International Journal of Engineering & Technology, 7 (3.8) (2018) 125-130

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Review on Security Based Vehicular Ad-Hoc Network

Sonika[1], Sandeep Kumar Arora[2*], Mahedi Masud[3]

[1]*Lovely Professional University*
[2]*Lovely Professional University*
[3]*Taif University, Saudi Arabia*
**Corresponding author E-mail:sandeep.16930@lpu.co.in*

Abstract

VANET a vehicular ad-hoc network provides the security to vehicles. To provide security in VANET, we are using Elliptical curve cryptography. In this paper we are going to discuss various techniques of cryptography, the techniques such are Advanced Encryption Standard, Data Encryption Standard, and Triple Data Encryption Standard. These techniques are part of symmetric and asymmetric cryptography. In addition to this there are some attacks which we are discussing in this paper like, masquerade attack, replay attack, insider attack, mutual authentication attack, and parallel session attack. These attacks are on different layer. At the end we are comparing these attacks with each other and compare their quality of services.

Keywords: *Elliptical Curve Cryptography; DES; AES; TDES; Security*

1. Introduction

A VANET is a security related network which provide a secure relation between vehicular. In this vehicular ad hoc network information is distributed among the vehicles with very high speed [1]. Engineers proposed VANET is as a trust based technology for intelligent transport system that is ITS. VANET (Vehicular ad-hoc network) shows some challenges of Mobile ad-hoc network that authorize cars to sharply communicate with other and with roadside infrastructure [2]. Mobile ad-hoc networks has some limitations like involving packets being dropped, packet delivery delay, mobility, security and waste bandwidth. Some engineers said that VANET is an advance version of MANET [2]. In which, communication has been done in between vehicle to vehicle (V to V), Inter roadside communication, vehicle to roadside unit (V to RSU), in a range of 100 to 300 m. VANET are dynamic in nature and its topology is change very rapid and often. In which, every node can flow freely in the community and each node can communicate with another node. The purpose of the VANET is to provide comfort to passengers and it is also used for existence saving of passengers. Every car or node communicates with other cars or nodes with multi hop or single hop [3]. VANET is secure as we all know so is provide some security related applications like traffic control and road security, toll collision, guidance information of tourist and natural calamities [4]. Yes of course, Vehicular ad-hoc carry many application with it but also there are some challenges, the main challenge is lies in securing the communication between cars. With important contributions of various engineers in securing vehicular network, authentication plays a vital role [4]. Some technologies like Bluetooth, ZigBee, Wi-Fi, Wi-max, 3G/4G-LTE (long term evolution) and 5G are present inside or outside of the vehicles [5]. Standard had been given by IEEE 802.11 that is stand on MAC (Medium access control), WAVE, IEEE1609.x, ISO CALM [5].

1.1 Characteristics of VANET

1.1.1 High Mobility

The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy. Thus, they remain inside each different communiqué variety for a very quick time, and hyperlinks are established and broken rapid which results to fast adjustments in network topology. Moreover, driving force conduct is tormented.By the necessity to react to the facts obtained from the network, which reasons modifications in the network topology. The speedy adjustments in community topology affect the community diameter to be small, even as many paths can be disconnected earlier than they may be used

.

1.1.2 Network Topology

The nodes can be changes their position or place with the help of high node mobility and random speed of vehicles.

1.1.3 Unbounded Network Size

VANET is not a bounded area it can be implemented for small area like a city or town; it also can be implemented of many cities and can be implementing in a country. Frequent exchange of information: The vehicular ad hoc network (VANET) in springing the nodes or cars to take messages from the different cars or vehicles and road side units.

1.1.4 Wireless Communication

VANET is designed for the wireless environment. Nodes are connected and exchange their information via wireless personal unique traits while compared with different kinds of MANETs, the

specific traits of VANET include. VANET is designed for the wireless surroundings. Nodes are related and trade their records via wireless. Therefore a few security degrees have to be taken into consideration in verbal exchange.

1.1.5 Predictable Mobility

Unlike MANETs, the network nodes (here motors) of VANET flow in a predefined way because roads format are fixed and motors should obey and comply with street signs, site visitors' indicators, in addition to reply to different moving vehicles The prediction of automobile position and their actions may be very tough. This feature of mobility modeling and prediction in VANET is based at the availability of predefined roadmaps models. The velocity of the vehicles is once more an essential for green community design automobiles, the position of node changes regularly.

1.1.6 High Computational Capacity

As vehicles are nodes in VANET, they can keep a sufficient number of sensors and enough conversation equipment inclusive of excessive pace processors, massive reminiscence size, superior antenna generation and present day GPS. These sources boom the computational strength of the node, which assist to create dependable Wi-Fi communiqué and to acquire accurate facts of node's modern function, velocity and route.

1.2 Architecture of VANET

This part depicts the framework engineering of vehicular specially appointed systems. VANET engineering can be partitioned into various structures in view of alternate point of view. VANET are utilized for communication between vehicles for the diverse sort of use, for example, street safety, stimulation, movement control, and so on. VANET give data auspicious to drivers and obliged specialists to give safety to clients.

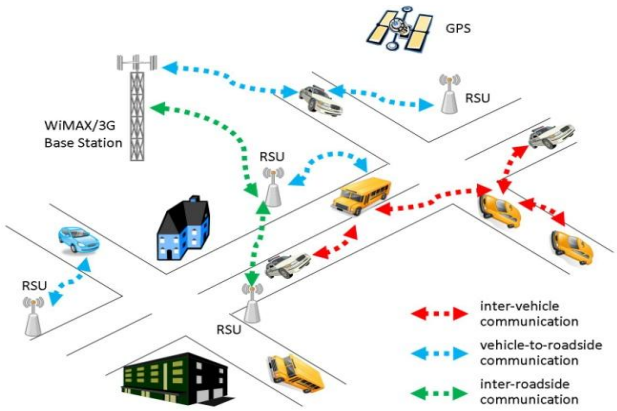

Fig.1:Architecture of VANET [8]

In VANET, there are two sorts of communication. One is distributed (P2P) referred to as V2V communication as appeared. V2V communication happens between vehicles. Second is the Vehicle-to-roadside unit (RSU) which is known as V2R, which happens amongst vehicle and RSU. In V2R communication, a vehicle speaks with the closest RSU. The required message is sent by RSU if and just if vehicles are in the scope of those RSU. Something else, RSU makes an impression on the neighbour RSU for communication. In which, communication is finished by take after three distinctive sort of process, for example,

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

1.3 Applications of VANET

1.3.1 Safety Oriented

Safety applications includes: monitoring of the neighboring path, for the coming vehicles, exterior of the road, road curves etc. [8].

1.3.2 Business Oriented

Business oriented applications will serve drivers different types of services such as the entertainment, web access, audio streaming and video streaming [8].

1.3.2 Collision Prevention and Avoidance

According to a survey some engineers said that 65% of accidents may be prevented when we provide warming information to the drivers few seconds before the collision. To provide the safety of the client, we need the application to be installed in the vehicle by the engineers whom provide the safety message.

1.3.4 Corporative Driving

Engineers should also be provided the signals to the drivers to the traffic changes and also about the lane exchanging message or warning.

1.3.5 Traffic Optimization

if the workers sending messages about the traffic jam, accident etc., to the cars can be optimized the traffic. So they can change their route or path and save their time and enjoy the traveling.

1.4 Challenges in VANET

1.4.1 Environmental Impact

Electromagnetic waves are using in VANET when the communication is being done. These electromagnetic waves are put effect on the environment which become a technical issue in VANET [12].

1.4.2 Network Management

In VANET we are using plenty number of nodes, these nodes have higher mobility and they are sometime changing their network topology and do instant change in the channel. Engineers may not be made any infrastructure like tree topologies of bus topologies because of these changes so it is hard to manage bye the management [12].

1.4.3 Congestion and Collision Control

Large amount of network is some time creates issue. The traffic load is minimum at the night in urban areas as compare to the day as well as in rural areas which creates partition of the network with high traffic area, which they occur the high congestion and collision in the network [12].

1.4.4 Security

As VANET mainly focuses on the road safety applications which are very life critical therefore at time of designing these, securities should be the first concern and the protection of messages must be satisfied [12].

1.5 VANETs Attacks

There are some common attack which find in the cryptography and security. The name of attacks and description of these attacks are listed below.

Table.1: Different attack and description [4]

S.no	Attack's Name	Description
1	Passive attack	Gain the information of target and no data changed
2	Active attack	create wrong data and send to receiver
3	Insider attack	Authenticate the user network and create problem easily
4	Outsider attack	Do misuse of network protocol in low range.
5	Malicious attack	Main motive to create the problem in the network and disrupts the VANET network.
6	Rational Attack	Attacker's personal benefit in it.
7	Black hole attack	In this the problems arises when a nodes rejects to take part in the network. The attacker now performs as DOS in the network.

1.6 Techniques for VANETs Network

1.6.1 Control Channel (CCH)

It control the frequency channel band 5.9 GHz (in America used for control channel 5.9GHz frequency band) from short to medium range communication. VANET network could have communication between vehicular as well as communication with units which is on the road (RSU) road side units and it is clear in either case the topology is changing very fast , this case are going in 30 miles hrs.at least it is in the city.[2,9].

1.6.2 Denial of Service (DOS)

The main object this attacks of the denial of service is to stop the access of the network services. The DOS occur when traffic of the channels system, thus access the network of vehicles. VANETs consists of (RODs) Road Side Units on the road and OBUs on board Units within the vehicles to allow the users communication in the network to pass information to one vehicle to other vehicles. Which mean the DOS attacks create the traffic in the network of the driving the participating vehicles in VANETs networks. The other type of the DOS is (DDOS) Distributed Denial of Services Attacks [9].

1.6.3 Dedicated Short Range Communication (DSRC)

This is a dedicated short range communications (DSRC) provides the frequency bands for communication system. The frequency channels (FCC) using bands by 5.850 to 5.925 GHz. Deducted short range communication work on standards IEEE802.11.p, and standard IEEE1609.1.4. This techniques work up to 1km to 200 km/n area covered. In the VANET network technology using control channels working on 5.9 GHz frequency bands and the number of control channels, used of 178, 174, 176, 180, and 182 used for control channels provides the services. [9]

1.6.4 Elliptic Curve Digital Signature Algorithm (ECDSA)

It receives the information via Message Dispatcher (MD) and converting the data information into digital form elliptic curve cryptography (ECD) module for periodic message. This is also used as a trusted platform module in VANET network.

1.6.5 Global Positioning System (GPS)

This technology based on the wireless connection in any network media. The main motive of this technology stores the all information data and time, also this technology storing the location information about all records. [10]

1.6.6 On Board Unit (OBU)

Vehicular network controls the channels with the reference of the on board unit. This network contains the information about security information. That is called OBU; this on board unit is fresh security system and pseudonym system.

1.6.7 Road Side Unit (RSU)

In the VANET network connected the road side units also Known as vehicles can connected to the infrastructure that is called road side units**.**

1.6.8 Trusted Platform Module (TPM)

It receives the information via Message Dispatcher (MD) and converting the data information into digital form elliptic curve cryptography (ECD) module for periodic message.

2. Related Work

In my review of literature I got some idea about VANET from different paper.In this paper author has said that spectrum allocated to Vehicle to vehicle having problem of less capacity which is due to increment in numbers of nodes. In addition to this the author presents the view about the need for car to car communication over fourth generation and beyond the fifth generation and also put emphasis on localization for the purpose of discovery of device. The important parameter which is found in this survey is gap or distance between the cars or nodes, which may be calculated by the received signal or from the position of the vehicles [1].Inthis paper the writer is put attention on the safety of two authorised vehicles and he also said that the vehicle's speed should be respectable. More than 10,000 people get injured and died by traffic accidents, he add this as a concern feature of vehicular ad-hoc network. The main cause of death or accident is lack security and less privacy of VANET. He also discussed some major attacks which happen in the VANET, like insider or outsider, active and passive, malicious [2].In next paper the author proposed a exploitation of networks diversity for cars communications, the open cellular network is related with the ad-hoc communication. In this paper the author's main focus on the MAC(802.11p)DSRC that is digital short range communication which is join the research area on offloading aspect only when than two vehicles are present. He also proposed the application based on heterogeneous vehicular network. He framed, if the requirements of need of applications be changed then the rule set bound to be changed as well [3].Author presents the architecture of Vehicular ad-hoc network for city traffic concern. In VANET the RSU and cars should be registered with the central controller so that each car and RSU will be authenticated in the network. For to avoiding the congestion between the vehicles and finding the misbehave vehicles play a significant role in Vehicular ad-hoc network. The results of this paper directly indicates on some protocols which are identifies the misbehaving cars even after the registration [4].The author of this paper is mention concern on Vehicular ad-hoc network which is faced high challenges only due to symmetric links of networks and rapidly changing technologies [5].The introduced scheme Timed Efficient Asymmetric Cryptography (TEAC) is based on a TESLA++ and an ECDLP (Elliptic Curve Discrete logarithmic Problem) approach which is a secure is an Asymmetric key cryptography. In addition to this scheme may help to provide security against memory DOS, Malicious attacks [6].This paper gives a general review on the exploration in VANET security and correspondence. It likewise gives parameters considered by the past specialists. After the study, it considered the verification and message sending issues required more research. Validation is first line of security in

VANET; it keeps away from assaults made by the malevolent hubs. Past research has concocted some Cryptographic, Trust based, Id based, and Group signature based verification plans. Speed of confirmation and protection safeguarding are the vital parameters in VANET verification. This paper displayed the AECC (Adaptive Elliptic Curve Cryptography), and EECC (Enhanced Elliptic Curve Cryptography) plans to enhance the speed and security of verification. In AECC, the key size is versatile, i.e. diverse sizes of keys are created amid the key age stage [7].The author discusses about the verbalization of frameworks security and productivity utilizing ECC encryption guideline, has represented the shortcoming of RSA encryption in Public Key structure. All together to build the speed of encryption and unscrambling, and in addition shortening the CPU execution cycle, the paper applies ECC calculation, which takes after the enhancement of quickened point duplication calculation to SSL VPN innovations, and incredibly enhances the information handling velocity of the server[8]**.** The instruction detection system (IDS) is assessed by recreation in rouge hubs that can dispatch distinctive assaults. The proposed IDS is fit for distinguishing a false data assault utilizing factual strategies adequately and can likewise identify different sorts of assaults. To start with, the hypothesis and usage of the VANET display that is used to prepare the IDS is talked about. At that point a broad re-enactment also, investigation of our model under various activity conditions is led to distinguish the impacts of these parameters in VANETs. What's more, the broad information assembled in the reproductions is introduced utilizing graphical and factual procedures. In addition, rouge hubs are presented in the system and a calculation is introduced to recognize these hubs [9]. Scheme to achieve fair and cooperative (SIRC) can animate vehicle or cars clients to help download-and-forward parcels for each other and comprises of agreeable downloading what's more, sending stage. Amid the helpful downloading stage, SIRC uses "virtual checks" related with the assigned verifier mark to guarantee reasonable and secure participation. In the meantime, to limit the installment danger of the customer vehicle, halfway prepayment methodology is embraced, i.e., the vehicles included in downloading parcels can just get some portion of the check some time recently the customer vehicle affirms the bundle gathering[10].

3. Techniques of Cryptography

Cryptography provides security to the network in VANET. There are many security techniques in cryptography such as, DES(data encryption standard), triple DES, RSA(Ron Rivest, Adi Shamir and Leonard Adlemanin), Blowfish, AES(Advance Encryption Standard).AES is the best technique as compare to other because, the block size of AES is 128, 192, 256 bits and three rounds be there for different bits of block size. AES also provides the excellent security as compare to other. Cipher type is same in all techniques expect the RSA, in RSA we are using Asymmetric block cipher. The comparison table of these different techniques is listed below in table one.

Table.2: Comparison table of Different Techniques of Security [11]

Factor	DES	3DES	RSA	Blow-fish	Diffie Hell-man	AES
Devel-oped year	IBM in 1975	IBM in 1978	Ron Rivest, Adi Shamir and Leonard Adleman in 1978	Bruce Schnei-er 1993	whit-fielddi ffie and martin hell-man 1976 uses key ex-chang e	Vin-cent Rij-men-joan-Dae-man in 2001
Key length	56 bits	(k1,k2, and k3)168 bits(k1 and k2 is same)112 bits	Depends on num-ber of bits in the mod-ules n where n=p*q	32-448 bits		128, 192, or 256 bits
Cipher type	Sym-metric block cipher	Sym-metric block cipher	Asym-metric block cipher	Sym-metric block cipher	man-age-ment sym-metric key cipher	Sym-metric block cipher
Block size	64 bits	64 bits	Variable	64 bits	64bits	128, 192 or 256 bits
Rounds	16	48	1	16	14	10(128 bits), 12(192 bits), 14(256 bits)
Speed	Slow	Very slow	Slowest	Slow	Slow	Fast
Securi-ty	Not secure enoug h	Ade-quate security	Least secure	Weak	Secure	Excel-lent

4. Security in VANET

It is said that the cryptography is a very essential protocol in terms of security. In cryptography we can get many things like maintain privacy with us only, verification of messages. Cryptography is comes from Greece, the meaning of cryptography is based on two Greek words “kryptos” and “graphein” , which means hidden and hidden writing respectively. In this authentication is more important which means the owner or sender can see the location of message and also check the medium from which the message comes. The cryptography is a methodology through which we can send and receive information from one node or point to another point with privacy [6]. Privacy means no another unauthorised node can see client’s information. CIA is the services which are provided by the cryptography, C stands on confidentiality, I define as integrity and A is availability. The brief introduction of this CIA is given in Fig. 2

Fig.2: Security requirement trade[11]

4.1.1 Message Confidentiality

The basic definition of confidentiality is that, it is believe or grantee that the information be secure. Only legitimate customers can see the information no third node or party can take part in this. In a VANET, the data traded is generally open, aside from those identified with the protection of clients.

4.1.2 Information integrity

It implies that the collector can guarantee of getting message. Message that has been issued and it has not been modified in travel. An attacker ought not to have the capacity to change messages.

One way hash functions frame the in the writing, the expression "legitimacy" implies both authentication and uprightness, and it is frequently mistaken being used for validation.

4.1.3 Availability

Availability requires that the data must be accessible to the real clients. DoS Attacks can cut down the system and henceforth data can't be shared. It implies that the system works legitimately and administration ought to be accessible 24*7.

4.1.4 Non-Repudiation

This technique does not give permission to the sender of a packet to refute the claim of not sending the packet.

4.1.5 Access Point

Access Control specifies and controls who can access what.

4.1.6 Authentication

Authentication mechanisms are doing help to make proof of identities. This process ensures that the origin of the message is correctly identified.

4.1Diffie Hellman

Diffie Hellman is basically used for key exchange between two nodes, because we are taking two cars in vehicular ad hoc network for sending and receiving the information about traffic. Through diffie Hellman we are providing the security in VANETs. The algorithm of this technique is given in table 3.In diffi Hellman key exchange we are taking "q" as a prime number "α" as a primitive root which is less than prime number. In this algorithm we are taking user A and user B key generation.A Alice and B Bob we are taking name as an example [15].

Table .3: Algorithm decryption of Diffie Hellman

USER Alice KEY GENERTAION	
Select private key Alice W_A	$W_A < q$
Public key calculating by Z_A	$Z_A = \propto^{WA} mod q$
USER Bob KEY GENERTAION	
Select private key of Bob W_B	$W_B < q$
Public key calculating by Z_B	$Z_B = \propto^{WB} mod\ q$
Secret key be calculating by the first user A(Alice) Key=$(Z_B)W_A\ mod\ q$	
Secret key be calculating by the second user B(Bob) Key=$(Z_B)W_B\ mod\ q$	

There are some decided values of each point. These values are given below in tabular form in Table 4.[15].

Table.4: Elements of Diffie Hellman and their desired values

Elements	Values
$\propto$	3
q	353
W_A	97
W_B	233

The values after compute $Z_A = 3^{97} = mod\ 353 = 40$

The values after compute $Z_B = 3^{233} mod\ 353 = 248$

After exchange their pubic key each node can compute a common Secret key:

Alice computes Key with the help of this formula which is written below:

Key=$(Z_B)W_A mod 353 = 248^{97} mod\ 353 = 160$

Bob computes Key with the help of this formula which is written below:

Key=$(Z_A)W_B mod 353 = 40^{233}\ mod\ 353 = 160$

4.2 DES

The DES stands on data encryption standard. In this data encryption standard has two functions one is encryption and second is data decryption with the help of key. In DES, there are 16 rounds function 64 bit used for the length of plaintext and 56 bits of keys used in this. There are some steps of DES are listed below:

1. Initial permutation (IP) function is the first step of DES, there are 64-bit plain text information is sent.
2. In the second step the IP works on Plaintext.
3. In the next step two halves are generated by Initial permutation which are sent messages LPT (Left plain text) and RPT (Right Plain Text).
4. After the upper step, Left plain text and Right Plain Text go through the sixteen rounds of encryption process.
5. At the end point , Left plain text and Right Plain Text are again connected and a FP that is called final permutation is works as a joinet or combine block.
6. The result of this system generates 64 bit of cipher text rounds.

4.3 Triple DES

In triple DES we are using two keys. Triple DES is calculated by this formula.

$$C = E\left(K_1, D\left(K_1, E(K_1, P)\right)\right) = E(K_1, P)$$

This upper formula is for cipher text and below is for plain text.

$$P = D\left(K_1, E\left(K_1, D(K_1, C)\right)\right) = D(K_1, C)$$

Where **K** is key
E is encryption
D is decryption
C is cipher text
P is plaintext [14 16]

4.4 RSA

Ron Rivest, Adi Shamir, and Len Adlemanis developed in 1977. The scheme of Ron Rivest, Adi Shamir, and Len Adleman is basically a block cipher in which the ciphertext and plaintext are integer between 0an $n-1$.[15]

The size of n is 1024 bits or it is 309 in decimal binary. The algorithm of RSA scheme has some ingredients which are listed below in Table 5.

Table .5: RSA elements

$r, s, two\ are\ prime\ no.$	These are chosen private
$N = rs$	These are calculated by publicly
$e, with\ (\emptyset(n), e) = 1; 1 < e < \emptyset(n)$	These are chosen public
$Z = e^{-1}(mod\emptyset(n))$	These are calculated by privately

The calculations of this RSA algorithm is

1. First we chose the two prime no which are $r = 17\ and\ s = 11$
2. Then calculate the N which is calculated by multiplying $rs = 17 * 11 = 187$
3. After calculating this we calculate pie with$\emptyset(n) = (r-1)(s-1) = 16 * 10 = 160$

4. Then we have e=7
5. Then we calculate $Z \equiv 1(mod 160) and\ this\ Z\ is < 160$. But the exact value of Z is 23, because the 23*7=161[15]

4.5 AES

This is stands on the Advanced Encryption standard. In this AES the no. of rounds depends on no. of key length which is in bytes.
For example:

Table 6: AES rounds and key length

No. of rounds	Key length(bytes)
10	16
12	24
14	32

Some more parameters of AES are given in Table 7.

Table.7: AES parameters in different units

Parameters	In words	In bytes	In bits
Key size	4/16/128	6/24/192	8/32/256
Plaintext block size	4/16/128	4/16/128	4/16/128
Rounds of key size	4/16/128	4/16/128	4/16/128
Expanded key size	44/176	52/208	60/240
No. of rounds	10	12	14

4.6 Blowfish

Blowfish has 64 bit cipertext, and it has variable length key . it is carrying two parts with itself first is subkey generation in which it converts the keys above 448 bits which is long to subkeys of 4168 bits. In second step Data Encryption involves the iteration of six-teen times for a simple function [14].

4.7 Attacks on Different Layer

When there are some merits there are also some demerits. We are observed some attacks from these schemes which are on different layers and these attacks put great effect on the layers and these attacks are directly get harm the network.
In security there are many attack find on different layer. These attacks put impact on network layer, transport layer; media access Control and physical layer. The attacks name are Masquerade attack, DOS, Malicious attack and Blackhole attack, session hi-jacking, parallel session, mutual authentication and insider attack. The table 8 shows the different attack on different layer and also mention the impact of attacks.

Table.8.Security Attack on different layer [4,7,13]

S.no	Types of Attacks	Layer	Impact on network
1	Masquerade Attack, Denial of Service (DoS), Replay Attack, malicious attack and black hole attack.	Network layer	Unauthorized access to the network, Reduction in throughput and PDR.
2	Session hijacking	Transport Layer	Terminates or delay the communication
3	Parallel session , Mutual authentication	MAC layer	Stop forwarding the network nodes, weak security.
4	Insider Attack	Physical layer	Network make com-plex

5. Conclusion

We have shown the various mechanisms of encryption and how it works. Different types of attacks has been carried and having various impact on the network. VANET is suffering from the dynamic environment nature and mobility aspects so we have to work to improve the security standards for VANET communication.

References

[1] Nshimiyimana A et.al. (2016), Comprehensive Survey of V2V Communication for 4G Mobile and Wireless Technology, *Proceedings of IEEE WiSPNET conference.*

[2] Bappadiyajana, Mitra S & Jayantaporay (2014), An Analysis of security Threats and Countermeasures in VANET, *Techno India University West bengal. India.*

[3] Valle F, Cespedes S.(2016), Improving Vehicular Applications through Network Diversity, *De chile, Santiago, Chile*.

[4] Prabha VL & Ranichitra A (2013), Isolating Malicious Vehicles and Avoiding collision between Vehicles in VANET,*International conference on communication and signal processing*, Vol.2, no.2 pp. 46-51.

[5] Jain J, Chahal N (2016), A Review on VANET, types, charecteristics and various Approaches, *International Journal of Enginnering Scineces & Research Technology*, pp-239-245.

[6] Mahagaonkar SN, Dongre N (2017), TEAC: Timed Efficient Asymmetric Cryptography for Enhancing Security in VANET, *International Conference on Nascent Technologies in the Engineering Field* .

[7] Godse SP, Mahalle PN, Wagh SJ (2017), Rising Issues in VANET Communication and Security: A State of Art Survey, *International Journal of Advanced Computer Science and Applications*, Vol. 8, no. 9, 2017, pp-245-252.

[8] Setiadi I, Kistijantoro AI, Miyaji A(2015), Elliptic Curve Cryptography: Algorithms and Implementation Analysis over Coordinate Systems, *School of Electrical Engineering and Informatics.*

[9] Li X, Liu J, Yao Q, & Ma J (2017), Efficient and Consistent Key Extraction Based on Received Signal Strength for Vehicular Ad Hoc Networks, *IEEE Access,*Vol. 5, pp.5281-5291.

[10] Chen L, Li Q, Martin KM, Ng SL(2015), Private reputation retrieval in public privacy-aware announcement scheme forVANETs, *IET Information Security*, Vol.4, pp.1-29.

[11] Soni S, Agrawal H, Sharma M(2012), Anlaysis and Comparisonbetween AES and DES Cryptogarphic Algorithm, *International Journal of Engineering and Innovative Technology*, Vol. 2, no.6, pp-362-365.

[12] Rahbari M & Jamali MAJ(2011),Efficient detection of Sybil attack based on cryptography in vanet, *International Journal of Scinetific and Engineering Research* , Vol.3, no.6, pp-185-195.

[13] Mandal PC(2012), Superiority of BlowfishAlgorithm,*International Journal Of AdvancedResearch in Computers Science and SoftwareEngineering*, Vol 2 no. 9, pp.14-20.

[14] Mitali VK & Sharma A (2014), A survey on various cryptographic techniques, *International Journal of Emerging Trends & Technology in Computer Science*,Vol.3, no.4, pp-307-312

[15] Iyer KBP, Anusha R, Priya RS(2014), Comparative Study on Various Cryptographic Techniques, *International Journal of Computer Applications*,pp-37-42