A SURVEY ON ENHANSING SECURITY BETWEEN V2V, V2I, V2R USING CRYPTOSYSTEM IN VANET

Dhara M. Patel[1], Ujas S. Patel[2]

[1]*Student (Master of engineering), Computer Engineering Department, L.C. Institute of Technology, Mehsana, Gujarat, India*
[2]*Assistant Professor, Computer Engineering Department, L.C. Institute of Technology, Mehsana, Gujarat, India*

ABSTRACT

Recent advances in wireless communication technologies and auto-mobile industry have triggered a significant research interest in the field of VANETs over the past few years. VANET consists of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications supported by wireless access technologies such as IEEE 802.11p.VANET developed an advanced traffic signaling system for message transmission.so when data transmission from source to destination node various attack and introduces in system and reduce PDR, Information Loss. In these paper we will work on The suggested cryptosystem like RSA and ECC using proposed scheme increase efficiency, latency , Packet Delivery ratio, Authentication and security between communication node.

Keywords : - *VANET, RSA, Authentication, ECC, V2V, V2I, V2R, IEEE802.11p*

1. INTRODUCTION

Federal Communication Commission (FCC) allocated a frequency spectrum for wireless communication vehicle-vehicle as well as vehicle-roadside. In 2003, Dedicated Short Range Communications (DSRC) Service is established by FCC [16]. DSRC is a communication service that uses the 5.850-5.925 GHz frequency band for the use of public safety as well as private application. Newly developed services and the allocated frequency enable vehicles and roadside units to form Vehicular Ad Hoc Networks (VANETs), in which the nodes can communicate wirelessly with each other without central access point VANETs share some same characteristics with Mobile Ad Hoc Network (MANET). Both VANET and MANET are characterized by the self-organization of the nodes and movement, but they are different in some ways. The unreliable channel conditions and high nodes mobility VANETs to have many challenging research issues, such as data sharing, data dissemination, and security issues[12].

The promises of wireless communications to support vehicular applications supported by wireless communications have led to us several research projects around world. FCC allocated DSRC to “increase traveller safety, reduce fuel consumption and pollution, and continue to advance the nation's economy”. National Highway Traffic Safety Administration (NHTSA) created the Vehicle Safety Communication Consortium (VSCC) to promote V2V networking for safety. There are several projects focusing to develop intelligent vehicles based on DSRC. The Car 2 Car Communications Consortium developed the C2C-CC project in Europe. The Internet ITS (Intelligent Transportation Systems) Consortium in Japan is one of the samples of VANETs projects[11].

1.1 Security Requirements for VANET[7]

Authentication: An authentication framework is necessary to identified and ensure that the participants are whom they claim to be to operate securely in VANETs. Means it is required for sender's messages that response in case of acknowledgement would be sent to legitimate sender.

Integrity: Integrity is required between two communicating nodes to protect data accuracy which is main security issue desirable in VANETs.

Confidentiality: The challenge to protect data content from the adversaries is confidentiality. Message security must be achieved through encryption schemas and similar encoding techniques to make it unreadable to the attackers.

Non-Repudiation: Non-Repudiation refers to somebody who possesses the private key corresponding to the signing certificate with reasonable certainty but if the key is not properly safeguarded by original owner, a major concern can be digital forgery.

Pseudonymity: Pseudonymity is the state of describing a disguised identity. A holder that is one or more human beings are identified but don't disclose their true names.

Privacy: The protection of personal information of drivers within the network from other nodes but extracted by authorities in case of accidents is a major privacy issue which is desirable for VANETs.

Scalability: The ability of a network to handle growing amount of work in a capable manner securely is Scalability, which is the main challenge in VANETs.

Consistency: In addition to authentication, consistency of the data must be required for the latest data. It should happen that the sender is authenticated but the data to be sent is false.

Availability of Data: Data from servers should available each and every time of client request. It is necessary to have alternatives of even strong communication channels in case of Denial of Service (Dos) attacks.

Mobility: The nodes communicating in VANETs constantly change their locations with different directions and speeds making the network dynamic in nature. So, in order to make communication successful, it is challenging to establish security protocols.

Key-Management: The key is used to encrypt and decrypt information during communication process. When designing security protocols for networks like VANET, the issue of key management must be resolved.

Location Verification: This is necessary to prevent many attacks and is helpful in data validation process. Thus to improve the Security of VANETs, a solid method is required.

1.2 Elliptic Curve Cryptographic Algorithm

Elliptic Curve Cryptography (ECC) is an alternative mechanism for implementing public-key cryptography.
The equation of an elliptic curve is given as,

$$\mathbf{Y^2 = x^3 + ax + b}$$

Where:
a and b are elements of a finite field with p n elements, where p is a prime number which is selected as larger than 3.The set of points on the curve is the collection of ordered pairs (x, y) with coordinates in the field and such that x and y satisfy the relation given by the equation $y^2 = x^3 + ax + b$ defining the curve, plus an extra point that is said to be at infinity.

- **Key Generation**

Key generation is an important part, where user has to generate public key and private key. The senders who want to send the message, he will first encrypt the message with receiver's public key and the receiver will decrypt that cipher text with its private key. Now, we have to select a number 'd' within the range of 'n'. Using the following equation we can generate the public key

$$\mathbf{Q = d*P}$$

d = The random number that we have selected within the range of (1 to n-1).
P is the point on the curve. 'Q' is the public key and 'd' is the private key.

- **Encryption**

Let 'm' be the message that we are sending. We have to represent this message on the curve.
Consider the message 'm' has the point 'M' on the curve E. Now, randomly select value of 'k' from [1 – (n-1)]. Two cipher texts will be generated let it be C1 and C2.

$$\mathbf{C1 = k*P}$$
$$\mathbf{C2 = M + k*Q}$$

Cipher text C1 and C2 will be send to the other user.

- **Decryption**

Here, in this decryption process receiver will decrypt the cipher text message with its own private key to get original message.

$$\mathbf{M = C2 – d * C1}$$

1.3 RSA Algorithm

RSA is a block cipher in which the plaintext and cipher text are integers between 0 and n- 1 for some n .Encryption and decryption are of the following form, for some plaintext block M and cipher text block C:

$$C = M^e \bmod n$$

$$M = C^d \bmod n = M^{e^{(d)}} \bmod n = M^{ed} \bmod n$$

Both sender and receiver must know the values of n and e, and only the receiver knows the value of d. This is a public key encryption algorithm with a public key of KU = {e,n} and a private key of KR = {d,n}.For this algorithm to be satisfactory for public-key encryption, the following requirements must be met:

1. It is possible to find values of e, d, n such that M^{ed} = M mod n for all M<n.

2. It is relatively easy to calculate M^e and C^d for all values of M <n.

- **Key Generation Algorithm**

1. Generate two large random primes, p and q, of approximately equal size such that their product n = pq is of required bit length, e.g. 1024 bits.
2. Compute n = pq and (φ) phi = (p-1) (q-1)
3. Choose an integer e, 1 < e < phi, such that gcd (e, phi) = 1.

4. Compute the secret exponent d, $1 < d < phi$, such that $e\ d \equiv 1 \pmod{phi}$.
5. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.
n is known as the modulus.
e is known as the public exponent or encryption exponent or just the exponent.
d is known as the secret exponent or decryption exponent.

- **Encryption Algorithm:**

Sender A does the following:-
1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer m
3. Computes the cipher text $c = m^e \bmod n$.
4. Sends the cipher text c to B.

- **Decryption Algorithm:**

Recipient B does the following:-
1. Uses his private key (n, d) to compute $m = c^d \bmod n$.
2. Extracts the plaintext from the message representative m.

2. LITERATURE REVIEW

2.1 MAvanet: Message Authentication in VANET using Social Networks.

In [6] this paper the authors have proposed an algorithm in which social networks are used to create an active topology from all possible users in sender's profile, who are active at a particular point of time. Message authentication is provided to user with QR (Quick Response) code. The system has an issue of time complexity and the authors concentrated on extracting topology using primary connection.

2.2 TDMAC: A Timestamp Defined Message Authentication Code for Secure Data Dissemination in VANET

In [11] this paper a light weight security solution for secure data dissemination among vehicles in VANET known as timestamp defined MAC(TDMAC) . The performance results of TDMAC are qualitatively and quantitatively efficient than existing MACs.

2.3 Security Enhancement in Group Based Authentication for VANET.

In [3] this paper authors have proposed a security schema and all the security tools like authentication, integrity, anonymity, Non-repudiation are satisfied by using the AES and ECDSA algorithm. The performance results of this algorithm are satisfied most of the security requirements but by using this the time is more required and all the process can be depends on group leader. Here GL is selected by the trusted authority.

2.4 Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks.

In [10] this paper proxy based authentication scheme (PBAS) to reduce the computational overhead of road side units (RSUs) using distributed computing. Proxy vehicles are used to authenticate multiple messages with a verification function at the same time. RSU is able to verify the outputs from the verification functions of the proxy vehicles.

2.5 RSU authentication by aggregation in VANET using an interaction zone.

In [1] this paper authors have proposed a security schema to firstly ensure identification for RSU by an Elliptic Curve Diffie-Hellman (ECDH) algorithm where the vehicle confirms that the two neighbours RSU have the same shared secret, then secondly the vehicle authenticates the message beforehand signing, using Elliptic Curve Digital Signature Algorithm (ECDSA).

3. COMPARATIVE TABLE

Table -1: Comparative Table

Sr .No.	Paper Title	Method	Advantage	Disadvantage
1	MAvanet:Message Authentication in VANET using Social Networks[6]	QR Code	Authentication is done.	Complex system, Time Consuming and Only for V2I communication for Limited active user
2	Security Enhancement in Group Based Authentication for VANET[3]	AES, ECDSA	Authentication, Integrity, Non-repudiation, Anonymity this all security property are satisfied.	Time consuming and depends on the group leader.
3	TDMAC: A Timestamp Defined Message Authentication Code for Secure Data Dissemination in VANET[11]	Timestamp, MAC	High Transmission Range	Message transmission rate, Message Drop with respect to simulation time
4	Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks[10]	PBAS	High Security, Estimate average message delay and loss ratio in real environment	Time consuming
5	RSU authentication by aggregation in VANET using an interaction zone[1]	ECDSA	High security	Authentication is time consuming

4. CONCLUSIONS

We have many research and survey paper different type of algorithm for VANET security come to know which are dynamic and dedicated to merge them to get better efficiency then perform individually using ECC and RSA algorithm and also analysis on performance parameter like PDR (packet delivery ratio), E2E(end-to-end delay) and latency. By use of ECC and RSA algorithm we can enhancing security between V2V, V2I, V2R with improve the latency and packet delivery ration also.

5. REFERENCES

[1] A.Bendouma and B.A. Bensaber, " RSU authentication by aggregation in VANET using an interaction zone" *2017 IEEE International Conference on Communications (ICC)*, Paris, 2017,pp.1-6.doi: 10.1109/ICC.2017.7997017

[2] Prof. G.A.Jagnade and Prof. S.I.Saudagar Prof. S.A.Chorey, " Secure VANET from vampire attack using LEACH protocol " 2016 IEEE International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016

[3] R. Waghmode, R. Gonsalves and D. Ambawade, "Security enhancement in group based authentication for VANET," 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2016, pp. 1436-1441. doi: 10.1109/RTEICT.2016.7808069

[4] P.A.Sumayya and P.S.Shefeena, " VANET Based Vehicle Tracking Module for Safe and Efficient Road Transportation System " 2014 sciencedirect International Conference on Information and Communication Technologies(ICICT 2014)

[5] Nicholas S. Samaras, " Using Basic MANET Routing Algorithms for Data Dissemination in Vehicular Ad Hoc Networks (VANETs) " 2016 IEEE Telecommunications forum (TELEFOR 2016)

[6] Anirudh Paranjothi, M.S.Khan, Mais Nijim, Rajab Challoo "Mavanet: Message Authentication in VANET using Social Networks " 2016 IEEE

[7] Vijay Kumar Tripathi and Dr. S.Venkaeswari "Secure Communication with Privacy Preservation in VANET-Using Multilingual Translation " 2015 IEEE Global Conference on Communication Technologies(GCCT 2015)
[8] Mrs. S.A.Abbad and Mr. S.P. Godse " Priority based emergency message forwarding scheme for time critical maodels in VANET " 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT)
[9] Tanjida Kabir , Novia Nurain and Md. Humayun Kabir " Pro-AODV(Proactive AODV): Simple Modifications to AODV for Proactively Minimizing Congestion in VANETs" 2015 IEEE
[10] Yiliang Liu,Liangmin Wang "Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks" 2014 IEEE
[11] Atanu Mondal and Sulata Mitra " TDMAC: A Timestamp Defined Message Authentication Code for Secure Data Dissemination in VANET " 2016 IEEE Advanced Networks and Telecommunications System (ANTS 2016)
[12] Yue Liu, J. Bi and Ju Yang, "Research on Vehicular Ad Hoc Networks," 2009 Chinese Control and Decision Conference, Guilin, 2009, pp. 4430-4435. doi: 10.1109/CCDC.2009.5192343
[13] Anand bihade, roshani talmale," Detection and Avoidance of road traffic congestion using VANET", Proceedings of IRAJ International Conference, 21st July 2013, Pune, India, ISBN.
[14] W. Liu, X. Wang, W. Zhang, L. Yang and C. Peng, "Coordinative simulation with SUMO and NS3 for Vehicular Ad Hoc Networks," 2016 22nd Asia-Pacific Conference on Communications (APCC), Yogyakarta, 2016, pp. 337-341. doi: 10.1109/APCC.2016.7581471
[15] Martins, David, And Herve Guyennet. "Wireless Sensor Network Attacks And SecurityMechanisms: A Short Survey", 2010 13th International Conference On Network-Based Information Systems, 2010.
[16] Hoang Lan Nguyen, Uyen Trang Nguyen," A Study Of Different Types Of Attacks In Mobile Ad Hoc Networks", Department Of Computer Science And Engineering, 2012, IEEE.
[17] http://learning.maxtech4u.com/vehicular-ad-hoc-network-vanet/
[18] http://ijarcsse.com/Before_August_2017/docs/papers/Volume_7/7_July2017/V7I7-0159.pdf
[19] https://www.researchgate.net/figure/280958696_fig1_Figure-1-VANET-Architecture
[20] https://www.cse.wustl.edu/~jain/cse571-14/ftp/vanet_security/index.html
[21] https://www.urbanafrica.net/news/huge-express-highway-planned-connect-nigerian-cities/
[22] http://shodhganga.inflibnet.ac.in/bitstream/10603/68269/7/07_chapter%201.pdf
[23] http://www.ijcte.org/papers/590-K172.pdf