International Journal of Security and Its Applications
Vol. 11, No. 4 (2017), pp.27-44
http://dx.doi.org/10.14257/ijsia.2017.11.4.03

Review of Vehicular Ad Hoc Network Security

Hari Krishna[1] and Sandeep Kumar Arora[2]

[1,2]*Department of Electronic and Communication Engineering,*
[1,2]*Lovely Professional University, Phagwara, Punjab, India*
[1]*hrkrishna116@gmail.com,* [2]*sandeep.16930@lpu.co.in*

Abstract

Vehicular Ad-hoc network (VANET) is a wireless communication among many vehicles. The main motive of VANET security is to not only to provide safety, secure communication and intelligent transportation service but also another service like entertainment, advertisement and offers based on location wise. As all the services related to communication are more important and vulnerable to attacks hence requires security. In VANET, vehicles represent the node and communication take place either between vehicle to vehicle (V2V) or vehicle to infrastructure (V2I). Securing communications between vehicles and the roadside unit is a great challenge. Various researchers had done a lot of work in terms of security in VANET communication but still, these are vulnerable. Some first-time attack such as the hidden vehicle, tunnel, wormhole attacks are presented in this paper and their possible cryptographic solution is also provided. In this paper, we will go through various security issues, routing protocol, challenges in VANET, several attacks, and their cryptographic solution.

Keywords*: Vehicular Ad-hoc Network, Road Side Units(RSUs), Cryptography, Attacks, Mobility*

1. Introduction

In recent years, Vehicular Ad-hoc Network (VANET) development has become an intelligent transportation system (ITS). VANET is a special case of Mobile Ad-hoc Networks (MANET) where vehicles are communicating node. The main objective of VANET is to provide road safety and excellent driving experiences as well as entertainment. The event activity sensed by embedded sensor as well as traditional sensor called onboard equipment (OBE) mounted on the vehicle. The sensed data is processed by on-board processors and share this data by direct mode of communication between vehicle and roadside units (RSU) by spontaneously creating a network popularly known as vehicular ad hoc network (VANET) [1-2].

In Vehicular ad hoc network, communication is classified into Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I) and hybrid communication similar to access points in traditional wireless networks, RSU is also placed on the road network at certain places to provide necessary infrastructure support [14, 18]. Vehicles are required to transmit safety and traffic related messages containing its speed, location, acceleration, hazard warnings, accident avoidance and route updates periodically as shown in Figure 1.

VANET requires following message exchange security issue: (i) Message integrity should be ensured by prevention of message content alteration. (ii) To avoid impersonation attack, message sender must be authenticated. (iii) Vehicle identity should be hidden from tracking (iv) Real-time constraint should be respected in order to deliver messages with acceptable time delay [2].

ISSN: 1738-9976 IJSIA

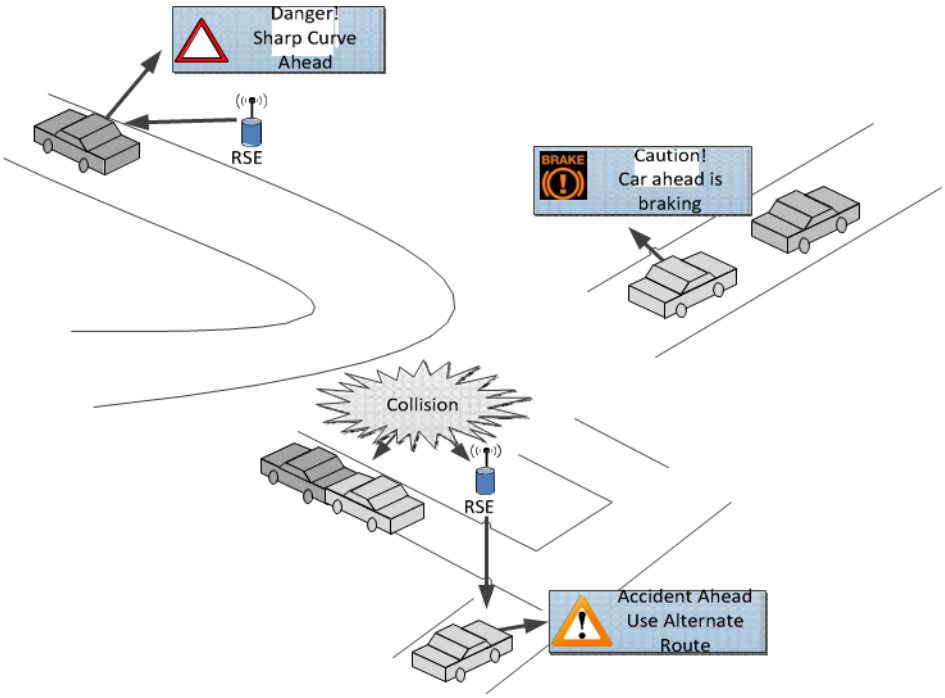

Figure 1. VANET Awareness

VANET architecture as shown in Figure 2. involves almost all the seven layer of OSI model varying from the physical layer to application layer, security attack and vulnerability exist on all the layers [11].

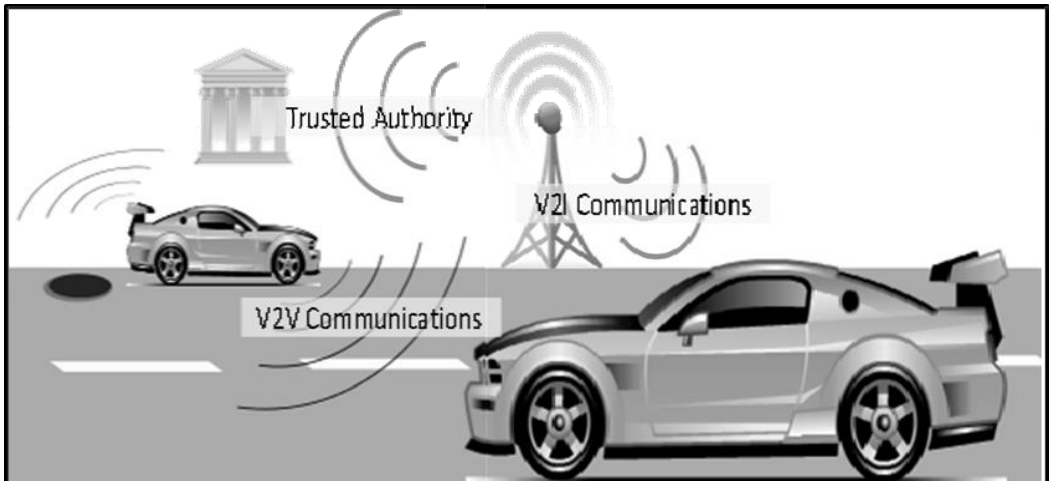

Figure 2. VANET Architecture

2. Previous Work

After going through various research papers, we have found that in previous studies there has been less focus on linking VANETs security issues with related cryptographic techniques which can entirely give a solution to the problem or reduce the problem and its effect. In [5] classification of attacks, presentation of attacker model and some first-time attack such as the hidden vehicle, tunnel, wormhole, Bush Telegraph are presented. They have also mentioned the requirement of secure message broadcasting in vehicular ad hoc network and group communication has been discussed and various security issues and solution are represented [3-4]. In [6, 9] provided the recent classification of attacks and

their categorical solution. In [7, 10] scaling of VANET security through cooperative message verification was presented [12]. As research in the field of VANET security is in developing phase so it will touch various axis at the same time, namely: wireless communications, protocols for physical and MAC layers, routing protocols and security [13]. This paper is devoted to providing comprehensive and structured overview of recent advance research like security, surveying, security threat, attack, vulnerability and some part of VANET security simulation tool.

3. VANET State of the Art

The basic VANET architecture is shown in Figure 3., which consist of following: (I) OBU (Vehicle equipped with on Board Unit), (II) RSU (Road Side Units) distributed everywhere as a part of network infrastructure and Trusted Authority (TA). In VANET two types of communication are possible V2V and V2I and RSU will act as a router having wider coverage than vehicle coverage. Generally, vehicles are equipped with Global Positioning System (GPS), ELP (Electronic License Plate) for identification, RADAR (Radio Detection and Ranging) / LASER (Light Amplification by Stimulated Emission of Radiation) for knowing the position of another vehicle. These systems are operated with battery power. At the backend, there may be a trusted authority installed. The RSU and OBUs communicate wirelessly with each other using the Dedicated Short Range Communications (DSRC) protocol, which has a bandwidth of 75 MHz at 5.9 GHz frequency, Whereas TA and RSU communicate with each other using fixed secure network like the internet [13].

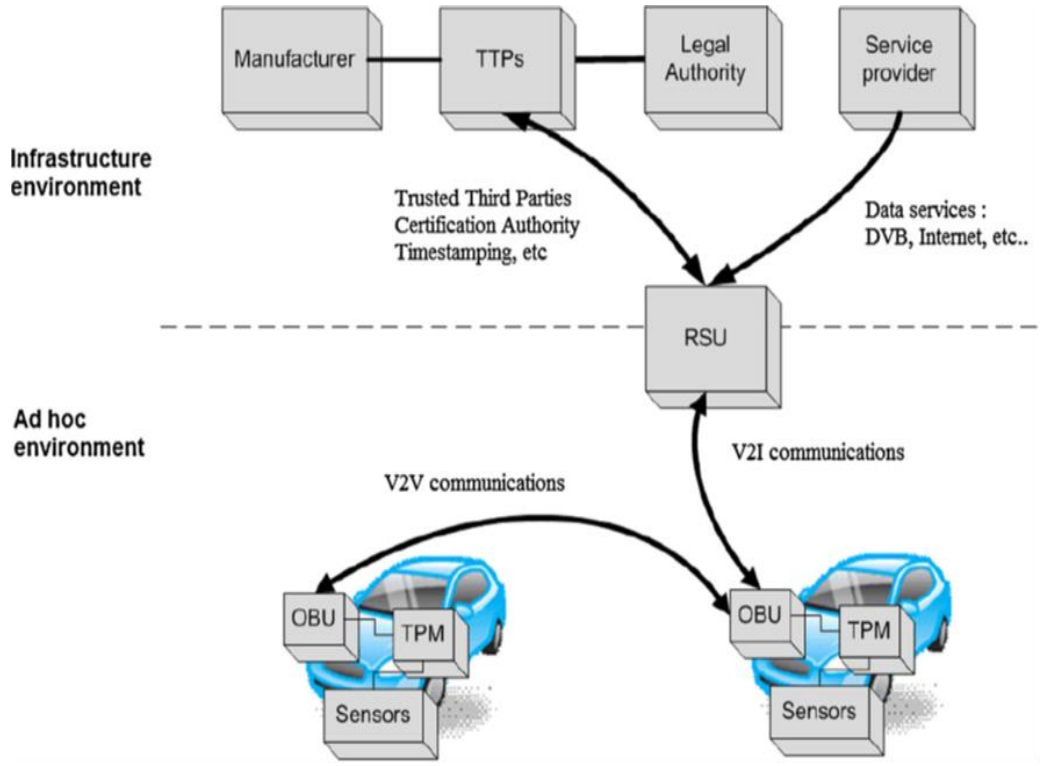

Figure 3. VANET Components

4. VANET Characteristic

Vehicular ad hoc network is a wireless communication where communication takes place between fixed unit such as RSU and highly mobile unit Vehicle. The characteristics of VANETs are basically a mixture of a wireless medium as well as different topologies in ad hoc and infrastructure modes. These characteristics are:

4.1. High Mobility

High mobility is one of the most important features of VANET nodes. Nodes move all the time with different speeds and directions in normal mode within the network. Highly mobile nodes reduce the mesh in the network. A relatively node in VANET has high speed with respect to MANET [10].

4.2. Dynamic Topology

As mobility increases, VANET topology is changing rapidly, therefore dynamic and unpredictable nodes moving in opposite directions have very less connection time, hence this topology facilitates the attack of the entire network, and makes difficult in the detection process of malfunction.

4.3. Frequent Disconnection

There are several factors which cause frequent disconnection such as high mobility of nodes, vehicles density in traffic, weather condition *etc.*

4.4. Availability of the Transmission Medium

In VANET the transmission medium is air. Being greatest advantage and universal availability of this wireless transmission medium, air causes security issue in inter-vehicular communication.

4.5. Anonymity of Support

In wireless communication, data transmission is anonymous. So if we kept the protocols aside, anyone equipped with a transmitter operating in the same frequency band can transmit and create traffic [4].

4.6. Limited Bandwidth

For VANET communication, the standardized DSRC band (5.850–5.925 GHz) can be considered as limited, because the width of the entire band is only 75 MHz.

4.7. Attenuation

Digital transmission of DSRC band frequency transmission has problems such as diffraction, dispersion, reflection, different types of fading, losses and propagation delays due to multipath reflections and Doppler effect *etc.*

4.8. Limited Transmission Power

Limited transmission power limits the distance that data can reach. In the WAVE architecture, this distance is up to 1000 m, however in emergency and public safety it is allowed to transmit with a higher power.

4.9. Energy Storage and Computing

VANET do not suffer from problems of energy, computing capacity or storage failure, unlike other mobile networks. However, we should keep in mind the real-time processing requires a large amount of information is also a challenge.

5. Routing Protocol in VANET

The aim of routing protocols is to ensure the selection of the best path for packets from source to destination in a timely manner. In a wireless or infrastructure-less environment, the flow of data with high mobility is a difficult task. Routing is considered as a major problem in VANET. In VANET, there are two main methods of routing: hop by hop routing and source routing. Routing protocols in VANET can be classified into following categories as shown in Figure 4.

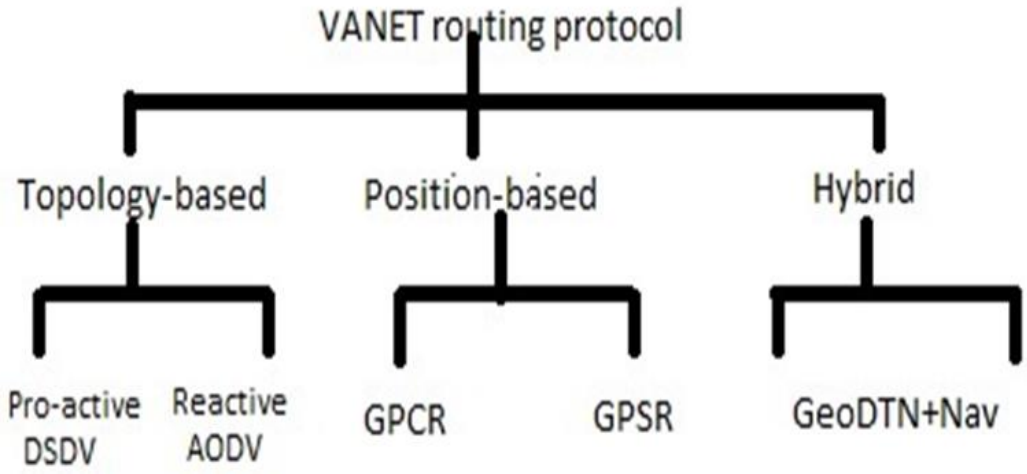

Figure 4. Classification of Routing Protocols

5.1. Topology-Based Routing Protocol

In this routing protocol, we use information of the links (roads) to route packets. In this protocols route discovery and maintain routing tables are important parameters. Generally, if topology based protocols exceed one hundred nodes, networks do not function properly. In this type, possible protocols are Topology-based routing (TBR), Position-based routing (PBR), Hybrid routing.

5.1.1. Proactive Routing Protocols

This protocol also called as “table-driven”, each node maintains one or more table information for all destinations. This class requires a periodic exchange of control packets between nodes for routing table update *e.g*. OLSR, DSDV and FSR *etc.*

5.1.2. Reactive/On-Demand Routing Protocols

In this path is computed on demand basis. The first phase is route discovery and to route data. In the second phase, routing of data when the network changes update in topology is required *e.g*. DSR, AODV *etc.*

5.1.3. Hybrid Routing Protocols

Hybrid protocols is the combination of the proactive and reactive protocol's mechanisms. The proactive protocols technique used just for the neighbor's discovery *e.g*. ZRP and HARP *etc.*

5.2. Position Based Geographic Routing Protocol

These protocols use data provided by global positioning systems for selecting the next hop destination, so between sources and destination, there is no overall route creation and update required. In this category, we find GPCR, GPSR. [15].

5.3 Cluster Based Routing Protocol

In Cluster based routing, neighbor's vehicles form a cluster. Every cluster has a "cluster-head", which is responsible for management of both functions inter and intra-cluster. The most critical required steps for the proper functioning of the network is a selection of the cluster and cluster-head. Cluster based routing protocol is considered as a greedy process in case of high mobility.

5.4. Broadcast Routing Protocol

In this protocol, flooding mechanism is used; in which each node broadcast messages to its entire neighbor node except the original sender. The responsibility of flooding mechanism is that message should reach to every node in the network. This method is suitable for a small number of nodes. It is a routing method frequently used in VANET to get information about traffic, emergency messages, weather, information between vehicles, and to provide advertisements and announcements.

5.5. Geo-cast Routing Protocol

This describes sending messages to all vehicles in a specific geographical area. It is very useful protocols in the case of informational VANET applications, connected to a specific region**.**

5.6. Infrastructure Based Routing Protocol

The "Infrastructure based routing protocols" are the routing mechanism protocols based on methods primarily for infrastructure networks, later on, it has adopted to VANET.

6. VANET Applications

Intelligent transportation system application means proper coordination between the driving system, danger notifications of the road, cooperation for collision avoidance, comfort applications for travelers are innovative ITS applications. They have also included the provision of mobile internet access, a variety of onboard services. VANET applications can be classified as follows: road safety, traffic efficiency. VANET applications are also classified into safety related applications and other applications [2].

6.1. Driver-Oriented Application

If the information received about the danger. it helps drivers for making a better decision [11].

6.2. Vehicle Oriented Application

In this application, we give command information to the vehicles. It increases automation and improves road safety.

6.3. Passenger-Oriented Application

In this application, user comfort and entertainment facility were employed like infotainment, Internet access [11].

6.4. Infrastructure Oriented Application

In the case of an intelligent transportation system, effective utilization of highways can be done [1].

6.5. Road Safety Application

In this category of applications, VANET provides collision avoidance and road work, dissemination of weather information and detection of mobile and fixed obstacles. We find application in Slow/Stop vehicle Ad- visor, Emergency Electronic Brake Light [8] It also tells about Post-Crash Notification, Cooperates Collision Warning.

7. VANET Security and Challenges

7.1. VANET Security Requirement

In VANET, security measurement is defined as how much secure a network is. In general, authentication, integrity, availability, access control, confidentiality and physical security are requirements of VANET, security [13].

7.1.1. Authentication

It ensures that message is trusted and the proper user is recognized. In some authentication process, the receiver must verify the sender Identity. On the other hand, the receiver only interested whether the sender has vehicle or not and its location.

7.1.2. Integrity

Integrity means the message sent by the user is neither modified nor altered by an unauthorized manner in the source to destination. A message can be intentionally modified by an attacker or may be by accidently (due to the faulty vehicle).

7.1.3. Availability

In VANET, availability means channel availability. Wireless channels should be available so that incoming vehicle can give notification of accident ahead or clear out the road for the emergency vehicle.

7.1.4. Confidentiality

In the case of VANET, confidentiality is the ability to prevent unauthorized nodes from accessing the message content.

7.1.5. Non-repudiation

In this security mechanism sender/receiver can prove the occurrence of the transaction.

7.1.6. Delay

When there is a delay in packet transmission due to late or out of time arrival of the packet. Delay is used to provide congestion free and transmitting the information [17].

7.2. VANET Attacks

As in various communication and data processing systems, various types of threats and attacks are possible. OBU control dozens of microprocessors capacity of processing and computing in comparison to a regular ad hoc network. Due to the high mobility in VANET, the feasibility of attacks is possible. Therefore, some attacks possible in the ad hoc network are impossible for VANET. Various classification discussed in several papers are classified as follows [11, 13].

In this paper, we will classify based on the cryptography which will give a better representation of our work: cryptographic solutions to VANET security issues 'Classification is shown in Table 1.

Table 1. Various Security Attacks in VANET

VANET threat and attack				
Availability	**Authenticity and authentication**	**Confidentiality**	**Integrity and data trust**	**Non-repudiation / Accountability**
Denial of service	Sybil attack	Eavesdropping	Message suppression	Loss of event traceability
Jamming	Reply attack	Information gathering	Fabrication / Alteration	
Greedy behavior	GPS Spoofing	Traffic analysis	Masquerade	
Broadcast tampering	Position faking		Reply	
Malware	Masquerading			
Spamming	Tunneling			
Black hole attack	Key / Certificate replication			
	Message tampering			
	Message suppression			
	Fabrication / Alteration			

7.2.1. Attacks on Availability

7.2.1.1. Denial of Service

These attacks are actually a family of attacks targeting the availability of network services which create serious consequences for VANETs applications. Because of this

impact, DOS attacks are classified in the class of dangerous attacks. The malicious nodes can perform DoS attack either internally or externally in the network. The primary focus of this attack is to block principal means of communication and interrupt the services.

7.2.1.2. Jamming Attack

The Moto of jamming attack is to disrupt the communication channel by transmission of the signal. It is also known as physical level of Denial of Service attack. Its main function is to lower the signal to noise ratio (SNR).

7.2.1.3. Greedy Behavior Attack

Greedy attack's, the attack on the functionality of the MAC layer the greedy node always tries to connect to the media and they do not follow the channel access method. The greedy node tries to prevent the support and services used by other nodes to use. The Greedy attacker tends to minimize waiting time for faster access.

7.2.1.4. Black Hole Attack

In ad hoc networks, black hole attack is considered as a conventional attack against the availability. In this, malicious node obstructs to participate in the routing table and it gets packets from the network so they declare themselves to be a part of the network.

7.2.1.5. Gray Hole Attack

Gray Hole is a variety of Blackhole attack. Gray hole attack prevents the data packet which is vulnerable.

7.2.1.6. Sink Hole

In this attack, malicious node tries to attract the packets from neighbor/adjacent node. It also allows eliminating or modifying the received packets before retransmission.

7.2.1.7. Wormhole Attack

In VANET application, when a malicious node is very close to receiving the center data from another node, attacker insert wrong information of location for confusing the receiving node.

7.2.1.8. Malware Attack

OBU and RSU are affected by malware. Malicious software filtered during the virus definition updating process.

7.2.1.9. Broadcast Tampering Attack

To hide the legitimate users, the attacker tries to insert fake security alert messages. Which will lead to accidents and affect the overall network security?

7.2.1.10. Spamming Attack

Attacker flooded the web to network with spam messages (*e.g*. advertisement) therefore performance and quality of service degraded.

7.2.2. Authenticity and Identification Attack

A major challenge of VANETs security is authenticity. All the TA available in the network first authenticates the user message before accessing them. Authenticity in a

vehicular network prevents attacker from both insides as well as outside. Attacks under this category are classified as follows:

7.2.2.1. Sybil Attack

The logic of Sybil attack is that; a malicious entity is a cause for creating multiple identities. this attack comes under dangerous attack [16].

7.2.2.2. GPS Spoofing/Position Faking Attack

In a VANET, information related to position is crucial and it should be accurate and authentic. In GPS spoofing, attacker generating localization signals stronger than the real satellite for the false location of the node [16].

7.2.2.3. Node Impersonation Attack

The aim of this attack is the violation of authentication process. Every node in VANET allotted with the ID during registration in the network. The attacker tries to get a valid ID and passes for another legitimate node in the network.

7.2.2.4. Tunneling Attack

In this attack, attacker create a private connection (tunnel), the same network but in the case of wormhole we assume attackers are external and they use different radio channels for the exchange of packet. In a vehicular network, two distant parts of the network are connected by tunneling attacker. This attack is very much similar to wormhole attack.

7.2.2.5. Key or Certificate Replication Attack

These attacks can take place in those networks where the duplicate key is used and certificates are used as proof of identification. Therefore, this kind of activity creates ambiguity to identify and authorize vehicle.

7.2.3. Confidentiality Attack

7.2.3.1. Eavesdropping Attack

Eavesdropping attack is passive and against confidentiality. An attacker can collect useful information such as location data which can be used for tracking purpose of vehicles.

7.2.3.2. Traffic Analysis Attack

The traffic analysis attack is a threat to the privacy of the user and confidentiality. The attacker analyzes collected data and tries to extract the maximum of useful information from the network**.**

7.2.3.3. Non-Repudiation Attack

This kind of error has the ability to verify that the sender and the receiver have sent or received the message respectively. In non-repudiation attack, it is considered that if data generated then it will be received by the receiver. In a VANET context, data manipulation belongs to user's safety and privacy is possible. So, it is suggested to take care of software security. The biggest problem in non-repudiation attack is the loss of event traceability.

7.2.3.4. Loss of Event Traceability

In VANET, we have not found any document which discusses this attack though it is an important to attack. It is a non-repudiation attack which takes action against the attacker. The attack comes under this category mainly based on the erasure of trace action and creates confusion for the audit entity. There is some attack serve as non-repudiation attacks such as Sybil and duplication of keys and certificate attack.

7.2.4. Some other Possible Attacks

There are some kinds of attacks which play role in VANET security.

7.2.4.1. Privacy attack

This kind of attack we discuss privacy related to driver and VANET users.

7.2.4.2. Timing attack

Data sending from sender to receiver node plays an important role in the Emergency message. The attacker does not forward this message quickly to the adjacent node. He/she forward received message after adding some delay. Hence adjacent node responds with some delay.

7.2.4.3. Man-in-the-Middle Attack

Attacker inserts a vehicle in between the vehicles in direct communication for controlling the communication and add some redundant information in the communication channel. This kind of attack violates the authentication and the integrity.

8. Cryptography

Cryptography deals with the security and it provides all type of security services. Modern cryptography provides security techniques like authentication, confidentiality, secret sharing, integrity, non-repudiation *etc.* For the satisfaction of security services, we use technique like encryption/decryption algorithms, hash function, Keys generation and exchange protocols, digital signature *etc.* as shown in Figure-5 [11].

8.1. Cryptographic Requirement

8.1.1. Confidentiality

This is the very first problem which occurs in cryptography. Confidentiality is only used to confirm that message is only read by authorized user. In this most of the information is public except privacy related message of user.

8.1.2. Authentication

Authenticate mean to verify the origin of the data, and if the user is the one who authenticated then data is delivered to user. The digital signature method is a technique of authenticity [11].

8.1.3. Integrity

Integrity means receiver is also capable of identifying the message whether it is altered or not during transmission of message. One-way hash functions are used for solution of integrity problems.

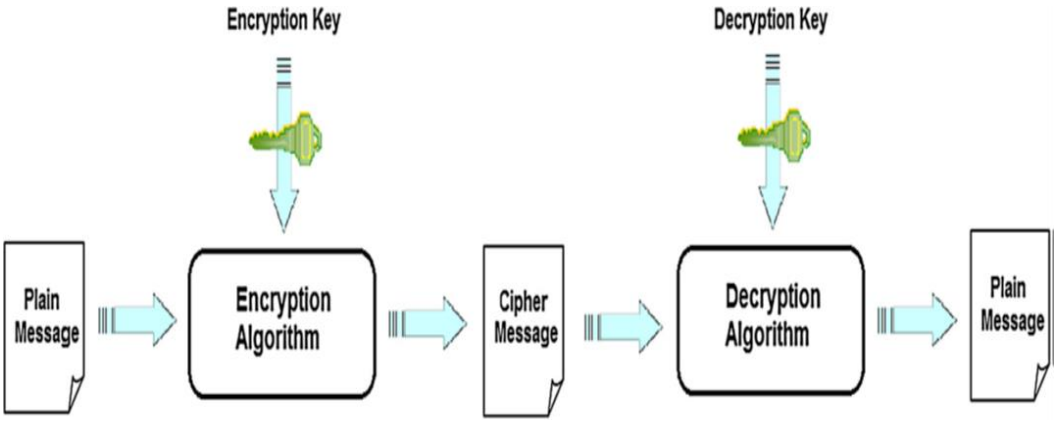

Figure 5. Encryption and Decryption Process

8.2. Encryption/Decryption

In Figure 5, A schematic representation of encryption/decryption principal of message is shown, which can be described as follows:

1) The algorithms used for encryption/decryption are set of operations depends upon mathematical functions which take clear message and encryption key as input and give encrypted message as output.

2) The encryption/decryption algorithms receive an encrypted message and a decryption key as input and corresponding output will give clear message as output.

8.3. Symmetric Cryptography

Symmetric cryptography also is known as secret key cryptography. Calculation of decryption key with the help of the encryption key can be done easily. In symmetric cryptography, security is maintained by keeping the key secret between communicating parties. The system is compromised if the key is leaked. The main drawback of symmetric cryptography is that both parties have access to the secret key.

8.4. Asymmetric Cryptography

Asymmetric cryptography also is known as public key cryptography. The principle of asymmetric cryptography is as follows:

1) Each user has a pair of key; one private key is for the user which should keep secret. Another public key is available to public.

2) If we are able to encrypt with the public key, the private key can be decrypt and vice versa.

3) But practically it is impossible (time and resources) to determine for *e.g*. the private key having information of the public one and vice versa.

4) It is usually slower when used for encryption purpose in symmetric algorithms. It is mainly used for the key exchange purpose and in digital signature authentication tool through digital certificates. The public key cryptography can be used to solve problems where secret key cryptography fails.

8.5. PKI, Digital Certificates and Timestamping

For a large number of user public Key Infrastructure, PKI requires the management of private and public keys which is a combination of hardware and software procedures components [1]. PKI ‘s most important are to be a trust third party between digital counterparts. With the help of the certification authority (CA) PKI ensures that role of

signed, delivers and keep up to date digital certificates information which considered as digital ID for an entity.

Electronic file binds together a public key with an identity the guarantee of the certification authority. The main work of certificate is to allows authenticate and signing certificates and also encrypt messages.

Time stamping is to certify the event (send/receive/signing of a message) happens at a given time. In this authentication and non-repudiation, attacks are possible.

In a VANET context, solutions related to PKI are given as Vehicular Public Key Infrastructure (VKPI) and use of digital certificates as a method of rapid authentication in a vehicular network [5].

9. Cryptographic Solution against VANET Security

In this section, we will summarize the existing security problem and its possible cryptographic solution. In Table 2. we have discussed all the recent attack and their cryptographic solutions without discussing their detail.

Table 2. Cryptographic Solutions for VANET Attacks and Vulnerabilities

ATTACK	COMPROMISED SERVICES	CRYPTOGRAPHIC SOLUTIONS
Eavesdropping	Confidentiality	-In this, we encrypt only required data which can minimize privacy risk of drivers like positioning data and vehicle identification data *etc.*
Jamming	Availability	-For this problem, switch the transmission channel, and use the Frequency Hopping Spread Spectrum (FHSS) in which cryptographic algorithm generate pseudo random number for the FHSS algorithm.
Traffic analysis	Confidentiality	-It is similar to eavesdropping. - VIPER algorithm used for V2I communications
DoS	Availability	-Use bit commitment and signature based authentication mechanisms. Which reduces the impact of almost of DOS attacks?

Sybil attack	Authentication Availability	Deploy a central Validation Authority which validates entity in real time. The validation process can be direct or indirect. Indirect validation, the node which wants to authenticate, establish a direct connection with the VA. - In the indirect method, an entity already enabled can accept an incoming entity.
Message tampering/ suppression/fabrication/ alteration	Availability Integrity Non-repudiation	-In this, we use a vehicular PKI (VPKI) or zero-knowledge techniques for the authentication between vehicles and for signing warning messages. -In this group, communications are established Keys can be managed by a Group Key Management system (GKM). This causes that an intruder could not be able to communicate with the group.
Broadcast tampering	Integrity	-This attack can be performed by a legitimate node of the network; cryptographic primitives are enabling to prevent it. However, a non-repudiation mechanism may exist.
Timing attack	Availability	-For packets of delay-sensitive applications, use the time stamping mechanism. To overcomes this problem, we should maintain time synchronization between the entities.
Illusion attack	Authentication Integrity	-Only authorized user can access hardware equipment and software. - Challenge/response mechanism used to verify updates or reading operations from the sensors. -Use trusted hardware for which it is practically impossible to change existing protocols and values, except

		by authorized.
Brute force	Confidentiality	-Use strong encryption and key generation algorithms, unbreakable within a reasonable running time [15]. This prohibits access to information to those who are not allowed.
Key and/or certificate replication	Confidentiality Authentication	-In this, we use certified and disposable keys and Check the validity of digital certificates in real time via CRL (Certificate Revocation List). - Use cross certification between the different certification authorities involved in VANETs security scheme.
GPS spoofing/Position faking	Authentication Privacy	-Use bit commitment and signature-based mechanisms with positioning systems to accept only authentic location data.
Replay	Authentication Integrity	Use time stamping technique for packets which their replay is dangerous [15]. We have discussed the problem of time synchronization between entities.
Loss of event traceability	Non-repudiation	-The Same proposition as illusion Attack.
Tracking/Social engineering	Privacy	In this, we use always variables MAC and IP address to separate the addresses from the identities of vehicles and drivers. MAC and IP addresses allocation must be managed by robust algorithms.
Node impersonation	Integrity Authentication Non-repudiation	- Use variables MAC and IP addresses for V2V and V2I communications. - Authenticate via digital certificates. - Strengthening the authentication mechanism

		using distance bounding protocols based on cryptographic techniques such as bit commitment and zero-knowledge.
Greedy Black hole Gray hole Sinkhole Wormhole Malware Masquerading Spamming Tunneling	Availability Authentication Integrity Confidentiality Non-repudiation	-For these attacks, cryptography does not offer real solutions but certainly suggested actions can reduce disastrous effects, such as digital signature of software and sensors. - Use trusted hardware for which it is practically impossible to change existing protocols and values, except by authorized.

10. Conclusion

Vehicular Ad-hoc Network consists of three pillars like Vehicular communication, Routing algorithm, and cryptography. These pillars of VANET plays important role to provide secure communication among vehicles and protect them from various types of attack. In this paper, I found VANET's most important problem is mobility of vehicle and this problem is solved by using cluster based routing protocol. There are several attacks so it becomes very important to secure the communication for preventing accidents to save the human life. Some first-time attacks such as hidden vehicle, creation of tunnel, wormhole attacks and their possible cryptographic solutions are also provided in this paper. In future, we can use Elliptic Curve Cryptography (ECC) to make our communication more secure and using ECC we can make intelligent transport system for the society.

References

[1] W. K. Chen, "Linear Networks and Systems (Book style)", Belmont, CA: Wadsworth, **(1993)**, pp. 123-35.
[2] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code", C. John Wiley & Sons, Inc: USA, **(1995)**.
[3] S. Choudhury, K. Bhatnagar and W. Haque, "Public Key Infrastructure Implementation and Design", Wiley: USA, **(2002)**, pp. 53-66.
[4] J. Blum and A. Eskandarian, "The threat of intelligent collisions", IT Professional, vol. 6, no. 1, **(2004)**, pp. 24-29.
[5] M. Raya, P. Papadimitratos and J. P. Hubaux, "Securing vehicular communications", IEEE Wireless Communications, vol. 13, no. 5, **(2006)**, pp. 8-15.
[6] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security, vol. 15, no. 1, **(2007)**, pp. 39-68.
[7] S. M. Safi, A. Movaghar and M. Mohammadizadeh, "A novel approach for avoiding wormhole attacks in VANET", Second International Workshop on Computer Science and Engineering, WSCE'09, Qingdao, **(2009)**, pp. 160-65.
[8] B. Mishra, P. Nayak, S. Behera and D. Jena, "Security in vehicular adhoc networks: A survey", Proceedings of the 2011 International Conference on Communication, Computing & Security, **(2011)**, pp. 590-595.
[9] A. Rawat, S. Sharma and R. Sushil, "VANET: Security attacks and its possible solutions", Journal of Information Operation and Management, vol. 3, no. 1, **(2012)**, pp. 301-304.
[10] S. Zeadally, R. Hunt, S. Y. Chen, A. Irwin and A. Hassan, "Vehicular ad hoc networks(VANETs): Status, results, and challenges", Telecommunication Systems, vol. 50, no. 4, **(2012)**, pp. 217-241.
[11] A. Dhamgaye and N. Chauhan, "Survey on security challenges in VANET", International Journal of Computer Science, vol. 2, no. 1, **(2013)**, pp. 88-96.

[12] E. M. Mathew and P. Arun Raj Kumar, "Threat analysis and defense mechanisms in VANEyT", International Journal of Advance Research in Computer Science and Software Engineering, vol. 3, no. 1, **(2013)**, pp. 47-53.
[13] M. N. Mejri, J. Ben-Othman and M. Hamdi, "Survey on VANET security challenges and possibl cryptographic solutions", Vechicular Communications, vol. 2, no. 1, **(2014)**, pp. 53-66.
[14] H. Jin and P. Papadimitratos, "Scaling VANET security through cooperative message verification", 2015 IEEE Vehicular Networking Conference, (VNC), Kyoto, **(2015)**, pp. 275-78.
[15] L. Bariah, D. Shehada, E. Salahat and Y. C. Yeun, "Recent Advances in VANET Security: A Survey", 2015 IEEE 82nd Vechicular Technology Conference VTC Fall, Boston, MA, **(2015)**, pp. 1-7.
[16] S. Bittl, A. A. Gonzalez, M. Myrtus and H. Beckmann, "Emerging Attacks on VANET Security based on GPS Time Spoofing", 2015 IEEE Conference on Communications and Network Security (CNC), Florence, **(2015)**, pp. 344-52.
[17] D. Saravanan, V. Agalya, J. Amudhavel and S. Janakiraman, "A Brief Survey on Performance Analysis and Routing Strategies on Vanets", Indian Journal of Science and Technology, vol. 9, no. 11, **(2016)** March, pp. 1-6.
[18] A. Malik and B. Pandey, "An Intelligent Authentication Based Vehicle Initiated Broadcast-Dynamic Path Data Collection Scheme in VANET", Indian Journal of Science and Technology, vol. 9, no. 16, **(2016)** April, pp. 1-7.

Authors

Hari Krishna, is currently pursuing M. TECH in Electronics and Communication Engineering with Spl. in Wireless Communication Systems at Lovely Professional University, India. His research interests include Ad-hoc Networks and Cryptography.

Sandeep Kumar Arora, is currently pursuing Ph. D. in Electronics & Electrical Engineering with Spl. in *Design of Secure Initiation Protocol in VANET*. He is working as an Asst. Prof. in Lovely Professional University since 2011. His research interest includes Wireless Sensor Networks, Computer Networks, Adhoc Networks Communications and Cryptography. He is an author of more than one dozen research papers indexed in Scopus.