# EFFICIENT PATH MAPS GENERATION USING DATA MINING ON DISTRIBUTED RSUs IN VEHICULAR AD HOC NETWORKS

A

Thesis

Submitted to

For the award of

**DOCTOR OF PHILOSOPHY (Ph.D)**

**in**

**COMPUTER SCIENCE AND ENGINEERING**


**Submitted By**

**Arun Malik**

**41300063**

**Supervised By**

**Dr. Babita Pandey nee Shukla**

**LOVELY FACULTY OF TECHNOLOGY AND SCIENCES**
**LOVELY PROFESSIONAL UNIVERSITY**
**PUNJAB**


**2018**

# DECLARATION

I hereby declare that the thesis entitled, **EFFICIENT PATH MAPS GENERATION USING DATA MINING ON DISTRIBUTED RSUs IN VANET** submitted for the Ph.D. Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

**Date:** **Investigator:** Arun Malik

**Registration No:** 41300063

**Signature of Advisor**

**Name:** Dr. Babita Pandey nee Shukla

**CERTIFICATE**

This is to certify that ARUN MALIK has completed his thesis titled *"Efficient Path Maps Generation Using Data Mining on Distributed RSUs in VANET" under* my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation has ever been submitted for any other degree or diploma.

**Signature of Advisor**

**Name:** Dr. Babita Pandey nee Shukla

**Date:**

# ABSTRACT

A vehicular ad hoc Network (VANET) comprises the self managing ad hoc mobile vehicles. VANET is inherited from Mobile Ad hoc Network (MANET) for improving Intelligent Transport System (ITS) where vehicles act as mobile nodes. VANET framework is designed using three essential communicating units- Road Side Unit present at road segments, On Board Unit present in vehicle, and backend infrastructure for interconnectivity among vehicles and internet. Communication can be established in vehicle-to-road units, inter vehicle units, and road-to-road side units. The major concern while communication is related to security, considering confidentiality, integrity, authentication as the prime services to be offered to the vehicles. Therefore, each connecting vehicle in VANET has to prove its liability through authentication and can take the benefit of other security services afterwards.

In this era of expanding transport facilities for users, intelligent pathway coordination and communication is required among the vehicles. Therefore, the current research in VANET is focused on reducing traffic congestion in rush hours of a day, and accidents on the road. In case of occurrence of traffic congestion or road accident, vehicles on the move get stuck that calls for an effective way of choosing an alternate path and hence clear up the jammed traffic. Alternative path map consists of segments that are less occupied and can be followed in unusual situations.

Therefore, the prime objective foundation on which this research work revolves around is to (1) propose a new scheme for data collection which will tend to improve throughput, packet delivery ratio, and reduce latency, (2) extract the possible paths from the data collected using association rule base mining on distributed RSUs, and (3) predict the common and most frequent paths on the basis of position, direction, time of day, and during any accident or jam.

In order to generate efficient path maps in unusual situations like congestion or road accidents, the first step is to collect data from each vehicle about the path that it traverses to reach from one source to destination. Data collection is dependent on numerous factors such as position, direction, and time of the day. RSUs present on the

other side, hold the data collected from different moving vehicles from different source to destination respectively. Vehicles while moving send the data about the path segments that they are going to traverse to their nearest RSU. For each vehicle separate path information is maintained from a specific source to destination.

Different data collection scheme (DCS) are investigated by researcher that can be either RSU initiated or vehicle initiated. In RSU initiated scheme, a beacon message is initiated by the RSU after a fixed interval of time say N seconds to the vehicles present in its vicinity. In response, every vehicle sends a packet to the RSU with information related to the partial path. Road side unit (RSU) use road side probing in which they initiate the procedure of probing in order to enquire every vehicle in its vicinity about the information related to traffic, environmental, or accidents information. On the other side, in vehicle initiated scheme, vehicle starts transmission of path information to the RSU. Vehicle Initiated can be further classified as Vehicle Initiated-RSU find mode (VIR) and Vehicle Initiated-Broadcast mode (VIB).

In VIR, before the vehicle initiates the transmission of packet, it first generates a RSU find message and broadcast it. RSUs which are currently in the vicinity of the vehicle will receive this message but the one who is close to the vehicle replies through a message detailing its address information. VIR is again categorized into two schemes. One is VIR-Complete Path (VIR-CP), here vehicle first collects the information for complete path and then transmit the packet to the RSU. Second is, VIR- New Segment (VIR-NS), here whenever a vehicle receives information related to new path, it transmits the packet to a specific RSU.

In VIB, the transmission of packets is initiated in the broadcast mode through vehicle to all the RSUs that are in its vicinity. VIB scheme is again categorized in two schemes. One is, VIB-Complete Path (VIB-CP), here vehicle first collects the information for complete path, that is, it covers all the path segments first and after reaching the destination it transmits the packet to the RSU. Second is, VIB- New Segment (VIB-NS), here whenever a vehicle receives information related to new path, it transmits the packet.

From the aforementioned existing DCSs, VIB-CP (Vehicle Initiated Broadcast Complete Path) is the best one whose performance index is high in provisions of communication overhead, average delay, and packet delivery ratio. But VIB-CP is still vulnerable to attacks, as an unauthenticated user can send the wrong data information to RSU. An attacker can also block the resources of RSU by sending unlimited messages. Various types of attacks are possible on VIB-CP that result in low evaluation of the VIB-CP based on communication overhead, packet delivery ratio and average delay. Therefore, improvement is required in VIB-CP as it didn't provide any security features.

With an aspiration to integrate security in existing DCS in VANET, an intelligent Authentication based Vehicle Initiated Broadcast Dynamic Path (IAVIB-DP) is proposed. In IAVIB-DP, Vehicle authentication is performed first on the RSU i.e. the authenticity of the vehicle is first proved at the RSU. A reciprocal security mechanism is required by the RSU to prove its authenticity to the vehicle in a view to support advance authentication mechanism. Once mutual authentication among RSU and vehicle is completed, vehicle may initiate communication with that RSU.

This work aims to implement and compare VIB-CP and proposed IAVIB-DP in OMNet++ to fetch the results in controlled environment set by user. OMNeT++ is an modular discrete event object-oriented network simulation framework that provides graphical user interface (GUI) for the simulation making it interactive system to work with. Moreover, it also provides mobility support in VANET. Communication overhead, Packet Delivery Ratio, and Latency is improved by using IAVIB-DP scheme while achieving authenticity of the vehicles.

Once the data is collected securely from proposed IAVIB-DP data DCS from different vehicles, data is stored at RSUs. Further, data mining is applied to extract all the possible paths considering one source and one destination. Association rule based mining is used to mine huge database to find common and frequent paths followed by different vehicles from one source to destination at distributed RSUs. Multiple paths may exist from a source to destination and this process is repeated for multiple source and destinations.

Minimum support and confidence are applied by setting threshold values that decide whether to accept or reject the pattern generated.This is required to accept the arrangements for further decision making. A prediction model is designed that is able to decide the next path to choose in unusual situations like accident, jams, or a particular time of day. Therefore, this study comes out with a smart way of getting the best path map at particular time of day to avoid delay. For society, it reduces delay during unusual situations such as in event of accident, theft, morning rush hours, ambulance.

# ACKNOWLEDGEMENT

I would like to present my deepest gratitude to **Dr. Babita Pandey nee Shukla** for her guidance, advice, understanding and supervision throughout the development of this thesis and study. I would like to thank to the **research project committee members** for their valuable comments and discussions. I would like to thank to **Lovely Professional University** for their support on academic studies and letting me involve in research study.

ARUN MALIK

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# LIST OF ABBREVIATIONS

| Abbreviation | Description |
|---|---|
| AP | Access Point |
| APt | Active Path Table |
| AU | Application Unit |
| CDT | Cell Dwell Time |
| CH | Cluster Head |
| CMP | Candidate Motion Arrangement |
| DCA | Digital Certificates Authentication |
| DCS | Data Collection Schme |
| DoS | Denial of Service |
| DSRC | Dedicated Short Range Communication Standard |
| GPS | Global Positioning System |
| GUI | Graphical User Interface |
| HMM | Hidden Markov Model |
| IAVIB-DP | Intelligent Authentication Based Vehicle Initiated Broadcast-Dynamic Path |
| INSA | Intermediate Node Selection Algorithm |
| IRE | Intermediary Re-Encryption |
| ISP | Internet Service Providers |
| ITA | Intelligent Transport Application |
| ITS | Intelligent Transport Systems |
| IVC | Inter Vehicle Communication |
| LT | Lane Table |
| MANET | Mobile Ad-Hoc Network |
| MDS | Minimum Dominating Sets |
| MP | Motion Arrangement |
| OBU | On Board Unit |
| PI | Performance Index |
| PL | Path Lane |
| PPC | Position Based Prioritized Clustering |
| PST | Probabilistic Suffix Trees |
| PUF | Physical Unclonable Functions |
| RBRA | Receiver Based Routing Algorithm |
| RCP | Resource Command Processor |
| RI | RSU Initiated |
| RS | Road Segment |
| RSU | Road Side Unit |
| SP | Service Provider |
| TOA | Time of Arrival |
| V2I | Vehicle To Infrastructure Communication |
| V2R | Vehicle-To-Road Side Unit |
| V2V | Vehicle To Vehicle Communication |
| VANET | Vehicular Ad-Hoc Network |
| VARM | VANET Association Rules Mining |
| VEINS | Vehicle In Network Simulation |

| | |
|---|---|
| VIB | Vehicle Initiated-Broadcast Mode |
| VIB-CP | Vehicle Initiated-Broadcast-Complete Path |
| VIB-NS | Vehicle Initiated-Broadcast-New Segment |
| VII | Vehicle Infrastructure Integration |
| VIR | Vehicle Initiated-RSU Find Mode |
| VIR-CP | Vehicle Initiated-RSU -Complete Path |
| VIR-NS | Vehicle Initiated-RSU - New Segment |
| WAVE | Wireless Access In Vehicle Environment |

# CHAPTER 1

# INTRODUCTION

In this chapter we have conducted a detailed literature survey based on the existing security solutions, data collection, data mining and path generation schemes. Based on the literature survey, the problem statements have been identified in VANET and multiple research objectives have been framed.

## 1.1 Introduction

With the increase in mobile devices like laptops, personal digital assistance, cell phones and handheld devices, a lot of maintenance in terms of communication and computation is required. Wired networks are difficult to implement as there capacity is less than wireless networks. In [1] it is discussed that one of the wireless networks, i.e, MANET, is a form of ad hoc network which helps in establishing communication for mobile devices by forming a temporary network. MANETs are used for numerous applications like commercial purpose, civilian place, and surveillance and also in entertainment field [2]. But in [3], it has been found that MANETs are vulnerable to various categories of attacks like denial of service, eaves dropping, spoofing or many more. The reason for these security attacks was given that as nodes have high mobility so even the owner of a node cannot have constant check on its movement. In [4], the author have shared that MANETs were originated while the execution of DARPA project. After some time, it was discovered that MANETs also offers some safety related applications [5].

VANET is a variant of MANET that works on the communication in vehicles [6]. Due to gradual increase in count of vehicles moving on the road, the count of road accidents, and traffic jams are also increasing at exponential rate.  Once an accident or traffic congestion has occurred, the new vehicles entering in that area are going to cause more congestion. Today, VANET has evolved as an amazing technology in field of transportation system and has become integral part of our daily life. VANET tend to improve the transport system and work to make it as ITS.

Over many years, VANETs are applied to distinct applications, varying from tracking of vehicle, in-vehicle surveillance, intelligent transport system and many more. Some of the countries like U.S, Europe and Japan are continuously working on improvising communication among vehicles. U.S had also proposed the drafts where it is mandatory to have communication among the vehicles. Indian companies like Efkon and Bosch are working on VANET projects such as automated fair collection and intelligent transport system respectively. Various companies like Audi, Honda, BMW, Toyota work on offering services in V2V communication.

There are various projects that have been undertaken on VANET by different countries like Japan and USA. A project, SEVECOM, based on secure vehicle communication provides full implementation scope of security for communication among vehicles [4]. Another project vehicle Safety Communications that started in 2002 and ended in 2004 determines the minimum requirements for safety [5]. Vehicle Infrastructure Integration (VII) aimed to provide coordination among different automobile manufactures [5].

Major concern of VANET is safety related and improving the traffic efficiency. The most important thing to be taken care in VANET is security while communicating. These security requirements come along with some challenges.

## 1.2 Literature Survey

This section presents the current information related to VANET by conducting theoretical and methodological survey. Firstly a detailed survey is done on security considerations in VANET along with the existing security solutions. Further, various DCSs are surveyed that are used in VANET such as Global positioning system (GPS), Cellular networks, client sever tracking update, RSU initiated (RI), and vehicle initiated (VI) to gather the traffic updates from the vehicles that are moving on road. Later, a survey on numerous data mining methods such as association rules, Classification, Clustering, and sequential mining is done followed by the path map generation mechanism.

### 1.2.1 Security Considerations in VANET

To provide security with proper preservation of privacy of the users or vehicle drivers is a very exigent task. Due to dynamic topology, regular detached networks, mobility modeling and predictions based varied applications of VANET system, their requirements related to message transfer, security and privacy could be of different types. Plenty of research work is focused on security and confidentiality in the field of VANET [7]-[13] that review issues related to security such as attacks, security requirements, security protocols, challenges in VANET.

In [14], the proposed scheme maintains privacy and avoids Sybil attack in VANET. To prevent Sybil attack from scheduled beacons interfere resistant module has been deployed to perform data analysis on the pre gathered data which is used to combine together beacons whereas to prevent Sybil attack from incident reporting communication, road side units are deployed to restrict nodes under Sybil attack in VANET and inform the revocation authority.

In [15], an algorithm based on digital certificate has been devised to offer security for VANET scenario. The proposed scheme overcome the threat of few serious interceptions such as man in the middle, masquerade attack with the help of low message passing technique that aims at decreasing bandwidth during authentication time.

In [16], a segmented attack-resistance tree model has been used to provide secure communication in VANET. Three different segments are utilized by this model to address the progressive acts of attack resistance process. In every segment, each attack-resistance pair involves definite attack action and its counteracting measure. On the basis of this proposed model a segmented attack-resistance game is examined to understand the communication and reliance between assailant and protector.

In [17], a secure communication method in VANET has been proposed to provide optimal path to the incident location for ambulance as early as possible. The proposed method utilizes symmetric encryption, message authentication code and digital signatures together in order to ensure the secure communication without the loss or steal of messages. Results of this proposed method are tested with NS2 simulator and provide the conclusion that this method is effective in real time VANET scenarios.

In [18], a novel protocol has been proposed based on genetic algorithm to prevent accidents on curved roads using VANET infrastructure. As on curved roads, environment obstacles prevents the straight the communication among vehicles due to which chances of accidents increases at such places. The proposed approach reduces the outline of entire uncovered and overlapped areas on the roads which are wrapped by more than one antenna.

In [19], an authentication protocol based on confidence estimation has been proposed. The proposed protocol is divided into two parts: direct and indirect confidence estimation. In direct confidence estimation a safe vector model is designed considering the security behavior of the moving vehicle. In indirect confidence estimation degree of confidence is computed on the basis of confidence vectors from the vehicles in VANET. To distinguish the faulty vehicles correlation coefficient is deployed by this proposed authentication protocol.

In [20], a novel intersection based physical routing protocol has been proposed that handle security and routing issues in VANET. The proposed protocol is categorized in two parts: security and routing. For routing purpose, this protocol chooses suitable intersection vigorously for transmitting the packets. For security purpose the model of mix zones is used to avoid vehicle trail by unauthorized users.

In [21], a security mechanism based on trusted computing skill has been proposed. The proposed protocol efficient prevents the faulty actions primarily for interfering with routing protocol without affecting the network's performance. With help of extensive simulation it was found that proposed protocol performs better in preventing against the faulty actions as compared to GPSR.

In [22], a novel trust based authentication scheme has been proposed to identify faulty and malicious vehicles in VANET. The proposed scheme presents a new trusted authentication model for VANET that consist of two modules. In first module new vehicles that are entering to network are introduced with the registration process in which a trust value has been allotted to every registered vehicle. In second module the existing vehicles that are already in the network has been introduced with the mechanism that update the trust value.

In [23], an efficient routing protocol based on anonymous location has been proposed to provide privacy and security at low computational cost. The proposed protocol provides mutual security by utilizing digital signatures and public key cryptography. Primary intend of this protocol is to offer security to all individuals in VANET.

In [24], to reduce the spread of fake messages, an event based reputation system has been proposed. This system prevents the VANET from the planned Sybil attack by handing over exclusive trusted and reputation value to every event. Privacy is maintained for the vehicle identity in this system. This system prevents the Sybil attacks from multiple sources without affecting the performance of VANET.

In [25], potential to transfer the messages among cars in secure manner with the help of cryptographic digital signature has been analyzed. The process of simulation is carried out on OPNET tool with connection to OpenSSL by using elliptic curve digital signature scheme.

In [26], a security framework has been described that utilize machine leaning methods to detect and classify different kinds of misbehaviors in VANET. For detecting the misbehaviors nodes with high accuracy the proposed framework formulates the final result by combining individual classifiers. Weka tool is used to segregate different zones of misbehaviors by evaluating the proposed security framework in VANET.

In [27], an authentication scheme has been described to provide authentication to vehicles in VANET scenario. The proposed scheme utilized aggregate signcryption and signature to provide many to one secure communication. For reducing the overhead due to communication and to increase the efficiency of network bath verification is used by this approach that facilitates RSU to authenticate the vehicles in an efficient manner.

In [28], a security framework based on honeypots concept has been described to provide security in VANET. The proposed framework not only provides the security required for data exchange among the vehicles, between vehicles and RSUs but also provide security to the entire architecture of VANET. The proposed framework prevents transfer of faulty data, illegal right to use of data and refuse of service.

In [29], an exhaustive message authentication scheme has been proposed that provide authentication among inter RSU ranges and between Intra RSU ranges .This authentication scheme also permits the hand off among different RSUs. This scheme provides an efficient secure communications by balancing the computational overhead.

In [30], a novel method for detecting the Sybil attack has been described for VANET. The proposed approach detects the faulty nodes acting as multiple nodes that are identified in a distributed mode with the help of RSUs. In this approach vehicle's need not disclose its identity to detect the faulty nodes.

In [31], a novel approach to preserve the privacy of vehicle location has been described. The proposed scheme prevents the mobile network nodes from the threat of physical layer attackers in network nobility based VANET by preserving the location information of the vehicles by utilizing cluster based fake point scheme.

In [32], a privacy preserving scheme depending on onion routing has been proposed. The proposed scheme works by actively establishing secret connection inside a network of authentic time Chaum Mixes. A mix is a device that receives predetermined length data packets from various sources, executes cryptographic encryption and then transfers the data packets to the next destination in an arbitrary order. By providing routing through mixes it becomes very difficult to identify who is talking to whom due to which user's privacy is not compromised.

In [33], technology that breach web surfers privacy has been described first and then system that protects the privacy of web surfers is described. The proposed system facilitates users to protect their privacy devoid of waiting for the new technological principles and new administration guidelines.

In [34], an efficient authentication scheme has been proposed that provide authenticity in both mobile and relay nodes. The proposed scheme prevent inside and outside authentication attackers. The scheme described in this paper provides high level of secrecy with low communication and computational overhead.

In [35], authors' have devised a scheme for authentication working on the mechanism of encryption using private key. Therefore, using private key method a safe connection is established between the two entities involved.

In [36], a novel protocol has been proposed that provides authentication among Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V) without disclosing vehicle's identity for preventing the driver;s privacy. The proposed work is focused on Physical Unclonable Functions (PUF) that dispenses the session key in a secure manner and ensures secrecy.

In [37], various types of attacks that are possible on distance bounding protocols are classified which can be further utilized for the systematic analysis of hazards against distance bounding protocols. A framework for security is also devised in this work to prevent the distance bounding protocols from different kind of possible attacks.

In [38], information delay that occurs due to one by one authentication has been addressed. To reduce the information delay and to reach legitimate time performance an efficient authentication scheme based on batch verification is proposed to make VANET more safe and well-organized.

In [39], an authentication scheme has been proposed that process multiple authentication request sent by numerous vehicles at the similar time. In this scheme various session keys are established for numerous vehicles during same time. The proposed scheme efficiently establish authentication among vehicles by using one verification function.

In [40], authors' have proposed a novel authentication based scheme that reduce the entrust authentication delay by establishing the session procedure dynamically in a fugitive manner. The proposed scheme increases the pace and computational effectiveness of authentication process among vehicles and RSUs and also prevents from the malicious attacks by defending the strength of VANET.

In [41], a novel authentication scheme has been proposed that provide the privacy to user location. Blind signature approach in elliptic curve area is used by the proposed scheme to provide authentication to the users. The proposed scheme performs efficiently in flawless exchange of messages in fast moving vehicles.

In [42], to attain trust in VANET a novel distributed and two-way model has been proposed. The referred model is helpful in identifying the correctness of vigilant messages sent by the vehicles regarding unusual incidents like accidents and hurdles on roads. Efficiency of the proposed model is analyzed in NS3 simulator.

In [43], an efficient trust management scheme has been proposed that provides reliability of packet transmission in VANET. Trust token are used by the proposed scheme to decide whether to drop or accept the data packet. Proposed scheme plays an important role to prevent the modification of data packets by identifying the malicious nodes in VANET.

In [44], authors have proposed hybrid authentication scheme. Proposed authentication scheme depends on signcryption without certification and pairing. The proposed scheme performs well still in the lack of RSU. Effectiveness and efficiency for the scheme proposed is analyzed by Qualnet simulator.

In [45], a scheme for authentication has been described that utilize identity based signature mechanism in a way to ensure multiple levels in secrecy to vehicles in VANET. This authentication scheme utilizes an efficient pseudonyms issuance mechanism with the help of which pseudonyms issuer allots pseudonyms that are unique to the vehicles. Moreover, every pseudonym binds vehicle with the expiration date due to which no public key certificate is required by this protocol to implement short term credentials.

In [46], biometric encryption based authentication scheme has been proposed that overcome the limitation of existing arbitrary key based authentication methods. The proposed scheme utilizes the combination of XOR and hash function for cryptographic calculations. The proposed scheme put more emphasis on improving the security using V2I type of communication in VANET.

In [47], a competent group signature based security solution that prevents denial of service attack without compromising the user privacy in VANET has been proposed. The proposed solution identifies and drops the fake data packets by verifying the signature among V2I and I2V communication. This security solution provides assurance that no one can create a profile of valid users and thus protect the privacy of users.

In [48], group signature based batch verification scheme to preserve the privacy of vehicles in VANET has been devised. The scheme proposed provides the privacy in V2V communication only. Proposed scheme utilizes key pairing approach to provide the secure inter vehicles communication in VANET.

In [49], an efficient authentication scheme has been proposed that provide VANET security from numerous conventional attacks possible in VANET. Proposed scheme share the session key in a very secure manner by using asymmetric encryption. In this scheme decryption can only be performed by the private key.

In [50], privacy preserving scheme to detect traffic congestion in VANET has been proposed. This scheme provides the privacy and security in inter vehicle communication. This scheme maintained the privacy by not allocating any unique identifier to the vehicles. Location of the vehicles are broadcast randomly without the dependency from the previous broadcast information due to which it becomes difficult to find whether the location information is coming from same vehicle or not.

In [51], a novel authentication scheme that preserves the privacy and conditional traceability for secure communication has been devised. The scheme proposed provides authentication by utilizing message authentication code generator and symmetric encryption for authentication and signing.

In [52], a privacy and security preserving using authentication mechanism has been detailed. To offer secure communication and furtive authentication, the scheme utilizes bilinear pairing in VANET environment.

The various types of security solutions available in literature for providing security and privacy in VANET are detailed in Table 1.1 below.

**Table 1.1: Security Solutions for Providing Security and Privacy in VANET**

| **Reference paper** | **Proposed Security solution** | **Approach or strategy** | **Communication type** | **Attacker** | **Attack model** | **Simulation Scenario/ tool** |
|---|---|---|---|---|---|---|
| [14] | Sybil attack detection and prevention scheme | Token based approach | V2V,V2I | Inside attacker | Attacks on authentication and privacy | Trace driven |
| [15] | Cost effective security protocol | Digital certificate | V2V,V2I | Malicious attacker | Masquerade attack | Theoretical Computational and cost analysis |
| [16] | Phased attack-defense tree model | Backward induction method | V2V | Inside attacker | Fabrication to provide the optimal path attack | Game Model |
| [17] | Secure ambulance | Message authentication | V2I | Malicious | Attacks on | NS2 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | communication protocol | codes, digital signature mechanism and symmetric encryption | | attacker | authentication and privacy | |
| [18] | GA based planning VANET infrastructure scheme | GA based approach | V2V,V2I | Prankster | Attacks on analysis of traffic | MATLAB |
| [19] | Security authentication method based on trust evaluation | Correlation coefficient , safe and confidence vector model | V2V,V2I | Eavesdropper and Malicious attacker | Attacks on authentication and secrecy | MATLAB |
| [20] | Junction –based geographical secure routing protocol | Greedy strategy and Concept of mix zones | V2V,V2I | Eavesdropper and malicious attacker | Attacks on privacy and privacy | VANET-sim |
| [21] | Trusted geographic information routing protocol | Trusted computing technology, passwords and digital certificates to deal with security threats | V2V | Inside attacker and malicious attacker | Location forging attack and fabrication attack | NS2 |
| [22] | Trusted vehicle authentication logic | Trust evaluation mechanism | V2V,V2I | Eavesdropper and prankster | Attacks on authentication | NS2 |
| [23] | Efficient unidentified location based routing protocol | Digital certificates, public key infrastructure and mixed zone based security approach | V2V,V2I | Eavesdropper and inside attackers | Attacks on privacy and integrity | Mobility simulator |
| [24] | Event based reputation system | Local certificate generation and validation | V2V,V2I | Eavesdropper and inside | Sybil attack | Trace driven |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | approach, Event status value and trusted value setting approach | | attacker | | |
| [25] | Elliptic curve digital signature algorithm | Elliptic Curve Encryption approach | V2V | Prankster | Attacks on authentication | OPNET |
| [26] | Misbehavior detection scheme | Ensemble learning approach | V2V | Eavesdropper and prankster | Attacks on liability and non-repudiation | WEKA and NCTUns-5.0 |
| [27] | Hybrid authentication protocol | Signcryption - cryptographic primitive approach | V2V | Prankster | Attacks on authentication and secrecy | NS-2 simulation |
| [28] | Honeypot solution for practical security | Honeypot concept | V2V and Intra-Vehicle Communication | Malicious attacker | Attacks on integrity and reliable data | Zenmap and OpenVas |
| [29] | Comprehensive message authentication scheme | Encryption concept | V2I,Intra-RSU communication and RSU-RSU | Prankster and Malicious attacker | Replay attack, false impression attack, message modification | NS2 |
| [30] | Sybil attack detection scheme | Privacy preserving beaconing and warning mechanisms | V2V,V2I | Inside attacker and eavesdroppers | Sybil attack | NS2 |
| [31] | Efficient physical layer location privacy scheme | Cluster based fake-point approach | V2V,V2I | Physical layer attacker | Location privacy attack | MATLAB |
| [32] | Privacy preserving | Onion routing approach | Network nodes | Eavesdropper | Traffic analysis | Onion router |

| | | | | | | |
|---|---|---|---|---|---|---|
| | scheme | | | | attacks | |
| [33] | Web surfer privacy scheme | Snooper Script | Intra vehicle | Prankster | Attacks on web surfing | Netscape Version 2.0 |
| [34] | Proficient shared authentication scheme | Key establishment scheme in view of symmetric polynomials | V2V,V2I | Hungry driver | Denial of service attack, replay attack | OMNET ++ |
| [35] | Private key based encryption algorithm | Cryptography based approach | V2V,V2I | Inside and outside attacker | Attacks on authentication and secrecy | QualNet |
| [36] | PUF Based Privacy Protection Method | Handover process and mutual authentication process | V2V,V2I | Eavesdropper | Eavesdropping attack, Replay attack, Masquerading attack | Not specified |
| [37] | Protocol to prevent distance hijacking attacks | Distance-Bounding | V2V | Inside attacker | Distance hijacking attacks | Not specified |
| [38] | Efficient authentication scheme based on batch verification | Bilinear pairing | V2V,V2I | Prankster | Replay attack | Not specified |
| [39] | Efficient batch authenticated scheme | Elliptic curve digital signature | V2V | Prankster and malicious attacker | Replay attack and non repudiation | NS2 |
| [40] | Lightweight identity authentication protocol | Dynamic session secret process and pre-key distribution approach | V2V,V2I | Eavesdropper and prankster | Eavesdropping attack, replay attack, location forging attack | Series of simulations on a freeway mobility model |
| [41] | Authentica | Blind | V2I | Eavesdr | Location | Not |

| | | | | | | |
|---|---|---|---|---|---|---|
| | tion scheme for location privacy | signature approach in elliptic curve area | | opper and Prankst er | privacy attack | specified |
| [42] | A collaborati on based scheme for managing alert propagatio n | decentralized and cooperative model | V2V,V2I | Inside attacker and prankst er | Attacks on authentic ation and secrecy | NS3 |
| [43] | Efficient trust manageme nt scheme | Trust token | V2I | Eavesdr opper and prankst er | Attacks on authentic ation and secrecy | NS2 simulatio n |
| [44] | Novel hybrid authentic ation method | Signcryption without certification and pairing | V2I | Prankst ers | Sybil attack | Qualnet |
| [45] | Authentic ation protocol with multiple level of anonymit y | identity based signature mechanism | V2V | Prankst er | Replay attack | QualNet |
| [46] | Novel approach to enhance the security through user authenticat ion | Biometric encryption approach | V2I | Malicio us attacker | Replay attack, Modificat ion attack | Java J2SE |
| [47] | Efficient group signature based security solution | Elliptic curve digital signature algorithm with private/public keys of trusted authority | V2V,V2I | Hungry driver and Inside attacker s | Denial of service attack, replay attack | Android platform and JAVA |

| | | | | | | |
|---|---|---|---|---|---|---|
| [48] | Batch verification scheme based on group signature | Key pairing approach | V2V | Malicious attacker and eavesdropper | Key duplication attack, eavesdropping | Not specified |
| [49] | Secure cross authentication protocol | Asymmetric encryption | V2I | Inside attacker, pranksters and malicious attacker | Attacks on authentication, Attacks on integrity and reliable data | Not specified |
| [50] | Privacy preserving scheme for traffic congestion detection | Information gathering over air traffic | V2V | Inside attacker and prankster | Traffic analysis and eavesdropper | Scalable wireless Ad hoc network simulator |
| [51] | Lightweight and efficient strong privacy preserving scheme | Message authentication code, Symmetric simulation | V2V,V2I | Hungry derivers and pranksters | Denial of service attack | Opportunistic networking environment |
| [52] | Privacy protection scheme | Bilinear pairing and elliptic curve | V2V,V2I | Malicious attacker and Eavesdropper | Forging attack | QualNet |

The security solutions are summarized on the basis of technical features of the solutions. Comparison among various security solutions is made on the basis of security solution, approach followed, communication type, attacker, attack model, and simulation scenario. The analysis of percentage of research papers on different communication types and security solutions offered in VANET are represented through Figure 1.1.

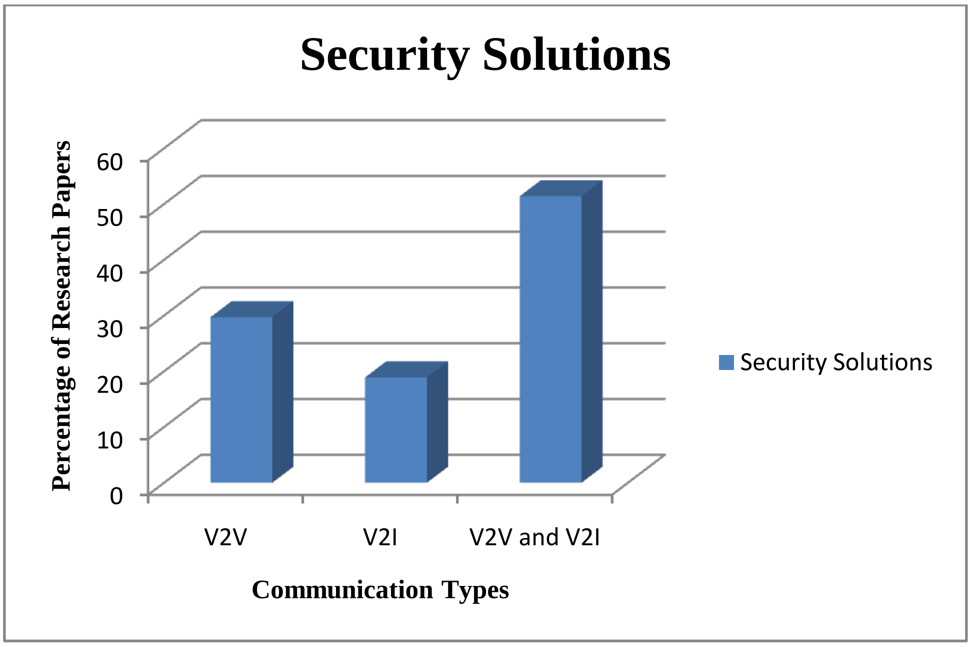


**Figure 1.1: Percentage of Research Papers for Each Communication Type**

According to this analysis, there are 29.7 % papers on security solutions using V2V, 18.9 % papers using V2I and 51.4 % papers using V2V and V2I both. From the above survey it is noticed that, security solutions can be given by offering authentication, confidentiality or privacy using both V2V and V2I. But most of the work done so far in security consideration of VANET revolves around providing authentication services. Therefore, in next section different authentication schemes available in VANET are considered.

### 1.2.2 Authentication Schemes in VANET

VANET offers safety based and non-safety based applications. Safety applications work on both, V2I or V2V. Non safety based applications are considered to augment traffic optimization, availability of services. It has been inferred in [53] that road conditions and warnings can be generated in VANET using cooperative learning. The architecture for communication in VANET consists of different domains of working like in-vehicle, where the requirements for vehicle is revealed, second is ad hoc to show how one vehicle communicates with other and last is infrastructure that represents how vehicle communicates with the fixed road side units [54].

In [55], it has been discussed that proxy encryption schemes are still vulnerable. So an improved scheme was proposed to overcome the problems like prevention to convert original text to delegate text.

In [56], different schemes have been presented for authentication to prevent the identity of user and to maintain the privacy of the system. But these systems make use of passwords that can be guessed or can be revealed.

In [57], a common furtive key has been reserved for multiple RSUs using the proposed symmetric key dependent approach. The key pre-required is initially shared through a secure mode, hence avoiding the need of procedure for key allocation during any handover.

In [58], a pair of private and public key featuring asymmetric key dependent approach has been described that works on contending for key verification and allocation.

In [59], depending upon the group based signature and identity based signature approach, confidentiality preserving scheme has been proposed. Confidentiality, security and efficient traceability has been obtained using group signature. On the other hand, identity based signature technique has been used to minimize the complication raised for handling the public key referred and the related certificate.

In [60], RAISE, a new message authentication based scheme that is RSU supported has been proposed. For verification, this scheme proves the authenticity result of the message transmission performed by the vehicle to all connected vehicles. This acts as a major work area of RSUs in this scheme.

In [61], authors have proposed an authentication and identification scheme. The identification number of vehicle has been utilized for authenticating and identifying the moving vehicle. Proposed scheme offers service required for authentication only in V2I based communication.

In [62], authentication scheme working in decentralized mode has been addressed. RSUs, in this scheme tend to maintain on-the-flutter engendered rush in their respective range of communication that is relatively high as opposed with the communication range of moving vehicle.

In [63], time stamp based authentication approach is proposed to provide authentication among vehicles and RSU. Legal users are protected from malicious attacks with the help of this authentication approach. This authentication approach provides privacy to every vehicle by not revealing the original identity of vehicles.

In [64], a light weight authentication scheme is mentioned that provides authentication among vehicles and RSUs in VANET. This scheme utilizes hash function, XOR operation and symmetric cryptography to provide privacy and security among vehicle and RSU in VANET.

In [65], a novel ID based authentication scheme is proposed to provide secure RSU to Vehicle communication in VANET. For authentication this scheme uses road pass ticket and vehicle plate number. The effectiveness of this scheme was analyzed by using Petri nets.

Based on the literature survey conducted on authentication schemes in VANET, the different schemes are compared as shown in Table 1.2 below.

**Table 1.2: Summary Table for Existing Authentication Schemes**

| **Reference Paper** | **Authentication Mechanism used** | **Vulnerability** |
|---|---|---|
| [55] | Proxy encryption | Allow further delegations of key to third party |
| [56] | Password based | Passwords can be guessed/revealed |
| [57] | Symmetric key based | Vehicle’s pseudonym ID compromise |
| [58] | Asymmetric key based | Security does not work well for complicated movements |
| [59] | Identity and group based signature approach | Compromise of identitty of user |
| [60] | k-anonymity approach | Misbehaving/ Faulty vehicles |
| [61] | Identification number of vehicle | Entry of illegitimate vehicles in network |

| | | |
|---|---|---|
| [62] | Group authentication protocol | Vehicle secret key compromise |
| [63] | Unique timestamps | Routing protocol is not secure |
| [64] | Hash function/ symmetric key | Privacy of V2V |
| [65] | Road pass ticket/ Vehicle plate number | Compromise of RSU secret key |

Table 1.2 states the authentication mechanism and persisting vulnerabilities in existing authentication schemes. For offering ITS in VANET, the data needs to be collected from the vehicles on road. Next section describes the existing schemes for collecting data.

### 1.2.3 Data Collection Schemes in VANET

Different schemes exist in literature that works on collecting path information from the vehicles. They might not work as actual DCSs but it becomes easy to fetch general information using them about the vehicles. Broadly the DCSs can be categorized as represented through Figure 1.2.

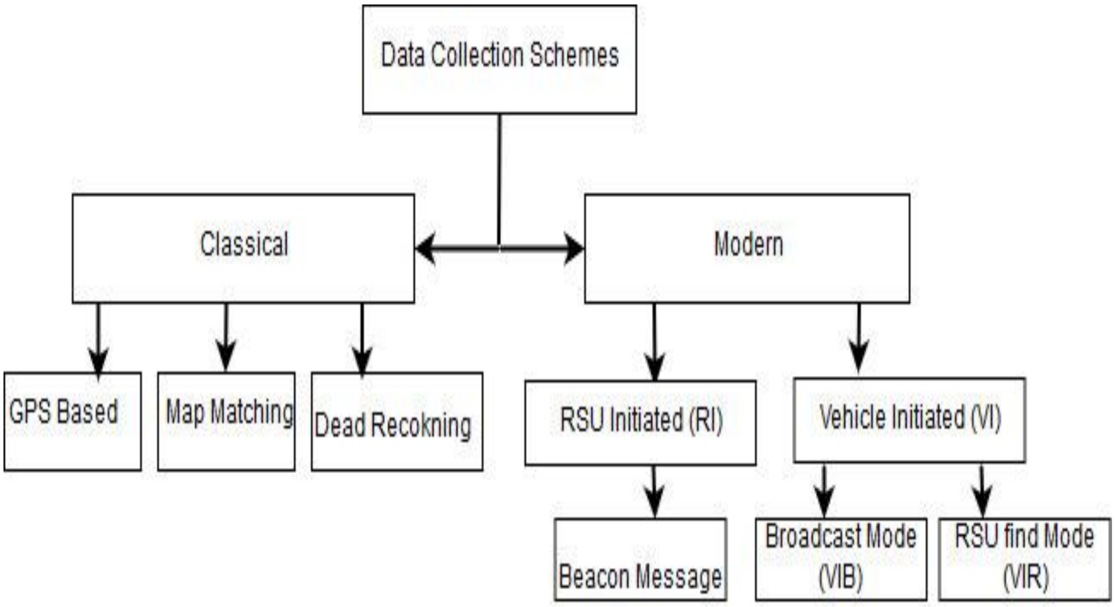


**Figure 1.2: Data Collection Schemes in VANET**

In [66], it has been explained that U.S Department of defense, evolved GPS in early 1973 by. GPS works on twenty four different satellites that function in the orbit which is moving around the earth. Each one of the 24 satellites revolves at the height of approximate 20,200 km around the earth and that too twice in a day. The

Placement of orbits is in such an order that every zone of earth is under surveillance using at-least 4 satellites. These 4 satellites work on passing the updated information collected to the GPS receivers.

In [67], authors worked on monitoring the data collected by noticing variable activities like humidity, fire, temperature, etc using GPS. Locating nodes that are currently moving in the network are tracked smoothly using GPS. Trilateration technique has been used along with Time of Arrival (TOA) for locating the current position of the vehicle. Various problems linked with obstacles due to line of sight in collection like trees, walls, buildings may lead to inaccurate tracking of location information.

In [68], authors have stressed on a point that GPS may not be available at all the times. Therefore, every vehicle should not be equipped with GPS as GPS sometime does not provide the robust solutions that may lead to serious problems in VANET.

In [69], author proposed a protocol that has been used to determine vehicle's location without using GPS considering above stated disadvantages. This scheme used a clustering based approach, for that different cluster heads have been nominated for taking responsibility of communication with the distinct nodes present in the current network working under a common system coordinator.

In [70], authors have worked on the map matching technique. This technique works with any other technique for tracking of position like GPS and is itself not working for position tacking. Map matching based technique fetches the location that is tracked using GPS and finally loads it on a map. This works for estimating and pinpointing the exact vehicle's location on the map.

In [71], author discussed various techniques for map matching considering the short time intervals for polling in order to match the GPS points. Therefore, a algorithm which works well for long polling time interval has been proposed.

In [72], to estimate the location of the neighboring nodes a method called as dead reckoning has been proposed. The current position of the vehicle can be estimated by fetching its last known position and by using the information related to vehicle's movement such as distance, speed, and time. The last known position of the vehicle has been found either by using GPS or may be any other reference point such as crossing, river, etc. Therefore, when the GPS losses its connection such as during travel under tunnel, dead reckoning works well under these situations to track the position.

In [73], authors worked on cellular architecture. Deploying the area and that area is divided into numerous cells. The vehicle location has been estimated using the signals obtained from the cells. Towers in each cell collect the information passed by the vehicles during handoff. This information helps in determining the level of congestion or any other unusual cellular activity.

In [74], poisson method that does not work for longer times, have been replaced by mean and variance for handoff traffic modeling. During the process of handoff, the traffic patterns have been identified. Finally, this leads to identify the patterns of traffic in VANET which are more constrained due to highly mobile vehicles.

In [75], for fetching the status of traffic congestion on road, a metric, CDT (Cell Dwell Time) has been proposed. Before a vehicle made a handoff to a new base station, CDT finds the active time of vehicle connection with a particular base station. Therefore, a large value of CDT showed the vehicle connectivity to a base station for a long time, and acted as a alarm for heavy road traffic congestion.

In [76], authors worked on various update procedures for estimating the moving vehicles position. Here, vehicles have been assumed as clients and on other hand a centralized database is assumed as a server. These methods have been used to track the movement of vehicles, so a wireless communication is set to send the updates from vehicle to the server. First, Point-Based technique, where after a certain distance threshold is reached then the vehicle, updates its location to the server. Second, in Vector-Based the update about location is based on time that takes two factors, that is, start point and velocity of the moving vehicle into consideration. Third, Segment-Based shows the operation of the segment-based approach, where vehicles send an update message to the server with their location based on the road segment they are about to traverse.

In [77], modern DCSs were proposed and divided in two broad types considering whether data collection procedure is RSU initiated or Vehicle initiated. In RSU initiated, a beacon message is sent by the RSU and in vehicle initiated approach, the packet transmission initiates from the vehicle in the broadcast mode.

In [78], a new road side probing scheme has been proposed, where RSU commenced the procedure of probing by enquiring each moving vehicle on the road. This is done to collect traffic, environmental, or accidents information.

In [79], two methods have been proposed using broadcast mode for collecting the data. First, the two hop confined broadcast method and second is probabilistic two hop confined broadcast method. Both of them worked to infer road traffic congestion and thus ultimately optimize the range of detection for a RSU to an extreme extent.

Based on the literature survey conducted on DCSs in VANET, the different schemes are compared as shown in Table 1.3 below.

**Table 1.3: Summary Table for Existing Data Collection Schemes**

| Reference Paper | Method Used | Shortcoming(s) |
|---|---|---|
| [66] | GPS | Not available all the times |
| [67] | Trilateration technique | Problem to find accurate path due to line of sight issues |
| [68] | Data fusion technique | Takes time to compute location |
| [69] | Clustering technique | Chance of position error |
| [70] | Map matching | Additional resources are required for finding location |
| [71] | Map Matching with long time intervals | No efficient determination of nearest GPS points |
| [72] | Dead Reckoning | Does not work for broader area |
| [73] | Cellular architecture | Handoff becomes difficult when mobile users increase |
| [74] | Hand off using mean and variance | Less effective in highway scenario |
| [75] | CDT | Accuracy is less for free flow traffic |
| [76] | Three tracking policies | Can be used only for small segments |
| [77] | RSU initiated and vehicle initiated | Do not offer security |
| [78] | RSU probing | More overhead on RSU |
| [79] | Two hop broadcast- confined and probabilistic confined | Probable outcomes- less accurate |

Table 1.3 states the data collection methods and their respective shortcoming(s). after data collection is over, some technique is required to obtain the desired information

from that huge bulk. Therefore, next section discusses the existing data mining techniques.

### 1.2.4 Data Mining Techniques in VANET

In [80] data mining is explained as a technique that works on extracting unambiguous information from the data collected using any DCS. Data mining evolved as a significant and prominent research area because of extracting meaningful information in the real world database. Major challenges in using any data mining technique are redundant data, massive data sets, and incomplete data.

Here various data mining techniques that have been used in the field of VANETs and their applicative service after being implemented have been discussed. Most of these data mining techniques have been used previously in other applications and industries, but mainly the focus is on predicting the future behavior on already available data.

#### *1.2.4.1 Forming Clusters*

Clustering works as an learning technique that is completely in a unsupervised mode. Clustering is assumed to have number of clusters, where each cluster is also referred as a class possessing the same properties. Every cluster has a pre nominated member called as a cluster head (CH). Inter-cluster association is very less as compared with intra-cluster association that is under observation of corresponding CH. To fetch the accurate real time information related to accidents or traffic jams, clustering technique is preferred. Different techniques using clustering have been devised in literature for mining data in VANET. Few of such techniques have been discussed below.

In [81], authors used HELLO messages in the proposed technique used to exchange state information among the vehicles. After a new vehicle joins the network it first enters unpredicted state. Within a specified time limit, if a message is not received the vehicle declares itself as CH. Otherwise, if it receives a message for connection from other vehicles; it has to registers itself under the existing CH as a new member node. In this technique, destination is already known to the node that helps to forward the message directly to the destination.

In [82], the similar mechanism is adopted which has been applied in above stated scheme for designing a cluster. A Node may be a member in multiple clusters. In that case, node is behaving as a gateway of two clusters and work to route the packets at the appropriate destination. Each node maintains two tables to track updation in the topology; first for neighbor ones and next for the neighbor clusters. If two different cluster heads appear in contact with each other, one of these has to leave its responsibility as cluster head and joins the other. Weighted factor is used to decide which CH should keep its state and which one not. To improve QoS this work also give emphasis on media access control.

Author in [83] proposed a multi-channel cluster oriented distributed scheme for offering QoS improvement in VANET. QoS is required for the real-time collected data that further helps to increase the throughput of traffic that is non-real time. The cluster formation is done using the classical techniques discussed above. This scheme uses two transceivers on each vehicle that can work concurrently on various channels. Members of cluster make use of a transceiver to interchange messages among them and service channel to communicate with the cluster head.

In [84]**,** a clustering technique is proposed using the analogy of minimum dominating sets (MDS) in order to appoint a CH. The approach used is well referred like position oriented prioritized clustering (PPC). This makes use of geographic location of the available nodes along with precedence of information related to traffic of vehicles in order to design cluster scenario.

In [85], author proposed a different clustering scheme for categorizing the vehicles in different zone depending upon their speed range. If vehicles are moving with same level of speed they are designated for one specific group or may be in the same forming cluster. For the minimum and maximum value, seven groups are defined according to the speed that moving vehicles must follow. If a vehicle belonging to any cluster changes speed after some time, then its group must be updated.

#### *1.2.4.2 Association Based Rules*

In [86], association is described as the interconnection among objects and depth of togetherness. Existing of one of the objects in a set assures the existence of related object using association rule. Further to guarantee the timely release of safety related information, plenty of effort has been done to minimize the delay and improve the packet exchanges.

In [87], author discovered that an organization can improve its decision making capability by determining the customer's past interest areas. As there has been a huge set of database that includes information from many users, a mining technique should be such that it can only provide the interesting products to the customers. Therefore, according to request of user, the association rules have been generated

In [88], VANET Association Rules Mining (VARM) scheme has been proposed According to this scheme, to detect faulty and malicious vehicles each vehicle aims to gather data for each of its neighbor in its vicinity and finally to mine different rules for temporal correlation.

In [89], considering an application of VANET authors have taken advantage of mining based on association rules. The major focus is to apply association rules mining in their proposed driving assistance system that is context-aware to dig out the control rules from the information system. It also prevents the traffic accidents to occur. Considering the current extracted control rules and vehicle situation information, a pattern similarity mechanism works on finding a correlation among the events in the information system and the current events that were the reasons for accidents or fatalities. Reflecting this feature, this work can offer drivers a effective and safe actions to be taken in order to stay away from an accident or reduce effect of such an accident occurring in near future.

In [90], it has been suggested that four ways are there to reduce the computational cost and thus to enhance the competence of association rules:

• Decrease count of elapses in database

• Sample the full database

• Make use of parallelization and for the prototype of organization add more constraints.

#### *1.2.4.3 Classification*

In [91], authors framed a model where using a training set (set of tuples), a set of predetermined classes are described. This data mining technique aims to define the grouping of unknown objects based on some of the attributes of this object. An input is required to be collected from each user, for example, in this scenario input is the training set, making it as a supervised technique. Therefore, it helps to frame a model and then accordingly train it.

In [92], different classification techniques have described that have been used in different VANET applications like induction based on decision tree, bayesian networks, reasoning for specific case, fuzzy logic techniques, neighbor k-nearest classifier, and finally genetic algorithm.

In [93], the proposed mechanism worked for offering a security approach based on engineering in VANETs. This is done for the validation of security required for distinguished VANET applications. For achieving this, the authors detailed the benefit of data mining using classification so as to investigate the huge range of VANET applications, classify them according them based on security requirements (e.g., severe authentication level required, replay attack susceptibility, etc.) and finally for every class offer a security solution. Using the model constructed, new application can be assessed based on their security requirements and the appropriate security measures can be applied.

#### *1.2.4.4 Sequential mining*

In [94], sequential mining has been devised to find out those events that generally occur frequently and mostly together. The sequence list can be generated depending upon the order of events or on the time basis. If an item occurrence time cross a set threshold value, the item is referred as frequent.

In [95], by formally defining movement patterns, a new algorithm has been designed to figure out the mining patterns that are frequent. This technique initially gets relevant spatio-temporal areas and fetches most frequently occurring spatio-temporal patterns on the basis of prefix and projection method using sequential areas.

In [96], for fast pattern mining authors suggests a new protocol DFS_MINE using approach like depth search in order to estimate the largest sequential pattern.

### 1.2.5 Salient Features of Data mining Techniques in VANET

Salient features of three data mining techniques in VANET discussed above is stated in Table 1.4 considering the usage of different methods for data mining, objectives of the approach, the dataset used, and their major benefits and contributions.

**Table 1.4: Salient Features of Data Mining Techniques**

| Data Mining Technique | Data Collection Method | Previous Data History | Maintenance of Datasets |
|---|---|---|---|
| **Forming Cluster** | Data having similar characteristics obtained from communicating vehicles only is stored in clusters | Previous data history is not maintained. Real time information related to congestion is collected | Data set is maintained by discovering the similar groups without known structures in data |
| **Association Based Rules** | Data is collected from vehicles and pattern is discovered based on historical data. | Previous data history is stored that helps in detecting events Real time information related to congestion is collected. | Data set is maintained by searching the relationship among the historical and new data |
| **Classification** | A training set is a prerequisite for mining depending on pre defined set of classes. | Collects real time congestion information, and generalize them using known structure. No previous data is maintained. | Data set is maintained by generalizing new data based on known structure. |

### 1.2.6 Logical Behavioral Arrangements

From the past few years, various government transportation organizations, employers and researchers have been paying concentration in the paths opted by their vehicles during their tours. This information was vital for numerous useful purposes like efficient study of traffic surroundings in a certain region, traffic and congestion control in city and appropriate scheduling along with shipment modeling for timely release of products [97]. Transportation agencies used some of the prior techniques like path side/tollbooth [97] ,mail- out mail- back analysis [97]–[100] and telephone analysis [101] of gathering the information about the paths opted by the vehicles during their journey for tracking the goods movement efficiently and moreover to identify some other efficient methods to deliver of goods. High respond time, erroneousness and high execution cost are the major problems associated with these techniques. The authors in [102] have proposed a computer visualization scheme to count moving vehicles on path which can be used to keep an eye on traffic data on main paths and to collect traffic data for path estimation intentions. This scheme consists of four types of image processing modules: a) path creation mining b) vehicle recognition c) measurement of vehicle speed d) Tracking movement of vehicles. The authors in [103] have projected the exploit of wirelessly fixed ATM based network units to trace motion of moving vehicles all the way through a geographical area. Routes traversed by the vehicles during their trip are described in the outline of a series of ATM units. In [104], three types of location tracing policies have been described by the author: (1) point-based, (2) vector-based, and (3) segment based. The authors in [105] have described a novel vehicle tracking scheme to make available precise data on directional traffic calculations at junctions. The mined count ups are provided to guess a source destination tour table that is essential data for traffic collision study as well as transportation planning. In [106] beaconing rate based, an adaptive intelligent approach have been proposed using fuzzy logic to regulate the message exchange rate among vehicles to describe on various types of incidents. In this approach, the proportion of moving vehicles in identical direction and the vehicle's condition are considered as key values of fuzzy system used for decision making, so as to amend the rate of beaconing as per traffic distinctiveness of vehicle. In [107], an automatic vehicle categorization and tracking technique have been proposed to estimate the vehicular movement traffic parameters at signalized intersections. This technique has a good talent to categorize the identified vehicles and then vehicle's movement parameters are calculated at intersection area.

In [108], a new technique is used to detect the number of moving vehicles and vehicle speed is measured in low light situations have been proposed. Centroid area difference method and normalized cross correlation method are used to notice the vehicles for detecting its headlight. Headlight is deployed to spot the movements of vehicle. Euclidean distance and Pin-hole methods are applied for estimating the speed of vehicle. In [109], a new non linear movement model using projection model and shape model have been proposed to track and detect vehicle in non linear motion. The precisely evaluated results of location and vehicle velocity are given by speed, posture, last location.

Various types of applications have been introduced in terms of data mining for variety of purposes. Predicting accidents that may happen in future in advance, association rule based mining is examined to avoid danger on the road. This method generates a large set of rules [110]. In [111] an vehicular data platform and two data mining models have been proposed. In vehicular data oriented platform vehicle based information such as safeguarding details can be smartly attached to description of vehicle drivers. Two distinguished data models are implemented using natural language processing. In [112] a status validation scheme using certificate revocation EKA2 have been proposed to carry out a reliable and trusted authentication by ensuring the trustworthiness of RFIDs considering validation of digital signature. The idea of data mining clustering method has been used to estimate the confidence level of digital certificates.

Route and Mobility forecasting have been studied and examined in numerous works. As in [113] to attain an proficient multi-hop broadcast, a reliable scheme based on mobility estimation for broadcast routing have been proposed. This scheme partitions the neighbors in numerous sets firstly in accordance to the movement route; then to predict maintain time of all neighbors this scheme utilize the position and velocity; finally multiple rebroadcast based nodes are chosen. In [114] a new approach for predicting the driver intention which utilizes driver's daily predictable nature. This approach predicts source and destination projected by driver by using probabilistic based model by surveillance of inherent behavior of their driving. To forecast the next path segment Hidden Markov Models (HMM) has been utilized. In [115] to predict next path segment, a amalgamation of probabilistic suffix trees (PSTs) and a Variable-order Markov Model is used. In [116] authors propose and tests algorithms to predict the route of the vehicle from source to destination based on GPS surveillances of the prior vehicles trips. The proposed algorithms utilize the fact for predicting the next segment that a huge section of a typical driver's tours are repeated. In [117] a receiver based routing algorithm (RBRA) is proposed that makes use of a routing metric. Routing metric considers the remaining lifetime of a link along with the length of each hop. Moreover, vehicles follow a newly designed mobility model that is designed to identify motion of moving cars. In [118] performance of routing protocol based on position in VANET is improved, for this an intermediate node selection algorithm (INSA) that predicts vehicle motions is proposed.

Based on the literature survey conducted on logical behavioral arrangements in VANET, the different methods are compared as shown in Table 1.5 below.

**Table 1.5: Salient Features of Existing Logical Behavioral Arrangements**

| Reference Paper | Salient Features |
|---|---|
| [102] | Count number of moving vehicles |
| [103] | Routes are traversed as outline of ATM units |
| [104] | Location tracking policies |
| [105] | Use of mined count ups |
| [106] | Moving vehicle and vehicle's condition used for decision making |
| [107] | Estimate the vehicular movement traffic parameters |
| [108] | Centroid area difference method and normalized cross correlation method for movements of vehicles. |
| [109] | Works on non linear movement model using projection model and shape model |
| [110] | Association rule based mining is examined to avoid danger on the road |
| [111] | Safeguarding details are smartly attached to description of vehicle drivers. |
| [112] | Data mining clustering method was used to estimate the confidence level of digital certificates. |
| [113] | Movement route, utilize the position and velocity of vehicles, and choose nodes |
| [114] | Predicting the driver intention which utilizes driver's daily predictable nature based on HMM. |
| [115] | PST and a Variable-order Markov Model is chosen to predict next path segment |

| | |
|---|---|
| [116] | GPS surveillances is used to predict the route of the vehicle |
| [117] | Mobility model was designed to identify motion of moving cars |
| [118] | INSA is used to predict vehicle motions |

Table 1.5 states the method for logical behavioral arrangements specifying their salient features.

### 1.2.7 Path Map Generation in Vehicular Ad hoc Network

In recent days, the major challenging application on VANET is to generate best path map for a vehicle. The segments a vehicle has to cross to arrive at the destination forms the best path with features like less time, without any traffic or collision issues. Therefore, for finding the best path, the need arises to collect the data from the vehicles moving on the road moving to same destination but opting different path segments under any unusual situations like bad road, or may be accident. The first concern for finding the best path to be opted by vehicle is to select an efficient DCS. The existing path identifying schemes are static in nature like GPS, as path information to a specific destination is not estimated based on any current unusual activity such as accident. Therefore, a dynamic DCS is that which collects information related to current situations is required and then data is stored at RSU after collecting it from the moving vehicles that are in its vicinity.

Afterwards, on the data stored at RSU, data mining is applied to generate the best and useful path map opted by the vehicles while moving to a destination. The collected information is very huge as the vehicles that are travelling on the road are more and are passing their segment information to the RSUs continuously. The paths following a particular source to a particular destination are decided by applying mining on the collected data. Mining should be applied in such a manner that the best path should get generated from the various paths exposed from specific source to destination, based on position, direction, time of the day, or any accidental case.

## 1.3 Problem Statement

The state-of-the-art on VANET has raised the following problems that are considered for the research work.

**Problem Statement 1:** Is there an authentication mechanism available that provides a secure connection between vehicle and the network? Does this mechanism avoid attacks on the network? Is it acceptable for the performance of VANET?

**Problem Statement 2:** How to collect the information from vehicle once authentication is performed? Is it possible to improve the performance of DCS along with maintaining security?

**Problem Statement 3:** What are the different parameters available for the evaluation of DCS effectively?

**Problem Statement 4:** How to generate path maps once the data is collected from the vehicles? What kind of rules can be generated to deduce the efficient paths in varying situations?

**Problem Statement 5:** How to build support and confidence in the generated rules for path maps?

In this work, problem of generating efficient path maps by applying data mining on the distributed RSUs in VANET have been addressed. A path map for a vehicle includes all the road segments that it should traverse to arrive at destination without any traffic or collision problems, within time, and reduces wastage of fuel.

To get the path information for a vehicle previous data need to be collected and thus a path map can be generated based on factors like position, direction and time of the day. So, complete area, for example a city, is divided into various regions and every region keeps one RSU installed, such that, complete area is covered by multiple RSUs. DCSs collect the information from the vehicles on road and then data is transmitted to the RSU that are in the vicinity as displayed in Figure 1.3. Once the overall data collection becomes over, mining can be applied on collected data to retrieve the best path map.

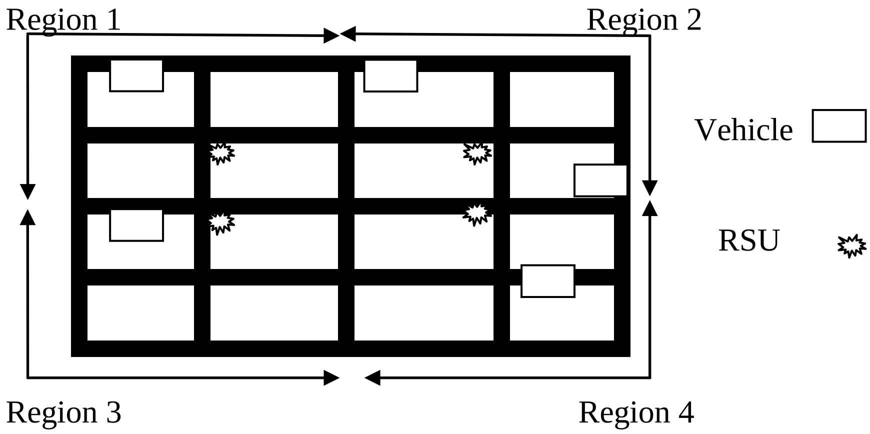


**Figure 1.3: Area consisting of 4 RSUs and moving vehicles**

## 1.4 Motivation

Rapid development of communication networks has encouraged vehicle to road side and inter-vehicle communication in VANET. VANET inbuilt characteristics tend to work on efficient traffic management on road, security on road, well maintained driving conditions. Therefore, congestion on road increases with the number of increasing vehicles on road that result in huge number of traffic accidents. The existing transportation systems are static in nature and are unable to respond well in unusual situations. Moreover, dynamic topology of VANET brings forward the challenge of security and safety of each vehicle that becomes part of the network.

Researchers have worked on numerous solutions to handle the unusual situation in VANET. For this data is collected from moving vehicles from particular source to destination. The data collected helps to identify the possible paths from a particular source to destination. Existing data collection schemes are not secure and any vehicle either legitimate or not can join the network and share the information. Illegitimate vehicles may pass wrong information to road side units and this result in false path information, which will ultimately become a situation of chaos.

Moreover, existing work is less concerned on security of vehicles and RSU that also affect the performance of VANET with fast moving vehicles and dynamic topology. Considering the security, efficiency, optimum resource utilization of VANET, a new improved data collection scheme as well path map generation method using distributed RSUs need to be launched. With an aim to improve existing system of transportation in unexpected situations in order to route the traffic accordingly and that too without losing the confidence of user in the system becomes novel concern in this research work.

## 1.5 Research Objectives

This section formulates the objectives based on the detailed literature survey conducted. First, research gaps are identified from the detailed literature study on data collection, mining and security for path generation in VANET. Later, challenges faced by VANET are drawn and final objectives are laid out to fill the gaps and to overcome the challenges.

A detailed literature study has resulted in drawing out the following research gaps:

- Existing data collection schemes are vulnerable to attacks because they have weak inbuilt authentication mechanisms.
- After collection, data mining is applied to take decisions. These decisions can be utilized to generate frequent paths for vehicles during unusual situations to avoid road jams or accidents.
- In literature reliability of the decision made is at stake, therefore, minimum support and confidence parameters should be taken into consideration before executing a decision.

The primary and key challenges in VANET depending on the practical perspectives are derived as mentioned below:

a) **Signal loss:** Obstacle can be created between the two communicating vehicles by placing any hurdle between them, which restricts the signal to arrive at the destination .Thus, expanding the fadedness of the transmitted signal [119].

b) **Limitations of Bandwidth:** Optimal utilization of bandwidth is essential in VANET, as no central authority is appointed in VANET to manage bandwidth and conflict operation.

c) **Connectivity:** Considering the dynamic network topology with high mobility, connectivity is considered as significant issue in VANET [120]-[121].

d) **Restricted efficient diameter:** To keep up the complete worldwide topology in VANET is impracticable for a vehicle because of confined effective diameter.
e) **Security and Privacy:** The security and protection is the most critical difficulties in VANET; getting of trustworthy data through its source is vital for recipient.
f) **Routing protocol:** Designing an efficient routing protocol to send a packet as soon as possible, especially in the earnest circumstance is considered to be a significant challenge in VANET system [122]-[124].

This research work aims to determine best paths to be followed by a vehicle from a particular source to destination so as to improve efficiency in terms of distance travelled and time taken. Distance can be reduced by providing shortest path and if any accident or rush is there in available path a different path should be suggested for vehicles to reduce the time taken. Paths that can be opted by a vehicle can be predictable or un-predictable. Predictable paths can be based on time of day like morning, evening, or night, but an un-predictable path is a consequence of any accident or jams. Various schemes were used in past for collecting the path information of a vehicle but they increased latency and reduces the packet delivery ratio during the communication. Therefore, a DCS is proposed that will improve the packet delivery ratio and reduces latency. Once the data is collected, data mining is applied on the data collected by RSU using association rule based mining to get the most common and frequent paths that vehicles traverse from one source to destination Finally different sets of data on the basis of position of vehicle, that is, to suggest relative paths, direction either forward or reverse, during time of the day (morning, afternoon, evening, and late hours), and alternate paths due to accidents or jams. For example, during the morning hours vehicle will be suggested to take an outer path rather than to travel inside the city to avoid rush. So our work is divided into three phases starting from data collection to data mining and then retrieving most common and frequent paths.

More specifically, this work covers the following objectives

1) To propose a new technique for data collection that will improve throughput, packet delivery ratio, and reduce latency.

2) To extract the possible paths from the data collected using association rule base mining on distributed RSUs.

3) To predict the common and most frequent paths on the basis of position, direction, time of day, and during any accident or jam.

## 1.6 Research Methodology

The proposed methodology based on the problem chosen for research work is represented through Figure 1.4

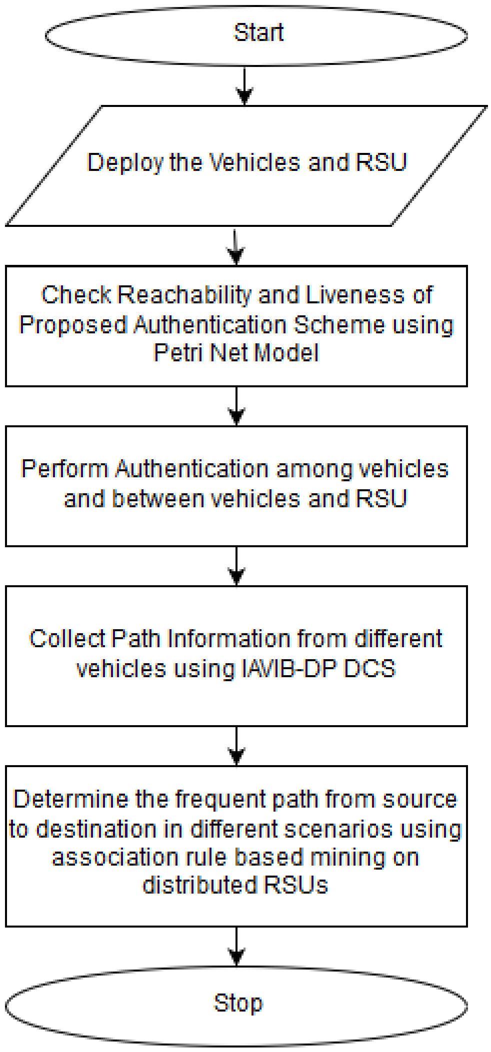


**Figure 1.4: Flowchart for Research Work**

The working mo/del of this research work consists of multiple RSUs that are connected to a centralized server as represented through Figure 1.5. Here, the vehicles operate using an OBU that has an AU within it. Vehicles collect the data on road from specific host to destination and send that data to the RSU that lies in its vicinity. RSU on receiving this information forwards it to the server. Server at last applies mining on data and helps in generating the efficient paths.

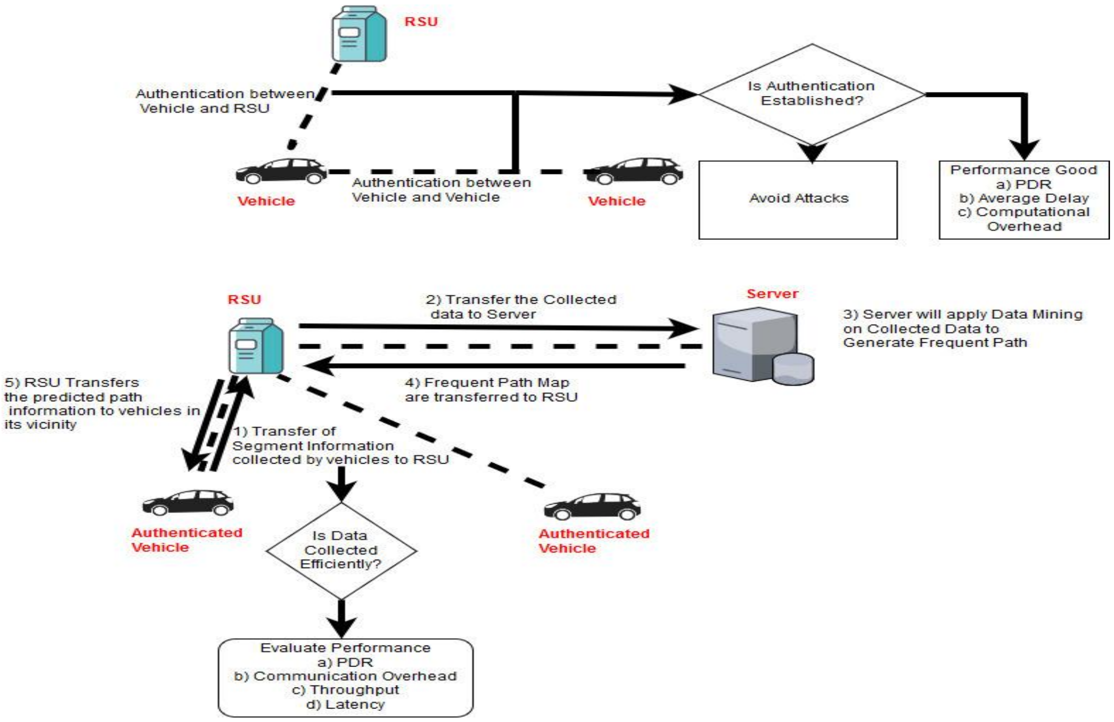


**Figure 1.5: Working Model**

## 1.7 Research Assumptions

To carry out this research work a simulation environment is created using vehicles and RSUs. Vehicles are equipped with OBU that makes use of transceiver and a GPS for location tracking. RSU collects the data in buffers and are responsible for clock synchronization among the vehicles using beacon messages after a fixed interval of time. The simulation scenario is chosen for the city based road scenario but not for the highway scenario. Moreover, the traffic is considered in one direction only. The various assumptions that are made for the research work are detailed below in Table 1.6.

**Table 1.6: Research Assumptions**

| **Parameter Name** | **Value** |
|---|---|
| Type of Channel | Wireless |
| Type of Network Interface | Physical Wireless Network |
| MAC protocol | IEEE802.11p |
| Communication range | 300m |
| Map Area | 1000*1000sq.m |
| Interface queue type | FIFO queue |
| Queue length | 100 packets |
| Radio Propagation Model | Two ray Ground |
| Number of vehicles | 100-1000 |
| Number of road and junction segments | 50 |
| Speed of vehicle | 40 m/s |
| Simulation time | 1000 seconds |
| Map Layout | CityMap |
| Data Payload size | 120 bits/packet |
| Header Size of Packet | 36 bits |
| Traffic Type | Constant Bit Rate |
| Physical Link Bandwidth | 2 Mbps |
| Scenario | Random mobility |
| Number of RSUs | 3 |
| RSU Memory Size | 2080768 bytes |
| Broadcast Interval of RSU Beacon | 15 seconds |
| Segment Size | 100 m |
| Support Threshold | 2 %-14 % |

## 1.8 Major Contribution of the thesis

This research work contributes various data collection schemes and then integrating one of them with an efficient authentication mechanism to provide security.

### 1.8.1 Conceptual Foundation

- Various security solutions and attacks on VANET have been determined.
- Authentication method has been selected
- A threshold value is estimated and based on that a data collection scheme integrated with authentication mechanism have formulated.
- Associative rule based mining is applied for data mining.
- Support and Confidence are defined for generating the path maps.

### 1.8.2 Experimental Analysis

- Authentication scheme has been evaluated.
- Data Collection scheme has been validated after integrating authentication against existing data collection schemes.
- Associative rule based data mining has been validated to generate the frequent paths opted by the vehicles.
- Support and Confidence are evaluated to generate path maps for the vehicles under different scenarios.

## 1.9 Organization of the thesis

The Chapter 2 presents the basic concepts that are required to fetch the detailed knowledge about VANET. It describes the applications, security requirements, attacks, and types of attackers in VANET.

Chapter 3 describes the different authentication schemes that can be applied in VANET to provide security. Comparison on existing authentication schemes is made and on the basis of comparison carried out a novel scheme is devised for authentication that works on two way authentication.

In Chapter 4, a security analysis of discrete event based threat driven authentication approach is performed. Here the performance of the authentication scheme is evaluated.

Chapter 5 discusses data collection schemes, which details the working of each scheme using algorithms. A new dynamic data collection scheme is proposed which is even efficient from existing ones based on throughput, packet delivery ratio, and latency.

In Chapter 6, path maps are generated from a particular source to destination based on data collected and decisions made. Confidence and Support values are evaluated for paths and a final path map is generated under different situations.

Chapter 7 performs a comparative analysis of proposed scheme with existing solutions while authentication, data collection, and for generating path maps.

Chapter 8 concludes the research work by highlighting the essential steps that are taken in order to generate path maps under different situations and availability. Later, future aspects are mentioned that can be considered for further research in this field.

# CHAPTER 2
# BASIC CONCEPTS

This chapter builds the knowledge about the basic concepts that may be required to understand VANET. Basic working of VANET, its applications, VANET Architecture, Communication types, attacks possible on VANET and security requirements are described.

## 2.1 Introduction

The excitement of research community has notably increased in VANET during the last few decades. VANET belong to a special category of MANET used in promoting communication among (a) neighboring vehicles (b) vehicles and neighboring RSU. These days, VANET has procured ample consideration to associate security on transportation system. Security acts as major barricade in the complete VANET deployment. VANET reveal various specific features like high mobility, fast dynamic network topology, frequent dissection etc. Due to these specific characteristics, various solution and protocols suggested for MANET might not be relevant or instantly suitable for VANET. Therefore, VANET requires its peculiar solution [125]. Scholars and industry broadly accepted that VANET can notably increase traffic safety, road efficiency and decrease environmental force [126]. According to a survey done in the field of VANET 60% of the accidents on the road could be prevented if an alert was generated at least half second before the accident was hand over to the driver [127].

In this era of competitive technologies, vehicles moving on the road not only consist of hardware materials but are equipped with numerous software technologies [128]. Therefore, manufactures of vehicles basically work to blend both hardware and software capabilities in vehicles. Vehicles have features such as computation, communication, on board units, and GPS for positioning. Vehicles on road communicate among themselves or with entity on road side to share information for optimizing the traffic management scenario. This open communication may further impose various challenges on security of the network and the vehicles.

VANET is presented like a variation of MANET that has all the communicating nodes taken as the moving vehicles. VANET performs vehicle to existing infrastructure and vehicle to other vehicle kind of communication. Therefore, VANET can be used for numerous applications, and hence is eligible for number of challenges. Number of applications of ITS like traffic alerts, identifying routes dynamically are supported by vehicular ad hoc network [129]. In recent years, GPS receivers are already provided in most of the vehicles like BMW, Ford that are making efforts to add power resources in them. VANET architecture includes RSUs, On Board units (OBU), Application unit (AU) [130]. Each vehicle has an OBU installed on it along with some sensors to collect the information. RSU is used as a connection between vehicle and internet. Service provider offers AU, which is used to provide interface to the vehicles.

A communication standard, IEEE 802.11p is used for VANET to provide help for ITS. IEEE 802.11p standard enables wireless nodes to fulfill short term communication among fixed road side units and high moving vehicles that IEEE 802.11 does not provide, as it takes too long to associate and authenticate with the service provider [131]. The current mode of operation using IEEE802.11p is denoted as wireless access in vehicle environment (WAVE), and it supports Dedicated Short Range Communication (DSRC) standard [132]. DSRC works as a communication standard that has been assigned 75 MHZ spectrum in frequency ranging from 5.850 to 5.925 GHZ band operating for the safety applications in vehicular networks. Spectrum is categorized in seven 10MHZ channels as displayed in Figure 2.1. One of the channels is reserved for controlling, other four channels are deployed for services, and remaining two channels are fixed for future applications [133].

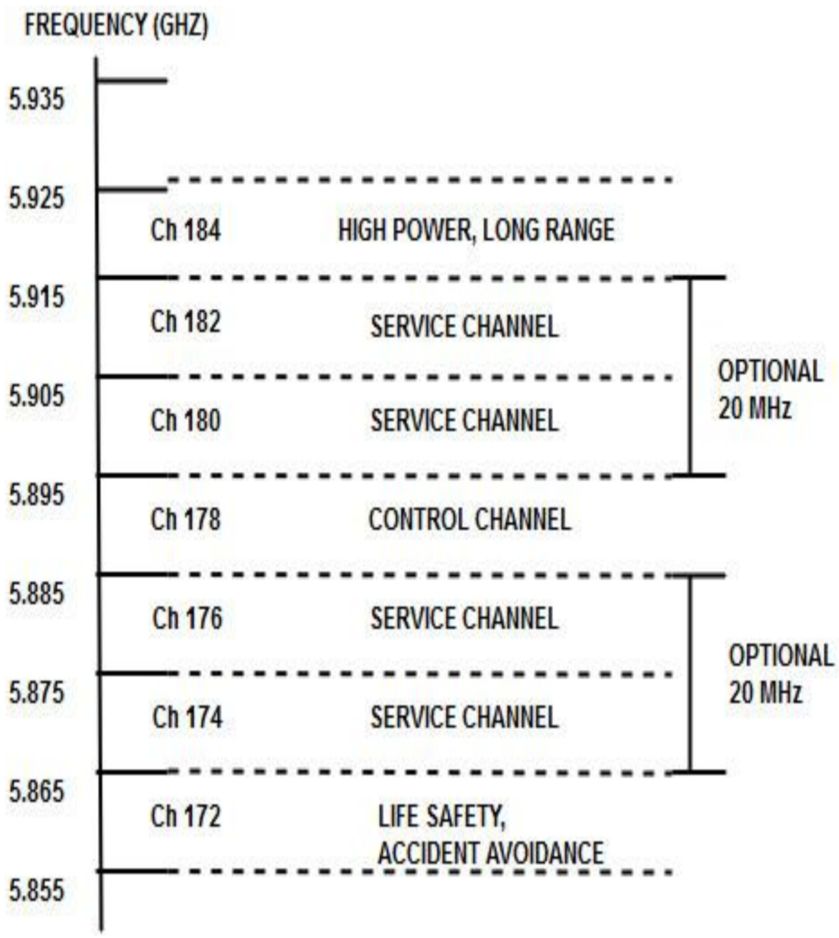


**Figure 2.1: VANET Spectrum [133]**

## 2.2 Applications of VANET

VANET can serve an ample series of services. According to a report of US Department of transport 75 various applications scenarios has already been indexed where VANET can be useful [134]. VANET offered application can be categorized in two distinguished categories: *Safety based and non-safety based applications.*

*Safety based applications* can also be referred as Intelligent Transport Applications (ITAs) .ITAs work as a integral unit of ITS and is one of the prime applicative area of VANET. ITA service includes collective traffic control, on board navigation, state of traffic jams while travel. The ideal schedule of traffic lights or to estimate the regulations of traffic flow by a centralized server, vehicle speed and frequency of traffic is continuously monitored by the RSU and this information is transferred to the server. This loop of feedback is highly appreciable in VANET as vehicles share the current road status among themselves. In event of accident the moving vehicles in VANET share the information with the RSU, which in response circulate this event to incoming vehicles on the same road segment and immediately inform the rescue team about accident. Multicasting or broadcast routing schemes are required by these kinds of applications for sending and getting the messages [135]-[136]. Safety based application are categorized into following:

a) **Dynamic traffic:** Vehicular nodes get the notification related to real time traffic that is stored at RSU whenever they require.

b) **Two way message exchange:** Vehicles exchange the messages among each other or with the RSU in their vicinity.

c) **Post accident warning:** Figure 2.2 shows after a accident has occurred vehicle can transmit a message containing the location to all the vehicles moving in its vicinity and can inform to highway patrol of rescue team for help [137].

d) **Road condition warning for control:** Vehicles moving on a road segment can inform other vehicles about the road characteristics like road curves, downhill or may be sudden rock slide.

e) **Collective accident warning:** An alert message is generated for all the vehicles to opt a different path way that are moving under crashed route [138].

f) **Traffic Monitors:** Continuous monitoring of traffic is performed by camera installation at the RSU that offers help when campaigning for less or even no acceptance of the driving offenses.

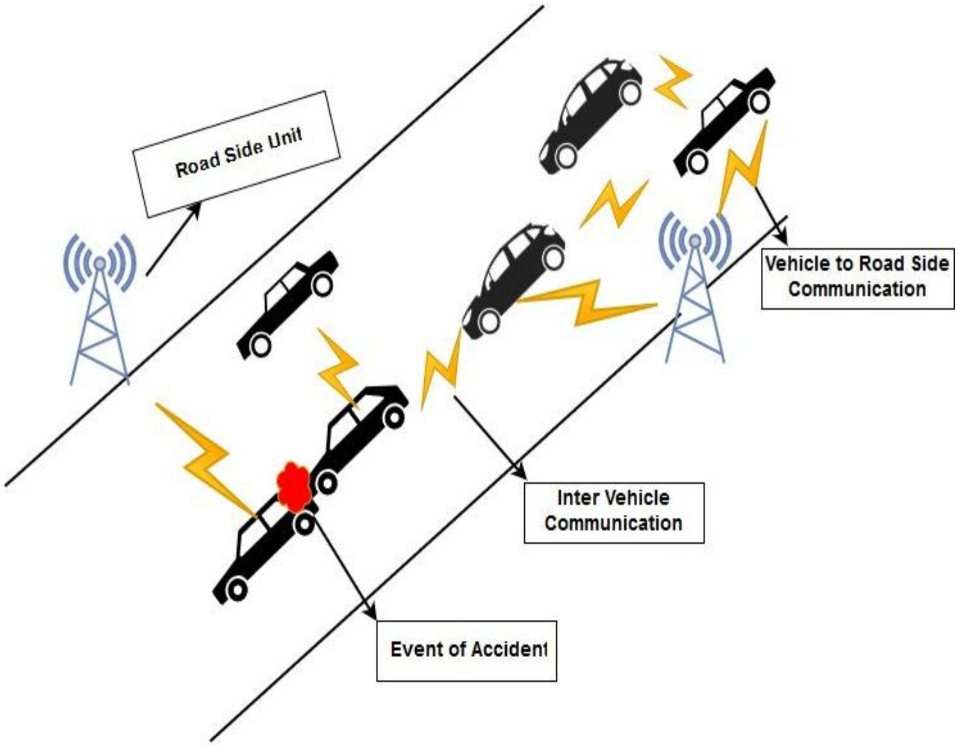


**Figure 2.2: Post Accident Warning**

*Non safety based applications* motive is to offer convenience to passengers or drivers by establishing communication with Internet service providers (ISPs) or among different moving vehicles. The services offered by such type of applications in VANET is to assure internet availability to all the vehicles moving on road so that they become able to download movies online, send emails, listen to music or can play games, do voice app based calls. With the existing network either static or dynamic networks are linked with the routers for message transmission among VANET and internet. Here, unicast routing mechanism is required to establish basic communication in the network [135]-[136]. Non safety based applications are categorized as:

a) **Internet Access:** If the RSU acts as router, vehicle may get access to internet using the services of RSU.
b) **Online Transfer of Video:** In the moving vehicle, driver may ask for online transfer of video related to his preferred list of movies.

c) **Path Alteration:** During traffic jam or rush hours, an alternate path planning can be conveniently done by the vehicles.
d) **Internet Browsing:** In case of traffic jam, the drivers can efficiently utilize their time by internet surfing, checking social sites, by using e-mails.
e) **Saving of Fuel:** Toll tax is collected from the moving vehicles without asking them to stop at the toll booth. This type of application avoids the waiting time of the vehicles during the manual toll collection and also helps in saving minimum 3% of the fuel.

The safety based applications are mainly dynamic in nature that requires a guaranteed quality of service in terms of communication overhead, security and latency. With a few seconds of time span a safety message should be floated to the appropriate vehicles in order to avoid the mishap on road. Based on this drivers can take the subsequent measures to not let this mishap to happen. For the effective implementation of the above scenario, security should be on the top priority. Security features helps in offering a method that assures that data was generated from a legitimate source (either RSU or vehicle) and that data is not modified or updated. On the other side, non safety based applications need to ensure secure transactions in applications like monetary transactions (toll collection at booth).

## 2.3 VANET Architecture

The Figure 2.3 shows architecture representing VANET [139]. The messages transmission is regulated among a RSU and a vehicle or among vehicles over WAVE. This communication mechanism works on transferring a plenty data options to users and drivers. Moreover, safety based applications are facilitated to offer a convenient driving and road security. The primary VANET apparatus are the OBU, AU, and RSU.

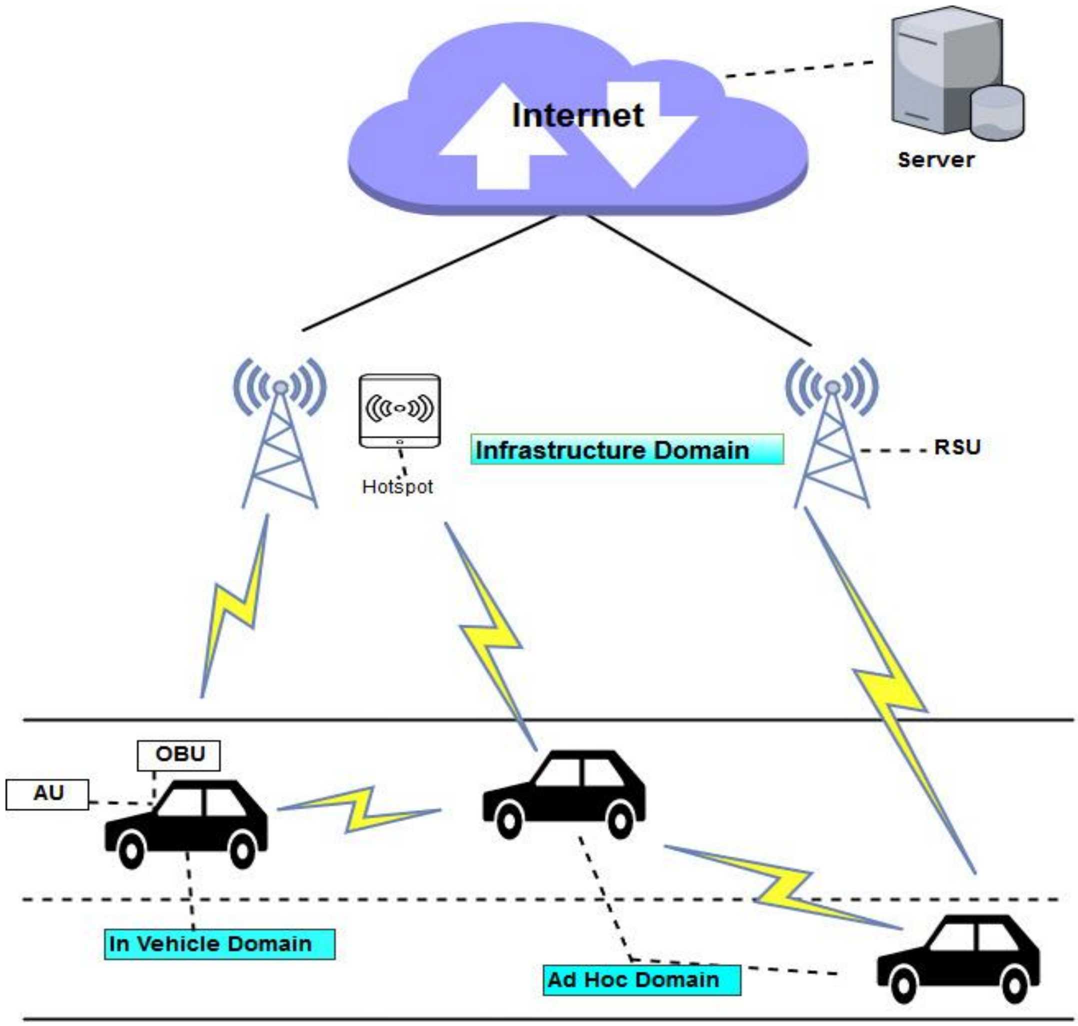


**Figure 2.3: VANET Architecture [139]**

### a) On Board Unit (OBU)

For data maintenance and recovery, OBU's resource command processor (RCP) that contains memory having read/write operations. To connect with other OBUs, a special interface referred as user interface is offered in OBU. It also carries a network based tool for DSRC that is dependent on IEEE 802.11p technology. For executing no safety based applications, OBU comprises one more device that considers radio technology like IEEE 802.11a/b/g/n. The primary role of OBU is for ad hoc and geological routing, jamming control, trustworthy message transmit, wireless radio access and information protection [139]-[140].

**b) Application Unit (AU)**

OBU's communication capabilities are utilized by the AU to take care of applications by mounting it inside the vehicles. Examples of AU can be any device that is trustworthy for implementing safety applications like routing or warnings of accidents having the capability of sending and receiving the messages, or a AU can be any regular device to carry out internet applications like internet. AU can either be fixed as a integral part of OBU or can be rooted in the vehicle. Dissimilarity among OBU and AU is reasonable only. AU establishes the communication with network exclusively through means of OBU that makes the accountability for all the mobility and functions associated with networking [139]-[140].

**c) Road Side Unit (RSU)**

It is a substantial piece of equipment positioned generally by the side of the road or at keen locations such as petrol pumps, hospitals and hotels. Radio technology like IEEE 802.11p decides whether to offer a short dedicated range of communication using RSU that outfits a specific device in network. To ensure communication available in infrastructural network, different network operated devices can be integrated with the RSUs [141]-[144].

Three distinguished domains are required for operation in VANET [145] as shown in Figure 2.3 above:

i. **In-vehicle Domain:** It consists of OBU and AU that is connected either through wireless or wired connection. OBU can communicate with internet by choosing one of the applications from AU.
ii. **Ad-Hoc Domain:** This domain works for V2V communication. It gives efficient way for communication among the moving vehicles.
iii. **Infrastructure Domain:** In this domain V2I communication is possible. Therefore, vehicle can pass the information to the RSU in its range.

The primary operations and measures concerned with the RSUs are:

a) Figure 2.4 shows the transfer of information to an available OBU as soon as OBU comes within the range of communication of RSU[139].

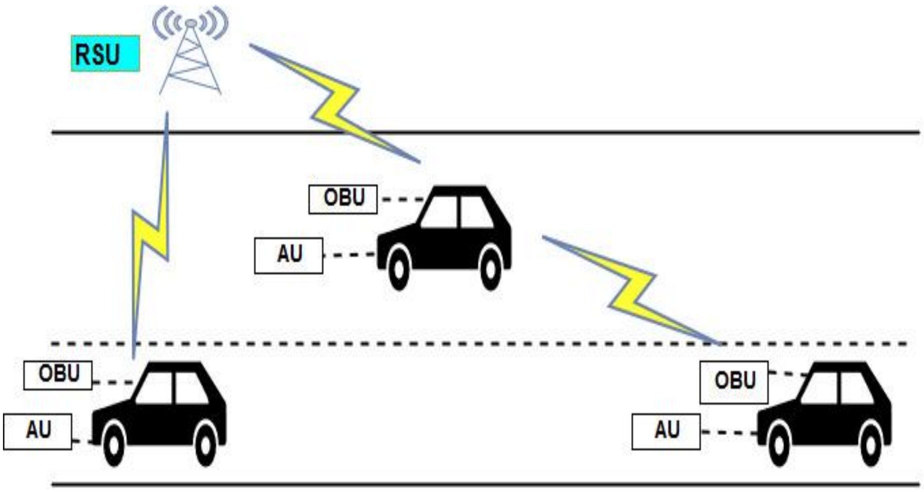


**Figure 2.4: Communication between OBUs and RSU**

b) Figure 2.5 shows to run the safety based applications like combined warning related to accident, post accident warning, control road risk warning (such as road curves, downhill etc) and to act as an reliable information source [139].

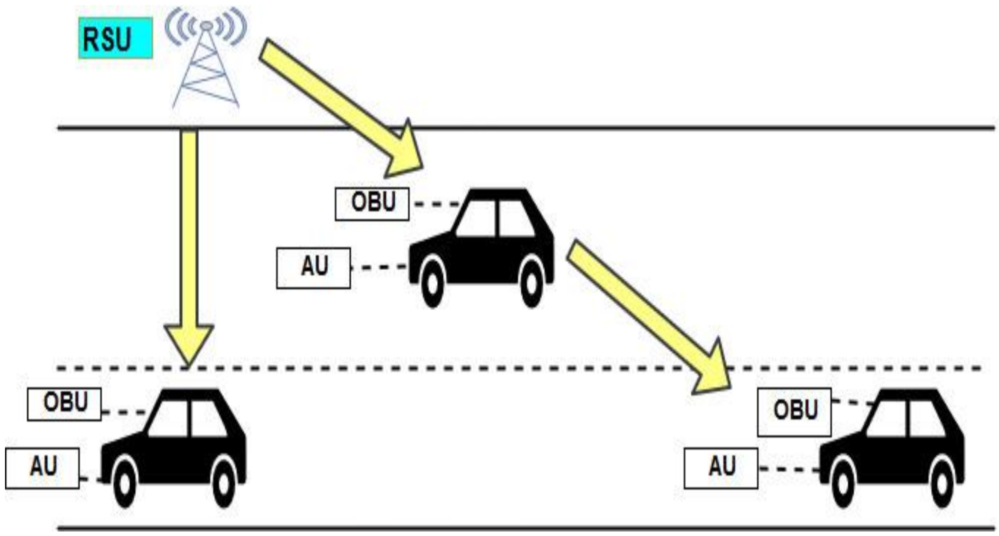


**Figure 2.5: RSU as an Information Source**

c) Figure 2.6 shows the provision of internet connectivity to OBUs [139].

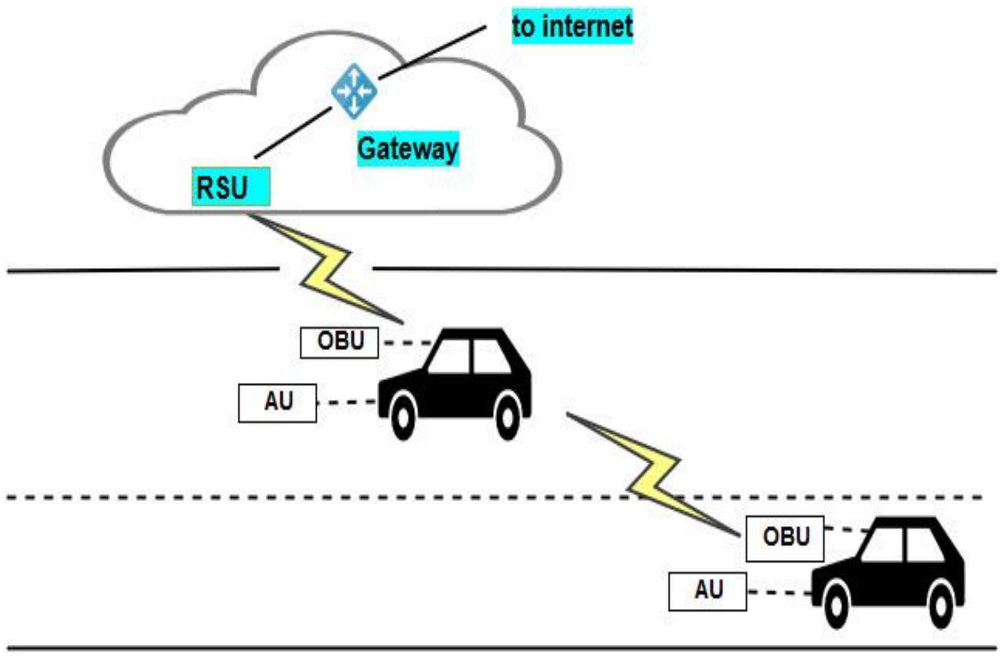


**Figure 2.6: Internet Access to Vehicles Provided by RSU.**

## 2.4 VANET Communication Types

The various types of communication in VANET and are as follow [146]:

**a) Intra- Vehicle Communication**

This type of communication includes a communication medium is provided to the AU by the OBU in order to implement to various collection of applications offered by service provider utilizing communication abilities of OBU [139]-[140],[147].

**b) Vehicle to Vehicle Communication (V2V)**

In this kind of communication incorporates vehicle which communicate with other vehicle directly if there is a specifically if there is an immediate remote connection between them, establishing a distinct bound vehicle V2V communication. But when no direct link is available among the vehicles then a devoted routing protocol can be utilized to forward the messages among the vehicles so that it reaches the target point, establishing a multi bound V2V communication [148].

**c) Vehicle to Infrastructure Communication (V2I)**

In this type of communication in order to amplify the communication range of vehicles and to take the advantages from the RSUs which are able to process the special application, vehicle establish communications with the RSUs forming V2I communication [149].

**d) Vehicle to Broadband cloud communication**

RSU can connect to the infrastructure or internet service provider that allows the OBU mounted on the vehicle to access the internet or infrastructure network [139]-[140],[147],[148].

## 2.5 Characteristics of VANET

The Characteristics corresponding to VANET differentiate them from other used networks that are ad hoc in working. The exclusive characteristics belonging to VANET that make them stand apart from other usual networks are as follow:

- **Frequent network topology changes:** With the high speed vehicles moving on the road, the VANET topology becomes very dynamic. The information is given by the system to the driver and conduct of driver is dependent on this received information leading to the frequent changes in topology of the network [149]-[151].
- **Ample power:** There are no constraints related to power in VANET, as using the battery with long life a constant power is offered to OBU by the vehicles [149]-[151].
- **Varying network density:** Network density in VANET is dynamic as it is dependent on the varying traffic density of the vehicles on the road. For example, in sub urban areas traffic density is low , whereas in event of traffic jam or accident traffic density is very high [149],[152].
- **Multiple scenarios of communication:** City traffic scenario and highway traffic scenarios are the two broad communication scenarios for VANET. In city scenario the environment is relatively complex and confusing as compared to highway traffic.

- **Prediction of mobility:** In VANET vehicles move in an arbitrary fashion as they are dependent on road topology. However, vehicles have to communicate with moving vehicles, follow the traffic signals, and look for the road signs forming a certainty related to their mobility[150],[152]-[154].
- **Wide range network:** The size of network scenario is very large mostly in case of city centre, urban areas that are crowded like highways, and while entering a huge city [149],[151].

## 2.6 Requirements and Attacks related to security and privacy faced by VANET

### 2.6.1 Security Requirements

VANET applications are diverse, their communication and /or necessities and concerns of privacy and security in VANET could be diverse too. Due to unique characteristics of VANET, like frequent change in network topology, high speeds of vehicles in the network, dynamic network density, extremely large amount of entities in the network, requirements and issues concerned with privacy and security are very challenging in VANET. A secure VANET system is competent of creating the accountability of drivers, at the same time preserving their privacy as much as needed. In view of above mentioned attacks, the subsequent requirement should be satisfied by the VANET security:

**a)** **Authentication:** The mandatory requirement that enhance the trust of society in VANET is authentication. Both, authentication of message among vehicles and nodes or vehicles authentication are significant requirements. Authentication of vehicle ensures that the message is originated from only the legitimate vehicle and it is not an infected or malicious one. If authenticity is not performed than there is a possibility of sybil attack in the network where the malicious vehicle is carrying multiple identities at same time. On the other hand, replay attack is possible if the messages related to safety are compromised. For preventing such type of attack, a timestamp on authenticated message should be included.

b) **Affirmation of data reliability:** There can be possibilities that sender can be legal but the messages generated by the sender include forged information. This type of requirements is known as "validity".

c) **Non Repudiation:** the life of a legal user can be spoiled by the illegal activity of an Illegal user. When an illegitimate user refuse to commit the ownership of sent messages or message content, it is referred as sender's non repudiation. On the other side, a receiver may refuse to accept the message; it is referred as receiver's non repudiation. In VANET, these kind of infected nodes can be identified using non-refutation.

d) **Message Integrity:** Integrity excludes the deletion, modification, replay or insertion of information to make sure that the information that is received at the destination is primarily same as originated by the authorized sender. Any data manipulation in a unauthorized way must be identified to preserve integrity.

e) **Availability:** Safety and non safety based applications are offered in VANET. In order to use these applications and for information exchange between two communicating entities, network availability must be ensured at every instant of time. The network availability to a genuine node can be reduced by an attacker by channel jamming, exhausting the power back of battery, disturbing protocol for routing etc.

f) **Confidentiality:** Information protection for being disclosed in unauthorized manner is confidentiality. Malicious node that is not allowed to fetch the information, confidentiality ensures non disclosure of information to these nodes. Therefore, for receiving the authorization to access the VANET information authentication is must.

g) **Accuracy of Location:** An attacker disseminates fake information related to its current location for misguiding the authentic nodes that are part of the network. Therefore, it becomes difficult to spot whether the vehicle sending this information is at a stated location or is at the correct place. Hence, acquiring the exact vehicle location becomes extremely challenging in VANET.

### 2.6.2 Attackers in VANET

The extent of the protection required to provide security in VANET can be easily determined by identifying the type and resources of the attackers. To organize the details of all possible attackers in any effective security system is really a very difficult task. The practical study of the application surroundings can assist in determining the types of distinctive attackers. The subsequent categories of attackers are recommended by the VANET [53],[154] as shown in Figure 2.7

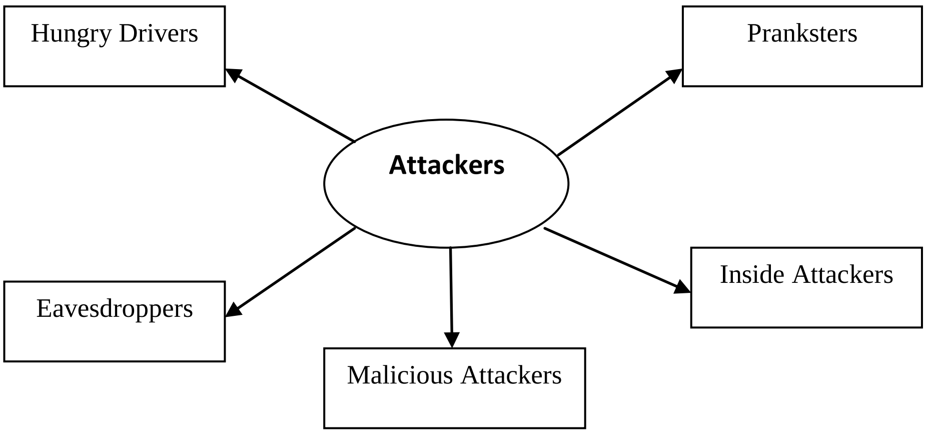


**Figure 2.7: Type of Attackers**

- **Hungry drivers:** All the drivers in VANET are not pursuing the rules decided by the application. Few drivers in the system always attempt to exploit the services provided by VANET, in spite of the cost to the system.
- **Eavesdroppers:** Such types of attackers can be anyone from an interested regulatory agency to a nearby neighbor annoying to contour drivers.
- **Pranksters:** Pranksters are the severe enemy in VANETs similar to computer and network security. Pranksters consist of exhausted youngsters probing for susceptibility and hackers searching for reputation through their exploits. Consider an example of prankster situated at roadside may simply generate “smart collision” through influencing one of the vehicles to speed up while convincing vehicle in front of it to slow down.
- **Inside attackers:** Such types of attackers are very illusory and it is extremely hard to preserve them. Scope to which VANETs are susceptible to these types of attackers relies on the choice of security design proposed by others.

- **Malicious attackers:** These types of attacker try to cause damage from the availability of VANET applications on the system. Typically, these attackers contains precise targets, while they have right to use more resources as compared to above mentioned attackers. For example, terrorists create a traffic jam few minutes before detonating a bomb by manipulating warning system.

### 2.6.3 Attacks in VANET

VANET are vulnerable to numerous types of attacks. With full power backup and expertise of an OBU containing dozens of microprocessors, are equipped in the vehicles, which lead to significant capacity of computing and processing. Due to this significant capacity of computing and processing, nodes in VANET have significant benefits as compared to regular ad hoc networks [155]. Therefore, lot of attacks possible in ad hoc network are not applicable in VANETs and reverse is also true [156]-[165]. The attacks in VANET can be classified as shown in Figure 2.8.

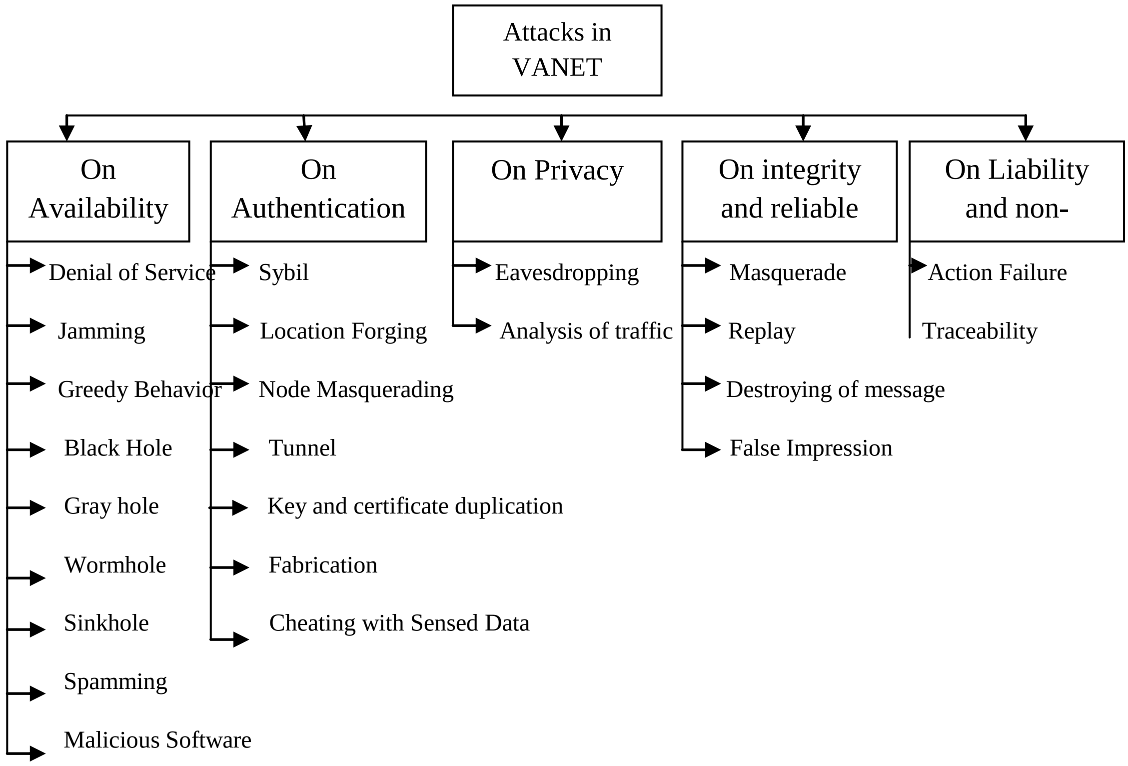


**Figure 2.8 Classifications of Attacks in VANET**

#### *2.6.3.1 Attacks on Availability*

This security feature is a vital part of VANETs. This gives assurance about the network efficiency by offering access to its valuable information at any moment. For most of the adversaries availability is a key target to compromise the network's performance. The attacks on availability are categorized as follow:

a) **Denial of service attacks (DoS):** DoS attacks in fact consist of a group of attacks focusing the availability of services provide by the network, which can have severe impact particularly for VANETs applications. Due to their impact DOS is considered as a dicey group of attacks. DOS may be implemented through the external or internal malicious nodes of the network [157] . Here, primary mode of communication is blocked by the attacker in order to interrupt the network services, due to which network services may not be accessible to the legal vehicles [166]. For example, overflowing the communication link by generating high volumes of messages through deliberately manufacturing. Due to which vehicles (RSU and OBU) may not be accepting the large quantity of acknowledged data.

b) **Jamming attack:** The physical level of DOS attack is known as jamming attack. Is defined as intentional transmission of messages to disturb the communication medium [167]. For an effective attack, the attacker must respond at same instant when the action of transmitting and receiving of useful signal occurs to create a jam.

c) **Greedy behavior attack:** As per the OSI reference model this attack on the MAC layer's performance is termed as greedy attack. The nodes compromised under this attack do not follow the protocol for channel access and they always try connecting to the communication medium by prohibiting non compromised nodes to continue using services and support. To access the communication channels in a quicker manner, a greedy node always work on reducing its time of waiting as compared to other non compromised nodes [168]-[169].

d) **Black hole attack:** For implementing this attack, faulty nodes receive packets containing data from the network and then deny taking part under the process of routing. This attack prevents the arrival of useful information to addressee mainly by disturbing the routing tables. In this attack faulty nodes always announces that they are part of network and are playing a part that is not the actual case [170]. The consequence of black hole attack is more hazardous for VANETs as compared to other ad hoc networks. A black hole attack can forward the data packets to a particular node that doesn't exist and thus leading to loss of data.

e) **Gray hole attack:** The main focus of this type attack is on the data packets of definite applications are removed that are susceptible to packets loss [171]. This attack is a variant of black hole attack.

f) **Wormhole attack:** This is a form of DOS attack which wants the involvement of minimum two nodes. In this attack an adversary A transmits a message to other attacker B which is physically at a distance from A. Attacker B broadcasts this entire message send by A to its neighboring nodes. This message advises the nodes in neighborhood of B, that A is their neighbor [172]. This type of attack permits switching over data packets between two or even more valid nodes and the non-neighbors nodes, ultimately creating imaginary roads.

g) **Sinkhole attack:** In this attack, faulty vehicles attracts nearby legitimate vehicles to transmit their packets to go through it, which helps in eliminating or changing the acknowledged packets and then retransmitting them finally. This attack is used to build up other attacks as either black hole attack or gray hole. [173].

h) **Spamming attack:** Main motive related to this attack is to put away bandwidth and create intended collisions.

i) **Malicious software attack:** In VANET system, OBU and RSU in vehicles are equipped with software components which can penetrate the faulty software in the network during the software update of VANET units. The injected virus by faulty software leads to disturbance in the regular VANET system functionality.

j) **Broadcast manipulate attack:** The adversary in this particular attack generate bogus aware message in the network which may cover up right safety messages to genuine users. This attack critically has an effect on the whole network security and also results in accidents.

#### *2.6.3.2 Attacks on authentication and secrecy*

Authentication plays a very important task in VANET security. In order to access available services all the nodes must authenticate themselves before entering in the VANET system. The entire network is compromised to very severe penalties if there is any attack which engages the authentication process. To protect the genuine nodes from the adversaries which are penetrating the VANET system by using incorrect identity, one must ensure the authenticity in VANET. The significance of authentication and secrecy process is realized every time a different vehicle requests to connect to the network and wants to make use of any type of service this network offers. The various types of attacks come under this category are as follow:

a) **Sybil attack:** The individual can behave as multiple entities at the same time in this attack which was first described and formalized in [174]. Vehicles duplicate the identities of multiple vehicles in this type of attack. These duplicate entities used to penetrate any category of attack in VANET system. The illusion that there may be increased vehicles moving on the road is created by these bogus entities [175]-[176].

b) **Location forging attack:** In VANET data related to location is significantly important , it must be authentic and highly accurate. In this attack fault node provides incorrect location information to the neighboring nodes. A position system (receiver) is mounted on each vehicle, which may receive signal generated by the means of a transmitter. This transmitter has ability to generate the localization signal even stronger than real satellites signals and thus this attack can be achieved [177].

c) **Node masquerade attack:** In VANET every vehicle is equipped with the network ID that distinguishes it from other vehicles of the VANET [170]. In this attack adversary obtain the valid network ID of some vehicle and pretend to be another vehicle. This comprises an infringement of authentication procedure in VANET.

d) **Tunnel attack:** To establish a confidential connection (tunnel), adversary uses the same network in this attack. This attack establishes the communication medium like tunnel between the two distinct network portions. Therefore, the fatalities of two far-away portions in network behave like neighbors and can be in touch [177].

e) **Key and certificate duplication attack:** This attack is used to create uncertainty by utilizing the duplicate keys and certificates as a recognition proof due to which it is very difficult for the authority to recognize a vehicle in case of clash.

f) **Fabrication attack:** This type of attack is deployed in VANET by broadcasting fake information in the network by the adversary. For example, a vehicle under this attack requiring speeding up his journey can behave as an emergency vehicle.

g) **Cheating with Sensed data:** In this attack adversary modify its supposed positions, speed, directions etc in order to get away legal responsibility, primarily in case of an accident.

#### *2.6.3.3 Attacks on Privacy and Confidentiality*

Privacy and confidentiality are the essential security prerequisites in VANET system. Privacy ensures that only validated users are capable of reading the data. If the privacy is absent, data exchanged among the nodes in VANET is more vulnerable to attacks such as offensive compilation of comprehensive data. In these attacks, the adversary can collect data based on the position of the vehicles, its path, data on nodes confidentiality, etc. In these attacks victim is not aware of the collection of sensitive data by the adversary using offensive means. However, if the exchanged data does not enclose any susceptible information than privacy is not essential [53]. The various types of attacks come under this category are:

a) **Eavesdropping attack:** In this attack, victim is not aware of the collection of sensitive data. This type of attack is easy to incorporate as it involves listening to media against the privacy of the vehicles. With the help of this attack, various valuable information collections can be done, like position of vehicles which can be further utilized for vehicle tracking.

b) **Attack on analysis of traffic:** The nature of this attack is a severe risk to the privacy and confidentiality of the users. Here, collected information is analyzed by the adversary by periodically listening to the network after a fixed segment and hence to mine the most useful information out of it.

#### *2.6.3.4 Attacks on integrity and reliable data*

Integrity prevents alteration of data exchanged in a system. Integrity aims to guarantee the protection of data from alteration or deletion. In these attacks, adversary primarily target V2V communication in comparison of V2I due to their vulnerability. The promising method to assist such types of attacks is the exploitation of sensors in vehicles [178]. The attacks under this category are as follow:

a) **Masquerade attack:** The adversary in this attack is concealed with the help of legitimate identity and generates faulty messages that have manifestation of approaching from a genuine node.

b) **Replay attack:** This attack involves the repeated broadcast of messages that is already sent to take the advantage of the messages at the time of their submissions. In this attack beacons are replayed to manipulate the positions and routing table of vehicle [179].

c) **Destroying/Obstruction/Forging/Modification of Messages:** This attack is against the reliability as it involves the process of destroying, forging and modifying the existing data. This attack can be injected by altering a definite message section that needs to be sent. For example, attacker inject a fake information in the received data representing a traffic jam and convert them to mislead users, indicating that no such traffic jam is there and road condition is ok.

d) **False impression attack:** This attack is an application of message forging attack. It involves the setting of willing sensors which produce forged data [180]. In this attack, adversary connect to the network in a genuine way due to which such types of attack are not detected by authentication mechanism.

Masquerade, replay, destroying/forging/obstruction/modification of messages, false impression attack can also be considered as attacks against privacy and confidentiality.

### *2.6.3.5 Attacks on Liability and non-repudiation*

To validate the authenticity that sender and receiver are the ones which are claiming to have transmitted or received the messages respectively is defined as non-repudiation. In context of VANET, origin of data non-repudiation confirms that data has been transmitted. Arrival of non-repudiation confirms in reverse that data has been delivered. The attacks in this type of category are as follow:

a) **Failure of actions traceability:** This attack involves taking action, consequently permitting adversary to refute to complete multiple actions. Such type of attack works on erasing the traces of actions and generating uncertainty in inspection unit. Sybil attack, key and certificate duplication attack can act as basis of non-repudiation attack.

## 2.7 Summary

VANETs are fetching recognition in ITS. It is expected that VANET will be installed in various countries within a short time for communication. Therefore, the basics of VANET are described in this chapter stating its applications, architecture and various characteristics. As multiple vehicle join and leave VANET, it becomes susceptible to various types of attacks. To provide security and privacy to such types of networks is very important for the reason that people's lives may be at risk due to it. Therefore, so far a detailed discussion is made on attackers and attacks existing in VANET. In next chapter a novel identity based scheme is proposed for two way authentication.

# CHAPTER 3

# A NOVEL IDENTITY BASED TWO WAY AUTHENTICATION SCHEME IN VANET

In this chapter the different authentication processes used in VANET are discussed. Later, a comprehensive identity based scheme is proposed to prevent attacks on the vehicles or their data which allows only legitimate users to communicate for the purpose of data collection. Performance analysis of proposed authentication scheme is made by comparing it with existing authentication schemes considering computational overhead, packet delivery ratio, and latency as the comparison parameters.

## 3.1 Introduction

To boost the trust of users in VANET, the initial requirement is to incorporate authentication service in the VANET. Authentication can be offered in different ways like message authentication and second is authentication of vehicles when vehicles communicate. Once the node is authenticated, it is assured that messages are originated from the legitimate node and not through a malicious one. Without authentication, there may be a scope of Sybil attack that at one time malicious node can present multiple identities. The compromise of safety associated messages may lead to the replay attack. To prevent replay attack, every message should carry an authenticated timestamp.

## 3.2 Authentication Process in VANET

Different schemes for authentication exist in literature. It is assumed that there are maximum three communication parties involved in VANET scenario: Service provider (SP), Access Point (AP), and the vehicle. SP helps the AP to access the internet services. AP is the fixed device along the road sides that is used to establish connection among the vehicles in its vicinity. The authentication scheme should be such that the computational overhead should be less. Authentication process can be further improvised by making it two-way. One from vehicle to AP and then AP also authenticate itself to the vehicle. The general process of authentication is given in Figure 3.1

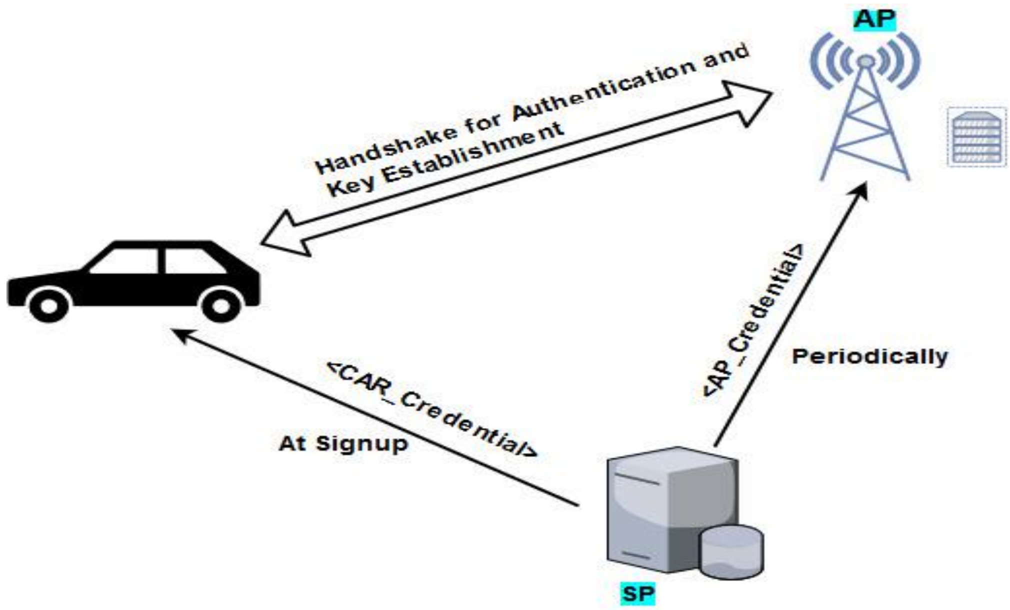


**Figure 3.1: Process of Authentication in VANET**

Various processes for providing authentication in VANET are:

### 3.2.1 Digital Certificates Authentication (DCA)

Digital certificates are used for authenticating vehicle to the AP. Here the SP provides the set of private and public keys and corresponding digital certificate to each vehicle as well as AP for each slot of time. The steps for the digital certificate process of authentication are as follows and are also shown in Figure 3.2.

**Step 1:** The SP allocates set of private and public keys and digital certificates to AP and vehicle during start up.

**Step 2:** Vehicle/car initiates the authentication process with the nearest AP by sending a message having its public key $<PK_{CAR}>$ along with certificate $<Cert_{CAR}>$.

**Step 3:** AP authenticates the user and sends a message incorporating AP's public key $<PK_{AP}>$ and digital certificate $<Cert_{AP}>$ to let it to be authenticate by the vehicle. AP also sends a nonce (n1) and private key to vehicle by encrypting entire message by public key of vehicle, so that it can only be opened by the temporary private key of vehicle.

**Step 4:** Vehicle in return sends nonce (n1) back for confirmation, new nonce (n2), all encrypted using the temporary key that is private and is communicated earlier. Therefore, message can only be decrypted by the AP as it pertain access to same temporary key.

Disadvantage of digital certificates is, if once the vehicle's private key is compromised then the authentication process becomes vulnerable to masquerading attack.

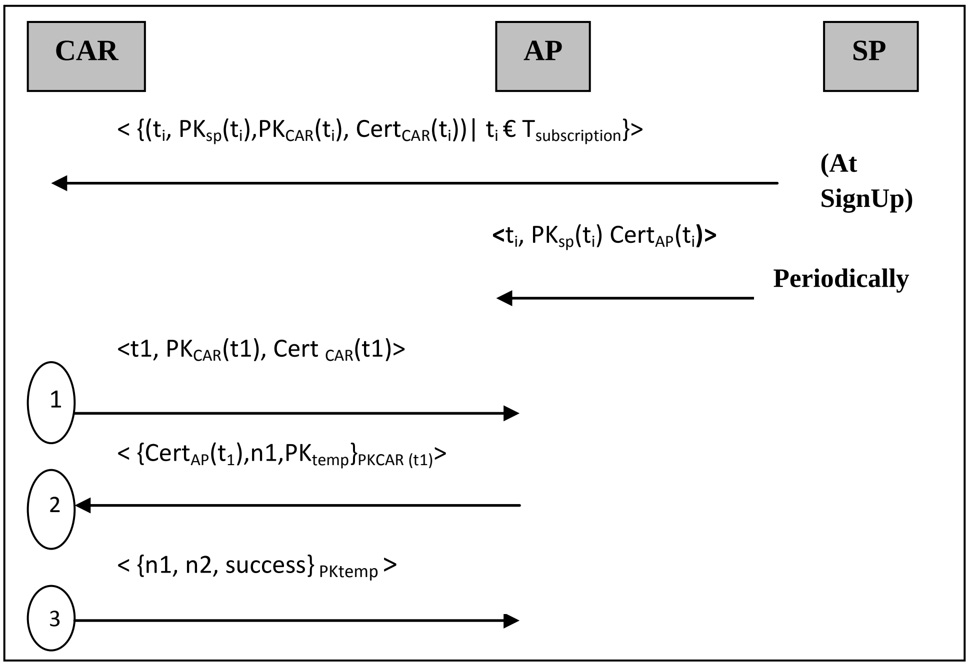


**Figure 3.2: DCA Process for Authentication**

### 3.2.2 Pairing

In this process SP issues some random secret communicating pairs to AP and vehicle based on the time stamps. The steps for the pairing process of authentication are as follows and are also shown in Figure 3.3

**Step 1:** At the time of sign up when vehicle enters the network, a set of random secret points for calculating keys is assigned to vehicle $<PN_{CAR}(t1)>$. The same set of secret points is also allotted to the AP $< PN_{AP}(t1) >$.

**Step 2:** Vehicle/car initiates the authentication process and send the secret point for that particular time to the AP. AP verifies the message for valid time stamp.

**Step 3:** AP now generates a secret key using the secret point of vehicle and secret point of itself for that particular time.

**Step 4:** AP then sends its secret point to the vehicle, so that the vehicle can also generate the secret key using same combination.

**Step 5:** At last the vehicle sends a nonce to AP encrypting it with the secret key generated, so that AP can decrypt it using the same secret key.

The disadvantage of pairing is that the secret point of AP can be used by a malicious node and it can generate a secret key and start communication with the AP.

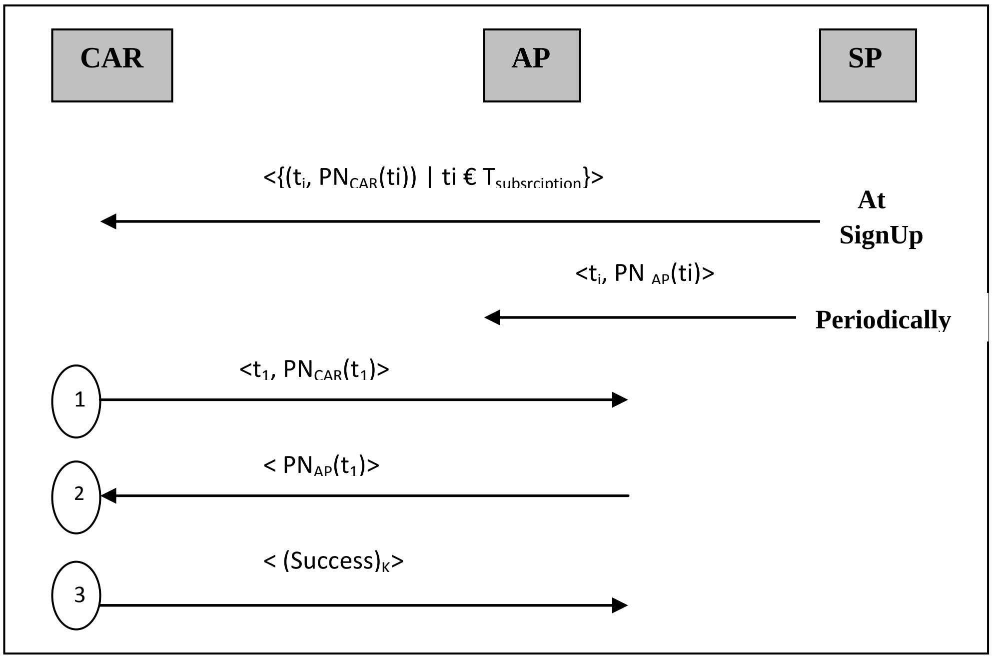


**Figure 3.3: Pairing Process for Authentication**

### 3.2.3 Intermediary Re-encryption (IRE)

The intermediary mechanism for authentication uses the concept of re-encryption. Each vehicle and AP has set of private and public keys along with the re-encrypt keys for each time slot. The general fundamental is that combination of public key of SP and re-encrypt key that belongs to the vehicle, gives public key of vehicle that can only be opened by the private key of vehicle. Similarly combination of public key of SP and re-encrypt key of AP gives public key of AP that can only be opened by the private key of AP. The steps for the IRE process of authentication are as follows and are also shown in Figure 3.4.

**Step 1:** During the sign up time, SP assigns AP and each vehicle with private keys, public keys and re-encrypt keys for the intermediary encryption.

**Step 2:** Keys are allotted for each time slot to AP as well as the vehicle.

**Step 3:** Vehicle initiates the authentication process with AP by sending a message at time t1, having nonce (n1) encrypted by the public key of SP *<PKSP>*.

**Step 4:** AP again encrypts the message with the re-encrypt key for that particular time t1. So the intermediary result is now a message that gets encrypted using public key issued to AP that can be decrypted using private key of same AP only.

**Step 5:** Now, AP sends nonce n1, new nonce n2 encrypted by public of SP. Vehicle again encrypts the message with the re-encrypt key $<ReKey_{CAR}>$and the result is the public key of vehicle that is decrypted using vehicle's private key only.

**Step 6:** At last, vehicle and AP can start communicating with each other using some secure encryption algorithm.

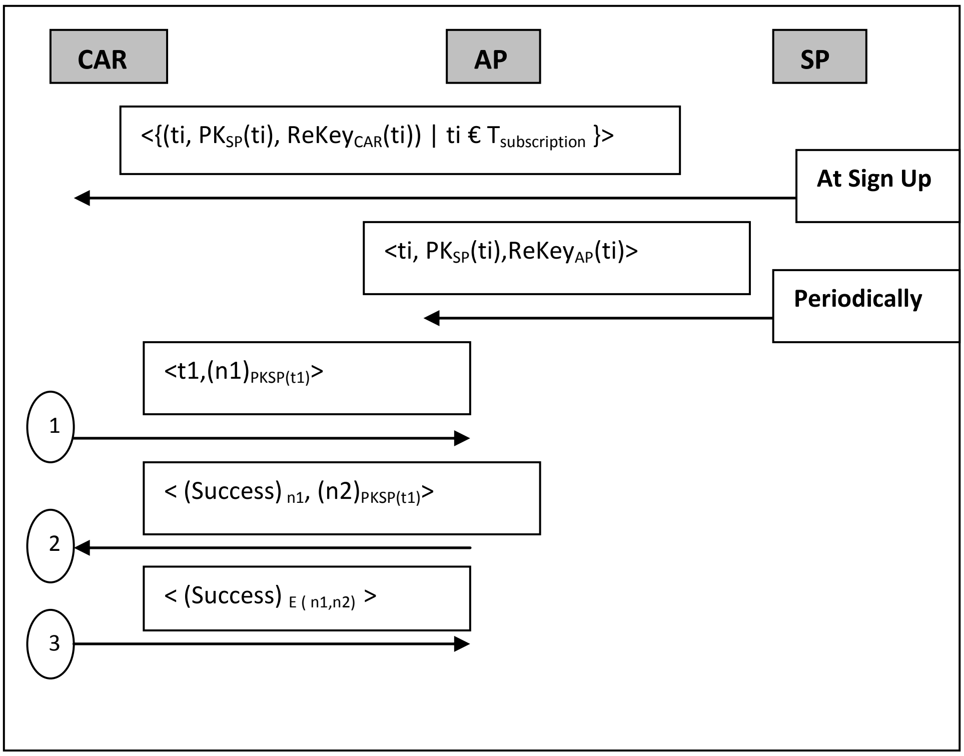


**Figure 3.4: IRE Process for Authentication**

## 3.3 Comparison of Existing Authentication Processes

Comparison is made among all the existing processes of authentication as given in Table 3.1 on the basis of encryption mechanism, number of messages required for communication, and point of attack.

**Table 3.1: Comparison of Various Authentication Processes in VANET**

| | **Encryption Mechanism** | **Number of Messages** | **Attack point** |
|---|---|---|---|
| **DCA** [56] | Asymmetric key | Number of messages required for authentication are large | Public key of vehicle is compromised |
| **Pairing** [56] | Symmetric key | Do not require extra messages. | Secret key is compromised |
| **IRE** [55] | Re-Encryption | At initial set up message required are more for key sharing. | Re-encryption key is compromised. |

The first step to assure security in network is authentication. Out of numerous processes discussed above for authentication IRE provides two-way authentication from AP to vehicle and vice versa. But still IRE is vulnerable to different types of attacks like:

a) **Masquerading attack:** The attacker can obtain the certificate and public key of the vehicle and imitate false identity. After that all the communication between the attacker and AP continues as if they are going among legitimate vehicle and AP. The masquerading attack detains the legitimate vehicle to access the services of the SP.

b) **DoS attack:** The attacker vehicles send frequent requests to the AP for authentication. This increases the number of requests that AP can handle. So as a result either AP can crash or its services are denied to the legitimate users.

c) **Eavesdropping:** The attacker can continuously hear the communication that SP is performing. As a result it can get the information on the air that is passed to vehicles by the SP.

d) **Man-in-middle attack:** This attack makes IRE insecure as explained below:

**Step 1:** On sign up vehicle and AP receives re keys from SP, if any attacker gets these re encrypt keys as man in middle, then it can inject attack in network.

**Step 2:** Car sends a message having nonce at time $t_1$ encrypted using SP's public key, attacker as middle man decrypts the message using re keys of AP.

**Step 3:** In this attack the actual communication between AP and vehicle as in IRE is interrupted and communication between vehicle and attacker initiates. As a result attacker can get all the information from the vehicle.

## 3.4 Proposed Scheme for Authentication

A new scheme is proposed to provide authentication in better way. This scheme includes the properties of IRE and works on overcoming the above stated attack. In this algorithm the concept of asymmetric encryption along with the re-encrypt key is used. This further enhances the security in authentication process.

### 3.4.1 Methodology

The proposed scheme uses asymmetric encryption for offering authentication among V2I and inter-RSUs. The scheme works well for the authentication of vehicle on RSU, that is, vehicle confirms its identity to RSU. A reciprocal security mechanism is required at the RSU to prove its authorization to the vehicle. For later communication, a secret session key is shared between RSU and vehicle during the authentication. To allow countermeasures for location confidentiality, session key should be shared in such a way it coordinates all the updates at vehicles and RSU. On the same grounds, handoff is performed among multiple RSU and authentication is required among inter-RSU. For the proposed scheme, authentication is needed one time between inter RSUs and V2I. The steps taken to carry out authentication are as follows and are shown in Figure 3.5.

**Step 1:** During the start up time, SP provides public, private and re-encrypt keys to AP and the vehicle for different time slots.

**Step 2:** Vehicle authenticate itself to the AP by sending the message containing the random nonce n1 along with public key of SP <$PK_{SP}$>, and secret key of vehicle <$PrK_{CA}$> encrypted with public key of AP. AP decrypts the message by applying its private key.

**Step 3:** Then**,** AP encrypts the message containing random nonce n1 and new nonce n2 along with secret key of vehicle by applying public key of SP and send the message to vehicle.

**Step 4:** Vehicle decrypts the message by applying its re-encrypt key <$ReKey_{CAR}$>. Combination of re-encrypt key of vehicle and pubic key SP generate public key of vehicle <$PK_{CAR}$> that can be decrypted by private key of vehicle.

**Step 5:** Similarly, Vehicle sends the message to AP containing random nonce n1 and new nonce n2 generated by AP along with secret key of vehicle by applying public key of SP.

**Step 6:** AP decrypts the message by applying its re-encrypt key. Combination of re-encrypt key of AP and pubic key SP generate public key of AP that can be decrypted by private key of AP.

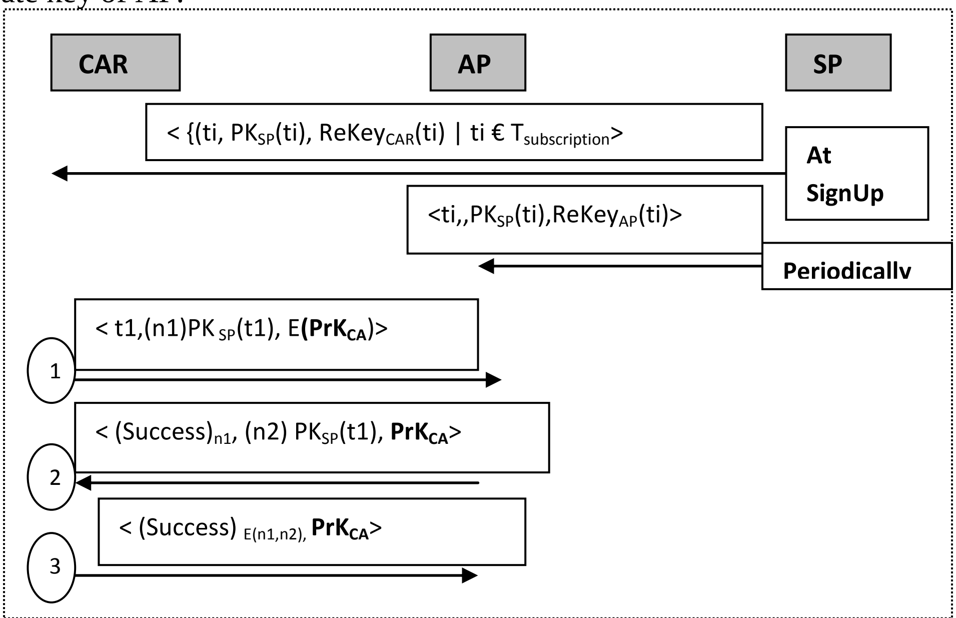


**Figure 3.5: Proposed Scheme for Authentication**

### 3.4.2 Algorithms for V2I and Inter RSU Authentication

Authentication among V2I is performed by carrying out the steps mentioned in algorithm 1 and for inter RSUs authentication the steps to be carried out are specified in algorithm 2. Notations opted for writing algorithm 1 and 2 are listed in Table 3.2 as shown below.

**Table 3.2: Notations referred in algorithm 1 and 2**

| Notation | Description |
|---|---|
| $PBV_k$ | Vehicle's Public key |
| $PRV_k$ | Vehicle's Private key |
| $RE_{kv}$ | Vehicle's Re-encrypt key |
| $RE_{kr}$ | RSU's Re-encrypt key |
| $SS_k$ | Session key |
| $PBR_k$ | RSU's Public Key |
| $PRR_k$ | RSU's Private key |
| $PB_{SP}$ | Service Provider's Public key |
| $V_h$ | $h^{th}$ Vehicle on road |
| $RSU_h$ | $h^{th}$ RSU among all |
| $X_1,X_2$ | Random values |
| T | Time |

**a) Algorithm 1: V2I Authentication**

Input: $PBV_k$ , $PRV_k$, $RE_{kv}$, $RE_{kr}$, $SS_k$, $PBR_k$ , $PRR_k$, $PB_{SP}$

1. Initiating Authentication($V_i$, $RSU_i$)
2. SP->$V_i$:({ $PBV_k$, $PRV_{k,}$ $RE_{kv,}$ $SS_k$}, $t_i$)
3. SP->$RSU_{i:}$({ $PBR_k$, $PRR_{k,}$, $RE_{kr,}$, $SS_K$},$t_i$)
4. $V_i$->$RSU_i$: $PBR_k${$t_1$,$X_1$, ,$SS_K$}
5. $RSU_i$->$V_i$:$PB_{SP}${$SS_k$ ,$X_1$,$X_2$,$t_2$}
6. $V_i$:$RE_{kv}${ $PB_{SP}${$SS_k$ ,$X_1$,$X_2$,$t_2$}}
7. $V_i$->$RSU_i$: $PB_{SP}${$SS_k$ ,X2,$t_3$}
8. $RSU_i$: $RE_{kr}${ $PB_{SP}${$SS_k$ ,$X_1$,$X_2$,$t_2$}}
9. Finish authentication at both vehicle and RSU

**b) Algorithm 2: Inter RSU Authentication**

Input: $RE_{kr}$, $SS_k$, $PBR_k$ , $PRR_k$, $PB_{SP}$

1. For h=1to n-1 do
2. For p=i+1 to n do
3. Initiating Authentication($RSU_h$, $RSU_p$)
4. SP->RSU:({ $PBR_k$, $PRR_{k,}$, $RE_{kr,}$, $SS_K$},$t_h$)
5. $RSU_h$->$RSU_p$: $PBR_k${$t_1$,$X_1$, ,$SS_K$}
6. $RSU_p$->$RSU_h$:$PB_{SP}${$SS_k$ ,$X_1$,$X_2$,$t_2$}

7. $RSU_h$:$RE_{kr}${ $PB_{SP}${$SS_k$ ,$X_1$,$X_2$,$t_2$}}
8. $RSU_h$->$RSU_p$ : $PB_{SP}${$SS_k$ ,$X_2$,$t_3$}
9. $RSU_p$: $RE_{kr}${ $PB_{SP}${$SS_k$ ,$X_1$,$X_2$,$t_2$}}
10. Finish authentication on both the RSUs

## 3.5 Performance Evaluation of Proposed Scheme

Simulation is treated as a key tool for evaluating the performance of a network protocol. Therefore, by conducting simulation the proposed scheme is evaluated and is effectiveness is find by comparing it with existing authentication schemes [35], [45], [57], [58] mentioned in literature based on computational overhead, packet delivery ratio, and latency. Network and traffic simulation, both are part of extensive simulation. For network and traffic simulation, OMNet++ and sumo simulator are used respectively. In Table 3.3 and 3.4, the parameters required for the network and traffic simulations are listed.

**Table 3.3: Traffic Simulation Parameters for Authentication**

| | |
|---|---|
| Dimension of space | 1000m x 1000m |
| Scenario | Random mobility |
| Minimum Velocity | 0 km/h |
| Maximum Velocity | 120 km/h |

**Table 3.4: Network Simulation Parameters for Authentication**

| | |
|---|---|
| Data Payload size | 120 bits/packet |
| Range of RSU | 300m |
| Physical link bandwidth | 2Mbps |

Computational overhead, Packet Delivery Ratio, and Latency are evaluated by taking readings for proposed and existing authentication schemes from the network and traffic simulations environment displayed through Figure 3.6.

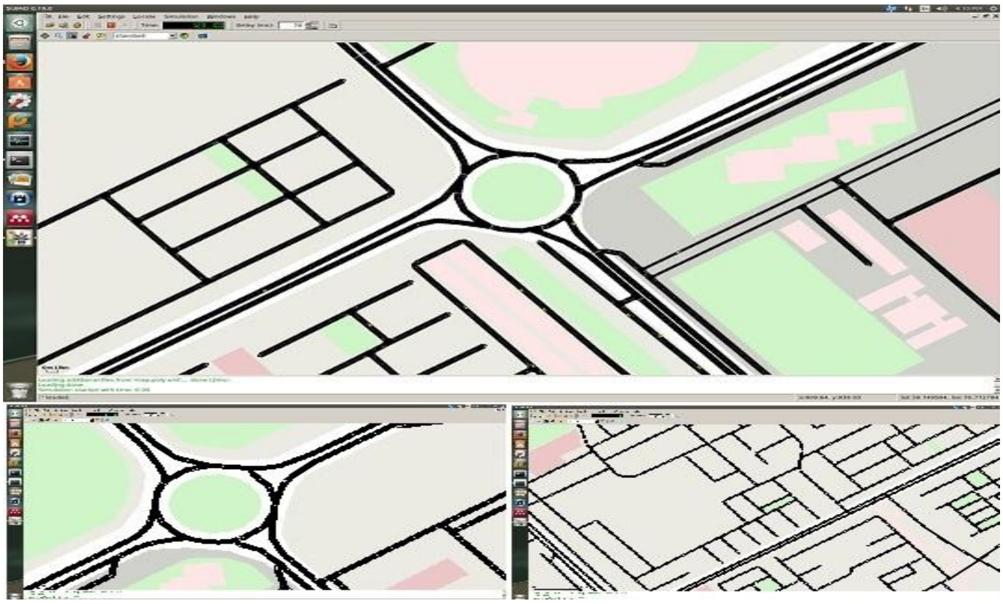

**Figure 3.6: Simulation Environment**

### 3.5.1 Computational Overhead

The indirect time or the excess time taken by a particular authentication approach to perform authentication among vehicles and RSUs is referred as computational overhead. Proposed scheme of authentication is compared with existing ones detailed in [35], [45], [57], [58] in terms of computational overhead is shown in Figure 3.7.

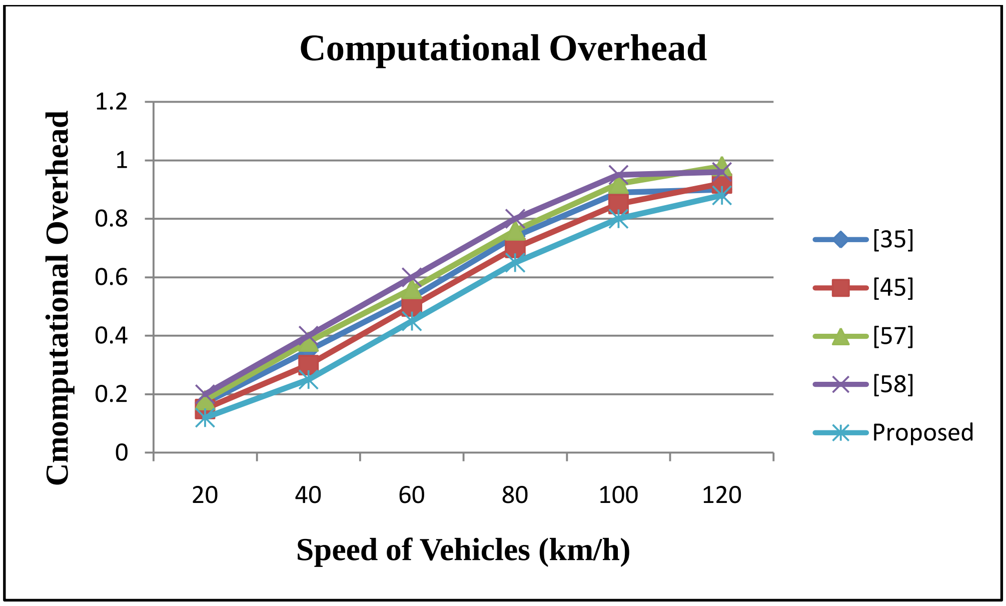


**Figure 3.7: Comparison of Existing Authentication Schemes with Proposed Scheme in terms of Computational Overhead**

The above graph shows that with the varying speed of vehicles, the computational overhead of the authentication schemes also varies. Computational overhead of scheme proposed in [35] is 2% to 10% more as compared to proposed scheme. Computational overhead of scheme proposed in [45] is 3% to 5% more as compared to proposed scheme. Computational overhead of scheme proposed in [57] is 6% to 13% more as compared to proposed scheme. Computational overhead of scheme proposed in [58] is 8% to 15% more as compared to proposed scheme. Therefore, it can be concluded that proposed authentication scheme performs well with minimum computational overhead even varying speed of vehicles. This is due to higher level of security offered using re-encrypt key by proposed scheme that reduces the number of message drop outs due to faulty vehicles. If the messages dropped out are less then no extra time is required for re-processing those messages and thus overall computational overhead of network is reduced.

### 3.5.2 Latency

Latency is the delay in receiving the packet by the destination. It can be seen in Figure 3.8 that latency in proposed scheme is less than existing authentication schemes.

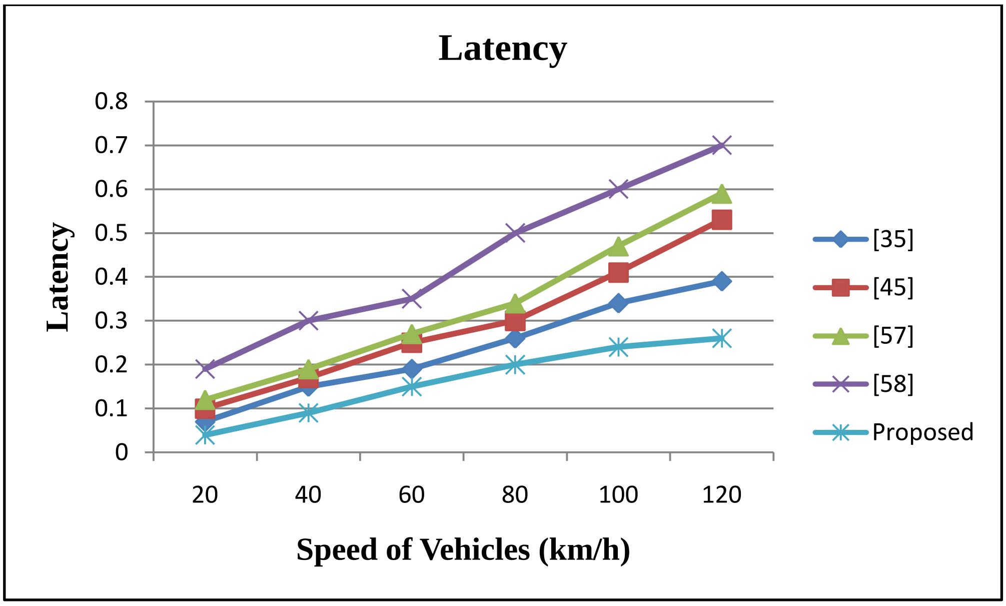


**Figure 3.8: Comparison of Existing Authentication Schemes with Proposed Scheme in terms of Latency**

The above graph shows that with the varying speed of vehicles, the latency of the authentication schemes also varies. Latency of scheme proposed in [35] is 3% to 13% more as compared to proposed scheme. Latency of scheme proposed in [45] is 6% to 27% more as compared to proposed scheme. Latency of scheme proposed in [57] is 8% to 33% more as compared to proposed scheme. Latency of scheme proposed in [58] is 15% to 44% more as compared to proposed scheme. Therefore, it can be concluded that proposed authentication scheme performs well with minimum latency even varying speed of vehicles. This is due to higher level of security offered using re-encrypt key by proposed scheme that reduces the number of message drop outs due to faulty vehicles. If the messages dropped out are less than the number of retransmissions as well as congestion is less in the network and thus reducing the overall latency of the network.

### 3.5.3 Packet Delivery Ratio

It represents the actual packets that are arrived at the receiving side to the total number of packets generated at the sending side. It can be visualized through Figure 3.9 that proposed scheme has higher packet delivery ratio as compared to the existing schemes.

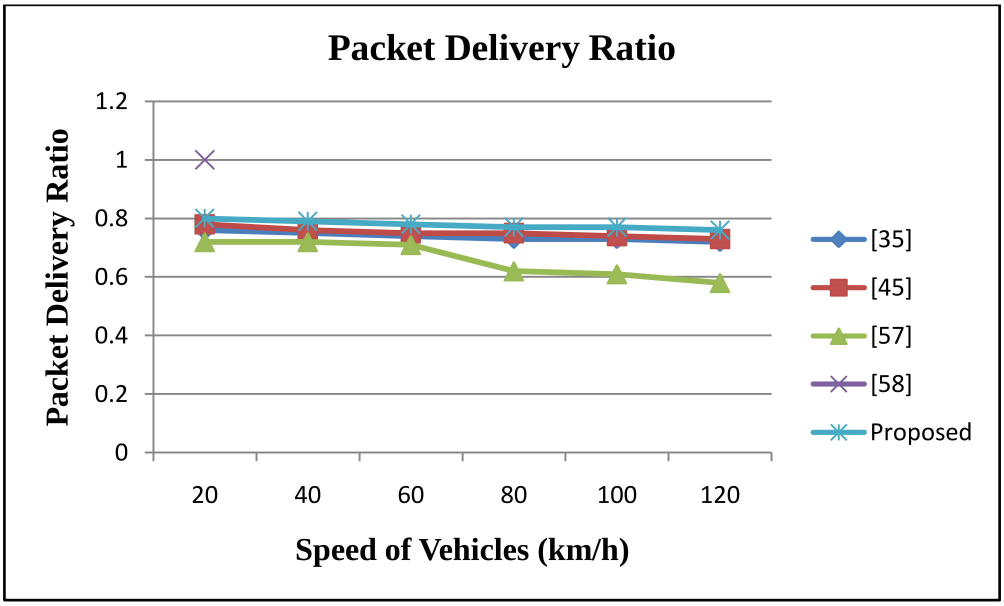


**Figure 3.9: Comparison of Existing Authentication Schemes with Proposed Scheme in terms of Packet Delivery Ratio**

The above graph shows that with the varying speed of vehicles, the packet delivery ratio of the authentication schemes also varies. Packet delivery ratio of proposed scheme in [35] is 4% less as compared to proposed scheme. Packet delivery ratio of proposed scheme in [45] is 2% to 3% less as compared to proposed scheme. Packet delivery ratio of proposed scheme in [57] is 7% to 18% less as compared to proposed scheme. Packet delivery ratio of proposed scheme in [58] is 20% to 35% less as compared to proposed scheme. Therefore, it can be concluded that proposed authentication scheme performs well with maximum packet delivery ratio even varying speed of vehicles. This is due to higher level of security offered using re-encrypt key by proposed scheme that reduces the number of message drop outs due to faulty vehicles. If the messages dropped out are less, than the ratio of number of messages received by RSU to those sent by vehicle are more and thus improving the overall packet delivery ratio of the network.

Table 3.5 summarizes and compares the performance of proposed scheme and existing schemes on different parameters. From the table below it can be deduced that proposed scheme evaluates to be better as compared to other existing schemes having less computational overhead, latency and high packet delivery ratio.

**Table 3.5: Performance Comparison of Existing Authentication Schemes and Proposed Scheme**

| **Parameters** | **[35]** | **[45]** | **[57]** | **[58]** | **Proposed Scheme** |
|---|---|---|---|---|---|
| **Computational Overhead** | Medium | Medium | High | High | Low |
| **Latency** | Medium | High | High | High | Low |
| **Packet Delivery Ratio** | Medium | Medium | Medium | Low | High |

For authentication schemes (considering speed of vehicles as 120), the value of computational overhead is High if it above 0.95, Medium if it ranges from 0.9 to 0.95, and is Low if is less than 0.9. The value of latency is high if it is above 0.5, medium if it ranges from 0.5 to 0.3, and is low if is less than 0.3. The value of packet delivery ratio is high if it is above 0.75, medium if it ranges from 0.75 to 0.55 and is low if is less than 0.55.

## 3.6 Summary

Various existing authentication processes are discussed for the vehicles in VANET. Out of all existing, IRE outperforms all the processes but still it suffers from different attacks like DoS, masquerading, eavesdropping. To overcome all these attacks, a new scheme for authentication is proposed that reduces the probability of these attacks during the sign up process. Simulation results in OMNet++ shows that proposed scheme evaluates to be better from existing schemes considering computational overhead, packet delivery ratio, and latency as evaluation concerns. Proposed scheme provides different algorithms for V2I and inter RSU authentication but does not offers authentication for V2V. To achieve the objective of collecting data in a secure manner from the vehicles on road it is essential to offer authentication among V2V and V2I. Therefore, in next chapter a threat driven authentication approach is proposed that provides efficient authentication among V2V and V2I. Therefore, data collection becomes more reliable by providing such type of complete authentication and will ultimately lead to take best decisions for path map generation. The proposed scheme is analyzed using Petri nets for depicting the lively/dynamic behavior of system.

# CHAPTER 4

# SECURITY ANALYSIS OF DISCRETE EVENT BASED THREAT DRIVEN AUTHENTICATION APPROACH IN VANET

In this chapter a threat driven complete authentication approach is proposed that tends to avoid the threats in VANET. The proposed approach provides different set of algorithms used in vehicle to vehicle and RSU to vehicle authentication. This approach is finally analyzed using Petri Nets and performance evaluation is done by taking communication overhead, throughput, packet delivery ratio, and average delay as evaluation parameters.

## 4.1 Introduction

Conventional authentication schemes discussed so far do not provide the complete authentication solution for VANET. As these schemes either offer authentication among the vehicles moving or between RSUs and vehicles. None of the earlier discussed authentication schemes provides authentication among the vehicles and between vehicles and RSUs together which results in lesser throughput and high computational overhead. Moreover, the existing authentication schemes are still vulnerable to various types of authentication attacks that also affect the network performance. Therefore, an authentication approach is proposed that provides authentication among the vehicles as well as the authentication between vehicles and RSUs. Hence, the proposed scheme provides the complete authentication solution for VANET.

## 4.2 Proposed Authentication Approach: Methodology

On initial set up during this approach, credential provider distributes the credentials to RSU and vehicle that join the VANET. After that, authentication is performed between RSUs and vehicles and among vehicles. The credentials used in network include public key and private key allotted to moving vehicle, vehicle’s session key, credential provider’s public key, re-encryption key of moving vehicle, fixed RSU's public key, fixed RSU's private key, re-encryption key allotted to fixed RSU. The detailed process of step by step authentication between RSU and vehicle is as follow:

- At a specific time instance $t_1$, vehicle initiate authentication by sending message choosing $X_1$ as the arbitrary number and $S_1$ as the session key. Message to be communicated is first encrypted by the fixed RSU's public key which is decrypted using the corresponding RSU's private key.
- RSU now at a specific time instance $t_2$, initiates transmission of message to vehicle generating its own arbitrary number let's say $X_2$, arbitrary $X_1$ received from vehicle, the session key $S_1$. After that, the full message is encrypted using the public key of credential provider.
- The combination of re-encrypt key provided to moving vehicle and credential provider's public key generates as a result the moving vehicle's public key. Therefore, now message that is appearing as encrypted through the public key of the moving vehicle is decrypted using only the moving vehicle's private key. Vehicle now verifies the $X_1$ arbitrary number generated by the vehicle.
- At a specific time instance $t_3$, message is now generated by the vehicle to RSU containing the same $S_1$ session key, $X_2$ arbitrary number generated by the RSU. At last, the message is encrypted using public key of credential provider.
- The combination of re-encrypt key of RSU and credential provider's public key generates the public key of fixed RSU. Therefore, now the message that is appearing as encrypted through the public key of the RSU is decrypted using only the fixed RSU's private key. At last, RSU verifies the arbitrary number generated by it.
- After both $X_1$ and $X_2$ are verified by vehicle and RSU respectively, authentication is done at both the ends and communication may be initiated now.

The detailed procedure for step by step authentication among two moving vehicles is as follows:

- Taking a specific time instance $t_1$, an arbitrary number $X_1$, and a session key $S_1$, vehicle $V_i$ forms a message. The message sent is first encrypted by Vehicle $V_j$ public key that is decrypted using its private key.
- Next, a message transmission is initiated by vehicle $V_j$ to vehicle $V_i$ where message contains $X_2$ that is arbitrary number generated by $V_j$, arbitrary number $X_1$ that was sent by vehicle $V_i$, and session key $S_1$. Finally, applying the public key of credential provider message is encrypted.
- The combination of re-encrypt key given to $V_i$ and credential provider's public key generates vehicle $V_i$'s public key. Therefore, now the message that is appearing as encrypted through the public key of the $V_i$ is decrypted using only the $V_i$'s private key. At last, $V_i$ verifies the arbitrary number generated by it.
- Taking a specific time instance $t_3$, the arbitrary number $X_2$ that was generated by $V_j$ is sent by vehicle $V_i$ to vehicle $V_j$ along with the session key $S_1$. After that, message is encrypted using public key of credential provider.
- The combination of re-encrypt key allotted to $V_j$ and credential provider's public key generates vehicle $V_j$'s public key. Therefore, now the message that is appearing as encrypted through public key of the $V_j$ is decrypted using only the $V_j$'s private key. At last, $V_j$ verifies the arbitrary number generated by it.
- After both $X_1$ and $X_2$ are verified by vehicle $V_i$ and $V_j$ respectively, authentication is done at both the ends and communication may be initiated now.

## 4.3 Algorithms for Establishing Mutual Authentication

### 4.3.1 Algorithm 1: Authentication between Vehicle and RSU

1: Start
2: Authentication Initialization
3: while session of authentication not come to end do
4: vehicle generates message having ($t_1$,$X_1$,$S_1$) encrypted using RSU's public key
5: Message is decrypted using RSU's private key.

6: RSU generates message having ($t_2$, $X_2$, $X_1$, $S_1$) encrypted using credential provider's public key.

7: vehicle's re-encryption key + credential provider's public key =>vehicle's public key

8: Message is decrypted using vehicle's private key

9: if $X_1$ that is generated at vehicle side matches with $X_1$ sent in the message by RSU then

10: it confirms verification of $X_1$

11: end if

12: vehicle generates message having ($t_3$, $X_2$,$S_1$) encrypted using credential provider's public key

13: RSU's re-encryption key + credential provider public key=>RSU's public key

14: Message is decrypted using RSU's private key

15: if $X_2$ that is generated at RSU matches with $X_2$ sent in the message by vehicle then

16: it confirms verification of $X_2$

17: end if

18: RSU and vehicle can proceed further with communication

19: end while

20: end

### 4.3.2 Algorithm 2: Authentication between Vehicle $V_i$ and Vehicle $V_j$

1: Start

2: Authentication initialization

3: while session of authentication not come to end do

4: $V_i$ generates message containing ($t_1$, $X_1$, $S_1$) encrypted using $V_j$'s public key.

5: message is decrypted using $V_j$'s private key.

6: $V_j$ generates message having ($t_2$, $X_2$, $X_1$, $S_1$) encrypted using credential provider's public key.

7: $V_i$'s re-encrypt key+ credential provider's public key => $V_i$'s public key

8: message is decrypted using $V_i$'s private key

9: if $X_1$ that is generated at vehicle $V_i$ side matches with $X_1$ sent in the message from $V_j$ to $V_i$ then

10: it confirms verification of $X_1$

11: end if

12: $V_i$ generates message having ($t_3$, $X_2$, $S_1$) encrypted using credential provider's public key.

13: $V_j$'s re-encrypt key + credential provider's public key =>$V_j$'s public key

14: message is decrypted using $V_j$'s private key

15: if $X_2$ that is generated at $V_j$ matches with $X_2$ sent in the message by $V_i$ to $V_j$ then

21: it confirms verification of $X_2$

16: end if

17: $V_i$ and $V_j$ can further proceed for communication

18: end while

19: end

## 4.4 Petri Net Model for Proposed Authentication Approach

Maintaining the flexible and simple nature, petri net is used widely to represent the dynamic behavior of a system. Petri net works like a mathematical or graphical tool that can be implemented for different systems. Information processing systems that are well known for being distributed, parallel, asynchronous, synchronous, stochastic, and/or non deterministic can be illustrated or learned using petri net tool. Petri net is generally used to design block diagrams, flow charts, and networks. Moreover, to simulate synchronized and lively actions related to a system petri net is used.

An authentication approach that is threat driven discrete event based for RSUs and vehicles has been proposed. Petri net model is used to analyze the proposed authentication approach that helps in processing the input data and to have a control on other arbitrary events. To carry out the different token values at firing of transition from one place to other, petri net model is used where P0 acts as an initial label marking. Petri net model for authentication approach proposed and the corresponding reachability are shown through Figure 4.1 and 4.2 respectively.

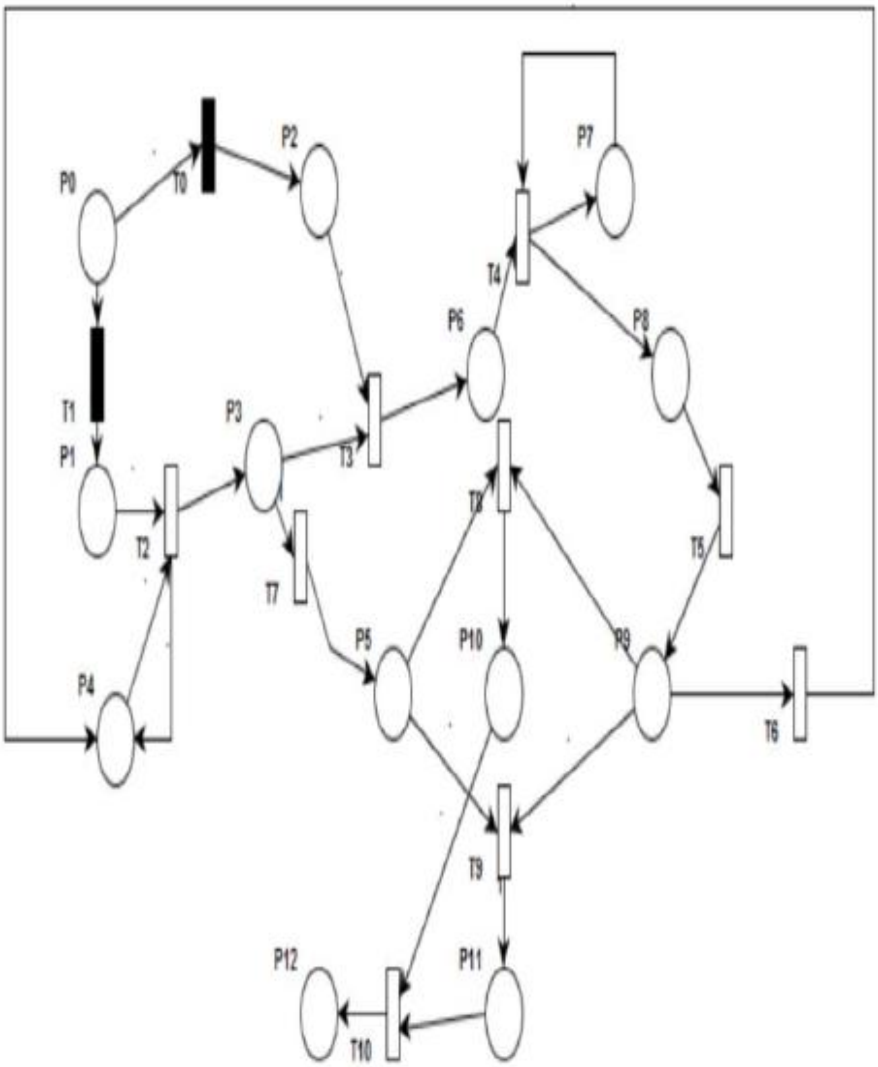


**Figure 4.1: Petri Net Model for Proposed Authentication Approach**

Correctness of the proposed approach for authentication can be assessed using Reachability and liveliness as its two prime properties. Reachabilty assures that we can move from one state to other. Liveliness is, if all the reachable states do not come to deadlock situation when they are fired. The proposed approach for authentication when tested using Petri net model it possessed both liveliness and reachability properties. Different categories of states and marking that are reached can be represented using reachability graph. In Figure 4.2 markings are represented through nodes and transition names are labeled on arrows to depict that after firing a certain transition the corresponding marking can be reached.

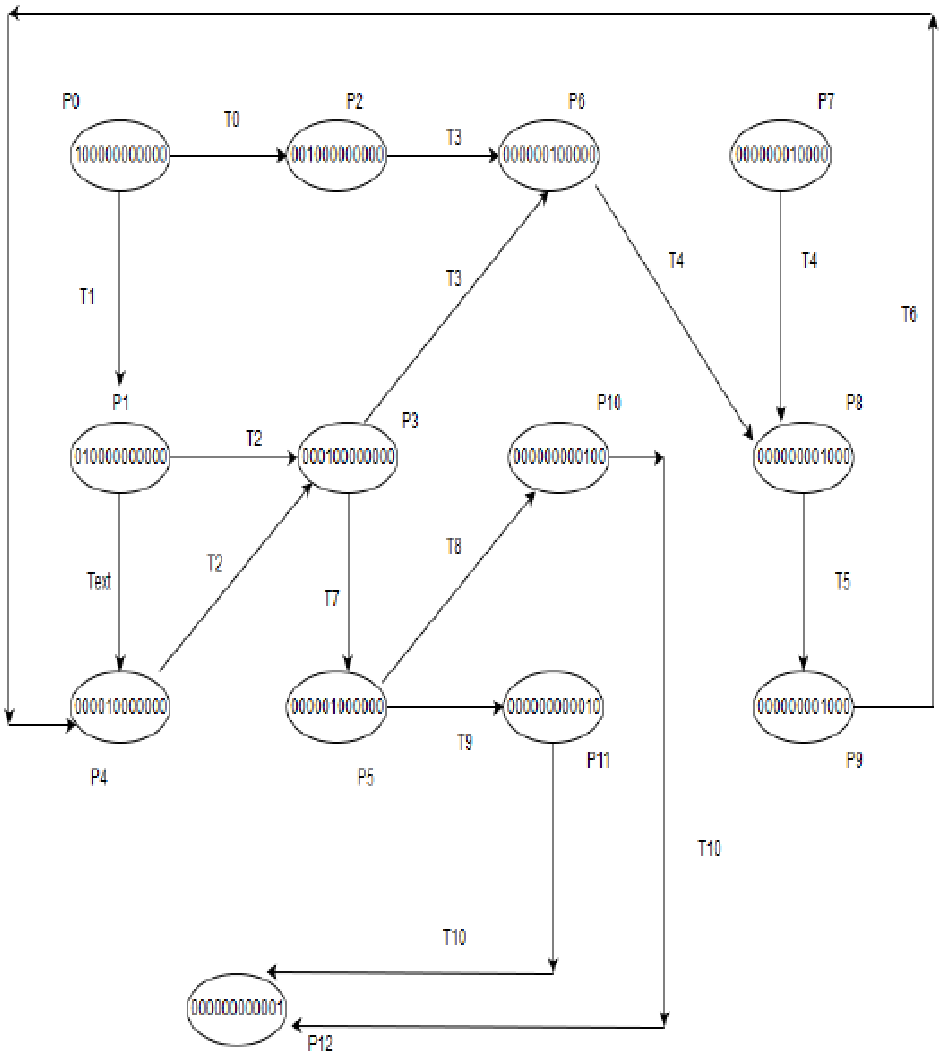


**Figure 4.2: Reachability graph for proposed authentication Approach**

For choosing the petri nets model for the proposed approach for authentication, description of places and the transitions that are used to represent the proposed approach are shown in Table 4.1 and 4.2 respectively. Petri net model is realized in Acer laptop working on Window 7 environment in order to analyze the proposed approach model. Under the given environment of simulation, the proposed model's methodology worked out efficiently. Whenever a vehicle joins a network, initially authentication is established between RSU and vehicle and among vehicles. Various categories of situations that vehicles and RSUs have to face during authentication are represented from T0-T10 transition as shown in Table 4.2.

**Table 4.1: Description of Places**

| State | Description |
|---|---|
| P0 | Credential provider’s working place |
| P1 | On board unit’s original place |
| P2 | RSU’s original place |
| P3 | Waiting place |
| P4 | On board unit working place |
| P5 | On board unit information is maintained |
| P6 | On board unit information is maintained |
| P7 | RSU’s working place |
| P8 | RSU’s waiting place |
| P9 | Information of RSU is maintained |
| P10 | Information verified -Yes |
| P11 | Information verified -No |
| P12 | Authentication workplace |

**Table 4.2: Description of Transition**

| Transition | Description |
|---|---|
| T0 | RSU’s receiving credentials |
| T1 | Vehicle’s receiving credentials |
| T2 | Data received from vehicle is processed |
| T3 | Data received from RSU and vehicle |
| T4 | Data received from RSU is processed |
| T5 | RSU data received |
| T6 | Data received from RSU is processed |
| T7 | Vehicle data received |
| T8 | RSU and vehicle data verified –Yes |
| T9 | RSU and vehicle data verified –No |
| T10 | Transmitting data used for authentication |

## 4.5 System Model

Utilizing the vehicle in network simulation (Veins) framework, the proposed approach used for authentication is compared with the existing authentication approaches used in [63], [64] and [65]. For VANET simulation, Veins is considered as an apt framework. The network simulator OMNet++ is used to execute model of simulation in Veins framework and for traffic simulation of road SUMO is used. The parameters taken for simulation in order to execute the model are mentioned in Table 4.3 and 4.4.

**Table 4.3: Traffic Simulation Parameters**

| Parameter Name | Value |
|---|---|
| Number of Vehicles | 5,10,15,20,25 |
| Maximum Speed | 40 m/s |
| Acceleration | 5m/s2 |
| Deceleration | 8m/s2 |
| Driver Fault | 0.5 |

**Table 4.4: Network Simulation Parameters**

| Parameter Name | Value |
|---|---|
| Network Simulator | OMNet++ |
| Simulation Time | 1000 sec |
| Area of Simulation | 1000 m x 1000 m |
| Simulation Set Up | Random and Cross roads |
| MAC Protocol | IEEE802.11p |
| Range of Transmission | 300 m |

## 4. 6 Results and Discussions

The performance comparison of proposed approach of authentication is made with the existing approaches of authentication mentioned in [63], [64] and [65] in terms of computational overhead, packet delivery ratio, throughput, and average delay.

Asymmetric algorithms are considered relatively slow in contrast to symmetric algorithms due to the use of very complex mathematical functions. Assuming the current age of computational technology, the size of key opted by an encryption algorithm is considered as a major security measure in VANET. In present scenario, asymmetric as well as asymmetric algorithms work on similar key size due to advancement in technology. The fact is, asymmetric algorithm security lies in the strength of its private key which is impossible to get retrieved using its public key. Moreover, the different secret keys required in asymmetric algorithm are less as compared with the symmetric algorithm. To offer privacy and security in short messages, asymmetric algorithms prove to be an efficient encryption in VANET.

The indirect time or the excess time taken by a particular authentication approach to perform authentication among vehicles and among vehicles and RSUs is referred as computational overhead. Table 4.5 illustrates the comparison of existing approaches mentioned in [63], [64] and [65] for authentication with the proposed approach of authentication. In Table 4.5, random number cost generation is represented by RN, hash function cost generation is represented by HF, asymmetric encryption execution cost using the re-encrypt key is represented by AE, symmetric encryption execution cost is represented by SE, XOR function execution cost is represented by XF.

**Table 4.5: Comparison of Computational Overhead Parameters for different Authentication Approaches**

| **Computational Overhead** | **Approach in [63]** | **Approach in [64]** | **Approach in [65]** | **Proposed Approach** |
|---|---|---|---|---|
| RN | 3 | 2 | 2 | 2 |
| HF | 4 | 9 | 2 | 0 |
| AE | 0 | 0 | 0 | 2 |
| SE | 2 | 6 | 2 | 0 |
| XF | 3 | 2 | 2 | 0 |
| Total Cost | 3RN+4HF+2SE+3XF | 2RN+9HF+6SE+2XF | 2RN+2HF+2SE+2XF | 2RN+2AE |

According to the above table, authentication approach mentioned in [63] has RN as 3, HF as 4, AE as 0, SE as 2, and XF as 3. Authentication approach mentioned in [64] has RN as 2, HF as 9, AE as 0, SE as 6, and XF as 2. Authentication approach mentioned in [65] has RN as 2, HF as 2, AE as 0, SE as 2, and XF as 2. The Proposed authentication approach mentioned has RN as 2, HF as 0, AE as 2, SE as 0, and XF as 0. Therefore the proposed approach has minimum cost as it uses only random number and asymmetric algorithm and no other hash function, symmetric encryption or XOR function is required.

Figure 4.3 represents that computational overhead of the proposed approach of authentication is relatively less in comparison to existing approaches of authentication mentioned in [63], [64] and [65].

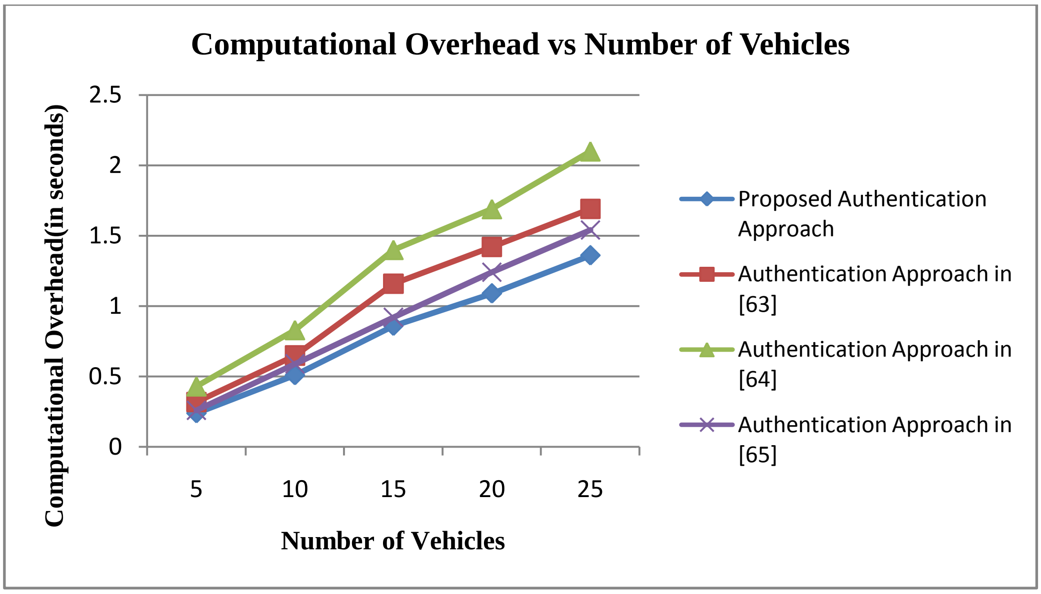


**Figure 4.3: Comparison of Computational Overhead for Proposed and Existing Authentication Approaches**

The above graph shows that with varying number of vehicles, computational overhead of the authentication schemes also varies. Computational overhead of scheme proposed in [63] is 3% to 13% more as compared to proposed scheme. Computational overhead of scheme proposed in [64] is 7% to 30% more as compared to proposed scheme. Computational overhead of scheme proposed in [65] is 0.3% to 7.2% more as compared to proposed scheme. Therefore, it can be concluded that proposed authentication scheme performs well with minimum computational overhead even with varying number of vehicles. The existing approaches of authentication mentioned in [63], [64] and [65] uses symmetric algorithm, XOR function, and hash function, whereas, the approach proposed for authentication work on asymmetric algorithm. Therefore, the computational overhead of existing approaches of authentication mentioned in [63], [64] and [65] is more as compared to the proposed approach of authentication.

Over a logical or physical communication channel, the number of packets that are sent within a specific time interval is referred as throughput. Figure 4.4 represents that throughput of the approach proposed for authentication is relatively more as compared to existing approaches of authentication mentioned in [63], [64] and [65].

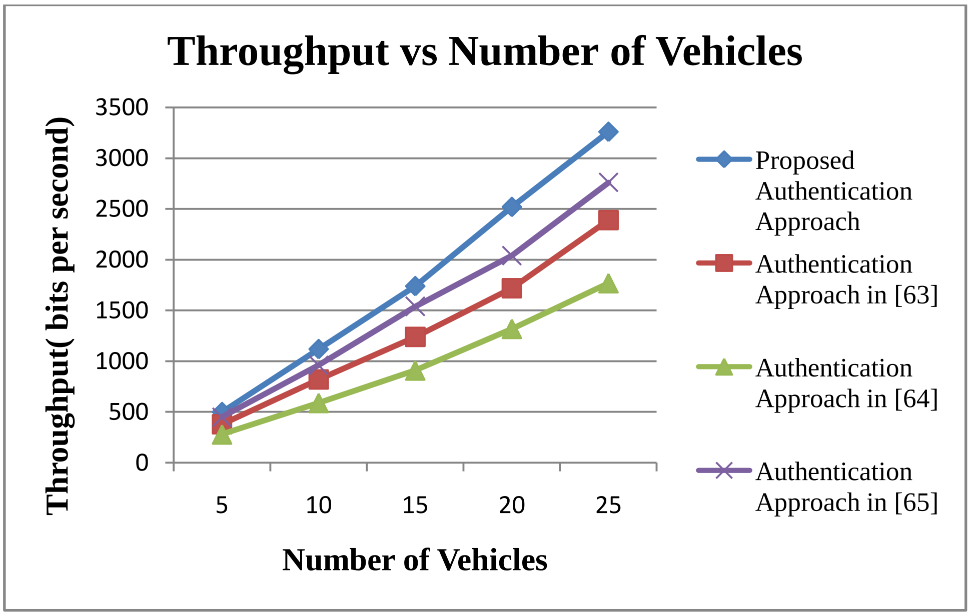


**Figure 4.4: Comparison of Throughput for Proposed and Existing Authentication Approaches**

The above graph shows that with varying number of vehicles, throughput of the authentication schemes also varies. Throughput of scheme proposed in [63] is 3% to 25% less as compared to proposed scheme. Throughput of scheme proposed in [64] is 6% to 43% less as compared to proposed scheme. Throughput of scheme proposed in [65] is 1% to 15% less as compared to proposed scheme. Therefore, it can be concluded that proposed authentication scheme performs well with maximum throughput even with varying number of vehicles.

Packet delivery ratio is the ratio of the data packets that are effectively arrived at the destination side to the data packets sent from sender side. Figure 4.5 represents that packet delivery ratio of the approach proposed for authentication is high as compared to the existing approaches of authentication mentioned in [63], [64] and [65].

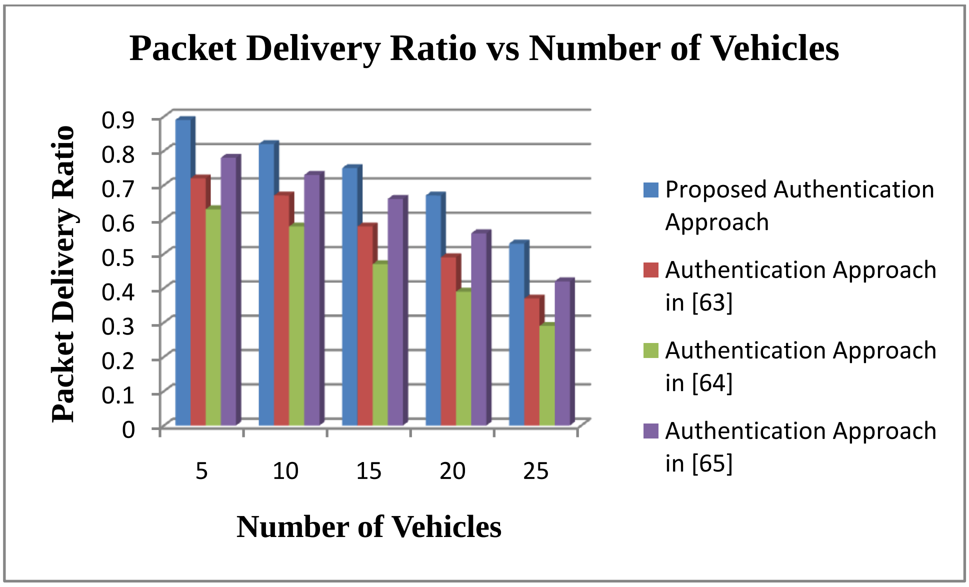


**Figure 4.5: Comparison of Packet Delivery Ratio for Proposed and Existing Authentication Approaches**

The above graph shows that with the varying number of vehicles, packet delivery ratio of the authentication schemes also varies. Packet delivery ratio of proposed scheme in [63] is 15% to 18% less as compared to proposed scheme. Packet delivery ratio of proposed scheme in [64] is 24% to 28% less as compared to proposed scheme. Packet delivery ratio of proposed scheme in [65] is 9% to 11% less as compared to proposed scheme.  Therefore, it can be concluded that proposed authentication scheme performs well with maximum packet delivery ratio even with varying number of vehicles.

Average delay is time elapsed by while sending packet from a specific source to a destination over the given logical or physical communication channel. Figure 4.6 represents that average delay of proposed approach of authentication is less as compared to existing approaches of authentication mentioned in [63], [64] and [65].

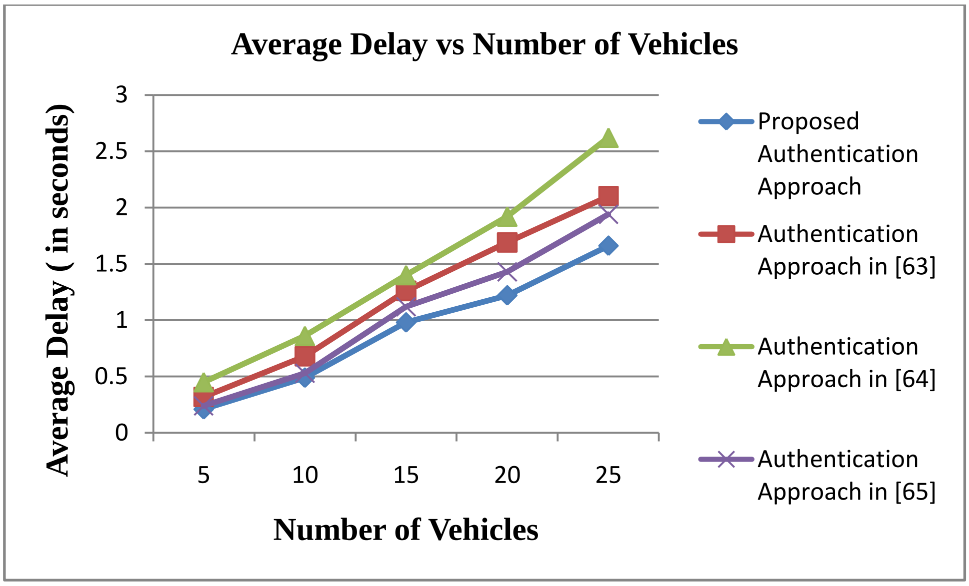


**Figure 4.6: Comparison of Average Delay for Proposed and Existing Authentication Approaches**

The above graph shows that with the varying number of vehicles, average delay of the authentication schemes also varies. Average delay of scheme proposed in [63] is 3% to 16% more as compared to proposed scheme. Average delay of scheme proposed in [64] is 8% to 32% more as compared to proposed scheme. Average delay of scheme proposed in [65] is 1% to 10% more as compared to proposed scheme. Therefore, it can be concluded that proposed authentication scheme performs well with minimum average delay even with varying number of vehicles.

## 4.7 Summary

In this chapter, discrete threat driven event based approach for authentication has been proposed. The proposed approach of authentication makes use of asymmetric algorithm, time dependent arbitrary numbers, and re-encrypt key to provide authentication between vehicles and RSUs and among vehicles. Veins framework and Petri Nets are used to analyze the proposed approach for authentication. After analysis through Petri nets model and working on its reachability graph, it has been identified that the proposed approach for authentication pertains the liveness and reachability property. Using the Veins framework it has been observed that proposed authentication approach performs better as compared to existing approaches for authentication detailed in [63],[64], and [65] in terms of computational overhead, effective packet delivery ratio, average delay, and throughput. It has also been concluded that the proposed approach offers both security and privacy between RSUs and vehicles and among vehicles, preventing VANET from various types of attacks based on authentication.

Once a initial trust is maintained using the efficient process of authentication between the RSUs and vehicles, the next step corresponds to collecting data from the moving vehicles and finally to store that data on RSUs. Next chapter works on detailing the existing schemes for data collection and later an improved scheme is proposed for data collection.

# CHAPTER 5

# PROPOSED INTELLIGENT AUTHENTICATION BASED VEHICLE INITIATED BROADCAST-DYNAMIC PATH DATA COLLECTION SCHEME IN VANET

In this chapter, the existing DCSs in VANET are compared using OMNet++. Later, an intelligent authentication based vehicle initiated broadcast- dynamic path (IAVIB-DP) collection scheme is proposed for VANET and is compared with best existing DCS. This chapter presents the vehicular mobility framework, simulation parameters, the simulator for network operation and use of all these in VANET simulation. The performance metrics have been designed to set a tradeoff between the different components of evaluation and analysis.

## 5.1 Introduction

The path information collection mechanism of a vehicle is anticipated by various authors using varied DCSs. Schemes are categorized into two, one are static and others are dynamic. The path information remains fixed in the static schemes and these schemes not get the updated information if any changes are made by vehicles or there is change in situation on the road. Considering the dynamic schemes behavior, they are capable of collecting the updated information about the path that vehicles are traversing.

## 5.2 Modern Data Collection Schemes

Modern DCSs can be divided in two broad types considering whether data collection procedure is RSU initiated or Vehicle initiated as shown in Figure 5.1.

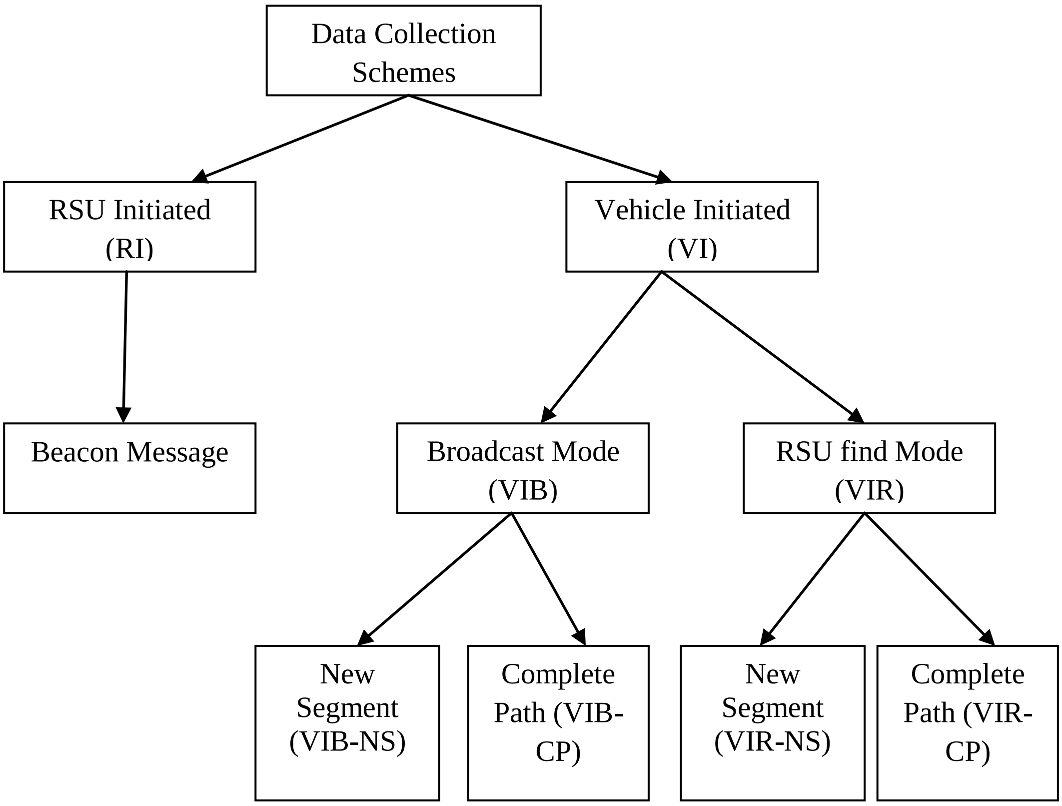


**Figure 5.1 Modern Data Collection Schemes in VANET**

### 5.2.1 RSU initiated (RI)

As the scheme is RSU initiated, RSU after a fixed interval of time, say, N seconds, generates a beacon message for the vehicles that are currently moving in its vicinity. In response, vehicle generates packets destined for the RSU containing the collected information of partial paths.

### 5.2.2 Vehicle Initiated-Broadcast mode (VIB)

As the mode of operation is vehicle-initiated, vehicle in broadcast mode conduct the transmission of packets to all RSUs belonging to its locality. VIB can be further working into two sub-domains.

***5.2.2.1 VIB-New Segment (VIB-NS):*** A packet is generated by the vehicle while moving on its paths whenever it collects new segment information.

***5.2.2.2 VIB-Complete Path (VIB-CP):*** A packet is transmitted by the vehicle when it has collected information related to complete path containing the details of all segments it has traversed after reaching its final destination.

### 5.2.3 Vehicle Initiated-RSU find mode (VIR)

A message is initiated by the vehicle for transmission of packets but before that vehicle broadcasts a find RSU message. The RSU which is in the vicinity of the vehicle and is nearest to it responds first using a message mentioning the address of RSU. This scheme is further categorized into two sub-schemes.

**5.2.3.1** ***VIR- New Segment (VIR-NS):*** A packet is transmitted by the vehicle to a specific RSU whenever it collects new segment information in its path.

**5.2.3.2** ***VIR-Complete Path (VIR-CP):*** A packet is transmitted by the vehicle when it has collected information related to complete path containing the details of all segments it has traversed.

## 5.3 Network Simulator

To evaluate the performance, DCSs are implemented in the veins framework. For performing network simulation for VANET, veins framework that is an open source vehicular network simulation is used. It is founded on two well known simulators: SUMO, a path traffic simulator and OMNeT++, an incident-based network simulator. Veins extends these two well known simulators in order to provide a detailed collection for inter vehicle communication (IVC) simulation. Figure 5.2-Figure 5.5 shows Veins Framework using SUMO and OMNeT++.

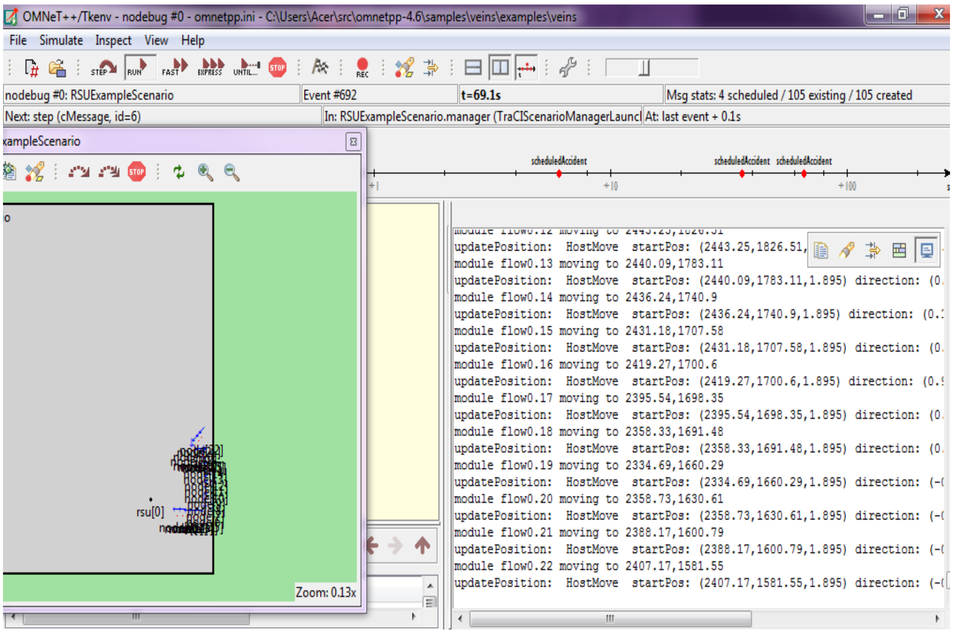


**Figure 5.2: RSU Scenario in OMNeT++**

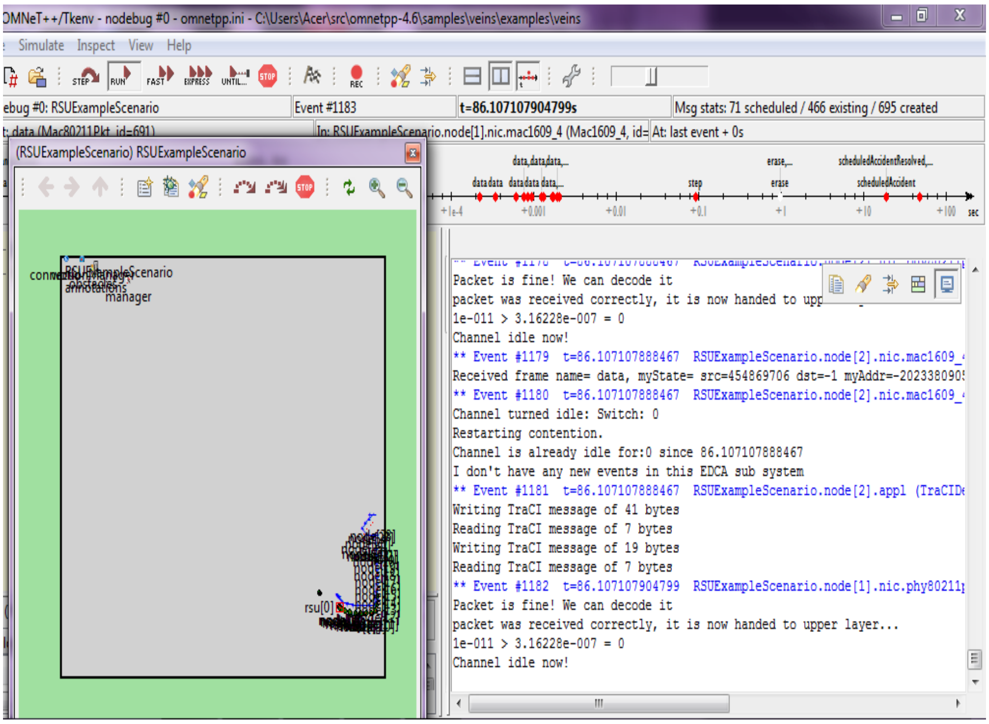

**Figure 5.3: Scheduled Event at RSU**

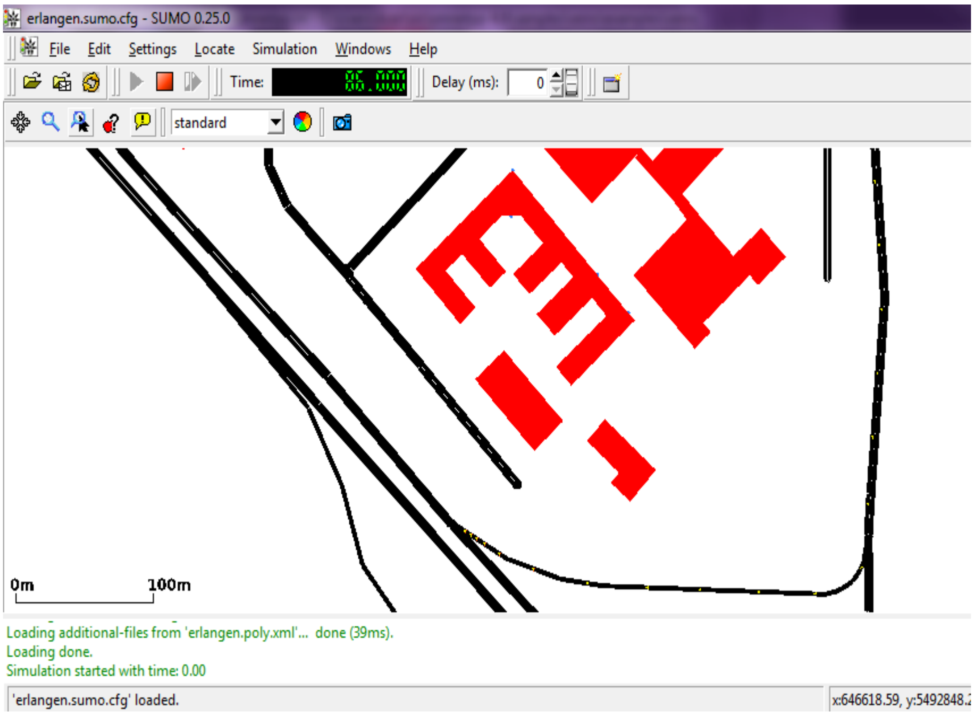

**Figure 5.4: Sumo Framework**

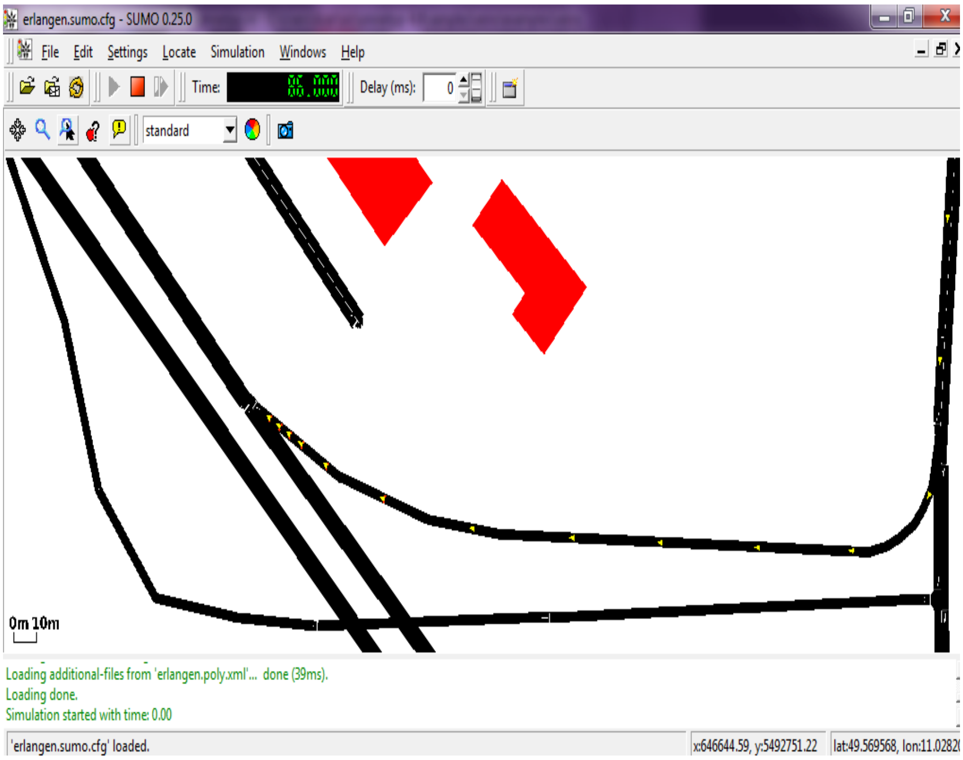


**Figure 5.5: Moving vehicles and hit event in SUMO**

## 5.4 Simulation Parameters

In Table 5.1, simulation parameters taken for carrying out all the experiments are mentioned.

**Table 5.1: General Simulation Parameters**

| Parameters | Value |
|---|---|
| Type of Channel | Wireless |
| Type of Network Interface | Physical Wireless Network |
| MAC protocol | IEEE802.11p |
| Communication range | 300 m |
| Map Area | 1000*1000sq.m |
| Interface queue type | FIFO queue |

| | |
|---|---|
| Queue length | 100 packets |
| Radio Propagation Model | Two ray Ground |
| Number of vehicles | 100-1000 |
| Speed of vehicle | 40 m/s |
| Simulation time | 1000 seconds |
| Map Layout | City Map |
| Size of data payload | 120 bits/packet |
| Bandwidth of Physical Link | 2 Mbps |
| Scenario | Random mobility |
| Type of Traffic | Constant Bit Rate |

## 5.5 Vehicular Mobility Framework

The extensive simulation is done by using City Map to generate the city network. The number of vehicles is set to 100, 200, 300, 400, 500, 600, 700, 800, 900, and 1000. Second, the communication range between RSUs and vehicles is set to a radius of 300m for every experiment. The experiments are carried out for 1000 seconds while collecting the paths opted by vehicles during their journey from source to destination.

## 5.6 Performance Metrics for Data Collection Schemes

Performance metrics are referred to generate a performance index in DCSs used in this research work. Performance metrics identified are communication overhead, packet delivery ratio, and latency.

### 5.6.1 Communication Overhead

Communication overhead is determined by total data messages that are transmitted taking into consideration the add up of vehicles generating these messages. Mechanism used to compute communication overhead is represented through equation 1.

$$Communication\ Overhead = \frac{\sum Total\ \ Messages}{\sum Number\ \ of\ Vehicles} \qquad (1)$$

### 5.6.2 Packet Delivery Ratio

It is the ratio of packets arrived at the destination to the packets that are originated from the source. The mechanism used to compute packet delivery ratio is represented through equation 2.

$$Packet\ Delivery\ Ratio\ = \frac{\sum Number\ of\ Packets\ Received}{\sum Number\ of\ Packets\ Sent} \qquad (2)$$

### 5.6.3 Latency

The average time taken by a packet carrying data in order to reach to a destination is known as delay. Delay includes all the possible delays due to route prediction, buffering, queuing. A measure of time delay experienced by a system is known as latency. The formula used to compute latency is represented through equation 3.

$$Latency = \frac{\sum Packet\ \ Receiving\ \ Time - Packet\ \ Sent\ Time}{\sum Total\ \ Number\ \ of\ Links} \qquad (3)$$

### 5.6.4 Performance Index (PI)

PI is used to estimate the efficiency and value of a DCS. A higher of PI states that a DCS is efficient. The value of PI is dependent on different parameters like communication overhead, packet delivery ratio, and latency. PI corresponding to a particular DCS tends to increase when communication overhead decreases and reverse is also true. Therefore, assuming the number of transmitted messages to be more, communication overhead of the network is going to increase and its PI is going to decrease. Secondly, PI corresponding to a particular DCS tends to decrease when its packet delivery ratio decreases and reverse is also true. Therefore, with increase in the number of data packets received at a destination, packet delivery ratio is more and hence PI is more. PI corresponding to a DCS increases when its latency decreases and reverse is also true. Therefore, if high delay is indulged in sending a packet, latency is more and its PI is going to decrease. The mechanism used to compute PI is represented through equation 4.

$$PI = \frac{k * Packet\ Delivery\ Ratio}{Latency * \text{Communication Overhead}} \quad (4)$$

Considering a constant value k , that relies on the number of vehicles on road.

## 5.7 Comparative Analysis of Existing Data Collection Schemes

Considering the fixed simulation parameters as mentioned in Table 5.1 and using OMNet++, different DCSs are implemented on a single RSU as represented through Figure 5.6.

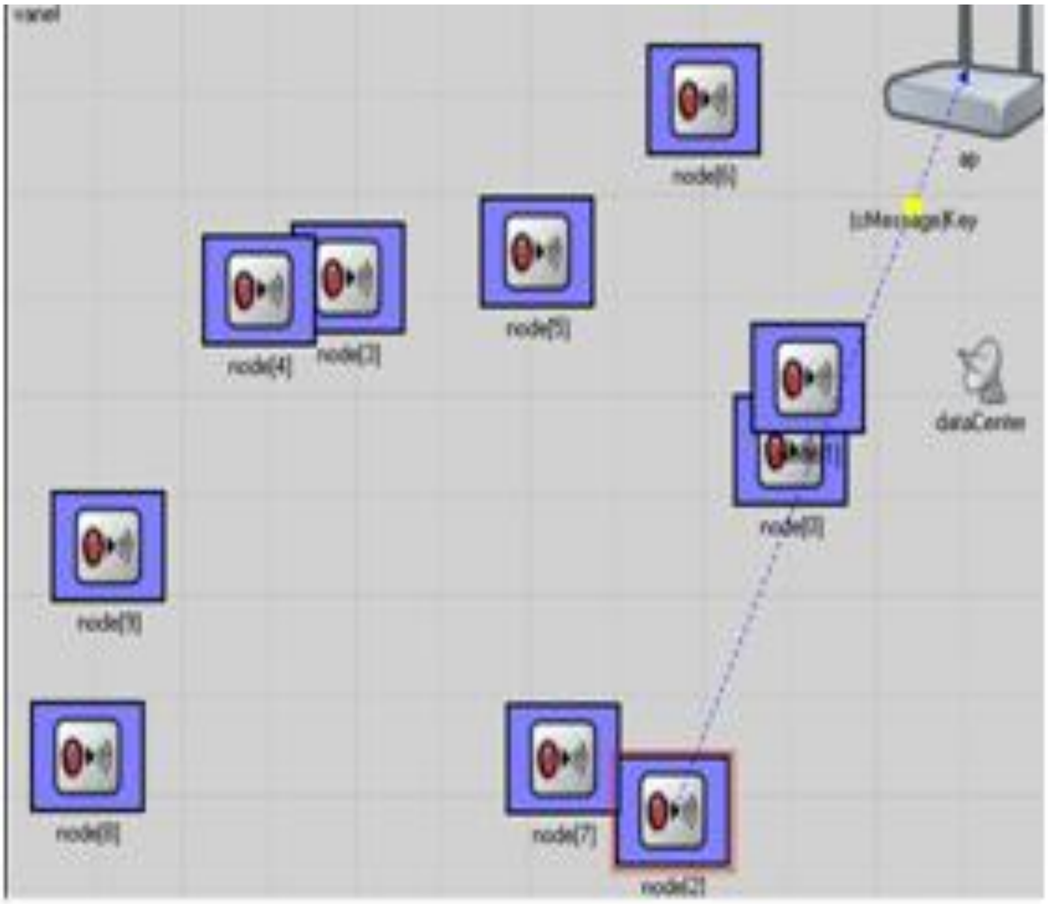


**Figure 5.6: Data Collection Scenario at Single RSU**

By taking readings from OMNet++ environment, the values of communication overhead, packet delivery ratio, and latency are determined as shown in Figure 5.7.

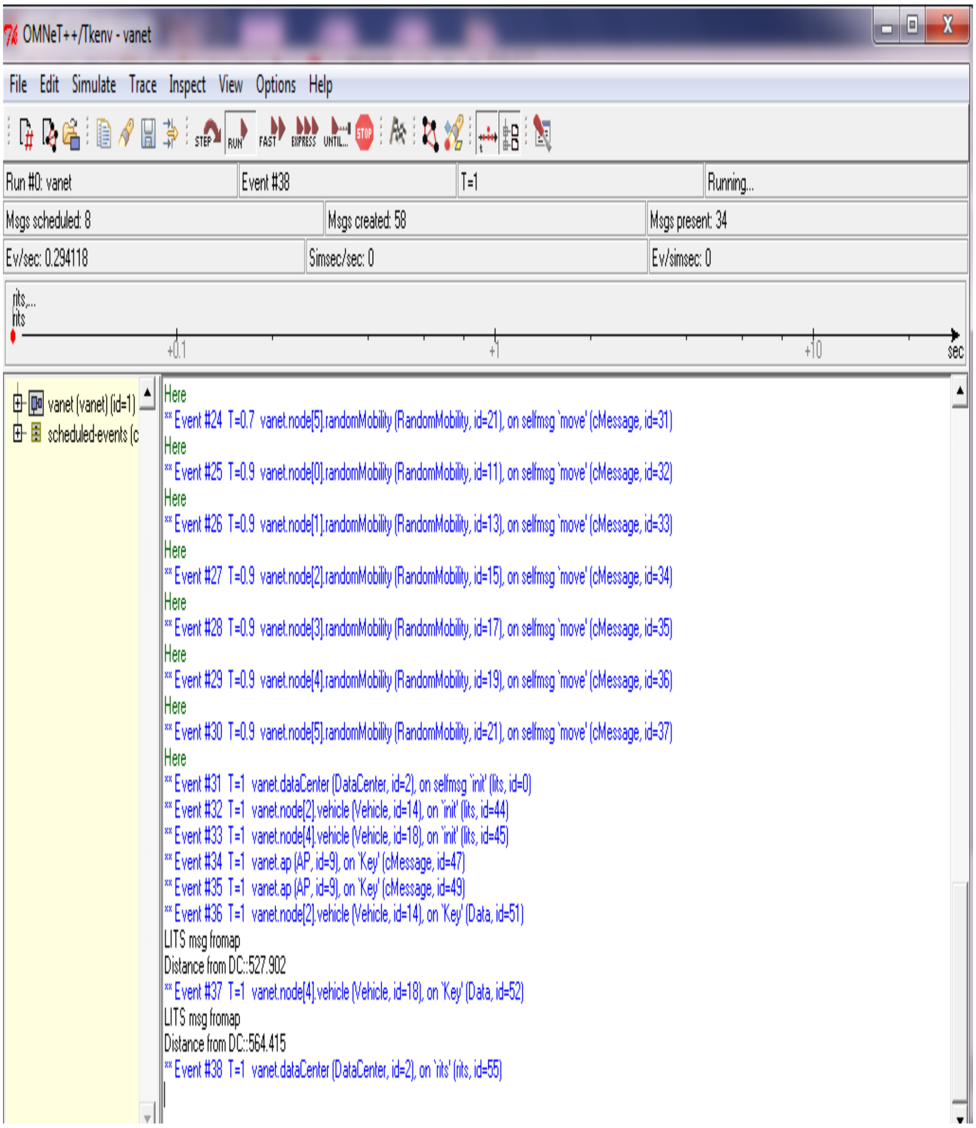


**Figure 5.7: Readings from OMNeT++ Environment**

Figure 5.8 reflects the comparative analysis of different DCSs in terms of communication overhead.

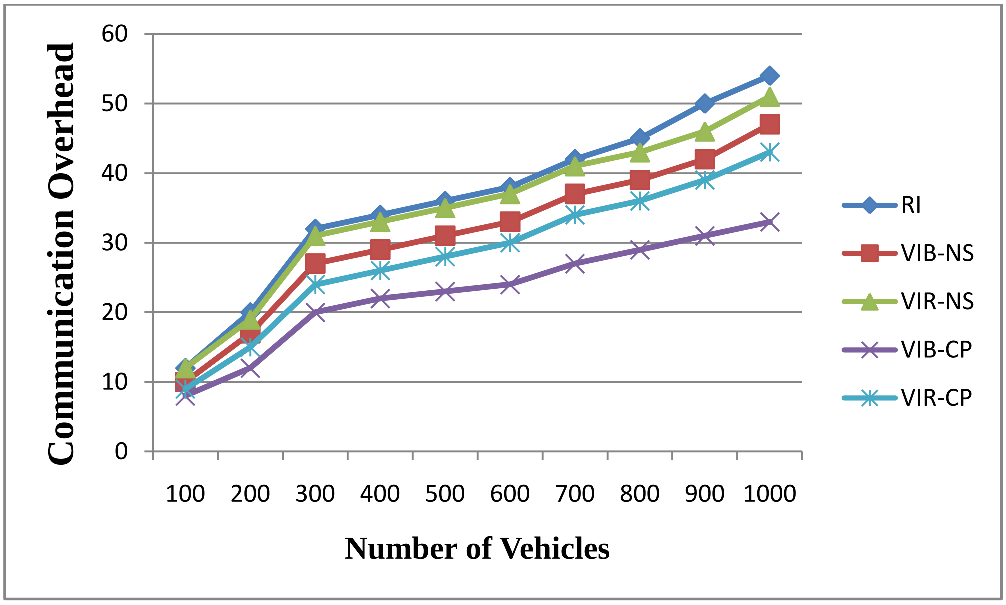


**Figure 5.8: Communication overhead for different DCSs with varying number of vehicles**

Considering variable number of vehicles, communication overhead of VIB-CP is 6 % to 35 % less than RI, 3% to 24% less than VIB-NS, 6% to 30% less than VIR-NS, and 1% to 16% less than VIR-CP. Therefore, it can be concluded that among existing DCSs, VIB-CP has minimum communication overhead as each vehicle generates less number of excess messages as compared to other schemes. Figure 5.9 shows comparative analysis of existing DCSs in terms of packet delivery ratio.

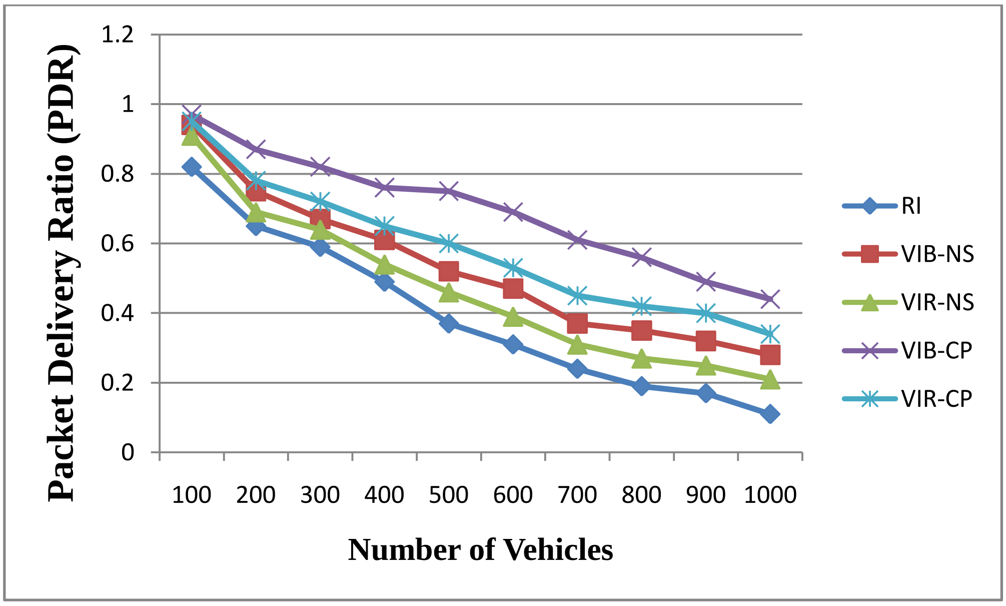


**Figure 5.9: Packet delivery ratio for different DCSs with varying number of vehicles**

With varying number of vehicles on the road, the packet delivery ratio of VIB-CP is 15 % to 33 % more than RI, 3% to 16% more than VIB-NS, 6% to 23% more than VIR-NS, and 2% to 10% more than VIR-CP. Therefore, it can be concluded that among existing DCSs, VIB-CP has high packet delivery ratio as each vehicle generates less number of excess messages as compared to other schemes leading to less congestion and maximum delivery at destination.

Figure 5.10 shows the comparative analysis of different DCSs in terms of latency.

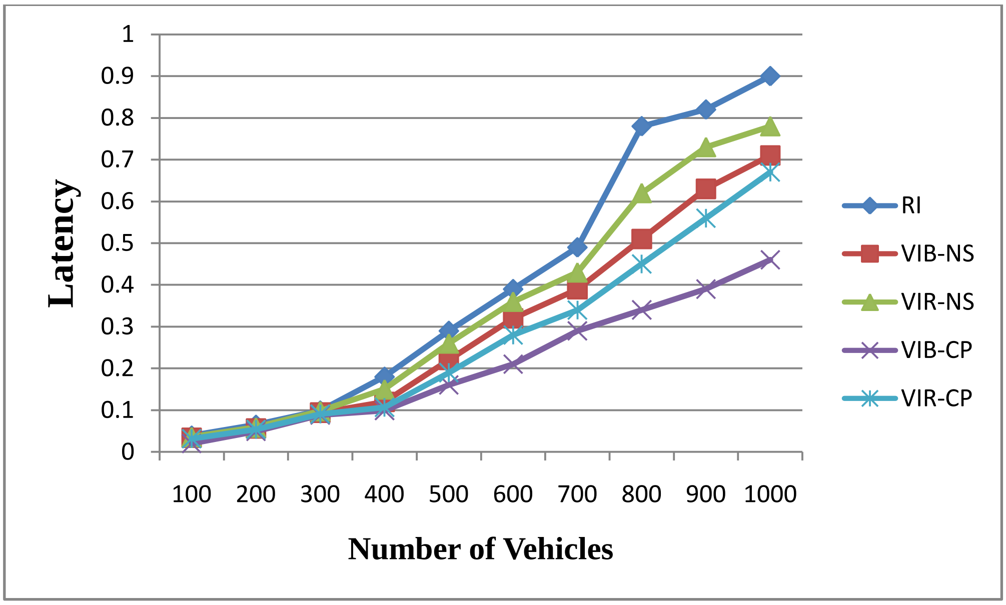


**Figure 5.10: Latency for different DCSs with varying number of vehicles**

With varying number of vehicles, the latency of VIB-CP is 1 % to 44 % less than RI, 0.5% to 25% less than VIB-NS, 1% to 32% less than VIR-NS, and 0.3% to 21% less than VIR-CP. Therefore, it can be concluded that among existing DCSs, VIB-CP has less latency as each vehicle generates less number of excess messages as compared to other schemes, leading to less excess time required due to buffering and processing. Figure 5.11 show comparative analysis of different DCSs in terms of PI.

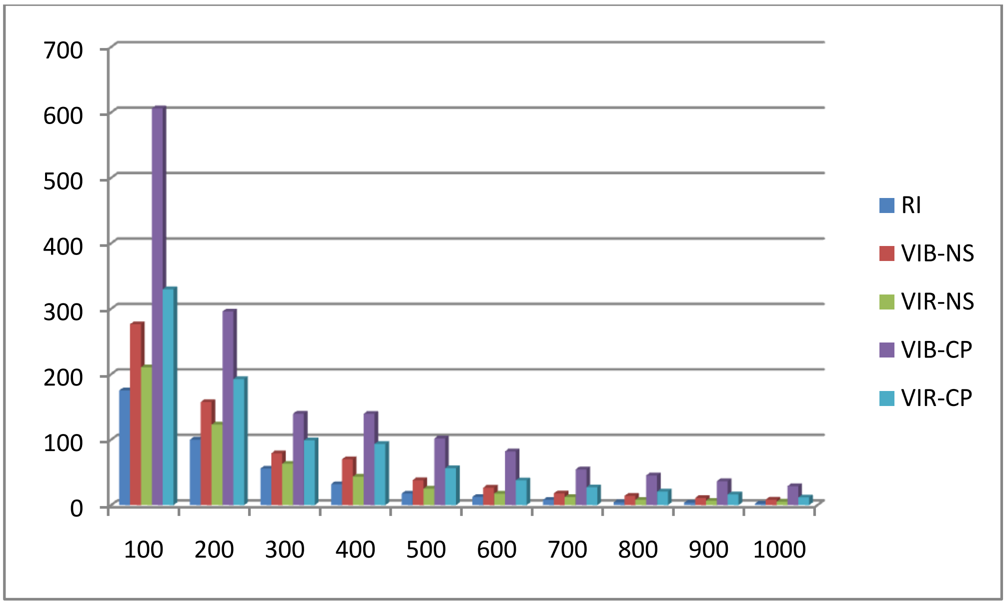


**Figure 5.11: Performance Index for different DCSs with varying number of vehicles**

With varying number of vehicles, the PI of VIB-CP is 3 % to 61 % more than RI, 2% to 47% more than VIB-NS, 3% to 56% more than VIR-NS, and 2% to 39% more than VIR-CP. Therefore, it can be deduced that among existing DCSs, VIB-CP has high PI with minimum overhead due to communication, high packet delivery ratio and low latency.

As shown in Table 5.2, different DCSs are compared depending upon the implementation work done.

**Table 5.2: Comparison of Modern Data Collection Methods in VANET**

| | **Performance Parameters** | | | **PI** |
|---|---|---|---|---|
| **Data Collection Scheme** | **Communication Overhead** | **Packet Delivery Ratio** | **Latency** | **PI** |
| **RI** | HIGH | LOW | HIGH | LOW |
| **VIR-NS** | HIGH | MODERATE | HIGH | WORST |
| **VIB-NS** | MODERATE | MODERATE | HIGH | AVERAGE |
| **VIB-CP** | LOW | HIGH | LOW | BEST |
| **VIR-CP** | MODERATE | MODERATE | MODERATE | BETTER |

The different range values corresponding to HIGH, MODERATE, and LOW for communication overhead, packet delivery ratio, latency and LOW, AVERAGE, WORST, BEST, BETTER for PI, considering the number of vehicles as 1000 are represented through Table 5.3 below.

**Table 5.3: Performance Range Values for communication overhead, packet delivery ratio, latency, and PI.**

| **Communication Overhead** | |
|---|---|
| HIGH | Above 50 |
| MODERATE | 40 to 50 |
| LOW | Less than 40 |
| **Packet Delivery Ratio** | |
| HIGH | Above 0.4 |
| MODERATE | 0.2 to 0.4 |
| LOW | less than 0.2 |
| **Latency** | |
| HIGH | Above 0.7 |
| MODERATE | 0.5 to 0.7 |
| LOW | less than 0.5 |
| **PI** | |
| BEST | Above 20 |
| BETTER | 10 to 20 |
| AVERAGE | 7 to 10 |
| LOW | 3 to 6 |
| WORST | Less than 3 |

Through the comparison shown in Table 5.2, it can be concluded that Vehicle initiated broadcast- Complete path is the best scheme as it reduces communication overhead, latency, and increases packet delivery ration to maximum extent. Next section discusses VIB-CP in detail.

## 5.8 VIB-CP DATA COLLECTION SCHEME IN VANET

As discussed earlier, vehicles in VIB-CP are entirely responsible for decision making whether to send or not any information to RSU. Here, a moving vehicle ($V_n$) stores roadway of complete road segments ($RS_n$) when they pass across the VANET, considering their arrival order relative to $RS_n$. On other hand, the vehicles after reaching their final destination, only work on broadcasting the data having complete path $CP_n$ to surroundings RSUs. The first algorithm shows the action related to vehicles that are part of VIB-CP scheme.

**ALGORITHM 1 ON VEHICLE SIDE($V_n$,$CP_n$[])**

1. for(;n==true;)
2. while $V_n$ keep on proceeding then
3. Get the segment of road $RS_n$;
4. while new fetched $RS_n$
5. Append $RS_n$ in complete path $CP_n$[];
6. end while
7. end while
8. if $V_n$ has reached to its destination then
9. Broadcast ($V_n$,$CP_n$[]) among nearby RSUs;
10. end if
11. end for

As soon as data is fetched by RSU, the complete path related information is inserted by RSU into the database. RSU does not intimate or trigger the vehicles to send the data and thus no beacon message or any timer is required in VIB-CP. Next, in VIB-CP, algorithm 2 reflects the action taken by each RSU.

**ALGORITHM 2 ON RSU SIDE (RSUAddr, LT[][])**

1. for (;n=true;)
2. while($V_n$, $CP_n$[]) is attained then
3. using lane table LT[][]maintain a new entry for $V_n$;
4. Append $CP_n$[] in LT[$V_n$][];
5. end while
6. end for

RSU obtains all the complete paths $CP_n$ information from the moving vehicles that are its range of transmission. According to arrival order of $CP_n$, RSU maintains a lane table (LT) by appending this path information in the lane table. VIB-CP is evaluated as the most likely and best DCS as compared to existing DCS. First disadvantage of VIB-VP is that it sends complete path information to RSU at the end but if this only packet gets lost the whole information is lost. Second disadvantage is that VIB-CP puts no extra efforts for data collection in a secure manner for VANET. Therefore, there are chances that a malicious vehicle may join the network and then sends fake and wrong data to RSU, resulting in bulk data collection at RSU. Moreover, the same malicious activity performing node can transfer data from moving vehicles also that are falling in range of a same RSU. To provide a solution to existing set of problem, an improved DCS is proposed which offers security during data exchange between RSU and vehicles and hence improving network efficiency by limiting the excess of overhead in network.

## 5.9 Proposed IAVIB-DP COLLECTION SCHEME IN VANET

This section introduces DCS, IAVIB-DP for VANET. According to this scheme the vehicle has to perform authentication at RSU to confirm that it is a legitimate one. For enhanced protection, there is a need of the RSU to substantiate that it is certified as well in order to comprise reciprocal verification. A tricky session key could be set up among RSU and vehicle for establishing the subsequent communication during authentication. A time-honored furtive session key could be required so that it synchronize changes both at RSU and vehicle so as to maintain the countermeasures of location confidentiality. When the reciprocated authentication among RSU and vehicle is completed, vehicle may initiate communication with authenticated RSU. On the way to a particular source to destination, Active path table (APt), accumulating the information of new path segments opted by the vehicle gets restructured. After a fixed value of threshold is reached, say ThSo, vehicle start transmitting the APt to RSU. To achieve the optimal length of message threshold is set to 3, otherwise retransmission of messages lost will become cumbersome in situation of lengthy message and will eventually decrease the network throughput. Once the moving vehicle transmit the information of its new path segments to the

RSU in the form of APt, that RSU adds the information of the new path segments to its path lane (PL) list consequently. If a new vehicle originates a message, the identity of that vehicle is included in the RSU database. On the other hand, if a vehicle with existing identity in PL list sends a message, in that case the new path segments mentioned in message are added to the existing paths information of that vehicle. Algorithm 3 represents action of moving vehicle in this proposed scheme and Algorithm 4 represents action of RSU in this proposed scheme. Notations used for writing algorithm 3 and algorithm 4 are shown in Table 5.4.

**Table 5.4: Notations for algorithm 3 and algorithm 4**

| NOTATION | DESCRIPTION |
|---|---|
| $PB_{sp}$ | Service Provider Public Key |
| $PBK_v$ | Vehicle's Public Key |
| $PBK_r$ | RSU's Public Key |
| $PRK_v$ | Vehicle's Private Key |
| $PRK_r$ | RSU's Private Key |
| $S_o$ | Session Key |
| $RK_v$ | Vehicle's Re-encrypt Key |
| $RK_r$ | RSU's Re-encrypt Key |
| $V_i$ | ith Vehicle |
| $RSU_j$ | jth RSU |
| Apt | Active path table |
| $Y_1$ | Random number |
| $Y_2$ | Random number |
| $NPS_g$ | New path segment |

| | |
|---|---|
| $ThS_o$ | Threshold value |
| $T_i$ | time nonce |

**ALGORITHM 3:** Action of Vehicle in the Proposed Scheme

1: Input: $PBK_v$, $PRK_v$, $RK_v$, $RK_r$, $S_o$, $PBK_r$, $PRK_r$, $PB_{sp}$

2: Begin

3: Start Authentication between {$V_i$ and $RSU_j$}

4:Service Provider assign ({$PBK_v$,$PRK_v$,$RK_v$,$S_o$},$t_i$) to $V_i$ and ({$PBK_r$,$PRK_r$,$RK_r$,$S_o$},$t_i$) to $RSU_j$

5: $V_i$ send $PBK_r${$t_1$,$Y_1$,$S_o$} to $RSU_j$

6: $RSU_j$ send $PB_{sp}${$S_o$ ,$Y_1$,$Y_2$,$t_2$} to $V_i$

7: $V_i$ apply $RK_v$ on $PB_{sp}${$S_o$ ,$Y_1$,$Y_2$,$t_2$} to get $PBK_v$ and perform decryption by applying $RK_v$.

8: $V_i$ send $PB_{sp}${$S_o$,$Y_2$,$t_3$} to $RSU_j$

9: $RSU_j$ apply $RK_r$ on $PB_{sp}${$S_o$,$Y_2$,$t_3$} to get $PBK_r$ and perform decryption by applying $PRK_r$.

10: end Authentication

11: SET $ThS_o$=3

12: while $NPS_g$[] is received by authenticated $V_i$ do

13: Add the new Valid entry of $NPS_g$[] to APt[][]

14: if SIZE(APt[][])<$ThS_o$ then

15: update the APt[][]

16: else

17: Send APt[][] to $RSU_j$ and reset APt=Null

18: end if

19: Until $V_i$ halt or reached to destination reiterate steps from 12-18

20. if vehicle halt or reached to destination

21. Send APt[][] to $RSU_j$

21: end while

22: end

**ALGORITHM 4:** Action of RSU in the Proposed Scheme

1: RSU sends beacon message to every vehicle $V_i$ in its vicinity after every 15 seconds.

2: Input: $PBK_v$, $PRK_v$, $RK_v$, $RK_r$, $S_o$, $PBK_r$, $PRK_r$, $PB_{sp}$

2: Begin

3: Start Authentication between {$V_i$ and $RSU_j$}

4:Service Provider assign ({$PBK_v$,$PRK_v$,$RK_v$,$S_o$},$t_i$) to $V_i$ and (f$PBK_r$,$PRK_r$,$RK_r$,$S_o$,$t_i$) to $RSU_j$

5: $V_i$ send $PBK_r${$t_1$,$Y_1$,$S_o$} to $RSU_j$

6: $RSU_j$ send $PB_{sp}${$S_o$ ,$Y_1$,$Y_2$,$t_2$} to $V_i$

7: $V_i$ apply $RK_v$ on $PB_{sp}${$S_o$ ,$Y_1$,$Y_2$,$t_2$} to get $PBK_v$ and perform decryption by applying $PRK_v$.

8: $V_i$ send $PB_{sp}${$S_o$,$Y_2$, $t_3$} to $RSU_j$

9: $RSU_j$ apply $RK_r$ on $PB_{sp}${$S_o$,$Y_2$,$t_3$} to get $PBK_r$ and perform decryption by applying $PRK_r$.

10: end Authentication

11: Start Communication ($RSU_j$)

12: GET APt[][] from $V_i$

13: while APt[][] is retrieved from authenticated $V_i$ do

14: In PL list add the new legal entry of APt[][]

15: if APt[][] is obtained from same $V_i$ then

16: Revise PL list after appending APt[][]

17: else

18: Update PL by adding ne valid entry of APt[][]

19: end if

20: Repeat the steps 12-19 until $V_i$ is in range of RSU

21: end while

22: End

In Table 5.5, comparison of the key features for VIB-CP and proposed IAVIB-DP scheme is made based on the algorithms.

**Table 5.5: Comparison between IAVIB-DP and VIB-CP based on key features**

| Key Features | IAVIB-DP | VIB-CP |
|---|---|---|
| Broadcast Based | Yes | Yes |
| Vehicle initiated | Yes | Yes |
| Authentication | Yes | No |
| Path Collection Type | Dynamic Path-Threshold Based | Complete Path |

According to Table 5.5, VIB-CP and IAVIB-DP are both vehicle initiated and operate in broadcast mode. The difference between VIB-CP and IAVIB-DP is in security feature and the method of collecting path information. IAVIB-DP offers security by using authentication as the initial step before starting actual communication and thus avoiding illegitimate access in the network. IAVIB-DP works on collecting the dynamic path rather than collecting the complete path and thus avoiding the overhead in single packet. Therefore, IAVIB-DP is better in terms of security and DCS in comparison to VIB-CP.

## 5.10 Packet Format for IAVIB-DP

In IAVIB-DP, vehicle sends dynamic path after collecting information for 3 path segments to RSU. RSU maintains this information on database maintained at server attached to it. The packet format used by vehicles for sending the path information to RSU is shown in Figure 5.12 below. Here the packet length is 156 bits including header and dynamic path information.

<table>
<tr><td colspan="2">pCreationTime<br>(6 bits)</td><td colspan="2">PSeqNo<br>(4 bits)</td><td colspan="2">PType<br>(2 bits)</td></tr>
<tr><td colspan="3">Vehicle ID<br>(10 bits)</td><td colspan="3">RSU ID<br>( 2 bits)</td></tr>
<tr><td colspan="3">Source Station<br>(6 bits)</td><td colspan="3">Destination Station<br>(6 bits)</td></tr>
<tr><td colspan="6">$DP_i$<br>( 120 bits)</td></tr>
</table>

**Figure 5.12: Packet Format for IAVIB-DP**

Fields used in packet for collecting path information are detailed below:

- **pCreationTime:** It is the time when the packet is created by the vehicle.
- **pSeqNo:** This is the unique identifier that shows the flow of packets comprising the full path information. For a particular source to destination, if vehicle is sending 5 packets for path collection, then their sequence numbers should be in order.
- **pType:** This value determines whether the packet is beacon packet, information packet, or unusual behavior detection (like accident) packet. If pType is 0, the packet is a beacon message from RSU to all the vehicles in its vicinity. If pType is 1, the packet is sent by vehicle to RSU that contains dynamic path information from a specific station to a destination. If pType is 2, the packet is sent by RSU to vehicle that contains path information from a specific station to a destination. If pType is 3, it contains any unusual activity reporting and alternate path information to be followed at that time.
- **Vehicle ID:** This field contains unique identifier of the vehicle that is collecting path information. It is set to all 1's in case packet is beacon message as it is broadcasted to all vehicles.
- **RSU ID:** This field represents the unique identifier of RSU which is in the vicinity of the vehicle to whom the path information is to be sent.
- **$DP_i$:** If the pType is 0, this field contains the values required for clock synchronization. If pType is 1, this field has the information related to 3 segments that are part of path. If pType is 2, this field has information containing path information sent by RSU. Otherwise, this field has the information of the segment with unusual activity on it.
- **Destination Station and Source Station:** Destination and source station are identifiers of the places for which the path information is being collected by the vehicle. If pType is 0, source address and destination address is set to all 0's.

## 5.11 Comparison of RBRA, INSA, VIB-CP and Proposed IAVIB-DP Scheme

Now, performance evaluation of proposed secure authentication based DCS has been investigated by comparing this scheme with the algorithms VIB-CP [77], RBRA [117], INSA [118].

### 5.11.1 Communication Overhead

The count of messages sent to destination in the execution of one simulation run is termed as communication overhead. Communication overhead is evaluated for the proposed IAVIB-DP scheme and algorithms described in [77],[117]-[118]. It is evaluated by considering all the vehicles and their number of messages sent in the given list for experiments under study. Communication overhead is calculated by taking different number of vehicles in given city network. Numerous different moving vehicles in given city networks are used to calculate communication overhead for this set of executed experiments. These executed experiments worked over the time period of 1000 seconds and vehicles count is set to raise from 100 to 1000 by taking a ultimate raise of 100 vehicles after each run of simulation. The number of messages originated from moving RSUs to moving vehicles and vehicles to RSUs in the given city networks is included in calculation of communication overhead.

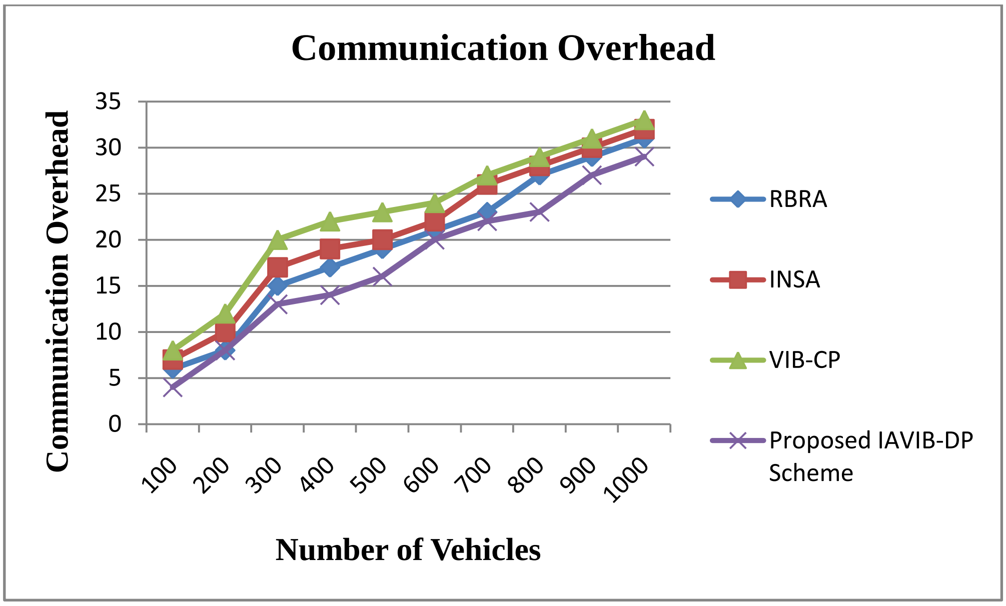


**Figure 5.13: Communication overhead with Different Moving Vehicles**

Figure 5.13 shows communication overhead gained by execution of proposed scheme and algorithms described in [77],[117]-[118] in the above mentioned city networks corresponding to different number of moving vehicles. Communication overhead of proposed scheme is 11% to 22% less than VIB-CP scheme proposed in [77], 0% to 11% less than RBRA scheme proposed in [117], and 5% to 14% less than INSA scheme proposed in [118]. The results after simulation confirms that communication overhead of proposed DCS evaluates to be less as compared to the algorithms described in [77],[117]-[118] as the number of messages are less because the dynamic path information is sent by a vehicle after a set threshold value and the messages due to malicious vehicles are refrained.

### 5.11.2 Packet Delivery Ratio

Packet delivery ratio is evaluated for proposed DCS and algorithms described in [77],[117]-[118]. Figure 5.14 shows that packet delivery ratio gained through execution of proposed scheme and existing algorithms described in [77],[117]-[118] in the above mentioned city networks relative to different number of moving vehicles.

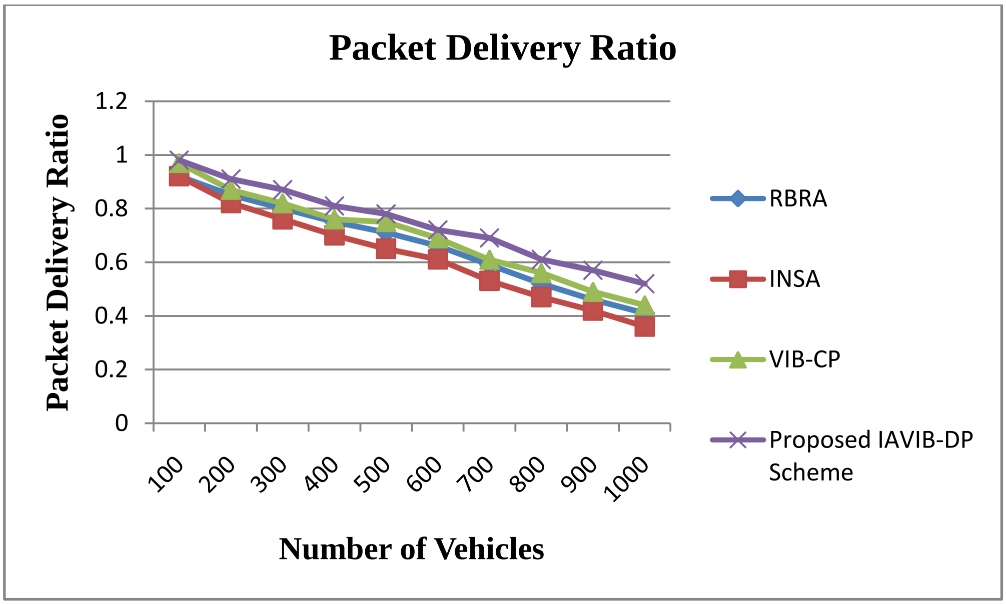


**Figure 5.14: Packet Delivery Ratio with Different moving Vehicles**

Figure 5.14 shows that packet delivery ratio of proposed scheme is 1% to 8% more than VIB-CP scheme proposed in [77], 6% to 11% more than RBRA scheme proposed in [117], and 6% to 16% more than INSA scheme proposed in [118]. The results after simulation confirms that packet delivery ratio of proposed DCS evaluates to be better as compared to the algorithms described in [77],[117]-[118] as due to less congestion in network with legitimate number of users the packets are safely destined to a particular RSU.

### 5.11.3 Throughput

Throughput is measured in messages per second. Figure 5.15 shows the throughput attained by the execution of the proposed scheme and the algorithms described in [77],[117]-[118] in the above mentioned city networks corresponding to different number of moving vehicles.

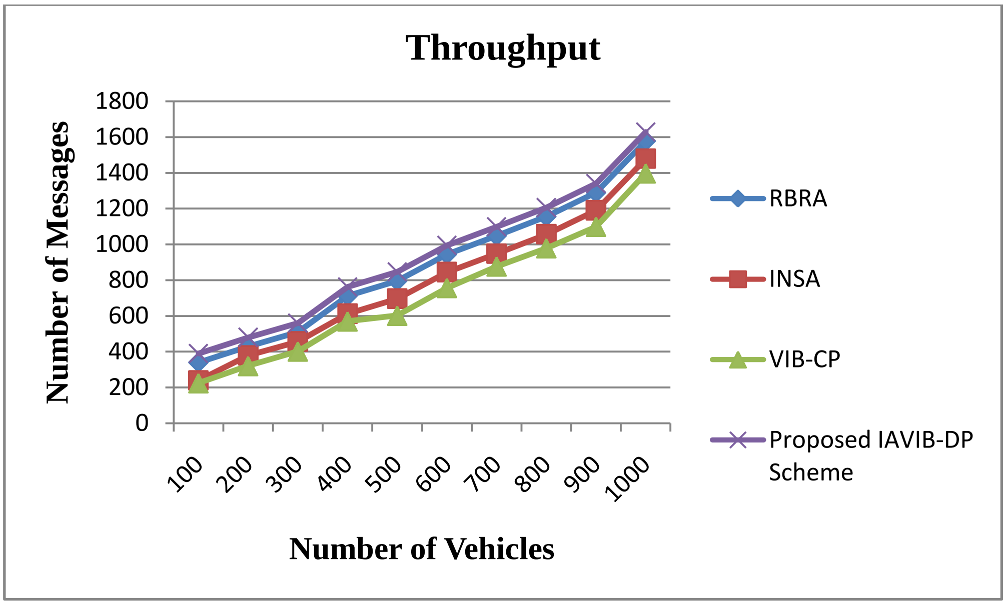


**Figure 5.15: Throughput with Different Moving Vehicles**

Figure 5.15 shows that throughput of proposed scheme is 9% to 14% more than VIB-CP scheme proposed in [77], 2.8% more than RBRA scheme proposed in [117], and 5% to 8.33% more than INSA scheme proposed in [118]. The results after simulation confirms that effective throughput of proposed DCS evaluates to be better as compared to the algorithms described in [77],[117]-[118] as only legitimate users can access the network, therefore congestion is less and hence more messages can be sent per unit of time.

### 5.11.4 Latency

Figure 5.16 shows the latency gained by the execution of the proposed scheme and the algorithms described in [77],[117]-[118] in the above mentioned city networks corresponding to different number of moving vehicles.

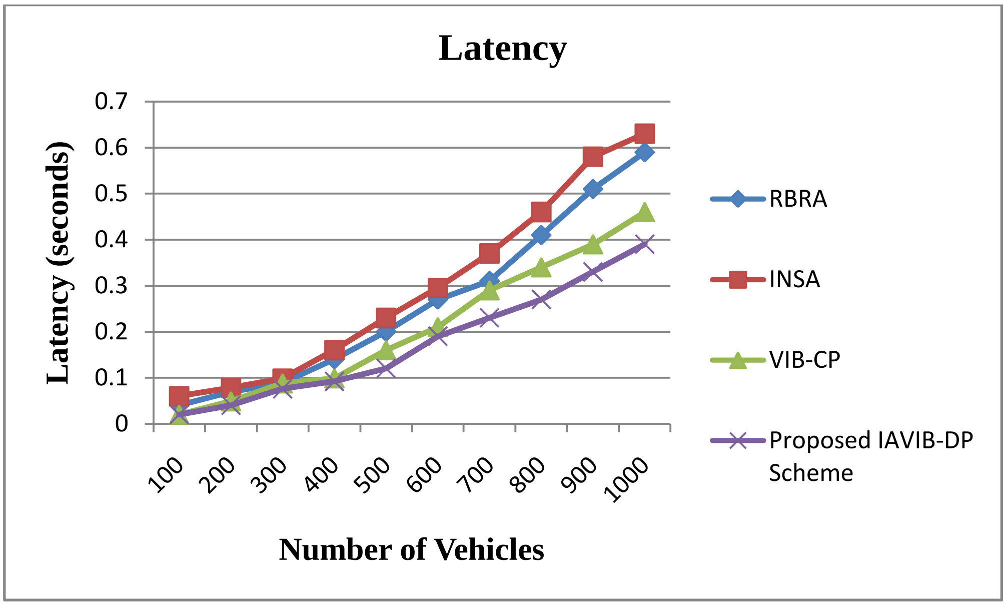


**Figure 5.16: Latency with Different Moving Vehicles**

Figure 5.16 shows that the latency of proposed scheme is 0% to 8.5% less than VIB-CP scheme proposed in [77], 1% to 20% less than RBRA scheme proposed in [117], and 3% to 35% less than INSA scheme proposed in [118].The results after simulation confirms that the latency of proposed DCS evaluates to be less as compared to existing algorithms described in [77],[117]-[118] as the number of messages are less because the dynamic path information is sent by a vehicle after a set threshold value and the messages due to malicious vehicles are refrained.

## 5.12 Summary

Earlier the schemes used for path identification were static and were hardware based. These schemes are not capable of gathering information in unusual situations like accidents or traffic jam. In order to generate effective path in unusual circumstances from a specific source to destination, algorithm based on dynamic DCS is required. Therefore, the existing DCSs are first compared based on communication overhead, packet delivery ratio, and latency. This comparison shows that VIB-CP is best among the existing DCS but it does not offer security while data collection. Therefore, an authentication based dynamic path collection scheme that is intelligent and vehicle initiated is proposed. According to this scheme, vehicle broadcast its APt to all the RSUs in its vicinity after a fixed threshold $ThS_o$. Vehicle reset this APt list and make it empty. Comparative analysis of VIB-CP, RBRA, INSA and proposed scheme is made by evaluating packet delivery ratio, communication overhead, throughput and latency. Results of comparison show that proposed scheme outperforms these existing schemes.

Once the data collection is over, next chapter focus on finding the common and frequent paths opted by the vehicles on distributed RSUs using association rule based mining approach. Finally minimum support and confidence is evaluated for the generated paths.

# CHAPTER 6

# AN ESTIMATION MODEL TO GENERATE PATH MAP FOR VEHICLES IN UNUSUAL ROAD INCIDENTS USING ASSOCIATION RULE BASED MINING IN VANET

This chapter works on filtering the data collected from the proposed IAVIB-DP DCS. From the different paths available from a single source to a specific destination, the best suited path to be followed in a given situation can be determined using logical behavioral arrangements. Support and confidence are evaluated to take the decision on best path map from a specific source to a destination.

## 6.1 Introduction

VANET works to provide wireless communication between vehicles and RSUs and among the vehicles [181]. Offering dedicated short range communication, an external gadget referred as OBU is outfitted with the vehicle that helps to set up communication with RSUs and other moving vehicles in VANET [182]. Safety as well as comfort on path come along in this kind of communication. V2R, V2V, and communication including both V2V and V2R are three distinguished categories of communication used in VANET [183]-[184]. VANET comes with specific set of features like fast dynamic network topology, high mobility, frequent dissection, and many more. In last few years, the research society eagerness has lead to noticeable improvement in VANET. As per the industry and researchers essentially accepted that for enhancing path effectiveness, traffic safety, and decrease ecological force, VANET can be implemented [185]. To estimate flow regulations of traffic and ideal schedules of traffic lights, preconfigured road side units collects data like vehicles speed and traffic frequency and transfers to a centralized server for this estimation [186]. In event of any accident, mobile vehicle even send this information to a RSU. RSU can now generate warning about jam to the ongoing traffic and immediately emergency rescue team can be contacted. Multicast or broadcast schemes for routing are required for these kinds of applications for sending and receiving messages.

One of the important concerns in VANET is to predict the path a vehicle should opt during a journey. There are number of benefits on getting the information related to the path on a destination in advance [187]-[188]. One of these benefits is that the jam level is already available for particular geographic areas on a fixed time of a day. Moreover, back up and barricades can be deliberately placed by the police officers and that may efficiently help in chasing during an escapee by a thief.

For behavior predicting, Logical behavioral arrangements are used in number of areas including medical drug cure behavior, financial reserves, behavior of customer procuring and behavior of robotic motion. Another way of using logical behavioral arrangements is like an approach of data mining for finding relationship between time based incidents or items [189]-[190]. Having the previous sequential arrangements, the future estimate of behavior can be done by continuously monitoring the incidents occurrences and their corresponding tendency of occurring. Logical behavioral arrangements may be utilized to offer an estimation of next expected vehicle's route In VANETs.

The collection of sequential mobility trace data is essential to predict routes by the use of logical behavioral arrangements. Therefore, there is a desire for collecting behavior of the moving vehicles as a proper sequence of path segments traversed by the vehicles on their journey. Data collection using the secure authentication method is implemented to gather the complete information about the paths traversed by the vehicles. The data collected using the above approach related to path segments traversed by a vehicle is transferred to multiple RSUs located on different geographical areas, during the vehicle's ongoing route from a particular local source to a local destination. After gathering the data, RSUs maintain a database containing the information of path segments traversed by all the vehicles. Later, on every individual RSU database, a frequent mining approach is used to find the frequent arrangements for a specific region within a persuaded threshold value. The main motive of doing this is (a) to maintain the past history of vehicle by storing the logical behavioral arrangements already traversed by it and to gather the current information related to path segments being traversed by the vehicle (b) to prepare a drive report in real time for the vehicles using the frequent arrangement data mining approach. A vehicle moving can consider this generated report as visualization for prediction of future path and then rely on the opted path segments.

## 6.2 Logical Behavioral Arrangements Formal Definitions

A formal set of definitions are required to estimate the movement behavior of vehicles moving in VANET, that makes use of logical behavioral arrangements for the route prediction. The customized definitions for illustrating the vehicle's motion arrangements in VANET are:

**Definition (a)**: For a specific map area or a physical region, let $S= \{S_1, S_2, S_3,...., S_i\}$ represents the set of segment of the different path segments that is used to illustrate path intersections and path segments. Definition (a) stated above can be well renowned through Figure 6.1 that represents a sample picture from a map areas or physical region used to illustrate the path intersections and path segments. It can be inferred that a path option offered in a particular path should be called as path segment, on the other hand, any path that is coupled with numerous directions is combined called as a separate path segment. Moreover, two or more path segments concurrently can be connected using a single path intersection.

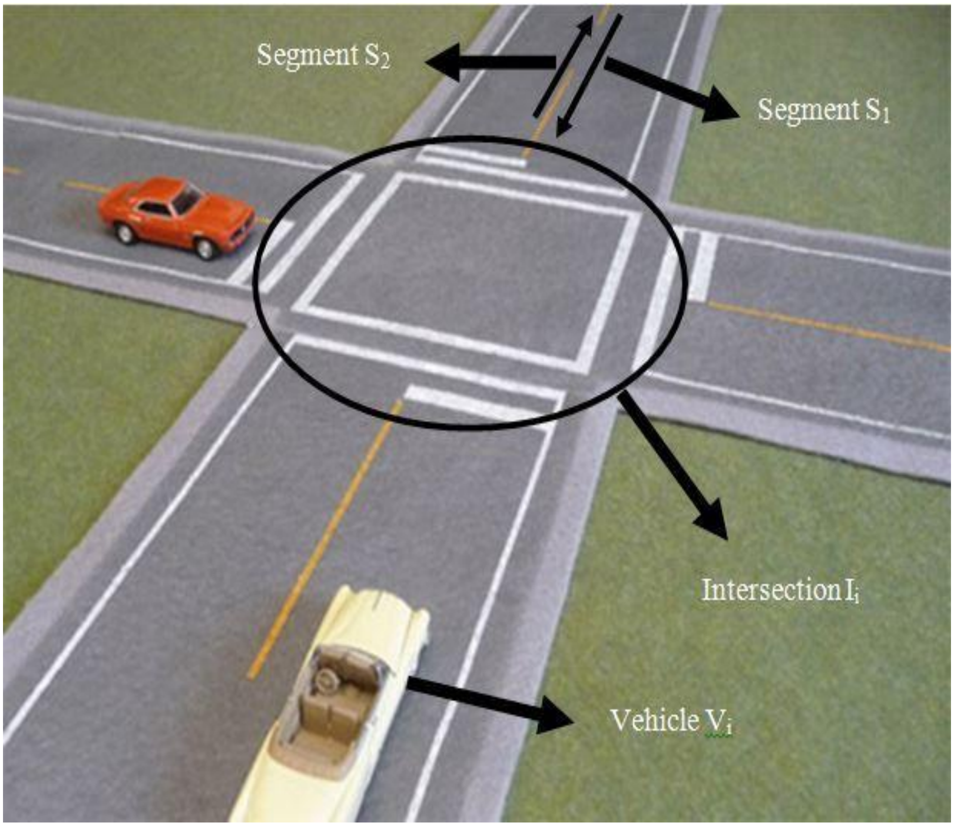


**Figure 6.1: Path Segments and Intersections**

**Definition (b):** For a specific physical area or region, let V= {$V_1$, $V_2$, $V_3$, ……, $V_n$} is the set of moving vehicles during a certain duration of time while moving in that area or region.

**Definition (c):** For a specific physical area or region, let MP= {$S_1$, $S_2$, $S_3$,………,$S_n$} is the set of vehicle's motion arrangement used for representing the traversed path segments by a vehicle $V_i$ while its moving in a specific region provided in the map. This set of vehicle's motion arrangements when they are observed travelling in a given specific region is then maintained in vehicle's motion database as represented through Table 6.1. Therefore, for every vehicle moving in the specified region, an entry is made in this motion specifying the motion arrangements of vehicles.

**TABLE 6.1: Motion Database-1**

| Vehicle Identification ($V_{id}$) | Motion Arrangements |
|---|---|
| $V_1$ | [$S_1$, $S_2$, $S_3$, $S_6$] |
| $V_2$ | [$S_3$, $S_6$, $S_7$, $S_9$] |
| $V_3$ | [ $S_3$, $S_6$, $S_7$, $S_9$, $S_{18}$] |
| …… | …… |
| $V_n$ | [$S_1$, $S_2$, $S_3$, $S_8$,………,$S_n$] |

**Definition (d)**: The frequently happening motion arrangements that may be ordered or their sub arrangements are referred as logical behavioral arrangements. If the elements order is restricted according to the MP arrangements, then a motion arrangement MP= {$S_1$, $S_2$, $S_3$,...,$S_n$} is believed to be sub arrangement of any MP or even as a logical behavioral arrangement. For example, the motion arrangement [$S_2$, $S_3$, $S_5$] is well thought-out to be a sub arrangement of the arrangements [$S_1$, $S_2$, $S_3$, $S_5$, $S_6$] and [$S_0$, $S_1$, $S_2$, $S_3$, $S_5$, $S_6$, $S_8$] but not a sub arrangement of [$S_1$, $S_2$, $S_3$, $S_4$, $S_5$,$S_6$, $S_7$]. In the last arrangement set, all the elements are present but they are following a separate sequence and therefore are not considered as a sub arrangement or logical behavior arrangement.

**Definition (e)**: In the database of motion arrangements, the count of motion arrangements is referred as the support of the motion arrangement MP, symbolized as Support (MP). Here, MP can be recognized as a sub arrangement or logical behavioral arrangement

**Definition (f)*:*** Considering MP= {$S_1$, $S_2$, $S_3$,………,$S_n$} as a motion arrangement. An inference in the manner $MP_1 \Rightarrow MP_2$ is referred as a motion rule R. $MP_1$ and $MP_2$ are opted as the sub arrangements of MP in such a way that they possess different path segments or elements in their respective set (i.e.,$MP_1 \cap MP_2 = \emptyset$). The rule's support is represented as **Support (MP),** where the proportion of motion arrangements available in the motion database having $MP_1 \cup MP_2$ (either taking both motion arrangements ($MP_1$ or $MP_2$) or by taking their union) is used to calculate MP. This can be taken as the probability $P(MP_1 \cup MP_2)$, that defines the motion arrangement probability as the union of $MP_1$ and $MP_2$. Therefore, it contains the information of each path segment that is part of $MP_1$ and $MP_2$. Confidence factor in rule R can be represented as **Confidence (CF).** In a motion database, the proportion of motion arrangements having $MP_1$ that also have $MP_2$ is a measure to build CF. $P(MP_1|MP_2)$ is referred as the conditional probability. Therefore,

$$\text{Support } (MP_1 \Rightarrow MP_2) = P(MP_1 \cup MP_2)$$

$$\text{Confidence } (MP_1 \Rightarrow MP_2) = P(MP_1 \cup MP_2)/P(MP_1)$$

In order to generate motion arrangements, the information about motion behavior (i.e. generated using the motion databases) of vehicle is collected using a secure method is the major concern. Utilizing the arrangements that are predefined and are maintained in the database, rules are generated. Considering the arrangement MP= [$S_2$, $S_3$, $S_5$, $S_6$]. The possible set of rules can be [$S_2$, $S_3$, $S_5$]$\Rightarrow S_6$, [$S_2$] $\Rightarrow$ [$S_3$, $S_5$, $S_6$], [$S_2$, $S_3$]$\Rightarrow$[$S_5$, $S_6$].

## 6.3 Determining the common and most frequent paths by using frequent arrangement mining approach

During the journey of a vehicle from a specific local source to destination, for estimating the most common and frequent paths taken by the vehicles depending on the logical behavioral arrangement, vehicular paths information is collected using the proposed DCS. According to the definitions stated in section 6.2, support and confidence are two major aspects that power up process of data mining using logical behavioral arrangement

### 6.3.1 Support

Arrangement set is the called as the collection of arrangements. On the same side, ***k-arrangement set*** is an arrangement set that contains k arrangements**.** The count of overall executed transactions that includes an arrangement set proves the existence of arrangement set. This can also be referred as support count. Relative support can be given as the second name for the support of arrangement set mentioned in section 6.2. On the other side, the frequency of occurrence is the measure of absolute support. If for an arrangement set MP, its relative support satisfies a pre-decided threshold for minimum support then MP can be confirmed as an arrangement set that is frequent. By choosing the minimum support value as 2, frequent motion arrangements are generated as depicted from example mentioned in Table 6.2-6.8. According to this example, for every vehicle that is moving in a specific region, an entry is maintained in the motion database interpreting its motion arrangements. After merging $MP_{k-1}$ with itself, a combination of candidate K-arrangement sets is generated to finally obtain $MP_K$. Candidates set generated can be represented like $CMP_k$. By examining the motion database in order to get the number of each arrangement and then collecting all these arrangements finally result in a set of frequent1 arrangement sets. This resultant set can be denoted as $MP_1$. Now, $MP_1$ can be used to obtain $MP_2$ that is the frequent 2-arrangement sets that can further be used to obtain $MP_3$ and so on until no more frequent K-arrangement sets are left for determination. To obtain each $MP_k$, a complete scan of motion database is required. A unique attribute referred as Apriori attribute is utilized to interpret the effectiveness of this level wise production of frequent arrangement sets. According to this attribute, for reducing the search space all the subsets that are nonempty should be frequent and must be a part of a frequent arrangement set.

**Table 6.2: Motion Database-2**

| VEHICLE ID | Motion Arrangements |
|---|---|
| $V_1$ | $[S_1,S_2,S_7]$ |
| $V_2$ | $[S_1,S_2,S_4]$ |
| $V_3$ | $[S_1,S_2,S_9]$ |
| $V_4$ | $[S_6,S_2,S_4]$ |
| $V_5$ | $[S_3,S_2,S_4]$ |
| $V_6$ | $[S_1,S_2,S_4]$ |
| $V_7$ | $[S_1,S_2,S_7]$ |
| $V_8$ | $[S_9,S_2,S_4]$ |
| $V_9$ | $[S_5,S_2,S_8]$ |

**Table 6.3: Generating Candidate 1 arrangement sets (CMP(1)) after scanning motion database**

| Arrangement Set | Support Count |
|---|---|
| $S_1$ | 5 |
| $S_2$ | 9 |
| $S_3$ | 1 |
| $S_4$ | 5 |
| $S_5$ | 1 |
| $S_6$ | 1 |
| $S_7$ | 2 |
| $S_8$ | 1 |
| $S_9$ | 2 |

**Table 6.4: Generating MP(1) by comparing minimum support count with candidate1 arrangement sets support count**

| Arrangement Set | Support Count |
|---|---|
| $S_1$ | 5 |
| $S_2$ | 9 |
| $S_4$ | 5 |
| $S_7$ | 2 |
| $S_9$ | 2 |

**Table 6.5: Generating candidate 2 arrangement sets CMP(2) by combining $MP_1$ with itself**

| Arrangement Set | Support Count |
|---|---|
| $[S_1,S_2]$ | 5 |
| $[S_1,S_4]$ | 2 |
| $[S_1,S_7]$ | 2 |
| $[S_1,S_9]$ | 1 |
| $[S_2,S_4]$ | 5 |
| $[S_2,S_7]$ | 2 |
| $[S_2,S_9]$ | 1 |
| $[S_4,S_7]$ | 0 |
| $[S_4,S_9]$ | 0 |
| $[S_7,S_9]$ | 0 |

**Table 6.6: Generating MP(2) by comparing minimum support count with candidate2 arrangement sets support count**

| Arrangement Set | Support Count |
|---|---|
| [$S_1$,$S_2$] | 5 |
| [$S_1$,$S_4$] | 2 |
| [$S_1$,$S_7$] | 2 |
| [$S_2$,$S_4$] | 5 |
| [$S_2$,$S_7$] | 2 |

**Table 6.7: Generating candidate 3 arrangement sets CMP(3) by combining $MP_2$ with itself**

| Arrangement Set | Support Count |
|---|---|
| [$S_1$,$S_2$,$S_4$] | 2 |
| [$S_1$,$S_2$,$S_7$] | 2 |

**Table 6.8: Generating MP(3) by comparing minimum support count with candidate 3 arrangement sets support count**

| Arrangement Set | Support Count |
|---|---|
| [$S_1$,$S_2$,$S_4$] | 2 |
| [$S_1$,$S_2$,$S_7$] | 2 |

A user estimated value of minimum support is required for mining logical behavioral arrangements. Vehicles during their journey to a specific source to a destination identify values of minimum support for all the paths traversed during the journey and record these values along with the frequency rate in the motion database. Consider an example, where the specified minimum support is either equal or may be greater from 2%, then the count of arrangements occurring is featured by their frequency in the motion database with a support of 2%. Here, 2%, 4%, 6%, 8%, 10%, 12% and 14% have been used as minimum support. Considering the above stated minimum support, the frequent motion arrangements generated using proposed DCS is compared with the frequent motion arrangements generated using the existing schemes detailed in [77],[117]-[118].

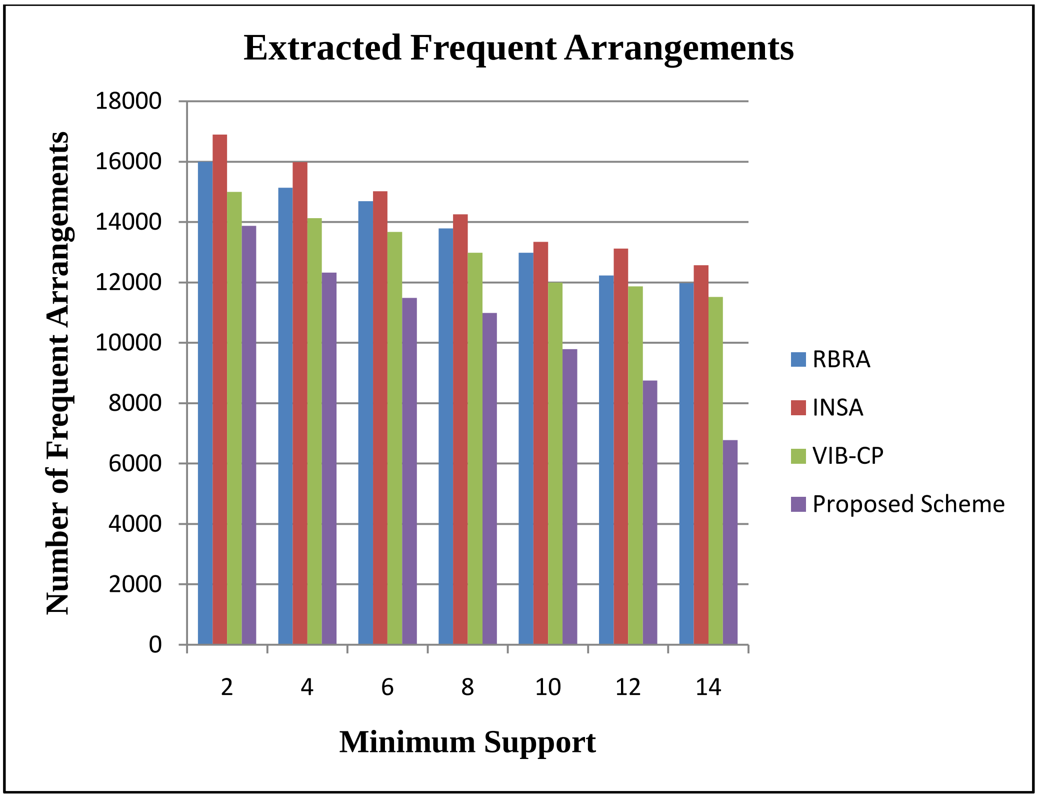


**Figure 6.2: Number of Frequent Motion Arrangements Vs Thershold With Minimum Support**

From the results presented from Figure 6.2, it can be concluded that proposed DCS generates accurate and less frequent motion arrangements in comparison to the schemes detailed in [77],[117]-[118]. With the increase in the minimum support value, the proposed DCS generates 6% to 26% less number of frequent arrangement than [77], 11% to 28% less number of frequent arrangement than [117], and 16% to 32% less number of frequent arrangement than [118]. It has been identified that in motion database, the frequency corresponding to the motion arrangement available as sub arrangements reduces with the increase in value of minimum support. When the value of threshold for minimum support increases from the specified value, the count of motion arrangements having this more minimum support becomes less. Hence, it becomes difficult to extract frequent arrangements as data becomes more sensitive. Therefore, to predict the perfect frequent motion arrangements, the value of minimum supports should be set appropriately.

### 6.3.2 Confidence

Confidence is considered as the next major aspect for mining logical behavioral arrangements and to generate the motion rules. These rules help in identifying the various set of ordered incidents that may occur based on the certain earlier happened order of incidents. Once the logical behavioral arrangements are extracted to produce the number of sub arrangements, motion rules must be generated for all the sub arrangements produced. Confidence in a particular motion rule helps in determining the probability of an incident to occur depending upon the earlier ordered incidents. An intersection shown in Figure 6.3 is taken as the reference example. The different rules generated from the intersection shown in Figure 6.3 are as follow:

- **Rule1:** $S_1 \Rightarrow S_2 \Rightarrow S_8$ (i.e. take U turn)
- **Rule2:** $S_1 \Rightarrow S_2 \Rightarrow S_7$(i.e. turn left)
- **Rule3:** $S_1 \Rightarrow S_2 \Rightarrow S_9$( i.e. moves straight ahead)
- **Rule4:** $S_1 \Rightarrow S_2 \Rightarrow S_4$ (i.e. turn right)
- **Rule5:** $S_6 \Rightarrow S_2 \Rightarrow S_4$ (i.e. take U turn)
- **Rule6:** $S_6 \Rightarrow S_2 \Rightarrow S_8$(i.e. turn left)
- **Rule7:** $S_6 \Rightarrow S_2 \Rightarrow S_7$( i.e. moves straight ahead)
- **Rule8:** $S_6 \Rightarrow S_2 \Rightarrow S_9$ (i.e. turn right)
- **Rule9:** $S_3 \Rightarrow S_2 \Rightarrow S_9$ (i.e. take U turn)
- **Rule10:** $S_3 \Rightarrow S_2 \Rightarrow S_4$(i.e. turn left)
- **Rule11:** $S_3 \Rightarrow S_2 \Rightarrow S_8$( i.e. moves straight ahead)
- **Rule12:** $S_3 \Rightarrow S_2 \Rightarrow S_7$ (i.e. turn right)
- **Rule13:** $S_5 \Rightarrow S_2 \Rightarrow S_7$ (i.e. take U turn)
- **Rule14:** $S_5 \Rightarrow S_2 \Rightarrow S_9$(i.e. turn left)
- **Rule15:** $S_5 \Rightarrow S_2 \Rightarrow S_4$( i.e. moves straight ahead)
- **Rule16:** $S_5 \Rightarrow S_2 \Rightarrow S_8$ (i.e. turn right)

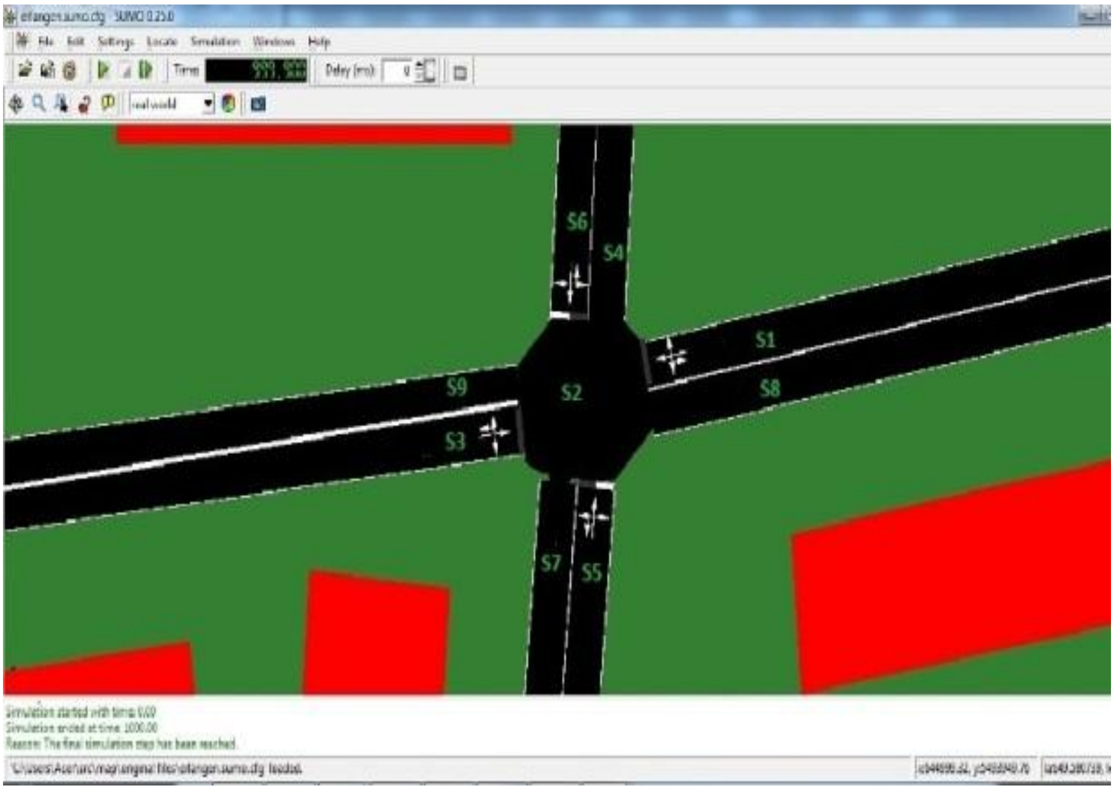


**Figure 6.3: Segment Intersection Scenario**

Confidence in a generated rule is determined by the number of its occurrences. For the existing schemes detailed in [77],[117]-[118] and for proposed DCS, the confidence is evaluated and is compared as shown in Figure 6.4 based on the rules generated above.

From the results it can be depicted that the confidence is much high in proposed DCS as compared to the existing schemes detailed in [77],[117]-[118] evaluated using the above generated rules. As an example, for the proposed DCS the confidence associated with Rule 4 is 43%. This affirms that 43% arrangements have proved that vehicles after crossing the path segments S1 and S2 opt the path segment S4 (right turn).

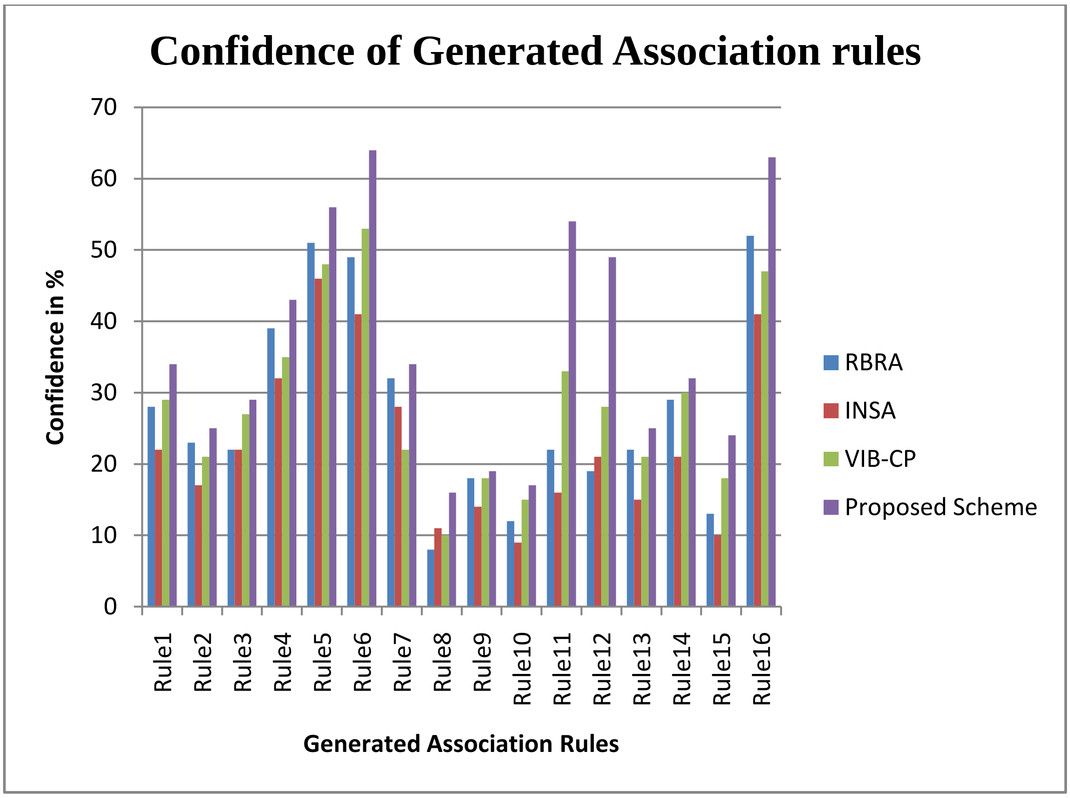


**Figure 6.4: Confidence of Generated Associated Rules**

The results in Figure 6.4 depict that, the confidence level of proposed DCS is 1 to 30% more than existing scheme [77] for different generated rules. The confidence level of proposed DCS is 1 to 45% more than existing scheme [117] for different generated rules. The confidence level of proposed DCS is 7 to 54% more than existing scheme [118] for different generated rules. The confidence of proposed DCS is high because information related to path segments is collected with a set threshold value and in a secure mode. Using this generated confidence of rule, a good prediction can be made. Therefore, confidence level can be used in emergency situations to notify the ambulance to either go straight path or may give an alternate best path according to the day time or during rush hours. It will ultimately help in reducing the delay in case of emergency for an ambulance. Moreover, during a theft, police can generate the confidence in different paths a burglar can opt and then chase him to catch him.

## 6.4 Summary

To analyze the path information traversed by the vehicles, their logical behavior arrangements are captured. For achieving this, first, the data is collected using the proposed authentication based DCS. Later, to determine the most common and frequent paths taken by vehicles, frequent data mining approach is applied on the distributed RSUs. Finally, a comparison is made between the proposed DCS and schemes described in [77],[117]-[118] in terms of support and confidence. Minimum support and high confidence are the two key aspects that determines the acceptance of frequent motion arrangements and hence will improve the decision making process.

# CHAPTER 7

# PERFORMANCE COMPARISON OF PROPOSED SCHEME WITH EXISTING SOLUTIONS DURING AUTHENTICATION, DATA COLLECTION AND PATH MAP GENERATION

This chapter works on performance evaluation and the comparison of existing solutions of authentication, data collection, and path map generation with the proposed solutions of authentication, data collection, and path map generation respectively.

## 7.1 Introduction

First, in this chapter a performance analysis is made among the existing approaches for authentication and the proposed authentication approach based on computational overhead, throughput, packet delivery ratio and average delay. Proposed authentication is further utilized in collecting data from the vehicles on the road. The authentication among vehicles and among vehicle and RSU allows only legitimate users to share the information of road status and thus avoid any unusual scenarios like accidents or traffic jams. Later, a comparative analysis of proposed DCS IAVIB-DP using authentication approach is made with the existing DCSs. Finally, minimum support and confidence for generated path maps is evaluated for existing schemes and the proposed scheme.

## 7.2 Simulation Tool

Veins framework is used in this research work to perform extensive simulation. Veins is preferred over other tools, as its offers a realistic vehicular network simulations using a broad suite of models. Veins make use of SUMO and OMNeT++ for a quick setup and running the simulations in interactive mode. SUMO is responsible for handling the traffic simulation on the road. On the other hand, OMNeT++ takes the responsibility of network simulation. Figure 7.1 shows the mapping of OMNeT++ and SUMO in Veins.

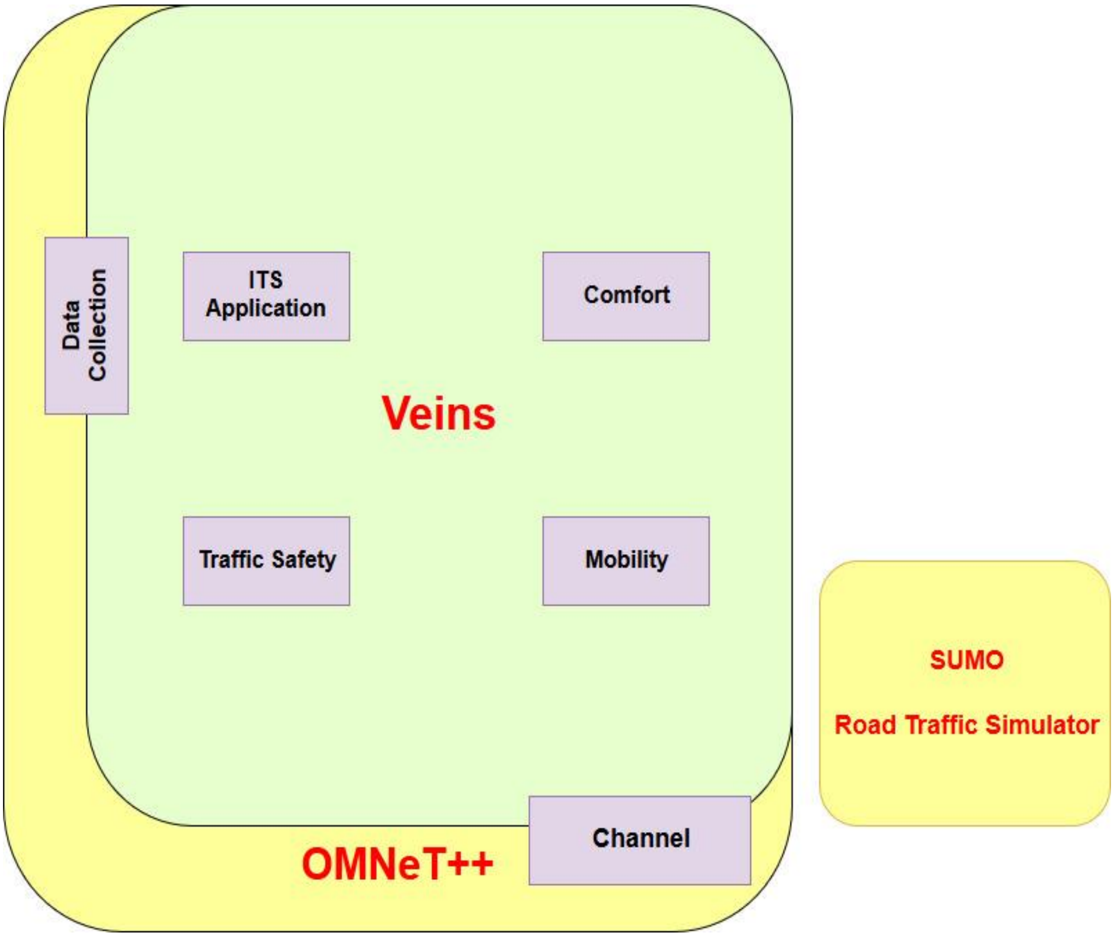


**Figure 7.1: Veins Framework**

## 7.3 Performance Evaluation Parameters

Following parameters are referred in this research work for evaluating the performance of authentication approaches and DCSs

a) **Computational Overhead:** This is the excess time required by any authentication approach for establishing communication in V2v and V2I. The value of computational overhead should be less for an effective scheme and enhances the network performance.

b) **Throughput:** This is calculated as number of packets sent over a period of time. Value of throughput should be high so that more number of packets can be transmitted over a channel. Therefore, for a network to perform well it's throughout should be high.

c) **Packet Delivery Ratio: T**he ratio of all packets that are successfully arrived at destination to all the packets sent is termed as packet delivery ratio. It is used to evaluate the network performance in uneven situations like network congestion. If the value of packet delivery ratio is high, means the network is performing well and its less value indicates the weak network performance.

d) **Communication Overhead:** communication overhead in data collection relies on the number of vehicles and the overall message sent after adding the additional information with them. Communication overhead should be less for any DCS for better network performance.

e) **Latency:** It is the delay in receiving the packet at destination. Latency occurs due to more communication overhead or bandwidth issues. For a network to perform well, its latency should be low.

f) **Average Delay**: If each packet in transmission incurs a different delay, then it results in average delay for that full transmission. Average delay should be less.

## 7.4 Simulation Parameters

This section shows the different simulation parameters used for data authentication, and data collection. In Table 7.1 and 7.2, the simulation parameters considered to execute authentication are mentioned, whereas Table 7.3 shows the simulation parameters considered to execute data collection.

**Table 7.1: Final Traffic Simulation Parameters**

| **Parameter Name** | **Value** |
|---|---|
| Number of Vehicles | 5,10,15,20,25 |
| Maximum Speed | 40 m/s |
| Acceleration | 5m/s2 |
| Deceleration | 8m/s2 |
| Driver Fault | 0.5 |

**Table 7.2: Final Network Simulation Parameters**

| Parameter Name | Value |
|---|---|
| Network Simulator | OMNet++ |
| Simulation Time | 1000 sec |
| Area of Simulation | 1000 meters x 1000meters |
| Simulation Set Up | Random and Cross roads |
| MAC Protocol | IEEE802.11p |
| Range of Transmission | 300 m |

**Table 7.3 Simulation Parameters for Data Collection**

| Parameters | Value |
|---|---|
| Type of Channel | Wireless |
| Type of Network Interface | Physical Wireless Network |
| MAC protocol | IEEE802.11p |
| Communication range | 300m |
| Map Area | 1000*1000sq.m |
| Interface queue type | FIFO queue |
| Queue length | 100 packets |
| Radio Propagation Model | Two ray Ground |
| Number of vehicles | 100- 1000 |
| Speed of vehicle | 40 m/s |
| Number of road and junction segments | 50 |

| | |
|---|---|
| Simulation time | 1000 seconds |
| Map Layout | CityMap |
| Dimension of Space | 1000 m ×1000m |
| Data Payload size | 120 bits/packet |
| Radio Range | 300 m |
| Type of Traffic | Constant Bit Rate |
| Bandwidth of Physical Link | 2 Mbps |
| Scenario | Random mobility |

## 7.5 Comparative Analysis of Proposed Authentication Approach with Existing Approaches

Different authentication approaches are compared in this section with the proposed authentication approach based on computational overhead, throughput, packet delivery ratio, and latency.

a) **Comparison on basis of Computational Overhead:** Computational overhead of the existing authentication approaches in [35],[45],[57],[58],[63],[64],[65] is compared with the proposed approach as shown in Figure 7.2 below.

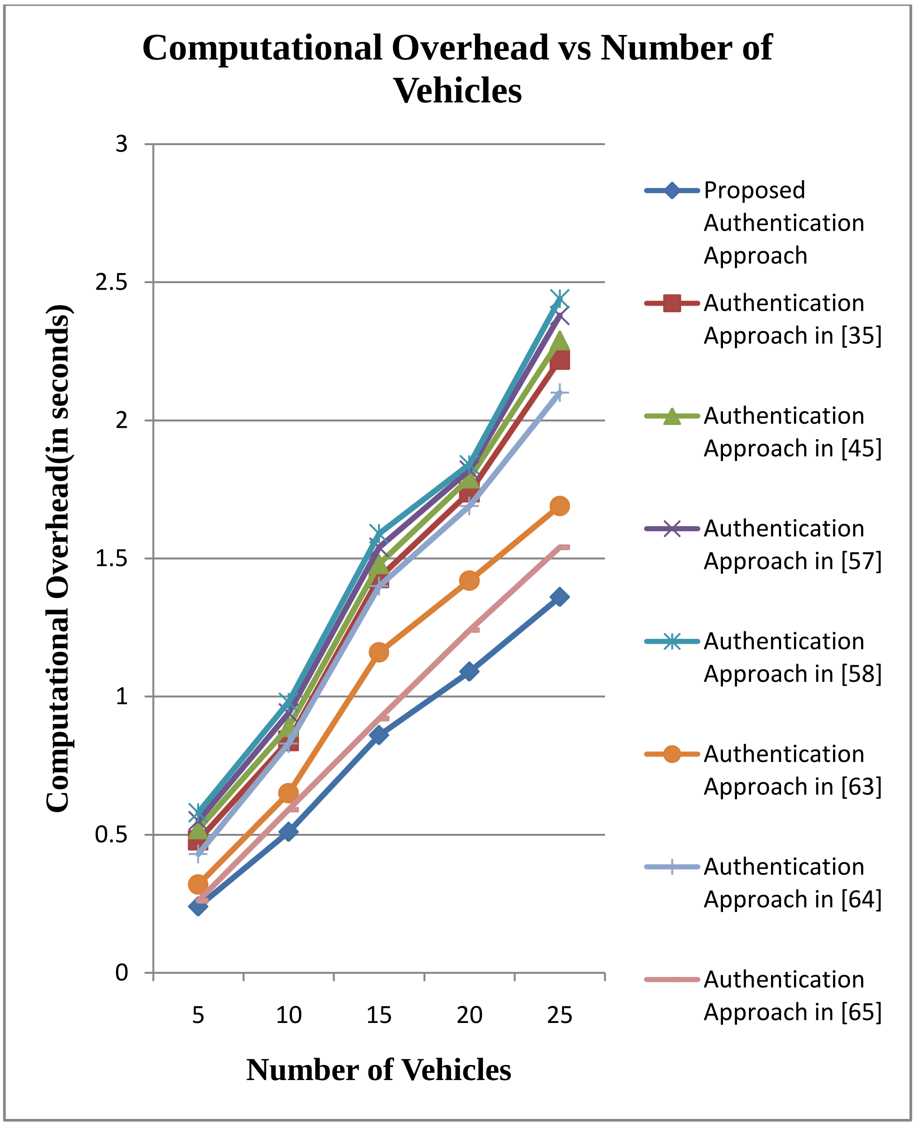


**Figure 7.2: Comparison on basis of Computational Overhead**

Figure 7.2 above shows that the computational overhead of authentication approach proposed is very less as compared to the existing authentication approaches in [35],[45],[57],[58],[63],[64],[65] considering more number of moving vehicles on the road. With the increase in number of vehicles, proposed authentication approach tends to offer less computational overhead than other approaches.

**b) Comparison on basis of Throughput:** Throughput of the existing authentication approaches in [35],[45],[57],[58],[63],[64],[65] is compared with the proposed approach as shown in Figure 7.3 below.

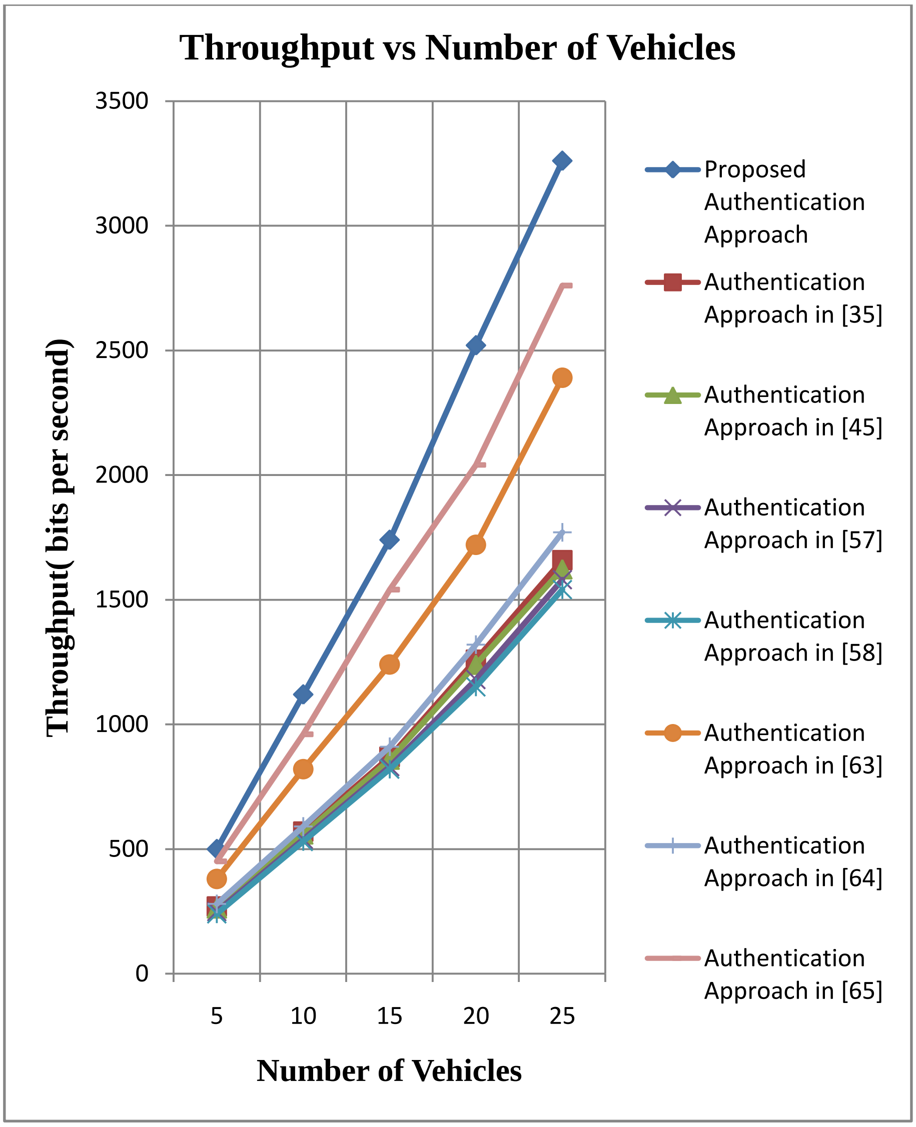


**Figure 7.3: Comparison on basis of Throughput**

Figure 7.3 above represents that the throughput of the proposed authentication approach is very high in comparison to existing authentication approaches in [35],[45],[57],[58],[63],[64],[65] considering more number of moving vehicles. With even these number of moving vehicles, the proposed authentication approach tends to offer high throughput than other approaches.

c) **Comparison on basis of Packet Delivery Ratio:** Existing authentication approaches in [35],[45],[57],[58],[63],[64],[65] is compared with the proposed approach on basis of packet delivery ratio as represented through Figure 7.4 below.

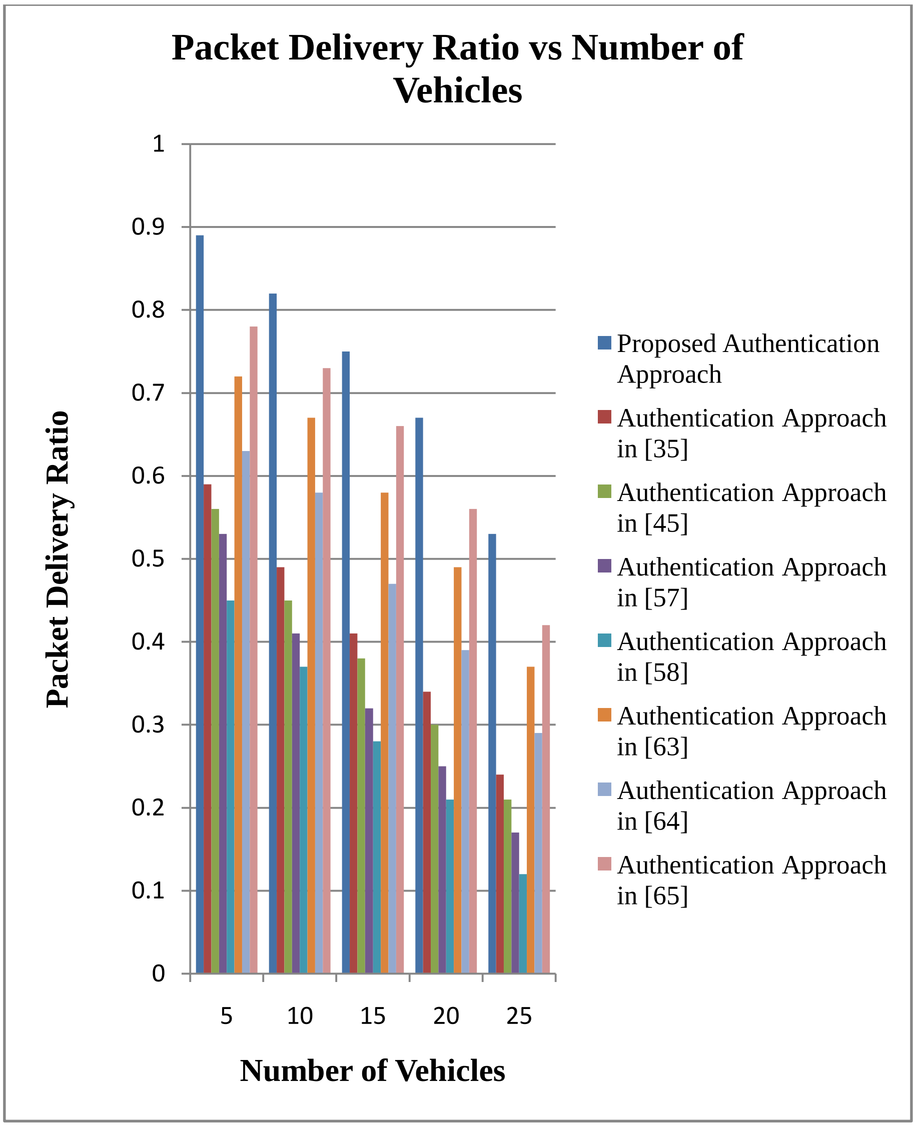


**Figure 7.4: Comparison on basis of Packet Delivery Ratio**

Figure 7.4 above reflects that the packet delivery ratio of the proposed authentication approach is very high in comparison to the existing authentication approaches in [35],[45],[57],[58],[63],[64],[65] considering more number of moving vehicles. With even these number of moving vehicles, the proposed authentication approach tends to offer high Packet Delivery Ratio than other approaches.

d) **Comparison on basis of Average Delay:** Average delay of the existing authentication approaches in [35],[45],[57],[58],[63],[64],[65] is compared with the proposed approach as shown in Figure 7.5 below.

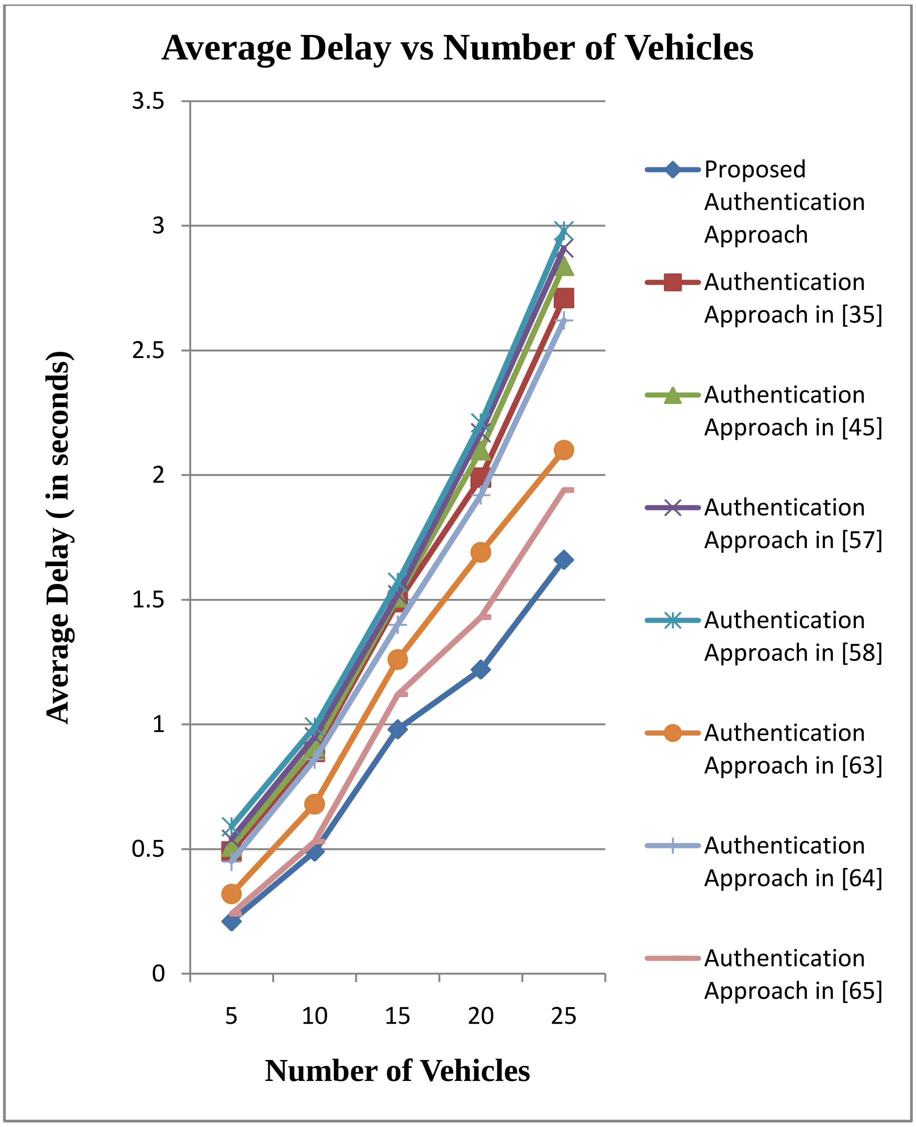


**Figure 7.5: Comparison on basis of Average Delay**

Figure 7.5 above shows that the Average delay of the authentication approach proposed is less in comparison to the existing authentication approaches in [35],[45],[57],[58],[63],[64],[65] considering more number of moving vehicles. With even these numbers of moving vehicles, the proposed authentication approach tends to offer less Average delay than other approaches.

## 7.6 Comparative Analysis of Proposed Data Collection Scheme with Existing Schemes

In this section proposed DCS IAVIB-DP using intelligent authentications is compared with existing DCSs RBRA, INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI on basis of throughput, latency, communication overhead, and packet delivery ratio.

a) **Throughput:** Throughput of existing DCSs RBRA, INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI is compared with the proposed intelligent authentication based IAVIB-DP DCS as shown in Figure 7.6 below.

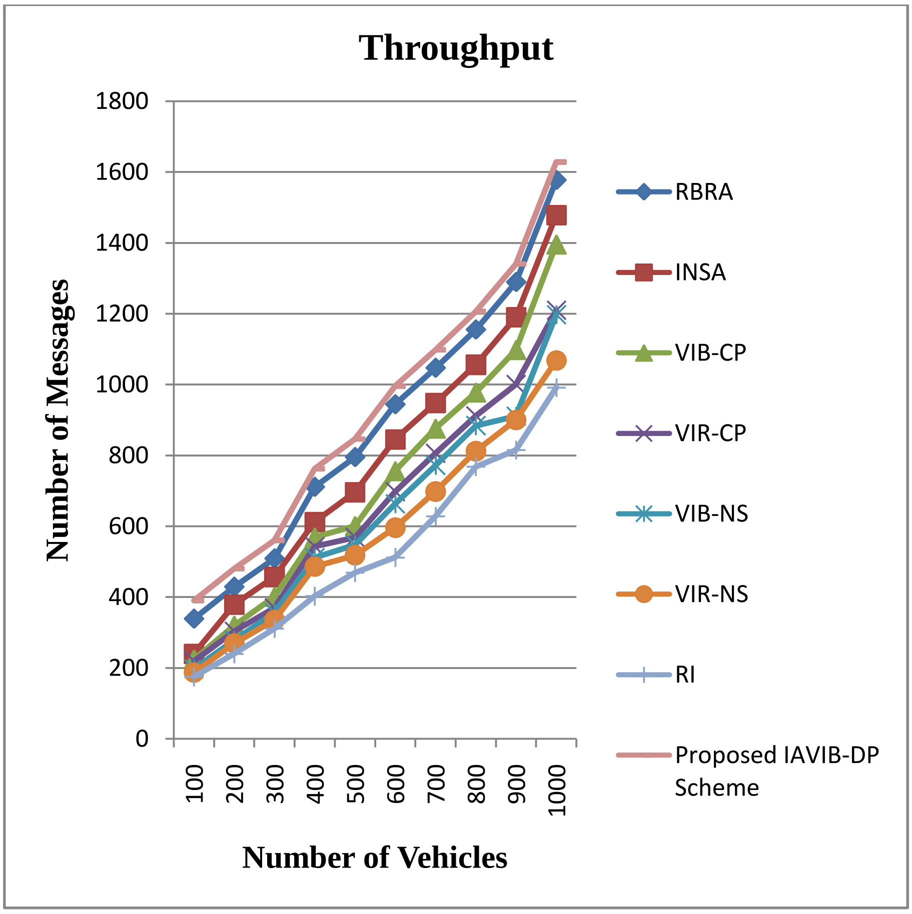


**Figure 7.6: Comparison of Data Collection Schemes on basis of Throughput**

Figure 7.6 above shows that the throughput of the proposed DCS is high in comparison to the existing DCSs like INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI. With even the more number of moving vehicles, the total messages sent over time are gradually increasing for the proposed IAVIB-DP scheme.

b) **Latency:** Latency of the existing DCSs RBRA, INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI is compared with the proposed intelligent authentication based IAVIB-DP DCS as shown in Figure 7.7 below.

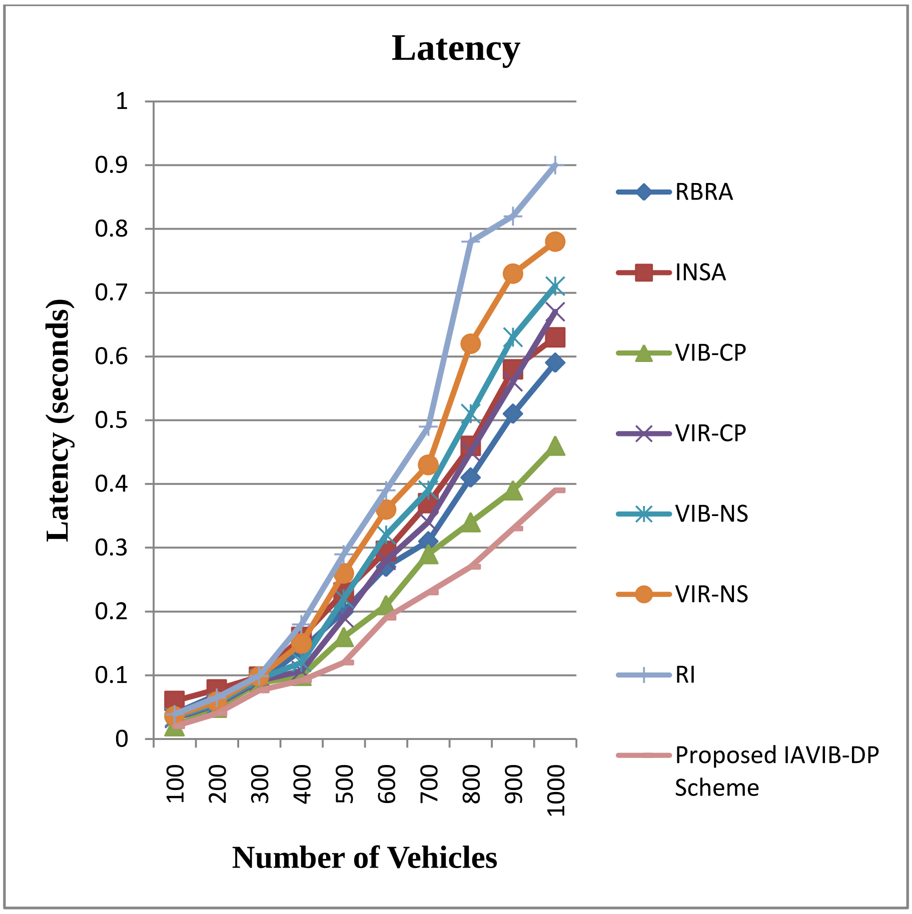


**Figure 7.7: Comparison of Data Collection Schemes on basis of Latency**

Figure 7.7 above shows that the latency of the proposed DCS is less in comparison to the existing DCSs like INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI. With even the increasing number of vehicles, the latency of proposed IAVIB-DP scheme remains low than other schemes.

c) **Packet Delivery Ratio:** For the existing DCSs RBRA, INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI , their packet delivery ratio is compared with the proposed intelligent authentication based IAVIB-DP DCS as shown in Figure 7.8 below.

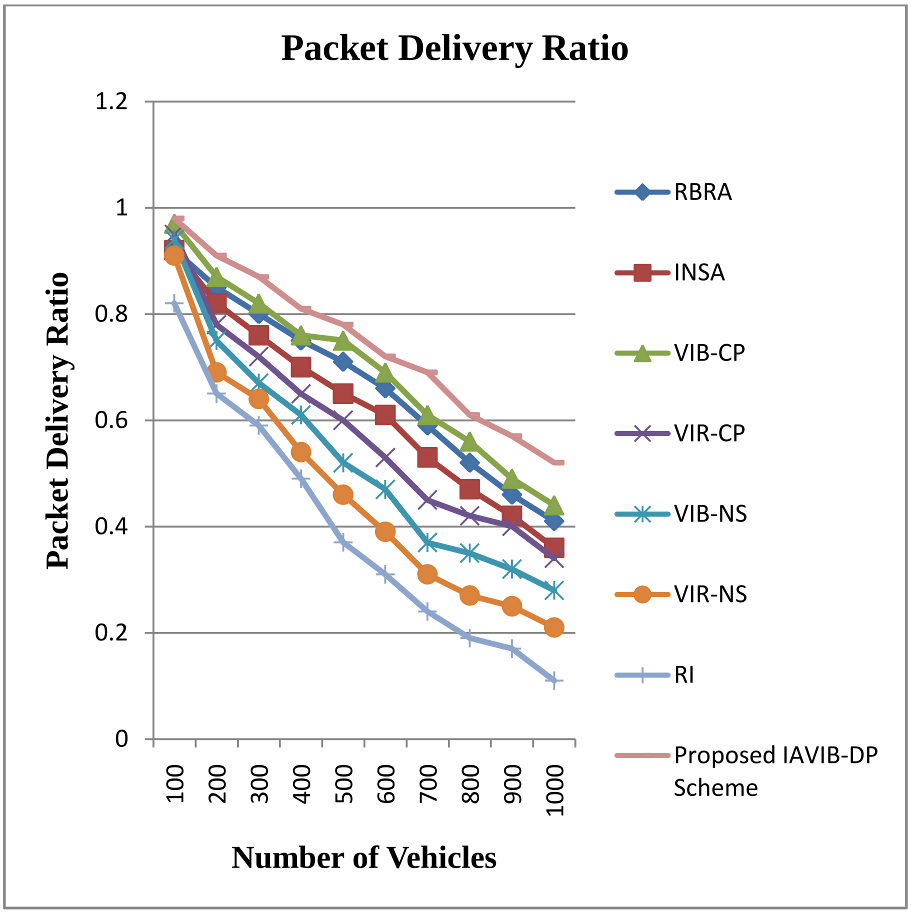


**Figure 7.8: Comparison of Data Collection Schemes on basis of Packet Delivery Ratio**

Figure 7.8 above shows that the Packet Delivery Ratio of the proposed IAVIB-DP DCS is high in comparison to the existing DCSs like INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI. With even increasing the overall vehicles on road, the packet delivery ratio of proposed IAVIB-DP scheme remains high than other schemes.

**d) Communication Overhead:** Communication overhead of the existing DCSs RBRA, INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI is compared with the proposed intelligent authentication based IAVIB-DP DCS as shown in Figure 7.9 below.

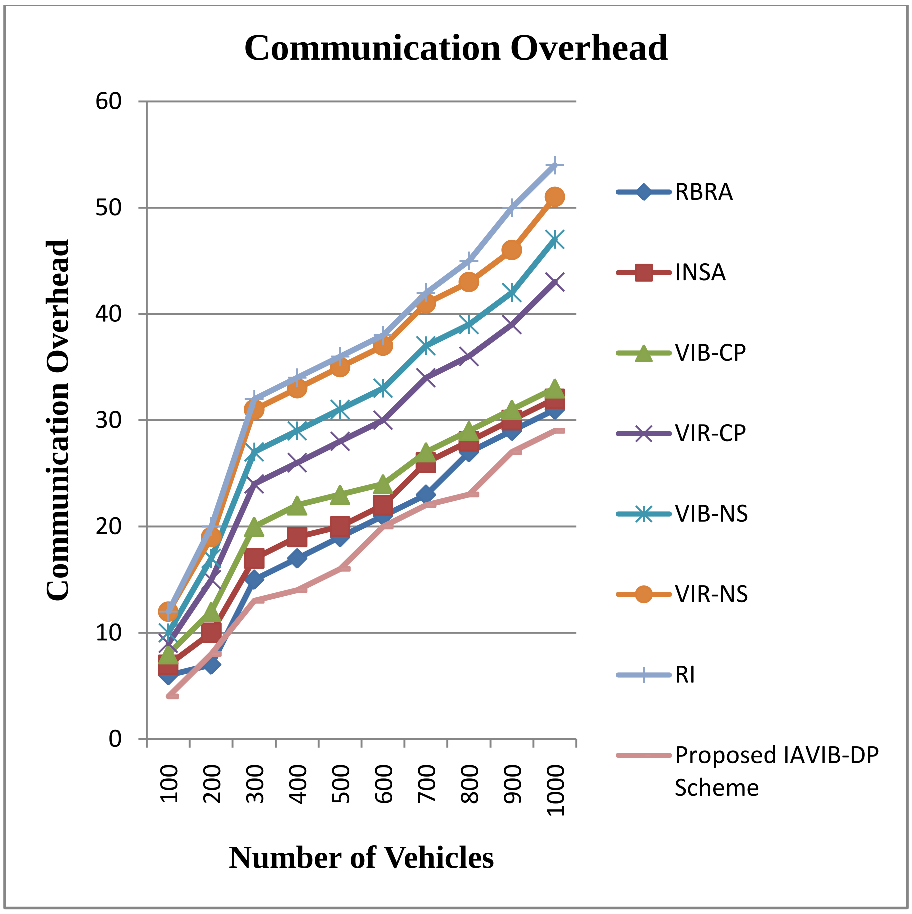


**Figure 7.9: Comparison of Data Collection Schemes on basis of Communication overhead**

Figure 7.9 above shows that the communication overhead of the proposed DCS is less in comparison to the existing DCSs like INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI. With even the increasing number of vehicles, communication overhead of proposed IAVIB-DP scheme remains low than other schemes.

## 7.7 Evaluating Minimum Support and Confidence of Generated Path Maps

The frequent motion arrangements that have been collected by using the proposed DCS IAVIB-DP is compared with frequent motion arrangements collected by the schemes RBRA, INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI as shown in Figure 7.10 below.

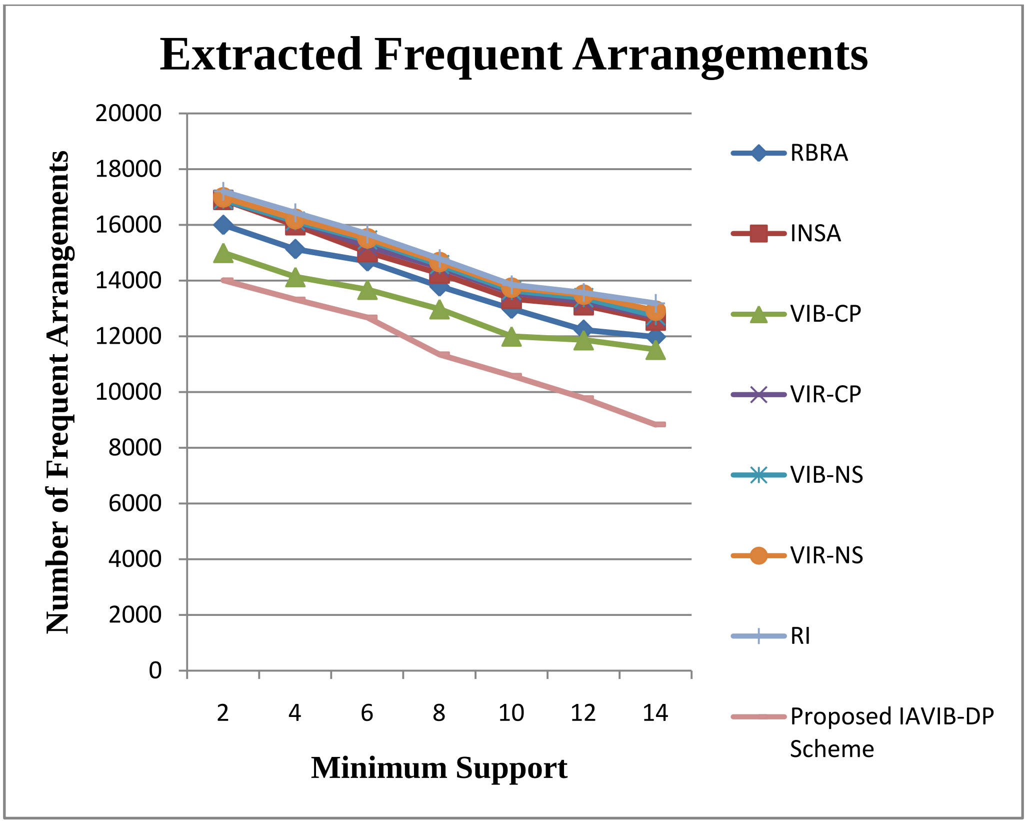


**Figure 7.10: Comparison of number of frequent arrangements with Minimum Support for different data collection schemes**

Considering the results reflected through Figure 7.10, it has been deduced that proposed DCS IAVIB-DP provides more accurate and less frequent motion arrangements as compared to the schemes RBRA, INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI.

The confidence of generated rules using Figure 6.3 in chapter 6 for the proposed DCS IAVIB-DP and the schemes RBRA, INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI is compared in Figure 7.11 below. Results depict that the confidence of the generated rules for the proposed DCS IAVIB-DP is much high as compared to the schemes RBRA, INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI.

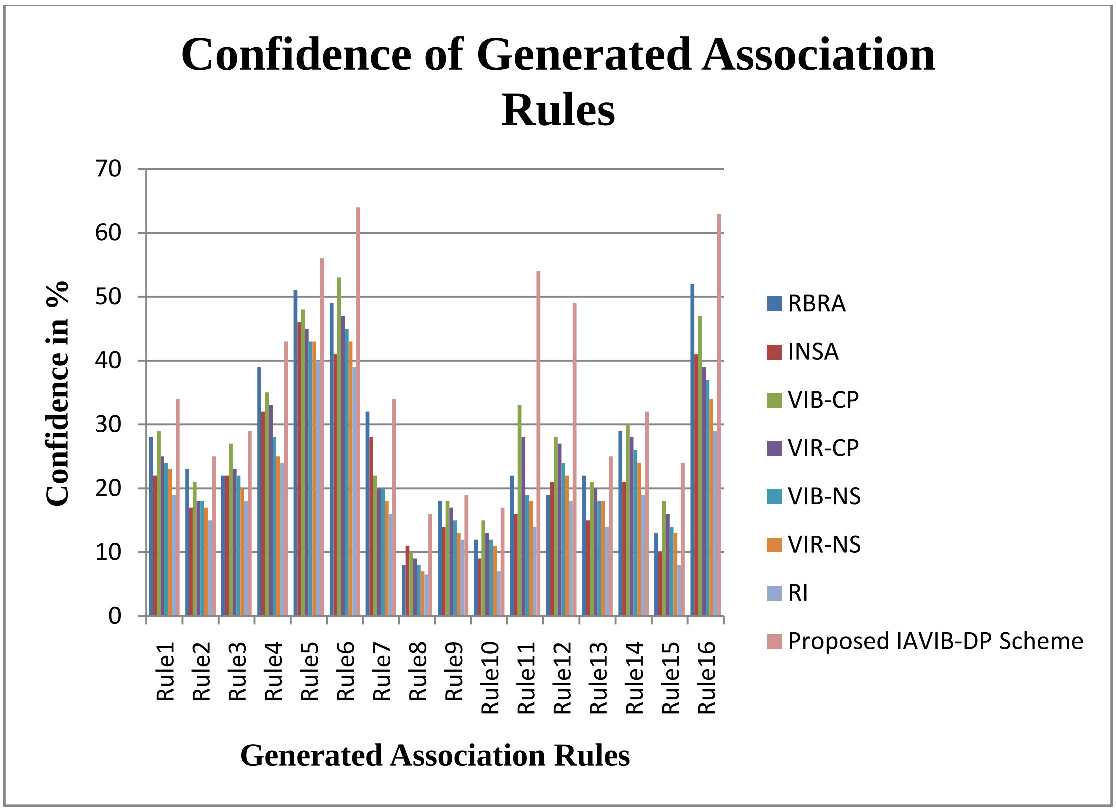


**Figure 7.11: Comparing Confidence of Generated Associated Rules for different data collection schemes**

## 7.8 Summary

This chapter evaluates the performance of the approach proposed for authentication and compares it with existing approaches. It has been discovered that the proposed approach has less computational overhead, less average delay and high throughput and packet delivery ratio in comparison of existing approaches. Later, the proposed intelligent authentication based DCS IAVIB-DP is compared with the existing schemes RBRA, INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI and discovered it to have high throughput, high packet delivery, less communication overhead and less latency than existing schemes. Extracted frequent paths on the basis of minimum support and motion rules on the basis of confidence are compared after collecting data from proposed IAVIB-DP and RBRA, INSA, VIB-CP, VIR-CP, VIB-NS, VIR-NS, and RI are compared. It is deduced that IAVIB-DP outstands other existing schemes as it offers less frequent motion arrangements leading to high confidence.

# CHAPTER 8

# CONCLUSION AND FUTURE SCOPE

Considering the undeniable fact the couple of hours are wasted every year for a human being on the road. Various causes that lead to this situation include road accidents, traffic jam due to rush hours or traffic lights. These events may be avoided by identifying an alternate path at that moment. Therefore, path maps need to be generated from source to destination under different situations on the road. User can pick the best path depending upon the accident, rush hours or during any other unusual event.

This research work aims at generating the efficient path maps on distributed RSUs using data mining approach. To achieve this, this research is divided into three objectives. First objective is, to propose a DCS that tends to improve the throughput, effective packet delivery ratio, and work on minimizing latency. Second objective is, to extract the possible paths from the data collected using association rule base mining on distributed RSUs. Third objective is, to predict the common and most frequent paths on the basis of position, direction, time of day, and during any accident or jam.

## 8.1 Contributions

In the verge of achieving first objective, that is to propose an efficient DCS from the vehicles, a detailed survey is conducted on existing DCSs. The existing DCSs do not assure security in terms of authenticity and are vulnerable to number of attacks like DoS. Therefore, a reliable and secure authentication process is required that must be incorporated before collecting data from the vehicles on the road. Several authentication process exist in literature, for example, digital signature, pairing, IRE, and many more. But, these are still vulnerable to attacks like DoS, masquerading, eavesdropping. Moreover, they do not provide V2I and inter RSU authentication separately. Therefore, discrete event based threat driven authentication approach has been proposed. This authentication approach utilizes asymmetric cryptography, re-encrypt key and time based arbitrary numbers to offer authentication among the vehicles on road and between RSUs and vehicles. The proposed authentication approach is analyzed by using Petri Nets and Veins framework. With the help of Petri nets model and its reachability graph, it has been observed that the proposed authentication approach acquires the reachability and liveness property. By working on Veins framework, observation was made on proposed authentication approach working better as compared to existing authentication approaches.

Once complete authentication process is over and trust is established among the vehicles and the RSUs, the next step is to initiate the data collection process from the vehicles on the road and maintain the data on RSUs. To figure out the data collection mechanism, the existing DCSs are evaluated based on their communication overhead, packet delivery ratio, and latency. Later, PI is evaluated for each DCS and based on the result it can be deduced that among all existing DCS, PI **of** VIB-CP is the highest as it has less communication overhead, high packet delivery ratio, and low latency. But VIB-CP do not provide authentication support, therefore, IAVIB-DP is proposed to offer authentication between RSU and vehicle before startup. According to this scheme, vehicle after a fixed threshold say ThSo broadcasts its $AP_t$ list to every adjacent RSUs and then reset the $AP_t$ list to NULL. VIB-CP and IAVIB-DP are evaluated and compared on basis of packet delivery ratio, communication overhead, and latency. Results of comparison reflect that IAVIB-DP is better in comparison to VIB-CP as it has low latency, high packet delivery ratio, and less communication overhead.

After the data is collected from different moving vehicles using secure DCS, a database is maintained for different possible paths from a particular source to a given destination. Using this pool of information, final decisions are to be made for choosing the best path in any unusual situation like accident, morning rush hours, patient having critical condition in ambulance etc. For doing so, logical behavioral arrangements of vehicles are captured to analyze the information about the paths traversed by the vehicles. Afterwards, frequent mining approach is used to fetch the common and frequent paths opted by the vehicles during their journey for path predictions. Proposed scheme in this research work is well compared with existing schemes mentioned in [77],[117]-[118] on the basis of extracted frequent motion arrangements and confidence of the association based rules. Association based rules are generated by applying constraints from the selected arrangements. Minimum support and confidence is required to accept the arrangements for further decision making.

This research work helps the novice to avoid delay by providing a smart way of getting the best path map at particular time of day and in case of unusual situations such as accident, morning rush hours, patient having critical condition in ambulance, and many more.

## 8.2 Future Scope

With the change in trend of lifestyle in the fast moving world of technology, people on road want to reach their destination in shorter span of time and on the best path way. VANET is providing solutions to warn moving vehicles regarding unusual events like accidents on jams on road. Moreover, people on road want the optimal path to be picked during these events.

This research work tends to improve the mechanism used to figure out best path along a road starting from a specific source and ending at a specific destination. Staking at future, VANET is more likely to provide incompatible solutions for time saving along with the safety

Considering the future aspect in VANET, to offer extra security with increase in potential throughput and minimizing the effect of delay, a variety of operations of data transmission can be evaluated in VANETs by implementing more efficient encryption strategies. The research work carried out inspires the novice to go for the best scheme available for collecting data in VANET. Additional security services such as integrity and confidentiality can be offered to the transmitted data by incorporating them in the proposed IAVIB-DP scheme

Moreover, this research work can be further extended in different application and project areas like smart vehicle, smart city, vehicle cloud, automated vehicle behavior standardization.

# LIST OF PUBLICATIONS

1. A. Malik, and B. Pandey, "Comparison of data mining techniques used in Vehicular Ad-hoc Networks." In Skillcon: National Conference on Management and Technology for Skill Developments, 2014.
2. A. Malik, and B. Pandey, "Performance analysis of various data collection schemes used in VANET." *Indian Journal of Science and Technology* 8, no. 15 (2015).
3. A. Malik, and B. Pandey, "An intelligent authentication based vehicle initiated broadcast-dynamic path data collection scheme in VANET." *Indian Journal of Science and Technology*9, no. 16 (2016).
4. A. Malik, and B. Pandey, "Performance analysis of enhanced authentication scheme using re-key in VANET." In *Cloud System and Big Data Engineering (Confluence), 2016 6th International Conference*, pp. 591-596. IEEE, 2016.
5. A. Malik, B. Pandey, and A. Gul, "A Novel Congestion Control Scheme in VANET." In *Computer Communication, Networking and Internet Security*, pp. 595-602. Springer, Singapore, 2017.
6. A. Malik, and B. Pandey, "Asymmetric encryption based secure and efficient data gathering technique in VANET." In *Cloud Computing, Data Science & Engineering-Confluence, 2017 7th International Conference on*, pp. 369-372. IEEE, 2017.
7. A. Malik, and B. Pandey, "An Efficient and Reliable Data Gathering Protocol Based on RSU Identification." In *Advanced Informatics for Computing Research*, pp. 343-354. Springer, Singapore, 2017.
8. A. Malik, and B. Pandey, "CIAS: A Comprehensive Identity Authentication Scheme for Providing Security in VANET." *International Journal of Information Security and Privacy (IJISP)* 12, no. 1 (2018): pp. 29-41.
9. A. Malik, and B. Pandey, "Security Analysis of Discrete Event Based Threat Driven Authentication Approach in VANET using Petri Nets." *International Journal of Network Security (IJNS)* 20, no. 4 (2018): pp. 601-608.
10. A. Malik, B. Pandey, and C. C Wu, "A Secure Model to Generate Path Map for Vehicles in Unusual Road Incidents using Association Rule Based Mining in VANET." *Journal of Electronic Science and Technology* (Accepted)**.**

11. A. Malik, and B. Pandey, "Security Vulnerabilities and Solutions in VANET: A Systematic Survey and Analysis."*Ad Hoc Networks* (Communicated).

# REFERENCES


[1] I. Chlamtac, M. Conti, and J. Liu, "Mobile ad hoc networking: imperatives and challenges." *Ad hoc networks* 1, no. 1 (2003): 13-64

[2] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An overview of mobile ad hoc networks: applications and challenges." *Journal-Communications Network* 3, no. 3 (2004): 60-66.

[3] L. Zhou, and Z.J. Haas, "Securing ad hoc networks." *IEEE network* 13, no. 6 (1999): 24-30.

[4] T. Leinmüller, L. Buttyan, J.P. Hubaux, F. Kargl, R.. Kroh, P. Papadimitratos, M. Raya, and E. Schoch, "Sevecom-secure vehicle communication." In *IST Mobile and Wireless Communication Summit*, no. LCA-POSTER-2008-005. 2006.

[5] S. Zeadally, R. Hunt, Y.S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges." *Telecommunication Systems*50, no. 4 (2012): 217-241.

[6] A. Festag, G. Noecker, M. Strassberger, A. Lübke, B. Bochow, M.T. Moreno, S. Schnaufer, R. Eigner, C. Catrinescu, and J. Kunisch, "'NoW–network on wheels': Project objectives, technology and achievements." (2008).

[7] M. Mejri, J.B. Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions." *Vehicular Communications* 1, no. 2 (2014): 53-66.

[8] B. Pan, and H. Wu, "Analysis of Safety Messages Delivery in Vehicular Networks With Interconnected Roadside Units." *IEEE Access* 5 (2017): 24873-24883.

[9] D. Gantsou, "VANET Security: Going Beyond Cryptographic-Centric Solutions." In *Vehicular Ad-hoc Networks for Smart Cities*, pp. 43-49. Springer, Singapore, 2015.

[10] K. Verma, H. Hasbullah, and A. Kumar, "Prevention of DoS attacks in VANET." *Wireless personal communications* 73, no. 1 (2013): 95-126.

[11] S.K. Dhurandher, M.S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Vehicular security through reputation and plausibility checks." *IEEE Systems Journal* 8, no. 2 (2014): 384-394.

[12] Y. Kim, I. Kim, and C.Y. Shim, "A taxonomy for DOS attacks in VANET." In *Communications and Information Technologies (ISCIT), 2014 14th International Symposium on*, pp. 26-27. IEEE, 2014.

[13] S. Panichpapiboon, and W.P. Atikom, "A review of information dissemination protocols for vehicular ad hoc networks." *IEEE Communications Surveys & Tutorials* 14, no. 3 (2012): 784-798

[14] R. Hussain, and H. Oh, "On secure and privacy-aware sybil attack detection in vehicular communications." *Wireless personal communications* 77, no. 4 (2014): 2649-2673.

[15] N. Varshney, T. Roy, and N. Chaudhary, "Security protocol for VANET by using digital certification to provide security with low bandwidth." In *Communications and Signal Processing (ICCSP), 2014 International Conference on*, pp. 768-772. IEEE, 2014.

[16] S. Du, and H. Zhu, "Modelling of Multiple Phased Attack on VANET Security." In *Security Assessment in Vehicular Networks*, pp. 35-42. Springer New York, 2013.

[17] C.L. Chen, I.C. Chang, C.H. Chang, and Y.F. Wang, "A secure ambulance communication protocol for VANET." *Wireless personal communications* 73, no. 3 (2013): 1187-1213.

[18] H. Ghaffarian, M. Soryani, and M. Fathy, "Planning VANET infrastructures to improve safety awareness in curved roads." (2012).

[19] A. Zhou, J. Li, Q. Sun, C. Fan, T. Lei, and F. Yang, "A security authentication method based on trust evaluation in VANETs." *EURASIP Journal on Wireless Communications and Networking* 2015, no. 1 (2015): 1-8.

[20] I. Bhattacharya, S. Ghosh, and D. Show, "An efficient and secured routing protocol for VANET." In *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*, pp. 775-783. Springer, Cham, 2015.

[21] C. Deng, "Towards a Trusted Vehicular Routing in VANET." In *Information Technology Convergence, Secure and Trust Computing, and Data Management*, pp. 103-117. Springer, Dordrecht, 2012.

[22] S. DasGupta, R. Chaki, and S. Choudhury, "TruVAL: trusted vehicle authentication logic for VANET." In *Advances in Computing, Communication, and Control: Third International Conference, ICAC3 2013, Mumbai, India, January 18-19, 2013, Proceedings*, vol. 361, p. 309. Springer, 2013.

[23] P. Dharani, S.S. Chakkaravarthy, M. Ganesan, E. Kamalanaban, P. Visu, P.R. Patil, and C. Mahesh, "An Unidentified Location-Based Efficient Routing Protocol in VANET." In *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*, pp. 415-421. Springer, New Delhi, 2015.

[24] X. Feng, C.Y. Li, D.X. Chen, and J. Tang, "EBRS: event based reputation system for defensing multi-source sybil attacks in VANET." In *International Conference on Wireless Algorithms, Systems, and Applications*, pp. 145-154. Springer, Cham, 2015.

[25] M. Franeková, and P. Lüley, "Security of digital signature schemes for Car-to-Car communications within intelligent transportation systems." In *International Conference on Transport Systems Telematics*, pp. 258-267. Springer, Berlin, Heidelberg, 2013.

[26] J. Grover, V. Laxmi, and M.S. Gaur, "Misbehavior Detection Based on Ensemble Learning in VANET." In *ADCONS*, pp. 602-611. 2011.

[27] Y. Han, D. Fang, Z. Yue, and J. Zhang, "SCHAP: The Aggregate SignCryption Based Hybrid Authentication Protocol for VANET." In *International Conference on Internet of Vehicles*, pp. 218-226. Springer, Cham, 2014.

[28] D. Gantsou, and P. Sondi, "Toward a honeypot solution for proactive security in vehicular ad hoc networks." In *Future Information Technology*, pp. 145-150. Springer, Berlin, Heidelberg, 2014.

[29] H.T. Wu, and W.S. Hsieh, "RSU-based message authentication for vehicular ad-hoc networks." *Multimedia tools and applications* 66, no. 2 (2013): 215-227.

[30] T. Zhou, R.R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP—Sybil attacks detection in vehicular ad hoc networks." *IEEE journal on selected areas in communications* 29, no. 3 (2011): 582-594.

[31] S. Taha, and X. Shen, "A physical-layer location privacy-preserving scheme for mobile public hotspots in NEMO-based VANETs." *IEEE Transactions on Intelligent Transportation Systems* 14, no. 4 (2013): 1665-1680.

[32] D. Goldschlag, M. Reedy, and P. Syversony, "Onion Routing for Anonymous and Private Internet Connections January 28-1999."

[33] J. Boyan, "The anonymizer-protecting user privacy on the web." (1997).

[34] S. Taha, S. Céspedes, and X. Shen, "EM 3 A: Efficient mutual multi-hop mobile authentication scheme for PMIP networks." In *Communications (ICC), 2012 IEEE International Conference on*, pp. 873-877. IEEE, 2012.

[35] M. Kaur, and P. Singh, "Performance evaluation of V2Vcommunication by implementing security algorithm in VANET." *Advances in Computing and Information Technology* (2012): 757-763.

[36] M. Kim, W. Choi, A. Lee, and M.S. Jun, "PUF-Based Privacy Protection Method in VANET Environment." In *Advances in Computer Science and Ubiquitous Computing*, pp. 263-268. Springer, Singapore, 2015.

[37] C. Cremers, K.B. Rasmussen, B. Schmidt, and S. Capkun, "Distance hijacking attacks on distance bounding protocols." In *Security and Privacy (SP), 2012 IEEE Symposium on*, pp. 113-127. IEEE, 2012.

[38] C.C. Lee, and Y.M. Lai, "Toward a secure batch verification with group testing for VANET." *Wireless networks*19, no. 6 (2013): 1441-1449.

[39] J.L. Huang, L.Y. Yeh, and H.Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks." *IEEE Transactions on Vehicular Technology* 60, no. 1 (2011): 248-262.

[40] J.S. Li, and K.H. Liu, "A lightweight identity authentication protocol for vehicular networks." *Telecommunication Systems* 53, no. 4 (2013): 425-438.

[41] C. Zhang, R. Lu, P.H. Ho, and A. Chen, "A location privacy preserving authentication scheme in vehicular networks." In *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, pp. 2543-2548. IEEE, 2008.

[42] A. Ltifi, A. Zouinkhi, and M.S. Bouhlel, "A cooperation based scheme for managing alert propagation in vanet." *Wireless Personal Communications* 85, no. 4 (2015): 2211-2231.

[43] Z. Wang, and C. Chigan, "Cooperation enhancement for message transmission in VANETs." *Wireless Personal Communications* 43, no. 1 (2007): 141-156.

[44] R.V. Pradweap, and R.C. Hansdah, "A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET." In *International Conference on Information Systems Security*, pp. 314-328. Springer, Berlin, Heidelberg, 2013.

[45] B. Bhavesh, S. Maity, and R.C. Hansdah, "A protocol for authentication with multiple levels of anonymity (AMLA) in VANETs." In *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on*, pp. 462-469. IEEE, 2013.

[46] P. Remyakrishnan, and C. Tripti, "A novel approach for enhancing the security of user authentication in VANET using biometrics." In *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2*, pp. 299-306. Springer, Cham, 2015.

[47] L. Malina, A. Vives-Guasch, J. Castellà-Roca, A. Viejo, and J. Hajny, "Efficient group signatures for privacy-preserving vehicular networks." *Telecommunication Systems* 58, no. 4 (2015): 293-311.

[48] L. Wei, J. Liu, and T. Zhu, "On a group signature scheme supporting batch verification for vehicular networks." In *Multimedia Information Networking and Security (MINES), 2011 Third International Conference on*, pp. 436-440. IEEE, 2011.

[49] C.S. Vorugunti, and M. Sarvabhatla, "POSTER: A Secure and Efficient Cross Authentication Protocol in VANET Hierarchical Model." In *International Conference on Distributed Computing and Networking*, pp. 461-462. Springer, Berlin, Heidelberg, 2013.

[50] F.M. Padron, I. Mahgoub, and M. Rathod, "VANET-based privacy preserving scheme for detecting traffic congestion." In *High Capacity Optical Networks and Enabling Technologies (HONET), 2012 9th International Conference on*, pp. 066-071. IEEE, 2012.

[51] M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang, "LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication." *Computing* 98, no. 7 (2016): 685-708.

[52] H. Zhu, T. Liu, G. Wei, and H. Li, "PPAS: privacy protection authentication scheme for VANET." *Cluster computing* 16, no. 4 (2013): 873-886.

[53] M. Raya, and J. Hubaux, "Securing vehicular ad hoc networks." *Journal of computer security* 15, no. 1 (2007): 39-68.

[54] M.L. Sichitiu, and M. Kihl, "Inter-vehicle communication systems: a survey." *IEEE Communications Surveys & Tutorials* 10, no. 2 (2008).

[55] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage." *ACM Transactions on Information and System Security (TISSEC)* 9, no. 1 (2006): 1-30.

[56] J. Liu, X. Hong, Q. Zheng, and L. Tang, "Privacy-preserving quick authentication in fast roaming networks." In *Local Computer Networks, Proceedings 2006 31st IEEE Conference on*, pp. 975-982. IEEE, 2006.

[57] J. Choi, S. Jung, Y. Kim, and M. Yoo, "A Fast and Efficient Handover Authentication Achieving Conditional Privacy in V2I Networks." *NEW2AN* 9 (2009): 291-300.

[58] S. Ohzahata, S. Kimura, and Y. Ebihara, "A fast authentication method for secure and seamless handoff." *Information Networking: Wireless Communications Technologies and Network Applications* (2002): 243-252.

[59] X. Lin, X. Sun, P.H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications." *IEEE Transactions on vehicular technology*56, no. 6 (2007): 3442-3456.

[60] C. Zhang, X. Lin, R. Lu, P.H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications." *IEEE Transactions on Vehicular Technology* 57, no. 6 (2008): 3357-3368.

[61] A. Mondal, and S. Mitra, "Identification, authentication and tracking algorithm for vehicles using VIN in centralized VANET." In *International conference of communication, network and computing, proceedings published by Springer LNICST*, vol. 108, pp. 115-120. 2012.

[62] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications." *IEEE Transactions on vehicular Technology* 59, no. 4 (2010): 1606-1617.

[63] M. Ashritha, and C. S. Sridhar, "RSU based efficient vehicle authentication mechanism for VANETs." In *Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on*, pp. 1-5. IEEE, 2015.

[64] M.C. Chuang, and J.F. Lee, "PPAS: A privacy preservation authentication scheme for vehicle-to-infrastructure communication networks." In *Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on*, pp. 1509-1512. IEEE, 2011.

[65] Y. Kim, and J. Lee, "A secure analysis of vehicular authentication security scheme of RSUs in VANET." *Journal of Computer Virology and Hacking Techniques* 12, no. 3 (2016): 145-150.

[66] E. Kaplan, and C. Hegarty, *Understanding GPS: principles and applications*. Artech house, 2005.

[67] A. Boukerche, H.A. Oliveira, E.F. Nakamura, and A.A. Loureiro, "Localization systems for wireless sensor networks." *IEEE wireless Communications* 14, no. 6 (2007).

[68] A. Boukerche, H.A. Oliveira, E.F. Nakamura, and A.A. Loureiro, "Vehicular ad hoc networks: A new challenge for localization-based systems." *Computer communications* 31, no. 12 (2008): 2838-2849.

[69] N. Lagraa, M.B. Yagoubi, and S. Benkouider, "Localization technique in VANETs using Clustering (LVC)." *International Journal of Computer Science Issues (IJCSI)* 7, no. 4 (2010).

[70] G.R. Jagadeesh, T. Srikanthan, and X. D. Zhang, "A map matching method for GPS based real-time vehicle location." *The Journal of Navigation* 57, no. 3 (2004): 429-440.

[71] J.S. Yang, S.P. Kang, and K.S. Chon, "The map matching algorithm of GPS data with relatively long polling time intervals." *Journal of the Eastern Asia Society for Transportation Studies* 6 (2005): 2561-2573.

[72] T. King, H. Füβler, M. Transier, and W. Effelsberg, "On the application of dead-reckoning to position-based routing for vehicular highway scenarios." In *Proceedings of the 2005 ACM conference on Emerging network experiment and technology*, pp. 258-259. ACM, 2005.

[73] A. Hac, "Cellular network model with hand off delays." In *Communications, 1995. ICC'95 Seattle,'Gateway to Globalization', 1995 IEEE International Conference on*, vol. 3, pp. 1834-1838. IEEE, 1995.

[74] M. Rajaratnam, and F. Takawira, "Hand-off traffic modelling in cellular networks." In *Global Telecommunications Conference, 1997. GLOBECOM'97., IEEE*, vol. 1, pp. 131-137. IEEE, 1997.

[75] W. Pattara-Atikom, and R. Peachavanish, "Estimating road traffic congestion from cell dwell time using neural network." In *Telecommunications, 2007. ITST'07. 7th International Conference on ITS*, pp. 1-6. IEEE, 2007.

[76] A. Civilis, C.S. Jensen, J. Nenortaite, and S. Pakalnis, "Efficient tracking of moving objects with precision guarantees." In *Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004. The First Annual International Conference on*, pp. 164-173. IEEE, 2004.

[77] A.F. Merah, S. Samarah, A. Boukerche, and A. Mammeri, "A sequential patterns data mining approach towards vehicular route prediction in VANETs." *Mobile Networks and Applications* 18, no. 6 (2013): 788-802.

[78] L. Yang, J. Xu, G. Wu, and J. Guo, "Road probing: RSU assisted data collection in vehicular networks." In *Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on*, pp. 1-4. IEEE, 2009.

[79] Y. Xu, Y. Wu, G. Wu, J. Xu, B. Liu, and L. Sun, "Data collection for the detection of urban traffic congestion by VANETs." In *Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific*, pp. 405-410. IEEE, 2010.

[80] J. Han, and M. Kamber, "Data Mining: Concepts and Techniques, 2nd editionMorgan Kaufmann Publishers." *San Francisco, CA, USA* (2006).

[81] R.A. Santos, R. M. Edwards, and N. L. Seed, "Inter vehicular data exchange between fast moving road traffic using an ad-hoc cluster-based location routing algorithm and 802.11 b direct sequence spread spectrum radio." In *PostGraduate Networking Conference*. 2003.

[82] Y. Guenter, B. Wiegel, and H.P. Großmann, "Medium access concept for VANETs based on clustering." In *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, pp. 2189-2193. IEEE, 2007.

[83] H. Su, and X. Zhang. "Clustering-based multichannel MAC protocols for QoS provisioning over vehicular ad hoc networks." *IEEE Transactions on Vehicular Technology* 56, no. 6 (2007): 3309-3323.

[84] Z. Wang, L. Liu, M. Zhou, and N. Ansari, "A position-based clustering technique for ad hoc intervehicle communication." *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 38, no. 2 (2008): 201-208.

[85] O. Kayis, and T. Acarman, "Clustering formation for inter-vehicle communication." In *Intelligent Transportation Systems Conference, 2007. ITSC 2007. IEEE*, pp. 636-641. IEEE, 2007.

[86] S. Vijayarani, A. Tamilarasi, and R. SeethaLakshmi, "Privacy preserving data mining based on association rule-a survey." In *Communication and Computational Intelligence (INCOCCI), 2010 International Conference on*, pp. 99-103. IEEE, 2010.

[87] S.J. Yen, and A.L. Chen, "An efficient data mining technique for discovering interesting association rules." In *Database and Expert Systems Applications, 1997. Proceedings., Eighth International Workshop on*, pp. 664-669. IEEE, 1997.

[88] J. Rezgui, and S. Cherkaoui, "Detecting faulty and malicious vehicles using rule-based communications data mining." In *Local Computer Networks (LCN), 2011 IEEE 36th Conference on*, pp. 827-834. IEEE, 2011.

[89] I.H. Bae, and S. Olariu, "A tolerant context-aware driver assistance system for VANETs-based smart cars." In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pp. 1-5. IEEE, 2010.

[90] S. Kotsiantis, and D. Kanellopoulos, "Association rules mining: A recent overview." *GESTS International Transactions on Computer Science and Engineering* 32, no. 1 (2006): 71-82.

[91] U.K. Pandey, and S. Pal, "Data Mining: A prediction of performer or underperformer using classification." *arXiv preprint arXiv:1104.4163* (2011).

[92] M. Sujatha, S. Prabhakar, and Dr G.L. Devi, "A Survey of Classification Techniques in Data Mining." *International Journal of Innovations in Engineering and Technology (IJIET)*2, no. 4 (2013).

[93] F. Kargl, Z. Ma, and E. Schoch, "Security engineering for vanets." In *4th Workshop on Embedded Security in Cars (escar 2006)*. 2006.

[94] A.J. Lee, Y.A. Chen, and W.C. Ip, "Mining frequent trajectory patterns in spatial–temporal databases." *Information Sciences* 179, no. 13 (2009): 2218-2231.

[95] J.Y. Kang, and H.S. Yong, "Mining spatio-temporal patterns in trajectory data." *Journal of Information Processing Systems* 6, no. 4 (2010): 521-536.

[96] I. Tsoukatos, and D. Gunopulos, "Efficient mining of spatiotemporal patterns." *Advances in Spatial and Temporal Databases* (2001): 425-442.

[97] E.L. Jessup, K.L. Casavant, and C.T. Lawson, *Truck trip data collection methods*. No. FHWA-OR-RD-04-10,. Oregon Department of Transportation, Research Unit, 2004.

[98] A. Protopapas, A. Chatterjee, T. Miller, and J. Everett, "Travel characteristics of urban freight vehicles and their effects on emission factors." *Transportation Research Record: Journal of the Transportation Research Board* 1941 (2005): 89-98.

[99] S.W. Lau, "Truck Travel Surveys: A review of the Literature and State-of-the-Art." (1995).

[100] E.R. Ruiter, "Development of an urban truck travel model for the Phoenix Metropolitan Area." (1992).

[101] K.J. Chen, K.K. Pecheux, J. Farbry Jr, and S.A. Fleger, "Commercial vehicle driver survey: assessment of parking needs and preferences." *No. FHWA-RD-01-160*. 2002.

[102] J. Soh, B.T. Chun, and M. Wang, "Analysis of road image sequences for vehicle counting." In *Systems, Man and Cybernetics, 1995. Intelligent Systems for the 21st Century., IEEE International Conference on*, vol. 1, pp. 679-683. IEEE, 1995.

[103] T. Liu, P. Bahl, and I. Chlamtac, "Mobility modeling, location tracking, and trajectory prediction in wireless ATM networks." *IEEE Journal on selected areas in communications* 16, no. 6 (1998): 922-936.

[104] Z.R. Zaidi, and B.L. Mark, "Real-time mobility tracking algorithms for cellular networks based on Kalman filtering." *IEEE Transactions on Mobile Computing* 4, no. 2 (2005): 195-208.

[105] S.M. Lee, and H. Baik, "Origin-destination (OD) trip table estimation using traffic movement counts from vehicle tracking system at intersection." In *IEEE Industrial Electronics, IECON 2006-32nd Annual Conference on*, pp. 3332-3337. IEEE, 2006.

[106] K.Z. Ghafoor, K.A. Bakar, M.V. Eenennaam, R.H. Khokhar, and A.J. Gonzalez, "A fuzzy logic approach to beaconing for vehicular ad hoc networks." *Telecommunication Systems* 52, no. 1 (2013): 139-149.

[107] C. Chai, and Y.D. Wong, "Automatic vehicle classification and tracking method for vehicle movements at signalized intersections." In *Intelligent Vehicles Symposium (IV), 2013 IEEE*, pp. 624-629. IEEE, 2013.

[108] I. Sina, A. Wibisono, A. Nurhadiyatna, B. Hardjono, W. Jatmiko, and P. Mursanto, "Vehicle counting and speed measurement using headlight detection." In *Advanced Computer Science and Information Systems (ICACSIS), 2013 International Conference on*, pp. 149-154. IEEE, 2013.

[109] F. Zhang, H. Li, K. Kone, and W. Zhang, "Vehicle Tracking Based on Nonlinear Motion Model." In *Proceedings of 2013 Chinese Intelligent Automation Conference*, pp. 403-410. Springer, Berlin, Heidelberg, 2013.

[110] A. Ait-Mlouk, F. Gharnati, and T. Agouti, "An improved approach for association rule mining using a multi-criteria decision support system: a case study in road safety." *European Transport Research Review* 9, no. 3 (2017): 40.

[111] G. Yan, D.B. Rawat, B.B. Bista, and A. Alnusair, "Mining vehicular data in VANET." In *TENCON 2013-2013 IEEE Region 10 Conference (31194)*, pp. 1-4. IEEE, 2013.

[112] Q. Zhang, M. Almulla, and A. Boukerche, "Performance analysis of an RFID Key Management scheme for vehicular networks." In *Selected Topics in Mobile and Wireless Networking (MoWNeT), 2013 International Conference on*, pp. 25-29. IEEE, 2013.

[113] P. Lai, X. Wang, N. Lu, and F. Liu, "A reliable broadcast routing scheme based on mobility prediction for VANET." In *Intelligent Vehicles Symposium, 2009 IEEE*, pp. 1083-1087. IEEE, 2009.

[114] R. Simmons, B. Browning, Y. Zhang, and V. Sadekar, "Learning to predict driver route and destination intent." In *Intelligent Transportation Systems Conference, 2006. ITSC'06. IEEE*, pp. 127-132. IEEE, 2006.

[115] G. Xue, Z. Li, H. Zhu, and Y. Liu, "Traffic-known urban vehicular route prediction based on partial mobility patterns." In *Parallel and Distributed Systems (ICPADS), 2009 15th International Conference on*, pp. 369-375. IEEE, 2009.

[116] J. Froehlich, and J. Krumm, "Route prediction from trip observations." *No. 2008-01-0201*. SAE Technical Paper, 2008.

[117] L. Wang, Y. Wang, and C. Wu, "A Receiver-Based Routing Algorithm Using Competing Parameter for VANET in Urban Scenarios." In *International Conference on Internet of Vehicles*, pp. 140-149. Springer, Cham, 2014.

[118] K. Park, H. Kim, and S. Lee, "Mobility state based routing method in vehicular ad-hoc network." In *Mobile Services (MS), 2015 IEEE International Conference on*, pp. 473-474. IEEE, 2015.

[119] J.J. Blum, A. Eskandarian, and L.J. Hoffman, "Challenges of intervehicle ad hoc networks." *IEEE transactions on intelligent transportation systems* 5, no. 4 (2004): 347-351.

[120] H. Hartenstein, and L.P. Laberteaux, "A tutorial survey on vehicular ad hoc networks." *IEEE Communications magazine* 46, no. 6 (2008).

[121] M.M Artimy, W.J. Phillips, and W. Robertson, "Connectivity with static transmission range in vehicular ad hoc networks." In *Communication Networks and Services Research Conference, 2005. Proceedings of the 3rd Annual*, pp. 237-242. IEEE, 2005.

[122] Y.W. Lin, Y.S. Chen, and S.L. Lee, "Routing Protocols in Vehicular Ad Hoc Networks: A Survey and Future Perspectives." *J. Inf. Sci. Eng.* 26, no. 3 (2010): 913-932.

[123] W. Chen, R.K. Guha, T.J. Kwon, J. Lee, and Y.Y. Hsu, "A survey and challenges in routing and data dissemination in vehicular ad hoc networks." *Wireless Communications and Mobile Computing* 11, no. 7 (2011): 787-795.

[124] M. Zhang, and R.S. Wolff, "Routing protocols for vehicular ad hoc networks in rural areas." *IEEE Communications magazine* 46, no. 11 (2008).

[125] Z. Wang, and C. Chigan, "Countermeasure uncooperative behaviors with dynamic trust-token in VANETs." In *Communications, 2007. ICC'07. IEEE International Conference on*, pp. 3959-3964. IEEE, 2007.

[126] T.Yasser, and P. Mühlethaler, "Vehicle Ad Hoc networks: applications and related technical issues", IEEE Communications Surveys, Volume 10, No. 3, 2008

[127] C.D. Wang, and J.P. Thompson, "Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network." U.S. Patent 5,613,039, issued March 18, 1997.

[128] P. Vijayakumar, M. Azees, A. Kannan, and L.J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks." *IEEE Transactions on Intelligent Transportation Systems* 17, no. 4 (2016): 1015-1028.

[129] S. Ezell, "Explaining international IT application leadership: Intelligent transportation systems." (2010).

[130] J. Nzouonta, N. Rajgure, G. Wang, and C. Borcea, "VANET routing on city roads using real-time vehicular traffic information." *IEEE Transactions on Vehicular technology* 58, no. 7 (2009): 3609-3626.

[131] A.O. Adebowale, "Wireless Access in Vehicular Environments (WAVE)." PhD diss., Department of Electrical and Electronic Engineering, University of Bristol, 2011.

[132] https://www.fcc.gov/wireless/bureau-divisions/mobility-division/dedicated-short-range-communications-dsrc-service

[133] Y. Qian, K. Lu, and N. Moayeri, "A secure VANET MAC protocol for DSRC applications." In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pp. 1-5. IEEE, 2008.

[134] CAMP Vehicle Safety Communications Consortium. "Vehicle safety communications project: Task 3 final report: identify intelligent vehicle safety applications enabled by DSRC." *National Highway Traffic Safety Administration, US Department of Transportation, Washington DC* (2005).

[135] Y. Wang, and F. Li, "Vehicular ad hoc networks." In *Guide to wireless ad hoc networks*, pp. 503-525. Springer London, 2009.

[136] V.Kumar, S.Mishra, and N. Chand, " Applications of VANETs: Present & Future". *Communications and Network, Scientific Research* 5 (2013): 12-15.

[137] W. Nesh, "Vehicular networking and its applications."*HCLTECH* (2011).

[138] X. Yang, L. Liu, N.H. Vaidya, and F. Zhao, "A vehicle-to-vehicle communication protocol for cooperative collision warning." In *Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004. The First Annual International Conference on*, pp. 114-123. IEEE, 2004.

[139] Car 2 Car Communication Consortium. "Car 2 car communication consortium manifesto." *Braunschweig, November* (2007).

[140] M.C. Weigle, and S.Olariu , *Vehicular networks: from theory to practice*. Chapman and Hall/CRC, 2009.

[141] R. Baldessari, B. Bödekker, M. Deegener, A. Festag, W. Franz, C.C. Kellum, T. Kosch, "Car-2-car communication consortium-manifesto(Version 1.1)." In *IEEE Vehiclular Technology Conference*. 2007.

[142] H. Hasbullah, and I.A. Soomro, "Denial of service (dos) attack and its possible solutions in VANET." *World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering* 4, no. 5 (2010): 813-817.

[143] F.Ye, S. Roy, and H. Wang, "Efficient data dissemination in vehicular ad hoc networks." *IEEE Journal on Selected Areas in Communications* 30, no. 4 (2012): 769-779.

[144] A. Rakhshan, and H. Pishro-Nik, "Improving Safety on Highways by Customizing Vehicular Ad Hoc Networks." *IEEE Transactions on Wireless Communications* 16, no. 3 (2017).

[145] S. Al-Sultan, M.M. Al-Doori, A.H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network." *Journal of network and computer applications* 37 (2014): 380-392.

[146] M. Faezipour, M. Nourani, A. Saeed, and S. Addepalli, "Progress and challenges in intelligent vehicle area networks." *Communications of the ACM* 55, no. 2 (2012): 90-100.

[147] M. Nekoui, and H. Pishro-Nik, "Analytic design of active safety systems for vehicular ad hoc networks." *IEEE Journal on Selected Areas in Communications* 31, no. 9 (2013): 491-503.

[148] P. Fernandes, and U. Nunes, "Vehicle communications: A short survey." *IADIS Telecommunications, Networks and Systems, Lisbon* (2007): 134-138.

[149] S. Yousefi, M.S. Mousavi, and M. Fathy, "Vehicular ad hoc networks (VANETs): challenges and perspectives." In *ITS Telecommunications Proceedings, 2006 6th International Conference on*, pp. 761-766. IEEE, 2006.

[150] J. Jakubiak, and Y. Koucheryavy, "State of the art and research challenges for VANETs." In *Consumer communications and networking conference, 2008. CCNC 2008. 5th IEEE*, pp. 912-916. IEEE, 2008.

[151] M. Nekovee, "Sensor networks on the road: the promises and challenges of vehicular adhoc networks and vehicular grids." In *Proc. Workshop on Ubiquitous Computing and e-Research,* vol. 47. 2005.

[152] M.D. TamilSelvan, V. Vasudevan, P.R. Parasuraman, and A.V. Aadhimoolam, "Mobility Prediction and Node Prediction Based Light-Weight Reliable Broadcast Message Delivery for Vehicular Ad-Hoc Networks." *International Journal of Advanced Research in Computer and Communication Engineering* 3 (2014): 5321-5325.

[153] F. Li, and Y. Wang, "Routing in vehicular ad hoc networks: A survey." *IEEE Vehicular technology magazine* 2, no. 2 (2007).

[154] B. Parno, and A. Perrig, "Challenges in securing vehicular networks." In *Workshop on hot topics in networks (HotNets-IV)*, pp. 1-6. 2005.

[155] A. Dhamgaye, and N. Chavhan, "Survey on security challenges in VANET 1." (2013).

[156] J.A. Freebersyser, and B. Leiner, "A DoD perspective on mobile ad hoc networks." In *Ad hoc networking*, pp. 29-51. Addison-Wesley Longman Publishing Co., Inc., 2001.

[157] D. Rampaul, R.K. Patial, and D. Kumar, "Detection of DoS Attack in VANETs." *Indian Journal of Science and Technology* 9, no. 47 (2016). Minhas, Rashid, and Muhammas Tilal. "Effects of jamming on IEEE 802.11 p systems." (2010).

[158] Y. Qian, and N. Moayeri, "Design of secure and application-oriented VANETs." In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pp. 2794-2799. IEEE, 2008.

[159] H. Kaur, S. Batish, and A. Kakaria, "An approach to detect the wormhole attack in vehicular adhoc networks." *International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN* 2248-9738 (2012): 86-89.

[160] G. Guette, and B. Ducourthial, "On the Sybil attack detection in VANET." In *Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE International Conference on*, pp. 1-6. IEEE, 2007.

[161] S. Sharma, and S. Sharma, "A defensive timestamp approach to detect and mitigate the Sybil attack in vanet." In *Contemporary Computing and Informatics (IC3I), 2016 2nd International Conference on*, pp. 386-389. IEEE, 2016.

[162] A. Rawat, S. Sharma, and R. Sushil, "VANET: Security attacks and its possible solutions." *Journal of Information and Operations Management* 3, no. 1 (2012): 301.

[163] J.M. Fuentes, A.I. González-Tablas, and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks." (2010).

[164] M.E. Mathew, and P. ARK, "Threat analysis and defence mechanisms in VANET." *Int. J. Adv. Res. Comput. Sci. Softw. Eng* 3, no. 1 (2013): 47-53.

[165] R.K. Sakib, and B. Reza, "Security issues in vanet." PhD diss., Department of Electronics and Communication Engineering, BRAC University, 2010.

[166] S. RoselinMary, M. Maheshwari, and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA)." In *Information Communication and Embedded Systems (ICICES), 2013 International Conference on*, pp. 237-240. IEEE, 2013.

[167] V. Pathak, D. Yao, and L. Iftode, "Securing location aware services over VANET using geographical secure path routing." In *Vehicular Electronics and Safety, 2008. ICVES 2008. IEEE International Conference on*, pp. 346-353. IEEE, 2008.

[168] Hamieh, Ali, Jalel Ben-Othman, Abdelhak Gueroui, and Farid Naït-Abdesselam. "Detecting greedy behaviors by linear regression in wireless ad hoc networks." In *Communications, 2009. ICC'09. IEEE International Conference on*, pp. 1-6. IEEE, 2009.

[169] M.S. Al-Kahtani, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)." In *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*, pp. 1-9. IEEE, 2012.

[170] M. Nogueira, H. Silva, A. Santos, and G. Pujolle, "A security management architecture for supporting routing services on WANETs." *IEEE Transactions on Network and Service Management* 9, no. 2 (2012): 156-168.

[171] W.R. Pires, T.H. Paula Figueiredo, H.C. Wong, and A.A. Ferreira Loureiro, "Malicious node detection in wireless sensor networks." In *Parallel and distributed processing symposium, 2004. Proceedings. 18th international*, p. 24. IEEE, 2004.

[172] S.M. Safi, A. Movaghar, and M. Mohammadizadeh, "A novel approach for avoiding wormhole attacks in VANET." In *Computer Science and Engineering, 2009. WCSE'09. Second International Workshop on*, vol. 2, pp. 160-165. IEEE, 2009.

[173] Burg, Adam. "Ad hoc network specific attacks." In *Technische Universität München, Institut für Informatik, Seminar Paper, Seminar Ad Hoc Networking: concept, applications, and security*. 2003.

[174] J.R. Douceur, "The sybil attack." In *International Workshop on Peer-to-Peer Systems*, pp. 251-260. Springer, Berlin, Heidelberg, 2002.

[175] M. Rahbari, and M.A. Jabreil Jamali, "Efficient detection of sybil attack based on cryptography in vanet." *arXiv preprint arXiv:1112.2257* (2011).

[176] A. Suman, and C. Kumar, "A behavioral study of Sybil attack on vehicular network." In *Recent Advances in Information Technology (RAIT), 2016 3rd International Conference on*, pp. 56-60. IEEE, 2016.

[177] M.A. Razzaque, A. Salehi, and S.M. Cheraghi, "Security and privacy in vehicular ad-hoc networks: survey and the road ahead." *Wireless Networks and Security* (2013): 107-132.

[178] K. Amirtahmasebi, and S.R. Jalalinia, "Vehicular Networks–Security, Vulnerabilities and Countermeasures." (2010).

[179] D.A. Rivas, J.M. Barceló-Ordinas, M.G. Zapata, and J.D. Morillo-Pozo, "Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation." *Journal of Network and Computer Applications* 34, no. 6 (2011): 1942-1955.

[180] H. Hamad, and S. Elkourd, "Data encryption using the dynamic location and speed of mobile node." *Journal of Media and Communication Studies* 2, no. 3 (2010): 67.

[181] R.S Shukla, D. Maurya, and B. Maurya, "Data dissemination under Load Distribution in hybrid network for VANET." In *System Modeling & Advancement in Research Trends (SMART), International Conference*, pp. 175-181. IEEE, 2016.

[182] C.H. Lee, K.G. Lim, B.L. Chua, R.K. Yin Chin, and K.T. Kin Teo, "Progressing toward urban topology and mobility trace for Vehicular Ad Hoc Network (VANET)." In *Open Systems (ICOS), 2016 IEEE Conference on*, pp. 120-125. IEEE, 2016.

[183] S. Zeng, Y. Huang, and X. Liu, "Privacy-preserving communication for vanets with conditionally anonymous ring signature." *International Journal of Network Security* 17, no. 2 (2015): 135-141.

[184] Y. Wang, H. Zhong, Y. Xu, and J. Cui, "ECPB: Efficient Conditional Privacy-Preserving Authentication Scheme Supporting Batch Verification for VANETs." *IJ Network Security* 18, no. 2 (2016): 374-382.

[185] G. Kwon, S. Lee, E. Moon, and D. Kim, "Position-freshness based intermediate node filtering for VANET." In *URSI Asia-Pacific Radio Science Conference (URSI AP-RASC)*, pp. 1-2. IEEE, 2016.

[186] X. He, H. Zhang, W. Shi, T. Luo, and N.C. Beaulieu, "Transmission capacity analysis for linear VANET under physical model." *China Communications* 14, no. 3 (2017): 97-107.

[187] M.H. Riaz, M.H. Kabir, M.F. Islam Shaon, and M.J. Hossain, "Implementation and comparison of routing protocol RIVER with other VANET protocols, " In *Electrical Engineering and Information Communication Technology (ICEEICT), 2016 3rd International Conference on*, pp. 1-4. IEEE, 2016.

[188] C.C. Lo, and Y.H. Kuo, "Traffic-aware routing protocol with cooperative coverage-oriented information collection method for VANET." *IET Communications* 11, no. 3 (2017): 444-450.

[189] F. Anwar, I. Petrounias, T. Morris, and V. Kodogiannis, "Discovery of events with negative behavior against given sequential patterns." In *Intelligent Systems (IS), 2010 5th IEEE International Conference*, pp. 373-378. IEEE, 2010.

[190] A.D. Lattner, A. Miene, U. Visser, and O. Herzog, "Sequential pattern mining for situation and behavior prediction in simulated robotic soccer." *RoboCup* 4020 (2005): 118-129.