Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 2, No. 4, February : 2024

THE EFFECTS OF A BLACK HOLE ON A NETWORK SYSTEM

Murlidhar Prasad Singh, Md Ehtashamoul Haque, Assistant Professor, Department of Computer Science and Engineering, B. P. Mandal College of Engineering, Madhepura, Bihar, India.
Rajiv Kumar Ranjan, Assistant Professor, Department of Computer Science and Engineering RRSDCE, BEGUSARAI, Bihar, India. Email id- rajivkr1234@gmail.com

Abstract— Due to their characteristics of continually changing topologies or a lack of infrastructure networks, wireless networks pose serious security risks. This type of network uses routing protocol to transfer data from source to destination. The majority of MANET routing protocols are open to several kinds of attacks. However, wireless ad hoc networks are vulnerable to malicious node attacks because of security flaws in the routing protocols. When a rogue node enters the MANET's wireless coverage area, it can interfere with communication. A significant security concern inside MANETs is the Black Hole Attack. One of these attacks is called "Black Hole," which compromises network integrity by entangling every data packet and causing connection failures. There will be data loss if the assault prevents the data packets from reaching the destination node.
Keywords— *MANET, Routing Protocols, Black Hole Attack, Compromises Network Integrity, Prevents Data Packets.*

INTRODUCTION

In essence, wireless networks serve as infrastructure networks, arranging communication amongst mobile nodes. Ad hoc networks are classified as infrastructural networks since they use mobile nodes instead of permanent infrastructure to connect with one another. The largest problem resulting from wireless or infrastructure is low network security. The use of wireless networks in communications networks has increased dramatically in recent years. The primary feature of wireless networks is information access regardless of a user's topological and geographic characteristics. Due to the Internet's explosive expansion in the last several years and the increasing use of tiny mobile devices as a means of communication and data sharing, wireless networks have all but collapsed. Being aware of potential attack vectors is always the first step in creating effective security solutions. Information transmission over the MANET must be secure in order for it to be done safely. Due to its shared wireless medium and lack of a central coordinating mechanism, MANET is more susceptible to assaults, and these attacks frequently target MANET. Security is the main issue in the MANET since its operation depends on the cooperation of the nodes that are a part of it. Ad hoc networks are used in many applications, particularly in the military and emergency services, where it is more difficult to meet security standards than in conventional wired networks. The fact that there is no centralized network management and that every node has designated other nodes to route its packets makes secure routing even more challenging in this situation. Therefore, the existence of any misbehaving nodes inside the network can quickly interfere with its functionality and harm its ability to communicate. As a result, safe routing is a crucial component that ad hoc networks must have in order to successfully commercialize and sustain secure applications. Thus, establishing secure routes by reducing the likelihood of abuse detection in MANETs is a crucial area of study. A crucial element of mobile ad-hoc networks is security. More secure wireless networks are becoming necessary as wireless technology gains popularity and is used more often. Particularly susceptible to a potent assault called the black hole attack are wireless networks. The networking field's most popular study topics these days are wireless networks. The most practical and likely method of internet communication is through wireless networks. There are two types of wireless networks: ad hoc networks and infrastructure networks.

LITERATURE REVIEW

A denial-of-service attack similar to a black hole attack was reported by Md Ibrahim Talukdar et al. against a general-purpose ad hoc on-demand distance vector protocol. It employs three methods: identified black hole AODV, regular AODV, and black hole AODV, where we find that black holes severely impair network performance. Using two methods an intrusion detection system (IDS) and an encryption technique (digital signature) with the preventive concept we have identified the black hole assaults within the networks.

In order to combat black hole attacks, Muhammad Salman Pathan et al. proposed an efficient and straightforward technique that improves the AODV routing protocol. Fake route request (RREQ) packets with an erroneous destination address are used by the MDBM mechanism to detect black hole attacks in order to identify black hole nodes before the true routing process begins. A simulation experiment has been done to confirm the effectiveness of the suggested detection and prevention plan.

The impact of a black hole assault on the network was presented by Layth A. Khalil A et al. To do this, we created a simulation of MANET circumstances, which included a black hole node that used the OMNET ++ simulator to show the impacts of a black hole assault. Several black hole attacks on the network's MANET performance have also been studied.

Using the AODV routing protocol, Pranjul Sarathe et al. provided an overview of several approaches and strategies for identifying and thwarting black hole attacks in MANETs. A significant security concern inside MANETs is the black hole attack. This happens when a black hole a malevolent node joins the network. This node acts as though it is the route to the destination during the route discovery process. It gathers all of the packets and leaves them there rather than forwarding them to the intended destination.

The black hole detection method in MANET using AODV and its prevention using AOMDV was described by Lokesh Baghel et al. Many routing protocols have been suggested, and AODV has been used in the implementation of the majority of them. In it, we use AOMDV to assess black hole attacks and compare each one's parameters with the results of AODV one at a time.

One of the well-known security risks for MANETs is the black hole attack, as explored by Taku Noguchi et al. A security attack known as a "black hole" occurs when a hostile node sends fictitious routing information, absorbing all data packets and leaving them unforwarded. Our proposal in this research is to avoid black hole attacks using a strategy based on at a fresh cutoff.

A comparative assessment and survey of sets of multipath routing protocols for mobile ad hoc networks was published by Tariq A. et al. in their paper On-demand Multipath Routing Protocols for Mobile Ad-Hoc Networks: A Comparative assessment. The results of this study will drive the development of new multipath routing techniques that address the issues this article has pointed out.

AODV PROTOCOL'S BLACK HOLE ATTACKS

All of the network's stations have their routing information managed using proactive table-driven protocols. Every station creates a unique routing table that may be used to find a way to a location and store data routing. The whole network must be updated if there is a change to the network topology. The Destination Sequenced Distance Vector Routing (DSDV), Optimised Link State Routing (OLSR), Wireless Routing Protocol (WRP), Cluster Gateway Switch Routing Protocol (CGSR), and Fish Eye State Routing Protocol (FSR) are a few of the table-driven protocols. Routing protocols that are On-demand or Reactive elaborate routes as needed. A node uses the route discovery technique to find the path to the target station before attempting to transfer data to any other station. Numerous on-demand driven protocols have been developed, including Ad hoc On Demand Distance Vector (AODV), Associativity Based Routing (ABR), Temporally Ordered Routing Algorithm (TORA), and Dynamic Source Routing Protocol (DSR). Routing protocols that are hybrid use both of the earlier kinds. Zone-based hierarchical link state (ZHLS), distributed

dynamic routing (DDR), and zone routing protocol (ZRP) are a few examples of hybrid routing protocols. The focus of this work is to analyse how black hole attacks affect MANETs that use AODV. The reactive routing technique known as AODV (Ad hoc On-Demand Distance Vector) is made up of two modules:

(i) Route Discovery Module- The source station S checks its routing database in order to transfer data to a specific station D. It uses this station D if it finds an entry there; if not, it starts the route discovery process (see Fig. 1), which entails the source station S flooding neighbouring stations with a route request (RREQ) packet. In order to find a new route (if the route sequence number is greater than that of RREQ) to the required destination in the RREQ packet, the intermediate station that the RREQ packet acquired last searches its routing table. A route reply (RREP) packet is sent via the pre-planned reverse route to the source station S if such a path is discovered. The intermediate station updates its routing table and sends RREQ to the neighbours if it is unable to locate a new route. Until RREQ is received by destination node D, this process is repeated. The pre-established reverse route is used by the destination node D to broadcast RREP to S.

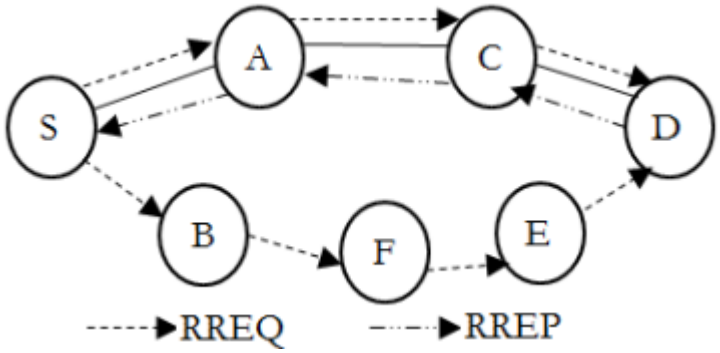

Figure 1- Route discovery mechanism of AODV protocol

(ii) Route Maintenance Module- Greeting messages are used by AODV to keep nodes connected. On behalf of the neighbours, each station waits for hello packages and sends them out on a regular basis. In the event that there is no connection interruption, a symmetrical link between stations is always maintained while Hello packets are sent in both directions. A route error (RERR) packet is transmitted to the source S if the station upstream is unable to fix the damaged link locally. This final step might restart the route finding process if needed. Multiple assaults can target MANETs. The threats against the most important layers of the network, physical layer, and MAC are known as general attack types. The two main objectives of network layer attacks are to either alter some of the properties of routing packets or prevent data packets from being sent. An adversary node can launch a simple assault by ceasing to transmit data packets. Consequently, the attacker station prevents the data exchange from occurring when it is selected as a route. A MANET that uses the AODV, a black hole station, suppresses network traffic by pretending to have enough new routes to all of the destinations that each station needs. The black hole station instantly answers that it is coming from the destination or from a station that has a sufficiently recent path to reach the destination station when a source station floods the RREQ packet for any destination node. In Fig. 2, a destination station D in MANETs is to receive information packets from source station S. Node M functions as a black hole node and is an attacker node. With a bogus reply RREP with a higher modified sequence number, the malicious node responds. Therefore, informational meals should be communicated from S to M rather than D.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 2, No. 4, February : 2024

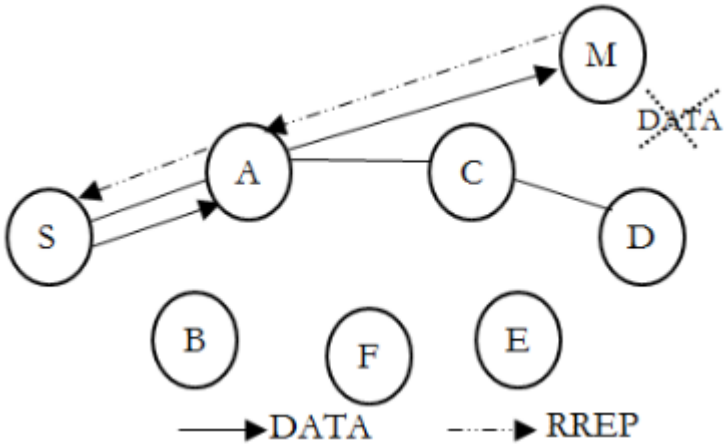

Figure 2- Black hole attack process

NETWORK SIMULATOR

Developed at the University of California, Berkley, NS is an event-driven network simulator programme that incorporates a variety of network objects, including applications, protocols, and traffic source behaviour. The NS is a component of the VINT project's software, which has received DARPA funding since 1995.

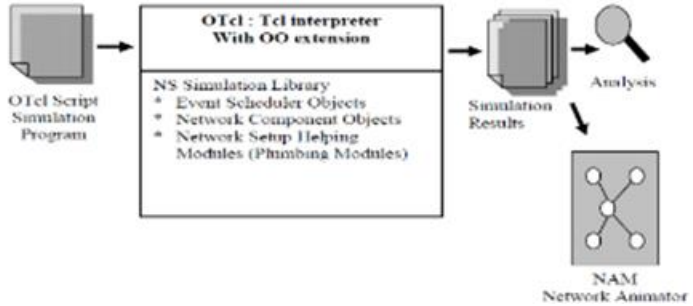

Figure 3-Network Simulator Architecture

The NSCL 2's use of the OTCL script interpreter is seen in Figure 3. Network objects and the network topology are configured using functions in the library, which notify the sources of starting and stopping packet transmission traffic through the event planner. To configure and run a simulation network, a user must write an OTCL script to start an event programme. NS interprets an OTCL script that a user has written. NS concurrently produces two primary analysis reports. One of these is called "network animator" object, and it displays the simulation's visual animation. Every object in the simulation acts according to the second trace. NS is the one who generated both of these files. This uses the GAWK script to retrieve data from the trace file in order to run several performance matrices. The performance matrix is also used to detect network behaviour.

(i) Advantages- A wide variety of protocols is supported by NS-2 at all tiers. For instance, NS-2 provides the ad-hoc and wireless network-specific protocols. The NS-2 open source model reduces simulation costs, and users may readily edit and update the programmes with the help of online documentation. Because it is written in C++, it can run on any machine that has the GNU C-compiler, gcc.

(ii) Limitations- Users of this simulator must be conversant with modelling techniques and developing scripting languages, as the Tool Command Languages can be challenging to comprehend and create. NS-2 can occasionally need more effort and time to mimic a particular job than other simulators. NS-2's graphical support is inadequate, and it lacks a Graphical User Interface, forcing users to interact with electrical devices through text instructions. Owing to the ongoing modifications made to the code base, the outcome might not be consistent and might include errors. NS-2 is unable to replicate issues related to bandwidth, power consumption, or energy conservation in wireless networks. There is a scalability issue with NS-2 in that it cannot have more nodes than 100.

(iii) Experimental Setup- the structure of network source or scenario file, and these files generated using which command have shown in below: Following files have been used for simulation.

(a) Traffic Pattern File- Ns cbrgen.tcl [-type cbr|tcp] [-nn nodes] [-seed seed] [-mc connections] [-rate rate]

(b) Scenario File - To generate the traffic movement file, following is example command.

./setdest -n <num_of_nodes> -p <pause_time> -s <maxspeed>-t <simtime> -x <maxx> -y <maxy> > < scenario file>

Here n – no. of nodes, p – pause time, s – speed, t – simulation time, and x, y – grid size.

CONCLUSION

In the theoretical portion of the research, it is evident to us that routing becomes a complicated problem because of the random mobility of the nodes. In MANET, several routing protocols are still in use. Every routing protocol has its own characteristics. We must select the appropriate routing protocol based on network environments. One type of DOS attack that can significantly impair MANET performance is the black-hole attack. To avoid network failures, it is crucial to detect black hole nodes in their early phases. As a result, the authors created a method for identifying and controlling various black hole attack types in MANET. He improved the AODV scheme to prevent attacks and connection breakdowns, boost packet reception ratios, and use a multipath technique for better outcomes when compared to the current AODV and black hole attack. The system performs better as a result of this. To address the shortcomings in the major accomplishments of low latency and high packet delivery friction, we have put out our own plan. It is determined that the suggested strategy outperforms the current plan. In the future, we plan to deploy multipath scheme for both detection and prevention of black hole attacks in wireless environments.

REFERENCES

[1] Tamilselvan, L.; and Sankaranarayanan, V. (2007). Prevention of blackhole attack in MANET. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications. AusWireless, 21-21.

[2] . Perkins, E. B. Royer, and S. Das, “Ad hoc on-demand distance vector (aodv) routing,” RFC: 3561, Nokia Research Center, 2003

[3] D. B. Johnson, D. A. Maltz, Y.C. Hu, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)”, IETF Draft, April 2003, work in progress. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt

[4] Mahmood, R.A., Khan, A.I.: A Survey on Detecting Black Hole Attack in AODVbased Mobile Ad Hoc Networks. In: International Symposium on High Capacity Optical Networks and Enabling Technologies (2007)

[5] http://www.isi.edu/nsnam/ns/.

[6] M. Abolhasan, T. Wysocki, E. Dutkiewicz, — A Review of Routing Protocols for Mobile Ad-Hoc Networks, Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.

[7] N.H.Mistry, D.C.Jinwals, M.A.Zaveri;” Prevention of Blackhole Attack in MANETs”. In Proceedings of EPWIE- 2009, Gujarat, India, pp 89-94, July 2009.

[8] http://www.isi.edu/nsnam/nam/.

[9] Ming-Yang Su and Kun-Lin Chiang, “Wei-Cheng Liao. Mitigation of Black Hole Nodes in Mobile Ad Hoc Networks” In: Proceedings of IEEE International Symposium on Parallel and Distributed Processing with Applications, 2010, Page:162-167.

[10] N.Jaisankar and R.Saravanan “An Extended AODV Protocol for Multipath Routing in MANETs” IACSIT International Journal of Engineering and Technology, Vol.2, No.4, August 2010 page: 394-400.

[11] Subhashis Banerjee and Koushik Majumder "A Survey of Blackhole Attacks and Countermeasures in Wireless Mobile Ad-hoc Networks" Springer-Verlag Berlin Heidelberg, SNDS 2012, CCIS 335, Page: 396–407.
[12] Nilima H Masulkar and Archana A Nikose "An Improved Multipath AODV Protocol Based On Minimum Interference"International Conference on Advances in Engineering & Technology – 2014.
[13] Swarnali Hazra and S.K. Setua "Black hole Attack Defending Trusted On Demand Routing in Ad-Hoc Network" Advanced Computing, Networking and Informatics – Volume 2, Smart Innovation, Systems and Technologies 28, Springer International Publishing Switzerland 2014 Page:59-63.
[14] Vimal Kumar and Rakesh Kumar "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network" International Conference on Intelligent Computing, Communication & Convergence Procedia Computer Science, Elsevier, 2015, Page: 472 – 479.
[15] Xiaoxia Qi1, Qijin Wang and Fan Jiang "Multi-path Routing Improved Protocol in AODV Based on Nodes Energy" International Journal of Future Generation Communication and Networking Vol. 8, No. 1 (2015).
[16] Vipul Maheshwari and Shrikant Jadhav "Survey on MANET Routing Protocol and Multipath Extension in AODV" International Journal of Applied Information Systems (IJAIS)– ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 2– No.4, May 2012.
[17] Versha Matre and Reena karandikar "A Literature Review of Reliable Multipath Routing Techniques" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 3 March 2015, Page No. 10599-10602.
[18] Nisha P John, Ashly Thomas** " Prevention and Detection of Black Hole Attack in AODV based Mobile Ad- hoc Networks - A Review" International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012 PP 1-6.
[19] Tariq A. Murshedi, Xingwei Wang, and Hui Cheng "On- demand Multipath Routing Protocols for Mobile Ad-Hoc Networks: A Comparative Survey" International Journal of Future Computer and Communication, Vol. 5, No. 3, June 2016 PP:148-158.
[20] Taku Noguchi and Takaya Yamamoto "Black Hole Attack Prevention Method Using Dynamic Threshold in Mobile Ad Hoc Networks" Computer Science and Information Systems ACSIS, Vol. 11, 2017 Page: 797–802.
[21] Lokesh Baghel, Prakash Mishra, Makrand Samvatsar and Upendra Singh "Detection of Black hole Attack in Mobile Ad hoc Network using Adaptive Approach" International Conference on Electronics, Communication and Aerospace Technology ICECA 2017 978-1-5090-5686.
[22] Pranjul Sarathe and Neeraj Shrivastava "A Review on Different Methods to Prevent Black Hole Attack in MANET" International Journal of Computer Sciences and Engineering Vol.-6, Issue-6, June 2018,Page: 1149-1156.
[23] Noguchi, Taku, and Mayuko Hayakawa. "Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks."IEEE International Conference On Trust, Security And Privacy In Computing And Communications 2018, Page: 539-544.