"Implementation of Session Initiation Protocol using Cryptography in VANET"

Realization of Dissertation Report

Submitted by
HARIKRISHNA

Under the Guidance of
Mr. Sandeep Arora
Assistant Professor

in partial fulfillment for the award of the degree of

MASTER OF TECHNOLOGY
IN
ELECTRONICS AND COMMUNICATION ENGINEERING

At
Lovely Professional University
Department of ECE
Jalandhar
April 2017

TOPIC APPROVAL PERFORMA

School of Electronics and Electrical Engineering

Program : P175::M.Tech. (Electronics and Communication Engineering) [Full Time]

COURSE CODE : ECE521 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** EEERGD0200

Supervisor Name : Sandeep Kumar Arora **UID :** 16930 **Designation :** Assistant Professor

Qualification : _____ **Research Experience :** _____

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Hari Krishna	11507917	2015	E1514	9458251390

SPECIALIZATION AREA : Wireless Communication **Supervisor Signature:** _____

PROPOSED TOPIC : Implementation of Session Initiation Protocol using Cryptography in VANET

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	6.50
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	6.50
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	6.50
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	6.50
5	Social Applicability: Project work intends to solve a practical problem.	6.50
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	6.50

PAC Committee Members		
PAC Member 1 Name: Rajeev Kumar Patial	UID: 12301	Recommended (Y/N): NO
PAC Member 2 Name: Lavish Kansal	UID: 15911	Recommended (Y/N): Yes
PAC Member 3 Name: Dr. Gursharanjeet Singh	UID: 13586	Recommended (Y/N): NA
DAA Nominee Name: Amanjot Singh	UID: 15848	Recommended (Y/N): NA

Final Topic Approved by PAC: **Implementation of Session Initiation Protocol using Cryptography in VANET**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11106::Dr. Gaurav Sethi **Approval Date:** 05 Oct 2016

Certificate

This is to certify that the Thesis titled "Implementation of Session Initiation Protocol using Cryptography in VANET" that is being submitted by "**HARI KRISHNA**" is in partial fulfillment of the requirements for the award of MASTER OF TECHNOLOGY DEGREE, is a record of bonafide work done under my /our guidance. The contents of this Thesis, in full or in parts, have neither been taken from any other source nor have been submitted to any other Institute or University for award of any degree or diploma and the same is certified.

Sandeep Kr. Arora
Assistant Professor
School of Electronics and Communication Engineering
Lovely Professional University
Phagwara, Punjab

Objective of the Dissertation is satisfied / unsatisfactory

Examiner I Examiner II

Acknowledgement

No volume of words is enough to express my gratitude towards my guide, **SANDEEP Kr. ARORA,** Assistant Professor, Electronics and communication Engineering Department, Lovely Professional University, who have been very concerned and have supervised the work presented in this thesis report. He has helped me to explore this vast field in an organized manner and provided me with all the ideas on how to work towards a research oriented venture.

I am also thankful to **Mr. Lavish Kansal**, Head of Department, Wireless Communication Department for the motivation and inspiration that triggered me for the thesis work.

Place: LPU, Jalandhar — Hari Krishna

Date: April,2017 — Reg No.11507917

Declaration

I certify that the work contained in Dissertation is original and has been done by myself under the general supervision of my supervisor. The work has not been submitted to any other Institute for any degree or diploma. I have followed the guidelines provided by the Institute in writing the thesis. I have conformed to the norms and guidelines given in the Code of Conduct of the Institute. Whenever I have used materials (data, theoretical analysis, and text) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references. Whenever I have quoted written materials from other sources, I have put them under quotation marks and given due credit to the sources by citing them and giving required details in the references.

Hari Krishna
Reg No. 11507917

Abstract

Vehicular Ad-hoc network (VANET) is a wireless communication among many vehicles. The main motive of VANET security is to not only to provide safety, secure communication and intelligent transportation service but also another service like entertainment, advertisement and offers based on location wise. As all the services related to communication are more important and vulnerable to attacks hence requires security. In VANET, vehicles represent the node and communication takes place either between vehicle to vehicle (V2V) or vehicle to infrastructure (V2I). Securing communications between vehicles and road side unit is a great challenge.

Security is one of the major concerns in VANETs as nodes in VANETs have high mobility. So, it is a challenging task to design an efficient solution for secure communication in VANETs due to high mobility of nodes.

In literature, many authentication protocols have been proposed for secure communication in VANETs using Session Initiation Protocol (SIP). SIP is widely used for signalling, and establishing communication between different nodes in VANETs. SIP uses the concept of Voice over Internet Protocol (VoIP) for communication between vehicles. It uses Hypertext Transfer Protocol (HTTP) digest for identity authentication between different vehicles during communication. In this dissertation, a SIP authentication protocol for various vehicles is proposed to address these issues. The proposed scheme is secure from various types of attacks. The security and performance analysis of the proposed scheme confirms the effectiveness of the scheme.

Table of Contents

List of Figures

List of Tables

CHAPTER 1
INTRODUCTION

1.1. Wireless Sensor Network

Now days, for facilitating avenue safety, traffic control, and infotainment dissemination for drivers and passengers Vehicular Ad-Hoc Network affords a promising community scenario. Wireless Networks are the network the various two nodes or any conversation devices that makes use of the radio waves to talk. As the growth in era, the usage of transportable and small community devices is growing every day. The requirement of wireless community has additionally extended. In early instances, stressed network become taken into consideration greater secure and speedy, however with the evolution of technology wi-fi community became more famous. Wireless networks due to their ease of access and infrastructural flexibility; they are used in small and massive industries.

A wi-fi group is any sort of portable workstation group that makes utilization of wi-fi records connections to plug network nodes. Wi-Fi system are computer network systems who are not related through links regardless of the kind. The utilization of a wi-fi group empowers organizations to keep the more luxurious approach of bringing links into homes or as a connection among one of a kind equipment locations. Wireless technologies range in a number of dimensions, most drastically in only how a great deal bandwidth they offer and the way far aside communicating nodes can be. Ad-hoc networks are multi-hop wireless networks that could perform minus the services of the hooked-up backbone infrastructure. While such networks have apparent applications from the army and disaster remedy environments, extra current works that contain stimulated their use even in ordinary wireless packet statistics networks have raised their significance. WSN has a bonus of being operated unattended inside the environment wherein continuous human monitoring is both unstable, inefficient or infeasible. Sensor nodes run on batteries and as soon as nodes are deployed their batteries cannot be recharged, so they have brief lifespan. Some large wonderful of wireless sensor network as proven in following:

- **Flexibility:** A wireless network is a flexible network. It is very easy to access network in devices from the nearest network converge area.
- **Increased mobility:** As there is no requirement of wires so user can easily access network from anywhere. In a wireless network, there is no longer bondage to the desk.

- **Cost effective:** As there is no requirement of wire so the wireless network is more cost effective than wired networks. In a wireless network, the labour and maintenance cost is also less.
- **Easy setup:** The wireless network can be installed quickly because wires are not required for the installation. The configuration of wireless network is easier than wired networks.
- **Expandable:** The wireless network can be easily expanded whenever required with the existing equipment's. But in wired networks, there is scope of more wires for expansions.
- **Health and safety:** As there is no connection of wires in wireless connection, it is not possible to make pin in wire.

Wireless Networks are the network between the two nodes or any communication devices that uses the radio waves to communicate as shown in Fig. 1.1. As the growth in technology, the use of portable and small network devices is increasing day by day. The need of wireless network has also increased. In early times, wired network was considered more secure and fast, but with the evolution of technology wireless network became more popular.

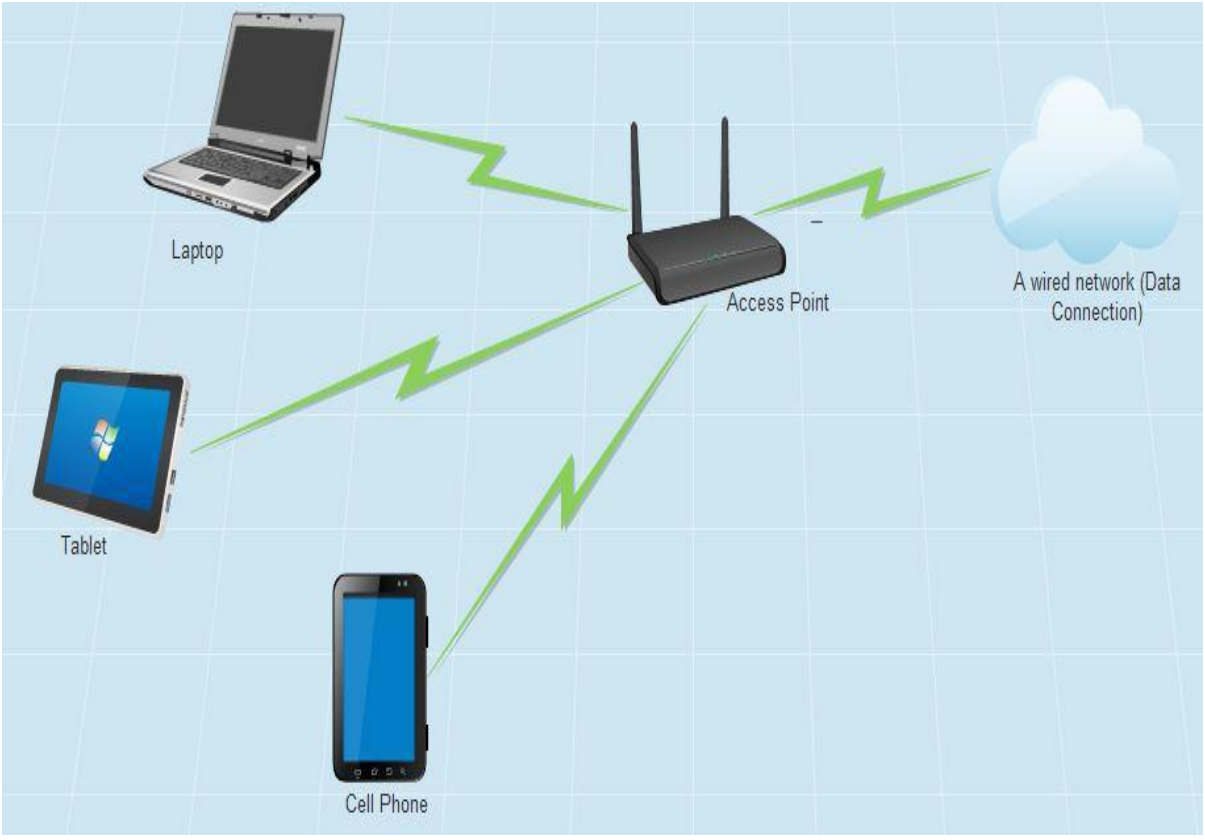

Fig. 1.1 Wireless Network

Wireless sensor organize comprises of substantial scope of little, low vitality, low value sensor nodes with compelled memory, computational, and discussion assets and a Base Station. These nodes constantly display environmental situations and gather targeted statistics approximately the physical environment wherein they are set up, then transmits the collected statistics to the BS. BS is a gateway from sensor networks to the outside international. The BS has a totally massive garage and huge facts processing abilities. BS is a door from sensor systems to the outside global. The BS has an absolutely monstrous carport and enormous actualities handling functions. It passes the information it gets from sensor nodes to the server from in which end-customer can get section to them. The sensors nodes are ordinarily conveyed around the range of the Base Station and shape associations as in accordance with the need of the Base Station. Today, wireless sensor networks are extensively utilized inside the business and modern locales comprising of for e.g. Ecological following, living space following, human services, method checking and observation [29]. For example, in a naval force put, we can utilize wireless sensor networks to screen a side interest. On the off chance that an occasion is hastened, those sensor nodes feel it and send the data to the base station (known as sink) by method for talking with various nodes. The utilization of wi-fi sensor systems is expanding day by day and on the equivalent time it confronts the issue of quality imperatives as far as limited battery lifetime. As each node relies on upon power for its exercises, this has end up being an essential issue in wireless sensor networks. The disappointment of one node can interfere with the entire machine or utility. Each detecting node can be in lively (to receive and transmission exercises), sit still and rest modes. Every sensing node can be in energetic (for receiving and transmission activities), idle and sleep modes. In active mode nodes consume energy when receiving or transmitting statistics. In idle mode, the nodes consume nearly the same amount of electricity as in energetic mode, at the same time as in sleep mode, the nodes shutdown the radio to keep the energy.

Ad hoc networks are characterised with the aid of being wireless networks in that each one of its nodes are efficiently energetic on communications. In other words, they do not need a hard and fast infra-shape as get entry to points to establish the network. In a radio conversation band, two or more automobiles or Intelligent Transportation System (ITS) stations routinely connect, creating an Ad Hoc network, because of this all stations recognise the placement, velocity and route of the other stations, turning into capable of offering signals and facts [31]. The class of wi-fi sensor network is shown in Fig. 1.2.

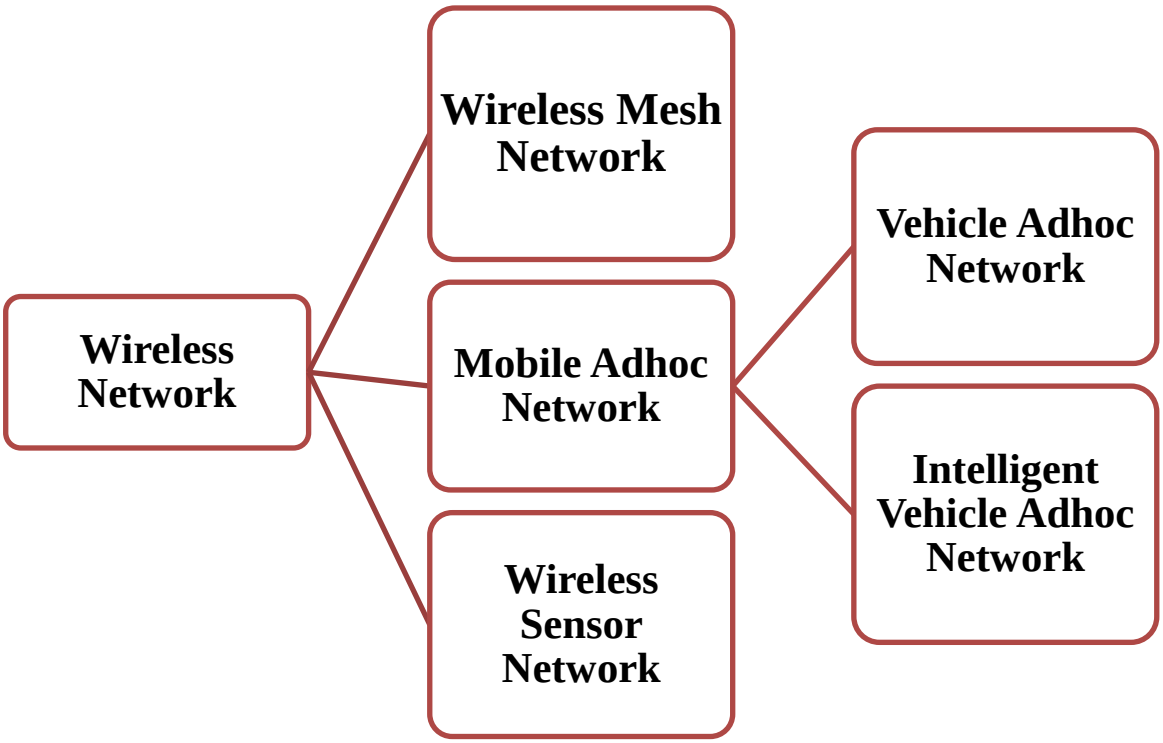

Fig. 1.2 Classification of Wireless Sensor Network

1.2 Vehicular Adhoc Network

Vehicles have been constantly evolving since their creation more than one hundred years ago. Some of the latest advantages include research in the field of wireless sensor networks which will allow a vehicle to communicate with other vehicles located within its neighbourhood. VANET stands for vehicular ad hoc network. VANET have most attractive topic in recent years. It is special kind of mobile ad hoc network. In which, communication has been done in between vehicle to vehicle (V to V), Inter roadside communication, vehicle to roadside unit (V to RSU), in a range of 100 to 300 m as shown in figure 2. VANET are dynamic in nature and its topology is change very rapid and often. In which, every node can flow freely in the community and each node can communicate with another node. The purpose of the VANET is to provide comfort to passengers and it is also used for existence saving of passengers. VANET is part of MANET in which every node travels generously in the community. It covers the entire community and maintains on related. Each node communicates with other nodes in single hop or multi hop. In VANET, On Board Units (OBUs) regularly broadcast

routine traffic-related messages with records approximately role, contemporary time, route, speed, acceleration/deceleration, traffic occasions, and so on. By being ready with conversation gadgets, vehicles can talk with every different in addition to with the roadside units (RSUs) placed at critical factors of the street, together with intersections or production websites. As VANET often broadcast and obtain visitors-related messages, drivers can get a better awareness in their using surroundings.

VANET is sub part of MANET. In a MANET, vehicles work in an associate to peer and freely within an organization or a centralised administration. To talk with nodes past the assortment, middle of the road nodes ahead messages to relax spot node over numerous jumps. Nodes in MANETs move very frequently so they change their position from one cell to another cell. This reasons node to move inside and out of wi-fi range ensuing in node unavailability, modifications in packet routes, and possibly lack of packets [33]. Since cell nodes keep running on batteries, the handling vitality to be had for every node is restricted Since cell nodes run on batteries, the processing energy to be had for each node is limited. Wi fi links have an impressively diminished limit when contrasted with wired connection. Wireless hyperlinks frequently suffer from the outcomes of multiple get right of entry to, fading, noise, and interference situations that anticipates it from handing over a throughput identical to the most throughput. Each mobile node can also have a specific hardware/software program configuration with extraordinary abilities. Designing protocols and algorithms for such heterogeneous, uneven links becomes a complicated process.

Due to the pervasive nature of cellular nodes, we cannot anticipate that they'll usually be underneath the control of their proprietors. Nodes might be stolen or tampered with. The shared wi-fi medium is on the market to both legitimate and illegitimate customers. The opportunity of eavesdropping, spoofing, and denial-of-carrier attacks are greater established compared to fixed line networks [7]. The packages related to MANETs variety from people who involve a small number of nodes to those containing tens of thousands of nodes. Scalability is an essential aspect of a success deployment of ad hoc networks. Compared to small networks, the community management algorithms of massive networks have to cope with altogether specific challenges in areas such as addressing, routing, vicinity control, interoperability, protection, mobility, wi-fi technologies etc. [8].

Vehicular Ad hoc Networks (VANET) have been added to gain more secure using environment via smart automobiles and smart roads. VANET incorporates critical types of elements: Road Side Units (RSUs), and On-Board Units (OBUs). RSUs are normally

established at a road-facet area to aid the statistics exchange with vehicles, even as OBUs are hooked up in automobiles to enable the periodic exchange of protection statistics for some secure and comfortable driving surroundings. Also, a special form of OBU named Public Safety On-board Unit (PSOBU) has been proposed to permit protection cars (like emergency medical provider or fire vehicles) to run certain public protection programs such as traffic signal prioritization for emergency automobiles. Adhoc wi-fi systems are depicted in light of the fact that the classification of Wi-fi systems that use multi-bounce radio transferring and can running without the guide of any consistent framework and nodes impart on the double among each other over Wi-fi channels. As the wireless channels are brazenly to be had and propagate through the air, security in adhoc networks is of number one challenge. In an adhoc, wi-fi arrange, the Routing and valuable asset control are executed in a dispensed way in which all nodes facilitate to allow report among them as a set. This requires each node to be more cunning all together that it might trademark each as a system have for transmitting and accepting certainties and as a group switch for Routing information from various nodes. As adhoc systems radically fluctuate from each unique in numerous components, a surroundings-specific and effective key control device is needed. To guard nodes contrary to listening in, the nodes need made a common concession to a mutual riddle or traded open keys. For out of the blue changing over adhoc systems the trading of encryption keys may likewise should be tended to accessible as needs be for, therefore without supposition about from the earlier arranged privileged insights and strategies.

1.2.1. Characteristics of VANET: The growth of the improved variety of cars are prepared with wi-fi transceivers to communicate with other motors. It has the traits of high node mobility and speedy topology modifications. VANET has grown to be a lively place of studies, standardization, and development as it has exquisite ability to enhance car and street protection, traffic performance and convenience in addition to consolation to both drivers and passengers. Vehicular networks will no longer only provide safety and lifesaving programs, but they may turn out to be a powerful communique device for his or her users. VANET have changed into a critical studies vicinity over the previous couple of years. VANET has its personal unique traits while compared with different kinds of MANETs, the specific traits of VANET include

- **Predictable mobility:** Unlike MANETs, the network nodes (here motors) of VANET flow in a predefined way because roads format are fixed and motors should obey and comply with street signs, site visitors' indicators, in addition to reply to different

moving vehicles The prediction of automobile position and their actions may be very tough. This feature of mobility modelling and prediction in VANET is based at the availability of predefined roadmaps models. The velocity of the vehicles is once more an essential for green community design.

- **High mobility and fast changing topology:** Vehicles pass very speedy in particular on roads and highways. Thus, they remain inside each different communique variety for a very quick time, and hyperlinks are established and broken rapid which results to fast adjustments in network topology. Moreover, driving force conduct is tormented by the necessity to react to the facts obtained from the network, which reasons modifications in the network topology. The speedy adjustments in community topology affect the community diameter to be small, even as many paths can be disconnected earlier than they may be used.
- **Geographic role to be had:** Vehicles may be geared up with cutting-edge, correct positioning structures integrated with the aid of digital maps. For example, international positioning system (GPS) receivers are very popular in motors which help to provide region statistics for routing functions. VANET may be carried out for one town, numerous towns or for countries. This way that community size in VANET is geographically unbounded.
- **Variable community density:** The community density in VANET varies relying at the site visitors load, which may be very high inside the case of a traffic jam, or very low, as in suburban regions. Due to excessive node mobility and random velocity of automobiles, the position of node changes regularly. As an end result of this, network topology in VANET tends to trade often
- **High computational capacity:** As vehicles are nodes in VANET, they can keep a sufficient number of sensors and enough conversation equipment inclusive of excessive pace processors, massive reminiscence size, superior antenna generation and present day GPS. These sources boom the computational strength of the node, which assist to create dependable wi-fi communique and to acquire accurate facts of node's modern function, velocity and route.
- **Wireless Communication:** VANET is designed for the wireless surroundings. Nodes are related and trade their records via wireless. Therefore a few security degrees have to be taken into consideration in verbal exchange. Time Critical: The records in

VANET need to be brought to the nodes with in time restrict so that a choice may be made with the aid of the node and carry out action as a result.

- **Sufficient Energy:** The VANET nodes haven't any issue of power and computation sources. This lets in VANET usage of stressful techniques consisting of RSA, ECDSA implementation and additionally affords unlimited transmission power.

1.3 Architecture of VANET

This part depicts the framework engineering of vehicular specially appointed systems. VANET engineering can be partitioned into various structures in view of alternate point of view. VANET are utilized for communication between vehicles for the diverse sort of use, for example, street safety, stimulation, movement control, and so on. VANET give data auspicious to drivers and obliged specialists to give safety to clients. In VANET, there are two sorts of communication. One is distributed (P2P) referred to as V2V communication as appeared. V2V communication happens between vehicles. Second is the Vehicle-to-roadside unit (RSU) which is known as V2R, which happens amongst vehicle and RSU. In V2R communication, a vehicle speaks with the closest RSU. The required message is sent by RSU if and just if vehicles are in the scope of those RSU. Something else, RSU makes an impression on the neighbour RSU for communication. In which, communication is finished by take after three distinctive sort of process, for example,

- Inter-vehicle communication (V2V)
- Vehicle to roadside communication (V2I)
- Inter-roadside communication

- **Vehicle-to-vehicle communication**: which is increasingly fundamental and essential in VANET inquire about, alludes to the in-vehicle space. Its communication can give an information trade stage to the drivers to share data and cautioning messages, in order to grow driver help. This is otherwise called bury vehicle communication or unadulterated specially appointed systems administration. In this classification, the vehicles convey among each other without framework bolster. Any significant data gathered from sensors on a vehicle, or conveyed to a vehicle, can be coordinated to neighbouring vehicles.

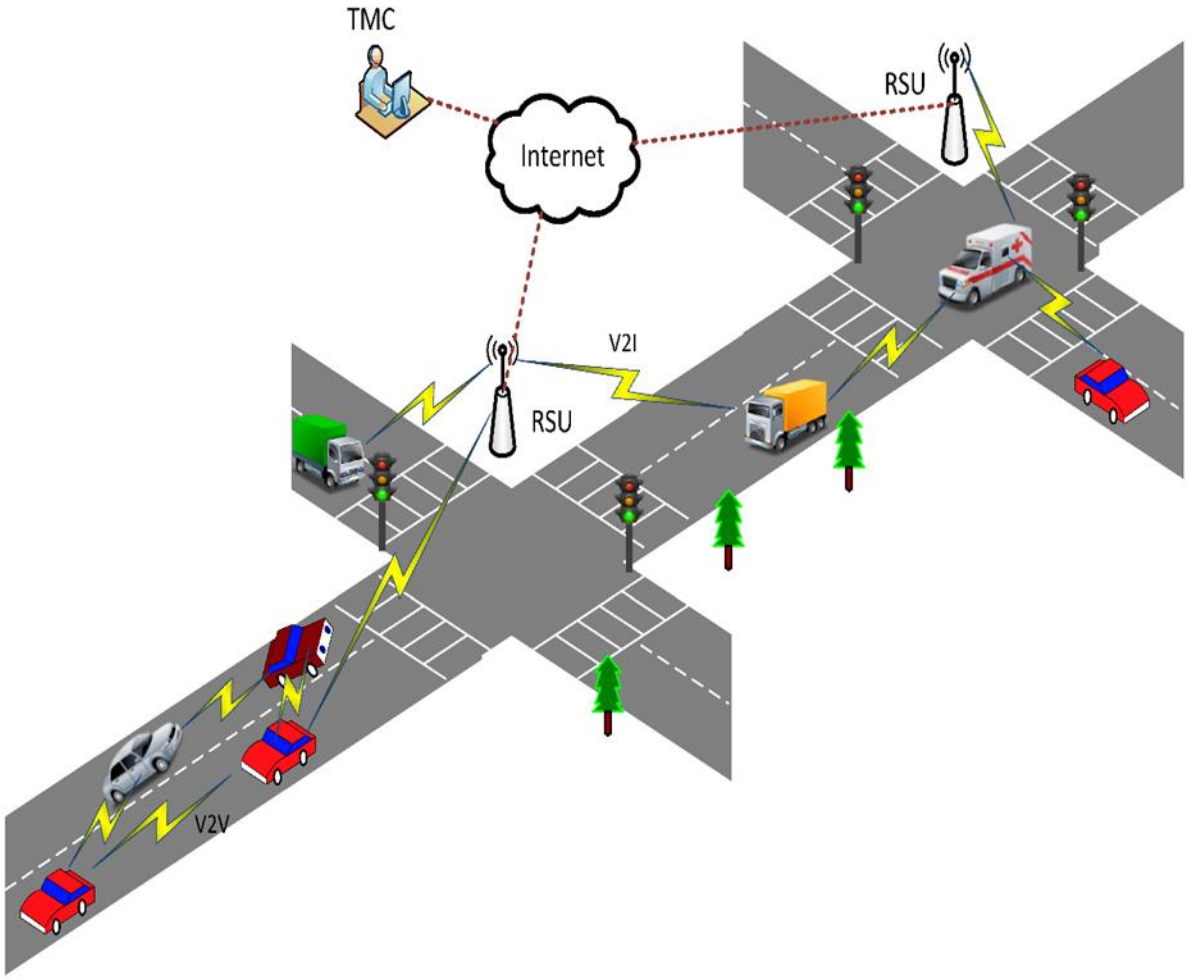

Fig. 1.3. VANET Architecture

- **Vehicle-to-road infrastructure (V2I) communication**: communication is another helpful research field in VANET. V2I communication empowers continuous activity/climate refreshes for drivers and gives ecological detecting and observing. This is otherwise called vehicle-to-vehicle (V2V) communication or unadulterated impromptu systems administration. In this classification, the vehicles impart among each other without foundation bolster. Any profitable data gathered from sensors on a vehicle, or imparted to a vehicle, can be coordinated to neighbouring vehicles [22].
- **Inter Roadside Communication:** This is otherwise called crossover Vehicles-to-Roadside Communication (VRC). Vehicles can utilize framework to speak with each other and trade data got from foundation or from different vehicles through specially appointed communication. Other than that, vehicles can speak with framework either in single-hop or multi-hop form contingent upon their area amid moving or stationary. This design incorporates V2V communication and gives more noteworthy adaptability in

substance sharing and expands arrange unwavering quality it implies that vehicles may impart by means of Wi-fi broadband components. As the broadband cloud may incorporate more movement data and observing information and in addition infotainment, this kind of communication will be helpful for dynamic driver help and vehicle following.

1.4 Application of VANET

The RSU can be dealt with as a get to point or switch or even a support point which can store information and give information when required [1]. VANET have been imagined to be useful in street safety and numerous business applications. For instance, vehicular systems are utilized to get ready drivers to planned congested roads, giving expanded handiness and viability. It is utilized to communicate accident guidance to drivers behind a vehicle to maintain a strategic distance from multi auto crashes. All information on the RSUs are broadcasted by vehicles. A grouping of utilizations is likewise done by as Car to Car Traffic applications, Car to Infrastructure applications, Car to Home applications and Routing based applications. In view of the kind of communication either V2I or V2V, we are orchestrating the uses of VANET into taking after classes:

- Safety oriented,
- Commercial oriented
- Convenience oriented and
- Productive Applications

1.4.1. Safety Applications: Safety applications encompass tracking of the encompassing road, drawing near motors, floor of the road, road curves and many others. The Road safety packages can be classified on numerous classes which include actual time traffic, co-operative message switch, put up-crash notification and traffic vigilance [3]. In Real-time site visitors information can be stored at the RSU and can be available to the automobiles each time and anyplace needed. This can play a vital function in fixing the troubles together with site visitors jams, avoid congestions and in emergency signals consisting of accidents and many others. In Post-Crash Notification car concerned in a coincidence might broadcast caution messages about its role to trailing cars in order that it can take choice with time [19].

1.4.2. Commercial Applications: Business applications will give update to the driver regarding offers, advertise about new goods and services. The Commercial applications can be aides in downloading of customized vehicle settings or transferring of vehicle diagnostics

from/to framework. Vehicles can get the opportunity to web through RSU if RSU is filling in as a switch Map of ranges can be downloaded by the drivers as per the essential before taking off to another zone for travel direction. Also, Content Map Database Download goes about as a gateway for getting gainful information from convenient issue zones or home station, On-ask for movie encounter won't be restricted to the prerequisites of the home and the driver can ask for persistent video hand-off of his most adored films. This is especially for the expert centres, who need to pull in customers to their stores. Statements like oil pumps, expressways restaurants to report their organizations to the drivers inside communication run. This application can be open even without the Internet.

1.4.3. Convenience Applications: This application is used to enhance traffic efficiency. By this application, traffic can be managed and degree of convenience for drivers can be increased. Route and journey planning can be made in case of road congestions. Parking Availability is also essential convenience software. It is notified regarding the provision of parking in the metropolitan towns helps to locate the availability of slots in parking plenty in a certain geographical region [2].

Fig 1.4 Electronic toll collections [2]

1.4.4. Productive Applications: We are deliberately calling it efficient as this utility is additional with the above noted applications. The Productive applications may be Time Utilization. By using this application, it is easy to predict the topography of the roads. Moreover, it helps driver to adjust vehicles speed and optimize their fuel usage [2]. One can browse the Internet whilst a person is waiting in vehicle for a relative or buddy and also Fuel Saving. This application can be used for the toll collection. Payment can be done electronically.

1.5 Challenging Issues in VANET

VANET seems simple and straight forward networks. But, designing and implementation of vehicular network is not easy. For the implementation of these networks, there are some technical as well as economic challenges [4]. The technical challenges are Message Authentication Code (MAC) design, congestion and collision control, network management, security issues and environmental impacts. As in VANETs, it is easy for adversary to still data, so security is major challenge in VANETs. Hence, in VANETs messages should be secured so that only legitimate user can access it. In addition, during the deployment of VANETs social and economic challenges are faced. It is quite difficult to convince manufacturers for the construction of such system which conveys the message during the traffic rules violation. This system is quite costly also, as such systems have high resource requirement [6].

1.6 VANET VS. MANETS

Table 1.1 VANETs vs. MANETs

Properties	**VANET**	**MANETs**
Node's mobility	Well defined mobility of nodes in vehicular ad-hoc network because of roadways.	Random mobility of node in mobile ad-hoc network.
Energy Constraint	Continuous energy is provided by vehicle. So there is no issue of energy conservation.	Energy conservation is issue because batteries are used for energy.
Connectivity	Disconnected network because of high dynamic nature.	No issue of connectivity.
Network Size	Large network can be available by using extended network.	Network size is limited.

Summary

VANET is the special elegance of Mobile advert hoc networks (MANET). The principal goal of the use of VANET is to offer safeness or comfort for passengers and drivers on the road however now so many accidents happens on the street because of attacks. If VANET cannot overcome the attacks and their community can't offer accurate facts and safety to consumer then it'd be unserviceable generation. VANET has drawn raise concentration in recent years due to its broad range of utility.

CHAPTER 2
REVIEW OF LITERATURE

Some examination has as of now been done in the regions of VANET applications and activity safety. The accompanying areas will give a short review of some of this exploration, which will help in the examination for this work.

Arshad R, Ikram N (2013), "Elliptic curve cryptography based mutual authentication scheme for session initiation protocol" [18].
In this paper, authors have said that Tsai's authentication scheme for session initiation protocol is at danger of user anonymity attack and stolen verifier attack. Moreover, it does not provide known-key secrecy and perfect forward secrecy. Keeping in mind they have offered ECC using discrete logarithmic problem. The proposed authentication scheme not handiest opposes these attacks but rather additionally manages more security and execution.

Xue Yang, Jie Liu, Feng Zhao, Nitin H. Vaidya (2004), "A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning" [19]: In this paper author proposed a Vehicular Crash Warning Communication (VCWC) protocol to enhance street safety. In particular, it portrays blockage control routes of action for emergency alerted messages so that a low emergency advised message transport deferral can be proficient and a broad number of harmonizing abnormal vehicles can be supported. It in like manner familiarizes a procedure with discard dull emergency advised messages, abusing the normal chain effect of emergency events.

Hamed Arshad & Morteza Nikooghada (2014), "An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC" [28]: In this paper, author have shown validation conspire for session initiation protocol is unreliable against user impersonation attacks. This means that a legal user can impersonate other legal users to perpetrate toll fraud and use the VoIP network for making free long distance calls. Keeping in mind the end goal to enhance the security and productivity, we have proposed an ECC based validation and key understanding plan for session initiation protocol. The proposed scheme frustrates different attacks, as well as demonstrates a superior execution contrasted

with the related plans. Henceforth, our proposed plan is more appropriate for IP-based communication frameworks.

Hang Tu, Neeraj Kumar, Naveen Chilamkurti , Seungmin Rho(2014), "An improved authentication protocol for session initiation protocol using smart card"[20]: In this paper, we recognized security imperfection in Zhang et al's. authentication protocol for SIP. Zhang et al. s protocol can't withstand the impersonation attack. We in this way proposed an enhanced protocol that dispenses with the shortcoming. As per our investigation and exchange, the proposed protocol accomplishes shared verification, withstands different attacks, and is more productive.

Aytunc Durlanik, and Ibrahim Sogukpinar (2007), "SIP Authentication Scheme using ECDH" [21]: In this review, another plan is proposed for security of SIP. Proposed technique depends on ECC. Favored properties of ECC are utilized for verification of Session initiation protocol. Along these lines article covers the essential components of Session Initiation Protocol and security consideration relying upon the test/reaction systems. The recommended authentication scheme using Elliptic Curve derived from Diffie Hellman Key Exchange compromises the same robust structure against offline password guessing and server spoofing attacks. In addition, it is more proficient and best in the applications/gadgets requires low memory and quick exchanges.

Liufei Wu, Yuqing Zhang, Fengjiao Wang, "A New Provably Secure Authentication and Key Agreement Protocol for SIP Using ECC" [22]: In this paper author have proposed another validation scheme for SIP, which defeats the intrinsic shortcomings of Otherwise known as plan, accomplishes the authentication and a common mystery in the meantime and gives provable security in CK security show. This arrangement fits conveniently in the SIP protocols as depicted in RFC3261. The new protocol has security properties required by SIP standard and requires just negligible changes to the standard. The plan is intended to give data confidentiality, data integrity, authentication, access control, and perfect forward secrecy, and it is secure against known-key attacks. Also, NAKE depends on ECC, so it is more proficient and ideal in the applications which require low memory and fast exchanges.

Fuwen Liu and Hartmut Koenig (2011), "Cryptanalysis of a SIP Authentication Scheme" [23]: In this paper, author have demonstrated that Yoon's scheme is vulnerable to

off-line dictionary and partition attacks. An attacker can recover the correct password in a reasonable time.

Yanrong Lu, Lixiang Li, Haipeng Peng, Yixian Yang (2015), "A secure and efficient mutual authentication scheme for session initiation protocol" [29]: In this paper, author have exhibited a cryptanalysis of an as of recently proposed Zhang et al's. plan and demonstrated that their plan is as yet helpless against insider attack and does not give mutual authentication. To wipe out these shortcomings, we propose an upgraded mutual authentication scheme which has greater security properties as well as is more effective in regards to execution contrasted and past plans. In this way, the proposed ECC-based plan accomplishes common validation and low algorithm cost.

Debiao He, Muhammad Khurram Khan, Neeraj Kumar (2015), "A new handover authentication protocol based on bilinear pairing functions for wireless networks" [33] : In this paper, authors have considered He et al. (2012b) proposed an enhanced handover authentication protocol for Wi-fi systems to beat security shortcoming in their past protocol. Nonetheless, in the wake of surveying their protocol and breaking down its security, we exhibit their protocol is till admired to the private key traded off issue. The examination demonstrates that their protocol is unreliable for useful application. We likewise propose another handover validation protocol. The examination demonstrates our protocol could defeat the shortcoming in He et al's. protocol at the cost of expanding computational cost marginally. In this manner, our protocol is more reasonable for Wi-fi systems.

Farash MS, Attari MA (2013), "An enhanced authenticated key agreement for session initiation protocol" [32]: Authors have demonstrated that the Xie's scheme is vulnerable to the impersonation attack in which an active adversary with-out knowing the users' password and the server's private key can easily impersonate the server to the users and share secret keys with them. As a result, Xie's scheme also suffers from the off-line password guessing attack. To overcome the security weaknesses, they proposed an improved scheme and it is secure against well-known crypto-graphical attacks such as guessing attacks, replay attacks, but also provides mutual authentication, perfect forward secrecy and secure password change.

Xie Q (2012), "A new authenticated key agreement for session initiation protocol"[25]: In this paper, Xie Q has shown that the security-enhanced scheme of Yoon *et al.* for SIP is vulnerable to off-line password guessing attack and stolen-verifier attack. We proposed several countermeasures for defending against these attacks. In addition, we proposed a new

security-enhanced scheme for SIP, which not only defends against the attacks mentioned above but can also maintain the efficiency of the scheme.

Chou-Chen Yang, Ren-Chiun Wang, Wei-Ting Liu (2005), "Secure authentication scheme for session initiation protocol" [27]: In this article, authors have described the original SIP authentication procedure based on HTTP digest authentication. We pointed out that the procedure of the original SIP authentication scheme is vulnerable to the off-line password guessing and server spoofing attacks. Thus, we proposed a secure authentication scheme for the Session Initiation Protocol to resist the above attacks.

Yoon EJ, Shin YN, Jeon IS, Yoo KY (2010), "Robust mutual authentication with a key agreement scheme for the session initiation protocol" [26]: Authors have demonstrated the vulnerabilities of Tsai's nonce-based authentication scheme for the session initiation protocol to offline password guessing attacks, Denning–Sacco attacks, and stolen-verifier attacks, and also pointed out that it does not provide perfect forward secrecy. Then, to resolve such security problems, they have presented a new authentication scheme based on the elliptic curve discrete logarithm problem for SIP. As a result, the proposed authentication scheme resists those attacks, while also provides more security and efficiency which can be executed faster than other previously proposed related schemes including Tsai's scheme.

Sherali Zeadally(2010),"Vehicular Ad hoc Networks (VANETS): status, results, and challenges"[30]: Author describes about the various research fields available in VANETs. Various parameters are defined such as quality of service, routing, broadcasting, securities. This paper also describes about the advantages, disadvantages and limitation of these parameters. There is also need of some modification regarding the reliable and secure VANET.

Bhuvneshwari.s et.al. (2013), "A survey on vehicular ad-hoc network" [31]: Author describes the favourable approach for the Intelligent Transport System (ITS). In this paper, describes the favourable approach for the Intelligent Transport System (ITS). In this paper, author describes the various constraints to be addressed while employing VANET. Due to high dynamic topology in the dense area, traditional MANET protocols unfavourable for VANET. The aim of this paper is to give an overview of the vehicular ad-hoc networks and the VANET routing protocols.

J.T. Isaac, S. Zeadally, and J.S. Camara, (2010) "**Security attacks and solutions for vehicular ad hoc networks" [36].** In this paper, authors talked about a portion of the significant security attacks that have been accounted for on VANET. The authors displayed

likewise the comparing security arrangements that have been proposed to keep those security attacks and vulnerabilities. The primary security territories that they concentrated on incorporate obscurity, key administration, protection, notoriety, and area. In VANET, the safeguard against traded off nodes, and pernicious ones can be guaranteed by applying such sorts of frameworks. Area alludes to vehicle position in VANET that can be considered as a standout amongst the most significant snippets of data in geographic Routing. It is frequently promptly accessible through situating administrations, for example, worldwide situating framework (GPS).

Irshad Ahmed Sumra et al. (2013) "Classes of attacks in VANET"[34]: proposed five particular directions of attacks and every radiance is expected to offer higher viewpoints for the VANET assurance. The authors endeavoured to embrace a characterization and a recognizable proof of various attacks in VANET. In top notch Organize Attacks, assailants can immediately influence diverse vehicles and foundation. These attacks are at the abnormal state of peril on the grounds that those affect the entire system. The assailant is particularly intrigued by changing over substance used in applications and mishandling it for his or her own special endowments. The 0.33 class-Timing Attacks is a kind of attacks wherein assailants' most essential objective is to include some time fit in unique message, for instance, to make delays with the goal to piece this message gone to the collector before the close of its lifetime. All unmoral messages, which cause horrendous sentiments of different drivers, are marked into the heavenliness Social Attacks. At last, attacks wherein following and observing exercises are refined are laying inside the brilliance Checking Attacks. The related works above caution a disturbing situation of VANET safety. In the following segments, we expect to stress security necessities in VANET, then present all the more succinctly the suitable attacks, their comparing countermeasures and promoter each other classification of these attacks.

Salman bin Abdulaziz, Al-kahtani (2012) "Survey on Security Attacks in Vehicular Ad hoc Networks (VANET)" [35]: In this paper authors recognized distinctive security attacks. They portrayed Insider versus Pariah. In the event that the assailant is a part node who can speak with different individuals from the system, it will be known as an Insider and ready to attack in different ways. Though, an untouchable, who is not confirmed to specifically speak with different individuals from the system, have a restricted ability to play out an attack. The second classification is Noxious versus Objective. A vindictive aggressor utilizes different

techniques to harm the part nodes and the system without searching for its own advantage. In actuality, a sound aggressor expects its own advantage from the attacks. The following class is Dynamic versus Detached. A dynamic assailant can create new information to harm the system though a latent aggressor just listen stealthily the remote channel yet can't produce new packet. Actually, there is another ascribe to portray an assailant, which is displayed in Nearby versus Expanded An aggressor is considered as nearby in the event that it is constrained in extension, regardless of the possibility that it has a few elements. Something else, an augmented aggressor expands its extension by controlling a few elements that are scattered over the system.

O. A. Wahab, H. Otrok, and A. Mourad () "**A cooperative watchdog model based on dempster–shafer for detecting misbehaving vehicles" [37]:** the author proposed the VANET QoS-OLSR protocol to keep up the security of VANET and also Stable the Packetes of the communication in the system and overhead minimization. They proposed new Group based protocol for VANET called VANET QoS-OLSR. To diminish the soundness of group they include the parameters including speed and separation that speak to the versatility measurements to the QoS work. select the ideal way, select the MPR nodes with the goal that they communicate the three message to at most extreme 2-jump away nodes .

H. Sharma and R. Garg, **(2014) "Enhanced lightweight sybil attack detection technique" [38]:** it is created to enhance the lightweight Sybil attack identification procedure. In lightweight procedure there is one disservice, the Sybil nodes whose speed is under 10m/s are likewise distinguished as genuine nodes. To enhance this, they improved the lightweight Sybil attack location strategy. At the point when new node enters a system its RSS esteem is checked and it is confirmed regarding RSS upper bound esteem. On the off chance that got RSS estimation of node surpasses the RSS upper bound esteem then that node is perceived as Sybil node generally as authentic node.

A.Joshi, R.kaur,(2015)"A Novel Multi-Cast Routing Protocol for VANET" [39]: Authors outline the idea of Routing protocol. Proactive, receptive and half and half protocols are the three unique classifications of Routing protocols for specially appointed information systems, as indicated by. The first is a proactive routing protocol, which depends on the intermittent communicate of information system topology. This sort of protocol guarantees that all nodes dependably have a refreshed information of ways to different nodes. Keeping in mind the end goal to do this, a lot of information system assets must be utilized, which can

seriously constrain the measure of information that can be exchanged. The second class, receptive Routing protocols, can be seen as an answer for proactive routing protocolsince they scan for a route when one is required. Some well-known receptive protocols are DSR, AODV, and DYMO. Ultimately, half and half Routing protocols are a blend amongst proactive and receptive protocols. The last protocol, half and half protocols, misuse the quick conveyance of packet from the proactive protocols and the low overhead from the responsive protocols. A regular case is the Zone Routing Protocol (ZRP).

S. Janakiraman, S. Rajasoundaran, P. Narayanasamy, (2012) "The Model — Dynamic and Flexible Intrusion Detection Protocol for high error rate Wireless Sensor Networks based on data flow"[40]: In this paper, author is talking about Dynamic and flexible intrusion detection model to detect the intrusion node and prevents the denial of service attack. Author has discussed the how the same node will work as detector as well as forward the information to next node and also discussed the symmetric key sharing for this mechanism.

Zezhong Zhang, Qingqing Qi, Neeraj Kumar, Naveen Chilamkurti and Hwa-Young Jeong, "A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography"[41]: In this paper, author is discussed that his proposed technique is able to withstand user anonymity and stolen verifer attack as well as other attack also. In this paper author is discussing about elliptic curve cryptography to prevent the attack.

CHAPTER 3
OBJECTIVES

Now-a-days, modernisation has changed the people lifestyle. Everyone wants comfort, entertainment and security in their life but same time there is a problem of information security arises. To overcome this problem the role of cryptographic algorithm takes place to secure user precious information from various kind of attack. In VANET also it has a great role and it's become very important when comes to human safety and security. In India, every year various road accident takes place. Our Indian government is planning for Smart City in which Intelligent Transportation System(ITS) will be required and all these things will be controlled using Internet of Things(IoT). Based on this future scope we have tried to focus only on Session Initiation Protocol (SIP) security. In this thesis, we have following objectives:

- **To compare Quality of Services (QOS) like path delay, throughput and packet delivery ratio w.r.t. number of nodes**.
- **To provide enhanced security for session initiation protocol using Elliptic Curve Cryptography**.
- **To compare and analyse elliptic curve cryptography with AES-Dydog cryptographic technique for session initiation protocol.**

CHAPTER 4
SECURITY AND ROUTING PROTOCOL

4.1 Routing Protocols in VANET

The routing protocol proposed for indicate point communications in VANET can be characterized into topology-based and position-based protocols. For the outline of vehicular system, routing protocol is the primary test because of increment in nature of element topology [8]. As Routing is the best way to transmit information from one vehicle to others. To give the safety or safe place to the individual, trading of messages ought to be finished with between vehicle communication. Routing in VANET is more testing than the MANET in light of exceedingly changes in element topology attributes [9,10]. So, finding and keeping up the best ways of communication in attractive condition is the most troublesome undertaking in VANET.

Topology based and position based routing protocol are predominantly utilized by the VANET framework. As in topology based Routing protocol, for sending information from source to goal it uses connection's data inside the system. It can be characterized by two approach: proactive and responsive Routing protocol. Proactive is table driven protocol which utilizes most limited way algorithm to exchange information. The tables are additionally imparted to the neighbours to locate the ideal way amongst source and the goal on the grounds that if any refresh required, then every node can refresh their routing table. Responsive routing protocol is approached request protocol since it keeps up route disclosure prepare inside the system. The routing protocol are named appeared in figure-4.1.

4.1.1 Topology Based Routing Protocols

These protocols discover the route and keep up it in a table (alleged table driven) before the genuine communication begins with the nodes. Topology based routing protocol utilize connection's data, which put away in the Routing table inside the system to send the information packet from source to goal. Topology based Routing methodology can be additionally sorted into Proactive (table-driven), Receptive (on-request) and Half breed.

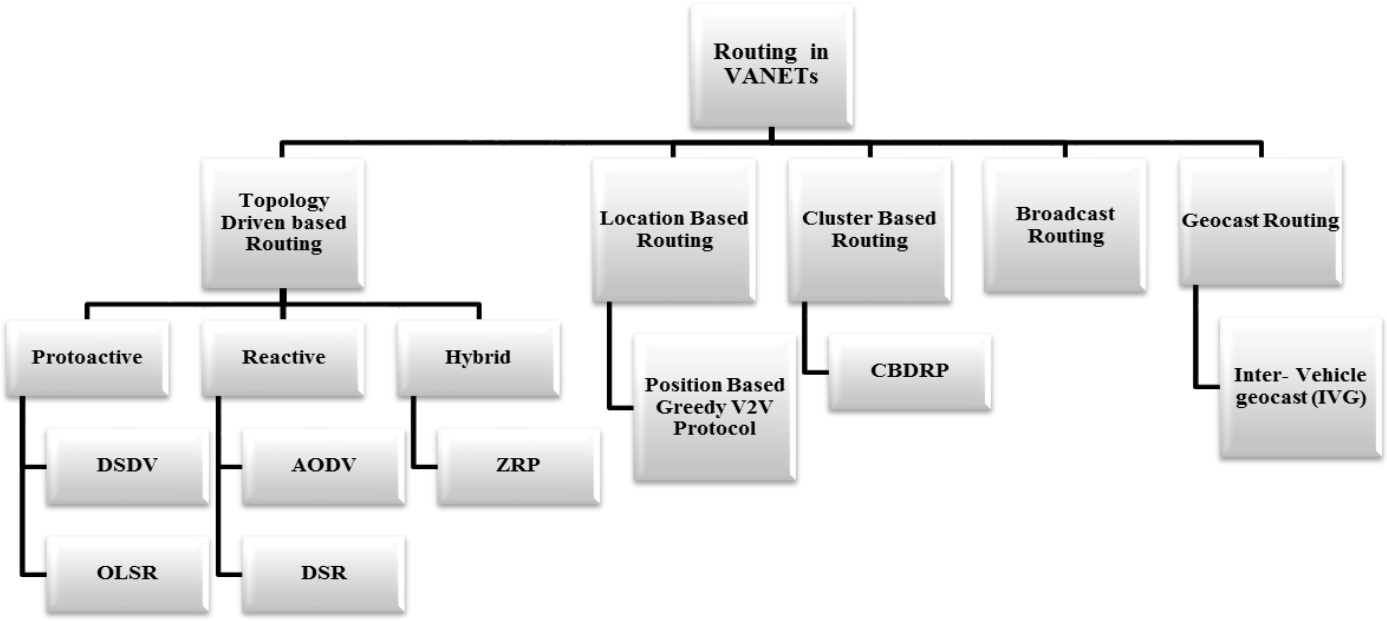

Fig. 4.1. Routing protocols used in VANET

4.1.1.1 Proactive Routing Protocols: In these protocols, also called "table-driven", each node maintains one or more tables containing routing information for all destinations. To keep routing tables updated, this class requires a periodic exchange of control packets between nodes.e.g. OLSR, TBRPF and so on.

- **Destination Sequenced Distance Vector (DSDV) Routing Protocol:** DSDV depends on the most limited algorithm. The primary reason for this algorithm is to tackle the Routing circle issue. Just a single circle or defeat is actualized from one node to other node. Every node in the Routing table is having its own succession number to be available in the system zone. Goal Sequenced Separate Vector is a soonest specially appointed routing protocol. It utilizes most limited way algorithm and gives one route to each node, which put away in the Routing table. Each routing table conveys data about all the system nodes, which can get to. In this protocol routing data is communicate occasionally and incrementally To keep up routes

unwavering quality every node of this system must communicate its route table intermittently to the neighbours. Be that as it may, DSDV protocols are not appropriate for extensive systems.

- **OLSR Routing protocol:** The Improved Connection State road Protocol. OLSR is a proactive connection state routing protocol which is utilized for strength and exactness of the vehicles. The idea of multipoint hand-off is utilized as a part of this protocol which forward communicate messages amid the flooding procedure, along these lines decreasing the message overhead. Advanced Connection State road protocol depends on the customary connection state system. OLSR continues Routing table conveys data about all conceivable outcomes of routes to the system nodes. This protocol is presented for exactness and solidness for information Routing in the system. If there should arise an occurrence of changed system topology every node must need to give its refreshed data to the specific nodes. Each system node gets refreshed data for just a single time, however unselected nodes are not ready to get refreshed data. OLSR disregard high assets functions of node, (for example, transfer speed, transmission run). In addition, it is reasonable for huge and thick system.

4.1.1.2 Reactive Protocols: In this family also known as "on-demand driven", the path computation is done only on request. Then the routing operation consists of two phases: the route discovery phase to route data and the updating phase executed when the network topology changes e.g. DSR [11], TORA and so on.

- **AODV (Ad Hoc on Demand Distance Vector):** This is a table-driven Routing protocol can be utilized as a part of unicast and multicast protocol. This protocol keeps up a table to the nodes when a demand is made by the source. Specially appointed On Request Remove Vector routing protocol is approached request in light of the fact that in AODV a route is produced when a system node needs to send information parcel to another. In this when a system node is demand for a route then route revelation process is enacted. It diminishes abundance memory prerequisites and route excess [37]. AODV can be pertinent to the extensive scale specially appointed systems.

- **The Dynamic Source Routing (DSR):** DSR protocol [37] exhibited in which use source Routing and keep up dynamic routes. It having two stages route revelation and route support. This protocol is a multi-hop Receptive Routing protocol. It arranges overhead reductions by diminishing occasional messages. This kind of protocol applies source Routing and keep up dynamic route. Two fundamental operations of DSR protocols are: Route Disclosure and Route Support that makes DSR protocol self-sorted out. In this protocol, each information conveys a total rundown of the middle of the road nodes, and if there is any fizzled route, source node ought to erase it from reserve. On the off chance that it stores other effective route to the goal in its reserve, it will trade the fizzled one by another fruitful route. Any periodical refresh is not required in DSR. In any case, DSR can't repair the broken connections locally. [11]

4.1.1.3 Hybrid Protocols: combination of receptive and proactive routing protocol which prompts diminish the underlying route disclosure delay in responsive Routing protocols e.g. ZRP, HARP [9]and so forth.

- **ZRP (Zone routing protocol):** A Routing zone is given to every one of the nodes and separated into covering zones. ZRP gives fringe throwing by IARP to control movement between zones. This is utilized to build the productivity of route system. This zone is a blend of privately gave nodes or the nodes which are outside the area zone. Nodes are effectively accessible with the nearby zone yet for the outside zone, it requires route revelation which can help neighbourhood Routing data.

4.1.2 Location Based Routing Protocols

The basic role of this Routing protocol is to discover the area of the goal node subsequently in position Based routing protocol every node decide area of itself and in addition goal node. In this topographical position of the node is utilized to locate the best route. There are numerous area administrations protocols are accepted and furthermore different models were additionally actualized for the area based protocols. Position based Routing protocol is additionally called geographic routing protocol. This protocol depends on the positional data in routing procedure; where the source sends a parcel to the goal utilizing its geographic

position. This protocol required every node can choose its area through the geographic position framework (GPS) help. With the progression of GPS based area administrations, position based Routing protocols are picking up significance. In these protocols, the bundle is sent with no learning of advanced guide to the one-jump neighbour, which is the nearest to the position of the goal. Area based protocols are appropriate for VANET. Area based Routing is comprehensively separated in two sorts; position based ravenous V2V protocols, postpone tolerant protocols.

4.1.2.1. Position Based Greedy V2V Protocols: In this insatiable sending procedure is utilized. Next node is passing the message to the most distant node to get the following goal. In this approach, middle of the road node ought to know the area of itself, area of the neighbour and area of most distant node. The postponement ought to be limited while transmitting the information between the nodes and to goal node.

4.1.3 Cluster Based Routing Protocols

Clustering is the procedure in which the system is separated into interconnected sub structure called as groups. Each packet having a cluster head which go about as a switch between every one of the packets and perform administration functions. Passage nodes give communication between the group heads. This procedure limits the Routing overhead and diminishing the system activity.

4.1.3.1 Cluster-Based Directional Routing Protocol (CBDRP): when the packet are sending, the main thing in this protocol matter is speed, speed and route. While moving in same bearing, source node is sending information to group head. Presently the duty of this is to forward the bundle to the packets inside [9].

4.1.4 Broadcast Protocols

Broadcast protocols are utilized for broadcasting messages to every one of the nodes in the system. This for the most part gives the data about activity proficiency, sharing, climate and estimating, street conditions among vehicles and conveying declarations. In this multi-hop packet are utilized for the message broadcasting. In VANET, it can be utilized for little quantities of nodes. The different Communicate routing protocol are BROADCOMM, UMB, VTRADE and DV-CAST [9].

4.1.5 Geocast Protocols

Geocast routing protocol [39] is mostly utilized for the security reason, activity effectiveness and so forth. Geo cast routing is fundamentally an area based multicast Routing. it transmits the data from one source vehicle to all vehicle which are situate at a particular place or district called ZOR (Zone of Significance).

4.1.5.1 Inter-Vehicle Geocast (IVG): The principle reason for the IVG Routing protocol is to educate vehicles about any peril at the interstate situated at hazard ranges called multicast gathering [39]. Accordingly give security by getting message cautions

4.2. Attacks on Vehicular Networks

Like any other communication and data processing systems, VANET are exposed to various types of threats and attacks. The absence of the energy problem and the ability of an OBU to accommodate dozens of microprocessors give the vehicle an important capacity of processing and computing. Compared to a regular ad hoc network [8], this represents two significant benefits for VANET nodes. Due to the high mobility in VANET, the two mentioned advantages affect the feasibility of attacks. Thus, there are possible attacks in an ad hoc network that will be impossible for VANET and vice versa [30].

Given the diversity of VANET possible threats and attacks, and in the interests of clarity and simplification, it is necessary to classify them. Several classifications have been proposed in the literature [8,34].

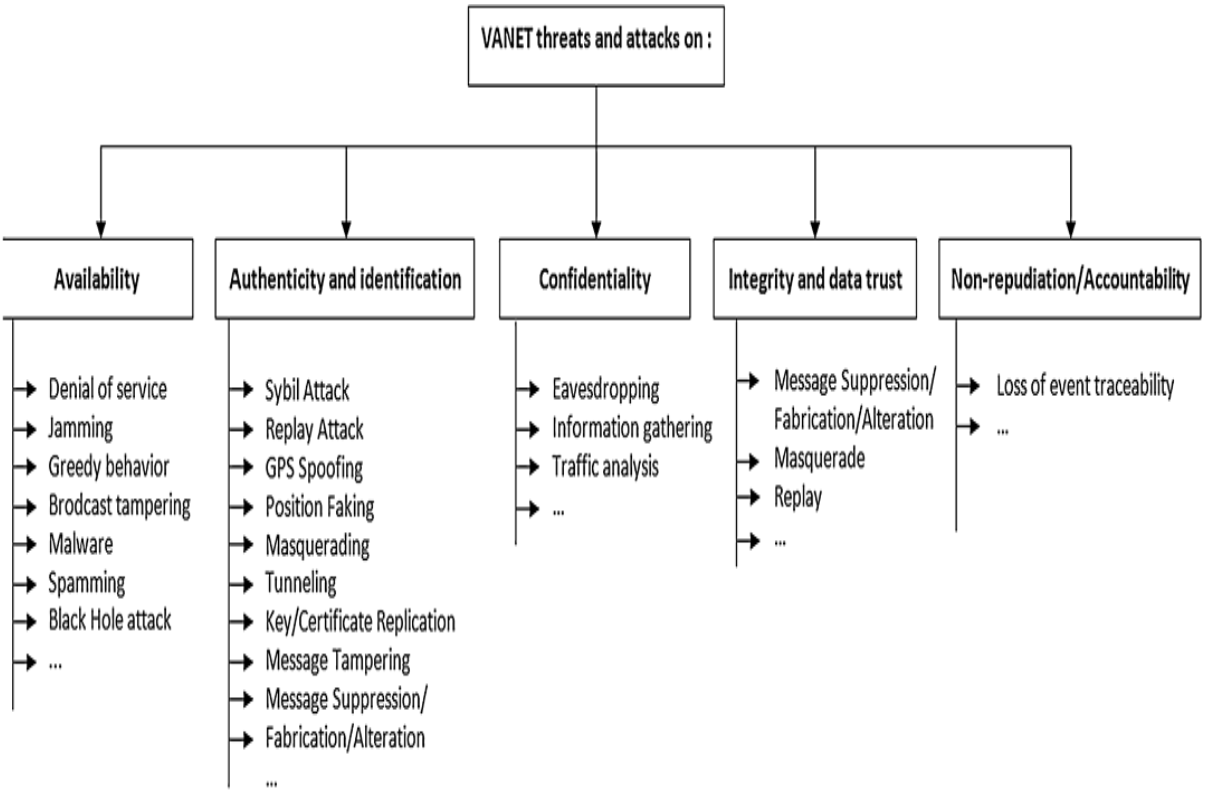

Fig. 4.2. Various attacks in VANET

4.2.1. Attacks on availability: Availability is a totally critical component for VANET. It ensures that the network is practical, and useful information is avail- able at any functioning time. This critical security requirement for VANET, which most important reason is to make sure the customers' lives, is a vital goal for most of the attackers. Several attacks are on this class, the maximum well-known are the Denial of Service attacks (DoS) [30].

- **Denial of Service attacks:** The Denial of Service (DoS) attacks actually include a family of attacks targeting the availability of network services, which can have serious consequences especially for VANET applications. Because of their impacts, DOS attacks are classified as a dangerous class of attacks. They can be performed by internal or external malicious nodes to the network. In these attacks, the attacker tries to block the principal means of communication and aims to interrupt services, so they will not be available to legitimate users [8]. As an example, flooding the control channel with high volumes of messages generated by intentionally manufacturing. The network nodes (OBU and RSU) will not be able to handle the huge amount of received data. DDoS attack (Distributed Denial of Service) is a variant of DOS attacks, it is a distributed attack ordered by a main attacker who plays the role of

"attack manager" with other agents who may be also victims unknowingly. The action methods of DDoS attacks are in most cases flooding the network and the results are always disastrous. Jamming, greedy behaviour, blackhole attack, are examples of DOS attacks.

- **Jamming attack:** The jamming attack, is a physical level of Denial of Service attack. Jamming in its basic definition is the transmission of a signal to disrupt the communications channel, it is usually intentional [12]. This lowers the signal to noise ratio (SNR: Signal to Noise Ratio) for the receiver. Unintentional interference is called "interference" and occurs when a transmission is made in a frequency band that is already in use and operational. For a successful adaptive jamming attack, the jammer must act at the same time that the activity of the useful signal to jam. It must also choose the most effective signal transmission model that merges the best the receiver. In a VANET network, jamming once successful, can have inevitable consequences. Some research works such as [12] have looked for some techniques to reduce the effect of jamming for mobile ad hoc networks.
- **Greedy behaviour attack:** The Greedy attack is an attack on the functionality of the MAC layer according to the architecture of the OSI model. The greedy node does not respect the channel access method and always tries to connect to the media. The main purpose is to prohibit other nodes to use the sup-port and services. A greedy behaviour node tries also to minimize its waiting time for faster access to the channel and penalize other non-compromised nodes. Greedy behaviour causes overload and collision problems on the trans- mission medium, which produces delays in authorized user's services. Greedy behaviour is independent and hidden to upper layers, then it cannot be detected by mechanism designed for those layers.
- **Blackhole attack:** The Blackhole attack is a protocol attack against the availability in ad hoc networks, it exists also for VANET. In Blackhole attack, the malicious node receives packets from the network, but it refuses to participate in the operations of routing data. This disrupts the routing tables and prevents the arrival of vital data to recipients mainly because the malicious node always declares being part of the network and able to participate, which is not the case practically. The effect of this type of attacks is more dangerous for VANET than other mobile networks. A Blackhole node can e.g. redirect the traffic that receives to a specific node which does

not exist in fact and this causes data loss [8]. Blackhole attack can also be used as a first phase of a man in the middle attack that we detailed later.

- **Grayhole attack:** This attack consists in removing only the data packets of certain applications that are vulnerable to packets loss. Grayhole is considered as a Blackhole attack variant. **Sinkhole attack:** This attack consists that the malicious node attracts neighbouring nodes so their packets go through it, this helps to eliminate or modify the received packets before re- transmitting them eventually. The Sinkhole attack can be used to mount other attacks as Grayhole and Blackhole [13].
- **Wormhole attack:** Wormhole is a foreswearing of administration attack, it requires the interest of no less than two nodes. It basically comprises that an assailant A makes an impression on an aggressor B geologically a long way from him, that B communicates totally. This message recommends to neighbouring nodes of B, that an is their neighbour. This attack permits at least two real nodes and non-neighbours (their radio transmission territories don't over-lap) to trade control information between them to make non-existent streets.
- **Malware attack:** Given the existence of a software components to operate the OBU and RSU, the possibility of infiltration of malware (malicious software) is possible in the network during the software update of VANET units [8]. The effect of a malware is similar to the effect of viruses and worms in an ordinary computer network, except that in a VANET network, disruption of normal functionality is always followed by serious consequences.
- **Broadcast tampering attack:** In this type of attack, the attacker tries to make and inject fake security alert messages in the network. This may hide the true safety messages to legitimate users, it can cause also accidents and seriously affect the overall network security. In general, this type of attack is possible for a legitimate node.
- **Spamming attack:** As in a web environment, the spam messages such as advertisements e.g. have no utility for users. In a VANET network which is a mobile radio environment, this type of attack aims to consume bandwidth and cause voluntary collisions. Given the lack of a centralized management of the transmission medium, this makes more difficult the control of such attacks [8].

4.2.2. Attacks on authenticity and identification: Authenticity is a noteworthy test of VANET security. Every current station in the system must verify before getting to accessible

administrations. Any infringement or attack including the procedure of ID or validation uncovered all the system to a genuine result. Guarantee valid ness in a vehicular system is to shield the credible nodes from outside or inside assailants invading the system utilizing a distorted personality. The significance of identification–authentication process originates from the way that it is every now and again utilized at whatever point a vehicle needs to join the system or an administration [27,28]. There are a few sorts of attacks in this classification.
-

- **Sybil attack:** The idea of the Sybil attack as presented for the first time is that a malicious entity can present multiple identities at once. One of the direct means by which two entities can convince a third that they are distinct is to run, at the same time, some tasks that one entity cannot do it alone. To ensure the identity of a node, several techniques have been proposed such as testing resources based on computational, storage and communication challenges [38]. The Sybil attack is a dangerous attack in a VANET environment, given the disastrous consequences it can cause.
- **GPS spoofing/position faking attack:** In a VANET, the position in-formation is of crucial importance, it must be accurate and authentic [8]. This attack consists on providing neighbours node a false location information. The exact location information can easily be obtained from a system such as GPS, whence the name of the attack: GPS spoofing. Each vehicle of a VANET is equipped with a positioning system (receiver), then the at-tack can be achieved using a transmitter generating localization signals stronger than those generated by the real satellites [5]. Successful GPS spoofing attack can facilitate other attacks such as attacks against applications which use the position of the node as an identification method [27].
- **Node impersonation attack:** Every vehicle has a network ID which allows to distinguish it among the other node of the VANET [9]. This identifier becomes especially important in case of problems. In the impersonation attack, the attacker obtains a valid ID and passes for another legitimate vehicle in the network. This constitute a violation of authentication process in the network [28].
- **Tunnelling attack:** The tunnelling attack is almost similar to the wormhole attack [4]. In this attack, attackers use the same net- work to establish a private connection (tunnel), while in the Wormhole the attackers (assumed to be external) use a different radio channel for the exchange of packets. The Tunnelling attack connects two

distant parts of the vehicular network by using an additional communication channel such as a tunnel [8]. Thus, the victims of two distant parts of the network can communicate as neighbours.

4.2.3. Attacks on Confidentiality

- **Eavesdropping attack:** In wireless networks, such as VANET, listening to the media is an attack easy to carry out. In addition, it is passive and the victim is not aware of the collection. Eavesdropping attack is against confidentiality, it is without imminent impact on the network [8]. Through this attack, several types of useful information can be collected such as location data that can be used for tracking vehicles.
- **Traffic analysis attack:** In a VANET, the traffic analysis attack is a passive serious threat against confidentiality and privacy of the users. The attacker analyses collected information also delete a part of the message, alter or make new messages which help him achieving its intended purpose of the attack [34].
- **Illusion attack:** A direct application of the fabrication of messages attack is the Illusion attack, which is an attack against integrity and data trust. It consists in placing voluntarily sensors which generate false data. These data can move normally in the network and require drivers interaction to make decisions. Authentication mechanisms are not able to detect this attack, because the attacker connects to the network in an authentic way. Masquerading, replay, tampering, deleting, manufacturing, alteration, and illusion of messages can be also considered as attacks against the authenticity and identification. after a phase of listening to the network, it tries to extract the maxi-mum of useful information for its own purposes.
- **Stolen verifier attack:** In this adversary tries to access user information from remote server [25,41]. Based on this information he/she will try to get information.

4.2.4. Attacks on Integrity and Data Trust

- **Masquerading attack:** In this attack, the attacker is hidden using a valid identity (called a mask), and tries to form a Blackhole or produce false messages that have the appearance of coming from an authentic node. For example, to slow down the speed of a vehicle or require it a lane change. A malicious node at-tempts to act as an emergency vehicle e.g. and thus cheat the other vehicles.

- **Replay attack**: This is a classic attack, it consists in replaying (broadcast) a message already sent to take the benefit of the message at the moment of its submission. Therefore, the attacker injects it again in the network packets previously received. This attack can be used e.g. to replay beacons frames [14,24], so the attacker can manipulate the location and the nodes routing tables. Unlike other attacks, replay attack can be performed by non-legitimate users [32,35,41].
- **Message Tampering/Suppression/Fabrication/Alteration:** As its name implies, this attack is against integrity it consists in modifying, deleting, constructing or altering existing data. It can occur by modifying a specific part of the message to be sent. For example, the attacker falsifies received data indicating that the route is congested, and changes them to deceive users, so it indicates that there is no congestion and traffic on the road is normal. In this attack, the attacker can also delete a part of the message, alter or make new messages which help him achieving its intended purpose of the attack.
- **Illusion attack:** A direct application of the fabrication of messages attack is the Illusion attack, which is an attack against integrity and data trust. It consists in placing voluntarily sensors which generate false data. These data can move normally in the network and require drivers interaction to make decisions. Authentication mechanisms are not able to detect this attack, because the attacker connects to the network in an authentic way. Masquerading, replay, tampering, deleting, manufacturing, alteration, and illusion of messages can be also considered as attacks against the authenticity and identification.

4.2.5. Attacks on non-repudiation and accountability

- **Loss of events traceability:** Despite its importance, we have not seen any document that addresses this attack that we find quite feasible in a VANET environment. In fact, this non-repudiation attacks consists of taking action, allowing subsequently an attacker to deny having made one or more actions traces and creating confusion for the audit entity. Some attacks can serve as preliminary to non-repudiation attack such as Sybil attack and duplication of keys and certificates.

4.2.6. Other attacks

- **Attacks on privacy:** These attacks represent a major violation of privacy of drivers and VANET users. Several studies in the literature classify the attacks of privacy as a separate category for VANET. As a practical example, we find: – Tracking: the pursuit of a vehicle during its journey [8,23].

Social Engineering: Knowing. whether a vehicle at a definite moment is in the garage or in circulation.

- **Timing attack:** The timing attack is to delay the transmission of messages with high requirements on propagation delay, and transmit them e.g. after adding time preventing their treatment in a normal way. Some classifications also consider this category as a separate family of attacks.
- **Brute force attack:** The Brute force attack can be against the confidentiality of exchanged messages or the encryption keys. It can be additionally against the recognizable proof or validation professional cess. This attack can be performed e.g. while attempting to discover the system ID of the vehicle by lexicon examining process. In a VANET situation where association times are moderately short, Savage constrain attack is difficult to direct, since it is tedious and asset escalated.
- **Man in the middle attack:** The man in the centre attack can be accomplished in a few settings. As its name shows, the at-tacker is embedded between the transmitter and the beneficiary. On account of VANET, the aggressor is a vehicle which is embedded between two vehicles that convey. The assailant controls the communication between the two nodes, while they trust that they are in direct communication with each other. In the writing, the man in the centre attack is utilized to damage the authentication and additionally the trustworthiness and non-renouncement instruments [41].

4.3. Security requirements in VANET

VANET must fulfil some security prerequisites before they are sent. A security framework in VANET ought to fulfil the accompanying prerequisites. The claim to secure the VANET are the equivalent to the safe alternate systems. The request of secure the VANET is to ensure the data by an unapproved node and the data can't be embedded or changed by an

unapproved individual. The goal is to give Authentication, Privacy, Uprightness and Accessibility.

- **Authentication:** Authentication guarantees that the message is created by the honest to goodness client. In VANET a vehicle responds upon the data originated from the other vehicle thus authentication must be fulfilled. It is the way toward confirming the character of somebody.
- **Availability:** Availability requires that the data must be accessible to the real clients. DoS Attacks can cut down the system and henceforth data can't be shared. It implies that the system works legitimately and administration ought to be accessible 24*7.
- **Non-Repudiation**: Non-repudiation implies a node can't deny that he/she doesn't transmit the message. It might be essential to decide the right arrangement in crash reproduction.

4.4 Cryptography

All the security administrations given by cryptography called cryptographic primitive. Present day cryptography offers a few security methods, for example, confidentiality, authentication, integrity, non-repudiation, secret sharing. To fulfill these security administrations, cryptography utilizes strategies, for example, encryption/unscrambling algorithms, Keys generation and exchange protocols, hash hash functions, digital signature and a lot of other techniques. In the accompanying, we primarily depend on the renowned reference [15] of Bruce Schneier for the introduction of the diverse cryptographic primitives.

- **Confidentiality:** It is the primary issue that has been postured to cryptography. Privacy is to guarantee that messages must be perused by the individuals who are approved. In a VANET, the data traded is generally open, aside from those identified with the protection of clients.
- **Authentication:** It enables the recipient to confirm the origin of the data, and if the issuer is the one who claims to be. A VANET client ought not have the capacity to go for another person. The advanced mark is a standout amongst the most utilized answers for validation issues.

- **Integrity:** It implies that the collector can guarantee that the got message is the message that has been issued and it has not been modified in travel. An attacker ought not have the capacity to change messages. One way hash functions frame the that in the writing, the expression "legitimacy" implies both authentication and uprightness, and it is frequently mistaken being used for validation.
- **Non-renouncement:** It is to guarantee that a player cannot deny having done an activity. In a VANET setting, a vehicle ought not have the capacity to deny sending a notice e.g. or, then again having done an attack.

4.4.1 Encryption/decryption

The principle of encryption and decryption of a message, described schematically in Fig., is as follows:

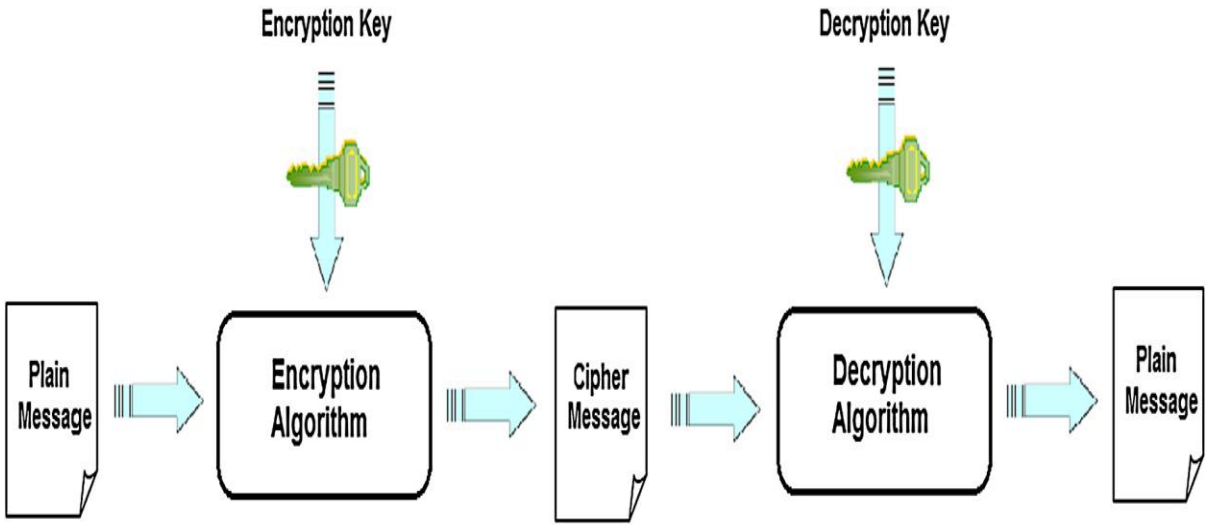

Fig 4.3 The principle of encryption/decryption.

- An algorithm for encryption/decoding, which is an arrangement of data operations handling in light of numerical functions, gets as information a reasonable message and an encryption key, then thus it yields a scrambled message.

- The encryption/decoding algorithm gets as info an encoded message and an unscrambling key, then therefore it yields the comparing clear message.

4.4.2 Symmetric cryptography

Likewise, called secret key cryptography. For this method, the decoding key can be effectively ascertained from the encryption key, practically speaking it takes the same. Security in symmetric cryptography depends on the capacity to keep the key mystery between imparting parties. In the event that the key is uncovered the framework is bargained. The prerequisite that both sides have admittance to the mystery key is one of the primary downsides of symmetric cryptography in contrast with uneven one[17].

4.4.3 Asymmetric cryptography

Additionally, known as open key cryptography. The guideline of Working is as per the following:

- Each client has a couple of keys, one private key that he should keep mystery, and the other open key that he should make it accessible to the general population.
- If we scramble with the general population key, just the private key can unscramble and the other way around.
- It is for all intents and purposes incomprehensible (time and assets) to decide e.g. the private key knowing the general population one and the other way around.

Asymmetric cryptography can also be used in encryption, but compared to symmetric algorithms it is usually slower. It is mainly used in the key exchange procedures and in digital signature authentication tool through digital certificates. The public key cryptography solves several problems which secret key cryptography does not succeed. Several proposed public key cryptographies based solutions for some security issues in VANETs will be discussed later.

4.4.4 PKI, digital certificates and timestamping*:* The management of private and public keys for a large number of users requires the establishment of a PKI: Public Key Infrastructure which is a set of software, hardware and procedures components. A PKI can provide several security services, the most important is to be a trust third party between digital counterparts. PKI ensures that role through the certification authority (CA), so it signed, delivers and keep up to date digital certificates which rep- resent a digital ID for an

entity. In fact, a certificate is an electronic file (can be stored in many forms), which binds together a public key with an identity with the guarantee of the certification authority. A certificate allows to authenticate and sign (signing certificates) and also encrypt messages (encryption certificates). Timestamping is also among the services that PKI can provide. It certify that an event (send/receive/signing a message, ...) happens at a given time. The timestamping faces basically to authentication and non-repudiation attacks. In a VANET context, several solutions e.g. propose the creation of a PKI related to VANETs named VPKI (Vehicular Public Key Infrastructure), and propose the use of digital certificates as a method of rapid authentication in a vehicular network. This pro- posed solution will be discussed later for some related attacks

4.5 Elliptic Curve Cryptography

ECC is a new cryptography technique, and considered as an excellent method because of the small size of key for the user. It is difficult to break. An attacker needs more time to exploit the key. ECC, with the size of 160-bit key provides better security than the protocol cryptography RSA with a size of 1024-bit. ECC provides the more security to the message. The key size is small, which gives the fast-cryptographic procedures, running on more compact software's. For the ECC, the hardware implementation is also compact due to a small key size. It is a sufficient cryptography system for wireless networks. Because it provides the bandwidth saving. ECC was introduced by V. Miller [16] and Neal Koblitz. ECC is a more secure algorithm; it cannot be easily breached by the intruder.

When there is a choice of elliptic curve it should rely on its domain parameters, the finite field representation, elliptic arc algorithms for field arithmetic as well as elliptic curve arithmetic. In the ECC, there is public key as well as a private key. Private Key is the hidden key of the algorithm. In the concept of symmetric key cryptography, there is only single key used for encryption and decryption. In asymmetric key cryptography, public key is used for message encryption. Public Key is distributed publicly and known to everyone. ECC has used asymmetric key cryptography scheme for encryption and decryption [18].

The ECC is used in huge application. ECC can give better security with small key size than other algorithms. By using the ECC, speed can be enhanced. This can enhance the bandwidth, and storage that are the fundamental limitations of resource-constrained devices. The Elliptic curve Discrete Logarithm Problem (ECDLP) (Hankerson et al., 2004) is the impossible computational problem for Elliptic curve [18,21].

In Figure 4.4, Elliptic curve whose point at infinity far to the top and bottom of graph.

$$Y^2=x^3+ax+b \quad \ldots\ldots (1)$$

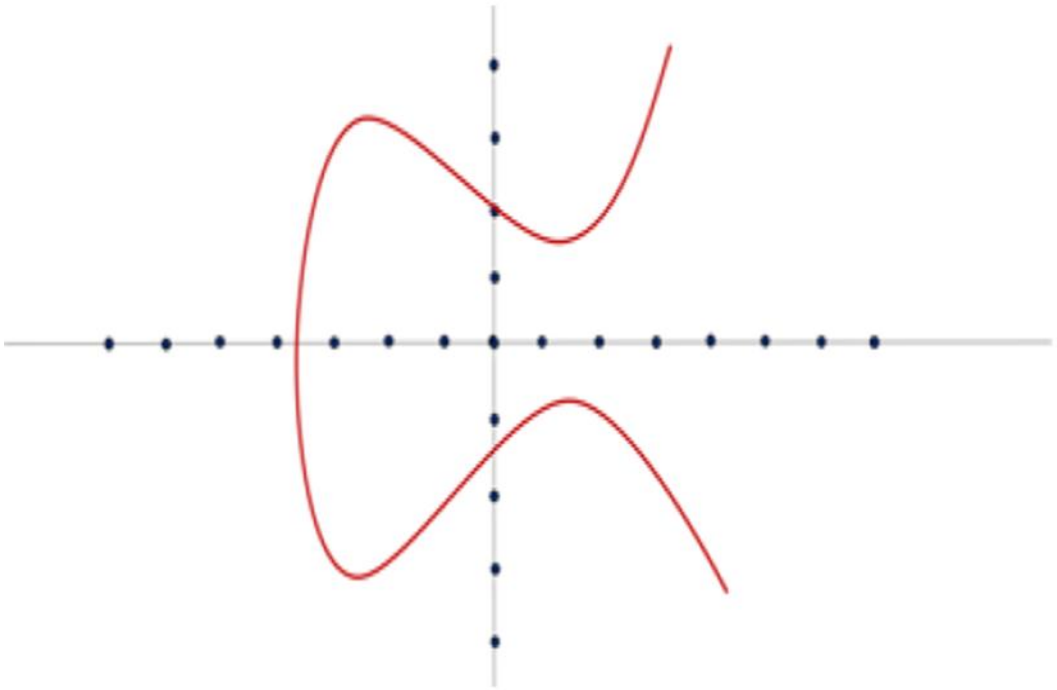

Fig 4.4. Elliptic curve

The Elliptic curve is applied to Abelian group. In Figure 4.5, P and Q are represented on curve for group law and line was drawn from P to Q until the line hit the curve again. It makes the point on the curve. Then, line was drawn from that point. The line was intersected on a curve, which makes the other point on the curve which is R=P+Q.

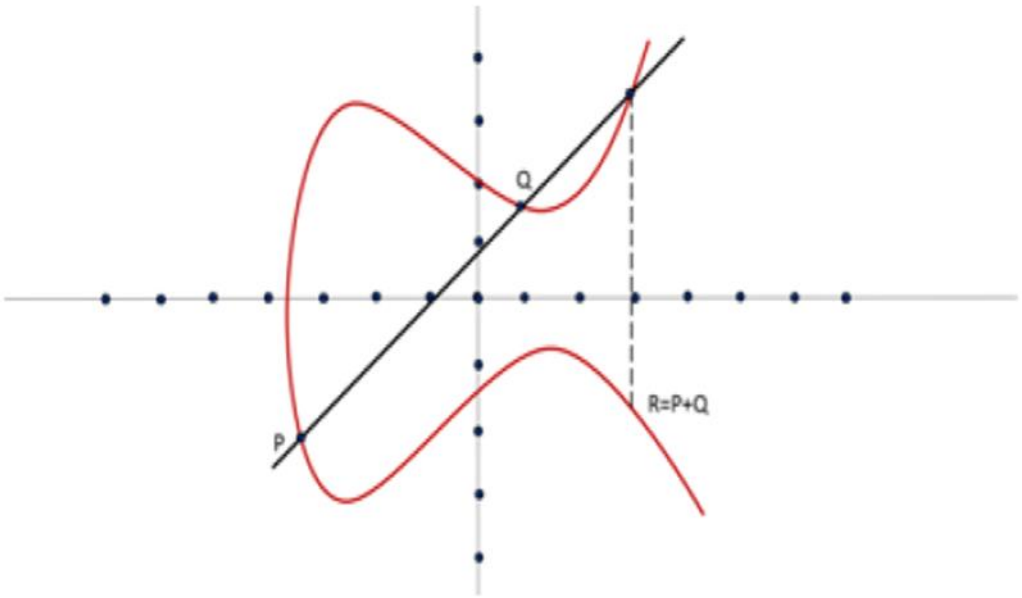

Fig 4.5 Group law on elliptic curve

4.6 Advanced Encryption Standard (AES)

The AES figure is for all intents and purposes Equivalent to the square figure, Rijndael figure created with two remarkable Belgian cryptographers. The algorithm characterized by means of AES is a symmetric-key algorithm, esteem a similar key is utilized for both information encoding and unscrambling. The inner rounds number of the figure is a component of the key length. The considerable number of rounds for 128-piece key's 10. Dislike its ancestor DES, AES does no longer utilize a Feistel arrange. Feistel systems don't encode a whole square for each emphasis, e.g., in DES, 64/2 = 32 bits are scrambled in one round. AES, on the other unmistakable hand, encodes every one of the 128 bits in a solitary new discharge. This is the one rationale why it has a similarly minimal number of rounds [15]. To improve the security, interchanges between remote nodes ought to be encoded to ensure the touchy information. Cryptography is an imperative instrument to accomplish the communication security in remote systems by changing over the decipherable plaintext into trivial figure content.

- Symmetric key symmetric block cipher.
- 128-bit data, 128/192/256-bit keys.
- Stronger and faster than Triple-DES.
- Provide full specification and design data

The Propelled Encryption Standard is a piece figure standard created by Joan Daemen and Vincent Rijmen and created by NIST, the US National Foundation of Gauges and Innovation. AES is a variation of Rijndael with a settled square size. AES figures utilize a 128-piece square and 128, 192 or 256-piece keys. The bigger square size opposes birthday attacks while the substantial key size averts beast drive attacks. It is effective in both programming and equipment. It was chosen through an open rivalry including many cryptographers amid quite a long while. For animal drive attack, AES is certainly more secure than DES because of the bigger size key, for measurable attacks, various tests have neglected to do factual examination of the ciphertext, and for differential and direct attacks, there are no differential and straight attacks on AES so far. The fundamental components of AES are: - AES does not utilize a Feistel arrange. It utilizes 10, 12, or 14 rounds. - 128-piece input/yield information square size - 128, 192, and 256-bits key sizes. The key size relies on upon the quantity of rounds. - AES utilizes one S-enclose which takes 8 bits and yields 8 bits.

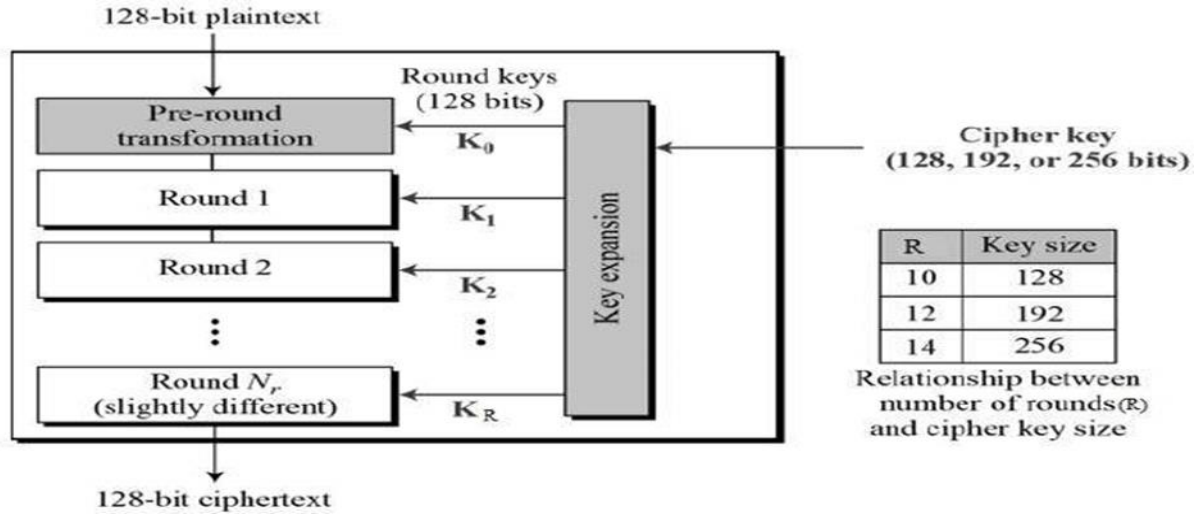

Fig. 4.6. AES Structure

4.7 Dynamic Intrusion Detection Protocol Model (DYDOG)

Wireless Sensor Networks (WSNs) are simply the accumulation – sorting out sensor nodes sent in different physical situations statically or progressively relies on the application. In Wi-fi condition these sensor nodes are protection less or defenceless against attacks. To take care of this issue the Intrusion Detection System (IDS) has been utilized and for remote systems, Dynamic Intrusion Detection System (DIDS) has been utilized. Be that as it may, this is not adequate to accomplish greatest versatility against attacks. Considering the issues here a DYDOG has technique is implemented to protect the node from various attack [40].

4.7.1 DYDOG technique

DYDOG is a technique to detect the several attacks like Blackhole attack, Wormhole attack, Sybil attack and selective forwarding attack, by creating the dynamic intruder detection node called Compromised Node(CN) in sensor node. Here node will be monitored by more than one. In this technique, we are detecting each and every node so that malicious node can be detected. Here the task of node is not only detecting or monitoring of the node but also, they a responsible for forward the node dynamically. The node itself takes decision/action against any kind of attack and send the update to their neighbour nodes without any cluster head [37]. Behaviour of node as forwarding node in the forwarding list is for a moment and then become idle dynamically until this node is one hope neighbour. The nodes will become only idle when they are one hop distance and they are not in the path of forwarding node. The nodes which are one hop distant from forwarding node will act as Intrusion detection when data transmission taking place and other nodes functionality are stable. At a single time one node is monitored by more than one DIDN node. If any malicious activity or attack is traced by any adversary node and other node has also sensed this activity then action will be taken against the malicious node. This is a method in which it is very difficult for intruders to identify and attack on intrusion detection node. we are considering the idle node which is one hope from forwarding node as Dynamic Intrusion Detection Node when these nodes are not coming in their forwarding path.

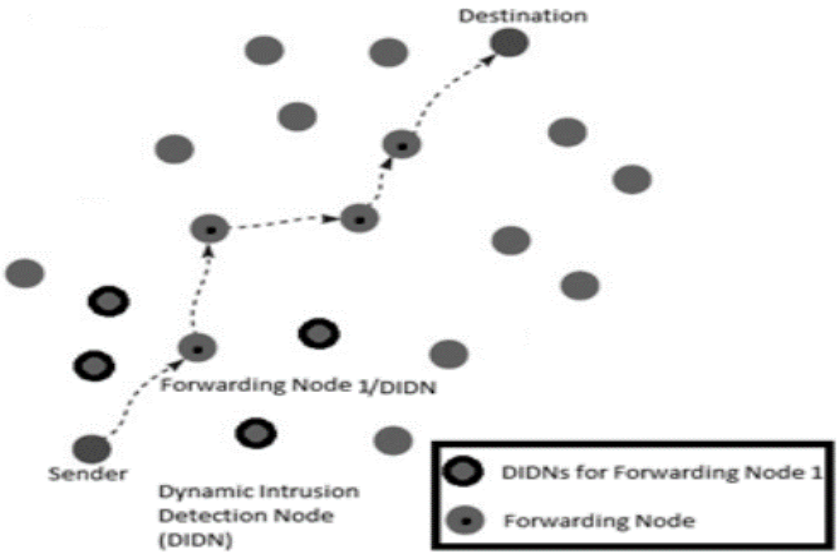

Fig. 4.7. DIDN and Forwarding nodes[40].

In worst case scenario, if the forwarding node is not detected by at least two Intrusion detection nodes or due to maximum mobility the data rate over the nodes will increase the overhead then the intrusion detection which is placed at one hop distance will select next hop neighbour node as DIDN for actual forwarding node if that monitoring node within the transmission range of forwarding node.

Since monitoring node is two hop distant from forwarding node. it happens only when higher data is transmitted but there is no need of maintaining two hop information all time to the forwarding node. During critical situation or higher data rate situation one hop distance monitoring nodes will share its own information with forwarding node as its second hop monitoring node dynamically with predefined node shared session key. In this way, we can increase the availability of Intrusion detection node in the worst scenario.

We select this Intrusion Detection Node using secure key management and malicious node are also avoided to act as monitoring node.

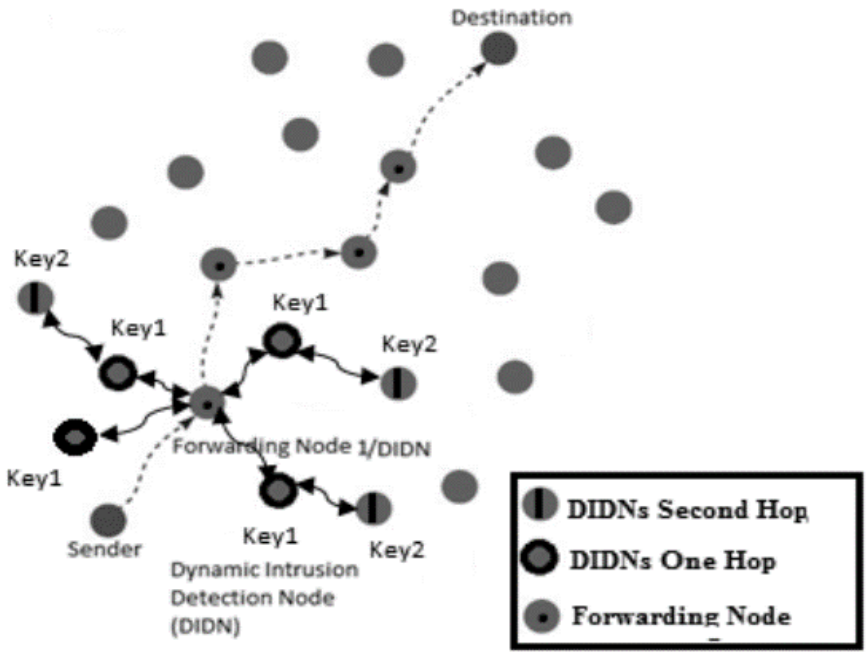

Fig. 4.8. Secure DIDN Selection (Hop-2) with Shared Secret Session Key (Key2)[40].

4.7.2 Secret Key management

For selection of DIDN we have to use secure way which identify malicious node from DIDN. To achieve this Intrusion detection node should maintain two secretly shared session key. The key will be generated using forwarding node partial data bits like sender's ID and monitoring

node's ID (node to be chosen as DIDN). These two ID's are concatenated in forwarding node and EX-ORed in intrusion detection node and send that key to forwarding node. By using reverse EX-OR operation, monitoring node's ID is checked. In this manner security is increased against intruder node. it is very difficult to find the session key within a particular session and using this authentication mechanism we can avoid malicious node [40].

4.7.3 Decision key for decision making Dynamic Intrusion Detection(DMDIDN)

In this we are talking about decision after attack is identified. When intruder attack is identified, more than one intrusion detection node monitoring forwarding node having one hop distance from that monitoring node. Each monitoring node should find attack as much as possible, but when any action is taken against these attack, Intrusion detection node will select alternative path and reroute the data via alternatively selected forwarding path after healing the attacked node or infected packet. Even though there are various intrusion detection node but only one will take decision of route change within intrusion time.

Here Forwarding node will send the decision key to their monitoring nodes and wait for reply from those nodes. The nodes reply with decision making key which is having TTL field to the forwarding node. the node which has lowest TTL value will be selected as decision making intrusion detection node. In next step for ensuring authentication the forwarding node will only send initial portion of data to the selected intrusion detection node. After this rest data will be sent to authentic node to make sure route selection. Depending on node mobility decision making node selection changes [40].

Summary

In this chapter illustrate the various routing protocol, troubles and their safety in VANET. Also explain various prevention techniques of attacks. In this chapter Elliptic Curve Cryptography, Advance Encryption Standard and Dynamic and Flexible Intrusion Detection Protocol (algorithms) - model has been explained for secure transmission in high error condition of Vehicular Ad-hoc Network. Here every single node acts as intrusion detection node in addition to forwarding node dynamically.

CHAPTER 5
RESEARCH METHODOLOGY

The Session Initiation Protocol (SIP) is widely used in the world of multimedia communication as a signalling protocol for controlling communication on the internet, establishing, maintaining, and terminating the sessions. To ensure communication security, many authentication schemes for the SIP have been proposed. However, those schemes cannot ensure user privacy since they cannot provide user anonymity. We have proposed the novel approach to secure the session against various attack like user anonymity, stolen verifier attack, and various denial of service attack.

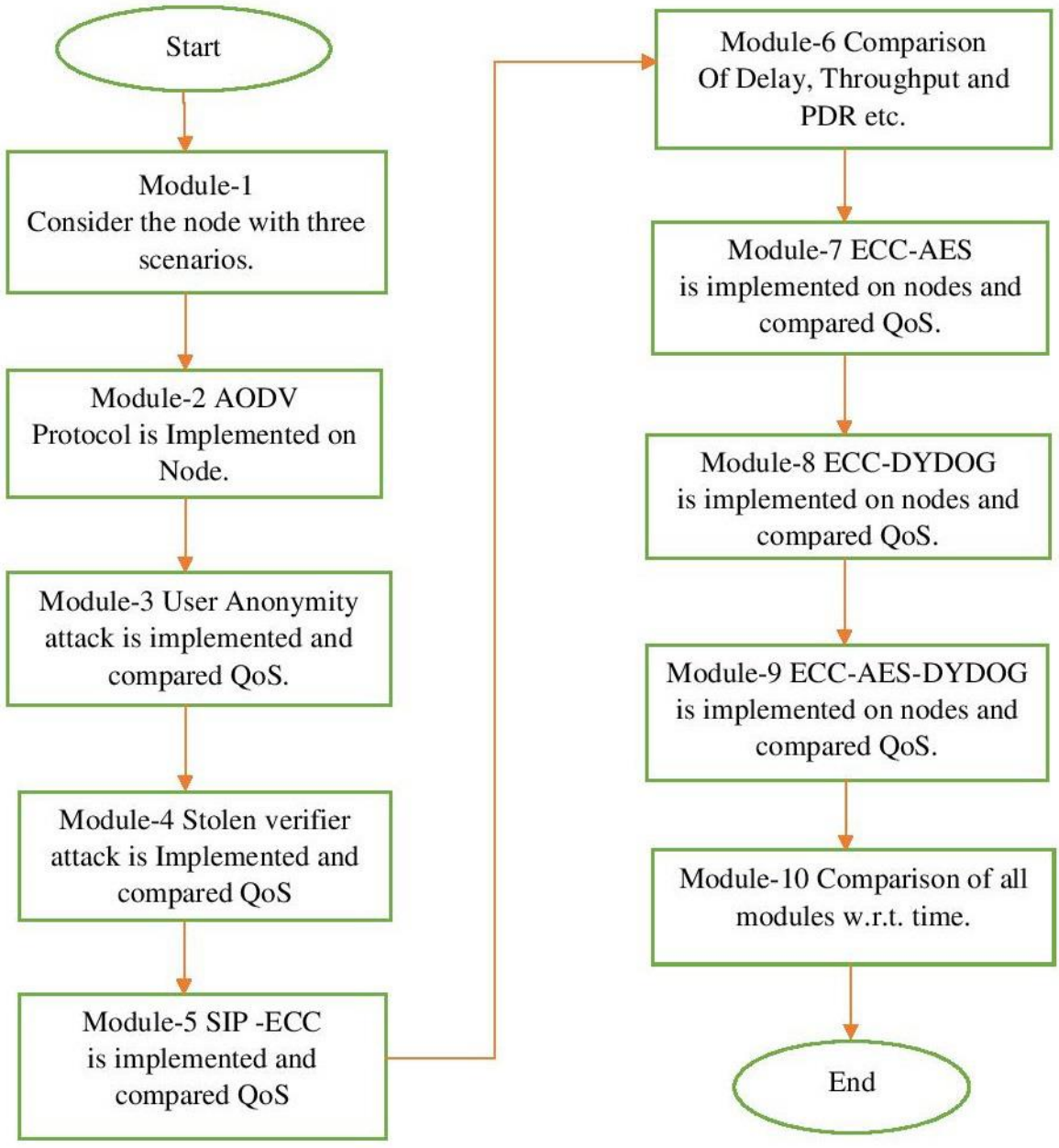

Fig. 5.1 Flow chart of research methodology

As one of the most important protocols supporting multimedia services, the Session Initiation Protocol (SIP) is widely used in both of the wired network and the wireless network. The SIP is an application layer control protocol which could create, modify and terminate sessions with one or more participants. These sessions include multimedia distribution, internet telephone calls and internet multimedia conferences. Authentication is the most important aspect in the SIP since it could stop illegal user to access the multimedia services. Therefore, authentication scheme for the SIP is gaining more and more concern in modern multimedia services. Many authentication schemes for the SIP were proposed in the past decade.

We have used various module to complete our objective they are as follows:

5.1 Module Description

Module description are as follows:

5.1.1 Module-1 Generation of traffic with respect to number of nodes

Let us take some nodes randomly and they start data transmission it means communication among them started. We don't know how to transmit the packets and basic needs of network topology. It can be wired or wireless or adhoc networks. Building a simple topology with minimum number of nodes for example 7 nodes will be deployed in the network. We are going to use AODV routing protocol to transmit packets. Node configuration, wireless configuration, channel type, cbr, sink, tcp and basic procedures will be used in the module. Node size, color, source and destination will be given by this module. This is just a simple packet transmission with simple topology. Considering there is no threat and attack we are observing the node's delay, throughput and packet delivery ratio.

5..1.2 Module-2 Implementation of AODV

In this module, we are going to implement the routing protocol to the node. We have taken Ad-hoc on-Demand Distance Vector protocol (AODV). We are going to build a complex topology with more number of nodes and same configurations will be set as above. In this we will be giving the mobility to all nodes with different timings. Hence nodes will be in mobile

at the respective time. Here we are using AODV protocol and node will be routed using the same. Some code minimization will be carried out in this module. We will take values of QOS parameters like average delay, packet delivery ratio, throughput at the corresponding time like 2,4,6,8,10. The values are inserted in a system generated trace file and graph will be schemeted for each parameter.

5.1.3 Module-3 User Anonymity Attack

User anonymity means that the adversary cannot get the user's identity from the message transmitted in the login and authentication phase. We have built a complex topology with more number of nodes and same configurations will be set as above. In this we will be giving the mobility to all nodes with different timings. Hence nodes will be in mobile at the respective time. Here we are using AODV protocol and we will be routed using the same. Some code minimization will be carried out in this module. USER ANONYMITY ATTACK will be introduced in the network to check the performance. We will take values of QOS parameters like end to end delay, packet delivery ratio, throughput at the corresponding time like 2, 4,6,8,10. The values are inserted in a system generated trace file and graph will be schemeted for each parameter. Attacker is trying to access the user identity and he/she is able to get the users identity by hook or crook. Now there will be some data loss when communication takes place among nodes. Here network performance will be degraded.

5.1.4 Module-4 Stolen Verifier Attack

In stolen Verifier Attack, the adversary steal the password-verifier stored in the database of the remote server and use it to login in the remote server. When the nodes are transmitting their packets this intruder steal password and get access of data so there is a loss in data transmitted and nodes energy is also increasing. We have built a complex topology with more number of nodes and same configurations will be set as above. In this we will be giving the mobility to all nodes with different timings. Hence nodes will be in mobile at the respective time. Here we are using AODV protocol and we will be routed using the same. Some code minimization will be carried out in this module. STOLEN VERIFIER ATTACK will be introduced in the network to check the performance. We will take values of QOS parameters like end to end delay, packet delivery ratio, throughput at the corresponding time like 2,

4,6,8,10. The values are inserted in a system generated trace file and graph will be scheme for each parameter. Here network performance will be degraded.

5.1.5 Module-5 Implementation of SIP-ECC

In this section, we have implemented the communicating node scenario. Let the intruder node is mixed among communicating node and he is trying to get user's identity from the message transmitted in the login and authentication phase. the user sends the protected identity. Then he will face with the computational Diffie-Hellman problem. Therefore, the proposed authentication scheme for the SIP could provide user anonymity.

The stolen-verifier attack means that the adversary steal the password-verifier stored in the database of the remote server and use it to login in the remote server. In the registration phase of the proposed scheme, the remote server stores username and password to remote server. The adversary could steal username and password. However, he cannot get the password verifier password since he does not the server's secret key. Therefore, the proposed authentication scheme for the SIP could withstand the stolen verifier attack.

5.1.6 Module-6 Comparison

The QOS values taken in module 2, module 3, module4 and module 5 will be added in a single user generated trace file and graph will be plotted correspondingly. This is just comparison module of AODV, USER_ANONYMITY, STOLEN VERIFIER and SIP ECC.

5.1.7 Module-7 ECC-AES

In this module, we have applied the novel technique (Advance Encryption Standard and Elliptic Curve Cryptography) on the different traffic scenario like 10, 30 and 50-nodes to protect the communication session from attack. AES is more secure than ECC as it uses 10, 12 and 14 rounds of processing for 128,192 and 256-bit key length respectively. Intruder node will try to get the packet but he/she is unable to get it since AES is used for authentication and node will ask for key shared between nodes. So, attacker is not able to attack since he/she doesn't have true key. There is some packet loss in the network due to link congestion or non-availability of bandwidth. Based on this we have calculated the QoS

parameter and compared with another module. After comparison, we have found that performance ECC-AES is more better than ECC.

Module-8 ECC-DYDOG

In this module, we have applied the ECC-Dydog encryption mechanism for securing the communication from malicious node so that we can protect our node from attacks. ECC-Dydog is implemented on different traffic scenario like low medium and high. We have calculated the QoS parameter after that we have compared these parameter with ECC implemented QoS parameter and found that ECC-DYDOG gives better results.

Module-9 ECC-AES-DYDOG

This is a module in which we have applied ECC-AES-DYDOG for encrypting the session among vehicles. This technique is implemented in low, medium and high traffic scenarios. Attacker node will drop the packet and this behaviour is detected by watchdog node. In dydog each node will behave as Watchdog node and this node will broadcast the attacker node ID in the network so that no other node will not communicate with attacker node. We are using AES for authentication of node. Hence, we are reducing the traffic and prevented attack in the network.

Proposed technique

Step-1: We have taken three scenarios like 10, 30 and 50 nodes and considered 50 node scenarios for analysing proposed technique. Moreover, four more nodes are considered i.e. node 51,52,53 and 54 which behaves as attacker node.
Step-2: To find the packet drop we have used Dydog technique**.**
Step-2.1: In Dydog technique all the normal node will behave like watchdog. We will observe the behaviour of every node.
Step-2.2: When source node will try to send packet to destination, attacker node will come forward in between and will receive the packet and drop it.
Step-2.3: The normal node behaving as watchdog will observe pattern of traffic flow from source to destination. When malicious node will drop packet, the watchdog node will detect this malicious node.

Step-3: Packet drop in the network may not be only due to attacker, it can also be possible that there is bandwidth blockage or link congestion. We will detect through AES to get to know whether these nodes are authentic node or not.

Step-4: Node, which has observed the node 51,52, 53 and 54 is dropping packet in the network, will ask their key. Node will reply with their key "XYZ" but the original key used in the network is "ABC".

Step-5: Since there is a mismatch in the key so observer node will consider that these nodes are not authentic and will confirm as malicious node.

Step-6: Now observer node will broadcast the malicious node ID in the network so that no other node will communicate with these malicious nodes.

Module-10 Final Comparison

In this module, we have done final comparison of all modules in a single graph window and find out the average delay, packet delivery ratio and average throughput with respect to time as well as number of nodes.

CHAPTER 6

SIMULATION AND RESULTS

6.1 Implementation

In this section, we are going to implement the base paper model assumption and try to get the results closest to base paper result. In base paper authors, have taken scenario of user anonymity and many more attacks. But we have implemented the two scenarios only first User anonymity and second Stolen verifier attack on network simulator-2. We will use the proposed Scheme(Module-9) To Overcome These Attacks.

6.2 Simulator

According to Shannon, simulation is "the process of designing a model of a real system and conducting experiments with this model for the purpose of understanding the behaviour of the system and/or evaluating various strategies for the operation of the system."

To test the proposed protocol, Network Simulator-2 is used. The first step of VANETs implementation is a simulation of the protocol. There are many network simulators available for network protocols like NS-2, OMNET++, MAPS^{TM}

Table-6.1 Simulation parameter

Simulation Parameters	**Values**
Number of nodes	10,30,50
Propagation model	Two ray ground
Antenna type	Omni directional
Routing protocol	AODV
MAC	802.11
Packet size	200
Simulation area	500*500

We have considered the above parameter given in the Table-6.1 to implement the node scenario in the Network Simulator-2. It is a tool which has following feature:

- It is used to check performance of the protocol which exists in the network.
- We can evaluate any new protocol before using in the network.
- We can use NS-2 for simulation of mobile adhoc network and protocol used.

- We can also simulate a no. of project on NS-2 which is not possible in real time

6.3 QoS Parameter

We have used following parameter for our study:

6.3.1 Delay

The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds.

6.3.2 Packet Delivery Ratio(PDR)

The calculation of Packet Delivery Ratio (PDR) is based on the received and generated packets as recorded in the trace file. In general, PDR is defined as the ratio between the received packets by the destination and the generated packets by the source.

Packet delivery ratio = (Received packets/generated packets) *100

6.3.3 Throughput

In data transmission, network throughput is the amount of data moved successfully from one place to another in a given time period, and typically measured in bits per second (bps), as in megabits per second (Mbps) or gigabits per second (Gbps).

6.4 Low Traffic Scenario (10-Nodes)

We are considering the low traffic in which only 10-nodes are communicating among themselves. Nodes are transmitting their data to interested user using Ad-hoc on-demand distance vector protocol (AODV). In this scenario, we have also considered that attacker node also mixed with nodes and try to access the data transmitted in the network. Here we are considering only user anonymity attack and stolen verifier attack. To save the node's session from user anonymity attack and stolen verifier attack we are using Elliptic Curve Cryptography(ECC) and comparing the QoS like delay, throughput and packet delivery ratio.

6.4.1 Average Delay:

Delay of nodes when simple AODV protocol is implemented it is less but when attackers are activated in the communication the delay is increasing in case of both user anonymity as well as stolen verifier attack. The increment in the delay during attack is attributed to the fact that the attackers do not forward the packet to the destination as a normal node. After the

application of the dydog mechanism along with the encryption techniques the value of delay is found to be best of all the other modules tested.

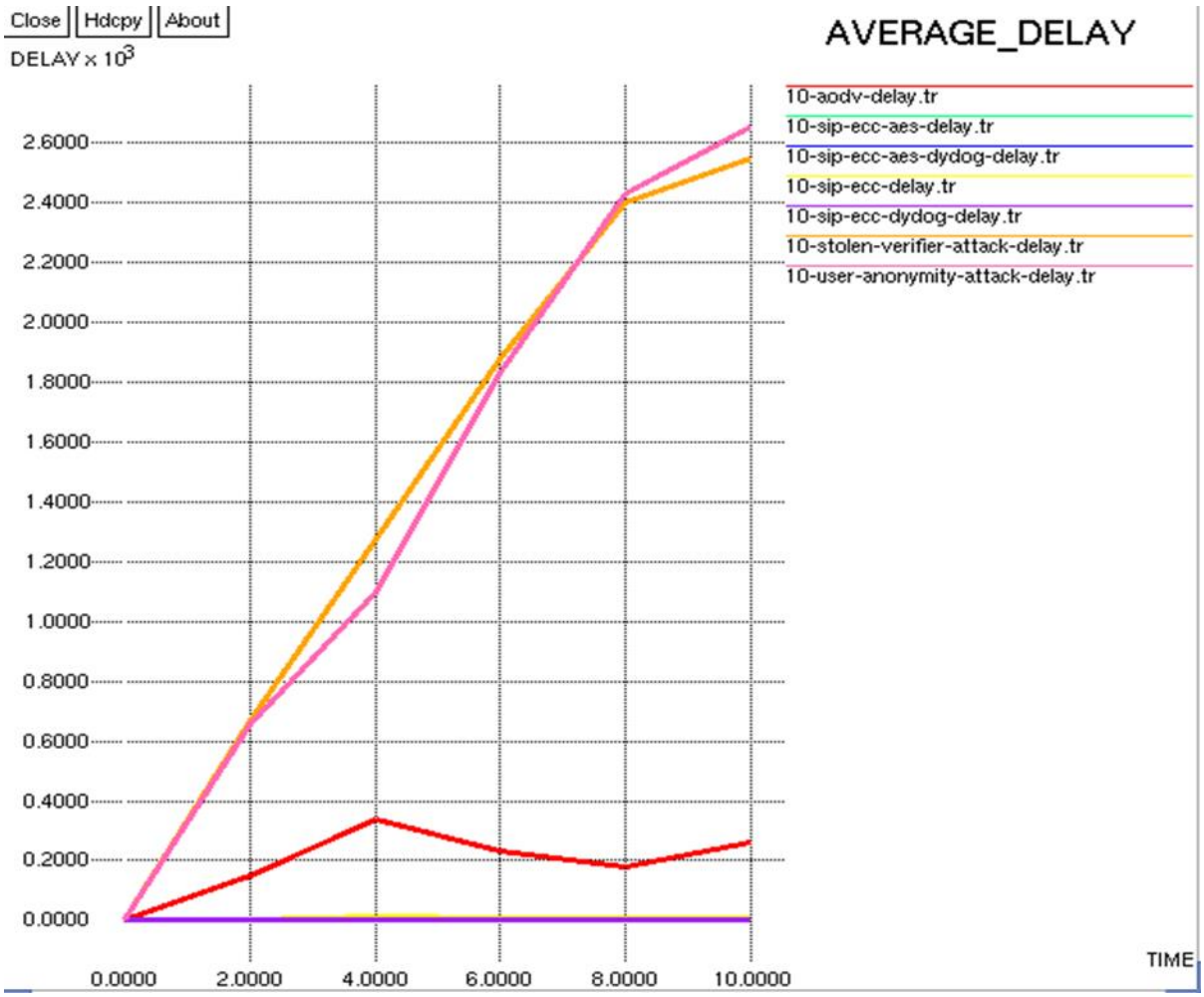

Fig 6.1 Comparison of average delay(10-Nodes)

6.4.2 Average throughput: In case of low traffic, the average throughput of the various nodes are shown in the Fig 6.2. When nodes are in communication using AODV protocol the throughput is initially increasing and after that slightly starts decreasing as time increases. It is because of congestion over the path increase as time passes. But in case of attacks throughput is less in comparison to previous case with the fact that very less packets reach to the destination. To improve the throughput, we have encrypted using AES when nodes wants to get packet, the observer node will detect the attacker node and broadcast their ID in

network traffic. Rest node in the network will not communicate with these nodes. Hence throughput is improved as we can see in the Fig 6.

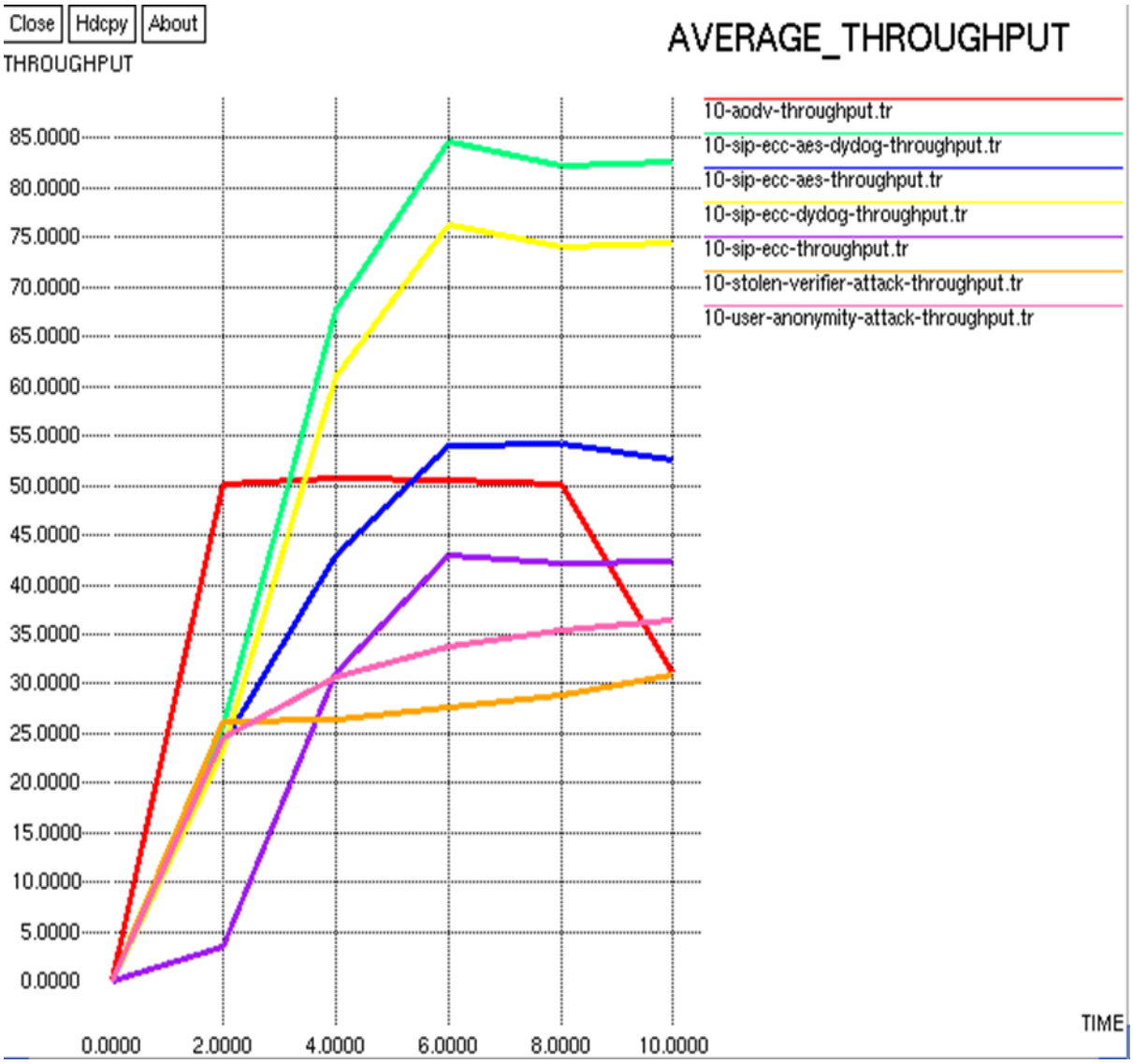

Fig. 6.2 Comparison of average throughput(10-Nodes)

6.4.3 Packet Delivery Ratio (PDR): In case of low traffic, the packet delivery ratio is shown in Fig 6.3 by observing the graph we can say that as time passes the PDR is normal in case of AODV but in case of attacks the PDR is very less since most of data traffic is created by attacker so there is a drop of packets but when our proposed technique is implemented in the network only authorised person is allowed to send so there will be no loss of data leading to increase in the PDR. The node has to pass the authenticity of 256 bit AES verification. Hence PDR is increased as shown in the given graph.

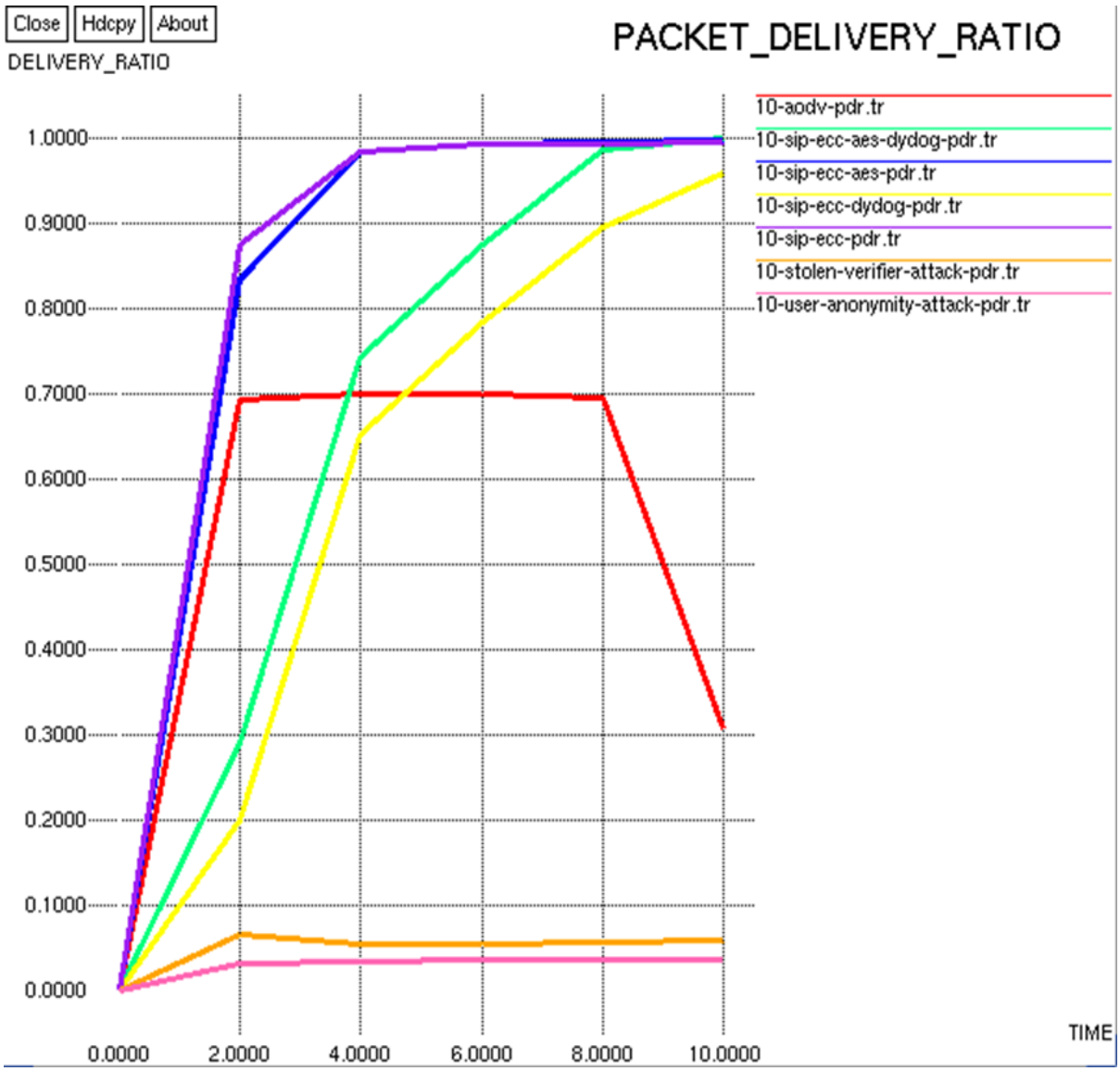

Fig 6.3 Comparison of PDR(10-Nodes)

6.5 High Traffic Scenario (50-Nodes)

We are considering the High traffic in which 30 and 50 nodes are communicating among themselves. We have analysed the impact of the number of nodes over the proposed scheme. It has been found that as the number of nodes increases in the network, the value for the packet delivery ratio goes down a bit. This is due to increased number of connections in the network leading to more congestion which furthermore leads to packet drops. But since the number of packets transmitted are also high due to augmented number of connections so the value for the throughput increases with the number of nodes. While on the other hand, the

delay is found to exhibit almost similar values in the high traffic scenarios. The below graph shows the performance of proposed scheme against number of nodes.

6.5.1 Average Delay:

Delay of nodes when simple AODV protocol is implemented it is less but when attackers are activated in the communication the delay is increasing in case of both user anonymity as well as stolen verifier attack the increment in the delay during attack is attributed to the fact that the attackers do not forward the packet to the destination as a normal node. After the application of the ecc-aes-dydog mechanism along with the encryption techniques the value of delay is found to be best of all the other modules tested.

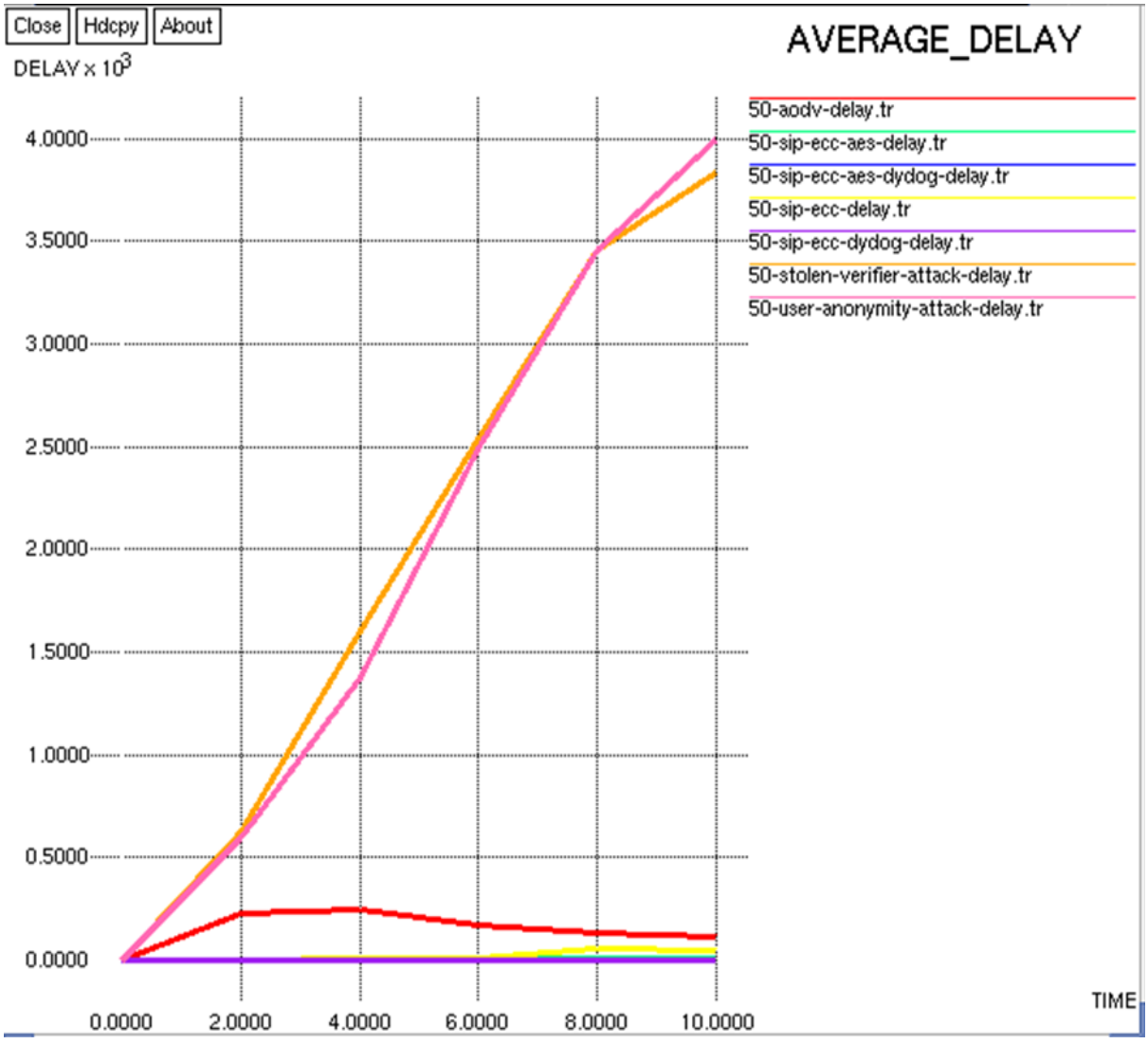

Fig 6.4 Comparison of average delay (50-Nodes)

6.5.2 Average throughput: In case of high traffic, the average throughput of the various nodes is shown in the Fig 6.5. When nodes are, in communication using AODV protocol the throughput is initially increasing and after that slightly starts decreasing as time increases. It is because of congestion over the path increase as time passes. Due to increase in node leads to high traffic in the network. To improve the throughput, we have encrypted using AES when nodes wants to get packet, the observer node will detect the attacker node and broadcast their ID in network traffic. Rest node in the network will not communicate with these nodes. Hence throughput is improved but less than low traffic scenario. as we can see in the Fig 6.5

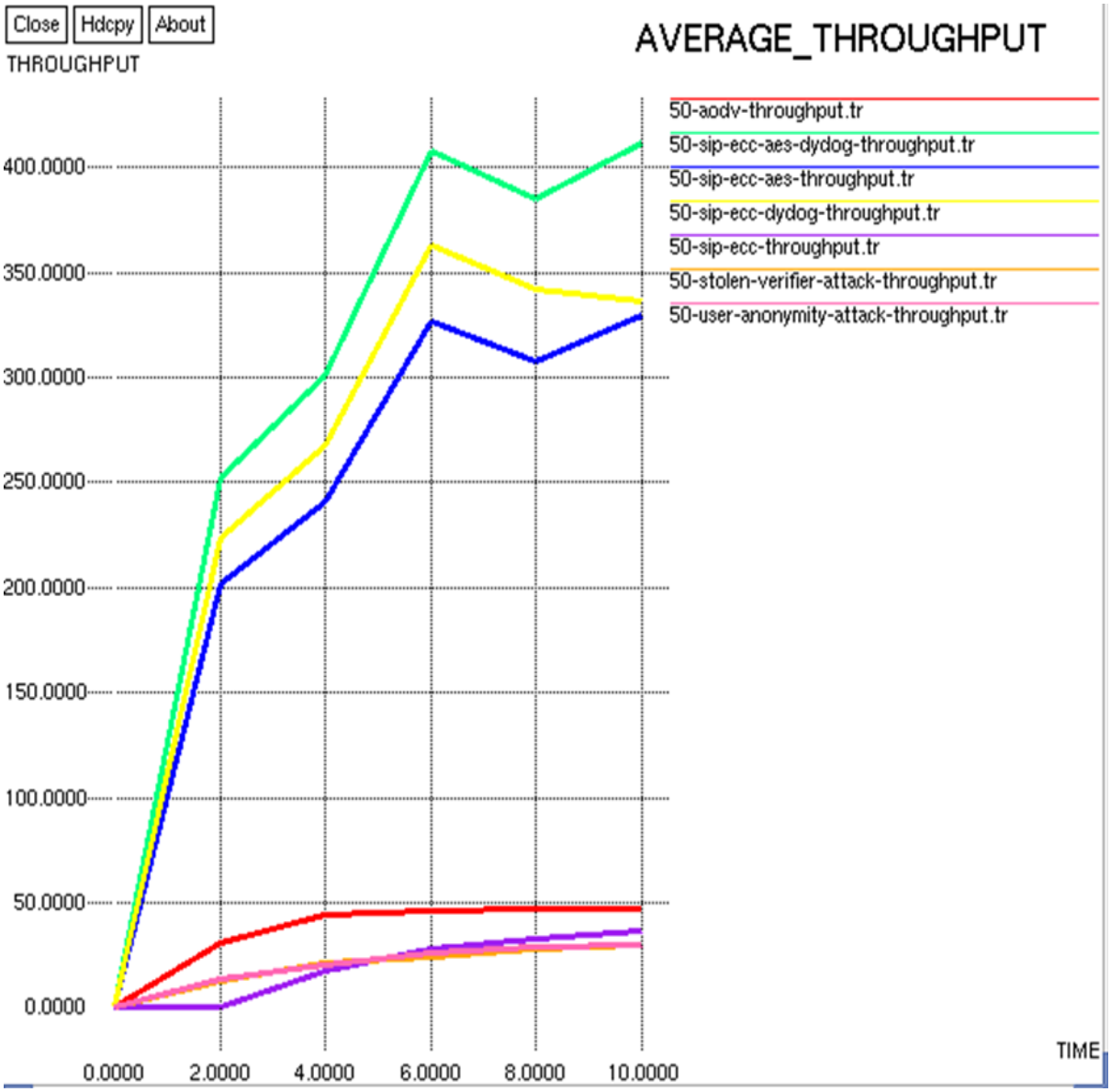

Fig 6.5 Comparison of average throughput(50-Nodes)

6.5.3 Packet Delivery Ratio (PDR): In case of high traffic, the packet delivery ratio is shown in Fig 6.6 by observing the graph we can say that as time passes the PDR is normal in case of AODV but in case of attacks the PDR is very less since most of data traffic is created by attacker so there is a drop of packets but when our proposed technique is implemented in the network only authorised person is allowed to send information. The node has to pass the authenticity of 256 bit AES verification. So there will be no loss of data but due to congestion PDR is little bit low compare to low traffic case.

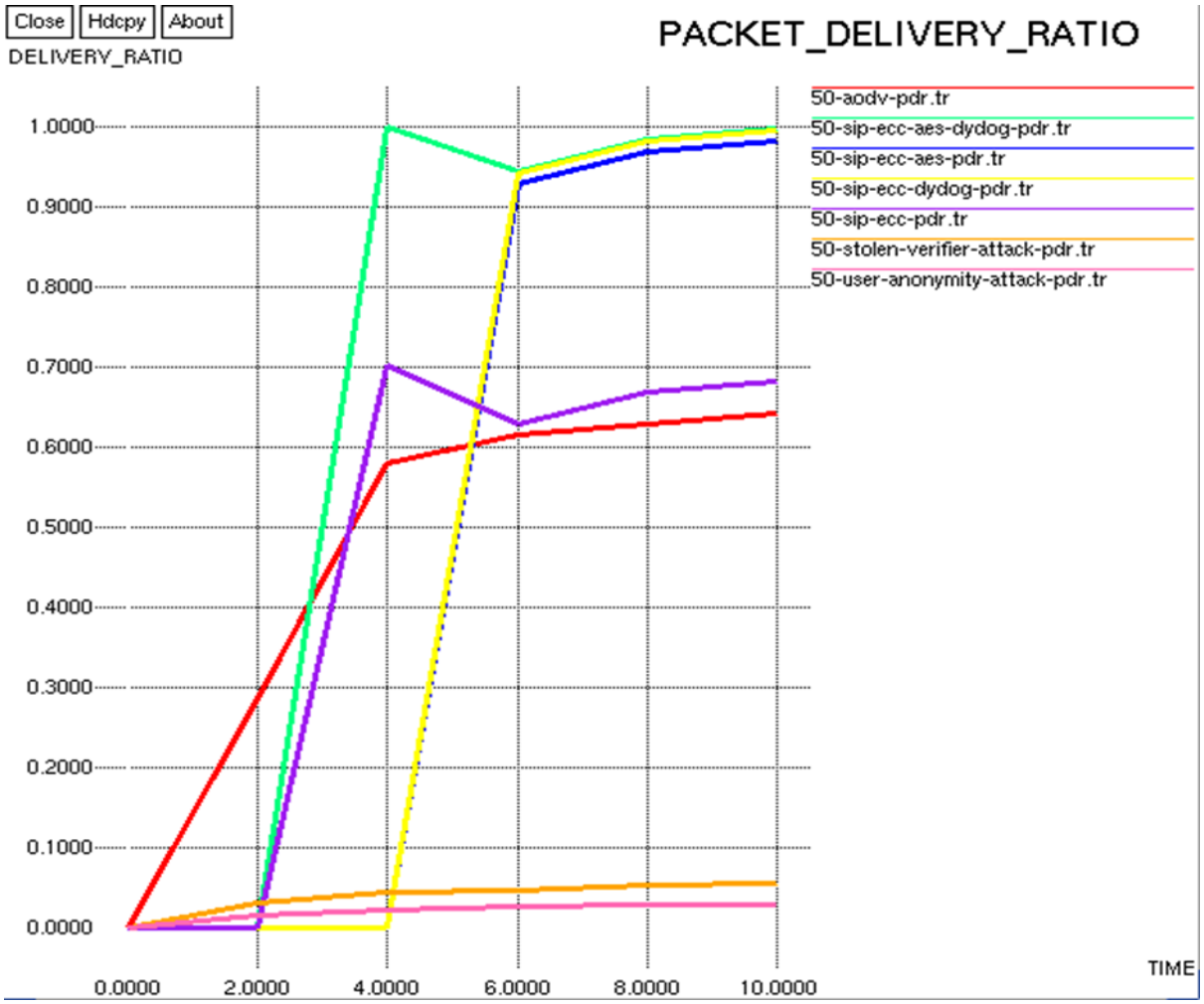

Fig 6.6 Comparison of PDR(50-Nodes)

CONCLUSION AND FUTURE SCOPE

In this thesis, authentication scheme with user anonymity for the SIP using the ECC is implemented. Security analysis shows that scheme is not only secure against common attack such as stolen-verifier attack, but also provides user anonymity. We have proposed novel technique ECC-AES-DYDOG to overcome the user anonymity and stolen verifier attack and compared the QoS parameters in different traffic scenario like Low(10-Nodes), Medium(30-Nodes) and High(50-Nodes). It can be also used for prevention of various Denial of Service attack (DOS) such as selective forwarding attacks, Blackhole attack, Wormhole attack, Sybil attack, Jamming attacks. The proposed scheme has shown better values because in dydog mechanism all the nodes (except the attackers) perform the function of observing their neighbourhoods. This leads to better and quick detection of the malicious nodes in the network thus leading to lower delays and high packet delivery ratio. These dydog nodes will identify the packet dropping nodes and perform their authentication as quickly than the other schemes.

In future, we can enhance the parameters of this novel technique by reducing the payload of the packet. We can also do following:

- To use SHA technique to increase the performance.
- To detect other attacks apart from user anonymity and stolen verifier attack.
- To compare their various security schemes to check its efficiency.

REFERENCES

[1]. V. Kumar, N. Chand, "Efficient Data Scheduling in VANETs," Journal of Computing, Vol.2, No.8, 2010, pp. 32-37,.

[2]. "EFKON Toll Management System website, "Available http://www.efkonindia.com/ EFKON_toll_management_system.php 2017.

[3]. X. Yang, L. Liu and N. Vaidya, "A vehicle-to-vehicle communication protocol for cooperative collision warning," 1st Annual International conference on Mobile and Ubiquitous Systems: Networking & Services, Mobiquitous, 2004, pp. 114-123

[4]. H. Hartenstein, K.P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," IEEE Communications Magazine, Vol.46, No.6, 2008, pp. 164-171.

[5]. I. Dalgic, H. Fang , "Comparison of H.323 and SIP for IP Telephony Signaling," in Proc. of Photonics East, SPIE, Boston, Massachusetts, 1999, pp. 106-122.

[6]. Stephan Eichler. "Security Challanges in MANET-based Telematics Environments". In Proceedings of the 10th Open European Summer School and IFIP WG 6.3 Workshop,Jun 2004.

[7]. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester. "An OverviewoMobile Ad Hoc Networks: Applications and Challenges". The CommunicationsNetwork, 3(3), 2004.

[8]. A. Dhamgaye, N. Chavhan, Survey on security challenges in VANET, Int. J. Comput.Sci.2 (2013) 88–96, ISSN 2277-5420.

[9]. J. Kakarla, S. Siva Sathya, B.G. Laxmi, B. Ramesh Babu, A survey on routing protocols and its issues in VANET, Int. J. Comput. Appl. 28 (4) (2011), ISSN 0975-8887.

[10]. Z. Wang, L. Liu, M. Zhou, N. Ansari, A position-based clustering technique for ad hoc intervehicle communication, IEEE Trans. Syst. Man Cybern., Part C, Appl. Rev. 38 (2) (2008) 201–208.

[11]. F.D. Rango, J.-C. Cano, M. Fotino, C. Calafate, P. Manzoni, S. Marano, OLSR vs DSR: a comparative analysis of proactive and reactive mechanisms from an energetic point of view in wireless ad hoc networks, Comput. Commun. 31 (16) (2008) 3843–3854.

[12]. L. Buttyan, J.-P. Nodeaux, Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Comput- ing, Cambridge University Press, 2008

[13]. A. Burg, Ad hoc network specific attacks, in: Seminar Ad hoc Networking: Concepts, Applications, and Security, 2003, TechnischeUniversitatMunchen, 2003.

[14]. B. Parno, A. Perrig, Challenges in securing vehicular networks, in: Workshop on Hot Topics in Networks (HotNets-IV), 2005, pp. 1–6.

[15]. BrouceSchneier, "Applied Cryptography. Protocols, Algorithms, and Source Code in C", John Wiley & Sons, Inc, 1996

[16]. L. Gollan, I.L. Gollan, C. Meinel, Digital signatures for automobiles, in: Systemics, Cybernetics and Informatics, SCI, Citeseer, 2002.

[17]. Mohamed Nidha lMejri, Jalel Ben-Othman, MohamedHamdi, "Survey on VANET security challenges and possible cryptographic solutions"..

[18]. Arshad R, Ikram N (2013) Elliptic curve cryptography based mutual authentication scheme for session initiation protocol. Multimed Tools Appl 66(2):165–178.

[19]. X. Yang, L. Liu and N. Vaidya, "A vehicle-to-vehicle communication protocol for cooperative collision warning," 1st Annual International conference on Mobile and Ubiquitous Systems: Networking & Services, Mobiquitous, 2004, pp. 114-123

[20]. H. Tu, N. Kumar, N. Chilamkurti and S. Rho, "An improved authentication protocol for session initiation protocol using smart card," Peer-to-Peer Netw. Applications, pp. 1-8, 2014

[21]. A. Durlanik, I. Sogukpinar "SIP authentication scheme using ECDH," World EnformatikaSocityTransations on Engineering Computing and Technology, Vol. 8, pp. 350–353, 2005

[22]. L. Wu, Y. Zhang and F. Wang, "A new provably secure authentication and key agreement protocol for SIP using ECC," Comput Stand Interfaces, Vol. 31, No. 2, pp. 286–291, 2009.

[23]. Liu FW, Koenig H, "Cryptanalysis of a SIP authentication scheme. In: 12th IFIP TC6/TC11 International Conference, CMS 2011, Lecture Notes in Computer Science, Vol. 7025, 2011, pp.134–143.

[24]. Tsai JL, "Efficient nonce-based authentication scheme for session initiation protocol. Int J NetwSecur8(3), 2009, pp.312–316.

[25]. Xie Q, "A new authenticated key agreement for session initiation protocol". Int Commun System 25(1), 2012, pp. 47–54.

[26]. Yoon EJ, Shin YN, Jeon IS, Yoo KY, "Robust mutual authentication with a key agreement scheme for the session initiation protocol", IETE Tech Rev 27(3), 2010, pp. 203–213.

[27]. C. Yang, R. Wang and W. Liu, "Secure authentication scheme for session initiation protocol," Computers & Security, Vol. 24, No. 5, 2005, pp. 381–386.

[28]. Hamed Arshad & Morteza Nikooghadam, " An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC", # Springer Science+Business Media New York 2014.

[29]. Yanrong Lu1, Lixiang Li, Haipeng Peng,Yixian Yang, "A secure and efficient mutual authentication scheme for session initiation protocol", © Springer Science+Business Media New York 2015.

[30]. Sherali Zeadally,Ray Hunt, Yuh-Shyan Chen, "Vehicular ad hoc networks (VANETS): status, results, and challenges" , © Springer Science+Business Media, LLC 2010.

[31]. Bhuvaneshwari.S, Divya.G, Kirithika.K. B and Nithya.S, "A Survey On Vehicular Ad-Hoc Network", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 10, October, 2013.

[32]. Mohammad Sabzinejad Farash, Mahmoud Ahmadian Attari, "An Enhanced Authenticated Key Agreement for Session Initiation Protocol",Issn 1392 – 124x, Issn 2335 – 884x (Online) Information Technology And Control, 2013, Vol.42, No.4.

[33]. Debiao He, Muhammad Khurram Khan, Neeraj Kumar (2015), "A new handover authentication protocol based on bilinear pairing functions for wireless networks", International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC), Vol. 18, No. 1/2, 2015.

[34]. Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan, "Classes of attacks in VANET", in Tenth International Conference on Wireless and Optical Communications Networks (WOCN), pp 1 - 5, 2013.

[35]. Al-kahtani, Salman bin Abdulaziz, Al Kharj, "Survey on security attacks in Vehicular Ad hoc Networks (VANET)", in 6th International Conference on Signal Processing and Communication Systems (ICSPCS), 2012, pp 1 - 9.

[36]. J.T. Isaac, S. Zeadally, and J.S. Cmara, "Security attacks and solutions for vehicular ad hoc networks", in IET Communications, 2009, pp. 894-903,.

[37]. O. A. Wahab, H. Otrok, and A. Mourad, "A cooperative watchdog model based on dempster–shafer for detecting misbehaving vehicles," Computer Communications, vol. 41, 2014, pp. 43–54.

[38]. H. Sharma and R. Garg, “Enhanced lightweight Sybil attack detection technique,” in Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th International Conference-. IEEE, 2014, pp. 476–481.

[39]. A. Joshi, R.kaur “A Novel Multi-cast Routing Protocol for VANET,” IEEE, 2015, pp. 41–45,

[40]. S. Janakiraman, S. Rajasoundaran, P. Narayanasamy, “The Model — Dynamic and Flexible Intrusion Detection Protocol for high error rate Wireless Sensor Networks based on data flow” International Conference on Computing, Communication and Applications, 2012, pp.1-6.

[41]. Zezhong Zhang, Qingqing Qi, Neeraj Kumar, Naveen Chilamkurti and Hwa-Young Jeong, “A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography”, Multimed Tools Appl, vol. 74 ,2015, pp. 3477‑3488.

PLAGIARISM REPORT

ORIGINALITY REPORT

%26	%14	%16	%12
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Zhang, Zezhong, Qingqing Qi, Neeraj Kumar, Naveen Chilamkurti, and Hwa-Young Jeong. "A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography", Multimedia Tools and Applications, 2015. Publication	%2