International Journal of Communication Networks and Information Security

ISSN: 2073-607X, 2076-0930

Volume 14 Issue 02 Year 2022 Page 99:110

Performance Ameliorations of AODV by Black Hole Attack Detection Utilizing IDSAODV as Well as Reverse AODV

Mohammed Al-Shabi

Department of Management Information System, College of Business Administration, Taibah University, Saudi Arabia.

mshaby@taibahu.edu.sa

Article History

Received: 24 Feb 2022
Revised: 27 May 2022
Accepted: 18 June 2022

Abstract

The so-called Black Hole Attack is among the most perilous and widespread security attacks in MANET nets, researchers have been tasked with developing strategies to detect it. Two of these methods are the Intrusion Detection System AODV (IDSAODV) as well as the Extended AODV. The present paper attempts to investigate the impact of a Black Hole Attack on the functionality of the network in the existence of single or more attackers. It also evaluates the Extended AODV and IDSAODV in a net in order to see how effectively they could detect and mitigate the attack. For the aim of evaluating its performance, the researchers utilized Throughput, Normalized Routing Load (NRL), and Packet Delivery Ratio (PDR). The comprehensive simulation results show that the IDSAODV application decreased the effect of the attacks. However, it raised the rate of packet delivery to sixty eight percent at the identical time. Reverse AODV, on the other hand, provided superior outcomes, with a PDR of 100%, but also resulted in an exceedingly higher NRL than the IDSAODV. Likewise, the simulation findings demonstrated that the attacking node's position tormented the IDSAODV's functionality.

Keywords: Mobile Wireless Networks, Black Hole Attack, IDSAODV, Reverse AODV.

1. Introduction

MANETS mobile private wireless networks are defined as a group of independent and self-managed mobile nodes without an infrastructure [1], where nodes cooperate to deliver messages to their targets using routing protocols responsible for finding the path between the source as well as target. Some of the MANET protocols, namely Ad-hoc On-demand Distance Vector (AODV), reverse-AODV (RAODV), Destination Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR), Ad-hoc On-demand Multipath Distance Vector (AOMDV), and Temporarily Ordered Routing Algorithm (TORA) [2]. Both AODV and DSR are two of the most requested protocols which are applied in MANETs [3]. Achieving security in these networks is a challenge that is difficult to achieve due to a variety of reasons, including changing topology, limited bandwidth, lack of central management, and constant mobility of nodes. Routing is vulnerable to many security risks and attacks, and the Black Hole assault is one of the latter; It drops packets into the network, thus preventing them from reaching their intended destination [4].

The black hole is considered as a particular type of brutal attacks, and it resembles a puncture which damages every data packet on its own [5]. The malicious nodes also disrupt route discovery, allowing the attacker to absorb network packets. The role of the intermediate nodes is to find a given correct path for the destination node in AODV path detection through sending "hello" packets to the neighbours. Instead of sending discovery packets to surrounding nodes, the rogue nodes seeking to react to the source ones with a fake path reply as though they have a proper path to the destination in AODV [6]. Consequently, the source node transfers its own data packets to the target node through the malicious node, assuming that latter is a correct path. The net, therefore, is vulnerable to a black hole assault, in which rogue nodes deliberately misbehave as well as cause harm to the node interface. The nodes in the net will generally be nervously looking for a path to the destination, using resources and causing packet loss [7]. The black hole attack occurs in MANET networks with single or more malicious nodes declaring that they have the shortest and most recent route leading to the target at the time of issuing a Route Request (RREQ) message by the source node to the surrounding nodes so as to discover that path.

The purpose of the present study is to investigate the impact of the black hole attack on the efficiency of MANET networks that utilize AODV as a transmit protocol. Furthermore, it aims to check the efficacy of IDSAODV and Reverse AODV protocols in detecting the black hole node by simulating different scenarios of the MANET network. This is for the goal of selecting which protocol provides the network with the preferable functioning, according to a set of variables like the throughput, the normal routing load, as well as the rate of packet transmission. Moreover, the remaining section of this research is organized as along these lines: The related studies are demonstrated in part 2. The Black hole attack in MANET security is discussed in the third part. The experimental study including the emulation materials as well as environment parameters are explained in section 4. In addition, the result and discussion implementation in AODV and Reverse AODV with different scenarios are illustrated in part 5. At last, the sixth part of this paper clarifies the conclusion as well as the prospective remarks.

2. Related Works

With the aim of founding dependable communication between the nodes in a given unsuitable milieu, MANET has become an essential study area [8]. However, these networks have several security issues. The authors of [9][10] have recommended improving MANET security. In particular, the authors of [11] proposed a neuro-fuzzy approach for MANETs that is similar to IDS. The IDS was introduced by the authors of [12] for the purpose of uncovering as well as recognizing the attackers by using an ambiguous method. In order to enhance the probability of detecting as well as preventing the black hole attackers in MANETs, the authors in [13] suggested an improved trust discovery technique. In case of the existence of malignant black hole nodes, this approach avoids the nodes of the black hole in MANETs, and it raises the throughput of the net, as well as reduces the packet loss together with the power consuming. Another solution suggested by the researchers [14] is an efficient detection method with low network overhead. Further, the authors [15].

proposed a new approach dependent upon an effective threshold value of the target sequence number to discover and restrain the nodes of the black hole, which outperforms the black hole assault. The authors in [16] showed that it affects interactive routing protocols more than other protocols because it requires the path on demand only, while non-interactive protocols depend on maintaining all paths permanently before sending the data. In contrast, the authors in [17] examined the impact of this assault over the net that utilizes AODV protocol, and they came to the conclusion that the black hole assault had significantly affected the packet delivery rate in the network. Others in [18] also tested the effect of increasing the number of attacking nodes and concluded that network performance deteriorated significantly, and its productivity decreased when the number of attackers increased.

Some researchers [19][20][21][22] went to find techniques to detect this attack and tried to prevent it. Researchers have classified black hole attack detection techniques into many categories, some of which depend on encryption, others that depend on determining the threshold of the number indicating the novelty of the path, and other techniques that depend on eavesdropping and achieving trust between nodes [23]. The authors in [24] proposed to IDSAODV by modifying the AODV protocol with aim of decreasing the effect of the Black Negev assault. Other researchers [25] have proposed Reverse AODV to prevent Denial of Service (DOS) assaults as well as conclude that it significantly improves packet delivery and network throughput.

While the authors in [26] combined the two previous improved protocols and achieved effective results in Mesh wireless networks, most researchers overlooked the effect of the location of the attacking node on the functioning of these particular protocols. In the present study, we investigated the influence of implementing both IDSAODV and Reverse AODV in the network in the event of one or more attackers, and the focus was on studying the cost of implementing these two protocols in the absence of an attack.

The reason for choosing them is that researchers in previous studies [24] and [25] ignored to study the cost of using them in the network in the absence of the attack, as we studied the impact of the performance of each of them on the location of the attacking node for the sender and receiver since these ideas have not been studied in advance.

3. Black hole attack in MANET

MANETs are vulnerable to various threats and attacks such as black holes, impersonation, wormholes, snooping, Address Resolution Protocol (MiTM attack), and Gray holes. Likewise, the indicated ones are either active or passive assaults [27]. This specific paper investigates the black hole assault, yet none of the other attackers is discussed.

3.1 The Black hole Attack in MANETS Dependent upon AODV Routing Protocol

The following describes how the black hole attack in MANETS networks, which uses the AODV routing protocol to find paths from the transmuting to the receiving nodes, operates:

- Sending a route request message (RREQ) to the surrounding nodes allows the source node to recognize the path when it needs to transfer the data packets to another one.
- The rogue node receives this message and then sends a path reply message RREP (Route Reply), informing the sender it owns the most current and very short route leading towards the destination.
- At the time the first RREP message coming from the rogue node reached the sender, the latter ignores any RREP messages that come from other nodes and only transfers the data packets along the route that the rogue one has defined.
- Malicious nodes receive and drop these packets, preventing them from reaching their actual time.

3.2 MANETS Black Hole Attack Detection Techniques

Several techniques have appeared for the purpose of revealing the black hole assault. The current study, however, concentrates on both IDSAODV and Reverse AODV.

3.2.1 AODV Intrusion Detection System (IDSAODV)

IDSAODV is an upgraded protocol from the AODV protocol proposed by the researchers to enhance the performance of MANETS networks in case of the existence of a black hole assault. Further, IDSAODV lets the source node ignore the created path by the first reply packet and the response by the second reply packet. IDSAODV assumes that the first (fastest) response always comes from an attacking node, but this assumption is not always correct. For instance, there may be a long distance between the attacking node as well as the source node while the target node may be close to the former one. In this scenario, the actual target node will provide the initial response. This particular protocol shows that this response will be ignored as well as the following response that may come from the black hole node [24].

IDSAODV algorithm is summarized along the coming lines:

1. The source node transfers a given route request message; RREQ is a public broadcast.
2. The source node receives multiple RREP; request-response messages.
3. The source node ignores the initial RREP packet assuming that it is sent by a rogue node.
4. The second reply packet is accepted by the source node, which regards it as a trusted node, updates its routing table, and starts sending its data according to the information in this packet.

3.2.2 Reverse AODV Protocol

This protocol was initially designed to solve the problem of reply packet loss since the Reverse AODV addressed the problem of Unicast Route Reply [28], which is one of the weaknesses of the AODV protocol that attackers use in their attack, making it utilize a suffix with aim of relieving the effect of the black hole assault [9]. This protocol relies on flooding the reply message in the network and creating several routing paths between the source and the target.

The working mechanism of the Reverse AODV protocol:

1. The source node broadcasts a public RREQ packet to its neighbour nodes, which in turn resends it to its neighbour nodes up to the time which it arrives at the target one.
2. When a RREQ message reaches the initial destination, it broadcasts to its neighbours a packet called Reverse Route) R-RREQ (which includes the route request-response information. Then, the neighbours, in turn, send this packet to their neighbours after modifying and updating them
3. routing tables the information till reaching the source node.
4. When R-RREQ packets come to the source node, the latter stores the available routing paths in order to transmit the data packets between the source as well as the target, selects a best (shorter and newest) path, and sends the data packets to the target through it.
5. In the event of failure of the chosen path, the source node chooses an alternative path from the stored paths. As a result, when an attacker is in the network, it will respond to the R-Request message directly, indicating it owns a particular route leading towards the destination. Whereas, the source node will not respond to it since it is excepting to receive the R-RREQ message from the target one, and it will isolate and delete it from its routing table. The Reverse AODV Protocol’s drawback is that it causes network overload and delays by flooding reply messages across the entire network.

4. Experimental Study

The researchers of this paper conducted a theoretical study on the mechanism of the black hole attack and how it affects the network performance, and they searched for the solutions proposed by the researchers to detect and mitigate its effects. First, the researchers used the NS2 network simulator [29] to build different scenarios to study the efficacy of some of these solutions with one or more attackers in the network. Then, they used the Nam 1.14 tool to show the network topology and the Trace files to calculate the results. Finally, they analysed the results to find out the most appropriate protocol to detect the black hole assault in MANET network under different values of some network parameters and according to the set of metrics.

4.1 Building the network model

The researchers used the NS2 network simulator to build a model of a MANET network consisting of 20 wireless connected nodes with the same capabilities (homogeneous). These nodes are spread randomly over an area measuring 1186 m * 600 m, with no considerations given to how many nodes should be included in a network. This number had been selected in such an arbitrary manner in order to create the MANET network and investigate how the black hole assault affected it. These nodes (except the attacking ones) have a motion with constant speed which is 2 m/s, and it represents the average walking speed that characterizes humans. In addition, some of these nodes generate data packets of 1500 bytes and send them to specific targets at a rate of 0.1 Mb/s using the AODV routing protocol to determine the paths to those targets.

4.2 Simulation Scenarios

The first scenario: This scenario aims to evaluate the functioning of a particular MANET network through utilizing AODV protocol while being subjected to a black hole attack by one or more attackers. That is to study the attacks' impact on network performance.

The second scenario: This scenario intends to assess how well a MANET network performs when subjected to a black hole assault by one or more attackers by applying both Reverse AODV and IDSAODV protocols. That is to study the efficacy of each of them in detecting the attack.

The third scenario: The goal of this scenario is examining the influence of how well both Reverse AODV and IDSAODV protocols perform with the location of the attacking node relative to the sending node.

Table 1. Demonstrates a group of network parameters and their own values.

Parameters	Values
Type of Channel	Wireless channel
Simulation time (second)	600
Package size	1500
Transport Layer Protocol	UDP
Data rates	0.1
Routing protocols	AODV without BH, Black hole AODV, IDSAODV, Revers AODV
Total Nodes	20
No. Attacker nodes	0,1,2,3
Nodes Speed (m/s)	2
No. of CRB connections	10
Simulation Area (m2)	1180*600

4.3 Performance Evaluation Parameters

In this paper, the researchers will depend on a set of parameters: packet delivery ratio, average throughput, and natural routing burden. Because throughput as well as packet delivery ratio are both utilized for the purpose of assessing how well the network performs, these parameters were chosen. Therefore, the higher the values of these criteria, the better the performance. While the overhead is used in routing to calculate the cost of implementing the routing protocol in the net regarding the routing packets number, and it generates to find and maintain paths between the sender and receiver. These parameters are clarified along the following lines:

4.4 PDR packet delivery ratio

This ratio will be reduced in the AODV black hole protocol provided that the attacker drops data packets. It is defined as the ratio of total number of the packets reached at the destination to the total number of packets sent from the source [29] and is given by:

$$PDF = \frac{\sum number\ of\ packets\ received\ by\ the\ CBR\ destination}{\sum number\ of\ packets\ send\ by\ the\ CBR\ sources} \qquad (1)$$

4.5 Average Throughout [kbps]

The data value reached at the network nodes in bits throughout the simulation time [29] will decrease with the presence of the attack because the attacker prevents packets from reaching the target and is given by the relation:

$$Average\ Throughput = \frac{\sum number\ of\ packets\ received\ by\ CBR\ destination}{Simulation\ time} \qquad (2)$$

4.6 Normalized Routing Load

It is defined as the ratio of the total number of received routing packets to the number of received data packets [30] and is given by:

$$\mathrm{NRL} = \frac{\sum \text{total number of routing packets received}}{\sum \text{total number of data packets received}} \qquad (3)$$

5. Results and discussion

5.1 The Results of the First Scenario

The results of figures 1, 2, and 3 demonstrate how MANET net employing the AODV routing protocol performs in both the normal state without an attack (represented in this state with several attacking nodes equal to zero) and during the existence of the black hole assault by a number of uncooperative attacking nodes (one, two, and three attacking nodes).

The results of Figurer 1 show that when an attacking node was present in the net, it caused the reduction of packet delivery ratio, which became 28% after it was 100% in the normal state (taking into consideration that there is no packet loss due to external conditions such as interference that may affect the link). The extensive loss of packets is due to the attacker's condition; the attacker is working.

Therefore, the packet delivery rate in some connections will reach zero. However, since there is more than one CBR connection between nodes in the business scenario, the value of the PDR in the network does not decrease to zero. From the figure, the researchers noticed that this percentage continued to drop as the attacking nodes number rose, reaching 18% when there are three attacking nodes.

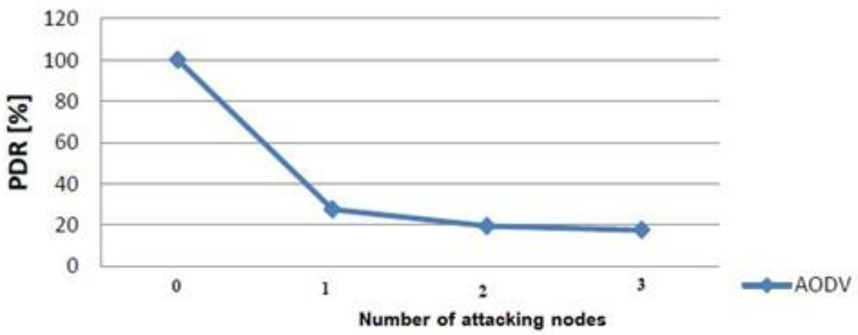

Figure 1. Relationship between Packet Delivery Ratio together with Attack Nodes Number in a MANET.

Figure 2 demonstrates how an attacking node existence in the network led to a decrease in the network throughput, as it became 23 kbps after it was 68 kbps in the normal state. That is clarified within the reality that the attacker is dropping the data packets that it receives instead of resending them to its targets. Furthermore, from the figure, the researchers noticed that the throughput continued to decrease with the increase of attacking nodes' number, reaching 15 kbps when there were three attacking nodes.

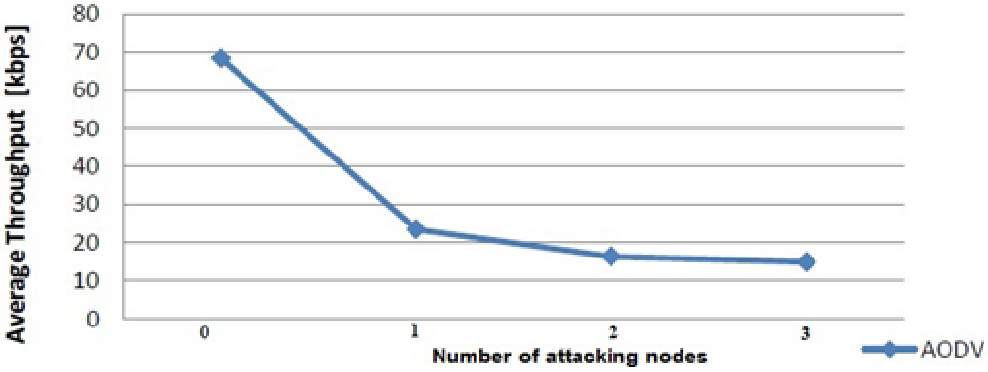

Figure 2. *Relationship between Average Throughput and Attacking Nodes Number In MANET.*

The figure 3 shows that NRL increased to 0.22 with the presence of an attacking node compared to 0.033 without an attack. It also continued to increase with the increase of the attackers' number, reaching 0.41 when there were three attacking nodes because of the decrease in the data packets number that arrived at the destination caused by the attacker drop. The data packets with the number of routing control packets remain the same.

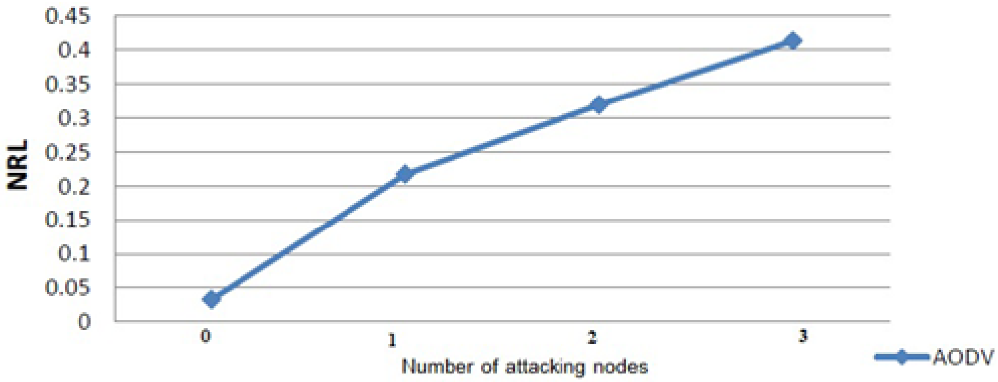

Figure 3. Relationship between the NRL As Well As Attacking Nodes Number in A MANET.

The preceding results highlight the negative impact a black hole assault would have on how a net performs.

5.2 Second Scenario Results

After applying both IDSAODV and Reverse AODV protocols in a particular net, each of them enhanced the network performance according to simulation findings, but with different percentages. For example, Figure 4 indicates that the IDSAODV increased the packet delivery rate to 68% when the attacking node was present, compared to 28% in the same network when using the AODV protocol. It also improved the rate of packet delivery when there were two or three attacking nodes, but it did not completely prevent the effect of the attack because it treats the first wrong response sent from the first attacking node and accepts the following response, which may be coming from the second or third attacking node. Therefore, it will not be able to detect the three attacking nodes.

The researchers also noticed that the Reverse AODV protocol raised the packet delivery rate to 100% for one or more attacking nodes. That is because this protocol does not allow the attacking node to declare itself that it has the correct and up-to-date path to the target and is waiting for a response from the actual target. It also replaces the current path used to transfer data with another path when it notices that the packets did not reach their destination according to this path.

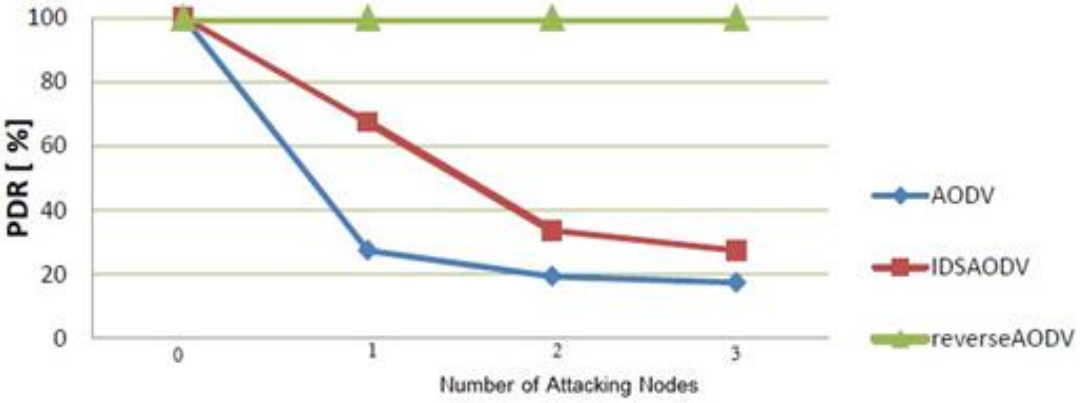

Figure 4. Relationship between Packet Delivery Ratio and Attacking Nodes number when using AODV, IDSAUDV, Reverse AODV

Figure 5 shows that the IDSAODV protocol increased the network throughput to 46 kbps when there was an attacking node, compared to 23 kbps in the same vulnerable network that used the AODV protocol. It also improved the network throughput when there were two attacking nodes. However, the improvement was slight when there were three attacking nodes due to its wrong prediction of the following reply packet. The researchers also noticed that the Reverse AODV protocol raised the throughput to 68 kbps, regardless of the number of attackers, which is the same as the network throughput in the absence of an attack in the network.

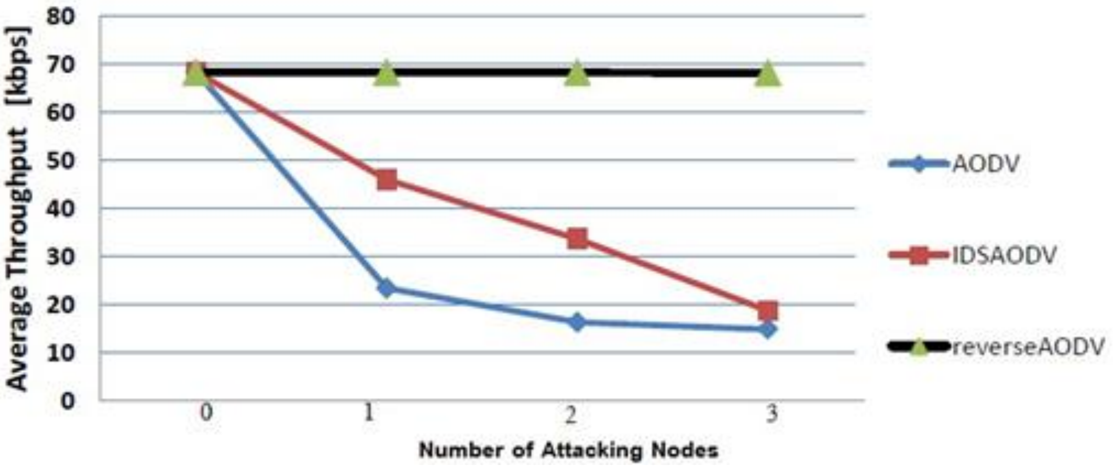

Figure 5. Relationship between *Network throughput and Number of Attacking Nodes when using AODV, IDSAUDV, Reverse AODV.*

Figure 6 shows that the IDSAODV did not cause any additional routing load because it did not use any additional control packets. In contrast, the Reverse AODV caused an increase in the average routing overhead due to its work that depends on immersing the R-RREQ packet in the network while the AODV sends one reply packet along the reverse path. This load increases proportionally with the number of attackers.

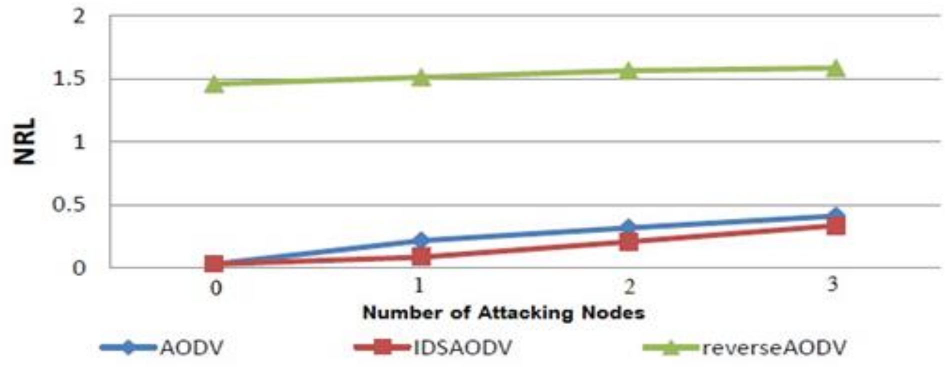

Figure 6. Relationship between Average Routing Load and Number of Attack Nodes under AODV, IDSAUDV, Reverse AODV.

5.3 The Third Scenario Findings

This study aims to investigate how the performance of the two protocols, IDSAODV and Reverse AODV, is influenced by the attacking node position. In this scenario, the researchers chose one to send and one receiving node in the network and located the attacking node according to three cases:

The attacker is close to the sending node BH, the attacker is midway between the transmitter and receiver BH, and the attacker is far from the sending node BH to study the effect of the performance of each protocol, Reverse AODV, IDSAODV, with the location of the attacking node. The researchers represented the locations of the three nodes on the horizontal axis.

In this scenario, the researchers noticed that they chose the sending and receiving nodes that move in the same direction and with the same step to nearby locations. Therefore, the distance from the attacking node to the sending node is estimated to be equal to the space from the receiving node to the attacking one if the attacker is located in the middle.

Figure 7 shows that the packet delivery rate when using IDSAODV is better when the attacker is near the sending node. The researchers noticed that the packet delivery rate decreased as the attacker moved away from the sender. That is because the IDSAODV protocol neglects the first reply packet expected to be coming from an attacker and depends on the second reply packet. The closer the attacker is to the sender, the faster his response. Therefore, the protocol expectation will be correct. However, his prediction may be wrong and may cause counterproductive results when the attacker is far from the sender, causing the rejection of the actual reply message and accepting the attacker's reply message, that causes the reduction of the packet delivery rate.

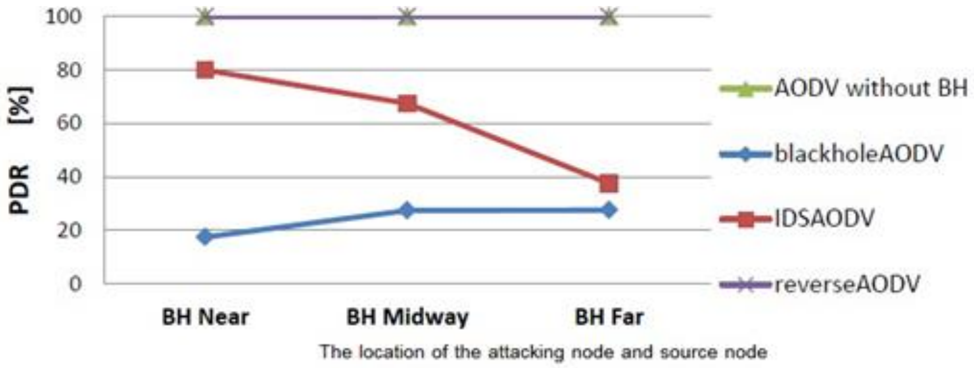

Figure 7. Relationship between *Packet Delivery Ratio and Attacking Node Location when using AODV, IDSAODV, Reverse AODV.*

The researchers also noticed that the attacking node position in the three cases did not influence the packet delivery rate provided by Reverse AODV due to the failure of this protocol to respond to any response coming from the attacking node regardless of its location and waiting for the response from the actual future.

Figure 8 shows that the network throughput using IDSAODV is better when the attacker is near the sending node. At the same time, the researchers noticed a decrease in the packet delivery rate as the attacker moved away from the sender. As it appears from the figure, the attacking node position did not influence the throughput provided by Reverse AODV in the cases. That is because of the drop of the response from the malicious node and the use of another routing path. Therefore, the packet arrival rate is high at the target.

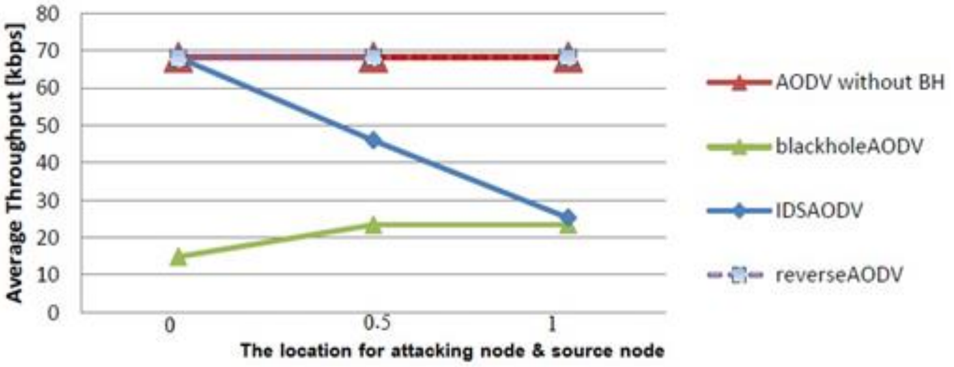

Figure 8. Relationship between Average Throughput and Location of the Attacking Node when using AODV, IDSAUDV, Reverse AODV.

From the previous two scenarios, the researchers concluded that the Reverse AODV protocol achieved better results in throughput and packet delivery when there was an attack by one or more attackers in the network. However, it caused an increase in the natural routing load. Therefore, it is considered the most suitable for detecting the black hole attack, and it was not affected by the node location attack in particular net. Table 2 summarizes the findings obtained in this paper.

Table 2. Advantages and Disadvantages of IDSAODV and Reverse AODV protocols

Protocol	Using extra Routing Packets	Advantages	Disadvantages
IDSAODV	No Extra routing packets were used.	Improved packet delivery and throughput with low routing drop.	The attacking node position has an impact on the protocol on the route between the source and the target, and it does not work properly when it is far from the source.
Reverse AODV	Use R-RREQ	Improved package delivery rate to nearly 100% and provided high average throughput.	An increase in average routing load, compared to AODV.

6. Conclusions and Recommendations

A black hole assault in a MANET network utilizing the AODV routing protocol causes throughput as well as packet delivery delays and high NRLs. In addition, network performance worsens with the increasing number of attacking nodes. The IDSAODV protocol may relieve the black hole assault effect and improve packet delivery rates and average throughput. However, its performance deteriorates when more attackers are involved. The location of the attacking node relative to the sending node affects network performance because the network performance decreases the closer the attacker is to the sender. The IDSAUDV protocol can improve network performance when the attacking node is closer to the source than when it is far from the source. The IDSAODV protocol provides better IDSAODV results in packet delivery and throughput but causes a relatively large routing load compared to IDSAODV. This paper was tested for static attacking nodes, so the researchers recommended studying network performance in the case of mobile attacking nodes.

There are many proposed algorithms for detecting black hole attack other than IDSAODV and Reverse AODV. Some of them rely on machine learning, while others rely on trust. Therefore, the researchers recommended studying these techniques and choosing the best and least expensive technology. In addition, attacks targeting other routing protocols can also be studied.

References

[1] Loo, J., Lloret Mauri, J. and Hamilton Ortiz, J. (2011). Mobile ad hoc networks: current status and future trends. Taylor & Francis.

[2] Haglan, H. M. et al. (2021). Analyzing the impact of the number of nodes on the performance of the routing protocols in manet environment. Bulletin of Electrical Engineering and Informatics, 10(1), pp. 434–440.

[3] Zarzoor, A. R. (2021). Enhancing dynamic source routing (DSR) protocol performance based on link quality metrics. in 2021 International Seminar on Application for Technology of Information and Communication (iSemantic). IEEE, pp. 17–21. doi: https://doi.org/10.1109/iSemantic52711.2021.9573233.

[4] Nabou, A., Laanaoui, M. D. and Ouzzif, M. (2018). Evaluation of MANET routing protocols under black hole attack using AODV and OLSR in NS3. in 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM). IEEE, pp. 1–6.

[5] Pathan, M. S. et al. (2019). An efficient scheme for detection and prevention of black hole attacks in AODV-based MANETs. International Journal of Advanced Computer Science and Applications, 10(1), pp. 243–251.

[6] Kamel, M. B. M., Alameri, I. and Onaizah, A. N. (2017). STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET. in 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). IEEE, pp. 1278–1282.

[7] Wadhwani, G. K., Khatri, S. K. and Mutto, S. K. (2020). Trust framework for attack resilience in MANET using AODV. Journal of Discrete Mathematical Sciences and Cryptography. Taylor & Francis, 23(1), pp. 209–220.

[8] Tilwari, V. et al. (2019). Contention window and residual battery aware multipath routing schemes in mobile ad-hoc networks. International Journal of Technology. Faculty of Engineering, Universitas Indonesia, 10(7), pp. 1376–1384.

[9] Narayana, V. L. and Bharathi, C. R. (2017). Identity based cryptography for mobile ad hoc networks. Journal of Theoretical and Applied Information Technology. Journal of Theoretical and Applied Information, 95(5), p. 1173.

[10] Rath, M. and Pattanayak, B. K. (2019). Security protocol with IDS framework using mobile agent in robotic MANET. International Journal of Information Security and Privacy (IJISP). IGI Global, 13(1), pp. 46–58.

[11] Chaudhary, A., Tiwari, V. N. and Kumar, A. (2016). Design an anomaly-based intrusion detection system using soft computing for mobile ad hoc networks. International Journal of Soft Computing and Networking. Inderscience Publishers (IEL), 1(1), pp. 17–34.

[12] Balan, E. V. et al. (2015). Fuzzy based intrusion detection systems in MANET. Procedia Computer Science. Elsevier, 50, pp. 109–114.

[13] Manoranjini, J., Chandrasekar, A. and Jothi, S. (2019). Improved QoS and avoidance of black hole attacks in MANET using trust detection framework. Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije. KoREMA-Hrvatsko društvo za komunikacije, računarstvo, elektroniku, mjerenja …, 60(3), pp. 274–284.

[14] Khamayseh, Y. M., Aljawarneh, S. A. and Asaad, A. E. (2018). Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency. Sustainable Computing: Informatics and Systems. Elsevier, 18, pp. 90–100.

[15] Gurung, S. and Chauhan, S. (2018). A dynamic threshold based approach for mitigating black-hole attack in MANET. Wireless Networks. Springer, 24(8), pp. 2957–2971.

[16] Arora, N. and Barwar, D. N. C. (2014). Evaluation of AODV, OLSR and ZRP Routing Protocols under Black hole attack. International journal of Application in Engineering & Management, 3(4), p. 2319.

[17] Sen, J. (2013). Detection of cooperative black hole attack in wireless ad hoc networks. arXiv preprint arXiv:1302.4882.

[18] Nisha, S. K. and Arora, S. K. (2013). Analysis of black hole effect and prevention through ids in manet. American Journal of Engineering Research (AJER), 2(10), pp. 214–220.

[19] Siddiqua, A., Sridevi, K. and Mohammed, A. A. K. (2015). Preventing black hole attacks in MANETs using secure knowledge algorithm. in 2015 International Conference on Signal Processing and Communication Engineering Systems. IEEE, pp. 421–425.

[20] Yasin, A. and Abu Zant, M. (2018). Detecting and isolating black-hole attacks in MANET using timer based baited technique. Wireless Communications and Mobile Computing. Hindawi, 2018.

[21] Tan, S. and Kim, K. (2013). Secure Route Discovery for preventing black hole attacks on AODV-based MANETs. in 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing. IEEE, pp. 1159–1164.

[22] Ram, A., Kulshrestha, J. and Gupta, V. (2021). Secure Routing-Based AODV to Prevent Network from Black Hole Attack in MANET. in Proceedings of 6th International Conference on Recent Trends in Computing. Springer, pp. 633–642.

[23] Gurung, S. and Chauhan, S. (2020). A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability. Wireless Networks. Springer, 26(3), pp. 1981–2011.

[24] Tan, N. D. and Van Tan, L. (2020). Implementation of Black Hole Attack on AODV Routing Protocols in MANET Using NS2. UTEHY Journal of Science and Technology, 25, pp. 45–51.

[25] Babu, E. S., Nagaraju, C. and Prasad, M. H. M. K. (2013). An implementation and performance evaluation study of AODV, MAODV, RAODV in mobile Ad hoc networks. vol, 4, pp. 691–695.

[26] Shree, O. and Ogwu, F. J. (2013). A proposal for mitigating multiple black-hole attack in wireless mesh networks. Scientific Research Publishing.

[27] Shrestha, S. et al. (2020). Securing blackhole attacks in MANETs using modified sequence number in AODV routing protocol. in 2020 8th International Electrical Engineering Congress (iEECON). IEEE, pp. 1–4.

[28] Kim, C., Talipov, E. and Ahn, B. (2006). A reverse AODV routing protocol in ad hoc mobile networks. in International Conference on Embedded and Ubiquitous Computing. Springer, pp. 522–531.

[29] Fall, K. and Varadhan, K. (2005). The ns Manual (formerly ns Notes and Documentation). The VINT project, 47, pp. 19–231.

[30] Sharma, A., Singh, R. and Pandey, G. (2012). Detection and Prevention from Black Hole attack in AODV protocol for MANET. International Journal of Computer Applications. Citeseer, 50(5).