An Efficient Session Initiation Protocol for Secure Communication in Vehicular Ad-hoc Networks

Thesis submitted in partial fulfillment of the requirements for the award of

Degree of

Master of Engineering
in
Information Security

Submitted By
Rajni Bala
801333021

Under the supervision of:
Dr. Neeraj Kumar
Associate Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

July 2015

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*An Efficient Session Initiation Protocol for Secure Communication in Vehicular Ad-hoc Networks*" in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Neeraj Kumar* and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

(Rajni Bala)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Neeraj Kumar)
Associate Professor,
Computer Science and Engineering Department

Countersigned by:

(Dr. Deepak Garg)
Head
Computer Science and Engineering Department
Thapar University
Patiala

(Dr. S. S. Bhatia)
Dean (Academic Affairs)
Thapar University
Patiala

ii

Acknowledgment

No volume of words is enough to express my gratitude towards my guide, **Dr. Neeraj Kumar**, Associate Professor, Computer Science and Engineering Department, Thapar 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 **Dr. Deepak Garg**, Head of Department, CSED and **Ms. Jhilik Bhattacharya**, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.

I would also like to thank the staff members and my colleagues who were always there in the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis.

Most importantly, I would like to thank my **parents**, **friends** and the **Almighty** for showing me the right direction out of the blue, to help me stay calm in the oddest of the times and keep moving even at times when there was no hope.

Rajni Bala

(801333021)

Abstract

Vehicular Ad Hoc Networks (VANETs) are used for communication between vehicles and have a large number of applications such as road safety, entertainment and traffic control. VANETs provide information to the drivers regarding safety alerts on time.

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

Abbreviations

AERIS	Application for Environment Research Program
AU	Application Unit
C2C	Car-to- car
CDPD	Cellular Digital Packet Data
CK	Canetti-Krawczyk
CSMA	Carrier Sense Multiple Access
DLP	Discrete Logarithmic Problem
DNS	Domain Name Server
DSRC	Dedicated Short Range Communication
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDLP	Elliptic Curve Discrete Logarithm Problem
FCC	Federal Communications Commission
HTTP	Hypertext Transport Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPV6	Internet Protocol Version 6
IrDA	Infrared Data
ISP	Internet Service Provider
ITS	Intelligent Transport System
LLC	Logical Link Control
MAC	Message Authentication Code
MANETs	Mobile Ad-hoc Networks
MAPS™	Message Automation and Protocol Simulation
MAPS™-HD	Message Automation and Protocol Simulation-High Definition
NHTSA	National Highway Traffic Safety Administration
NS-2	Network Simulator 2
OBU	On Board Unit
P2P	Peer-to-peer
R2S	Road-to-server

RSA	Rivest Shamir Adleman
RSU	Roadside Unit
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
SAE	Society of Automotive Engineers
TCP	Transport Control Protocol
TDMA	Time Division Multiple Access
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
V2V	Vehicle-to-vehicle
V2R	Vehicle-to-roadside
VANETs	Vehicular Ad-hoc Networks
VoIP	Voice Over Internet Protocol
WAVE	Wireless Access in Vehicular Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WMN	Wireless Mesh Network
WPAN	Wireless Personal Area Network
WSM	Wireless Service Manager
WSMP	Wireless Services Manager Protocol
WWAN	Wireless Wide Area Network

Chapter 1

Introduction

1.1 Wireless networks

Wireless Networks are the network between the two nodes or any communication devices that uses the radio waves to communicate as shown in Figure 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.

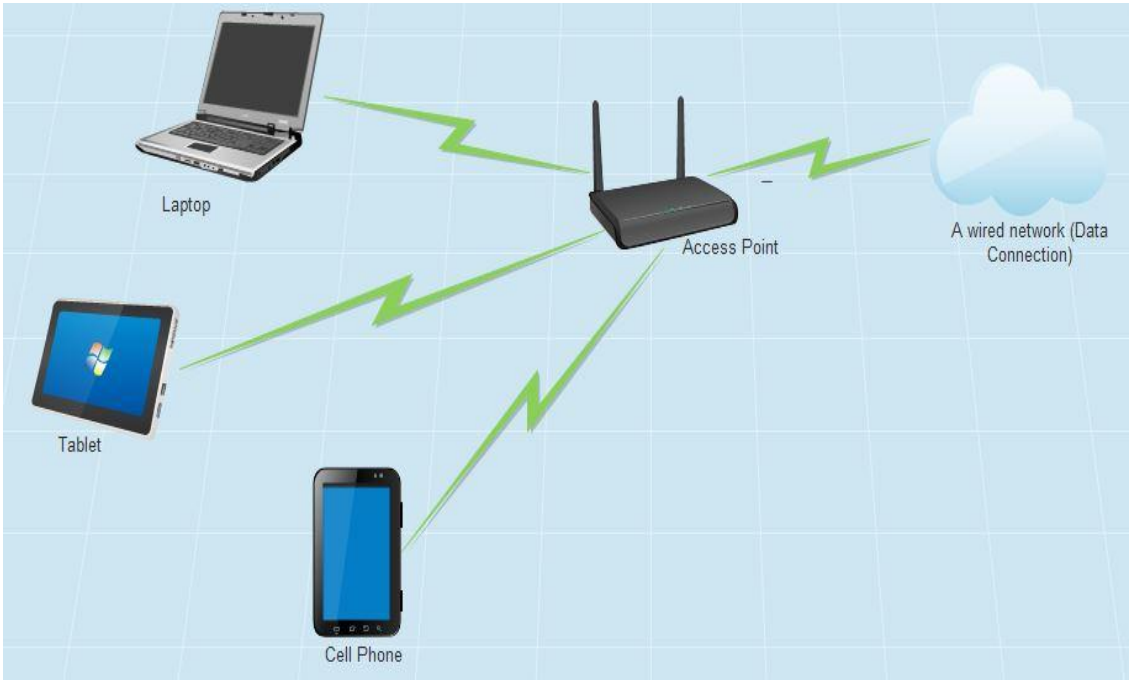

Figure 1.1 Wireless networks

1.2 Advantages of wireless networks

Wireless networks due to their properties of ease of access and infrastructural flexibility; find many uses in small and large industries. They being:

- **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 labor 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 equipments. But in wired networks, there is scope of extra wires for expansions.

1.3 Types of wireless networks

There are different types of wireless network as shown in Table 1.1. Which are mentioned below:

- **Wireless Personal Area Network (WPAN):** WPAN is used for the network in personal area like in the room. The range WPAN is expandable within area of 10 meters. In this network, the devices should be very close to each other for better communication. For example, connectivity between the printer and computer. WPAN creates the ad-hoc network between the participating devices.
- **Wireless Local Area Network (WLAN):** WLAN provides the network in a particular finite area like a college campus or an office building. WLAN uses the radio or infrared waves for the communication.
- **Wireless Mesh Network (WMN):** WMN is a network which uses a mesh topology for the communication between the radio nodes. The message can be forwarded by node on the behalf of another node. WMN is also called self re-routing network because of "self- heal" property of it.

- **Wireless Metropolitan Area Network (WMAN):** WMAN are used for network connectivity in a particular city or metropolitan area. In this network, the different building of the city communicates through this network.
- **Wireless Wide Area Network (WWAN):-** WWAN is a worldwide network, which provides network between the two different countries via multiple satellites. These satellites communicate through an Internet Service Provider (ISP).

Table 1.1 Comparison between different types of wireless networks

Type	Coverage	Performance	Technology
WPAN	Small Network/Within reach of person	Moderate	Bluetooth, IrDA, IEEE 802.15
WLAN	Within the reach of university campus/ building	High	IEEE 802.11 and Wi-Fi
WMN	In mesh cloud	High	IEEE 802.11, 802.15, 802.16
WMAN	Within city	High	IEEE 802.16 and WIMAX
WWAN	World wide	Low	CDPD, TDMA, Cellular 2G, 2.5G and 3G

1.4 MANETs

Due to the growth of industry and technology, the requirement of new wireless devices has increased in communication. There is one class of network, which is self-configuring, called Mobile Ad-hoc Networks (MANETs) [1]. MANETs are infrastructure-less networks. In MANETs, there is no requirement of base station for

each node. A wireless link is required for the communication of mobile devices. A node which is in the range of other node communicates directly and shares data with each other. When nodes are not in the range, in that case intermediate node acts as a router and select the route for communication. MANETs have a large number of applications such as relevance in disaster management. Applications of MANETs include the disaster management, ad-hoc classroom, in the field of battle and civilian application like outdoor meeting etc.

1.5 VANETs

Due to the growth of technology, the road traffic also increases. But the absence of safety in road traffic is the reason for increasing accident rates. In addition, there is wastage of energy and resources. Even pollution also increases. According to National Highway Traffic Safety Administration (NHTSA), figures of recent road accidents are:

- Millions of accidents every year.
- Nearly 1.3 million people due to road accidents every year.
- 20-50 million are injured.

For safety, one can use precautions like airbags and seat belts for the safety. But these cannot provide proper security. On the highway, one vehicle cannot predict speed of other vehicle. But Vehicular Ad-hoc Networks (VANETs) can predict the speed of other vehicles. The message can be sent to vehicle by using this network and chances of an accident can be reduced. So VANETs can be used for enhancing road safety.

VANETs are used for communication between vehicles for the different kind of application such as road safety, entertainment, traffic control, etc. VANETs provide information timely to drivers and required authorities to provide safety to users. In VANETs, there are two kinds of communication. One is peer-to-peer (P2P) known as V2V communication as shown in Figure 1.2. V2V communication occurs between vehicles. Second is the Vehicle-to-roadside unit (RSU) which is known as V2R, which occurs between vehicle and RSU. In V2R communication, a vehicle communicates with the most nearest RSU. The required message is sent by RSU if

and only if vehicles are in the range of those RSU. Otherwise, RSU sends a message to the neighbor RSU for communication.

One more type of VANETs is available which is called intelligent VANETs. In these networks, multiple technologies are integrated for better and intelligent communication. These network technologies are Wireless Access in Vehicular Network (WAVE) IEEE 1609, Bluetooth, Wi-Fi IEEE 802.11p, WiMAX IEEE 802.16 and ZigBee as described in Figure 1.3. VANETs are considered under the category of intelligent transport systems (ITS). There are two kinds of communication in ITS. One is V2V, which occurs between vehicles. Second is V2R, which occurs between vehicle and RSU. VANETs are a current topic for the various researches in wireless communications. The main issues in wireless network are energy consumption and security of the network. VANETs are implemented by using the technology Dedicated Short Range Communication (DSRC) which is one kind of Wi-Fi. There are other wireless technologies like WiMAX, cellular, etc.

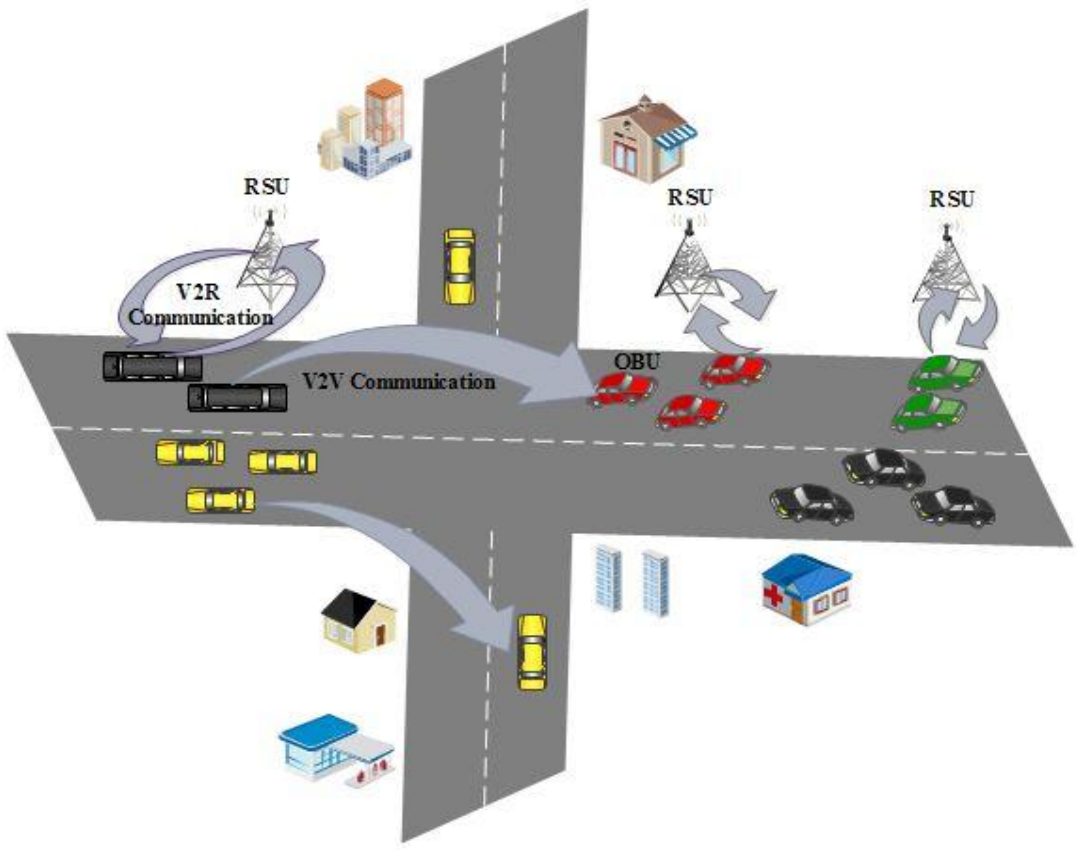

Figure 1.2 Basic VANET scenarios

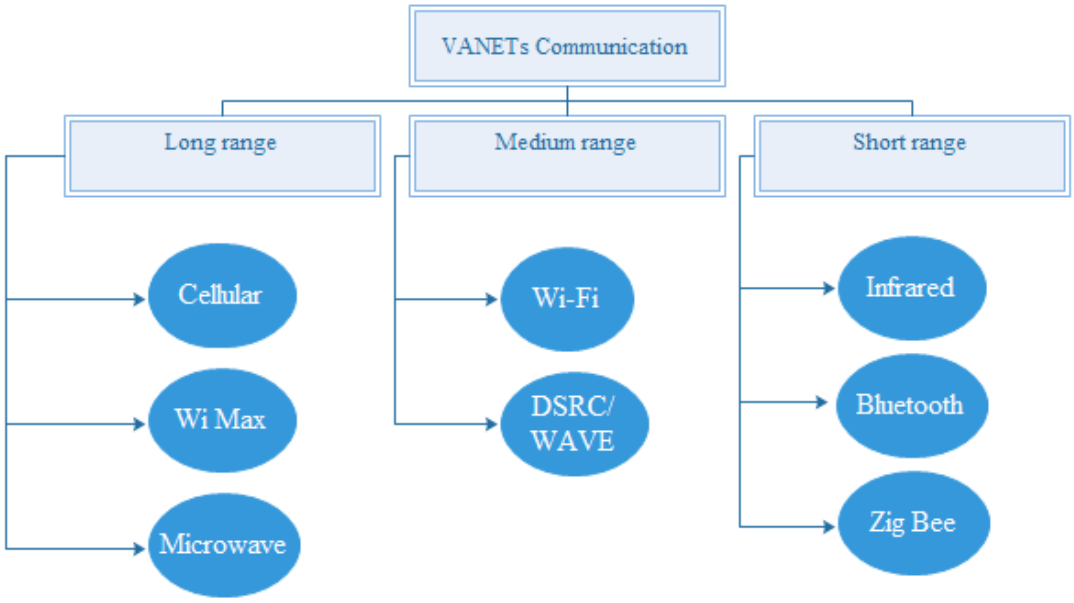

Figure 1.3 VANETs communication according to range

1.6 VANETs vs. MANETs

Basically, VANETs are the part of MANETs, but still there is difference between these networks. There are following difference between MANETs and VANETs shown in Table 1.2.

Table 1.2 VANETs vs. MANETs

Properties	VANETs	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.

1.7 Applications of VANETs

RSU acts as a buffer point or router. Data is stored in RSU and gives the data to the user whenever required [2]. Vehicles either upload or download the data. Applications of VANETs depends upon type of communication occurred, i.e. V2V communication, V2R communication, vehicle to building communication and routing based application. The classifications of these applications are:

- Convenience oriented
- Safety oriented
- Productive applications
- Commercial oriented

- **Convenience oriented 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. The classification of this application is:
    - **Parking availability:** In metro cities, a parking space in parking lots can be easily searched using this application.
    - **Electronic toll collection:** This application can be used for the toll collection. Payment can be done electronically shown in Figure 1.4. On Board Unit (OBU) should be readable by toll collection point. This application is beneficial for drivers as well as for toll operators.

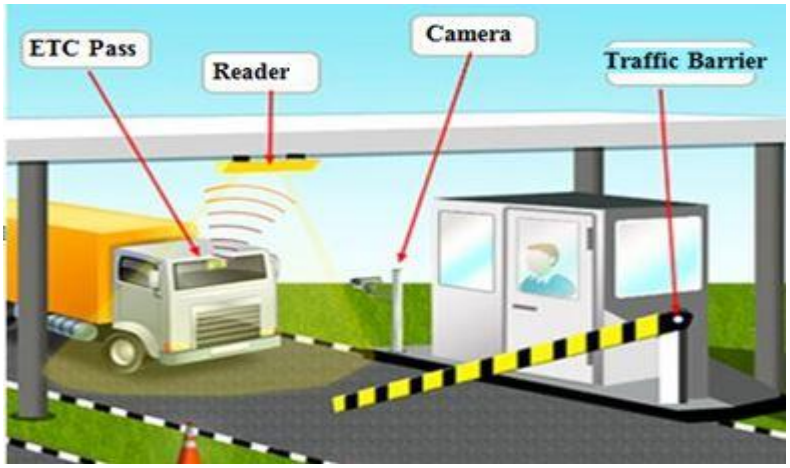

Figure 1.4 Electronic toll collections [3]

- **Active prediction:** 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 [4].
- **Route diversions:** This application can be used in the planning of routes in the case of road congestions.

➢ **Safety oriented applications:** This application is used for safety purpose. These applications include road safety, surface of the road, diversions on roads and vehicle communication etc. The application can be classified as follows:

- **Cooperative collision warning:** It gives the warning to the drivers about the crash route. Thus, drivers can act accordingly [5].
- **Post crash notification:** If the accident occurs, the vehicles which are involved in that accident will broadcast warning message to the other vehicles on the road. So that, other vehicles can take decisions on right time. The whole scenario is Figure 1.5.

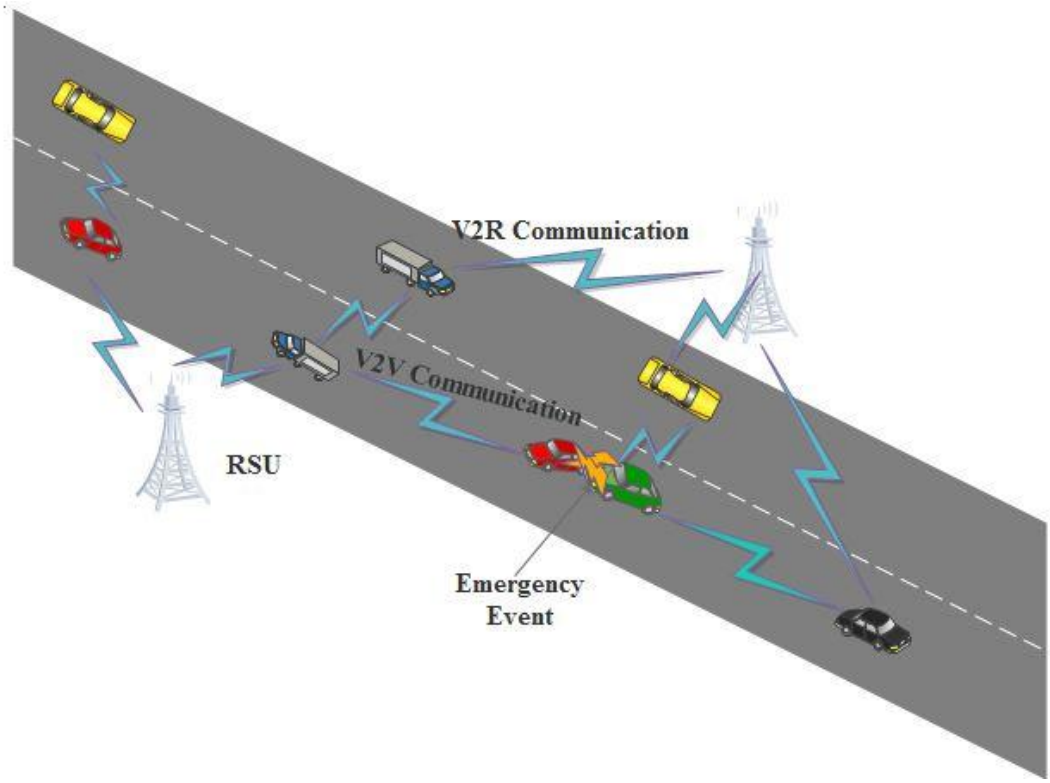

Figure 1.5 Emergency situations notification.

- **Traffic vigilance:** A camera is installed at the RSUs. The camera acts as monitoring device for vigilance on the traffic. Traffic rules violation can be checked by using this camera [6].
- **Real-time traffic:** RSU acts as buffer point. All real-time traffic is stored in RSU and can be used whenever required. This is important application of VANET. By using this application, one can avoid accidents, traffic jams etc.
- **Road hazard control notification:** One vehicle communicates with other vehicle to tell the road conditions like road curve, landslide on road, sudden downhill etc.

Productive applications: Types of Productive applications are discussed below and described in Figure 1.6.

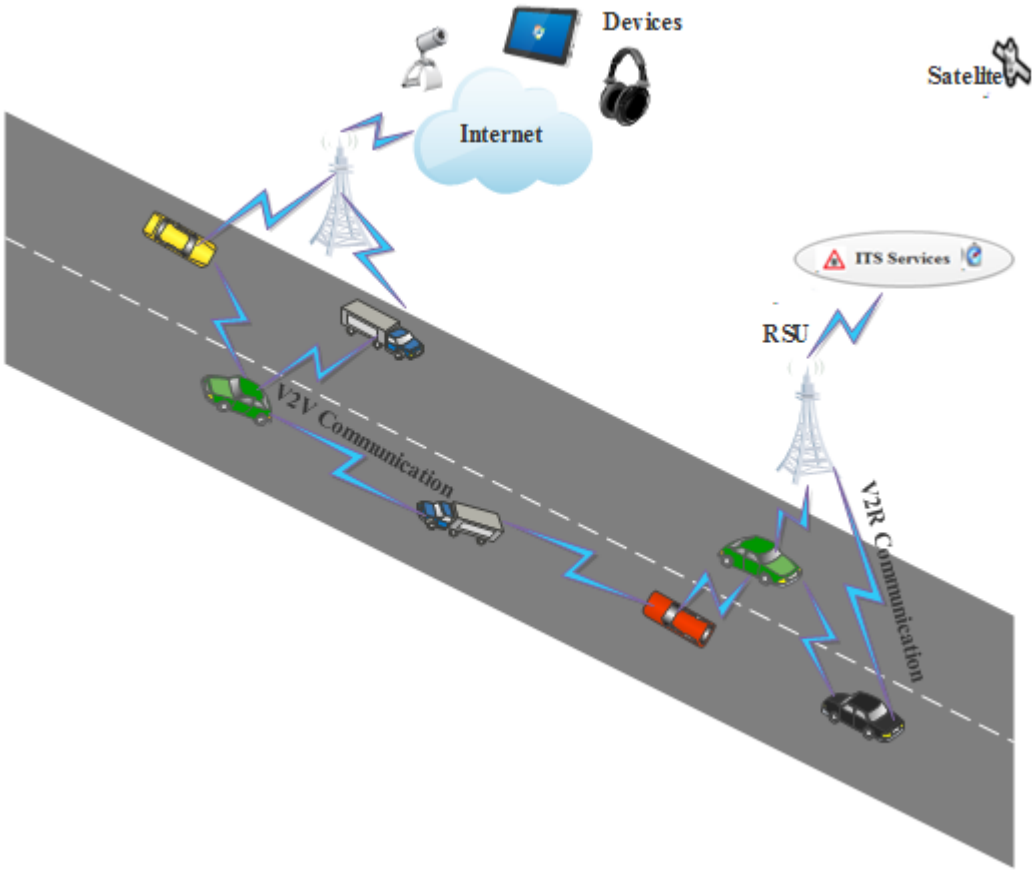

Figure 1.6 Productive applications of VANETs

- **Fuel saving:** using the electronic toll, time and fuel can be saved. There is no need to stop at every toll booth. Hence, efficiency of engine increases and 3% fuel can be saved.
- **Time utilization:** By using this application, one can utilize time whenever stuck in the traffic jam. This application Provides facility to download email. The internet facility can be used when someone is waiting for a friend or relative in the vehicle.
- **Environmental benefits:** Applications for the Environment Research (AERIS) program [7] works on environment friendly real-time transportation. This research program works with V2V communications for the better research and results. By connecting with this research they get to know about the negative effects of vehicle communication in the environment. So they can mitigate these effects and makes a "green" environment.

➢ **Commercial oriented applications:** Applications used for Commercial purpose by the driver or travelers are known as commercial applications of VANETs. This application provides entertaining services like web access or music, etc. The classification of this application is:

- **Internet access:** RSU acts as a router. The driver can use the internet through RSU.
- **Real-Time video relay:** Videos, on-demand movies etc. can be played inside the vehicle. This application provides us facility of real-time video relay.
- **Remote vehicle personalization/ diagnostics**: By using this application, personalized vehicle setting can be downloaded. This also helps uploading of vehicle diagnostics from/to RSU.
- **Value-added advertisement:** This application can provide the information about stores, restaurants etc. to the vehicles. If the traveler wants some information it will be convenient for him/her. This application is used by service providers. For this application, no Internet is required.

- **Digital map downloading:** Before starting journey, user can download the map for that region. Hence it can help in travel guidance. By using this application, user can conveniently reach their destination.

1.8 Challenges in VANETs

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 economical challenges [8]. 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.

1.9 Motivation

In VANETs, security is a serious issue. The message sent by RSU/OBU should be secured. These messages contain important information and critical data. A message is sent by vehicle to other vehicle. It should not be modified or deleted by an attacker. In VANETs, there is human life at stake, where wrong messages may cause an accident. So the security of VANETs is important as its concerns human lives. Information between the two vehicles should be exchanged securely and timely. Driver privacy should be there for secure VANETs communication.

For resolving the security issue, VANETs uses a protocol called Session Initiation Protocol (SIP) for secure communication. SIP is a communication protocol, which is used to establish, change and terminate multimedia sessions [9]. SIP uses the concept of Voice over Internet Protocol (VoIP) for communication between vehicles or any entity. So, SIP is used frequently in VoIP communication. SIP provides the

integrity, authentication etc. So by using the concept of SIP, security of VANETs is enhanced in this dissertation.

MAPS^{TM} is used for the simulation of the SIP protocol. MAPS^{TM} is the simulator which is used for the security protocol of VANETs. Implementation of proposed scheme is done using this simulator and various tests are performed. Proposed scheme is compared with existing schemes. After the comparison, proposed protocol gives the better result than pervious protocols.

1.10 Thesis outline

There are 6 chapters in this thesis. Which are described as follows:

- In chapter 1, introduction about wireless networks, comparison between VANETs and MANETs, various applications and challenges are illustrated.
- Chapter 2 describes the survey of various existing schemes.
- In chapter 3, the proposed scheme of the SIP protocol is given.
- In chapter 4, Implementation and simulation of SIP are provided.
- Simulation results and discussion are shown in chapter 5.
- Finally, in chapter 6, the conclusion of proposed scheme with future scope is given.

Chapter 2

Literature Review

2.1 VANET overview

VANETs are part of MANETs, which has come into existence due to growth in wireless networks. VANETs are the network, which are used for communication between the vehicle and near objects for various applications like traffic congestion control and accident control. The importance of VANETs is increasing day by day. Many countries deploy VANETs for the daily application. In Japan, the spectrum of 5.8GHZ is allotted to the electronic toll collection deployment. The Federal Communications Commission (FCC) of the USA gives 75MHz of licensed spectrum for VANETs. European communities give a 5875-5905MHz spectrum for the road safety applications in Europe.

2.2 VANET architecture

For the implementation of VANETs, user can do integration with different organizations, service provider and governmental authority.

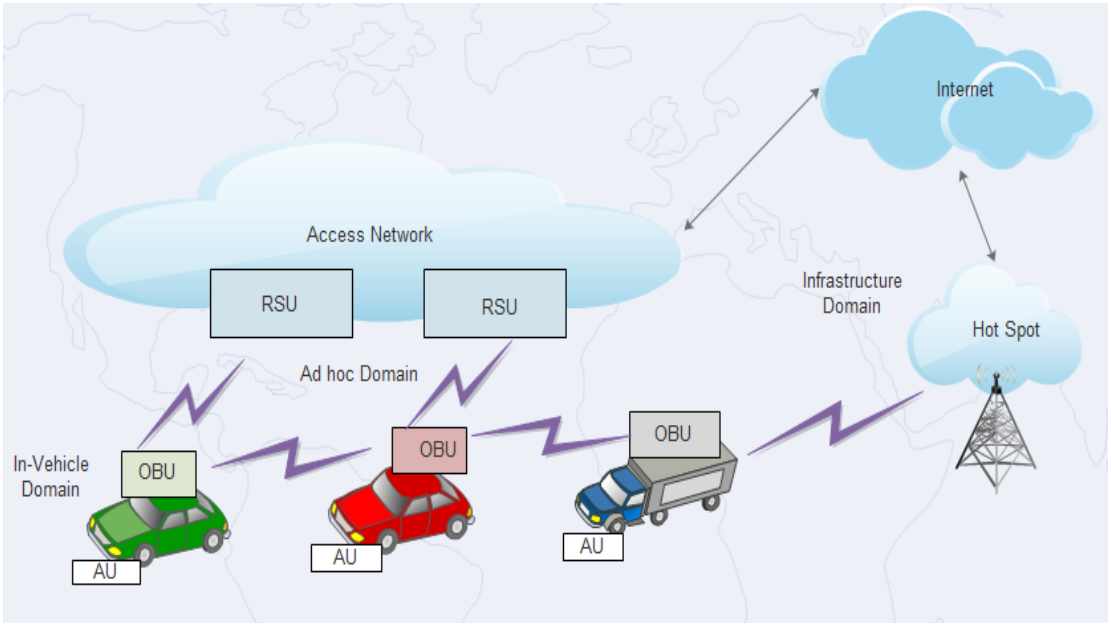

Figure 2.1 C2C-CC reference VANETs architecture [10]

In VANETs architecture, there should be communication between vehicles as well as between fixed RSUs. There is one kind of architecture called Car-to-Car (C2C-CC) [10]. Figure 2.1 explains this architecture. There are two types of units available in the vehicle, according to this architecture:

- Application Unit(AU) and
- OBU.

AU runs set of applications on vehicles. OBU is used for the communication capabilities. OBU is used for DSRC as well as road safety. User can use portable device for AU. It can be easily attached or detach from OBU. OBU communicate with RSU and form an ad hoc network domain. Infrastructure network and RSU are connected to each other, by which they can attach to the Internet. With the help of RSUs and OBUs, users can access the infrastructure as well as internet.

2.3 Standards, regulations & layered architecture

For VANETs, there should be common standard. These standards should be agreed by all participating organizations and authorities. A set of rules and regulation is called standard. This is followed in the equipments of VANETs, developed by different groups like SAE and IEEE. There is one common standard given by IEEE, which is IEEE 802.11p [12]. This standard is variant to the IEEE standard 802.11a. IEEE 802.11a covers the wireless network but IEEE 802.11p covers the specific properties of vehicular networks. There is one more IEEE 1609 group which is working on vehicular networks and provided the necessary services required for VANETs. This group uses the payload of IEEE 802.11p.

The WAVE is divided into DSRC. FCC of the USA gives 75MHz of licensed spectrum for DSRC communication in VANETs. This spectrum supports both safety and non-safety applications [13]. In this spectrum, there are seven 10MHz channels and 5MHz guard bands. DSRC provides the communication to RSUs as well as OBUs. IEEE 1609 and IEEE 802.11p are the standard followed by DSRC. In Figure 2.2, there is a complete architecture of DSRC. IEEE 1609 group overview of this architecture is given below:

- **IEEE 1609.1:** This is the standard that allows the multiple applications, when RSUs communicate with OBUs. This works on the application layer [13].
- **IEEE 1609.2:** This standard provides the security services for the communication [13]. For example the encryption of message and device authentication.
- **IEEE 1609.3:** This is the standard that gives the networking services, which are included WSM protocol and Specific stack for WSMP [13].
- **IEEE 1609.4:** This is the standard uses for the IEEE 802.11p enhancements. It also supports the multi-channel operation [14].

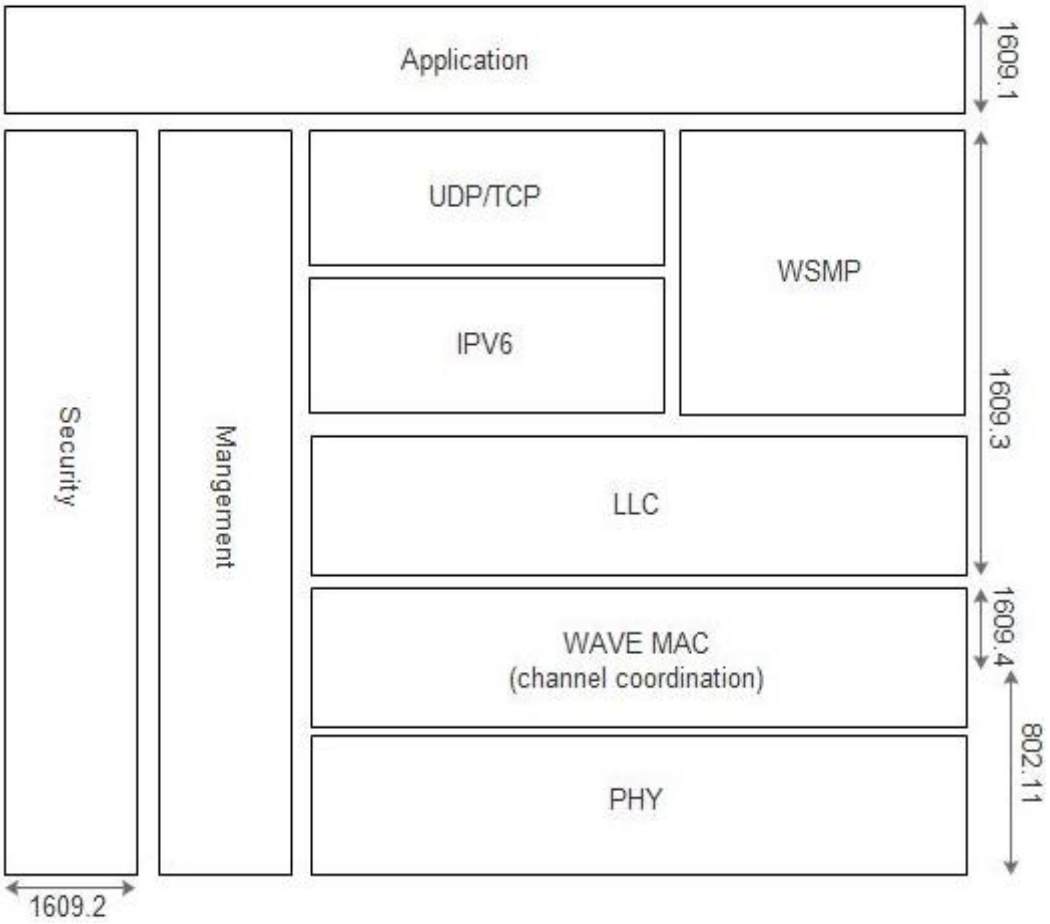

Figure 2.2 IEEE layered architecture [14]

2.4 SIP for VANETs

SIP is an application layer Protocol. SIP is a communication protocol, which is used for establishing, change and terminates multimedia sessions. [9]. SIP uses the concept of VoIP for communication between vehicles or any entity. So, SIP is used frequently

in VoIP communication. SIP provides the integrity, authentication, etc. According to RFC2617 [15], SIP uses the Hypertext Transfer Protocol (HTTP) digest for the identity authentication.

HTTP is a vulnerable protocol. It cannot resist various attacks, i.e. off-line password guessing attack [16, 17, 18]. For communication between the user and the remote server, authentication is required. User and server check the legality of each other. In existing protocol SIP, there is an issue of authentication because of HTTP digest. In SIP protocol, there are register servers, redirect servers, proxy servers and user agents. The request and response communication is occurring in SIP. These are following steps:

- Firstly, client registers themselves with register server using the register message. This message is stored by the registered server. Then the client communicates with the server.
- After the communication gets started between client and server, then the client sends the invite message to a proxy server.
- The proxy server checks the server address through Domain Name Server (DNS) by using the redirect server.
- After receiving the server address, the message is sent to the server by the proxy server.
- After the successful acceptance of message from server. The OK (200) message is sent to the user by the proxy server.

Client and server can terminate their call by using simple BYE message. If one sends the BYE message, the other will terminate the call by sending the OK message.

SIP is used for the authentication between the vehicles and server. Firstly, there is a connection establishment between the server and RSU. After the establishment of a connection between the server and RSU, server gives all values of a smart card to the RSU as shown in Figure 2.3. Due to communication, there is a registration between the server and RSU using the smart card. Now, vehicles are ready for V2V and V2R communication with authentication.

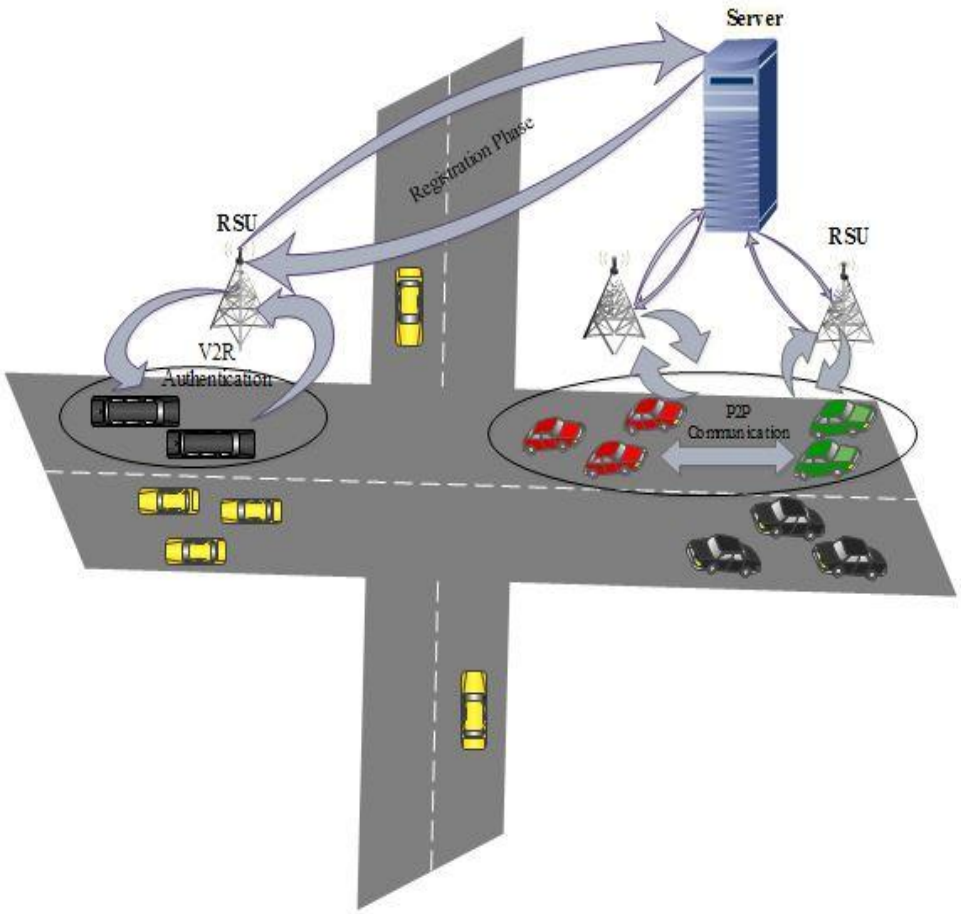

Figure 2.3 SIP Authentication Protocol

2.5 ECC Based authentication protocol for SIP

Elliptic curve cryptography (ECC) based authentication protocol in VANETs provides the secure authentication. SIP uses ECC for the secure authentication. This scheme is better than other cryptography algorithms. Firstly, ECC is discussed, then ECC is implemented in SIP for the better authentication protocol.

2.5.1 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 conventional cryptography RSA [19] 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 extra 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 [20] and Neal Koblitz [21]. 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 [22] 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.

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.
In Figure 2.4, Elliptic curve whose point at infinity far to the top and bottom of graph.

$$Y^2=x^3+ax+b \quad \text{..... (2.1)}$$

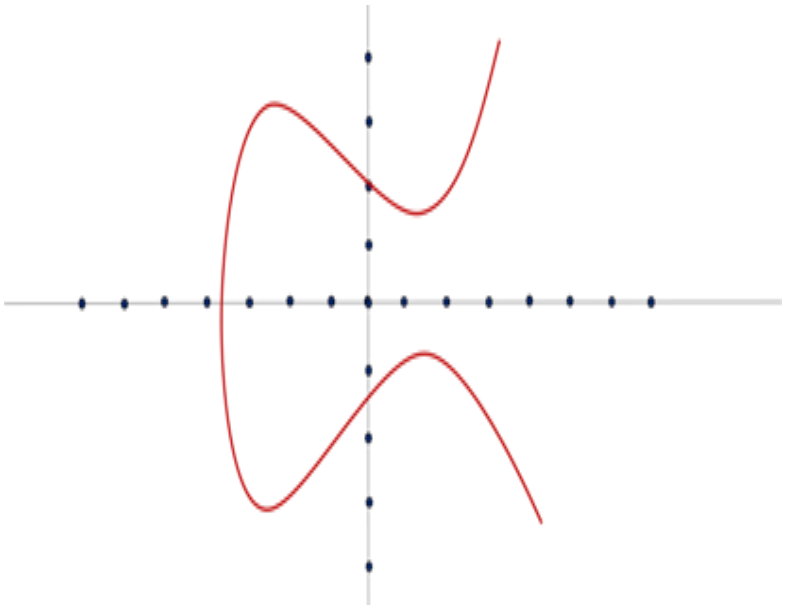

Figure 2.4 Elliptic curve

The Elliptic curve is applied to Abelian group. In Figure 2.5, 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.

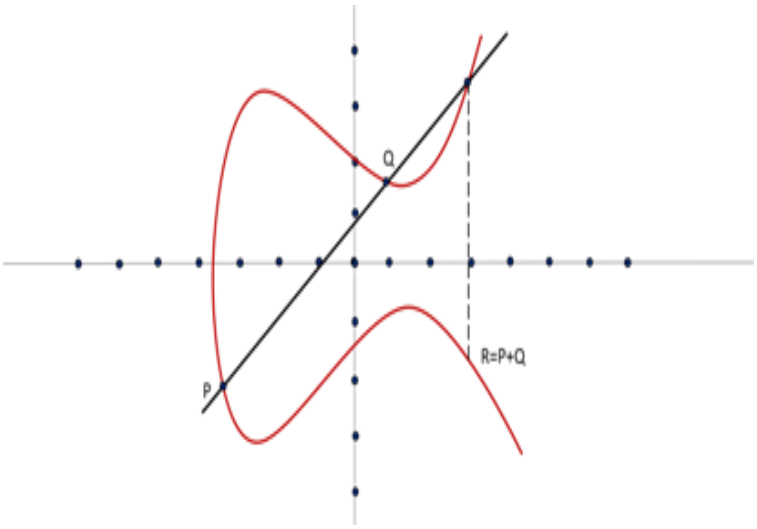

Figure 2.5 Group law on elliptic curve [23]

2.6 Related work

For communication between the user and the remote server, authentication is required. User and server check their authenticity. In existing protocol SIP, there is an issue of authentication due to HTTP digest. Analysis of all the vulnerabilities in existing research is done. Various researchers give different methods for the enhancement on SIP protocol and tried to enhance the security and integrity of the SIP protocol.

Yang *et al.* [24] proved that SIP cannot resist off-line password guessing attack. Yang *et al.* [24] proposed a scheme by using the concept of the key exchange protocol Diffie-Hellman [25] to solve the SIP authentication. Diffie-Hellman key exchange protocol uses the concept of Discrete Logarithmic Problem (DLP). The server gives the large prime as well as generator. Firstly, client and server authenticate each other then the password is shared. After the authentication, they can share resources with each other. There are still some flaws in this scheme. Security issue of SIP protocol is still in this scheme.

Huang *et al.* [26] proposed a protocol to improve the weakness of Yang *et al.* [24] protocol. Because Huang *et al.* [26] proved that Yang *et al.* [24] protocol is vulnerable to offline password attack by the cryptanalysis of Yang *et al.* [24] protocol. SIP was proposed by Huang *et al.* [26].This scheme is more efficient than Yang *et al.* [24] scheme. Huang *et al.* [26] uses more random number than the previous scheme. But Huang *et al.* scheme is still vulnerable to offline password guessing attack. Jo *et al.* [27] found that Huang *et al.* [26] still cannot withstand offline password guessing attack.

Then Durlanik *et al.* [28] proposed an authentication protocol. Durlanik *et al.* [28] used the concept of ECC for the SIP protocol. 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. The similar security level is provided by ECC with small key size as of RSA. For the ECC, less memory and low bandwidth is required. In Durlanik *et al.* scheme, Password is already shared with the SIP server by the SIP client. They authorize each other. Two keys are with server and client. Using the properties of ECC, the protocol is designed for SIP.

Wu *et al.* [29] also proposed a scheme using the concept of ECC. By the use of ECC, Wu *et al.* [29] finds the solution to authenticate key agreement problem in existing SIP. Wu *et al.* [29] scheme provides the mutual authentication by using the key agreement protocol. It gives the security like CK (Canetti-Krawczyk) security model. Later on, Yoon *et al.* [30] demonstrated that Durlanik *et al.* [28] and Wu *et al.* [29] protocol is not secure and cannot resist various attacks.

Yoon *et al.* [30] proposed a scheme by using the concept of ECC to improve the security of the SIP protocol. Yoon *et al.* [30] protocol is based on password based protocol. In Yoon *et al*. [30] scheme, there is enrollment phase, which is better than Wu *et al.* [29] scheme. So the Yoon *et al.* [30] scheme provides better security. In this scheme, key is established before the communication. Password is protected in this scheme, so it difficult by a notorious password attacker to guess the password. It is said that it is password protected based key agreement protocol in which mutual authentication is also there.

But Gokhroo *et al.* [31] and Pu [32] proved that Yoon *et al.* [30] protocol still cannot resist replay attack. Pu proved that offline password attack is possible in Yoon *et al.* [30] scheme. By using the dictionary attack, the attacker can guess the password

by single message transcript. So this scheme is not secure even thought it uses ECC. In this scheme, the session key can be easily derived from capturing the message exchanged between client and server

Tsai *et al.* [33] proposed a scheme for SIP using nonce-based authentication. Tsai *et al.* proved that Yang *et al.* [24] scheme has a high computational cost and the same issue with Durlanik *et al.* [28] scheme. Then Tsai *et al.* [33] proposed a scheme, which works on low power equipment. Computational cost of Tsai *et al.* [33] scheme is low. Tsai *et al.* [33] used the nonce-based authentication. In this scheme, client and server authenticate each other before the communication. Firstly the session key is shared and then authentication occurs. This scheme resists various attacks. But this scheme also fails to resist Denning-Sacco attacks and off-line password guessing attacks.

Yoon *et al.* [34] proposed a new scheme to overcome the issue of Tsai *et al.* scheme. Yoon *et al.* [34] proposed a scheme for SIP using DLP on elliptic curves. But Yoon *et al.* [34] protocol is still vulnerable proved by Xie [35]. Xie proved that Yoon *et al.* scheme cannot withstands stolen verifier attack and offline password guessing attack. Xie also proposed a scheme, which is more secure and efficient. In Xie scheme, password is encrypted by using a symmetric encryption algorithm. For the authentication of the client, Xie used the Diffie–Hellman key exchange value. For the server authentication, server signature is used. So, this scheme is more secure.

Arshad *et al.* [36] proved that Tsai *et al.* [33] scheme is not secure and proposed a new scheme using ECC. Arshad *et al.* [36] proved that Tsai *et al.* scheme does not provide perfect forward secrecy. To provide prefect forward secrecy, Arshad *et al.* [36] proposed a scheme by using ECC. In this scheme, mutual authentication is also there. Arshad *et al.* [36] used the DLP property of ECC and gives a novel scheme. Arshad *et al.* [36] scheme resists various attacks and also provides better security. Arshad *et al.* scheme is a faster algorithm than its previous counterparts.

After that, He *et al.* [37] proved that Arshad *et al.* [36] protocol cannot resist various attacks. In Arshad *et al.* [36] scheme, offline password guessing attack is possible by attacker. He *et al.* [37] proposed enhanced scheme than Arshad *et al.* scheme. He *et al.* [37] also used ECC. He *et al.* [37] scheme provides better security. This scheme is more efficient than Arshad *et al.* [36] scheme.

Tang *et al.* [38] proposed a SIP protocol which is efficient and flexible. Tang *et al.* [38] used the password authentication key agreement protocol. By using this protocol mutual authentication occurs in SIP. Tang *et al.* [38] scheme provides the mutual authentication as well as a session key agreement. In this scheme, updation of password can be easily done and there is no need to maintain a verification table. This scheme is more efficient because the password table is not required for verification.

But Tang *et al.* cannot resist an impersonation attack as was specified by Tu *et al.* [39]. Tu *et al.* [39] proposed a new scheme to resist impersonation attack. Tu *et al.* used the additional calculation and improved the algorithm. The computational overhead is increased and overall security also increased. Tu *et al.* [39] scheme gave the mutual authentication and was fast, as compared to other algorithms. Tu *et al.* [39] proposed efficient scheme for SIP by using smart card.

Wang *et al.* [40] proposed a new scheme using the concept of two-variant hashing operation. Security level increased but with the use of two-variant hashing computational cost increased as well. So this overhead can be ignored. As in this scheme, there is no requirement to maintain a verification table. So this scheme is more fast and efficient.

Chen *et al.* [41] proved that Wang *et al.* [40] scheme was not secure from parallel session attack. Then Chen *et al.* [41] proposed a protocol which withstands a parallel session attack as well as a verifier impersonation attack. Chen *et al.* improved the scheme of Wang *et al.* [40] In this scheme various hash functions are used and verifier table was not required, but the Chen *et al.* [41] protocol was still weak.

Yeh *et al.* [42] proposed a more efficient scheme. SIP needs the efficient method for the mutual authentication in unfavorable environments. Yeh *et al.* [42] used the ECC in smart cards. In this scheme, DH- based authentication is used. It is more efficient than other scheme. But Yeh *et al.* [42] scheme had some issues. Mutual authentication in Yeh *et al.* [42] scheme is weak and could not resist the stolen verifier attack.

To solve all these issues in this dissertation, a scheme is proposed which is more secure and efficient by using the ECC and smart cards for SIP. By using this scheme, various attacks in VANETs can be resisted. The computational overhead increased, which can be ignored. Overall security is enhanced in this scheme.

Table 2.1 Existing SIP scheme comparison

Schemes	Techniques	Vulnerabilities (attacks)	Key Management
Yang *et al.* [24]	HTTP Digest	Offline Password Guessing	DH Key Exchange
Huang *et al.* [26]	One-way Hash	Offline Password Guessing	DH Key Exchange
Durlanik *et al.* [28]	ECC (ECDH)	Denning-Sacco, Stolen Verifier	Public Key
Wu *et al.* [29]	ECC	Denning-Sacco, Stolen Verifier	Public Key
Yoon *et al.* [30]	ECC	Relay attack, Offline Password Guessing	Public Key
Tsai [33]	Nonce	Denning-Sacco, Offline Password Guessing	Public Key
Xie [35]	ECDH	Denning-Sacco	Symmetric Key
Arshad *et al.* [36]	ECDLP	Offline Password Guessing	Public Key
He *et al.* [37]	ECC	Denning-Sacco	Public Key
Tang *et al.* [38]	Smart Card	Impersonation attack	DH Key Exchange
Tu *et al.* [39]	Smart Card	Stolen Verifier attack	Public Key
Wang *et al.* [40]	Smart Card	Parallel Session attack	Public Key
Chen *et al.* [41]	Smart Card	Impersonation attack	Public Key
Yeh *et al.* [42]	ECC	Stolen Verifier attack	Public Key

2.7 Problem statement

VANETs fascinated many research institutes to do work on vehicular network applications. Even many automotive industries are working on it. With the growth in technology, the use of portable and small network devices is increasing day by day. The need of VANETs also increased. There are technical, social and economic challenges in VANETs communication. Security is the main technical issue of VANETs. During VANETs communication, message should be secured so that an attacker cannot reveal it. VANETs give us road safety. VANETs message should be secured and only legitimate user can only access it.

A security efficient algorithm should be designed for VANETs. There should be proper protocol followed for security. So, smart card is used for SIP protocol of VANETs. Existing algorithms have issue of security and these algorithms are vulnerable to various attacks. Improved scheme provides better result of security.

MAPS^{TM} [43] simulator is used for implementation in a simulation environment. Security enhancement of proposed protocol was checked by using the graph of a particular area. Then, security and performance analysis of proposed algorithm is done with existing algorithm.

2.8 Objective

The primary objective of thesis is to improve the security of SIP for VANETs. It used a realistic model for VANETs communication. Extra parameters are added in algorithms to improve the security.

Chapter 3

Proposed Solution

3.1 Proposed authentication protocol

In this authentication protocol, ECC based secured authentication protocol has been proposed. The different notation used in this scheme is described in the Table 3.1. Phases of this scheme are:

- System setup phase
- Registration phase
- Vehicle to RSU authentication phase
- Password change phase

Table 3.1 Notation used in the proposed scheme

Symbols	Definition
$\|\|$	String contention operation
G_k	Cyclic group of prime order n of k
h(.)	Secure one-way hash:(0,1) → (0,1)
K	Large prime generator of group
$H_1(.)$	Secure one-way hash of G_K
N	Order of Elliptic Curve
$\oplus$	Exclusive operation
P(X)	Random polynomial
P_{ri}	Private key of system
P_{pu}	Server public key
Y	Shared session key between A and B
×	scalar multiplication of Elliptic Curve
S_r	Secret key of user
T	Timestamp
$H_2(.)$	Secure one-way hash of Z^*_K
A	Client
B	Server
Usr	Username of user
P_{wd}	Password of user
$H_3(.)$	Secure one-way hash of Z^*_K
F_k	Finite prime field
$E_K(a, b)$	Elliptic curve over a field F_K (finite)
$Mac_{m,t}$	message authentication code of m at t

3.1.1 System setup phase

There are various formulas for the key generation. In this scheme, system parameters are set up by the client and the server. Then the client and server choose an elliptic curve of order n over $E_k(a,b)$ generated by K. P_{ri} is a private key of the system is randomly selected. Point multiplication is used for computation of authentication key Z_k. Finally, all values are stored in a smart card, i.e. $(C_A, D_A, h(.), H_1(.), H_2(.), H_3(.))$ on the server side.

3.1.2 Registration phase

In this phase, all values are set up in a smart card for the client and then the client register to the remote server. All these values stored in a smart card are kept secret. In this scheme, there are three hash computations and three exclusive OR operations as shown in Figure 3.1. Firstly, $P(a_i)$ (eq. 3.1) is chosen from the polynomial:

$P(X) = p_n x^n + p_{n-1} x^{n-1} + \ldots\ldots\ldots\ldots\ldots\ldots + p_2 x^2 + p_1 x^1 + p_0$. equation of degree n.

Choose all the parameters from the equation, i.e. $p_n, p_{n-1}, \ldots\ldots p_2, p_1, p_0$.

$$P(a_i) = \sum_{i=0}^{n} p_i \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.1)$$

- **Step 1:** $A \rightarrow B(id, P_{wd})$: To compute P_{wd}, the user enters his/her id and P_{pu} and obtain $P_{wd} = h(P_{pu} \oplus P(a_i))$ where $P(a_i)$ is a random number chosen from polynomial. id and P_{wd} verified the identity of user and server. To register the user to the server, id and P_{wd} was sent to a remote server. Then, user was eligible for communication.
- **Step 2:** The server computed $S_r = P_{ri} \times H(id) \in G_k$ and authenticates the user. The server calculated $C_A = h(id \oplus P_{wd})$ and $D_A = h(P_{wd} \,||id\,||t_1)$. In D_A, Timestamp was applied to provide the integrity. After that, all values provided to a smart card and stored in it and keep it secret and these values sent to the user.
- **Step 3:** A smart card is sent by the server to the user. Then user store the random number $P(a_i)$ in a smart card and these values remained secret in smart card, i.e. $(C_A, D_A, h(.), P(a_i), H_1(.), H_2(.), H_3(.))$.

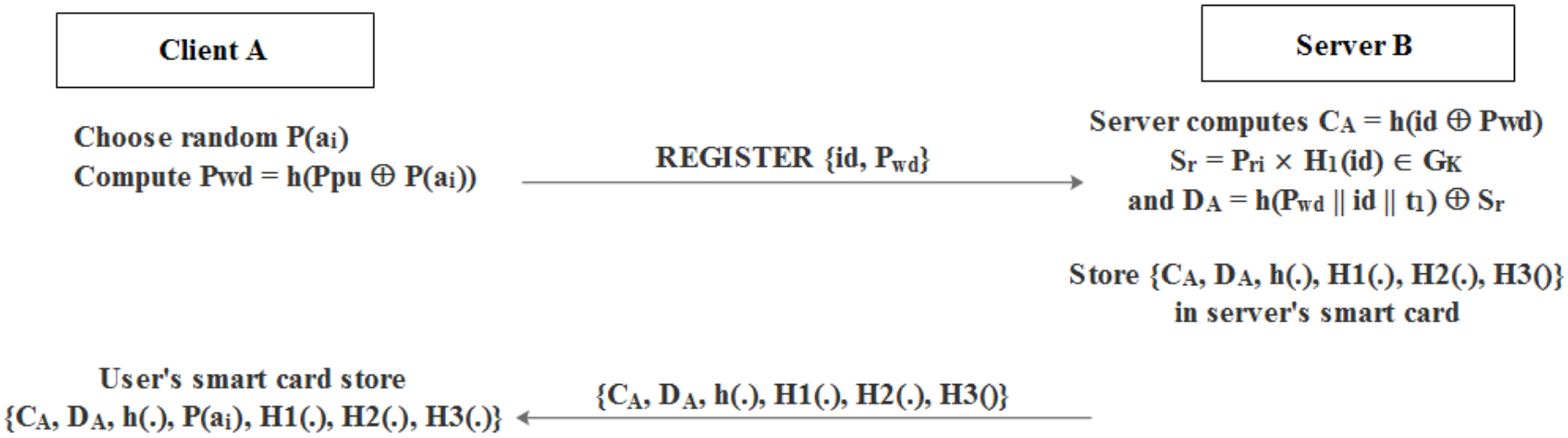

Figure 3.1 Registration phase of proposed protocol

These are stored by the user on a smart card.

3.1.3 Vehicle to RSU authentication

In Vehicle to RSU authentication phase, client communicated with the remote server. For this, client user-name and password was required.

- **Step 1:** $A \rightarrow B$: Request $(Usr, T_2, N_A, R_A, mac_{m,t3})$: Firstly, the user computed $P_{wd} = h(P_{pu} \oplus P(a_i))$ and $C_A^{'} = h(id \oplus P_{wd})$. Then checked C_A was equal to $C_A^{'}$ or not. If they were equal, then calculated the $V = h(P_{wd} \,||id)$ and $S_r = (D_A \oplus V)$. After this, the user took a random point R_A on curve $E_K(a,b)$. At the timestamp T_2, the user calculated $t_2 = H_2(T_2, N_A = R_A + t_2 \times S_r)$ and $R_A^* = R_A^x \times K$. Then user computed the $mac_{m,t3}$, for the message m and sent it to the remote server with his/her id and P_{wd}.
- **Step 2:** $B \rightarrow A$: Challenge $(realm, T_4, N_B, N_Y)$: After the request received from the client, the server computed U_{IDA} by transforming into $H_1(id)$ which is one-way hash digest. Then the server computed $R_A^{'} = N_A - P_{ri} \times t_2 \times U_{IDA}$. The Server verified that, whether R_A^* is equal to $R_A^{X^{'}} \times K$ or not. If they were equal, then a point was chosen by server, i.e. R_B. Then calculated N_B, Y and N_Y at timestamp T_4. After that, it verified the MAC [11]. If they were equal, then authenticated the user otherwise rejects it. Finally, the server sent challenge message to the user.
- **Step 3:** The user received the challenge message from the server. User computed the value of $R_B^{'} = N_B - t_4 \times S_r$, in which $t_4 = H_2(T_4)$. Then the user computed Y^*, N_Y^* and verified N_Y is equal to N_Y^* or not. If they were equal, then server was authenticated, otherwise rejects the request.
- **Step 4:** Response $(realm, Usr, h(Usr \,||realm\,||Y)$: User calculated $h(Usr \,||realm\,||Y)$ and response message was sent to server.
- **Step 5:** After the authentication of the server, the response message was sent by the client and received by the server. Then server B computed response* and check whether response* = response. If they were equal, then the

connection was accepted. Server sent the invite message as shown in Figure.3.2.

3.1.4 Password change phase

- **Step 1**: Value of password can be changed by the user after giving the new value of Usr and P_{pu}^{*}. Then client calculated $P_{wd} = (P_{pu}^{*} \oplus P(a_i)$ and updated in a smart card.
- **Step 2:** When the server got the demand for password change. $C_A^{*} = (id \oplus P_{wd}^{*})$, $D_A^{*} = h(P_{wd} \,||id\,||t_1) \oplus S_r$ is computed by server and new value is stored in server smart card.

In password change phase, the smart card changes the value of C_A, D_A with C_A^{*}, D_A^{*} without informing the server.

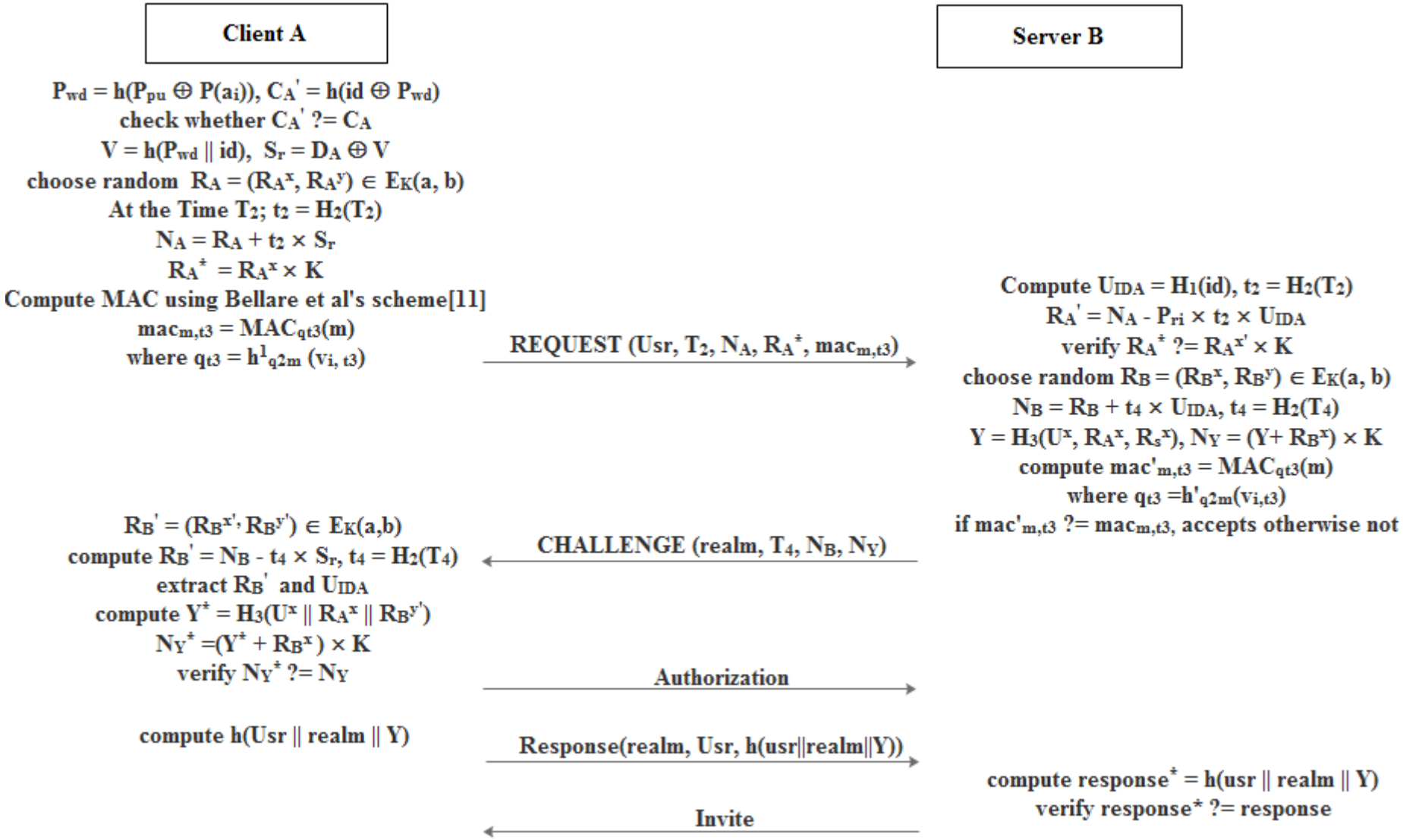

Figure 3.2 Vehicle to RSU authentication phase

Chapter 4

Implementation and Simulation

4.1 Implementation

In this chapter, implementation model of proposed algorithm is given. For the implementation, Message Automation and Protocol Simulation (MAPS^{TM}) [43] simulator is used with real map of the city. In previous chapter, proposed authentication protocol is in algorithmic form.

4.2 Simulator

According to Shannon [44], simulation is "the process of designing a model of a real system and conducting experiments with this model for the purpose of understanding the behavior of the system and/or evaluating various strategies for the operation of the system."

To test the proposed protocol, MAPS^{TM} simulator 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[45], OMNET++ [46], MAPS^{TM} [43]. These simulators are used for micro and macro both levels of transportation. During the simulation of VANETs, the important parameter is node mobility. In this dissertation, real world node model is used for correct results.

MAPS^{TM} [43] is used to generate the SIP protocol communication. In this dissertation, different test cases were used for the SIP protocol. By using this simulator, proposed scheme is compared with existing schemes. Brief introduction about MAPS^{TM} simulator as follows:

4.2.1 MAPS™

This simulator is designed for the SIP. MAPS™ is used for simulations of user agents. By using this, protocol conformance testing is performed. MAPS™ is of two types:

- MAPS™ SIP Protocol Test Tool
- MAPS™ SIP Conformance Test Suite

VoIP is also simulated by MAPS™. MAPS™ can act as SIP entity as well as generate any SIP message. MAPS™ is powerful simulator. This simulator supports various traffic events like call etc., features of MAPS™ simulator:

- IP packet Spoofing
- RTP Extended Header
- INVITE message with 'Priority' and 'Subject' of headers
- MAPS™ SIP used for different simulation
- MAPS™ SIP uses different parameter for calling purpose
- Generation R2S-KeepAlive packets

MAPS™ SIP used for online captured packet analyzing, and also checks the SIP signaling by using real-time environment. The MAPS™ HD [43] simulator is used for high volume traffic.

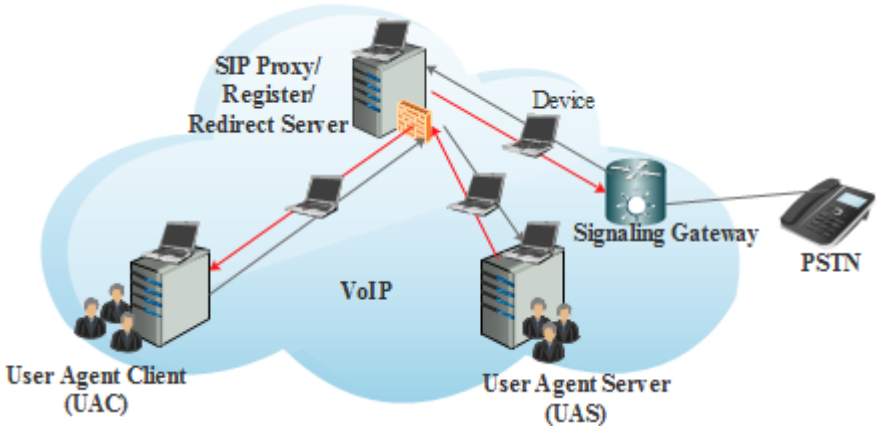

Figure 4.1 MAPS™ Scenario

4.2.2 Main features

- Supports peer to peer gateway testing
- Real time environment for all messages can be used for simulation
- TCP and UDP both are supported by MAPS™
- It provides the voice feature for next generation traffic
- VoIP implementation is supported by this simulator
- Simulate SIP header as well as full message of SIP
- If any instant message is supported by MAPS™ simulator

- Automatic call and generation script is supported by it
- It handles the as many retransmissions
- When there is request through proxy. It handles the strict as well as loose routing
- Media can be created before call establishment by using this simulator

Other notable features include

- Support for SIP conformance testing
- Interfaces to Portable VoIP and T1/E1
- Multi-protocol call trace for VoIP

Table 4.1 Standards of supported protocols

Supported Protocols	Specifications Used
SIP	RFC 3261
SIP Extensions	RFC 3262, RFC 3515

4.3 Simulation setup & implementation

In this dissertation, MAPS^{TM} simulator was used simulation. Parameters used for MAPS^{TM} simulator as described in Table 4.2.

Table 4.2 Simulation setup

Types	Parameters
Data packet size	512 bytes
Scenario	Urban
Channel Type	Wireless Channel
Bandwidth	2Mbps
Traffic Type	TCP
MAC type	IEEE 802.11p

Firstly, client server system was setup in this simulator as shown in Figure 4.2. While proxies test, MAPS^{TM} can act as User Agent Client (UAC) and User Agent Server (UAS). UAC (MAPS^{TM}) received the message. UAC sends the unmodified messages

to the UAS. Client server system is configured after all these requests. System is ready for call generation after the system setup.

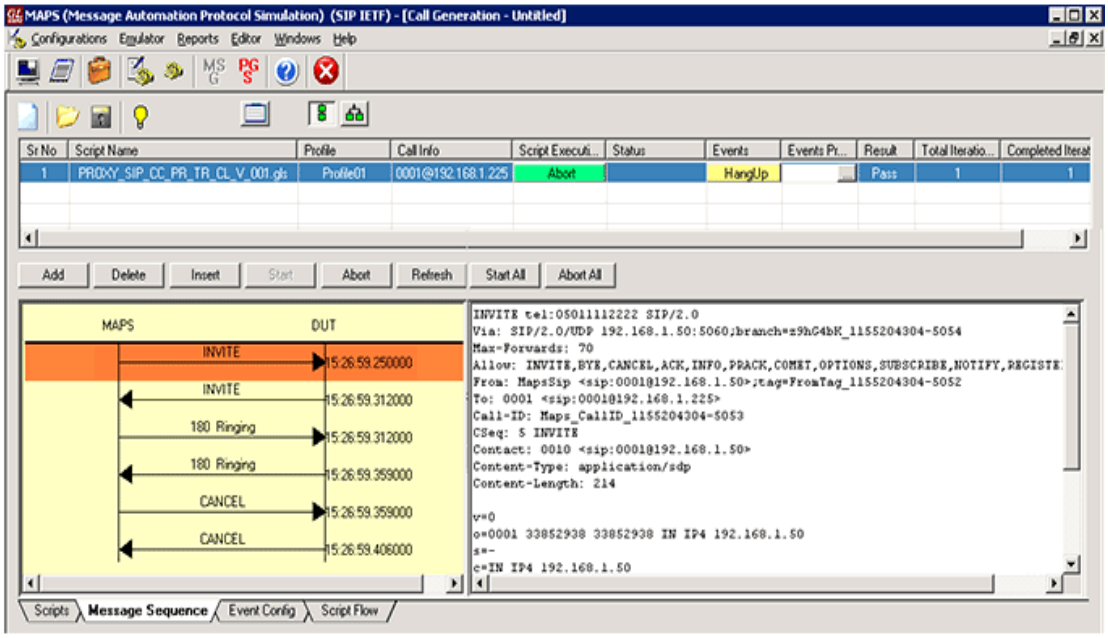

Figure 4.2 System setup phase in MAPS^{TM} simulator

After the system setup, SIP calls were generated. Then, Communication was possible between client and server shown in Figure 4.3.

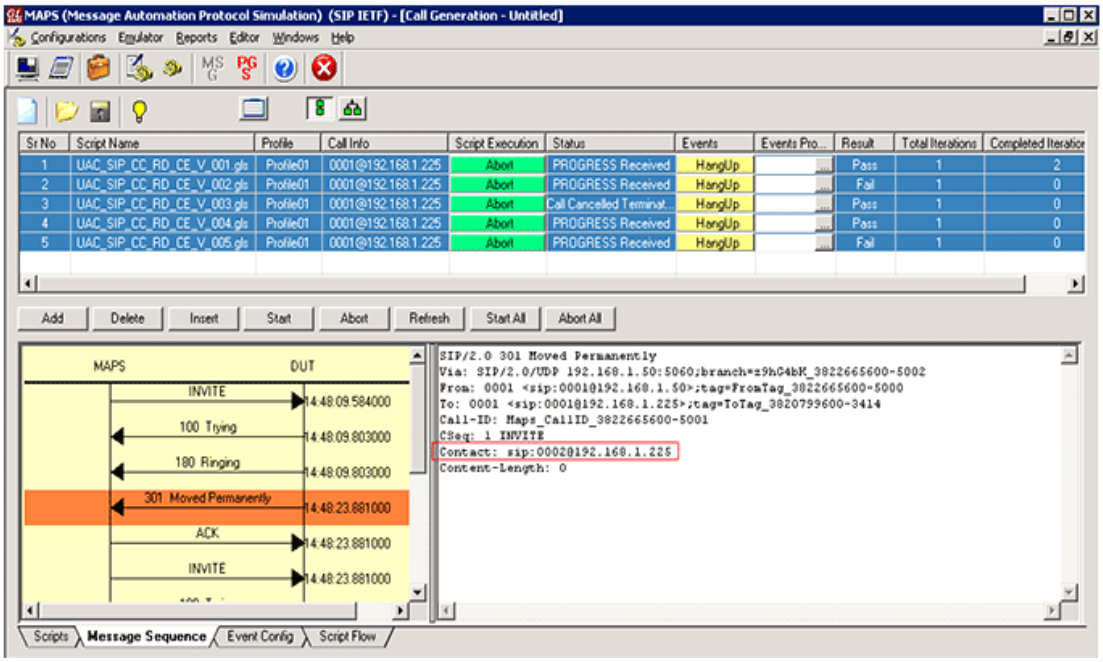

Figure 4.3 Call generation during system setup phase

By using call Generation phase in the simulator, outgoing communication as well as control communication was simulated. After call generation of communication, client and server were registered as shown in Figure 4.4. Then, authentication was occurred between client and server.

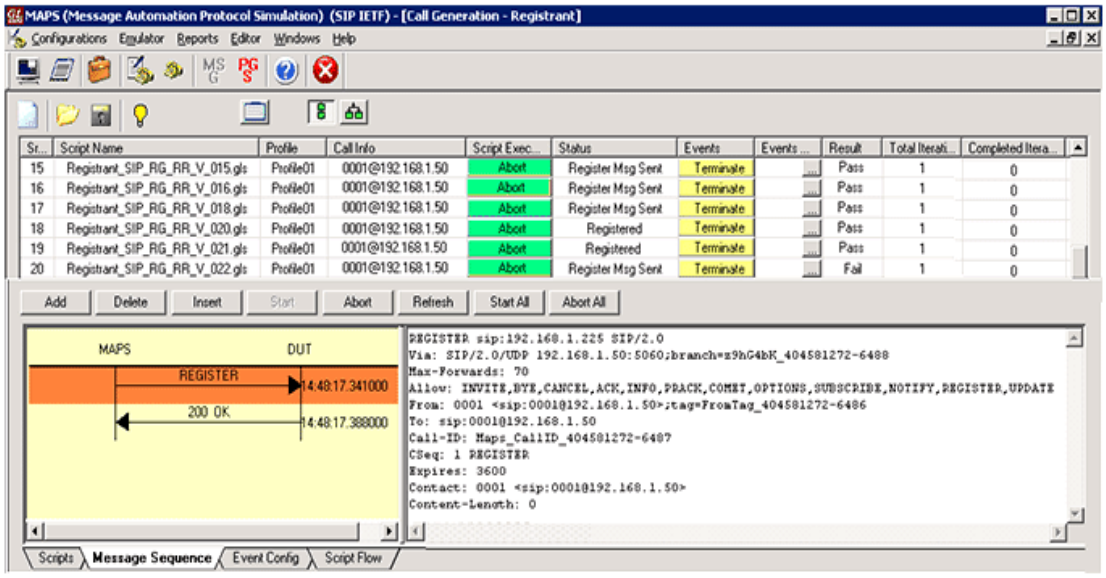

Figure 4.4 Registration phase during simulation

After the registration between client and server, calls can be sent and received. Call reception between client and server as shown in Figure 4.5.

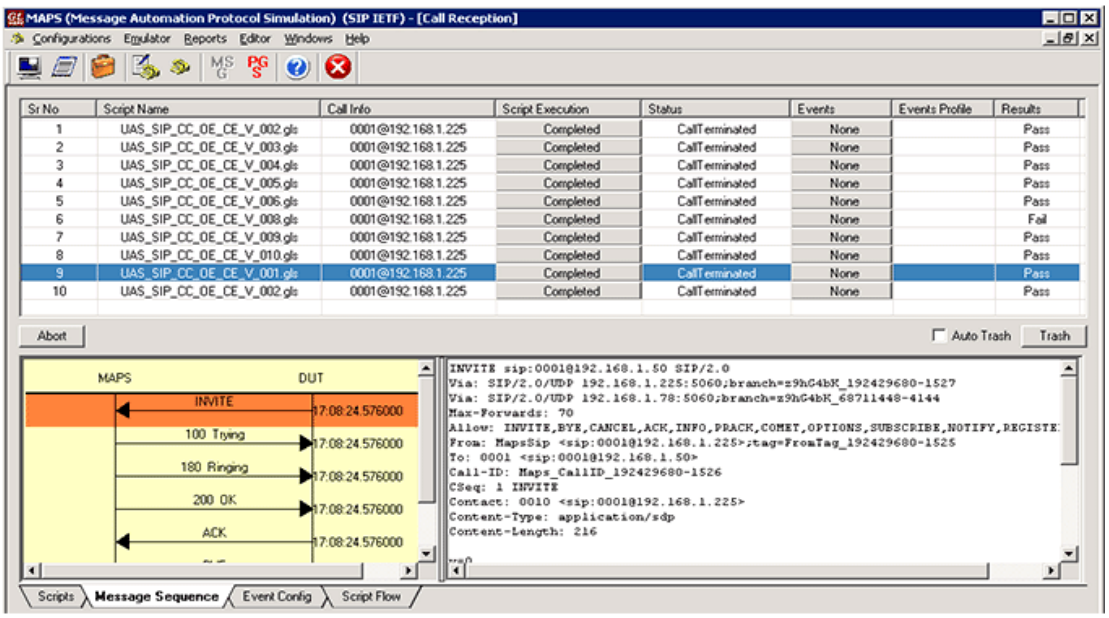

Figure 4.5 Successfully call reception

MAPS^{TM} checks the incoming message by using ‘recv’ instruction.

After all the phases, a successful connection is established between client and server as shown in Figure 4.6. Now user can communicate by sending ‘recv’ message or can terminate a connection by using ‘terminate’ message.

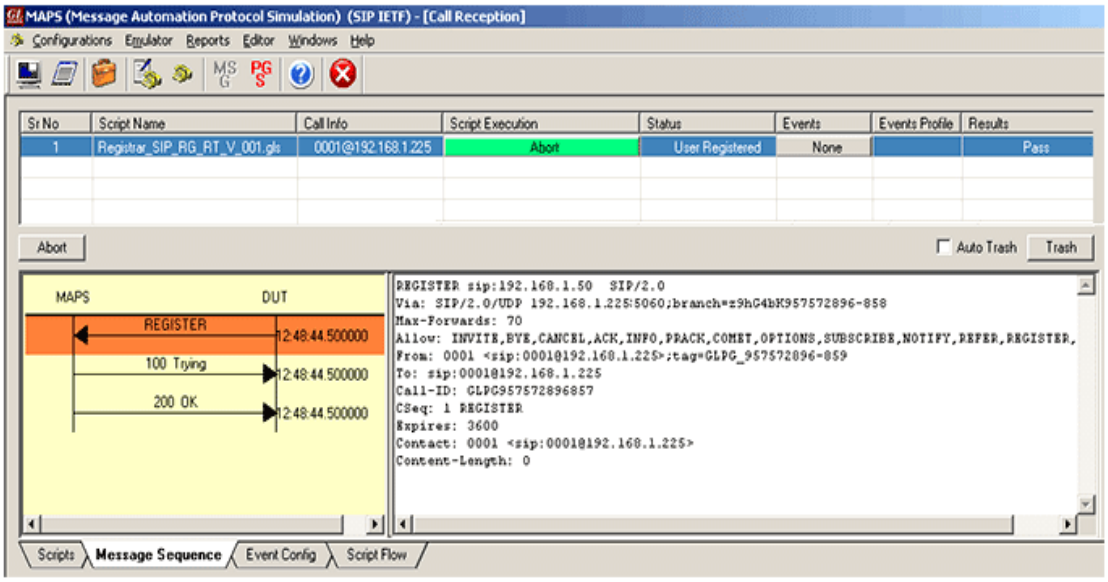

Figure 4.6 Successfully connection between client and server

Chapter 5

Results and Discussion

5.1 Results

The Results of the simulation are shown in this chapter. A local area map loaded with traffic is used for simulation as shown in Figure 5.1. All parameter is analyzed by using traffic of this map. Yeh *et al.* [42] scheme is compared with proposed scheme using this urban area map.

Figure 5.1 Local area google map

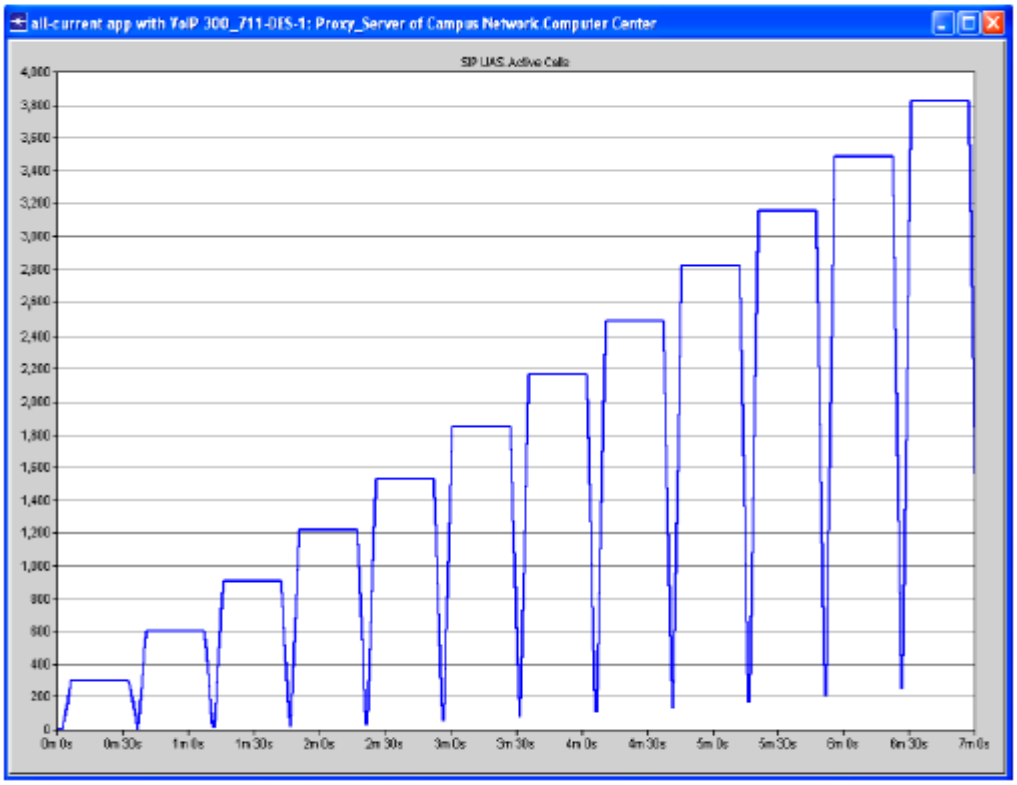

Figure 5.2 Active SIP calls

Firstly, the Simulator sends SIP active calls as shown in Figure 5.2 to the local urban area. All active calls to checks the communication of VANETs.

After sending the active SIP calls to the all vehicles, the end to end delay is computed using parameters. In Figure 5.3, proposed scheme takes less delay. End to end delay of proposed scheme is .04 and Yeh *et al.* scheme is 0.12 after the computation.

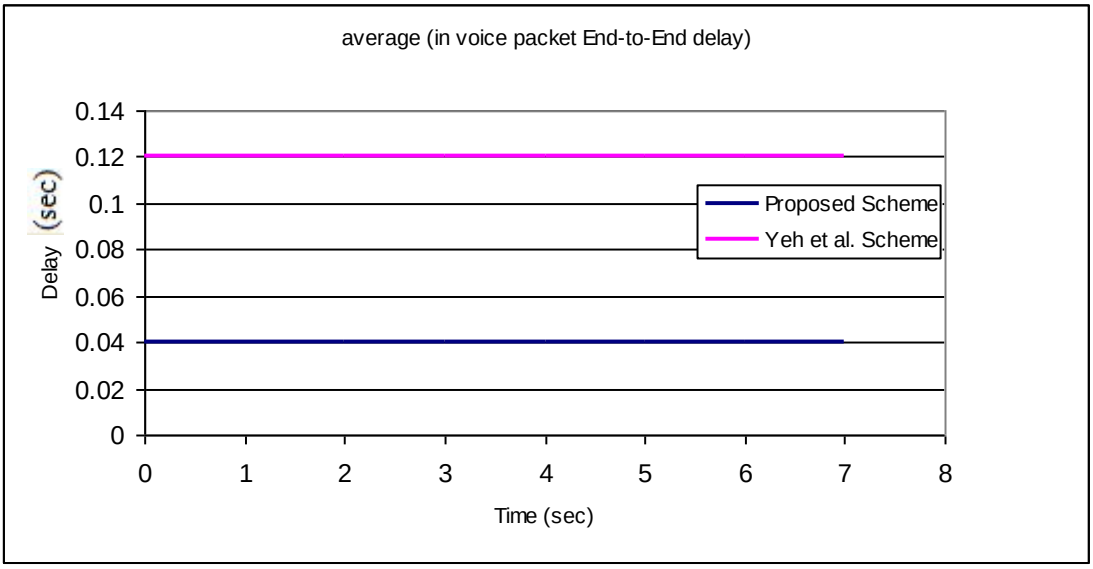

Figure 5.3 End to end delay comparison

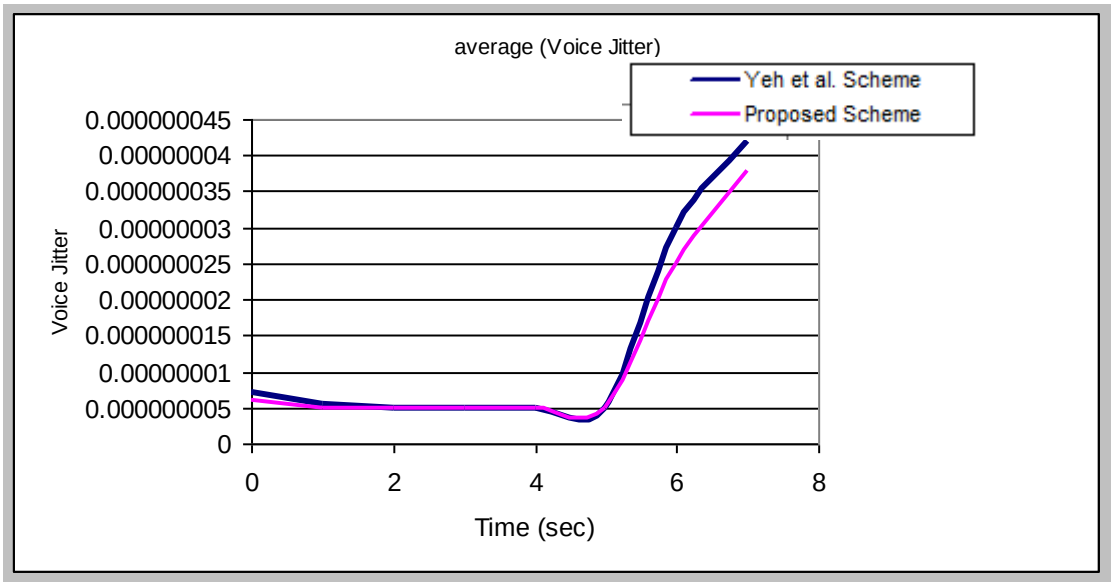

Figure 5.4 Voice jitter comparison

Voice jitter of proposed scheme is slightly less Yeh *et al.* scheme as shown in Figure 5.4. Computation cost of proposed scheme is slightly less that of *Yeh et al.*

5.2 Security analysis

Proposed scheme provides P2P communication as well as mutual authentication. Proposed scheme provides security from various attacks, i.e. masquerade attack, replay attack, stolen verifier attack etc. Security analysis of proposed scheme is shown below:

5.2.1 Masquerade attack resistant

The attacker should know P_{pu}, which is the user's password for the verification of identity in the login phase to perform this attack. Since $P_{wd} = h(P_{pu} \oplus P(a_i))$, $C_A = h(id \oplus P_{wd})$, $N_A = R_A + t_2 + S_r$ and $R_A^* \times K$. All these parameters are calculated by using scalar multiplication and one-way hash function. It is impossible for the intruder to masquerade as the legitimate user without the client id i.e. P_{pu} and $P(a_i)$. One legitimate user can't behave as the other legitimate user without having the password of user.

5.2.2 Parallel session attack resistant

Server gave the cipher message code for N_A, R_A^* etc., which are instances of authentication protocol in scheme. In this dissertation, timestamp was used for random point R_A calculation. So, that it resists the parallel session attack.

5.2.3 Insider attack resistant

In proposed authentication protocol, the registration of the user has happened using the $P_{wd} = h(P_{pu} \oplus P(a_i))$ over a secure channel. The value of $P(a_i)$ is generated randomly. So that risk of insider attack is avoided.

5.2.4 Password guessing attack resistant

In proposed authentication protocol, password is computed by using $P_{wd} = h(P_{pu} \oplus P(a_i))$ randomly selected from the elliptic curve and then one way hash

with a secret key. Its value stored in the smart card. So while transmitting the SIP message, it is impossible to guess the password by the attacker. In this, ECDLP is used in of R_A^* and $R_A^* \times K$ of and $(Y + R_B^*)$ of $(Y + R_B^*)$ times K. So it is impossible to get the session key. Whenever there are changes in user's password, the values in smart card are also changes.

5.2.5 Stolen Verifier attack resistant

In proposed authentication protocol, there is no requirement of maintaining any verifier table for the user password. Only the server master key Y is required. So the attacker fails if he/she tries for verifier table. So the stolen verifier attack is not possible.

5.2.6 Replay attack resistant

In proposed scheme, N_A, R_A^* is randomly chosen in the secret key cipher, which is not same in each authentication session. Time-stamping is also used in this scheme. Attacker fails if he/she tries to replay the same message. The validity of the user is also there, which is authenticated by the server. So, the attacker fails to be a legitimate user.

Table 5.1 Security analysis with referenced scheme

Attack Types	**Yeh *et al.* Scheme [42]**	**Proposed Scheme**
Masquerade attack resistant	Yes	Yes
Insider attack resistant	Yes	Yes
Parallel session attack resistant	Yes	Yes
Password guessing attack resistant	Yes	Yes
Replay attack resistant	Yes	Yes
Stolen Verifier attack resistant	No	Yes
Mutual authentication	Provided but weak	Provided and strong
P2P communication	No	Yes

5.2.7 Mutual authentication

In proposed scheme, there is mutual authentication between the user and server by using the key exchange protocol Elliptic Curve Diffie-Hellman (ECDH). In this dissertation, MAC scheme is used for the mutual authentication of a message. When the server receives the challenge from the client, server sends the correct response if and only if the server's identity is authenticated. If R_A^* is equal to $R_A^* \times K$.

5.2.8 P2P communication

In proposed scheme, concept of timestamp is used. At a particular time Δt , when the message is sent and alive. This scheme provides P2P communication at that particular time Δt . Then the time overhead decreases during communication.

5.2 Performance analysis

Proposed scheme is compared with the referenced scheme in performance analysis. Communication cost, security and vulnerability are discussed. It enhances the security and preserving the integrity of SIP. In Table 5.1; various attacks are listed. In proposed scheme, time overhead increased because of extra calculation of time-stamp and MAC.

The Complexity of this scheme is more because, Polynomial is used for the generation of public key. But, overall security increased in this proposed scheme. This scheme is more efficient than existing schemes. Let T_{esm}, T_h, T_{mac}, T_{eca} *and* T_{ecp} denotes the time for the elliptic curve scalar operation, one-way hash, the message authentication code, elliptic curve addition and elliptic curve polynomial operation separately. The executing time for hash function operation, elliptical curve operation and MAC operations are 0.0005s, 0.0087s and 0.0004s respectively [47]. The computation cost of proposed scheme $1T_h$ *and* $1T_{eca} + 2T_h$ of user and server respectively in the registration phase. In vehicle to RSU authentication phase, the computation cost of my scheme $1T_{ecp} + 7T_h + 2T_{eca} + 4T_{esm} + 1T_{mac}$ *and* $1T_{ecp} + 5T_h + 1T_{eca} + 2T_{esm} + 1T_{mac}$ of user and server respectively. In this phase, T_{mac} time was additional, which increased the time overhead. But enhance the security and integrity of the algorithm. In Table 5.2, Yeh *et al.* [42] scheme is compared with proposed scheme authentication scheme and conclude that my scheme is more efficient.

Table 5.2 Computational compression with referenced scheme

Phase		**Yeh *et al.* Scheme [42]**	**Proposed Scheme**
Registration Phase	User Side	*1Th*	*1Th*
		≈ 0.0005s	≈ 0.0005s
	Server Side	*1Teca + 2Th*	*1Teca + 2Th*
		≈ 0.0097s	≈ 0.0097s
V2R authentication	User Side	*1Tecp + 7Th +*	*1Tecp + 7Th +*
Phase		*2Teca+4Tesm*	*2Teca+4Tesm+ 1 Tmac*
		≈ 0.0644s	≈ 0.0648s
	Server Side	*1Tecp + 5Th +*	*1Tecp + 5Th +*
		1Teca+2Tesm	*1Teca+2Tesm + 1Tmac*
		≈ 0.0373s	≈ 0.0377s

Chapter 6

Conclusion and Future Scope

6.1 Conclusion

In this dissertation, security flaw of Yeh *et al.* [42] authentication scheme for SIP is analyzed. Yeh *et al.* [42] scheme can't withstand the stolen verifier attack and P2P communication is not available. In proposed improved scheme, all these weakness are removed. By using the MAPS^{TM} simulator, proposed authentication protocol is implemented. In which, end-to-end delay of proposed scheme is analyzed. Proposed protocol end-to-end delay is compared with Yeh *et al.* [42] scheme. End-to-end delay of proposed scheme is less. According to security analysis, proposed scheme withstands the stolen verifier attack and P2P communication is also available. According to performance analysis, proposed scheme gives the time overhead. But integrity and security is increased. This factor can be ignored. Proposed scheme is more efficient.

6.2 Future Scope

I would like to extend the current work in vehicular cloud computing. Time overhead should be reduced in proposed scheme to increase the efficiency. The detail to this work is the future of this thesis.

References

[1] "Cisco Website," [online]. Available: http://www.cisco.com/cisco/web/solutions/smallbusiness/resourcecenter/articles/work from anywhere/what is a wireless network/index.html. [Accessed May 2015].

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

[3] "EFKON Toll Management System website," 2013, [online]. Available: http://www.efkonindia.com/EFKON_toll_management_system.php [Accessed: May 2015].

[4] "Scania Group Website," 2013, [online]. Available: http://www.scania.com [Accessed: May 2015].

[5] 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.

[6] "Traffic Vigilance Website," 2014, [online]. Available: http://www.teletrafficuk.com/products-concept-ii.htm [Accessed: May 2015].

[7] "Intelligent Transport System Website," 2012, [online]. Available: www.its.dot.gov/aeris [Accessed: June 2015].

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

[9] 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.

[10] H. Moustafa, Y. J. Jhang, “Vehicular Networks techniques Standard and Application,” CRC Press, 2009.

[11] M. Bellare, R. Canetti and H. Krawczyk “Message authentication using hash functions the HMAC construction,” RSA Lab CryptoBytes, Vol. 2, No. 1, pp. 12-15, 1996.

[12] D. Jiang, L. Delgrossi, “IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments,” In Vehicular Technology Conference, 2008, pp. 2036-2040.

[13] H. Hartenstein, K. P. Laberteaux, "VANET Vehicular Applications and Inter-Networking Technologies," Wiley Publications, pp. 368, 2009.

[14] K. Y. Ho, P. Kang and C. H. Hsu, "Implementation of WAVE/DSRC Devices for Vehicular Communications," in International Symposium on Computer Communication Control and Automation, Vol.2, No. 1, 2010, pp. 522-525.

[15] J. Franks, P. H. Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen and L. Stewart, “RFC2617: HTTP Authentication: Basic and Digest Access Authentication,” IETF, pp. 1-34, 1999.

[16] S. Salsano, L. Veltri and D. Papalilo, “SIP security issues: the SIP authentication procedure and its processing load,” IEEE Netw J., Vol. 16, No. 6, pp. 38-44, 2002.

[17] D. Geneiatakis, T. Dagiuklas, G. Kambourakis and C. Lambrinoudakis, “Survey of security vulnerabilities in session initial protocol,” IEEE Commun. Surv, Vol 8, pp. 68-81, 2006.

[18] D. Sisalem, J. Kuthan and S. Ehlerts, “Denial of service attacks targeting a SIP VoIP infrastructure: stack scenarios and prevention mechanisms,” IEEE Netw. J., Vol. 20, No. 6, pp. 26-31, 2006.

[19] RL. Rivest, A. Schamir and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems”, Communications of the ACM, Vol. 21, No.2, pp. 120-126, 1978.

[20] N. Koblitz, A. J. Menezes, and S. A. Vanstone, “The state of elliptic curve cryptography. Design, Codes, and Cryptography,” Vol. 19, Issue 2-3, pp. 173-193, 2000.

[21] VS. Miller, “Use of elliptic curves in cryptography,” Advances in Cryptography-Crypto’85, Springer Verlag, Vol. 218, No. 2, pp. 417-426, 1986.

[22] J. Menezes, E. Teske and A. Weng, “Weak fields for ECC.CORR 2003-15”, Technical Report, University of Waterloo, 2003.

[23] Martin, Leslie, “Elliptic Curve Cryptography”, Advanced Combinatorics, An ECC research project, 2006.

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

[25] W. Diffie, M.E. Hellman, “New directions in cryptography,” IEEE Trans. Information Theory, Vol. 22, No. 6, pp. 644-654, 1976.

[26] H. Huang, W. Wei and G. Brown, “A new efficient authentication scheme for session initiation protocol,” Proc JCIS, Vol. 02, No. 1, 2006.

[27] H. Jo, Y. Lee, M. Kim, S. Kim and D. Won "Off-line password guessing attack to Yang's and Huang's authentication schemes for session initiation protocol," Proc INC, IMS IDC, pp. 618–621, 2009.

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

[29] 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.

[30] E.J. Yoon, K.Y. Yoo , C. Kim, Y.S. Hong, M. Jo and H.H. Chen, "A secure and efficient SIP authentication scheme for converged VoIP networks," Comput Commun, Vol. 33, No. 14, pp. 1674–1681, 2010.

[31] M.K. Gokhroo, C.D. Jaidhar and A.S. Tomar, "Cryptanalysis of SIP secure and efficient authentication scheme," Proc ICCSN, 2011, IEEE 3rd International Conference on, pp. 308–310.

[32] Q. Pu, "Weaknesses of SIP authentication scheme for converged VoIP networks," IACR Cryptol ePrint Arch, pp. 464, 2010.

[33] J.L. Tsai, "Efficient nonce-based authentication scheme for session initiation protocol," Int J Netw Secur, Vol. 9, No.1, pp. 12–16, 2009.

[34] E. Yoon, Y. Shin, I. Jeon and K. Yoo, "Robust mutual authentication with a key agreement scheme for the session initiation protocol," IETE Tech Rev, Vol. 27, No.3, pp. 203–213, 2010.

[35] Q. Xie, "A new authenticated key agreement for session initiation protocol," Int J Commun Syst, Vol. 25, No. 1, pp. 47–54, 2012.

[36] R. Arshad, N. Ikram, “Elliptic curve cryptography based mutual authentication scheme for session initation protocol,” Multimedia Tools Application, Vol. 66, No. 2, pp. 165–178, 2013.

[37] D. He, J. Chen and Y. Chen, “A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography,” Secur Commun Netw, Vol. 5, No. 12, pp. 1423–1429, 2012.

[38] L. Zhang, S. Tang and Z. Cai, “Efficient and flexible password authenticated key agreement for Voice over Internet Protocol Session Initiation Protocol using smart card,” Int J Commun Syst., Vol 27, No. 11, pp. 2691-2702, 2014.

[39] 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.

[40] X.M. Wang, W.F. Zhang, J.S. Zhang and M.K. Khan, “Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards,” Comput. Stand. Interfaces, Vol. 29, No. 5, pp. 507‑512, 2007.

[41] H. Chen, H.C. Hsiang and W. K. Shih, “Security enhancement on an improvement on two remote user authentication scheme using smart cards,” Futur. Gener. Comput, Vol. 27, No. 4, pp. 377-380, 2011.

[42] H.L. Yeh, T.H. Chen and W.K. Shih, “Robust smart card authentication scheme on SIP using elliptic curve cryptography,” Comp. stan. and interf, Vol. 36, No.2, pp. 397-402, 2014.

[43] “MAPS™ SIP Protocol Emulator Website,” 2014 [online]. Available: http://www.gl.com/sip-rtp-protocol-simulator-maps.html [Accessed June 2015].

[44] R. E. Shannon, "Introduction to the art and science of simulation," in 30th conference on winter simulation, IEEE Computer Society Press, 1989, pp. 7-14.

[45] M. Greis, "Ns Tutorial," [Online]. Available: www.isi.edu/nsnam/ns/tutorial/index.html. [Accessed January 2013].

[46] "OMNET++ Website," 2001, [online]. Available: https://omnetpp.org/ [Accessed June 2015].

[47] D. He, He, N. Kumar, M. Khan and J.H. Lee, "Anonymous two-factor authentication for consumer roaming service in global mobility networks." Consumer Electronics, IEEE Transactions on, Vol. 59, No.4, pp. 811-817, 2013

Publication

1. Rajni Bala, Neeraj Kumar, "An efficient session initiation protocol for secure communication in vehicular adhoc networks", Springer International Conference on Emerging Research in Computing, Information, Communication and Applications (ERCICA-15), Nitte Meenakshi Institute of Technology, Yelahanka, Banglore, India, 2015. **[Accepted and yet to Presented]**

Video Link

https://www.youtube.com/watch?v=ruxJURs17I8&feature=youtu.be

Plagiarism Report

Turnitin Originality Report

An Efficient Session Initiation Protocol for Secure Communication in Vehicular Ad-hoc Networks by Rajni Bala

From Thesis (ME 2013-2015 Batch)

Processed on 09-Jul-2015 01:06 IST
ID: 554687353
Word Count: 9812

Similarity Index	Similarity by Source	
7%	Internet Sources:	3%
	Publications:	7%
	Student Papers:	0%