Comparison of AODV, DSR and OLSR Performance Under Black Hole Attack in Mobile Ad Hoc Networks

S. Kalichurn*, and E.O. Ochola

***Abstract*—**Black Hole attacks manipulate MANET routing protocols by deceiving nodes sending data into believing that the malicious Black Hole node has the optimal route available for data transmission to the intended recipient node. The ability to implement the appropriate routing protocol is essential in minimising the impact Black Hole attacks have on MANETs. In this study, the AODV, DSR and OLSR protocols were simulated under no attack as well as under Black Hole attack scenarios to determine which of these protocols performs best. The results were analysed using the performance metrics of Throughput, End-to-End delay and PDR. The results of the simulations show that AODV is more vulnerable to Black Hole attacks than DSR or OLSR. Furthermore, the results show that the adverse effects of a Black Hole attack on Throughput, End-to-End delay and PDR were more significant in AODV as opposed to DSR, which had the best overall performance. Future work to analyse the effects that Black Hole attacks have on the performance of Mobile Ad-hoc Networks in terms of mean delay time, packet overhead and memory usage could also be conducted.

Keywords*—AODV Protocol, Black Hole Attack, DSR Protocol, Mobile Ad-Hoc Networks, OLSR Protocol, Proactive routing protocols, Reactive routing protocols*

I. Introduction

A Mobile Ad-hoc Network (MANET) is a temporary, ever-changing, wireless network, formed by a group of self-organising mobile devices, without the need for any centralised network management or fixed networking infrastructure [1]. Nodes in a MANET need to be able to cooperate and communicate with each other to implement standard networking functionality, to compensate for the lack of a centralised network management authority [2].

In a MANET, nodes within transmission range communicate by forwarding messages directly to each other while nodes that are not within transmission range are dependent on intermediary nodes to facilitate communication using either Proactive, Reactive or Hybrid routing protocols. The purpose of a MANET routing protocol is to establish an optimal path (one with the least hops) from the sender node to the receiver node [2]. MANET routing protocols need to function in different networking contexts, ranging from small ad-hoc groups to larger, more complex mobile multi-hop networks. Most MANET routing protocols are designed based on the presumption that all other nodes in the MANET can be trusted and are fully cooperative [1]. However, should one of these nodes be compromised, the entire MANET is vulnerable to various attacks, including the Black Hole attack.

Black Hole attacks manipulate MANET routing protocols by deceiving the node sending information into believing that the malicious Black Hole node has the most optimal route available for data transmission to the intended recipient node. The malicious intent of the Black Hole node is to hinder the route discovery process and to intercept all network communication, resulting in data packets being discarded before reaching their intended destinations [3]. This deliberate dropping of packets by a malicious node is known as a Black Hole attack [2].

The purpose of this paper is to compare the performance of the MANET routing protocols AODV, DSR and OLSR protocols under Black Hole attack. The implementation and evaluation of the Black Hole attack were performed using Network Simulator (NS-2). The simulation results were analysed using Throughput, End-to-End delay and PDR, as the analysis of the simulation results is essential in understanding the behaviour and performance of these protocols, as well as in determining weaknesses for further improvements.

II. Background

MANET routing protocols are classified based on how nodes build and maintain communication routes within the MANET.

Reactive routing protocols (such as Ad-hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR)) establish routes to destination nodes only when the source node does not have a valid (active) route available for data transmission to occur, via the Route Discovery process. Reactive routing protocols have a much lower control overhead as routes are only created when they are required; however, route discovery can cause the MANET to suffer long delays [4].

Proactive routing protocols (such as Optimised Link State Routing Protocol (OLSR)) function by ensuring updated records of network routes are stored, as all nodes in the network have a local routing table that it uses in determining how to establish a connection with other nodes in the network. Nodes exchange topology information to maintain a consistent

S. Kalichurn, School of Computing, University of South Africa, P O Box 392, Pretoria, 0003, South Africa.

E.O. Ochola, School of Computing, University of South Africa, P O Box 392, Pretoria, 0003, South Africa.

network view in their local routing tables. This exchange of information among nodes results in a high control overhead [4].

Hybrid routing protocols (such as Zone Routing protocol (ZRP)) use proactive routing protocols to obtain the initial network topology and any other unknown routing information. Once the initial network topology is obtained, the hybrid protocol uses the reactive routing protocols mechanisms to maintain the routing information when any changes occur in the network topology [2].

A. Ad-hoc On-demand Distance Vector (AODV)

AODV utilises conventional routing tables, containing a single entry per destination node along with the most recently used sequence numbers. Sequence numbers provide the ability to determine how fresh a route is relative to other routes. A key feature of AODV is the automatic expiry of a routing entry that has not been recently used [5]. AODV routes are built using a Route Request (RREQ). A source node will broadcast an RREQ to its neighbouring nodes across the MANET when it needs to communicate with a destination node for which no route exists (or no recent route exists). Each node receiving the RREQ broadcast first refreshes its information about the source node and then sets up a route back towards the source node. Nodes receiving the RREQ will only send a Route Reply (RREP) message if it is either the intended destination node or if it has a route to the destination with a sequence number that is greater than or equal to the sequence number contained in the RREQ [4]. If required, an RREP is unicast back to the source node. Once the first RREP is received, the source node can begin forwarding data packets to the respective destination nodes. If a source node receives an RREP containing a route with a larger sequence number or if it receives an RREP with an equal sequence number but with a lower hop count, the routing information is refreshed for that destination node, and the new route will be used. A route will be preserved for as long as it remains actively used. If at any point a break in the network occurs, a Route Error message (RERR) is sent to inform the other nodes of the breakage [4]. Suppose an active route breaks while in use, the node upstream of the break will notify the source node of the breakage. If the source node wishes to continue with the communication, a new route discovery must be initiated to find an alternative route to the destination node.

In Fig. 1, node R wishes to establish communication with node W, for which there exists no direct route. An RREQ is broadcast to all of R's neighbouring nodes across the MANET. Once W receives the RREQ it sends a reply (RREP) message to R using its neighbouring nodes T and U. The reply is then propagated using neighbouring nodes of T and U until it finally goes back to R. Once node R receives the first RREP (in this case via W-T-R), communication between R and W can begin.

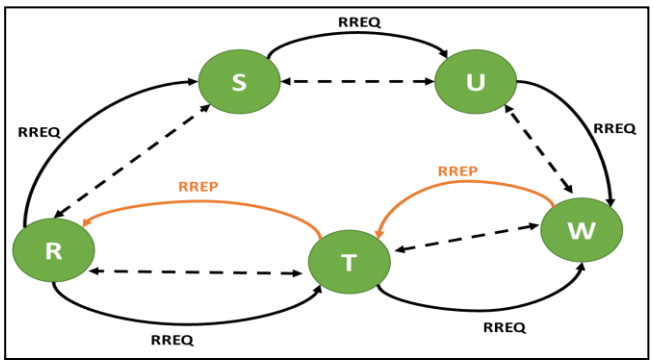

Fig. 1 – AODV route establishment.

B. Dynamic Source Routing (DSR)

The DSR protocol is a simple and efficient reactive routing protocol designed expressly for use in multi-hop MANETs. DSR enables the network to be entirely self-organised and self-configured without requiring any networking infrastructure or centralised administration. DSR is made up of a route discovery and route maintenance mechanism, enabling nodes to discover and maintain routes in the MANET [6]. Whenever, when a node needs to transmit data packets, it first checks the route cache for an available route to the destination. If an active route does not exist, the route discovery process will be launched by broadcasting the RREQ packet which contains the address of the destination node, the address of the source node and a unique identification number. When the RREQ message is received by a node that does not have a route to the destination (and it is not the destination node), the node adds its address to the route record and then rebroadcasts the packet to its neighbouring nodes. A receiving node only processes the RREQ if it has never seen the request before thereby decreasing the number of RREQs processed, which reduces delay. When the RREQ message reaches either the destination node or an intermediate node which contains a new route to the destination node, an RREP packet is created and sent to the source node [4]. The source node can start transmitting packets to the destination node as soon as it has received the first RREP packet [7].

In Fig. 2, node 1 wishes to establish communication with node 8, for which no direct route exists. A route request (RREQ) is broadcast to all of node 1's neighbouring nodes across the MANET.

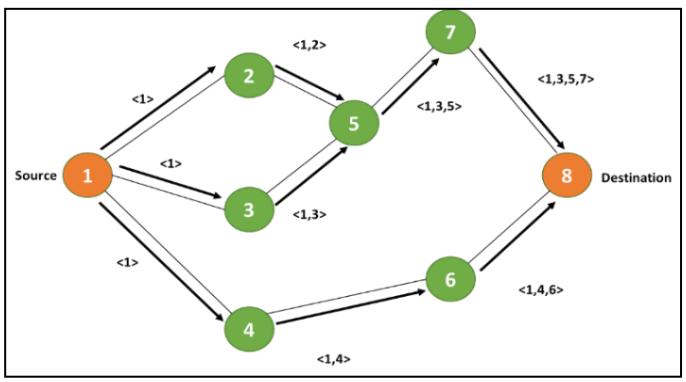

Fig. 2 – DSR route discovery.

In Fig. 3, once node 8 receives the request it sends a reply (RREP) message to node 1 using the shortest path (made up of nodes 8-6-4-1). The reply is then propagated using this path (nodes 8-6-4-1) until it reaches node 1. Once node 1 receives the RREP, packet transmission can begin between node 1 and 8.

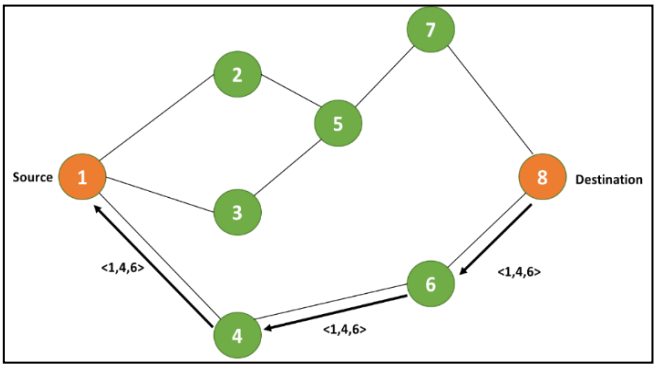

Fig. 3 – DSR route reply propagation.

C. *Optimized Link State Routing Protocol (OLSR)*

The OLSR protocol is a proactive routing protocol based on the link state algorithm, implemented by a table-driven approach [4]. The key benefit of using this protocol is that a route is immediately accessible from the standard routing table, which eliminates delays caused by route discovery, as each node always maintains possible routes to all other nodes within the MANET [8]. OLSR minimises control traffic overheads by using selected neighbouring nodes to retransmit control messages, called Multi-Point Relays (MPR). The nodes which are not part of the MPR still receive and process broadcast packets but do not retransmit them. This technique significantly decreases the number of retransmissions needed to send messages to all nodes in the network [7]. OLSR control messages are categorised into two types, i.e. HELLO and Topology Control (TC) messages. HELLO messages are sent by all nodes to their neighbours to get to know them and find out their link statuses through the responses received. TC messages are broadcast packets that contain information about the one-hop neighbours of nodes.

In Fig. 4, node A is the source node. Node A has five neighbouring nodes (nodes B, C, D, E and F). However, only two nodes have been selected as multi-point relays (nodes C and E), as such, only these nodes can retransmit control messages.

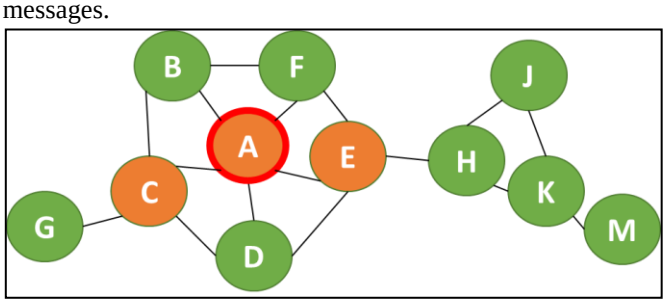

Fig. 4 – OLSR multi-point relays.

D. *Black Hole Attack in AODV, DSR and OLSR*

Black Hole attacks are caused when malicious nodes exploit vulnerabilities in routing protocols by claiming to have the shortest path to a given destination. Black Hole attacks increase the network overhead and increase the energy consumed by the network, which finally leads to the demise of the network. This attack can be perilous and critical data could be lost forever, as the dropped data packets are not checked or verified in any way [3].

For Black Hole attacks in MANETs using the AODV protocol, the malicious node will first search for the active route existing between the source and destination node. The Black Hole node will then reply to the RREQ almost immediately with an RREP containing spoofed information, without executing the standard AODV route discovery process [9]. These RREPs are sent with high sequence numbers as higher sequence numbers are perceived to come from fresher routes. This route is then used for data transfer between the source node and the "destination" node (impersonated by the malicious node), resulting in all data being sent to the malicious Black Hole node. The standard communication between the source and intended destination will no longer exist, thereby creating a Black Hole. The source node may never realise that the Black Hole exists as the source node believes it is transmitting data to the intended destination [8].

When a MANET using the DSR protocol is under Black Hole attack, the malicious node announces itself as having the shortest path to the destination node it plans to intercept. The malicious node does this to manipulate the route discovery mechanism into identifying it as the shortest path between the source and the destination node, thereby compromising the MANET [7].

When a MANET using the OLSR protocol is under Black Hole attack, the malicious node uses false HELLO or TC messages to manipulate its way into earning a privileged position within the network, to become an MPR. The malicious node will receive all routing messages from its neighbouring nodes and then drops them, resulting in the creation of a Black Hole attack [10].

III. Related Work

Over the recent years, many researchers have conducted various studies aimed at detecting and eliminating Black Hole attacks in MANETs, as well as, the effect Black Hole attacks have on MANETs. However, many inefficiencies and issues still exist today. As such, research needs to be conducted on Black Hole attacks in MANETs as it continues to be a relevant area of study.

The study in [8], analysed and compared the AODV and OLSR protocols using Packet Delivery Ratio (PDR) and Throughput as performance metrics. Their simulation results showed AODV generally outperforms OLSR while under regular operation as well as under Black Hole attack. Both AODV and OLSR showed decreased values in PDR and Throughput when compared under regular operation and Black

Fig. 8 shows the throughput results of AODV, DSR and OLSR under regular operation (without any attacks), as well as under Black Hole attack, with varying mobility speed. Raising the mobility speed of nodes in the MANET did not bring a notable change in throughput across all scenarios (under regular operation or Black Hole attack). Throughput for AODV, DSR and OLSR peak at a mobility speed of 60m/s and then decreases. The decrease in throughput can be attributed to the rapid changes in the location of nodes, which may cause changes in the route to the destination while some packets have already been sent from the source node using an outdated route, resulting in the loss of data packets. Under Black Hole attack, throughput decreases as the malicious Black Hole node discards some of the packets being transmitted. AODV's average throughput drops drastically by 43.16%, from 13.4kbps to 7.61kbps, compared to DSR's average throughput which drops by 28.68%, from 13.82kbps to 9.82kbps and OLSR's average throughput which drops by 25.96%, from 9.16kbps to 6.81kbps.

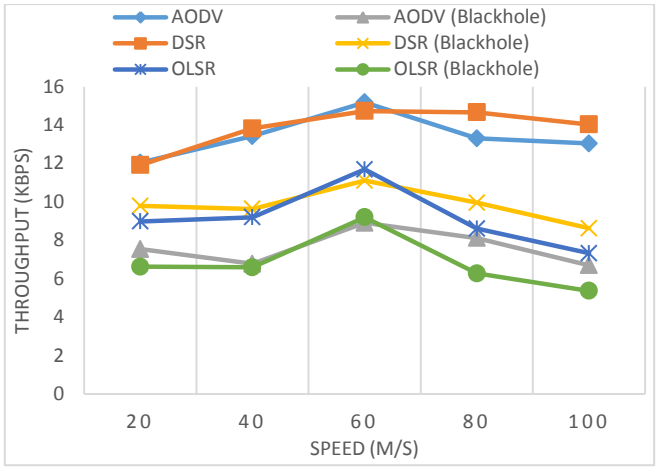

Fig. 8 – Node Mobility vs Throughput.

Fig. 9 shows that under regular operation, the end-to-end delay in OLSR is significantly lower than AODV and DSR. The end-to-end delay in OLSR remains relatively constant even as the node mobility speed increased, due to OLSR being a proactive routing protocol, with route calculations and establishment done in advance, for all potential destinations, regardless of node mobility speed. The end-to-end delay for AODV and DSR under no attack increases as the node mobility speed increases due to the rapid node location changes occurring. The end-to-end delay for AODV and DSR under Black Hole attack is reduced, as the Black Hole node responds to the route request immediately without querying the routing table, resulting in a shorter route discovery process time. The change in end-to-end delay for OLSR under Black Hole attack is insignificant.

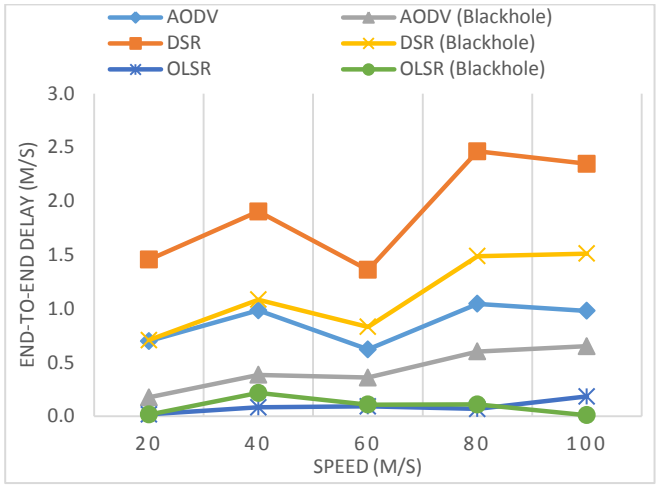

Fig. 9 – Node Mobility vs End-To-End Delay.

Fig. 10 shows the packet delivery ratio of AODV, DSR and OLSR under regular operation (without any attacks), as well as under Black Hole attack, with varying mobility speed. Under regular operation, as the node mobility speed increased, the packet delivery ratio also increased and peaked at 60m/s, after that a gradual decrease was observed in AODV and DSR and a more significant decrease in the PDR of OLSR at higher mobility speed. Under Black Hole attack, the PDR of AODV decreased on average by 46.17%, which was significantly more than the average decrease in the PDR of DSR and OLSR, at 31.33% and 25.62%, respectively. DSR performed the best under Black Hole attack, upholding an average PDR of 56.28%.

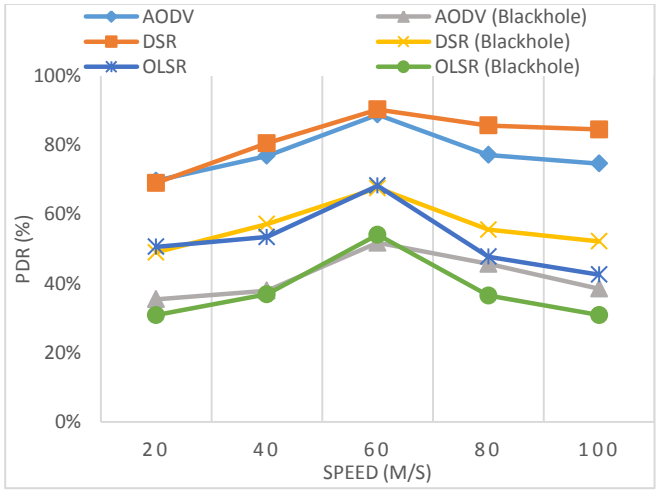

Fig. 10 – Node Mobility vs PDR.

VI. Conclusion

In this paper, three routing protocols, namely AODV, DSR and OLSR, were evaluated under no attack as well as under Black Hole attack scenarios using NS-2. The results of the simulations conducted prove that the existence of Black Hole nodes in a MANET severely impacts the overall performance of the network system in terms of Packet Delivery Ratio, End-to-End delay and Throughput.

The following observations were made based on the results of the simulations; when a MANET is under regular operation, it outperforms a MANET that is under Black Hole attack in terms of average throughput and PDR in AODV, DSR and OLSR. This occurs due to the Black Hole node claiming to have the shortest route to the destination node by responding with a quick RREP to the source node. In terms of End-to-End delay in both AODV and DSR, the results show that a MANET under Black Hole attack has a reduced End-to-End delay. This reduction in End-to-End delay is not seen as a positive sign as the Black Hole node compromises the network communication to achieve this reduction. Whereas, End-to-End delay in OLSR remained relatively unchanged under Black Hole attack.

To conclude, the adverse effects that Black Hole attacks have on the overall performance of MANETs were more significant in AODV than in DSR or OLSR. This result proved that AODV is more vulnerable to Black Hole attack than DSR or OLSR and the effects of a Black Hole attack are greater in AODV. Based on the observed simulation results, DSR performs the best while under Black Hole attack in terms of all the simulation parameters.

VII. Future Work

There is a need for analysis to be conducted on other Reactive and Proactive Routing protocols to determine which protocol can best mitigate the effects of Black Hole attacks. Future work to analyse the effects that Black Hole attacks have on the performance of Mobile Ad-hoc Networks in terms of mean delay time, packet overhead and memory usage could also be conducted. The effects multiple Black Hole attacks have on the performance of Mobile Ad-hoc Networks is also important to determine which protocol best withstands the effects of a cooperative Black Hole attack.

References

[1] A. Nabou, M. D. Laanaoui and M. Ouzzif, "Evaluation of MANET Routing Protocols under Black Hole Attack Using AODV and OLSR in NS3," *2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pp. 1-6, 2018.
https://doi.org/10.1109/WINCOM.2018.8629603

[2] S. Aluvala, K.R. Sekhar and D. Vodnala, "An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks," *2nd International Conference on Intelligent Computing, Communication*, 2016.
https://doi.org/10.1016/j.procs.2016.07.382

[3] F. Tseng, H. Chiang and H. Chao, "Black Hole along with Other Attacks in MANETs: A Survey," *Journal of Information Processing Systems*, vol. 14, no. 1, pp. 56-78, 2018.

[4] B. Shivahare, C. Wah and S. Shivhare, "Comparison Of Proactive And Reactive Routing Protocols In Mobile Adhoc Network Using Routing Protocol Property," *IJETAE*, vol. 2, no. 3, pp. 356-358, 2012.

[5] A. Arya, B.P. Chaurasia and S.K. Gupta, "Performance Analysis of Optimize AODV and AODV Routing Protocol," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 9, pp. 456-460, 2015.

[6] H. Liu and Z. Shang, "Comparing the Performance of the Ad-hoc Network under Attacks on Different Routing Protocol," *IJSIA*, vol. 9, no. 6, pp. 195-208, 2015.
https://doi.org/10.14257/ijsia.2015.9.6.19

[7] M. Salehi and H. Samavati, "DSR vs OLSR: Simulation Based Comparison of Ad Hoc Reactive and Proactive Algorithms under the Effect of New Routing Attacks," *2012 Sixth International Conference on Next Generation Mobile Applications, Services and Technologies*, pp. 100-105, 2012.
https://doi.org/10.1109/NGMAST.2012.29

[8] K.S. Praveen, H.L. Gururaj and B. Ramesh, "Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols," *International Conference on Computational Modeling and Security*, vol. 85, pp. 325-330, 2016.
https://doi.org/10.1016/j.procs.2016.05.240

[9] P. Dwivedi and S. Gupta, "A Survey on Route Maintenance and Attacks in AODV Routing Protocol," *International Journal of Computer Applications*, vol. 133, no. 9, pp. 23-26, 2016.
https://doi.org/10.5120/ijca2016908012

[10] A. Nabou, M. D. Laanaoui, and M. Ouzzif., "Effect of Single and Cooperative Black Hole Attack in MANET using OLSR protocol," *2nd International Conference on Networking, Information Systems & Security*, pp. 1-5, 2019.
https://doi.org/10.1145/3320326.3320408

[11] A. Adel and M. Melad, "Performance Evaluation of AODV, DSR, OLSR, and GRP MANET Routing Protocols Using OPNET," *International Journal of Future Computer and Communication*, vol. 5, pp. 57-60, 2016.
https://doi.org/10.18178/ijfcc.2016.5.1.444

[12] I. Nurcahyani and H. Hartadi, "Performance Analysis of Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) Under Black Hole Attacks in Mobile Ad Hoc Network (MANET)," *2018 International Symposium on Electronics and Smart Devices (ISESD)*, 2018.
https://doi.org/10.1109/ISESD.2018.8605445

[13] S. Singh and D. Choudhary, "AODV vs. OLSR: An Analytical Approach to Study Black Hole Attack," *International Journal of Computer Applications*, vol. 172, pp. 30-34, 2017.
https://doi.org/10.5120/ijca2017915208

[14] K. O. Basulaim and S. A. Aman, "Solution for Black Hole and Cooperative Black Hole Attacks in Mobile Ad Hoc Networks," *Egyptian Computer Science Journal*, vol. 41, no. 1, pp. 66-81, 2017.

[15] A. K. Jain and V. Tokekar, "Mitigating the effects of Black Hole attacks on AODV routing protocol in mobile ad hoc networks," *2015 International Conference on Pervasive Computing (ICPC)*, pp. 1-6, 2015.
https://doi.org/10.1109/PERVASIVE.2015.7087174

[16] M. A. A. Careem and A. Dutta, "Reputation based Routing in MANET using Blockchain," *2020 International Conference on Communication Systems & NETworkS (COMSNETS)*, 2020.
https://doi.org/10.1109/COMSNETS48256.2020.9027450