Journal of Physics: Conference Series **1427** (2020) 012015 doi:10.1088/1742-6596/1427/1/012015

Security of Vehicular Ad-Hoc Networks (VANET): A survey

Zehra Afzal, Manoj Kumar
Department of Computer Science and Engineering, SMVD University, Katra (J&K), India
[1]18mms014@smvdu.ac.in, [2]vermamk@gmail.com

Abstract: In the previous couple of years, various types of researchers concentrate on Vehicular Ad-hoc networks (VANET) field due to various facilities it provides. VANET a subgroup of mobile ad-hoc network (MANET), refers to a group of intelligent nodes i.e. (vehicles) on the road. These intelligent vehicles interact with one other or with the road side unit (RSU) for providing safer roads and a more efficient driving experience and providing security against attackers. In VANET messages are conveyed in an open wireless channels Security is therefore the most concerning issue in VANET. In this paper several types of the security issues, requirements, attacks, attackers in VANET have been described and some recent solutions to solve the security problems with their advantages and disadvantages have been discussed.

1. Introduction

Vehicular ad-hoc network (VANET) is also termed as network on wheels that provides interaction between mobile nodes [1, 16]. This network is a special type of mobile ad-hoc network where nodes are self sustain and interact with each other in an infrastructure less environment [2]. In recent years Vehicular ad hoc networks i.e. (VANETs) had gained interest due to the large number of Traffic accidents, road congestion, fuel consumption, and environmental pollution that have caused serious issues. Accidents due to these vehicles is a constant problem in progressed and progressing countries both that had resulted an immense loss in life and property. Therefore to make the journey secure, adequate, and entertaining and to minimize these issues, Intelligent Transportation System i.e. (ITS) introduced vehicular networks to design a safe and sound infrastructure for moving vehicles [19].

Vehicular ad-hoc network focus on providing valuable traffic management and safety of passengers, while offering convenience and entertainment for drivers and passengers all through their journey [7].In VANETs, communication is carried out by exchanging messages using Vehicle to Vehicle (V2V) and Vehicle to Roadside unit (V2I) communications.

Vehicles in VANET interact with other moving vehicles with the help of On board Units (OBUs) by constructing Mobile ad-hoc Networks (MANETs) that allow wireless interaction in an exclusively distributed manner and they can interact with Road-side Units (RSUs) with the help of infrastructures. The protocol used by VANET for Dedicated-short range-communications (DSRC) is Wireless Access communication in Vehicular Environment (WAVE) operating in 5.9GHz frequency band and is based on IEEE 802.11p standard. Communication in VANET can be categorized into four types [20].

In vehicle communication, this type of communication refers to in vehicle discipline and is more significant and important in research area of VANET. This type of communication system i.e. In vehicle communication system can track down a vehicle's performance and particularly exhaustion and laziness of a driver, which is severe for the driver and safety of public.

Vehicle to vehicle (V2V): this type of interaction i.e. vehicle to vehicle provides a platform for the drivers to send warning messages and share information to each other, so as to widen assistance of drivers.

Vehicle to roadside unit (V2I): This type of interaction is other important research area in VANETs that provides actual traffic and weather updates for drivers and keeps an eye on surrounding environment.

Vehicle-to-broadband cloud (V2B): in this type of communication the internet may include more traffic information and data, thus communication of this will be useful for assisting active drivers and keeping track of vehicles.

Vehicular ad-hoc network (VANET) focus is to improve the flow of traffic for assuring safe drive and thus reducing the traffic accidents which is solved by delivering rightful information to the drivers or to the communicating nodes. Modification of any type to this critical time information may advance to failure of system that may affect to safety of people on the road. Thus, in order to secure its smooth and effortless interactions, this critical information must be secured and hence security is on the top vision of research in VANET [24].

This paper presents a view about VANET characteristics, applications, security requirements and explores challenges in security of the VANET as well as the current solutions to provide security in VANET in an extensive mode. The rest of this paper is organized as follows: Section2expands VANET characteristics and applications. Section3 details the security in VANET. Section4 presents the attacker model. Section 5presents the proposed solutions and in section 6 this paper is concluded.

2. Characteristics and applications of VANET:

2.1 Characteristics of VANET: VANET is a wireless network with fixed and mobile nodes communicating with each other. Such system has certain characteristics such as frequent disconnections, No power constraints, and dynamic topology [3, 21].

Compared to the MANET, VANET has relatively higher mobility. In VANET, vehicles move randomly within the network and their movement is constrained to the network topology. Due to the high node mobility, VANET topology is dynamic and unpredictable [8]. Following are the certain main characteristics of VANET:

- Predictive Mobility.
- Dynamic Topology.
- No power constraints.
- Variable network density.
- Large scale network.
- High computational ability.

Table 1 : VANET characteristics

Characteristics	**Description**
Predictive mobility	In VANET here nodes move in a random fashion so it differs from other type of ad-hoc networks because vehicles are stiff by the requirements of vehicular network to obey the signs of road , traffic regulations and to reply to another vehicles on the road [3].
Dynamic topology	Due to the high mobility topology of the network alters fast, the durations of the communications are short and density of nodes varies extensively [8].
No power constraints:	Unlike in MANETs power is not a serious issue in vehicular networks, because nodes in this network are provided with the ability of continuous Power transmission to the OBU with the help of Battery with long life [6].
Variable Network density:	In VANET network density is not same in vehicular networks .it can be very high in dense areas i.e. in traffic jam situations and can be very low in case of urban areas due to low traffic so network density is variable in VANET [8].
Large scale network	The network in vehicular ad-hoc networks is scalable .A large numbers of new nodes can be added to this network [3]
High computational ability:	A very large no of resources such as processors, huge memory GPS are equipped by nodes in vehicular communication. Processing capacity of network is increased with the of vehicular communication [6].

2.2 Applications of VANET: Vehicular ad-hoc network (VANET) allows the evolution of a numerous applications and provides a huge range of messages to drivers and passengers travelling on the road [20]. Combining the on-board devices with the interface of a network, sensors of several type and GPS receivers, provides the capability to gather, compute and disperse messages in vehicles about themselves and the surrounding environment to the other communicating nodes that has led to improvement of road safety and the comfort of passengers. These Applications of Vehicular network are divided into following two categories [21]:

- Comfort/entertainment applications
- Safety applications

.

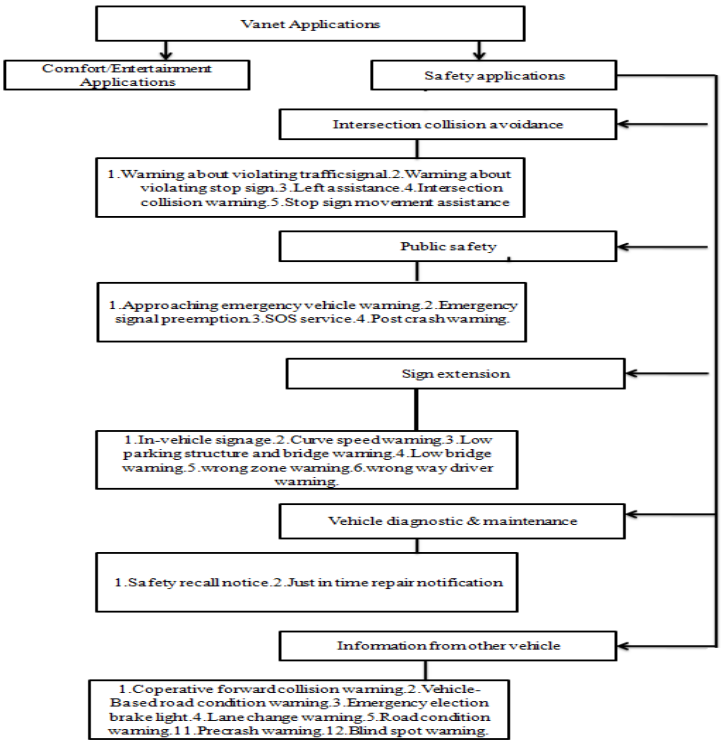

Figure 1: Applications of VANET

Comfort/Entertainment applications are also referred to as non-safety applications, with an aim to improve drivers and passengers comfort levels and improve efficiency of traffic. These applications provide Drivers or Passengers with the updates of traffic and weather and provide the location of the restaurant, Petrol-station or Hotel nearest with their prices. They also provides passengers with the advancement to play games online , access the internet and send or receive messages right away while the vehicle is connected to the infrastructure network[15].

Safety applications provides an capability to collect information from the sensors of vehicles and from other communicating vehicles or both for processing and exchanging this information as safety messages to other vehicles or infrastructure unit(RSUs) and for communication with other vehicles or infrastructures vehicles use wireless communication technology, that provides applications in a wider range and led to increase in safety on the road[16]. Safety applications using V-2-V communication or V-2-I communication are categorized as shown in figure1**.**

3. Security in VANET:

With the Development of vehicular networks it provides exchange of data in a wireless channels that tends to increase in requirements of security. Users of this network also expect security of VANET in terms of integrity, confidentiality, availability and so on like as other networks [10, 22].

3.1 Entities concerned with VANET security:

The various entities involved in security of VANET are described in table 2:

Table 2: Entities of VANET

Entity name	***Description***
Vehicle	It comprises of all categories of vehicular nodes i.e. cars, buses etc.
Infrastructure	It includes roadside units(RSUs)
Driver	The driver is chargeable for vehicle movement from one place to other.
Third parties	It includes traffic management authorities.
Attackers	Attackers include unauthorized nodes that perform malicious activities.

3.2 Security Requirements: These requirements of security leads to increase of processing and exchange of data in vehicular networks.
These requirements in security include the following:
Authentication: It makes sure that the user which sends a message is a legitimate user or not using certificate. Or the receiver verifies the sender of a message via a pseudonym [8, 9].
Availability*:* It ensures that the resources are available all the time by opposing to Denial of Service attack for functioning normally. Because a message becomes of no sense if there is delay in message send by the sender [4].
Confidentiality*:* It is used to ensure that the message that is send between two communicating parties remains secret and is hidden from adversaries. This is mainly done using encryption of data from plain text to cipher text [9].
Non-repudiation: This is used to ensure that a person who sends a message can't deny later that he has not sent a particular message. Also can be used to find the person who performs malicious activity even after harm is done [4].
Integrity*:* It ensures that there is no alteration of data between the sender and receiver of message. It can be mainly done with the help of Digital signature [14, 10].
Privacy: it is used to hide the identity of the driver and location information against nodes that are not authorized so that no one can trace the movement of any nodes [22].

Data verification: it is used to eliminate misleading messages. This is mainly used for detecting correctness of date and check whether sender is legitimate or especially between neighboring vehicles [6, 4}.
Access control: it is used to ensure that all nodes are working according to rules and roles privileges *[10, 9]*.

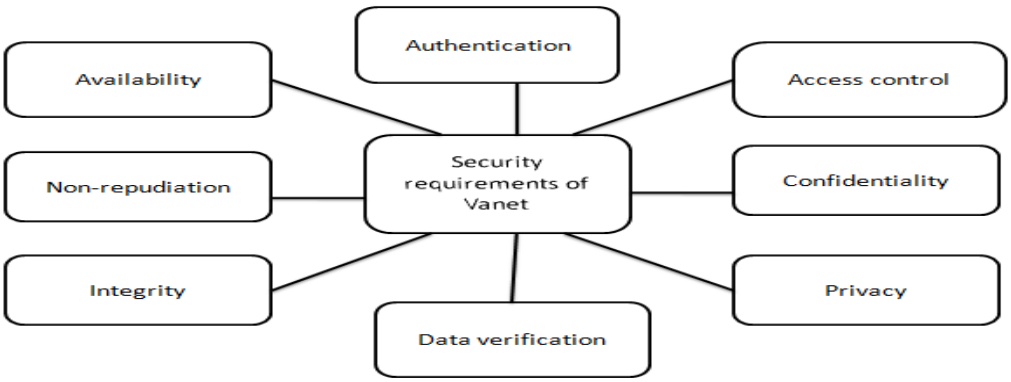

Figure 2: Requirements of Security

4. Attacker Model:

Implementation of a security system for vehicular ad-hoc network is difficult and challenging and also due to , frequent disconnection in VANET communication due to highly dynamic nature of VANET with often, instant arrivals of vehicles and instant departures , using wireless channels for exchanging important and safety information, leads to several security hazards and attacks in VANET. In this model, we will discuss various attacks and attackers in vehicular communication.

4.1 Attackers in VANET: attackers in vehicular ad-hoc network are one of the key concerns of the researchers. Attacker is a person which performs attacks in these vehicular networks and they cannot be done without the involvement of these attackers [23, 6].

The fig 3 presents the several attackers types that perform these attacks.

Insider attacker: Inside attacker is the one which is present on the verified users on the network.

Outsider attacker: Outsider is one which is not present on the network and thus has bounded capacity to attack [6].

Malicious attacker: Malicious attacker is an attacker which performs the attack for any personal benefit.

Rational attacker: Rational attacker is the one which performs the attack for its personal benefit and expected profit [23].

Active attacker: It is the one that generates signals or packets

Passive attacker: passive attacker is the one that which senses the network only.

Local attacker: It is the one that works within limited scope even on numerous nodes or infrastructures.

Extended attacker: extended attacker is the one that enlarge his capacity by controlling several entities dispersed over the network.

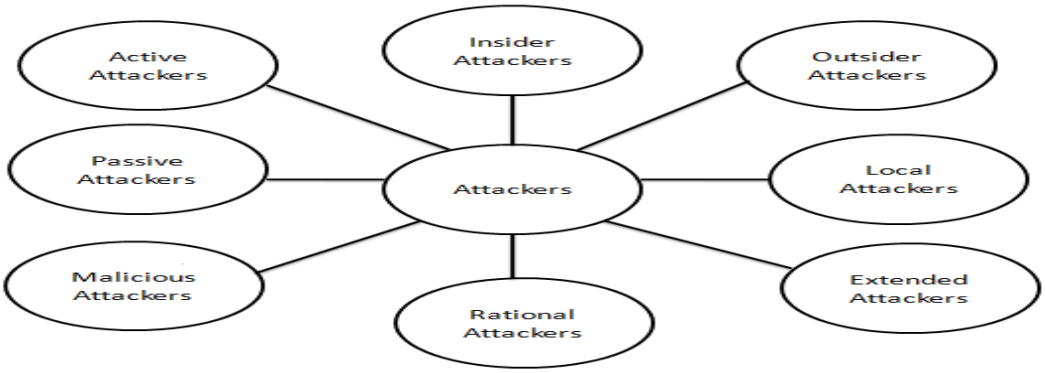

Figure 3: Attackers in VANET

4.2 Attacks in VANET:

Attacks refer to any malicious activity performed on system that has adverse effect on the network. The basic idea behind performing these attacks is to get the secret information in the network or to degrade the systems normal functioning so that it does not work properly that leads to various threats these attacks degrade the integrity, confidentiality and authenticity of system and are categorized into various classes [3, 24].

Class 1: Attacks on availability.
Class 2: Attacks on authentic and identification.
Class 3: Attacks on confidentiality.
Class 4: Attacks on integrity and data trust.
Class 5: Attacks on Non-repudiation /Accountability.

4.2.1 Attack on Availability:

Availability is one of the basic factors for VANET. This assures that the useful information is available always when the system is communicating and the network is functional. It is one of the crucial security requirements for vehicular networks whose aim is to ensure user's lives and it is a main target for attacks by the attackers. Some of the attacks on availability are [3, 6].

- *DOS*: it is an attack in which the resources and the services are made inaccessible by an attacker to the users in the network and is done by either making the channel busy or by "Sleep Deprivation" [24].
- *Black Hole Attack*: In this a node that is not authorized announces that it have the shortest path and then routes and redirects them to get the data and when this false route is taken by a node, depends on this unauthorized node to either leave or forward the packet wherever that node wants The unauthorized node is then able to either alter the data or keep it [9, 6].

- *Malware:* In this type of attack an attacker consume the bandwidth of a network by sending spam messages in the network and increase the latency of data transmission. This type of attack is also difficult to control because of the absence of a particular infrastructure units and central administration. An Attacker sends spam messages as an advertisement messages to a group of users to just consume the bandwidth of network as the users receiving these messages does not need these messages because these are of no use [10, 14].
- *Spam*: In this types of attack spam messages are send by nodes present inside the network so as to increase rate of transferring the messages, latency and utilization of bandwidth in network [24].
- *D-DOS:* Distributed Denial of Service attack is a denial of service attack from different locations [8,10].
- *Wormhole attack*: In this type of attack, an attacker overhears the data transferred over the wireless communication channel that can lead to serious threats [23].
- *Jamming attack***:** Jamming attack is a type of attack in which a signal is transmitted by the attacker to distract the communication channel ,that is mostly intentional and it lowers the Signal to Noise ratio for the receiver[9]
- *Greedy behaviour attack:* This type of attack according to the architecture of OSI model is an attack in which attackers, attack on the functioning of the Medium access layer. Attacker in this type of attack also minimize waiting time of a node for faster access due to which other nodes gets compromised and also causes collision problems and overburden on transmission channel that produces delays in services of authorized users[4,14]
- *Broadcast tampering attack*: In broadcast tampering attack, an attacker tries to provide and send wrong messages as emergency messages in network that hides the actual safety messages to authorized users in the network which can cause accidents and severe effects in vehicular ad-hoc network [24].

4.2.2 Attack on Authenticity and Identification:

- *Sybil Attack:* In this type of attack an attacker provides illusion to nodes of many vehicles on the road so that they can change their route for attackers' goal [22].
- *Relay Attack*: this type of attack involves capturing and replaying the packet to distract the authorities and protect identity of nodes in any accident [6, 8].
- *GPS spoofing/position-faking*: location information is of great importance in vehicular network so this information must be right and authentic. In this type of attack an attacker provides the neighboring nodes with wrong location information so as to hide its actual position information that is confidential [24].
- *Tunnelling:* This type of attack involves connecting two different parts of vehicular network by using additional communication channel such as tunnel [6, 24].
- *Key/Certificate Replication:* This attack consist of use of duplicate keys and certificates which are used as proof of identification which makes more difficult for certified authorities to identify a vehicle particularly in case of accidents.

4.2.3 Attack on Confidentiality:

- *Eavesdropping attack:* This type of attack is against confidentiality. In this attack an attacker attempts to get useful information in a network such as location, private information of nodes that can be used for tracking vehicles and to perform various attacks [3, 6].
- *Traffic analysis attack*: One of the serious hazards to confidentiality and privacy is the traffic analysis attack in which attackers analyzes the collected information and tries to get the useful information as much as possible for its own purpose [22, 14].

4.2.4 Attack on Integrity:

- *Masquerading attack:* In this type of attack, attacker produce a wrong message that looks like coming from an authentic user and is covert using a identity of a authentic user (called mask) and aims to form a black hole [9,10].
- *Message tampering/Suppression/Fabrication/Alteration*: this attack consists of modifying, altering, deleting, constructing existing data[24,3]
- *Illusion attack*: This type of attack consists in producing false data generated by sensors that are placed intentionally in the network . This data moves freely in the network and needs cooperation of driver for making decision. This type of attack cannot be detected by authentication mechanism, because the attackers are communicating with the network in a authentic way [10, 8].

4.2.5 Attack on Non-repudiation:

- *Loss of Event traceability*: Attackers in this type of attack provides denial of a node in a vehicular communication [3].

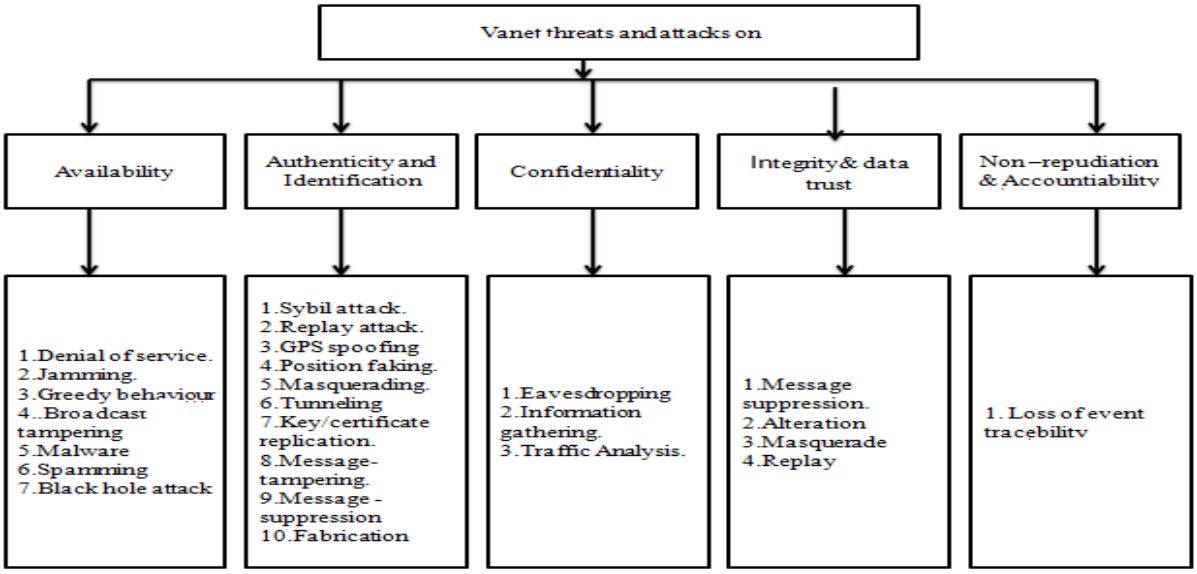

Figure 4: Attacks on VANET

5. Solutions from literature survey and their drawbacks: Many security solutions have been proposed for vehicular ad-hoc networks and to solve the problems that arise due to these security issues in VANET a large no of research papers had also been introduced. Researchers in [25] offered use of infrastructure i.e. Vehicular Public Key infrastructure (VPKI) as a solution for threats in VANET, where all communicating node have a Public and Private Key pair. Whenever a Vehicle forwards a secret information, it signs it with the Public Key of the receiver since the public keys are known to everyone and only the authentic user can decrypt the message because only that user will have the particular private key[6,26].*Drawbacks*: PKI can't satisfy the requirements of VANET's as it can't preserve conditional privacy. Another drawback is how to verify sender of public key is really who he claims he is. To overcome these drawbacks, we use digital signature scheme in above architecture. Digital signatures are a common way to enhance the security based on VANET's. Digital signature is digitally signed signature that binds the certificate holder identity with a public key and it also ensure integrity and non-repudiation so that the sender can't deny later that he has not sent the message [27].*Drawbacks*: certificate management, requires message is too long because of certificate i.e. 2m, and also requires a lot of time for verification process. Identity based cryptography: Each vehicle has a unique id. Public key is calculated from identity. We get public key as f(IDA), so it reduces the need of certificate and certificate management and here private key is inverse of public key and cannot be calculated by you. It can be calculated by TTP (private key generator).online connectivity to TTP is required .once received no need to connect to TTP.IT includes 4 phases Setup phase, Extract, Encryption and Decryption [11, 12]. *Drawbacks:* If TTP is compromised the private keys are also compromised. Other solution that has been suggested by the researchers is use of certification authority (CA) and needs infrastructure for Vehicular network. To manage it also needs a large number of authorities. But till now we do not have any existing authority that mange this network i.e. VANET the solutions suggested in [28, 3] by researchers is the use of CA to handle all the Certificate operations i.e. Creating, Renewing and revoking, and this certified authority should be responsible for key generation and storage of these keys with managing and broadcasting the certification revocation list. *Drawbacks:* Increases the cost of initial deployment when compared to public key authentication. Group based Signature scheme: Group signature scheme grants permission to the members of a group to sign message on behalf of a whole group with the help of single group key these signatures can be verified. In this method group of vehicles are formed .The group presents a geographical area of 300 meters around the vehicle. Each of the group will have a group leader which is offline generating symmetric encryption key and private and public key for the digital signature of the group. In PKI due to absence of groups, for verifying the certificates of communicating nodes there are delays due to many returns to RSU to or to authenticate the sender again and again that leads to a limitation of resources [13, 5].In the group-based scheme unless the GL wants to return to RSU there is no return to this unit and also unique individual cannot trace the message it is only done by the group manager .In short individuals identity that signs the messages is kept secret [5].*Drawbacks:* the main drawback of this solution is that if a vehicle leaves or joins the new group, the trusted authority needs to again compute the entire group-key that puts an extra load on TA due to the large number of computations.

Related work	Advantages	Disadvantages
Vehicular public key infrastructure[25,6,26]	Secure the exchange of data between the network Provide confidentiality, integrity and authenticity of messages	Cannot ensure sender of public key is really who claims he is. Cannot preserve conditional privacy of drivers.
VPKI with Digital signature[27,28]	Provide the confidentiality, integrity, non-repudiation and authentication requirements.	Verification time is too long. Increases storage requirements as the size of message increases due to certificates and keys.
Identity based framework[11,12]	Does need to store public keys of all the vehicles reduce the storage. Also reduces impersonification attack.	If TTP gets compromised keys also gets compromised.
Certification Authority(CA)[28,3]	Much more scalable. Need to trust only on single Certification authority (CA).	Requires a public key Infrastructure. Cost of initial deployment increases when compared to public-key authentication
Group signature based scheme[13,5]	Allows member of any group to sign a message on behalf of a group which can be verified by a single group key (i.e. reduces storage of keys) Provides privacy of messages.	If a vehicle leaves a group or joins a new group the Trusted-Authority needs to compute whole group keys which puts extra burden on TA

6. Conclusion:

This paper constitutes a comprehensive review of VANET security, after discussing characteristics, applications. Then threats or attacks to VANET and solutions to these security problems were introduced. In addition to this some issues in security such as requirements of security, attacker profiles and attacks has been pointed out and certain solution with advantages and disadvantages are highlighted.

REFRENCES:

1) Abbasi, Arshad Ahmed, and Adnan Shahid Khan. "A review of vehicle to vehicle communication protocols for VANETs in the urban environment." *Future Internet* 10.2 (2018): 14.

2) Lim, Kiho, and D. Manivannan. "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks." *Vehicular Communications* 4 (2016): 30-37.

3) Hasrouny, Hamssa, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. "VANet security challenges and solutions: A survey." *Vehicular Communications* 7 (2017): 7-20.

4) Samara, Ghassan, Wafaa AH Al-Salihy, and R. Sures. "Security analysis of vehicular ad hoc networks (VANET)." In *2010 Second International Conference on Network Applications, Protocols and Services*, pp. 55-60. IEEE, 2010.

5) Hasrouny, Hamssa, Carole Bassil, Abed Ellatif Samhat, and Anis Laouiti. "Group-based authentication in V2V communications." In *2015 Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, pp. 173-177. IEEE, 2015.

6) Engoulou, Richard Gilles, Martine Bellaïche, Samuel Pierre, and Alejandro Quintero. "VANET security surveys." *Computer Communications* 44 (2014): 1-13.

7) Meneguette, Rodolfo Ipolito, Luiz Fernando Bittencourt, and Edmundo Roberto Mauro Madeira. "A seamless flow mobility management architecture for vehicular communication networks." *Journal of Communications and Networks* 15, no. 2 (2013): 207-216.

8) Mejri, Mohamed Nidhal, Jalel Ben-Othman, and Mohamed Hamdi. "Survey on VANET security challenges and possible cryptographic solutions." *Vehicular Communications* 1, no. 2 (2014): 53-66.

9) Dai Nguyen, Huu Phuoc, and Rajnai Zoltán. "The Current Security Challenges of Vehicle Communication in the Future Transportation System." In *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)*, pp. 000161-000166. IEEE, 2018.

10)Li, Chun-Ta, Min-Shiang Hwang, and Yen-Ping Chu. "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks." *Computer Communications* 31, no. 12 (2008): 2803-2814.
11) Sun, J., Zhang, C., Zhang, Y. and Fang, Y., 2010. An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Transactions on Parallel and Distributed Systems*, *21*(9), pp.1227-1239.
12) Sun, Jinyuan, Chi Zhang, and Yuguang Fang. "An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks." In *MILCOM 2007-IEEE Military Communications Conference*, pp. 1-7. IEEE, 2007.
13)Guo, J., Baugh, J.P. and Wang, S., 2007, May. A group signature based secure and privacy-preserving vehicular communication framework. In *2007 Mobile Networking for Vehicular Environments* (pp. 103-108). IEEE.
14) Raw, Ram Shringar, Manish Kumar, and Nanhay Singh. "Security challenges, issues and their solutions for VANET." *International journal of network security & its applications* 5, no. 5 (2013): 95.
15) Liang, Wenshuang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie. "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends." *International Journal of Distributed Sensor Networks* 11, no. 8 (2015): 745303
16) Rasheed, Asim, Saira Gillani, Sana Ajmal, and Amir Qayyum. "Vehicular ad hoc network (VANET): A survey, challenges, and applications." In *Vehicular Ad-Hoc Networks for Smart Cities*, pp. 39-51. Springer, Singapore, 2017.
17) Shah, Syed Adeel Ali, Muhammad Shiraz, Mostofa Kamal Nasir, and Rafidah Binti Md Noor. "Unicast routing protocols for urban vehicular networks: review, taxonomy, and open research issues." *Journal of Zhejiang University SCIENCE C* 15, no. 7 (2014): 489-513.
18) Shah, Syed Adeel Ali, Muhammad Shiraz, Mostofa Kamal Nasir, and Rafidah Binti Md Noor. "Unicast routing protocols for urban vehicular networks: review, taxonomy, and open research issues." *Journal of Zhejiang University SCIENCE C* 15, no. 7 (2014): 489-513.
19) Shrestha, Rakesh, Rojeena Bajracharya, and Seung Yeob Nam. "Challenges of future VANET and cloud-based approaches." *Wireless Communications and Mobile Computing* 2018 (2018).
20) Liang, Wenshuang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie. "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends." *International Journal of Distributed Sensor Networks* 11, no. 8 (2015): 745303.
21)Kumar,Vishal,ShailendraMishra,andNorottamChand."ApplicationsofVANETs:present&future."CommunicationsandNetwork, 5,no.01(2013):12
22) kelareshtaghi,kavehBaksh,et al."survey on vehicular adhoc networks and its access Technologies Security Vulnerabilities and Countermeasures."arXiv preprint arXiv:1903.01541(2019)
23)S.Zeadally,RHunt,Y-S.Chen,A, Irwin,A.Hassan."vehicular adhoc Networks :status ,Results,Challenges"Springer Science,2010.
24) Kaur, R., Singh, T.P.&Khajuria,V.(2018,May)."Security issues in vehicular ad-hoc network (VANET).In 2018 2nd International conference on trends in Electronics and Informatics (ICOEI),pp.884-889.IEEE,2018.
25) M.Raya, P.Papadimitratos, andJP.Hubaux,"Securing vehicular communications,"IEEE Wireless Communication., vol.13, no.5, pp.8-15, oct 2006.
26) Salem, Ahmed H., Ayman Abdel-Hamid, and Mohamad Abou El-Nasr. "The case for dynamic key distribution for PKI-based VANETS." *arXiv preprint arXiv: 1605.04696* (2016).
27) Qu, Fengzhong, Zhihui Wu, Fei-Yue Wang, and Woong Cho. "A security and privacy review of VANETs." *IEEE Transactions on Intelligent Transportation Systems* 16, no. 6 (2015): 2985-2996.
28) Laberteaux, K. P., Hu, Y. C., & Haas, J. (2016). *U.S. Patent No. 9,461,827*. Washington, DC: U.S. Patent and Trademark Office.