INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 4)
Available online at: www.ijariit.com

Black hole attack analysis in vehicular ADHOC Network

Krishan Kumar
krishan.kkl007@gmail.com
CBS Group Of Institution, Jhajjar, Haryana

Sonia Sharma
snsharma804@gmail.com
CBS Group Of Institution, Jhajjar, Haryana

ABSTRACT

The use of wireless links furnishes a VANET unsafe to malicious attacks for example Denial of Service, black hole attack, Sybil attack, selective forwarding and altering routing information. In Vehicular Networks are contemplated as the unique class of wireless networks, also called as VANET. It is a major part of Intelligent Transport System (ITS). VANET technology is recognized for enhancing road safety and transport efficiency. But, there are huge security issues in VANET, therefore, there must be a reliable way for communication which is quite tedious and important concern. In this review article, we studied Black Hole attacks under CBR/UDP traffic pattern using various protocols from various research papers of high quality. There are possibilities of various attacks like an active and passive attack on the network to access data. As we know there are many issues in VANET and especially security issues. Our research work will be carried out using NS-2 simulator. Besides this, a detailed study of the attack examined because there are abundant numbers of attack available. These attacks are divided into an active and passive attack and further, these two are classified. In this review paper, we convoluted the diverse class of attacks and their depth in an ad-hoc network.

Keywords— *Black Hole Attack, Network, Secure, End to End Delay, Adhoc, Protocol, VANET, Packet*

1. INTRODUCTION

MANET is a kind of wireless ad-hoc network and it self-configuring network of mobile routers connected by wireless links the union of which forms an arbitrary topology. The routers, the participating nodes act as a router, are free to move randomly and manage themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion or may be connected to the larger Internet. A mobile ad hoc network is a collection of self-configuring and an adaption of a wireless link between communicating devices (mobile, devices) to form an arbitrary topology without the use of existing infrastructure. In wireless network technology, the simulative analysis is a significant method to understand the performance of routing protocol

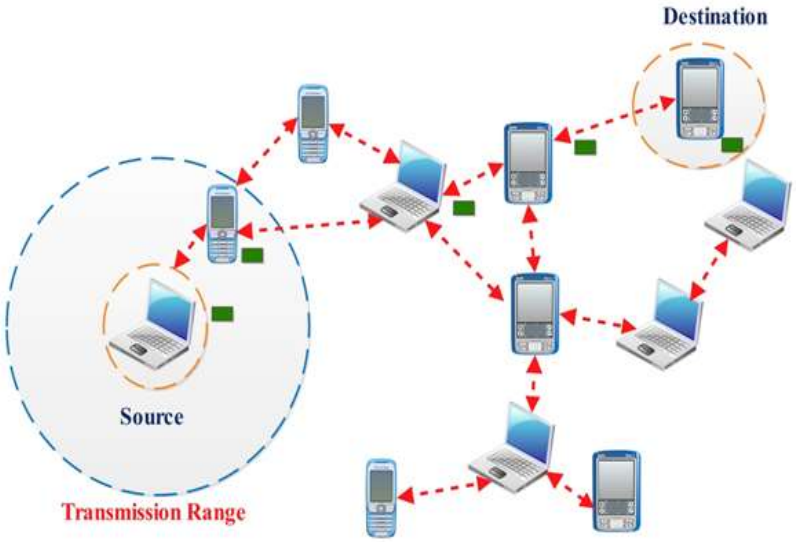

Fig. 1: Overview of MANET architecture

Nowadays numerous kinds of experiments in VANET transportations have been recognized and addressed. A large number of routing protocols have been proposed for VANET. A VANET routing rules the two-way transmission objects interchange messages; it includes the process of creating a route, choice in sending, and action in continuing the route or improving from

© 2018, www.IJARIIT.com All Rights Reserved

routing failure. VANET location-based protocols can be categorized as Position-based and Topology-based. The topology-based routing protocols can further be divided into proactive & reactive protocols. Enough research has already been carried out which includes the comparison of various routing protocols and their performance evaluation based on different mobility models. It will be interesting to evaluate the performance of one of the routing protocol by varying the number of mobile nodes.

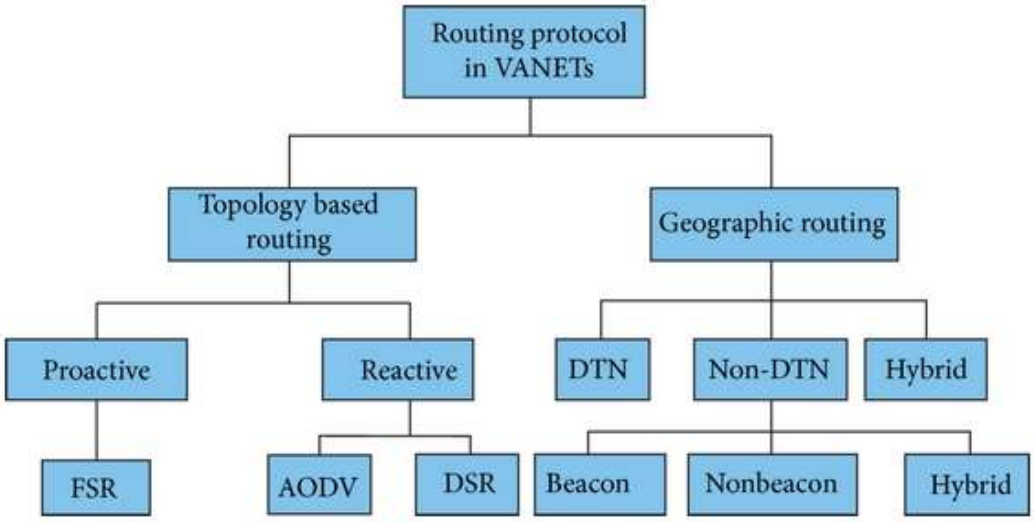

Fig. 2: Routing Protocol flowchart of VANET

2. RELATED WORK

Due to Mahesh Kumar, Kuldeep Bhardwaj: VANETs) are a specific type of the MANETs to assist communications among nearby devices or vehicles. VANET is mostly planned to make available safety-related information by warning drivers about road conditions, accidents, and traffic management by helping drivers to discover the best available path to their destination. A number of distinctive properties make VANETs vulnerable for attackers to exploit and to decrease the normal performance of the networks. Black hole attack in Vehicular Ad Hoc Network is the most severe problem associated with the field of computer networking where the black node absorbs all the data packets in the network. In Black hole attack, a malevolent node utilizes its routing protocol in order to announce itself for having the direct path to the destination node. The main target of the paper is to measure the impact of Blackhole attack on the VANET's AODV routing protocol. Measurements of several parameters with inclusive analysis and comparisons are presented [7]. P.S Hiremath and Anuradha: The Mobile ad-hoc networks (MANETs) networks that are defined as the wireless self-configuring networks that are capable of operating without the support of any fixed infrastructure and a central coordinator which makes the routing a complicated task. One of the main challenges in MANET is to design a robust security solution that can protect MANET from various routing attacks. MANET is vulnerable to different types of attacks such as black hole, sybill attack, wormhole attack, gray hole attack and so on. Among them, a black hole is considered to be a major attack which affects the entire network performance based on routing, packet delivery ratio, throughput, and an end to end delay of packets. The communication takes place between two parties by sharing their information like from-node to next-hop-node's information. In this paper, an adaptive method for detection and prevention of black hole attack in a MANET is proposed based on the Data Access Table, which is an array that maintains from-node to next-hop-node's information. We choose AODV as routing protocol and NS2 as simulator tool. The results are compared with a threshold-based algorithm for detection and prevention of cooperative black hole attack in a MANET. The adaptive method gives better performance than the threshold based algorithm, in terms of throughput, packet delivery ratio and end-to-end delay [9]. Surmukh et al: To make the drive safer in future vehicular ad hoc network can ease our life. For its success, it needs efficient routing protocols for communication among vehicles. Such communication can either through roadside units (RSUs) or onboard units (OBUs) in the vehicles. In this paper, we are exploiting various existing routing protocols like AODV, AOMDV, DSR, and DSDV by varying the velocity of vehicles and then comparing their performances with respect to throughput, an end to end delay, packet delivery ratio and normalized routing load during communication [11]. Elias C. Eze et al: Recent advances in wireless communication technologies and the automobile industry have triggered a significant research interest in the field of VANETs over the past few years. VANET consists of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications supported by wireless access technologies such as IEEE 802.11p. This innovation in wireless communication has been envisaged to improve road safety and motor traffic efficiency in the near future through the development of Intelligent Transport Systems (ITS). Hence, government, automobile industries, and academia are heavily partnering through several ongoing research projects to establish standards for VANETs. The typical set of VANET application areas, such as vehicle collision warning and traffic information dissemination have made VANET an interesting field of wireless communication. This paper provides an overview of current research state, challenges, and potentials of VANETs as well the way forward to achieving the long-awaited ITS [12].

3. ATTACKS: ACTIVE AND PASSIVE

Wormhole Attack: In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message is tunneled. This tunnel between two colluding attacks is known as a wormhole. In DSR, AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Wormholes are dangerous because they can do damage without even knowing the network.

© 2018, www.IJARIIT.com All Rights Reserved

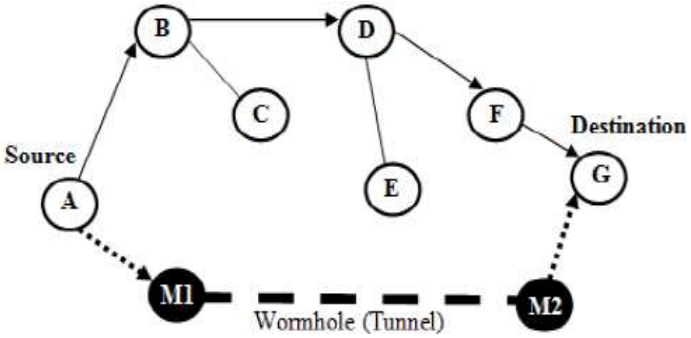

Fig. 3: Wormhole attack configuration

Sybil attack: The Sybil attack especially aims at distributed system environments. The attacker tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from source to destination. A consequence of this is that attackers have a harder time to destroy the integrity of information

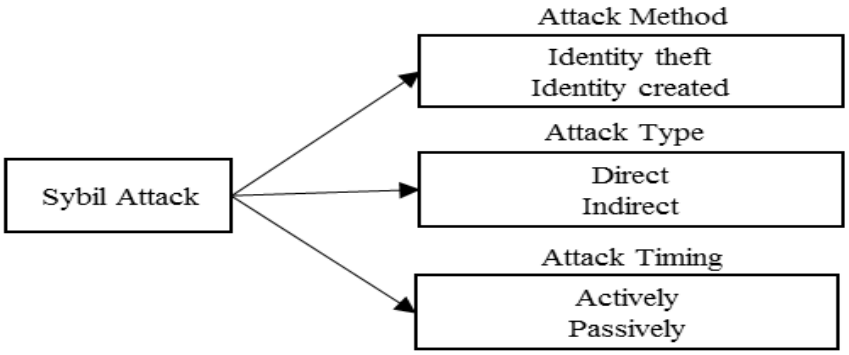

Fig. 4: Sybil attack details

Gray-hole attack: This attack is also known as routing misbehaviour attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertises itself as having a valid route to the destination while in the second phase, nodes drop intercepted packets with a certain probability.

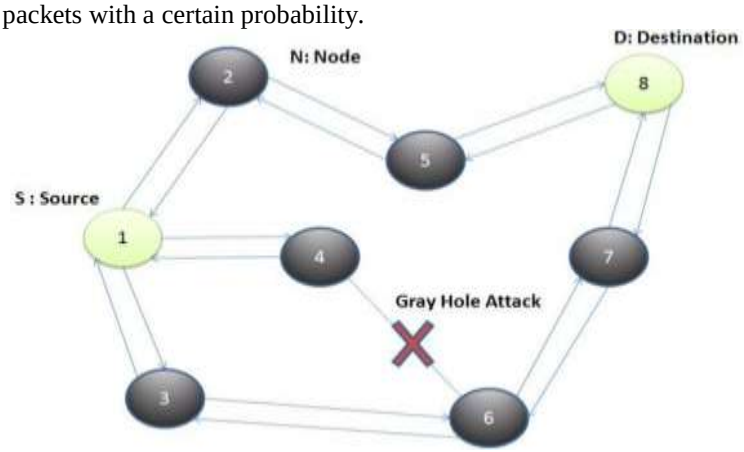

Fig. 5: Gray hole attack

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 listens to the requests in a flooding-based protocol.

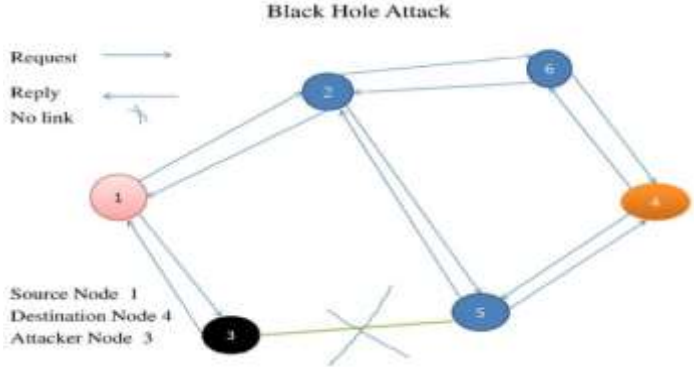

Fig. 6: Blackhole attack diagram

© 2018, www.IJARIIT.com All Rights Reserved

PASSIVE ATTACKS

Traffic Monitoring: It can be developed to identify the communication parties and functionality which could provide information to launch further attacks. It is not specific to MANET, another wireless network such as cellular, satellite, and WLAN also suffer from these potential vulnerabilities.

Eavesdropping: The term eavesdrops implies overhearing without expending any expending any extra effort. In this intercepting and reading and conversation of the message by unintended receiver take place. Mobile host in mobile ad-hoc network shares a wireless medium. Majorities of wireless communication use RF spectrum and broadcast by nature. The message transmitted can be eavesdropped and fake message can be injected into the network.

Traffic Analysis: Traffic analysis is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.

4. SECURITY ISSUE IN VANET

Among all the challenges of the VANET, security got less attention so far. VANET packets contain life critical information hence it is necessary to make sure that these packets are not inserted or modified by the attacker; likewise the liability of drivers should also be established that they inform the traffic environment correctly and within time. These security problems do not similar to the general communication network. The size of the network, mobility, geographic relevancy etc makes the implementation difficult and distinct from other network security.

Real-time Constraint: VANET is time critical where the safety-related message should be delivered with 100ms transmission delay. So to achieve real-time constraint, the fast cryptographic algorithm should be used. Message and entity authentication must be done in time.

Data Consistency Liability: In VANET even authenticate a node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency. Correlation among the received data from a different node on particular information may avoid this type of inconsistency.

Low tolerance for error: Some protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in a very short time. A small error in the probabilistic algorithm may cause harm.

Key Distribution: All the security mechanisms implemented in VANET dependent on keys. Each message is encrypted and needs to decrypt at receiver end either with the same key or a different key. Also, the different manufacturer can install keys in different ways and in public key infrastructure trust on CA become a major issue. Therefore the distribution of keys among vehicles is a major challenge in designing security protocols.

Incentives: Manufactures are interested to build applications that consumer likes most. Very few consumers will agree with a vehicle which automatically reports any traffic rule violation. Hence successful deployment of vehicular networks will require incentives for vehicle manufacturers, consumers and the government is a challenge to implement security in VANET.

High Mobility: The computational capability and energy supply in VANET is same as the wired network node but the high mobility of VANET nodes requires the less execution time of security protocols for the same throughput that wired network produces. Hence the design of security protocols must use the approaches to reduce the execution time. Two approaches can be implemented to meet this requirement

5. CONCLUSION

MANET and VANET are tremendously receptive to attacks that are due to the dynamic nature of its network field. In consideration of such types of intrusion, routing attacks have received considerable attention since it might cause the foremost devastating harm to MANET. Routing in MANET and VANET is a tedious task due to the network's continual topological changes, limited bandwidth, and power. A routing approach for a mobile ad hoc network should, therefore, shows a high degree of adaptability with respect to the very high dynamics of the network. VANET has the ability to deploy a network in a tedious situation where the classic network cannot be implemented. As VANET has a huge area of application but on the other side, there are many difficulties and challenges which must be overcome. To provide such security in different protocols, certain new techniques must be incorporated to make it more secure against various types of active and passive attacks.

6. 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 Blackhole 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 Blackhole Attack in MANET", IEEE International Conference On Recent Trends in Electronics Information Communication Technology, India, pp. 1960-1964, 2016.

© 2018, www.IJARIIT.com All Rights Reserved

[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] Mahesh Kumar, Mr. Kuldeep Bhardwaj,"Impact of the Blackhole on AODV based routing in Vehicular Ad-hoc Networks", International Journal of Wired and wireless communication, Vol 4, issue 1, Oct 2015.
[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– 22 February 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.

© 2018, www.IJARIIT.com All Rights Reserved