International Journal of Grid and Distributed Computing
Vol. 9, No. 11 (2016), pp.17-34
http://dx.doi.org/10.14257/ijgdc.2016.9.11.02

Review of Vehicular Ad Hoc Network Security

Kuldeep Kumar and Sandeep Kumar Arora[1]*

[1, 2] Discipline of Electronics and Communication Engineering,
Lovely Professional University, Jalandhar, Punjab, India-144411
Email: [1]kuldeep.etah@yahoo.com, [2]sandeep.16930@lpu.co.in

Abstract

In the near future we know that vehicles will communicate with each other to make Vehicular ad hoc network and gives the concept of intelligent transportation system. In this paper we presented the review of security in VANET. Consequently, several researchers represented the attacks and solutions in vehicular communication We analyzed some of the security problems and proposed solutions to overcome it. We discussed the need for robust Vehicular Ad hoc networks, which is very strongly dependent on their security and privacy features. This paper will review the existing attacks in VANET in the perspective approach of security.We also provided the solutions to the particular attack in VANET.

Keywords*: Vehicular Ad Hoc Network (VANET), Attacks, Security, Privacy,Certificate Authentication (CA)*

1. Introduction

At the present time, road transportation and traffic activities are involved in our important daily life. So new improvements in this area are going on day by day for improving the safety and driving conditions. The number of vehicles on the roads has been rising significantly, leading to increase in traffic-based issues such as accidents and congestion. [1] Five million vehicles accidents and a combined price of accidents and congestion totaling or so $300 billion are according annually within the USA. In worldwide, more than 500 thousand people died in road traffic accidents every year and this amount is increasing year by year and injures around fifty times of this number. Even due to high traffic rate there is wastage of time and fuel.

The most important factors of traffic safety are driving, more accurate positioning, weather information and early warnings of upcoming dangers (e.g. Traffic jam, accidents) would be highly useful for driver. [3] For this we require a new type of technology known as VANET (Vehicular Ad-hoc Networks) is being developed.

The Vehicular Ad hoc network is a subclass of Mobile Ad-Hoc Networks (MANETs) in which communication nodes are above all vehicles and this means that all nodes can move easily within the network coverage and stay connected. Individual node can communicate with each other in single hop or a multi hop. In Vehicular Ad Hoc Networks, communication is divided in to two different categories.

Sandeep Kumar Arora is the corresponding author.

ISSN: 2005-4262 IJGDC

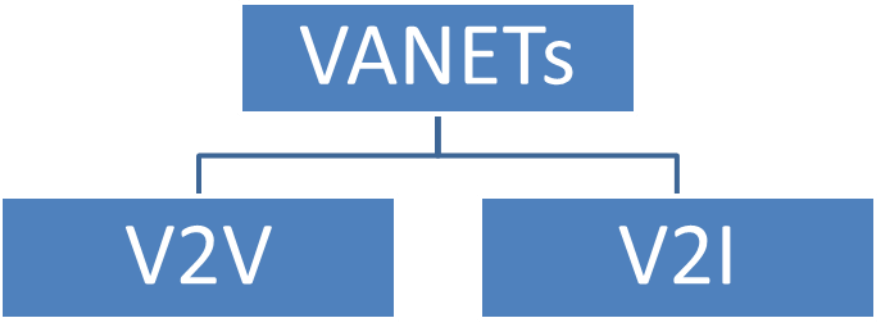

Figure 1. Categories of VANETs Communication

V2V is vehicles to vehicles communicate with each other. Furthermore, V2I vehicles can communicate to an infrastructure *i.e*. vehicles communicate collected information to the nearest Road Side Units(RSUs) in demand to distribute the information more rapidly and more efficiently. Based on these communications in VANETs can offer a wide range of services as shown in Figure 1.

In general, Wireless Ad hoc Network is node-to-node communications all nodes are able to a router the data. There are two kinds of nodes:

(i) Road Side Units (RSUs) (ii) On Board Unit (OBUs)

In RSUs fixed nodes provisioned along the road and OBUs refers to express nodes (*i.e*. Automobiles) which equipped mutually with the help of radio interference [6] are produced comfort and online entertainment services (*i.e*. toll Payment, internet, music, *etc*.) applications for passenger and driver. The facilities it offers in VANETs; intelligent vehicular networks are used in wireless medium as shown in Figure 2. so different types of attacks occurred in vehicular ad hoc network. This paper presents security issues and challenges in vehicular communication.

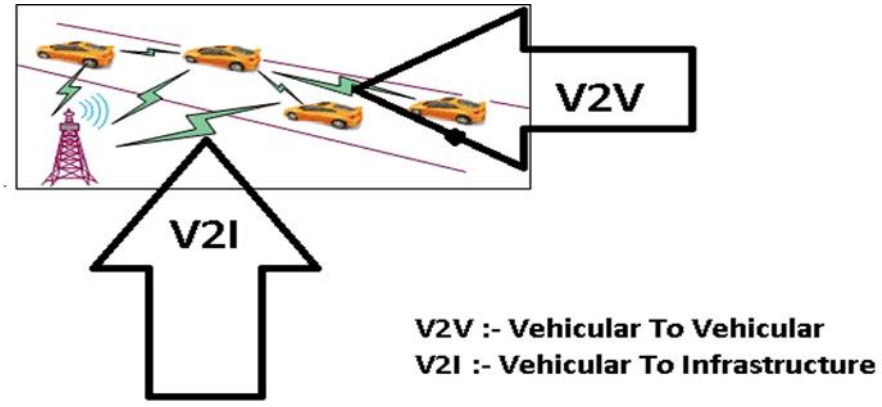

Figure 2. Vehicular Ad Hoc Network

The architecture of vehicular ad hoc networks contains several software and hardware components which includes the seven layers namely physical layer, datalink layer, network layer, transport layer, session layer, presentation layer, application layer, of the Open System Interconnection (OSI) nodes. All layers are vulnerable to attacks. There are many tools and techniques to deal with VANETs security is cryptography [4]. In this paper, we are discussing the security challenges and main attacks on VANET and additionally discussed the present resolution for these attacks.

2. Related Work

Several researchers studied security and attacks related to vehicular communication. In this paper, Khaleel Marshad [5], vehicles in a groups, and messages are forwarded to all group members by the group leader. Hence, the privacy of all group members is secured by privacy of the group leader. Furthermore, if group leader is selected malicious vehicle, total group member's privacy may be leaked. So this problem overcome by a used group signature which is using a secure scheme in which unique group public key is related with multiple group private keys. Even though an eavesdropper can know that a message is sent by the group, it cannot recognize the sender of the message pseudonym is joined with a group signature to avoid storage pseudonyms and licenses in vehicles. In [1] J.M. d. Fuentes, A.I. González-Tablas, A. Ribagorda, they talked about overview of the security issues with a cryptography point of view details or some presenting solutions. The security of vehicular networks focused on a specific issue on include key management, privacy, anonymity, reputation, and location.

In Raya and Hubaux [7], they discussed the security weaknesses and challenges in vehicular ad hoc networks if Vehicular Ad hoc Network users use the same Identity Document (ID) whenever send a message, a malicious node could hack to their message and construct a profile of their positions, which exposes their privacy. It's planned to deceive attackers. Pseudonyms preserves the location privacy of a user by breaking the likability between two locations. A vehicle can from time to time update its pseudonym. The powerful enemy may still link new and old pseudonyms by monitoring the spatial and temporary relations between both new and old locations. It's were posed the three techniques namely mix zones, silent period, and vehicular ad hoc anonymity.

The previous related works aware situation of VANETs security. In the following sections, we aim to highlight security requirements in Vehicular ad hoc network, then introduce in the possible attacks and solution in vehicular communication. The consequently section will represent the different advances of characteristics and features all these condition.

3. Characteristics of Vehicular Ad Hoc Networks

The characteristics of Vehicular Ad hoc Networks are mainly a combination of wireless medium characteristics. A VANET can be utilized to offer following characteristics in the communication. [11] VANETs has its own separate characteristics given below.

1) **High Mobility: -** In VANETs, nodes are frequently moving at high speed. A node positions predict and creating security of node privacy.
2) **Unbounded networks size: -** Vehicular network can be built for small city, numerous cities, countries, and for worldwide. So network size in Vehicular ad hoc network is geologically unbounded network size.
3) **Anonymity of the support: -** Wireless medium is generally used in data transmission. Transmitter operating on the same frequency band can transmit and hold the band for data transmission.
4) **Rapidly changing network of dynamic topology: -**The position of node changes regularly due to high node mobility, dynamic topology in rapidly changing vehicular network changes frequently.
5) **Enough Energy: -**The nodes do not have issue of energy and computation power resources. Because we can provide power from battery also.
6) **Frequent disconnections: -**The rapidly changed network topology and high mobility of nodes along with another different conditions such as weather, climate mass of traffic perform disconnections of vehicles.
7) **Better Physical Protection: -** Vehicular Ad hoc network nodes are physically

superior protected. Thus, nodes are more challenging to settlement physically and decreases the effect of infrastructure attack in VANETs.

8) **Availability of the transmission medium: -** The transmission medium of Vehicular Ad hoc Network is air. We can transmit the data wirelessly but in wireless transmission the major concern is security advantages in Inter Vehicular. Communication (IVC), becomes the starting point of some security matters.
9) **Time Critical: -** The information in vehicular ad hoc network should be delivered to the node with in real limit so a choice will be created by the nodes and perform action consequently.
10) **Energy storage and computing: -** Unlike alternative kinds of mobile networks, VANETs don't suffer from issues of energy, computing capability or storage failure. However, real-time operation demands huge quantity of data could be a challenge to stay in mind.
11) **Wireless Communication: -** VANETs is intended for wireless surroundings. All nodes are connected and conversation their information through the wireless communication. Hence, some security can be implemented over it.
12) **Limited bandwidth: -** The standardized DSRC band (5.850–5.925 GHz) for VANET are often thought-about as restricted, the dimension of the complete band is just seventy-five megahertz rate. Restrictions of use in some countries recommend that these seventy-five megahertz rate are not at all allowed and the most theoretical output is twenty-seven Mbps.
13) **Limited transmission power: -** The transmission power is restricted within the WAVE design, that limits the gap that information will reach. [2] This distance is up to one thousand meter. However, in sure specific cases like emergency and public safety, it's allowed to transmit with a better power.
14) **Attenuations:** - Dedicated short-range communication (DSRC) band has conjointly transmission issues associated with digital transmission with such frequencies, like reflection, optical phenomenon, dispersion, differing kinds of fading, losses and propagation delays thanks to multi-path reflections.

4. Vehicular Ad Hoc Network Applications

VANETs will play important role will be applications classified into two general types. [3][4][7].

A. Safety Related Applications

There are some applications used to increase for safety. There applications will be categorized in subsequent manner.

1) Collision Avoidance: If drivers were provided a warning a second before collisions so that seventy percentage accidents will be avoided [4]. If driver come to be warning messages on time, collisions will be avoided.
2) Cooperative Driving: Driver will send signal for traffic related warnings like lane amendment warnings, curve speed warnings, *etc*. There signal will cooperate the motive force for associate interrupts and safe driving.
3) Traffic optimization: Traffics will optimize by way of utilization causation signal like accidents, traffic jams *etc*. towards the vehicles so that they will be opted for their alternative paths and may save the time also.

B. User Based Applications

VANETs is utilized to supply subsequent services for the users excluding protection.

1) Peer to peer applications: These applications is helpful to produce facilities like sharing movies, music, *etc*. amongst the vehicle within the networks.

2) **Internets Connectivity**: Individual users always need to connects with the net every time. Therefore, Vehicular ad hoc network offers the constant connect to the internet.
3) **Other type of services**: VANETs may be used in alternative users primarily based on applications like all payments facilities to gather the toll taxes, to find the nearest fuel stations, eating place such as restaurant *etc*.
4) **Driver-oriented applications**: To assist the drivers on the road if it receives data concerning the risks ahead, traffic, *etc*. [3]
5) **Vehicle-oriented applications:** In this application, permitting to provide data to their vehicles to extend automation and improve road safety.
6) **Passenger-oriented applications:** For the comfort of the user with new on-board services (e.g. documentary, web access). Infrastructure-oriented application so as to form higher use of road infrastructure.

In general, we tend to conclude that the majority of the analysis in papers VANET measures much in agreement that the most applications dedicated for conveyance networks may be sorted into three categories.

C. **Applications for road safety**: It's mainly enhance travel safety and scale back road accidents, VANET applications offer collisions shunning and road work, detection of mobile and stuck obstacles and dissemination of weather data. During this class of applications, we find e.g.: Slow/Stop Vehicle Advisor, Emergency Electronic stoplight. [7] Post-Crash Notification, "Road Hazard Management Notification" collaborate Collision Warning.

D. **Applications for driver assistance**: They aim to facilitate driving and assist the motive force in specific things like passing vehicles, bar of channel outputs, detection and warning of holdup, warning of potential traffic jams, *etc*. During this class we discover e.g.: engorged road notification, parking available notification, toll plaza collections. [7]

E. **Applications of passenger's comfort:** These applications area unit for the comfort of the motive force and passengers, they basically give services like mobile web access, messaging, discussion between vehicles, cooperative network games, *etc*. within the remainder of this section we have a tendency to limit ourselves to the outline of some services and samples of applications of vehicle-to- vehicle communication systems.

5. Various Challenges and Issues in VANETs

VANET differentiates a unique network although the characteristics. However, deployment of the VANETs to some characteristics executes to some challenges. These are may be categorized into subsequent classes. [11]

A. Technical Challenges

The technical challenges cope up with the technical obstacles that ought to be resolved before the preparation of VANET. Some challenges areas are given below.

1) **Network Management:** In VANETs channel condition modification and topology changes frequently due to high mobility. we can't use tree like structures due to freely change in topology.
2) **Congestion and collision control:** In rush hour, the traffic is more in urban area as compared to the urban area. [4]
3) **Environmental Impact:** The electromagnetic (EM) waves are used for vehicular ad-hoc network communication. EM waves are highly effected due to atmosphere. Hence, to deploy the VANET the environmental effect needs to be measured.

4) **MAC Design:** Shared medium is used to speak in VANET therefore the medium access control is that the key issue. Various approaches used in VANET are TDMA, SDMA, and CSMA [15] *etc*.
5) **Security:** The purpose of VANET is to provide the road safety application. Hence messages should be secure.

B. Social and Economic Challenges

Social and economy also create challenges in VANET. It's hard to design such a system which tells about traffic rule violation [1] because this kind of system are rejected by user but the warning message of police trap is appreciated by them. Therefore, to encourage the manufacturers to deploy Vehicular ad hoc network can get very little incentives.

6. Security Challenge of VANETs

A. Security issues in VANETs

Security got less attention to this point. The packets contain life critical information in VANET hence it is necessary to made send packets so it is not changed by the attacker. In VANETs security [6] is major concern as compare to general communication. The difficult to implementation to makes size of network, high mobility, geographically relevancy *etc*.

B. Security Challenges in VANETs

The various security challenges are planning of VANET design, security protocols, scientific discipline formula, cryptographic algorithm solution *etc*. The subsequent list presents some security challenges. [11]

1) **Real time Constraint**: Vehicular ad hoc network is time critical wherever safety connected message ought to be delivered with 100ms transmission delay. Therefore, to realize real time constraint, fastest cryptographic algorithmic rule ought to be used. Message and entity authentication should be tired time.
2) **Data Consistency Liability**: In VANETs even verification of node will perform malicious activities which will cause accidents or disturb the network. Therefore, a mechanism ought to be designed to avoid this inconsistency. Correlation among the received information from totally different node on explicit data might avoid this sort of inconsistency.
3) **Low tolerance for error**: The basis of probability is design some protocols in VANET. In VANETs, life critical information is used and action performed for very short time. In probabilistic formula occurrence of small error might cause problem.
4) **Key Distribution:** VANETs is a key dependent safety mechanism. Every encrypted message is decrypted at receiver side either with same key or completely different key. [2] Every manufacturer uses different security mechanism for installation of keys and in case of public key infrastructure trust on CA become a big issue. Therefore, distribution of keys among vehicles may be a major challenge in planning a security protocols.
5) **High Mobility:** The mobility is a major issue because the speed of the vehicles is unpredictable.
6) **Low complexity security algorithms***:* In VANET some current security protocols like DTLS, SSL/TLS, WTLS [4] usually uses RSA based public key cryptography. RSA algorithmic program uses NP-Hard resolution on prime no. as it requires more time hence we go for less time consuming algorithm like ECC (Elliptic curve cryptography) For bulk encryption AES may be used.

7) **Transport protocol choice:** For secure dealings over informatics we prefer DTLS over TLS as DTLS operates over connectionless transport layer. IPsec needs several messages to set up to avoid IP traffic. When vehicles don't seem to be in motion we can use IPsec and TLS**.**

C. Security Requirements in VANETs

VANETs should satisfy some security necessities before they're deployed. [10] A security system in VANET ought to satisfy the subsequent necessities.

1) **Authentication**: It means the message is generated by authentic user.
2) **Availability**: Data should be offered to the authentic users which can overcome the DoS attack.
3) **Non-Repudiation**: Non-repudiation suggests that a node cannot deny that he doesn't transmit the message. it's going to be crucial to work out the proper sequence in crash re-establish.
4) **Privacy**: Privacy of the node should be maintained.
5) **Data Verification**: A regular verification is required to maintain the integrity of the data.

7. Security Challenges of VANETs

A. Attackers on Vehicular Ad Hoc Network

VANETs is to be secure that initial we've got to know who exist the offender, their capability and nature to crash the systems. These attackers of capability are also divided into three types:

1) **Outsider and Insider:** Outsiders area unit the intruders and thus restricted capability to attacks and whereas Insider area unit the attested memberships of networks.
2) **Rational and Malicious**: Rational attacker have only private profits. Whereas malicious attacker hasn't at all personal profits to attacks, they only injured the function of the networks.
3) **Active and Passive**: Active attacker generate signals or packet whereas passive attacker solely senses the networks.

B. Attacks in the VANETs

To get higher protection from the attackers we have the tendency to have the data regarding the attacks in VANET against security needs. Attacks on completely different security demand are shown in Figure 3. [7]

Impersonate: In this type of attack malicious node assumes that the privileges and identity of a licensed nodes, furthermore to form uses of networks resource that will not offered there to disrupt the conventional function of the networks or to under traditional circumstances. This attack is performed by active attacker and they will be insider's or outsider's attacker.

These attacks are multilayers attacks mean that attackers will exploits either transport layer, application layer, or network layer, susceptibility. These attacks are often performing in two behaviors.

(i) False Attributes Possession **(ii)** Sybil Attribute

i) False attributes possession: Under this category of attack, the attacker steals some properties of authorized user and it try to profess of being authorized user [8] and try to send messages. Hence any vehicle can claim to be a police, ambulance or fire brigade and give command to free the traffic.

ii) Sybil Attribute: Mainly in this kind of attacks, attackers use totally different identity on identical times.

1) **Session hi-jacking:** The beginning of the sessions most of authentication method is finished. Therefore, it's straight forward the session to hijack after connections in the network. Attacker lead of session between node during in this types of attacks.
2) **Identify revealing**: In general, the vehicles obtaining owner's identity by owner is itself driver so identity will be place the privacy's in danger.
3) **Position Tracking**: The position of a given moments or the trail follow on an amount your time is accustomed track the vehicles and acquire info of drivers.
4) **Repudiation:** This is often completely different from the impersonate attack. During this attack or additional entity has common identity hence it's simple to want indistinguishable and hence they'll be repudiation.
5) **Eavesdropping:** It's a most typical attack on confidentiality. This attack is performing over to network layer attack and passive in nature. The goal of this attack is to induce the access of confidential information.

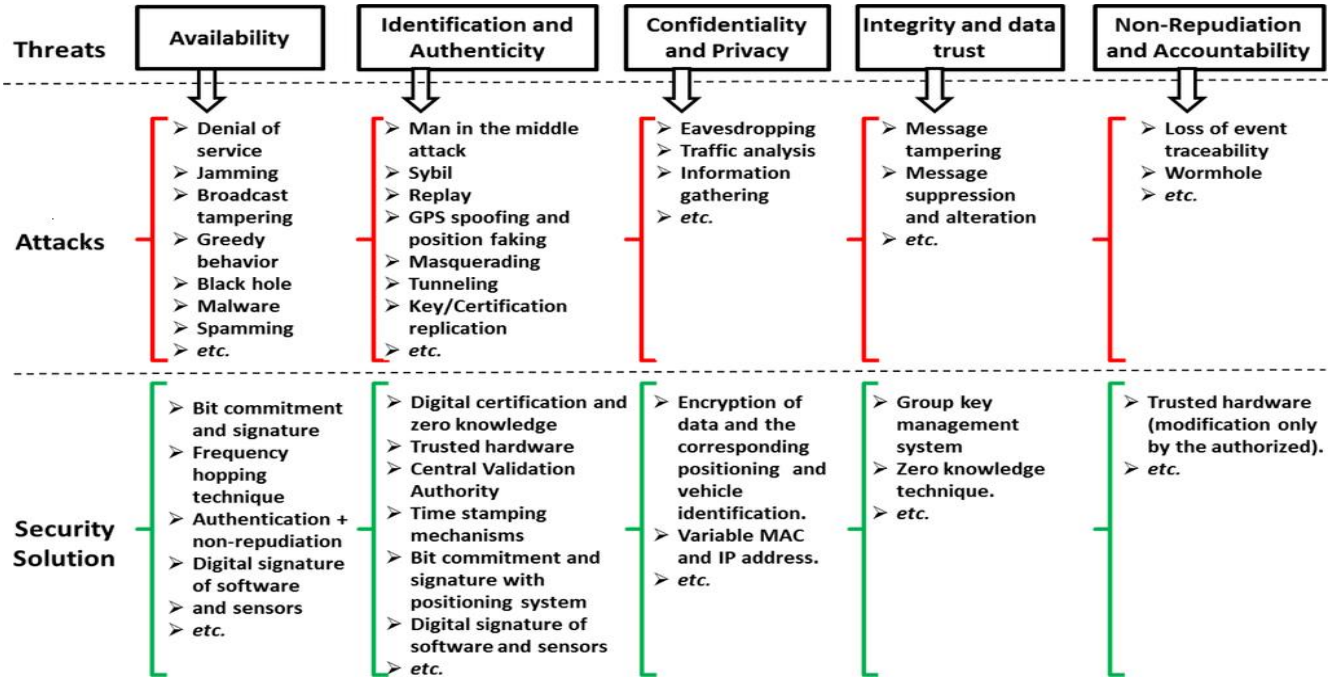

Figure 3. Classifications of Attacks and Solutions

6) **Denial of Service:** DoS attack is very crucial in which the services are not offered to nodes properly due to the attack performed by the attacker node. [8]

(i) Jamming: The attacker will sense the frequency on which the user is transmitting the data and try to jam the data.

(ii) Synchronize Flooding: During this method, giant number of synchronize request is transported to the casualty node, spoofing the despatcher address. The casualty node sends back the Synchronizer acknowlegement to the spoofed address however casualty node doesn't get any acknowlegement packets reciprocally. [2] A casualty node's buffer by this result to half opens association to holder. As a significance, the genuine request is rejected.

(iii) Distributed DoS attack: It is one more type denial of service attack. During this type of attack, so many attackers attacks the casualty node and avoids genuine user from get into the service.

7) Routing attack: During this attack, the assaulter either disturbs or drop the packets The common routing attacks occur in the VANETs is given below [7][12]

i) Black Hole attack: During in this kind of attack, offender first of all attracts the nodes to transmit the packet through itself. It is done by continuous causing the malicious route reply with contemporary route and low hop count. Once attracting the node, once the packet is forwarded through this node, it mutely drops the packet as shown in Figure. 4.

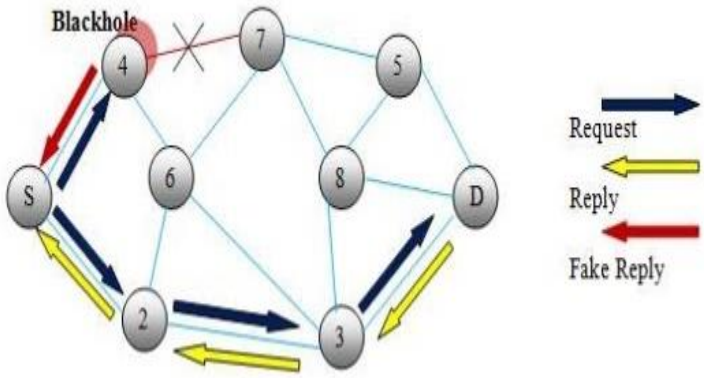

Figure 4. Black Hole Attack

ii) Worm Hole attack: In this type of attack somebody receives packets at one point within the network, tunnels them to a different purpose within the network, so replays them into the network from that time. This tunnel between two adversaries referred to as wormhole. It is often established through one long-range wireless link or a wired link between the 2 adversaries. Therefore, it's easy for the somebody to form the tunneled packet arrive before different packets transmitted over a traditional multi-hop route as shown in Figure 5.

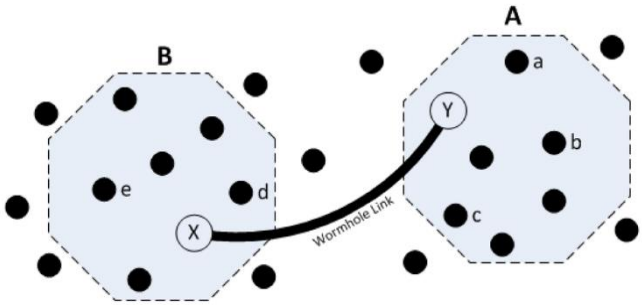

Figure 5. Worm Hole Attack

iii) Gray Hole attack: This is the extension lead of black hole attack. During this kind of attack, the malicious node behaves just like the black hole attack however it drops the packet by selection as shown in Figure 6. This choice can be of two kinds:
a) A work of attacker node is to drop the packet of User datagram protocol (UDP). However, the transmission control protocol packets are going to be forward.
b) The premise of probabilistic distribution on attacker node will drop the packet.

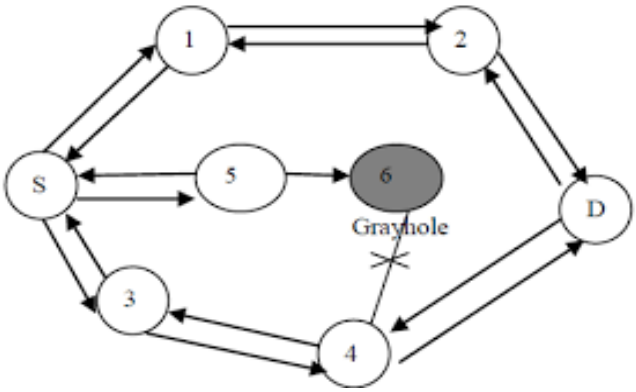

Figure 6. Gray Hole Attacks

8. Cryptographic Primitives and Tools

A. Cryptographic primitive:

We denote by cryptography primitives, all the protection services that cryptography provided. Fashionable cryptography offers many security techniques like confidentiality, authentication, integrity, non-repudiation, secret sharing, *etc*. To satisfy these security services, cryptography uses ways like encryption/decryption algorithms, Keys generation and exchange protocols, hash functions, digital signature and other alternative techniques. Within the following we have a tendency to primarily trust the known reference [14] of Bruce Schneider for the presentation of the various science primitives.

1) **Confidentiality:** It's the primary weakness that has been display to cryptography. Confidentiality is to confirm that messages will solely be browse by those that are licensed. In a VANET, the data changed is generally public, except those associated with the privacy of users.
2) **Authentication:** It permits the receiver to verify the origin of the info, and if the establishment is that the one who claims to be. VANET user must not be able to pass for somebody else. The digital signature is one solution to be provided here.
3) **Integrity:** It means the receiver is ready to confirm that the received message is that the message that has been issued and it's not been altered in transit associate assailant shouldn't be able to modify messages. Unidirectional hash functions type the premise solutions set for integrity issues. It ought to be noted that within the literature, the term “authenticity” means that each authentication and integrity, and it's typically confused in use with authentication.
4) **Non-repudiation:** It's to confirm that a player cannot deny taking done associate action. During a VANET context, a vehicle shouldn't be able to deny causation a warning e.g. or having done associate attack.

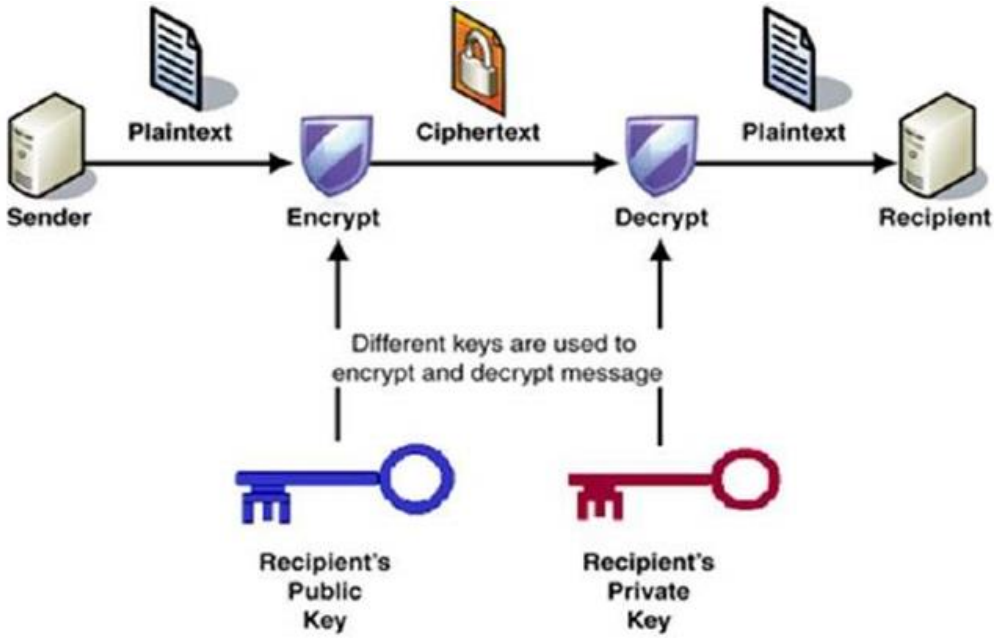

Figure 7. The Principle of Encryption Decryption.

B. Encryption/Decryption

The principle of coding and coding of a message, delineated schematically in Figure 7., is as follows: associate algorithmic rule for encryption/decryption, that could be a set of information operations process supported mathematical functions, receives as input a transparent message associated a coding key, then as a result it outputs associate encrypted message. The encryption/decryption algorithmic rule receives as input associate encrypted message and a coding key, then as a result it outputs the corresponding clear message.

C. Symmetric Cryptography

Also known as secret key cryptography. For this method, the coding key are often simply calculated from the encoding key, in apply it takes a similar. [2] Security in cruciform cryptography relies on the flexibility to stay the key secret between act parties. If the key's discovered the system is compromised. Their ability that each parties have access to the key key's one among the most drawbacks of cruciform cryptography as compared to uneven one.

D. Asymmetric Cryptography

Also referred to as public key cryptography. The principle of Functioning is as follows: every user encompasses a combine of keys, one personal key that he should keep secret, and therefore the alternative public key that he should build it on the market to the general public. If we tend to write with the general public key, solely the personal key will decipher and the other way around. it's much not possible (time and resources) to see e.g. the personal key knowing the general public one and the other way around. uneven cryptography may be utilized in coding, however compared to trigonal algorithms it's sometimes slower. it's in the main utilized in the key exchange procedures and in digital signature authentication tool through digital certificates. the general public key cryptography solves many issues that secret key cryptography doesn't succeed. many projected public key cryptographies primarily based solutions for a few security problems in VANETs are going to be mentioned later.

E. PKI, Digital Certificates and Timestamping

The management of personal and public keys for an outsized variety of users' needs the institution of a PKI (Public Key Infrastructure), that may be a set of computer code, hardware and procedures elements. [2] A PKI will give many security services, the foremost necessary is to be a trust third party between digital counterparts. PKI ensures that role through the certification authority (CA), therefore it signed, delivers associate in nursing carry on so far digital certificates that represent a digital ID for an entity. In fact, a certificate is associate in electronic file (can be hold on in several forms), that binds along a public key with associate in nursing identity with the guarantee of the certification authority. A certificate permits to manifest and sign (signing certificates) and additionally cipher messages (encryption certificates). Timestamping is additionally among the services that PKI will give. It certifies that an occasion send happens at a given time. The time stamping faces essentially to authentication and non-repudiation attacks in a very VANET context, many solutions e.g. propose the creation of a PKI associated with VANETs named VPKI (Vehicular Public Key Infrastructure) [6,13], and propose the utilization of digital certificates as a technique of fast authentication in a very conveyance network. This proposed resolution is mentioned later for a few connected attacks.

WE HAVE MENTIONED SOME IMPORTANT SOLUTIONS. PROVIDES THE COMPARISON AMONG ALL SOLUTIONS.

Table 1. Vanet Attacks and its Solutions

Serial No.	VANET ATTACKS	Safety Requirement	VANET Solutions	Technology
1	Denial of Service(DOS)	1. Availability 2. Authentication	Use bit commitment and signature primarily based authentication mechanisms that reduces the impact of virtually of DOS attacks	1.One Way Hash Function 2.Symmtric Cryptography
2	Greedy Black hole Gray hole Sinkhole Wormhole Malware Masquerading Spamming Tunneling	1.Availability 2.Authentication 3.Integrity 4.Confidentiality 5.Non-repudiation	For these attacks, cryptography doesn't supply real solutions, however bound urged actions will scale back black effects, like digital signature of package and sensors. Use trustworthy hardware that it's much not possible	---

			to vary existing protocols and values, except by approved	
3	Jamming	1.Availability	Switch the transmission and use the frequency hopping technique FHSS (Frequency Hopping Spread Spectrum) that involves scientific discipline algorithmic rules to get pseudo-random numbers for the hopping algorithm. This proposal needs a modification of the used customary that presently permits solely the OFDM	---
4	Sybil attack	1.Availability 2. Authentication	In the case of the presence of authentic and secure links with sure nodes, [14] proposes to scale back the impact of the Sybil attack by corroboratory unknown nodes with the strategy of secure location verification. For this methodology, [6] proposes the employment of approved certification	---

5	Routing Attack	1. Authentication	Safe and Efficient Ad hoc Distance Vector	1. Symmetric Cryptography 2. MAC
6	Eavesdropping	1. Confidentiality	Encrypt solely knowledge that has preponderating importance and that manipulation puts in risk the privacy of the motive force (positioning information, vehicle identification information.	---
7	Traffic analysis	1.Confidentiality	Same proposition as eavesdropping. Use algorithms like VIPER for V2I communication	---
8	Replay Attack	1.Authentication 2.Integrity	Use timestamping technique for packets that their replay is dangerous [8]. For this proposition, we have a tendency to encountered the matter of your time synchronization between entities.	1. Symmetric Cryptography 2.MAC
9	Node impersonation	1.Integrity 2.Authentication 3.Non-repudiation	Use variables MAC and IP informatics addresses for V2V and V2I communications • demonstrate via digital certificates [9]. • Strengthening the authentication	1.Cryptographic Certificate

			mechanism victimization distance bounding protocols supported cryptologic techniques like bit commitment and zero-knowledge.	
10	Man in the middle attack	1.Authentication 2.Integrity 3.Confidentiality	Use a powerful authentication technique like digital certificates and zero-knowledge	---
11	Information Disclosure	1.Privacy	Secure Message Transmission and Non-Disclosure Method	1. Asymmetric Cryptography
12	Timing attack	1. Availability	Use the timestamping mechanism for packets of delay-sensitive applications. For this proposition, we tend to encountered the matter of your time synchronization between the entities	---
13	False Warning	1. Authentication 2.MessageIntegrity 3. Nonrepudiation	Genuine and Authentic Routing for Ad hoc network	1.Cryptographic Certificate
14	Brute force	1.Confidentiality	Use sturdy encoding and key generation algorithms unbreakable	---

			among an inexpensive time period [8]. This prohibits access to info to people who aren't allowed.	
15	Resource Consumption	1. Availability 2. Authentication	Safe and Efficient Ad hoc Distance Vector	1.One Way Hash Function
16	Key and/or certificate Replication	1.Authentication 2.Confidentiality	Use certified and disposable keys. Check the validity of digital certificates in real time via CRL (Certificate Revocation List) [1], which represents a real hard problem in VANETs. Use cross certification between the different certification authorities involved in VANETs security scheme Use strong encryption and key generation algorithms unbreakable within a reasonable running time [8]. This prohibits access to information to those who are not allowed.	---
17	GPS spoofing/Position	1.Privacy 2.Authentication	Use bit commitment and	

	Faking		signature based mechanisms with positioning systems to accept only authentic location data	---

9. Conclusion

Vehicular Ad hoc Networks (VANETs) have become widespread in Intelligent Transportation Systems. They have been designed to supply road safety and services for passenger's comfort. Given their importance associated with the security of humans' lives, VANETs attract attackers and represent a favorites target for many kinds of attacks that consequences vary from negligible to severe. Therefore, securing VANETs poses an excellent challenge. During this paper, and when reviewing the assorted recent aspects of VANETs of art just like standardization, routing protocols, comes and applications, we tend to determine the existing security problems in VANETs and classify them from a cryptography purpose of read. Also, we studied and compare the assorted cryptography solutions that are on an individual basis planned for these attacks and judge their potency. Even a crucial interest has been given by the analysis to the topic, it's noteworthy that the utilization of recent ideas, together with homomorphic coding and ID-based cryptography alternative future works to hide the weaknesses of the prevailing schemes and adapt to the intrinsic options of conveyance communication. Thus, our analysis is one step nearer towards the planning and development of effective security schemes to support the protection of vital services supported by VANETs.

References

[1] J. M. de Fuentes, A. I. G. Tablas and A. Ribagorda, "Overview of Security issues in Vehicular Ad Hoc Networks", Handbook of Research on Mobility and Computing, (**2010).**
[2] M. N. Mejri, J. B. Othman, M. Hamdib, "Survey on VANET security challenges and possible cryptographic solutions", **(2014)**.
[3] X. Lin, "Security in Vehicular Ad Hoc Network", IEEE communications magazine, **(2008)**, pp. 88-95.
[4] R. S. Raw, M. Kumar and N. Singh, "Security Challenges, Issues and their Solutions for VANET", vol. 5, no. 2, **(2013)**, pp. 1-6.
[5] K. Mershad and H. Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks", vol. 62, no. 2, **(2013)**, pp.23-30.
[6] A. Burg, "Ad hoc network pecific attacks", Seminar Ad hoc Networking: Concepts, Applications, and Security, 2003, Technische Universitat Munchen, **(2003)**.
[7] M. Raya, "The Security of Vehicular Ad Hoc Networks", SASN'05, Alexandria, Verginia, USA, **(2005)**, pp. 11-21
[8] G. M. T. Abdalla, M. A. AbuRgheff and S. M. Senouci, "Current Trends in Vehicular Ad Hoc Networks", University of Plymouth, UK, **(2013).**
[9] L. Bariah, D. Shehada, E. Salahat and C. Y. Yeun, "Recent Advances in VANET Security: A Survey", Khalifa University, Abu Dhabi, **(2015).**
[10] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin and A. Hassan, "Vehicular ad hoc networks (VANETs): status, results, and challenges", Telecommun. Syst., vol. 50, no. 4, **(2012)**, pp. 217–241.
[11] A. Hamieh, J. Ben-Othman and L. Mokdad, "Detection of radio interference attacks in VANET", Global Telecommunications Conference, **(2009)**, pp. 1–5.
[12] S Balasubramani, S. K. Rani and K. Suja Rajeswari, "Review on Security Attacks and Mechanism in VANET and MANET",Vehicular Communications, vol. 5,no. 3, **(2016)**, pp. 35-45.
[13] G. Samara, W. A. H. Al-Salihy and R. Sures, "Security Analysis of Vehicular Ad Hoc Networks(VANET)", Universiti Sains Malaysia, **(2010).**
[14] S. V. Menezes and D. Hankerson, "Guide to elliptic curve cryptography", Springer Professional Computing Springer, New York, **(2004)**.
[15] P. Papadimitratos and Z. J. Haas, "Secure Data Transmission in Mobile Ad Hoc Network", ACM Workshop on Wireless Security, San Diego, CA, September, **(2003)**.

Authors

Kuldeep Kumar, he 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 Adhoc Networks and Cryptography.

Sandeep Kumar Arora, he 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 a member of IEEE and also the author of more than one dozen research papers indexed in S.