Comparative Analysis of Secure Routing Protocol with Malicious Node Attack in VANET Using CBR/UDP Traffic: A Review

Himanshi
M.Tech Scholar, ECE Department
M.R.I.E.M, Rohtak
mahihooda9@gmail.com

Kirti Dahiya
Assistant Professor, ECE Department
M.R.I.E.M, Rohtak
kirtidahiya@mriem.org

Abstract – One of biggest challenges to implement adhoc network is its dynamic topology and security issue. There are possibilities of active and passive attack in network to alter the authentic data or to steal the data. There are various types of passive attacks which are very dangerous for effective communication. Black hole attack in Vehicular Ad Hoc Network is major problem related with the field of computer networking. In this paper we present the performance analysis of the black hole attack in Vehicular Ad Hoc Network. We elaborate the different types of attacks and their depth in ad hoc network. The performance metric is taken for the evaluation of attack which depends on a packet end to end delay, network throughput and network load. In reference work black hole attack used in network communication using AODV protocol. There are many problems in VANET and specifically security issues. Besides this need a security algorithm which helps to secure our privacy so that unauthorized person cannot access data.

Keywords*–VANET, Packet Network, Security, End to End Delay, Adhoc, Protocol, Black Hole Attack*

*****

1. INTRODUCTION

VANET plays a major role in networks due to their application of ad hoc network technology. Vehicular Ad-Hoc Network is a technology that has attracted several industries. Security parameters in VANET are now receiving popularity in the research community. In VANET environment, significant decision format has to be determined with the problems related to attack modeling, optimizing response and allotment of defense resources in a wide manner. However, a single defense mechanism cannot provide solution to the attack models that are affecting the VANETs. The game theory model is used as a defense mechanism against sophisticated and complex type of attacks arising in VANET.

The security applications help to keep lives move smoothly and recover traffic conditions during problematic cases [7]. VANET plays a major role in networks due to their application of ad hoc network technology. Vehicles are the best part of those networks and their capability is to be efficiently handled in self organizing networks with no previous knowledge about the nodes in the network. Their safety altitude is very low and they are highly susceptible components of the network which can be targeted easily.

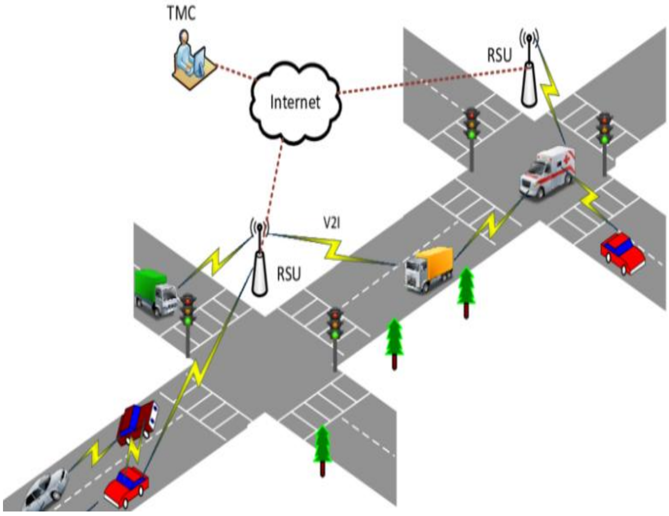

Figure 1 Vehicular Ad hoc Networks configuration

2. RELATED WORK

P.S Hiremath et al: A MANET is a group of computing nodes or cell or other devices used for communication which are capable of communication among each other with no support of an infrastructure that is fixed. The proposed method is based on adaptive fuzzy inference system for MANET in order to detect and prevent the cooperative black hole attack. The popular protocol utilized in MANET is on-demand distance vector protocol, and is simulated using NS2. The simulated results of the proposed method are compared with that of an adaptive method, wherein source node checks all nodes activity by using DAT table that maintains from-node-to-next-node's information and declares black hole node by channel overhearing method. It is observed that the proposed method based on adaptive fuzzy logic system shows better performance as compared to adaptive method in terms of throughput, end-to-end delay and packet delivery ratio [8].

Sathish M et al: Ad hoc On Demand Distance Vector (AODV) routing is an extensively accepted routing protocol for MANET. The inadequacy of security considerations in the design of AODV makes it vulnerable to black hole attack. In a black hole attack, malicious nodes attract data packets and drop them instead of forwarding. Among the existing black hole detection schemes, just a few strategies manage both single and collaborative attacks and that too with much routing, storage and computational overhead. This paper describes a novel strategy to reduce single and collaborative black hole attacks, with reduced routing, storage and computational overhead [6].

Roshan Jaha et al: Routing in vehicular ad-hoc network is current area of research due to fast mobility of vehicles. A new route in very less time has to be developed to communicate with the base station. If any node behaving like malicious and creates attack on network, than whole communication will be squeeze. This paper presents a routing strategy to prevent from attack and identify the malicious node. The strategy has been implemented on QualNet 5.0 and compared with other routing protocols in the presence of malicious nodes [5].

Heithem Nacer et al: VANET was proposed in order to prevent accidents and to improve road safety. Indeed, IEEE 1609.4 was developed to support multi-channel mechanism to provide both safety and non-safety applications. The CCH interval is also a key parameter for the 802.11p MAC protocol. In order to get a wide view of the different techniques used to broadcast a message, we evaluate the performance of the 802.11p MAC protocol with various vehicle densities and different CCH interval settings. Moreover, we propose SABM, a Scheduling Algorithm for vehicles attempting to transmit a Beacon Message, which firstly adjusts the CCH interval according to the road traffic and then schedule the safety messages based their priorities. The simulation results show that SABM outperforms the IEEE 802.11p MAC protocol. [4].

Bharti et al: VANET are the promising approach to provide safety to the drivers and which is a growing technology. VANET is the new form of MANET. There are different types of attack but in our paper we are discussing about Black hole attack. There are two types of traffic pattern CBR and TCP. In this paper, we are analyzing the Black hole attack using CBR (Constant Bit Rate) and TCP (Transmission control Protocol) traffic pattern in Manhattan Grid scenario under AODV protocol. The purpose of this paper is to analyzing the different traffic pattern with Black hole attack and without Black hole attack on the basis of Performance metrics Throughput, end-to-end delay and Packet drop ratio. The simulation setup compromises with different no. of Vehicular nodes using Constant speed. In this we are using simulation NS2 [2].

Sagar R Deshmuk et al: The self configuring and infrastructure less property of MANETs makes them easily deployable anywhere and extremely dynamic in nature. Lack of centralized administration and coordinator are the reasons for MANET to be vulnerable to active attack like black hole. Black hole attack is ubiquitous in mobile ad hoc as well as wireless sensor networks. Black hole affected node, without knowing actual route to destination, spuriously replies to have shortest route to destination and entice the traffic towards itself to drop it. Network containing such node may not work according to the protocol being used for routing. This article proposes an AODV-based secure routing mechanism to detect and eliminate black hole attack [3].

Salim Lachdhaf et al: VANETs are used to provide an efficient Traffic Information System (TIS), Intelligent Transportation System (ITS), and Life Safety. The mobility of the nodes and the volatile nature of the connections in the network have made VANET vulnerable to many security threats. Black hole attack is one of the security threat in which node presents itself in such a way to the other nodes that it has the shortest and the freshest path to the destination. Hence in this research paper an efficient approach for the detection and removal of the Black hole attack in the Vehicular Ad Hoc Networks is described. The proposed solution is implemented on AODV Routing protocol one of the most popular routing protocol for VANET. The found results show the efficacy of the proposed method as throughput and the delivery ratio of the network does not deteriorate in presence of the back holes The strategy can detect both the single Black hole attack and the Cooperative Black hole attack in the early phase of route discovery [1].

3. ATTACKS IN ADHOC NETWORK

Securing wireless adhoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information [9-10]. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

Passive Attacks

Passive attacks are the attack that does not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping .Detection of these attack is difficult since the operation of network itself does not get affected.

Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. Active attacks can be internal or external.

- External attacks are carried out by nodes that do not belong to the network.
- Internal attacks are from compromised nodes that are part of the network.

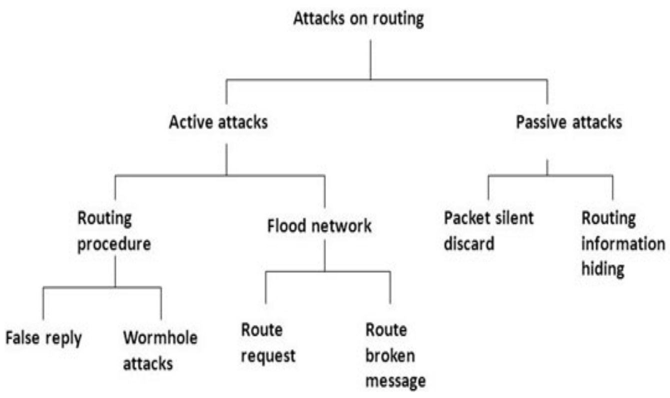

Figure 2 Various Attacks in WSN

Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication

Black hole Attack: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol [12].

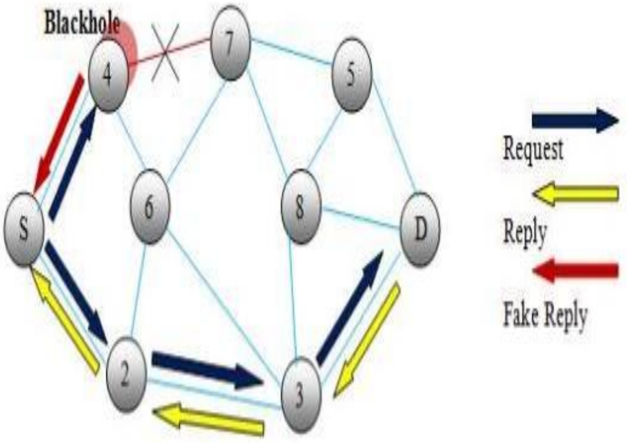

Figure 3 Black hole attack diagram

5. TECHNICAL CHALLENGES

The technical challenges deals with the technical obstacles which should be resolved before the deployment of VANET. Some challenges are given below:

Network Management: Due to high mobility, the network topology and channel condition change rapidly. Due to this, we can’t use structures like tree because these structures can’t be set up and maintained as rapidly as the topology changed.

Congestion and collision Control: The unbounded network size also creates a challenge. The traffic load is low in rural areas and night in even urban areas. Due to this, the network partitions frequently occurs while in rush hours the traffic load is very high and hence network is congested and collision occurs in the network.

Environmental Impact: VANETs use the electromagnetic waves for communication. These waves are affected by the environment. Hence to deploy the VANET the environmental impact must be considered.

MAC Design: VANET generally use the shared medium to communicate hence the MAC design is the key issue. Many approaches have been given like TDMA, SDMA, and CSMA etc. IEEE 802.11 adopted the CSMA based Mac for VANET.

Security: As VANET provides the road safety applications which are life critical therefore security of these messages must be satisfied [14].

Social and Economic Challenges

Apart from the technical challenges to deploy the VANET, social and economical challenges should be considered. It is difficult to convince manufacturers to build a system that conveys the traffic signal violation because a consumer may reject such type of monitoring. Conversely, consumer appreciates the warning message of police trap. So to motivate the manufacturer to deploy VANET will get little incentive

6. CONCLUSION

VANET playing a great importance in our life due to vast potential it has still many challenges left in order to overcome. Security of VANET is one of the important features for its deployment. In our review paper, we have analyzed the behavior and challenges of security threats in Vehicular Ad-Hoc networks with solution finding technique. In our base work black hole attack used in network communication using AODV protocol. As we know there are many issues in VANET and specially security issues. After going through various research papers need to work so efficiently to overcome with the challenges. With pace of time new technology came into existence to enhance the parameters. In these days machine learning and artificial intelligence are very popular with IoT concept. We can adept these technology for further enhancement.

REFERENCES

[1] Salim Lachdhaf,, Mohamed Mazouzi, " Detection and Prevention of Black Hole Attack in VANET Using Secured AODV Routing Protocol", Conference Paper, DOI: 10.5121/csit.2017.71503 Natarajan Meghanathan et al. (Eds) : NeTCoM, CSEIT, GRAPH-HOC, NCS, SIPR – 2017 pp. 25– 36, 2017

[2] Bharti, D.P.Dvedi, " Performance Analysis of Black hole Attack using CBR/UDP Traffic Pattern with AODV routing Protocol in VANET", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2016): 6.391

[3] Sagar R Deshmukh, P N Chatur, Nikhil B Bhople," AODV-Based Secure Routing Against Black hole Attack in MANET", IEEE International Conference On Recent Trends in Electronics Information Communication Technology, India, pp. 1960-1964, 2016

[4] Heithem Nacer and Mohamed Mazouzi, "A Scheduling Algorithm for Beacon Message in Vehicular Ad Hoc Networks",International Conference on Hybrid Intelligent Systems (HIS 2016),Marrakech, Morocco, pp. 489-497, 2016.

[5] Roshan Jahan, Preetam Suman, "Detection of malicious node and development of routing strategy in VANET," 3rd International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, pp. 472-476, 2016

[6] Sathish M, Arumugam K, S. Neelavathy Pari, Harikrishnan V S, "Detection of Single and Collaborative Black Hole Attack in MANET," International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE, pp.2040-2044, 2016.

[7] Sathish M, Arumugam K, S. Neelavathy Pari, Harikrishnan V S, "Detection of Intelligent Malicious and Selfish Nodes in VANET using Threshold Adaptive Control," 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA), IEEE, 2016

[8] P.S Hiremath and Anuradha T, "Adaptive Fuzzy Inference System for Detection and Prevention of Cooperative Black Hole Attack in MANETs", International Conference on Information Science (ICIS), pp.245-251, 2016

[9] P.S Hiremath and Anuradha T, "Adaptive Method for Detection and Prevention of Cooperative Black Hole Attack inMANETs", International Journal of Electrical and Electronics and Data Communication, Volume-3, Issue-4, pp.1-7, 2015

[10] R. Khatoun, P. Guy, R. Doulami, L. Khoukhi and A. Serhrouchni, "A Reputation System for Detection of Black Hole Attack in Vehicular Networking," International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC), 2015

[11] Surmukh, S.; Kumari, P.; Agrawal, S. Comparative Analysis of Various Routing Protocols in VANET. In Proceedings of 5th IEEE International Conference on Advanced Computing & Communication Technologies, Haryana, India, 21–22February 2015

[12] Elias C. Eze, Sijing Zhang and Enjie Liu," Vehicular Ad Hoc Networks (VANETs): Current State, Challenges, Potentials and Way Forward", Proceedings of the 20th International Conference on Automation & Computing, Cranfield University, Bedfordshire, UK, 2014

[13] Sabih ur Rehman, M. Arif Khan, Tanveer A. Zia, Lihong Zheng, "Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges", Journal of Wireless Networking and Communications, 2013, pp. 29-38.

[14] Sirwan A.Mohammed and Sattar B.Sadkhan, "Design Of Wireless Network Based On Ns2", Journal of Global Research in Computer Science (jgrcs), Volume 3, No. 12, December 2012.

[15] Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan," Denial of Service (DOS) Attack and Its Possible Solutions in VANET", International Scholarly and Scientific Research & Innovation 4(5) 2010, World Academy of Science, Engineering and Technology, Vol:4 2010-05-25.