International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

A Survey on the Major Security Issues in VANET

Ruchika[1], Rozy Rana[2], Preeti Saini[3]

[1, 2, 3]Assitant Professor, Chitkara University, Punjab, India

Abstract: ***Vehicular Ad hoc network (VANET) is an emerging infrastructure less network. VANET is developed by applying the techniques of Mobile ad hoc networks (MANET) in the field of vehicles. It is a communication network which provides safety measures and traffic analysis to users while driving. VANET is also known as Intelligent Transportation networks. It plays a major role in reducing accidents and improving traffic on the roads. Security is always an issue in the field of networking. Here it is also playing a major role because it's sharing safety information to the users and exploitation of this information can create a huge loss. In this Survey paper, we discussed the existing security threats and attacks i.e. availability and confidentiality with their challenges and future scope.***

Keywords: VANET, DOS Attack, Availability, Confidentiality, DSA, RSA

1. Introduction

Mobile communication techniques are becoming more and more advanced by providing communication between different devices at anytime and anywhere. It becomes easier to exchange the valuable information between the devices [9]. Hence there comes the need of exchanging the information between the mobile devices. Intelligent Transportation System (ITS) has taken a step forward in improving the road safety and driving environment. To detect the driving, safety conditions and share the nearby information with the vehicles, they [10] create an apt network known as VANET. Vehicular Ad-hoc Network (VANET) is one of the advancement of the Mobile Ad-hoc Network (MANET). It is a variation of Mobile Ad-hoc network (MANET) [22]. As more and more vehicles are increasing in numbers therefore, the need of road safety is becoming more important aspect. For creating a mobile network, VANET makes use of mobile as nodes . Hence, the vehicles act as wireless router that connect with other vehicles that helps in road safety and efficient driving, by providing alert to the vehicles in the neighborhood about accident coming in the way. In VANET each node is vehicle and communicates with other vehicles directly which is also known as Inter-Vehicle communication. To detect road collisions, efficiency in traffic, VANET will help further in reducing accidents on roads. In VANET network, communication is done in two ways vehicle to vehicle (V2V) where direct communication takes place and in vehicle to infrastructure (V2I) communication takes place with existing infrastructure through some fixed equipment placed in the road such as GSM, UMTS, and WIMAX network [10].

In VANET architecture, it involves various hardware & software components where vehicles are equipped with a unit known as OBU (Onboard Units) that help in V2V and V2I communication. Also vehicles have sensors that help in detecting the few measures like fuel consumption and road status. This sensorial information can be shared with others that will help in road safety and awareness.

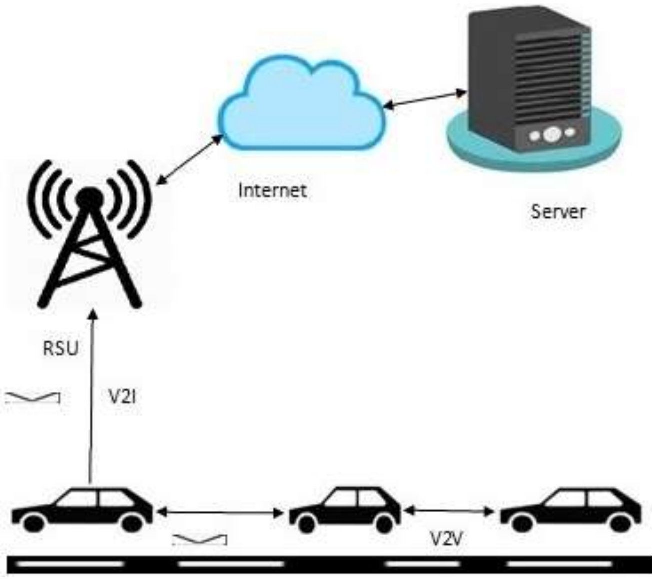


Figure 1: VANET

There are many challenges that need to be addressed in the VANET. As the network is open and wide, the security issues are more Challenging because of unique features of network, such as the high-speed mobility and increasing network entities. It is very important to deal with the system requirements that value the suitable operation of the network. There can be a possible security threats which may lead to a failure. Several requirements related to security issues in VANET are: integrity, authentication, non-repudiation, confidentiality, availability, access control.

In this paper we have discussed the attacks that hampered the security of VANET [18]. VANET is open to many attacks .There are various security threats in VANET (**fig 1.)** which are not only affecting the privacy but also compromising traffic safety that eventually leads to loss of life. In this paper the various security threats in VANET have been discussed in this paper. The major motivation that leads us to write out this survey is to see the work that has been done in the field of security in VANET till now

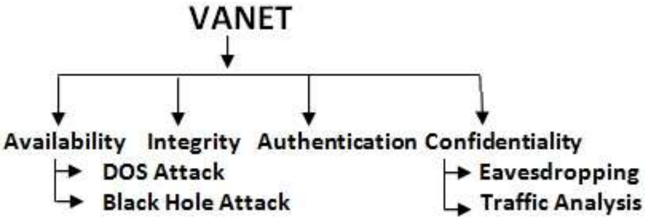


Figure 2: Various attacks in VANET

2. Literature Review

VANET is improving the performance of flow of vehicles on the road. It provides updated information about road traffic and traffic jams. Some of the cryptographic solutions have been discussed one by one [20]. Most of the Researchers [20] have worked on the VANETs security field that deals with an exact problem or general surveys. But this paper is covering all the security issues that have been discussed in VANET. However some paper has given the security threats that can come in VANET and other papers also provide the solutions to follow along with those threats.
In this paper Rashmi Mishra et.al [1] discussed about all the attacks that came in VANET and their possible prevention measures for road safety. There were various types of attacks like Sybil attack, impersonation, bogus information, Denial of service attack, Replay attack, timing attack etc. Different types of security solutions are provided like ARAN named as Authenticated Routing for Ad-hoc Network, Secure and Efficient Ad hoc Distance vector protocol (SEAD) , one Time cookie, ARIADNE, Elliptical curve parameter, A-SAODV, SAODV. Some of them used the third party CA (certificate authority) method to authorized user to enter the network. But this technique should work very fast i.e. within nanoseconds otherwise it will create chaos in the network. In future there is need to work on more secure protocols so that malicious user will not get any personal information.

In paper [4] the author mentioned a method to perform public key cryptography to encrypt the messages between the user and the road side unit so that no third entity can access the any type of information about the user. An algorithm used carry and forward mechanism in order to broadcast data to authenticate users. In this way, the broadcasting becomes more efficient. Some assumptions have been made e.g. road side unit is present at each and every traffic signal point and intersection road and also at the main area of communication like, bridges, tunnels, railway crossing etc. Every vehicle should be equipped with GPS with Driver License Number, Password, and an inbuilt system that shows the vehicle number. The confidential password, the number plate and driving license number provides the security against the brute-force attack, because it requires a numbers of iterations which is significantly large. By using confidential pass word. It provides extra security against social engineering.

In paper [5] the authors summarized and compared the different classes of defense mechanisms such as Public Key, Symmetric and Hybrid, Certificate Revocation, ID-based Cryptography based on the factors like Infrastructure less or infrastructure oriented, key used (public, symmetric or secret), identification approach (centralized or decentralized), communication(pair wise / group wise) and purpose of the defense mechanism for various security threats

This paper [6] discussed about the application areas, security threats and their consequences of VANET into the highly populated cities dealing with the problems such as long hour’s traffic-jams and pollution which is making cities life insecure and non-livable. The idea of Smart cities is emerging by developing the smart mobility concept.

In this paper [2], the major concern is on security and privacy of the vehicles. Several approaches have been discussed for future security attacks. The work should be done on security checks when vehicle comes in contact from one Road side unit (RSU) to another Road side unit (RSU). There is need to work on validating the certificates and then distribute those certificate securely and efficiently. To maintain the integrity, there must be clear idea about assigning trust values to vehicles. If IP Address changes then there is need to change the MAC Address otherwise it will become easy to attack.

This paper [3] discussed the significance of the message between the vehicles and several issues that is required to give the better results in the VANET. A chart of various VANET entities, security requirements, and range of attacks are described. Also for secure VANET environment discussion was made on the existing issues. To build up a good security system in VANET, lot of understanding of essential components is required. Location information is important in the field of the security of the messages. In future, there should be some focus on how to provide the accurate information related to location in case if there is some collision/accident occurs on the road then the location of the vehicle gets changed due to hit. So, there should be provision of providing the accurate information about location. Lot of discussion is required on GPS lack of coverage problem.

In this paper Ghassan sharma et al. [7], have given the new solutions to keep the network more secure. Single hop and multihop are the two methods to provide security. Through single hop it is possible to broadcast the message to the destination while in Multi hop when the message is not encrypted there are chances that the message gets modified. So, work in the area of multi hop network needs to be required. Focused areas will be creation, verification and testing of certificates otherwise this process will slow down the message and it will reach the destination very late. For the communication to take place there is need to work on providing equipment in the cars that is required for DSRC radios.

In this paper Muhammad Rizwan Ghori et al.[8] new, have thrown some light over the security issues in VANET how it is lagging behind in terms of security. The work needs to be done in tunneling attack otherwise there will be chaos in the network. Also, in replay attacks focus should be on securing the Internet IP address and MAC address because if attacker got the access on these address there are chances of accident, collision and jams on the roads. There should be more focus on Confidentiality and availability because not much work has been done in this field.

3. Attacks in Availability and Confidentiality

In VANET, confidentiality and availability is the vital security prerequisite. The main aim of VANET is to send messages between vehicle to vehicle (V2V) and Vehicle to infrastructure (V2I). The goal is to make sure that message is secure and not accessible to an unauthorized user. There are several attacks that are related to confidentiality. Malicious Attackers observe the communication between vehicles and they are passive attackers which mean their aim is to gather the information. The characteristic of confidentiality is to analyze the traffic flow when communication takes place between vehicles. While in availability, its purpose is to make the network available for the users. If the network is not available, communication cannot takes place [9].

Several attacks related to confidentiality and Availability is given below:

Availability attacks

DOS attack: Denial of services (DOS) attack is quite clear by its name which means all the services related to network are denied. It is the one of the key attack in the availability of the network. Its work is to jam the network so that communication won't take place in the channel. The key objective of the DOS attack is to keep away the authorized users from accessing the network. The main purpose is to send high frequency signals to the network near the Road side units (RSU) so that messages cannot be exchanged between vehicles and RSU. Its main purpose is to overwhelm the network so that it will eventually get crashed [9].

Black Hole Attack: Black hole attack is also the key attack in Availability. In this attack, the malicious node sends a malicious route reply to draw the attention of other vehicles to transmit the message all the way through itself and when they send the packet the malicious node drop the packet. A Gray Hole attack is the development of Black hole attack [23]. Here, the attacker drops every packet selectively [9].

Confidentiality

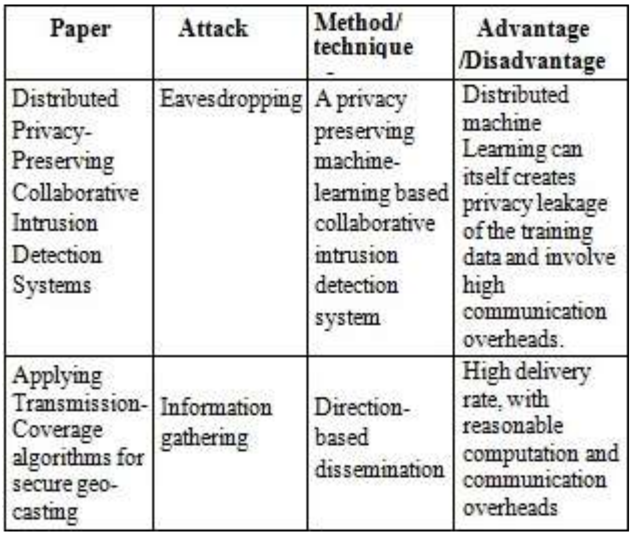
Eavesdropping

Eavesdropping is one of the key attacks in the confidentiality in VANET. Its main aim is to target the confidentiality of the network. It occurs in network layer. In Eavesdropping, attacker listens to the communication that occurs between two nodes. Aim is to get the confidential information like passwords and all the important data[9]. Attacker can attack as it pretends to be a false Road side unit (RSU) with the target of getting important valuable information. The basic goal is to monitor the communication that takes place between vehicle to vehicle (V2V) and vehicle to infrastructure (V2I)[9].

Traffic analysis: Traffic analysis is a major threat in VANET. It is a threat to a person's privacy and security. Its basic work is to attack the user's privacy by getting the traffic information packets. In the traffic information packets there can be information related to user's vehicle registration number, the user's location, travelling route of the user and all the information that attacker can user for the attacks. It is a serious threat to person's confidentiality [9].

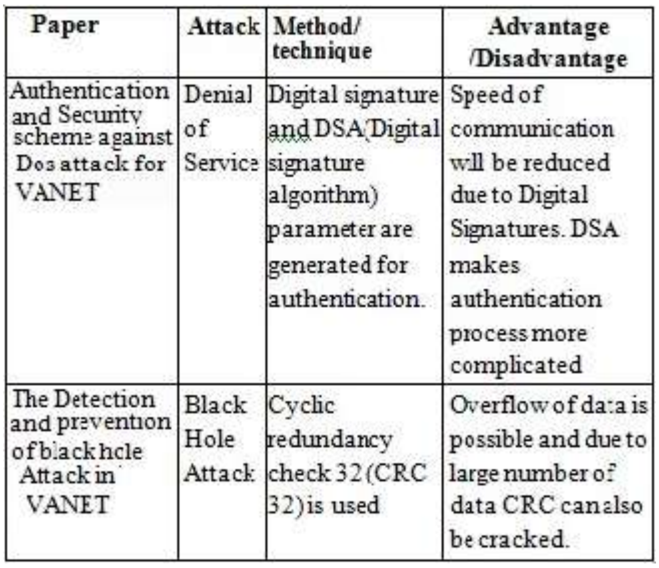
4. Work Related

Sonali godke [10] proposed a mechanism that focuses on denial of service attack (dos).digital signature and digital certificates are the methods that has been used to retain the authencity of the message. The focus of the work is to provide authentication by using digital signature. Authentication is done using DSA (digital signature algorithm) parameter which is used to create different keys every time. Here V2V communication takes place by verifying the digital certificate as well as digital signature. The main limitation of using the DSA parameter is that the process of authentication is more complicated every time, DSA signature computes different digital signatures for a same message due to this DSA behave very oddly. Salim Lachdhaf[11], represented a secured Ad-hoc on demand distance vector for Black hole attack. In the proposed strategy, cyclic redundancy check (CRC-32) bits have been used as a hash function. The change was made on the Route Request (RREQ) message format of AODV. The motive is to replace the destination IP address with CRC-32 bit address that will not change the RREQ Message format and will not create extra overhead. The limitation is that for large data blocks there are chances of passing the errors. Unfortunately, it supports integrity of small data blocks. Overflow of data is possible in CRC and also CRC can be cracked. This paper [12] discussed the network-level threats/attacks. They design a privacy-preserving machine-learning based collaborative intrusion detection system. The distributed machine learning is a appropriate framework for the design of scalable and implementable collaborative detection algorithms. As the eavesdropping can be done by monitoring the communication of other vehicles, and use them to access specific information like toll services, invade a specific vehicle, masquerade as its identity, and send out forged warnings that can interrupt the highway. The method employs the alternating direction method of multipliers to a class of ER minimization problems and trains a classifier to detect the attacks. In paper [13] Trujillo, Orozco and Kim discussed the traffic analysis attack in social networks where it is possible to track the identities of the users through intersection attacks or traffic analysis attacks using an unknown communication system. The work is to express how intersection attacks can unveil structural properties and significant details from an anonymous social network. We are able to know user's centrality to detect which are the most influential users in a network by using social network analysis techniques and getting several social network measures. The paper [14], the authors deal with the traffic analysis attack to smart homes, where antagonist interrupt the Internet traffic from/to the smart home gateway and profile residents' behaviors through digital traces. The design considers the resource constraints and the network energy consumption in IoT devices, while achieving strong differential confidentiality assurance so that combatant cannot link any traffic flow to a specific smart home



Paper	Attack	Method/ technique -	Advantage /Disadvantage
Distributed Privacy-Preserving Collaborative Intrusion Detection Systems	Eavesdropping	A privacy preserving machine-learning based collaborative intrusion detection system	Distributed machine Learning can itself creates privacy leakage of the training data and involve high communication overheads.
Applying Transmission-Coverage algorithms for secure geo-casting	Information gathering	Direction-based dissemination	High delivery rate, with reasonable computation and communication overheads

Figure 3: Confidentiality



Paper	Attack	Method/ technique	Advantage /Disadvantage
Authentication and Security scheme against Dos attack for VANET	Denial of Service	Digital signature and DSA(Digital signature algorithm) parameter are generated for authentication.	Speed of communication will be reduced due to Digital Signatures. DSA makes authentication process more complicated
The Detection and prevention of black hole Attack in VANET	Black Hole Attack	Cyclic redundancy check 32(CRC 32)is used	Overflow of data is possible and due to large number of data CRC can also be cracked.

Figure 4: Availability

5. Conclusion and Future Scope

In Today's scenario, population is rising due to which vehicles are increasing in numbers that directly affects the road behavior. This condition will led us to think more about road safety conditions. So, VANET is the foremost way out to make available improved road safety and other applications for drivers and passengers [15]. In this paper, a survey of security attacks in confidentiality and availability is presented. It is required to deeply study those threats vulnerability and come out with proper actions to deal with [16]. There are several techniques like Data Mining, Machine Learning and AI (artificial intelligence) are needed to analyze those attacks. VANETs are adhoc networks, highly dynamic, with little access to the network, infrastructure and offering multiple services. The feasible method/techniques in the confidentiality for the traffic analysis and passive eavesdropping attacks can be App fingerprinting and identification. App fingerprinting is a frame that unlocks a range of new challenges to directly provide user privacy and security[17]. In availability, we discussed two attacks Denial of service Attack (DOS) and Black Hole attack. In Dos attack, to compute digital signature, DSA parameter is applied and it gives us different result every time. In digital signature, the authentication and verification process is time consuming and it slow down the speed of communication. Digital signature works on providing the authenticity of the message but it doesn't work on the secrecy of the message. To provide the secrecy we need some techniques. On the other hand, DSA is slower in encryption and validation. To overcome this problem RSA can be used with digital signatures. For verification of digital signature, RSA is best choice. While in Black Hole Attack, large number of packets can create overhead in CRC32. There is need to secure CRC32 otherwise it can be cracked [17]. It is better to be aware of these challenges so that proper actions can be taken by keeping users safety and future in mind.

References

[1] Rashmi Mishra, Akhilesh Singh, Rakesh Kumar , "VANET Security : Issues, Challenges and Solutions", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) , 2016, pp. 1051-1055.

[2] Mohammed Saeed Al-kahtani , "Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)", 6th International Conference on Signal Processing and Communication Systems, 29 April 2013.

[3] Dilendra Shukla, AkashVaibhav, Sanjoy Das, Prashant Johri, "Security and attack analysis for vehicular ad hoc network -A survey", 2016 International Conference on Computing, Communication and Automation (ICCCA), 16 January 2017, pp.625-630.

[4] Mohinder Kuma, Opinder Kumar ,"Enhancing Security in VANET in terms of Confidentiality and Authentication", International Journal of Computer Applications (0975 – 8887), Volume 67– No.24, April 2013.

[5] Ahmed Shoeb Al Hasan, Md. Shohrab Hossain, and Mohammed Atiquzzaman, "Security Threats in Vehicular Ad Hoc Networks ", 2016 Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, 2016, Jaipur, India.

[6] Bhawna Chaudhary, Sheetal Singh, "Vehicular Ad-Hoc Network for Smart Cities", Proceedings of the First International Conference on Information Technology and Knowledge Management pp. 47–51, 2018, Vol. 14, pp. 47-51.

[7] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)", 4th International Conference on New Trends in Information Science and Service Science, May 11-13,2010, Gyeongju, South Korea.

[8] Muhammad Rizwan Ghori, Kamal Z. Zamli, Nik Quosthoni, Muhammad Hisyam, Mohamed Montaser,"Vehicular Ad-hoc Network (VANET): Review", 2018, Kuantan, Malaysia.

[9] Irshad Ahmed Sumra, Halabi Bin Hasbullah, Jamalul-lail bin AbManan," Attacks on Security Goals (Confidentiality,Integrity, Availability) in VANET: A Survey", Kuala Lumpur, Malaysia.

[10] Sonali Ghodke, Rohini Bhosale, AUTHENTICATION AND SECURITY SCHEME AGAINST DOS ATTACK FOR VANET, 2018, Maharashtra, India.

[11] Salim Lachdhaf, Mohammed Mazouzi , Mohamed Abid, “SECURED AODV ROUTING PROTOCOL FOR THE DETECTION AND PREVENTION OF BLACK HOLE ATTACK IN VANET”, Advanced Computing: An International Journal (ACIJ), Vol.9, No.1, January 2018.

[12] Tao Zhang , Quanyan Zhu,IEEE ,Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING OVER NETWORKS, VOL. 4, NO. 1, MARCH 2018.

[13] Alejandra Guadalupe Silva Trujillo, Ana Lucila Sandoval Orozco, Luis Javier García Villalba , Tai-Hoon Kim, “A traffic analysis attack to compute social network measures”,pp 1-15, 14 June 2018.

[14] Jianqing Liu,Chi Zhang and Yuguang Fang, “EPIC: A Differential Privacy Framework to Defend Smart Homes Against Internet Traffic Analysis”,pp 1206-1217, IEEE INTERNET OF THINGS JOURNAL, VOL. 5, NO. 2, APRIL 2018.

[15] Muhammad Anwar Shahid, Arunita Jaekel, Christie Ezeife, Qasim Al-Ajmi, Ikjot Saini. "Review of potential security attacks in VANET", 2018 Majan International Conference(MIC), 2018.

[16] Mauro Conti, Tooska Dargahi, Ali Dehghantanha. "Chapter 1 Cyber Threatm Intelligence: Challenges and Opportunities", Springer Nature, 2018.

[17] Vincent F. Taylor, Riccardo Spolaor, Mauro Conti, Ivan Martinovic. "Robust Smartphone App Identification via Encrypted Network Traffic Analysis", IEEE Transactions on Information Forensics and Security, 2018.

[18] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, Alejandro Quintero,”VANET Security surveys ”,computer communications,2014.

[19] Abdennour Zekri, Weijia Jia. "Heterogeneous vehicular communications: A comprehensive study", Ad Hoc Networks, 2018.

[20] Mohamed Nidhal Mejri, Jalel Ben-Othman, Mohamed Hamdi. "Survey on VANET security challenges and possible cryptographic solutions", Vehicular Communications, 2014.

[21] Yilin Shen, Ying Xuan, My T. Thai. "On local approximation of minimum-latency broadcast scheduling in 3D MANETs", 2011 – MILCOM 2011 Military Communications Conference, 2011.

[22] Sivakumar, R. Manoharan T.. "OPRM: an efficient hybrid routing protocol for sparse VANETs.(on-demand routing protocol with proact", International Journal of Computer Applications in Technology, April 20 2015 Issue.

[23] Jayant Vats, Gaurav Tejpal, Sonal Sharma. "Enhance mechanism for the detection and correction of routing attacks made by obstructive nodes", 2017 2nd International Conference on Communication and Electronics Systems (ICCES), 2017.