March - April 2020
ISSN: 0193-4120 Page No. 9103 - 9109

An Overview of Security in VANETS

[1]Karan T P, [2]Mamatha Jadhav V
[1]Student, [2]Assistant Professor, Department of Computer Science and Engineering, Ramaiah Institute of Technology, Bengaluru – 54
[1]karantp96@gmail.com, [2]mamsdalvi@msrit.edu

Article Info
Volume 83
Page Number: 9103 - 9109
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 09 April 2020*

Abstract
Vehicular communication is one of the growing aspects in the communication industry. Cooperative Intelligent Transportation Systems (CITS) in view of a correspondence among vehicles and clever roadside foundation can be of an extraordinary advantage with respect to street security, traffic blockage and ecological effect of the vehicle. Some characteristics of VANET are high mobility of the nodes, dynamic nature of the network, self-organisation and distributed networking. In such a communication system, it is difficult to establish a fixed security model. Because of high mobility of the nodes, the nodes may be exposed to multiple security attacks. The packet communication in VANET is open-environment making it susceptible to attacks. Such attacks may damage the nodes and the network entirely. There are various studies related to the security in VANET. But the security field in VANET is ever growing as there cannot be a limit to the ways which the attackers may exploit and harm the network. Some schemes have been proposed for the security in VANET. These schemes have been implemented via simulations of the network because it is hard to establish and monitor a vehicular ad hoc network physically. The paper presents an overview of the security in VANET by discussing various security attacks, attackers and a few proposed schemes based on security

Keywords; *VANETs, security attacks, security schemes*

I. INTRODUCTION

With the continuous growth of technology, it is necessary to opt for more advanced and optimised forms of communication. The establishment of a wired communication is becoming outdated and is being replaced by wireless communication. In wireless communication too there are various advancements. The establishment of the network has become more dynamic and more responsive to the changes in the environment. One such dynamic wireless mode of communication is the vehicular ad hoc networks. In simple words, vehicular ad hoc networks (Vanets) are communication networks established between any two vehicles or among a group of vehicles. It need not be restricted to communication only among vehicles. The vehicles can communicate with other road side units (RSUs) and exchange information to optimise the routing of the vehicles. As the name itself says, Vanets are ad hoc networks. They do not have a fixed topology that must be maintained for communication. There are various routing protocols specified for Vanets like the ad hoc on demand distance vector routing (AODV) protocol. Based on the type of entities involved, there are three basic types of communication in Vanets – vehicle-to-vehicle communication (V2V), vehicle-to-infrastructure communication (V2I) and vehicle-to-anything (V2X) communication. V2V communication can be considered as communication between two vehicles near each other. Each vehicle can share information regarding its position. V2I communication deals with the communication between the vehicles and road side units. The road side units may be the cell phone tower or any such entities that can help broadcast information to a vehicle in the network. V2X communication is basically the communication

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9103 - 9109

between the vehicle and anything that can share information.

Some of the characteristics of Vanets are high mobility of the nodes, dynamic nature of the network, self-organisation and distributed networking. Vanets have their disadvantages as well. The topology is not fixed and is very susceptible to changes because of the high mobility nature of the nodes. Because of a varying topology, the nodes are vulnerable to attacks. It is easy for attackers to target such a network which does not have a fixed topology as there are multiple opportunities to harm the network. Therefore, security in Vanets is a challenging but highly important aspect. For instance, a network may have emergency messages which should not manipulated or tampered with. Such messages should be given more priority than regular route update messages. Such emergency messages may contain information about traffic incidents or road condition, etc. Modification of such messages may lead to an erratic behaviour like traffic jams, topology changes and impact on the drivers' behaviour. Some attackers may spread bogus information about the road condition for an optimised route for itself which may be harmful for the network. It is necessary to gather information about such messages and the nodes transmitting such messages in order to take preventive measures among such nodes and have an optimised communication. The other security challenges incorporate the mass size of the system, the high versatility and dynamic topology of the vehicles which may bring about successive separations and short association lengths, errors in key appropriation in VANET, number of bundles directed in the wake of discovering great course and client protection while following the vehicles and so on requires the need of research in this field.

The research in the field of security for Vanets is not new and has been an ongoing process for a few years. There are papers that discuss the various types of security attacks in Vanets. Research to design and specify some security schemes to protect the network has also been in the works. This paper gives an overview of the various attacks and a few security schemes defined for Vanets.

This paper gives an outline of the ongoing exploration progresses in VANET security benefits by indicating the premise of VANET security, grouping different assaults and looking over different papers that have proposed security schemes to conquer the various security attacks.

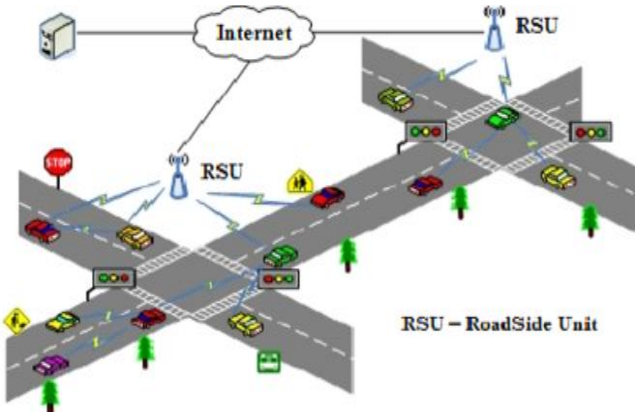

Fig 1. A Typical VANET Scenario

II. SECURITY ATTACKS IN VANETS

a. Sybil attacks

Sybil attack [[5]] is a type of bogus attack [[4]] in Vanets. In sybil attacks, the intruder intentionally claims the identities of the vehicles and uses these identities to disturb the functionality of Vanets. The malicious node impersonates as other nodes and claims the resources that are meant for the honest nodes. The attacker will generate multiple false identities randomly and uses them to infiltrate and harm the network. Detection of the attacker is difficult because the attacker impersonates the node making the sender believe that it is legitimate. There are certain schemes being used for the detection of such malicious nodes in the network. The sender can use the geographical location of the nodes in the network to determine if the node is indeed genuine or has been impersonated. This may be difficult in a large-scale network, but it can be managed in

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9103 - 9109

clusters. Realisation of the malicious node should be given more priority if a sybil attack has been detected. It is necessary to diffuse the attack when it does not have a severe impact on the performance of the network. In a cluster network, the identities can be stored in a centralised server which can authenticate whether the node belongs to the network or it is a malicious node. This process is not straightforward in case of sybil attacks as the malicious node impersonates the honest existing nodes. The honest nodes in a network can be assigned a unique ID which only the network nodes can identify thereby helping identify if the node is malicious. In case of a misbehaviour in the network, the sybil node will simply blame other nodes in the network therefore confusing the system. The malicious nodes can be detected using techniques like position verification and message authentication. The honest node can send periodic beacons or signals indicating its current status with respect to the network. Some RSUs maybe the point of communication for the beacon messages. The beacon messages can be authenticated to guarantee security during packet delivery. The malicious nodes can be detected by comparing the vehicle ID of broadcast and received messages.

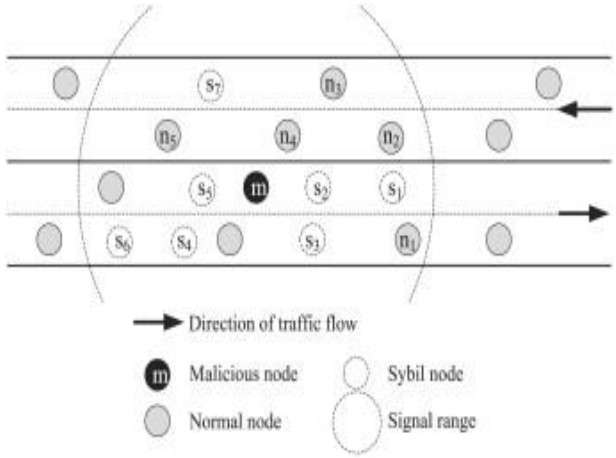

Fig 2. A representation of Sybil Attack

b. Masquerading

Masquerading, in simple words, means to act as someone else. An attacker poses as someone that the sender and the receiver trust. The attacker personates some other vehicles by providing false ID. It is an attack on authenticity. Masquerading attacks [[6]] may not alter the data that is being transmitted but it can interrupt and delay the transmission of the messages. The attacker may observe the network and can modify a route to pass through it. The attacker can receive the messages from a sender and send an entirely different message to the actual receiver by impersonating as the sender. If the receiver and sender do not have an agreed upon authentication procedure, the attacker can easily harm the network in this manner. The attacker will intercept the acknowledgment message from the receiver and sends a harmful acknowledgement to the sender impersonating the receiver. There are various methods to defend against masquerading like using certificates, digital signatures. Masquerading in one of the easier attacks to defend from but it is also easier for attackers. If the attackers can get information about the topology and the network itself, then they can act as they belong to the network and harm the network.

c. Black hole attack

In black hole attack [[3]], the malicious node broadcasts to the network claiming that it has the shortest path to the destination node. Some protocols that have been observed under black hole attacks are Ad-hoc On-demand Distance Vector routing protocol (AODV) and the Optimised Link State Routing protocol (OLSR). The black hole attacks in AODV is of two types. The first is the internal black hole attack in which the malicious node is fitting itself between the source and the destination. The internal attack is more difficult to defend because of the attacker behaves as a legitimate member of the network. The malicious node will make itself available in the active data route without checking its routing tables and will broadcast that it has the shortest path to the destination. Since the shortest path is the optimal path, the sender node accepts the route and sends the information through the malicious node. In external black hole attack, the

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9103 - 9109

attacker is not part of the network but can deny access to network traffic. External attack becomes an internal attack when it takes control of a node in the network and disrupts the network. The malicious node will observe the active route and sends a route reply packet with a spoofed destination address and a low hop count. This route reply packet helps the malicious node to get into the network as it has broadcasted to have the shortest route to the destination. The malicious node will then drop all the data belonging to the route. In OLSR black hole attack, the attacker node ensures that all the data will go through it by acting as a bridging node between the source and the destination. The malicious node gets a privileged position in the network to carry out attacks. This has a larger effect than a malicious node near the sender or destination nodes because the attacker node gets complete control of the network.

d. Denial of Service

This attack is done to restrict users from accessing the network. The attacker aims to jam the network by sending unusable information. The attacker may also broadcast false messages about the network thereby restricting the users' access to the network. One such example would be broadcasting a lane closure message to not allow other nodes to communicate with the node. Denial of service [[8]] influences the availability of the network. The node trying to communicate with another node is blocked by the attacker and denes service for the node. The requesting node may not know the actual truth about the network an may choose to believe the message that has been broadcasted by the malicious node. Denial of service is a network attack. Denial of service done through several different mediums is called a distributed denial of service attack. The malicious nodes may adapt and employ different mediums to infiltrate and harm the network. Several messages are sent to RSUs and other vehicles to jam the communication between the vehicle and RSU and reduce the efficiency. Identification of nodes in denial of service attacks should be efficient and fast to achieve minimum harm. Denial of service can work along with impersonation attack by acting as an honest node of the network and restricting access to other nodes in the network.

III. PROPOSED SCHEMES IN VANETS

Security in Vanets is majorly based on trust between the nodes in the network. The following proposed schemes are also based on trust between the vehicles and also between vehicles and roadside units and between the vehicles and the infrastructure.

a. Trust based routing

In Vanets, the vehicles actively collect and share information to its neighbouring vehicles. An efficient message trustworthiness scheme is necessary to share messages in a timely manner [[1]]. There have been many researches in the trust management in Vanets which use trust as a basic criterion for interaction. However, only depending on the trust values from peer nodes may lead to incorrect decisions. Trust management can be classified into centralised and distributed. The two classifications have their shortcomings as well. Centralised management does not scale well whereas distributed approach faces security and node management issues. Therefore, a centralised server with distributed approach to communicate with the nodes can be established in the network to exchange and update the trust levels and traffic related information.

The centralised server can be implemented in the cloud which helps to scale and provides a layer of security. The vehicles can be the client nodes. The base theory of this scheme is to verify the trust levels of the vehicles that are sending the messages. The centralised server decides upon a certain threshold value to verify the trust levels of the vehicles. A random ID is assigned to the client nodes along with a default trust level. The vehicles communicate with the centralised server to exchange traffic related event messages. When a

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9103 - 9109

vehicle observes a critical event, it broadcasts the message to the neighbouring nodes and the centralised server. The vehicles that receive the message need to authenticate whether to accept the message or not based on the trust levels. The vehicle queries the server to obtain the updated trust levels of the vehicles. After receiving the response, it checks whether the trust level satisfies the threshold value earlier decided upon. If it satisfies, the event message is accepted. Otherwise, it is rejected.

The central server collects, stores, manages and updates all the information related to the network. It calculates and updates the trust level based on the reported event messages. Upon a request from a vehicle, the server sends the most recently updated trust levels of the vehicles. The server updates the trust level based on a voting mechanism on the feedback messages.

This scheme was proposed in [[2]] by RakeshShrestha et.al. The trustworthiness of the messages was observed to be high. The scheme was observed to be energy efficient and effective in real time.

b. PKI based V2V

Public Key Infrastructure is one of the basic security schemes. In a network, there is generally a dedicated node for the public key generation and sharing. The PKI based security scheme has the following environmental parts: vehicle groups, road side units and infrastructure. The vehicle groups are spread over geographical areas with group leaders and members. RSUs relay the information between vehicles and infrastructure and vice versa. Infrastructure is responsible for a Public Key Infrastructure that ensures a layer of security. The vehicles are formed into groups dynamically and a group leader is selected. The groups are formed based on the direction and speed of the vehicles. The group leader forms a separate group key pair for its group members. This key pair is encrypted with a group key. A group-based Hybrid Trust Model [[9]] is adopted to evaluate the trustworthiness of the vehicles in the Vanets based on their behaviour in the groups.

Various parameters contribute towards defining the trustworthiness of a vehicle that are related to communication, GPS sensors or the transmission/reception of the vehicles. A certain threshold is assigned to the parameters to be measured against. If the trust score exceeds the threshold level, the vehicle is deemed trusty otherwise misbehaviour detection algorithms have been defined that help filter out malicious nodes and take specific actions. The most trustworthy vehicles could be group leaders while the malicious nodes should be broadcasted to the group to alert the members.

c. Group based authentication in V2V communications

In V2V communication, the information exchange through wireless channels require a secure environment to avoid attacks. Injection of erroneous messages, revelation of identity, unauthorised access, usurpation of identity, denial of service, etc are examples for attacks found in a wireless channel. HamssaHasrouny et.al [[7]] propose a group-based authentication for V2V communication. The vehicles moving in the same direction are grouped into cluster. Depending on the speeds of the vehicles the groups may not be constant and keep changing. To keep in touch, the vehicles can broadcast a message to refresh their adherence and position within the group. A group leader can be chosen offline which can generate private and public keys for digital signature of the group. The group leader will change the keys periodically when a member is joining or leaving the group without the help of a CA.

Within the group, the authentication is done with RSU. For a new vehicle joining the group, the RSU authenticates the vehicle with the CA and generates a new symmetric encryption key and offline private

Published by: The Mattingley Publishing Co., Inc.

and public keys for the digital signature. The overlapping vehicles have the signatures of both the groups.

Group management is necessary to have an updated information about the members in the group and to have an updated digital signature for the group. The first vehicle that authenticates with the RSU is elected as group leader. The second vehicle to authenticate is elected as group leader backup. The group leader creates a groupID and generates an offline digital signature and symmetric encryption key for the group and broadcasts it. For every new vehicle that joins the group, the group leader regenerates the digital signature and the symmetric encryption key and broadcasts them.

The messages that are transmitted within the group follow a certain encryption procedure. The message is first encrypted by the group symmetric key and the group public key. This is signed by the private key of the group. The constant changing of the keys makes it easier to defend from attacks like eavesdropping, man-in-the-middle, privacy violation, etc. But the constant changing of the keys is not the most feasible solution for security in a large scale model.

d. Fuzzy logic-based trust model

Fuzzy logic is an approach to computing based on degrees of truth rather than the usual true or false. The truth values in fuzzy logic may be any value between 0 and 1. Estimating trust is a difficult activity which is simplified using fuzzy logic. Fuzzy logic-based trust models provide a natural outline to handle with uncertain behaviour and acceptance of inaccurate values. The importance of fuzzy based trust model contains critical characteristics like trustworthiness assessment for decisions given by a vehicle. The aim of fuzzy based trust model is to establish trustworthy values of data received. The fuzzy logic-based models determine the trust levels of the vehicles based upon three modules. These three modules act like trust metrics and help in determining the trust levels of the members in the network. Trust metrics tell about the properties of trust. Trust metrics are an essential significance for the trust models. Trust metrics ensure which trust model for VANET really exist in current scenarios.

The nodes or vehicles in a vehicular adhoc network have a common characteristic wherein any vehicle that passes through an event will gather information about the event. The data is shared through clustering mechanism. The vehicle takes necessary decisions and decides whether to broadcast the information or not. Fuzzy logic is one of the methods how the vehicles can be organised into clusters. Each cluster elects a cluster head depending upon a method that has been decided beforehand. The cluster head collects information about the events based on trust levels that are determined using game theory methodology. The addition of the vehicle to the cluster is shared using probabilistic forwarding method. Replication mechanism is used to broadcast information about the event to every vehicle in the cluster. The cluster head is responsible for sharing the information with its cluster members. If a vehicle that leaves the cluster is the cluster head, then the cluster head position is assigned to another vehicle. The trust parameter is kept as an important issue. In [[10]], an analysis of various trust models satisfying trust metrics is performed. The fuzzy logic-based trust model is observed to satisfy all the considered trust metrics.

IV. CONCLUSION

Vehicular ad hoc network is the future of vehicles, drivers and passengers. There is a need of more research here as a result of its significance and dangers required for people. This paper plans to provide an overview of the various types of attacks to the security of Vanets and provides some methods or schemes to establish security. In this paper we have examined different security attacks on Vanets. The paper additionally exhibits a review of some proposed security plans to guard against such assaults.

REFERENCES

[1] AmiraKchaou, RymaAbassi, SihemGuemara El Fatmi, "*A New Trust Based Routing Protocol for VANETs*",2018 Seventh International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, 2018, pp. 1-6.

[2] RakeshShrestha, RojeenaBajracharya, SeungYeob Nam, "*Centralised Approach for Trustworthy Message Dissemination in VANET*", NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, 2018, pp. 1-5.

[3] VimalBibhu, Kumar Roshan, Dr. Dhirendra Kumar Singh, "*Performance Analysis of Black Hole Attack in Vanet*", International Journal of Computer Network and Information Security, 47-54, 2012

[4] Asline Cedes, N. Edna Elizabeth, "*Verification Based Authentication Scheme for Bogus Attacks in VANETs for Secure Communication*", 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2018, pp. 0388-0392.

[5] Celestine Iwendi, MueenUddin, James. A. Ansere, P. Nkurunziza, J. H. Anajemba, Ali Kashif Bashir, "*On Detection of Sybil Attack in Large-Scale VANETs Using Spider-Monkey Technique*", in IEEE Access, vol. 6, pp. 47258-47267, 2018.

[6] Nice Mathew, V. Uma, "*VANET Security – Analysis and Survey*", 2018 International Conference on Control, Power, Communication and Computing Technologies (ICCPCCT), Kannur, 2018, pp. 100-106.

[7] HamssaHasrouny, Carole Bassil, Abed EllatifSamhat, AnisLaouiti, "*Group-Based Authentication in V2V Communications*", 2015 Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP), Beirut, 2015, pp. 173-177.

[8] RajdeepKaur, Tejinder Pal Singh, VinayakKhajuria, "*Security Issues in Vehicular Ad-hoc Network (VANET)*", 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, 2018, pp. 884-889.

[9] HamssaHasrouny, Carole Bassil, AbedEllatifSamhat, AnisLaouiti, "*A Security Solution for V2V Communication within VANETs*", 2018 Wireless Days (WD), Dubai, 2018, pp. 181-183.

[10] S. Sumithra, Dr. R. Vadivel, "*An Overview of Various Trust Models for VANET Security Establishment*," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bangalore, 2018, pp. 1-7.