IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Literature Review of Detection and Prevention of Black Hole Attack in Mobile ad-hoc Network

[1]Jagrati Chaturvedi, [2] Ramnaresh Sharma,

Research Scholar, Computer Science & Engineering Dept,MPCT Gwalior

Professors, Computer Science & Engineering Dept,MPCT Gwalior

Abstract: This a survey paper, In wireless network, Security it's a major issue due to their features of dynamically changing topologies or lack of infrastructure network. In this kind of network transmit the data for source to destination using routing protocol. Most of the routing protocols for MANETs are vulnerable various types of attacks. However, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. A malicious node can get within the wireless range of the nodes in the MANET and can disrupt the communication process. One of the major security issues in MANET is Black hole attack. Black Hole is one of these attacks, which Attack against network integrity engrossing all data packets in the network and create link break problem. Where the data packets are do not reach the destination node on account of this attack, data loss will occur. In the study many techniques were introduced by researchers to find the attacks in the MANETs.

Keywords: MANET, AODV, security Attack, multipath AODV Performance Metrics, NS-2.

I INTRODUCTION

Wireless networks are basically infrastructural networks, which are responsible for coordinating communication between mobile nodes. Ad hoc networks fall under the category of infrastructural networks, where mobile nodes communicate between each other with no fixed infrastructure. Low network security is the biggest issue due to wireless or infrastructure.

Currently wireless networks have grown significantly in the field of telecommunication networks. Wireless networks have the main characteristic of providing access of information without considering the geographical and the topological attributes of a user. Over the past few years, the wireless network has almost exploded due to the rapid development of the Internet, and also the growth of small mobile devices as an instrument of communication and data exchange.

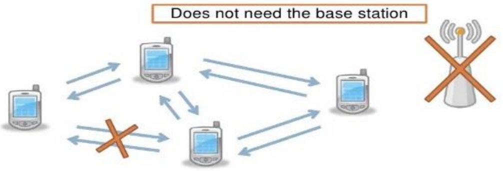

Figure 1 General wireless ad hoc networks.

Understanding the possible form of attacks is always the first step towards developing good security solutions. Security of communication in the MANET is important for safe transmission of information. The absence of any central coordination mechanism and shared wireless medium makes MANET more vulnerable to attacks, with many attacks affecting MANET. Since the functioning of the MANET requires cooperation from the nodes participating in the network, security is a primary concern in the MANET. Many applications, especially military and emergency rescue, are based on ad hoc networks, where implementing security requirements are harder than in traditional wired networks.

Secure routing is also difficult here due to the absence of centralized administration in the network and each node has specified other nodes to route their packets. So the presence of any misbehaving nodes in the network can easily disrupt the operation of the network, damaging communication within the network. Thus, secure routing is an important aspect that has to be incorporated with ad hoc networks for successful commercialization of such networks, and to support secure applications. Therefore, providing safe pathways through the mitigation of abuse detection in MANETs is an important and important research topic. Security is an essential component for mobile ad-hoc networks.

The increasing popularity and usage of wireless technology is creating a need for more secure wireless networks. Wireless networks are particularly vulnerable to a powerful attack known as the black hole attack. This project researched and developed a new protocol that prevents this kind of attacks on a wireless network. Wireless networks have become the most prevalent areas of research in the networking. Wireless networks are the most convenient and probable solution of communication over the internet. Wireless

Networks are categorized as Infrastructure Networks and Ad-Hoc Networks.

The rest of the paper begins in Section II, III and section IV Review of research Papers, AODV, multipath AODV, network simulator and last;y discussed about conclusion and References.

II REVIEW OF RESEARCH PAPERS

In this section gives a overview of previous research papers below:

Md Ibrahim Talukdar et. al. [26] presented a denial-of service attacks like black hole attacks on general-purpose ad hoc on-demand distance vector protocol. It uses three approaches: normal AODV, black hole AODV, and detected black hole AODV, wherein we observe that black holes acutely degrade the performance of networks. We have detected the black hole attacks within the networks using two techniques: (1) intrusion detection system (IDS) and (2) encryption technique (digital signature) with the concept of prevention.

Muhammad Salman Pathan et. al. [25] presented the AODV routing protocol is improved by incorporating an efficient and simple mechanism to mitigate black hole attacks. Mechanism to detect black hole attacks from MANET (MDBM) uses fake route request (RREQ) packets with an unreal destination address in order to detect black hole nodes prior to the actual routing process. Simulation experiment conducted has verified the performance of the proposed detection and prevention scheme

Layth A. Khalil A et. al. [24] presented the impact of black hole attack on the network. To accomplish this, we mimicked MANET conditions, including a black hole node using the OMNET ++ simulator to demonstrate the effects of a black hole attack, and several black hole attacks on the MANET performance of the network has investigated.

Pranjul Sarathe et. al. [22] presented a surveyed of some techniques and methodologies for detecting and preventing black hole attack in MANET using the AODV routing protocol. One of the major security issues in MANET is the black hole attack. This occurs when a malicious node referred to as a black hole joins the network. During the process of route discovery, this node acts as if it is the route to the destination and takes all the packets into it and does not forward it to the desired destination, instead it leaves all the packets.

Lokesh Baghel et. al. [21] presented the black hole detection approach in MANET using AODV using AODV and its prevention using AOMDV. Various types of routing protocols have been proposed and most of them have been implemented using AODV. In it we analyse black hole attack using AOMDV and compare their parameters one by one with the output of AODV.

Taku Noguchi et. al. [20] discussed that black hole attack is one of the well-known security threats for MANETs. A black hole is a security attack in which a malicious node absorbs all data packets by sending fake routing information and leaves them without being forwarded. To protect against a black hole attack, in this paper we propose a black hole attack prevention method based on a new threshold.

Tariq A et. al. [19] presented a On-demand Multipath Routing Protocols for Mobile Ad-Hoc Networks: A Comparative Survey, this paper Author to provide a survey and compare sets of multipath routing protocols for mobile ad-hoc networks. This survey will motivate the design of new multipath routing protocols, which overcome the weaknesses identified in this paper.

Nisha P John et. al. [18] In this research paper, an ad-hoc network is a collection of mobile nodes that dynamically form a temporary network and are infrastructure less. Networks are protected using many firewalls and encryption software's. But many of them are not sufficient and effective due to its limited power and mobility. The ultimate goal of the security solutions for wireless networks is to provide security services, such as authentication, confidentiality, in- terrify, anonymity, and availability, to mobile users. Black hole attack is one of the severe security threats in ad-hoc networks which can be easily employed by exploiting vulnerability of on- demand routing protocols such as Ad-Hoc On-Demand distance vector.

Versha Matre et. al. [17] This paper introduces a reliable on-demand routing approach to protect the black hole attacker, which relies on models with varying levels of trust dependent on our computer. In our approach, black hole attackers are identified and isolated in the context of data forwarding. Simulation and analysis justify our proposal against black hole attack for on-demand routing in ad-hoc networks. The simulation result analyzes and justifies our reliable proposal against black hole attack for on-demand routing in ad-hoc networks.

Vipul Maheshwari et. al. [16] presented a Survey on MANET Routing Protocol and Multipath Extension in AODV, in this paper Author focuses on Ad-hoc on demand Multi-Path Distance Vector routing challenging AODV in performance. In this synopsis, we propose to enhance the Ad hoc On-demand Multipath Distance Vector routing protocol for MANETs to a delay-aware multi-path protocol. The focus area is to improve the QoS in MANETs by creating a protocol, which considers delay requests of real-time multimedia applications (voice and video) in making routing decisions.

Xiaoxia Qi et. al. [15] In this paper main focus on energy-constrained of Ad Hoc network; this is a multi-path routing protocol In AODV that based on nodes energy. EM-AODV designs methods of obtaining nodes energy by upgrading the route discovery and route maintenance process of AODV, in this work calculates the path of comprehensive energy derived path priority by routes total hops and nodes energy to format the multi-path routing mechanism. The energy as the metric prerequisite during the routing process, by setting nodes energy bound and balancing nodes data forwarding to postpone network lifetime.

Vimal Kumar et. al. [14] presents a more efficient solution for detecting a black hole attack in MANET with lower communication costs, which is particularly weak compared to infrastructure-based networks due to its mobility and shared broadcast nature. It can be seen that the proposed work is more secure than existing solutions. We have compared its performance to the standard AODV routing protocol. The experimental results suggest that the proposed approach is superior to the standard AODV.

Swarnali Hazra et. al. [13] presented a Literature Review of Reliable Multipath Routing Techniques, in this paper Author present the review of previous one approach, nowadays the demand of network is increasing rapidly. The ever increasing usage of such network requirements additionally demands fast recovery from network failures. Multipath routing is one in all the most promising routing schemes to accommodate the various needs of the network. It has basic features like load balancing and improved bandwidth. Author Cho et al. introduced a reliable multipath routing scheme known as directed acyclic graphs. The property of directed acyclic graph is that they allow multipath routing with all possible edges whereas ensuring secured recovery from single point of failures. We have used the concept of DAG in our proposed method.

Nilima H Masulkar et. al. [12] In this paper discussed about frequent link failures problem in the MANET due to the mobility of the node and the use of unreliable wireless channels. The main goal of the proposal method is to determine all node-disjoint routes from source to destination with minimal routing overhead. When the route is broken, the data is continuously transmitted through another route. Also, in selecting the node disjoint path; The protocol also takes into account the energy and distance of the intermediate node en route to extend the network over the lifetime.

Subhashis Banerjee et. al. [11] In this paper reviewed black hole and co-operative black hole attacks in mobile ad-hoc networks. An attempt has also been made to fully analyse various existing schemes against black hole attacks and find out their advantages and disadvantages.

N.Jaisankar et. al. [10] This paper uses the extended multidimensional AODV scheme. The proposed multipath routing scheme provides improved performance and scalability by computing multiple routes in a single route search. Also, it reduces routing overhead by using secondary paths. This scheme computes a combination of node-disjoint paths and fail-safe paths for multiple routes and provides all intermediate nodes of the primary path with multiple routes to the destination.

Outcome of Literature Survey: From literature review, it is learned that MANETs are one of the most important future technologies in the area of computer networks. MANETs often suffer from security attacks because of their specification such as open medium, dynamic topology, lack of central monitoring and management, cooperative algorithms and unclear defence mechanism. The main issues of our work path break due to dynamic topology, random mobility models and various types of security issues. After going through the literature, we have found the multipath strategy, and this concept used our work for elimination of black hole attack.

III AODV ROUTING

In November 2001 the MANET Working Group for routing of the IEFT community has published the first version of the AODV Routing Protocol. AODV belongs to the class of Distance Vector Routing Protocols. In a DV every node knows its neighbors and the costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbors periodically its whole routing table. So they can check if there is a useful route to another node using this neighbor as next hop. When a link breaks a Count-To- Infinity could happen. AODV is an 'on demand routing protocol' with small delay. That means that routes are only established when needed [3, 25, and 31].

AODV is a reactive routing protocol used to find a route between a source and a destination, and allows mobile nodes to obtain new routes for new destinations in order to establish an ad hoc network. In this order several messages are exchanged, different types of link are established, and many information can be shared between the participant's nodes. In AODV protocol we find hello message and three others significant type of messages, route request RREQ, route reply RREP and route error RERR. The Hello messages are used to monitor and detect links to neighbors, every node send periodically a broadcast to neighbors advertising it existent ,if a node fails to receive an hello message from neighbor a link down is declared. In order to communicate every node must create routes to the destinations, to achieve that the source node send a request message RREQ to collect information about the route state; if the source receives the RREP message the route up is declared and data can be sent and if many RREP are received by the source the shortest route will be chosen. Any nodes have a routing table so if a route is not used for some period of time the node drop the route from its routing table and if data is sent and a the route down is detected another message (Route Error RERR) will be sent to the source to inform that data not received.

III PROBLEM STATEMENT

Due Wireless mobile networks without fixed infrastructure consist of mobile hosts that move randomly in and out of each other communication range resulting in Authors have addressed the problem of link stability to a network topology where the nodes can move continuously mobility, leading to frequent route changes, link break problem occur. These link problem faces due to kind of security issues or attacks like as black hole attack. I have study the literature review and find that most of routing protocols are find the route from source node to destination node and send packet via single path. Most of the quality routing protocols are Single path and Single constrained. Wireless Ad Hoc on demand routing currently an area of research among most of the networking community.

MOTIVATION: This work inspires us to build an attack-free network. Because MANET is often associated with security issues such as open media, dynamically changing its topology, lack of central monitoring and management, cooperative algorithms and no clear defence mechanisms. This causes a lot of data loss and we have tried to solve this problem in work.

IV HOW BLACK HOLE WORKS

In this section black hole attack is discussed in detail and how it affects the network. In this attack, a black hole node tries to send a fake RREP for a route request, being the shortest route to the destination. These false RREPs deceive the source to divert network traffic toward the black hole node for eavesdropping or absorbed traffic to discard data packets.

There are two stages of black hole attack. In the first phase, the malicious node uses an ad node routing protocol such as AODV to advertise as a valid route to the destination node. Even if the route is suspicious, intended to interrupt the packet. In the second stage, the attacker node drops the intercepted packet without forwarding it. A more subtle form of this attack occurs when an attacker node suppresses or modifies packets originating from certain nodes, while leaving data packets unaffected from other nodes. This makes it difficult for other nodes to detect malicious nodes. In this work, however, a defense mechanism against a collaborative black hole attack in AOD is proposed that relies on the AODV routing protocol.

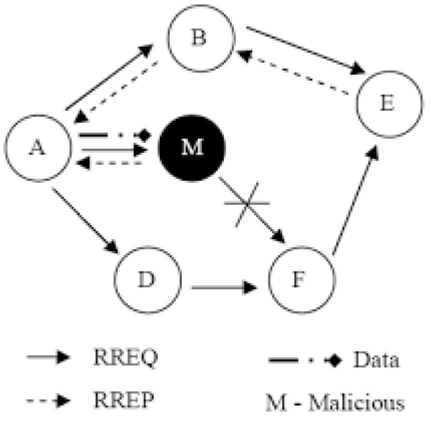

Figure: 1 black hole attack link break

Among black hole attacks is that malicious nodes do not initially send actual control messages. For a black hole attack, the malicious node waits for the neighbouring node to send the RREQ message. When a malicious node receives an RREQ message, without checking its routing table, immediately sends an incorrect RREP message that routes to the destination, a higher serial number for the victim node to settle in the routing table Specifies, do not correct before sending to your node. Therefore requesting the nodes assumes that the route discovery process is complete and ignores other RREP messages and starts sending packets to the malicious node. The malicious node attacks all RREQ messages in this way and occupies all routes. Therefore all packets are sent at a point when they are not forwarding anywhere. This is called a black hole attack.

The malicious node messages the wrong RREP message as if it comes from another victim node instead of itself; all messages will be sent to the victim node. By doing this, the victim node intercepts all incoming messages. This causes the attack link brake problem as shown in the figure above. Black hole attack affects the entire network. This degrades the performance of the network. Problems such as packet loss and delay increase. After launching a black hole attack, the attacker has unauthorized access to the given network. Following are the symptoms that can be seen in the network due to black hole:

- Decrease in Network utility.
- Increase the Traffic Load.
- Increase the Packet Loss.
- Increase Delay.

V MULTI PATH AODV

In this work, Multipath AODV or Modified AODV: Multiple root discovery procedures are used in this scheme, by which multiple routes are discovered. Continuous route breakdown causes intermediate nodes to fall packets because there is no alternate route available to the destination. Therefore, this scheme provides an alternative route for data transfer.

Modification in Ad hoc on demand distance vector routing Source Code

We have modified the code below to correct the black hole attack:

- In AODV main file should change "finding route to the destination" to "finding multiple routes" to the destination.
- The receive request method should be modified to receive the RREQ with the same ID as previous one in order to create the multiple reverse routes. The receive reply method should be modified to accept the multiple route reply to create the multiple forward routes.
- The receive reply method should be modified to forward RREP packet to every reverse route. The receive error method should be modified to check if the node still has another active route to the destination. If the node still has another active route to the destination, the node no needs to forward the RERR packet. Route resolve method for source node should be set to switch from one active path to another active path and switch back in next transmission.
- The set of the route selector counter should be added for every node in case of one source may have to transmit to more than one destination. The route selector counter is for the source node to switch from the best route to the second route in the next transmission and switch back in the Next

NETWORK SIMULATOR

NS is an event driven network simulator program, developed at the University of California Berkley, which includes many network objects such as protocols, applications and traffic source behavior. The NS is a part of software of the VINT project [15] that is supported by DARPA since 1995.

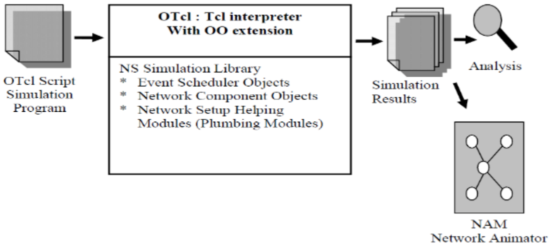

Figure-2 Network Simulator Architecture

Figure 2 illustrates how the NSCL 2 functions using the OTCL script interpreter. To configure and run a simulation network, a user must write an OTCL script to initiate an event program; network objects and the network topology are configured using its functions in the library, which informs the sources of starting and stopping packet transmission traffic through the event planner. The OTCL script written by a user is interpreted by NS. NS creates two main analysis reports simultaneously. One of them is named (network animator) object which shows the visual animation of the simulation. The second trace is the object in which all objects in the simulation behave. Both of these have been created as files by NS. This extracts data from the trace file with the help of GAWK script to perform various performance matrices. And with the help of the performance matrix, network behavior is detected.

Advantages

- NS-2 can support a significant range of protocols in all layers. For ex., the ad-hoc and Wireless network specific protocols are delivered by NS-2.
- Open source model of NS-2 saves the cost of simulation, and online documents allow the users easily to modify and improve the codes.
- It can run on any system having GNU C-compiler gcc as it is written in C++.

Limitations

- People who want to use this simulator need to familiar with writing scripting language and modeling technique, the Tool Command Languages somewhat difficult to understand and write.
- NS-2 is sometimes more complex and time-consuming than other simulators to model a desired job.
- NS-2 provides a poor graphical support, no Graphical User Interface; the users have to directly face to text commands of the electronic devices.
- Due to the continuing changing the code base, the result may not be consistent, and contains bugs.
- NS-2 cannot simulate problems of the bandwidth, power consumption or energy saving in wireless network. NS-2 has a scalability problem number of nodes cannot be exceeded to 100.

Experimental Setup: This section gives 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.

Traffic Pattern File:

```
Ns cbrgen.tcl [-type cbr|tcp] [-nn nodes] [-seed seed] [-mc connections] [-rate rate]
```

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.

Transmission.

IX CONCLUSION

Our report contains two parts: one is theoretical study and other is simulation base study. In theoretical part of study, it is clear to us that due to the random mobility of node, routing becomes a complex issue. Till now many routing protocols are used in MANET. Each routing protocol has unique features. Based on network environments, we have to choose the suitable routing protocol. Black-hole attack is included in the category of DOS attacks that can seriously harm the performance of MANETs. Detection of black hole node during early stages is of much importance in order to prevent the network failures. Accordingly, the authors developed a scheme for detecting and managing different kind of black hole attacks in MANET. The modified AODV scheme to avoiding attack or link break problem, and increase the packet receiving ratio and multipath approach better results compare existing AODV with black hole Attack. This gives a better result for the system. We have proposed our scheme to overcome the deficiencies found in the Major achievements of high packet delivery friction and low delay. It is concluded that the proposed approach provides better results than the existing scheme.

In future we have implemented black hole attack in Wireless environment and prevention and detection using multipath Scheme/

REFERENCES

[1] Elizabeth M. Royer, and Chai Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, April 1999, Page: 46-55.

[2] L. Wang, Y. Shu, M. Dong, L. Zhang and O. Yang, "Adaptive Multipath Source Routing in Ad hoc Networks", IEEE ICC 2001, vol.3, June 2001, Page: 867-871.

[3] Amitabh, M. and Ketan, M.N. "Security in wireless Ad hoc networks", The handbook of ad hoc wireless networks, CRC press, 2003 Page: 499-549.

[4] N. Jaisankar, N. Saravanan, and K. D. Swamy, "A Novel Security Approach for Detecting Black Hole Attack in MANET", Proc. Business Administration and Information Processing Heidelberg, 2010, Page: 217-223.

[5] V. Palanisamy, P. Annadurai and S. Vijayalakshmi, "Impact of black hole attack on multicast in ad hoc network", Computational Intelligence and Computing Research, 2010 IEEE International Conference on 28-29 Dec. 2010.

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

[7] S. Jain, M. Jain and H. Kandwal "Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks" J. Computer Applications, vol. 1, 2010 Page: 37-42.

[8] Ajay Jangra, Nitin Goel, Priyanka and Komal, "Security Aspects in Mobile Ad Hoc Network (MANETs): A Big Picture" International Journal of Electronics Engineering, 2(1), 2010, Page: 189-196.

[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.

[24] Layth A. Khalil A, Dulaimi1 R. Badlishah Ahmad, Naimah Yaakob, Mohd Hafiz Yusoff and Mohamed Elshaikh" Black hole attack behavioral analysis general network scalability" Indonesian Journal of Electrical Engineering and Computer Science Vol. 13, No. 2, February 2019, Page: 677-682.

[25] Muhammad Salman Pathan1, Jingsha He2, Nafei Zhu3, Zulfiqar Ali Zardari4, Muhammad Qasim Memon5, Aneeka Azmat6 "An Efficient Scheme for Detection and Prevention of Black Hole Attacks in AODV-Based MANETs" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 1, 2019, Page: 243-251.

[26] Md Ibrahim Talukdar , Rosilah Hassan , Md Sharif Hossen ,Khaleel Ahmad ,Faizan Qamar , and Amjed Sid Ahmed "Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature" Hindawi Wireless Communications and Mobile Computing Volume 2021 Page: 1-13.

[27] Deshmukh, Sagar R., and P. N. Chatur. "Secure routing to avoid black hole affected routes in MANET." In Colossal Data Analysis and Networking (CDAN), Symposium on, pp. 1-4. IEEE, 2016.

[28] F. H. Tseng, L. Chou, and H.C. Chao: A survey of black hole attacks in wireless mobile ad hoc networks, International journal on Human centric Computing and Information Sciences, 22 Nov 2011, Page: 1-16.

[29] L. Yingbin, H. V. Poor, and Y. Lei, "Secrecy Throughput of MANETs under Passive and Active Attacks," Information Theory, IEEE Transactions on, vol. 57, 2011, Page: 6692-6702.

[30] Bindra, G.S., Kapoor A., Narang A., Agrawal A. "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs", IEEE Conference on System Engineering and Technology (ICSET), 11-12 Sept. 2012, Page: 1-5.

[31] R. H. Jhaveri, "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs," Third International Conference in Advanced Computing and Communication Technologies (ACCT), 2013, Page: 254-260.

[32] N. Kalia, and K. Munjal, "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol" International Journal of Engineering and Advanced Technology (IJEAT), Vol. 2, No. 3,2013,Page: 529-533.

[33] K. S. Chavda, and A. V. Nimavat, "Removal of Black Hole Attack in AODV Routing Protocol of Manet", Proc. IEEE conference on computer networks, Tiruchengode, India, 2013,Page: 207-212.

[34] Shurman, M., Yoo, S.M. and Park, S. "Black hole attack in mobile Ad hoc networks", Proceedings of ACM southeast regional conference, 2014 Page: 96-97.

[35] HodaRafiee Pour, MarjanKuchaki Rafsanjani, and Hamid Saadat "A New Zone Disjoint Multi Path Routing Algorithm to Increase Fault-Tolerant in Mobile Ad Hoc Networks" Applied Mathematics & Information Sciences An International Journal.Appl. Math. Inf. Sci. 9, No. 1, 2015, Page: 433-444.

[36] T. Sasilatha, S. Vidhya and P. Suresh Mohan Kumar "Detection and Elimination of Black Hole and Grey Hole Attack on MANET" International Journal of Pure and Applied Mathematics Volume 116 No. 24 2017, Page: 235-242.

[37] Nigahat and Dr. Dinesh Kumar "A Review on black hole attack in mobile ad hoc networks" International Journal of Engineering Sciences & Research Technology March, 2017 Page:556-561.

[38] Dr. T.Sivaraman "Link Based Bandwidth Aware Multipath Routing Protocol in MANET". International Journal of Engineering Science Invention Page NCIOT- 2018 Page: 70-76

[39] G. Stephanie Vianna, T. Vishnu Priya and M. Sathya "Trust based approach to overcome black hole attack in MANET" International Journal of Pure and Applied Mathematics Volume 118 No. 22 2018, Page: 1763-1769.

[40] Network Simulator Official Site for Package Distribution, web reference, http://www.isi.edu/nsnam/ns.