International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 6, ISSN No. 2455-2143, Pages 123-127
Published Online in IJEAST (http://www.ijeast.com)

REVIEW ON SECURE ENGINEERING FOR SAFER TRANSPORTATION IN VEHICULAR AD HOC NETWORKS

Aditi Malviya
Amity University,
Noida, Uttar Pradesh, India

Abstract: This paper investigates the threats in vanet system and aims to assess all the vulnerabilities that a vanet architecture faces. Increasing quality of service is the aim and has been done in this paper by investigating all the threats that a vanet system is prone to .A few drawbacks in the vanet system have been brought out that can be worked upon in future.

I. INTRODUCTION-

Internet and network infrastructure has been continuously evolving in the past 40 years and has affected every individual life by opening a vast number of possibilities. The modern lifestyle has almost everything linked with computers and communication. Information systems and data transfer in is these days is almost a part of every object. One category of this type of smart devices is intelligent vehicles , intelligent transport systems and communication capable roadside infrastructure. A network comprising of this kind of a smart vehicular system is called vehicular ad-hoc network .These vehicles basically function as computer in the network directly connected to each other instead of having a server or a hub. These vehicles form temporary network .Each vehicle serves as wireless router that are able transmit data in the range 100-300 metres. Due to mobility of these vehicles they constantly keep on disconnecting and connecting to neighbor networks ,linking different vehicles to each other .The vanet infrastructure even comprises of InfoStations and Road Side Units.

Vanets have proved to be quality systems in assessing the traffic challenges, keeping the drivers informed and aware of the road environment giving them a window to respond to the abnormal incidents that can occur. Vanets have made the road transportation systems into safer and better system The technology that we have engrossed in our daily lives has given us many facilities but it has also given a spark to dangerous technology abuse and cyber attacks .Vanet sytems have advanced and so have the various criminal activities with it. The various cyber crimes in this domain include cyber espionage, eavesdropping, pranksters and phishing schemes. Though the development in vanet architecture is much appreciated it is very essential to investigate and assess the data security and confidentiality issue in vanets. Despite the advantages of vanets, there are numerous challenges in aspects of security and privacy. Inter-vehicle communication (IVC) has grown as a absolute necessary futuristic component, and this paper investigates about the security threats and the vulnerable nature of vanet architecture. The prevalent security threats faced in vehicle-to-vehicle (V2V) and vehicle-to infrastructure (V2I) communication are focused upon in this paper.. Security issues and the necessary requirements that the architecture should engross are discussed in this paper. This paper is structured in six sections: section I is the introduction and the identified sources of attacks. Malicious exploitation in VANET is presented in section II. Section III elaborates attacks against routing protocols. Section IV demonstrates an execution of black hole attack, and outlines a general methodology adopted by attackers. Conclusions are given in section VI.

II. SOURCES OF ATTACKS AND MALICIOIUS ACTIVITIES IN VANETS

VANETs are extensively vulnerable and prone to attacks. These vulnerabilities hamper the efficiency of the network, stimulating problems in the network posing dangerous security threats. The severity of attacks launched by the attackers can be assessed by its impact on the victim. The mentioned section puts a light on the vulnerable nature of vanets.

Jamming –The act of deliberately generating a blockage or restriction in the path of signals restricting the to reach the another node.

Forgery-This is the activity by which false hazard warnings are transmitted to vehicle in a vanet with intention to create a chaos and makes the vanet system to compromise with the correctness and validity of the network.

Impersonation-This refers to the act when any vehicle tries to act as any other vehicle in the network to gain access to information that it is not entitled to. Also involves alteration, fabrication and relaying of message.

Privacy –This activity involves the illegal action of accessing the driver's personal information and violates privacy. Attacks on driver privacy causes severe vulnerability in VANET because of the mobile and frequently changing nature of vehicular node topology. Driver' confidential data can be accessed by means of illegal traffic tampering traffic related messages communicated by the driver, management messages, and even from transaction based messages in case of automated payments. Such scam cases activities have increased among networking devices as cyber attackers get a chance to spread spurious messages in the network. VANET was initially aimed at integrating mobile connectivity vehicles to expedite data transfer while traveling.. An major concern issue in vanet environment is security, where a malicious node interference may cause harm human life, in the context of public adoption of the technology. A vehicular network is open for connections and easy to access from anywhere in the given DSRC range which makes it a easy target for malicious users. Disabling or interfering with the OBUs, damaging with the road side infrastructure, removing, destroying is also a big security issue in vanets. OBUs are tampered in a manner similar to that of modifying an odometer in earlier vehicles. Application of electric fields and malware that aim to damage OBUs are of concern and need to be addressed for safe VANET communications. Although the OBUs could be subject to periodic examinations and inspections for any signs of tampering, limitations exist in relation to the frequency of inspection and the honesty of technicians performing the inspections. To ensure reliability and security in V2I communication, on side road unit damage has to be concerned about.

Attacks against routing-

VANET are moden vehicular network which enhances road safety, traffic and dissemination of information for drivers and passengers. The vanet architecture relies on dynamic routing protocols due to the mobile nature of its nodes. For the security of the complete vanet sytem secure routing protocol are very essential. Routing being the backbone of vanet network makes it the network part which is most prone to susceptible operations and attacks [12]. Malicious nodes in VANET can exploit the co-operative routing algorithms to launch routing attacks, similar to BH and rushing attacks. Mostly the attacks in a vanet target the routing protocol or the packet that are transferred between the nodes.

Impersonating: This involves stealing the credentials of another vehicle similar to type of a spoofing.. It also involves advertising of fake route metrics to create a confuse the topology, false sequence numbers are communicated to delay the messages in the network. Flooding with DoS attacks, modifying of RREQ message implanting false paths, generating false routes messages obstructing a packet transfer route or hiding a genuine route leading to other vehicles being misinformed.

Application Attacks: Most vanets applications focus on safety and comfort. The messages received and send by these application is the main target area of the attackers . Attackers interfere with the data of the actual messages and forward incorrect or the tampered message to other network nodes that may lead to disasters in the vehicular road network .One of the common application attack is the fake information attack in which an attacker injects bogus data into the vanet and these altered messages directly affects the communication of vehicles on the road. Another catastrophic attack is the alteration and delay of warning messages, that compromises the trust between the entities of the vanet architecture. Another use of of vanet technology is to enhance the comfort of vehicle owners in a vanet infrastructure. Parking assistance is an example of comfort application that helps in locating a parking space by the communication between the RSU and the OBU of the particular vehicle.

Timing Attack: The main objective of this attack is to delay a message by introducing a new time slot in the message. Content of the message is not altered but the message is delayed which renders it useless for the receiver expecting the message . Safety applications ought to be time critical and a minor delay in transmission coud lead to disaster. figure. 3 depict a timing attack scenario where an attacker ‘C’ receives a warning message ‘Warning! Accident at location Y’ from other vehicle ‘B’. Under normal operating conditions, this message would have been transmitted to a nearby vehicle ‘D’ instantly, but the attacker ‘B’ deliberately does so after some time, thus causing ‘D’ not to evade the sight [17].

Attack on comfort application • Social Attack: Social attacks are a class of attack where the attackers modify/aggravate the behavior of legitimate vehicles by sending immoral messages to them. This is a kind of emotional and social attack that indirectly creates problems in the network by enticing legitimate users to show angry behavior when they receive such kind of derogatory messages. figure. 4 depict this scenario, where an attacker ‘B’ intentionally passes a message ‘You are Idiot’ to a nearby vehicle ‘C’.

Timing attack in VANET When ‘C’ receives this message, his driving behavior is aggravated which results in an increase in the speed of the vehicle.

The episode culminates in disturbing/distracting the other users on the network.

Monitoring Attack: Monitoring and tracking of the vehicles, illegally listening to the communication between V2V and V2I and misusing any confidential information is the motive of this attack, figure.5 depicts this scenario

III. ATTACK-PROCESS MECHANISM AND AN ILLUSTRATION OF NETWORK LAYER ATTACK

This given section describes in detail about attack process in VANET and the communication link between the user ,attacker and the RSU. The various steps to launch an attack in the network[18]:

An attacker initiates launching a attack on target vehicle and even on the RSUs, based on the extent of damage intended by the attacker.

The attacker receives a valid message from another vehicle/RSU expecting the attacker to forward/reroute the message.

The attacker alters/intercepts the contents of the message and passes this message to other vehicles/ RSU. • The attacker might also impersonate/masquerade as another vehicle, launches timing attacks or other types of attacks on other vehicles.

Monitors the communication between the vehicles or infrastructure and achieves his/her benefit

IV. RESULTS & INVESTIGATIONS

Despite a tremendous potential and application to enhance road safety and to facilitate traffic management, VANET suffers from a range of security and privacy issues that have dramatically restricted their applications as yet. The research confirms that whereas VANET has emerged as an active area of research, standardization, and development due to its tremendous potential to improve vehicle and road safety, improve traffic efficiency and enhance driving comfort, a strong emphasis needs to be laid on designing novel VANET architectures and implementations. VANET suffers from considerable threats to security of the users, and therefore research needs to be focused on specific areas including routing, broadcasting, QoS and security. This paper describes attack process mechanism and illustration of Black hole attack, which investigate how intruder capture the route and send a false message to other nodes. It also compares different types of security attacks in VANET with attacker types and respective security attributes which shows the effect of different types of attack in various environments.

V. IMPACT OF THE ATTACKS ON THE VEHICULAR NETWORK ARCHITECTURE

With the evolving network nudging towards wireless connections, VANET system(vehicles and RSUs) have devices that are resource constrained and need high security, scalability and good data management . The fundamental part of vehicular network is internet, it makes a way for lots of insecure end-points. A larges amount of data is generated smart vehicular nodes and communicable RSUs from disparate networks. This brings the attackers and hackers with an chance to break into these resources and repositories of valuable data to gain unauthorized access into confidential stuff that can have a strong impact on the use of vehicular network technology. The trending routing protocols in vanets like context-aware policy routing allows its components (vehicles and RSUs) to transmit information and even sharing of links. The genuine RSU and on-board unit (OBU) messages in VANET are safe, but link sharing by malicious nodes is considered to be dangerous.

Interacting with these links has changed the VANET landscape, and malware spread more easily by extensive VANET devices. 'Masquerading' and 'trust' act as the social bait where a hacker, masquerading as a known vehicle sends malicious links, trusting the transmitter makes the victim to click on the posted information links. The hacker puts links that have messages relating popular topics, that coud affect other other travellers in the vehicles , accessing the informative services. Once the links are clicked, they can attack the whole VANET network along with disconnecting that vehicle . Malicious extensions are spread in the infotainment gadgets and disable antivirus/ encryption software of the respective vehicle. Besides focusing on the network vulnerability protection, making the VANET networks more resilient to security threats could prevent a lot of damages to the technology, as follows:

• Theft of data: This involves theft of driver information or financial information about parking slot issues. Also includes credit card credentials, drivers' important data and sometimes drivers' intellectual property data or marketing plans. The attacks most profoundly affect the user credentials. Stolen credentials along with infecting the target vehicle with malware lead to that vehicle to be listed on a botnet causing the attack, making it more powerful. These activities damage the encryption systems of the device and also interfere with sensitive information [20].

• Loss of time: It can take much time for a vanet network to recover once it is affected by a attacker even in case of a suspicion. Data the requires complete reframing, recovery or reconstruction.

• Monetary loss: Theft of data often occurs along with financial losses due to maligned activities of attackers. •

Disabled and crippled services: Protesters and even some government authorities may discourage the use of vanet technology. Cases of cyber crime and information misuse are frequently reported .This is possible when looked into the malicious intent of the hackers.

• Legal exposure: any of the above scenario could expose a taxi firm or a car rental enterprise to law suits for data loss. VANET attacks not only impact vehicles and RSUs, but also, all the linked devices that connect to a VANET device in any connected stages and have a chance of facing a vanet attack. The vehicular ad hoc networks are seen to have much in scope in of Internet of Things (IoT) .The security breach in vanets can adversely affect the connected devices. With advance in IOT, more and more objects ranging from smart homes and smart cities to including household gadgets, health monitors, palmtops and smart phones, doors and safety systems etc. have digital representations that allow them to be accessed and controlled from anywhere. These devices can be interconnected using the wireless LAN networks similar to VANET, or might have an interlinked VANET network. The VANET attacks mentioned can negatively affect the operation of the 'device intelligence everyday things' architecture. With widespread ubiquity of internet, the attackers are also finding innovative ways to break into the network and harness the resources, and to maliciously corrupt the data and effective communication between various elements of the integrated architecture. With increasing number of vehicles being added to the VANET, it is important to approach security threats from a more comprehensive point of view, analysing all the requirements that need to be met for a secure network [21]. It is understood that attacks and incursions are going to happen. In the future work, we plan to outline a framework for network security resiliency, in order to detect, access, predict and mitigate the damage from VANET attacks as they happen. The authors propose to gain an expert understanding of how attacker work, how attackers think, and attacks are launched and executed and which node in the network is the most vulnerable. NCTuns simulator will be used to create realistic scenarios that emulate real-world attack traffic. This would include vulnerability testing, where attacks will be mounted against the targeted node using databases of known malware, incursions, intrusions and other attacks.

VI. CONCLUSION

It is concluded that apart from having of good encryption mechanism , efficient and secure routing , the VANET architecture always remains prone to security breaches because the attacker even without gaining access always has the option of listening to the communication . The investigation brings out a few practices and theories that can be employed to minimize the security issues in VANET . Major security issues and other adverse issues that can occur in vanets are also looked into in the paper. We conclude that in the evolving network environment, VANET should be engrossed with a better security architecture, with user privacy being considered as the as the most important exponent of VANET architecture . The study of security strategies and flaws is expected to create to even more efficient routing protocols, that would contribute in enhancing quality-of service. Due to mobile nature of vehicles, large infrastructure, rapidly restructuring topology ; a fundamental characteristic of VANETs is to ensure safer transmission of data in their critical time window. This paper examines various security threats in VANETs, how they are implemented and what impact they have on the VANET security architecture. It describe the attacks and their process mechanisms , illustrates the Black hole attack and gives a comparative analysis of various types of security attacks and their attributes. Safer on road transportation refers to ways and methods for minimizing the risk of a person using the road transport network from facing any harms.. The maximum achievable degree of safety shall be reached in case of goods transportation by roads. Monitor and validating the road safety issues, comprising comprehensive checks on drivers, vehicles and safety processes.

VII. REFERENCES

1. Dua A, Kumar N, Bawa S, A Systematic Review on Routing Protocols for VehicularAd Hoc Networks, Vehicular Communications,2014,1(1),33-52.
2. Issariyakul T.,Hossain E.”Introduction to Network Simulator NS2, Springer.
3. Asim Rasheed , Haleemah Zia, Farhan Hashmi, Umair Hadi, Warda Naim, Sana Ajmal ,Fleet & Convoy Management Using VANET [Fig.] An example of a generic VANET layout , Journal of Computer Networks, 2013, Vol. 1, No. 1, 1-9.
4. Tajinder Kaur, A. K. Verma, Simulation and Analysis of AODV routing protocol in VANETs , International Journal of Soft Computing and Engineering (IJSCE) ,ISSN:
5. 2231-2307, Volume-2, Issue-3, July 2012.
6. C. Perkins, E. Royer, and S. Das,”Ad hoc On-Demand Distance Vector (AODV) Routing," IETF, RFC 3561, 2003.
7. Karnadi, F. K., M. Zhi Hai, et al. (2007). Rapid Generation of Realistic Mobility Models for VANET. IEEE Wireless Communications and Networking Conference, 2007.WCNC 2007.
8. Xin Yang, Zhili Sun, Ye Miao, Ning Wang, Shaoli Kang, Yingmin Wang and Yu Yang. Performance Optimisation for DSDV in VANETs , 2015 17th UKSIM-AMSS International Conference on Modelling and Simulation.