International Journal of Computer Applications Technology and Research
Volume 3– Issue 5, 284 - 291, 2014, ISSN: 2319–8656

A Study of Sybil and Temporal Attacks in Vehicular Ad Hoc Networks: Types, Challenges, and Impacts

Deepika Shrivastava
DCEA, NITTTR
Bhopal, India

Ankur Pandey
DCEA, NITTTR
Bhopal, India

Abstract: In recent years, the number of automobiles on the road has increased tremendously. Due to high density and mobility of vehicles, possible threats and road accidents are increasing. Wireless communication allows sending safety and other critical information. Due to this inherent wireless characteristic and periodic exchange of safety packets, Vehicular Ad-hoc Network (VANET) is vulnerable to number of security threats like Sybil attack or temporal attack. In this paper, a detailed discussion has been done on both the type of attacks. With the help of already published works, some approaches have also been studied which have proved to be of significance in detection of these attacks.

Keywords: attacks; malicious; OBU; RSU; VANET

1 INTRODUCTION

During the past few years, there has been very rapid growth in wireless communication which has provided number of opportunity in computer networking aiming for data transfer where wired communication cannot be imagined in the real world. Wireless communication has provided the ability to communicate with the mobile devices in the continuously changing topology. This wireless communication of mobile devices has led to the creation of the term MANETs (Mobile Ad Hoc Networks).

Vehicular Ad Hoc Networks (VANET) is a special class of MANET where communicating nodes are vehicles. An ad hoc network [1] consists of group of nodes that can transmit and receive information with each other through wireless medium, either with a fixed infrastructure with or without any centralized management. Each node performs the functioning of router also. VANET differs from MANET due to its unique characteristics. Connections between vehicles are short lived. Network topology is dynamic, nodes move in and out of the range of neighboring nodes very quickly. Density of network also changes dynamically.

1.1 VANET vs. MANET

Unlike MANETs, the vehicle's mobility in VANETs is restricted by predefined roads. Vehicle's velocities are also restricted due to level of congestion on the roads, speed limitation, and traffic control mechanisms. In addition, given the fact that future vehicles can be equipped with devices with potentially longer transmission ranges, rechargeable source of energy, and extensive onboard storage capacities, processing power and storage efficiency are not an issue in VANETs whereas, this issues exits in MANETs. From these features, VANETs are considered as an extremely flexible and relatively “easy-to-manage” network pattern of MANETs.

1.2 VANET Model

A Vehicle deployed in the network contains following components. These components are displayed in Figure 1.

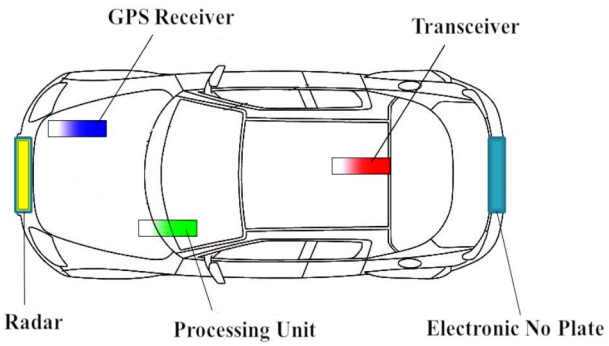

Figure 1. VANET Model

- A GPS navigation system
- Microwave radar that can detect objects at certain distance
- A computing unit, which will provide data processing, computing and storage
- A wireless transceiver, which provides standard communication for VANET
- A unique ID, such as an electronic license plate

1.3 Features of VANET

Some of the important features of the VANET are listed below:

- The movements of these nodes are very fast
- The movements of nodes are restricted by road topology
- Vehicle acts as transceiver i.e. sending and receiving at the same time while creating a highly dynamic and continuously changing network.
- The vehicular density varies from time to time. For example, density gets increased during day time and decrease at night.

2 APPLICATIONS OF VANET

The safety and security approaches of VANET have led its existence into number of applications. Figure 2 shows some of the most common applications of the VANET.

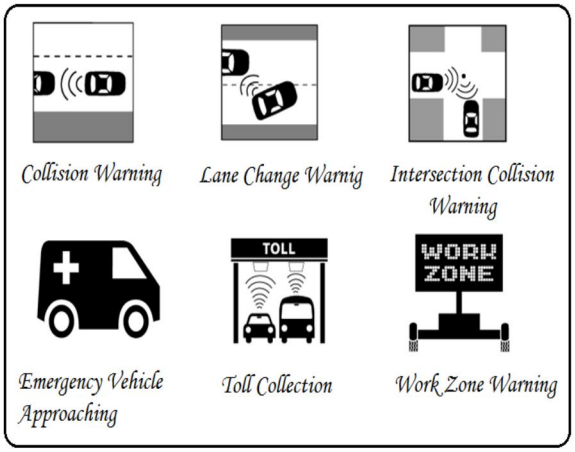

Figure 2. Applications of VANET

2.1 Increase Traveler Safety

VANET senses and provides information like intersection collision warning, lane change warning, emergency brake applied by the front vehicle warning, curve turn warning, etc, which effects the travelers safety. Traveler can take the proper measures to avoid unwanted situations like slowdown the vehicle.

2.2 Traffic Information

Warning related to traffic jams ahead, traffic signals, emergency vehicle approaching, availability of parking slot, etc, which certainly reduces the travel time and fuel consumption.

2.3 Road Condition and weather Info.

Notification of damaged road, spreading of oil, speed breaker, slippery road, weather information, landslides in the mountain regions assists the passenger to handle the unknowing situation.

2.4 Internet Access via RSUs

One can browse internet, check mail, find restaurants, gas stations, etc, in the nearby area along the road. A Roadside Services Database will be installed from the local area that will be connected to the corresponding RSUs. It thus increases the onboard luxury. Passengers may share some common interests, chat and children can play online games etc.

2.5 Electronic Toll Collection

Non-safety applications increase the overall comfort of the driver. Electronic toll collection and parking lot payment are few possible non-safety applications. Instead of driver having to stop at each and every toll booth to make a payment, the payment will be made electronically through the network. Also, a number of entertainment features have been proposed for vehicular networks, such as transferring of music and video files for in-car entertainment.

3 COMMUNICATION IN VANET

VANET communication is used to improve vehicle's passenger safety by means of inter-vehicle communication. In Vehicular Ad Hoc Network, communication is based on Dedicated Short Range Communication (DSRC) band [5]. The two types of communication devices employed in VANETs are as shown in Figure 3 –

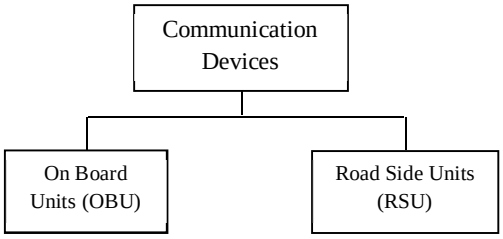

Figure 3. Communication Devices Deployed in VANET

- Vehicles or On Board Units (OBUs)
- Road Side Units (RSUs) are fixed infrastructure on the road

3.1 VANET Architecture

An instance of the architecture of vehicular network is as shown in Figure 4.

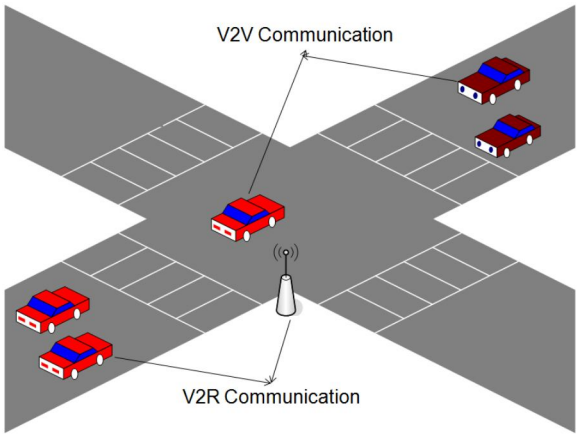

Figure 4. VANET Architecture

- Vehicle to Vehicle (V2V): Vehicles communicates with each other through wireless medium.
- Vehicle to Road side unit (V2R): Vehicles communicates with fixed infrastructure via wireless communication.
- Road side unit to Road side unit (R2R): A RSU communicates with another RSU through wired channel.

3.2 Safety Message Transmission

VANET is needed for automated and intelligent Transportation Systems (ITS). In the case of an accident, inter vehicle communication can be used to warn other vehicles approaching

the site. Each node in VANET periodically broadcasts beacon packets to announce its presence to neighboring nodes. Each beacon packet contains sender identity, position, time-stamp and speed etc. A safety message is shown in Figure 5. The difference between the beacon packets and safety packets is that the former does not have warning field and safety packets are sent only on the occurrence of specific event.

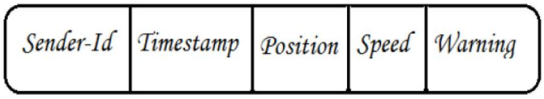

Figure 5. A Safety Message Format

Two kinds of message transmission take place in VANET –

- Periodic messages or Beacon Packets: They are sent with the intention of providing non-critical information (e.g. Sender-ID, GPS position, speed, direction etc). These packets are broadcasted at a regular time interval.
- Event-driven messages or Safety Packets: Event-driven messages are those messages which are generated on the occurrence of certain life critical incident (e.g. lane change or braking of the front vehicle)

3.3 Wireless Radio Channel

The wireless radio channel makes a great impact on the reception of packets. Path loss and shadowing causes the fluctuation in the received signal strength. Path loss [6] is caused by dissipation of the power radiated by the transmitter as well as due to the effects of the propagation channel. Shadowing is due to obstacles between receiver and transmitter that attenuate signal power through reflection, absorption, scattering and refraction. Both path loss and shadowing are caused due to long distances therefore they are considered as large-scale propagation effects.

Multipath is due to the receiving of multiple components of the signal. These components may be attenuated, delayed, shifted in phase and/or frequency from the LOS (Line of Sight) signal path at the receiver. Variations due to multipath are considered as small-scale propagation effects as they are on the order of the wave length. There exists number of different models for signal propagation between the receiver and the transmitter. Some models are mentioned below:

- Free Space Model
- Ground Reflection Model
- Shadowing Model
- Empirical Path Model

4 Wireless Technology in VANET

Here the wireless technologies have been divided into two broad categories. On one side, there are large area technologies as GSM, GPRS or UMTS, which have moderate bandwidth. On the other side, there is much higher bandwidth than the local area technologies such as WLAN (Wireless Local Area Network). There exist two different standards for Wireless LAN i.e. HIPERLAN from European Telecommunications Standards Institute (ETSI) and 802.11 from Institute of Electrical and Electronics Engineers (IEEE).

Nowadays, the 802.11 standard totally dominates the market and the implementing hardware is well engineered. Local Area Networks (LAN) and Metropolitan Area Networks (MAN) are standardized under the IEEE 802.11 WLAN protocols, which is the part of the IEEE 802 family. The IEEE 802 family has Internet Protocol (IP) layer with its routing protocols, e.g. AODV or DSR for mobile ad hoc networks, Logical Link Control layer (LLC), MAC (Medium Access Control) layer and finally PHY (Physical) layer. Figure 6 shows the OSI layered model of VANET.

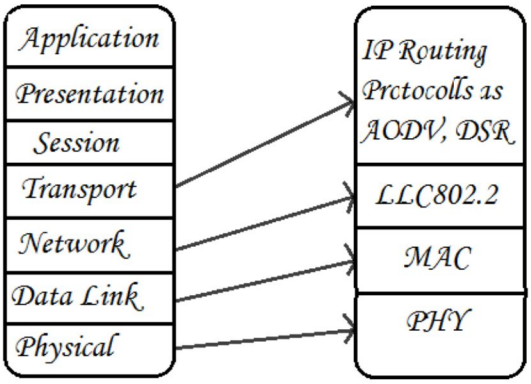

Figure 6. OSI Model for Wireless Communications

The IEEE 802.11 standard is constructed for wireless local area network technology (WLAN). Currently, 802.11 describe two specific operational modes. These modes are infrastructural and infrastructure-less based networks. The infrastructure-less based networks has been generally termed as Ad-hoc networks. Ad-hoc networks use Wi-Fi technology for Internet connectivity. It relies on the information distributed through a cluster of interconnected vehicles to transport, share, and receive information. The IEEE 802.11p standard is the adaption of the 802.11 protocol for WAVE (Wireless Access in Vehicular Environments).

5 Security Constraints in VANET

There are number of challenges in implementing security techniques in VANET. Few of the significant ones are listed below:

5.1 Equilibrium between Authentication and Privacy

For authentication of all message transmission, the identification of the vehicle from which message has been sent is required to track down. In general, people will not like to reveal their privacy to others; therefore this has to come in equilibrium. Therefore a system needs to be introduced which keeps the balance between the authentication of message and privacy of an individual.

5.2 High Mobility

Due to high mobility and rapidly changing topology, the protocol cannot be based on handshaking. So, it's a real challenge to implement and maintain the network.

5.3 Real-time Guarantees

As the major VANET applications are used for collision avoidance, hazard warning and accident warning information, so applications require strict deadlines for message delivery.

5.4 Central Authority

All the VANET nodes i.e. the vehicles are required to register with a central authority and already have a unique identity in the form of a license plate. Central Authority is a kind of infrastructure which maintains records of all vehicles.

6 SAFETY REQUIREMENTS FOR VANET

There are many safety requirements which should be taken in order to ensure safety of the passengers and the vehicle. Few significant safety requirements are discussed below:

6.1 Authentication

Authentication is required in VANET to assure that the messages are sent by the actual nodes. So, the effect of attack by greedy drivers and other adversaries can be reduced to a greater extent. Basic authentication scheme include attaching the sender's identity, it raises privacy concerns, as it would allow tracking of vehicles.

6.2 Message Integrity

This is required to ensure that the packet/data has not been tampered or altered after it was generated. Integrity is not only concerned with the original source of data but also whether it has been modified since its creation.

6.3 Message Non-repudiation

In this security based system a sender cannot deny the fact having sent the message. But that doesn't mean that everyone can identify the sender only specific authorities should be allowed to identify a vehicle from the authenticated messages it sends [2].

6.4 Entity Authentication

It is required to ensures that the message received is not very old i.e. the message is send within a very short period. It ensures that the sender who has generated the message is still inside the network.

6.5 Access Control

It specifies the roles and privileges to be given to the nodes in the network and what each node can do in the network and what messages can be generated by it.

6.6 Message Confidentiality

It is a system which is required when certain information need to be kept private. This can only be done by the law enforcement authority vehicles to communicate with each other to convey private information. An example would be, to find the location of a criminal or a terrorist.

6.7 Privacy

This system is used to ensure that the information is not leaked to the unauthorized people who are not allowed to view the information.

6.8 Real-time Guarantees

It is essential in a VANET, as many safety related applications depend on strict time guarantees. This can be built into protocols to ensure that the time sensitivity of safety related applications such as collision avoidance is met.

7 ATTACKS ON VANET

Incorrect information sent by a malfunctioning or attacker node might jeopardize the security and safety of the vehicles and endangers other vehicle's approaching the site. Emergency vehicle warning would have to be compromised without assurance that transmission is done from an actual emergency vehicle. Thus, it is challenging job to identify if the node spreading traffic safety information is malicious or not.

7.1 Bogus Information

Attacker sends inaccurate information into the network in order to achieve personal benefit. Selfish vehicles may attempt to clear up the path ahead with false traffic reports to reach his destination in the shortest possible time; criminals being chased by the police may disseminate the bogus information to other vehicles in order to block police cars, and terrorists may produce serious traffic collisions with contradictory traffic announcements.

7.2 Imposture

Attackers pretend or use other vehicle's identity to create illusion. For example, a vehicle may pretend to be a fire brigade or police car or ambulance van to free the traffic flow for its benefits. This type of attack is usually performed to impersonate a legitimate vehicle or RSU.

7.3 Denial-of-Service

Attacker may deny the other vehicles to use the VANET network by channel jamming or aggressive injection of dummy message.

8 TEMPORAL ATTACKS

Temporal attacks stands for time related attacks like, delay in packet forwarding and repeating the packet sent at earlier time interval. There are three types of temporal attacks. Each type of temporal attack is explained below:

8.1 Replay Attack

An attacker can replay the received packets apart from acting as a normal node (forwards all the received packets). In this attack, packets are fraudulently repeated. This operation is carried out by a malicious node that intercepts the safety packet and retransmits it. This type of attack is usually performed to impersonate a legitimate vehicle or RSU. Since, Basic 802.11 security does not contain sequence numbers; therefore it provides no protection against replay. Because of keys can be reused, it is possible to replay stored messages with the same key without detection to insert bogus messages into the system.

A typical replay attack scenario in VANET is shown in Figure 7. Attacker is repeatedly sending the message send by vehicle V1 to vehicle V2.

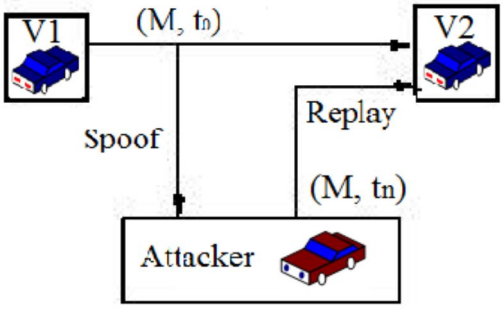

Figure 7. Packet Replay Attack

8.2 Delay Attack

In this attack, a vehicle delays the packet being forwarded by certain time duration in the network. It is more harmful than replay attack as vehicles may not get enough time to respond to particular emergency situation. For Example: Attacker node N_a observes 'CLEAR ROAD' ahead at time t_0. Instead of forwarding the 'ROAD IS CLEAR' message to the other vehicles in the road; it introduces the delay of time t_d. Suppose after t_d time there is congestion in the road, but the attacker node Na will forward the packet observed at time t_0. The other vehicle instead of decreasing the speed they will increase their speed after receiving the delay message 'TRAFFIC JAM'. This will lead to severe results like loss of life and property. Figure 8 shows the delay attack on VANET.

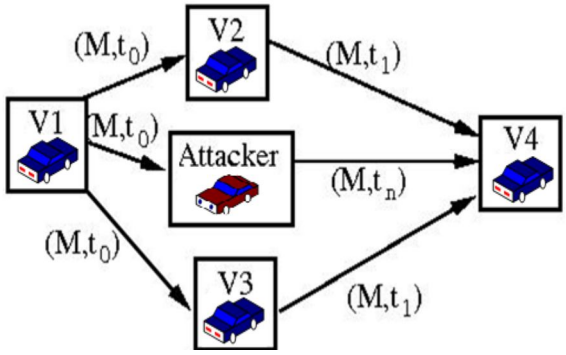

Figure 8. Packet Delay Attack

8.3 Suppression Attack

In this attack, an attacker selectively drops packets received from the neighbors, these packets may hold critical safety related information for the receiver, the attacker suppress or block these packets and can use them again at later time [10]. Such type of attack can prevent warning messing to be forwarded. For instance, an attacker may block a congestion warning, so vehicles will not receive the warning and forced to wait in the traffic for the long time. Figure 9 shows the suppression attack on VANET.

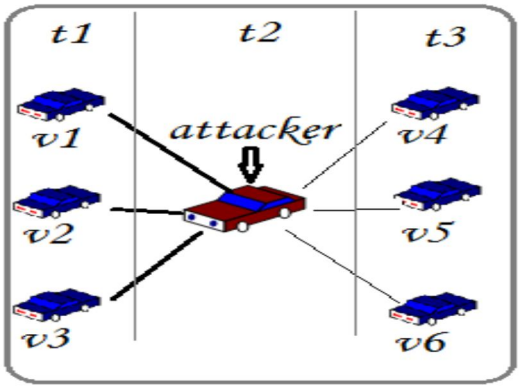

Figure 9. Packet Suppression Attack

8.4 Related Work

This section explores the previous work done on temporal attacks and their detection approaches in VANET. It is a normal phenomenon to forward each received packet to neighboring nodes VANET. Malicious nodes can adversely impact this process by purposely interfering in-between the packet transfer among the vehicles.

In [3] Aijaz et. al. have presented various types of attacks on inter-vehicle communication systems. They analyzed how an attacker can modify the sensor readings and the input of an on-board unit (OBU). Here, the authors proposed plausibility checks using constant system examinations, but no detailed discussion on implementation of plausibility check is presented. In [13] M. Raya and J.P. Hubaux have discussed number of unique challenges in VANETs. They describe how adversaries use safety applications to create various attacks and security problems.

In [4] Nai-Wei et. al. have presented an illusion attack in VANET. In this attack, a malicious node creates a particular traffic situation and sends fraud traffic warning messages to other nodes for convincing them that a traffic event has occurred. To detect and defend against the illusion network, plausibility validation network model is introduced in this paper. However, they did not implement this attack and its defense approach in any simulator. In [27] Yan et. al. have proposed a position verification approach for detection of position related misbehaviors.

In [28][29] Raya et. al. have suggested the use of VPKI (Vehicular Public Key Infrastructure) as a solution, where each node will have a public/private key. When a vehicle sends a safety message, it signs it with its own private key and adds the Certificate Authority (CAs) certificate. In [30] Ren et. al. have proposed the use of the group signature, but the biggest disadvantage of this method is its overhead because every time any vehicle enters the group area, the group public key and the vehicle session key for each vehicle that belongs to the group must be changed and transmitted. Another issue is that VANET mobility prevents the network from making a static group, as topology is dynamic in nature.

In [14] Golle et. al. have proposed an approach to detect and correct malicious data in VANET. They assume that vehicular

node is maintaining a model which consists of all the information that nodes has about the network. When a node receives a message, it compares received message with VANET model. If the received message does not comply with the VANET model, it is considered an invalid message. This approach requires gathering of sufficient messages to perform fraud message detection and suspicious data correction. The VANET model used in this paper is predefined and not flexible to switch to a new one. It is not feasible to design a model based on global knowledge of the network. Schmidt et. al. [33] constructs reputation models for other vehicles based on the claims from sending vehicles. In this way, they create a model of normal behavior of nodes in VANET. If the behavior of a node differs from the normal behavior, it is marked as suspicious.

9 SYBIL ATTACK

A Sybil attack is a type of attack in which a malicious node illegitimately fabricates multiple vehicle identities. In a Sybil attack, there are two types of nodes that are malicious node or Sybil attacker and Sybil node as shown in Figure 10.

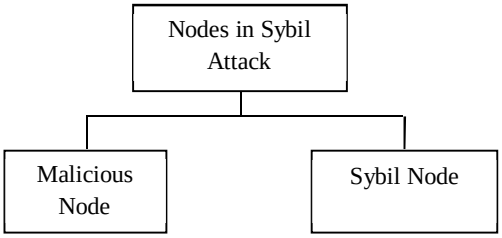

Figure 10. Nodes Participates in Sybil Attack

- Malicious node/Sybil attacker: The node which spoofs the identities of other nodes.
- Sybil node: Additional identities created by the malicious node are known as Sybil nodes.

Figure 11 shows the typical Sybil attack in VANET scenario. Sybil attacker is spoofing the identities of A, B, and C. The impact of Sybil attack gets severe when all identities created by attacker participate simultaneously in the network. Sybil attack is classified into two categories. Both of them are explained below:

Case 1: When Sybil attacker creates the identities of actually existing node in the network. Let N is the set of all vehicles in VANET and S is the set of all Sybil nodes. In this case $S \subseteq N$.

Case 2: When Sybil attacker creates the identities from outside the network. Let N is the set of all vehicles in VANET and S is the set of all Sybil nodes. In this case $S \not\subset N$.

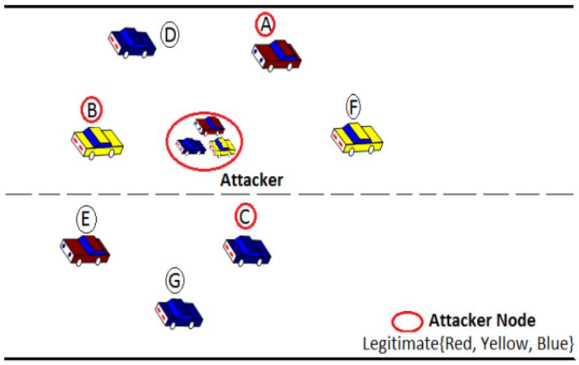

Figure 11. Sybil Attack in VANET

As messages are broadcast over the shared communication media, it is easy for a malicious node to get additional identities either by stealing or fabricating them. The main motive of Sybil attack detection approach is to ensure that each physical node is bound with only one valid identity.

9.1 Related Work

VANETs are vulnerable to many security threats and attacks. Various types of attacks in VANET are presented in [3][4]. An opponent or attacker may secretly listen on the channel easily and modify or insert the wrong information in the network. It is a normal phenomenon to forward each received packet to neighboring nodes VANET. Malicious nodes can adversely impact this process by purposely interfering in-between the packet transfer among the vehicles. Sybil attack is one of the major concerns in the VANET scenario. In Sybil attack, a malicious node illegitimately spoofs the identities of other nodes. It pretends or impersonates the original node to benefit itself.

In [11], Douceur et. al. was the first to describe and formalize the Sybil attack in the context of peer to peer networks. It can easily defeat reputation and threshold protocols intended to protect against it. In [12] resource testing was one of the methods proposed to defend a Sybil attack. It is assumed that physical resources of each node are limited. Unfortunately, this method is not suitable for Ad Hoc networks because an attacker can have more resources than honest nodes. Some papers such as [13][14] introduced the use of Public Key Infrastructure (PKI) algorithms for VANETs in which public key cryptography is used to provide solution to the security problem in VANETs.

In [15] a multi-factor authentication scheme is used in addition to public key information. A certificate is issued to all vehicles. These contain not only the public key information but also contain a set of physical attribute values of a vehicle, such as transmitter coverage, radio frequency fingerprint and so on, recorded by CA. In [16] Hubaux et. al. have introduced verifiable multilateration method for performing distance bounding. In this approach, two or three fixed units (RSUs) are used to perform distance bounding. This method is not a very appropriate method to detect Sybil attack as it involves RSUs as a key player in detection mechanism. This method is more infrastructures dependent.

In [17] Demirbas et. al. have presented a Sybil attack detection scheme in wireless sensor networks using multiple sensors Received Signal Strength Indicator (RSSI) measurements. However, it does not mention how to identify honest neighboring nodes. This scheme cannot be applied in situations where nodes are moving, not trusted or may collude in hostile environment. The method suggested in [18][19] requires some trusted monitors for observing the behavior of nodes in a network. This is not realistic in VANET because the Sybil attacker may penetrate these trusted observing nodes and these Sybil nodes will report fake data. A secure hardware based method is proposed in [20] which are built on trusted platform module (TPM). Secure information is stored in shielded locations of the module, where any type of forging or modification of data is impossible. Hence, communication between TPMs of the vehicles is protected from the Sybil attack.

In [21] Guette et. al. have analyzed the effectiveness of Sybil attack in various assumptions of transmission signal tuning and antenna. They showed the limitation of RSS based Sybil attack detection in VANET. In [22] Xiao et. al. have proposed a localized and distributed scheme to detect Sybil attacks in VANETs. The approach takes advantage of VANET traffic patterns and road side base stations. In [23] Zhou et. al. have proposed a privacy preserving method for detecting a Sybil attack with trustable roadside boxes and pseudonyms. Vehicles are assigned a pool of pseudonyms from a centralized unit, which are used for generating traffic messages instead of real identities for privacy reason. Pseudonym belonging to a vehicle is hashed to a unique value. Vehicles cannot abuse these pseudonyms for a Sybil attack. This scheme provides privacy but it is based on the assumption that individual vehicles are registered and managed by trusted authorities.

In the approach discussed in [24][25], RSUs are the only components that issue the certificates to all vehicles passing across them. It is very rare to have two vehicles passing by multiple RSUs at exactly the same time due to the difference of moving dynamics of multiple vehicles. Two messages will be treated as a Sybil attack issued by one vehicle if they have similar time-stamp series issued by RSUs. In [26] Shaohe et. al. have proposed a cooperative RSS based Sybil attack detection for static sensor networks where all nodes have fixed transmission power either it are honest or malicious. This approach does not rely on the accurate position of the nodes rather relative distance among the nodes is used. Each node overhears packets and computes the distance to other nodes using received signal strength. In [7] Jyoti et. al. have proposed and implemented RSS-based Sybil attack detection technique in VANETs. The detection method was based on the similarity in RSS value received by the RSUs.

10 CONCLUSION

Malicious nodes are harmful for proper functioning of VANET applications. If correct traffic information is not delivered to the drivers before the vehicle approaches to the location of occurred event, critical problems can significantly alleviate. In Sybil attack, a malicious node forges multiple or fake identities (either present in the network or not), in order to disrupt the proper functioning of VANET applications. It creates an illusion on road, leading to disruption in the network scenario. In Temporal attacks, a malicious node either impedes or delays the forwarding of critical safety messages received from neighboring nodes. It can also perform replay attack by repeatedly sending the information of events occurred earlier. In this paper, both the attacks are discussed in detail and their solutions which have been proposed in previous studies are mentioned.

11 REFERENCES

[1] C. Siva Ram Murthy, B.S. Manoj, Advanced Information Networking and Applications, 2007. AINA '07. 21st International Conference. In Ad Hoc Wireless Networks: Architectures and Protocols, 2007.

[2] Antonios Stampoulis, Zheng Chai, “A Survey of Security in Vehicular Networks”.

[3] Amer Aijaz, Bernd Bochow, Florian Dtzer, Andreas Festag, Matthias Gerlach, Rainer Kroh, and Tim Leinmller, “Attacks on Inter Vehicle Communication Systems - an Analysis”, In Proc. of WIT, pp. 189-194, 2006.

[4] Nai-Wei Lo, Hsiao-Chien Tsai, “Illusion Attack on VANET Applications - A Message Plausibility Problem”, In Proc. of IEEE Globecom Workshops, pp. 1-8, 2007.

[5] Jiang, L. Delgrossi, “IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments”, In Proc. of Vehicular Technology Conference (VTC), pp. 2036-2040, 2008.

[6] A. Goldsmith, Wireless communications. In Cambridge University Press, 2005.

[7] Jyoti Grover, Nitesh Prajapati, Manoj Singh Gaur, and Vijay Laxmi, “RSS-based Sybil Attack Detection in VANETs”, In IEEE Proc. of the International Conference (TENCON), pp. 2278-2283, 2010.

[8] Nitesh Kr. Prajapati, Jyoti Grover, and M.S Gaur, “Implementation of Temporal Attacks in Vehicular Ad Hoc Networks”, International Conference on Electronic, Information and Communication Systems Engineering (ICEICE2020) 28-30 March, Jodhpur, India.

[9] Jyoti Grover, V.Laxmi, M.S Gaur and Nitesh Kr. Prajapati, “A Distributed Sybil Attack Detection Approach using Neighboring Vehicles in VANET”, The Computer Journal (Oxford), Special Issue on Security and Privacy in Innovative Communication and Services.

[10] B. Parno and A. Perrig, “Challenges in Securing Vehicular Networks”, In Proc. of HotNets-IV, 2005.

[11] John R. Douceur, “The Sybil Attack”, In IPTPS 01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp. 251-260, London, UK, 2002. Springer-Verlag.

[12] James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig, “The Sybil Attack in Sensor Networks: Analysis & Defenses”, In IPSN '04: Proceedings of the 3rd International Symposium on Information processing in Sensor Networks, New York, USA. ACM.

[13] M. Raya and J.P. Hubaux, "Securing Vehicular Ad-hoc Networks", Transactions of Journal of Computer Security, Vol. 15, Issue 1, pp. 39-68, 2007.

[14] Philippe Golle, Dan Greene, and Jessica Staddon, "Detecting and Correcting Malicious Data in VANETs", In Proc. of 1st ACM International workshop on Vehicular Ad-hoc Networks, pp. 29-37, New York, USA, 2004, ACM.

[15] S. Pal, A.K. Mukhopadhyay, and P.P. Bhattacharya, "Defending Mechanisms against Sybil Attack in Next Generation Mobile Ad Hoc Networks", Vol. 25, pp. 209-214. IEEE Technical Review, 2008.

[16] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo, "The Security and Privacy of Smart Vehicles", In IEEE Proc. of Security and Privacy, pp. 49-55, 2004.

[17] Murat Demirbas and Youngwhan Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", In Proc. of International Symposium on World of Wireless, Mobile and Multimedia Networks (WOWMOM), pp. 564-570, 2006.

[18] Chris Piro, Clay Shields, and Brian Neil Levine, "Detecting Sybil Attack in Mobile Ad hoc Networks", In Proc. of Securecomm and Workshops, pp. 1-11, Sept. 2006.

[19] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, and Abraham D. Flaxman, "SybilGuard: Defending against Sybil Attacks via Social Networks", Transactions of IEEE/ACM Transition Networks, Vol. 16, Issue 3, pp. 576-589, 2008.

[20] Gilles Guette and Ciaran Bryce, "Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)", pp. 106-116, 2008.

[21] Gilles Guette and Bertrand Ducourthial, "On the Sybil Attack Detection in VANET", In IEEE Proc. of International Conference on Mobile Ad-hoc Networks and Sensor Systems, pp. 1-6, 2007.

[22] Bo Yu Bin Xiao and Chuanshan Gao, "Detection and Localization of Sybil Nodes in VANETs", In Proc. of the Workshop on Dependability Issues in Wireless Ad-hoc Networks and Sensor Networks, pp. 1-8, New York, USA, 2006, ACM.

[23] Tong Zhou, R.R. Choudhury, Peng Ning, and K. Chakrabarty, "Privacy-Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks", In Proc. of Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous), pp. 1-8, Aug. 2007.

[24] B.Turgut, D.Zou, C.C. Soyoung, and Park Aslam, "Defense against Sybil Attack in Vehicular Ad-hoc Network based on Roadside Unit Support", In IEEE Proc. of Military Communications Conference (MILCOM), pp. 1-7, 2009.

[25] Chen Chen, Xin Wang, Weili Han, and Binyu Zang, "A Robust Detection of the Sybil Attack in Urban VANETs", In IEEE Proc. of ICDCS Workshops, pp. 270-276, 2009.

[26] Xin Zhao, Shaohe Lv, Xiaodong Wang, and Xingming Zhou, "Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks", In IEEE Proc. of International Conference on Computational Intelligence and Security (CIS), 2008.

[27] Gongjun Yan, Stephan Olariu, and Michele C. Weigle, "Providing VANET Security through Active Position Detection", Transactions of Computer Communications, Vol. 31, Issue 12, 2008.

[28] M Raya, P Papadimitratos, and J.P. Hubaux, "Securing Vehicular Communications", In IEEE Transactions of Wireless Communications, Vol. 13, Oct. 2006.

[29] M. Raya and J. P. Hubaux, "The security of VANETs", In Proc. of 2nd ACM International Workshop on Vehicular Ad-hoc Networks, 2005.

[30] W Ren, K Ren, W Lou, and Y Zhang, "Efficient User Revocation for Privacy-aware PKI", In Proc. of 5th International Conference (ICST), 2005.

[31] R. K Schmidt, T. Leinmuller, E. Schoch, A. Held, and G. Schafer, "Vehicle Behavior Analysis to Enhance Security in VANETs", In Proc. of Vehicle to Vehicle Communication (V2VCOM), 2008.