# A Study about Role of Neural Networks in Wireless Networks: MANET



**Manmohan Sharma, Dr. Mohanjeet Singh**

RIMT University, Mandi Gobindgarh, India

Patel Memorial National College, Rajpura, India

## Abstract

The term "mobile ad hoc network" refers to a system that consists of mobile nodes that are self-governing and independent and that connect with one another using wireless networks but have no permanent infrastructure. A Mobile Ad hoc Network, abbreviated as MANET, is a collection of mobile nodes that number more than two and have the ability to configure themselves. It is a network that does not require any infrastructure; thus we do not require any form of base stations or access points to use it. It is dynamic in nature, which means that nodes are free to move in and out of the network at any time and from any location. Additionally, the network itself is mobile. MANET is susceptible to a wide variety of security flaws on account of its core properties, which include the absence of permanent infrastructure, dynamic topology, and wireless nature. Black Hole Attack is one type of potential security risk. During this type of attack, a rogue node will pretend to be one that has the shortest path between the source and the destination. As a consequence of this, the source node makes the decision to send the data packets through the malicious node, and the malicious node then makes the decision on whether to forward or drop the packet that was sent by the sender. Therefore, in order to ensure safe transmission in the face of the Black Hole Attack, researchers have periodically presented a variety of various security mechanisms and routing algorithms.

**Keywords:** Mobile Adhoc Network (MANET), Black Hole Attack, Routing Protocol

**DOI Number: 10.14704/nq.2022.20.9.NQ44341** **Neuro Quantology 2022; 20(9):2937-2946**

**Introduction**: A mobile ad-hoc network is a wireless network that does not rely on a fixed infrastructure for communication [1][3][4]. Instead, each node in the network functions independently as a router and is responsible for either receiving or delivering messages. Because there is no node that is in charge of managing the network as a whole, all of the nodes that are part of the network are responsible for doing so. It is also possible to define it as a system of mobile nodes that are autonomous and independent of one another and that transfer data to other nodes in a network in the absence of any permanent infrastructure. In contrast to this, a cellular network is one in which two mobile nodes connect with one other through the use of wires and cables.

There are two primary channels via which communication may take place in a MANET: the first is a direct communication channel that is activated when two nodes are physically close to one another. The issue occurs, however, when the communicating nodes are not in the same range; in this case, they resort to peer-to-peer communication that involves many hops via intermediary nodes. MANETs often make use of on-demand routing protocols that are founded on the flooding method.

Finding the path by which a message sent by a sender will be received by a receiver or a reply sent by a receiver will be sent back to the sender is what routing is all about. MANET uses specific protocols, one of which is called the flooding technique, to facilitate the message transmission process when multiple hops are involved.

One type of ad hoc network known as a mobile ad hoc network, or MANET, is characterised by having a number of mobile nodes that are able to configure themselves and change their location at any given moment [6]. It is an infrastructure-less network, which means that we do not need any kind of fixed or stationary base stations, access,

and each mobile node acts as a router. This means that nodes in MANET provide route paths that assist in the process of forwarding a message from its source to its destination. It is a network that is capable of self-organization and adaptation.

Because of this, there is no central supervision, and as a result, nodes in the network are free to freely enter or exit the system owing to the network's mobile nature, which results in frequent route breakage. Messages are transmitted to their destinations over a radio channel that is shared by several users.

In this scenario, nodes interact with one another through connections that involve many hops. Nodes or devices in a MANET should be able to detects its connectivity with other nodes or devices in the network and perform the handshakes for communication between them and share necessary information. Additionally, it should be able to identify the type of devices to which it is connected as well as the other parameters of those devices [7]. Because of the features of MANET, such as its dynamic topology and lack of infrastructure, [8] there is a lack of coordination, and because we do not have any nodes that monitor our network, there are various security attacks [9, 10] that are conceivable on this.

Flooding [1][2][5][11] is indeed a technique in which a node delivers the message to all of its neighbours, and those neighbours further broadcast the message until it is disseminated throughout the whole network. Flooding is a technique in which Blind flooding is the term used to describe the transmission of a message in the manner described above [1][2][5][11]. Efficient flooding, on the other hand, describes the transmission of a message that is restricted to a certain region of geography or to a subset of nodes. However, flooding itself has certain problems with overhead and collision, and academics have been trying for a long time to find solutions to these problems.

When opposed to wired networks, MANETs are more prone to being attacked by malicious software because to the inherent qualities that they possess. In MANET, attacks are categorised according to the source of the attacker or the conduct of the attacker, whichever comes about first. On the basis of the source, it is further subdivided into Internal attacks, in which the intruder is a part of the network, and External attacks, in which the attacker is not a part of the network but tries to access the network and, once it has access, it starts doing activities that interrupt the performance of the network. The attacker keeps their position inside the network and attempts to get access to communications for which they do not have permission. And on the basis of behaviour, it is classified as Active attacks, in which the intruder attempts to modify the messages that are sent by the sender, and Passive attacks, in which the intruder only listens to the communication that takes place between the sender and the receiver, without making any changes to the messages that are being sent.



**Literature Review:**

Patel and Dadhaniya [16] presented a three-step host-based intrusion detection method in which each node operated as its own intrusion detection system (IDS). It does so by examining the sequence number that is produced by the rogue node in question. If the sequence number that is generated by the replying node is greater than the sequence number that is generated by the source node, then the replying node is considered to be a malicious node, and the messages that are sent by it are also blocked. This is done by transmitting the node id to all of the other nodes. The results of the simulations performed for this article demonstrated that there was a rise in both the PDR and the average throughput.

Deng et al. [17] suggested a method in order to address the issue of the Black Hole Attack. Along with the RREP message, information regarding the neighbour of the replying node is also requested using this method. When the RREP message reaches its source, the source, rather than sending the message immediately, sends another message to the neighbour of the replying node, inquiring as to whether or not the intermediate node that is replying for the RREQ message actually has a path to its destination. But it had a flaw in that it raised the communication cost, which meant that it could only be used to verify the identity of a node if there was reasonable suspicion that it was malevolent. It also made the assumption that Black hole nodes could not collaborate with one another.

In their paper [18], Raj and Swadas introduced a method known as DPRAODV for detecting black hole nodes based on the RREP sequence number and the threshold value. The node that is transmitting this RREP will be considered malicious if the value of the RREP sequence number turns out to be larger than the threshold value. In addition, the malicious node is removed from the network by broadcasting the control message ALARM to every other node, and a list of nodes that are banned from the network is compiled. The results of the simulation indicated that there was an increase in the percentage of packets that were successfully delivered, but there was also an increase in the routing overhead and the amount of time it took for messages to be delivered.

The working of the source node was modified by Mistry et al. [19] by the addition of a new function for storing RREP messages for some specified time, a table which stores these RREP messages, a timer, and Mali node id for detecting black hole node and to keep record of all malicious nodes present in network. These additions were made so that the source node could better keep track of all malicious nodes. The RREP message that is placed in the database and has the greatest value of the destination sequence number is discarded by this method. Additionally, the node that sent the RREP will be deemed malicious, and its identity will be recorded as the malicious id for the network. Although using this strategy results in a greater memory and time overhead, the increased packet delivery ratio compensates for that burden.

Bhosle et al. [20] presented a watch dog approach for detecting the existence of an attacker node in which an additional piece of information would be maintained in tables on all of the nodes. In this, the nodes keep track of the packets that they send as well as the packets that they drop, and if the value of the packet drop ratio climbs over the threshold, the node will be regarded to be an attacking node.

Neha et al. [21] presented a comparative study about work done and further required to be done in Mobile Adhoc Network. Various techniques were analysed and accordingly summary was provided in the form of a table.

A Step Verification Algorithm was presented by Neha et al. [12] to be utilised in MANET for the purpose of locating and isolating Black Hole attacks. Using this method, it is possible to identify a single black hole node and then remove that node from the network. Nodes are responsible for maintaining a malicious table, which contains the entries of malicious nodes that have been discovered in the past as malicious nodes, and they search the entry in that malicious table for detection of malicious node or black hole node. If the node id matches in that table, the node in question is discarded, and if it does not match, further mechanism to detect it is initiated.

Baited Black Hole DSR is utilised by Brinda et al. [13] for the purpose of detecting and avoiding the black hole assault. Additionally, they incorporate the notion of detecting cooperative black hole attacks. BDSR employs the notion of delivering bait id and attempts to entice hostile nodes into replying with bogus routing information by using this method. The early part of the process involves proactive detection, whereas the latter part of the process involves reactive detection. The proactive detection node is responsible for locating the malicious node, and in cases when reactive detection is performed, it helps to cut down on overhead and resource waste.

Nath et al. [15] research provides dependable and secure cluster routing, in addition to proposing a novel technique for the detection of black hole attacks and giving a new approach for their prevention. The Friendship Table is the first thing that this algorithm examines. If the node in question is already present in the buddy table, then it will only send the received packet; otherwise, it will continue passing the packet on to an unknown node or do additional checks. In the following stage, it will test the stranger's degree of trust by sending a sham package to it. The trust level of the stranger node is determined by utilising the k factor, and based on the value of the k trust level, the system chooses whether or not to add a new entry to the friend ship table and whether or not to send the received packet to its destination.

After making modifications to the standard AODV protocol, Kaur et al. [14] offered a modified approach as a means of detecting and protecting against black hole attacks. There are several vulnerabilities in the AODV routing protocol, which can make MANET susceptible to a wide range of attacks that can be triggered by a wide

number of nodes both inside and outside the network. Through the use of this method, the performance of the network is improved.

Chavda et al. [22] suggested a method that involves the comparison process being carried out. In this method, rather than comparing the destination sequence number of the RREP with the source sequence number, they compare the destination sequence numbers of the RREPs that have been received. Then, the technique chooses the RREP that has the highest destination sequence number value, with the stipulation that the difference between the two destination sequence numbers should not be unusually large. When compared to the standard AODV protocol, the results of the simulation shown that the suggested method provides a high value of both PDR and throughput.

Mistry et al. [19] gives a new technique, in which they conducted a modification in the functioning of source node by the introduction of some new function in it, a timer, table, and Mali node id for keeping record of everything malicious. This new method was developed by Mistry et al. The use of this technology results in a memory and time overhead that is increased.

**Related Work:**

Black hole attack [12-15] is one of them. In this assault, there is a malicious node that says that it is having the shortest way between the source and the destination. When the source chooses that route, the malicious node begins to drop all of the packets that are arriving from the source. When a black hole node is presented with route request RREQ packets, it will immediately respond with a REPP packet that contains the minimal hop count from that node to the destination as well as a high sequence number to the destination.

There are two different approaches to attacking a black hole: single and cooperative. Assuming that a source node "S" wants to send a message to a destination node "D," the first step in the process is to define a route for the message's transmission. This step is taken during the route discovery process, which involves broadcasting an RREQ to all of the nodes that are connected to the source node and receiving RREP from nodes for that RREQ. When a malicious node or a black hole node with the identifier "M" receives a route request, it will respond to the source by claiming to have the quickest path to the destination. Then the node "S" selects this route and rejects reply messages from all of the other nodes. It then begins transmission via the malicious node "M" route, which ultimately leads in the black hole node "M" dropping all of the packets [8]. The procedure for a single black hole assault is illustrated in Figure 1, which describes the situation.



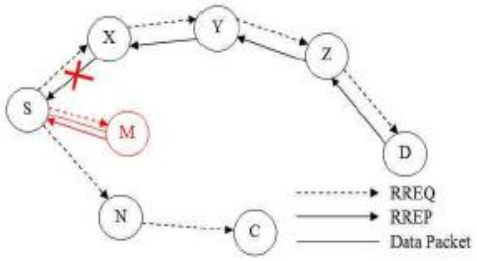


Figure 1: Single Black Hole Attack

When there are two malicious nodes working together to carry out an attack on a network, this type of attack is referred to as a cooperative black hole attack. This is because as network security improves, intruders become more aware of certain things and are able to launch new attacks against the network. The concept of a cooperative black hole attack is depicted in Figure 2, along with the entire procedure.

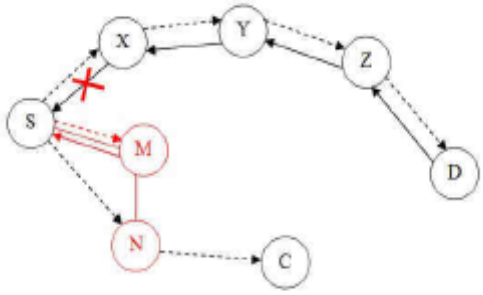


Figure 2: Cooperative Black Hole Attack

In this particular instance, two nodes in the network known as Node M and Node N are both acting maliciously in the network and, with the assistance of one another, both carry out the black hole attack in the network. When RREP from

Node M is examined by another node to see whether or not Node M is having path to destination, the node that tells the source node S that Node M is having path to destination is Node N, which is also a malicious node.

In many settings in the modern world, security is built on a strategy known as "in-depth defence," which involves the deployment of many layers of protection to prevent adversaries from breaking security standards. According to this strategy, even if the adversary manages to penetrate one of the layers of defence, he will not be able to cause significant harm since the other levels will give an acceptable amount of support to the layer that was penetrated.

A mobile ad hoc network (MANET) is a network that lacks infrastructure and is instead self-configured by mobile devices that communicate with one another using wireless connections. Because each mobile device in a MANET has full autonomy and the ability to travel in any direction, the connections between mobile devices and other devices frequently shift. This is because each mobile device in a MANET is completely independent of the others.

MANETs are becoming increasingly important for a variety of applications because they do not require a permanent communication infrastructure in order to establish a dynamic network. Some of these applications include military battlefield communications, relief and emergency operations, environmental protection, taxi networks, and independent space communications. The ever-increasing need for MANETs has given rise to several security challenges, particularly with regard to the implementation of critical security applications. MANETs, on the other hand, are intrinsically unsafe owing to the fact that their wireless media is shared and there is no centralised authority to oversee them. The one-of-a-kind qualities of MANETs have given rise to brand new concerns about the design of security [23].

Threats may be posed to MANETs just as they can be posed to other forms of radio-based network technologies. These dangers include both external attackers from other countries and internal network abusers. As a result, many different forms of information, including data encryption, access control, identity management, and intrusion detection, are needed to safeguard these kinds of networks. This is a requirement for many different types of technology [21].

Wireless networks have their own unique set of challenges and needs for defense. These issues are caused by the characteristics of wireless networks, which may be broken down into the following categories [21]:



- Structures that are centralised and integrated, such as routers, are not always present in wireless networks. Because of this, their approaches to network security are often decentralised, dispersed, and reliant on the collaborative efforts of all network nodes.
- It can be challenging to keep track of mobile nodes in a wireless network due to the fact that they often relocate, particularly in big networks.
- In contrast to wired networks, wireless networks do not have any common defensive lines to protect their users. It is not necessary for an attacker to have direct physical access to the link in order to target any node from any direction.
- The vast majority of wireless routing systems include the nodes themselves performing the function of routers (this is especially true in ad hoc networks), and packets go via a variety of hops. Because of this, it is impossible to put complete faith in any node to perform a task like routing.

A wireless network's absence of a set topology and its restricted access to resources like electricity i.e. Power, processors, and memories are two further inherent characteristics that contribute to the existence of security flaws in the system.

In past few years, this network type i.e. Adhoc networks have gain many importance in certain application areas like military, civilian tasks, etc. Because of certain characteristics of ad hoc networks, an attacker has several possibilities to cause disruptions in these networks. These characteristics include the dynamic nature of the network structure, the mobility of the nodes, the requirement that the nodes trust each other in order to facilitate straightforward communication between them, the restriction of available power, the absence of centralised management to investigate behaviours and functions, and the haziness of the defensive boundaries. The following is a list of

characteristics of the MANET that contribute to its complicated operation [24][25]:

- It is not necessary to have a central administrator when using nodes because they may organize the internal network activities themselves.
- MANET is open to participation from a wide variety of wireless devices, which can join and begin exchanging data. So, this feature is referred to as Heterogeneity.
- In the same way that there is a finite amount of energy, there is also a finite amount of resources, which are shared with other devices.
- There are no restrictions on a node's ability to join or exit the network. As a result, there is no set standard for the number of nodes that should be present in a MANET.
- Due to the fact that mobile nodes are wireless devices, their battery life is restricted.
- It is impossible to have direct communication between two nodes that have been located at such a great distance from one another. As a result, the intermediate nodes are the ones that are utilized to move the packets from their source to their final destination.
- In a dynamic topology, individual nodes have the ability to freely enter and exit the network. As a direct consequence of this, maintaining the network is challenging, and route discovery must also be performed several times i.e. repeatedly.

**Results:**

Within ad hoc networks, the black hole assault is regarded as one of the most perilous forms of active attack. The action taken by the black hole node consists of replying to all path request packets, giving the impression that it possesses the most direct route to the target node, and then deleting all packets that it has received.

The network assumed here in this paper is representing certain scenarios:

- Normal Scenarios i.e. Without attack
- With attack Scenario

It was tried to generate and collect for analyzing the result on the basis of few list of parameters those are making direct impact on the performance. Name of these few parameters are Throughput (TH), Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), Normalized Routing Load (NRL).

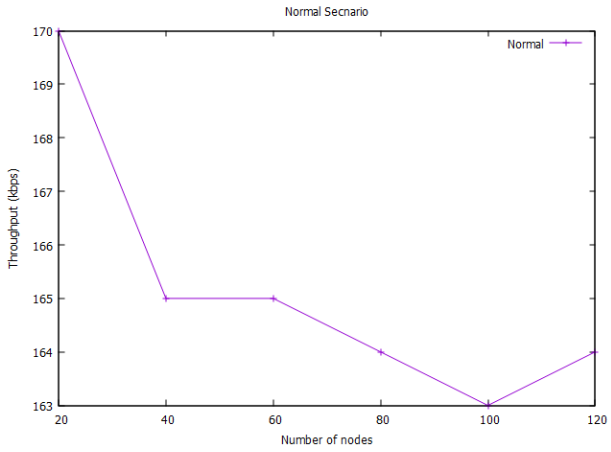


Figure 3: Graphical representation showing the normal scenario of network for Throughput as a Parameter

For Throughput as a parameter, experiment was performed and result values are collected. In Figure 3, scenarios are only assumed under normal conditions, actually when there is no existence of attack. This is also true that values showing in Figure 3 could vary depending from scenario to scenario, And the same is equally true for other parameters as well.

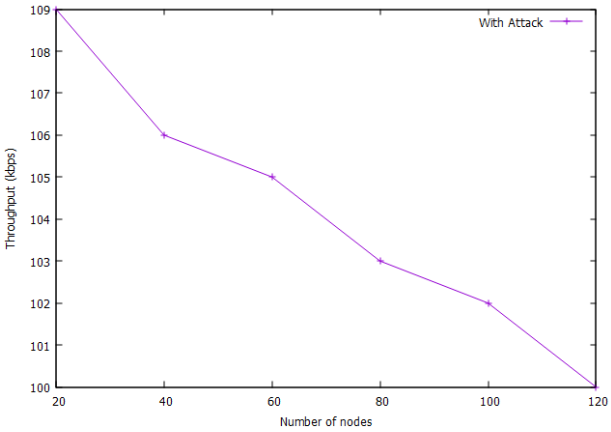


Figure 4: Graphical representation showing the scenario of network for Throughput as a Parameter in which Black Hole Attack is performed

In Figure 4, it can be easily monitored that the Throughput has affected and has decreased significantly, which means that malicious node

has made their impact in the network and Black Hole attack is successful to affect this network.

Similarly, this can also be observed for Packet Delivery Ratio i.e. PDR as a parameter also, that has received good results in a normal scenario, when actually the black hole node is not available and Black Hole attack is not implemented. Figure 5 can be checked to study this parameter. This figure shows the results those are obtained for the various scenarios depending upon number of nodes. In this result, the number of nodes taken are 20, 40, 60, 80, 100, 120. And as per these available results, good number of packets are being delivered in the network in the situation of no black hole attack.

But once the attack is implemented and the malicious node becomes active in the network then it starts affecting the packets and it becomes challenging to deliver the defined packets successfully. Figure 6 is showing such graphical representation in which due to Black Hole attack Packet Delivery Ratio is getting affected and there is a lot of variation in results on comparing it with Normal Scenario i.e. without attack. The PDR value which was approximately 90 (as per Figure 5) for 20 nodes is now at approximately 30 (as per Figure 6) for same number of nodes. This is directly showing the affect of Black Hole attack on the network because malicious node are targeting packets in this case. The same can also be observed for other number of nodes like 40, 60, 80, 100, 120 as per figures available in the paper.

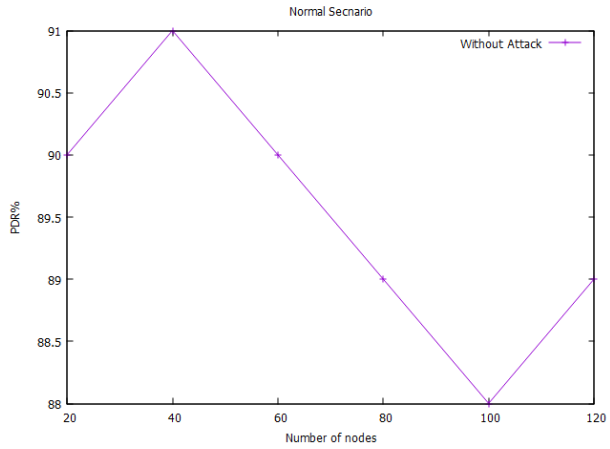


Figure 5: Graphical representation showing the normal scenario of network for Packet Delivery Ratio (PDR) as a Parameter

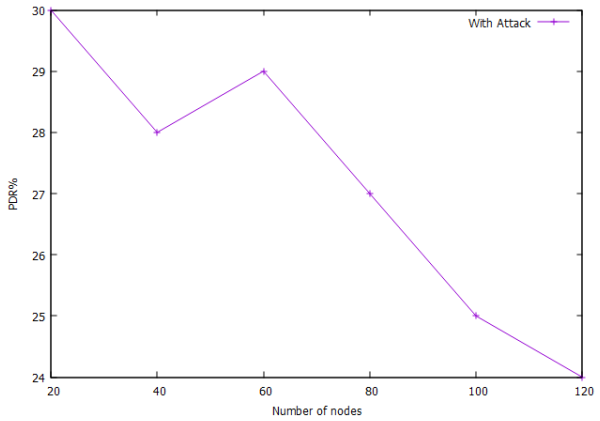


Figure 6: Graphical representation showing the scenario of network for Packet Delivery Ratio (PDR) as a Parameter in which Black Hole Attack is performed

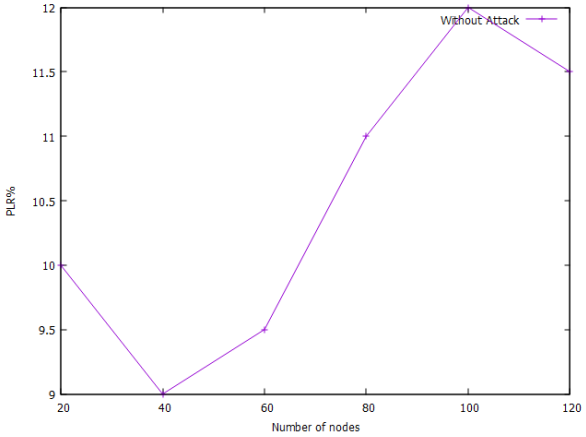


Figure 7: Graphical representation showing the normal scenario of network for Packet Loss Ratio (PLR) as a Parameter

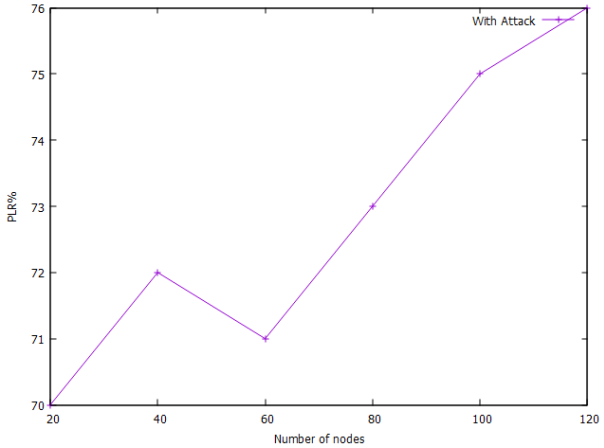


Figure 8: Graphical representation showing the scenario of network for Packet Loss Ratio (PLR) as a Parameter in which Black Hole Attack is performed

Figure 7 and Figure 8 are presenting the network scenarios for Packet Loss Ratio i.e. PLR. In proportion to the degree to which the PLR is reduced, the data transfer rate will increase, leading to improved network performance. As per this parameter, one can know about the packet loss. This is obvious that every network always wishes to achieve highest level of performance but due to loss of packets in the network, attaining this highest level of performance becomes challenging. Figure 7 is showing the representation in normal scenario conditions in which Black Hole attack is not yet implemented and one is trying to get the best PLR results. But Figure 8 shows the scenarios when Black Hole attack is implemented and accordingly due to this malicious node presence, loss of packets are increasing.

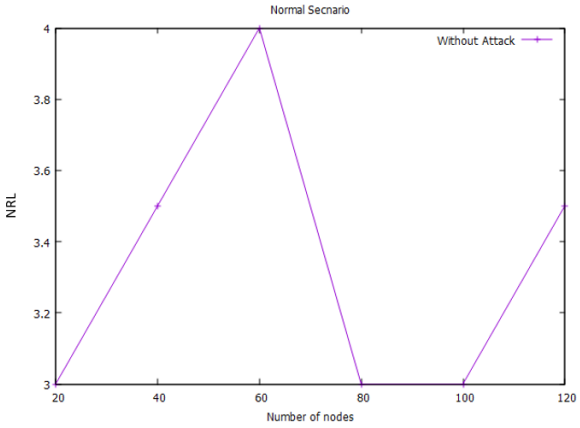


Figure 9: Graphical representation showing the normal scenario of network for Normalized Routing Load (NRL) as a Parameter

Regarding Normalized Routing Load (NRL) is also important to know. The routing procedure is required less frequently when the network topology is more consistent and undergoes fewer changes. This is because the routing tables stored in the nodes are less likely to become unstable and are more likely to remain unchanged. As a direct consequence of this, time and resources allocated to the network are used up in the process of transferring data packets rather than routing packets. As per Figure 9, one can check that NRL value is not much changing its value with respect to the number of nodes. But this change is very frequent, as per Figure 10, due to presence of malicious node and Black Hole attack. This means that burden on the network is regularly increasing during Black Hole attack which leads to result of decreasing network performance.

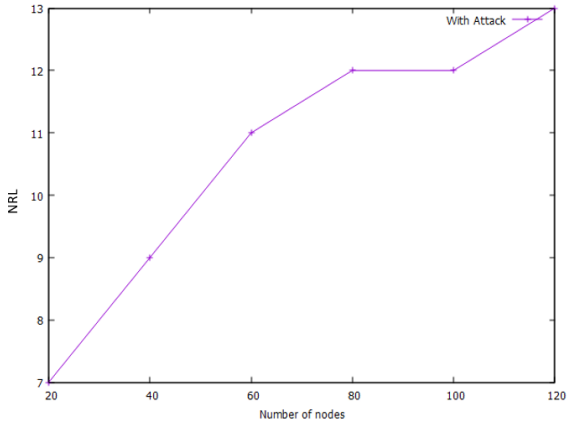


Figure 10: Graphical representation showing the scenario of network for Normalized Routing Load (NRL) as a Parameter in which Black Hole Attack is performed

## Conclusions:

The main objective of this paper is to check and analyze the affect on the performance once the nodes will have an existence of malicious node among them. In the results shown above, level of affect can be checked for certain performance parameters. Almost every parameter is facing challenges while the attack has started its functioning in the network. Therefore, there is a strong need to understand the network, its nodes and requirements of user so that accordingly the affect of Black Hole attack can be reduced.

## References

1. Y. Ko, N.H. Vaidya, "Flooding-Based Geocasting Protocol for Mobile Ad Hoc Networks", Mobile Networks and Applications; Dec 2002; 7, 6; ABI/INFORM, Global pg. 471.
2. A. Qayyum, L. Viennot, A. Laouiti, "Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks", in Proceedings of the 35th Hawaii, International Conference on System Sciences – 2002.
3. C.M. Cordeiro and D.P. Agrawal, "Mobile ad hoc networking", GBR Research Center for Distributed and Mobile Computing, ECECS, University of Cincinnati.

4. L.M. Feeney, "Lecture Notes on Introduction to MANET Routing". Available: http://www.nada.kth.se/kurser/kth/2d1490/05/lectures/feeney_mobile_adhoc_routing.pdf.
5. S. Pleisch, M. Balakrishnan, K. Birman, R.V. Renesse, "MISTRAL: Efficient Flooding in Mobile Ad-hoc Networks", MobiHoc'06, May 22–25, 2006, Florence, Italy.
6. Gupta K. Anuj, Sadawarti Harsh and Verma K. Anil, Review of various routing protocols for MANETs, Inter. J. Info. and Ele. Eng., 1 (2011), 251 – 259.
7. Goyal Priyanka, Parmar Vinti and Rishi Rahul, MANET: vulnerabilities, challenges, attacks, application, Inter. J. Computational Eng. & Management 11(3) (2011).
8. Arti and S. S Tyagi, Study of MANET: Characteristics, challenges, application and security attacks, Inter. J. Adv. Research in Comp. Sci. and Soft. Engineer., 3(5) (2013), 252-257.
9. A. K. Luhach and R. Luhach, Research and implementation of security framework for small and medium sized E-commerce based on SOA, J. Theoretical and Appl. Infor. Tech., 82(3) (2015).
10. Luhach, Ashish Kr, Sanjay Kr Dwivedi and Chandra Kr Jha, Applying SOA to an E-commerce system and designing a logical security framework for small and medium sized E-commerce based on SOA, Computational Intelligence and Computing Research (ICCIC), 2014 IEEE Inter. Conf. on IEEE, 2014, pp. 1-6.
11. Y. Yi, M. Gerla and T.J. Kwon, "Efficient flooding in ad hoc networks using on-demand (passive) cluster formation".
12. Sharma Manmohan, Neha, "Step verification for detection of black hole attack in MANET", Inter. Conf. Adv. in Appl. Engineer. & Tech., 10(2) (2015).
13. Raja Karpaga Brinda and P. Chandrasekar, Defense strategy for the detection of black hole attack in Dsr, Inter. J. Engineer. Sci., Journal Anu Books, 5(2011), 36-47.
14. Jaspinder Kaur and Birinder Singh, "Detect and isolate black hole attack in MANET using AODV Protocol", Inter. J. Adv. Res. Comp. Eng. & Tech. 3(2) (2014), 334-338.
15. Nath Ira and Rituparna Chaki, "BHAPSC: A new black hole attack prevention system in clustered MANET", Inter. J. Adv. Research in Comp. Sci. and Soft. Eng., 2(8) (2012), 113-121.
16. N. Patel, A. Dadhaniya, "Detection of Black Hole Attack in MANET using Intrusion Detection System", International Journal of Advance Engineering and Research Development (IJAERD, Vol 1, Issue 5 May 2014.
17. H. Deng, W. Li, and D.P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazines, vol. 40, no. 10, October 2002.
18. P.N. Raj, P.B. Swadas, "DPRAODV: A Dyanamic Learning System against Black Hole Attack in AODV Based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, pp 54-59 2009.
19. N. Mistry, D.C. Jinwala, M. Zaveri, "Improving AODV Protocol against Black hole Attacks", in Proc. of the International Multi Conference of Engineer and Computer Science, Vol. 2, 2010.
20. A.A. Bhosle, T.P. Thosar and S. Mehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol.2, No.1, February 2012.
21. Neha, M. Sharma, "A Survey on Black Hole Attack Detection and Prevention Techniques", International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol.3, Issue IV, April 2015.
22. K. S. Chavda and A. V. Nimavat, Removal of black hole attack in AODV routing protocol of MANET, 4th ICCCNT - 2013, July 4 -6, 2013, Tiruchengode, India, IEEE-31661.
23. F. R. Yu and H. Tang, "Distributed node selection for threshold key management with intrusion detection in mobile ad hoc networks," Wireless Networks, vol. 16, no. 8, pp. 2169–2178, 2010.
24. Farahani G., "Black hole attack detection using K-nearest neighbor algorithm and reputation calculation in mobile ad hoc networks", Security and Communication Networks, 2021.
25. A. Vij and V. Sharma, "Security issues in mobile adhoc network: a survey paper," in Proceedings of the International Conference

on Computing, Communication and Automation, Greater Noida, India, April 2016.
26. H.S. Bedi, K.K. Sharma, and R. Gupta, "A Review Paper on Performance Analysis of IEEE 802.11 e", 1st International Conference on Computing, Communications, and Cyber-Security (IC4S 2019), 2020, pp. 47-56.
27. Z.G. Khaki, and H.S. Bedi, "Transient correction using EDFA: in-line optical fibre with feedback", International Conference on Computing Sciences, 2012, pp. 233-238.
28. Bedi, Harpreet, Kamal Kumar, and Gupta Raghav. "A review paper on improving the network efficiency of IEEE 802.11 e networks." Intelligent Circuits and Systems (2021): 206-211.
29. Harpreet Bedi, Kamal Kumar Sharma; Analyses of CSMA/CA Protocol Without Using Virtual Channel Sensing in DCF Mode, Global Emerging Innovation Summit (GEIS-2021) (2021) 1: 484.
30. Harpreet Singh Bedi, Kamal Kumar Sharma, Shakti Raj Chopra, and Balraj Singh Analysis of QoS parameters using different back off window algorithm in the IEEE 802.11e networks, Advances and Applications in Mathematical Sciences Volume 21, Issue 10, August 2022, Pages 6147-6157 © 2022 Mili Publications, India
31. Harpreet Singh Bedi, Utilization of a Wireless Network Performing CSMA/CA with Random Backoff Algorithm Published under licence by IOP Publishing Ltd Journal of Physics: Conference Series, Volume 2327, 4th International Conference on Intelligent Circuits and Systems 07/04/2022 - 09/04/2022 Online