Eurasian Journal of Analytical Chemistry
ISSN: 1306-3057 OPEN ACCESS 2018 13 (SP): 359-368

An Extensive Analysis of the Security Challenges of VANET (V2V-Communication) and its Possible Solutions

Aaryesh Kumar, Nimish Pathak, Dr.C. Vijayakumaran

Received 08 November 2018 ▪ Revised: 30 November 2018 ▪ Accepted: 06 December 2018

Abstract: Vehicle-to-vehicle communication (V2V) is the process of transmitting data wirelessly between vehicles. By relaying the information about location and speed data between vehicles is via an ad hoc network is the primary aim of V2V communication. This communication takes place over an ADHOC mesh.V2V communication is thought to be the better alternative for the current vehicular(original equipment manufacturer: OEM) embedded systems which have features like adaptive cruise control, rear parking sonar and backup camera because the V2V technology enables an ubiquitous 360-degree awareness of surrounding threats. With the further advancement of the v2v communication many security flaws were found. The best way to analyze these flaws would be through a bi-directionally coupled simulation environment made of OMNET/SUMO, ns2 /SUMO, etc. Many possible attacks like botnet, GHOST, congestion etc. are being used to exploit the system every day, which can be simulated and studied in the simulated environment. In the starting we discuss about the general VANET characteristics, in the second part we discuss about all the existing flaws with which the system can be attacked and in the third and last part we discuss about the solutions to those problems and how the present conditions can be improved through the implementation.

Keywords/ Abbreviations: PKI: Public Key Infrastructure, DOS: Denial of Service, MAC: Message Authentication Code, ARAN: Authenticated Routing for Ad-hoc network, SEAD: Secure and Efficient Ad-hoc Distance Vector routing protocol cryptographic, CA: Certificate Authority, TFD: Time Frequency Distribution, RSU: Road Side Unit, CRL: Certificate Revocation List, OEM: Original Equipment Manager, OBU: Onboard Units

INTRODUCTION

Autonomous vehicles platooning has been a key subject of importance in the 21st century because of its ability to benefit road transportation, improving traffic efficiency, enhancing road safety and reducing the fuel consumption of the vehicles. A Special class of ad-hoc routing based network known as VANET i.e. vehicular ad hoc network has been of keen significance in road transportation and security applications. Registration and management of the individual identities of the driver are handled by the On-Board units (OBUs) and Roadside units (RSUs).The RSUs have been installed to gather information and the vehicles that are handled by the VANET are primarily installed with the OBU's. Such vehicles are able to traverse freely on a specified modular road network, and are able to communicate with each other or with RSU's and other identified authorities. The communication channel could be either a single or multi-hop mode of data transmission using the DSRC (Dedicated Short Range Communication) on V2V or V2X.V2V communication is technically a form a large-scale distributed embedded systems. In recent future most of the vehicles are subjected to be equipped with wireless on board units GPS (Global Positioning System),

Aaryesh Kumar, Dept. of Computer Science Engineering, SRM Institute of Science and Technology, Chennai, India. E-mail: aaryeshkumar_su@srmuniv.edu.in

Nimish Pathak, Dept. of Computer Science Engineering, SRM Institute of Science and Technology, Chennai, India. E-mail: nimishpathak_vi@srmuniv.edu.in

Dr.C. Vijayakumaran, Associate Professor, Dept. of Computer Science Engineering, SRM Institute of Science and Technology, Chennai, India. E-mail: vijayakumaran.c@ktr.srmuniv.ac.in

EDR (Event Data Recorder), (OBU), and sensors (radio-detection units RADAR and LIDAR/LADAR) as shown in Fig.1.Traffic congestion status is measured using such equipments and other statistical data is also recorded and then automatically necessary actions are taken in the vehicle itself and the information is relayed to other vehicles and RSU's.

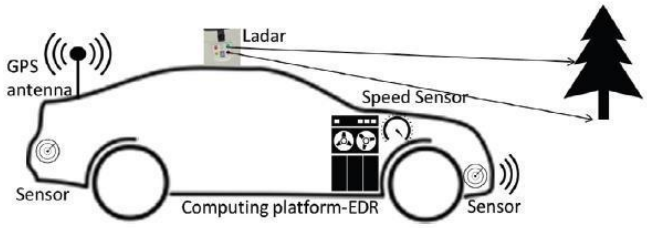


Figure1: Future vehicle design

The system which exists in the present day works more like a WAN or Internet where each car on the network acts like a computer. In today's world almost all cars are equipped with a form of digital circuit inside it with CPUs to take certain important decisions (OBU) for e.g. when the car speeds up your seat belts get tighter or when the car detects that it's raining it automatically starts the wiper etc. The car communicates to each other like how computers communicate to each other on a network and find a solution to make the whole journey more efficient and safe.

VANET CHARACTERISTICS AND SECURITY LIMITATIONS

VANET basic characteristics

The very basic forms of communications can be seen in the figure 2 where u have v2x (x=I, v) and i2v type of communications.

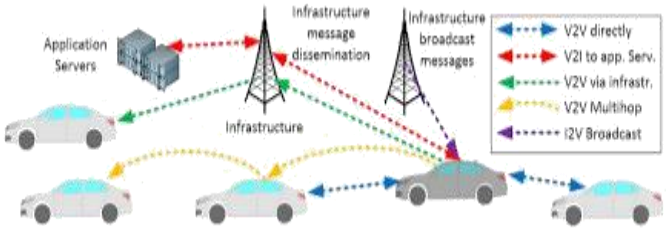


Figure 2: Basic infrastructure

These vehicular-ad hoc network uses 802.11 IEEE standard protocols, 4G/LTE, 5G/LTE for WLANS.

By studying the various documents [1][2][3][4][5] we can generalize v2v into two basic things for characterization

i) *Network topology and the communication mode and* ii) *Vehicles and drivers.*

i. VANET attributes related to Network-Topology and Communication-Mode*:*
   - Large Scalable networks: As discussed VANET is a form of WAN and can be implemented for large cities/multiple cities or even a country as a whole. Thus requires regular and immense management of security protocols.
   - Wireless communication*:* The vehicles (nodes in a WAN) are connected through wireless channel and exchange large amount of data thus requires highly-secured network.
   - High mobility and rapidly changing network topology: Nodes are able to move at a very high speed and more so they move randomly thus it becomes burdensome to predict their ideal positions and the topology of the specific network. It leads to *disconnection issues and impossibility of handshake.*

ii. VANET Characteristics related to Drivers and Vehicles:
   - *High CPU power and extra processing energy:* The vehicles are equipped with powerful OBUs which have powerful CPUs and memory just like a computer and have batteries on which the system runs the highly complex cryptographic calculations.
   - *Calculating time and position*: GPS is a common installment on numerous vehicles as many applications rely on position and geographical addressing. A non-tamper able system ensures that the location of nodes is kept private from the attacker.
   - *The nature of the participants:* A larger proportion of drivers are considered to be good and law abiding citizens and are regular users of the service.

- *Prevailing law enforcement agencies:* The malicious attacker can be caught by the law enforcement services.
- *Central registration with regular maintenance and inspection*: vehicles have a unique id (license plate). Vehicles go through periodic maintenance check for software/hardware and firmware updates. In PKC (Public key Cryptography), maintenance is for updating Keys, Certificates and updating CRL with fresh CRL (Certificate Revocation List).

VANET Security Challenges and Some Limitations

On the very basic level it is very similar to a computer network where u have computer/cars communicating with each other and like all computer networks this system can be exploited in various forms. In VANET, security must guarantee that the exchanged messages are not maliciously modified by the attackers, also the driver's system should notify the traffic environment-parameters correctly within the given time period.

i. Some of the Basic form of security challenges are:
- *The Network size*: The large geographical area, the high mobility, the dynamic nature of the topology, the short connection duration and the frequent disconnections is a major security issue .The size of the network is large and grows uncontrollably but it is scalable in nature and continues to grow without any global authority to govern its standards.
- *The information verification*: Trust is one of the core requirements of the system as there is continuous exchange of data between nodes and central systems, there should be a proper system to verify the authenticity and integrity of the data. *Trustworthiness of the data* is more useful compared to that of the nodes transmitting it.
- *Distribution of keys*: Security mechanisms uses cryptographic keys, which make their secure-distribution highly important.
- *The Forwarding algorithms*: used to transfer the data in the best manner to all the nodes in the system, whether you are using a UDP broadcast communication (v2v based on configured hops) or communication with a central authority to get the required road conditions, weather factors etc.

ii. Some of the limitations are:
- *Probability involved in algorithms*: Every algorithm's probability has some error which can affect the outcome and people's life.
- *Environmental influence:* due to the magnetic waves, the channel in which the data exchange is going on gets affected and it would lead to loss of data, handshake errors etc.

The above mentioned limitations can be better handled in a proper manner if we implement the required properties properly

ATTACK'S VS ATTACKER'S

In this section we will discuss on the different types of attacks done on the different levels of the v2v infrastructure and also the types of attackers. Many researchers in [2][3][5][6][7][8][9] investigated the attacks in VANETs and came to certain conclusions on it. By classifying the attacks into categories we can establish better control on it. The characterization of the attacks can be done as follows basically into four groups. (1) Threat to the wireless interface of the driver, (2) Threats related to the hardware and software, (3) threats to the sensors of the vehicles and

Threats to the physical infrastructure of CA's (or vehicle manufacturer). The following section presents us with a basic idea of such threats:

A. ATTACK'S

1. Threats to the Wireless Interface of the driver*:*

i. Identity and geographical position tracking (Location-time Tracking): The driver is breached by the attacker in order to track and gain important authentication information from the individual which could be used for malicious activity. For example, some of the rental car companies use their vehicular tracking system to keep records of their customer's movement for various malicious activities, which is a major breach of the privacy of the user.

ii. DoS(Denial of service)**:** Resources and the various services of the v2v are made unavailable to the user network by a malicious attacker. This can take place by either blocking the physical channel or by "Sleep Deprivation **DoS**"

iii. DDoS (Distributed Denial of Service): DOS attacks occurring from various geographical location to the network are considered to be a form of DDOS attacks. It can make the channel unavailable or drain out the power through sleep deprivation based DDos attacks.

iv. Sybil Attack: In this attack a similar identity is issued to multiple vehicles travelling on road hence an illusion is presented to other vehicles when a wrong message is sent to the vehicles ultimately benefitting the attacker.

v. Malware Infection**:** a node/attacker inside the network (in a car) transmits spam messages into the network to increase latency and bandwidth consumption of the network. Due to the lack of necessary security-controls in the infrastructure and centralized administration it becomes cumbersome to control such kind of attacks. Spam messages may be disseminated by the attacker to a group of multiple users, and these messages are rendered useless by the users similar to advertisement messages, it may contain certain malwares in it which could trigger malfunction behavior in the system. For e.g. Broadcasting RAIN weather messages over the network to different cars would trigger the windshield unnecessarily and cause driving nuisance to the driver. It may sometimes contain malicious data in it which could infect the OBUs of the vehicles with viruses and trojans.

vi. Man in the Middle Attack (MiM): While communication is established between two vehicles a malicious node is able to listen to the data exchange and after gaining certain authentication information required for communication it itself communicates with each of them and presents false information to each other and causing various nuisance to the driver by sending unnecessary messages.

vii. Brute force Attack: the attacker tries to get user-personal information such as password or PIN or to decrypt the data, or to validate network security by the help of trial and error based algorithms which directly attacks the authentication part of the networking system. It includes algorithms like rainbow-table based attacks or basic dictionary attacks to crack into the system.

viii. Black Hole Attack: Shortest path algorithms are used by the network to send data, AODV protocol is such a protocol. In this attack the attacker after getting into the network pertains to be the part of the shortest route to each vehicle by broadcasting wrong location information due to which the vehicles get tricked into transmitting the messages to them which the attacker after obtaining them obtains the important information in them and later on drops the packet, leading to the failure of information exchange between particular nodes.

2. Threats related to Hardware and Software

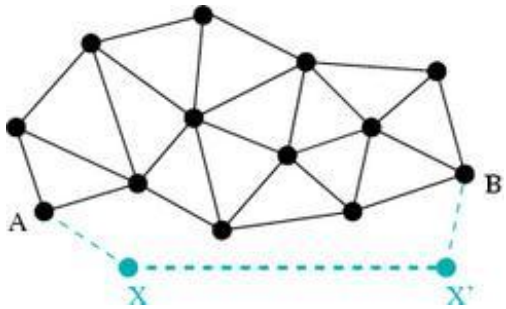
Other than the threats presented like Sybil attack, DoS, Malware, spam, Brute force and Man in middle mentioned above in sub-section (1), we can list:

i. Message Suppression or alteration: By understanding the software and hardware used in the OBUs and RSUs, one can trigger certain malfunction in them. By exploiting certain messages either by suppressing them or altering them or even delaying them could trigger unnecessary response from the software used in the RSUs and OBUs. The hardware can also be exploited by altering various messages. Thus to avoid this the only way is to authenticate the message being transferred and coming up with come mechanism which would make the message opening/capturing difficult for attackers

ii. Assuming the identity of a node (Spoofing or Impersonation or Masquerade): The attacker impersonates as a specific node after getting into the network and this procedure is known as the black hole problem. To gain access to restricted messages and to avail privileges of the user profile the attacker declares itself to be a good/normal node as the culprit gains unauthorized access, this is a type of replay attack where attacker tries to imitate a legitimate user/RSU by using earlier generated/used frames from the communication channel in the new connections which it establishes with various nodes/vehicles. There are various forms of spoofing which exploits the software vulnerabilities to gain certain kind of privileges in the network. By understanding the hardware and software vulnerabilities one can exploit it by spoofing in the correct manner.

iii. Tampering with the Hardware of the vehicle: This is one of the major breaches as the employees fiddle with the hardware in a malicious during the yearly maintenance of the vehicle, in the vehicle manufacturers service centers, it is generally done to either to get or put special data into the OBUs of the car , for *e.g.* A Trojan can be installed on the main CPU board of the car to compromise the control of the driver on the car, one can trigger brake clutch, almost all the things through the circuit of the car. We have to understand a car as a form of computer on the network which can be infected in the similar manner with viruses, which compromises the user's control over his/her system, allowing the attacker to control the car. Some worst cases could be that he could power-off the car on a high speed national highway. Not only manufacturer's employee but a lot of hackers know how to install such viruses onto the circuit board of a car.

iv. Wormhole attack: Overhearing data; it is almost a form of black hole attack where the malicious node (insider node generally) impersonates to be the closest node and tunnels the message to some other part of the network causing various software malfunctions on the car like drop of important authentication messages etc. As you can see in the figure X' node takes in the data by acting as the nearest node and then redirects it to some other point. (form of routing attacks) vehicles. Hence the neighboring vehicles receive the message after a delayed period or sometimes after the particular event has occurred, for which the information was generated.



3. Threats to the sensors of the vehicle:

Other than the GPS spoofing as mentioned earlier in section (2), some of the other attacks are:

i. Illusion attack: The sensors reading of the vehicle are purposefully deceived by the attacker in order to perceive wrongful data calibrations, thus the broadcasted messages to the neighbors are subjected to failure and hence leads to attainment of wrongful information by the user. There are various machines which can be used to make and broadcast sensor readings.

ii. Jamming attack: The radio frequencies used by VANET nodes for sensory purpose are being jammed, sensors for moisture readings are jammed, the sensors present behind the car for parking are sometimes fiddled with, sensors for objects in front of the car are tampered with etc. are some of the malicious things done by the attacker to cause loss of important data.

4. Threats against the physical infrastructure: There are various common attacks which can be done to the CAs, RSUs or car manufacturers which can exploit the network.

1. Unauthorized access: malicious content tries to gain access to the network services of the CAs or RSU by the various network attacks, spoofing attacks, or in some cases in-person spoofing attacks to gain access to the system without having the proper security credentials and privileges. This causes accidents, damage or spying of confidential data.

B. ATTACKER'S

A common interest of researches has been VANET attackers as mentioned in [2][3][7][10].Depending upon their actions and targets a number of canonical names have been listed below:

1. Greedy/Selfish driver: Such a driver is able redirect the traffic by enabling attacks for self-benefit or by causing road congestions by relaying accident messages, or else freeing the road way by sending false messages depending upon the need.
2. Malicious attackers/Pranksters: he/she has specific targets, or may cause malfunction and har to the VANET application by Dos, DDos etc. attacks.
3. Eavesdropper/Listener: Information about varied resources is gathered by the attacker for the purpose of self-gain, or for further investigating the network for security loops.
4. People working inside: Malicious employee might succumb to usage of firmware update or key distribution to cause hardware tampering. They are generally.
5. Grey-hole attack: A misleading malicious node programmed by the attacker causes the network to transfer the data packet forward to other hosts but occasionally this affected node retires for a while and conforms to its normal behavior. Basically it performs a black hole attack or a wormhole attack but switches its behavior from time to time to confuse the software's security protocols.(form of routing attacks, which are triggered to exploit the network by exploiting certain vulnerabilities in the message processing and transmitting power of the software/hardware used in the VANET).
6. Cheating with position and timestamp information (GPS spoofing): False positions and timestamps of the location are generated by the vehicles causing various kinds of accidents, by giving rise to falsified GPS locations one can cause wrong messages to be delivered to the driver .
7. Timing attack: A delay is inserted before forwarding the received messages by addition of invalid timeslots created by the malicious responsible for leaking the infrastructure

information to black hat people leading to unnecessary vulnerability exploitation of the system and also causing harm.

The attackers are classified into:

- *Insider and outsider*: An authenticated user represents as an insider of the network whereas the outside user has limited capacity to attack because of various unauthenticated status restricted access to various service, granted to him.
- *Active vs. passive*: Signals or packets are generated by an active attacker whereas the passive one only listens in the network.
- *Local vs. extended*: Attacking a particular node/driver or a particular RSU is the primary aim of a local attacker whereas the extended attacker works by widening his scope by controlling several entities which are scattered across the network.

Table 1: classifying the attacks based on the four categories of threats

Threats to the Interfaces	Mode of Communication	The name of the attack
Wireless interface of the vehicle	V2V	- Sybil - Malware infection -Black hole, -Greyhole. - Location Tracking - DoS, DDoS - Man in middle - Brute force
Hardware and Software	V2V,V2I	Alteration/ Fabrication. - Replay - Masquerade/spoofing - Malware infection - Man in middle - Brute force V2V,V2I DoS - Spoofing and Forgery. - Cheating with position info (GPS spoofing). - Sybil - Tampering hardware of the vehicle - Routing attacks: Black hole attack, wormhole attack and Greyhole attack.
Sensors of the Vehicle	V2V	- Illusion attack - Jamming attack Cheating with position info(GPS spoofing)
Infrastructure e	V2V, V2I	- Tampering hardware of the Vehicle. - DoS, DDoS - Unauthorized access to the Facilities.

The above table helps us classify these attacks into the 4 categories and tells us about the communication mode (V2V or V2I or both) which is being compromised.

SOME FAMOUS SECURITY INFRASTRUCTURES BEING USED

The underlying foundation that is responsible for the framework of the system is known as an *infrastructure.*

It is a key component in development of the Security architecture hence provide an efficient security design. It delineates the utmost potential risks that may be specific to certain environment and enables application of security control when required.

Here we describe PKI i.e. public key infrastructure because of its immense popularity.

A. Public key Infrastructure

Public key infrastructure is one of the most common form of security enabled on vast WAN type of networks, it helps in the identification and distribution of public encryption keys. Data is exchanged in a secure fashion over the routing networks which helps to verify the personal identities of the other party. PKI comprises of software, hardware, various policies and standards. These in unison are responsible for the revocation, administration, distribution and creation of keys and digital certificates used in the security infrastructure. The components included in the PKI are as follows:

- A trustworthy root parameter, called a Root certificate authority (CA), is considered to be a potential trusted parameter and is capable of providing services to authenticate the identities of the entities.
- A subordinate CA which holds the duty of registrations and is, certified by a root CA. The root permits the use of certificates for specific purposes. Its primary purpose is the protection of the root CA. Attacks can be checked before reaching the root CA as are first supposed to pass through the subordinate CA. It can be accessed by both root and subordinate CA.
- Issued certificated and private keys are present on each vehicle in the form of a 'certificate store'. This is what the basic idea for the PKI presents, the high level of security architecture is used by adding more layers of authentication In Europe and USA, they have built their own VANET-security architecture using PKI.In Europe(EU) there exists a different PKI architecture as shown by ETSI in [12] which defines the important security aspects for intelligent transportation system .In USA, the VSC-A (Vehicle Safety Communications- Applications) authority, has considered the usage of NHTSA (National Highway Traffic Safety Administration) [11] with its security architecture for VANET.

MITIGATING THE ATTACKS

Many specialists have researched on methods for tackling the attacks mentioned in the above and they have been described below;

1. Against the threats to the wireless interface of the driver:

i. Attack encompassing Tracking, Eavesdropping and Traffic analysis :

The only solution for this is to maintain the privacy of the driver, there have been a lot of cures developed to overall maintain the privacy of the driver within the network, the true identity of the vehicle is kept hidden with the use of a set of anonymous keys which are constantly or variably changing with time according to the driving speed of the vehicle or through the use of pseudonyms [15] or either using asset of group signatures should also be used as mentioned in [11][13][14], which are some certain ways to maintain privacy.

The researchers in [3] suggests the pre-loading of anonymous keys in the TPD (tamper proof device) which are recognized by the regional certificate authority and can be detected back to Electronic License Plate authorities (ELP).At the very basic idea we have to maintain a pseudo information which cannot be tracked and should be changing according to the situations i.e. should use the current driving parameters as input to create different keys so that one can maintain his identity with the system but also not get recognized by the attackers.

ii. For DOS attack:

It can be decreased to some extent by using the digital signature method [16], to ensure secure and reliable message communication and authentication Digital signatures are used. It is an active security measure that is attained by digitally signing the data [1], all in all it takes time for the attacker to penetrate a system running on customized hardware which is using non- public protocols. In Dos, DDos attacks the major solutions aside from adding different digital signatures and symmetric keys would be to identify the attacker based on certain algorithms which could rule out the attacker form the network, which is shown through a trust model proposed in [17] that ensures trustworthiness of the vehicle by calculating, the trust metric values of nodes participating in VANET. By calculating the number of

accepted and received messages it calculates the trust value which is used to rule out the attacker from the network through the help of a fuzzy based approach to identify malicious nodes, and this information is utilized by sending a direct request to the RSU or CA and is driven to action when the threshold (which is the case of DDoS, Dos attacks) is exceeded.

iii. For Malware and Spamming:

The only way to avoid malware implantation would be to have digital signatures involved in every hardware and software part of your car and to get it updated/checked on regular bases. Avoid the use of non-trusted/pirated/customized software, only use trusted hardware as it makes it very difficult to replace the existing protocols and values, monitor data excluding authorized nodes. Manufacturing companies need to regularly check the software being installed on the car for vulnerabilities, and have a systemized check on the employees to avoid malicious employees adding malware to the vehicle.

iv. Sybil attacks

Sybil attack basically forges a vehicle identity in multiple places, the only way to avoid this is to maintain a TFD – database which will store node information and rule out identical nodes, u can use the location attribute to rule out the fake nodes on the network, in [3], Sybil attacks are prevented by making use of location and various other information of the transmitting node and coming to a logical conclusion whether the information presented by it is logically correct or not. Messages are received by vehicles and corresponding certificate are examined along with its, life time and location. If it is correct logically then the vehicle accepts the message, or else it informs the nearest certificate authority. The other way is to make a temporary changing certificate system which would give the authenticity of a node i.e. A Central Validation Authority is deployed (VA), which validates entities in real time directly or indirectly using temporary Certificates [18].

v. Man in the middle attacks

The only way to avoid others from listening to the v2v communication or even letting them access the tunnel for v2v communication would be to use strong authentication methods like digital certificates which use strong digital signatures [7] and establishing connections between nodes via secure keys or encrypting the data being transmitted.

2. Attacks pertaining to hardware and software

i. Message tampering

There are many ways, one way to avoid message tampering would be to use some form of group signatures [13], which not only helps to maintain your privacy but also helps in maintaining the authenticity, integrity, and accountability of the nodes on the network in which tampered messages for unauthorized node are detected by the use of probability-based signature verification scheme/algorithm, such a method is usually called data correlation. Other way would be to use the similarity algorithm [20] which propose to use a trust management framework and a reputation management framework whose values are calculated via the similarity algorithm and trust of messages content value between vehicles to help driver to believe or not to believe the received message. By calculating the trust value if it surpasses a threshold they take appropriate action and rebroadcast the message, Otherwise they drop it and report the activity to the CA or the RSU.

ii. For spoofing attacks

One of the quintessential ways to prevent the spoofing attacks, would be to maintain the identity of the vehicles in the network and removing the nodes that project a malicious identity as we have discussed above but if at the end the message is somehow being tampered and deployed in the network then you need to use the advanced form of vehicular PKI (VPKI) as used by the EU and VSC-A for authenticating the processes and message exchange between vehicles.

VPKI possesses a group of trusted third parties such as, one certificate authority in each city/state or country, with authorized certificate authorities in the particular area, certificate authorities act mutually and can be recognized by the vehicles in different countries or areas with the help of data sharing among them.

A set of private and public keys are issued for each and every vehicle along with the use of temporary or short-time based certificates with anonymous keys which are continuously changing according to the driver's speed [19][15].

Electronic License Plates on the vehicles and their corresponding pseudonyms can only be differentiated by legal authorities so a circulated signed message along with its certificate is authenticated via a certificate authority and is legislated as vehicles passes through a certain route. Hence a secure channel of communication is established between authenticated users.

iii. Resistance offered against routing attacks (Black hole, Greyhole and Wormhole):

Soft wares and the sensors make us of the digital signatures to avoid data tampering or being accessed by the attacker, and help to rule out fake messages being broadcasted on the network. In ARAN (Authenticated Routing for Ad-hoc network and SEAD (Secure and Efficient Ad-hoc Distance Vector routing protocol cryptographic) [2],symmetric cryptography cryptographic certificate, one way hash function and MAC (Message Authentication Code) are used respectively to solve these issues which involve at the very core spoofing identity to get access to the message on the network. In [7], an effective technique is discussed to tackle the Wormhole attack and the various other routing attacks in the network with the understanding of HEAP. It is a protocol based on the AODV algorithm and makes us of geographical criterias to limit the travelled distance from source to destination, if the limit is surpassed then the data/packet is dropped. The HEAP protocol basically works on ruling out improper locations or spoofed locations and is mostly used to stop Sybil attacks and similarly uses fuzzy based approach to calculate the authenticity of the message from the various parameters of the message.

3. Attacks on the vehicular sensors

i. Against jamming attacks

The only solution to this problem would be to switch between the available wireless technologies in the vehicle to continue monitoring the environment if one type of sensors are blocked like suggested by the authors in [21].

4. Attacks against the Physical Infrastructure

i. For unauthorized access:

At the very core, the only way to avoid unauthorized access to CAs and RSUs network would be by implementing proper identification of the individual (but also maintaining the drivers privacy at the same time) through the help of TFD and the pseudo keys in it which can help authenticate users in the network and administrators separately at the same time [3] and also by implementing proper digital certificates with digital signatures and cryptographic symmetric methods to encrypt the network so that only authorized users with the correct digital signatures can access it. The other part of this problem is that instead of virtually attacking the network they try to physically attack it by visiting the service in the real world and tampering with it which can only be avoided by implementing proper security officials to maintain a watch over the area for illegal access to the facilities of CAs and OBUs.

CONCLUSION

With the advancement in transportation technology the risks are also increasing with it, stats show that there had been more than 11 million accidents this year and people die or get involved in accidents more now, this shows that although we have developed the technology but have not made it more secure as (the increase in accidents per year show that).Due to increasing number of accidents on the roads users want safety and security on the most common medium of travel and a strict procedure to check the misbehavior and malicious activities of others that may cause harm to fellow travelers and also to the collateral as a whole. Certain preventive measures are to be enabled in near future and more efforts are undertaken by authorities to pertain a secure VANET environment.

REFERENCES

[1] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil, “Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions”, published in Communications Surveys & Tutorials, IEEE (Volume:13 , Issue: 4), pages 584-616, July 2011.

[2] Gh. Samara, W.A.H. Al-Salihy, R. Sures, “Security analysis of of Vehicular Ad Hoc Networks (VANET)”, published in Network Applications Protocols and Services (NETAPPS), **2010** Second International Conference on, pages 55-60, IEEE.

[3] M.N. Mejri, J. Ben-Othman, M. Hamdi, “Survey on VANET security challenges and possible cryptographic solutions”, Vehicular Communications 1 pages 53–66, 2014.

[4] N.K. Chauley, “Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study”, International Journal of Security and Its Applications vol.10, No.5 pp.261-274, 2016.

[5] B. Mokhtar, M.Azab, “Survey on Security Issues in Vehicular Ad Hoc Networks”, Alexandria Engineering Journal, 54, 115-1126.

[6] K. Lim, D.Manivannan, “An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks”, Vehicular Communications 4, p 30-37, 2016.

[7] V. Hoa LA, A. CAVALLI, “Security Attacks and Solutions in Vehicular ad hoc networks: a survey”, International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.

[8] A.Y. Dak, S. Yahya, M. Kassim, “A Literature Survey on Security Challenges in VANETs”, published in International Journal of Computer Theory and Engineering, Vol. 4, No. 6, December 2012.

[9] M. Raya, A. Aziz, J.P. Hubaux, “Efficient Secure Aggregation in VANETs”, Proceeding VANET '06 Proceedings of the 3rd international workshop on Vehicular ad hoc networks, pages 67-75.

[10] M. Raya, J.P. Hubaux , “The Security of Vehicular Ad Hoc Networks”, SASN’05 Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, November 7, 2005, Alexandria, Virginia, USA, pages 11-21.

[11] W. Whyte, A. Weimerskirch, V. Kumar, T. Hehn, “A Security Credential Management System for V2V Communications”, IEEE Vehicular Networking Conference, 2013.

[12] ETSI TS 102 940 V1.1.1- ITS - Communications security architecture and security management.

[13] J. Guo, J.P. Baugh, Sh. Wang, “ A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework”, Published in CD-ROM Proceedings of the Mobile Networking for Vehicular Environments (MOVE) workshop in conjunction with IEEE INFOCOM, Alaska, May 2007.

[14] F.M. Salem, M.H. Ibrahim, I. Ibrahim, “Non-Interactive Authentication Scheme Providing Privacy among Drivers in Vehicle-to-Vehicle Networks”, Sixth International Conference on Networking and Services, 2010. [15]ETSI TR 102 893 V1.1.1- ITS- Security- Threat, Vulnerability and Risk Analysis.

[15] M. Raya, J.P. Hubaux, “The Security of Vehicular Ad Hoc Networks”, SASN’05 Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, November 7, 2005, Alexandria, Virginia, USA, pages 11-21.

[16] H. Hasrouny, C. Bassil, A. Samhat, A. Laouiti, “Security Risk Analysis of a Trust model for Secure Group Leader-based communication in VANET”, Second International Workshop on Vehicular Adhoc Networks for Smart Cities, IWVSC'2016.

[17] M.S. Al-kahtani, “Survey on security attacks in vehicular ad hoc networks (VANETs)”, in: 6th International Conference on Signal Processing and communication Systems (ICSPCS), IEEE, pp. 1–9, 2012.

[18] R.Rajadurai, N.Jayalakshmi, “Vehicular network: properties, structure, challenges, attacks, solution for improving scalability and security”, International Journal of Advance Research, IJOAR .org, Volume 1, Issue 3, March 2013.

[19] P. Caballero-Gil, “Security issues in VANET”, available: http://cdn.intechopen.com/pdfs-wm/12879.pdf, 2011.

[20] R. Engoulou, « Securisation des vanets par reputation des noeuds », thesis report, Ecole Poly technique de Montreal, 2013.