Security mechanism for Collision Avoidance and Attack Prevention Formants

Harpreet Kaur[1],
Punjabi University,Patiala, India

Mrs.SupreetKaur[2]
Punjabi University, Patiala, India

Abstract*—The VANETs are the vehicular ad-hoc networks, which facilitates the communication between the vehicles within the same cluster and with vehicles in the other clusters. The VANETs are being used to provide various types of information based upon the traffic jams, accident prevention, location of other nodes in the cluster, etc. to the vehicular nodes. The new era will be comprised of the automatically driven vehicular nodes in the VANET clusters, where the computer operated vehicles will automatically drive themselves, manages the traffic or will perform several other operations together. The hackers, the selfish drivers, terrorist or other individual or groups may attacks the VANETs for their own reasons. A selfish hacker may clear its way by sending false information or disabling other nodes by several forms of denial of service attacks. In this paper, the issue of the unavailability of the nodes is being addressed using the new security scheme for the VANETs with automatically driven vehicles. The proposed scheme will comprise of false information detection, malicious node marking, traffic pattern analysis, packet flood detection modules. The proposed scheme will mark the hackers or malicious nodes on the basis of false information detection on the very first step. Afterwards it will analyze the traffic coming from the nodes, and will apply the pattern and flood detection modules over the traffic being received from the various components of the VANET cluster. The attacking patterns or floods will be detected and their sources will be mitigated through the security mechanism. The performance of the proposed scheme will be evaluated using several parameters like throughput, end to end delay, packet delivery ratio, data drop rate, etc.

Keywords: VANETs, security, DDoS, false information, malicious nodes

I. INTRODUCTION

VANET is a technology in which vehicles act as nodes to create network. VANET is class of mobile ad hoc network that aims at providing safety of vehicles, passengers and drivers. Vehicular networks have been developed to improve the safety, security and efficiency of the transportation systems. Using VANET we can implement intelligent road traffic management system. In VANET nodes can be self-organizing and self-managing system which can distribute traffic and information regarding vehicles [1]. Vehicular communication system is created in VANET for reliable and efficient distribution of data so that passenger feel ease and safe. VANET can improve the safety of passengers and provide accident prevention. VANET contains two type of communication: vehicle to vehicle and vehicle to infrastructure communication. In vehicle to vehicle, communication done with the help of On board units which contain GPS and Omni direction antenna. For road traffic information and other real time information we can use V2V communication. In vehicle to infrastructure, communication done with the help of Road side units.Road side unit connect the vehicles on the road and then connect to other devices like internet, RSU store information about vehicles and traffic [4].V2V and V2I both are used to increase the security .Security requirements in VANET are integrity, authentication, non-repudiation, availability, Confidentiality and privacy etc[8]. Security of VANET from various attacks is very important. There are various attacks in VANET like malware attack, black whole attack, message suppression attack, fabrication attack, Alteration attack, Denial of service attack, Distributed Denial of Service Attack. The distributed denial of service (DDoS) can be classified as the most dangerous attack, which can be launched on the automatically driven VANET nodes.

II. SECURITY REQUIRMENTS OF VANET

The security of VANET is extremely important for secure transmission of data in network .Following are some requirements of VANET.

A. Authentication:- For secure transmission of data in the network, authentication of messages and its sender is must. Authentication ensure that legitimate vehicles are communication within the network and work properly. Otherwise without authenticationmalicious user sending false information in the network [8].

B. Integrity: - Integrityassure that same message is received at receiver end by nodes and RSU as what it has been generated by sender.Digital signature with password access are used to prevent the integrity of message [7].Data integrity assure that there is -

No modification during transmission.

No forged or false messages.

No replayed messages.

C. Confidentiality: - Confidentiality assure that information will only be access by legitimate parties. For group communication confidentiality requirement is useful in which only members of group are allowed to access the information [8].

III. VARIOUS TYPE OF ATTACKS IN VANET

The security is most analytical part of VANET.Transmitted information throughout the network cannot be modified so security is important aspect.There is possibility of various attacks on VANET like Sybil attack, man in middle attack, wormhole attack, denial of service attack, malware attack, black hole attack, spamming etc. Some of the attacks are mentioned below.

Denial of service attack :

Denial of Service (DoS) is the most damaging attacks in the network. In dos attack, malicious node or attacker may attack on node resources. The main purpose of attackerin overwhelm the node resources such that nodes cannot perform important task. The victim nodes becomes busy in message verification which is send by attacker and cannot be able communicate with other nodes in the network.The attacker can also attack on channel to jam the communication between nodes [9].

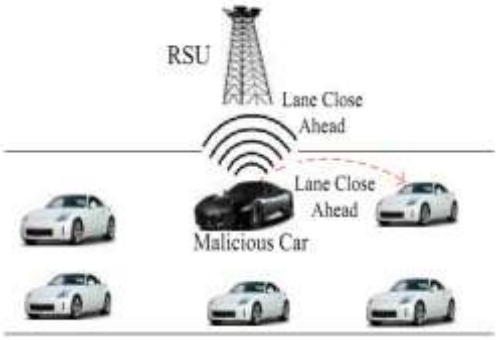

Fig 1: DOS Attack [10]

The existing solution of DOS attack is based on OBU (on-board unit).On Board unit install on each vehicle. The processing unit pass information to OBU to switch channels technology (or) to use frequency hopping technique. Channel Switching, technology switching, FHSS and multiple radio Transceiver switching options are available to detect received message [9].

Distributed Denial of service attack :

The Distributed Denial of Service attack (DDoS) is more intense than the DoS attack. In DDOS a number of malicious vehicles attack on a legitimate vehicle in a distributed manner from different locations and timeslots. The DDos attack will affect the communication of the VANET node, and will forcibly breaks its communication with other nodes in the cluster. In this situation, the hackers can take control of the node can move in any direction on any speed, which may cause collision, traffic jam, etc. Two type of attacks are possible in DDOS attack. In first type attack, attacker take control over all the nodes and try to degrade the performance of network. In second type of attack, attacker attack at infrastructure from different location because of that when rest of nodes in network want to access the road side unit, then at that time RSU is not able to respond them and this cause denial of service attack [9].

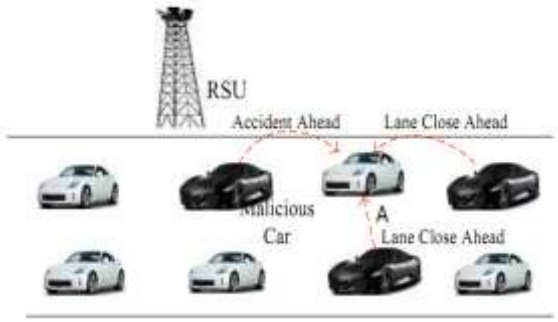

Fig 2: DDOS Attack [10]

The attacks on VANETs can be classified as per following:

Insider Vs Outsider

In the same network, a node can interact or communicate with other members of network is called insider. This type of attacker might have access to gain the Knowledge about the network and then use this information to launch the attack. Insider attack is very dangerous attack as compare to other attacks. Outsider who have limited ability to attack, cannot directly communicate with other member nodes of network [7].

Malicious Vs Rational

A malicious attacker destroy the nodes of network without looking for its personal benefit. Rational attacker are more predictable and these attacker looking for its personal benefit [7].

Active Vs Passive

An active attacker can generate some new packets to destroy the network whereas passive attacker are less dangerous and cannot generate new packets to destroy the network [7].

IV. LITERATURE REVIEW

S. Roselin Maryetal [1], has proposed an algorithm to improve the security of VANET i.e. Attacked Packet Detection Algorithm. Before the verification time this algorithm is applied to detect DOS attack. It also minimize the overhead delay. This algorithm is based on the technique which scans the position of nodes and then calculates the movement of vehicles in the term of distance

and displacement of the nodes in the cluster to protect against DOS attack for VANET architectures.

Marco Tilocaetal.[2], proposed a solution against selective jamming attack.For data communication between nodes Time Division Multiple Access (TDMA) approach is used. In this paper SAD-SJ(self-adaptive decentralized solution) minimize the overhead. SAD-SJ abrogate the attack and it is self- adaptive. In SAD-SJ at any time nodes can join and leave the network without hindering the security of rest of nodes.

Md. MonzurMorshedet al.[3], has proposed a new secure routing protocol for the MANETs.The new protocol is called CBSRP (Cluster based secure routing protocol). The proposed protocol is based upon the digital signatures and one-way hashing in order to establish the secure communication between two links. Additionally, the proposed protocol also compute and select the cluster head node, which manages the whole security procedure defined under the protocol for the MANETs.

SeuwouPatriceet al.[4], has Proposed a solution against Security in Vehicular Ad hoc Networks (VANETs). In this paper the authors have done detailed security analysis and discussed various attacks and possible threats to security in VANET. Also the limitations of current and challenges to the security mechanisms have been analyze.There is possibility of various attacks on VANET, authors classifies attacks into two types: Logical and Physical attack. Physical attack arise due to event data recorder and tamper proof devices. Virus and Trojan horse are the main reason of logical attacks.

Sumra A.I.et al.[6], has proposed three trust levels in peer-to-peer vehicular network i.e. Zero level, weak level and strong level. In Zero level trust, attacker is able to launch attack on whole network. In weak trust level, attacker is able to launch attack within particular region. But In strong trust level, all the nodes in the network are trusted and work properly because there is no attacker in the network.

Mohammed Saeed [7], has proposed survey on various VANET attacks. According to him intelligent transportation system give us safety on roadand provide traffic pattern analysis. The proposed survey based on the detection of existing attacks and try to find out future security attacks.

Aditya Sinha et al. [9],introduces a solution against preventing VANET fromDOS and DDOS attacks. In this paper, network availability on DOS is presented with its severity levels. To overcome the DOS attacks, a new approach has been introduced. In this approach, author use Revocation techniques and DSRC channel. In this proposed solution limited number of messages at given stamp of time will received by any node in network.

V. CONCLUSION

The main purpose of VANET is to save human lives on the road. Due to Denial of Services or Distributed Denial of Services, when nodes and road side unit are not able to send or receive important information then VANET becomes useless technique. Therefore, protection from DOS and DDOS attacks is mandatory. So, we propose a new technique for Detection and Prevention from DDOS. We expect that our approach will intensely compete against DDOS attack, because if network nodes will not accepting trash message from the attacker nodes, its processing resources will not be overwhelmed and always be available for other nodes.

REFERENCES :

[1]S.RoselinMary, M. Maheshwari, Thamaraisselvan, "Early Detection of DoS Attack in VANET Using Attacked Packet Detection Algorithm (APDA)," vol. 1, *IEEE*, 2013.

[2] MarcoTiloca, Domenico De Guglielmo, Gianluca Dini and Giuseppe Anastasi, "SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks," vol. 18, pp. 1-8, *IEEE 18th conference on Emerging Technologies and Factory Automation*, 2013.

[3] Md. MonzurMorshed, Md. Rafiqul Islam, "CBSRP: Cluster Based Secure Routing Protocol,"IACC, vol. 3, pp. 571-576, *IEEE*, 2013.

[4] Seuwou, Patrice, Dilip Patel, Dave Protheroe, and George Ubakanma. "Effective security as an ill-defined problem in vehicular ad hoc networks (VANETs)," *Road Transport Information and Control (RTIC 2012), IET and ITS Conference*, pp. 1-6, 2012.

[5] Dias, João A., João N. Isento, Vasco NGJ Soares, FaridFarahmand, and Joel JPC Rodrigues. "Testbed-based performance evaluation of routing protocols for vehicular delay-tolerant networks," pp.51-55, *IEEE*, 2011.

[6] Sumra, Irshad Ahmed, HalabiHasbullah, J. A. Manan, MohsanIftikhar, Iftikhar Ahmad, and Mohammed Y. Aalsalem. "Trust levels in peer-to-peer (P2P) vehicular network," *ITS Telecommunications (ITST), 2011 11th International Conference*, pp. 708-714. *IEEE*, 2011.

[7] Mohammed Saeed Al-Kahtani "Survey on Security attacks in Vehicular ad hoc networks", vol. 1,issue 1,*IEEE*, 2013.

[8] AyonijaPathre, ChetanAgawal, Anurag Jain "Identification of malicious vehicle in VANET Environment from DDOS attack," vol. 4,*Journal of Global Research in computer Science*,2013.

[9] Aditya Sinha, prof. Santosh K Mishra "Preventing VANET from DOS & DDOS Attack," vol.4, *International journal of engineering trends and Technology*,2013.

[10] VinhHoa LA, Ana CAVALLI " Security Attacks and solutions in Vehicular AdHoc Network : A Survey," vol. 4, *International Journal in AdHoc Networking System*, 2014.