Development of a Secured Watchdog Mechanism under Blackhole Attacks in Mobile Ad-Hoc Networks

I.T. Ayorinde[1], C.A. Fehintola[2] and O.D. Adeniji[3]
Department of Computer Science,
University of Ibadan, Ibadan,
Nigeria.

Email: [1]temiayorinde@yahoo.com,
[2]fehintola.cecilia94@gmail.com,
[3]sholaniji@yahoo.com

ABSTRACT

Mobile Ad-hoc network (MANET) is an example of mobile wireless network characterized by dynamic topology, self-organization, auto-configuration, lack of infrastructure and decentralized administrator which makes it more useful in military battlefield, smart buildings and emergency use. In MANET, mobile nodes are connected to each other and they don't depend on a central node to coordinate communication or carry information between them; Instead, they work together to carry information between nodes that cannot reach each other directly. The vulnerability of nodes in MANET has become a major issue despite many security schemes that have been proposed in the literature. Hence, this study develops a secured watchdog mechanism that enhances the performance of routing protocols in MANETs. The experiment of the secured watchdog under blackhole attacks was simulated using the Network Simulator (NS) 2.35 to test for the vulnerability of routing protocols in the (presence of blackhole attacks). The experimental results in terms of average throughput, end-to-end delay and packet delivery ratio for all the scenarios show that the newly developed model has a better performance compared with the existing model.

Keywords: *MANETs, Blackhole, Secured watchdog, Route request (RREQ), Route reply (RREP)*

African Journal of Computing & ICT Reference Format:

I. T. Ayorinde, C. A. Fehintola and O. D. Adeniji (2019),
Development of a Secured Watchdog Mechanism under
Blackhole Attacks in Mobile Ad-Hoc Networks,
Afr. J. Comp. & ICT, Vol.12, No. 3, pp. 85 - 92.

I. INTRODUCTION

Advancement in the ~~field of~~ internet due to wireless network technologies gives rise to many new applications. Mobile ad-hoc network (MANET) is one of the most promising and demanding fields for research and development of wireless network. As the major interest of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc network has now become one of the most vibrant and active field of communication and networks [1]. Routing is a way of transmitting data or packets from source node to destination node.

Security is an important factor in wireless ad-hoc network. There must be safety in transmitting data packets between two wireless sensor nodes. The nodes possess a unique characteristic which results in consequential challenges to security design. Compared to other wireless networks, wireless sensor networks (WSNs) have more security problems and this may be due to their nature of broadcasting messages, resources and their environment [2]. Wireless networks have gained a lot of popularity today, as the users want wireless connectivity irrespective of their geographical positions and MANET is one of such wireless ad-hoc networks. The openness of the mobile ad-hoc networks makes it vulnerable to security threats and this is due to the fact that MANET is an infrastructure less network environment and nodes moves randomly. There is an increase of threats in MANET which generally reduces its performance in the network [3].

Black hole attack, Wormhole and Gray hole attack are part of the security threats in which the traffic is redirected to such a node that actually does not exist in the network by sending the false data streams to the target nodes [4]**.** Black hole attack occurs when a malicious node broadcasts itself as the most optimal node for data forwarding. The malicious nodes then drop packets and hence deny the service in the network. Figure 1 shows the diagram of a blackhole attack [5].

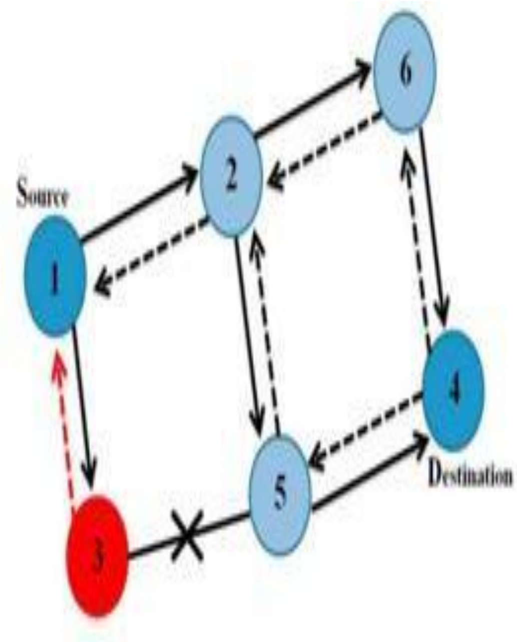


Figure 1: Blackhole Attack [5]

Collaborative attacks have more harsh effects on MANETs than particular single attacks. Due to increasing demand of using MANETs, various types of protocols and secure algorithms have been developed one after the other but still, there is lack of completely secured protocols which makes communication border free [3, 6].

Watchdog algorithm is a checking mechanism which acts as a trust system for most of the Ad Hoc and WSN. Watchdog detects the malicious misbehaviour of nodes by listening to the next Hop transmission. In certain cases, watchdog may overhear that its next node has failed to forward the packet within a certain amount of time period, thereby increasing the failure counter of the watchdog. When the malicious node exceeds the failure counter and the predefined threshold, the watchdog reports it as misbehaving node [7]. Figure 2 shows the diagram of a watchdog mechanism.

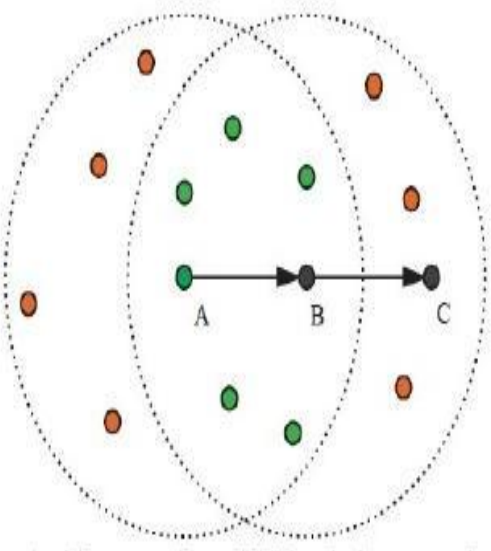


Figure 2: Watchdog mechanism [7]]

From Figure 2, node A, which intends to send a packet to node C, can eavesdrop the sent traffic of the node B and determine whether or not the node B will send the packet to C.

The watchdog mechanism has its weakness in terms of failure in detecting malicious nodes (black hole nodes) in the presence of partial dropping of packets which can lead to packet loss thereby decreasing the performance of routing protocols in the network. Hence, this study develops a secured watchdog mechanism that enhances the performance of routing protocols in MANET The secured watchdog mechanism monitors the network and identifies malicious nodes (black hole nodes) on time so as not to cause damage to the network and increase the performance of routing protocols.

II. REVIEW OF RELATED WORKS

In [8], the authors proposed an algorithm to develop a baited blackhole dynamic source routing (BDSR) so as to be able to detect and avoid the blackhole attack based on merging proactive and reactive defence architecture in MANET by using the virtual and non-existent destination address to bait the malicious node to reply RREP. Even though dynamic source routing (DSR) can know all the addresses of nodes among the route after the source node receives the route reply (RREP) from the destination node, the source node cannot identify exactly which intermediate node has routing information to destination node and reply RREP. This situation makes the source node sends packets to the shortest path that the malicious node claim and the network suffer black hole attack that causes packet loss. The BDSR modifies DSR's packet format of route request (RREQ) and RREP to help BDSR detect malicious node. In terms of RREP, the Reserved field was changed to Record address field that will record which node start to reply RREP. The Record address field stores the address of node that replies RREP. BDSR increases RREQ' packets that are the same with original RREQ packet format except its Target address field uses an address that is random, virtual and non-existent.

In [1], the authors developed watchdog concepts that were to eliminate misbehaviour of blackhole nodes which are the HALT, ACKNOWLEDGEMENT, NUMBERING AND DETECTION GRAPH. The halt concept was basically used to remove the ambiguous collision in which a sender node is not able to overhear from receiver node receiving the packet due to traffic from other nodes at its end. This mechanism can be used to halt the process of the sender end till it receives the acknowledgment from the receiver node which otherwise can be considered as malicious. The halting of the process would not allow other neighboring nodes of sender to send packets while it is receiving acknowledgment from the receiver. Halt mechanism helps in removing the core disadvantage of the Watchdog algorithm.

The acknowledgement concept was to remove the two main disadvantages of the watchdog algorithm receiver collision and limited transmission power. The numbering concept removed the false misbehavior and helps us to improve the efficiency of the algorithm. The detection graph concept helped to remove colluding and partial dropping in the watchdog algorithm. In this there is a sender and a receiver which maintain all the traffic rate .The amount of data sent from the sender and received are all maintained. So when a malicious node drops some packets as in partial dropping or in colluding, the destination node receives the packets and checks it with the inflow sent from the sender.

In [9], the authors proposed an enhanced adaptive acknowledgement (EAACK) scheme that was designed to tackle the weakness of watchdog scheme which are false misbehaviour, limited transmission power and receiver collision. An introduction of digital signature to prevent the attacker from forging acknowledgement packets was also proposed.

In [7], the authors proposed a watchdog algorithm to solve the impartial removal malicious nodes, limited power transfer and node conspiracy. The watchdog technique was modified and improved by enhancing the security in wireless sensor network.

In [10], the authors proposed a technique to resist smart blackhole attacks by employing timers and baiting messages. The proposed technique consists of two phases: Baiting and Non-neighbor Reply. In baiting phase, each node has a bait-timer, the timer has its value set randomly to B seconds, and each time the timer reaches B it creates and broadcasts a bait request with a randomly generated fake id. The blackhole node receives any route request it responds to with a reply claiming that it has the best path even if it does not exist. When the black-hole receives the baited request sent, it sends a reply to the source node claiming that it has a route; when the source node receives the reply it immediately considers the node which responded as a black-hole and adds it to the black-hole list because it claimed to have a route to a fake node.

In Non-neighbor Reply phase each node knows its adjacent nodes because of the hello message broadcasting process. When the source node receives a reply it checks the id of the Node With the Shortest Path if it is in the black-hole list; then it discards the reply; otherwise it checks if the id exists in the neighbor list by comparing the ID with ones in the neighbor list; if Nodes With Shortest Path (NWSP) is not a neighbour node then the source node discards that reply to avoid any communication with unknown nodes. The proposed technique provides a self-detection and isolation for any black-hole node which enables the connectivity between MANET nodes. The suggested technique does not use the black-hole alarm in order to prevent any smart black-hole node from using this feature by broadcasting false alarms.

III. METHODOLOGY

The model developed in this study is termed secured watchdog mechanism. It detects the actual cause of packet loss. The secured watchdog notices that whenever the packet sending time is greater than the packet storing time, it sends an alert to the network and marks the node as malicious. The pseudocode for the operation is given below:

Pseudocode of the Secured Watchdog Mechanism:

```
1.  Start
2.  Source Node sends RREQ
3.  Waits for a response
4.  Stores all the received RREPs in RREP
    table.
5.  If the sending time of packet is greater
    than the storing time, then use the route,
    node normal, go to step 9.
6.  If the packet sending time is less than the
    packet storing time, calculate the difference
    between the sequence number of nodes and
    the sequence number of current node.
7.  If the difference is large and within the
    range of suspected nodes sequence, calculate
    the percentage of packet loss of nodes
    suspected to be malicious, if the percentage
    of packet loss is greater than the value of the
    percentage of packet loss, mark node as
    malicious.
8.  Sends data packet through the route.
9.  Stop.
```

The new model of a secured watchdog mechanism developed in this study uses the parameters shown in Table 1.

Table 1 Simulation parameters.

Parameter	**Value**
Simulator	Ns-2.35
Simulation time	100sec
Total number of nodes	25, 50, 100 and 150
Observation parameter	Packet delivery ratio, throughput and end to end delay
No of malicious nodes	1-2
Attack	Blackhole
Data packet size	512byte

Simulation size	500m x 500m
Protocol	Ad-hoc On- demand Distance Vector (AODV)
Pause time	5secs
Connection	CBR (constant bit rate)
Mac protocol	802.11
Data rate	0.5 Mbps
Transport protocol	UDP

IV. IMPLEMENTATION AND DISCUSSION OF RESULTS

The experiment of the secured watchdog under blackhole attacks was simulated using the Network Simulator (NS) 2.35 to test for the vulnerability of routing protocols in the presence of blackhole attacks.

Figure 3 shows the results of end to end delay between the existing model and the newly improved/developed model. The end to end delay was calculated using different nodes. It shows that the new model turned out to be lower than the existing model which is an indication of a better performance. The lower the end to end delay, the better performance of the protocol in the network.

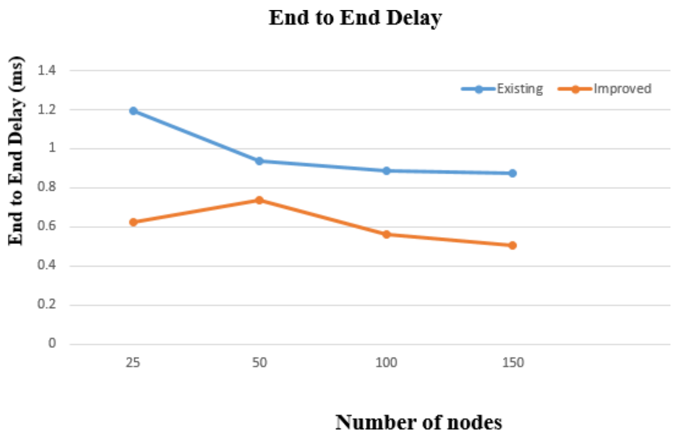


Figure 3: End to End Delay Vs Number of Nodes

Figure 4 shows the results of average throughput between the existing model and the improved model.

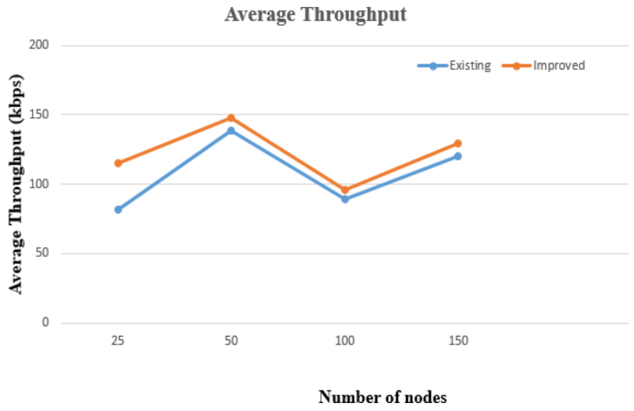


Figure 4: Average Throughput Vs Number of Nodes

The average throughput was calculated using different nodes. It shows that the improved model turned out to be higher than the existing model. This shows a good performance because the higher the average throughput means the better performance of the protocol in the network.

Figure 5 shows the results of packet delivery ratio between the existing model and the improved model. The packet delivery ratio was calculated using different nodes. It shows that the improved model turned out to be higher than the existing model. This shows a good performance because packet drops are reduced. The higher the packet delivery ratio means the better performance of the protocol in the network.

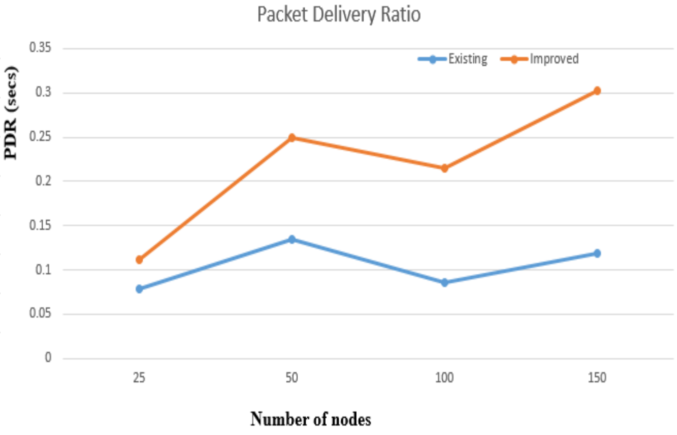


Figure 5: Packet Delivery Ratio Vs Number of Nodes

All the results shown in Figures 3 – 5 are also represented in Tables 2 – 4 for more clarity.

Table 2: End to end delay in meter per second (ms) between existing model and the improved model

Number of nodes	Existing Model [10]	Improved Model
25	1.197	0.620
50	0.938	0.739
100	0.889	0.563
150	0.873	0.507

Table 3: Average throughput in kilobytes per second (kbps) between existing model and the improved model

Number of nodes	Existing model [10]	Improved model
25	81.388	115.229
50	138.527	147.468
100	89.642	96.174
150	120.600	129.411

Table 4: Packet delivery ratio (%) between existing model and the improved model

Number of nodes	Existing model [10]	Improved model
25	0.07967	0.1110
50	0.13542	0.2509
100	0.08663	0.2155
150	0.11960	0.3031

In Table 2, the end to end delay for the improved model was reduced. In Table 3, the average throughput was increased. Also, in Table 4, the packet delivery ratio also increased. In general, the overall experiment shows that the network performance was increased and improved when compared with the existing model.

Figures 6 and 7 show the NAM files for the scenarios and simulations of 25 and 50 nodes respectively.

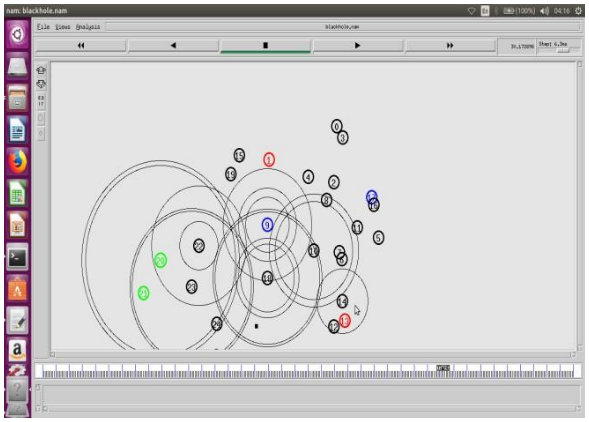


Figure 6: NAM file showing the scenario and simulation of 25 nodes.

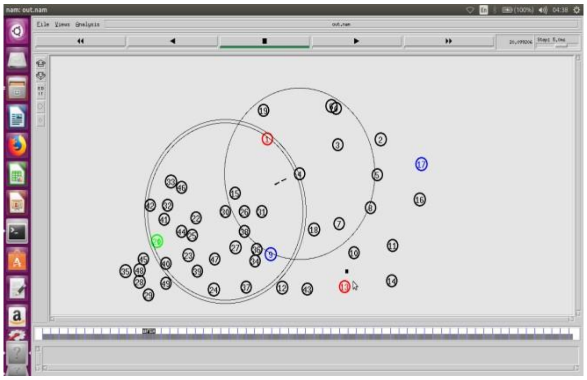


Figure 6: NAM file showing the scenario and simulation of 25 nodes.

V. CONCLUSION

The newly developed or improved model detects blackhole nodes when it drops all the received data packets destined for specific destinations. From the result analysis, it can be concluded that the new model gives better results when compared with the existing model at different scenarios. The average throughput and packet delivery ratio performance were increased while the end to end delay was reduced which shows better performance on the network.

REFERENCES

[1]. S. Bora, S. Singh, S. Mohamad Arsalan and A. Bijalwan (2014). Watchdog: A Study on Examining and Eliminating Misbehaviour.

International Journal of Computer Applications, *87*(3), 1–3. https://doi.org/10.5120/15185-3541

[2]. K. S. Praveen, H. L. Gururaj and B. Ramesh (2016). Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols. *Procedia Computer Science, 85*(Cms), 325–330. https://doi.org/10.1016/j.procs.2016.05.240

[3] D. Baberwal and M. Bundele (2015). Detection and Prevention of Black Hole Attack for Dynamic Source Routing in Mobile ad-hoc Network. *International Journal of Innovations & Advancement in Computer Science*. Delhi, April, 2015.

[4]. D. Kajaree and R. Behera (2017). A Survey on Web Crawler Approaches. *International Journal of Innovative Research in Computer and Communication Engineering*, *5*(2), 1302–1309. https://doi.org/10.15680/IJIRCCE.2017.

[5]. V. Dwivedi and S. Ahmad (2016). Detection and Prevention Methods of Black Hole & Gray Hole Attacks in MANET – A Critical Survey. *International Journal of Computer Science and Information Technologies* 187– 192.

[6]. A. Rana, V. Rana and S. Gupta (2015). EMAODV : Technique to Prevent Collaborative Attacks in Manets, *Procedia Computer Science 70*, 137–145. https://doi.org/10.1016/j.procs.2015.10.060

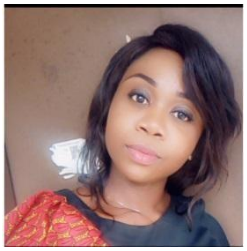
[7]. A. Forootaninia and M. B. Ghaznavi-Ghoushchi (2012). An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDS in Wireless Sensor Networks. *International Journal of Network Security & Its Applications* (IJNSA), 2012, (4) 161-178.

[8]. P. Tsou, J. Chang and Y. Lin (2011). Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs. *(ICACT), 2011*, 755–760.

[9]. R. Jeyaawinothini, B. Leena and P. Gnanasundari (2014). Detection of Misbehaving Nodes Using an Enhanced Acknowledgment Based Intrusion Detection Technique in MANETs. *International Journal of Science, Engineering and Technology Research* (IJSETR) *3*(4), 914–920.

[10]. A. Yasin and M. Abu Zant (2018). Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. *Wireless Communications and Mobile Computing, 2018*, 1–10. https://doi.org/10.1155/2018/9812135

Dr. Ibiyinka Temilola AYORINDE graduated from the Federal University of Technology, Akure, Ondo State in 1995 with Bachelor of Technology (B.Tech.) degree in Computer Science. She had her MSc. and Ph.D degrees in Computer Science from the University of Ibadan where she is currently a faculty member. Dr. Ayorinde joined the service of the University of Ibadan in 2010. Prior to this period, she had lectured at the Polytechnic Ibadan for almost a decade and had also worked in the industry during the early days of her career as both programmer and systems analyst. Her research interests include: Knowledge Representation, Ontology, Software Engineering, Machine Learning and ICT. She can be reached on phone number: +2348035289814 and email address: temiayorinde@yahoo.com



Cecilia Adejoke FEHINTOLA is a graduate of computer science. She earned her B.Sc. degree in computer science at Bowen University, Iwo, Osun State, Nigeria in 2015 and also M.Sc. computer science at the University of Ibadan, Ibadan, Nigeria in 2019. Her areas of interest include networks and information security, wireless sensor networks and Ad-hoc Networks. She can be reached on phone number: +2348135564287 and email address: fehintola.cecilia94@gmail.com

Oluwashola David ADENIJI had his PhD degree in the department of Computer Science, University of Ibadan where he is also a faculty member. His research areas include *Wireless Communication, Data Communication, RFID and System Security. He can be reached on telephone number:* +23407065370344 and email address: sholaniji@yahoo.com