Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

A Survey on Various Kinds of Security Attacks Facing in Vehicle to Vehicle and Vehicle to Infrastructure Communication

Jyothi N, Dr.Rekha Patil
Dept. of Computer Science and Engineering,
PDA college of Engineering, Kalaburagi,
India

Abstract:- **Vehicular Ad-hoc Networks (VANETs) is also known as a subset of Mobile Ad-hoc Networks (MANETs) which refers to a set of smart vehicles used on the road. These vehicles provide communication services among one another or with Road Side Infrastructure (RSU) based on wireless Local Area network (LAN) technologies. The important benefit of VANET is to enhance the road safety and vehicle security while protecting privacy of drivers from attacks perpetrated by adversaries. Security is one of the most critical issues related to VANETs from the information transmitted that is distributed in an open access environment. VANETs face many challenges they generate the security requirements along with the threats and certain architectures are introduced with the various categories of applications in VANETs. Hence we introduced to solve the security problem and several existing attacks to defend against them and discuss possible future security attacks with critical analysis. This research will gain best understand of VANETs security issues and attacks from the study.**

Key Words: Local Area Network, Mobile ad-hoc Networks, Road Side Unit, Smart Vehicle, Vehicular ad-hoc network.

I. INTRODUCTION

VANETs are taken more attention from the end user due to its potential safety and non-safety applications. An attacker is one type of end user, but their role in the network is negative and creates problems for other components of network. Through different scenarios it will explain the effect of these attacks on other components of network. Trusted Platform Module (TPM) is a security hardware module and it provides the secure communication in network, so we will discuss in detail how this security module will handle these newly address in network [1]. To preserve the privacy, the Reputation Label Certificate (RLC) to evaluate the reliability of message for every vehicle in its communication range. When RLC of vehicle is revoked, its security and privacy will not be protected. Finally, theoretical analysis and simulations show that our scheme can efficiently meet the requirements of security and privacy in VANETs [2]. The twofold scenarios are analysed in VANET and highlight their limitations. Secondly, a new velocity based pseudonym changing (VBPC) strategy for preserving location privacy of vehicles in VANET. The simulation results show that Velocity based Pseudonym changing strategy is used to protect location privacy of vehicle in VANET [3].

Therefore different techniques have been proposed to hide the pseudonyms changes and make it difficult to link pseudonyms together. Most of these techniques do not fully quarantine privacy when changing a pseudonym under some situations such as low traffic. [4]. The privacy information related to the location of the vehicles need to be concealed with utmost care in the vehicular network since its disclosure leads to a diversified number of attacks that degrades the performance of the network. An effective variant ring signature based pseudonym changing mechanism (EVRS-PCM) is contributed for privacy preservation under decentralization and reduced density of vehicles [5].The privacy information related to the location of the vehicle need to be concealed with utmost care in the VANET work since its disclosure leads to a diversified number of attacks that degrades the performance of the network [6].To formulate a dual pseudonym based privacy preservation scheme for facilitating an effective degree of collaboration among the vehicular nodes of the network [7]. A scheme for anonymous pseudonym-renewal and pseudonymous authentication for vehicular ad-hoc networks over a data-centric Internet architecture called Named Data networking (NDN) in a traffic information sharing demo application and deployed it on Raspberry pi-based miniature cars for evaluation [8]. The central building block of secure and privacy preserving vehicle communication (VC) systems is a vehicular public key Infrastructure (VPKI), which provides vehicles with multiple anonymised credentials termed as pseudonyms. The state-of-the-art and show its availability, resiliency, and scalability towards a cost-effective VPKI deployment [9]. The effective file transfer between vehicles is fundamental to many emerging vehicular infotainment applications in the highway. The fully distributed scheme that relies on the collaboration of cluster members, CFT does not require any assistance from roadside units or access points [10].

This paper surveys advances on concerns to classify the attacks according to their characteristics, the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

requirements involved, and the defences that could be used. A description of the type of attackers will also be introduced. To the best of our knowledge, this is the first endeavour to provide a comprehensive overview of the presenting security threats while keeping in mind all of the other aspects involved in such attacks consists of a new approach. A global security architecture in VANETs will also be proposed to classify VANETs threats while considering the security layer level in the system.

The organization of this paper is as mentioned below, Section 2 discussed about the reviews on the state-of-the-art network in addressing the techniques to design effective by considering security in the past few years. Section 3, explains about the description of the proposal given in the literature on the different security requirements in VANETs applications. Section 4, does a comparative analysis of various security algorithms are examined, and section 5, concludes the paper.

II. TYPES OF MALICIOUS VEHICLES AND ATTACKS

The malicious vehicles launch attacks on legitimate vehicles in several ways. The malicious vehicles are attackers vehicles, classified as follows with several security attacks on Vehicular ad-hoc networks.

A. ***Insiders vs. Outsiders:*** A member node who can communicate with other members of the networks in a network is known as insiders and can attack in various ways. The outsiders can communicate directly with the members of the network have a limited capacity to attack.

B. ***Malicious vs. Rational:*** A malicious attacker uses various methods to damage the member nodes and the network without looking for its personal benefit. On the contrary, a rational attacker expects personal benefit from the attacks. Thus, these attacks are more predictable and follow some patterns.

C. ***Active vs. Passive:*** An active attacker generate new packets to damage the network whereas a passive attacker only eavesdrop the wireless channel that generate new packets.

D. ***Bogus Information:*** Attackers may transmit incorrect information in the network for its own advantage. An attacker may transmit wrong information about the traffic conditions in order to make its movement easier on the road.

E. ***Denial of Service (DoS):*** Attackers may transmit dummy messages to jam the channel and to reduce the efficiency and performance of the network. The malicious black car transmit a dummy message “Lane close Ahead” to a legitimate car behind it and also to an Road Side Unit (RSU) to create a jam in the network, which is given in figure.1.1. The Distributed DoS (DDoS) is more serve than the DoS where a various number of malicious cars attack on a legitimate car in distributed manner form different locations and timeslots, given in figure.1.2, that a number of malicious black cars attack on VI from different locations and time so that VI cannot communicate with other vehicles.

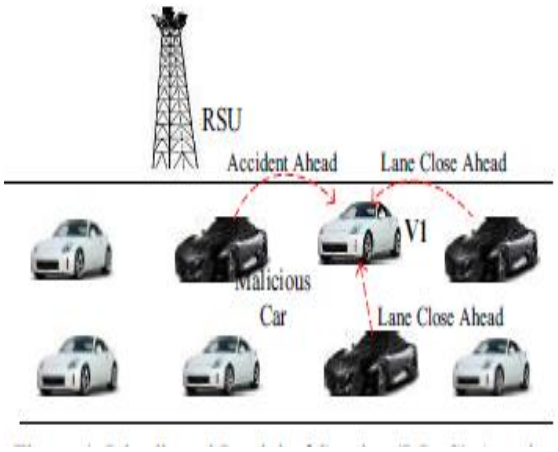

Figure.1.1 Denial of Service Attacks

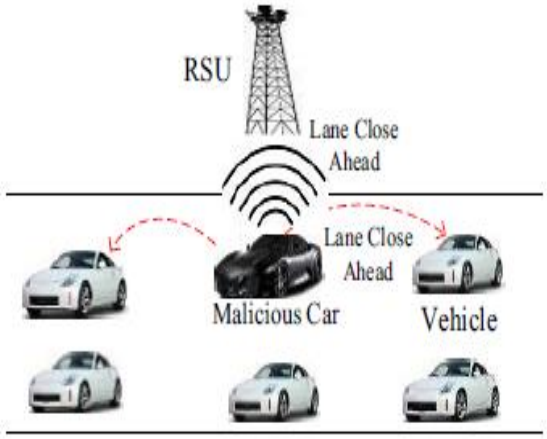

Figure.1.2 Distributed Denial of Service attack

F. ***Masquerade:*** A Vehicle fakes its identity and pretends to be another vehicle for its own advantage. It is achieved using message fabrication, alteration and replay. A malicious vehicle or attacker can pretend to be an ambulance to defraud other vehicles to slow down and yield.

G. ***Black hole attack*****:** A black hole is an area of the network where the network traffic is redirected. However, either there is no node in that area or the nodes reside in that area refuse to participate in the network. This causes data packets to be lost. Figure.1.3, illustrates a black hole attack where the black hole is formed by a number of malicious nodes, which refuses to transmit the messages received from the legitimate cars C and D to the cars E and F

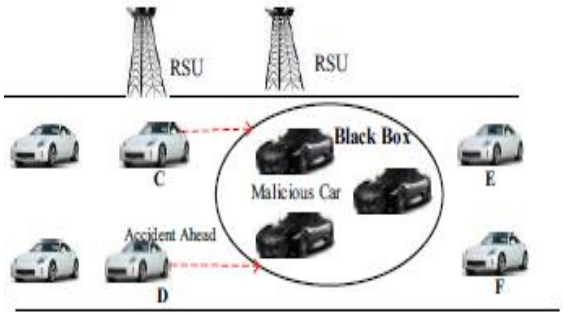

Figure.1.3 Black Hole attack

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

H. *Malware and Spam*: Malware and spam attacks such as viruses and spam can cause serious disruptions in the normal operations. Malware and spam attacks are normally executed by malicious insiders rather than normally executed by malicious insiders rather than outsiders whenever On-Board Units (OBU) of vehicles and road side units (RSUs) perform software updates. These attacks increase transmission latency, which can be alleviated by using a centralized administration.

I. *Timing Attack:* Transmitting data at the right time from one vehicle to another vehicle is significantly important to achieve data integrity and security. In timing attacks, whenever malicious vehicles at the right time but they add some timeslots to the original message to create delay.

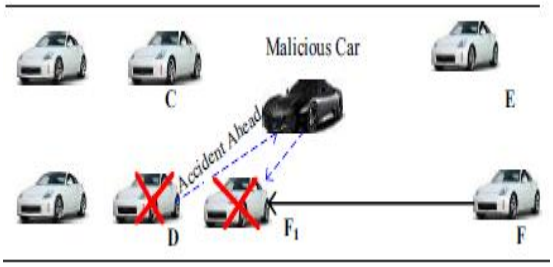

Figure.1.4 Timing Attacks

The neighbouring vehicles of the attackers receive the message after they actually require it. The figure.1.4, shows about the timing attack in which "Accident Ahead" message it does not transmit it to the vehicle whenever it is at the right position F but transmits by adding some timeslots so that whenever the vehicle receive the message it is on the spot where the accident takes place.

III. SECURITY REQUIREMENTS IN VANETS

Before addressing security issues of VANETs, it is paramount to address the requirements the system must respect for the appropriate operation of the network. Failure to respect a requirement may lead to a possible security threat. The main requirements defined in [11 and 12] are: authentication, integrity, confidentiality, non-repudiation, availability, access control, real time constraint and privacy protection. Most of these requirements are related to general security issues and others are specific to VANETs. The following section gives the details pertaining to these requirements.

A. *Authentication:* This is one of the main requirements for any system. In VANETs, it is very important to have certain information about concerning the transmitting node, such as its identification, and that of the message sender as well as its property and location. It is important to authenticate all users and messages which transit through the network. Authentication controls the authorization levels of vehicles.

In VANETs, authentication prevents Sybil attacks by assigning a specific identity to each vehicle. For instance, congestion avoidance prevents a single car from claiming to be a set of one hundred vehicles in order to give the illusion of a congested road. Powerful authentications provide legal evidence using external mechanisms; such as traditional law enforcement authorities to detect attacks [13] there are several types of authentication approaches [14] ID authentication allows a node to identify the transmitter of a message in a unique manner. This authentication also allows a node to belong to the network. When the ID authentication is set, it is easy to avoid certain attacks such as impersonation or fake nodes. Property authentication helps to determine what kind of entity is communicating: a car, an RSU or another type of equipment. Location authentication helps to authenticate the node position when a location application is involved.

B. *Integrity*: Integrity ensures that a message was not altered between the moment it was sent and received as the received message must match the message sent. The receiver will then be able to corroborate the sender's identity during the transaction [15]. Integrity protects against the unauthorized creation, destruction or alteration of data. If a corrupted message is accepted, the integrity property is violated and the protocol would be deemed flawed. To achieve integrity, the system must prevent attackers from altering messages since the contents of message must be trusted. Outsiders will return from interjecting message through authentication. A security protocol ensures that data are not compromised when they are forwarded from one secure car to another, its final destination, due to the message appended signature form secured traffic lights. The message can also be verified with similar ones that are generated in its immediate geographical neighbourhood within a short moment of time.

C. *Confidentiality:* During communication between entities, outsiders are not able to understand confidential information that pertains to each entity. This can be achieved due to message encryption that can protect the confidential information of each driver such as usage profiles and users identity. Message confidentiality in VANETs depends on the specific application such as those used for toll payments, where vehicles need internet service from RSUs, must be kept confidential by way of encryption schemes. Confidentiality is achieved by using public or symmetric key encryptions to ensure secure communication. In V2I communication, the RSU and the vehicle share a session key that is generated after mutual authentication. All of the messages are subsequently encrypted for confidentiality with the session key and they are also attached to the MAC (Message Authentication Code) for message authentication. Non-repudiation: is defined as the impossibility for one of the entities involved in a communication to deny having participated in all or part of a communication event. This protects against false denials involved in the communication. Non-repudiation provides the receiver with proof that the sender is accountable for the messages it generated. The main goal of non-repudiation consists of collecting, maintaining, making available and validating undeniable evidence about a claimed event or an action in order to resolve disputes about the occurrence or non-occurrence of that event or action. Non-repudiation depends on authentication, but it generates solid proof as the system can identify the attackers who cannot deny their crimes. Violators or

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

misbehaving users cannot deny their actions. Any car information (speed, time, trip route and violation) will be stored in a Tamper Proof Device (TPD) and any authorized official will be able to retrieve such data.

D. ***Availability:*** The network and applications should remain operational even in the presence of faults or malicious condition. This requires not only secure but also fault-tolerant design, resilience or depletion attack, as well as survivable protocols, which resume their normal operations after faulty participants are removed. An adequate routing protocol is needed to reach all of the required recipients that may be unknown to the sender. Also, certain message (e.g. an icy road warning) must be kept in a specific resources manipulated by the protocol. For example, for a key-exchange protocol, we must be sure that a session will really be established. Therefore, if users x1 requests the servers both have knowledge of the new session key. Many applications need faster responses from sensors or ad hoc networks since delays make certain message meaningless or they may have devastating consequences. Especially in cases where the application layer is not reliable, it can store partial messages that are completed in future transmissions to make the information forever available. Therefore, a real-time or a near real-time approach will be required for many applications used in VANETs [16].

E. ***Access Control:*** The requirement has the role of determining rights and privileges in the network. Some sensitive communications such as those from police cars or other law enforcement authorities must not be heard by the other nodes in the network. Access to specific services provided by the infrastructure nodes and the other nodes is determined through local policies. As part of access control, authorization establishes the rights of each network node. The service requires some credentials for the clients in the form of a ticket. There are two tickets such as., Ticket Granting service (TGS), the TGT allows the client to obtain TGSs grant while TGSs grant service access to the clients. Hence, clients must first obtain a TGT before they request a TGS for each service they wish to use. Therefore, the access control provides another warranty which prevents unauthorized people from accessing the services for which they do not have access rights.

IV. COMPARATIVE ANALYSIS

Table 1 shows the discussed popular security algorithms.

Author	Methodology	Performance Measures	Advantages	Limitations
Pandi Vijayakumar et al. [17] [2016]	Dual Authentication and key management techniques for secure data transmission in VANETs	Key computation time, key size and key recovery time in the	Efficiently distribute a group key to a group of users and to update group keys during the users join and leave operations	Lack of vehicle's location privacy in case of intruders in networks.
P.vijayakumar et al. [18] [2018]	Computational efficient privacy preserving anonymous mutual and batch authentication schemes for VANETs.	Verification time in ms, Number of received messages and total number of messages.	Provides the anonymous authentication with low certificate and signature verification cost in VANET.	The gesture based authentication schemes is missing in the networks.
Haowen Tan et al. [19] [2017]	Dual authentication and key management techniques for secure data transmission in VANETs.	The malicious attacker can impersonate legitimate vehicle and process all information needed.	Authentication time and key size.	Improper scheme in case of resistance to replay attack and masquerade attack
SK Hafizul et al. [20] [2018]	Efficient password based conditional privacy preserving authentication and group key agreement protocol for VANETs.	Execution time and communication cost.	Traffic efficacy and safety of the vehicles	Lack of random oracle mode for provable security.
Wenjia Li et al. [21] [2016]	An attack resistant trust management scheme for securing VANETs	Number of nodes, precision, recall, node motion speed and communication overhead	Data trust and node trust is updates with trustworthy in networks.	Doesn't addressed with different malicious attacks in networks.
Kiho Lim et al. [22] [2016]	An efficient protocol for authenticated and secure message delivery in VANETs.	Message transmission delivered and original message delivered,	Higher computational power.	Reduction of communication and computation overhead using fast authentication is required.

Table-1: Comparative Analysis of different authors

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

V. CONCLUSION

Secure data forwarding is one of the important challenges in VANET. If message forwarding is not secure it can cause fake messages delivery by malicious nodes, misguiding nodes in the network. This may cause accidents or traffic on road side .Hence, great challenge is to implement VANETs in value-added services due to the intruder vehicles and several security attacks. This paper comprised of a comprehensive state-of-art review on security issues and attacks on VANETs. Some security issues such as security requirements, adversary's profiles and attacks in VANET have been pointed out. On the basis of comparison between different schemes, it is clear that security while protecting privacy of drivers from attacks is useful in performance improvement of VANETs. This survey will be useful for the researched group those interested in the development, modification or optimization of security algorithms for VANETs.

REFERENCES:

[1] Sumra, I.A., Abdullah, A., Ahmad, I. and Alghamdi, A., 2016. "Towards Improving Security in VANET: Some New Possible Attacks and Their Possible Solutions". *Journal of Internet Technology*, *17*(4), pp.821-829

[2] Wang S. and Yao N. 2019. "A RSU-aided distributed trust framework for pseudonym-enabled privacy preservation in VANETs. *Wireless Networks*, *25*(3), pp.1099-1115.

[3] Ullah, I., Wahid, A., Shah, M.A. and Waheed, A., 2017, April. VBPC: "Velocity based pseudonym changing strategy to protect location privacy of vehicles in VANET." In *2017 International Conference on Communication Technologies (ComTech)* (pp. 132-137). IEEE.

[4] Amro, B., 2018. "Protecting privacy in VANETs using mix zones with virtual pseudonym change". *arXiv preprint arXiv:1801.10294*.

[5] Kalaiarasy, C., Sreenath, N. and Amuthan, A., 2019. "An effective variant ring signature-based pseudonym changing mechanism for privacy preservation in mixed zones of vehicular networks". *Journal of Ambient Intelligence and Humanized Computing*, pp.1-13.

[6] Förster, D., Löhr, H., Grätz, A., Petit, J. and Kargl, F., 2017. "An evaluation of pseudonym changes for vehicular networks in large-scale, realistic traffic scenarios". *IEEE Transactions on Intelligent Transportation Systems*, *19*(10), pp.3400-3405.

[7] Chowdhury, M., Gawande, A. and Wang, L., 2017, September. "Anonymous authentication and pseudonym-renewal for VANET in NDN". In *Proceedings of the 4th ACM Conference on Information-Centric Networking* (pp. 222-223). ACM.

[8] Noroozi, H., Khodaei, M. and Papadimitratos, P., 2018, June. VPKIaaS: "A Highly-Available and Dynamically-Scalable Vehicular Public-Key Infrastructure". In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks* (pp. 302-304). ACM.

[9] Luo, Q., Li, C., Ye, Q., Luan, T.H., Zhu, L. and Han, X., 2017, May. CFT: "A cluster-based file transfer scheme for highway VANETs." In *2017 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

[10] V.S. Yadav, S. Misra, M. Afaque, Security of Wireless and Self-Organizing Networks: Security in Vehicular Ad Hoc Networks, CRC Press, 2010, pp. 227–250.

[11] Stampoulis, A. and Chai, Z., 2007. A survey of security in vehicular networks. *Project CPSC*, *534*.

[12] Parno, B. and Perrig, A., 2005, November. Challenges in securing vehicular networks. In *Workshop on hot topics in networks (HotNets-IV)* (pp. 1-6).

[13] Kargl, F., Ma, Z. and Schoch, E., 2006, November. "Security engineering for VANETs". In *4th Workshop on Embedded Security in Cars (escar 2006)*.

[14] Biswas, S. and Mišić, J., 2010, May. "Proxy signature-based RSU message broadcasting in VANETs." In *2010 25th Biennial Symposium on Communications* (pp. 5-9). IEEE.

[15] Raya, M., Papadimitratos, P. and Hubaux, J.P., 2006. Securing vehicular communications. *IEEE wireless communications*, *13*(5), pp.8-15.

[16] Pandi Vijayakumar, Maria Azees, Arputharaj Kannan, and Lazarus Jegatha Deborah. "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks." IEEE Transactions on Intelligent Transportation Systems 17.4 (2016).

[17] Vijayakumar, P., Chang, V., Deborah, L.J., Balusamy, B. and Shynu, P.G., 2018. "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks". *Future generation computer systems*, *78*, pp.943-955.

[18] Tan, H., Choi, D., Kim, P., Pan, S. and Chung, I., 2017. Comments on "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks". *IEEE Transactions on Intelligent Transportation Systems*, *19*(7), pp.2149-2151.

[19] Islam, S.H., Obaidat, M.S., Vijayakumar, P., Abdulhay, E., Li, F. and Reddy, M.K.C., 2018." A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs". *Future Generation Computer Systems*, *84*, pp.216-227.

[20] Li, Wenjia, and Houbing Song. "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks." IEEE Transactions on Intelligent Transportation Systems 17.4 (2016): 960-969.

[21] 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.

[22] La, V.H. and Cavalli, A.R., 2014. "Security attacks and solutions in vehicular ad hoc networks: a survey".