International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V11I3202182
Volume 11 Issue 3 July 2021

VEHICULAR ADHOC NETWORK BLACK HOLE ATTACK ANALYSIS SURVEY PAPER

Sakshi Gaur
Research Scholar,
Singhania University, Jhunjhnu
sakshigaur3793@gmail.com

Dr. Amit Sanghi
Associate Professor, CSE Department
Marudhara Engineering College, Bikaner
dr.amitsanghi@gmail.com

Abstract--- **Because of the utilisation of wireless connections, a VANET is vulnerable to malicious attacks such as Denial of Service, black hole attacks, Sybil attacks, selective forwarding, and changing routing information. Vehicular Networks, sometimes referred to as VANETs, are a special type of wireless network. It is an important component of the Intelligent Transportation System (ITS). The use of VANET technology has been shown to improve road safety and transportation efficiency. However, because VANET has significant security concerns, a reliable method of communication is required, which is a time-consuming and critical worry. In this review study, we looked into Black Hole attacks employing multiple protocols from high-quality research articles in a CBR/UDP traffic pattern. In order to access data, several methods such as active and passive attacks are possible. As we all know, VANET has a lot of problems, especially security problems. The NS-2 simulator will be used to carry out our investigation. A careful analysis of attack was also conducted because there are a large variety of attacks accessible. These attacks are separated into active and passive attacks, which are then classed further. We examine the many types of assaults and their depth in ad hoc networks in this review study.**

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

I. INTRODUCTION

MANET is a type of wireless ad-hoc network that consists of a self-configuring network of mobile routers connected by wireless connections that form an arbitrary topology when combined. The routers, which are the participating nodes that operate as routers, are free to move about and manage themselves as they see fit; as a result, the network's wireless architecture can change quickly and without warning. It is possible for such a network to function alone or to be connected to the broader Internet. A mobile ad hoc network is a collection of communication devices (mobile devices) that self-configure and adjust wireless links to construct an arbitrary topology without the usage of existing infrastructure. Simulative analysis is an important tool for understanding the performance of routing protocols in wireless network technology.

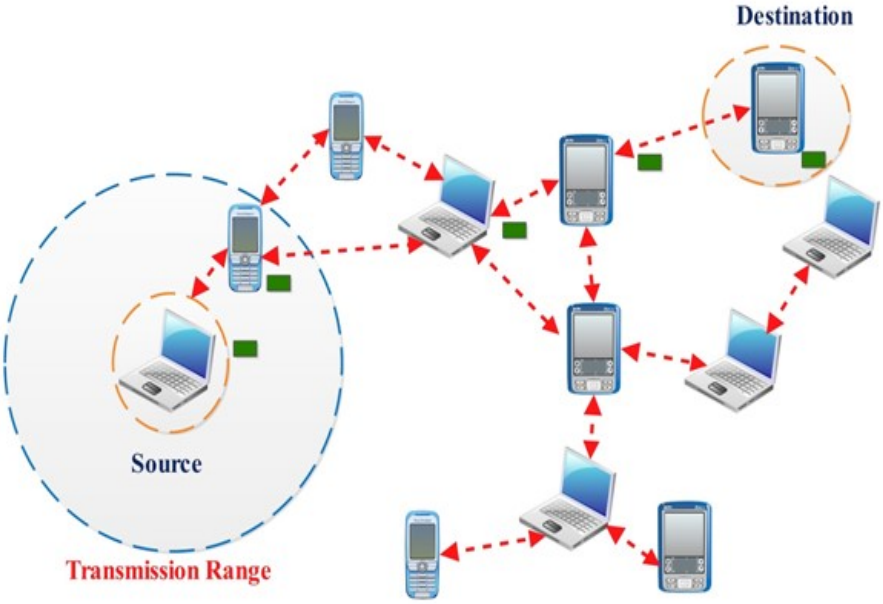

Figure 1 Overview of MANET architecture

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V11I3202182
Volume 11 Issue 3 July 2021

Several types of VANET transportation trials have been identified and handled in recent years. For VANET, a wide variety of routing protocols have been suggested. A VANET routing rule governs how two-way transmission objects exchange messages; it encompasses the process of defining a route, making a sending decision, and taking action to keep the route running or improve it in the event of a routing failure. Position-based and Topology-based protocols are two types of VANET location-based protocols. Routing methods based on topology are further separated into proactive and reactive protocols. There has already been enough study done, including a comparison of several routing protocols and their performance evaluation using various mobility models. It will be interesting to see how one of the routing protocols performs when the number of mobile nodes is changed.

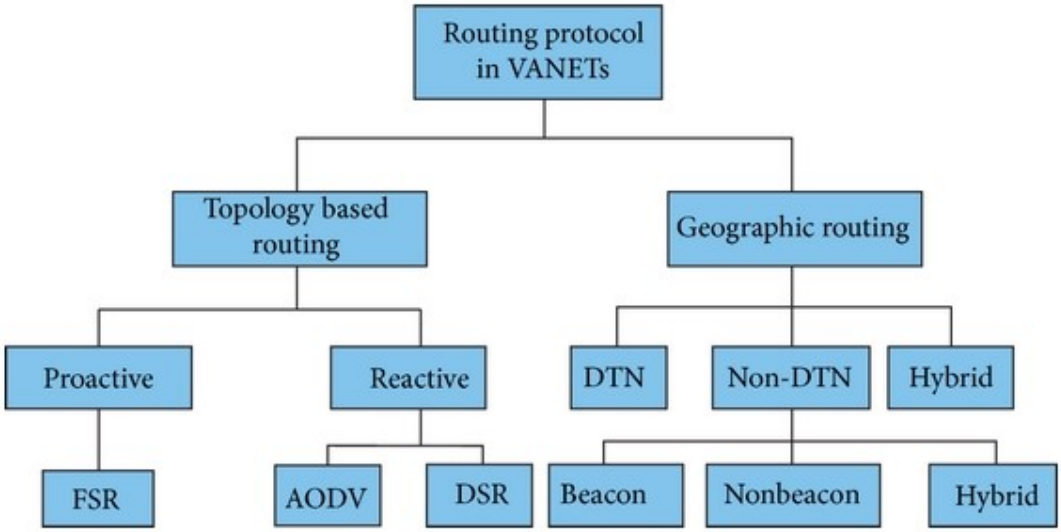

Figure 2 Routing Protocol flowchart of VANET

II. RELATED WORK

Due VANETs (Mahesh Kumar and Kuldeep Bhardwaj: VANETs) are a sort of MANET that helps equipment or vehicles communicate with one other. VANET is primarily intended to provide safety-related information to drivers, such as warnings about road conditions, accidents, and traffic management, as well as assisting drivers in finding the best possible route to their destination. VANETs have a variety of unique qualities that make them vulnerable to attackers and reduce the networks' usual performance. The most serious challenge related with the topic of computer networking is a black hole attack in which the black node consumes all of the data packets in the network. A hostile node uses its routing protocol to declare that it has a direct path to the destination node in a black hole attack. The main goal of the research is to assess the impact of a black hole attack on the AODV routing protocol on the VANET. The results of measurements of numerous parameters, as well as comparisons and analyses, are provided [7]. P.S. Anuradha and Hiremath: The Mobile adhoc networks (MANETs) networks are characterised as wireless self-configuring networks capable of operating without the assistance of any fixed infrastructure or a central coordinator, making routing a difficult operation. Designing a comprehensive security system that can defend MANET from multiple routing threats is one of the primary difficulties in MANET. MANET is susceptible to a variety of assaults, including black holes, sybill attacks, wormhole attacks, grey hole attacks, and so on. Among them, a black hole is a serious assault that has an impact on the overall network's performance depending on routing, packet delivery ratio, throughput, and packet end-to-end latency. Communication occurs when two parties exchange information, such as from-node to nexthop-node information. An adaptive strategy for detecting and preventing black hole attacks in a MANET is suggested in this study, which is based on a Data Access Table, which is an array that stores information from one node to the next. As a routing protocol, we used AODV, and NS2 as a simulator tool. In a MANET, the findings are compared to a threshold-based approach for detecting and preventing cooperative black hole attacks. In terms of throughput, packet delivery ratio, and end-to-end latency, the adaptive technique outperforms the threshold-based algorithm [9]. Surmukh and colleagues: To make driving safer in the

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V11I3202182
Volume 11 Issue 3 July 2021

future, we can use a vehicle ad hoc network. It requires effective routing protocols for vehicle communication in order to succeed. Roadside units (RSUs) or on-board units (OBUs) in the cars can be used to communicate. Various known routing protocols, such as AODV, AOMDV, DSR, and DSDV, are exploited in this article by altering vehicle velocity and evaluating their performance in terms of throughput, end-to-end latency, packet delivery ratio, and normalised routing load during communication [11]. Elias C. Eze and colleagues: Over the last several years, developments in wireless communication technologies and the auto-mobile sector have sparked a surge in research interest in the topic of VANETs. Wireless access methods such as IEEE 802.11p facilitate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications in the VANET. Through the development of Intelligent Transport Systems, this advancement in wireless communication is expected to increase road safety and traffic efficiency in the near future (ITS). As a result, the government, the automobile industry, and academia are working together on numerous active research initiatives to develop VANET standards. VANET has become a popular wireless communication sector due to the typical collection of VANET application areas, such as car collision warning and traffic information distribution. This study gives an overview of the present status of research, problems, and potentials of VANETs, as well as the path to the long-awaited ITS [12].

III. ATTACKS: ACTIVE AND PASIVE

An attacker obtains 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. When routing control messages are tunnelled, routing might be disturbed. A wormhole is a tunnel that connects two collaborating attackers. Because of broadcasting, this attack in DSR, AODV, might block the detection of any routes and potentially construct a wormhole for packets that are not addressed to themselves. Wormholes are difficult to identify since the path used to transmit data is often not part of the actual network. Wormholes are harmful because they may inflict damage to a network without even knowing about it.

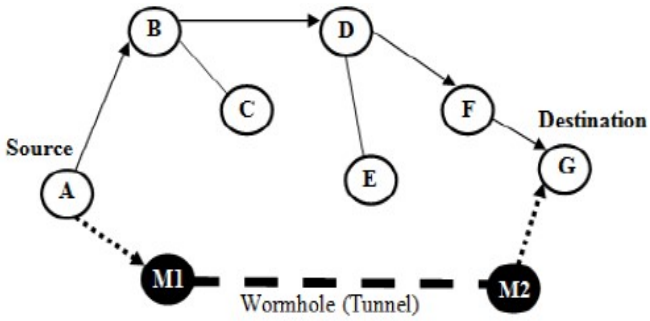

Figure 3 Wormhole attack configuration

Sybil attack: The Sybil attack targets distributed system setups in particular. Instead of acting as a single identity/node, the attacker tries to act as numerous separate identities/nodes. This enables him to falsify the outcome of a voting process utilised in threshold security systems. Because ad hoc networks rely on node-to-node communication, many systems include redundant methods to ensure that data is delivered from source to destination. As a result, adversaries will find it more difficult to compromise information integrity

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V11I3202182
Volume 11 Issue 3 July 2021

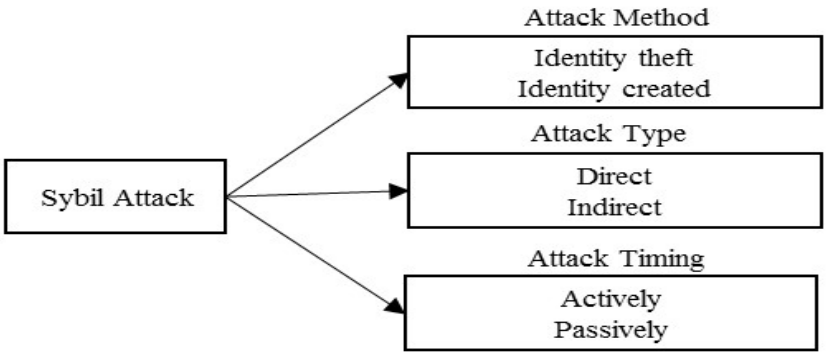

Figure 4 Sybil attack details

Gray-hole attack: Also called as routing misbehaviour attack, this attack causes messages to be dropped. There are two phases to the grey hole attack. In the first phase, nodes advertise that they have a legitimate path to their destination, whereas in the second phase, nodes with a specific probability delete captured packet.

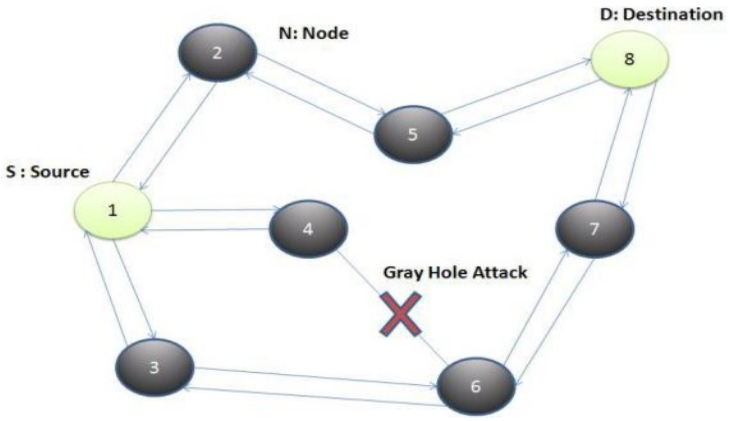

Figure 5 Gray hole attack

An attacker publishes a zero metric for all destinations in a black hole attack, leading all nodes around it to redirect packets towards it. A rogue node broadcasts fictitious routing information, claiming to have found the best path, causing other good nodes to route data packets via it. Instead than forwarding packets properly, a rogue node removes all packets it receives. In a flooding-based protocol, an attacker listens to the requests.

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V11I3202182
Volume 11 Issue 3 July 2021

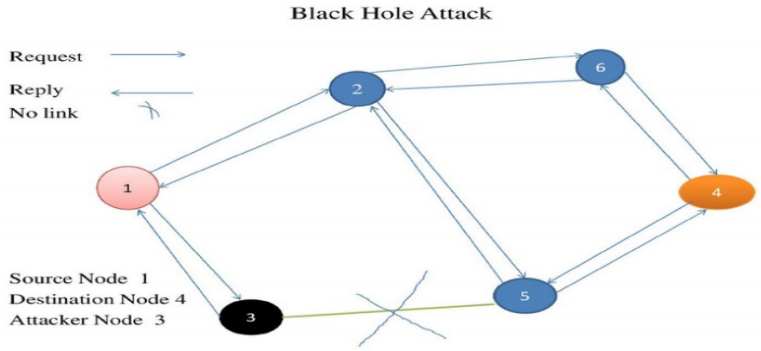

Figure 6 Black hole attack diagram

ATTACKS THAT ARE PASSIVE

Traffic Monitoring: It may be built to discover communication parties and capabilities that might be used to launch additional assaults. Other wireless networks, such as cellular, satellite, and WLAN, are also susceptible to same potential vulnerabilities.

Eavesdropping: The phrase eavesdrops refers to overhearing without putting out any additional effort. This results in the communication being intercepted, read, and conversed with by an unexpected receiver. A wireless medium is shared by mobile hosts in a mobile ad-hoc network. By nature, the majority of wireless communication uses RF spectrum and broadcasts. The transmission of messages can be intercepted, and a bogus message can be introduced into the network.

Traffic analysis is a passive attack that gathers information about which nodes connect with one another.

Traffic analysis: It is a passive attack that gathers information about which nodes connect with one another and how much data is handled.

SECURITY ISSUE IN VANET

Security has received little attention among the VANET's issues thus far. Because VANET packets carry life-essential information, it is vital to ensure that they are not inserted or manipulated by an attacker; similarly, drivers' responsibility should be defined to ensure that they accurately and timely notify the traffic environment. These security issues are not the same as those that occur in a normal communication network. The network's scale, mobility, geographic relevance, and other factors make deployment complex and different from traditional network security measures.

Real time Constraint: VANET is a time-critical network, and safety-related messages must be transmitted with a 100ms transmission delay. As a result, a fast cryptographic technique should be utilised to meet the real-time limitation. Authentication of messages and entities must be completed in a timely manner.

Data Consistency Liability: In a VANET, even authenticated nodes might engage in malevolent behaviour that can result in network disruption or accidents. As a result, a system should be created to prevent this contradiction. This sort of discrepancy may be avoided by correlating the incoming data from separate nodes on certain information.

Low error tolerance: Some protocols are built on a probabilistic foundation. VANET uses life-critical information to take actions in a very short amount of time. A little inaccuracy in a probabilistic algorithm can have serious consequences.

Key Distribution: All of the security measures in VANET rely on keys for their operation. Each communication is encrypted, and the receiver must decrypt it using the same or a different key. Furthermore, different manufacturers might install keys in various ways, making confidence in the CA a critical challenge in the public key infrastructure. As a result, distributing keys across automobiles is a significant difficulty in developing security standards.

Incentives: Manufacturers are motivated to provide apps that consumers like the best. Few people will agree that a car that automatically reports any traffic offence is a good idea. As a result, effective adoption of vehicular networks would necessitate incentives for car manufacturers, customers, and the government. Security in VANET is a difficulty to execute.

High Mobility: VANET nodes have the same processing capabilities and energy supply as wired network nodes, but their high mobility necessitates shorter security protocol execution times for the same throughput as wired networks. As a result, measures to minimise execution time must be used in the design of security protocols. To achieve this criteria, two ways can be used.

IV. CONCLUSION

Due to the dynamic nature of its network field, MANET and VANET are extremely vulnerable to assaults. Routing attacks have gotten a lot of attention in the context of such intrusions since they have the potential to do the greatest damage to MANET. Due to the network's constant topological changes, limited bandwidth, and power, routing in MANET and VANET is a time-consuming process. As a result, a routing solution for a mobile ad hoc network should be very adaptable to the network's high dynamics. VANET can deploy a network in difficult situations when a traditional network cannot be deployed. Although VANET offers a wide range of applications, it also has a number of hurdles and challenges to solve. Certain new strategies must be implemented into different protocols to guarantee such protection against various forms of active and passive assaults.

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] Mahesh Kumar, Mr. Kuldeep Bhardwaj,"Impact of Black hole 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, 21–22February 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.