Rising Issues in VANET Communication and Security: A State of Art Survey

Sachin P. Godse
Research Scholar: Department of Computer Engineering
Smt. Kashibai Navale College of Engineering, SPPU, Pune, India

Parikshit N. Mahalle
Professor: Department of Computer Engineering
Smt. Kashibai Navale College of Engineering, SPPU, Pune,India

Sanjeev J. Wagh
Professor: Department of Information Technology
Government College of Engineering Karad

***Abstract*—VANET (Vehicular Adhoc Network) has made an evolution in the transportation hi-tech system in most of the developed countries. VANET plays an important role in an intelligent transportation system (ITS). This paper gives an overall survey on the research in VANET security and communication. It also gives parameters considered by the previous researchers. After the survey, it considered the authentication and message forwarding issues required more research. Authentication is first line of security in VANET; it avoids attacks made by the malicious nodes. Previous research has come up with some Cryptographic, Trust based, Id based, and Group signature based authentication schemes. Speed of authentication and privacy preservation are the important parameters in VANET authentication. This paper presented the AECC (Adaptive Elliptic Curve Cryptography), and EECC (Enhanced Elliptic Curve Cryptography) schemes to improve the speed and security of authentication. In AECC, the key size is adaptive, i.e. different sizes of keys are generated during the key generation phase. Three ranges are specified for key sizes: small, large, and medium. In EECC, added an extra parameter during the transmission of information from, the vehicle to the RSU for key generation. This additional parameter gives the information about the vehicle ID, and the location of the vehicle to the RSU and the other vehicle. Under the communication issue of VANET, the paper gives priority based message forwarding for improving the message forwarding scheme. It handles emergency situations more effectively.**

***Keywords*—Vehicular Adhoc Network (VANET); Adaptive Elliptic Curve Cryptography (AECC); Enhanced Elliptic Curve Cryptography (EECC); authentication; message forwarding**

I. INTRODUCTION

The VANET becomes a milestone in an intelligent transportation system. It helps to automate the traffic monitoring system more efficiently. In VANETs nodes, there is nothing, but vehicles and the RSU (Road Side Unit), which communicate with each other. RSU's are deployed on the roads, and help to maintain the communication when the vehicles are not in the coverage of each other. There are different issues in VANET. Due to an open medium of VANET, the outside nodes can easily, access the network. Security is a major challenge in VANET. Malicious nodes can carry different attacks to misguide the driver. Communication is the heart of all networks; in VANET, the nodes are moving fast so, there is the need of a faster and smart communication mechanism, to handle emergency situations [11]. In this paper, Section 1 gives an introduction of VANET, communication. Section 2 gives a detailed literature survey of the authentication and communication issues in VANET. Section 3 gives an analysis about the research parameter considered by the previous researchers, and the area for new research. Section 4 gives the objectives and solutions for the same.

A. VANET Architecture

The VANET architecture is shown in Fig. 1. It shows the scenario of the vehicular adhoc network, and the different ways of communication in VANET. There are three ways of communication, namely, V2V (Vehicle to Vehicle), V2I (Vehicle to Infrastructure), and I2V (Infrastructure to Vehicle) [1].

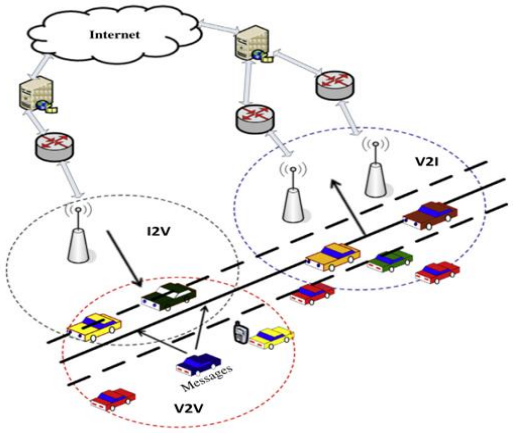

Fig. 1. VANET architecture [1].

B. Communication in VANET

1) **Wireless Access in Vehicular Environment (WAVE)**: Lots of efforts have been made to design the new standards for the services and the interfaces for VANET. These standards form the basis for a wide range of applications in the vehicular network environments. A set of standardized services and interfaces defined under WAVE is shown in Fig. 2. These services and interfaces cooperatively enable a secure V2V and V2R communications in a rapidly changing communications environment where communications and transactions need to be completed in a short time frame.

The WAVE architecture is developed, based on the IEEE 802.11p and the IEEE P1609 standards (Nadeem, 2004). The IEEE 802.11p deals with the physical and Media Access Control layers, whereas the IEEE 1609 deals with the higher-layer protocols [3].

2) **WAVE Architecture:**

The IEEE 1609 family of standards for WAVE:

The IEEE has defined four standards, and released them for trial use (IEEE, 2007). Fig. 2 shows the architecture of the WAVE family, of standards. These standards can be defined as follows [3]:

IEEE 1609.1(Resource Manager):

This standard defines the services, and the interfaces of the WAVE Resource Manager applications. It describes the message formats and the response to those messages. It also describes the data storage format that is used by the applications to access other architecture.

IEEE 1609.2 (Security Services):

This standard defines security and secure message formatting, and processing. It also, defines how secure messages are exchanged.

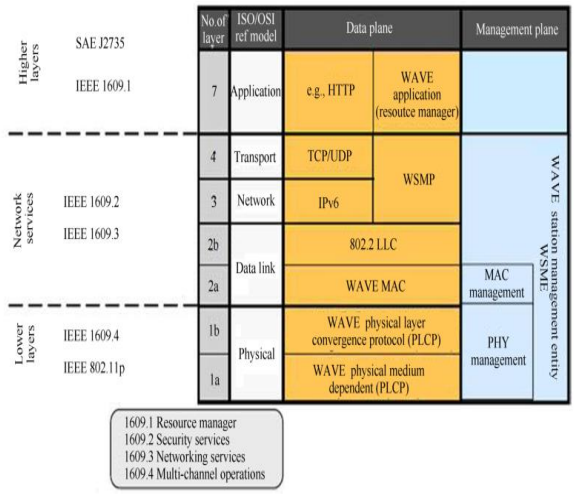

Fig. 2. WAVE architecture (showing protocol stack) [18].

IEEE 1609.3 (Networking Services):

This standard defines the routing and transport layer services. It also defines a WAVE-specific message alternative to IPv6 that can be supported by the applications. This standard also defines, the Management Information Base (MIB) for the protocol stack.

IEEE 1609.4 (Multi-Channel Operations):

Multi-Channel Operations: This standard defines, the specifications of the multi-channel in the DSRC. This is an enhancement to the IEEE 802.11a Media Access Control (MAC) standard.

II. Literature Survey on Authentication & Communication in VANET

VANET can be affected by many attacks like denial of service, message suppression, and the propagation of false message attacks etc. In order to increase safety, in data transmission, security, is the most important challenge in VANET [2], [17]. The Literature survey shows some requirement to achieve security, Leinmuller Schoch et al. (2007), timely delivery, location accuracy, correctness of message privacy and liability, as security requirements. Razzaque M. et al. (2013) stated that the security model in VANET should satisfy the authentication, verification of data consistency, message integrity, availability, non-repudiation, privacy and traceability, revocation and real-time constraints as a security requirement [16]. Ahmad Yusri Dak et al. (2012) stated that availability, Authentication, Integrity, Confidentiality, and non-repudiation are security requirements.

Table 1 shows the detailed survey of the research in VANET along with its strength, weakness, and future scope of the research. For survey purpose paper from communication and security in VANET are considered. Studied papers are from 2004 to 2016.

Table 2 shows the parameters considered by a previous researcher. After study of each paper, which parameters are consider by researcher is identified. Using identified parameters value, pie chart is drawn. Fig. 3 shows Pie chart. Pie chart gives details about which parameter how much percentage of work is already done. It gives area from VANET research which required more research focus.

TABLE I. Survey on Security and Communication in VANET

Reference	Scheme	Strength	Weakness	Future Scope
[19] 2016	A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET	1. No need of storage for Storing a large pool of pseudonyms. 2. Not using a Certificate Revocation List (CRL) 3. Valuable information is secured as compared to a server.	**1.** If CA, RA, or RSU compromise, the scheme can fail.	1. Authentication process speed can improve. 2. Trust value of CA, RA and RSU can be used to find a compromise node.
[20] 2016	Security Enhancement in Group Based Authentication for VANET	1. Group based V2V communication framework is proposed to secure VANET and preserve privacy. 2. This scheme eliminates the need to sign message in V2V communication, which leads to faster authentication.	1. Digital signature generation and verification of a message in V2V communication requires more time, which degrades the performance of the network.	1. Can improve the digital signature generation process. 2. Can use cluster based group formation to improve the process of authentication.
[21] 2016	Vehicular Authentication Security Scheme (VASS)	1. The computation effort is much lower than the other methods in hash function 2. VASS has the properties of security such	1. Vehicle to infrastructure communication not considered.	1. Vehicle to Infrastructure authentication can be provided.

		as privacy, authentication, and Sybil attack.		
[22] 2016	Secure and distributed certification system architecture for safety message authentication in VANET	1. Resists against false public-key certification. 2. Provide secure and distributed certification system 3. Each RCA delegates subordinates RSUs for the Certificate management and hence increasing its availability for the vehicles.	1. The Storage required more as each vehicle maintains a long-term private-key, a long-term public-key, an implicit certificate, a short-term key pair and a public-key certificate delivered by the RCA. 2. High transmission range required to transmit various safety messages.	1. Can reduce the key sizes and subsequently, speed of authentication**.**
[23] 2016	A Secure and Efficient V2V Authentication Method in Heavy Traffic Environment	1. Accelerates message processing by sending a low data volume for communication in areas of heavy traffic. 2.Blocks replay attacks by checking time stamps	1. Vehicle to infrastructure communication not considered.	1. Vehicle to Infrastructure authentication can be provided.
[4] 2014	A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles	1. Cooperative watchdog model where evidences are aggregated and a cooperative decision is made. 2. Incentives are given in the form of reputation to motivate vehicles to behave cooperatively. 3. Two phase model.	1. No priority given to messages. 2. No security for data, which may be accessed by an in between node.	1. Priority based packet handling. 2.Detection model.
[5] 2013	A Hybrid Bio-inspired Bee swarm Routing protocol for safety applications in Vehicular Ad hoc Networks (VANETs)	1. Uses multiple paths simultaneously, between the source and the destination to send packets in order to reduce the transmission time. 2. HyBR guarantees data transmissions in real time to help drivers make safe decisions and to improve road safety 3. Works with VANET high density and VANET low density	1. Density prediction mechanism is not provided.	1. Density prediction and according to that , switching of algorithm (high/low).
[6] 2014	An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks	1. Advanced secure scheme based on Clustering and Key Distribution (SCKD) among members and cluster-heads in VANET. 2. Secure end-to-end communication scheme deploys the proxy signature, blind proxy signature, hashed message authentication code, and symmetric cryptography	1. Required more memory to store keys, certificates etc. 2. Large traffic overhead 3. If CA fails, the entire network will fail.	1. On road storage terminals are installed to store every vehicle secure data. 2. CA replica, which works when primary CA fails.
[7] 2014	Collaborative trust aware intelligent intrusion detection in VANETs	1. Trust aware Collaborative Learning Automata based Intrusion Detection System.	1. Required automation zone setup 2. Attack detection states should be added in database 3. GPSR/Internet needed for every vehicle 4. Every vehicle has to send its data separately.	1. Provide smart storage terminal on road side. 2. Machine learning based attack detection methodology. 3. Packet aggregation and forwarding.
[8] 2014	Learning Automata-based Opportunistic Data Aggregation and Forwarding scheme for alert generation in Vehicular Ad Hoc Networks	1. Learning Automata-based Opportunistic Data Aggregation and Forwarding (LAODAF). 2. LA predicts the mobility of the vehicle and adaptively, selects the path for forwarding, 3. RSUs to collect and forward the data from respective regions	1. Large set of Road Side Units required 2. Message flooding attack 3. Large memory storage required at Road Side units	1. Send large packet with slow vehicle and small packet with fast vehicle. 2. Delete data after efficient Interval
[9] 2009	Secure V2V Communication With Certificate Revocations	1.Tries to address the problem of access to revocation information using a concept called freshness that does not require the PKI to distribute the CRLs and the OBUs to maintain the CRLs. 2.Reduces the storage requirement at the OBU and provides a constant time algorithm that is independent of the number of certificates revoked, to verify a signed message.	1. If the certificate of the CA is compromised then freshness checks shall not work 2. The CoS decreases as the rate of revocation increase.	1. Private and Public key is generated by an individual node, and just gets verified by a trusted server. 2. Dynamic freshness check threshold
[10] 2013	A Categorized Trust-Based Message Reporting Scheme for VANETs	1. A categorized decentralized trust management and evaluation scheme for nodes in VANETs 2. Role-based trust and experience-based trust is integrated, while using an opinion piggybacking process when needed.	1. It only considers current message details not history 2. Piggybacking not authenticated	1. Authenticate Piggybacking node. 2. Maintain piggyback, messages and nodes history, and used for penalty or trust building 3. Dedicated task to RSU.

		3. Determine the degree of trustworthiness of a node's.		
[12] 2014	A social network approach to trust management in VANETs	1. A novel voting scheme. 2. Each vehicle has different voting weight according to its distance from the event. 3. The vehicle, which is closer to the event, possesses higher weight.	1. Time is an issue in waiting for packet accessing or decision taking. 2. Piggybacking delay or forgery source	1. Authenticate source of piggybacking 2. Performance algorithm to select time delay for packet accessing or decision taking.
[14] 2004	On Secure and Privacy-Aware Sybil Attack Detection in Vehicular Communications	1. To cope with Sybil attack twofold strategy is used. 2. Pseudonym less beaconing in order to preserve privacy.	1. RSU overhead 2. Road network density not considered 3. More n/w traffic	1. Classify network traffic in low and high density. 2. Use piggyback packet to reduce beacons.

TABLE II. PARAMETERS IN THE PREVIOUS RESEARCH

Reference	PARAMETERS							
	Throughput	**Delay**	**Network overhead**	**Efficient event handling**	**Packet Delivery Ratio**	**Secure messaging**	**Node security**	**Trusted system**
[19] Ubaidullah Rajput et al. 2016	----	**Yes**	**Yes**	----	**Yes**	----	**Yes**	----
[20] Rajkumar Waghmode et al. 2016	----	**Yes**	**Yes**	----	----	**Yes**	**Yes**	----
[21] Yongchan Kim et al. 2016	----	**Yes**	**Yes**	----	----	**Yes**	**Yes**	----
[22] Tiziri Oulhaci et al. 2016	**Yes**	----	----	**Yes**	----	**Yes**	**Yes**	----
[23] Myoung-Seok et al. 2016	----	----	----	**Yes**	----	**Yes**	**Yes**	----
[4] Omar Abdel et al. 2014	**Yes**	**Yes**	----	----	**Yes**	----	**Yes**	**Yes**
[5] Salim Bitam et al. 2013	**Yes**	**Yes**	**Yes**	----	**Yes**	----	----	**Yes**
[6] Ameneh Daeinabi et al. 2014	----	**Yes**	----	----	----	**Yes**	**Yes**	**Yes**
[7] Neeraj Kumar et al. 2014	----	----	**Yes**	----	**Yes**	----	**Yes**	**Yes**
[8] Neeraj Kumar et al. 2014	**Yes**	**Yes**	**Yes**	----	**Yes**	----	----	----
[9] Ashwin Rao et al. 2007	----	----	**Yes**	----	----	----	**Yes**	**Yes**
[10] Merrihan Monir et al. 2013	**Yes**	----	----	**Yes**	----	**Yes**	**Yes**	**Yes**
[12] Zhen Huang et al. 2014	**Yes**	----	----	**Yes**	----	----	**Yes**	**Yes**
[14] Rasheed Hussain et al. 2014	**Yes**	----	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	----

Yes: parameter Considered for research ----: Parameter not considered for research

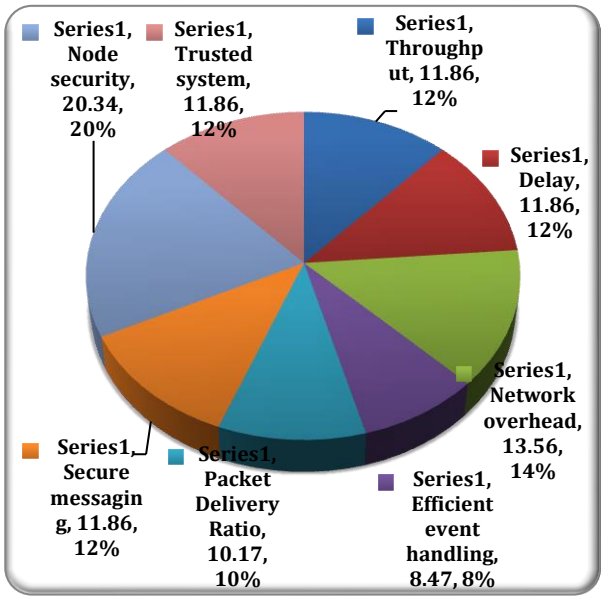

Fig. 3. Previous research work on different parameters.

Fig. 3 shows that there is a need of more research in secure message forwarding, emergency event handling and packet delivery ratio. Secure message forwarding and efficient event handling can be the objectives of future work. Considering this need priority based message forwarding for emergency event handling is the objective set for research. Secondly, as VANET, is a dynamic network, density and speed of the vehicle is another issue to increase the overhead. As authentication is the start of any secure communication if speed of authentication is improving, it can help to give time for RSU to serve more number of vehicles. The Packet delivery ratio can improve by attack detection and improving speed while communication. Considering this need faster and secure authentication objective is set for research.

III. OBJECTIVES AND PROPOSED SOLUTIONS FOR THE SAME

A. Objectives:

1) To provide faster authentication in VANET.

2) To provide a secure and priority based message forwarding system.

B. Proposed Framework

Fig. 4 shows framework which is designed for research work. It gives direction for research to achieve set objectives. As per framework first task is setting topology of VANET for experimentation; secondly, authentication of vehicle. In authentication first task is to implement basic ECC algorithm for authentication then variation in ECC by AECC and EECC algorithms is achieved. Third task gives malicious node detection while authentication and last task will be priority based message forwarding.

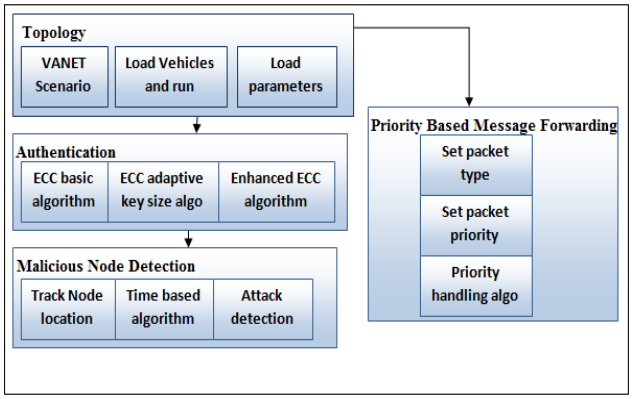

Fig. 4. Framework for the proposed work.

Detailed description of each framework blocks is given below.

A. Topology

It shows the front end of the project where the vehicle scenario is created using VSIM (VANET Simulator) tools. VSIM is used for objective implementation and testing. VSIM is a java based simulator, which provides different classes to create an environment for VANET. Protocols and ideas can implement in a simulator using JAVA. Different maps are available to test protocols; the map can upload in the simulator. Different road scenarios are available for each map; we can upload those scenarios in a simulator after uploading the map. The simulator has different input parameters like number of vehicles, time stamp of each vehicle, road traffic density, event priority, time slot, etc. that can provide to the simulator.

B. Authentication

The authentication scheme is implemented in three different ways- ECC based authentication, Adaptive ECC based authentication, and Enhanced ECC based authentication. Table 3 shows the terms used for Adaptive ECC, and the Enhanced ECC algorithm for authentication.

a) ECC Based Authentication: authentication using elliptic curve cryptography.

1) Elliptic curve cryptographic algorithm:

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography.

Fig. 5 shows simple Elliptic Curve which considered for ECC algorithm.

TABLE III. TERMS USED FOR ALGORITHM

Terms /Notations	Meaning
P	Key pool
Ts	Time slot.(Re-generate keys after every Ts seconds)
G	Key Generator
m,a,b	Unique parameters
K	Keys
Pu	Public key
Pr	Private key
Vc	Current vehicles
NR	Neighbor RSU
Ks	Key size
Kx	New Key
Us	Public key server
Re	Verify – Sybil attack, replica attack

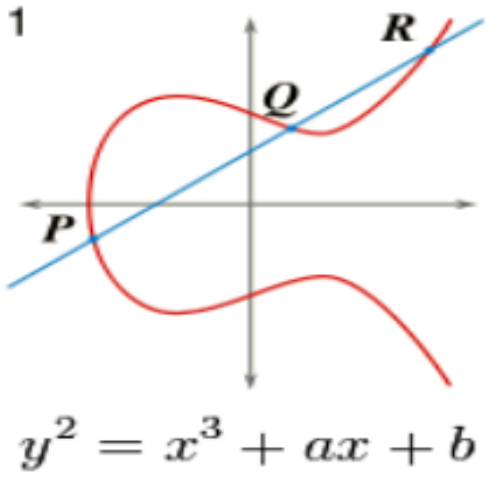

Fig. 5. Simple elliptic curve.

The equation of an elliptic curve is given as,

y2 = x3 + ax + b [15]

Few terms that will be used,

E -> Elliptic Curve

P -> Point on the curve

n -> Maximum limit (This should be a prime number)

2) Key generation

Key generation is an important part where need to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. Now, number 'd' selected within the range of 'n'. Using the following equation Public key will be generated.

Q = d * P

Where,

d = the random number that have been selected within the range of (1 to n-1).

P = the point on the curve.

'Q' is the public key and 'd' is the private key.

3) Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 – (n-1)]. Two cipher texts will be generated.

Let it be C1 and C2.

C1 = k*P

C2 = M + k*Q

C1 and C2 will be sent.

4) Decryption

We have to get back the message 'm' that was send to us.

M = C2 – d * C1

M is the original message that we have send.

b) AECC (Adaptive Elliptic Curve Cryptography) based authentication: The ECC algorithm for authentication in VANET, can fail, if the user side password is cracked by an attacker using a permutation and combination of alphabets. So, the password is a main flaw in this. This problem can be overcome by, either adding some parameter along with the password for key generation, or using an adaptive key size algorithm. This algorithm uses the random key size where no attacker can guess, the key size at the current time, and tries to break it. This system uses a cooperative system to decide the key size after every defined timeslot. When an attacker tries to guess the key to break the system as the ECC is strong enough this does not happen easily. But when an attacker succeeds to do so, because of the adaptive key size (AKS) algorithm, the key is no longer relevant to that attacker.

Algorithm / Pseudo code for AECC based authentication:

Input:

G, {Ts}, {Ks, P}, {V}

Output:

Random_Keys, Access Granted/Rejected

Algorithm:

1. Sync {V,RSU,S} -> Ts-Time Slot
2. Server Generated TimeSlots {Ts} & KeySizePool {Ks,P}
3. Generate ECC initial parameters G,PW
4. SessionKeyDistribution {Rc, Rs}
    a. Generate Random variable rA
    b. Compute Ra & Wa
    c. Get Ks -> {KsP}
    d. Generate K -> Ks size Client Side
    e. Generate K -> Ks at Server Side
5. Session Key verify – H{K}
    a. Generate Hash{P}
    b. Verify
6. Session Granted/Rejected

End

c) EECC (Enhanced Elliptic Curve Cryptography) based authentication: In the Enhanced ECC algorithm, we added an extra parameter during the transmission of information from the vehicle to the RSU for key generation. This additional parameter gives the information about the vehicle ID, and the location of the vehicle to the RSU, and the other vehicle. This additional parameter is also used in key generation. This algorithm provides replica and Sybil attack detection along with authentication.

Algorithm / Pseudo code for EECC Based Authentication:

Input:

G, {V}, {Ts}, {Ks, P}

Output:

Detect Attack, Access Granted/Rejected

Algorithm:

1. Generate ECC initial parameters G,PW
2. SessionKeyDistribution {Rc, Rs}
    a. Generate Random variable rA
    b. Compute Ra & Wa
    c. Get Ks -> {KsP}
    d. {ID, K,L,TS} -> RSU
    e. Verify V by RSU
    f. If Verifed
        i. Generate K -> Ks size Client Side
        ii. Generate K -> Ks at Server Side
    g. End IF
    h. Else
    i. Start Re_verify
        1. Vehicle shares new {id, TS, L}
        2. Verify by RSU and Server
    ii. End
    i. End Else
3. Session Key verify – H{K}
    a. Generate Hash{P}
    b. Verify
4. Session Granted/Rejected

End

C. Malicious Node Detection

1) Track node location: Algorithm for tracking the location of vehicles from which a message is received or which it is trying to communicate.

2) Time based algorithm: Assigning time stamp to the message.

3) Attack detection: Using node location and time stamp information Sybil and replica attack detection will be achieve.

D. Priority based Message Forwarding

In VANET, different types of messages are used-depending on the type of information in the messages, e.g.

1) Safety messages like tunnel ahead, speed limit, diversion, speed breaker, etc. [13].

2) Alert messages, like accident ahead, weather condition, congestion, etc.

3) User comfort messages, like navigation info, social networking info, video/audio data, etc.

Different types of messages have got different priorities based on their criticality. There is a need of message forwarding on the basis of priority of messages. The lower priority message should be denied by, a vehicle if any, higher priority message arrives. Here, message is classified into three different classes: emergency vehicle, accident, road block and traffic jam.

Priority, parameter and priority based message forwarding algorithm:

Priority based Message Forwarding:

Priority:

1. 0 – Emergency vehicle
2. 1 – Accident, road block
3. 2 – Traffic jam

Parameter:

1. Event Generator
2. Destination x, y
3. Distance
4. Speed

Algorithm:

1. Push – Source Vehicle node
    a. Generate packet with priority
    b. Forward message to nearest RSU/Vehicle
    c. If Destination is in vehicles range
        i. Broadcast it
        ii. End
    d. Else
        i. RSU
            1. Verify Message
            2. Store packet in database for time Threshold t
            3. Scheduling algorithm
2. Pull
    a. Step 1
        i. Pull Priority-0,1,2 messages
        ii. Sort by ascending by distance (Less Distance First-LDF)
            1. Broadcast message one by one
3. Schedule–Vehicle and RSU
    a. If current time < t
        i. Pull Algo
    b. Else
        i. Remove packet from Database
4. Forwarding– Vehicle
    a. Pull Algorithm
5. Verify message
    a. Verify location
    b. Authenticate packet
    c. If Not verified
        i. Drop packet

IV. Conclusions

VANET is an upcoming area of research as it provides an Intelligent Transportation System. Under ITS the user gets different services that come under two categories safety/security and user comfort. Security and message forwarding are the major challenges in VANET.

As the nodes in VANET are moving faster the network is highly unstable. There is the need of a faster authentication mechanism, which makes the RSU more efficient to serve more number of vehicles. This paper proposed a time efficient and an attack resistant protocol based on ECC, which reduced the time required for authentication as the key size is smaller in ECC, as compared to the other cryptographic technique. Framework is designed for research work, which shows the techniques needed to achieve the objectives.

Priority based message forwarding algorithm used to handle prioritized messages. This helps to improve critical information sharing in VANET.

References

[1] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, Alejandro Quintero, “VANET security surveys”, In: ELSEVIER Computer Communications 44, PP 1-s13 , 2014.

[2] V.S. Yadav, S. Misra, M. Afaque, “Security of Wireless and Self-Organizing Networks: Security in Vehicular Ad Hoc Networks”, . In: CRC Press, pp. 227–25, 2010.

[3] A jafari, S.AI Khyatti, A. Dogman, “performance evaluation of ieee 802.11p for vehicular communication networks”. In: IEEE Conference CSNDSP-2012.

[4] Omar Abdel Wahab, Hadi Otrok, Azzam Mourad, "A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles”. In: ELSEVIER Computer Communications 41 ,PP 43–54, 2014.

[5] Salim Bitam, Abdelhamid Mellouk, Sherali Zeadally, “A Hybrid Bio-inspired Bee swarm Routing protocol for safety applications in Vehicular Ad hoc Networks (VANETs)”. In: ELSEVIER Journal of Systems Architecture 59 ,PP 953–967, 2013.

[6] Ameneh Daeinabi, Akbar Ghaffarpour Rahbar, “An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks”,. In: ELSEVIER Computers and Electrical Engineering 40 ,PP 517–529, 2014.

[7] Neeraj Kumar, Naveen Chilamkurti, “Collaborative trust aware intelligent intrusion detection in VANETs”,. In: ELSEVIER Computers and Electrical Engineering ,2014.

[8] Neeraj Kumar, Naveen Chilamkurti, Joel J.P.C. Rodrigues, “Learning Automata-based Opportunistic Data Aggregation and Forwarding scheme for alert generation in Vehicular Ad Hoc Networks”,. In: ELSEVIER Computer Communications 39 ,PP 22–32, 2014.

[9] Ashwin Rao, Ashish Sangwan et. al “ Secure V2V Communication with Certificate Revocations”. In: IEEE ,2007.

[10] Merrihan Monir, Ayman Abdel-Hamid, Mohammed Abd El Aziz, “A Categorized Trust-Based Message Reporting Scheme for VANETs.”, In: Springer CCIS 381, PP. 65–83, 2013.

[11] Chin-Ling Chen, Ing-Chau Chang et al, “A Secure Ambulance Communication Protocol for VANET”,. In: Springer Wireless Pers Commun, 73 PP. 1187–1213, 2013.

[12] Zhen Huang, Sushmita Ruj et al. “A social network approach to trust management in VANETs”, In: Springer Peer-to-Peer Netw. Appl. 7 PP. 229–242, 2014.

[13] Jyoti Grover,Vijay Laxmi,Manoj Singh Gaur, “Attack models and infrastructure supported detection mechanisms for position forging attacks in vehicular adhoc networks”,. In: Springer CSIT 1(3), PP. 261–279, September 2013.

[14] Rasheed Hussain, Heekuck Oh, "On Secure and Privacy-Aware Sybil Attack Detectionin Vehicular Communications",. In: Springer Wireless Pers Commun, 2014.

[15] Kristin Lauter, "The Advantages of elliptic Curve Cryptography For Wireless Security", In: IEEE Wireless Communications 2004.

[16] Shidrokh Goudarzi, Abdul Hanan Abdullah, "A Systematic Review of Security in Vehicular Ad Hoc Network", In: the 2nd Symposium on Wireless Sensors and Cellular Networks (WSCN'13) 2013.

[17] M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", In: IEEE Wireless Communications, Vol 13, October 2006.

[18] Elias C. Eze, Si-Jing Zhang, En-Jie Liu, Joy C. Eze "Advances in vehicular ad-hoc networks (VANETs) : Challenges and road-map for future development", International Journal of Automation and Computing, 13(1), PP 1-18, February 2016..

[19] Ubaidullah Rajput, Fizza Abbas, Heekuck Oh, "A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET",.In: IEEE Access, October 25, 2016.

[20] Rajkumar Waghmode, Rupali Gonsalves, Dayanand Ambawade, "Security Enhancement in Group Based Authentication for VANET",. In: IEEE International Conference on Recent Trends in Electronics Information Communication Technology, May 20-21, 2016.

[21] Yongchan Kim, Jongkun Lee, "A secure analysis of vehicular authentication security scheme of RSUs in VANET". In: Springer-Verlag France, 2016.

[22] Tiziri Oulhaci, Mawloud Omar, Fatiha Harzine, Ines Harfi, "Secure and distributed certification system architecture for safety message authentication in VANET". In: Springer Science+Business Media New York, 2016

[23] Myoung-Seok Han,Sang Jun Lee,Woo-Sik Bae, "A Secure and Efficient V2V Authentication Method in Heavy Traffic Environment.", In: Springer Science+Business Media New York, 2016.