International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 644–653

Impacts of Black Hole Attack on Mobile Ad-hoc Networks

Kavita Arora*[1], Dr. Kavita[2], Dr. Vishal Jain[3]

[1]*Research Scholar, Department of Computer Science and Engineering*
Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan, India
Assistant Professor, Faculty of Computer Applications,
Manav Rachna International Institute of Research and Studies

[2]*Associate Professor, Department of Computer Science and Engineering*
Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan, India

[3]*Associate Professor, Department of Computer Science and Engineering*
Bharati Vidyapeeth's Institute of ComputerApplications and Management (BVICAM)

Abstract

MANET has a cluster of mobile devices which combine together to establish a short-term network in the areas which do not have a fixed networkinfrastructure. These are self-governed networks with varying topology.This distinctive feature of continuously changing topology along with absence of any central coordinator in these temporary networks enhances chances of various security attacks.Black hole attack is one such challenging issue in MANETs in which, a malevolent node gives false information for the RREQ even in the absence of any functional pathto the terminal node and for this uses routing protocol to proclaim the shortest path to the destination. When it acquires the data packets, as per its basic characteristic, itblocks and later on drops them too. In this paper, our emphasis is to studyBlack hole attack in conglomeration with Ad-hoc On-Demand Vector (AODV) routing protocol. Black Hole attack and AODV are reviewed together and the consequences are elaborated by description of the disruptions resulting from attack andrepercussions on the performance of MANET. Our further work covers the study of detection and prevention mechanismsavailable for Black hole attack in AODV.

Keywords*: Mobile Ad-hoc Network, Black hole attack, AODV routing protocol.*

1. Introduction

Wireless networks are the networks which are not connected by any cables and the nodes communicate without therestriction of wired connections. These networks use the radio waves to connectthe devices. The wireless networks are further categorized as: Infrastructure based networks and ad-hoc networks.A MANET is based on mobile wireless nodes [1]. It is an auto configured assembly of nodes which are not dependent on a fixed infrastructure so as to sustain the interconnectionbetween them [2]. These nodes rely on each other to relay data packets[3] .The mobile devices are autonomous in nature which can move randomly in the network and can organize themselves arbitrarily.As the nodes are free to connect or disconnect with the network any moment oftime, this entails to frequent interruptions in communication links in the network.

ISSN: 2233-7857 IJFGCN

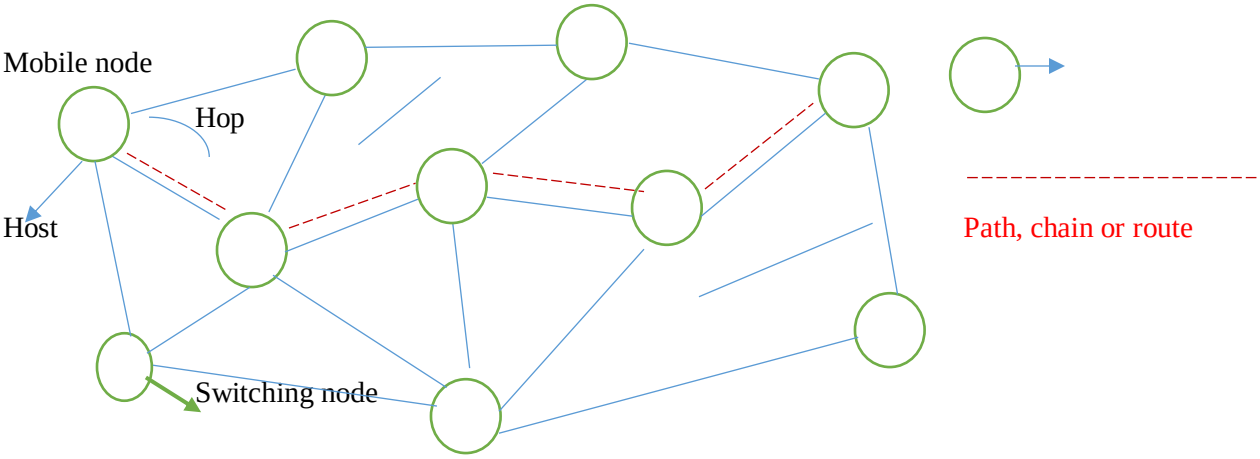

Figure 1: Mobile ad-hoc network

In the latest past, MANETs have seen a tremendous growth and have emerged as valuabletechnology[4]. In these networks, the nodes involved are coupled in a P2P and multi-point manner without using any central controlling station. Each participating node can interact with each other and performs a dual role of a host as well as a router. These nodes can either communicate directly if the neighboring node is found within the radio range or can opt for multihop method.The network's performance is based upon coordination between participating nodes.

As in wired networks, for a secured communication process to take place, many safety mechanisms like firewalls and gateways are present. Any such kind of security mechanism is absent in ad-hoc networks.Moreover, the nodes are dynamic enough, require high power utilization to move in and out and networks.The portability of nodes in these networks makes them prone to different security attacks resulting mainly from inhabitance of malicious nodes. Since ad-hoc networks have no any robust mechanism to identify and combat these attacks, thus these malevolent nodes become capable enough to topple either the complete network or a part of it or may capture the data under transmission. In addition to this a variety of aftereffects are also associated with a variety of attacks. Thus security is a key concern in MANETs owing to itshighly vulnerable nature and can be accessible to authorized users as well as malevolent attackers[5].

2. Major security attacks in MANET

ISSN: 2233-7857 IJFGCN

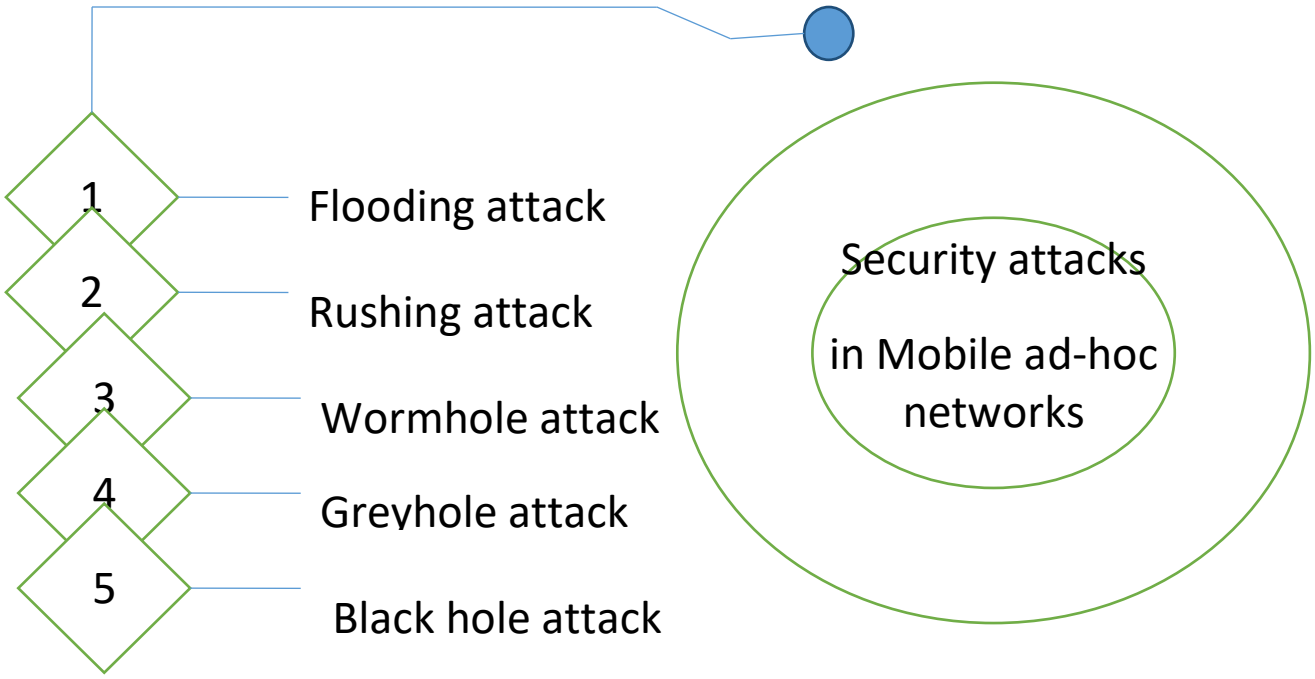

Figure 2: Security attacks in MANETs

1. Flooding attack: In this security attack, attacking node disrupts transmission of packetsby delugingfake RREQ messages to non-existent destinations and engulfs the network resources.
2. Rushing attack:Known as a harmful security attackwherein malicious node takes advantage of vulnerability of ad-hoc networks. The malevolentconduct of the nodes is exhibited in different ways as to data traffic is discarded either of specific nodes, while behaving normally for remaining nodes.
3. Wormhole attack: The other name given to this attack is Tunneling attack wherein a wormhole creates a path which appears to be an avenue from source to the destination, but the messages are always tunneled to the misbehaving node.
4. Grayhole attack: This attack is considered as a slow poison in the network as we can never determine the severity of packet loss. This attack is quite similar to black-hole attack as both attacks drop messages in the same way[6]. The difference is that here, the attacker nodenever forwards the data blocks and thus subterfuge source node by dropping selective data blocks.
5. Blackhole attack: In this attack, a malevolent node makes use of routing protocols to proclaim possession of the shortest path to the destination node and subsequently instead of forwarding the packets, swallows data blocks as it takes all the routes towards itself. This attack is also identified as a full packet drop attack in ad-hoc networks [7].

3. Black Hole Attack

ISSN: 2233-7857 IJFGCN

Routing protocolsface lot many security issues in MANET because of theirubiquitousnature.Other than that, these networks suffer several attacks due to presence of the malevolent nodeswhich envisageeither toattack the data blocks or by dropping, delaying or altering them.

BHA is such a grave and extensive security issue in MANET, which begins with route discovery phase. This attack corresponds to Denial of Service (DoS) attack[8]. It happens in parity to black hole in the universe wherein everything disappears. This attack falls under the category of active attacks and is one of the serious attacks on routing protocols which takes place in the network layer of OSI model and unswervinglyimpacts the parameters of the network.Main cause of this attack arises upon when a malevolent or selfish node joins the network with a week routing infrastructure and passes a fake Route Reply message to the source node for the commencement of discovery of route [9].

Under BHA, the attacker node adds a spoof route and then proclaims itself to have the shortest route to goal node by forwarding either a fake REEP or highest sequence number. As soon as source node gets to know about this route, itstarts forwarding the datablocks enroute this malevolent node, the selfish node subsequently engulfseach one of them. This way, the attacker node makes a fool of every node by breaking the communication between the nodes. It is not easy to identify the behavior of the selfish node[10] and the discernment of such attacks in MANET is also quite difficult because of absence of central controller, bandwidth limitations and dynamic topology.

Engendering of this attack is coherent as very few or no particular tools or innovatory attack techniques are involved. In addition to this, as nodes are participating in routing of data packets, they can ruin netowrks[11]. Nonetheless, this attack seriously corrupts the routing tables maintained by the routing protocols.Augmenting the severity related to the attack, there could be addendum likelihood suffering from the denial of network services and losing confidential data too.

3.1 A black hole has the following attributes:

a) The malicious node administersAODV so as to proclaim possessing a valid route to the goalinstead of certitude that mentioned route is counterfeited for ambushing packets.
b) Subsequently this node engrosses the data traffic followed by dropping of the packets.

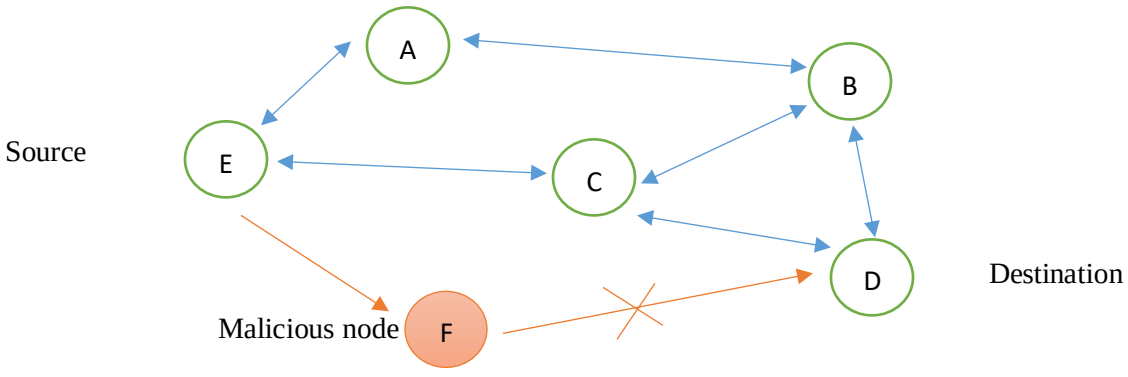

Figure 3: MANET under Blackhole Attack

3.2 Problems faced by Network due to BHA

ISSN: 2233-7857 IJFGCN

1. BHA is considered to be one of the very severe and widespread active attacks which degrades performance and reliability of the network.
2. BHA takes place because of a selfish node which consciously misbehave in network which not only adds a spoof route but also pretends to have a shortest path leading towardsgoal node. Furthermore, attacker node swallowsall the data blocks too leading to data loss in MANET.
3. In BHA, malicious node generates a smashed node interface which in turn causes all the other nodes continuously trying to find a path towards destination node, which causes consumption of battery in addition to loss of data packets.
4. In BHA, the presence of the selfish node reduces the ratio of end-to-end packet delivery as this node incontinentlyabsorbs the data blocks and never forwards them to the nearest neighbor.
5. Black hole attack can take place either by plunging someparticular data blocks destined to a delineatedgoal nodeor arbitrarilychosenchunk of packets or the entire packet set and as a result the destination node turns out to be unreachable and suspends the ongoing communication between two junctions in the network.

In nutshell, BHA in MANETs degrades the network performance, cause a low Packet Delivery Ratio, less throughput and muddles route discovery process.

4. Approaches for BHA detection and mitigation

The BHA in Mobile Ad-hoc Networks is contemplated to be very active and extensive attacks whichdiminishes the network's performance and reliability as the malevolent node drops incoming packets.

Arouting protocol is a set of rules which governs the nodes as they are responsible for best route discovery for transmission of data packets[12]. Till date, various authors have surveyed on distinct detection approaches which strive to solve the issues related to BHA on AODV routing protocol and outlined their pros and cons as well. The utmost sought after algorithms are reactive routing protocols as they incur minimum computational overheads and bring out the best transmission when required[13]. Nonetheless, a concrete number of simulations have also been conducted which illustrate the consequences of this attack on AODV routing protocoland how to trounce from the consequences of this attack.

In most of the cases, the research work of authors focuses on the packet drop caused by the attack and appraise the aftermath on the Delay, PDR and Throughput.

In [14], as per authors, in order to ascertain the BHA in MANETs, if RREP is over-heard, then every node cross checks the same with its next neighboring node. If no link is found between Route Reply forwarding node and its neighbor, then the RREP forwarding node is contemplated to be the malevolent node. This elucidation is in accordance with the hypothesisof existence of more than one malevolent nodes in the network.

In [15], the prospective method named SAODV is meant to detect malicious node causing BHA, depending on opinion of neighboring nodes. As per this technique, all the nodes in SAODV maintain two individual tables, one which has ids of neighbor nodes and second to identify the nodes as per node receives RREP against the RREQ, an opinion message is transmitted to neighboring nodesregarding the node proclaiming to possess the activities performed by them in the network. If every node responds with NO message, then that particular node is detected as the malevolent node and anotification alarm is broadcasted in the network. This proposed method suffers from the limitations of high overhead for the exchange of opinion messages.

In [16], as per the authors, the proposed technique "Blackhole Detection System" is used for detection ofBHA by verifying Route Reply emanating across network. It says that in case, RREQ is encountered and anode instantly forwards a Route Reply messageto the source node without even evaluating the

ISSN: 2233-7857 IJFGCN

routing table, there are chances the malicious node has done so. In such a case, the improvised system dumps this RREP packet emanating from the attacker node and selects the succeeding RREP packet.

In [17], a novice attack detection and prevention technique proposed by the authors is applicable on Proactive as well as Reactive protocols. Here in this technique, a particular kind of packet called Bluff Probe is used for the purpose of identification of the malicious nodes leading to Black Hole attack. This packet contains ID of a non-existing destination and the broadcast message to be remitted by source node, before actual RREQ is forwarded. In return, malicious node replies with RREP once it receives the RREQ through the interposed node, while other nodes directRREP to theirneighbor nodessince they don't have a fake destination id in their routing table.

In [18], Redundant route and Unique sequence number scheme mechanism has been proposed by the authors. The method proposes to opt for the safe route owing to the observation of RREP packet to check if the routes in network are sharing the same hop. In case, no such shared hops are found on any of the route, the sender node waits for a further RREP packet. By the time it finds a route with the shared hop or the routing timer expires, on the basis of the information retrieved, the sender node can decide the safe route and avert the blackhole attack.

In [19], a modified version of AODV termed as DPRAODV (Detection, Prevention and Reactive AODV) has been proposed. It informs the participating nodes regardingexistence of malevolent node in the network, by sending Alarm packets. In this technique, the RREPforwarded by the attacker node is discarded and the details about the same are also removed from the routing table. The main drawbacks of this method are increased routing overhead and average end-to-end delay.

In [20], a method has been proposed which discuss the special category of nodes known as guard nodes used for detection of black-hole nodes in MANETs. These guard nodes basically verify the conduct ofparticipating nodes with help of routing tables in which the trust value of each node is maintained and is determined owing to its behavior in the network. This value diminishes if the node reverts with Route Reply only but does not forward the Route Request. In case, this value diminishes underneath the set threshold value, the node is immediately blocked and the guard nodes transmit the alarm packets to all its neighbor nodes informing about the malicious node. The constraint about this particular technique is that some special type of guard nodes are required to sheath the whole network and moreover it incurs an excessive overhead due to numerous tables.

In [21], the proposed method has been evolved to combat BHAby means of timers and baiting messages. This method is divided into two parts: one is baiting and second is non-neighbor reply. With regard to first phase, each node has a bait-timer with its value arbitrarily set to B seconds. When the timer reaches B, a bait request is broadcasted with anarbitrary forged identification. As per the innate deportment of a black-hole node,when it encounters RREQ, it replies to source node about having a best and shortest path. In turn on receiving RREP, source nodetreats responding node as the malicious node and it gets listed as a black-hole node. In the second phase of the technique, every node is familiar to its neighboring nodes. In case a RREP is encountered by the source node, the id of the node is established with the shortest route and if the id exists in the list of blacklisted nodes, the received RREP is discarded in order to circumvent any further communication with such attacker nodes.

In [22], authors have proposed an algorithm to keep a check on the behavior of a malevolent node in the BHA.For the purpose of enticing data packets apropos, the attacker node as per its basic characteristic, forwards fake RREP packets following the RREQ message. It simply forwards the route reply messages regardless of the fact that the nodedoesn't possess a routetowards goal node and moreover it does so without consulting the routing table. As a result, the ratio of RREP sent and RREQ does not match. The proposed algorithm Opinion AODV makes use of this certitude for detection of malicious node. To do this, the routing table is appended with two additional fields: Request weight

ISSN: 2233-7857 IJFGCN

and Reply weight. Request weight and Reply weight signify the count of RREQ and RREPforwarded respectively. Thus this method with the help of the modules collects the feedback of black hole attack.

The following table shows the comparative analysis of the various Black Hole attack detection and mitigation techniques. Every technique has its own pros and cons with a different approach followed.

Table 1: Comparative table for various BHA detection and mitigation techniques.

ISSN: 2233-7857 IJFGCN

Detection Method	Results	Paper
SAODV method	Maintains two individual tables to match RREP received against RREQ; transmits an opinion message to assess the RREP message; suffers from limitations of high overhead for exchange of opinion messages.	SAODV: Black hole and gray hole attack detection protocol in MANETs,
Blackhole Detection System	Detects BHA by verifying RREP; assumes if against a RREQ, a RREP is sent by a node without evaluation of routing table; there is a probability that malicious node has done this.	Black Hole Attack in Mobile Ad Hoc Networks.
Novice Attack detection and prevention technique	Applicable on Proactive and Reactive protocols; "Bluff packet" is used for verification of malicious node; source node sends RREQ through a fake id and malicious node replies to it and thus intercepted by specially designed packets.	Design Enhancements in ZRP for Detecting Multiple Blackhole Nodes in Mobile Ad Hoc Networks
Redundant Route and sequence Number Scheme	Opts for safe routing by observing RREP packet to check if routes in network share the same hop; if such a route is found or routing timer expires, the safe route is decided on the information received and tries to avert BHA.	Blackhole Attack in Mobile Ad Hoc Networks
DPRAODV protocol	Informs the participating nodes about the existence of attacker node by forwarding "Alarm packets" which help to detect attacker node; RREP received from this node is discarded and removes the node from the routing table. Main drawback of this method is increased routing overhead and average end-to-end delay.	DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV Based MANET
GNB-AODV	Verifies the conduct of participating nodes using routing tables which maintain the trust value of nodes and is determined by their behavior; value of a node diminishes by threshold value if reverts with RREP without RREQ; transmits the alarm packets and blocks the node. Disadvantage of this method is excessive overhead incurred due to numerous tables.	GNB-AODV: guard node based – AODV to mitigate black hole attack in MANET
Opinion AODV algorithm	Checks behavior of a malevolent node; uses the approach by appending the routing tables with two additional fields: Request weight and reply	The black-hole node attack in WSN

ISSN: 2233-7857 IJFGCN

	weight. Using these, matches the ratio of RREQ sent and RREP received.	

5. CONCLUSION and FUTURE SCOPE

MANETs are extensively used networks in recent times as it is easy to deploy themirrespective of the geographic curb. These networks are flexible enoughsince the nodes are free toenter or exit and there is no controlling body to keep a check on thesemoving nodes. Owing to thischaracteristic, MANETs become quite prone to several security as well as routing attacks. There can be Active or Passive attacks, information may leak, fake RREP or DoS. The other situations can be compromised links and link attacks which canclog the communication between the nodes. Due to the malicious behavior of the nodes, these attacks may lead to demolished links also.

Security of ad-hoc networks is a prime concern mainly to safeguard them from the aftermaths of the attacks. Our work emphasizes on one of significant securitymenace – Black hole attack. This attack harms network's performance and focuses on aversion of any kind of communication in the network. We have studied the various impacts of this attack in AODV protocol.AODV is responsible to locate the shortest routing path between nodes so as to convey messages. Different researchers have managed to provide different detection and mitigation approaches for the eviction of BHA in AODV. Every method has its own merits and demerits as the no method is self-sufficient in terms of efficacy and competence.

In our future work, we intend to design and develop a novice algorithm named E-AODV (Efficient AODV) which can reduce the impacts of BHA to manifolds. Our future work will be based on the detection mechanism of BHA with respect to Probability and estimation of Threshold value. With this we will try to enhance AODV routing protocol and add a certain functionalities to it to discernmalicious nodes causingblack-hole attack and counter the harm Induced. This approachwill alsowork on improvement of the performance of the network on various parameters viz a viz packet failure, overhead and throughput. We also intend to develop the simulation of our proposed methodology for the evaluation of its performance.

References:

1. P. Dewal, G. S.Narula and V. Jain, "A Survey of Intrusion Detection Systems and Secure Routing Protocols in Wireless Sensor Networks", *International Journal For Research in Emerging Science and Technology,* Vol. 3, No. 1, **(2016)**, pp. 16 – 20.
2. V. Kumar and R. Kumar, "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network", Proceedings of*International Conference on Intelligent Computing, Communication & Convergence, (***2015)**.
3. S. Banerjee, M. sardar and K. Majumdar, "AODV Based Black-Hole Attack Mitigation in MANET", Proceedings of *International Conference onAdvances in Intelligent Systems and Computing, (***2014)**.
4. S. Badiwal, A. Kulshreshtha and N.Garg, "Analysis of Black Hole Attack in MANET using AODV Routing Protocol", *International Journal of Computer Applications,* Vol. 168, No.8, **(2017)**.
5. V. Khandelwal and D. Goyal, "BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs", *International Journal of Advanced Research in Computer Engineering & Technology,* Vol. 2, No. 4, **(2013)**.

ISSN: 2233-7857 IJFGCN

6. K.Arora, Kavita, V. Jain, "A Study on Attacks in Mobile Ad-Hoc Networks", *International Journal of Advanced Science and Technology*, SERSC, Vol. 29, No. 8s,**(2020)**,pp. 279-289.
7. Z. A. Zardari, J. He, N. Zhu, K. H. Mohammadani, M. S. Pathan, M. I. Hussain and M. Q. Memon," A Dual Attack Detection Technique to Identify Black and Gray Hole Attacks Using an Intrusion Detection System and a Connected Dominating Set in MANETs", *Journal of Future Internet*, Vol. 11, No. 61, **(2019)**,pp 1-17.
8. V. Kamatchi, R. Mukesh, and Rajakumar,"Securing Data from Black Hole Attack Using AODV Routing for Mobile Ad Hoc Networks", *Advances in Computing & Inform. Technology,* AISC 177, **(2013)**, pp. 365–373.
9. A. Singh, K. P. Kalita and S. P. Medhi, "BLACKHOLE ATTACK ON MANET AND ITS EFFECTS", Proceedings of *International Conference on Computing for Sustainable Global Development, (***2018)**.
10. K. V. Kumar and K. Somasundaram, "DETECTION OF BLACK HOLE ATTACKS IN MANETS BY USING PROXIMITY SET METHOD", *International Journal of Computer Science and Information Security*, Vol. 14, No. 3,**(2016)** .
11. N. Mittal and L. Chand, "Prevention and Detection Techniques under Black Hole Attack in MANETS: A Survey", *Advances in Wireless and Mobile Communications,* Vol. 10, No.4, **(2017)**, pp. 551-558.
12. R. singla, "A Literature Survey on Challenges and Issues on Mobile Ad Hoc Networks", *International Journal of Computer Science and Information Technologies*, Vol. 7, No. 1,**(2016)** , pp. 157-162.
13. Y. Shashwat, P. Pandey, K.V. Arya and S. Kumar, "A modified AODV protocol for preventing blackhole attack in MANETs", *INFORMATION SECURITY JOURNAL,* Vol. 26, No. 5,**(2017)** , pp. 240–248.
14. G. Gupta and R. K. Pateriya , "Approach for detecting Black hole attack in MANETs", *International Journal of Engineering Research and Technology*, Vol. 2, No. 9, **(2013)**.
15. S. Dhende, S. Musale, S. Shirbahadurkar and A. Najan, "SAODV: Black hole and gray hole attack detection protocol in MANETs," *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, **(2017)**,pp. 2391–2394,.
16. M. Shurman, S. Yoo and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks", *Proceedings of the 42nd annual Southeast regional conference ACM-SE 42 ,(***2004)**.
17. Shree, R.Dwivedi and S.K. Pandey, "Design Enhancements in ZRP for Detecting Multiple Blackhole Nodes in Mobile Ad Hoc Networks", International Journal of Computer Applications, Vol. 18 No. 5, **(2011)**, pp. 6–10.
18. Al-Shurman, M. Yoo and S.M. Park, "Blackhole Attack in Mobile Ad Hoc Networks*", Proceedings of the 42nd Annual ACM Southeast Regional Conference,* **(2004)**.
19. P.N.Raj and P.B. Swades, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV Based MANET", *International Journal of Computer Science Issues,* Vol. 2, (**2009)**, pp. 54-59.
20. A. R. Rajeswari, K. Kulothungan, and A. Kannan, "GNB-AODV: guard node based – AODV to mitigate black hole attack in MANET," *International Journal of Scientific Research in Science, Engineering and Technology*, vol. 2, no. 6, **(2016)**, pp. 671–677.
21. A. Yasin and M.A. Zant, "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique", *Wireless communications and Mobile computing*, **(2018)**.
22. N. Sharma and A. Sharma, "The black-hole node attack in WSN," *Proceedings of 2nd International Conference on Advanced Computing & Communication Technologies*, **(2012)**.

ISSN: 2233-7857 IJFGCN

ISSN: 2233-7857 IJFGCN