Impact of Black Hole Attack on Reactive and Proactive Routing Protocols in MANET

Shade KUYORO, Deborah ALEBURU, Monday EZE and Folasade Osisanwo
Department of Computer Science, Babcock University, Illishan-Remo, Nigeria.
afolashadeng@gmail.com, debaleburu56@gmail.com, eze_monday@yahoo.com, osisanwof@gmail.com

Abstract— Mobile Ad-hoc Networks (MANETs) is a self-configurable network, such that nodes connect and disconnect from the other nodes in the network automatically at any point in time. MANETs are vulnerable to various security attacks due to its characteristics of flexibility, distributed operation, node to node connectivity and so on. The focus of this work is on determining the effect of Black hole attack on MANET using Reactive routing Protocols - Ad-hoc On-Demand Routing protocol (AODV), and Temporally Ordered Routing (TORA); and Proactive routing Protocol - Optimized Link State Routing (OLSR) and Destination-Sequenced Distance- Vector (DSDV). Two network scenarios were simulated (with Black hole and without Black hole) using Network Simulator (NS-2.35) and the performance metrics considered are throughput, Packet Delivery Rate (PDR), and End to End Delay. The result showed that there were decrease in the throughput, Packet Delivery Rate and End- to-End Delay, when the network is under blackhole attack; this is more evident in AODV as compared to other routing protocols.

Index Terms—Black Hole Attack, End to End Delay, MANET, Packet Delivery Rate, Self-Configurable, Simulator, Throughput.

1 Introduction

THE existence of wireless networks has been the bedrock of meeting the demand for network environment without limiting time and places that the widespread of mobile devices and other inventions brought about. Wireless networks can be classified into infrastructure network using facilities such as base station and access point, and infrastructure-less network composed of mobile devices. This infrastructure-less networks are referred to as Ad hoc network, which is defined as a collection of two or more devices or nodes or terminals with wireless communications and networking capability that communicate with each other without the aid of any centralized administrator. [1]

Mobile Ad-hoc Network (MANET) is self-configurable network, where nodes connect and disconnect from each other within the network automatically at any time. Some of the characteristics of MANET are flexibility, distributed operation, addressing mobility, node to node connectivity and so on. The data routing in MANET are done based on node discovery and transmission, that is, the node receive the request message and forwards it to the neighboring node for further transmission to ensure that its reaches the particular destination and together with the aid of route reply message communication occurs; each node behaves like a relay agent to route the data traffic. The routing protocols in MANET include Ad-hoc On Demand Routing protocol (AODV), Optimized Link State Routing (OLSR), Destination-Sequenced Distance- Vector (DSDV), Temporally Ordered Routing (TORA) and so on.

MANET is susceptible to various security attacks because of its open medium, dynamic change in topology, lack of central authority for the management and monitoring, distributed operation, lack of infrastructure features. [2] Thus, there is need for secure way of transmission and node communication in MANET. This is a very challenging and vital issue as there is an increasing threats of attack on the Mobile Network continuously. Some of the attacks to MANETs include Wormhole, Black hole, Sybil, flooding, routing table overflow, Denial of Service (DoS), selfish node misbehaving, and impersonation attacks. The Black hole attack is considered to be the most deadly of all attacks as it swallows up packets (i.e. it collects packets and does not deliver the packets to its destination). [3]

Different solutions have been proffered in literature to alleviate this problem however most of the existing solutions do not support multiple black hole attack scenario (where more than one node acts as a black hole); while some solutions added to the delay and overhead time. Thus, there is need for solutions that can address black hole attacks (both single and multiple black hole attack scenarios) as well as reduce packet delay time. This work focuses on examining the effect of black hole on MANETs using proactive protocol (OLSR, DSDV) and reactive protocol (AODV, TORA) to determine which of the routing protocols is more susceptible to black hole attacks.

2 Related Works

Deng et al [4] proposed a solution for detecting the single black hole node in MANET. In this approach, the intermediate nodes send a RREP message together with the next hop information. After this information has been received, the source node sends further request to the next hop node to make sure that it has the route to the intermediate node or not. If the path is in existence, the intermediate node will be trusted and the source node will send data packets through that trusted node. If the path does not exist, the reply message from intermediate node will be ignored and an alarm message will be broadcasted to isolate the detected node from network. The drawback of this approach is that the routing overhead and end to end delay is going to be increased and also if the black hole nodes function together as a team in order to drop packets, then this approach is not efficient.

Ramaswamy et al [5] proposed a methodology for AODV-based MANET to identify multiple black hole nodes cooperating as a group. AODV routing protocol is slightly modified by this technique, it basically makes use of the Data Routing Information (DRI) table in addition to the cached and current routing tables. In this methodology each node maintains an additional Data Routing Information (DRI) table.

Lu et al [6] proposed a protocol that modifies the behavior of the original AODV by introducing a data structure referred to as trust table at every node. This table is responsible for holding the addresses of the reliable nodes. The RREP is extended with an extra field called trust field. In order for a node to be added to the trust table of another node, it needs firstly to pass behavioural analysis filter. Once the behavior of the broadcasting node is normal, it is added to the trust table of the receiving node.

Lalit, Vishal, & Nagesh [7] proposed a solution for AODV in MANET based on examining the source and intermediate node sequence number to determine who has sent back RREP and if there is large difference between them or not. Then it compares the first destination sequence number with the source node sequence number, if much difference exist, then it is clear that the node is a black hole node.

Vani & Sreenivasa-Rao [8] proposed a solution to black hole attack by modifying the AODV. Here the RREP received at the source node is compared with the threshold value. If the sequence number is within the threshold value then the RREP is coming from valid node, if the sequence number in RREP is greater than threshold value then such node will be detected as malicious.

Medadian & Fardad [9] solution adjudged that if a node is the first receiver of a RREP packet, this node forwards packets to the source and judges the replier. The judgment process depends on the opinion of network's nodes about replier. The activities of a node are logged by its neighbors, and each neighbor must send their opinion about a node. When all opinions of neighbors are collected by a node, it decides if the replier is a malicious node, the decision is applied according to number of rules. As in the simulation the proposed solution detects cooperative/multiple black hole nodes and increases performance in terms of packet delivery rate PDR and throughput, which it is better than that of standard AODV, but as appears in the simulation, the proposed solution causes minimal additional delay and overhead.

Kalia & Munjal [10] (2013) presented a mechanism to detect the multiple black holes by modifying the AODV protocol. This method used the fake RREQ message to attract the malicious node to respond the fake RREP message such that there are more than one malicious node who will reply the fake RREQ packet. In this mechanism, before discovering the actual route for data transmission in AODV, a fake RREQ packet is broadcasted which includes the target or destination address which does not exist in reality. The multiple black hole nodes will immediately respond to the fake RREQ packet as they do not care about whether the fake target addressed node exists or not in the network. Basically, this mechanism enhances the security of the AODV protocol with low routing overhead than other methods in MANET and also provide high packet delivery ratio.

Vasantha et al [11] aimed at analyzing and strengthening the security of routing protocol Ad-hoc On Demand Distance Vector (AODV) for MANET. The Proposed Solution referred to as PL2 provides alteration in AODV protocol for ensuring security against Black hole attack using NS2 Simulation. PL2 method is called PreLude, PostLude method. The proposed solution is an extension of the main AODV routing protocol to uncover secure routes and prevent Black hole attack on MANET. The main idea of this solution is based on time and neighborhood parameters. In this solution the existence of malicious activities are first searched for, and then once any is detected and removed. Route discovery process in this modified AODV is same as original AODV, however when transmitting data packets, prelude and postlude messages are included. Simulation results reveal that the proposed solution works well in the detection of Black hole attack and there is not much overhead.

Arathy and Sminesh [12] proposed a strategy to detect single and collaborative black hole attacks. The proposed D-MBH algorithm detects single and multiple black hole nodes using an additional route request with nonexistent target address, computes a threshold ADSN, creates a black hole list and invokes the proposed D-CBH algorithm. Using ADSN, black hole list and next hop information extracted from RREP, the D-CBH algorithm creates a list of collaborative black hole nodes leading to reduced routing and computational overhead.

3 Methodology

3.1 Simulation Environment

Network Simulator 2 (NS-2) was used to simulate networks with and without Black hole attacks for AODV, TORA, OLSR, DSDV routing protocols. Two scenarios were considered in setting up the simulation environments for the four routing protocols used in this work. In the first scenario the functioning of AODV, TORA, OLSR, DSDV routing protocol is simulated under normal condition with twenty (20) and eighty (80) nodes respectively. In the second scenario the black hole node is introduced in the functioning of AODV, TORA, OLSR, DSDV routing protocol with twenty (20) and eighty (80) nodes.

The list of parameters used when setting up the network environment is as follow:

TABLE 1
NETWORK CONFIGURATION FOR THE SIMULATION

Channel Type (chan)	**Wireless channel type**
Radio Propagation model (prop)	Two-Ray ground
Network interface type (netif)	Phy/WirelessPhy
Medium Access Control (MAC) type (mac)	Mac/802_11
Interface queue type (ifq)	Queue/DropTail/PriQueue but CMUPriQueue for DSR
Link Layer type (ll)	LL
Antenna model (ant)	OmniAntenna
Interface queue length (ifqlen)	10
Number of nodes (nn)	20, 80
Routing Protocol (rp)	AODV, DSDV,TORA,OLSR
Topography (x,y)	(400 X 400)m, (800 X 800)m
Duration for simulation (Stop)	150s

2.2 Network Evaluation using Performance Metrics

The following performance metrics were considered for the evaluation of MANETs routing protocols in this work.

(a) Average End-to-End Delay: This metric describes the packet delivery time; the lower the end-to-end delay the better the performance of the network.

$$D = Td - Ts \qquad (1)$$

Where Td is the time of packet arrival at the destination (Receiver Time) and Ts is the packet forward time at the resource node (Sender Time).

(b) Packet Delivery Ratio (PDR): This is the ratio of the data packets delivered to the destinations to those generated by the Constant Bit Rate (CBR) sources. The PDR shows how successful a protocol performs delivering packets from source to destination. The higher the PDR better the result.

$$\text{PDR} = \frac{\text{Total No of Packets Received}}{\text{Total No of Packets Sent}} \qquad (2)$$

(c) Throughput: Throughput is the ratio at that a network forward and reached information. To calculate the throughput, we used the formula.

$$Tp = Pa/Pf \qquad (3)$$

So Pa is the packets received and Pf is the forwarded packets sum above specific time n conclusive.

4 RESULT AND DISCUSSION

4.1 Throughput

Table 2 presents the tabular representation of throughput for 20 and 80 nodes in the four routing protocols considered with and without Black hole attack respectively and Figures 1 and 2 present graphical representation of throughput for 20 and 80 nodes in the four routing protocols considered with and without Black hole attack respectively.

TABLE 2
THROUGHPUT FOR 20 AND 80 NODES WITH AND WITHOUT BLACK HOLE (BH)

	20 NODES		**80 NODES**	
Protocol	**TP**	**TP (BH)**	**TP**	**TP (BH)**
AODV	129	55	178	70
TORA	137	129	157	123
OLSR	135	85	200	123
DSDV	128	75	156	90

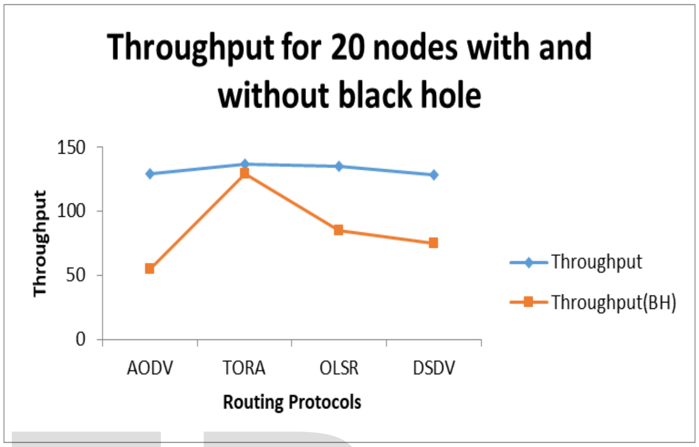

Fig. 1. Throughput for 20 nodes with and without Black Hole Attack

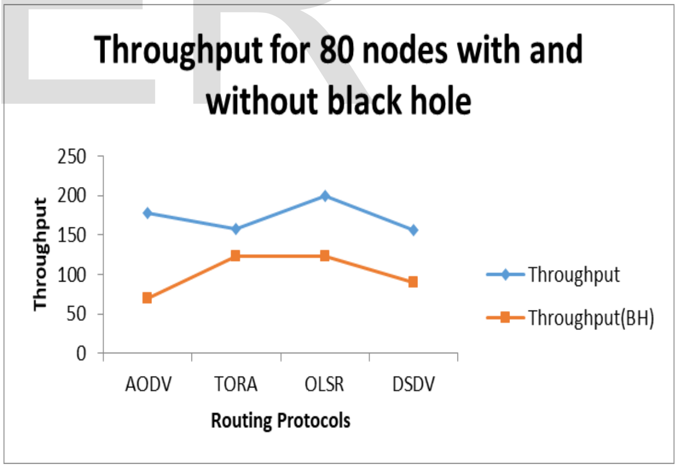

Fig. 2. Throughput for 80 nodes with and without Black Hole Attack

4.2 Packet Delivery Ratio (PDR)

Packet Delivery Ratio depends on the protocol routing procedure and number of nodes involved. Table 3 presents the tabular representation of packet delivery ratio for 20 and 80 nodes in the four routing protocols considered with and without Black hole attack respectively and Figures 3 and 4 present graphical representation of packet delivery ratio for 20 and 80 nodes in the four routing protocols considered with and without Black hole attack respectively.

TABLE 3
PDR FOR 20 AND 80 NODES WITH AND WITHOUT BLACK HOLE (BH)

	20 NODES		80 NODES	
Protocol	PDR	PDR (BH)	PDR	PDR (BH)
AODV	92	54	75	35
TORA	50	35	80	71
OLSR	83	55	93	64
DSDV	65	42	64	47

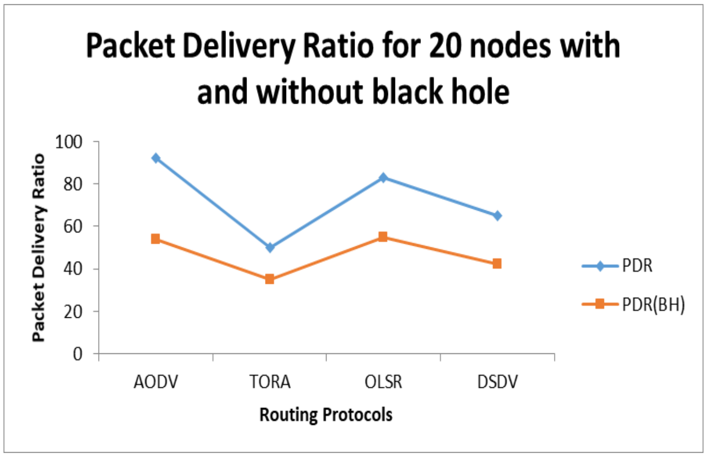

Fig. 3. PDR for 20 nodes with and without Black Hole Attack

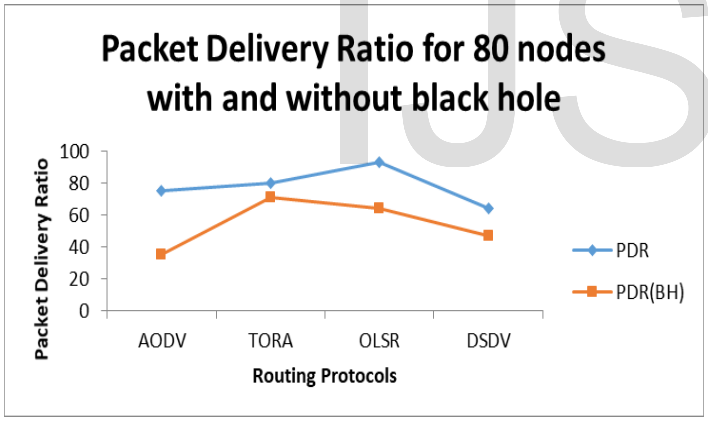

Fig. 4. PDR for 80 nodes with and without Black Hole Attack

4.3 Packet End to End Delay

Packet end to end delay in case of Black Hole attack and without attack depends on the protocol routing procedure and number of nodes involved. Table 4 presents the tabular representation of End-to-End Delay for 20 and 80 nodes in the four routing protocols considered with and without Black hole attack respectively and Figures 5 and 6 present graphical representation of End-to-End Delay for 20 and 80 nodes in the four routing protocols considered with and without Black hole attack respectively.

TABLE 4
DELAY FOR 20 AND 80 NODES WITH AND WITHOUT BLACK HOLE (BH)

	20 NODES		80 NODES	
Protocol	Delay	Delay(BH)	Delay	Delay(BH)
AODV	0.33	0.22	0.39	0.27
TORA	0.31	0.27	0.34	0.29
OLSR	0.24	0.18	0.28	0.2
DSDV	0.16	0.12	0.21	0.16

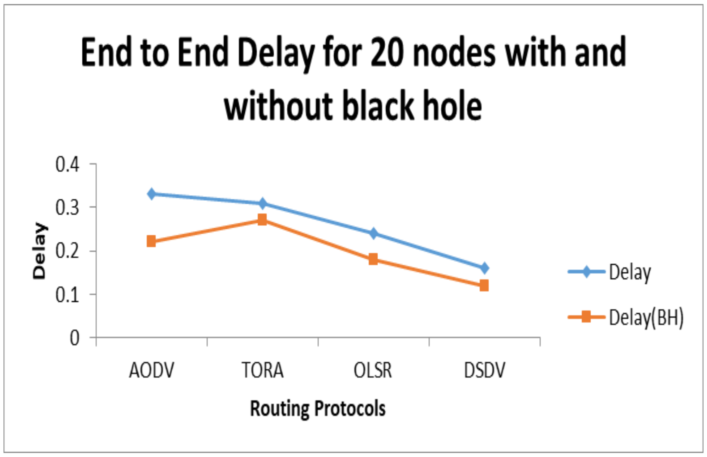

Fig. 5. Delay for 20 nodes with and without black hole attack

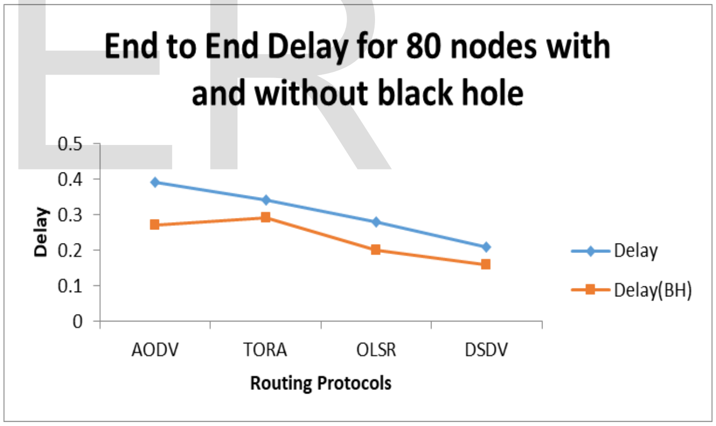

Fig. 6. Delay for 80 nodes with and without black hole attack

It can be observed from the results that AODV and OLSR is more susceptible to black hole attack in the reactive and proactive protocols respectively.

5 CONCLUSION AND RECOMMENDATIONS

In this paper, four (4) routing protocols, reactive (AODV, TORA) protocol and proactive (OLSR, DSDV) protocol were simulated using two different scenarios. In the first scenario, the routing protocols were simulated under normal network condition using low mobility and low traffic (20 nodes) and high mobility and high traffic (80 nodes) respectively. In the second scenario, the routing protocols were simulated with the presence of black hole in the network.

The effect on the performance of the network was analyzed with respect to performance metrics such as Throughput, Packet Delivery Ratio and End to End Delay. The susceptibility of four protocols AODV, TORA, OLSR, DSDV were analyzed, based on this research and the analysis of simulated result, it was concluded that the impact of black hole attack is severe on AODV and OLSR in the reactive and proactive protocols respectively.

In further research, it is recommended that the analysis of Black Hole attack be extended to other MANETs routing protocols. Other types of attacks such as Wormhole, Jellyfish and Sybil attacks need to be studied in comparison with Black Hole attack categorizing them based on the effect on network performance. Also, the best elimination strategy for Black hole attack can be determined in further research.

6 References

[1] W. Wei-Chen and L. Horng-Twu (2015), "A Study on High Secure and Efficient MANET Routing Scheme," Journal of Sensors, vol. 2015, Article ID 365863, 10 pages, 2015. doi:10.1155/2015/365863

[2] J. Swati (2013). Simulation and Analysis of Performance Parameters for Black Hole and Flooding Attack in MANET using AODV protocol. Retrieved from https://www.scribd.com/doc/85671348/Final-Dissertation

[3] U. Irshad and U.R. Shoaib (2012). Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols. (Master's Thesis)

[4] H. Deng, W. Li and D. Agrawal (2002). Routing Security in Wireless Ad Hoc Networks University of Cincinnati, IEEE Communication Magazine.

[5] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, (2013). Prevention of cooperative black hole attack in wireless ad hoc networks.

[6] S. Lu, L. Li, K. Y. Lam, and L. Jia (2010). SAODV: A MANET routing protocol that can withstand Black Hole attack. Computational Intelligence and Security, 2009. CIS "09, 2,

[7] H. Lalit, V. Vishal, and C. Nagesh (2011). Preventing AODV Routing Protocol from Black hole attack. International Journal of Engineering Science and Technology (IJEST), 3(5), 3927–3932.

[8] A.Vani and D. Sreenivasa-Rao (2011). Removal of Black hole in Adhoc wireless networks to provide confidentiality security. International Journal of Engineering Science and Technology (IJEST), 3(3)

[9] M. Medadian and K. Fardad (2012). Proposing a Method to detect black hole attacks in AODV routing protocol. European Journal of Scientific Research

[10] N. Kalia, K. Munjal (2013) "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol". International Journal of Engineering and Advanced Technology (IJEAT), Vol. 2, Issue-3, February 2013.

[11] S.V. Vasantha (2014) International Journal of Computer Science and Mobile Computing, Vol.3 Issue.11, November- 2014, pg. 570-576

[12] K. S.Arathy, C. N. Sminesh (2016) A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016) Procedia Technology 25 (2016) 264 – 271