International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-7)

Research Article | **July 2017**

A Novel Mechanism for Detecting DOS Attack in VANET Using EAPDA

Sheethal D
M.Tech, Department of Digital Electronics & Communication Systems, Adichunchanagiri Institute of Technology, Karnataka, India

Chandrashekhar H.K
Associate Professor, Department of Electronics & Communication, Adichuchanagiri Institute of Technology, Karnataka, India

Abstract—

Security is the major concern with respect to the critical information shared between the vehicles. Vehicular ad hoc network is a sub class of Mobile ad hoc network in which the vehicles move freely and communicate with each other and with the roadside unit (RSU) as well. Since the nodes are self organized, highly mobile and free to move therefore any nodes can interact with any other node which may or may not be trustworthy. This is the area of concern in the security horizon of VANETs. It is the responsibility of RSU to make the network available all the time to every node for secure communication of critical information. For this, network availability occurs as the major security requirement, which may be exposed to several threats or attacks. The vehicles and the RSU are prone to several security attacks such as masquerading, Sybil attack, alteration attack, Selfish driver attack, etc. Among these Denial of Service attack is the major threat to the availability of network. In order to shelter the VANET from DoS attack we have proposed Enhanced Attacked Packet Detection Algorithm which prohibits the deterioration of the network performance even under this attack. EAPDA not only verify the nodes and detect malicious nodes but also improves the throughput with minimized delay thus enhancing security. The simulation is done using NS2 and the results are compared with earlier done work.

Keywords—VANET, Ad hoc network , OBU , RSU, GPS.

I. INTRODUCTION

Vehicular ad hoc network is a special form of MANET which is a vehicle to vehicle & vehicle roadside wireless communication network. It is autonomous & self-organizing wireless communication network, where nodes in VANET involve themselves as servers and/or clients for exchanging & sharing information [3]. With a sharp increase of vehicles on the road, new technology is envisioned to provide facilities to the passengers including safety application, assistance to the drivers, emergency warning etc. Vehicular Ad-Hoc Networks (VANETs) is an application of MANETs that allows for communication between road transports vehicles and promotes safety on roads. There is however situations that could cause harm to the vehicle and/or its occupants; vehicles could be tracked, followed or have their messages monitored. Vehicular ad hoc network (VANET) is a sub class of MANET with some unique properties. VANETs have emerging out these days due to the need for supporting the increased number of wireless equipments that can be used in vehicles [1]. Some of these products are global positioning system, mobile phones and laptops. VANETs have some dissimilar properties then MANETs like road pattern restrictions, no restriction on network size, dynamic topology, mobility models, and infinite energy supply, localization functionality and so on. All these characteristics made VANET environment a challenging for developing efficient routing protocols. The major factor in it is the rapidly moving mobile nodes. The increasing mobility of people has caused a high cost for societies as consequence of the increasing number of traffic congestion, fatalities and injuries. Vehicular Ad-Hoc Networks (VANETs) envisage supporting services on Intelligent Transportation Systems (ITSs), as collective monitoring of traffic, collision avoidance, vehicle navigation, control of traffic lights, and traffic congestion management by signaling to drivers. VANETs comprise vehicles and roadside equipments owning wireless interfaces able to communicate among them by wireless and multi-hop communication VANET security should satisfy four goals [5], it should ensure that the information received is correct (information authenticity), the source is who he claims to be (message integrity and source authentication), the node sending the message cannot be identified and tracked (privacy) and the system is robust.

In the year 1998, the team of engineers from Delphi Delco Electronics System and IBM Corporation proposed a network vehicle concept aimed at providing a wide range of applications [1]. With the advancements in wireless communications technology, the concept of network car has attracted the attention all over the world. In recent years, many new projects have been launched, targeting on realizing the dream of networking car and successful implementation of vehicular networks. The project Network On Wheels (NOW) [1] is a German research project founded by Daimler Chrysler AG, BMW AG, Volkswagen AG, Fraunhofer Institute for Open Communication Systems, NEC Deutschland GmbH and Siemens AG in 2004, the project adopts an IEEE 802.11 standard for wireless access. The main objectives of this project are to solve technical issues related to communication protocols and data security for car-to-car communications. The Car2Car Communication Consortium [16] is initiated by six European car manufacturers. Its goal is to create a European industrial standard for car-to-car communications extend across all brands. FleetNet [1] was another European program

which ran from 2000 to 2003 this ad hoc research was dominated by efforts to standardize MANET protocols, and this MANET research focused on the network layer[1], the ultimate challenge was to solve the problem of how to reach nodes not directly within radio range by employing neighbors as forwarders, while the European Commission is pushing for a new research effort in this area in order to reach the goal of reducing the car accidents of 50% by 2010, aiming to reach a satisfactory level of secure VANET. Car TALK 2000 is a European Project focusing on new driver assistance systems which are based upon inter-vehicle communication. The main objectives are the development of cooperative driver assistance systems on the one hand and the development of a self-organizing ad-hoc radio network as a communication basis with the aim of preparing a future standard.

II. VANET WORKING

Vehicular Networks System consists of large number of nodes, approximately number of vehicles exceeding 750 million in the world today [4], these vehicles will require an authority to govern it, each vehicle can communicate with other vehicles using short radio signals DSRC (5.9 GHz), for range can reach 1 KM, this communication is an Ad Hoc communication that means each connected node can move freely, no wires required, the routers used called Road Side Unit (RSU), the RSU works as a router between the vehicles on the road and connected to other network devices. Each vehicle has OBU (on board unit), this unit connects the vehicle with RSU via DSRC radios, and another device is TPD (Tamper Proof Device), this device holding the vehicle secrets, all the information about the vehicle like keys, drivers identity, trip details, speed, rout …etc., see figure 2.

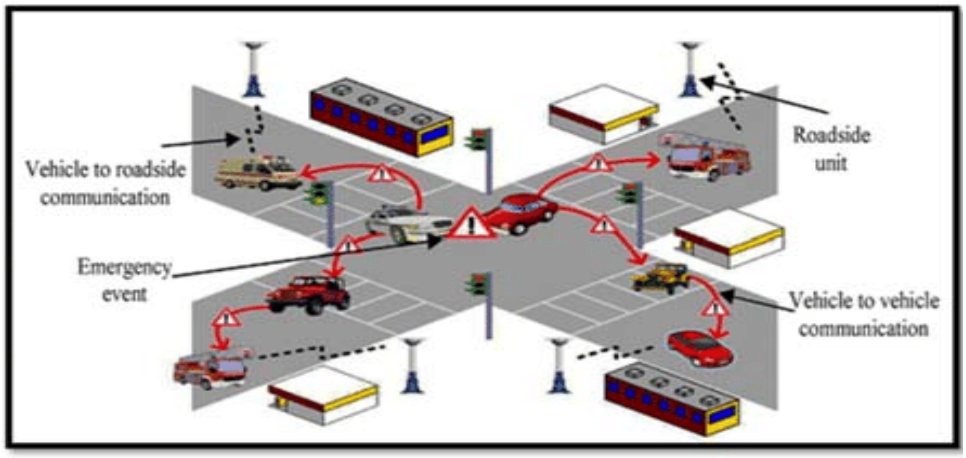

Fig1. VANET Structure

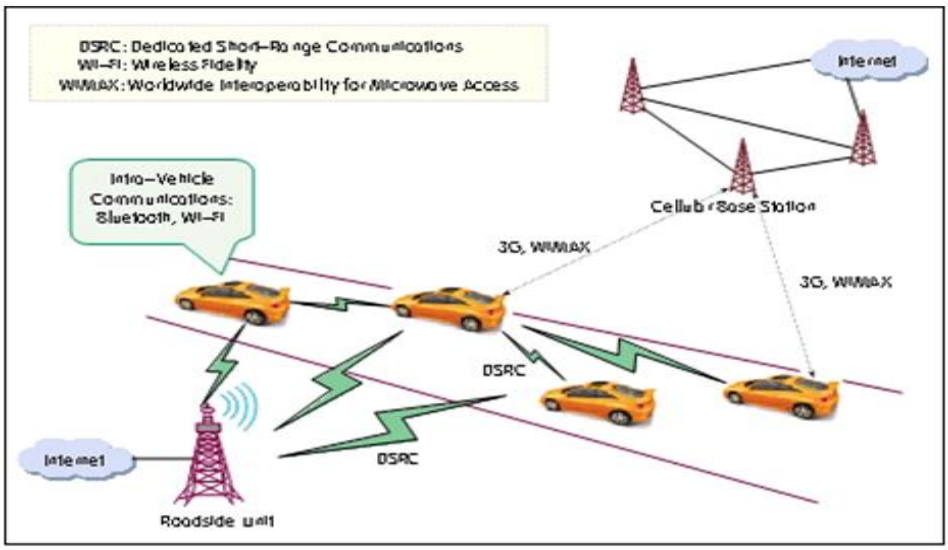

Figure 2. VANET Communication

III. VANET CHARACTERISTICS

The characteristics of a vehicular ad hoc network are unique compared to other mobile ad hoc networks. The distinguishing properties of a VANET offer opportunities to increase network performance, and at the same time it presents considerable challenges. A VANET is fundamentally different [5] from other MANETs.

High Mobility:

The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy [2].

Rapidly changing network topology:
Due to high node mobility and random speed of vehicles, the position of node changes frequently. As a result of this, network topology in VANETs tends to change frequently [3].

Unbounded network size:
VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded [3].

Frequent exchange of information:
The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units. Hence the information exchange among node becomes frequent.

Wireless Communication:
VANET is designed for the wireless environment. Nodes are connected and exchange their information via wireless. Therefore some security measure must be considered in communication[2].

Time Critical:
The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly.

Sufficient Energy:
The VANET nodes have no issue of energy and computation resources. This allows VANET usage of demanding techniques such as RSA, ECDSA implementation and also provides unlimited transmission power [2].

IV. NETWORK ATTACK

Network attacks are always on the top of the list and are classified as a top priority since it can be dangerous to the entire network. A single successful network attack may easily affect the whole network. Few example of network attack are such as Denial of service (DOS) Attack and Sybil Attack.

Denial of Service attack:
This attack happens when the attacker takes control of a vehicle's resources or jams the communication channel used by the Vehicular Network, so it prevents critical information from arriving. It also increases the danger to the driver, if it has to depend on the application's information.

Sybil Attack:
This attack happens when an attacker creates large number of pseudonymous, and claims or acts like it is more than a hundred vehicles, to tell other vehicles that there is jam ahead, and force them to take alternate route[3][4]. Sybil attack depends on how cheaply identities can be generated. For instance an attacker can pretend and act like a hundred vehicle to convince the other vehicles in the road that there is congestion, go to another rout, so the road will be clear.

V. APPLICATION ATTACK

In application attack class, the attacker attention is no other than to manipulate application content for its own benefit. These attackers will tend to suppress or alter the actual message and change it with a false content which may cause harm to other vehicle. This type of attack might be done by either malicious or rational attacker for fun or to serve their own benefits. Few examples of application attack are such as message suppression attack, fabrication attack, alteration attack [1].

Fabrication Attack:
An attacker can make this attack by transmitting false information into the network, the information could be false or the transmitter could claim that it is somebody else .This attack includes fabricate messages, warnings, certificates, identities [4].

Alteration Attack:
This attack happens when attacker alters an existing data, it includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted [3]. For instance, ban attacker can alter a message telling other vehicles that the current road is clear while the road is congested [5].

VI. CONCLUSION

Security is the major issue to implement the VANET. The study of attacks revealed that the attacker generally targets the network layer directly or indirectly hence the routing protocol must be secure enough to prevent the most types of attacks. Each solution must preserve the security requirements like authentication, integrity, and privacy which are more targeted. Vehicular Ad Hoc Networks is an emerging and promising technology, this technology is a fertile region for attackers, who will try to challenge the network with their malicious attacks. This report gives a wide analysis for the

current challenges and solutions. Apart from ensuring availability of information that provides a safer driving behavior and a better travelling experience, the network is an economic, communication, and knowledge management enabler. However, despite the benefits, information security threats and privacy issues pose an enormous challenge to VANET expansion

REFERENCES

[1] Surmukh Singh, Sunil Agrawal VANET Routing Protocols: Issues and Challenges Proceedings of 2014 RAECS UIET Panjab University Chandigarh, 06 – 08 March, 2014.

[2] Komal Mehta, Dr. L. G. Malik, Dr. Preeti Bajaj. Security Challenges, Issues And Their Solutions For VANET. International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013. Ambedkar Institute of Advanced communication Technologies & Research Delhi,India.

[3] Patrick I. Offor. Vehicle Ad Hoc Network (VANET): Safety Benefits and Security Challenges. Nova Southeastern University (po125@nova.edu). December 3, 2012.

[4] Bijan Paul, Md. Ibrahim, Md. Abu Naser Bikas. VANET Routing Protocols: Pros and Cons. International Journal of Computer Applications (0975 – 8887) Volume 20– No.3, April 2011.

[5] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures. Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET). National Advanced IPv6 Center, Universiti Sains Malaysia Penang, Malaysia. June 28, 2010.

[6] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures. Security Analysis of Vehicular Ad Hoc Networks (VANET). 2010 Second International Conference on Network applications, protocols and services.

[7] Arzil.S.A, M. H. Aghdam, and M. A. J. Jamali, (2010) ―Adaptive routing protocol for vanets in city environments using real-time traffic infor- mation,‖ in Proc. ICINA.

[8] Bi.Y, L. Cai, X. Shen, and H. Zhao, (2010) ―A cross layer broadcast protocol for multihop emergency message dissemination in intervehicle communication,‖ in Proc. IEEE ICC.

[9] Fall.K and K. Varadhan, (2000) ―ns notes and documents,‖ The VINT Prohect. UC Berkeley, LBL, USC/ISI, and Xerox PARC. [4] Fogue.M, P. Garrido, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni,(2011) ―Analysis of the most representative factors affecting warning message dissemination in VANETs under real roadmaps,‖ in Proc. 19th Annu. Meeting IEEE MASCOTS, Singapore.

[10] Jianwei.N, L. Chang, C. Canfeng, and M. Jian, (2009) ―Adaptive copy and spread data dissemination in vehicular ad-hoc networks,‖ in Proc. IEEE ICCTA.

[11] Krajzewicz.D, G. Hertkorn, C. Rossel, and P. Wagner, (2002) ―SUMO (Simulation of Urban MObility)—An open-source traffic simulation,‖ in Proc 4th MESM, Sharjah, UAE.

[12] Krauss.S, P. Wagner, and C. Gawron,(1997) ―Metastable states in a microscopic model of traffic flow‖ Phys. Rev. E, vol. 55, no. 5, pp.5597–5602.

[13] Mariyasagayam.N, H. Menouar, and M. Lenardi, (2009) ―An adaptive forwarding mechanism for data dissemination in vehicular networks,‖ in Proc. IEEE VNC, Tokyo, Japan.

[14] Martinez.F.J, M. Fogue, M. Coll, J.-C. Cano, C. Calafate, and P.Manzoni, M. Crovella, L. Feeney, D. Rubenstein, and S. Raghavan, Eds.,(2010) ―Evaluating the impact of a novel warning message dissemination scheme for VANETs using real city maps,‖ in Proc. NETWORKING, Berlin/Heidelberg, Germany.

[15] Tee.C and A. Lee, (2009) ―Adaptive reactive routing for VANET in city environments,‖ in Proc. 10th ISPAN, Kaoshiung, Taiwan.

[16] Miao.L, F. Ren, C. Lin, and A. Luo, (2009) ―A-ADHOC: An adaptive real- time distributed MAC protocol for vehicular ad hoc networks,‖ in Proc.4th ChinaCOM, Xi'an, China.

[17] Slavik.M and I.Mahgoub, (2010) ―Stohastic broadcast for VANET,‖ in Proc.7th IEEE CCNC, Las Vegas, NV.

[18] Suriyapaibonwattana.K and C. Pornavalai, (2008) ―An effective safety alert broadcast algorithm for VANET,‖ in Proc. ISCIT.

[19] Suriyapaiboonwattana.K, C. Pornavalai, and G. Chakraborty, (2009) ―An adaptive alert message dissemination protocol for VANET.

