A survey of the Reactive Routing protocol in VANET with Road Side Units

Amandeep Kaur[1],Tanisha Saini[2]
[1]*M.Tech(Scholar),* [2]*Assistant Professor*
Chandigarh Group of College, Landran

Abstract - Vehicular Ad Hoc Network that formed between vehicles. Security in vehicle ad-hoc network plat very important role. VANET is a subcategory of mobile ad hoc network. It is an emerging new technology to information between vehicles to vehicles. VANETs are measured as one of the most noticeable technologies for improving the efficacy and safety of transportation systems. VANET mostly used to exchange traffic information between the vehicles and prevent accident. In VANETs the high mobility of the nodes is the main concern. AODV protocol is a re-active routing protocol / on-demand routing protocol which resources if there is information to be send then the path will establish. In this paper, AODV is the most normally used topology based on routing protocol for VANET. Using of broadcast information's in the on-demand distance vector route discovery stage caused it is enormously susceptible against various attack. In balanced AODV because it expects all network/system vehicle nodes behave usually. If network sensor nodes are out of simple behaviour then they verified as malicious vehicle node.

Keywords: Vehicle ad-hoc network, AODV routing protocol, broadcast message and Balanced-AODV protocol.

I. INTRODUCTION

In recent years, develop in the wireless communication network and connection of internet as a significant part of our lives. In latest years, driving is an individual of the most incident characteristics of traffic safety. A novel apprehension of Wi-Fi road situation is looking speedily. For this cause a progressive type of data technology defined vehicular ad –hoc network is being implemented[1]. Vanet are the sub-class of mobile ad-hoc network in which transmission vehicle nodes are normally vehicles. Vanet is a mechanization that uses transferring vehicles as phases in a system to initialize a movable network .Vanet network described further as shown in Figure no. 1: Two types of the Vehicle ad hoc network communication have been characterized are[2]:

A. Vehicle-to-Vehicle

In Vehicle to vehicle message, a vehicle communicates to another vehicle in the network/system to alter the information related traffic jams, accidents on roads etc.

B. Vehicle-to-Infrastructure [3]

In vehicle-to-infrastructure, a vehicle give a message with locked equipment unit allocated as the road side unit. Road Side unit connect each other through wireless medium / wired program.

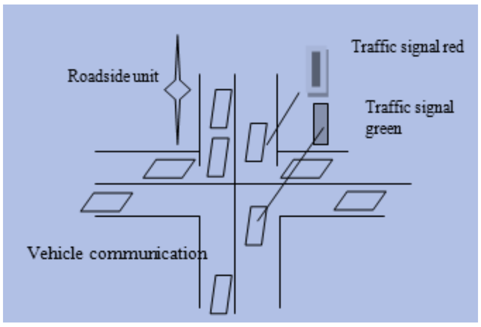

Fig.1 Vehicle ad-hoc network

Vehicular Adhoc Network (VANET) is a special case of Mobile Adhoc Network (MANET) in which mobile knots are vehicles. The distinctive characteristics of VANET are the knots are high mobility and tend to follow planned routes instead of moving at random. Furthermore, vehicles not only communicate with every other but also connect to Road-Side Units (RSUs) and Base Station. VANETs are expected to support several types of services such as route planning, traffic alert dissemination, context aware infotainments [4], and mobile vehicular cloud services. Some characteristics of VANETs resembles with the characteristics of MANETs [5] like highly dynamic topology, frequent disconnected network, Mobility modeling and Prediction, Communication Environment etc. A vehicular ad-hoc network (VANET) adds capacity in the vehicles. Dedicated Short Range Communications (DSRC) Wireless Access for Vehicular Environment (WAVE) has been approved as standards for PHY and MAC layers for vehicular networks. As mobiles are familiar and used by us in our day to day life, likewise the future of VANETs is undoubtedly secure. It has become the part of the government projects. In India, National Highways Authority of India is planning to replace manual toll collections at plazas with electric toll collection (ETC) systems across the country. The ETC system will be created on radio frequency identification (RFID), which will be complemented through a wireless on-board unit (OBU) on a vehicle, as well as a stationery roadside unit (RSU) at the toll piazza. Use of vehicular ad-hoc network have many advantages like Self-configuring nodes are also routers, Flexible ad hoc can be temporarily setup at any time, in any place, Lower getting-started costs and so many other benefit of use vehicular network[6].

Roadside sensor nodes measure the road condition at several positions on the surface, collective the measured standards & communicate their amassed value to an approaching vehicle [7]. The vehicle generates a cautionary message & dispenses it to all automobiles in a certain geographical region, potentially using wireless multi-hop statement. For post-accident examination, sensor nodes continuously measure the road condition and supply this info within the WSN itself. When a coincidence occurs, road condition data stored over a sufficiently long period can be used for criminal modernization of road accidents. In contrast to the accident prevention service, such an accountability service requirements to be constrained to a well specified group of end-users, e.g. insurance companies or the road patrol. Information stored within the WSN can also be exploited to judge a driver's driving style according to the road complaint at the moment of an accident [8].

II. RELATED WORK

Christophe J et.al (2005) describes a new model for highway traffic and events that can be used to automatically produce movement files readable by the NS-2.28 simulator. Through reproductions of such vehicular networks using flooding and IEEE 802.11 for safety-related applications [9]. **Mandeep Kaur et al,; (2016)** presented RTMU is using various mathematical computations for traffic pattern investigation to detect the aberration in data traffic between the cluster nodes. All of the nodes in the scenario are GPS location aware nodes and sharing their location actively with RTMU. Also all of the VANET nodes connect with each other through RTMU[10]. **Nikita Lyamin et al., (2014)** applied the new method for real-time detection of Denial-of-Service (DoS) attacks in IEEE 802.11p vehicular ad-hoc networks (VANETs) is planned. The study is focused on the "jamming" of periodic position messages (beacons) exchanged by vehicles in a platoon. Prospects of attack detection and false alarm are projected for two different attacker models.[11] **Vinh Hoa LA et al,; (2014)** present in this paper a survey of VANETs attacks and solutions in sensibly considering other similar works as well as informing new attacks and categorizing them into different classes [12].

Table no. 1 Differentiate the various techniques and Performance parameters.

Year	Attack /Technique/Model Used	Performance Parameters
2005	Modeling Highway traffic [13]	Packet, Lower Density and Higher Density
2016	AODV or TORA[14]	-
2015	Dynamic Source Routing[15]	E2E,PDR,Goodput and Throughput
2013	DDoS Intruder[16]	Detection Rate and Acceptance rate of Packets

III. APPLICATIONS AND THREATS OF VANET

We are arranging the applications of VANETs into following classes:

1) Security oriented
2) Commercial oriented
3) Suitability oriented and
4) Creativity Applications

These beings the most mutual damaging attack found in VANET concerning communication networks are the DoS attack. Such an attack denies all facilities providing by the VANET [13].

1) Application Mode
2) Network Mode

IV. ROUTING PROTOCOL IN VANET

Routing Protocol directs the way to ex-change a data between sender and receiver; it adds the process in implementing a route, conclusion to forward the packets and maintaining to route/ recovering from routing fail. The huge amounts of routing protocol have been implemented to offer speedily and secure routing of data. But each protocol is appropriate for a dissimilar scenario and no protocol topology based protocols, position-based protocols, cluster based protocols and broadcast based protocols. Various types of routing Protocols:

1) Ad-hoc on demand Distance Vector

The information in this segment concerning the Ad Hoc on Demand Distance Vector Protocol (AODV) protocol is taken from the RFC. AODV is a reactive protocol, i.e., so the ways are created and preserved only when they are desirable. Also the information about the active neighbours is received through the discovery of the destination host. When the conforming route breaks, then the neighbours can be notified. The route discovery is used by distribution the RREQ message to the neighbours with the demanded destination sequence number, which prevents the old material to be replied to the demand and also prevents looping problem, which is essential to the old distance vector protocols. The route demand does not add any new information about the past hosts only it surges its hop metric. Each passed host makes update in their own routing table about the entreated host. This information helps the sink reply to be easily routed back to the requested host. The route reply use RREP message that could be only generated by the terminus host or the hosts who have the information that the destination host is alive and the joining is fresh[14].

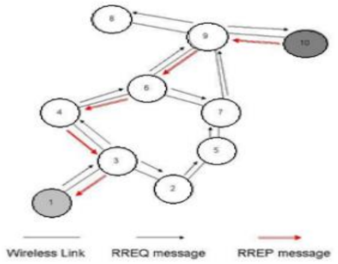

Fig.2 Aodv Protocol

2) *Balanced-AODV*

Is a source initiated routing protocol & usages HELLO letters to recognize its neighbors? Source node broadcasts a route request to its neighbors which fill advancing to the destination. Then the terminus unicast a route reply packet to the sender. Each node preserves broadcast-id which increases for new RREQ. When a RREQ arrives at a node, it checks the broadcast id if it is minus than or alike to previous memo then it will discard the packet [15]. To avoid delay in communication and power consumption as well as decrease in packet delivery ratio we planned B-AODV with link/path negotiation and failure prevention with load factor. The main motive behind this planned work is that we want to transfer data packages by using minimum link failure.

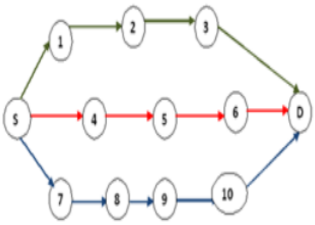

Fig.3 B-AODV Protocol

Table 2: Various types of Attacks

Attack Name	Description
Worm Hole Attack	receives a packet at one point and tunnels it to one more malicious knob in the system.
Sybil Attack	many copies of malicious knobs
DDoS Attack	Unwanted Request Sent
Black Hole Attack	malicious node easily misroute network traffic to it.

V. CONCLUSION

In this study, author have concluded that nevertheless of the secure routing protocols, the VANET construction continues to remain possibly insecure as the attacker can eavesdrop in even without ahead traceable physical access. Thus, the protocol strategies prove to be security-naive. Various apparatuses have calculated and pointed out and tools used by the attackers posing as innocent vehicles in the network, to implement attacks by misusing the weaknesses in the protocol designs. The integration of RSUs and comfort applications in VANET has also led to increased network vulnerabilities. The study also analysed a few practices and theoretical constructs employed to mitigate the insecurities in VANET their drawbacks were studied. Major security flaws in VANET and their adversaries are also presented in the paper. Arrive at a conclusion that amidst the evolving network environment, VANET needs to be supported with more secure architecture, with privacy of the users being acknowledged as the foremost exponent of VANET requirements.

VI. REFERENCES

[1]. Hao, Yong, Yu Cheng, Chi Zhou, and Wei Song. "A distributed key management framework with cooperative message authentication in VANETs." IEEE Journal on selected areas in communications 29, no. 3 (2011): 616-629.

[2]. Lu, Rongxing, Xiaodong Lin, Xiaohui Liang, and Xuemin Shen. "A dynamic privacy-preserving key management scheme for location-based services in vanets." IEEE Transactions on Intelligent Transportation Systems 13, no. 1 (2012): 127-139.

[3]. Choudhary, Parul. "A literature review on vehicular Adhoc Network for intelligent transport." In Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on, pp. 2209-2213. IEEE, 2015.

[4]. Lin, Xiaodong, and Xu Li. "Achieving efficient cooperative message authentication in vehicular ad hoc networks." IEEE Transactions on Vehicular Technology 62, no. 7 (2013): 3339-3348.

[5]. Raya, Maxim, Adel Aziz, and Jean-Pierre Hubaux. "Efficient secure aggregation in VANETs." In Proceedings of the 3rd international workshop on Vehicular ad hoc networks, pp. 67-75. ACM, 2006.

[6]. Studer, Ahren, Elaine Shi, Fan Bai, and Adrian Perrig. "TACKing together efficient authentication, revocation, and privacy in VANETs." In 2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp. 1-9. IEEE, 2009.

[7]. Hao, Y., Cheng, Y. and Ren, K., 2008, November. Distributed key management with protection against RSU compromise in group signature based VANETs. In IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference (pp. 1-5). IEEE..

[8]. Merlin, Christophe J., and Wendi Beth Heinzelman. "A study of safety applications in vehicular networks." In IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005., pp. 8-pp. IEEE, 2005.

[9]. Kaur, Mandeep, and Manish Mahajan. "Protection Against DDOS Using Secure Code Propagation In The VANETs." (2016).

[10]. Lyamin, Nikita, Alexey V. Vinel, Magnus Jonsson, and Jonathan Loo. "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11 p Vehicular Networks." IEEE Communications letters 18, no. 1 (2014): 110-113.

[11]. Verma, Karan, Halabi Hasbullah, and Ashok Kumar. "Prevention of DoS attacks in VANET." Wireless personal communications 73, no. 1 (2013): 95-126.

[12]. H. Füßler, M. Mauve, H. Hartenstein, and D. Vollmer, “A Comparison of Routing Strategies in Vehicular Ad-Hoc Networks”, Reihe Informatik, March 2002.

[13]. Kaur, Mandeep, and Manish Mahajan. "Protection Against DDOS Using Secure Code Propagation In The VANETs." (2016).

[14]. Rawat, Ajay, Santosh Sharma, and Rama Sushil. "VANET: Security attacks and its possible solutions." Journal of Information and Operations Management 3, no. 1 (2012): 301.

[15]. Jadhao, A.P. and Chaudhari, D.N., “A Novel Approach For Security Aware Topological Based Routing Protocol In Vehicular Adhoc Network”, International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013.