ISSN No. 0976-5697

Volume 7, No. 3, May-June 2016

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review: Analysis of Various Attacks in VANET

Shikha Sharma[1] & Er.Shivani Sharma[2]
M.TECH Scholar[1] & Assistant Professor[2]

Abstract: In Vehicular communication, the security of the system averse to the attacker is very essential part in vehicular technology. There are various types of attacks arises in the network. In this paper we will study about Sybil attack. Sybil attacks have been appraised as a significant security threat to ad-hoc networks. The Sybil attack in computer security is an attack where the original identity of a vehicle is distorted or stealing by an attacker to create multiple dummy identities. Detecting such type of attacker & the authentic vehicle is a provocation task in VANET. This survey paper briefly furnishes the Sybil attack in VANET.

Keywords: Vehicular Ad-hoc Network (VANET), security, Sybil attack

INTRODUCTION

From the last few years, growth of wireless products on motorized vehicles involved remote keyless entrydevices, laptops, and mobile telephones, automotive industries have opened a huge change of prospect for both drivers and their passengers. Vehicular Adhoc Networks (VANETs) have engaged a lot of awareness in research section because of theirvaried value and services, namely vehicle security, automated toll payment, traffic management,improvement in navigation, location-based services for finding the nearest propellant stations, travel cottage or restaurants and simply access to the Internet.[6]Vehicular communication is specified as communication between the vehicles.[1] It is a subscription of MANET. It is an important and prominent area of research in the field of vehicular technology. Vanets are self-configuring systems where nodes are act as vehicles.Vanet is an Intelligent Transportation System in which vehicle act as sender, receiver & router to broadcast the information to the vehicular network. Its aim to provide timely information, security, & management of network. Vanets are dynamic in nature because connection between nodes is impermanent. It is designed for vehicle and vehicle and vehicle to infrastructure communication.[8] Due to accidents and road mortality increasing day by day, people are facing problem & need safety. so security in VANET is very essential, because the message sent by one vehicle might have important outcome such as accident prevention. Its main objective of exploiting vanet is to diminishing the level of accidents and provides safety to the passengers sitting in the vehicles.[8]

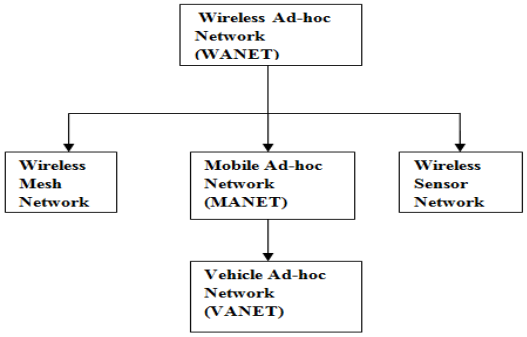

Fig 1: Hierarchy of Wireless Ad-hoc Network[6]

VANET OVERVIEW

VANET ARCHITECTURE

Vanet design largely composed of vehicles, road side units and infrastructure domain (I), communication is regulated largely by using wireless standards e.g. (IEEE 802.11p) .RSU act like a router and has high horizon than vehicle horizon.RoadSide Units (RSUs) arestands for fixed nodes provided along the path.On Board Unit (OBU)introducing to mobile nodes (i.e. vehicles) provisioned with some sort of radio interface that give the authority for communicating with other nodes in wireless manner**.**Vehicles are installed with on board unit for transmission. It is also installed with GPS for knowing its exact position as well as for tracking other vehicles. ELP is a electronic license plate is also set in the vehicle for recognition. A certificate authority (CA) service in the design for providing services and applications.[1]

Intelligent transportation system

It means that the vehicle itself proceed as a sender, receiver and router for distributing/disseminating the data information. It is a technique for transmitting information and provide communication facility to transport infrastructure and vehicles. It is based on IEEE 802.11p standard for (wave) wireless access for vehicular environment. ITS provides two types of communication in vanet. First is V2V mean vehicle to vehicle and second is vehicle to infrastructure (V2I). V2V communication uses multi-hop communication (multicasting/distributing) for communication of data.V2I communication composed of two type of communication. First Naive broadcasting which fabricate warning at systematic intervals and Intelligent broadcasting which generates messages on demand.

V2I uses single hop communication.RSU transmit message to the vehicle in domain. It has a high bandwidth connection between the vehicles and the RSU's.[1]

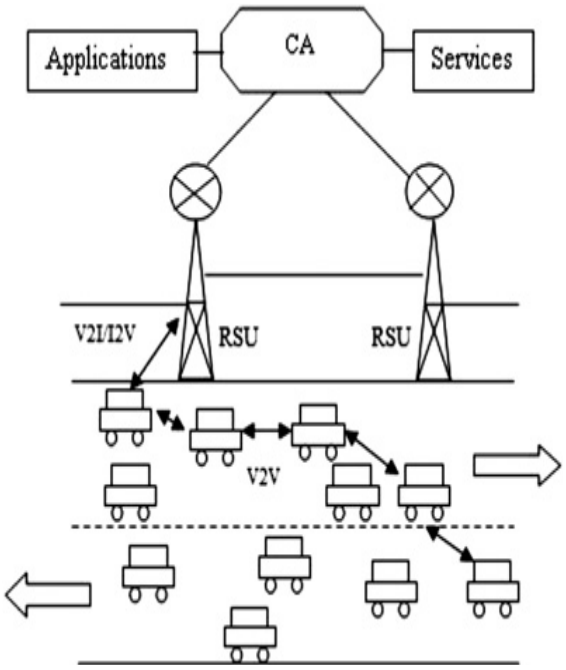

Fig 2: VANET Architecture[1]

VANET STANDARDS

Standards are basically used for the expansion/growth of the product and also to accommodate users to demonstrate and differentiate the products. Many standards are used such as security, services, routing & so on. These are some standards which are used in VANET such as DSRC and wireless access in vehicular environment (WAVE). These standards are defined by FCC in IEEE 1609.14 and 802.11p. DSRC is developed by the USA. The communication takes place between V2V and V2I within this domain. It provide the communication range from 300km to 1km. WAVE is also acknowledged as IEEE 802.11p.It furnishing the ITS application for a small range communication .It composes the standard of IEEE 1609.This is the upper layer standard.[1]

ATTACKS

There are various types of attacks that can affect the entire system or can mortify the execution of system. These attacks can be marked into subsequent types:[7]

Impersonate: In impersonate attack attacker assumes the identity and benefits of anapproved node, either to make use of network assets that may not be convenient to itunder normal position, or to distort the normal functioning of the network. Thistype of attack is completed by active attackers. They may be insider or outsiders. Thisattack is multilayer attack which means attacker can utilize either network layer, applicationlayer or transport layer unsafely.[5]

• **Denial of Service**: DoS attacks are most famous attacks in this list. In this attack attacker check the authorised user to use the service from the suffered node.In this,attackers may transfer dummy messages to jam the channel and thus, diminish the effectiveness and completion of the network. In this figure a malicious black car forges a great number of fake identities and transfer the dummy messages "Lane close ahead" to a authorised car behind it and even to an RSU to generate a illusion in the network.[6]

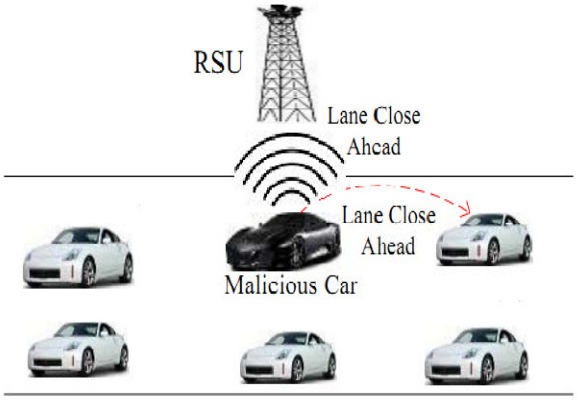

Fig3: Denial of Service Attack (DOS)[6]

• **Routing attack**: Routing attacks are those attacks which utilize the risk ofnetwork layer routing protocols. In this type of attack the attacker either releases the packet or disorders the routing process of the network. Following are the most common routingattacks in the VANET:

Black Hole attack: In this type of attack, the attacker firstly engage the nodes totransfer the packet through itself. When some malicious user enter into the network and stop onward messages to next nodes by releases messages are called as black node.[6]

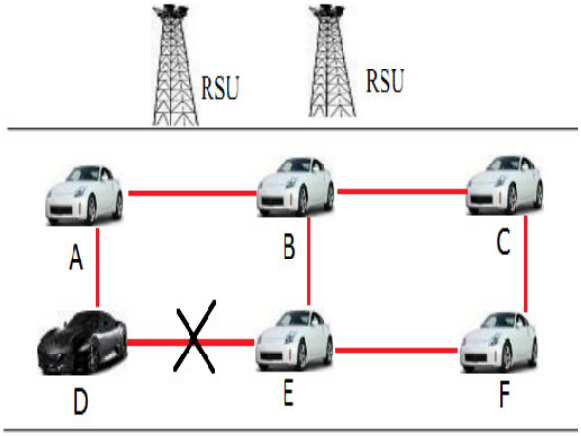

Fig 4: Black hole attack [6]

Gray Hole attack: This is the addition of black hole attack. In this type of attack the malicious node behaves like a black node but it releases the packets selectively.[6]

Worm Hole attack: It is provocation to observe and stop this attack.In this attack, an competitor receives packets at one point and tunnels them to another point in the network, and then repeat them into the network from that point. This tunnel between two competitors are called wormhole.It can be created through a single long-range wireless link.[6]

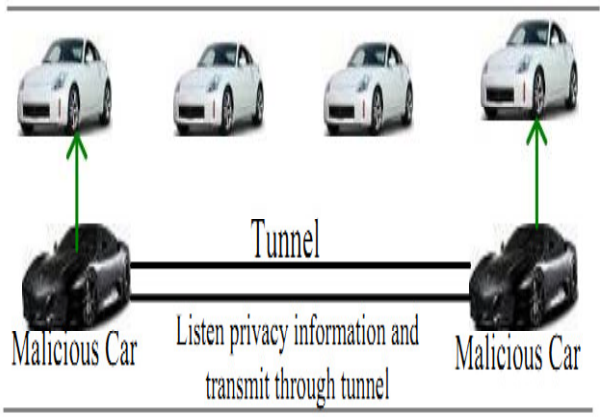

Fig 5: worm hole attack [6]

LITERATURE SURVEY

Sourav Kumar Bhoi et.al [1] Vehicular communication is an substantialarea of research in the field of vehicular technology. The developmentof software and hardware in communication systems execute to the propagation of new networks.The main idea behind using this new technology is to create an accident free environment. New designs, protocols and implementations are used in vehicular ad-hoc network (VANET) to provide Intelligent Transportation Services. It is also reconsidered the purpose of VANET which provides services to the users. The main motive of this study area is to analyze the popular ideas in vehicular communication.

YUN-WEI LIN et.al [2] Vehicular Ad hoc Network (VANET), a description of mobile ad hoc networks (MANETs), is a assuring passage for the intelligent transportation system (ITS). The design of routing protocols in VANETs is essential and serious issue for the smart ITS. The key difference of VANET and MANET is the determinate mobility designand swiftly fluctuating topology. In this exploration, we mainly studied new routing outcomes in VANET. We introduce unicast protocol, multicast protocol, geocast protocol, mobicastprotocol, and broadcast protocol. In this we determined that carry-and-forward is the recent and key contemplate for the layout of all routing protocols in VANETs. With the acknowledged of multi-hop forwarding and carry-and-forward techniques, min-delay and delay-bounded routing protocols are considered in VANETs. Besides, the temporary network fragmentation problem and the broadcast storm problem are further observed for the layout of routing protocols in VANETs. The temporary network fragmentation problem created by prompted changeable topology connections on the performance of data transmissions.The broadcast storm problem affects the rate of message delivery. The key challenge is to reduce these problems to provide routingprotocols with the low communication delay, the low communication overhead, and the low time complexity. The challenges and the broad view of routing protocols for VANETs are finally considered.

Mina Rahbari et.al [3] Vehicular communications play a essential role in providing safety transportation by means of safety message transmission. Researchers have contemplated many solutions for securing safety messages. Protocols based on a fixed key infrastructure are more adaptive in implementation and also manage stronger security. The determination of this paper represent a method based on a fixed key infrastructure for detection impersonation attack, in other wordsi.e. Sybil attack, in the vehicular ad hoc network. This attack puts a great effect on the performance of network. The proposed method, using an cryptography mechanism to detect the Sybil attack. Finally, using Mat lab simulator the results of this approach are reconsidered, This method has low delay for detection Sybil attack, because most operations are done under Certification Authority, so this schema is a effective method for detection Sybil attack.

Manjunatha T. N et.al [4] Due to broadcastWireless Sensor Networks (WSNs) and reduction of tamper-resistant hardware, security in sensor network is the major drawback. Research is being done on several security attacks on wireless sensor networks. Wireless Sensor Networks are briskly gaining interests of researchers from academia, industry, emerging technology and defence. WSNs consists hugenumber of sensor nodes and a minor sink nodes or base station are extended in the field to assemble information about the category of physical world and transmit it to interested users, typically which are used in applications, such as, habitat monitoring, military surveillance, environment sensing and health monitoring. When a node illegallyasserted multiple identities or claims fake id, is called Sybil attack. In Any network it is particularly sensitive to the Sybil attack where in a malicious node disorder the proper activity of the network. This paper target considered variety of security issues, security threats, Sybil attack and various methods to prevent Sybil attack.

Ram Shringar Raw et.al [5] Vehicular Ad hoc Networks (VANETs) is the challenging approach to provide safety to other applications and the drivers as well as passengers. It becomes a key component of the intelligent transport system. A lot of works have been done towards it but security in VANET got less focus. In this, we have discussed about the VANET and its technical and security aspects. We have also discussed some major attacks and solutions that can be implemented against these attacks. We have compared the solution using various parameters. Lastly we have described the mechanisms that are used in the solutions.

Vinh Hoa LA et.al [6] Vehicular Ad hoc Networks (VANETs) have emerged recently as one of the most focusing topic for researchers and automotive industries due to their cracking potential to boost traffic safety, capability and other extra services. However, VANETs are themselves sensitive against attacks that can directly lead to the division of networks and then possibly affront big losses of time, money, and even lives. This paper represents a survey of VANETs attacks and solutions in carefully examined other similar works as well as updating new attacks and differentiating them into various classes.

Priyanka Sirola et.al [7] Vehicular Ad-hoc Network (VANET) is a step-up & most demanding research area to provide Intelligent Transportation System (ITS) services to the end users. The implementation of routing protocols in

VANET is an imperative task as of its high mobility & frequent link forcibly separated topology. VANET is basically used to provide various commercial services to each and every end user; these services are further compelled to provide an effective driving environment. At present, to provide efficient communication in vehicular networks many routing protocols have been designed, but the networks are sensitive to many threats in the presence of malicious nodes.security is the major concern for variety of VANET applications where a unauthorised message may directly or indirectly affect the human lives. In this paper, we investigate the many security issues on network layer in VANET. In this, we also determine routing attacks such as Sybil & Illusion attacks, as well as available solutions for such attacks in existing VANET protocols.

Jaydip Kamani et.al [8] In Vehicular Communication, the security system against the attacker is very crucial. Sybil attacks have been regarded as a serious security threat to ad hoc networks and sensor networks. It is an attack in which an original identity of the vehicle is disrupted or stolen by an attacker to creates illegal multiple fake identities. Detecting such type of attackerand the original vehicle is a demanding task in VANET. This survey paper briefly represents many Sybil attack detection mechanism in VANET.

Kumud Dixit et.al [9] during the last few years, a vehicular ad hoc network (VANETs) was comprising focused by researchers. A vehicular ad hoc network (VANETs) is a subclass of Mobile ad hoc networks builds to make sure the safety of road accidents. VANET is a type of mobile peer to peer network, although it expose some various characters (fast moving, short lived connection etc). VANET is different from MANET due to large scale networks, higher mobility of nodes, geographically constrained topology and frequent network divisioning. In this paper, we present a survey on trust based routing in AODV based VANET to find secure location. In this discussed about VANETs, their applications, characteristics, attacks, routing protocols and represent a review of different researchers on trust based VANET.

Xia Feng et al. [10]Sybil attack can counterfeit traffic summary by sending wrong messages with multiple illegal identities, which often considered traffic jams and even leads to vehicular accidents in vehicular ad hoc network (VANET). It is very difficult to be defended and detected, especially when it is launched by some cooperteattackers using their legal identities. In this paper, we propose an event based reputation system (EBRS), in which dynamic reputation and trusted value for each event are hired to conceal the expansion of false messages. EBRS can detect Sybil attack with falseidentities and thefted identities in the process of communication,it also contened against the conspired Sybil attack since each event has a unique reputation value and trusted value.

Sybil Attack

In this attack, attacker creates different personalities to restoring different centres. This attack is very serious attack in which a vehicle can claimed at different places with several fake identities at the same time and generating huge security risks in the network. A Sybil attack is harmful for network topologies and connections as well as network bandwidth consumption. In this Figure an attacker A transfers multiple messages with different identities to the other vehicles. Thus, other vehicles perceive that there is currently a bulky traffic. Detecting such type of attacker and the real vehicle is a provocation task in VANET.[6]

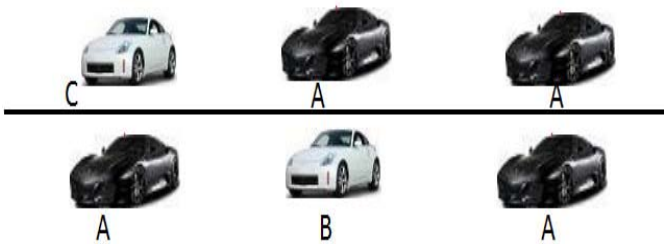

Fig 6: Sybil Attack

Security requirement for VANET

1. Authentication

Authentication protects that the message is created by the authorised user. In Vanet, a vehicle behave upon the information came from the other vehicle therefore authentication must be pleased.[5]

2. Message Integrity

Integrity of message preserved that the message is not changes in passage that the messages from the driver receives are not False.[8]

3. Message Non-Repudiation

In this security based system a sender can be recognize easily. But only identified control is accepted for sender recognition. Vehicle could be identified from the validate messages it sends.[5]

4. Access control

Vehicles must comply according to rules and they should only perform for those tasks that they are approvedto do. Access control is protected if nodes proceeds according to particular approval and create messages tenderly.[5]

5.Message confidentiality

Confidentiality is compulsory to conserve privacy in a system. Law enforcement authority can only appoint the privacy between communicating nodes.[7]

6. Privacy

This system is used to protected that the information is not confined to the unsanctioned people. Third parties should not be consummate to trace vehicle movements as it is a discontinuity of personal privacy. Location privacy is also important so that no one should be able to consume the past or future positions of vehicles.[8]

CONCLUSION

Vehicular Ad Hoc Networks is encouraging technology, which gives generous chances for attackers, who will try to provocation the network with their harmful attacks. This paper gave a extensive inspection for the contemporaryprovocation and resolution, and attacker for these solutions, in our future work we will propose new results that will help to conserve a securer VANET network, and try out it by simulation.

REFERENCES

Sourav Kumar Bhoi, Pabitra Mohan Khilar "Vehicular communication: a survey" August 2013.

Yun-Wei Lin1, Yuh-Shyan Chen and Sing-Ling Lee "Routing Protocols in Vehicular Ad Hoc Networks:A Survey and Future Perspectives"2010.

Mina Rahbari and Mohammad Ali Jabreil Jamali "efficient detection of sybil attack based on cryptography in VANET"nov 2011.

Manjunatha T. N, Sushma M. D, Shivakumar K. M "Security Concepts and Sybil Attack Detection in Wireless Sensor Networks"april 2013.

Ram Shringar Raw, Manish Kumar, Nanhay Singh "security challenges,issues and their solutions for vanet"sept 2013.

Vinh Hoa LA, Ana Cavalli " security attacks and solutions in vehicular ad hoc networks: a survey"april 2014.

priyanka sirola, amit joshi, kamlesh C. Purohit "An Analytical Study of Routing Attacks inVehicular Ad-hoc Networks (vanets)"July 2014.

Jaydip kamani,Dhaval parikh "A Review on Sybil Attack Detection Techniques"Mar 2015.

Kumud Dixit, Krishna Kumar Joshi, Neelam JoshiA Novel Approach Of Trust Based Routing To Select Trusted Location In AODV Based VANET: A Survey" 2015.

Xia Feng1 · Chun-yan Li2 · De-xin Chen3 · Jin Tang1 "A method for defensing against multi-source Sybil attacks in VANET"January 2016.