JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Vol.-16, No.-3, March (2021) pp 13-30 ISSN (Print) 0973-8975

IMPACT OF BLACK HOLE ATTACK ON THE PERFORMANCE OF DYNAMIC SOURCE ROUTING AND OPTIMIZED LINK STATE ROUTING PROTOCOLS IN MANETS

Waqas Khan[1], Vishwesh Laxmikant Akre[2], Khalid Saeed[3], Asif Nawaz[4] Tariq Bashir[5], Adil Khan[6], Naveed Jan[7], Sheeraz Ahmed[8], Zia Ullah Khan[9]

[1]Deptt of Computer Science, IBMS, University of Agriculture Peshawar, Pakistan

[2]Computer and Information Science, Dubai Women's College, Higher Colleges of Technology (HCT), Dubai, UAE

[3]Deptt of Computer Science, Shaheed Benazir Bhutto Univ Sheringal, Pakistan

[4]Faculty of Electronics, Higher Colleges of Technology, Dubai, UAE

[5]Deptt of Electrical Engineering, COMSATS University Islamabad, Pakistan

[6]Department of Computer Science, AWKUM University, Pabbi Campus, Pakistan

[7]Deptt of Information Engg Tech, University of Technology, Nowshera, Pakistan

[8]Department of Computer Science, Iqra National University Peshawar, Pakistan

[9]Directorate of Science & Technology, Govt. of KPK, Peshawar, Pakistan

Corresponding Author: Dr. Sheeraz Ahmed

Email: sheerazahmed306@gmail.com

https://doi.org/10.26782/jmcms.2021.03.00002

(Received: January 21, 2021; Accepted: March 15, 2021)

Abstract

Mobile Ad-Hoc Networks (MANETs) are a collection of mobile nodes which are free to move from one place to another place without a central control entity. In MANETs the nodes are dependent on each other and the communication among mobile nodes is multi-hop due to which there are security issues in the MANETs protocols. Optimized Link State Routing (OLSR) and Dynamic Source Routing (DSR) protocols are mostly used as proactive and reactive routing protocols in MANETs. This research work analyzed the performance of the OLSR and DSR protocols in the presence and absence of black hole (BH) attack in terms of throughput, end-to-end delay, packet delivery ratio (PDR), and network load in various scenarios using OPNET Modeler 14.5 simulator. The results obtained in this research show that BH attack significantly degrades the performance of both DSR and OLSR protocols but due to the reactive nature of DSR routing protocol the performance is more degraded in DSR routing protocol as compared to OLSR routing protocol in the presence of BH attack.

Keywords: MANETs, Ad-Hoc Routing Protocols, OLSR, DSR, Malicious Nodes, Black Hole Attack.

I. Introduction

Mobile Ad-Hoc Networks (MANETs) are a group of wireless nodes which can be set up dynamically anytime and anywhere without using any pre-existing network infrastructure. It is a self-governing structure of moveable nodes linked using a wireless link. MANETs is a network containing a collection of mobile nodes which is competent enough of interconnecting through every node not wanting a central management system. Furthermore, Ad-Hoc networks containing sets of mobile nodes collaborate by exchanging information on behalf of mutual trust to let communications outside through the control system [XVIII].

Some ad-hoc network protocols which have been designed and developed for the MANETs are DSDV, OLSR, ABR, AODV, DSR, etc. It's a form of Ad-Hoc networks created on 802.11 IEEE standard which is interconnected on separate and scatter situation which has no significant system. MANETs routing protocols have unsettled network size which increases the range and size of the node for examining flexibility and arbitrary changes in their positions in the network mechanism [XXIII]. MANETs do not have any fixed topology, in which the nodes are highly moving in the unrestricted area. Sometimes in Ad-Hoc Networks mobile nodes may link the network while other nodes can depart. Therefore, nodes consigned freely to travel randomly in all routes.

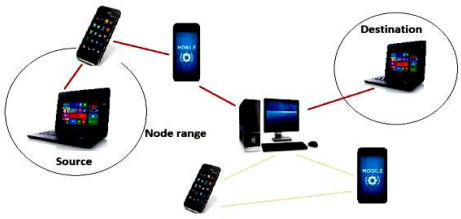

Fig. 1: Ad-Hoc Network [III]

A. Security Issues in MANETs

This research focused on security issues in MANETs and recommended security features in routing protocols in MANETs. MANETs are extensively used but it has certain vulnerabilities. Thus, they need some security mechanisms to protect them from such sorts of problems. Some of the main security problems that occurred in MANETs are discussed as follows:

Scalability

The numbers of wireless nodes in MANETs remain unorganized. Every node inside the radius of the network can participate in the operation of the network. Thus, an attacker can utilize these parameters to have an approach to the resources of the network.

Exposed Wireless Channel

In MANETs communication is done using the medium of air in its place of cables. So, definitely, an attacker can be able to access the network through this medium.

Absence of Main Point Controller

Access viewpoint exists in the ad-hoc network such as a router, entrance points, etc do not exist in MANETs, which observers the network's traffic surpasses after it. Thus, the communication between the wireless nodes in the MANETs is taking place without including the central station controller and every mobile node performs as a router that can forwards and receives the coming packets. So, this deficiency of central control leads MANETs more vulnerable to attack.

Resource Limitations

Every node in MANETs has limited resources just as bandwidth, computational ability, battery lifetime, etc. Thus, an intruder can easily consume these resources which results in it inaccessible to execute the node processes.

Flexibility

Such like each node in MANETs can travel freely, so the nodes could be connected or departed the wireless networks anytime without sharing the information with further mobile nodes in the communication channel. Therefore, it gives a chance to the attacker for accessing the network channel through a vague node.

Active Network Topology

MANETs topologies modify vigorously. Thus, the information packet could be followed dissimilar routes to reach from starting nodes to endpoint nodes. Therefore, an intruder could be definitely present himself on every route [VIII].

B. Routing Protocols in MANETs

The procedure of choosing a path in the network is called routing. It is the process that is generally accomplished by a dedicated device named a router. Routing is an act that shows moving a data packet through an inter-network from a starting point to the endpoint. In MANETs, protocols identify exactly how a router interconnects through each other's, and broadcasting data information that allows them to choose paths amongst any two mobile nodes that exist in the networks.

No, any particular protocol is appropriate for entirely computer networks impeccably. Such types of protocols are being selected accordingly by their network features, as well as dimensions, concreteness and flexibility of mobile node. Hence this research emphasizes the basis of the performance analysis of ad-hoc routing protocols, which specifically come under two categories, proactive, reactive protocols (DSR, OLSR).

DSR Protocol

DSR is a popular reactive routing protocol in MANETs. It is a well-organized routing protocol and it is designed for use in multi-hop ad-hoc networks [XI]. DSR routing protocol permits each mobile node to dynamically conclude the paths from sender to the receiver node.

OLSR Protocol

OLSR is a proactive routing protocol. In this protocol, every mobile node is used for holding routing table information to each and every mobile node in the

communication networks. Therefore, the route will be directly accessible continuously as soon as required. OLSR is a basic link-state protocol and it is an optimized form in which the topologies change causes the flooding of the topologies information's to entirely accessible hosts in the computer networks. OLSR optimized the reactivity of topological, change by dropping the highest time intervals for periodic handling messages broadcast.

C. Black Hole (BH) Attack in MANETs

The BH is a type of network layer attack which can occur in MANETs. BH attack is a well-known and major attack in the MANETs environment [XV]. During this attack, the functioning and competence of MANETs reduce vividly by the mischievous specific node. So this attack disturbs functionalities of the ad-hoc network by drops all the incoming data packets. This network layer attack works base on two dissimilar stages; firstly, it advertises a false route that contains a malicious node. Secondly, it dropped all incoming data packets [XXII].

As a malicious, node advertised itself on utilizing its routing protocols for taking the shortest route to the receiver node or to that data packet it wants to interrupt. After that this unfriendly mischievous node broadcast its accessibility of new route unrelatedly of examining her routing table information. So in this technique, the malicious node will each time have the accessibility in responding to the routes request and therefore they intercept the incoming data packets and hold them. The attacker node response will be accepted by the demanding node before the reaction of response from the sender node therefore an attacker and the fake path is generated. Once this path is created, right now it's upon the node whether to drops every data packet or forwards it to the unidentified addresses. Following is the process that how an attacker node fixes in the data paths differs. As shown in Figure. 2 that how BH problems rise, now node (A) wants to send a data packet to the node (D) and originate the routes discovering procedure. Thus if the node (C) claiming that it has the fresh sufficient route to the destination node as quickly as it received the RREQ packet then it will send the reply to the node (A) instead of some other nodes.

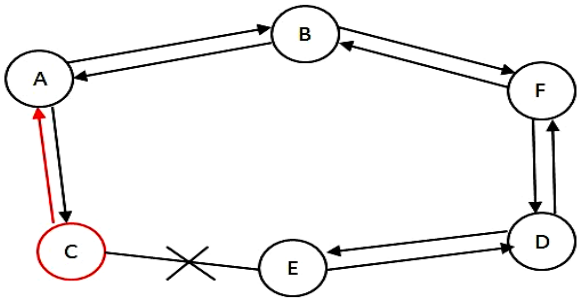

Fig. 2: BH Attack [IV]

Since node (A) will consider that this route is active and hence active route discovering process is completed. So therefore node (A) will ignore all other incoming replies and node (A) will be starting to send data packets, to node (C). Therefore in this manner, all incoming data packets should be discarded or consume [XII].

MANETs is the main focus of research community since more than one decade. Authors in [X] performed an analysis of malicious nodes in MANETs. Researchers in [XIX] performed a comparison of different routing protocols in MANETs. The rest of the research paper is organized as follows. Section II includes the relevant literature, section III explains the simulation environment, section IV discusses the results in detail, section V concluded this research, section VI contains future research directions and at the end there are references.

II. Literature Review

Authors in [XXIII] proposed a trust model known as Generalized Trust Model (GTM) which is generalized for different routing protocols in MANETs. GTM offers lightweight communication, self-adaptability, effective identification as well as removing malicious nodes in the process of routing. GTM has been applied to different proactive, reactive and geographic routing protocols in MANETs. Simulation in this research has been done using NS-2 simulator. Results obtained in this research revealed that the proposed model improves the performance of the network in terms of throughput, end to end delay, packet delivery fraction and routing load when GTM was compared with other models.

Authors in [XX] presented vulnerabilities in OLSR routing protocol versus cooperative misbehavior nodes in MANETs. The main concept of the OLSR routing protocol is that it uses a multi-point relay. The purpose of using a multipoint relay is to reduce the number of duplicated broadcasted packets in the network. The authors proposed an optimized scheme known as neighbor-trust-based. The basic idea used in this research is the collaboration among neighbors for detecting the misbehavior nodes. The idea in this research has been implemented using the NS-2 simulation tool.

Authors in [V] proposed a mechanism for defending as well as detecting collaborative against DSR routing protocol using elliptic curve digital signature algorithm. The proposed mechanism is suitable for MANETs environment because it provides efficient transmission, computation and is very resistant against the collaborative attack. The authors in this research revealed that this research is unique in the sense that existing relevant research did tackle either single attack or uncoordinated attacks.

Authors in [VI] proposed a security mechanism against routing as well as DOS attacks. These attacks consume the capacity of the link and also drop packets. The authors in this research proposed the prevention and detection mechanism of these attacks. The proposed mechanism has been applied to the OLSR routing protocol in MANETs. The results obtained in this research revealed that the proposed mechanism provides secure communication and improves the performance of the network in terms of throughput, packet delivery ratio and routing load.

Authors in [XIV] compared the performance of cryptographic solutions which are specifically designed for MANETs based on the chaotic maps and RSA. Results obtained in this research revealed that RSA is the best security solution but it has more time complexity. The time complexity has a negative effect on the performance of the network especially in terms of end-to-end delay. Therefore it has

been concluded in this research that chaotic map based cryptographic technique is good alternative to the RSA because it provides appropriate security with less overhead.

Authors in [VII] evaluated the impacts of BH attacks on the performance of the mobile ad-hoc network. They used network simulator NS-2 for BH attack, and also measured the packet deficiency in the ad-hoc networks with and without the presence of BH attack. They further suggested an easy solution besides the BH attack. Their way out improve the ad-hoc network performing in the existence of BH problem by approximately 19%.

Authors in [XXIII] investigated MANETs mainly reactive and proactive routing protocols such as TORA, DSR, AODV and OLSR. Their key concern about the ad-hoc network is that the damage of connection at particular moments and regeneration, of connection at a specific position as it comprises of routers, which exist mobiles in character. Their result revealed that OLSR and AODV proficient for greater data packet delays and network load as associated with TORA. That's why because of the localization, the method used in TORA. On the other side when segment interruption is considered in both protocols OLSR and AODV are executed very constantly and launched rapid links amongst mobile nodes not including any extra delays. Though, TORA indicates high end-to-end delay because of the creation of impermanent loops inside the networks.

Authors in [II] investigated the three ad-hoc routing protocols namely DSR, AODV and DSDV. AODV is a reactive routing protocol and is better since its ability to retain connections by periodic exchange of communication, which is essential for TCP base network traffic and AODV executes probably. Delivered virtually totally data packets at little nodes flexibility, and dropping to converge, when nodes movement increases. On the other hand, the DSR routing protocol remains very well at an entire flexibility rate and movements. DSDV executes nearly as well as DSR protocol.

Authors in [XIII] investigated various kinds of network attacks in MANETs. Their method was extremely protected because they mostly focused on malicious nodes, detecting mischievous network links and numbers of substantial data packets dropping in the network links. Their implementation is on detection and avoidance of mischievous mobile nodes by starting packets lose and incoming messages damaging harmful attacks, by employing a semantic protection method. They use an algorithm to identify intruder nodes mischievous links and starting attacks to avoid these intruders from transmission networks. The estimate outcomes showed that the methodology successfully identified and avoids such types of intruder nodes and connections in MANETs.

Authors in [I] evaluated the performance of DSR, AODV and OLSR for dissimilar numbers of instantaneous video broadcasts. They use end-to-end delay, routing overhead, packets delivery ratio and packet delay variation jitter as estimating metrics. Their outcomes specify that the DSR routing protocol outperforms OLSR and AODV in terms of packet delay variation and end-to-end delay and observes to be the best effective ad-hoc routing protocols when interactive program traffic and particularly video traffics are measured.

Authors in [IX] evaluated that BH attack is prevented through the service of an endpoint sequence number which is a transfer by the RREP nodes. When a huge change is accounted for, amongst the sender mobile node sequences number and the intermediary node sequences number at that point that node is confirmed as attacker node. Their simulations outcome show improved performance in terms of end-to-end delay and PDR.

Authors in [XXII] concluded that in MANETs the BH attacks established on generating false RREP in reply to receives RREQ data packets. Though further harmful attack which is named a deep BH attack is presented and estimated. In this attack, a fake RREP message is broadcasted more powerfully than the previous one. They used NS-2 for simulation results. This represents that deep BH attacks are associated with a normal BH and self-cantered mobile nodes are extra destructive and lead to networks' rejection of services. The outcome of this attack is weakening in the numbers of ad-hoc networks end-to-end delay and routing data packets especially associated with the selfless mobile node. In contrast to a normal BH attack, the simulation result of different attacks account for the impact of BH attack, on more destructive network structures.

Authors in [XII] examined the effect of BH attacks on the networks performing in relationships of load, delay, and throughput of DSR, OLSR, and AODV ad-hoc routings protocol. The simulation outcomes demonstrate that's when there were malicious nodes in the networks it drops the whole operation of the ad-hoc networks by interrupting the mobile nodes which are sent from source to destination node when the data packets being routed. They examine that the effects of the malicious node on the communication networks extremely interfere with the performances which are indications of more information damage.

Authors in [XVIII] investigated the functioning of the ad-hoc routing protocol in mobile network conditions. Their objective of research work out is to calculate the applicability, of these ad-hoc protocols in dissimilar mobile traffics circumstances. They deliberated topologies-based ad-hoc routing protocol. Inside topologies base, ad-hoc routing protocols both reactive protocols AODV, DSR and proactive protocol DSDV are used for the analysis. They discovered that operations of the three topologies-based ad-hoc routing protocols, which are both reactive (AODV and DSDV) and proactive protocol DSR increases their node number. They also discovered their performances based on packet delivery ratio, delay and throughput.

Authors in [III] incline to focus on the common attacks within MANETs that differ in their essence like Sleep Deprivation attack DOS etc. They adopt several methods for the detection of different kinds of attacker nodes. Hence there were massive numbers of methods to identify several kinds of attacks, in ad-hoc network securities. They suggested modifying the CBDS method to address another type of attack in MANETs just similar to DOS attacks and sleep deprivation attacks.

III. Preliminaries

This section includes the system model, buffer constraints of mobile nodes, and performance evaluation parameters.

A. System Model

The system model consists of a network model and a traffic model.

Network Model

In this research, two different routing protocols in MANETS are used such as DSL and OLSR. Simulation has been done using the OPNET simulator. There are 30 wireless mobile nodes deployed in the MANETs environment. The simulation area set in OPNET is 1000m x 1000m. The parameters used to carry out simulation in this research are reflected in table 1.

Table 1: Simulation Parameters

Simulator	OPNET
Routing Protocols	DSR, OLSR
Number of Nodes	30
Mobility Model	Random waypoint
Simulation Time	200 sec
Simulation Area	1000m × 1000m
Nodes Speed	10m/sec
Type of Traffic	Constant Bit Rate (CBR)

Traffic Model

The type of traffic used to simulate this research is the constant bit rate. The movement of the mobile nodes is random as per the random waypoint mobility model and the movement of nodes has been set to 10m/sec as shown in table 1.

B. Buffer Constraints of Mobile Nodes

In this research, the mobile nodes and BH nodes have different buffer constraints. The buffers of the mobile nodes have been set to the optimal value whereas the BH nodes have minimum buffer space because the function of the BH node is to drop the packets instead of forwarding them.

C. Performance Evaluation

To evaluate the performance of DSR and OLSR routing protocols in MANETs the following parameters are used.

Throughput (bits/s)

It is the number of packets sent and the total numbers of packets successfully transferred to their desired endpoint per unit of time which defines the normal speed of successfully transferred messages above the transmission network. It also measures the efficiencies of the communication network [XVI].

Packets Delivery Ratio (PDR)

Packet delivery ratio is described as the fractions of the total received information packet next to the endpoint over the number of information packets delivered by the starting points. It's an essential metric, in a communication network. This metric tells how reliable the protocol is [IX].

(PDR) = (Total Packets Received/Total Packets Sent) × 100

Average End-To-End Delay (sec)

The average end-to-end delay indicates how much longer it will take a data packet, to travels from starting node to endpoint node. Therefore in route detection, propagation delay queuing and transfers time contains delay [XVIII]. End-to-end delay is calculated as follows.

End to End Delay = (Packets receiving time - Packets initialization time)

Network Load (Bits/sec)

The Network load, characterizes the overall loads in (bit/sec) submit to wireless LAN layer by totally high layers in entirely WLAN nodes of the communication networks. So network load is defined as when there is a lot of data packets arrived at the communication networks and that is not easy for the network to handles completely the incoming data packets [XVII].

IV Results and Discussion

In this research four metrics are calculated for every scenario to evaluate the performances of OLSR and DSR protocols in the presence and absence of BH attack.

A. Throughput Analysis

It is defined as the number of data packets sent and a total number of data packets successfully transmitted towards their desired endpoint in each unit of time. It explains the average rates of successful information transferred over a transmission network. It also measures the capability of the organization, and it is measured in "bps".

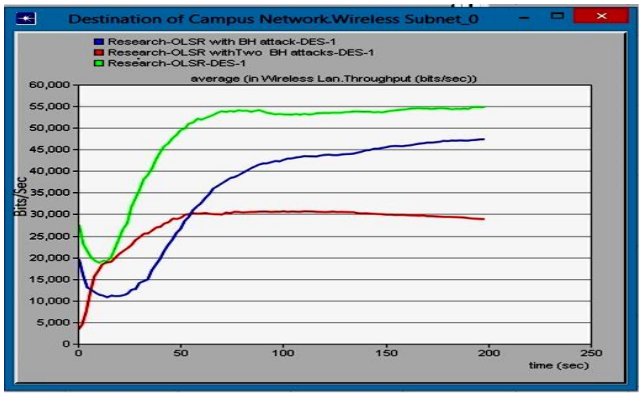

Fig. 3: Results simulation of throughput for "normal" OLSR besides single and double BH attacks

Figure 3 demonstrates the throughput, for the "normal" OLSR routing protocol amongst the source node and destination node besides single and two BH attacks within the transmission system. Their average throughput is analyzed for normal, OLSR is calculated approximately 52768.64 (bps) if there were single BH node in transmission system their "throughput" slightly decrease with an estimate of 40973.08 (bps) and when there are two malicious nodes the throughput further decreases which are calculated as 27744.93 (bps).

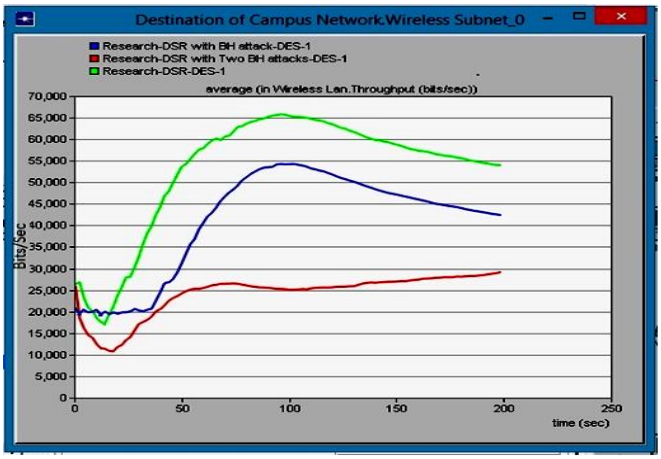

Fig. 4: Simulation results of throughput for "normal" DSR besides single and double BH attacks

Figure 4 shows the throughput for the "normal" DSR routing protocol amongst the source node and destination node besides single and two BH attacks within the transmission system. Their average throughput is analyzed for normal, DSR is calculated approximately as 48115.07 (bps) if there were one BH node in transmission system their "throughput" slightly decline with an estimate of 35792.04 (bps) and when the malicious nodes increase from one to two then the throughput further decreases which are calculated as 24119.61 (bps).

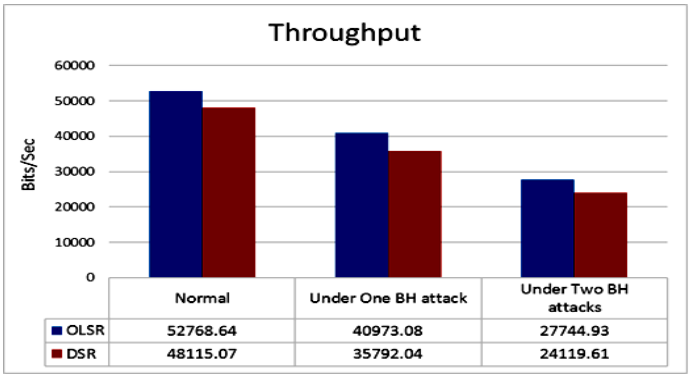

Fig. 5: Average throughput for OLSR and DSR bits/sec

Figure 5 specifies the simulations results of throughput, of OLSR in normal is greater than DSR under one malicious node. DSR protocol further decreases as related to OLSR routing protocol in the system. The declines in the throughput DSR protocol are further decreased from OLSR when the malicious node that exists within the system rises to two. Since, the existence of malicious mobile nodes, which execute the BH attack within transmission networks permits a lesser number, of data packets would be delivered efficiently to their desire endpoint.

B. Packet Delivery Ratio (PDR) Analysis

It is described as the fractions of overall received information packets, to the endpoint above the total numbers of information packets, sent through the starting point. It is a significant "metric" in the transmission network. This metric tells how reliable the protocol is.

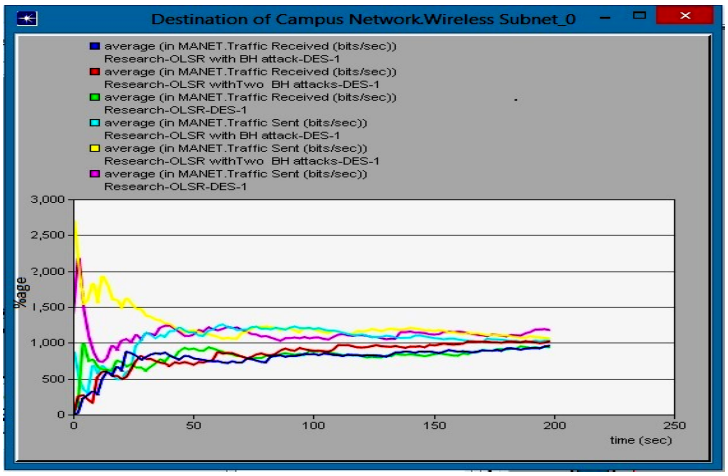

Fig. 6: Simulation results of PDR for "normal" OLSR besides single and two BH attacks

Figure 6 illustrates the relationship of PDR for the "normal" OLSR routing protocol amongst the source node and destination node besides single and two BH attacks within the transmission system. Their aver of PDR is analyzed for normal, OLSR is calculated approximately 98% if there were single BH node in transmission system their PDR slightly decrease with an estimate of 81% besides 19% of data deficiency within communication system and if there were two BH nodes in the transmission then the PDR further decreases which analyzed as 73% besides 27% of data deficiency occurred within the transmission system.

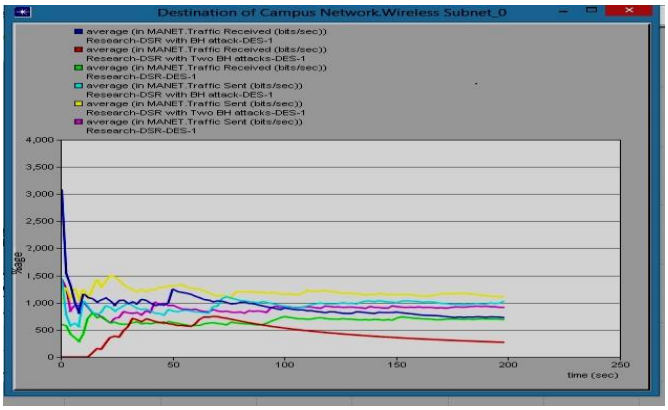

Fig. 7: Simulation results of PDR for "normal" DSR besides single and two BH attacks

Figure 7 explains the relationship of PDR for the "normal" DSR routing protocol amongst the source node and destination node besides single and two BH attacks within transmission networks. Their aver of PDR is analyzed for normal, DSR is calculated approximately 93%, if there is one BH node in transmission system their PDR slightly decrease with an estimate of 75% besides 15% of data deficiency occurs in the transmission system and if there were two BH nodes in the transmission then the PDR further decreases which examined as 67% within 33% of data deficiency occurs in the transmission system.

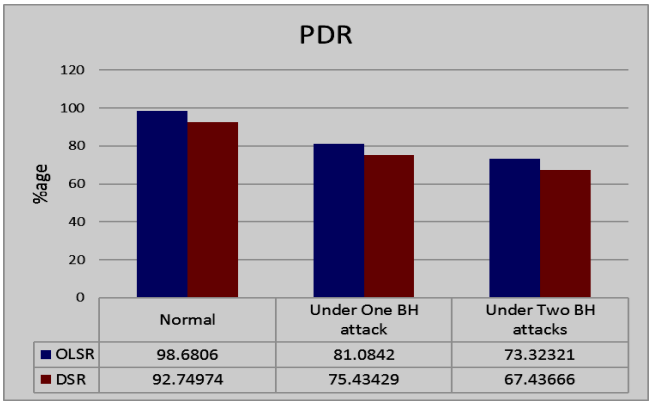

Fig. 8: Packet Delivery Ratio (Pkt/sec) of OLSR and DSR

Figure 8 specifies the simulation result which determines PDR of DSR protocol decreased as compared to Normal OLSR under one malicious mobile node. DSR routing protocol slightly decreased when compared with OLSR protocol within the system, and when the malicious nodes increased to two DSR further decreases from OLSR.

Therefore it determines that when the BH node increases in the transmission networks the PDR drops. As the existence of BH nodes within the system makes lesser numbers of data packets reach their final endpoint.

C. End-To-End Delay Analysis

End to End Delay indicates that how much time a data packet would take when it passes from starting node to endpoint node. It contains delay using propagation delay, transfer time, route discovery and queuing. It is a suitable metric for understanding the delay, which is produced when discovering a route from starting point to an endpoint.

End to End Delay = Packet receiving time – Packet initialization time

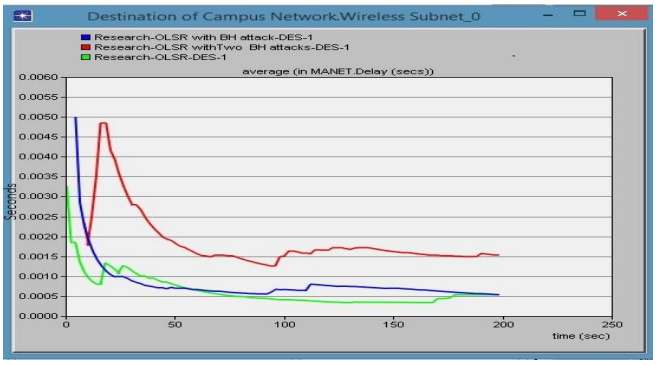

Fig. 9: Simulation results of delay for "normal" OLSR besides single and two BH attacks

Figure 9 clarifies the delay, for the "normal" OLSR routing protocol amongst the source node and destination node besides single and two BH attacks within the transmission system. Their aver of delay is analyzed for normal, OLSR is calculated approximately 0.000635 sec if there is a single BH node in transmission system their delay slightly increased with an estimate of 0.000788 sec, and when there are two malicious nodes the delay further increased which is calculated as 0.001779 sec.

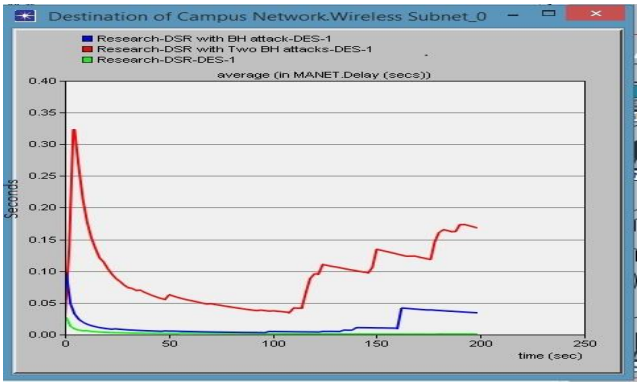

Fig. 10: Simulation results of delay for "normal" DSR besides one and two BH attacks

Figure 10 reveals the delay, for the "normal" DSR routing protocol amongst the source node and destination node besides single and two BH attacks within the transmission system. Their aver of delay is analyzed for normal, DSR is calculated approximately 0.002171 sec if there were single BH node in transmission system their delay slightly increased with an approximation of 0.014499 sec, and when there are two malicious nodes the delay further increased which is calculated as 0.096003 sec.

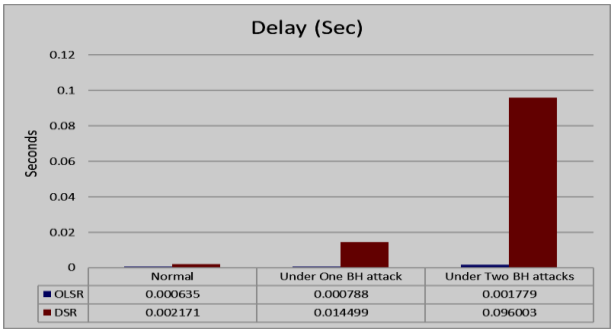

Fig. 11: OLSR and DSR End-to-End delay (sec)

Accordingly, to the simulation analysis, the average end-to-end delay increased of DSR as associated to normal OLSR protocol in the presence of one BH attack, end to end delay more increased of DSR than OLSR routing protocols. The end-to-end delay is more increases when the numbers of BH nodes rise to two as of DSR protocol than OLSR protocol in the network.

This increase in delay within the situation of BH attack, which happens in the presence of malicious attacker nodes that's why the data packets can't reach their final endpoint node.

D. Network Load Analysis

The network load signifies the overall loads in (bit/sec) that submit to the "wireless LAN" layer, through the overall upper layer in entire WLAN mobile nodes in the transmission networks. Once there is more data traffic arriving upon the transmission networks, which is complicated in support of transmission system to manage completely that traffic, that's why it is named as "network load".

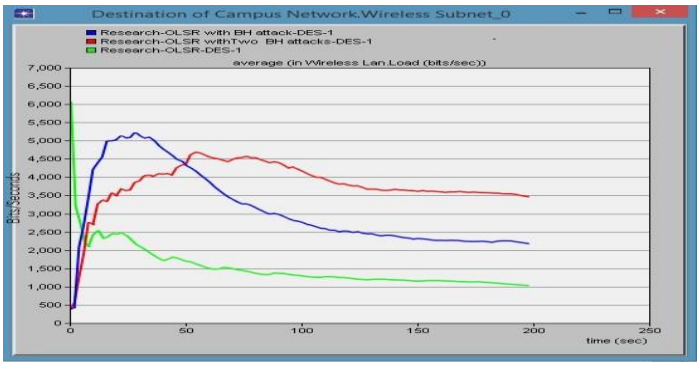

Fig. 12: Network load (bit/sec) with single and two BH attack represents normal OLSR

Figure 12 enlightens the network load, for the "normal" OLSR routing protocol amongst the source node and destination node besides single and two BH attacks within the transmission system. Their average of network load is analyzed for normal, OLSR is calculated around 1529.755 (bps), if there were single BH node in transmission system their network load slightly increases with an estimate of 3087.675 (bps), and when there are two malicious nodes the network load further increases which calculate as 3779.357 (bps).

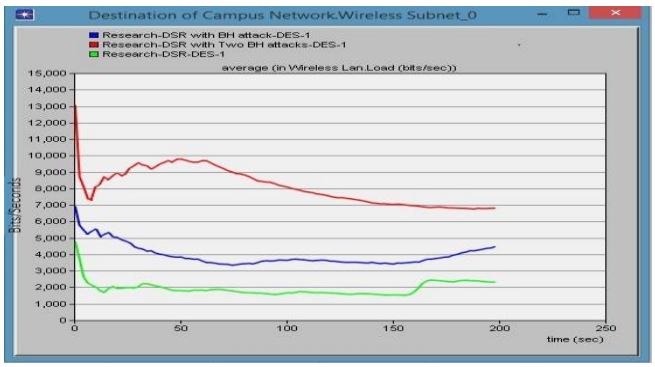

Fig. 13: Network load (bit/sec) with single and two BH attack represents normal DSR

Figure 13 clarify the network load, for the "normal" DSR routing protocol amongst the source node and destination node besides single and two BH attacks within the transmission system. Their average network load is analyzed for normal, DSR is calculated about 1937.004 (bps), if there are single BH node in transmission system their network load slightly increased with an estimate of 3950.589 (bps), and when there are two malicious nodes the network load further increased which is calculated as 8103.456 (bps).

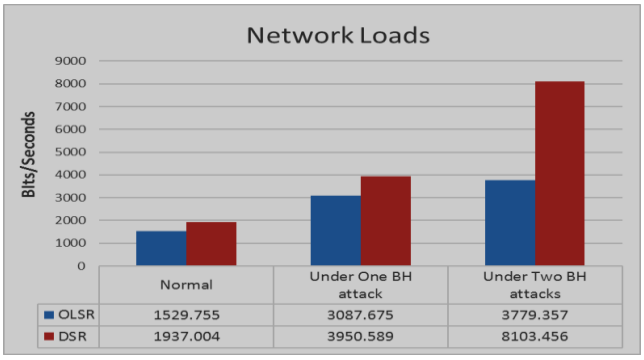

Fig. 14: Network load (bit/sec) of OLSR and DSR

The simulation results show that the network load of DSR increased DSR as compared to normal OLSR protocols. In the presence of one BH attacker node, network load further increased of DSR protocol than OLSR routing protocol. The network load increased more when the numbers of BH nodes rise to two as of DSR protocol than OLSR protocol in the MANETs.

V. Conclusion

To sum up the above discussion, it is crystal clear that this research work focused on the impact of BH attacks on the performing degradations of ad-hoc routing protocols OLSR and DSR in MANETs. Moreover, this research compared and analyzed the performance of OLSR and DSR routing protocols in the presence of BH attack using "OPNET Modeler 14.5", in terms of throughput, PDR, end-to-end delay and network load. Based on simulations done, the obtained results show that PDR and throughput drop in the presence of BH attacks. As onward PDR and throughput drops more in the network when the number of BH nodes increases in the network. Furthermore the end to end delay and network load, It is also noticed from the simulation results, that the average end to end delay and network load rises in the presence of BH attack. This research study concluded that the OLSR routing protocol performs better than the DSR routing protocol with and without the presence of BH attacks in all simulation scenarios.

VI. Future Work

Future research works recommended based on this research are as follows:

- Ad-hoc networks are extremely vulnerable to different kinds of security threats without the presence of a strong defense method, that's why further research work should be required within this crucial matter to identify different threats and then developing countermeasures for these threats.
- DSR routing protocol requires further improvement of features to be protected and useful within harmful scenarios.
- An efficient mechanism of BH detection and elimination is required in different MANETs routing protocols.

Conflict of Interest:

No conflict of interest regarding this article

References

I. Adam, G., Kapoulas, V., Bouras, C., Kioumourtzis, G., Gkamas, A., &Tavoularis, N. (2011, October). Performance evaluation of routing protocols for multimedia transmission over mobile ad hoc networks. In Wireless and Mobile Networking Conference (WMNC), 2011 4th Joint IFIP (pp. 1-6). IEEE.

II. Ade, S. A., &Tijare, P. A. (2010). Performance comparison of AODV, DSDV, OLSR and DSR routing protocols in mobile ad hoc networks.

International Journal of Information Technology and Knowledge Management, 2(2), 545-548.

III. Aggarwal, R., &Rana, S. A. (2014). Comparitative Survey on Malicious Nodes and Their Attacks in MANET. (IOSR-JCE), 16(3), (PP 93-101).

IV. Arora, N., &Barwar, N. C. (2014). Performance Analysis of Black Hole Attack on different MANET Routing Protocols. International Journal of Computer Science and Information technologies, 5(3), 4417-4419.

V. Babu, E. S., Naganjaneyulu, S., Rao, P. S., & Reddy, G. N. (2019). An Efficient Cryptographic Mechanism to Defend Collaborative Attack Against DSR Protocol in Mobile Ad hoc Networks. In Information and Communication Technology for Intelligent Systems (pp. 21-30). Springer, Singapore.

VI. Chaurasia, M., & Singh, B. P. (2018). Prevention of DOS and Routing Attack in OLSR Under MANET. In Proceedings of International Conference on Recent Advancement on Computer and Communication (pp. 287-295). Springer, Singapore.

VII. Dokurer, S., Erten, Y. M., &Acar, C. E. (2007, March). Performance analysis of ad-hoc networks under black hole attacks. In SoutheastCon, 2007. Proceedings. IEEE (pp. 148-153). IEEE.

VIII. Garg, N., & Mahapatra, R. P. (2009). MANET Security issues. IJCSNS, 9(8), 241.

IX. Jaiswal, P., & Kumar, D. R. (2012). Prevention of Black Hole Attack in MANET. IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN, 2250-3501

X, Jamal, T., & Butt, S. A. (2018). Malicious node analysis in MANETS. International Journal of Information Technology, 1-9.

XI. Johnson, D. B., Maltz, D. A., &Broch, J. (2001). DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc networking, 5, 139-172.

XII. Kaur, T., & Singh, A. (2013). Performance Evaluation of MANET with Black Hole Attack Using Routing Protocols. International Journal of Engineering Research and Applications (IJERA) ISSN, 2248(9622), 1324-1328.

XIII. Mamatha, G. S., & Sharma, D. S. (2010). A highly secured approach against attacks in MANETS. International Journal of Computer Theory and Engineering, 2(5), 1793-8201.

XIV. Mohammad, A. A. K., Mahmood, A. M., & Vemuru, S. (2019). Providing Security Towards the MANETs Based on Chaotic Maps and Its Performance. In Microelectronics, Electromagnetics and Telecommunications (pp. 145-152). Springer, Singapore.

XV. Mohammad, S. N., Singh, R. P., Dey, A., & Ahmad, S. J. (2019). ESMBCRT: Enhance Security to MANETs Against Black Hole Attack Using MCR Technique. In Innovations in Electronics and Communication Engineering (pp. 319-326). Springer, Singapore.

XVI. Mohebi, A., Kamal, E., & Scott, S. (2013). Simulation and analysis of AODV and DSR routing protocol under black hole attack. International Journal of Modern Education and Computer Science, 5(10), 19.

XVII. Mani, U., Chandrasekaran, R., & Dhulipala, V. S. (2013). Study and analysis of routing protocols in mobile ad-hoc network. Journal of Computer Science, 9(11), 1519.

XVIII. Rohal, P., Dahiya, R., &Dahiya, P. (2013). Study and analysis of throughput, delay and packet delivery ratio in MANET for topology based routing protocols (AODV, DSR and DSDV). international journal for advance research in engineering and technology, 1. (Vol. 1, pp. 54-58).

XIX. Roy A., Deb T. (2018) Performance Comparison of Routing Protocols in Mobile Ad Hoc Networks. In: Mandal J., Saha G., Kandar D., Maji A. (eds) Proceedings of the International Conference on Computing and Communication Systems. Lecture Notes in Networks and Systems, vol 24. Springer, Singapore

XX. Saddiki, K., Boukli-Hacene, S., Gilg, M., & Lorenz, P. (2018, September). Trust-Neighbors-Based to Mitigate the Cooperative Black Hole Attack in OLSR Protocol. In International Symposium on Security in Computing and Communication (pp. 117-131). Springer, Singapore.

XXI. Sajjad Muhammad, Khalid Saeed, Tariq Hussain, ArbabWaseem Abbas, Irshad Khalil, Iqtidar Ali, Nida Gul. : Impact of Jelly Fish Attackonthe Performance of DSR Routing Protocol in MANETs, J. Mech. Cont.& Math. Sci., Vol.-14, No.-4, July-August (2019) pp 132-140

XXII. Salehi, M., Samavati, H., &Dehghan, M. (2012, May). Evaluation of DSR protocol under a new Black hole attack. In Electrical Engineering (ICEE), 2012 20th Iranian Conference on (pp. 640-644). IEEE.

XXIII. Shrestha, A., &Tekiner, F. (2009, December). On MANET routing protocols for mobility and scalability. In Parallel and Distributed Computing, Applications and Technologies, 2009 International Conference on (pp. 451-456). IEEE.

XXIV. Tariq Hussain, Iqtidar Ali, Muhammad Arif, Samad Baseer, Fatima Pervez, Zia Ur Rehman. : AN INVESTIGATION OF THE PERFORMANCE OPTIMIZED LINK STATE ROUTING PROTOCOL ON THE BASIS OF MOBILITY MODELS, J. Mech. Cont.& Math. Sci., Vol.-15, No.-9, September (2020) pp 306-327.

XXV. Vamsi, P. R., & Kant, K. (2017). Generalized trust model for cooperative routing in MANETs. Wireless Personal Communications, 97(3), 4385-4412.