INTERNATIONAL JOURNAL OF TECHNOLOGY AND COMPUTING (IJTC)
ISSN-2455-099X,
Volume 2, Issue 6 June 2016.

A REVIEW ON MULTIPLE MALICIOUS AND IRRELEVANT PACKET DETECTION IN VANET

Gurjinder Singh [a,*] , Er. Sushil Kamboj [b]

[a]M-Tech. Student, guri2053@gmail.com SUSCET Tangori

[b] er.kamboj@gmail.com, SUSCET, Tangori

A B S T R A C T

A Vehicular Ad-Hoc Network or VANET is a form of Mobile Ad-Hoc Network or MANET which provides communication between vehicles and between vehicles and road-side base stations. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbors and other vehicles in the network. VANET is different from MANET due to high mobility of nodes and the large scale of networks. Security and privacy are the two main concerns in designing a VANET .Although there are many proposed solutions for improving securities in VANET but security still remains a delicate research subject. The main objective of the system are to propose the algorithm for detection of multiple malicious, invalid and irrelevant requests sent and received from multiple vehicles at a time and to analyze and detect the attacks in the efficient and effective manner for secure environment. In this system we are proposing the MIPDA algorithm for detecting and analyzing the denial-of-service (DOS) attack. And will also apply the proposed algorithm for detection of multiple malicious, invalid and irrelevant requests sent and received from multiple vehicles at a time. To analyze the behavior of proposed method using various performance parameters such as: Packet loss, Life time of network, Total energy consumed, Number of dead nodes and alive nodes, Frequency, Node Velocity.

Keywords: VANET, MIPDA, RSU, DOS, MANET, Packet Loss, Node Velocity

I. INTRODUCTION

A Vehicular Ad hoc Network (VANET) is a significant innovation toward avoiding such deadly traffic mishaps with the assistance of a variety of state-of-the-art Safety applications. A VANET is a self organized, multipurpose, service oriented Communication network enabling vehicle-to-vehicle and vehicle-to-roadside

infrastructure communication for the purpose of exchanging messages to ensure an efficient and comfortable traffic system on roads. It is commonly anticipated that this network would play an effective role for active safety in roads and highways. It is stated earlier that in VANET, the connectivity is done among vehicle to vehicle and vehicle to road side infrastructure (RSU) and vehicle or road side infrastructures to the central authority responsible for the network maintenance. The basic tool for communication is the short range radios that are being installed in any of the nodes. Vehicular node has the shortest transmission range. RSU's are spread sporadically or regularly depending on the deployment of the network in any particular region. In real life RSU's are spread sporadically. They act as an intermediary node between the Central Authority (CA) and Vehicular Node (VN) [1].

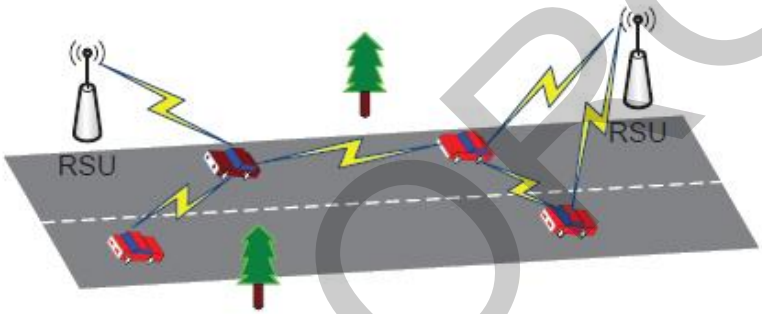

Fig. 1.1. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Communication in VANET.

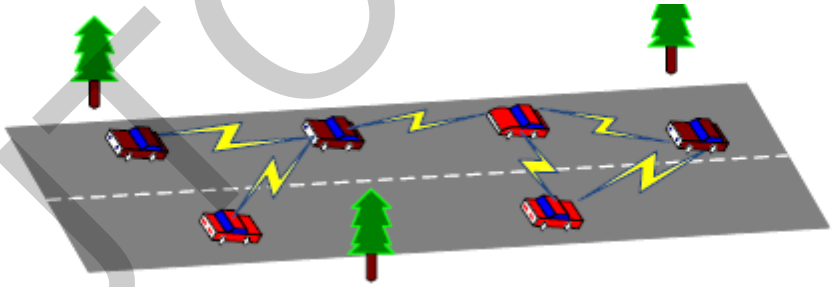

Fig. 1.2. Vehicle-to-Vehicle (V2V) Communication in absence of the roadside

By introducing several different lifesaving applications for traffic management, driver's safety, and driver's assistance. Research on VANETs has drawn a substantial interest among researchers, entrepreneurs, and car manufacturers around the world. Different aspects of VANET research have been discussed and analyzed with the goal of developing new, improved systems for safe traffic environment.

A. BLOOD VESSEL SEGMENTATION

I. Security Vulnerabilities of VANETs

Vehicular ad hoc networks are also prone to several vulnerabilities and attacks. These vulnerabilities can cause small to severe problems in the network and also poses some potential security threats which can deteriorate their functioning. The following section gives a general overview of Vehicular Communications vulnerabilities which are discussed in [4].

a. ***Jamming:*** The jammer deliberately generates interfering transmissions that prevent communication within their reception range. Fig. 1 illustrates that an attacker can relatively easily partition the vehicular network. As the network coverage area (e.g., along a highway) can be well-defined, at least locally, jamming is a low effort exploit opportunity.

b. ***Forgery:*** The correctness and timely receipt of application data is major vulnerability. The attacker forges and transmits false hazard warnings which are taken up by all vehicles.

c. ***Impersonation:*** Message fabrication, alteration, and replay can also be used towards impersonation. For example, an attacker can masquerade as an emergency vehicle to mislead other vehicles to slow down and yield. A vehicle owner deliberately stealing another vehicle's identity [5] and attributing it to his or her own car or vice versa.

d. ***Privacy:*** The inferences on driver's personal data could be made, and thus violating his or her privacy. The vulnerability lies in the periodic and frequent vehicular network traffic: Safety and traffic management messages, transaction based communications (e.g., automated payments).

e. ***Authentication:*** Authentication and the inherent integrity property counter the in-transit traffic tampering and impersonation vulnerabilities.

II. Challenges of VANET

VANETs are an instantiation of mobile ad hoc networks (MANETs) [43]. MANETs have no fixed infrastructure and instead rely on ordinary nodes to perform routing of messages and network management functions. However, vehicular ad hoc networks behave in different ways than conventional MANETs. Driver behaviour, mobility constraints, and high speeds create unique characteristics of VANETs. These characteristics have important implications for designing decisions in these networks.

a. Node Velocity

One of the most important aspects of mobility in VANETs is the potential node velocity. Nodes either denote vehicles or road side units (RSUs) in this case. Node velocity may range from zero for stationary RSUs or when vehicles are stuck in a traffic jam to over 200 km per hour on highways. In particular, these two extremes each pose a special challenge to the communication system. In case of very high node velocities, the mutual wireless communication window is very short due to a relatively small transmission range of several hundred meters [80]. For example, if two cars driving in opposite directions with 90 km/h each, and if we assume a theoretical wireless transmission range of 300m, communication is only possible for 12 seconds. Moreover, the transceivers have to cope with physical phenomena like the Doppler effect. In the review of issues related to inter-vehicle communication in [13], it is shown that routes discovered by topology-based routing protocols get invalid (due to changing topology and link failures at high speeds) even before they are fully established. High node velocities means frequent topological changes. However, a slow movement usually means stable topology, but a very high vehicle density, which results in high interference, medium access problems, etc. For such reasons, very scalable communication solutions are required.

b. **Movement Patterns**

VANET are characterized by a potentially large number of nodes that are highly mobile (i.e. according to cars' speed). This high mobility can be more or less important depending on road nature (small streets vs. highways). Vehicles do not move around arbitrarily, but use predefined roads, usually in two directions. Unpredictable changes in the direction of vehicles usually only occur at intersections of roads. We can distinguish three types of roads [80]:

- **City roads:** Inside cities, the road density is relatively high. There are lots of smaller roads, but also bigger, arterial roads. Many intersections cut road segments into small pieces. Often, buildings right beside the roads limit wireless communication.

- **Rural roads:** These roads usually have much larger segments, which means that intersections are more rare than in cities. Traffic conditions often do not allow the formation of a connected network, because too few vehicles are on the road. The overall direction of rural roads changes more frequently than the direction of highways.

- **Highways:** Highways typically form a multi-lane road, which has very large segments and well-defined exits and on-ramps. High speed traffic encountered here. A node can quickly join or leave the network in a very short

time leading to frequent network partitioning and topology changes. These movement scenarios pose special challenges particularly for the routing. Even on a highway, that gives smooth traffic in one direction, frequent fragmentation was encountered in [13]. In the simulation of 9.2 miles of a highway, in [13], a link lifetime of only about 1 minute was obtained even when driving in the same direction (assuming 500 ft radio range).

c. Node Density

Apart from speed and movement pattern, node density is the third key property of vehicular mobility. The number of other vehicles in mutual radio range may vary from zero to dozens or even hundreds. If we assume a traffic jam on a highway with 4 lanes, one vehicle at every 20 meters and a radio range of 300m, every node theoretically has 120 vehicles in his transmission range. In case of very low density, immediate message forwarding gets impossible. In this case,

more sophisticated information dissemination is necessary, which can store and forward selected information, when vehicles encounter each other. In this case, the same message may be repeated by the same vehicle multiple times. In high density situations, the opposite must be achieved. Here, a message should be repeated only by selected nodes, because otherwise this may lead to an overloaded channel.

III. VANET System Architecture

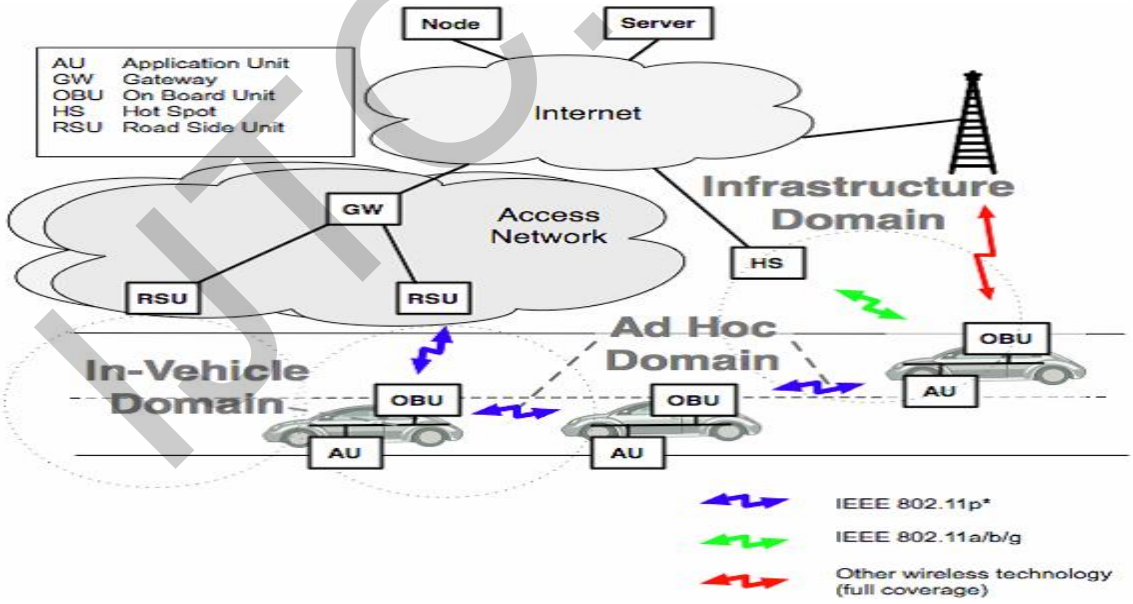

Fig. 1.3. Architecture of VANET

A VANET system architecture consists of different domains and many individual components as depicted in Figure 13. The figure shows three distinct domains (in-vehicle, ad hoc, and infrastructure), and individual components (application unit, on-board unit, and road-side unit).

In-vehicle domain: This consists of an on-board unit (OBU) and one or more applications units (AU) inside a vehicle. AU executes a set of applications utilising the communication capability of the OBU. An OBU is at least equipped with a (short range) wireless communication device dedicated for road safety, and potentially with other optional communication devices (for safety and non-safety communications). The distinction between AU and OBU is logical; they can also reside in a single physical unit. Ad hoc domain: An ad hoc domain is composed of vehicles equipped with OBUs and road-side units (RSUs), forming the VANET. OBUs form a mobile ad hoc network which allows communications among nodes without the need for a centralised coordination instance. OBUs directly communicate if wireless connectivity exists among them, else multi-hop communications are used to forward data. Infrastructure domain: The infrastructure consists of RSUs and wireless hotspots (HT) that the vehicles access for safety and non-safety applications. While RSUs for internet access are typically set up by road administrators or other public authorities, public or privately owned hot spots are usually set up in a less controlled environment. These two types of infrastructure access, RSU and HT, also correspond to different applications types. In case that neither RSUs nor HT provide internet access, OBUs can also utilise communication capabilities of cellular radio networks (GSM, GPRS, UMTS, HSDPA, WiMax, 4G) if they are integrated in the OBU, in particular for non-safety applications.

II. RELATED WORK

It should come as no surprise that a number of research papers have proposed and analyzed various security, privacy and anonymity schemes in recent years. In this chapter, we survey the existing work on VANET security and privacy.

Qi Zhang et al.[1] in 2016 investigated the collection, diffusion, and dissemination of congestion information and the automatic generation and update effect of road network congestion information. Furthermore, we analyze the dissemination effect of different traffic inflow volumes, information packet loss rates, and different rates of IVTIS vehicles. The simulation results show that the proposed system has good autonomy and overall performance in terms of the real-time collection and rapid dissemination of congestion information in a large-scale urban road network. Autonomous vehicle traffic information systems are an important research direction

for next-generation traffic information systems. Existing centralized traffic information systems involve a large initial investment and high operating costs. Furthermore, they suffer from the following problems: the need to communicate large amounts of data, requiring a longer time for road network coverage, unsteady transmission, and the need for an automatic generation and update method for road network congestion information in a large-scale urban road network. T overcome these problems, this paper proposes an intelligent vehicular traffic information system (IVTIS) based on a vehicular ad hoc network (VANET).

Abdul Quyoom et al.[2] in 2015 proposed an Malicious and Irrelevant Packet Detection Algorithm (MIPDA) which is used to analyze and detect the Denial-of Service (DoS) attack. As a result, the attack is eventually confined within its source domains, thus avoiding wasteful attack traffic overloading the network infrastructure. It also reduces the overhead delay in the information processing, which increases the communication speed and also enhances the security in VANET. Security of Vehicular Ad Hoc Networks (VANET) plays a very important role in order to sustain critical life. VANET is a subtype of MANET. For the secure communication of critical life related information, network must need to be available at all the times. The network availability is exposed to several types of attacks and threads possible in VANET. These security attacks and threats include Sybil attacks, misbehaving nodes generate false information, jamming attacks, selfish driver attack, wrongs vehicle position information. These attacks make other vehicles unsecure. Among all these attacks, denial-of-service (DoS) attacks is a major threat to the information economy.

Lynda Mokdad et al.[3] in 2015 proposed a new algorithm DJAVAN (solution of Detecting Jamming Attacks in Vehicle Ad Hoc Networks) to detect a jamming attack in VANETs using the Packet Delivery Ratio (PDR) and with the performance analysis, we determine the threshold that can make the difference between an attack and a poor radio link. With development of wireless communications in the two last decades, new infrastructures have been developed. One of them is the Vehicular Ad hoc Networks (VANETs). They are considered as ad hoc networks with the particularity that the topology is always changed, that make more complicated the resource management and open some beaches in security. Specifically on the Physical and MAC layers that are more vulnerable as they are built on distributed systems and a fluctuating radio channel. Thus, it is not easy to know when transmitted data are not delivered to the destination, if this is due to an attack or to a propagation problem.

Arif Sari et al.[4] in the 2015 has investigated the current and existing security issues associated with the VANET and exposes any slack amongst them in order to lighten possible problem domains in this field. There

is a significant increase in the rates of vehicle accidents in countries around the world and also the casualties involved ever year. New technologies have been explored relating to the Vehicular Ad Hoc Network (VANET) due to the increase in vehicular traffic/congestions around us. Vehicular communication is very important as technology has evolved. The research of VANET and development of proposed systems and implementation would increase safety among road users and improve the comfort for the corresponding passengers, drivers and also other road users, and a great improvement in the traffic efficiency would be achieved.

Karan Verma et al.[5] in the 2014 proposed approach requires fewer resources and is easy to deploy. Simulation results have shown that this method is efficient and effective to defend against and detect DoS attacks. Specifically, this method provides a faster detection time, lower storage capacity and computational cost. The vehicular ad-hoc Network (VANET) has drawn increasing attention in recent years due to its wide range of applications. At the present time, a vehicle's communication is exposed to many security threats such as Denial of Service (DoS) attacks, in which a malicious node forges a large number of fake identities. Internet Protocol (IP) spoofing of addresses – is initiated to disrupt the proper functioning of the fair data transfer between two fast moving vehicles.

V.Lakshmi Praba et al.[6] in the 2013 presented recent developments in wireless communication technologies led to the evolution of Vehicular Ad hoc Network (VANET). The main goal of VANET is to afford communication between vehicles without negotiating security. Regulating the traffic and identifying malicious vehicles plays an important role in VANET. In this paper, traffic control is achieved by sustaining the distance between the vehicles and the malicious vehicles are secluded and further communication is blocked with the malicious vehicles. The existing Ad hoc On Demand Distance Vector (AODV) protocol has been suitably modified to achieve the above mentioned road safety measures. The Proposed protocol was analyzed using the performance metrics Packet Delivery Ratio, Dropped Packets and Routing Overhead.

Albert Wasef et al.[7] in the 2013 proposed an Expedite Message Authentication Protocol (EMAP) for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation checking process. The revocation check process in EMAP uses a keyed Hash Message Authentication Code HMAC, where the key used in calculating theHMAC is shared only between nonrevoked On-Board Units (OBUs). In addition, EMAP uses a novel probabilistic key distribution, which enables nonrevoked OBUs to securely share and update a secret key. EMAP can significantly decrease the message loss ratio due to the message verification

delay compared with the conventional authentication methods employing CRL. By conducting security analysis and performance evaluation, EMAP is demonstrated to be secure and efficient.

II. RESEARCH PROBLEM

Security of Vehicular Ad Hoc Networks (VANET) plays a very important role in order to sustain critical life. VANET is a subtype of MANET. For the secure communication of critical life related information, network must need to be available at all the times. The network availability is exposed to several types of attacks and threads possible in VANET. These security attacks and threats include Sybil attacks, misbehaving nodes generate false information, jamming attacks, selfish driver attack, wrongs vehicle position information. These attacks make other vehicles unsecure. Among all these attacks, denial-of-service (DoS) attacks is a major threat to the information economy. In this paper**,** we are proposing model in order to detect the attacks using Malicious and Irrelevant Packet Detection Algorithm. The mechanism is attached with each and every RSU. Moving vehicles can communicate with RSU through MIPDA mechanism. It is to detect a certain position of the vehicles which will generate the harmful message for other vehicle. After detecting the information of the vehicle position, this information is stored in the certain RSU. And MIPDA algorithm is detecting the position of the vehicle and detects the malicious and invalid packet sent through that vehicle. We will also apply the proposed algorithm for detection of multiple malicious, invalid and irrelevant requests sent and received from multiple vehicles at a time and to analyze and detect the attacks in the efficient and effective manner for secure environment.

III. RESEARCH OBJECTIVES

VANET is a kind of networks in which moving vehicles can communicate with each other. The communication has been done in between cars to road side units, car to car in a short range of 100 to 300 m. VANET is a self-organized network, it has no fixed infrastructure and can be considered as a special implementation of the mobile ad hoc network (MANET). The objective of this

The objectives of the research work are:

1. To study and use the VANET system architecture.
2. To identify the various attacks on VANET and use the detection mechanism.
3. To propose the MIPDA algorithm for detecting and analyzing the denial-of-service (DOS) attack.

4. Also apply the proposed algorithm for detection of multiple malicious, invalid and irrelevant requests sent and received from multiple vehicles at a time.

5. To analyze the behavior of proposed method using various performance parameters such as:

- Packet loss
- Life time of network
- Total energy consumed
- Number of dead nodes and alive nodes
- Frequency
- Node Velocity

REFERENCES

[1] Qi Zhang, Hao Zheng, Jinhui Lan, Jianwei An, And Hong Peng, *"An Autonomous Information Collection And Dissemination Model For Large-Scale Urban Road Networks"* In The IEEE Transactions On Intelligent Transportation Systems, VOL. 17, NO. 4, APRIL 2016.

[2] Abdul Quyoom, Raja Ali and Devki Nandan Gouttam, *"A Novel Mechanism of Detection of Denial of Service Attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)"* in the International Conference on Computing, Communication and Automation (ICCCA2015).

[3] Lynda Mokdada, Jalel Ben-Othmanb, Anh Tuan Nguyen, *"DJAVAN: Detecting jamming attacks in Vehicle Ad hoc Networks"* in the Elsevier 2015.

[4] Arif Sari1, Onder Onursal2, Murat Akkaya, *"Review of the Security Issues in Vehicular Ad Hoc Networks (VANET)" i*n the Int. J. Communications, Network and System Sciences, 2015, pp. 552-566.

[5] Karan Verma, Halabi Hasbullah, *"IP-CHOCK (filter)-Based Detection Scheme for Denial of Service (DoS) attacks in VANET"* in the proc. IEEE, 2014.

[6] V.Lakshmi Praba, A.Ranichitra, *"Isolating Malicious Vehicles and Avoiding Collision between Vehicles in VANET"* in the International conference on Communication and Signal Processing, April 3-5, 2013.

[7] Albert Wasef and Xuemin, *"EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks"* in the IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 1, JANUARY 2013.

[8] Yeongkwun Kim and Injoo Kim, *"Security Issues in Vehicular Networks"* in the ICOIN 2013.

[9] Prabhakar M., Dr. J.N. Singh And Dr. Mahadevan G., *"Defensive Mechanism For Vanet Security In Game Theoretic Approach Using Heuristic Based Ant Colony Optimization"* in the International Conference on Computer Communication and Informatics (ICCCI -2013), Jan. 04 – 06, 2013, Coimbatore, INDIA.

[10] Rasheed Hussain, Fizza Abbas, Junggab Son, and Heekuck Oh, *"TIaaS: Secure Cloud-assisted Traffic Information Dissemination in Vehicular Ad hoc Networks"* in the 2013 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing.

[11] T.W. Chim, S.M. Yiu and Lucas C.K. Hui, *"VSPN: VANET-based Secure and Privacy-preserving Navigation"* in the IEEE Transactions on Computers, 2013.

[12] M. N. Majeed, S. P. Chattha, A. Akram, and M. Zafrullah, "Vehiculara d hoc networks: History and future development arenas," *Int. J. Inf. Techno. Elect. Eng.*, vol. 2, no. 2, pp. 25–29, Apr. 2013.

[13] F. Ahmed-Zaid *et al.*, "Vehicle Safety Communication-Applications (VSC-A) final report: Appendix volume 3 Security," Nat. Highway Traffic Safety Admin., Washington, DC, USA, Sep. 2011.

[14] S. P. Fekete, C. Schmidt, A. Wegener, H. Hellbruck, and S. Fischer, "Empowered by wireless communication: Distributed methods for selforganizing traffic collectives," *ACM Trans. Auton. Adapt. Syst.*, vol. 5, no. 3, Sep. 2010, Art ID 11.