IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Enhancing Efficiency of Prediction based Authentication for Vehicle to Vehicle Communication

Jayshri A. Marathe[1], Satpalsing D. Rajput[2]

M.E Student, Department of Computer Engineering, SSBT COET, Jalgaon, India[1]

Asst. Professor, Department of Computer Engineering, SSBT COET, Jalgaon, India[2]

Abstract: VANET uses vehicles as mobile nodes to create mobility in a network. A challenging problem is to design a broadcast authentication scheme for secure vehicle-to-vehicle communications. When an oversized variety of beacons arrive in a very short time, vehicles are at risk of computation-based Denial of Service attacks that excessive signature verification exhausts their procedure resources. An economical broadcast authentication scheme known as Prediction based Authentication (PBA) which not solely defend against computation-based DoS attacks, additionally resist packet losses caused by high quality of vehicles. In contrast to most existing authentication schemes, PBA is an efficient and lightweight scheme since it is primarily built on symmetric cryptography. Again to reduce the verification delay for some emergency applications, PBA is designed to exploit the sender vehicle's ability to predict future beacons earlier. Addition, to stop memory-based DoS attacks, PBA solely stores shortened re-keyed Message Authentication Codes (MACs) of signatures without decreasing security. An overview and qualitative comparison of PBA with authentication and without authentication is presented. Evaluation of the performance metrics such as Delivery Rate, Overall Storage Size, Loss Rate, Throughput and Control Overhead using NS-2 simulator are done.

Keywords: VANETs; broadcast communication; signatures; DoS attacks; prediction-based authentication.

I. INTRODUCTION

VANET are self-organizing networks built up from moving vehicles that communicate with each other to prevent contrary circumstances on the roads, and to achieve more efficient traffic management. VANET have recently attracted extensive attentions as a promising approach to enhancing road safety, as well as improving driving experience. The main objective of deploying VANET is to reduce the level of accidents. It has a great effect on passenger's safety and for drivers to drive smoothly in the urban area. As vehicles population increases day by day the rate of accidents also increases, therefore it is compulsory for the vehicles to communicate with each other.
VANETs is as an extension of mobile ad-hoc networks (MANETs) where there are not only mobile nodes, named On-Board Units (OBUs), but also static nodes, named Road Side Units (RSUs). As VANET is a sub category of MANET, it gives communication by redirecting datagram over multi hop wireless links. By using a Dedicated Short-Range Communications (DSRC) [1] technique, vehicles equipped with wireless On-Board Units (OBUs) can communicate with other vehicles and fixed infrastructure Road-Side Units (RSUs), located at critical points of the road [2]. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are considered as two basic types of communications in VANET.

Vehicle-to-Vehicle (V2V) Communication
Installing fixed infrastructure on roads causes huge expenses, so V2V communication will be required to extend the effective range of networked vehicles. V2V communication is the real ad hoc communication. This type of communication is mainly used in safety applications like safety warning, traffic information, road obstacle warning, intersection collision warning etc. Each vehicle is equipped with GPS (Global Positioning System), sensors, networking devices, digital map which has the road segment information, and computing devices. VANET is a self-organizing mobile ad hoc network in which to acquire the position information of neighboring nodes, each node periodically exchanges a list of all neighbors it can reach in one hop, using a HELLO control message or a beacon that contains its ID, location, speed, and a timestamp. Vehicles sense its own traffic messages and communicate with its neighbouring vehicles by broadcasting beacon or HELLO messages periodically. Figure 1 shows Element of Beacon Control Message. V2V communication uses both unicast and multi-cast packet forwarding techniques between source and destination vehicles. Unicast forwarding means that a vehicle can only send/receive packet to/from its direct neighbours. While multi-cast forwarding empowers the exchange of packet with remote vehicles using the intermediate

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

vehicles as relays. In V2V communication, both types of forwarding are used for different type of applications and protocols. Figure 2 shows vehicle to vehicle communication in VANET.

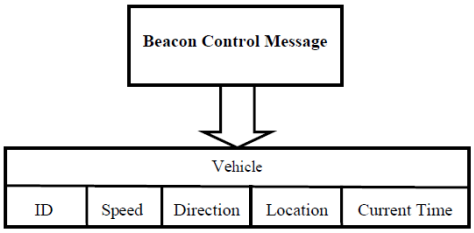

Fig.1. Major Element of Beacon Control Message

.

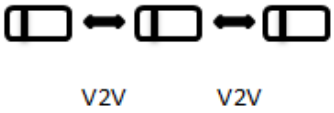

Fig.2. VANET: V2V Communications

V2V communication is organize by the vehicle producing its own network and provides information without assistance from the infrastructure. It is generally used to provide safety services including emergency information as well as anti-collision messages and alerts. Various requirements for security should be satisfied because V2V communication depends on information broadcast by internal network participants, and erroneous information could cause a fatal accident.

Once VANETs become available, numerous safe, commercial and convenient services can be deployed through a variety of vehicular applications. These applications mostly rely on vehicles OBUs to broadcast outgoing beacon messages and validate incoming ones. The broadcast beacons often contain information about position, current time, speed, direction, driving status, etc. For example, by frequently broadcasting and receiving beacons, drivers are better aware of obstacles and collision scenarios. They may act beforehand to avoid any possible damage, or to assign a new route if there is a traffic accident in the existing route. However, before implementing these attractive applications, particularly safety-related ones, first address and resolve VANET-related security issues [3], [4], [5].

To secure vehicular networks, an authentication scheme is necessary to ensure messages are sent by legitimate vehicles and not changed during transmissions. Otherwise, an attacker can easily disrupt the normal function of VANETs by injecting bogus messages. Therefore, vehicles should broadcast each message with a digital signature. However, the current VANET signature standard [6] using Elliptic Curve Digital Signature Algorithm (ECDSA) would cause high computational overhead on the standard OBU hardware, which has limited resources for cost constraints. Prior work has shown that one ECDSA signature verification requires 20 milliseconds on a typical OBU with a 400 MHz processor [7]. When a large number of signed messages are received in a short time period, an OBU cannot process them before their dedicated deadline. Attacks such as the computation-based DoS attacks can be easily initiated in a high density traffic scenario even without any malice. For example, when traffic related messages (beacons) are sent 10 times per second as suggested by the DSRC protocol [1], [6], a vehicle is overwhelmed with more than five neighbors within its radio range. To defend against such attacks, most existing schemes [8], [9], [10] make use of the technology of identity-based batch verification [11] or aggregate signature [12] built on asymmetric cryptography to improve the efficiency of verification. In identity-based batch verification, the computational cost is dominated by a few operations of pairing and a number of operations of point multiplication over the elliptic curve [13]. It is affordable for RSUs, but expensive for OBUs to verify the messages [14]. Again, if attackers inject false beacons, the receiver is hard to locate them so that these schemes are also vulnerable to the computation based DoS attacks [15]. Thus, giving an effective authentication scheme under high-density traffic scenarios is a big challenge for V2V communications.

Overview of VANET

The era of VANET is now evolving, gaining attention and momentum. Researchers and developers have built VANET simulation software to allow the study and evaluation of various routing, and emergency warning protocols. VANET simulation is different from MANETs simulation because in VANETs, vehicular environment imposes new issues and requirements, such as constrained road topology, multi-path fading and roadside obstacles, traffic flow models, trip models, varying vehicular speed and mobility, traffic lights, traffic congestion, drivers behavior, etc. Each vehicle in VANET is having a communication device installed in it for receiving and sending the messages over wireless VANET. Collision warning, Road congestion and in place traffic view will give the driver essential tool to decide the best path along the way.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Broadcast communications are critically important, as many safety-related applications rely on single-hop beacon messages broadcast to neighbor vehicles. Broadcast is done if there is requirement to transmit data to maximum nodes possible, which is the case when an accident or an event occurs. Broadcast uses concept of "Flooding" to a large degree which is supported by the large resources present on the nodes. Surveys have revealed that broadcast is more efficient when small numbers of nodes are involved. Figure 3. shows Broadcasting beacon messages.

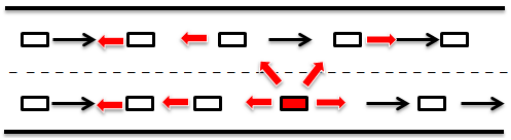

Fig. 3. Broadcast Beacon Message

VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network. VANET turns every participating vehicle into a wireless router or node, allowing vehicles approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As vehicles fall out of the signal range and drop out of the network, other vehicles can join in, connecting vehicles to one another so that a mobile Internet is created.
The primary goal of VANET is to provide road safety measures where information about vehicles current speed, location coordinates are passed with or without the deployment of Infrastructure. VANET also provides value added services like email, audio/video sharing etc,. VANET messages are divided into two types based on the distance that they are going to spread, which means these packets are either single-hop beacons or multi-hop traffic data.
For secure multi-hop traffic data, the standard ECDSA scheme [6] performs well when messages are sent infrequently. For efficient broadcast authentication, there are some works [8], [9], [10] using batch signature verification [11] or aggregate signature schemes [12] for V2I communications. An RSU will verify multiple received signatures at the same time such that the total verification time could be reduced. In RSU, the computational cost is mainly dominated by a few operations of pairing and a number of operations of point multiplication over the elliptic curve [13]. It is affordable for RSUs, but expensive for OBUs to verify the messages [14].
Furthermore, if attackers inject false beacons, it is so hard for the receiver to locate them that these schemes are also vulnerable to computation-based DoS attacks [15]. In addition, there are some works [16], [19] that rely on RSUs or other vehicles to achieve the authentication for vehicular communications. These schemes must assume the RSUs or vehicles as co-operators are trusted in VANETs. Moreover, the performance of authentication delay cannot be guaranteed for multiply transmissions, especially when the packet loss rate is high. For resource-limited environments, researchers have explored lightweight broadcast authentication schemes, such as TESLA-based authentication schemes [21], [22], [23], [25], [26].
Prediction-Based Authentication (PBA) is used to defend against computation-based DoS attacks for V2V communications. Unlike most of existing schemes based on asymmetric cryptography [8], [9], [10], [15], [16], [17], [18], [19], [20], PBA is primarily implemented on symmetric cryptography, whose verification is more than 22 times faster than ECDSA. In addition, PBA resists packet losses naturally. Similar to mobile wireless networks, packet losses are common in VANETs. PBA is designed on the TESLA scheme [21], [22], [23], which is proposed to secure lossy multicast streams with hash chains. With TESLA signatures piggyback, PBA operates smoothly even when the packet loss rate is high.
PBA also aims at improving the efficiency of authentication. Certain vehicular applications requires receiver to verify urgent messages immediately. To support instant verification, exploitation of the property of predictability of a future beacon, constructing a Merkle Hash Tree (MHT) [24] to generate a common public key or predication outcome for the beacon.

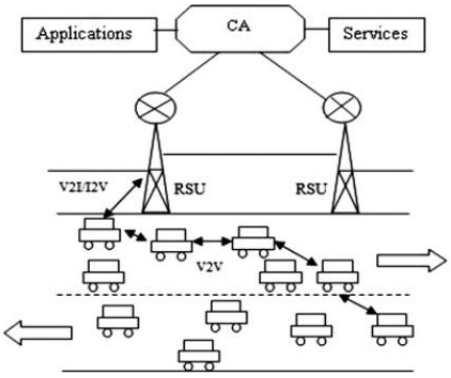

Fig. 4. VANET Architecture

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

With the prediction outcome known in advance, receivers can instantly verify the incoming beacon. If a mechanism brings a large storage burden, an attacker would initiate memory based DoS attacks where an OBU is overwhelmed by storing a large number of unverified signatures. To defend against such attacks, PBA records shortened re-keyed MACs instead of storing all the received signatures. Figure 4 shows VANET Architecture.

II. LITERATURE SURVEY

There is lots of research done on the Authentication, Security and Privacy in VANET. Many researches on Mobile Ad-Hoc Networks (MANETs) have been done where VANETs routing protocol has taken as a new protocol exist in the network. This protocol or system allows cars to talk to each other where a wireless device sends information to nearby vehicles. Wireless Ad Hoc Network (WANET) has many categories such as wireless mesh networks, wireless sensor networks and MANETs. VANETs is a subset of MANETs with a unique characteristic of dynamic nature or node mobility, frequent exchange information, real time processing, self-organizing, infrastructure less nature, low volatility and distance. It is considered the first commercial vehicles of MANETs. In VANETs, security and privacy are identified as major challenge.

J. H. Schiller in [27], Mobile ad hoc networks (MANETs) are a subclass of wireless ad hoc networks having special characteristics of dynamic network topology and moving nodes. Mobile ad hoc networks (MANETs) are infrastructure-less network of mobile devices connected wirelessly, self-configuring networks designed to support mobility. Each device changes its links to other devices frequently resulting in a highly dynamic and autonomous topology. Mobile ad hoc networks (MANETs) are a type of wireless networks that do not require any fixed infrastructure. MANETs are attractive for situations where communication is required but deploying a fixed infrastructure is impossible. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. Networks may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network.

In [1], VANET provide to manage the communication between the vehicles. Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication methods are supported under the VANET environment. In cryptography, a message authentication code (MAC) is a short piece of information used to authenticate a message i.e, to confirm that the message came from the stated sender (its authenticity) and has not been altered in transit (its integrity). On Board Unit (OBU) and Road Side Unit (RSU) are used to carry out the communication process. Vehicular Ad Hoc Networks (VANETs) are created by applying the principles of mobile ad hoc networks (MANETs) - the spontaneous creation of a wireless network for data exchange - to the domain of vehicles. They are a key component of intelligent transportation systems (ITS).

Studer et al., in [29], propose a key management scheme to satisfy the security and privacy requirements in VANETs. They use short-lived keys to sign messages to preserve the OBUs privacy, and revoke the certificate timely if the OBUs misbehavior is detected.

Hass et al., in [30], make use of Certificate Revocation Lists (CRLs) to distribute the revocation information in VANETs, which could help a receiver OBU check the revocation status of a sender. As the size of CRL is expected to be large, they use a Bloom filter [33] to store the certificate identifiers, which would take less memory and computational overhead to determine whether a certificate is on the CRL or not.

Wasef et al. in [31], employ a keyed MAC function to do fast checking process for the OBUs certificate, to reduce the authentication delay caused by checking the long CRL.

Sun. et al., in [17], propose a privacy preserving defense scheme by combining the mechanism of pseudonyms and the technology of identity-based threshold signature [34], to achieve the conflicting goals of privacy and traceability. To hide the identity of the signer, group signature-based schemes [35], [36] are made use of in [20], [28], [29]. However, these schemes would fail if a group manager who possesses the group master key arbitrarily reveals the group members identity. In addition, for V2V communications, the selection of group leader will sometimes become a bottleneck as OBUs could not find a trusted entity among vehicles. In [32], the authors introduce a random key-set based authentication protocol to preserve the vehicles privacy.

Stude et al., in [26], propose VAST to provide a wide range of possible authentication properties. Unfortunately, similar to the basic TESLA, VAST does not enable instant authentication. In safety-related applications, delayed verification is not favorable when the receiver wants to instantly verify the time-sensitive messages.

Hsiao et al., in [7], propose a one-time signature scheme named FastAuth to provide lightweight, timely and non-repudiation authentication for vehicle-to-vehicle communications. In FastAuth, they use chained Huffman hash trees to generate a common public key and minimize the signature size for beacons sent during one prediction interval.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

FastAuth first exploits the predictability of future beacons to achieve the instant authentication in VANETs. However, there is one drawback in FastAuth: once the receiver misses a beacon, it cannot work in the rest of the current prediction interval. To deal with packet losses, they add the schemes of Reed-Solomon (RS) Coding [37] and Public Key Rebinding. However, more communication overhead is required in wireless lossy environments, as well as the computational overhead. PBA scheme is motivated by FastAuth, but it belongs to TESLA-based authentication schemes. With TESLA signatures piggyback, PBA could resist packet losses naturally.

In [38], VANET have some important characteristics such as nodes forming the networks are vehicles, restricted vehicle movements on the road, high mobility of vehicles and rapid changes in topology and time-varying vehicle density. As the network topology in the VANETs is frequently changing, finding and maintaining routes is very challenging in VANET. To facilitate communication within a network, a routing protocol is used to find reliable and efficient routes between nodes so that message delivered between them in timely manner.

Jayakumar et al., in [38] in propose Topology based routing protocols depend on the information about existing links in the network and use them to perform packet forwarding. The topology based routing protocols can be further subdivided into proactive, reactive, and hybrid protocols.

Li. et al., in [39], and Qabajeh et al. in [40], position is one of the most important data for vehicles. In VANET each vehicle wishes to know its own position as well as its neighbor vehicles position. A routing protocol using position information in known as the position based routing protocol. Position based routing protocols need the information about the physical location of participating vehicles be available. This position can be obtained by periodically transmitted control messages or beacons to the direct neighbors. A sender can request the position of a receiver by means of a location service.

SH Kim et al., in [41], propose an efficient authentication scheme should guarantee timely message authenticity and non-repudiation. Meanwhile, it should resist packet losses and DoS attacks for relevant applications in VANETs. These properties are Timely authentication, Non-repudiation, Anonymity, Traceability, Unlinkability, Conditional Privacy, Packet losses resistant, DoS attacks resistant.

III.PROPOSED ALGORITHM

Prediction-based Authentication (PBA) scheme defend against computation-based DoS attacks which is an efficient broadcast authentication scheme, and prevent packet losses caused due to high mobility of vehicles. PBA uses symmetric cryptography which makes it an efficient lightweight scheme. The memory-based Denial of Service attacks are prevented using shortened re-keyed Message Authentication Codes of signatures.

Prediction Based Authentication System Module:

The following are the details in the sender side and receiver side details involved in the communication.

Sender

- Chained keys generation
- Position prediction
- Merkle hash tree construction
- Signature generation

Receiver

- Attack packet detection
- Signature Verification

Overview of Prediction Based Authentication Scheme

Prediction based authentication is used in the sender side to detect Denial-of-Service attacks before the signature verification. Enhanced attacked packet detection algorithm is used at the receiver side to detect malicious node. To reduce the verification delay, PBA is designed to exploit the sender vehicles ability to predict future beacons in advance. Applications rely on vehicles OBUs to broadcast outgoing beacon messages and to validate incoming ones. The broadcast beacons often contain information about position, current time, speed, direction, driving status, etc.

By frequently broadcasting and receiving beacons, drivers are better aware of obstacles and collision scenarios. They may act early to avoid any possible damage, or to assign a new route in case of a traffic accident in the existing route. PBA makes use of both ECDSA signatures and TESLA-based scheme to authenticate beacons. Similar to the TESLA scheme, PBA also requires loose time synchronization. In VANETs, it is naturally supported since messages sent by GPS-equipped vehicles are time stamped with nanosecond-level accuracy.

PROTOCOL OVERVIEW:

PBA includes the process of generating a signature by a sender and verifying the signature by a receiver. First, each vehicle splits its timeline into a sequence of time frames. Each time frame is also divided into a sequence of beacon

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

intervals, which we remark I_0; I_1; . . . ; I_n. In a time frame, to send the first beacon B_0 for I_0, a vehicle will perform four steps: chained keys generation, position prediction, Merkle hash tree construction, and signature generation.

A. Sender Side Process

- Chained Keys Generation:

At the beginning of a time frame, each vehicle generates n chained private keys for the next n beacons. It uses one interval worth of private key for authentication as the TESLA scheme. In the following description, we call these private keys TESLA keys.

- Position Prediction:

At each beacon interval, each vehicle predicts its position broadcast in the next beacon. To do so, vehicles model all the possible results of movements between two consecutive beacons based on information of the past trajectory. Figure 5 shows Movements of Vehicle and Table 1 shows Prediction Table.

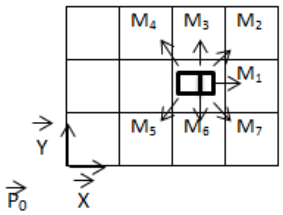

Fig. 5. Movements of Vehicle

TABLE I PREDICTION TABLE

Results	Movements
M_1	(1, 0)
M_2	(1, 1)
M_3	(0, 1)
M_4	(-1, 0)
M_5	(0, 0)
M_6	(0,-1)
M_7	(1,-1)

- Merkle Hash Tree Construction:

After position prediction, the vehicle will construct one interval worth of a public key and private keys. These private keys are associated with the results of movements. MHT structure is proposed to ties these pre-computed keys together and then generates a single public key or prediction outcome for all the possible movements. Figure 6 shows Merkle Hash Tree.

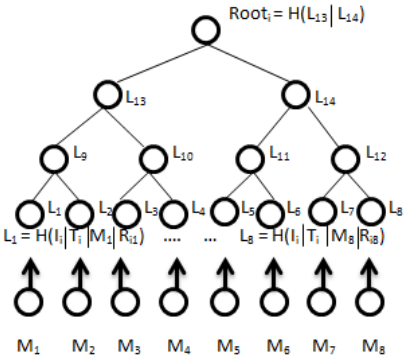

Fig. 6. Construct a Merkle hash tree

- Signature generation:

After position prediction and MHT construction, a vehicle signs the commitment of the hash chain and the prediction outcome from MHT using ECDSA signatures, and broadcasts it along with the first beacon B_0 in the time frame. For the rest of beacons such as B_1;B_2; . . .;B_n, the vehicle signs the message and the prediction outcome from MHT using the TESLA keys assigned in the intervals I_1; I_2;. . . ; I_n. It contains public keys, time stamp T_0, and other important parameters.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

B. Receiver Side Process

Attack packet detection:

It is based on the position changing requirements. Attacked packets are identified by the following parameters Frequency (f), Velocity (v), is Coefficient which is determined by the road characteristics and (VMax) is the maximum speed.

After receiving a beacon, a vehicle will perform the following two steps:

a) Selfgenerated MAC storage:

To reduce the storage cost of unverified signatures, the receiver only records a shortened re-keyed MAC. When the receiver keeps the used key secret, PBA provides security guarantees according to the size of beacon interval and network bandwidth.

b) Signature verification:

For the first beacon, the receiver veryfies the ECDSA signature. To verify the following signed Bi, the receiver will get the corresponding TESLA key, and reconstruct the prediction outcome from MHT. If a matching MAC of prediction outcome is found in the memory, the receiver authenticates the beacon instantly. Otherwise, the receiver authenticates it with the later TESLA key.

Figure 7 shows Flow Chart of PBA Architecture.

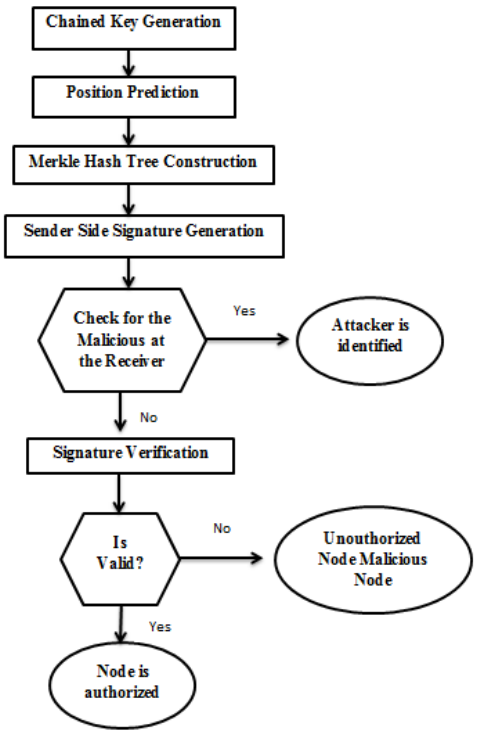

Fig. 7. Architecture of PBA

Algorithm 1: ALGORITHM WITH AUTHENTICATION

Step1: Before sending any beacon, a vehicle first generates n chained keys for signing and a commitment K_0 like the TESLA scheme.

Step2: For every two consecutive beacons, such as B_{i-1} and B_i, PBA requires the sender to model all the possible results of the distance vector differences or movements between them.

Step3: At each beacon interval, each vehicle predicts its position broadcast in the next beacon.

Step 4: Given the prediction table, the vehicle needs to generate a single public key (or prediction outcome) for all the possible movements.

Step 5: It first generates private keys, which are associated with the results of movements.

Step 6: After generating the commitment K_0, constructing the prediction table with a local coordinate, and producing the MHTs root $Root_1$ for the next beacon B_1, the sender broadcasts the first beacon in a time frame.

Step 7: For the first beacon B_0, ECDSA signature can provide the property of non-repudiation.

Step 8: Public key rebroadcasting. As K_0 is only sent at the beginning of a time frame, if a vehicle A encounters a vehicle C after C broadcasts its current K_0, A cannot verify Cs beacons until the next time frame.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Step 9: Similarly, m_2 also includes the random value and off-path nodes for I_2.
Step 10: To construct the signature of m_i, the sender first picks the TESLA key K_i for the interval I_i.
Step 11: Then, by performing the steps of position prediction and MHT construction, it obtains the root value $Root_{i+1}$ for I_{i+1}.
Step 12: Finally, the sender signs mi and $Root_{i+1}$ with K_{0i}.
Step 13: Reducing the communication overhead. As the random value and off-path nodes are contained in the message, the size of beacon is larger than before.
Step 14: To reduce the communication overhead, the number of off-path nodes with Huffman hash tree instead of Merkle hash tree could decrease.

Time Complexity of Algorithm 1 : n O(log n)

Algorithm 2: ALGORITHM WITHOUT AUTHENTICATION
Step 1: For every two consecutive beacons, such as B_{i-1} and B_i, PBA requires the sender to model all the possible results of the distance vector differences or movements between them.
Step 2: At each beacon interval, each vehicle predicts its position broadcast in the next beacon.
Step 3: After generating the commitment K_0, constructing the prediction table with a local coordinate, and producing the MHTs root $Root_1$ for the next beacon B_1, the sender broadcasts the first beacon in a time frame.
Step 4: Then, by performing the steps of position prediction and MHT construction, it obtains the root value $Root_{i+1}$ for I_{i+1}.
Step 5: Finally, the sender signs mi and $Root_{i+1}$ with K_{0i}.
Step 6: Reducing the communication overhead. As the random value and off-path nodes are contained in the message, the size of beacon is larger than before.
Step 7: To reduce the communication overhead, we could decrease the number of off-path nodes with Huffman hash tree instead of Merkle hash tree.
Time Complexity of Algorithm 2 : n O(n)

IV. RESULTS AND DISCUSSION

A. Implementation Details

PBA scheme is implemented using NS2. "NS2" stands for Network Simulator Version 2 is a widely used simulator for networking due to its nature of open-source simulation tool that runs on Linux, freely available, modifiable source code according to user needs. C++ is used as backend for data and Tcl is used as frontend for scripting. Developing each steps C++ classes and use a OTcl configuration interface to put together objects instantiated from these class. After simulation, NS2 outputs either text-based simulation results. To interpret these results graphically and interactively, tools such as NAM (Network AniMator) and XGraph are used. Network Simulator is programme using the C++ and provides a simulation interface through OTcl. It has an object-oriented dialect of Tcl (Tool Command Language). The user describes a network topology by writing OTcl scripts, and then the main Network Simulator program simulates that topology with specified parameters. Both algorithms are executed to get comparative output. Performance is evaluated in terms of time complexity to get results.

B. Datastructure

The PBA for vehicle to vehicle communication is implemented and run on NS2 Simulator. Steps like Chained Key Generation, Position Prediction, Merkle Hash Tree, Signature verification C++ _le is created and classes are declared and finally these classes are called in Tcl Script as the front end of simulation. Graphs are generated as output of the simulation.

C. Experimental Setup

Experimental setup is the part of research in which the experimenter analyzes the effect of contribution on existing system. Importance and unique aspect of setup used in experiments are introduced in experimental setup section.

D. Simulation Environments

Simulation environment introduces the necessary medium, virtual conditions, system softwares required to run experimental setup. Parameters are the various numerical or other measurable factor forming one of a set that defines a system or sets the conditions for operation. Necessary minimum hardware and software requirements to run the experimental setup is as follows:

- Operating System: LINUX, UBUNTU, WINDOWS
- RAM : 1 GB Minimum

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

- Hard Disk : 1 GB Minimum
- Processor : Intel Core 2 Duo (32 Bit)
- Front End Tool : Tcl
- Back End Tool : C++

E. Parameters

The parameters commonly used in VANETs are listed in Table II.

TABLE II PARAMETERS

Parameter	Value
ECDSA Signature Size	256 bits
Bandwidth of DSRC Channel	5 Mbps
Beacons Lifetime N	5(0.5 sec)
Packet Loss Rate p	0.3
Traffic Density	32 vehicles
Traffic type	CBR(Constant bit rate)
Simulator	NS 2.35

F. Performance Metrics

Performance Metric used in prediction is time complexity. Time complexity is calculated and compared for both algorithms below.

TABLE III TIME COMPLEXITY OF ALGORITHM 1

Algorithmic Steps	Execution Time
Generating n chained keys and commitment Ko	O(1)
Modelling all possible movements	O(1)
Prediction of position in next beacon	O(log n)
Generating public key	O(n)
Generating private key	O(1)
Constructing prediction table and producing MHT root	O(1)
ECDSA signature provides property of non-repudiations	O(1)
Public key rebroadcasting	O(n)
m2 and off-path nodes	O(n)
Constructing signature of mi	O(1)
Obtaining root value	O(n)
Sender signs miandRooti+1withK0	O(1)
Reducing communication overhead	O(1)

TABLE IV TIME COMPLEXITY OF ALGORITHM 2

Algorithmic Steps	Execution Time
Modelling all possible movements	O(1)
Prediction of position in next beacon	O(log n)
Constructing prediction table and producing MHT root	O(1)
Obtaining root value	O(n)
Sender signs miandRooti+1 withK0	O(1)
Reducing communication overhead	O(1)

Time Complexity of Algorithm 1 : n O(log n)
Time Complexity of Algorithm 2 : n O(n)

From above given Time complexities Algorithm 1 i.e, with authentication takes more time as compared to Algorithm 2 i.e, without authentication.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

G. Simulation Results

After analysis of PBA scheme, graph generated by various parameters applying authentication is generated and again generated same graph without application of authentication. Finally analysis of combined graph is shown below:

1. Delivery Rate: Number of Packets Sent by sender node Vs Number of Packets Received by receiver node.

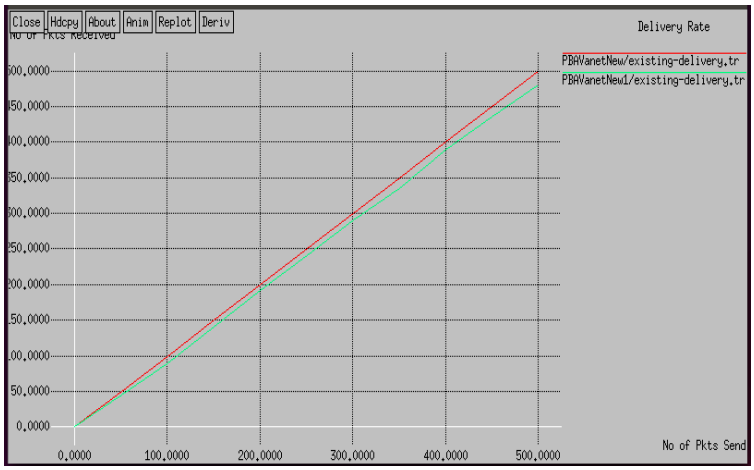

Fig.8. Number of Packets sent versus Number of Packets received.

Analysis: Loss rate would be more in non authentication system so number of packets sent and received would be different.

2. Time Frame Vs Sender Computation cost.

Sender's computation cost reduce with the increasing of time frame because hash and MAC operations, which are done much faster than the operations of ECDSA verification, have a high proportion in the overall computation, especially when the time frame is set to be a large value.

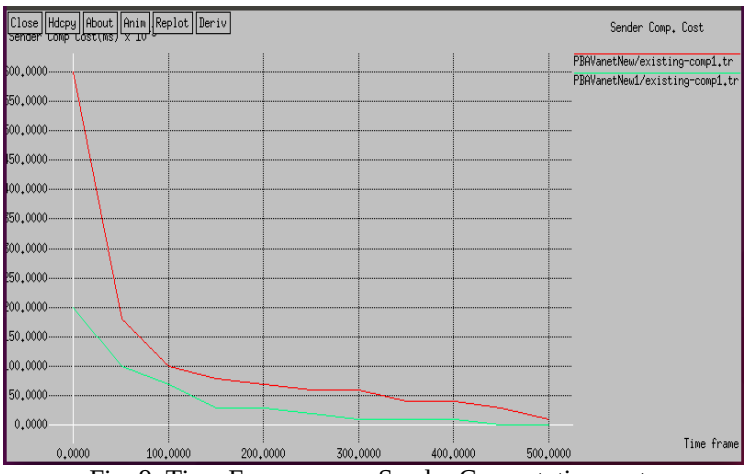

Fig. 9. Time Frame versus Sender Computation cost.

Analysis: Non authentication system, would not require to generate signatures and authenticate nodes, which will decrease overall computation cost.

3. Time Frame Vs Receiver Computation cost.

Receiver's computation cost reduce with the increasing of time frame because hash and MAC operations, which are done much faster than the operations of ECDSA verification, have a high proportion in the overall computation, especially when the time frame is set to be a large value.

Analysis: Non authentication system would require less cost as it does not have to calculate keys or verify signature of packets received.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

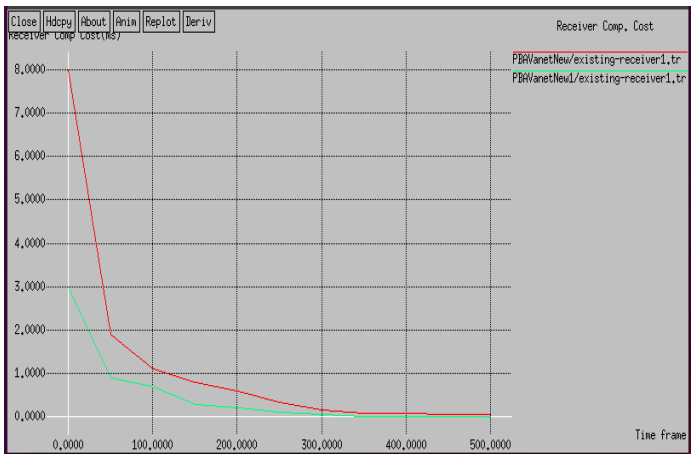

Fig. 10. Time Frame versus Receiver Computation cost.

4. Time Frame Vs Storage Size.

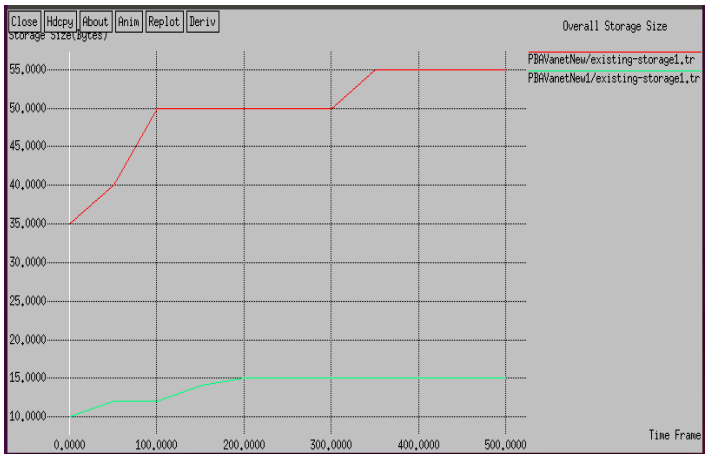

Fig.11. Time Frame versus Storage Size.

Analysis: Storage size would be decreased in non authenticated system as it no need to store keys and history.

5. Time Vs Number of Packet Lost.

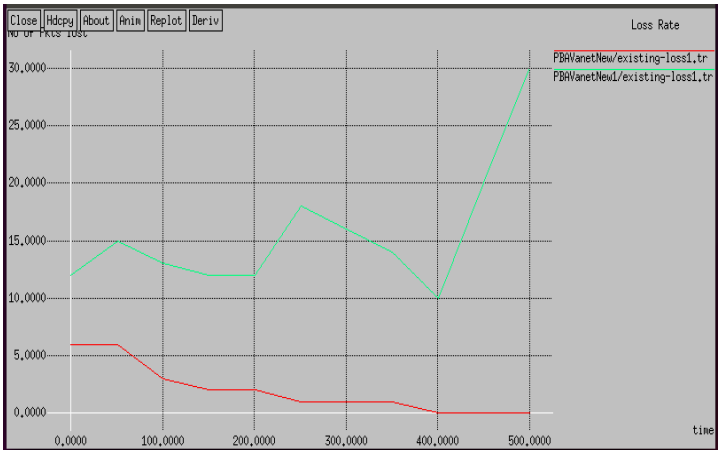

Fig. 12. Time versus Number of Packet Lost.

Analysis: Number of packets would be lost more in non-authentication system as the traffic data would affect routing and un authenticated nodes will have influence on network.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

6. Average number of On Board Unit Vs Overall delay.

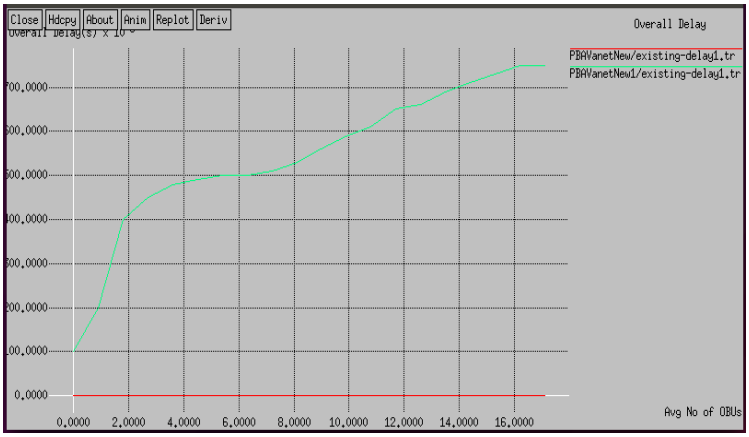

Fig. 13. Average number of OBU versus Overall Delay.

Analysis: Delay is more without authentication as time for rerouting of packets is more.

7. CBR Rate Vs Overall Delay.

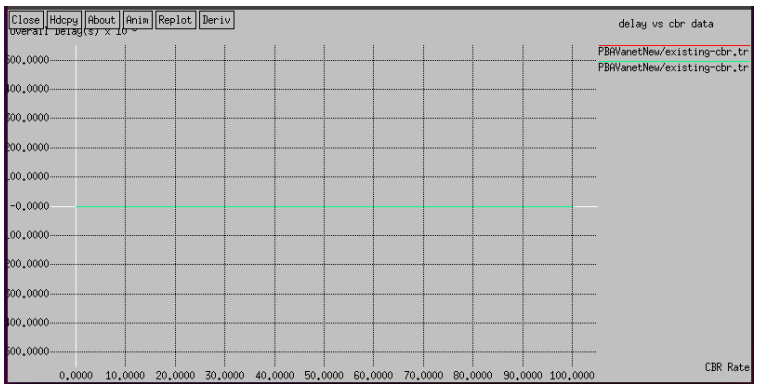

Fig.14. CBR Rate versus Overall Delay

Analysis: Packet dropping would be more due to CBR traffic for non authentication system. Which will eventually increase the delay of overall system.

8. Number of Nodes Vs Control Overhead.

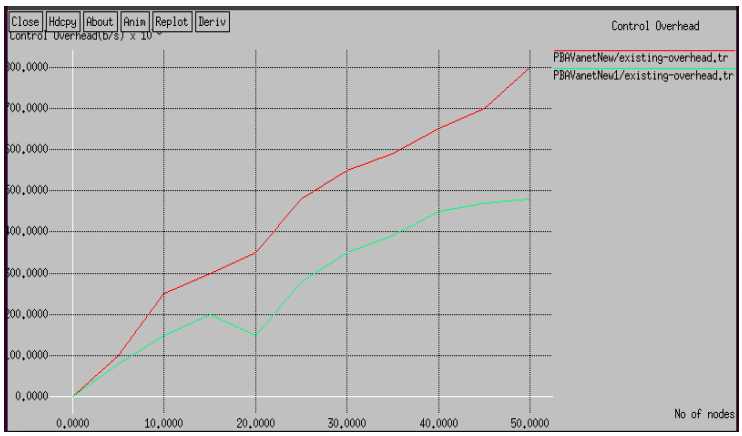

Fig. 15. Number of Nodes versus Control Overhead.

Analysis: Control overhead would be less as generation and verification of keys would not be required.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

9. Number of Nodes Vs Throughput.

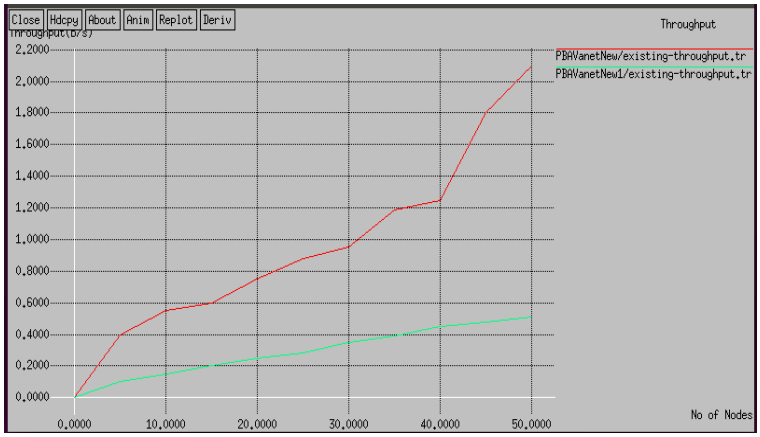

Fig. 16. Number of Nodes versus Throughput.

Analysis: Overall Throughput will be decreased for non authentication system. As delivery rate will be low and loss rate would be high.

H. Discussion

Results of experiment state that generated Algorithm for PBA with authentication and without authentication, Time Complexity of Algorithm 1 is more than Algorithm 2. As O(logn) is better than O(n), thus PBA with authentication is efficient and secure than that of without authentication, various graph are generated to show comparison between both Algorithms.

V. CONCLUSION

For V2V communications, an effective, efficient and scalable broadcast authentication scheme to provide both computation-based DoS attacks resilient and packet losses resilient in VANETs. Moreover, PBA has the advantage of fast verification by leveraging the predictability of beacons for single-hop relevant applications. After comparison between with and without authentication, with authentication is more efficient but takes more time as compared of without authentication. To defend against memory-based DoS attacks, PBA only keeps shortened MACs of signatures to reduce the storage overhead. By theoretical analysis, PBA is secure and robust in the context of VANETs. Through a range of evaluations, PBA has been demonstrated to perform well even under high-density traffic scenarios and lossy wireless scenarios.

In the future, same authentication mechanisms can be extended for other wireless ad-hoc network.

REFERENCES

[1] ASTM, "E2213-03,standard specification for telecommunications and information exchange between roadside and vehicle systems-5.9 ghz band dedicated short range communications (dsrc) medium access control (mac) and physical layer (phy) specifications," ASTM International, vol. 4, pp. 17-18, 2003.

[2] F. Bai, T. Elbatt, G. Hollan, H. Krishnan, and V. Sadekar, "Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective," in Proceedings of IEEE Workshop on Automotive Networking and Applications (AutoNet). San Francisco, CA, USA, 2006, pp. 1-25.

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

[4] S.-B. Lee, G. Pan, J.-S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," in Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing. ACM, 2007, pp. 150-159.

[5] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of computer security, vol. 15, no. 1, pp. 39-68, 2007.

[6] I. T. S. Committee et al., "IEEE standard for wireless access in vehicular environments- security services for applications and management messages," IEEE Std, pp. 1609-2, 2013.

[7] H.-C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "Flooding- resilient broadcast authentication for vanets," in Proceedings of the 17th annual international conference on Mobile computing and networking. ACM, 2011, pp. 193-204.

[8] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE, 2008, pp. 246-250.

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

[10] K.-A. Shim, "Reconstruction of a secure authentication scheme for vehicular ad hoc networks using a binary authentication tree," IEEE Transactions on Wireless Communications, vol. 12, no. 11, pp. 5386-5393, 2013.

[11] M. Bellare, J. A. Garay, and T. Rabin, "Fast batch verification for modular exponentiation and digital signatures," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1998, pp. 236-250.
[12] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in Eurocrypt, vol. 2656. Springer, 2003, pp. 416-432.
[13] D. Hankerson, J. L. Hernandez, and A. Menezes, "Software implementation of elliptic curve cryptography over binary fields," in International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2000, pp. 1-24.
[14] T. Unterluggauer and E. Wenger, "Efficient pairings and ecc for embedded systems," in International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2014, pp. 298-315.
[15] Y. Jiang, M. Shi, X. Shen, and C. Lin, "Bat: A robust signature scheme for vehicular networks using binary authentication tree," IEEE Transactions on Wireless Communications, vol. 8, no. 4, pp. 1974-1983, 2009.
[16] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 62, no. 7, pp. 3339-3348, 2013.
[17] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, 2010.
[18] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in vanets," IEEE Journal on selected areas in communications, vol. 29, no. 3, pp. 616-629, 2011.
[19] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 57, no. 6, pp. 3357-3368, 2008.
[20] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE, 2008, pp. 1229-1237.
[21] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The tesla broadcast authentication protocol," Rsa Cryptobytes, vol. 5, 2005.
[22] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast," in Network and Distributed System Security Symposium, NDSS, vol. 1, 2001, pp. 35-46.
[23] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 56-73.
[24] R. C. Merkle, R. Charles et al., "Secrecy, authentication, and public key systems," 1979. [25] C. Lyu, D. Gu, X. Zhang, S. Sun, and Y. Tang, "Efficient, fast and scalable authentication for vanets," in Wireless Communications and Networking Conference (WCNC), 2013 IEEE. IEEE, 2013, pp. 1768-1773.
[26] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient vanet authentication," Journal of Communications and Networks, vol. 11, no. 6, pp. 574-588, 2009.
[27] J. H. Schiller, Mobile communications. Pearson Education, 2003. [28] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks. ACM, 2007, pp. 19-28.
[29] A. Studer, E. Shi, F. Bai, and A. Perrig, "Tacking together efficient authentication, revocation, and privacy in vanets," in Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on. IEEE, 2009, pp. 1-9.
[30] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for vanet," in Proceedings of the sixth ACM international workshop on Vehicular InterNETworking. ACM, 2009, pp. 89-98.
[31] A. Wasef and X. Shen, "Emap: Expedite message authentication protocol for vehicular ad hoc networks," IEEE Transactions on Mobile Computing, vol. 12, no. 1, pp. 78-89, 2013.
[32] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing privacy using symmetric random key-set in vehicular networks," in Autonomous Decentralized Systems, 2007. ISADS'07. Eighth International Symposium on. IEEE, 2007, pp. 344-351.
[33] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," Communications of the ACM, vol. 13, no. 7, pp. 422-426, 1970.
[34] J. Baek and Y. Zheng, "Identity-based threshold signature scheme from the bilinear pairings," in Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on, vol. 1. IEEE, 2004, pp. 124-128.
[35] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Crypto, vol. 3152. Springer, 2004, pp. 41-55.
[36] D. Chaum and E. Van Heyst, "Group signatures," in Advances in CryptologyEUROCRYPT91. Springer, 1991, pp. 257-265.
[37] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," Journal of the society for industrial and applied mathematics, vol. 8, no. 2, pp. 300-304, 1960.
[38] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocols-a review," Journal of Computer science, vol. 3, no. 8, pp. 574-582, 2007.
[39] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," IEEE Vehicular technology magazine, vol. 2, no. 2, 2007.
[40] L. K. Qabajeh, M. M. Kiah, and M. Qabajeh, "A qualitative comparison of position based routing protocols for ad-hoc networks," International Journal of Computer Science and Network, vol. 9, no. 2, pp. 131-140, 2009.
[41] S.-H. Kim and I.-Y. Lee, "A secure and efficient vehicle-to-vehicle communication scheme using bloom filter in vanets," International Journal of Security and Its Applications, vol. 8, no. 2, pp. 9-24, 2014.

BIOGRAPHY

Jayshri A. Marathe is a M.E Student in Computer Engineering Department, SSBT COET Bambhori Jalgaon, North Maharashtra University. I received B.E in 2012 from SSBT COET Bambhori, Jalgaon, India. Mine research interests are Computer Networks (wireless Networks), Fuzzy Logic, Agile Methodology, etc.