue Node Detection

The honest nodes can decide whether a value being shared is correct or not by using a decision table shown in Figure 4-5 which is shown as an example and is directly derived from the Greenshields's model as shown in Figure 4-1c. This means that if the density of the vehicles on the highway and the flow is constant then the speed of vehicles must also be constant. Similarly, if the density decreases and the flow increases then the speed must be increasing. Moreover, if the density is increasing and the flow is decreasing then the speed must be decreasing.

As in the case of our simulation if the value of Flow being reported by a node is decreasing but the speed and density reported from that node remain constant then the value being reported is false. Similarly, another case could be when a node reports a decreasing value of flow and increasing value of density but the average speed remains constant in that region then again this implies that the data being reported is false and can be discarded.



| FLOW \ DENSITY | INCREASING | CONSTANT | DECREASING |
|---|---|---|---|
| INCREASING | FALSE | FALSE | SPEED<br>INCREASING |
| CONSTANT | FALSE | SPEED<br>CONSTANT | FALSE |
| DECREASING | SPEED<br>DECREASING | FALSE | FALSE |

**Figure 4-5: Decision for Data Correctness**

The results show that by using our technique, messages can be authenticated based on the relevance and freshness of data without authenticating the identity of nodes. Such nodes can then be reported or their messages be simply discarded. Also, the information about an accident can be propagated down the highway gradually and gracefully so that the traffic keeps flowing as long as it can and comes to stop gradually.

## 4.4 Simulation Setup

In order to check the proposed model it is simulated using OMNET++, SUMO [81] and VACaMobil [82]. OMNET is a modular C++ library and framework that is used for network simulations. Simulation of Urban Mobility

(SUMO) is a software tool used to generate vehicular traffic by specifying speed, types, behaviour of vehicles and road types and conditions. VACaMobil is a car mobility manager for OMNET that works in parallel with SUMO. The scenario is simulated with parameters shown in Table 2. In order to validate the model, an accident is simulated which takes place at t=180 sec and the results are recorded. Nodes 0, 1, 2, 3, 4 suffer an accident and block all three lanes of the highway. The result for $\text{Speed}_{\text{AVG},}$ $\text{Density}_{\text{AVG}}$ and $\text{Flow}_{\text{AVG}}$ are shown in Figure 4-6, Figure 4-7 and Figure 4-8 respectively.

Another scenario is simulated when there are three rogue nodes which start sending low false values of $\text{Flow}_{\text{OWN}}$ from t=180 sec, incorrectly indicating an accident up ahead. The time t=180 sec is chosen in the simulation so that there are sufficient vehicles in the simulation and the supposed accident is caused at nearly the end of the highway in the simulation. The results for this scenario (where every 10th node is a rogue node) for $\text{Density}_{\text{calc}}$ and $\text{Speed}_{\text{AVG}}$ are shown in Figure 4-12 & Figure 4-13 respectively whereas the $\text{Flow}_{\text{AVG}}$ values for 6 vehicles (out of which 2 are rogue) are shown in Figure 4-14. This means that we are looking at the flow values for a total of 6 vehicles at a time in order to understand the effect of the false information in the immediate vicinity of the rogue nodes.

| Simulation Parameter | Value |
|---|---|
| Simulation Time | 500 sec |
| Scenario | 3 Lane Highway |
| Highway Length | 5-Kms |
| Max Vehicle Speed | 28 m/sec or 100 Km/hr |
| Mobility Tool | VACaMobil |
| Network Simulation Package | OMNET++ |
| Vehicular Traffic Generation Tool | SUMO |
| Vehicle Density | 20-30 veh / Km |
| Wireless Protocol | 802.11p |
| Vehicle Inter-Arrival rate | 1s, 2s and 3s |
| Transmission Rate | Every 0.2s, 0.5s and 1s |
| Transmission Range | 500m in each direction |

**Table 4.1: Simulation Parameters**

The scenario is simulated with parameters shown in Table 4.1. In order to gather data for anomaly detection we use different scenarios. The data is gathered when there is no accident and no rogue nodes to understand and develop the model under normal circumstances. Data is also collected for runs in case of an actual accident to understand how parameters will change. Furthermore, rogue nodes are inserted in both cases i.e. in case of normal conditions (no-accident) and in case of an actual accident to see how well our IDS works. The simulations are carried out with varying values of the following parameters:

**1) Density:** The density of nodes is an important parameter for ad-hoc networks and especially for VANETs. As the channel bandwidth is limited, it is essential to keep it under consideration and observe its effects on any system. In this work, we vary the density of vehicles by changing their inter-arrival time i.e. the time that they are inserted in the simulation. We use OMNET’s exponential inter-arrival distribution with a time of 1, 2 and 3 seconds.

**2) Beaconing Rate or Sampling Rate:** This is the beaconing time period after which each vehicle is transmitting its parameters to other vehicles. We have used variable time periods to observe the effects of this on VANETs in general and the proposed IDS in particular. We have used time periods of 0.2, 0.5 and 1 seconds. It is worth mentioning that the recommended beaconing rate in IEEE 809.11p is a 100 milliseconds (0.1 sec). The minimum time period of 0.2 seconds was chosen as the generated data set was becoming too large and data processing was becoming a problem.

**3) Number of Rogue Nodes:** The number of rogue nodes is varied to evaluate the performance of the proposed scheme and the IDS in these circumstances. The number of rogue nodes is increased from 0 to 40% of the total number of vehicles in the simulation.

## 4.5 Results

### 4.5.1 Actual Accident Scenario - No Rogue Nodes

The results for the actual accident scenario when there are no rogue nodes are shown in Figure 4-6, Figure 4-7 and Figure 4-8. These results are shown for a vehicle to show how the parameters change in an actual accident scenario. It can be seen from Figure 4-7 that the accident is causing the number of vehicles (density) to build up after the accident. Similarly, the flow value that each vehicle is computing is decreasing immediately after the accident (Figure 4-8). Also, as the vehicles come to a stop their speeds decrease quite abruptly (Figure 4-6). This result gives a true - real VANET model against which received values are compared in case of rogue nodes.

The simulation was run multiple times to study the effect of density and transmission interval on the performance of the proposed mechanism and is shown in Figure 4-9, Figure 4-10 and Figure 4-11.

**REAL ACCIDENT SCENARIO**

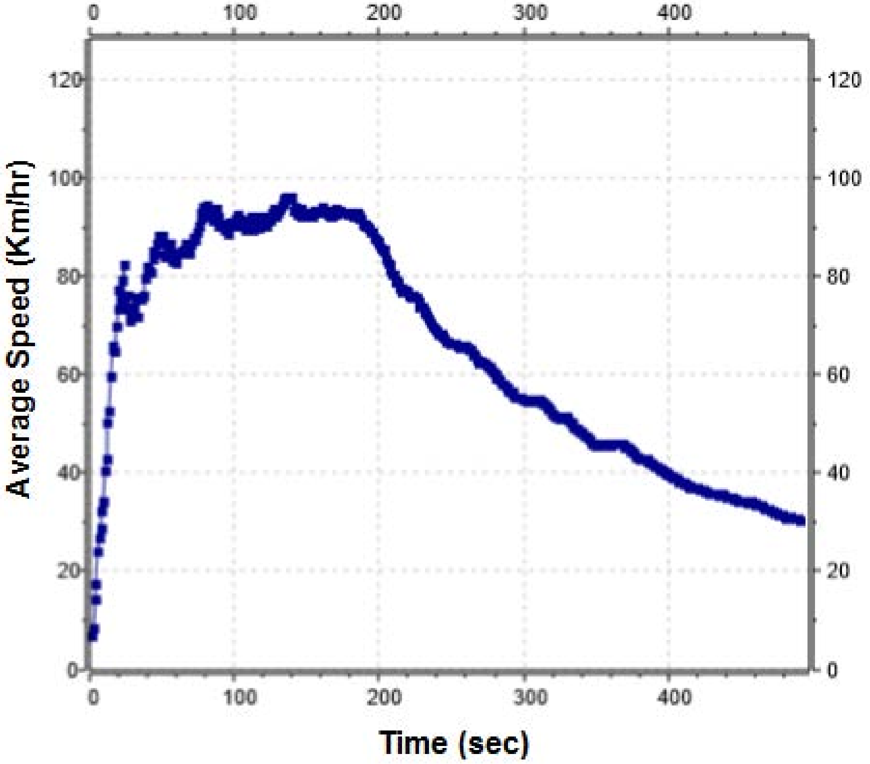


**Figure 4-6: Decreasing speed in real accident scenario**

**Explanation of Fig. 4.6:** The Average speed of vehicles goes down due to the accident which is occurring at t = 180 sec. The vehicles reduce their speed as they approach the accident. As the speed of each vehicle goes down, the flow parameter that each vehicle is calculating also goes down for that region. This parameter is then transmitted to other vehicles coming behind which become aware of an ‘incident’ up ahead.

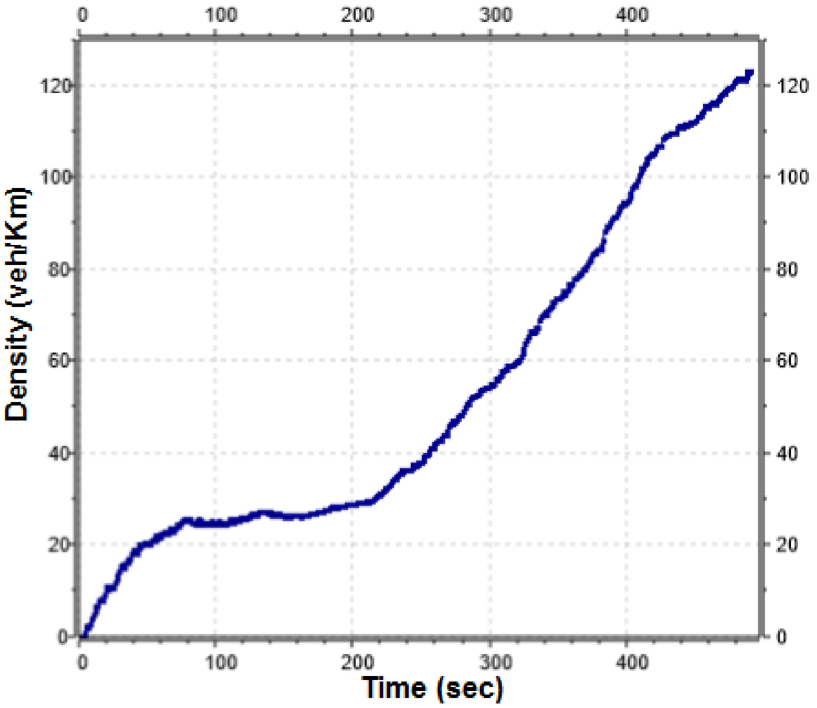


**Figure 4-7: Increasing density in real accident scenario**

**Explanation of Fig. 4.7:** As the vehicles approach the accident region, the density being calculated by vehicles starts increasing when the accident occurs at t=180 sec. This is in accordance with the Figure 4-5.

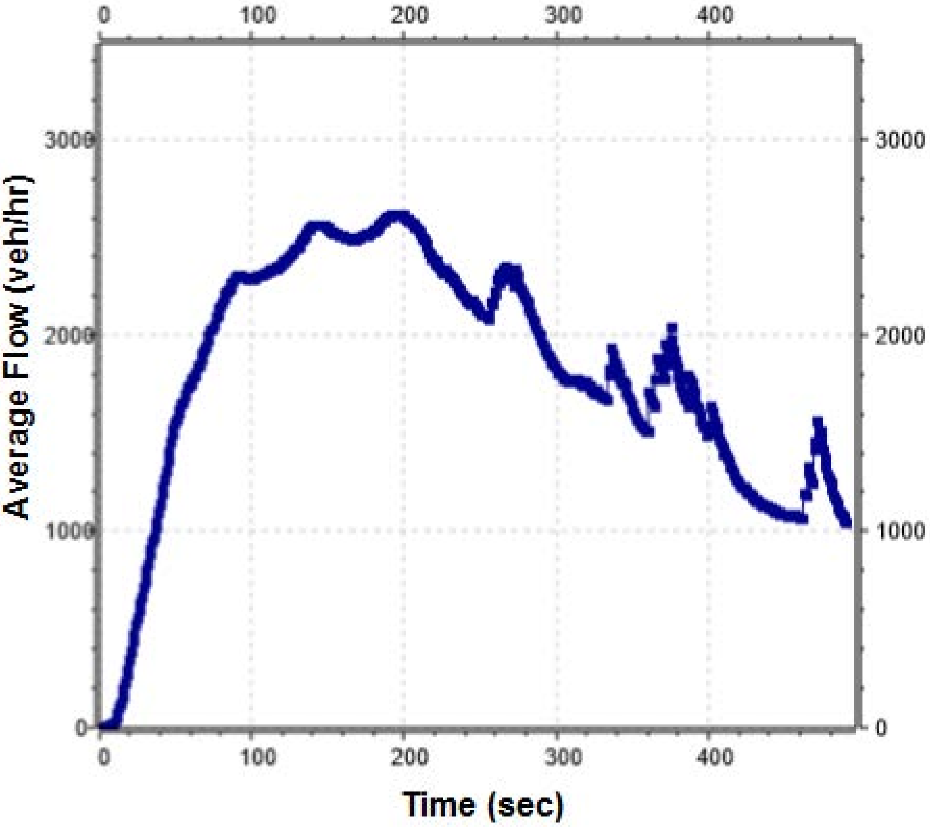
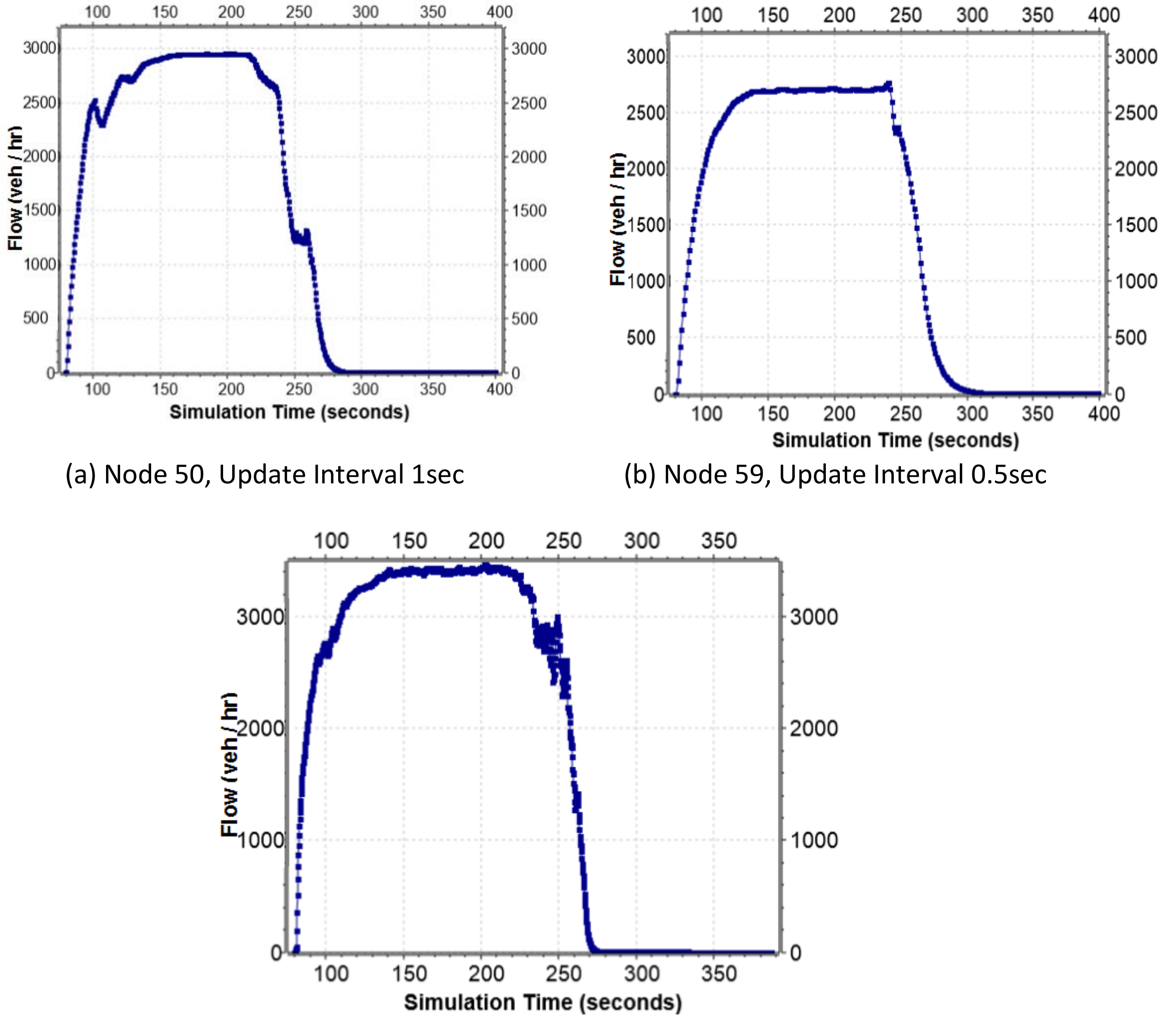


**Figure 4-8: Decreasing flow in real accident scenario**

**Explanation of Fig. 4.8:** The Average Flow of all vehicles in the simulation is shown in Figure 4-8. As expected the value of flow starts decreasing a little after the accident occurs at t=180 sec.

More results for the actual accident scenario without rogue nodes are shown in Figure 4-9, Figure 4-10 and Figure 4-11. The density of vehicles (controlled by Inter-Arrival Time) and the update interval (transmission rate) are varied in the simulations to study their effects. What is noteworthy here is that the flow parameter gradually decreases which proves our earlier assumption. In Figure 4-9 (a), (b) & (c) the results are shown for the value of Flow$_{AVG}$ for vehicles that are starting at approximately t=80 sec and an accident occurs at t=180 secs for the same density of vehicles.



(a) Node 50, Update Interval 1sec

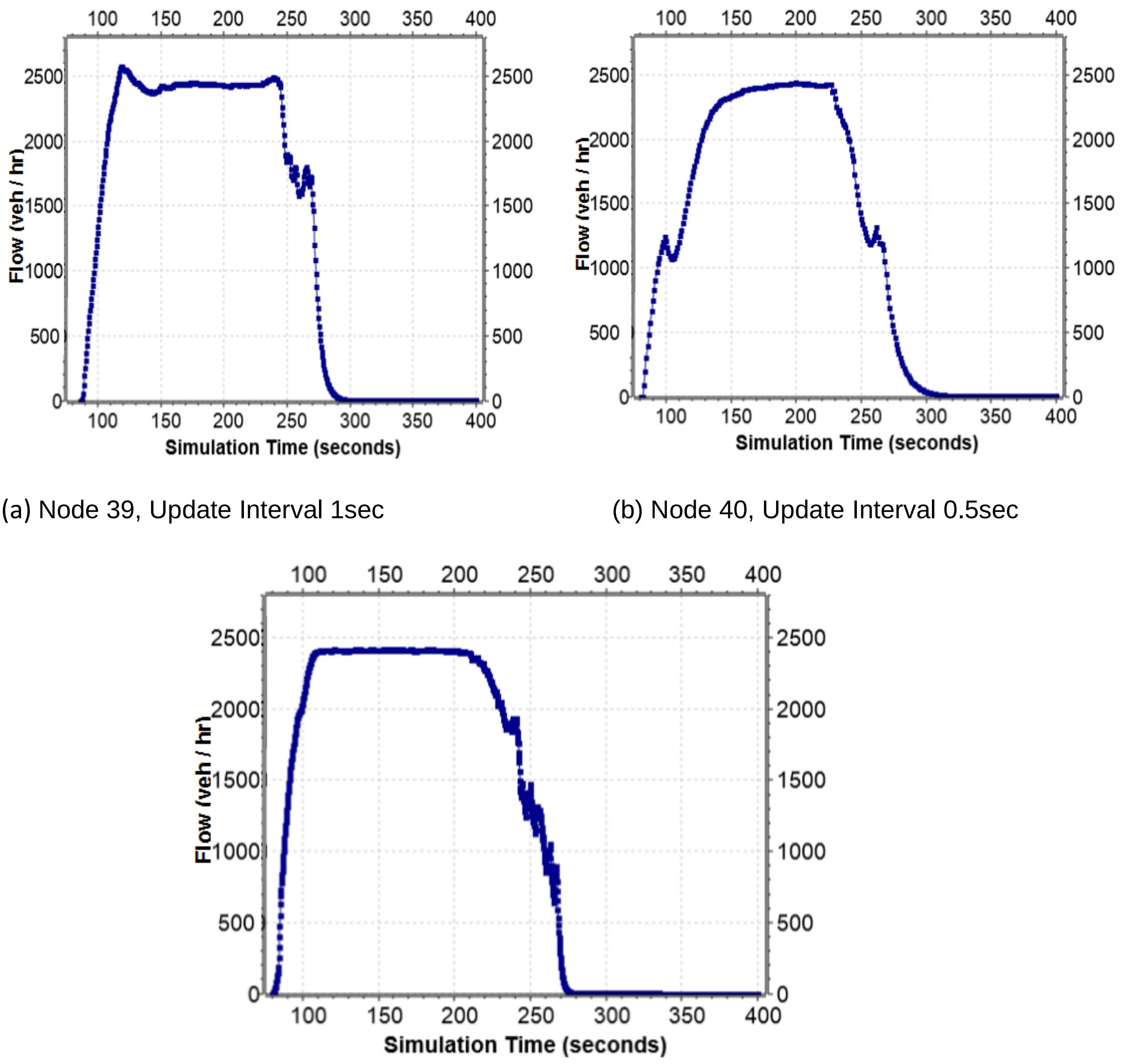
(b) Node 59, Update Interval 0.5sec

(c) Node 56, Update Interval 0.2sec

**Figure 4-9: Accident Scenario: Inter-Arrival time = 1 sec: All Vehicles starting at approx t = 80sec**

**Explanation of Fig. 4.9:** It can be seen in Figure 4-9 that the value of the Flow parameter reduces to zero quickest when the update interval (transmission rate) is the lowest i.e. 0.2 sec as shown in Fig. 4.9 (c).

Figure 4-10(a, b, c) show the results when the density is kept constant (inter arrival time = 2 sec), the update interval is varied and an accident occurs at t=180s.



(a) Node 39, Update Interval 1sec

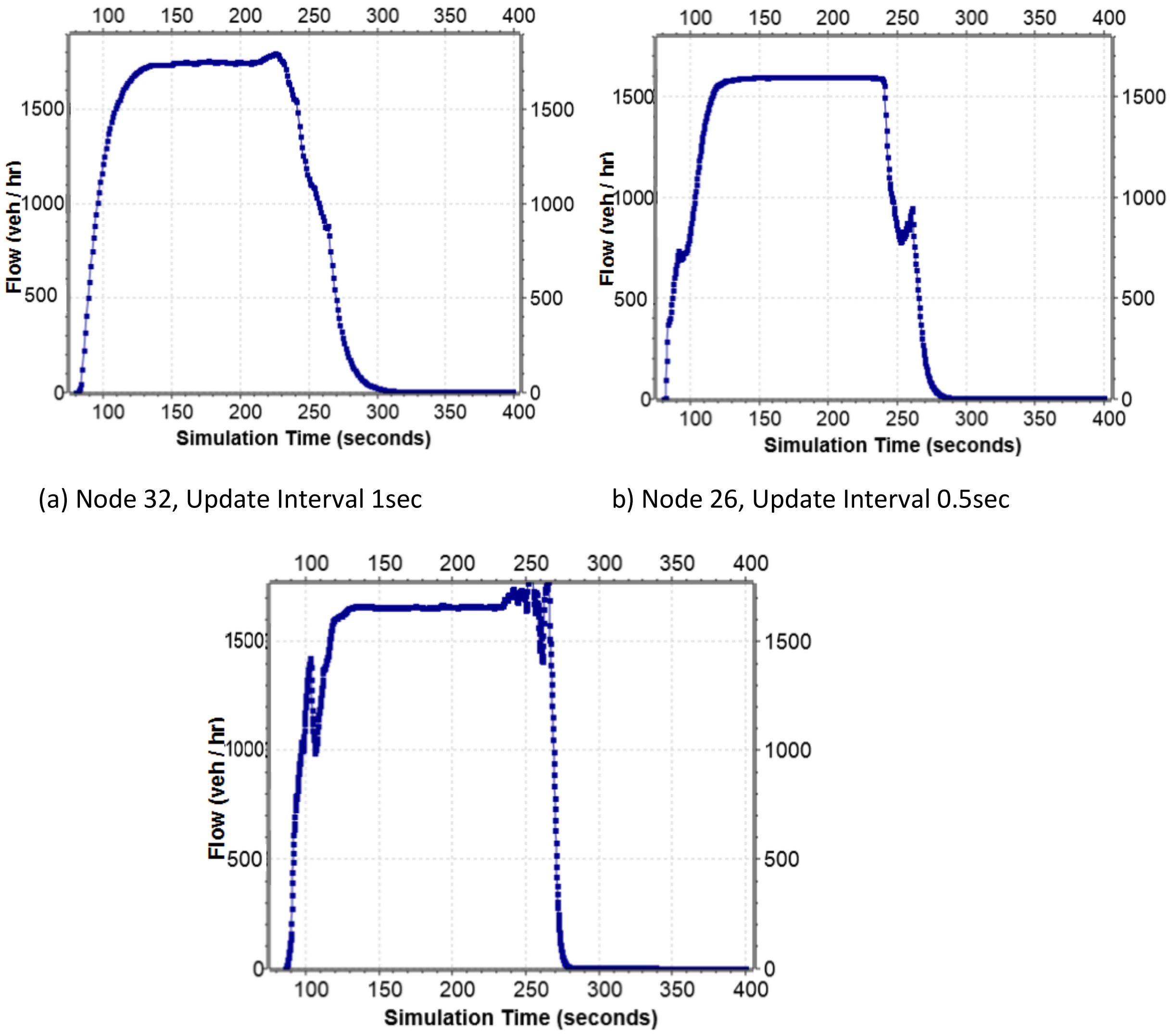
(b) Node 40, Update Interval 0.5sec

(c) Node 36, Update Interval 0.2sec

**Figure 4-10: Accident Scenario: Inter-Arrival time = 2 sec: All vehicles starting at approx t = 80sec**

It can be seen from Figure 4-10 that the value of the Flow parameter settles down quickest when the update interval has the lowest value i.e. in Fig. Figure 4-10(c).

Figure 4-11(a, b, c) show the results when the density is kept constant (inter arrival time = 3 sec), the update interval is varied and an accident occurs at t=180s.



(a) Node 32, Update Interval 1sec

b) Node 26, Update Interval 0.5sec

(c) Node 24, Update Interval 0.2sec

**Figure 4-11: Accident Scenario: Inter-Arrival time = 3 sec: All vehicles starting at approx t = 80sec**

In Fig. 4.11, the inter-arrival time between vehicles is 3 sec. It can be seen the flow value reaches zero quickest at approx. t=275 sec when the update interval is the smallest i.e. 0.2 secs.

**Comparison of Simulations:**

It can be seen from Figure 4-9, Figure 4-10 and Figure 4-11 that the value of the Flow parameter doesn’t depend on the density of vehicles but only on the transmission rate as can be seen from Figs. 4.9 (c), 4.10 (c) and 4.11(c) where it reduces to zero quickest. The density of vehicles in the simulation is the highest in Fig. 4.9 and lowest in Fig. 4.11 but the Flow parameter is only dependent on the update interval or the transmission rate.

### 4.5.2 No Accident - Rogue Node Scenario

In Figure 4-12, Figure 4-13 and Figure 4-14 every 10th vehicle is a rogue node which are travelling normally without any accident and the rogue nodes are transmitting a low false value of Flow whereas the others are transmitting a (true) high value. In this case, the rogue nodes are not modifying the values of density or speed and can easily be seen and classified as faulty or rogue values.

**ROGUE NODES SCENARIO**

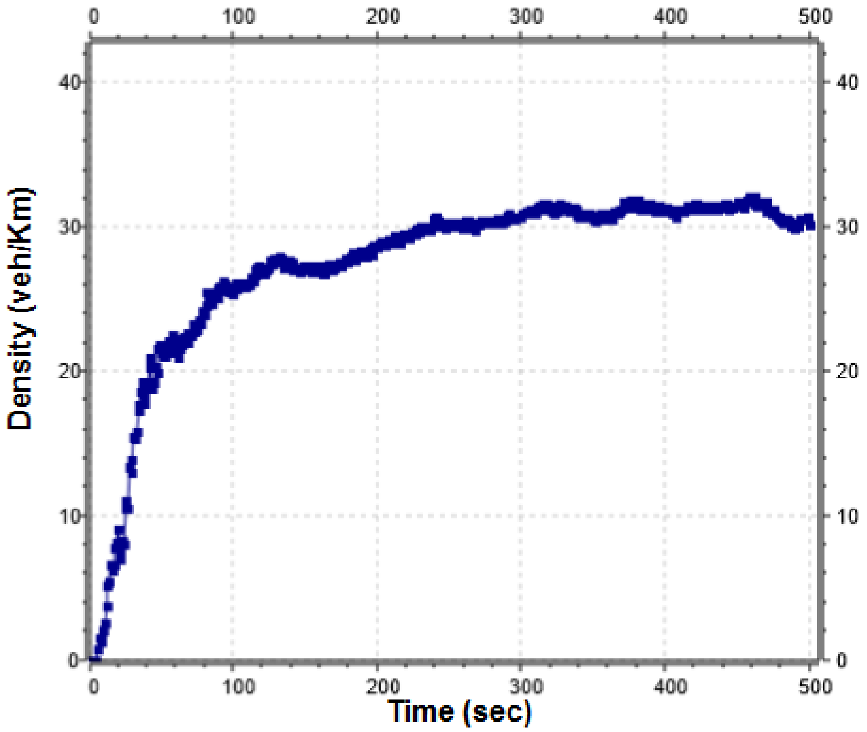


**Figure 4-12: Constant density in case of No Accident**

**Explanation**: In Figure 4-12, the constant density is showing a normal flowing traffic without a sudden build-up of vehicles in a region at any time.

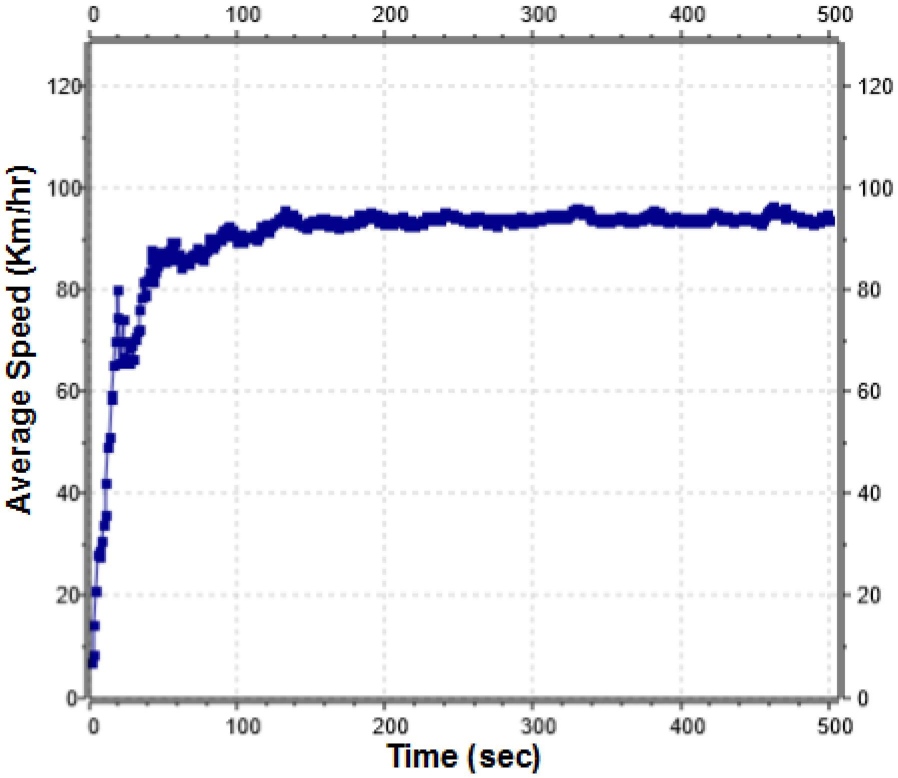


**Figure 4-13: Speed in No Accident Scenario**

**Explanation**: In Figure 4-13, the average speed of vehicles shows no sudden decrease which shows normal flowing traffic i.e. no accident.

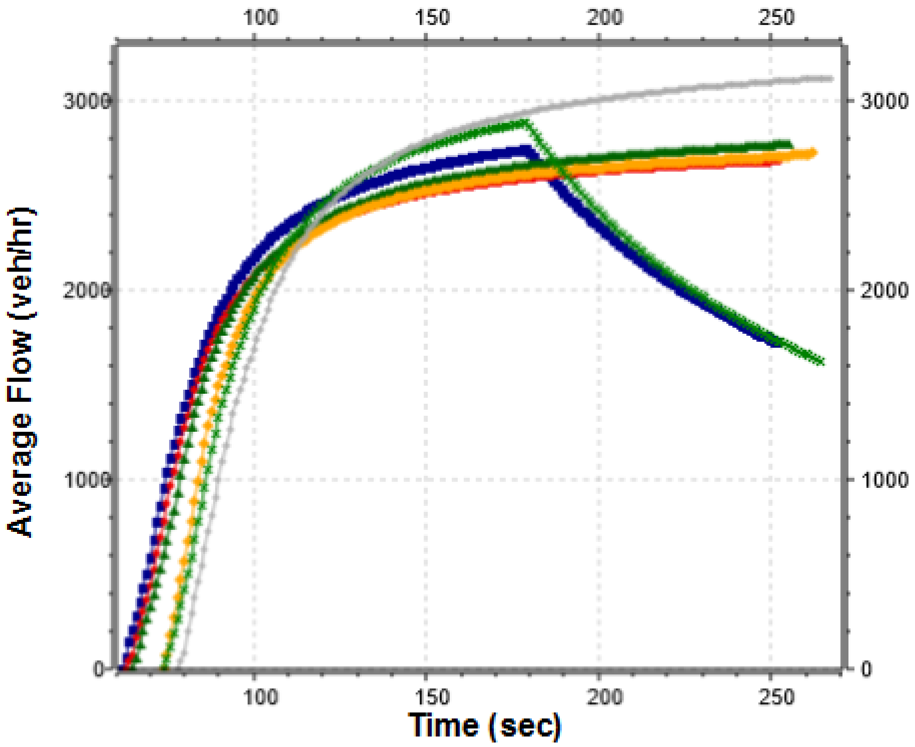


**Figure 4-14: 2 Rogue Nodes reporting low value of flow**

**Explanation:** In Figure 4-14, it can be seen that all honest vehicles are reporting a higher value but two nodes start reporting a decreasing value of Flow. As the values of density and speed don’t show any signs of an accident in Figs. 4.12 and 4.13, it can be confidently assumed that the two low values of flow are false and can be rejected.

### 4.5.3 Normal Traffic - No Accident - No Rogue Nodes

In order to understand the parameters under normal circumstances we need to record the traffic data in case of normal traffic i.e. when there is no accident and no rogue nodes. Figure 4-15 shows the recorded data for the 100th node when update interval is 1sec and inter-arrival rate is 1 sec. As expected, the average value of Flow ($\text{Flow}_{\text{AVG}}$), calculated values for flow ($\text{Flow}_{\text{OWN}}$) & the received flow values from other vehicles ($\text{Flow}_{\text{RCVD}}$) are all quite close to each other and the received values ($\text{Flow}_{\text{RCVD}}$) are in fact within one standard deviation of the ($\text{Flow}_{\text{AVG}}$) as calculated by the node.

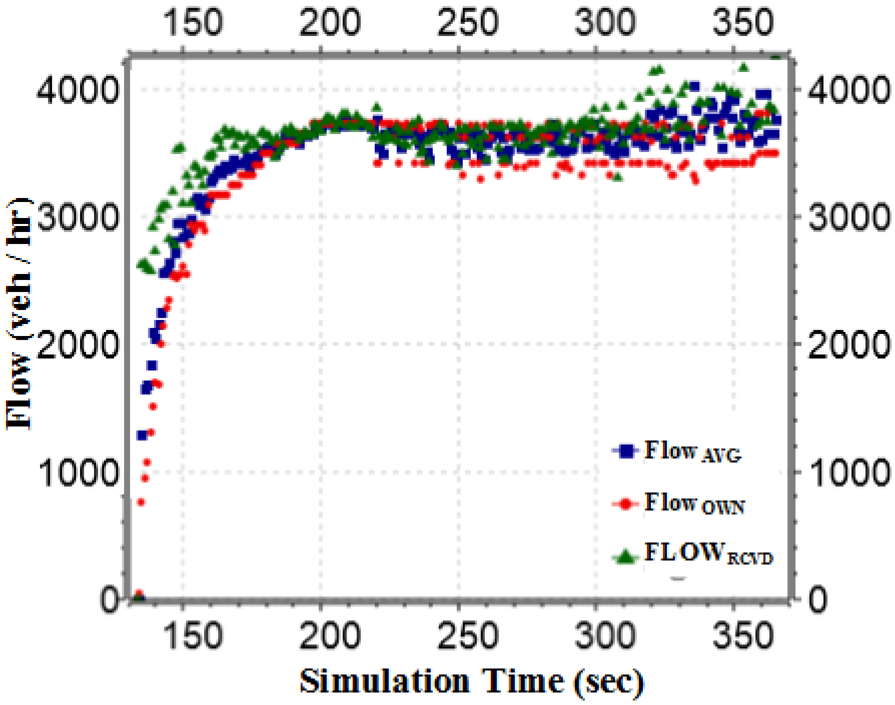


**Figure 4-15: Distribution of $\text{Flow}_{\text{AVG}}$, $\text{Flow}_{\text{OWN}}$ & $\text{Flow}_{\text{RCVD}}$ in case of Normal Traffic / No-Accident and all Honest Nodes**

## 4.6 Performance Analysis

### 4.6.1 Fault Tolerance

The traffic parameters are being received from other vehicles and they are being compared with the readings calculated by the receiving vehicle itself and other vehicles. Therefore, this introduces a built-in fault tolerance in the network which is highly useful and desirable for highly volatile and rapidly changing VANETs. Even if a node is able to distort the values of the reported parameters (Density, Flow and Speed) so as not to raise a red flag with other vehicles, it results in a small error in the overall reading as shown in Figure 4-16, it shows values of $\text{Flow}_{\text{own}}$ in case of no accident and two rogue nodes that start transmitting a false value of Flow at t=180 sec and the average value of flow shown in blue line. This value shows that even if the false flow values are not rejected initially they will cause little deviation if the number of rogue nodes is small as compared to honest nodes in the neighbourhood.

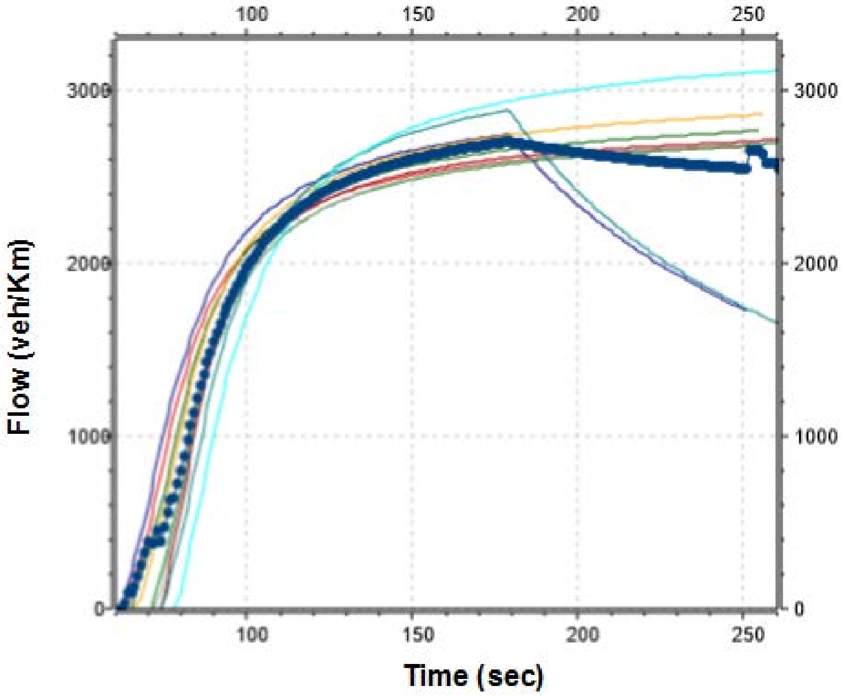


**Figure 4-16: Average Flow in case of No-Accident with rogue nodes**

### 4.6.2 Self Detection and Correction

In a vehicular ad-hoc network with fast moving nodes, it is highly desirable for the nodes to be able to detect and correct data on their own. Due to the volatile nature of VANETs it is impractical to use any techniques that rely on reputation or trust of users to ensure correctness of information. Moreover, a valid identity of vehicles is important for distinguishing them from each other but should not be used as the basis of the acceptance of information in a protocol. This means that an authenticated node doesn't guarantee that the node will behave honestly.

With the latest technology being introduced in the vehicles including radars and cameras for obstacle detection, these technologies can be combined with a technique like ours to ensure safety of travel. With driver-less features becoming a reality with Google car, it is important that the vehicle starts behaving autonomously not only in terms of driving but also planning ahead. This means that at high speeds on the highways, a driverless car should be able to estimate or predict the road and traffic conditions quite early and with reasonable accuracy. This is only possible if the highway traffic is modelled and used by the OBUs to detect and correct anomalies in the information being received. The notion of revocation quickly in a highly agile and temporary network doesn’t seem realistic.

### 4.6.3 Congestion Avoidance

In case of emergency messages in VANETs, the currently proposed method of propagating such messages is by relaying the message by receiving vehicles to others behind them. This can cause a broadcast storm where every vehicle is relaying the same message repeatedly and flooding the region in an attempt to inform other vehicles of the emergency. This quickly, consumes the small bandwidth available and can choke the network. However, in our proposed scheme there is no channel congestion as there is no need for multi-hop retransmissions and a sudden drop in the flow or speed values can indicate an emergency. Moreover, as only the vehicles within range behind the vehicle experiencing the accident receive the emergency message, they are able to identify that vehicle quickly as they have communicated with it before. These vehicles then modify their own values of flow and send them to others.

### 4.6.4 Resilience to Sybil Attacks

In case of a Sybil attack, an attacker presents multiple identities with an intent to either vote out a user maliciously or in our case more likely to create the illusion that there is congestion or accidents up ahead. All vehicles are reporting their location along with their speed, density and flow values in their vicinity. In case of a Sybil attack, an honest vehicle which is behind a Sybil node will receive multiple (false) messages with different identities and each message will report a low value of flow but if the vehicle's own speed is not decreasing then it can start ignoring those messages. Therefore, C-DAC provides resilience against Sybil attacks.

### 4.6.5 Scalability

It can be seen from Figure 4-9, Figure 4-10 & Figure 4-11 that the density has a negligible effect on the working of the method i.e. all vehicles receive the information about the attack at the same time (i.e. such as Figure 4-9b, Figure 4-10b and Figure 4-11b) if the update interval is the same. This shows that the proposed mechanism is scalable. Also, it is clear that the update interval has a significant impact on the information flow as the value settles down the quickest (as shown in Figure 4-9c, Figure 4-10c and Figure 4-11c) when the update interval is the smallest i.e. 0.2 sec as compared to the others when the update interval is higher. However, this is acceptable as the standard update interval in VANETs can be as low as 100 msec or 0.1 sec.

### 4.6.6 Comparison

The success rate of the proposed scheme C-DAC is compared with the AMBA (Adaptive and mobility based algorithm) presented in [80]. The success rate is the percentage of vehicles within a 3km distance that receive the emergency message successfully and is shown in Figure 4-17. In our scheme C-DAC, the success rate reaches 100% as there is no congestion because the emergency messages are not being relayed as in AMBA. Instead, in C-DAC the emergency info is being propagated through communication of some global traffic parameters as discussed previously and information can be relayed to all nodes even very large distances away.

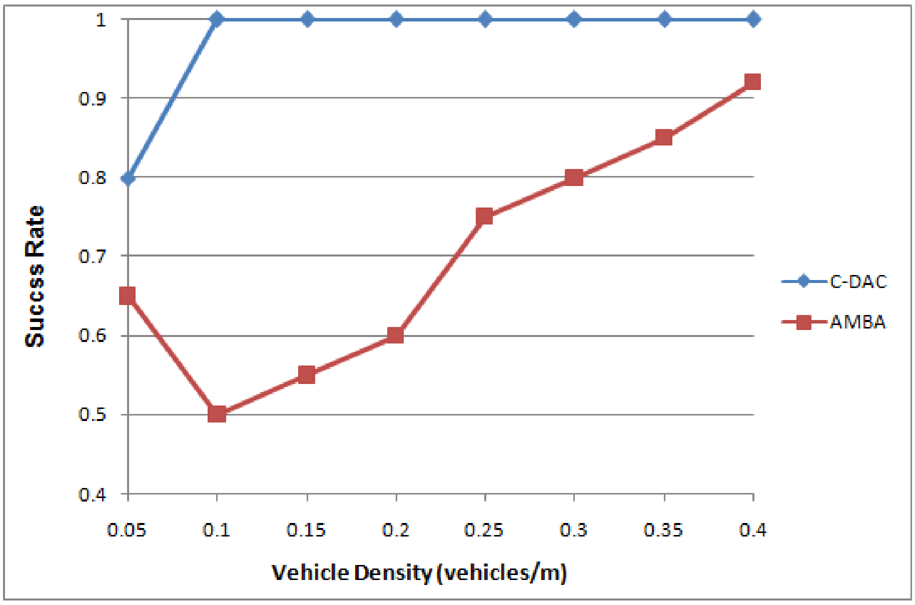


**Figure 4-17: Percentage of vehicles within the distance 3000m that received the emergency information successfully**

## 4.7 Related Work

Due to the highly volatile and ad-hoc nature of VANETs, the cryptographic algorithms that are to be used in VANETs have to be designed to be a trade-off between security and performance. Moreover, malicious behaviour e.g. injection of false data is still possible even in case of strong cryptography. Researchers in [58] suggest using data centric techniques to make information in VANETs more reliable by data centric trust establishment.

Some data centric misbehaviour detection techniques have been proposed in [83], [84]. In [83] the authors propose a model of VANETs to be used to detect and correct errors in the data being sent out by vehicles. The messages that conform to the model is accepted and rejected otherwise. However, the authors do not specify the model in detail but only the events. In the proposed scheme a VANET model is defined and implemented against which messages are judged for correctness. In [84] emergency messages are relayed and false information is identified based on the kind of message and the subsequent behaviour of the sending vehicle. Such a technique will not be feasible for emergency messages which need to be acted on quickly. Also, such a scheme will increase the computation cost for the nodes.

A misbehaviour detection system and eviction mechanism is proposed in [56] where nodes are termed misbehaving if their info is inconsistent with the situation. Once a node is classified as misbehaving node then the neighbouring nodes can temporarily evict them by sharing warning messages about them and later their credentials are passed on to the CA which revokes them by adding them to a Revocation List (RL). However, RLs are themselves difficult to manage which is why data centric schemes are more suited to VANETs.

## 4.8 Summary & Research Methodology

The proposed scheme, C-DAC, is a decentralized mechanism that enables the nodes to detect and correct the data in the network. In a highly dynamic and fast moving network it is necessary to have a decentralized mechanism that enables the users to form an opinion about the validity and reliability of the data being exchanged without having prior knowledge of or interaction with the users. Moreover, as each node is calculating the parameters itself and sharing, comparing these parameters with other users in the network in its vicinity, each node should be able to experience the event directly as it gets closer. As the vehicle can trust its own data, therefore, once it detects false data it will start discarding the data it receives from that particular node. It then has the ability to report the identity of this node to others but they will have to form their own opinion about the malicious node.

The presented technique, C-DAC will be unable to identify the actual rogue node during a Sybil attack when the rogue node is presenting multiple identities / pseudonyms. Moreover, if there are multiple attackers that collude to launch an attack e.g. two or three cars intentionally block the lanes of the highway and send multiple messages with different identities reporting an accident or congestion then it will not be detected by C-DAC. The reason is that in such an attack the data will satisfy both the VANET model and will also match the vehicle’s own readings. However, such an attack is very expensive to launch as it requires multiple rogue nodes to be present together in a region.

In case of an actual accident the density increases all of a sudden whereas the flow value doesn’t go down as quickly, therefore, the flow value that a vehicle will calculate will increase for a short time before going down. During this transition phase, it is difficult to distinguish between a rogue node and an honest node except for the vehicle’s own observations and calculations. However, in the next chapter a statistical technique is presented that resolves this issue.

# Chapter 5： A Host Based Intrusion Detection System (IDS) for VANETs

## 5.1 Introduction

VANETs will become a reality in the very near future. The tremendous safety, convenience and commercial potential of vehicular networks will not only drive its deployment but will be fuelled by its demand as well once consumers realize its effectiveness. VANETs have the ability to make roads safer especially in conditions which are currently considered hazardous and unavoidable. Imagine the ability to be able to navigate safely in otherwise very dangerous driving conditions like fog, accidents, black ice. However, there are some very serious security issues that need to be addressed before the full potential of VANETs can be realized. Vehicular networks are very fast moving and highly dynamic due to which it is very important that the information being shared is authentic and actionable. As encounters will be short lived and the received information has to be acted upon very quickly, therefore, it is important that the reliability of the information is ascertained quickly.

In ad-hoc networks, maintaining and depending on trust or reputation is very expensive and a complex concept. In VANETs, centralized trust has long been debated as it is difficult to maintain, update and use. The existing mechanism for authenticating messages in vehicular networks involves the use of cryptography [27], [85], [28] and trust [39], [86], [87]. Cryptographic techniques involve paired keys and overhead in terms of computing cost, storage and time. Even with cryptographic techniques, security lapses are inevitable leading to intrusions due to stolen keys or compromised Trusted Authorities etc. An attack is especially difficult to prevent when it is launched from within the network. Due to the wireless and mobile nature of vehicular networks and its dynamic topology, it is not possible to use the same intrusion detection mechanisms that are used in wired networks. Therefore, it is essential that an intrusion detection system is deployed to detect attacks and help secure VANETs. The proposed IDS will detect different types of attacks launched by rogue or compromised nodes in the network. The IDS will then be able to minimize the damage to the network by taking necessary actions. The proposed IDS work in a distributed manner and is designed for deployment at each host node in the vehicular network.

Intrusion detection systems are very effective as they are able to detect attacks from insiders at real time but at the same time need to be updated for new attacks. Moreover, IDS need strong authentication and identification systems in order to work properly. Intrusion prediction systems on the other hand try to predict new attacks that can protect the system from unknown attacks. However, the probability thresholds need to be set carefully in such intrusion prediction systems to get accurate results. This work proposes an IDS that does not use trust or reputation and only relies on the analysis of the received data to detect intrusions in the network. The statistical technique used in the IDS declares data true or false which leads to the node being declared honest or rogue instead of the other way around.

## 5.2 IDS Overview

The host based Intrusion Detection System proposed in this work is deployed at each vehicle and is able to detect intrusions in VANETs and then take corrective measures to contain the damage. In order to train the IDS, a model of the network under normal conditions is needed so that deviations (anomalies) from the normal behaviour can be detected and alarms can be raised i.e. other vehicles can be informed. In the proposed model discussed in the previous section, the vehicles send their speed, calculated average flow, calculated density and location information to other vehicles. Also, each vehicle calculates its own value of average flow which provides them with a very good estimate of the traffic in their vicinity and up ahead as well.

The proposed IDS is shown in Figure 5-1. The IDS works by first collecting the data from neighbouring vehicles and using the host based intrusion detection mechanism to detect intrusions while incorporating the attack warnings from other vehicles. Once the intrusion is detected then a vehicle responds to the threat by taking some action i.e. rejecting the data from that vehicle, classifying the attack and then disseminating the information to other vehicles in the neighbourhood.

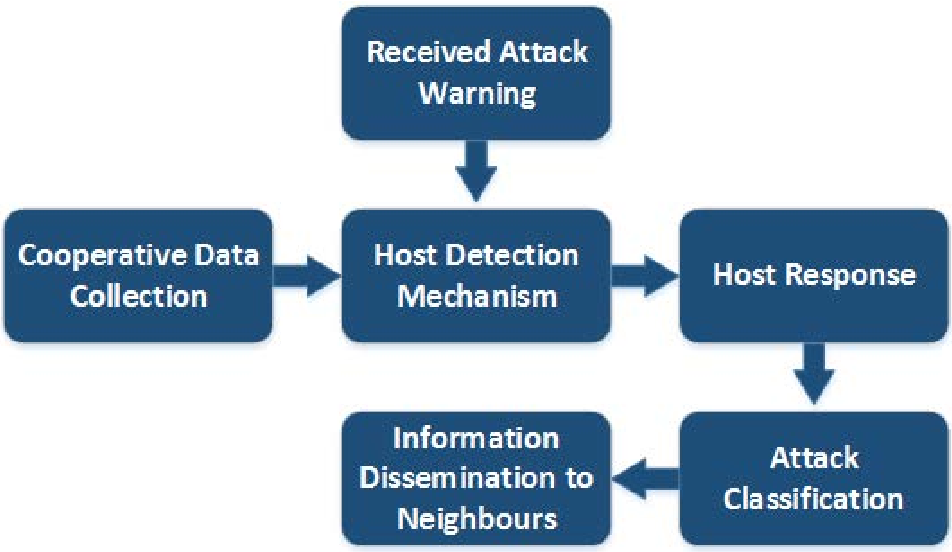


**Figure 5-1: Proposed Intrusion Detection System for VANETs**

### 5.2.1 Cooperative Data Collection

Using the proposed scheme each node (vehicle) collects data from other nodes (vehicles) in its vicinity to model the traffic around it. The vehicles cooperate with each other and share the values of their parameters using the Greenshield's model described above. As a vehicle will receive the parameter values from all other vehicles within range, therefore, each vehicle has information about all the vehicles in that region. Due to this each vehicle can calculate the (estimate) mean $\mu$. The trace data has shown that under all conditions the flow values will be close together and will lie within two standard deviations of the mean. This means that all vehicles that are within communication range are calculating very similar value of the Flow$_{AVG}$ as they are under similar traffic conditions. This is obvious as all nodes are dependent on other nodes to calculate their parameter values in all circumstances i.e. free flowing traffic and in case of an accident.

### 5.2.2 Normality Test

In order to check if we can apply t-test to our data we check if our data set follows a normal distribution. When all the readings / data has been gathered for a simulation, the conditions of the central limit theorem apply and we approach a normal distribution. To show this we plot the frequency distribution of the Average Flow Values (Flow$_{AVG}$) of a random node e.g. Node No. 90 in our simulation with vehicle inter-arrival time of 2 sec, transmission interval of 0.5 sec from simulation time t=203 sec to t=325 sec as shown in Figure 5-2. The data is slightly left skewed as vehicles start from rest and therefore, have lower values of flow in the beginning. This means that we are now in a position to set up a hypothesis test and use the t-test for detecting false values reported by a rogue / malicious vehicle. The t-test for comparing the two population means is used as the sample size can be small.

The parameter values follow a normal distribution and as the received values are in pairs, therefore, we use the paired t-test to calculate the probabilities associated with getting values in different ranges. The standard deviation and the test statistic $t_o$ are calculated as:

$$t_o = \frac{\bar{x} - \bar{y}}{\sqrt{\frac{s_x^2}{n_1} + \frac{s_y^2}{n_2}}}$$

Here, $\bar{x}$ is the mean difference of the received values and $\bar{y}$ is the mean difference of vehicle's own calculated values, $s_x$ and $s_y$ are the standard deviations of received and vehicles own calculated values respectively. $n_1$ and $n_2$ are the number of samples for the received and own values respectively. The degrees of freedom will be:

$$n_1 + n_2 - 2$$

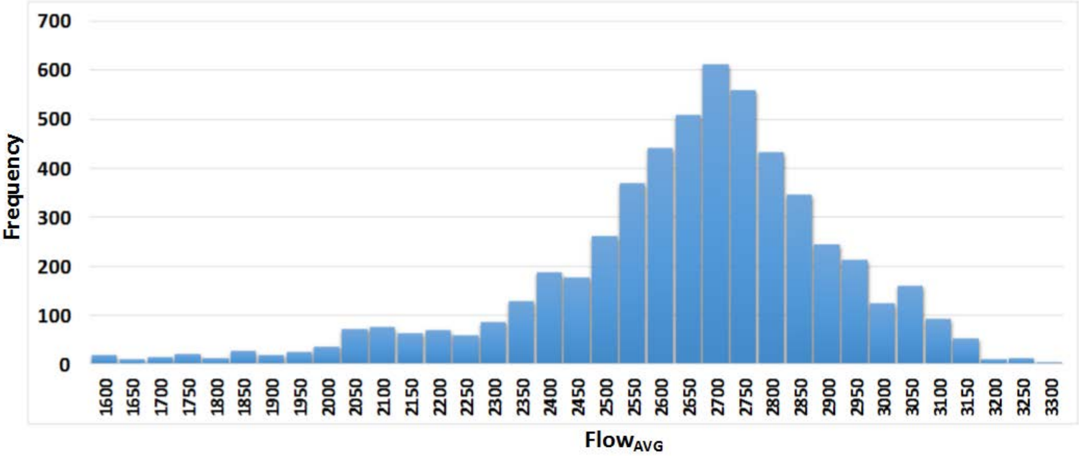


**Figure 5-2: Normal Distribution of Flow$_{AVG}$ for Node 90 from t=203s to t=325s**

The algorithm of the proposed IDS is given in below:

**Algorithm 1: Algorithm for proposed IDS**

**Each received msg contains: (each vehicle's calculated) Flow, Speed, Density**

```
FOR each msg received DO
    Update $Density_{calc}$
    Update $Speed_{AVG}$
    $Flow_{OWN =}$ $Speed_{AVG}$ x $Density_{calc}$
    IF  Hypothesis Test == Reject
    (i.e. $Flow_{Rcvd}$ - $Flow_{OWN}$ > Threshold : t-test carried out here)
       THEN
       Reject Data
       (Node could be reported to authorities here but not being dealt with in this
       algorithm)
       Calculate $Flow_{AVG}$
    END IF
    ELSE
       Accept Data
       Calculate $Flow_{AVG}$
END FOR
```

The data is collected from all neighbouring nodes and checked if there is a significant difference between the calculated and received values. If there is a significant difference then the node is monitored and some parameter values are collected (accepted) initially. Once sufficient samples have been collected then the t-test is carried out. If the t-test gives a result within the acceptance region then the data is accepted else rejected. If the data is rejected then the node is highlighted as rogue and the attack is classified as Information Attack and subsequent values from that node are rejected. A message can then sent to other users informing them of the rogue node and the type of attack being launched by that node. The flow chart is given in Figure 5-3.

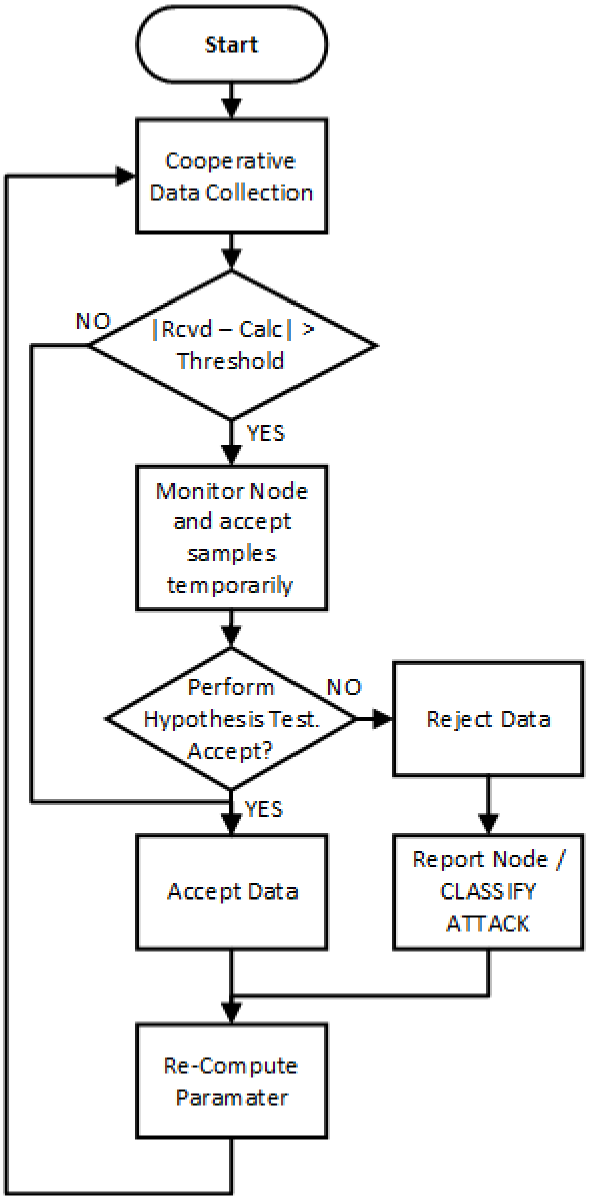

Start
Cooperative Data Collection
NO
|Rcvd – Calc| > Threshold
YES
Monitor Node and accept samples temporarily
Perform Hypothesis Test. Accept?
NO
Reject Data
YES
Accept Data
Report Node / CLASSIFY ATTACK
Re-Compute Paramater

**Figure 5-3: Flow Chart of proposed IDS**

### 5.2.3 Hypothesis Testing for Data Correctness

Hypothesis testing is a common technique used in engineering applications to test two claims when only one of them can be true. The hypothesis testing approach also assigns a confidence interval to a range of values that enables us to accept a claim with a certain confidence. This suits us as in our VANET model and proposed IDS there are two possibilities i.e. either the node is honest and we accept its data or the node is rogue and we reject its data. To check whether hypothesis testing works well in our model, we ran the simulations numerous times in OMNET++ and then exported the data to MS Excel and Matlab to analyse and visualize it.

We use hypothesis testing to decide whether a received parameter value should be accepted or not. If the received value is within the 99% confidence interval i.e. within the acceptance region, then the value is accepted. If the received flow value is within the rejection region then it is rejected. This is shown in Figure 5-4. There are always two hypotheses stated, there is the null hypothesis $H_o$ which we want to test (and assumed to be correct) and alternate hypothesis $H_a$. If the null hypothesis is rejected then the alternate hypothesis is accepted and if we do not have enough evidence against the null hypothesis then it is accepted. The null hypothesis $H_o$ in our case is that the data (Flow value) received is from an honest node. The alternate hypothesis $H_a$ is that the value received is false (from a rogue node) and we fail to accept (reject) it. In other words we say that we don't have enough evidence to accept the received data and therefore, we reject it. The Hypotheses that will be tested in the host IDSs are stated below:

**$H_o$: Accept Received data (Node is Honest)**

**$H_a$: Reject (Fail to Accept) Received data (Data is false Node is Malicious or Rogue)**

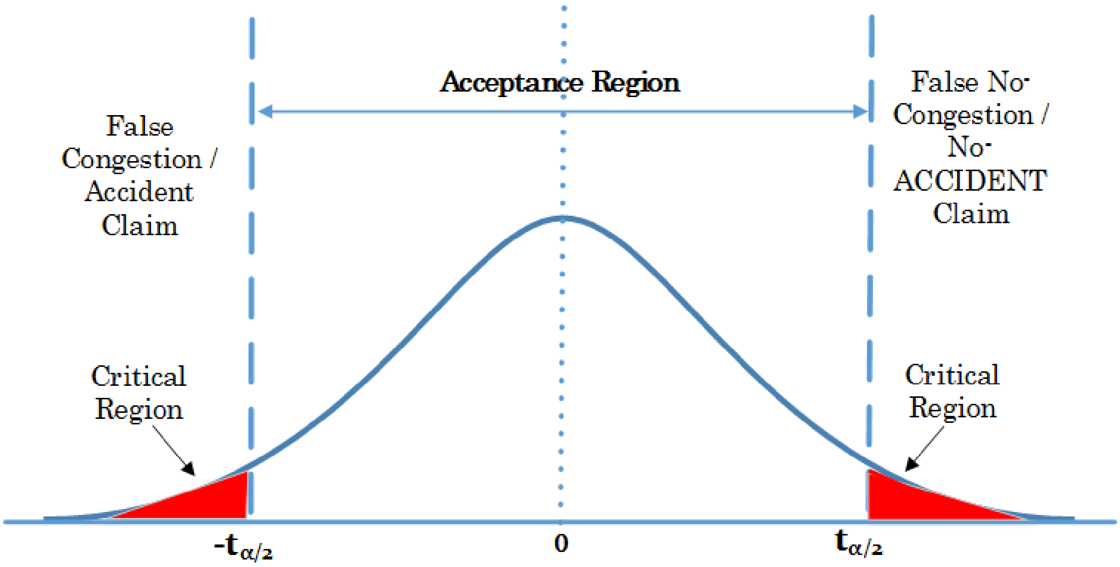


**Figure 5-4: Distribution of $t_o$ for $Flow_{AVG}$**

The IDS in each vehicle also computes a p-value that helps it in accepting or rejecting the null hypothesis. The p-value gives the probability of getting a value which is at least as extreme so, the p-value gives information about the weight of evidence against the null hypothesis $H_o$ i.e. the smaller the p-value the greater the evidence against $H_o$. There are two types of errors associated with hypothesis testing as shown in Table 3. In our scenario, Type-2 error (false negative) is not very serious as the worst case scenario is slowing down whereas Type-1 error (false positive) is very serious.

| | **Node is Honest - H$_o$** | **Node is Rogue - H$_a$** |
|---|---|---|
| **Accept H$_o$** | No Error | Type 2 Error |
| **Reject H$_o$** | Type 1 Error | No Error |

**Table 5.1: Decisions in Hypothesis Testing**

Therefore, keeping this in view we use a wide confidence interval. The level of significance is denoted by α. The usual values of α are taken to be 0.01(1%) or 0.05(5%) which means the probability that the test statistic falls in our acceptance region is 1 - α and the confidence interval for the two values of α = 0.01 and 0.05 are 99% and 95% respectively. We take the value of α to be 0.01 and as this will be a two-tailed test therefore, the upper and lower limit of our acceptance region will be $t_{\alpha/2}$ & $-t_{\alpha/2}$ as shown in Figure 5-4. The degrees of freedom will be $n_1 + n_2 - 2$ and the corresponding limits can be looked up from the t-table. This means that the probability is α that the test statistic $t_o$ falls in the region $t_o > t_{\alpha/2}$ or $t_o < -t_{\alpha/2}$ when the null hypothesis $H_o$ is true. Therefore, we will reject the received value if it is outside the acceptance region i.e. we reject the value if either:

$$\boldsymbol{-t_{\alpha/2} > t_o > t_{\alpha/2}}$$

In our case the received flow values for any chosen node are always within the acceptance region or within the 99% confidence interval as long as the node is honest. In the case of an accident as the values will drop, they will have an impact on all vehicles in the region which will bring down the Flow$_{AVG}$ value for the region and as a result the values are still within the acceptance region as the standard deviation increases.

As shown in Figure 5-4, there are two cases where the rogue node will falsify its values i.e. it can either deny congestion or accident or it can wrongly give the impression of congestion or accident. Therefore, the IDS can decide which category the false information falls under depending on whether $t_o > t_{\alpha/2}$ or $t_o < -t_{\alpha/2}$.

## 5.3 Simulation under Different Conditions

### 5.3.1 Simulation Setup

In order to check the proposed IDS extensive simulations were done using OMNET++, SUMO [81] and VACaMobil [82]. OMNET is a modular C++ library and framework that is used for network simulations. Simulation of Urban Mobility (SUMO) is a software tool used to generate vehicular traffic by specifying speed, types, behaviour and number of vehicles. SUMO also sets up road types and conditions. VACaMobil is a car mobility manager for OMNET that works in parallel with SUMO.

| Simulation Parameter | Value |
|---|---|
| Simulation Time | 500 sec |
| Scenario | 3 Lane Highway |
| Highway Length | 5-Kms |
| Max Vehicle Speed | 28 m/sec or 100 Km/hr |
| Mobility Tool | VACaMobil |
| Network Simulation Package | OMNET++ |
| Vehicular Traffic Generation Tool | SUMO |
| Vehicle Density | 20-30 veh / Km |
| Wireless Protocol | 802.11p |
| Rogue Vehicles | Varied from 5% to 40% |
| Transmission Range | 500m in each direction |

**Table 5.2: Simulation Parameters**

### 5.3.2 Simulation Parameters and Assumptions

The simulation is run on a 3 lane highway (motorway i.e. no traffic signals) with a total length of 5 Kms and the total simulation time is 500 secs. On average there are 20 to 30 vehicles per kilometre stretch of the highway. The vehicles start from rest when they enter the simulation and gradually attain a maximum speed of 100 km/hr. The transmission power is set so that each vehicle can receive transmissions from up to 500m from either side. Moreover, the vehicles are assumed to have directional antennas so that they can determine if a signal was received from the front or back. The number of rogue vehicles is varied from 5% to 40% of the total vehicles in the simulation to study the effect on the stability and performance of the proposed IDS. The simulation doesn’t assume any radars, cameras on-board. The simulation parameters are shown in Table 5.2.

### 5.3.3 No Accident - Rogue Nodes Scenario

A scenario is simulated in which there is no accident but rogue nodes start transmitting a low false value of Flow after t=160 sec. We run the simulations both with and without the proposed IDS and also vary the number of rogue / malicious nodes and collect the data. The results are shown with and without the proposed IDS in Figure 5-5, when there are 20% rogue nodes. As shown in **Error! Reference source not found.** the flow value goes down at first while the IDS runs the hypothesis tests to evaluate the received data and then starts to reject the false values. However, in the absence of the IDS (Figure 5-5) the Flow value is reduced as all the values are accepted.

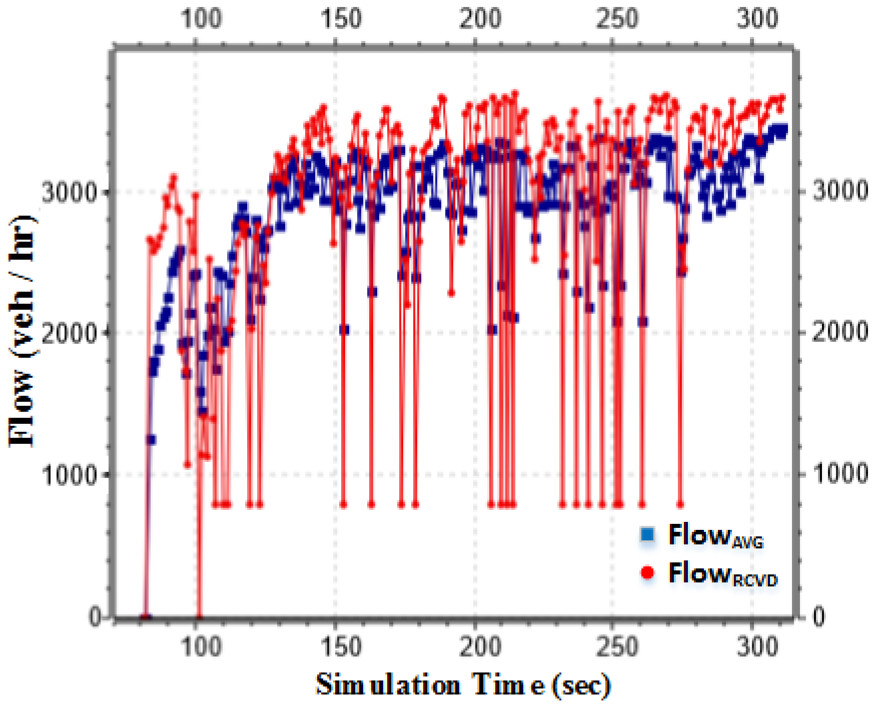


**Figure 5-5: No Accident Scenario - 20% Rogue Nodes start transmitting false values at t=160sec Without IDS**

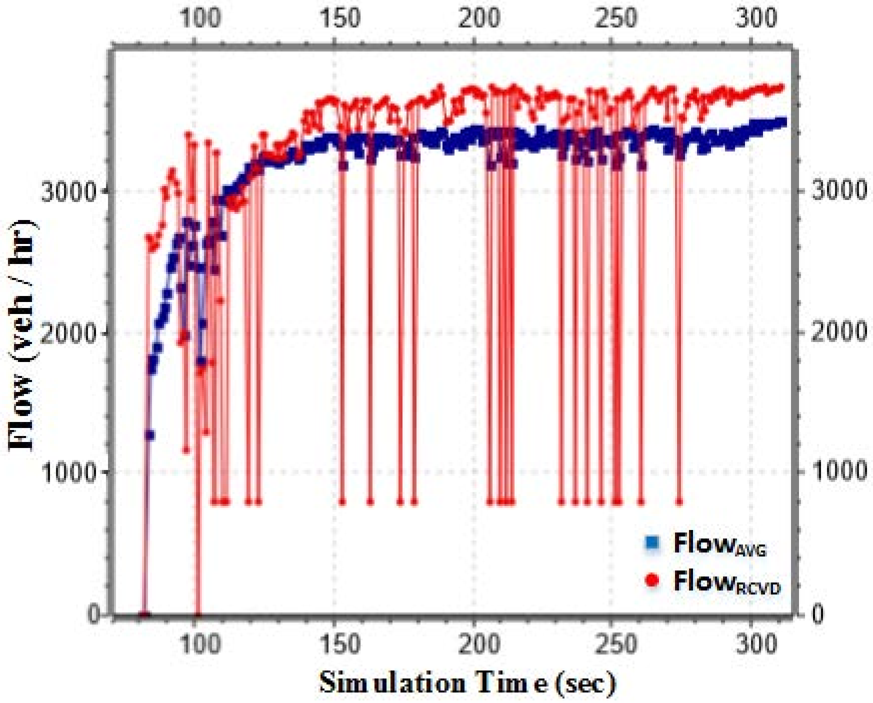


**Figure 5-6: No Accident Scenario - 20% Rogue Nodes start transmitting false values at t=160sec With IDS**

### 5.3.4 Accident Scenario - Rogue Nodes Scenario

An accident scenario is simulated where rogue nodes start transmitting false (high) values after t=230 sec after an accident has occurred to deny the accident. The time t=230s is chosen so that the accident occurs at the end of the highway in the simulation. The simulation is run both with and without the IDS and the results are shown in Figure 5-7 & Figure 5-8 respectively. Figure 5-7 shows that honest nodes have started transmitting the low flow values to account for the accident but the rogue nodes are still transmitting high values to show as if there is no accident.

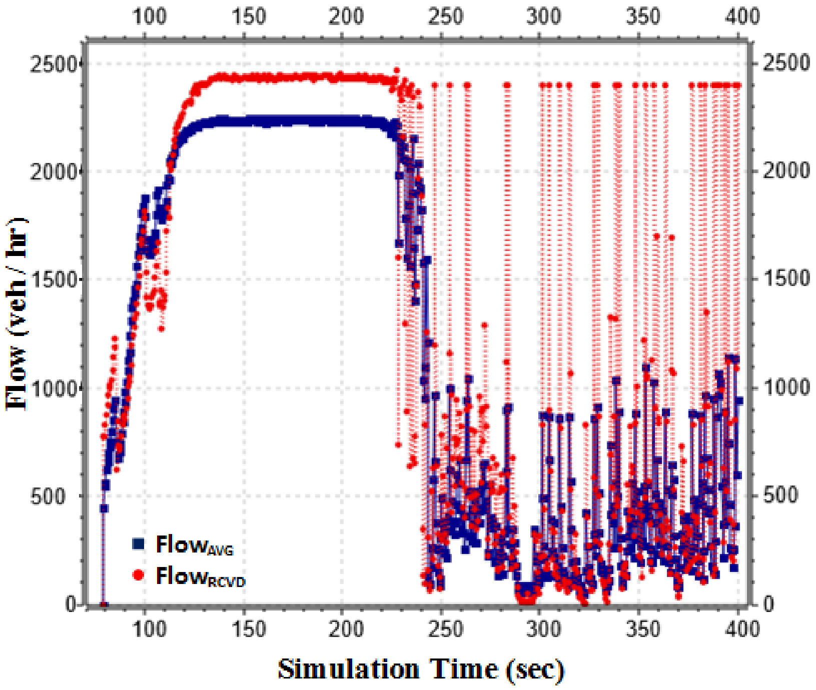


**Figure 5-7: Accident Scenario: 20% Rogue Nodes - start transmitting false values at t=230sec Without IDS**

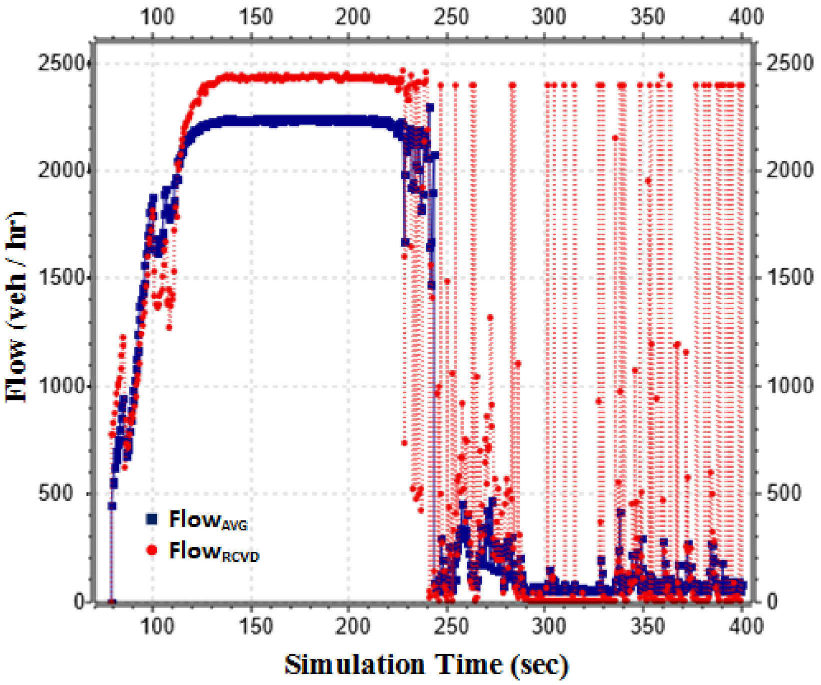


**Figure 5-8: Accident Scenario: 20% Rogue Nodes - start transmitting false values at t=230sec With IDS**

It can be seen in Figure 5-8 that the very high values by rogue nodes are being rejected by the IDS.

# 5.4 Performance Evaluation

## 5.4.1 Evaluation Metrics

The performance of the IDS is tested by computing the True Positive (TP) rate (detection rate), the false positive rate and the detection time. The number of rogue nodes was increased from 5% to 40% to test how successfully the proposed IDS classifies rogue nodes as rogue and honest nodes as honest. We also compare our results with that of two previous schemes that deal with false information attacks i.e. [84] and [69]. The metrics used are described below:

#### 5.4.1.1 True Positive (TP):

This is the detection rate of rogue nodes (RNs) i.e. what percentage of rogue nodes is detected and classified as rogue nodes. This is also referred to as sensitivity and is calculated as:

$$TP = \frac{No.of\ RNs\ detected\ correctly}{Total\ No.of\ Rogue\ Nodes}$$

#### 5.4.1.2 False Positive (FP):

This is the percentage of honest nodes (HNs) incorrectly classified as rogue nodes. Specificity is defined as the number of honest nodes correctly identified and given as:

$$Specificity = \frac{No.of\ Honest\ Nodes\ Identified\ Correctly}{Total\ No.of\ Honest\ Nodes}$$

and the false positives are calculated as:

$$FP = 1 - Specificity$$

#### 5.4.1.3 Overhead:

The overhead is the cost incurred due to the IDS working and the extra data that is exchanged with other vehicles. It is an important metric as it is a measure of the efficiency of any scheme.

### 5.4.2 Comparison with Existing Schemes

The proposed IDS is able to detect false information attacks very effectively by only analysing the data without taking into account any Trust or Reputation scores. The proposed mechanism is compared with two schemes i.e. DCMD [84] and ELIDV [69]. ELIDV uses the greedy forwarding protocol i.e. the vehicle which is furthest away from the communicating vehicle transmits the packets. Therefore, if a vehicle is a forwarder node then it should be located on the transmitter's radio range boundary. ELIDV analyses the behaviour of the nodes after it sends an emergency message to determine if the information is correct or not. DCMD checks the time it takes the message to reach the node receiver based on the claimed position. Even if the sender changes the time stamp, it can still be detected as the sender vehicle doesn't know the distance to the receiver node accurately.

### 5.4.3 False Information Attack Detection

The detection rates are shown in Figure 5-9 and false positive rates are compared in Figure 5-10. The detection rate (True Positives) of the proposed scheme is better than DCMD and ELIDV up to 30% rogue nodes and almost the same as

ELIDV after that till 40%. The false positive rate of the proposed scheme is better than DCMD and ELIDV up to 20% rogue nodes but increases slightly above ELIDV at 40%. The proposed IDS works better than DCMD and ELIDV mainly because the other two schemes are based on verifying the claimed location of the vehicles whereas the proposed IDS looks at the overall situation of traffic and analyses to see if it receives emergency messages from other vehicles in the same region. This means that in DCMD and ELIDV, as the number of rogue nodes increases, the performance of the system degrades. However, in the proposed IDS even if vehicles collude they can't affect the overall parameter values in the whole region. This performance comparison can be seen in Figure 5-9 and Figure 5-10.

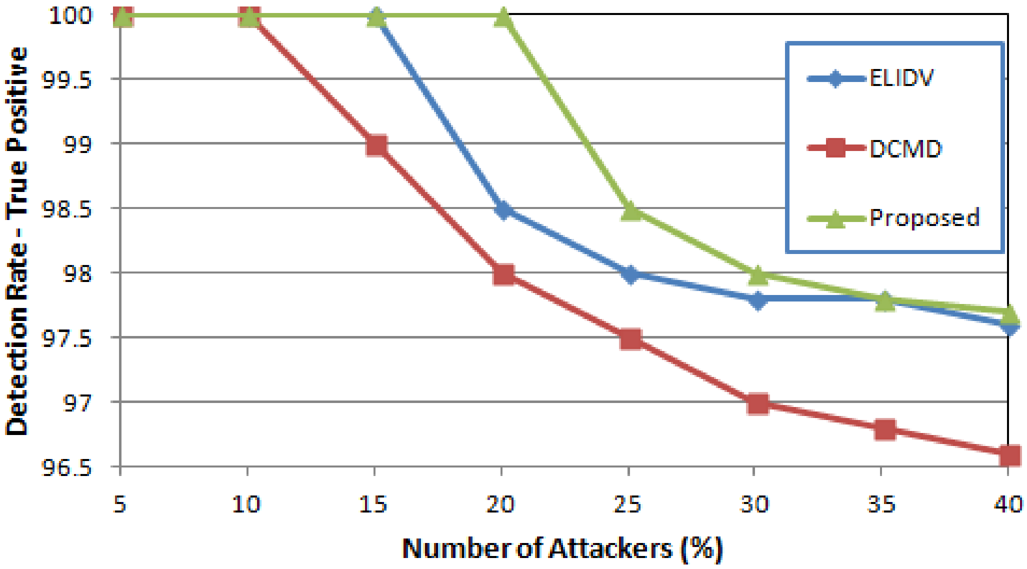


**Figure 5-9: Detection Rate Comparison in case of False Information Attack**

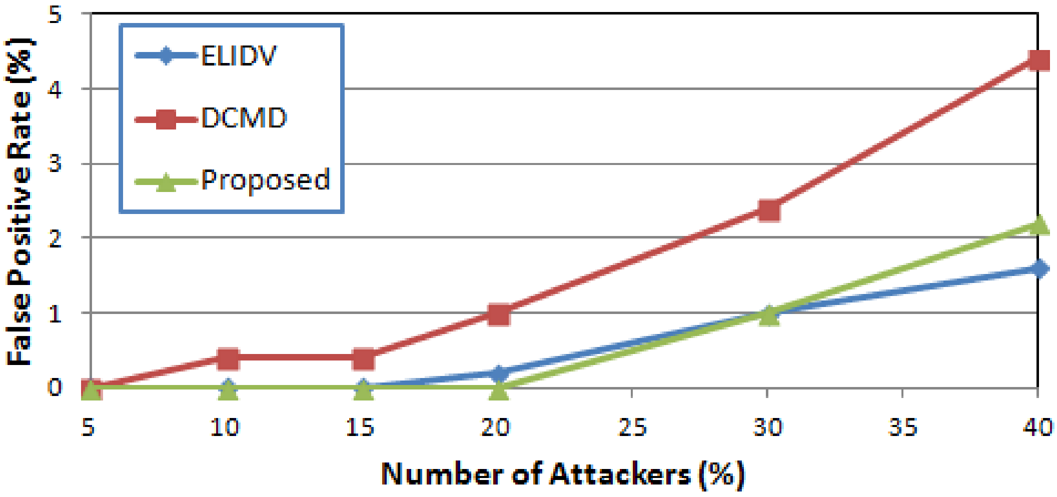


**Figure 5-10: False Positive Rate Comparison in case of False**

### 5.4.4 Resilience to Sybil Attacks

In a Sybil attack, an attacker presents multiple identities with an intent to either create the illusion of congestion or accidents or deny their existence. So, a rogue vehicle will send multiple messages in order to cause confusion in the network by bringing the parameter value down. However, the proposed IDS aggregates the parameter values, therefore, the IDS will work very well and will be resilient to Sybil attacks as long as the total number of Sybil identities is less than 40% of the total identities (nodes) as shown in Figure 5-9 & Figure 5-10.

### 5.4.5 Overhead Comparison

The overhead of the proposed IDS is compared with the schemes in [84] and [69] and result is shown in Figure 5-11. The overhead in the proposed IDS is less as compared to DCMD and ELIDV except when there are 40% nodes at which point it is slightly higher than DCMD. The overhead in the proposed IDS increases with the increase in number of rogue nodes as the IDS starts to collect more past values to run the hypothesis test. However, the proposed IDS does not need to keep past parameter values as long as they agree with the calculated values which is the reason why the initial overhead is low and increases with the increase in the number of rogue nodes as shown in Figure 5-11.

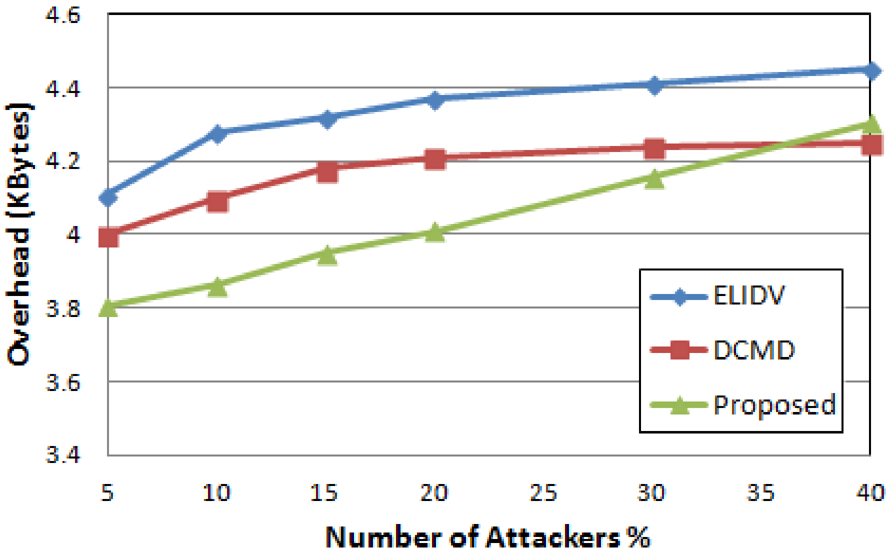


**Figure 5-11: Overhead Comparison in case of False Information**

### 5.4.6 Bootstrapping Problem

Any system needs time to start-up and start working correctly which is known as bootstrapping. Similarly, the proposed IDS has to start-up and collect a few samples before it can give correct decisions. The analysis shows that the IDS can bootstrap quickly and can give correct decisions by successfully conducting tests by taking only 7 samples from any node and performing the t-test on the population mean of two populations. The 7 samples can be collected in a minimum of 0.7 seconds if the beaconing rate is 100 ms. This means that the IDS enables the nodes to quickly decide whether to accept or reject the data received without generating a lot of overhead. Therefore, the bootstrapping problem is quite manageable in the proposed IDS.

### 5.4.7 Countermeasures & Fault Tolerance

The proposed VANET model and exchange of parameters give the vehicular network a built-in resilience to launch countermeasures against false information attacks. The data is highlighted as false or malicious if it does not conform to the VANET model or if it fails the hypothesis test. The countermeasures include rejecting the data of that node and reporting the node as malicious. This was shown in **Error! Reference source not found.** & Figure 5-8 where the values were too low or too high as compared to the node's own values and were detected (and then rejected) by the IDS. The IDS is therefore, fault tolerant as it can work in the presence of false information.

### 5.4.8 Effective Information Dissemination

The widely proposed method of propagating emergency messages is by repeatedly broadcasting the message by vehicles to others behind them. This can quickly cause a broadcast storm in an already bandwidth limited channel. In the proposed scheme there is no channel congestion as there is no need for multi-hop retransmissions and the information is still disseminated effectively.

### 5.4.9 Limitations of proposed IDS

The proposed IDS works extremely well when the difference between the received values and the calculated values is high i.e. the values being received from the rogue nodes are too high or too low. However, if the rogue nodes coordinate and gradually decrease (or increase) their parameter values and launch the attack over some time then it will be very difficult to detect the attack. The reason is that the gradual decrease in the parameter values will not be flagged as an anomaly and thus never tested for correctness. However, as discussed previously doing this defeats the main purpose of the rogue / malicious vehicles i.e. to cause maximum damage or confusion in the network.

## 5.5 Summary & Research Methodology

The results show that the proposed IDS is scalable and has an excellent performance when the number of rogue nodes is small. The performance degrades when the number of rogue nodes increases but still works reasonably well. The proposed model and IDS demonstrate the effectiveness of the statistical technique used to determine if the data is false based on the overall collected data without using Trust or reputation scores. The IDS does not depend on any infrastructure which is a major benefit as compared to other schemes. The false data is much easier to detect if it differs too greatly from the calculated data and difficult to detect if it varies slightly. However, the target of the rogue node is to drop or raise the value of its parameters quickly to damage the network and increasing or dropping it gradually is not in its interest.

In the future, the work can be extended by modifying the IDS to detect other types of attacks in VANETs such as Denial of Service and false position reporting by rogue nodes in the network or a stationary user outside the network. This can be done by simulating the attacks using the developed platform and then detecting them with the help of anomaly or rule-based detection.

# Chapter 6 : Identity Management and Sybil Attack Detection in VANETs

## 6.1 Introduction

The concept of identity in computer networks has been under discussion for a long time now. An excellent definition of identity in networks is given by J. R. Doucer in [45] as:

> *"An identity is an abstract representation that persists across multiple events"*

Identities are important in networks as they establish a user's physical presence in the network. Therefore, it is important that these identities are easy to create, use and verify. However, there are many complexities involved in the creation and verification of identities in the digital world that will be discussed in detail in this chapter. It is also important to note that the failure to handle identities in VANETs can result in Sybil attack which can have serious consequences. The Sybil attack and its detection will be discussed later in this chapter but first the security and privacy goals in VANETs are discussed briefly to understand the intricacies.

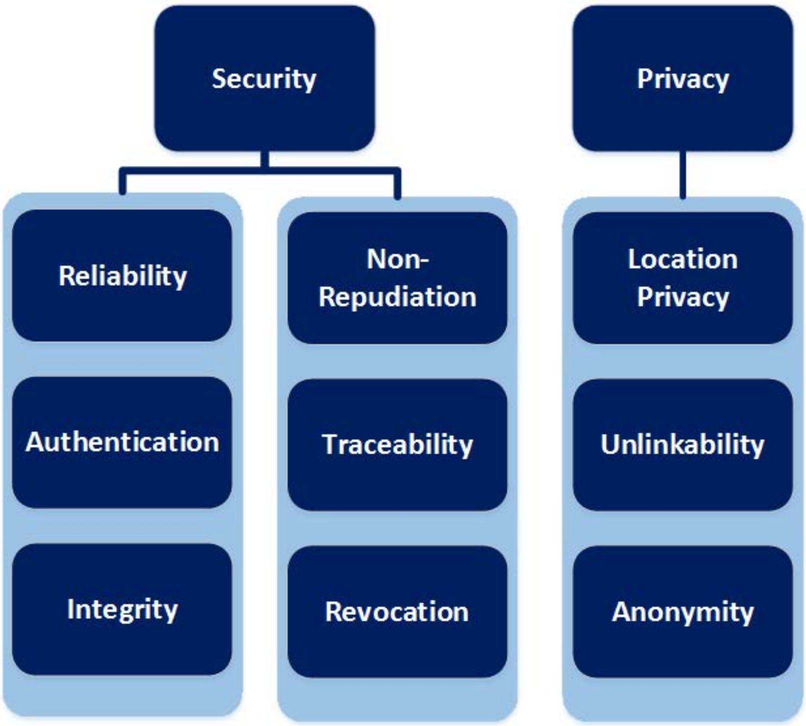


**Figure 6-1: Security and Privacy Goals in VANETs**

## 6.2 Security and Privacy Goals in VANETs

The security and privacy goals in VANETs, how they are achieved and what they provide are shown in Figure 6-1. Thus the goals are:

i. Reliability

ii. Location Privacy

iii. Non Repudiation

### 6.2.1 Reliability

As the information in VANETs is very critical for safety, it is imperative that it should be reliable. Reliability is achieved through authentication, which ensures the integrity of the messages, i.e., they have not been tampered with in transit. Authentication can be done between the Certificate Authority and the vehicle using PKI.

### 6.2.2 Location Privacy

It is essential for VANET security that the location of a vehicle is transmitted while preserving the location privacy of the user. However, this location information can be used by adversaries in tracking vehicles or routes. As discussed previously, location privacy requires unlinkability, which ensures anonymity. This unlinkability is achieved by changing Pseudonyms so that successive messages can't be linked to each other.

### 6.2.3 Non-Repudiation

Another requirement for VANETs is non-repudiation, which means that users should not be able to deny sending a message so that they can be tracked and penalized in case of a false message. This is achieved by making the messages traceable but only by the authorities so that they can be revoked. We have proposed in [6] that the tracing should be done by multiple authorities in order to provide extra security and privacy.

## 6.3 Identity in VANETs

The current concept of identity in VANETs needs to be revisited. The existing concept of using the identity (ID) of the vehicle i.e. Vehicle identification number (VIN) number or its registration number might not be useful for the authorities as the driver can later deny using the vehicle when a particular violation occurred or claim that it was stolen. On the other hand, it is also possible that the vehicle might actually be stolen and might be used to launch an attack from inside the VANET. Our scheme provides a solution to these problems.

The nature of VANETs requires reliability of messages and this implies authentication and non-repudiation. Moreover, the messages being transmitted by the vehicles should be verified quickly and efficiently. At present we are only presenting the mechanism for V2I communication as the RSUs have much higher computation power available than the OBU. We present a way to join the driver's identity with that of the vehicle and use this as the Digital Identity in VANETs (DIVA). The idea is that when there is a driver's (human's) ID being used for signing the messages, the user will be bound to act much more responsibly as it can carry serious consequences. DIVA scheme uses ID based cryptography which enables the user to encrypt the messages to the RSU using the RSU's public ID and sign it using his own ID. Furthermore, we propose two trusted authorities (TA1, TA2), as shown in Figure 6-2, for added security and privacy and to remove the strong assumption of tamper proof devices for keeping the ID of the user secure.

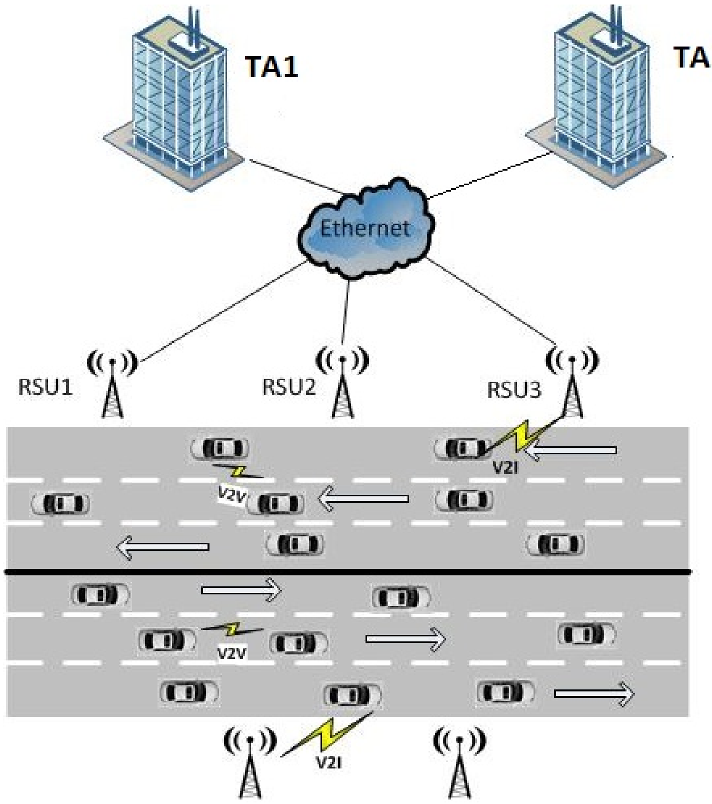


**Figure 6-2: Proposed VANET Architecture**

### 6.3.1 Digital Identity in VANETs

The current concept of identity in VANETs is the registration number of the vehicle or the VIN number of the vehicle [24], [88]. However, this identity is not very useful as it is the driver who is responsible for the vehicle and not the owner. Also, the driver might later deny using the vehicle at the time a violation occurred. Therefore, the current suggestions of revoking a vehicle in case of a violation are not really practical as it is the driver who should be penalised and not the vehicle. Also, penalising a vehicle is difficult as the vehicle might be used by multiple drivers.

In order to solve the above mentioned issues, a scheme is proposed - Digital Identity in VAnets - DIVA [6]. We propose that the driver's identity (driver's license) be linked to the vehicle thereby, forming a new joint identity. This allows authorities to penalise the driver by giving penalty points (in case of minor offence) or driver revocation (in case of serious offence). However, the identity of the driver and the vehicle are only authenticated with the TAs that do not share this information with any other entity. Furthermore, it is only the TAs who can de-anonymize the driver and vehicle and nobody else. This digital identity (combination of the Driver Identity- DrID and the vehicle identity - VID), will now function as the digital identity (DID) in VANETs as shown below (Figure 6-3).

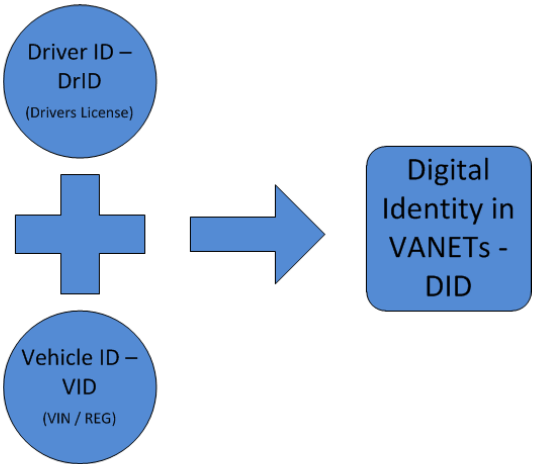


**Figure 6-3: Digital ID (DID) in VANETs**

### 6.3.2 Assumptions

We propose minor changes in the capability of the OBUs. The enabling technologies are already in place to be made use of for making our system smarter and more efficient. We propose that the OBU, apart from having some storage and processing power has following added capabilities:

i. The ability to read a driver's license

ii. An on-board keyboard for input.

iii. An LCD screen

iv. Wireless Internet capability

These capabilities of the OBU are shown in Figure 6-4.

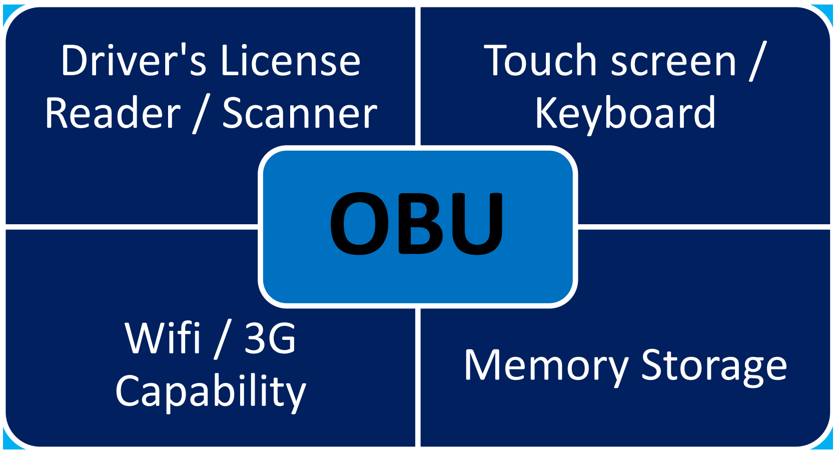


**Figure 6-4: OBU Capabilities**

### 6.3.3 Registration and Key Management

The OBU connects to the TAs using wifi / 3G using TLS/ SSL and establishes a secure connection. The driver first authenticates himself with TA1 using two factor authentication (TFA). The driver has to swipe his driver’s license and use the keyboard to enter his PIN or password and another piece of information which only the holder of the license will have (e.g. a number on the driver’s license counterpart in UK or the output of a smart phone app corresponding to the driver’s license number). The PIN or password is a pre-set password between the user and the TA1 - Licensing Authority (e.g. DVLA in the UK). This password can initially be setup between the two parties while getting the driver’s license and then the user has the option of changing this by going online at the authority’s website. In [26], authors propose a similar technique i.e. the user has many keys with him at home provided by the TA which the user manually stores in the OBU before going out. Similarly, the OBU authenticates itself withTA2 - Motor Vehicle Registration Authority, which contains the record of all vehicles, where driver enters a password for the vehicle and some information which is provided in the Vehicle Registration document (i.e. ensuring TFA). This ensures that the vehicle is indeed being operated by the owner or an authorized person.

Upon successful authentication the driver is issued a token- TK1 by TA1 which is signed by TA1 and the master secret key s1 is also transferred to OBU. Similarly, the OBU is issued a token - TK2 by TA2 and issued the master secret key s2.This key setup mechanism is shown in Figure 6-5.

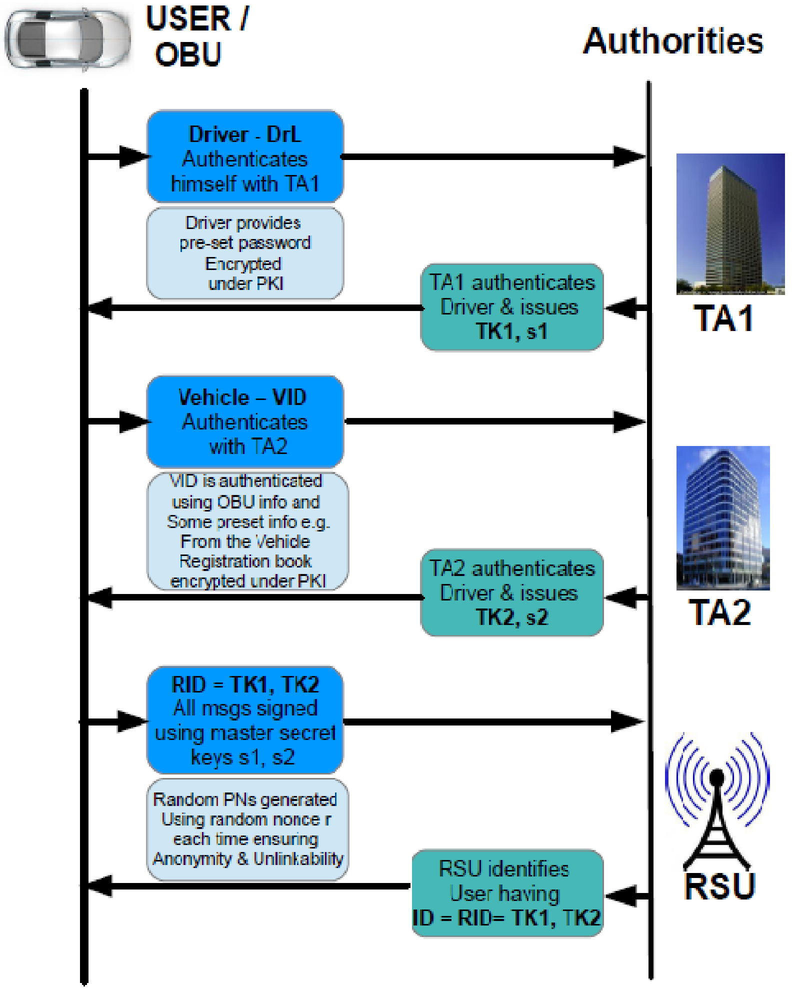

USER / OBU
Authorities
Driver - DrL Authenticates himself with TA1
Driver provides pre-set password Encrypted under PKI
TA1 authenticates Driver & issues TK1, s1
TA1
Vehicle – VID Authenticates with TA2
VID is authenticated using OBU info and Some preset info e.g. From the Vehicle Registration book encrypted under PKI
TA2 authenticates Driver & issues TK2, s2
TA2
RID = TK1, TK2 All msgs signed using master secret keys s1, s2
Random PNs generated Using random nonce r each time ensuring Anonymity & Unlinkability
RSU identifies User having ID = RID= TK1, TK2
RSU

**Figure 6-5: Sequence Diagram for Proposed Scheme**

### 6.3.4 Scheme Details

The tokens and master keys $s_1$, $s_2$ received by the user are used to generate PNs to sign and encrypt messages sent to the RSUs. Our scheme uses the Boneh and Franklin's Identity Based Encryption using Weil pairing [23] and extends the schemes presented in [24], [89]. The OBU uses the public ID of the RSU to encrypt its messages whereas the RSU uses its private key $d_{ID}$ to decrypt the message. The details of our scheme are given below in detail.

**i. Setup:**

Let G1 be a group of prime order q. Let e : $G_1 x G_1 \rightarrow G_2$ be an admissible bilinear map i.e. $e(aP; bQ) = e(P;Q)^{ab}$ for all $P, Q \epsilon G_1$ and all a; b ϵ Z and let P be a generator of $G_1$. In such groups the DDH problem is easy but the CDH problem is believed to be hard [21] e.g. given $P; aP; bP; cP\epsilon G$ and any $a; b; P \epsilon Z,$ there exists an efficient algorithm to determine ab = c mod q by checking $e(aP; bP) = e(P; cP)$ while there exists no algorithm to compute $abP\epsilon G$ within polynomial time.

TAs pick a random $s_1$ and $s_2 \epsilon Z$ and set $P_{pub} = s_1P$.Choose hash functions $H_1, H_2, H_3, H_4$. System Parameters are $\{P, P_{pub}, H_1, H_2, H_3, H_4\}$. The master keys are $s_1$ and $s_2$.

**OBU Uses:**

*PID (Pseudo-ID)* = TK1‖TK2, where ‖denotes concatenation

$g_{ID} = e(Q_{ID}; P_{pub}),$

$ID_1 = r.P$

$ID_2 = PID \oplus H (r.P_{pub})$, where ⊕ denotes XOR operation,

where r is a random nonce and changes each time therefore,

$ID_1$ and $ID_2$ change providing unlinkability

$$SK_1 = s_1.ID_1 , SK_2 = s_2.H(ID_1 \| ID_2),$$

$$ID^i = ID_1^i \| ID_2^i$$

**ii. Extract:**

For a given RSU ID, the algorithm computes

$Q_{ID}$ = H$_1$($ID$) and set private key of RSU to $d_{ID}$= $s_1.Q_{ID}$

**iii. Encryption:** Compute $Q_{ID\_RSU} = H_1(ID_{RSU})$

$$\sigma_\mathrm{i} = SK_1^i + H_2(M_i)SK_2^i$$

Set $R = H_3\,(\sigma_i, M_i)$

The transmitted message has the following format:

$$\{U, V, W, X\} = \{ID, \sigma_i \oplus H_2\,(g_{ID}^r), M_i \oplus H_4(\sigma), R \cdot P\}$$

**iv. Decryption and Signature Verification:**

In order to verify the signature the RSU does

1. Compute $\sigma$ = V $\oplus H_2\,(e\,(d_{ID}; ID_1))$ where $ID_1 = rP$

2. Compute $M = W \oplus H_4(\sigma)$

3. Set $R = H_3\,(\sigma, M)$:

Test that $X = R.P$ and if not then reject the message.

**iv. Traceability & Revocation:**

In the event of a violation or misuse the RSU can trace the user by doing the following:

$$
\begin{aligned}
ID_2 \oplus H(s_1.\,ID_1) &= PID \oplus H(r.P_{pub}) \oplus H(s_1.ID_1) \\
&= PID \oplus H(r.s_1.P\ ) \oplus H(r.s_1.P\ ) \\
&= PID \\
&= \mathrm{TK1} \,\|\, \mathrm{TK2}
\end{aligned}
$$

The RSU can now add the tokens TK1 and TK2 to its RL and also forward to other RSUs for adding to their RL. RSU now sends the tokens to TA1, TA2 to de-anonymize and penalise the user.

## 6.3.5 Authentication & Non-Repudiation

The user authenticates himself with TAs to get $s_1$, $s_2$ and TK1, TK2 and then signs all messages to RSU based on his secret keys SK1 and SK2 which are based on TK1 and TK2. Therefore, nobody else can forge a user's signature without knowing TK1 and TK2. Moreover, even if the RSU or the master key is compromised, the attacker still won't be able to determine the real ID of the user i.e. DrL and VID. The attacker only retrieves TK1 and TK2 which only TA1 and TA2 can trace. Therefore, there is an added layer of security and privacy in our scheme. Similarly, the driver can't deny having authenticated themselves with TAs using TFA thereby preventing impersonation. However, authentication only proves that a user was trusted at least when the keys were issued [27]. To check if the user has been revoked since then, the RL would have to be looked up and the information in messages would have to be verified by correlating it with other sources for reliability.

### 6.3.6 Location Privacy

As explained in earlier, in order to preserve the privacy of the user it is important that two messages of the same user are unlinkable. Therefore, it is necessary that each message uses a different PN. In our scheme we are generating the PNs at the OBU and each PN is different from the previous as a random nonce r is used to generate the $ID_1$, $ID_2$ and r is changing each time. This ensures that messages are unlinkable but at the same time traceable by the authorities. Moreover, we are encrypting messages which ensure that an eaves dropper can’t listen in and hence can’t use the location info for profiling or tracking, making our scheme very secure.

### 6.3.7 Traceability and Revocation

In order to fully de-anonymize a user, RSU will contact TA1, TA2 and provide them TK1, TK2. Our scheme offers authorities the ability to separately revoke the driver and vehicle depending on the nature of the offence. This added benefit enables the authorities to penalise the driver for minor faults by assigning points on the driving license or cancelling a driver license in case of accumulating large number of points. Also, the problem of long RLs can be solved if master keys of TAs are changed regularly e.g. every day. In this case, all users will have to update their master keys by authenticating themselves with TA1 and TA2 daily. Therefore, RSUs will have to maintain short RLs for the current day only as only those users will become part of VANET who have the current valid master keys and all others will be unable to join the network.

## 6.4 Performance Analysis of DIVA

### 6.4.1 RSU Latency

To compute latency at the RSU, we use the same parameters as in [24] i.e. key sizes of 160 bits and the time required for a pairing operation to be 7.3 ms and for point multiplication to be 8.5ms. We compare our scheme with PACP [24] and ECPP [28] protocols. The dominating operations in our scheme for RSU to perform decryption, signature verification include two pairing operations (PO) and one point multiplication (MP). We ignore the time required for Hash and XOR operations in all cases as they are negligible. ECPP requires 13 MPs, 6 POs and PACP requires two POs and one MP for verification at RSU. However, in both PACP and ECPP the RSU generates and verifies the PN tokens and short lived key pairs respectively for the vehicles which cause the extra delay as shown in Figure 6-6. The graph shows the latency when only one token is being generated for each vehicle as number of vehicles increase from 1 to 100. In our scheme as the PNs are being generated at the OBU there is no extra delay at the RSU and hence the reduced latency at RSU which is desirable.

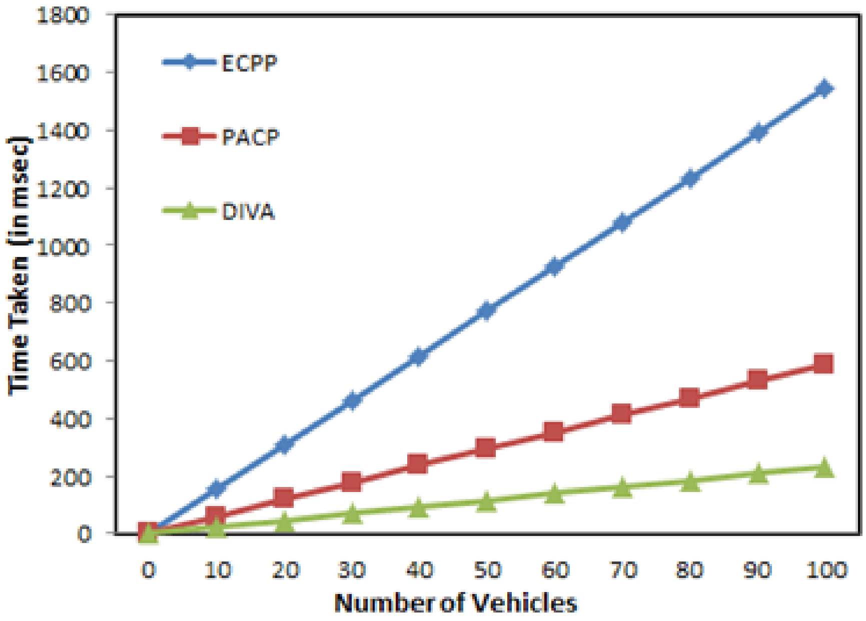


**Figure 6-6: Comparison of Protocol Latency at RSU**

## 6.4.2 OBU Computation & Storage Cost

It is important that the messages are being signed and encrypted by the OBU in a very short time. Our scheme requires 6 point multiplications and 1 pairing operation at the OBU to sign and encrypt a message which gives a delay of less than 58.3ms using same values as used for calculating latency. Also, in our scheme OBUs need to compute $g_{ID}$ once for each RSU saving a lot of computation time at the OBU. As the PNs are being generated at the OBU, there is no storage or replenishing requirements at the OBU as in the case of public and private key pairs or certificates.

### 6.4.3 Comparison in terms of desirable properties

A comparison of our scheme with PACP[24] and ECPP[28] in terms of desirable properties is given in table below:

| | ECPP | PACP | DIVA |
|---|---|---|---|
| **Separate Driver Identity** | NO | NO | YES |
| **Anonymous Authentication** | YES | YES | YES |
| **Unlinkability** | YES | YES | YES |
| **Encryption** | NO | YES | YES |
| **Tokens / Certificates Required from RSU** | YES | YES | NO |
| **RSU Latency** | HIGH | MED | LOW |
| **Revocation Delay** | HIGH | MED | LOW |

**Table 6.1: Comparison of Proposed Scheme with others in terms of desired properties**

## 6.5 Security Analysis of DIVA

### 6.5.1 Privacy Preservation

In the proposed scheme - DIVA, the vehicles have the ability to generate their own PNs (*$ID_1$, $ID_2$*) using the tokens TK1, TK2 from the TAs. Also, a random nonce *r* is used to generate *$ID_1$, $ID_2$*. This enables the vehicles to change their PNs periodically which give them unlinkability and ensure privacy. This is done by:

$$ID_1 = r.P$$

$$ID_2 = PID \oplus H\ (r.P_{pub})$$

*Where PID(Pseudo-ID)* = TK1‖TK2 and *r* is the nonce

The PN is $ID \quad = \ ID_1 \ \| ID_2$

### 6.5.2 Unforgeability

The one time signature of vehicles in DIVA is unforgeable due to the DDH problem in ***G*** being easy and the CDH problem being hard, it is difficult to derive SK1 and SK2 from $ID_1$, $P_{pub}$ and *P*. Therefore, It is infeasible to forge a valid signature. The signature is given by

$$\boldsymbol{\sigma}_{\mathrm{i}} = \boldsymbol{SK_1^i + \ H_2(M_i)SK_2^i}$$

*Where*

$$\boldsymbol{SK_1 = s_1.ID_1 \text{ and } SK_2 = s_2.H(ID_1 \| ID_2),}$$

### 6.5.3 De-Anonymizing and Revocation

One of the advantages of DIVA is that even if the secret keys $s_1$ and $s_2$ are compromised, the adversary still only manages to obtain the tokens - TK1 and TK2. These tokens can only be linked to the original Identity of the user by the two trusted authorities and therefore, only the trusted authorities can reveal the true identity of the user.

## 6.6 Impact of DIVA in VANETs

Some incentives for both parties i.e. the road users and the authorities are listed below:

- The owner can opt for mandatory authentications in order to start the vehicle and after regular time intervals to ensure security of vehicle.
- Authorities will be able to accurately identify the driver of a vehicle that is involved in any traffic violation and the driver will not be able to refute the evidence.
- Toll collection can be automated by identifying users from their tokens and charging their linked accounts.

The identities created in VANETs using the above method solve many security and privacy problems discussed previously. However, there are still some issues that need to be resolved. One of these is that as each vehicle can either generate its own Pseudonyms (PNs) or has public / private key pairs stored, therefore, a malicious vehicle will be able to use more than one identity (PN) at a time and claim multiple identities. This will be discussed in detail next.

## 6.7 Sybil Attack in VANETs

In VANETs, a malicious or rogue node can launch a Sybil attack i.e. when a rogue node claims multiple identities simultaneously with malicious intent. In order to achieve this vehicle transmits multiple messages each with a different ID to indicate that it is not one vehicle but many vehicles thereby creating a situation where these identities can be used with intent to disturb or damage the network. The IDs could either have been spoofed or stolen from compromised nodes. This is done to achieve a variety of goals including: creating a false impression of traffic congestion, outvote honest users, disable a functional network that works on a majority rule. Also, Sybil identities can also inject false information in the network causing it to degrade or collapse. The node that is claiming multiple identities is referred to as malicious and its fake identities are referred to as Sybil identities. The goal of detecting a Sybil attack is to identify the false (additional) identities being claimed by a malicious node as Sybil identities and additionally identify the malicious node if possible.

The wireless connectivity in VANETs is based on IEEE 802.11p protocol and provides wireless connectivity through the standard known as Wireless Access in Vehicular Environments (WAVE) or Dedicated Short Range Communication (DSRC). The WAVE / DSRC standard provides the basic radio standard for connectivity in VANETs. Vehicles use it to communicate with each other i.e. vehicle to vehicle (V2V) and with the infrastructure (Road Side Units - RSUs) i.e. vehicle to infrastructure (V2I) communication. Vehicular networks are very fast moving and highly dynamic due to which it is imperative that the information being shared is authentic and reliable. The interactions are short lived and information exchanged has to be processed quickly, therefore, it is important that the reliability of the information is assessed quickly. Therefore, like any other attack, there will be Sybil attacks in VANETs for various malicious intents and purposes and it is important to devise strategies to counter them.

### 6.7.1 Response to Sybil Attack

Sybil attack can be responded to in three steps; the first step is to detect that a Sybil attack is ongoing - attack detection, secondly the Sybil nodes have to be identified - Sybil identification and third the malicious (attacker) node has to be identified - attacker identification. In VANETs, none of the these are easy due to the nature of the network e.g. if a Sybil attack is established and there are two actual (physical) nodes in front then it is very difficult to ascertain which one is the malicious node creating the Sybil nodes

### 6.7.2 Sybil Attack Detection Techniques in VANETs

Sybil attacks can occur in VANETs as the identities are not authenticated by the users and any vehicle carrying valid certificate / keys are allowed to become part of the network. However, due to the broadcast nature of VANETs a vehicle can use many different identities at the same time while transmitting [90]. In [83], [91] four methods of detecting Sybil attacks in wireless ad-hoc networks are identified:

i. Radio resource testing

ii. Identity registration

iii. Position verification.

iv. Key validation for random key pre-distribution.

Radio resource testing is not suitable in VANETs as a malicious vehicle might be carrying more than one radio and is also not constrained in terms of resources. Similarly, identity registration does not prevent Sybil attacks in VANETs as identities can be obtained from compromised nodes or may be stolen. In vehicular networks, vehicles authenticate themselves with a central authority to obtain credentials that are used to become part of the network. The authentication establishes the identity of the users i.e. they are who they say they are and then they are issued with certified keys also called Pseudonyms (PNs). The security keys are used for signing their outgoing messages and are used by the receivers to authenticate the messages. However, due to privacy concerns hundreds of PNs are issued to one user so that they can be switched periodically to avoid being tracked. This means that vehicles can have many identities in their possession that can be used to claim multiple identities simultaneously which results in a Sybil [45] attack. Such attacks are not only difficult to detect but also have serious consequences. The attacking node is called the malicious user and the identities it claims are called the Sybil identities / nodes. The malicious user might use their own keys, as a user can have many keys, or keys stolen from others. Therefore, the reliance on PKI does not protect the network from Sybil attacks [90].

In order to preserve privacy, strict registration is not feasible in VANETs [92]. Absence of a Central Authority (CA) in VANETs results in identity registration difficulties and this makes Sybil attacks possible [45]. Moreover, assigning a unique identity is not scalable and therefore, unsuitable for VANETs. Different mechanisms [83], [92] have been proposed for position verification including signal strength measurement in [93], [40], direction of arrival in [83].

However, when traffic is heavy then it becomes difficult to determine direction of incoming messages.

In [94], a scheme is discussed where the Road Side Units (RSUs) are connected to the Central Authority (CA) to authenticate the vehicle identities. Also, the paper proposes that all PNs of a user hash to the same value so that a malicious vehicle can’t use its PNs to claim multiple identities. However, there are two problems with the proposed mechanism in [94]. First, the assumption of RSU being readily deployed along the highways is costly and depending on them can be problematic if they are compromised. Secondly, the scheme will not be able to detect Sybil nodes that are using PNs from different vehicles which are either stolen or obtained otherwise.

### 6.7.3 Game Theory in Network Security

Game theory has mostly been used for modelling the cooperative behaviour of nodes in networks including VANETs in [95], [96], [97], [98], [99], [100]. However, in some cases, game theory has also been applied to network security. Game theory has been used for modelling user behaviour for information security in [101] & [102]. It has been used for intrusion detection as a game between the attacker and the defender in [103], [104], [105], [106], [107]. In [108], a game theoretic model is presented for vehicular networks that take into account attacker behaviour for defensive resource allocation. The model is based on betweenness centrality i.e. how many nodes are connected to a node and therefore, that node is most vulnerable to attack. The model then discusses different strategies of the attacker and defender based on the most vulnerable node but does not deal specifically with Sybil attacks. In [103], a game theoretic model is proposed for collaborative networks such as wireless networks and social networks where good users detect bad users by playing the game repeatedly. The good users get a positive pay-off for collaborating with good users and negative pay-off for collaborating with bad users. This enables the user to detect malicious users and break ties with them. In [109], the author proposes a game theoretic model for a voting mechanism to out-vote a malicious vehicle injecting false data in vehicular networks.

The model in [103] does not provide a mechanism to detect the attacks. Moreover, the model is generalized for intruder detection and packet forwarding attacks. Similarly, the work in [109] deals with false information attacks without providing a method to detect false information attacks. However, this paper presents a mechanism that first detects a Sybil attack and then is used to detect the malicious node and its Sybil identities using a game theoretic model.

## 6.8 Proposed Game Theoretic Approach to Sybil Node Detection in VANETs

Game theoretic approaches have been proposed to enhance and improve network security. Game theory helps in scenarios where multiple players with conflicting goals compete with each other while trying to maximize their own pay off or reward. Moreover, game theory is very useful in analysing different scenarios before determining the appropriate course of action [110]. This approach provides a way to predict the behaviour of the attacker and strategies for the defender in different scenarios which helps in improving the network architecture and security.

The key to using a game theoretic approach is to formulate a game so that each player is able to maximize their own profit using a minimax strategy while reaching the Nash Equilibrium (NE). Nash Equilibrium is defined as a set of strategies such that each player (node) maximizes his / her pay-off given the strategies of other players. Moreover, NE is the selection of choices such that no player would deviate from this selection independently without compromising his reward.

The game is designed so that the best response of each user is to cooperate. We also discuss the actions of the honest nodes and the attacker in VANETs with an ability to launch a Sybil attack i.e. to claim multiple identities simultaneously with malicious intent. We define the Sybil attack as a game between the attacker and the honest nodes such that it captures the essential characteristics of a vehicular network. The game is a non-cooperative, dynamic game of complete information between an honest node H and a Sybil attacker S. These terms are explained below:

**i) Non-Cooperative Game:** A game is non-cooperative if the entities are interacting competitively.

**ii) Dynamic Game:** A dynamic game involves multiple stages or moves by the players and they get a payoff at the end of each stage / move.

**iii) Complete Information Game:** A game of complete information is one in which all players know the payoff of every player.

In a game the strategy of the *i*th user is given by $s_i$ and the set of strategies of all players except *i* is represented by $s_{-i}$. The utility of a player *i* is given as $u_i$. Now the Nash Equilibrium (NE) is given as:

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i \ , s_{-i}^*) \qquad (6\text{-}1)$$

where $s^*$ is the dominant strategy of the players. The above expression means that the NE is the outcome when both players are playing their dominant strategy (to maximize their payoff) such that no player can gain by deviating independently from this strategy.

## 6.8.1 Game Model

The game model is simplified for explanation with one Verifier ***V*** and two other (physical or actual) nodes: Node 1 (N1) & Node 2 (N2). The same model will then be expanded to consider situation when there are more than 3 nodes in total. The verifier knows that one of ***N1*** or ***N2*** is malicious but it doesn't know which one. Therefore, ***V*** queries ***N1*** & ***N2*** if they have had contact with the new nodes before. The Payoff or Utility matrix of the first stage of the proposed game is shown in Table 6.2. The two nodes and their responses are shown along with their pay-offs. The two possible strategies of the nodes are a) Reply or b) Don't Reply to a query from another (third node). If one node replies and the other doesn't then the node that replies receives a positive pay-off and the other one receives a negative pay-off and all Sybil nodes become suspect. Also, the node that doesn't reply will subsequently be highlighted as the suspect node. This means that not replying is a strictly dominated strategy and can never be the best response so will never be chosen. Therefore, the dominant strategy in this case is for both nodes to reply (either honestly or dishonestly), this is the first stage of the two stage game. An example pay-off matrix is shown in Table 6.3 in which the dominant strategy is highlighted in yellow and is the best response for both vehicles.

| Node 2<br>Node 1 | Reply | Don't Reply |
|---|---|---|
| Reply | $(\alpha_B, \alpha_B)$ | $(\alpha_A, -\alpha_A)$ |
| Don't Reply | $(-\alpha_A, \alpha_A)$ | $(\alpha_B, -\alpha_B)$ |

**Table 6.2: Game Pay Off / Utility Matrix for Stage - 1**

| Node 2<br>Node 1 | Reply | Don't Reply |
|---|---|---|
| Reply | (1, 1) | (10, -10) |
| Don't Reply | (-10, 10) | (-5, -5) |

**Table 6.3: Example Utility Matrix for Stage - 1:**

| Node 2<br>Node 1 | Seen Before | Not Seen Before |
|---|---|---|
| Seen Before | (A, A) | (0, 0) |
| Not Seen Before | (0, 0) | (A, A) |

Table 6.4: Game Pay Off / Utility Matrix for Stage - 2

| Node 2<br>Node 1 | Seen Before | Not Seen Before |
|---|---|---|
| Seen Before | (10, 10) | (0, 0) |
| Not Seen Before | (0, 0) | (10, 10) |

Table 6.5: Example Utility Matrix for Stage - 2

The second stage of the game is shown in Table 6.4. If ***N1*** replies honestly that it hasn't heard from the new nodes before and ***N2*** replies that it has heard from them before then both nodes receive a zero (or negative) pay-off. This means that ***V*** cannot distinguish between the malicious and honest node but can safely assume that all the suspect nodes (identities) are Sybil nodes. Table 6.5 shows an example matrix for stage 2 with numerical weights allocated and the dominant strategy of both vehicles is highlighted in yellow which is the best response for both vehicles i.e. both vehicles agree with each other when responding to the verifier vehicle.

### 6.8.2 Finding Nash Equilibrium

The solution of the proposed model is finding the NE so that it is in the best interest of all users to be honest. Therefore, two example payoff matrices are created as shown in Table 6.3 and Table 6.5 to represent the game as an extensive form game as shown in Figure 6-7. Extensive form game allows sequencing of player’s possible moves, their possible choices at every decision point and the pay-offs received by each player. The extensive form representation allows the whole game to be represented in one diagram. Backward induction is then used to find the solution to the game which is shown by the dotted lines. Backward induction means that the solution to the game is found by starting from the last stage of the game by looking at the dominant strategy and working upwards to find the Nash Equilibrium at each stage. Backward induction solution is shown using the dotted lines in Figure 6-7. The solution shows that in order to maximize their payoff, both honest and malicious nodes will be truthful which will help identify the Sybil nodes. In stage 1, the NE is Reply-Reply and in stage 2, there are two Nash equilibriums i.e. Yes-Yes and No-No. This means that both nodes are better off by being honest and worse off if they are dishonest (disagree with each other).

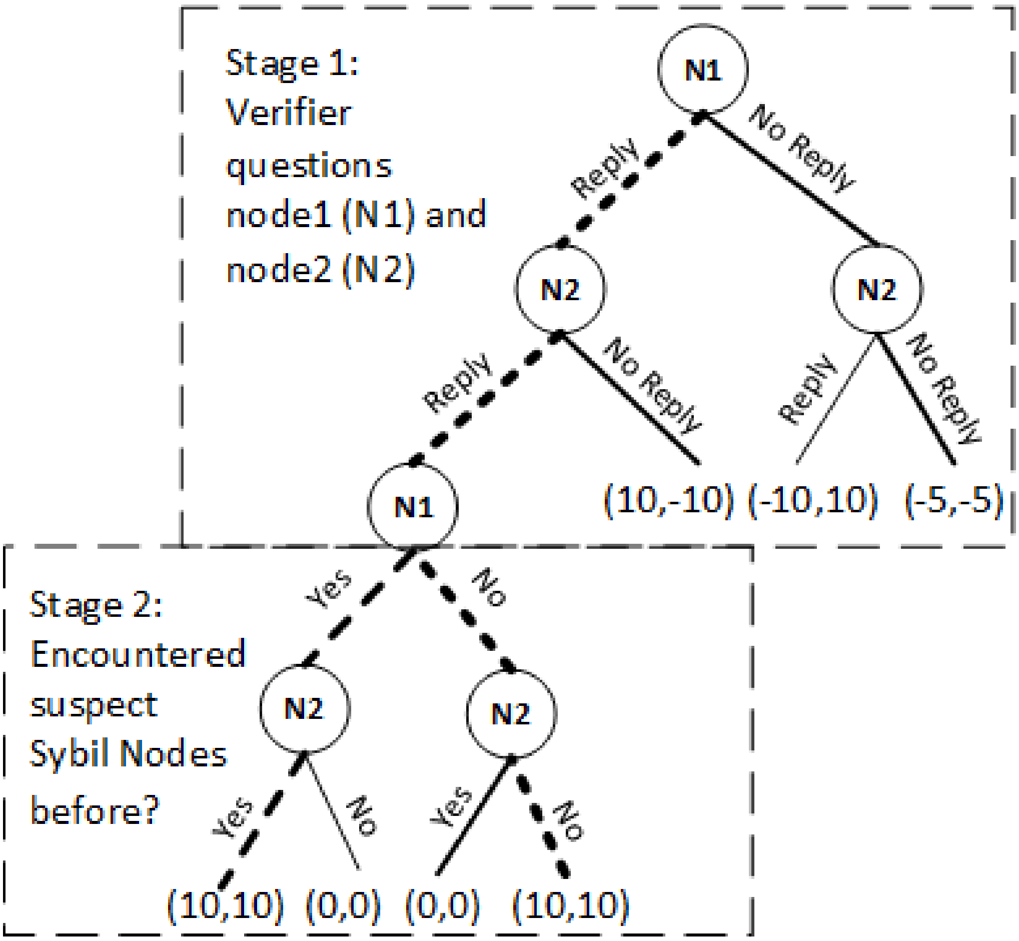


**Figure 6-7: Extensive Form Game Representation and Game Solution using Backward Induction**

### 6.8.3 Attack Model

There are different ways in which a Sybil attack can take place in VANETs. We will be looking at the Sybil attack by making some assumptions.

**Assumptions**: We make the following assumptions in our game theoretic model:

i. The vehicles are equipped with directional antennas so they can determine whether a transmission has been received from their front or back.

ii. The verifier node can choose other nodes that are some distance ahead of it.

iii. Majority of the nodes in the network are honest.

### 6.8.4 Sybil Attack Detection

In vehicular networks, the nodes are communicating with other nodes and sharing their position and speed info periodically. This enables each node to monitor the traffic conditions in their surroundings. This means that vehicles will approach each other gradually but if there are a group of vehicles that suddenly appear in the vicinity of a vehicle then it is an indication of a Sybil attack. This can be seen in Figure 6-8 where a vehicle launches a Sybil attack by reporting false density parameter starting from t=285 sec whereas other nodes are reporting a lower value. Also, there is a direct correlation of speed of vehicles with the number of vehicles i.e. if there are more vehicles in a particular area then the speed of vehicles will decrease. Therefore, if a Sybil attack is launched then the number of vehicles in an area increases suddenly but the speed of vehicles does not change and the reason is that the speed of vehicles is changing based on the actual number of vehicles and not on the number of vehicles being reported.

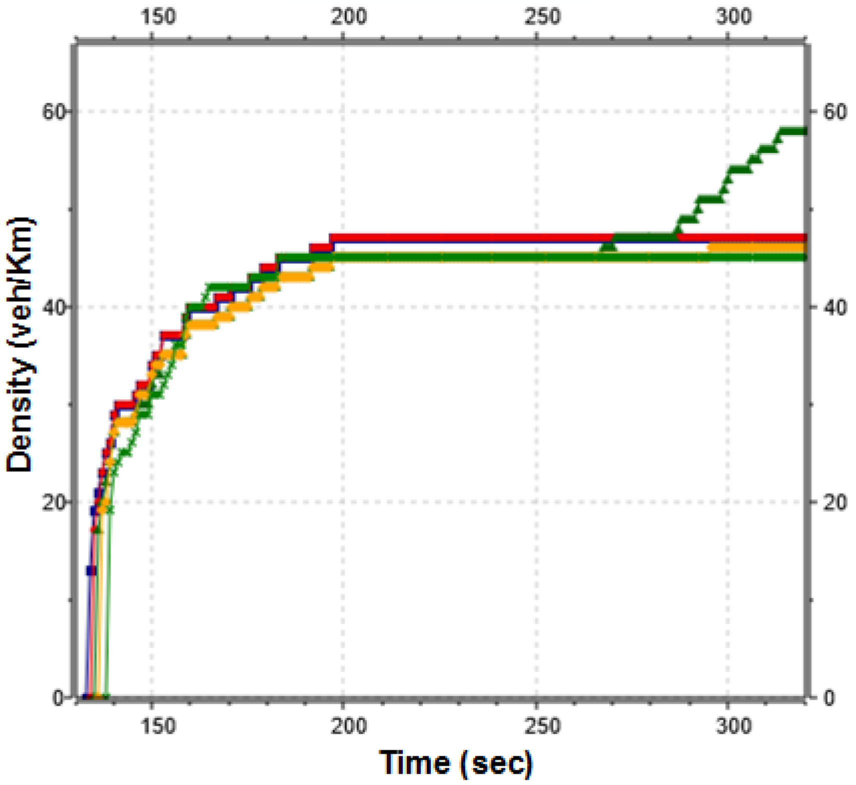


**Figure 6-8: Sybil Attack Detection in VANETs**

### 6.8.5 Strategic Physical Separation

One of the results that we were able to obtain is that there is a strong advantage to having the Verifier and the other two nodes in a line or longitudinally placed as shown in Figure 6-9. This enables the verifier V to query the other two nodes as the other two nodes should hear / interact with the suddenly appearing nodes before they become visible to V. We use this to our advantage in detecting malicious and Sybil nodes as the directional antenna in vehicles is able to determine if the transmission is being received from ahead or behind the vehicle.

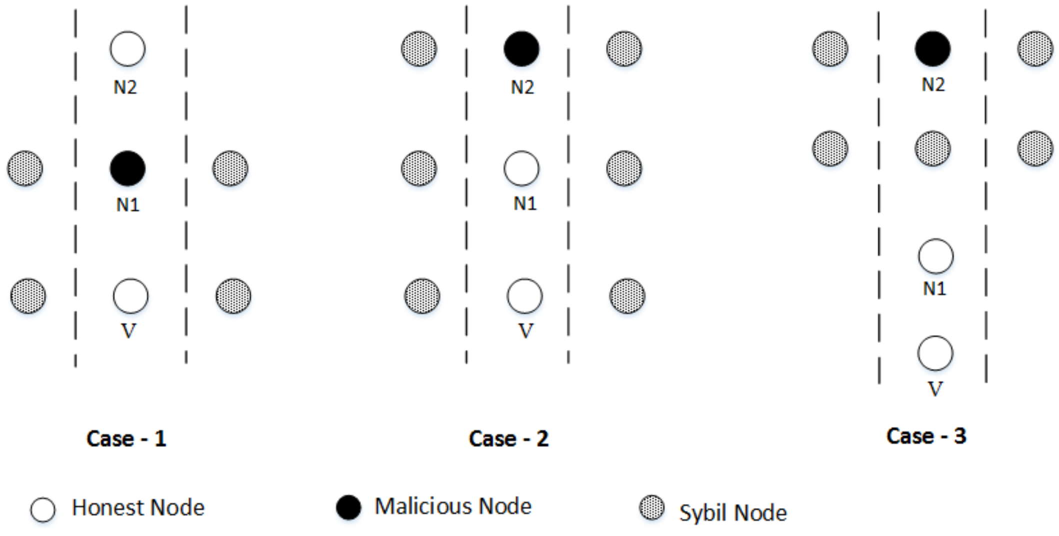


**Figure 6-9: Sybil Attack in VANETs**

## 6.8.6 Revocation and Reporting

Once the nodes N1 & N2 are given negative pay-offs, they are monitored for a while and the negative score is recorded. Subsequently, this negative score can be used to confirm whether a node is indeed malicious or not e.g. if the verifier overtakes N1 and it is still receiving the transmission of the fake Sybil nodes from in front of it then it can safely decide that N2 is malicious and N1 is honest. This information can then be shared with other nodes so that they can be ignored / revoked.

## 6.8.7 Detecting Sybil Nodes with only two physical nodes

### 6.8.7.1 Malicious Node between two Honest Nodes

One of the cases we have considered is when the malicious node N1 is in between two nodes i.e. the verifier ***V*** and another node ***N2*** that have been in contact with for a while in the past (shown in Figure 6-9). As shown, the malicious node ***N1*** creates the Sybil nodes and transmits their locations as shown dotted in the figure. As the Sybil nodes appear suddenly, the verifier ***V*** is suspicious of these nodes and it knows that they haven't caught up from behind it. So, ***V*** reconfirms the same by asking ***N1*** and ***N2***. Now the two stage game starts: In the first stage the verifier ***V*** queries ***N1*** and ***N2*** if they have seen / encountered the Sybil nodes before. The nodes ***N1***, ***N2*** have the option of replying or not replying. If ***N2*** replies and ***N1*** doesn't reply then ***N1*** is the malicious node and the Sybil identities are assumed to have been generated by it. This situation is shown in Table 6.2 and Table 6.3 i.e. ***N2*** gets a positive pay-off and ***N1*** gets a negative pay-off. If both ***N1 & N2*** reply and ***N1*** says that it has not encountered them before and ***N2*** replies that it has encountered them before then all new nodes are considered suspect (Sybil) nodes and are discarded as false nodes. Also, both ***N1*** and ***N2*** get a negative pay-off as shown in Table 6.4 and Table 6.5. In this case, it will not be possible to determine whether ***N1*** is malicious or ***N2*** but at the same time all Sybil nodes are detected and their positions are discarded.

#### 6.8.7.2 Malicious Node in front of two Honest Nodes creating Sybil identities around them

The second case we consider is when a malicious node *N2* is in front of two nodes ***V*** and ***N1***. This is shown as case 2 in Figure 6-9 where the Sybil nodes are generated as shown. As the Sybil nodes appear all of a sudden close to ***V***, therefore, ***V*** queries ***N1*** and ***N2***. Again, if ***N1*** and ***N2*** give conflicting replies then both get a negative pay-off but all new nodes will be deemed suspect and highlighted as Sybil nodes. Once nodes are marked as Sybil nodes then their positions and future messages are discarded.

#### 6.8.7.3 Malicious Node creating Sybil identities in front of two honest nodes

In this case, if the Sybil identities are created in front of the two honest nodes i.e. ***V*** and ***N1*** and they become visible to ***V*** and ***N1*** gradually as they come within range then there is no way of detecting the Sybil nodes by the proposed method.

### 6.8.8 Detecting Malicious and Sybil Nodes when number of honest nodes are greater than Malicious Nodes

We now expand the original scenario and consider the case when there are ***n*** number of malicious nodes and ***p*** number of honest nodes in range of the verifier ***V***. Now as long as ***p*** is greater than ***n*** i.e. the number of honest nodes is greater than the number of colluding malicious nodes then the verifier ***V*** will be able to play the same game and detect the malicious nodes and the Sybil nodes. However, now the game pay-off for the second stage will become $\boldsymbol{A}/\boldsymbol{p}$ instead of $\boldsymbol{A}$.

## 6.9 Performance Evaluation of Proposed Game Theoretic Model

In order to check the proposed model it is simulated using OMNET++, SUMO [81] and VACaMobil [82]. These parameters are chosen as they are typical of a highway scenario and number of rogue nodes are varied to test the system under various conditions.

| Simulation Parameter | Value |
|---|---|
| Simulation Time | 500 sec |
| Scenario | 3 Lane Highway |
| Highway Length | 5-Kms |
| Max Vehicle Speed | 28 m/sec or 100 Km/hr |
| Mobility Tool | VACaMobil |
| Network Simulation Package | OMNET++ |
| Vehicular Traffic Generation Tool | SUMO |
| Vehicle Density | 20-30 veh / Km |
| Wireless Protocol | 802.11p |
| Rogue Vehicles | Varied from 5% to 40% |
| Transmission Range | 500m in each direction |

**Table 6.6: Simulation Parameters**

The scenario is simulated with parameters shown in Table 6.6. In order to validate the model we implement the game theoretic model in a vehicle which is the verifier vehicle that is able to challenge the vehicles in front of it and assign them pay-offs depending on their response based on Table 6.2 and Table 6.4.

Malicious vehicles are introduced in the simulation that start generating messages using different (Sybil) identities in order to give the illusion of more vehicles in the vicinity. The number of malicious vehicles is then increased and the results are recorded.

### 6.9.1 Comparison of Proposed Game Theoretic Model with previous schemes

In this section we discuss the performance of the proposed mechanism as compared to two other existing works. We compare our work to the Cooperative Location Verification (CLV) scheme given in [111] and Secure Location Verification (SLV) given in [112]. We compare our proposed scheme in terms of the successful detection rate of the malicious vehicles when the percentage of malicious vehicles increases from 5% to 40%. The comparison of the proposed method with CLV and SLV is shown in Figure 6-10.

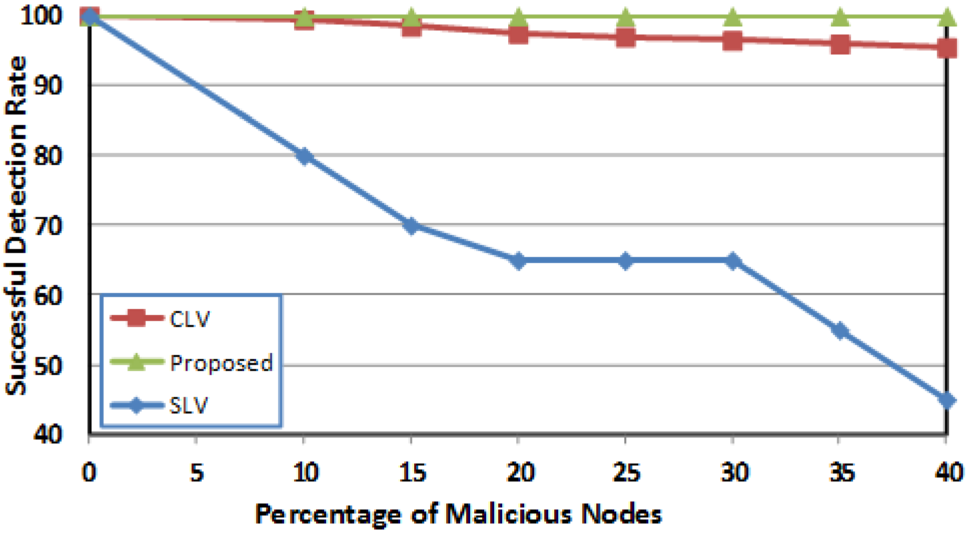


**Figure 6-10: Comparison of Proposed Game Theoretic Scheme with previous schemes**

### 6.9.2 Effectiveness of Game Theory

The adoption of game theory works very well to detect and correct Sybil attacks in VANETs. The game is designed so that it is in the best interest of all players to act honestly. As vehicles try to increase their pay-off, they will have to be honest. By being dishonest, the illusion they try to create is still detected and they get a negative pay-off which will lead to their revocation. The two stage game works effectively to detect Sybil nodes and malicious nodes that create them.

## 6.10 Summary & Research Methodology

The proposed scheme DIVA solves an important practical problem in VANETs i.e. how should the user be revoked / penalised effectively while preserving the user privacy. DIVA is based on combining the identity of the driver

(Driver's License etc) and the identity of the vehicle (Vehicle registration number etc.) to produce a new identity known as Digital ID (DID) in VANETs. The driver and the vehicle authenticate themselves with two different trusted authorities and obtain different keys. The advantage of this is that the privacy of the user is preserved and the vehicle or the driver can't be identified by anyone other than the trusted authorities working together. If a situation arises that the user has to be identified then both trusted authorities have to work together to reveal the true identity of the user. The use of the driver's real identity will force the user to behave honestly and responsibly and the authorities will be able to penalise them if he doesn't.

DIVA enables the user to preserve their privacy by changing their Pseudonyms after generating it themselves. This obviates the generation and replenishing problem of PNs. It also reduces the storage requirement and cost of the OBU. The proposed scheme uses IBE to encrypt its communication with the RSUs thereby securing its communication. We show that our scheme is more efficient in terms of faster computation when compared with two other similar privacy preserving encryption schemes.

In this chapter, a game theoretic model is also presented to detect the wrong use of the identities in VANETs. A game theoretic framework is developed and shared that can detect malicious and Sybil nodes. The proposed method is unique as it can successfully detect the Sybil nodes even if the number of malicious nodes and honest nodes in the network is the same. However, in this situation the verifier is unable to detect between the honest and malicious vehicles. Moreover, the proposed scheme can successfully identify the malicious nodes and all Sybil nodes as long as the number of honest nodes is greater than the number of colluding malicious nodes. Moreover, the proposed game theoretic model is not dependent on any hardware such as radars, Lidars or RSUs.

# Chapter 7 : Conclusion and Future Work

This thesis presented an overview of the security and privacy issues in VANETs. The connected car and vehicular networks will be a reality in the next few years as the required technology is already available and there is already demand for it. The requirement of the user to be connected anywhere-anytime will also fuel the deployment of vehicular networks. This thesis covered the existing works that proposed solutions to the identified problems in VANETs. Trust and reputation has long been used in online networks as a measure of trustworthiness of the user and the information that is being shared. Researchers have proposed different mechanisms to give reputation scores and maintain them in both a centralized and decentralized manner. However, for ad-hoc and dynamic networks such as VANETs, it is not very straight forward. The difficulties arise due to the inherent nature of VANETs i.e. nodes are fast moving, topology is changing continuously, the number of nodes can be very large, the number of nodes can increase very sharply and most importantly the information being shared in VANETs can have life threatening consequences. Therefore, trust and reputation based schemes are not very suitable for VANETs and a different approach is needed that fulfils the stated requirements.

## 7.1 Contributions

The main problem that has been addressed in this thesis is the security and privacy issues associated with the VANETs. The overall contributions of this thesis are discussed below briefly.

### 7.1.1 Establishing Security and Privacy Requirements for VANETs

This thesis investigated the various security and privacy issues in the emerging vehicular ad-hoc networks. The traditional security and privacy techniques employed in other sensor networks are not feasible for vehicular networks. Similarly, trust and reputation schemes are not suitable due to the fast moving and ephemeral nature of VANETs. Due to the unique nature of VANETs the security and privacy requirements also differ from other ad-hoc sensor networks. Therefore, the security and privacy requirements are established and their dependencies are highlighted so that they can be achieved and implemented.

### 7.1.2 Implementing a Data Traffic model for VANETs

A data traffic model for VANETs is implemented that obviates revocation lists which are difficult to implement and use. The proposed method is a data centric method for detecting rogue nodes in VANETs. The proposed data centric method - C-DAC, is not only suitable for VANETs but is also very effective in conveying information to long distances without causing congestion in the network by avoiding broadcast storms. This model gives the proposed system the ability to define a normal behaviour for VANETs and then classify any deviations from this as anomalous behaviour.

### 7.1.3 Developing a Host Based IDS for VANETs

This thesis also presents a host based intrusion detection system for VANETs that is based on the VANET model developed. The proposed host based IDS has the ability to detect false data injected into the network by rogue nodes automatically based on hypothesis testing and t testing. The IDS is validated by extensive simulations under different conditions and the effect of the parameters are recorded. The IDS performance is compared with other previous schemes [86] and [71], proposed for VANETs and is found to be better in terms of true positives, false positives and CPU overhead.

### 7.1.4 Proposing a new ID Management Technique in VANETs

The identity in VANETs is also a tricky issue and this thesis presents a method - DIVA, to generate and manage these identities so that the user's privacy can be assured while providing non-repudiation and traceability to the trusted authorities. The thesis proposes to merge the identities of the driver and the vehicle together to form a new digital identity. The power of completely de-anonymizing a user is split between two authorities so as to improve the security and privacy from the user's perspective. The performance of the presented scheme DIVA is compared to other schemes namely PACP [24] and ECPP [28], and is found to be more efficient in terms of the latency at the RSU.

### 7.1.5 Developing a Game Theoretic model for VANETs to detect Sybil Attacks

The thesis also discusses Sybil attacks in VANETs and presents a method to detect the malicious and Sybil nodes based on game theory. The game theoretic model is described in detail and the solution to it is discussed. The proposed mechanism has the ability to detect the malicious nodes and their generated Sybil nodes. The proposed method also shows that the vertical separation of the vehicles can be helpful in determining the truthfulness of the identities without the use of any hardware. The model is validated by simulation and is found to be better than the existing methods CLV [113] and SLV [114].

## 7.2 Future Work

Due to the unique nature of VANETs and their imminent deployment, it is imperative that these security and privacy issues are addressed as soon as possible. Some of the areas on which we plan to continue our research are discussed below.

### 7.2.1 Reporting / Revoking Rogue Nodes

This thesis has presented an IDS which identifies rogue nodes based on a data centric mechanism. However, this work doesn’t address the problem of dealing with these rogue nodes i.e. how should they be reported to the authorities and to other vehicles and any revoking mechanism. Therefore, the work can be extended by proposing mechanisms that address these issue and present a solution.

### 7.2.2 Securing Autonomous Vehicles against Remote Hacking

This thesis does not deal with the hacking of autonomous vehicles. However, this is going to be a major challenge going forward in the development and deployment of Autonomous vehicles. It is clear that the control systems and the messaging part of the vehicle will be connected to the On-Board Unit (OBU/CPU) of the vehicle. But this introduces the problem of remote hacking. Therefore, addressing this problem can be a very pertinent and important piece of work for the future.

### 7.2.3 Using RSUs to improve the performance of Data Centric Schemes

The data centric work presented in the thesis does not use RSUs for rogue node detection. The main reason for this was the high cost of deployment of RSUs, the serious consequences if they are compromised and their deployment at regular intervals of the highway. However, it is clear that RSUs will be deployed to some extent at some stage of the VANET deployment. Using RSUs to assist vehicles in computing the correct value of parameters can be very beneficial for the network. The RSUs have a unique advantage as they can be trusted by the nodes in the network, therefore, the RSUs can calculate a global parameter for each region and share this value with the vehicles in that region. This will help the vehicles in reducing the error in their own readings and calculation of the global parameter.

### 7.2.4 Extending the developed Intrusion Detection System to detect other attacks

The proposed IDS in the thesis detects false information attacks. However, the proposed work can be extended by modifying the IDS to detect other types of attacks in VANETs such as Denial of Service and false position reporting by rogue nodes in the network or a stationary user outside the network. This can be done by simulating the attacks using the developed platform and then detecting them with the help of anomaly or rule-based detection.

### 7.2.5 Ability to anonymously share data and access Location Based Services

As VANET deployment spreads, it is reasonable to expect that the vehicles will share not just the traffic information but much more. The readings from hundreds of on-board sensors can be used to form weather or traffic maps. Similarly, Location Based Services (LBS) should be accessible to VANET users without compromising on Privacy. Also, vehicles can share entertainment material amongst themselves but it is imperative that the anonymity of both the users is ensured. Therefore, it is important that schemes are devised and implemented that enable users to share data and access LBS without worrying about their privacy and security.

# BIBLIOGRAPHY

[1] A. Tovey, “The Telegraph,” 18 March 2015. [Online]. Available: http://www.telegraph.co.uk/finance/budget/11480796/Driverless-cars-get-boost-with-100m-funding-in-Budget.html. [Accessed 21 August 2015].

[2] GM News, “GM,” 25 Feb 2013. [Online]. Available: http://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2013/Feb/0225_4g-lte.html. [Accessed 21 August 2015].

[3] IEEE, “IEEE ITSS,” 15 September 2014. [Online]. Available: http://its.ieee.org/2014/09/15/you-wont-need-a-drivers-license-by-2040/. [Accessed 21 August 2015].

[4] Ford, “Ford,” [Online]. Available: https://developer.ford.com/. [Accessed 21 August 2015].

[5] GM, “GM - Developer Network,” [Online]. Available: https://developer.gm.com/. [Accessed 21 August 2015].

[6] K. Zaidi, Y. Rahulamathavan and M. Rajarajan, “DIVA-Digital Identity in VANETs: A multi-authority framework for VANETs,” in *19th IEEE International Conference on Networks (ICON),* Singapore, 2013.

[7] K. Zaidi, M. Milojevic, V. Rakocevic, A. Nallanathan and M. Rajarajan, “Host Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection,” *IEEE Trans. on Veh. Technology,* no. 99, 2015.

[8] K. Zaidi, M. Milojevic, V. Rakocevic and M. Rajarajan, “Data-centric Rogue Node Detection in VANETs,” in *IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2014.

[9] K. Zaidi and M. Rajarajan, “Vehicular Internet: Security & Privacy Challenges and Opportunities,” *Future Internet,* vol. 7, pp. 257-275, 2015.

[10] K. Tofel, “Connected cars expected to be a $1B business for AT&T in 2015,” ZD NET, 19 May 2015. [Online]. Available: http://www.zdnet.com/article/connected-cars-expected-to-be-a-1b-business-for-at-t-in-2015/. [Accessed 19 August 2015].

[11] H. Hartenstein and K. Laberteaux, “A Tutorial Survey on Vehicular Ad hoc

Networks," *IEEE Commun. Mag*, vol. 6, no. 46, p. 164–171, Jun. 2008.

[12] M. Faezipour, M. Nourani, A. Saeed and S. Addepalli, "Progress and Challenges in Intelligent Vehicle Area Networks," *Communication of the ACM*, vol. 55, no. 2, pp. 90-100, 2012.

[13] J. J. Haas, Y-C.Hu and K. P. Laberteaux, "Real-world VANET Security Protocol Performance," in *Proc. IEEE Global Telecommun. Conf*, 2009.

[14] US DOT, "Vehicle Safety Communications Project Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC," U.S. Department of Transportation, National Highway Traffic Safety Administration, 2005.

[15] "US Department of Transportation (ITS)," September 2013. [Online]. Available: https://www.pcb.its.dot.gov/eprimer/module13p.aspx. [Accessed 10 September 2015].

[16] M.-J. C. S.-L. W. P.K. Sahoo, "SVANET: A Smart Vehicular Ad Hoc Network for Efficient Data Transmission with Wireless Sensors," *Sensors 2014*, pp. 22230-22260, 2014.

[17] "Society of Automotive Engineers," 16 Feb 2010. [Online]. Available: http://www.sae.org/standardsdev/dsrc/DSRCImplementationGuide.pdf. [Accessed 10 Sep 2015].

[18] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 6, no. 22, pp. 644-654, 1976.

[19] R. L. A. S. a. L. A. Rivest, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM* , vol. 2, no. 21, pp. 120-126, 1978.

[20] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, p. 203–209, 1987.

[21] V. S. Miller, "Use of elliptic curves in cryptography," *Advances in Cryptology—CRYPTO'85 Proceedings*, pp. 417-426, 1985.

[22] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Cryptology, Springer.*, pp. 47-53 , January 1985.

[23] D. Boneh and M. Franklin, "Identity-based Encryption from the

WeilPairing," in *Advances in Cryptology (CRYPTO)* , 2001.

[24] H. Dijiang, S. Misra, M. Verma and G. Xue, "PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems,* vol. 3, pp. 736-746, 2011.

[25] S. An-Ni, S. Guo, D. Zeng and G. Mohsen, "A Lightweight Privacy-Preserving Protocol using Chameleon Hashing for Secure Vehicular Communications," in *IEEE Wireless Communications and Networking Conference (WCNC),* 2012.

[26] R. Lu, X. Li, T. H. Luan, X. Liang and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," *IEEE Transactions on Vehicular Technology,* vol. 61, no. 01, pp. 86-96, 2012.

[27] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad hoc Networks," *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks,* vol. 15, no. 1, p. 39–68, 2007.

[28] R. Lu, X. Lin, H. Zhu, P. H. Ho and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," in *IEEE 27th Conference on Computer Communications,* 2008.

[29] I. Blake, G. Seroussi and N. Smart, "Advances in elliptic curve cryptography," *London Mathematical Society Lecture Note Series 317,* 2005.

[30] "Elliptic curve cryptosystems," *Mathematics of Computation,* pp. 203-209, 1987.

[31] X. Lin, X. Sun, P.-H. Ho and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communication," *IEEE Transactions on Vehicular Technology,* vol. 56, no. 6, p. 3442–3456, 2007.

[32] S. Ahren, E. Shi, F. Bai and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," in *6th Annual IEEE Communication Society Conference on Sensor, Mesh and Ad Hoc Communication and Networks SECON'09,* 2009.

[33] J. J. Haas, Y-C.Hu and K. P. Laberteaux, "Efficient Certificate Revocation List Organization and Distribution," *IEEE Journal on Selected Areas in*

*Communications*, vol. 29, no. 3, p. 595–604, 2012.

[34] 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*, vol. 21, no. 9, p. 1227–1239, 2010.

[35] F. Qu, Z. Wu, F. Wang and W. Cho, “A Security and Privacy Review of VANETs,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 1524-9050, 2015.

[36] J. Choi and S. Jung, “A Security Framework with Strong Non-Repudiation and Privacy in VANETs,” *6th IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 1-5, 10-13 Jan 2009.

[37] T. W. Chim, S. Yiu, L. Hui and V. Li, “Security and Privacy Issues for Inter-vehicle Communications in VANETs,” *6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 2009. SECON Workshops '09*, pp. 1-3, 22-26 June 2009.

[38] M. Al-kahtani, “Survey on security attacks in Vehicular Ad hoc Networks (VANETs),” *6th International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1-9, 12-14 Dec 2012 .

[39] Q. Li, A. Malip, K. Martin, S. Ng and J. Zhang, “A Reputation-based Announcement Scheme for VANETs,” *IEEE Transactions on Vehicular Technology*, vol. 61, no. 9, pp. 4095-4108, 2012.

[40] B. Yu, C. Xu and B. Xiao, “Detecting sybil attacks in vanets,” *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746-756, 2013.

[41] M. Saggi and R. Kaur, “Isolation of Sybil attack in VANET using neighboring information,” *IEEE International Advance Computing Conference (IACC)*, pp. 46 - 51, 12-13 June 2015.

[42] K. Rabieh, M. Mahmoud, T. Guo and M. Younis, “Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs,” *IEEE International Conference on Communications (ICC)*, pp. 7298-7303, 8-12 June 2015.

[43] C. Chen, X. Wang, W. Han and B. Zang, “A Robust Detection of the Sybil Attack in Urban VANETs,” *29th IEEE International Conference on*

*Distributed Computing Systems Workshops. ICDCS '09.* , pp. 270-276, 22-26 June 2009 2009.

[44] Y. Hao, J. Tang and Y. Cheng, “Cooperative Sybil Attack Detection for Position Based Applications in Privacy Preserved VANETs,” *IEEE Global Telecommunications Conference (GLOBECOM 2011),* pp. 1-5, 5-9 Dec 2011.

[45] J. R. Doucer, “The Sybil Attack,” *Peer-to-peer Systems,* pp. 251 - 260, 2002.

[46] Y. Wu, F. Meng, G. Wang and P. Yi, “A Dempster-Shafer theory based traffic information trust model in vehicular ad hoc networks,” *International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC),* pp. 1-7, 5-7 Aug 2015 .

[47] S. Harit, G. Singh and N. Tyagi, “Fox-Hole Model for Data-centric Misbehaviour Detection in VANETs,” *Third International Conference on Computer and Communication Technology (ICCCT),* pp. 271-277, 23-25 Nov 2012.

[48] Z. Cao, J. Kong, U. Lee, M. Gerla and Z. Chen, “Proof-of-relevance: Filtering false data via authentic consensus in Vehicle Ad-hoc Networks,” *IEEE INFOCOM Workshops,* pp. 1-6, 13-18 April 2008.

[49] F. Ghaleb, M. Razzaque and A. Zainal, “Mobility pattern based misbehavior detection in vehicular adhoc networks to enhance safety,” *International Conference on Connected Vehicles and Expo (ICCVE),* pp. 894-901, 3-7 Nov 2014 .

[50] N. Alsharif, A. Wasef and X. Shen, “Mitigating the Effects of Position-Based Routing Attacks in Vehicular Ad Hoc Networks,” *IEEE International Conference on Communications (ICC),* pp. 1-5, 5-9 June 2011 .

[51] L. He and W. T. Zhu, “Mitigating DoS attacks against signature-based authentication in VANETs,” *IEEE International Conference on Computer Science and Automation Engineering (CSAE),* pp. 261-265, 25-27 May 2012.

[52] J. Ben-Othman and L. Mokdad, “Modeling and verification tools for jamming attacks in VANETs,” *IEEE Global Communications Conference*

*(GLOBECOM),* pp. 4562 - 4567, 8-12 Dec 2014 .

[53] J. Benin, M. Nowatkowski and H. Owen, "Framework to Support Per Second Shifts of Pseudonyms in Regional VANETs," in *Vehicular Technology Conference (VTC 2010 Fall),* 2010.

[54] J. Benin, M. Nowatkowski and H. Owen, "Unified pseudonym distribution in VANETs," in *IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob),* 2010 .

[55] B. Liu, J. T. Chiang, J. J. Haas and Y.-C. Hu, "Short Paper: A practical view of mixing identities in vehicular networks," in *Proceedings of the fourth ACM conference on Wireless network security,* 2011.

[56] M. Raya, P. Papadimitratos, I. Aad, D. Jungels and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communication,* vol. 25, no. 8, pp. 1557-1568, 2007.

[57] J. Haas, Y.-C. Hu and K. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET," in *6th ACM international workshop on VehiculAr InterNETworking,* 2009.

[58] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung and J.-P. Hubaux, "Secure vehicular communication systems: implementation, performance, and research challenges," *IEEE Communication Magazine,* vol. 46, no. 11, pp. 110-118, 2008.

[59] O. Abumansoor and A. Boukerche, "Towards a secure trust model for vehicular ad hoc networks services," in *IEEE Global Telecommunications Conference (GLOBECOM 2011),* 2011 .

[60] J. Zhang, "A survey on trust management for vanets," in *IEEE International Conference on Advanced Information Networking and Applications (AINA),* 2011.

[61] P. Wex, J. Breuer, A. Held, T. Leinmuller and L. Delgrossi, "Trust Issues for Vehicular Ad Hoc Networks," in *Vehicular Technology Conference,* 2008.

[62] D. Ma and G. Tsudik, "Security and privacy in emerging wireless networks," *IEEE Wireless Communications,* vol. 17, no. 5, pp. 12-21, 2010.

[63] K.-A. Shim, “CPAS: An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks,” *IEEE Transactions on Vehicular Technology,* vol. vol. 61, no. 4, p. 1874–1883, 2012.

[64] H. Lu, J. Li and M. Guizani, “A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs,” in *IEEE Computing, Communications and Applications Conference (ComComAp)*, 2012.

[65] C. Zhang, X. Lin, R. Lu and P.-H. Ho, “An efficient RSU-aided message authentication scheme in vehicular communication networks,” in *IEEE International Conference on Communications (ICC'08)*, 2008.

[66] R. Puttini, J.-M. Percher and L. M. a. R. D. Sousa, “A fully distributed IDS for MANET,” in *9th International Symposium on Computers and Communications*, 2004.

[67] E. M. Shakshuki and N. K. a. T. R. Sheltami, “EAACK - a secure intrusion-detection system for MANETs,” *IEEE Transactions on Industrial Electronics,* vol. 60, no. 3, pp. 1089-1098, 2013.

[68] A. Nadeem and M. Howarth, “Protection of MANETs from a range of attacks using an intrusion detection and prevention system,” *Telecommunication Systems,* vol. 52, no. 4, pp. 2047-2058, 2013.

[69] H. Sedjelmaci, S. Senouci and M. Abu-Rgheff, “An Efficient and Lightweight Intrusion Detection Mechanism for Service Oriented Vehicular Networks,” *IEEE Internet of Things Journal,* vol. 1, no. 6, pp. 570-577, 2014.

[70] A. Tomandl, K. Fuchs and H. and Federrath, “REST-Net: A dynamic rule-based IDS for VANETs,” *IEEE Wireless and Mobile Networking Conference (WMNC),* pp. 1-8, 2014.

[71] H. Sedjelmaci, S. Senouci and M. Feham, “An efficient intrusion detection framework in cluster-based wireless sensor,” *Security and Communication Networks,* vol. 6, no. 10, pp. 1211-1224, 2013.

[72] H. S. a. S. M. Senouci, “A New Intrusion Detection Framework for Vehicular Networks,” in *IEEE International Conference on Communication (ICC),* 2014.

[73] H. Sedjelmaci and S. Senouci, “An accurate and efficient collaborative intrusion detection framework to secure vehicular networks,” *Computers & Electrical Engineering,* vol. 43, pp. 33-47, 2015.

[74] E. Shakshuki, N. Kang and T. R. Sheltami, “AACKA Secure Intrusion-Detection System for MANETs,” *IEEE Transactions on Industrial Electronics,* vol. 60, no. 3, pp. 1089-1098, 2013.

[75] J. Hortelano, J. Ruiz and P. Manzoni, “Evaluating the Usefulness of Watchdogs for Intrusion Detection in VANETs,” in *IEEE Int. Conf. Commun. Workshops (ICC)*, 2010.

[76] N. Bimeyer, C. Stresing and K. Bayarou, “Intrusion detection in VANETs Through Verification of Vehicle Movement Data,” in *IEEE Vehicular Networking Conference (VNC)*, 2010.

[77] H. Sedjelmaci, T. Bouali and S. Senouci, “Detection and Prevention From Misbehaving Intruders in Vehicular Networks,” in *IEEE GLOBECOM 2014*, Austin, USA, 2014.

[78] T. Gazdar, A. Rachedi, A. Benslimane and A. Belghith, “A Distributed Advanced Analytical Trust Model for VANETs,” in *IEEE GLOBECOM*, California, USA, 2012.

[79] B. D. Greenshields, “A study of traffic capacity,” in *Highway research board proceedings, vol. 1935. National Research Council (USA), Highway Research Board*, 1935.

[80] K. Hafeez, L. Zhao, B. Ma and J. Mark, “Performance Analysis and Enhancement of the DSRC for VANET’s Safety Applications,” *IEEE Transactions on Vehicular Technology,* vol. vol.62, no. 7, pp. 3069-3083, 2013.

[81] M. Behrisch, L. Bieker, J. Erdmann and D. Krajzewicz, “Sumo - Simulation of Urban Mobility: An overview,” in *3rd International Conference on Advances in System Simulation SIMUL* , 2011.

[82] M. Baguena, S. Tornell, A. Torres, C. Calafate, J.-C. Cano and P. Manzoni, “Vacamobil: Vanet car mobility manager for omnet++,” in *IEEE International Conference on Communications Workshops ICC*, 2013.

[83] P. Golle, D. Greene and J. Staddon, “Detecting and correcting malicious

data in VANETs," in *1st ACM Int. workshop Veh. ad hoc networks,* 2004.

[84] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak and I. Stojmenovic, "On data-centric misbehavior detection in VANETs," in *IEEE Veh. Technol. Conf. (VTC Fall),* 2011.

[85] P. Papadimitratos, A. Kung, J. P. Hubaux and F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems: A Position Paper," in *Workshop on Standards for Privacy in User-Centric Identity Management*, 2006.

[86] U. Minhas, J. Zhang, T. Tran and R. Cohen, "Towards expanded trust management for agents in vehicular ad hoc networks," *International Journal of Computational Intelligence: Theory and Practice (IJCITP),* vol. 5, no. 1, pp. 3-15, 2010.

[87] A. Patwardhan, A. Joshi, T. Finin and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc," in *3rd Annual Int. Conf. Mobile Ubiquitous Systems*, 2006.

[88] M. Burmester, E. Magkos and V. Chrissikopoulos, "Strengthening Privacy Protection in VANETs," in *IEEE Intl Conference on Wireless and Mobile Computing,* 2008.

[89] C. Zhang, R. Lu, X. Lin, P.-H. Ho and X. Shen, "An Efficient Identity based Batch Verification Scheme for Vehicular Sensor Networks," in *27th IEEE Conference on Comp. Communications INFOCOM 2008,* 2008.

[90] C. Piro, C. Shields and B. N. Levine, "Detecting the sybil attack in mobile ad hoc networks," in *IEEE Securecomm and Workshops*, 2006.

[91] J. Newsome, E. Shi, D. Song and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *3rd international symposium on Information processing in sensor networks*, 2004.

[92] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Workshop on hot topics in networks (HotNets-IV),* 2005.

[93] B. Xiao, B. Yu and C. Gao, "Detection and localization of sybil nodes in VANETs," in *Workshop on Dependability issues in wireless ad hoc networks and sensor networks*, 2006.

[94] T. Zhou, R. Choudhury, P. Ning and K. Chakrabarty, "P2DAP-Sybil attacks

detection in vehicular ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 582-594, 2011.

[95] S. Shivshankar and A. Jamalipour, "An Evolutionary Game Theory-Based Approach to Cooperation in VANETs Under Different Network Conditions," *IEEE Transactions on Vehicular Technology,* vol. 64, no. 5, 2015.

[96] T. Chen, L. Zhu, F. Wu and S. Zhong, "Stimulating Cooperation in Vehicular Ad Hoc Networks: A Coalitional Game Theoretic Approach," *IEEE Transactions on Vehicular Technology,* vol. 60, no. 2, pp. 566 - 579, 2011.

[97] Y. Huang, H. Wu, Y. Zhang, X. Guan and T. Ohtsuki, "Improve the performance of bus-assisted vehicular ad hoc networks via cooperative game theory," *9th International Conference on Communications and Networking in China (CHINACOM),* pp. 176 - 180, 14-16 Aug 2014.

[98] Y. Li, K. Ying, P. Cheng, H. Yu and H. Luo, "Cooperative data dissemination in cellular-VANET heterogeneous wireless networks," *4th International High Speed Intelligent Communication Forum (HSIC),* pp. 1-4, 10-11 May 2012.

[99] F. Roberto, J. Celestino and H. Schulzrinne, "Using a symmetric game based in volunteer's dilemma to improve VANETs multihop broadcast communication," *22nd IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC),* pp. 777 - 782, 11-14 Sep 2011.

[100] M. Bilal and P. Chan, "A Game Theoretic Coalitional Bidding Scheme for Efficient Routing in Vehicular Ad Hoc Networks," *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom),* pp. 1638 - 1645, 16-18 Nov 2011.

[101] J. Grossklags, N. Christin and J. Chuang, "Secure or Insure? A Game-Theoretic Analysis of Information Security Games," in *17th Int. Conf. World Wide Web (WWW ',08)* , 2008.

[102] J. Grossklags, N. Christin and J. Chuang, "Predicted and Observed User Behavior in the Weakest-Link Security Game," in *1st Conf. Usability, Psychology, and Security (UPSEC ',08),* 2008.

[103] G. Theodorakopoulos and J. Baras, “Game theoretic modeling of malicious users in collaborative networks,” *IEEE Journal on Selected Areas in Commun.*, vol. 26, no. 7, pp. 1317-1327, 2008.

[104] T. Alpcan and T. Basar, “A game theoretic approach to decision and analysis in network intrusion detection,” *42nd IEEE Conf. on Decision and Control,* pp. 2595-2600, 2003.

[105] T. A. a. T. Baar, “A Game Theoretic Analysis of Intrusion Detection in Access Control Systems,” *43rd IEEE Conf. Decision and Control,* pp. 1568-1573, Dec 2004.

[106] T. A. a. T. Baar, “An Intrusion Detection Game with Limited Observations,” in *12th Int. Symp. Dynamic Games and Applications,* 2006.

[107] M. Bloem and T. A. a. T. Baar, “Intrusion Response as a Resource Allocation Problem,” *45th IEEE Conf. Decision and Control,* pp. 6283-6288, Dec 2006.

[108] T. Alpcan and S. Buchegger, “Security games for vehicular networks,” *IEEE Transactions on Mobile Computing,* vol. 10, no. 2, pp. 280-290, 2011.

[109] M. Raya, M. Manshaei, M. Flegyhzi and J.-P. Hubaux, “Revocation games in ephemeral networks,” in *15th ACM Conference on Computer and Communications Security*, 2008.

[110] L. Xiannuan and Y. Xiao, “Game theory for network security,” *IEEE Communications Surveys & Tutorials,* vol. 15, no. 1, pp. 472-486., 2013.

[111] P. Zhang, Z. Zhang and A. Boukerche, “Cooperative location verification for vehicular ad-hoc networks,” in *IEEE International Conference on Communications (ICC),* 2012.

[112] J.-H. Song, V. W. Wong and V. Leung, “Secure location verification for vehicular ad-hoc networks,” in *Global Telecommunications Conference (IEEE GLOBECOM),* 2008.

[113] N. Lyamin, A. Vinel, M. Jonsson and J. Loo, “Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks,” *IEEE Commun. Letters,* vol. 18, no. 1, pp. 110-113, 2014.

[114] B. Pooja, M. Manohara Pai, R. Pai, N. Ajam and J. Mouzna, “Mitigation of insider and outsider DoS attack against signature based authentication in

VANETs," *Asia-Pacific Conference on Computer Aided System Engineering (APCASE)*, pp. 152-157, 10-12 Feb 2014.