International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 3, June 2019, pp. 1968~1977
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i3.pp1968-1977

Intelligent black hole detection in mobile AdHoc networks

Yaser Khamayseh, Muneer Bani Yassein, Mai Abu-Jazoh
Department of Computer Science, Jordan University for Science and Technology, Jordan

Article Info

Article history:

Received Feb 9, 2018
Revised Sep 14, 2018
Accepted Oct 10, 2018

Keywords:

Aodv
Black hole node
Detection
Features
Hybrid
Manets
Routing

ABSTRACT

Security is a critical and challenging issue in MANET due to its open-nature characteristics such as: mobility, wireless communications, self-organizing and dynamic topology. MANETs are commonly the target of black hole attacks. These are launched by malicious nodes that join the network to sabotage and drain it of its resources. Black hole nodes intercept exchanged data packets and simply drop them. The black hole node uses vulnerabilities in the routing protocol of MANETS to declare itself as the closest relay node to any destination. This work proposed two detection protocols based on the collected dataset, namely: the BDD-AODV and Hybrid protocols. Both protocols were built on top of the original AODV. The BDD-AODV protocol depends on the features collected for the prevention and detection of black hole attack techniques. On the other hand, the Hybrid protocol is a combination of both the MI-AODV and the proposed BDD-AODV protocols. Extensive simulation experiments were conducted to evaluate the performance of the proposed algorithms. Simulation results show that the proposed protocols improved the detection and prevention of black hole nodes, and hence, the network achieved a higher packet delivery ratio, lower dropped packets ratio, and lower overhead. However, this improvement led to a slight increase in the end-to-end delay.

Corresponding Author:

Yaser Khamayseh,
Department of Computer Science,
Jordan University for Science and Technology,
22110, Irbid, Jordan.
Email: yaser@just.edu.jo

1. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile devices that are connected via wireless links; these devices dynamically constitute a temporary network without a need for a central management or network infrastructure. Each mobile device in the MANET communicates directly with other mobile devices within its radio range, while it can communicate with nodes that are located outside its radio range through intermediate nodes. Moreover, all the nodes must cooperate in forwarding the packets in the network [1]-[3]. MANETs have many distinct characteristics: dynamic network topology, no infrastructure, multi-hop routing, limited resources, and limited bandwidth [4]-[10]. There are various applications for MANETs ranging from the battlefield to classrooms [5], [11]-[13]. The Ad hoc On-Demand Distance Vector (AODV) is a reactive routing protocol that is specifically developed for MANETs. AODV is based on two mechanisms for routing, which are: route discovery and route maintenance [5], [8], [14]. The widespread use of MANETs is being challenged by many factors, in particular, the issue of security. Nodes are assumed to *trust* each other and to work closely with each other to perform the routing operations. This trust assumption violates the security principles of networks [3], [4], [14]. There are many types of attacks that can threaten MANETs. Black hole attacks can greatly compromise the network resources and degrade its performance [6]. In these attacks, malicious nodes join the network, claim that they have the best path to destination nodes during the routing discovery operation, and finally, simply drop all the data packets that go through them.

Networks employ several mechanisms to protect themselves from attacks. Unfortunately, these measures do not guarantee full protection from attacks. Hence, a second line of defence that has the ability to detect emerging vulnerabilities is needed. Many systems have been developed for this purpose, most notably intrusion detection systems (IDSs). However, these network-based IDSs cannot deal easily with the huge amount of data passing through the network. Therefore, a focused feature selection strategy for deciding on the most important features might be beneficial. Then, these selected features can be fed into a learning model to build an effective detection mechanism. The use of a focused dataset will improve the accuracy and speed of detections [3], [15], [16].

Several techniques have been proposed for the detection and the prevention of such attacks. Generally, these techniques are divided into two categories: securing existing protocol or using intrusion detection systems (IDS) [8]. P. Raj *et al*. [17] proposed a secure AODV routing protocol known as the Detection, Prevention and Reactive AODV (DPRAODV). In addition to the basic AODV operation, the proposed protocol developed introduced the dynamic threshold value. According to the proposed protocol, the dynamic threshold value is calculated and updated when the RREP packet is received from the replying node the first time. The main drawback of this technique is that it is only based on a high destination sequence number feature to differentiate a malicious node from a normal node. In addition to that, the network overhead will be increased due to the exchange of ALARM messages. Moreover, in large networks, the use of this technique will require a lot of time as all the nodes in the network will have to be notified. Mistry *et al*. [18] proposed a solution to black hole attacks based on the original AODV. Their approach depends mainly on modifying the functionality of the source node. This technique increases the end-to-end delay.

Khamayseh *et al*. [11] proposed a MI-AODV protocol, which is built on top of the original AODV protocol. According to the proposed protocol, the original AODV is extended to have extra structures, where each node has a Trust Table containing the addresses of the trust nodes. In addition to that, the RREP is extended to have an additional field (trust field), which is used to indicate if the replying node is reliable or not. The authors in [8] proposed an improvement to the original AODV protocol to enhance its security against black hole attacks. In the proposed protocol, each node in the MANET has two tables, namely a Suspect Table and a Black Table. These tables are designed to contain the addresses of the intermediate nodes which failed to send the data through them. In addition to that, there is an additional acknowledgement packet. Khare *et al*. [19] proposed a Secure Ad-hoc On-Demand Distance Vector routing (SAODV) protocol. As in the original AODV, the source node in the proposed protocol tries to discover the route to the destination node by flooding the RREQ message across the network. The neighbouring nodes receive the RREQ and send the RREP back to the source node if they have a valid route in their routing table. According to the SAODV protocol, the source node does not select the route from the first reply. The main drawback of using this technique is that it increases the end-to-end delay.

Intrusion Detection Systems (IDSs) can be classified into two main types: anomaly-based and signature-based (Misuse detection model) [20]. An IDS depends heavily on the existence and availability of good and representative datasets. For this purpose, in 1999, a special dataset, known as the KDDCUP'99, was collected from real network traces [21]. Feature reduction is used to reduce the complexity and computation time of the model, where using one of the feature reduction techniques will lead to an increase in the performance of the IDS. In [20], Wa'el *et al*. proposed the Rough Set Classification Parallel Genetic Algorithm (RSC-PGA), which is a hybrid model for feature reduction. This model was tested using the KDDCUP'99 dataset. The authors in [22] employs rough theory to deal with vagueness and uncertainty in decision systems. This tool is used to identify the relevant features from all decision system features, thereby contributing to the building of an efficient rule set for classification. In the proposed model, the features are selected according to the calculation of both the discernibility matrix and information gain, where the classification produced using the selected features of both methods gives better and more accurate results than the use of the selected features using each method individually.

In order to compare the performances of different classifiers in intrusion detection, the authors in [23] analysed the C4.5 and Naïve Bayes (NB) classifiers using the KDDCUP'99 dataset. The authors reduced the 41 KDD features to 11 features and 7 features using the information gain measure. The NB and C4.5 classifiers were evaluated on the dataset using all the features, the selected 11 features and the selected 7 features. The results of the experiments showed that, in general, the overall performance of the C4.5 was better than that of the NB, where the C4.5 had the lowest error rate and the highest classification accuracy. On the other hand, the C4.5 increased the true positive rate and achieved better detection rates. Moreover, the results for both classifiers showed that their performance became more efficient when the information gain technique was used to select the relevant features. Results show that the information gain is a successful measure for selecting the most relevant features [24], [25].

Researchers in [20] proposed a set of relevant features that contribute to the detection of DoS attacks. For this purpose, they applied the NSL KDD dataset to the C4.5 algorithm with a 6-fold cross validation using the Orange canvas data mining tool to analyse this dataset. The performance was measured in terms of the accuracy and classification time. The obtained results showed that the increase in the relevant features set reduced the classification time and increased the classification accuracy.

The authors in [26] proposed a detection technique for selected black hole attacks by deploying several IDS nodes in MANET. The IDS nodes perform an anti-black hole function that estimates a suspicious value of the node. This is calculated based on the abnormal difference between the RREP and RREQ messages transmitted from the node. In [27], the authors proposed the IDAD technique, which is based on both Intrusion Detection and Anomaly Detection. This technique assumes that the activities of any node in the network is monitored. In addition, it assumes that the anomalous activities of an intruder can be identified from the normal activities of the normal nodes. The audit data, which is a pre-collected set of anomalous activities, should be available to the IDAD system, where this system compares every activity in the network with the audit data to detect the black hole node.

From the previous works, it was noted that many of the proposed techniques for securing an existing protocol against black hole attacks lacked a full understanding of the behaviour of the network with regards to black hole attacks. Moreover, most of the IDS-based techniques use either the KDDCUP'99 dataset or the NSL KDD dataset. The latter is a subset of the original KDD dataset. Both datasets are out-dated and were collected for wired domain attacks. A new MANET-oriented dataset with a focused and effective feature selection mechanism was created by [28]. This dataset is utilized to design two techniques to secure the AODV protocol against black hole attacks.

This paper is divided into 4 sections; Section 1 presents an overview of MANETS and black hole attacks. Moreover, it presents and discusses previous studies in relation to this research. Section 3 describes the proposed schemes: the BDD-AODV protocol, and Hybrid protocol. The results of the proposed solution are presented in Section 4. Finally, Section 5 concludes this work and suggests some ideas for future work.

2. PROPOSED SCHEMES

A host-based IDS was used by the nodes in the MANET, with each node being equipped with an IDS to collect the audit data. Meanwhile, an anomaly-based detection scheme was used for the detection task. This work proposed two techniques to detect and prevent black hole attacks. These techniques use the dataset developed by [28]. The general framework considered in this paper is shown in Figure 1. The detection phase is considered in this work.

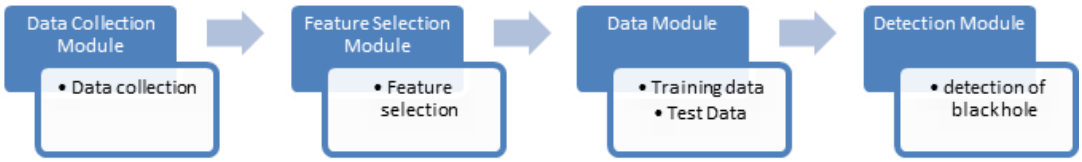


Figure 1. Proposed Intrusion Detection Model

To examine the ability of the dataset in [28] to detect black hole attacks, two routing protocols were proposed, namely: the BDD-AODV protocol and the Hybrid protocol, where these protocols depend on the BDD features. The following subsections demonstrate the working mechanisms of the BDD-AODV protocol and the Hybrid protocol.

2.1. BDD-AODV protocol

The BDD-AODV protocol modifies the behaviour of the original AODV, where each node is required to have three tables: a Trust Table, a Black Table, and a Count Table. The Trust Table includes a list of trusted nodes in the network, while the Black Table contains a list of the nodes marked as black nodes. The Count Table maintains the following statistics about the on-going activities of the network for the reply node: count of RREP from this node, count of maximum destination sequence number from the RREP of this node, and count of the low hop count reply from the RREP of this node. Moreover, the RREP in the BDD-AODV protocol has two extra fields, namely, the replying node and the replying hop count. Figure 2 depicts the BDD-AODV algorithm.

Handle RREQ Message	Handle RREP Message by Source node	

If (source node of the RREQ is not exist in TT)
Insert source node of the RREQ to TT
If (destination node of the RREQ is not in TT)
Insert destination node of the RREQ to TT
If (last node that sends the RREQ is not in TT)
Insert last node of the RREQ to TT
If (Intermediate node doesn't have valid route to destination)
Re-broadcast RREQ
If (RREQ is received by destination node, intermediate has a valid rout or malicious node) → Unicast RREP to the source node
	If (destination node of the RREP is not in TT) → Insert destination node of the RREP to TT	

Handle RREP Message by Intermediate node	If (RREP sender! = Replying node) → Add RREP sender to the TT
	If (Replying node is not in CT)
	Add Replying node to the CT
	Count of RRER from the Replying node =1
	If (dst sequence number > 6292) → Max high sequence =1
	Else → max high sequence = 0
	If (1 < replying hop count <= 2) → Low replying count =1
	Else low replying count =0
	Else If (Replying node in CT)→ ++ Count of RRER
	If (destination sequence number > 6292) → Max high sequence destination ++
	If (replying hop count > 1 and <= 2) →Low replying hop count hop ++
		If (replying node exists in TT)
		Send data packet
		Else If (replying node exist in BT)
		Discard RREP and wait another RREP
		Else If (Count of RRER from the Replying node = max high sequence destination = replying ho count and Count of RRER from the Replying node>=1)
		Add Replying node to the BT
		If (replying node exists in BT)
		Discard RREP and wait another RREP
		Else send data packet

If (source node of the RREP is not exist in TT)
Insert source node of the RREP to TT
If (destination node of the RREP is not exist in TT)
Insert destination node of the RREP to TT
If (RREP sender! = Replying node) →Add RREP sender to TT		

Figure 2. BDD-AODV algorithm

2.2. Hybrid protocol

The Hybrid protocol combines both BDD-AODV and MI-AODV [11] protocols to derive a more realistic and effective detection mechanism. In the MI-AODV protocol, the trust field is used to indicate if the replying node is reliable or not. It is given a value of either 0, 1 or 2. In the Hybrid protocol, each node is provided with two tables, namely, a Trust Table and a Black Table. In addition to that, every source node in the network is provided with a Count Table. The processes for the handling of the RREQ in the BDD-AODV protocol and Hybrid protocol are similar. Figure 3 shows the algorithm for the handling of the RREQ messages.

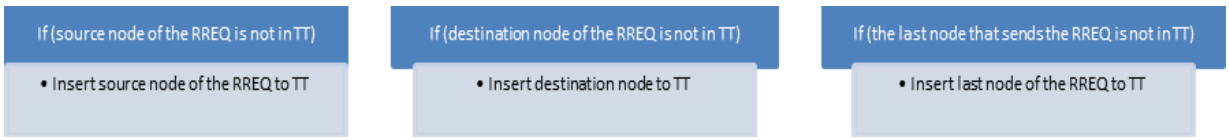


Figure 3. Handling of RREQ Messages in Hybrid Protocol

Figure 4 shows the algorithm for the handling of the RREP by the source node.

Handle RREP Message by Source node	
If (destination node of the RREP does not exist in the TT) → Insert destination node of the RREP to TT	

If (RREP sender! = Replying node) → Add RREP sender to the TT
If (Replying node does not exist in CT) { Add Replying node to the CT
Count of RRER from the Replying node =1
If (destination sequence number > 6292) → Max high sequence destination =1
Else max high sequence destination =0
If (replying hop count > 1 and <= 2) → Low replying hop count hop =1}
Else low replying hop count hop =0}
Else If (Replying node exists in the CT) { Count of RRER from the Replying node ++
If (destination sequence number > 6292) →max high sequence ++
If (replying hop count > 1 and <= 2) → low replying hop count ++}
	If (Trust field value = 1 or 2)
	If (Replying node does not exist in TT)
	Insert Replying node to TT and Send data packet
	Else If (Trust field value = 0)
	If (Count of RRER from the Replying node = max high sequence destination = replying to count and Count of RRER from the Replying node > = 1) → Add Replying node to the BT
	Else If (Trust field value equal -1)
	If (Replying node does not in BT) →Insert Replying node to BT
	If (Replying node does not exist in BT) → S sends the data packet
	Else Discard RREP and wait for another RREP}

Figure 4. Algorithm for the handling of the RREP by the source node

3. SIMULATION AND ANALYSIS OF RESULTS

To evaluate the performance of the proposed protocols, simulation experiments were conducted. GloMoSim simulator was used to evaluate the performance of four different protocols, namely, the Hybrid protocol, BDD-AODV protocol, MI-AODV protocol, and original AODV protocol. Table 1 summarizes the simulation parameters.

Table 1. Simulation Parameters

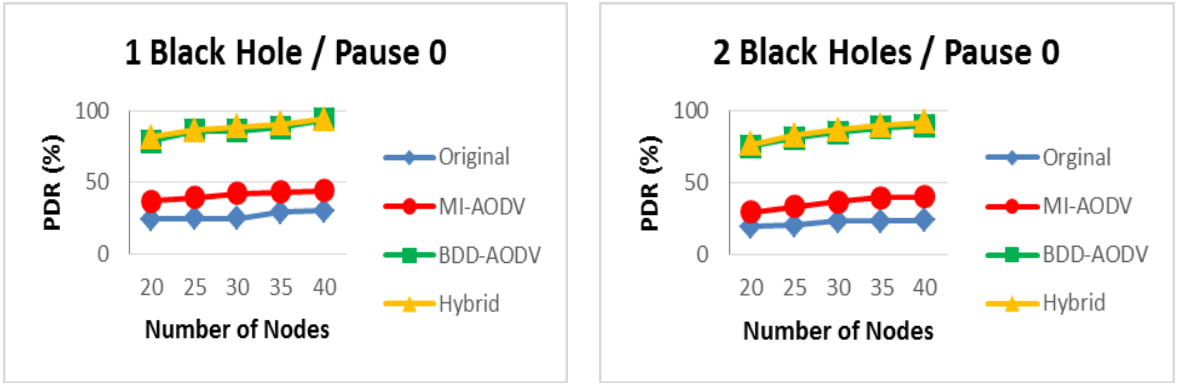
Parameter	Value	Parameter	Value
Simulator	GloMoSim 2.03	Minimum nodes' velocity	0.5 meter/second
Simulation duration	1200 seconds	Maximum nodes' velocity	2 meter/second
Number of nodes	20, 25, 30, 35,40	Radio range	250m
Mobility Model	Random waypoint	Bandwidth	2 Mb/s
Pause time	0, 10	Traffic Type	CBR
Simulation area	1000 m * 1000 m	CBR packet size	512 tes

Four performance matrices were measured: Packet Delivery Ratio (PDR), Dropped Packets Ratio, Average End-to-End Delay and Overhead. Eight different scenarios that were simulated in this research. These scenarios were simulated with different parameters, where these parameters had a direct impact on the black hole attack. These parameters are: the total number of nodes, the number of black hole nodes, and the pause time (2 pause time values were tested: 0 and 10. A pause time of 0 indicates a high mobility, while a pause time of 10 indicates a slow mobility).

3.1. High mobility scenarios

In all the following figures, the blue line represents the original AODV protocol, the red line represents the MI-AODV protocol, the green line represents the BDD-AODV protocol, and the orange line represents the Hybrid protocol.

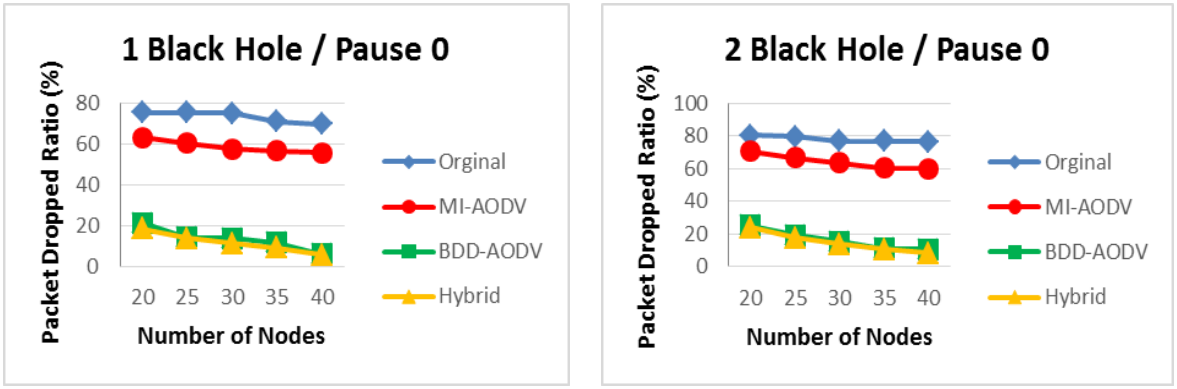
Figure 5 shows an improvement in the Packets Delivery Ratio (PDR) for all the 4 protocols for a network that was being attacked by 1 and 2 black hole(s). The obtained results show that the Hybrid protocol in the network, which was attacked by one black hole node, had the highest packet delivery ratio. As shown in Figure 5, the PDR increased when the number of nodes increased. As a result of increasing the number of normal nodes in the network, the source node had a better chance of receiving the RREP messages from the normal and reliable nodes. It was noted that the existence of a second black hole node caused a slight decrease in the packet delivery ratio.



(a) (b)

Figure 5. Packet Delivery Ratio with Pause Time 0, (a) 1 Black Hole, (b) 2 Black Holes

Figure 6 shows that the BDD-AODV and Hybrid protocols contributed to a decrease in the number of dropped packets compared to the original AODV and MI-AODV protocols for a network that was attacked by 1 and 2 black holes.

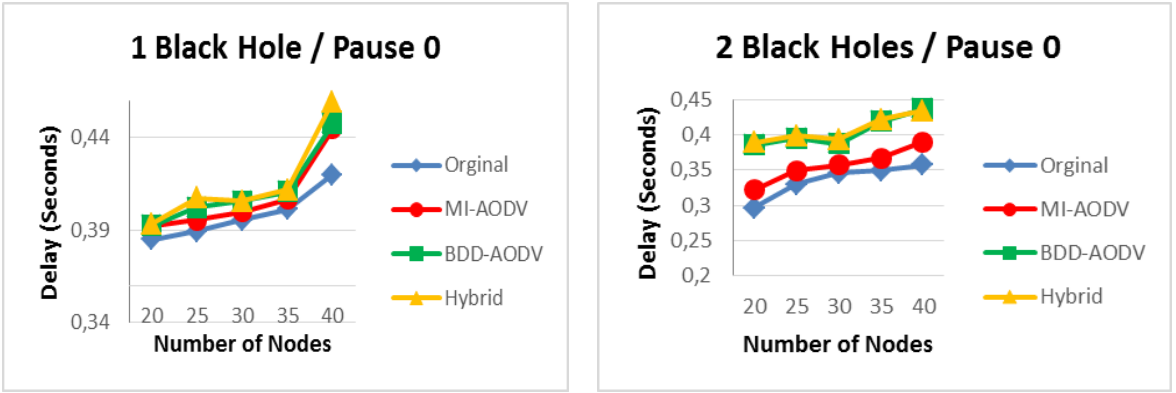


(a) (b)

Figure 6. Packet Drop Ratio with Pause Time 0, (a) 1 Black Hole, (b) 2 Black Hole

As shown in Figure 6, the number of dropped packets decreased as the number of nodes increased from 20 to 40. Within this interval, each source node was surrounded by more normal neighbors, while the number of black hole nodes in the network was fixed at 2. Therefore, the source nodes in the network had the chance to receive more alternative active routes to the destination from the normal and reliable nodes. The agreement between the results of the dropped packets and packet delivery ratio could be observed. Moreover, increasing the number of black holes led to increase in the number of dropped packets.

Figure 7 shows the end-to-end delay results for the Hybrid, BDD-AODV, MI-AODV and orginal AODV protocols when the network was attacked by 1 and 2 black holes. On the other hand, Figure 7 shows the end-to-end delay results when the network was attacked by two black hole nodes. According to the results in both figures, the Hybrid and BDD-AODV protocols increased the end-to-end delay compared to both the MI-AODV and original AODV protocols. For a network attacked by one black hole, the original AODV achieved the best end-to-end delay result, while the Hybrid protocol acheived the highest end-to-end delay result.

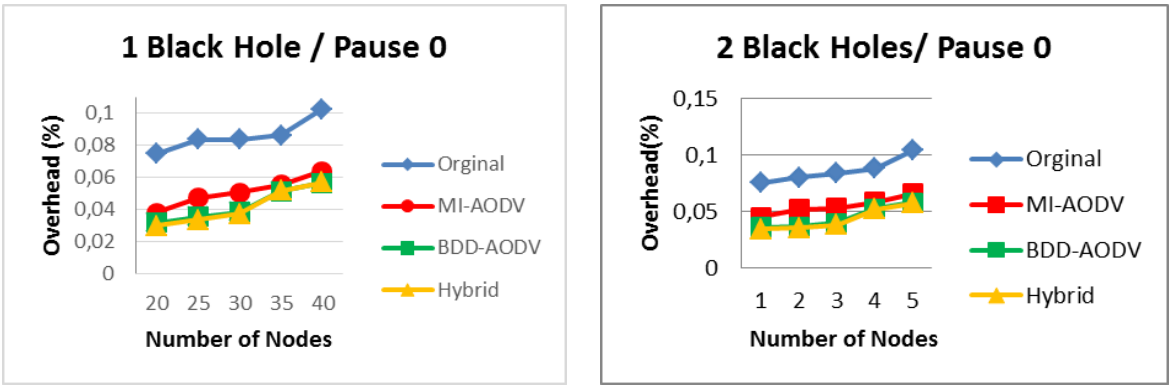


(a) (b)

Figure 7. Delay with Pause Time 0. (a) 1 Black Hole, (b) 2 Black Hole

As shown in Figure 7, the end-to-end delay increased for all the protocols when the number of nodes increased. This increase in the number of nodes decreased the chances of the destination node becoming the neighbour of the source node. Therefore, the packets were transmitted over several hops in order to reach the destination node. Moreover, the Hybrid and BDD-AODV protocols were required to perform more operations to detect and avoid the black hole node, and hence, increased the delay. A similar pattern was obtained in the case of a network being attacked by two black hole nodes. The original AODV achieved the best end-to-end delay compared to the other three protocols, while the Hybrid protocol achieved the highest end-to-end delay result.

As shown in Figure 8(a), the overhead increased as the number of nodes increased from 20 to 40 nodes. This could be interpreted to mean that the increase in the number of nodes in the network led to an increase in the number of control packets (e.g. RREQ and RREP) that were exchanged through the network. The original AODV achieved a significantly higher overhead against all the other protocols due to the existence of the black hole and the lack of any detection and prevention mechanism.

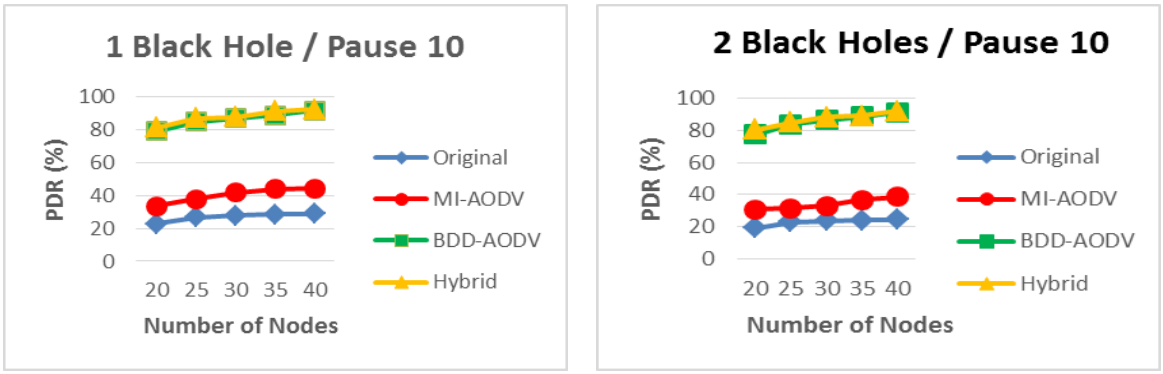


(a) (b)

Figure 8. Overhead with Pause Time 0, (a) 1 Black Hole, (b) 2 Black Hole

3.2. Low Mobility Scenarios

The performance of the tested protocols was evaluated under the assumption of low mobility. As shown in Figure 9, for networks attacked by one black hole and two black hole nodes, the Hybrid and the BDD-AODV protocols outperformed both the MI-AODV and the original AODV protocols in terms of the packet delivery ratio.

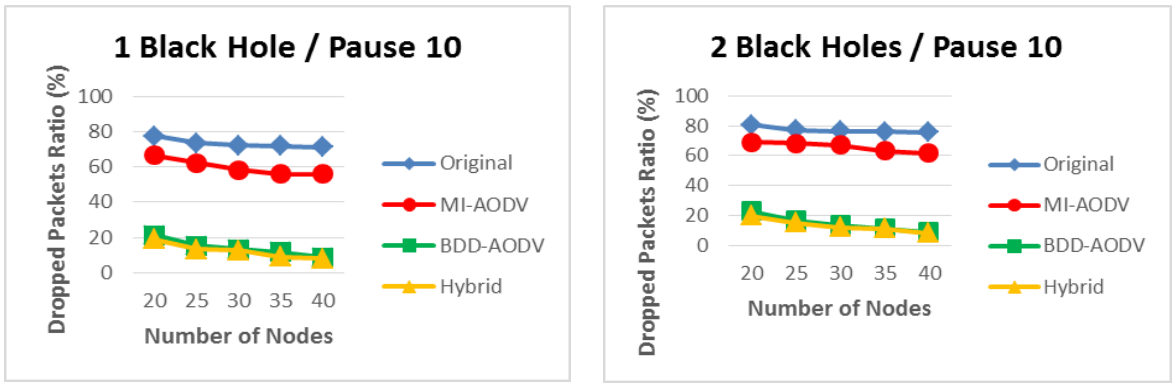


(a) (b)

Figure 9. Packet Delivery Ratio with Pause Time 10, (a) 1 Black Hole, (b) 2 Black Holes

Figure 9(a) shows the packet delivery ratio results for a network that was being attacked by one black node. The packet delivery ratio increased when the number of nodes in the network increased from 20 to 40 nodes. Within this interval, increasing the number of nodes in the network led to a decrease in the chances of the black hole nodes to obtain RREQ messages. Thus, the chances of the black hole nodes dropping data packets also decreased. Moreover, increasing the number of normal nodes in the network increased the possible number of node neighbours, hence increasing its chances of getting to the destination node(s) successfully. Figure 9(b) shows that the packet delivary ratio increased when the number of nodes increased from 20 to 40 nodes. The addition of a second black hole had a negative effect on the packet delivery ratio.

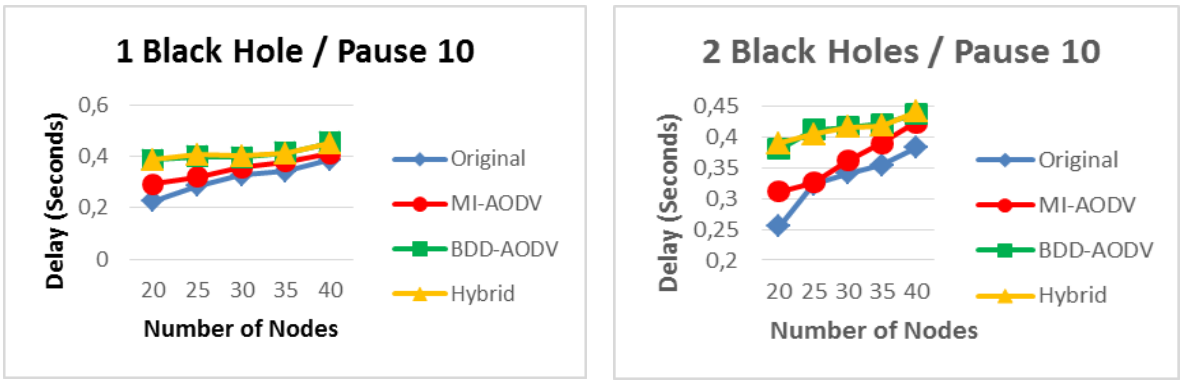
Figure 10 shows that the dropped packets ratio for all the protocols decreased as the number of nodes increased from 20 to 40 nodes. Again, adding a second black hole increased the number of dropped packets for both cases. From Figure 9 to Figure 10, the agreement between the dropped packets results and packet delivery ratio results can be observed, where the protocol which had a high dropped packets ratio was the protocol with a low delivery ratio.



(a) (b)

Figure 10. Dropped Packets Ratio with Pause Time 10, (a) 1 Black Hole, (b) 2 Black Holes

Figure 11 shows the end-to-end delay results for a network being attacked by one and two black hole nodes. The Hybrid and BDD-AODV protocols worked properly with a pause time of 10, where these two protocols increased the end-to-end delay compared to the MI-AODV and original AODV protocols.



(a) (b)

Figure 11. Delay with Pause Time 10, (a) 1 Black Hole, (b) 2 Black Holes

As shown in Figure 11(a), the end-to-end delay increased for all the protocols when the number of nodes increased from 20 to 40 nodes. The Hybrid protocol achieved the highest end-to-end delay results compared to the other three protocols, while the original AODV achieved the lowest end-to-end delay results. This difference in the results was due to the difference in the packets delivery ratio obtained from each protocol, where increasing the packets delivery ratio required more time, thereby increasing the end-to-end delay results.

For a network attacked by two black hole nodes, the original AODV showed the best end-to-end delay compared with the other protocols. The Hybrid protocol showed the highest end-to-end delay results. Figure 11(b) shows the end-to-end delay results for a network being attacked by two black hole nodes. Any increase in the PDR resulted in an increase in the end-to-end delay. As the Hybrid protocol had the highest PDR, hence it had the highest end-to-end delay.

For a pause time of 10, the Hybrid and BDD-AODV protocols outperformed the MI-AODV and the original AODV protocols with respect to the overhead. Figure 12 shows the overhead results for networks being attacked by one black hole and two black holes.

(a) (b)

Figure 12. Overhead with Pause Time 10, (a) 1 Black Hole, (b) 2 Black Holes

As shown by Figure 12, the overhead increased as the number of nodes increased from 20 to 40 nodes. This indicated that increasing the number of nodes in the network will lead to an increase in the number of control packets (e.g. RREQ and RREP) exchanged through the network. Figure 12(b) shows that the overhead results for the original AODV was significantly higher than the overhead for the other three protocols. This was due to the impact of black hole nodes in the original AODV and the absence of any detection and prevention mechanism. Decreasing the impact of black hole in the network led to a decrease in the network overhead.

4. CONCLUSION AND FUTURE WORK

A common threat to MANETs is black hole attacks. This paper was built on top of the work done in [28] to enhance the security level in MANETS. To fully utilize the BDD dataset, a BDD-AODV protocol was proposed, which depends on the features of the BDD dataset to build its prevention and detection mechanisms. The BDD-AODV protocol modifies the behaviour of the original AODV, making it more secure against black hole attacks, where it checks the reliability of the node that sends the RREP message. The Hybrid protocol was created by combining the MI-AODV and BDD-AODV protocols, including all the features of the BDD dataset. In other words, the working mechanism of the MI-AODV protocol was combined with the working mechanism of the BDD-AODV protocol in order to create a Hybrid protocol. As in the BDD-AODV protocol, each node in the MANET has a Trust Table, a Black Table, and a Count Table. Simulation results showed that the BDD-AODV and the Hybrid protocols reduced the impact of black hole attacks and outperformed both the original AODV and MI-AODV protocols in terms of the PDR, dropped packets ratio, and overhead, while the end-to-end delay was maintained in some intervals.

The cooperative and selective black hole nodes were not considered in this work. The cooperative black hole problem occurs when more than one black hole cooperates together. On the other hand, the selective black hole attacks select a set of data packets to be dropped, delivered to the destination node, or modified. It is proposed that the behaviour of cooperative and selective black holes be studied and the BDD dataset be expanded to include the relevant features that contribute to the detection of these attacks. Moreover, it is proposed that the BDD-AODV and Hybrid protocols be enhanced with certain mechanisms to solve these two problems. In addition, the experimental results showed that the end-to-end delay in the Hybrid and BDD-AODV protocols was higher than the delay in the original AODV. Therefore, there is a need for further improvements in order to reduce the delay values.

REFERENCES

[1] Ochola E. O. and Eloff M. M., "A Review of Black Hole attack on AODV Routing in MANET," *ISSA*, 2011.
[2] T. Kaur and A. Singh, "Performance Evaluation of MANET with Black Hole Attack Using Routing Protocols," *International Journal of Engineering Research and Applications (IJERA)*, vol/issue: 3(4), 2013.
[3] S. Kumar, *et al.*, "An Empirical Critique of On-Demand Routing Protocols against Rushing Attack in MANET," *International Journal of Electrical and Computer Engineering (IJECE)*, vol/issue: 5(5), pp. 1102-1110, 2015.
[4] Aarti and S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol/issue: 3(5), 2013.
[5] R. M. Desai, *et al.*, "Routing Protocols for Mobile Ad Hoc Network - A Survey and Analysis," *Indonesian Journal of Electrical Engineering and Computer Science*, vol/issue: 7(3), pp. 795-801, 2017.
[6] A. P. Murdan and A. Bhowon, "Mobile Ad Hoc Networks in Presence of Black Hole Attack," *Indonesian Journal of Electrical Engineering and Computer Science*, vol/issue: 7(2), pp. 577-582, 2017.
[7] Goyal, *et al.*, "MANET: Vulnerabilities, Challenges, Attacks, Application," *International Journal of Computational Engineering & Management (IJCEM)*, vol.11, 2011.
[8] B. Nawafleh, *et al.*, "Improved AODV Protocol to Detect and Avoid Black Hole Nodes in MANETs," Master Thesis in Computer Science, Dept.of Comp.Sci., JUST Univ., 2012.
[9] Baadache, *et al*., "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks," *International Journal of Computer Science and Information Security (IJCSIS)*, vol/issue: 7(1), 2010.
[10] Saini, *et al.*, "Comparison between Various Black Hole Detection Techniques in MANET," *National Conference on Computational Instrumentation*, 2010.
[11] Y. Khamayseh, *et al*., "A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol/issue: 3(1), 2011.
[12] Battula, *et al.*, "Mixed signal based transmission in mixed layers for high throughput wireless network," *Elixir International Journal*, 2011.
[13] Taneja, *et al.*, "A Survey of Routing Protocols in Mobile Ad Hoc Networks," *International Journal of Innovation Management and Technology*, vol/issue: 1(3), 2010.
[14] Singh, *et al.*, "Security Issues And Link Expiration In Secure Routing Protocols In Manet: A Review," *Network*, vol/issue: 3(7), 2014.
[15] Liu, *et al.*, "Toward Integrating Feature Selection Algorithms for Classification and Clustering," *Knowledge and Data Engineering, IEEE Transactions*, vol/issue: 17(4), 2005.
[16] John, *et al.*, "Irrelevant Features and The Subset Selection Problem," *ICML*, vol. 94, 1994.
[17] Raj, *et al.*, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET," *International Journal of Computer Science Issues (IJCSI)*, vol. 2, 2009.
[18] Mistry, *et al.*, "Improving AODV Protocol Against Attacks," *International Multi Conference of Engineers and Computer Scientists (IMECS)*, vol. 2, 2010.
[19] Khara, *et al.*, "Security in Routing Protocol to Avoid Threat of Black Hole Attack in MANET," *International journal of Electrical, Electronics & Communication Engineering*, vol. 2, 2012.
[20] Bhoria, *et al.*, "Determining Feature Set of DOS Attacks," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, 2013.
[21] KDDCUP, 1999. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.
[22] Rissino, *et al*., "Rough Set Theory–Fundamental Concepts, Principals, Data Extraction, and Applications," *Data Mining and Knowledge Discovery in Real Life Applications*, 2009.
[23] Upendra, "An Efficient Feature Reduction Comparison of Machine Learning Algorithms for Intrusion Detection System," *International Journal of Emerging Trends & Technology in Computer Science*, vol. 2, 2013.
[24] M. Tavallaee, *et al.*, "A detailed analysis of the KDD CUP 99 data set," *Proceedings of the Second IEEE international conference on Computational intelligence for security and defense applications (CISDA'09). IEEE Press, Piscataway, NJ, USA*, pp. 53-58, 2009.
[25] J. Mchugh, "Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory," *ACM Transactions on Information and System Security*, vol. 3, 2000.
[26] M. Y. Su, "Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks through Intrusion Detection Systems," *Computer Communications*, vol/issue: 34(1), 2011.
[27] Alem, *et al.*, "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection," *IEEE*, vol. 3, 2010.
[28] M. B. Yassein, *et al*., "Feature Selection for Black Hole Attacks," *Journal Of Universal Computer Science*, vol/issue: 22(4), pp. 521-536, 2016.