Indian Journal of Science and Technology, *Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/106423, December 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Comparative Analysis of Sybil Attack Detection Techniques in VANETs

Appan Chawla[1], Rajeev Kumar Patial[1] and Dilip Kumar[2]

[1]Department of Electronics and Communication, Lovely Professional University, Phagwara, Punjab – 144411, India; appanchawla@gmail.com, rajeev.kumar@lpu.co.in
[2]Department of Electronics and Communication, Sant Longowal Institute of Engineering and Technology, Longowal, Punjab – 148106, India; dilip.k78@gmail.com

Abstract

Vehicular Ad-Hoc Networks (VANETs), an emerging profile for the improvement of road safety that has a unique ability to possess inter-vehicle as well as vehicle-to-Road Side Unit communication that is to be implemented all across the globe in coming years. Since the communication is carried out along an open wireless medium which makes the network more vulnerable to attacks. Vulnerability of the network can either be the transmission of false information or vehicles assigned with fake identity, and they can possess identity of authorized vehicles or can even attack anonymously. Several techniques have been developed till date for the detection of unauthorized or illegitimate vehicles that downgrades the security of the network. This paper summarizes different techniques that have been developed for the detection of Sybil attack in VANETS.

Keywords: Ad-Hoc Networks, Sybil Attack, Vehicular Ad-Hoc Networks, Vehicular Ad-Hoc Network Attacks

1. Introduction

A great development can be seen in wireless technology in recent years. Ad – hoc networks is a live example of wireless network in which a user can have access to the facilities of wireless networks within a specified range. Ad-hoc is the most explored branch of wireless infrastructure-less network i.e no infrastructure is required to setup the network. It can be setup anytime and anywhere using pre-installed network hardware in the nodes. Vehicular Ad – hoc networks (VANETs, vehicles on road act as nodes of the network), the subclass of Mobile Ad – hoc networks (MANETs, only smartphones are required to setup the network) have gained much popularity these days. It provides a high speed and high mobility communication to be possible in-between the nodes within a specified range. The vehicles (that act as nodes in the network) can communicate within the range of network either stationary or in motion.

The communication in VANETs is carried out in three possible ways i.e. Vehicle-to-Vehicle (V2V), Vehicle-to-Road side unit (V2RSU) and Road side unit-to-Road side unit (RSU2RSU). The Road side units are deployed at the road sides or the nearby buildings. Communication in vehicles is possible through the On-Board-Unit (OBU) installed in the vehicles over a Dedicated Short Range communication (DSRC). The network in VANETs has no fixed infrastructure, so they rely on themselves for any network functionality. VANETs follow the IEEE 802.11p standards assigned to Wireless Ad-hoc Vehicular Environment (WAVE).

*Author for correspondence

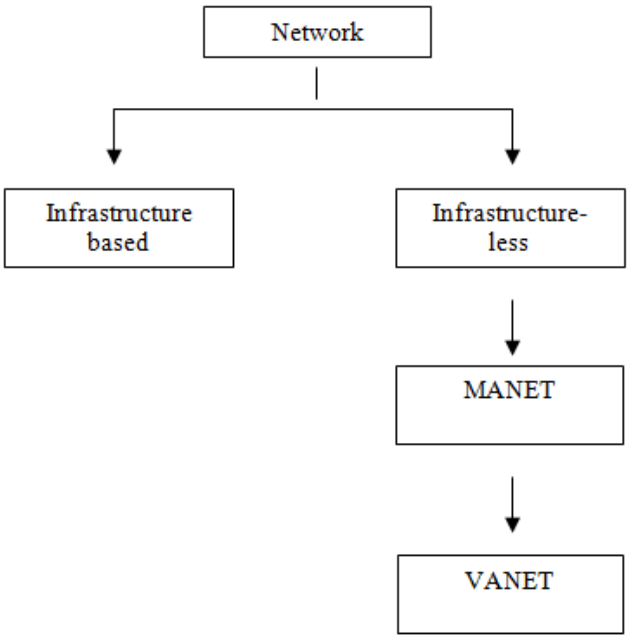

Figure 1. Network hierarchy.

As we know that Ad-hoc network is an open communication network, so there is a possibility of breeching inside the network. Therefore, security of this network is the main issue that is to be taken care of. VANET supports real time communication therefore some security techniques such as authentication, privacy, confidentiality, non-repudiation etc. must be followed in order to transmit as well as receive the information correctly and efficiently. Many attacks are possible that can inject fake information, send false alerts which could create delays, congestion or even jam the network or make the network unavailable for the node. There are several attacks possible that affects the safety and privacy of the vehicle, such as Sybil attack, Intrusion, Data fusion, Denial of Service (DoS), Black hole, Illusion etc.

Most of the attacks that are common in VANETs has been discussed in various research papers have been summarized in this paper. Moreover, for securing the network and preventing it from being attacked by any third-party node, several aggregations schemes are described briefly.

Farzad Sabahi[1] describes different attacks to vehicular networks that alter the security of the network. Various attacks have been discussed in his paper and they are classified into different categories such as attacks to availability, attacks to authentication, and attacks to confidentiality.

Table 1. VANET attacks

Threats to Availability	Denial of Service (DoS)
	Black-hole attack
	Spamming attack
	Malware attack
	Mischievous attack
	Broadcast tampering
Threats to Authentication	Masquerading
	Replay Attack
	GPS spoofing
	Tunneling
	Sybil attack
	Message tampering
Threats to Confidentiality	Eavesdropping

1.1. Threats to Availability

- **Denial of Service (DoS):** The main aim of the attacker is to reduce the performance of the network and overcome the resources of the network available to the nodes, such that the legitimate users of the network cannot utilize the resources[2].
- **Black-hole Attack:** In this type of attack, when the data packets are directed towards the node that previously existed in the network but presently does not exist in the network[3] or is out of the coverage area of the network (called the black-hole node) are lost in the network.
- **Spamming Attack:** The attacker sends unnecessary messages in the network that are of no use to increase the transmission latency and to consume maximum bandwidth of the network.
- **Malware Attack:** In these types of attacks, the attacker injects virus in the network that interrupts the normal procession of the network.
- **Mischievous Attack:** This attack is performed by the legitimate users of the network for their own benefit such as by providing wrong details of traffic jams or route information.
- **Broadcast Tampering:** In this the authentic user of the network transmits fake safety messages in the network that could lead to road accidents

1.2 Threats to Authentication

- **Masquerading:** The attacker sends the message to another vehicle in the network and it appears as the message is sent by the legitimate user of the network.
- **Replay Attack:** The attacker sends the previously generated messages in the network again[5].
- **GPS Spoofing:** The attacker can send fake location information to the GPS device located at the OBU of the vehicle by using a GPS simulator to generate stronger signal to spoof the GPS satellite.
- **Tunneling:** The attacker connects the different locations of the network through an extra communication channel that forms a tunnel between the nodes. Any data transmitted in the tunnel[6] is assumed as it is coming from the nearby vehicles. The attacker can take the advantage of the tunnel by performing a traffic analysis.
- **Sybil Attack:** In this the attacker creates multiple identities (called Sybil identities) and sends messages to the nearby vehicles[7]. This appears as if the messages are transmitted by valid users of the network. The attacker transmits fake information in the network.
- **Message Tampering:** The attacker modifies or changes the information received from the nearby vehicles and transmits further[8], but the actual information is not transmitted.

1.3 Threats to Confidentiality

Confidentiality of messages in the network is the major concern of security of VANETs and is more vulnerable to attack. The attacker can capture the information of the other vehicles (known as Eavesdropping) through broadcast of communication packets and can use the information later on without the permission of the vehicle attacked on.

Mohanty and Jena[9] focused on some of the data aggregation techniques to provide security to network by securing it from several attacks using syntactic, semantic and cryptographic techniques that allowed the network to share information securely with confidentially in an efficient manner Table 2.

Data is aggregated to solve the bandwidth utilization problem i.e. maximum amount of data packets can be transmitted within low bandwidth.

Aggregation techniques can be classified into two types:

a. **Syntactic aggregation:** In this the data packets from multiple vehicles are collected and compressed or encoded to form a unique record.
b. **Semantic aggregation:** In this the information received from the individual vehicle is modifies and only the useful information is kept such as instead of transmitting the information of location of each vehicle, only the number of vehicles in a given area is sent.

There are several other attacks in Ad – hoc networks that are possible in VANETs are: Timing attack, Home attack, Man in the middle attack, Traffic analysis, Social attack, Brute force etc.

Research is still an ongoing process to secure vehicular networks from being attacked by the illegal activities of the illegitimate users. Many techniques have been developed and several others are under research that could prove to be more efficient than that which has already been undergone a research process, to provide security to VANETs.

Furthermore, regarding VANETs is discussed in this paper in detail. This paper id divided into 6 sections namely Section I, Section II, Section III, Section IV, Section V and Section VI.

Table 2. Secure data aggregation techniques

Aggregation scheme	Attacks secured
Syntactic	Spoofing, Bogus information, False Data injection, Forgery attacks
Semantic	False information dissemination
Cryptographic	Forging of atomic reports, Forging of aggregates, suppression of aggregates

Section I gives a brief summary of the work presented in the paper. Section II is the overview of VANETs and describes about the architecture, communication patterns, threats, security and application in VANETs. Section III focuses on the work that has to be pursued further i.e. Sybil Attack detection in VANETs and what actually the meaning of this paper is. Section IV describes various techniques for the detection of Sybil Attack. Section V concludes the whole paper in a brief summary and section VI provides the future work that can be done in this field.

2. Overview of VANETs

Vehicular Ad – hoc networks comprises of large no. of mobile nodes that are able to communicate with each other within a specified range. The Federal Communication Commission (FCC) of United States has allocated Dedicated Short Range Communication (DSRC) licensed spectrum of 75 MHz[10] with a bandwidth of 5.9 GHz and protocol assigned to vehicular networks is IEEE 802.11p as discussed in section I.

In Europe DSRC communication is carried out over a spectrum of 30 MHz over 5.9 GHz band which is used for many applications such as parking management, traffic telematics, transport management etc.[11]. As DSRC system of communication across Europe is not standardized, so it is not used in all the countries[12].

2.1 VANET Architecture

VANET architecture consists of a Road Side Unit (RSU) and an On-Board Unit (OBU) that is installed in the vehicles. The vehicles transmit messages from OBU to another OBU or from OBU to RSU and messages can be trans-received from RSU to RSU.

If any vehicles transmit a message but there is no other vehicle in the specific range a certain vehicle, then the message is stored at the RSU and can be retrieved when any vehicle comes in the its range.

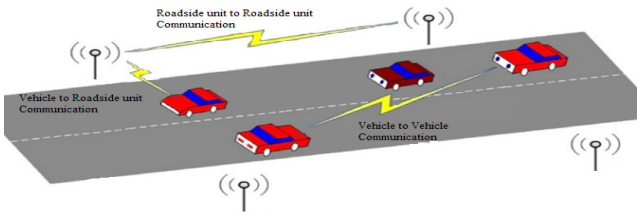

Figure 2. Architecture of VANET.

2.2 Communication Patterns in VANETs

Schoch et al.[13] provided various communication patterns with purpose, communication mechanism, direction, QoS is all described with an example.

- **Beaconing:** Information is updated about the speed, positon and the nearby vehicles among the nodes. The data packets are broadcasted through link layer over single-hop communication.
- **Geo broadcast:** Information about sudden occurrence of an even or an abnormality is broadcasted over a larger area in which sender attaches the determined location with message.
- **Unicast Routing:** Unicast transportation of messages in a specified direction. Multi-hop communication is more suitable for this communication.
- **Advanced information Dissemination:** Provides information to the vehicles those experiences a delay due to network partitioning. The messages with high priority are handled first when the bandwidth is available for a limited period.
- **Information Aggregation:** Communication overhead is reduced which in turn decreases the probability of collision and dropping of packets.

2.3 Security Threats and Attacks

As already discussed in section I briefly about VANET attacks that are classified as follows: threats to –

a) Availability
b) Authentication
c) Confidentiality

All these attacks can be further classified as[14]

a) Network Attacks
These attacks are considered to be of high priority as these directly affect whole of the network and make the network unavailable for the legitimate user. Various attacks that comes under this category are Dos, Distributed DoS (DDoS), brute force, malicious node, node impersonation, Sybil attack.

b) Application Attack
The most important application of VANET is safety of the user. This attack affects the safety of the user by changing the content of the actual message and transmitting the fake message. Fake information dissemination and bogus information are some that the attacks that comes under this category.

c) Timing Attack
The main aim of the attacker is to add some time delay in the original message so that the message is not transmitted at the required time but is transmitted after some other instant of time when the information is not required. This could cause misshaping on the road.

d) Social Attack
In this the attacker transmits unnecessary messages in the network to diver the attention of the user. The

attacker transmits the information that is not related to the required information such as attacker can send jokes that frustrated the legitimate user which in turn affect the user to user to keep an eye on road.

e) **Monitoring Attack**
The attacker monitors the network and listens to the conversation messages between the vehicles and misuses the required information shared between the vehicles. All the vehicles have unique identification that helps them to provide the actual location, the attacker can disclose the unique ID of a certain vehicle in the network which affects the privacy of the vehicle.

2.4 Applications

VANET provides a variety of applications that could led to the advancement of standard of vehicles on roads. This advancement is called as Intelligent Transport Communication (ITC) system, the author in[15] classified various applications as follows:

a) **Safety**
Safety application includes monitoring of vehicles on roads, surface of road, and curves on road. It includes traffic analysis, message transfer, crash notification, hazard control notification, and collision warning.

b) **Commercial**
Commercial applications provide the vehicle with entertainment services such as audio and video streaming and web access services. The driver can have internet access.

c) **Convenience**
These increases the efficiency of traffic by traffic management which includes route diversions, electronic toll collections, parking availability etc.

d) **Productive**
Some positive aspects can be extracted from these productive applications such as environmental benefits, time utilization and fuel saving.

3. Sybil Attack in VANETs

VANETs consist of two types of vehicles or nodes or users i.e. legitimate user and illegitimate user. Legitimate users are referred to as authentic or valid users of the network whereas illegitimate users are referred to as invalid users in the network. The legitimate are assigned with unique identification number with each vehicle whereas illegitimate user uses the fake identity or unknown identity or the identity of the vehicle that was previously present in the network but currently is out of coverage area of the network or left the network.

The nodes or vehicles i.e. the legitimate users of the network that are able to forge their original identity to acquire an unknown identity or the identity of any other vehicle that is existing or previously existed in the network, are said to Sybil nodes and the attacker is called as Sybil attacker.

The Sybil attacker can also create multiple identities and can disseminate false information in the network for his personal benefits.

4. Detection Techniques

Several techniques have been introduced for the detection of threats in vehicular network. This paper focused on some specific techniques for the detection of sybil nodes that are responsible for fake information dissemination in the network.

Based on some of the attacks, solutions for detection and injection of fake information in the network is provided.

Sybil attack

Trusted certification method presented by Sannella[16] proved to be the most effective method to detect Sybil attack. Each node in this is issued a certificate for authentication by Centralized Central Authority (CCA). Node with a certificate of authentication is legitimate and other will be fake.

Trusted devices approach by Yu and Lau[17] prevents the attacker node to get mapped with the network hardware. One-to-One mapping of each node in the network is done with a hardware device and assumed that attacker node will not get mapped with the hardware.

Detection approach by Grover J. et al[18] identifies the Sybil attack from the information received from beaconing packets that validates the authenticity of the node in the network and consists of the location coordinates and neighbor information of the node. As no two nodes can possess same location coordinates and same set of neighbors and that too for a time period greater than threshold value. Moreover, the transmit power of the Sybil identities will be different from the legitimate nodes while sending the beaconing packets.

Triki et al (2013)[19] presented a privacy preserving solution to protect against Sybil attack. Author proposed two authentication techniques–RFID tag that are embedded in the vehicle used to get the vehicle authenticated at the nearby RSU. This gets a validation certificate for a shorter lifetime. The other technique uses the certificate obtained in the first technique to validate the vehicles.

A robust detection of Sybil attack by Chen et al (2009)[20], detects the Sybil attack on the basis of motion trajectories of the vehicle. Here each vehicle is assigned different signatures depending upon motion trajectories. The statistical judging is conducted on different set of signatures by using hypothesis testing method that differentiates the vehicles from the Sybil nodes.

A timestamp series approach proposed by Park et al (2009)[21] to secure against Sybil attack in a vehicular specially appointed system taking into account street side unit support. The proposed approach works well when RSU is accessible and vehicle has communication capability. In this methodology RSUs are the main segments giving the endorsements. It is not possible that two vehicles are passing through various PSUs precisely at the same time due to Variance of flow of vehicles. The technique developed as time-stamp arrangement technique needs neither vehicle based open key base nor Internet access at the Road Side Unit.

Zhaou et al (2011)[22] Proposed P2DAP strategy for recognition of Sybil attack. Author introduced a lightweight and versatile convention to distinguish Sybil attacks. This strategy does not require any hub in the system to share its personality and hence security of the vehicle is increased.

Xiao, Yu and Gao (2006)[23] proposed a lightweight security strategy for identifying and limiting Sybil nodes in VANETs. This is taken from measurable investigation of sign quality dispersion diagrams. The plan ends up being a method wherein every node in the system can perform the discovery of nodes through area check. With a specific end goal to beat the impediments of the fundamental plan, the author proposed a method to keep Sybil aggressor to conceal for each other. RSU is utilized to have better results. The Accuracy of area confirmation is improved with the help of measurement calculations. The calculations can distinguish Sybil attacks by recognizing the sign quality conveyance with respect to time.

A cooperative Sybil attack in VANETs by Hao Y. et al (2011)[24] proposed a security convention to distinguish Sybil attacks for position based applications. Vehicles in our convention distinguish sybil assaults by looking at the judiciousness of positions of vehicles locally. The attack identification has attributes of correspondence and GPS position of vehicles which are incorporated for message propagation. No additional equipment and little correspondence and calculation overhead will be acquainted with vehicles. Accordingly, here convention is light weighted and appropriate for genuine applications

Yu B. et al (2013)[25] proposed a strategy to check the positions of potential Sybil nodes. We utilize a Random Sample Consensus (RANSAC)- based calculation to make this strategy more hearty against anomaly information created by Sybil hubs. In any case, a few natural downsides of this technique brief us to investigate extra methodologies. They presented a measurable strategy and configured a framework that can confirm where a vehicle originates from. The framework is has made a Presence Evidence System (PES), with which we can improve the identification precision utilizing investigation over a perception period.

5. Conclusion

In VANETs, there is continues transmission and reception of data in between the nodes. For efficient sending and receiving of message, information should be correctly transmitted. Fake information dissemination in the network deteriorates the security of the vehicle and safety of users on roads. Detection of nodes transmitting fake information and solution to prevent such behavior is a much popular topic in research. In this paper different proposed techniques for detection of Sybil Attack are discussed and that have been in the recent researches.

6. Future Work

Most of the research is conducted to improve the security and safety of VANETs. There exists a good trade-off between security and efficiency. Further research could be conducted in vehicular networks to make it more efficient. However, we cannot call a system to be ideal system that can be 100 percent secure, but there might be an advanced level techniques to be developed in future to make the vehicular networks secure and safe enough to implement Intelligent Transport Communication (ITC) all across the globe.

7. References

1. Farzad Sabahi, The security of vehicular adhoc networks. IEEE Third International Conference on Computer Intelligence, Communication system and Networks; 2011.
2. Hasbullah H, et al. Denial of Service (DOS) Attack and Its Possible Solutions in VANET. World Academy of Science, Engineering and Technology; 2010.
3. Sharma S, Gupta D. R. Simulation Study of Blackhole Attack in the Mobile Ad hoc Networks. International Conference on Network Applications, Protocols and Services; 2008.
4. Krishnamurthi N. et al. Topology control for future airborne networks. 28th IEEE conference on Military communications 2009.
5. Parno B, Perrig A. Challenges in Securing Vehicular Networks. The HotNets-IV; 2005
6. Akanksha Saini HK. Comparison between Various Black Hole Detection Techniques in MANET. The National Conference on Computational Instrumentation; 2010.
7. Guett G, Bryce C. Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs). WISTP; 2008.
8. S. Zeadally, *et al.* Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges; 2010.
9. Sagarika Mohanty, Debasish Jena. Secure data aggregation in vehicular-adhoc networks: A survey. Elsevier, Procedia technology 6. 2012. p. 922-29.
10. Maxim Raya, Jean-Pierre Hubaux. Securing vehicular ad hoc networks. Journal of computer security 15. 2007. p. 39-68.
11. Franciscatto BR, Souza AC, Defay C, Trang TT, Vuong TP. High gain microstrip patch antenna array using multiple substrate layers for DSRC applications, in Antennas and Propagation in Wireless Communication (APWC). 2012 IEEE-APS Tropical conference on. 2012. p. 736-39.
12. ETSI, Available from: http://www.etsi.org/standards.
13. Schoch E, Kargl F, WeberM. Communication patterns in VANETs. IEEE Communication Magazine. Nov 2008. p. 119-25.
14. Irshad Ahmed Sumra, Iftikhar Ahmed, Halabi Hasbullah Jamalul-lail bin Ab Manan. Classes of attacks in VANET. IEEE; 2011.
15. Vishal Kumar, Shailendra Mishra, Narottam Chand. Applications of VANETs: Present & Future. A Journal on Computer and Networks. 2013. p. 2-15.
16. Sannella MJ. Constraint satisfaction and debugging for interactive user interfaces. [Doctoral Thesis]. University of Washington; 1994
17. Yu YT, Lau MF. A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions. Journal of system and software; 2005.
18. Grover J, Gaur MS, Prajapati VLNK. A Sybil attack detection approach using neighboring vehicles in VANET. SIN'11, Sydney, Australia; 2011.
19. Triki B, Rekhis S, Chammem M, Boudriga N. A Privacy Preserving Solution for the Protection against Sybil Attacks in Vehicular Ad Hoc Networks. IFIP WMNC; 2013.
20. Chen C, Wang X, Han W, Zang B. A Robust Detection of the Sybil Attack in Urban VANETs. 29th IEEE International Conference on Distributed Computing Systems Workshops; 2009.
21. Park S, Aslam B, Turgut D, Cliff C. Zou. Defence Against Sybil Attack in Vehicular Ad Hoc Network Based On Roadside Unit Support. IEEE; 2009.
22. Zhou T, Choudhury RR, Ning P, Chakrabarty K. P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks. IEEE Journal on Selected Areas in Communications. Mar 201; 29 (3).
23. Xiao B, Bo Yu, Gao C. Detection and Localization of Sybil Nodes in VANETs. DIWANS'06, Los Angeles, California, USA. Sep 25 2006.
24. Hao Y, Tang J, Yu Cheng. Cooperative Sybil Attack Detection for Position Based Applications in Privacy Preserved VANETs. IEEE Globe com proceedings; 2011.
25. Bo Yua, Xu C-Z, Xiao B. Detecting Sybil attacks in VANETs" Elsevier; 2013.