Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2016, Article ID 6463157, 8 pages
http://dx.doi.org/10.1155/2016/6463157

Research Article

The Improved Overhearing Backup AODV Protocol in MANET

Elham Zamani and Mohammadreza Soltanaghaei

Department of Computer Engineering, Islamic Azad University, Isfahan (Khorasgan) Branch, Isfahan, Iran

Correspondence should be addressed to Elham Zamani; zamanielham85@yahoo.com

Received 17 August 2015; Revised 27 December 2015; Accepted 3 January 2016

Academic Editor: Rui Zhang

Mobile ad hoc network (MANET) is one of the most widely used networks, which has attracted attentions, having features such as limited energy resources, limited bandwidth, and security weaknesses due to lack of a central infrastructure. Safe and suitable routing is one of the research aspects of MANET. In this paper, a proposed method, called M-AODV, which is a type of overhearing backup protocol, based on AODV, is presented. The simulation results of this protocol, applied by NS2 simulator, showed the improvement of packet delivery rate and reduction of overhead and delay. Moreover, to assess the security of the proposed protocol, we simulated M-AODV and AODV protocols under black hole and wormhole attacks, using no security solution. The results showed that M-AODV had been improved in terms of packet delivery ratio, and the delay had been reduced as well, but the amount of overhead had been increased.

1. Introduction

MANET is a subset of ad hoc networks. MANET is a mobile, dynamic, and self-constructed network, which includes mobile nodes such as cell phones and laptops. In MANET, nodes can freely enter or exit their network; therefore, the network topology is constantly changing and it is important to find the right path and select the next node. The most important issues in MANET are security and routing. MANETs are currently widely used around the world, but they are, unfortunately, extremely vulnerable. MANETs had been under different attacks all the time. So it had been considered to use processes and algorithms to have features such as confidentiality and availability [1, 2]. Therefore, a way must be found to make them secure. There are different routing methods in this network, but each of them has some defections and has been vulnerable against some attacks.

The main motivation of this study is improving a routing protocol in MANET because finding an efficient routing protocol which can also address malicious behaviors in the best manner has always been in researchers' minds. Therefore, in this study, the researchers try to improve the quality and security of MANETs. Metrics considered in this study are packet delivery ratio, delays, and overhead, which are calculated in two different scenarios with different number of nodes and pause times. Then, the black hole and wormhole attacks scenarios are investigated under these metrics. In wormhole, two collusion nodes build a link called wormhole and they tunnel packets through their link. In black hole attack the collusion node introduces itself as a legit one to have a path to destination but instead uses that packet and modifies it [3, 4].

The rest of this paper is arranged as follows: related works are discussed in Section 2; in Section 3, the proposed solution is presented; and, in Section 4, simulation results are shown. In Section 5, conclusions and suggestions for further studies are provided.

2. Related Work

Lai et al. proposed AODV-BR protocol [5]. In this method, creating an alternative route depends on overhearing route reply (RREP) messages. No additional message is required during the construction of alternative routes. Using these alternative routes, AODV-BR can offer a more stable connection compared with AODV. In AODV-BR, there is no problem for building alternative routes in the reply phase. This makes the management and maintenance of the alternative routes become easier. When topology changes improperly (e.g., when the speed increases), the alternative routes, being

made in reply phase, may even break if the main paths fail. In AODV-BR, when a node detects the failure link, it applies a single data broadcast to its neighbors, which sends the packets to destination via the alternative route and then sends a RERR packet to the source node to recreate a route discovery phase. The issue of "one-hop data broadcasting" minimally affects heavy network traffic because it creates loads of unnecessary and duplicate data packets that travel through alternative routes [5–7].

Lai et al. also introduced the AODV-LR method [5]. It tries to repair link failures without informing the source node and disrupting data delivery. Since transmission performance can be improved, if a link failure can be repaired locally, there would be no need for any data retransmission of the source. Local link repairs may increase the number of data path hops and thus increase the delay. To solve this problem, using a threshold, a decision is made over policies to be used: starting a local repair process or applying a new route.

Lai et al. created AODV-ABR [5]. In this method, when a node detects a link failure, it runs a handshake process between the neighbors to repair the broken path, rather than applying a one-hop data broadcast to the neighbors. Handshake process is completed by two one-hop control signals: BRRQ (Backup Route Request) and BRRP (Backup Route Reply).

Lai et al. and Zhou and Li [5, 8] introduced AODV-ABL, which is an adaptive backup routing protocol along with local repair. In this protocol, backup routes will be created by overhearing reply messages (RREP) and data packets. Alternative nodes in backup routes, which are close to the destination, may get lost. In this protocol, nodes work in a promiscuous mode; that is, these nodes can receive unicast and broadcast packets and also accidentally hear unicast packets, having been distributed by their neighbors. Each node has a main and an alternative routing table. AODV-ABL sends data according to the routes in the main routing table and stores the alternative routes in the backup routing table.

Zhou and Li [8] proposed AODV-BFABL. In scenarios with bidirectional traffic load, when the source node sends data to the destination, the destination node transmits data to the source as well. AODV-BFABL protocol is developed for such scenarios and created based on AODV-ABL, but it has two fundamental improvements. First, it merges the original and alternative routing tables; that is, there will be only one entry per destination node in the table. When it overhears a better backup route, it will replace the responsible entry in table with the backup routes, as far as possible, and improve the correspondence with the changes in network's topology. Second, AODV-BFABL randomly overhears data packets being uploaded from the source node to the destination and vice versa in order to prevent losing routes which are one step away from the destination node. In order to keep the paths to the source node, AODV-BFABL protocol adds two fields to AODV-ABL, which save hops of current node to the source as well as the sequence number of source node routing.

Patil et al. [7] proposed AR-AODV protocol, which is an improved form of AODV. This protocol overcomes link failure of predecessors by local repair design. In this method, data packets, instead of being dropped, are sent through alternative routes. Data packets also carry information about the node which has also an alternative route. If a link fails and there is no alternative route in the node, it will search for an alternative route. If the desired input is found, the superior node will transmit the packet to that node with alternative route and will, then, send data packets to the destination.

Table 1 summarizes the collected material. If an entry is empty, it means that the information in studied articles could not be found. AODV-BR protocol creates alternative routes by overhearing the reply messages. In AODV-LR, link failures are repaired locally. In AODV-ABR, if a link failure is detected, handshake process between neighbors will be executed. In AODV-ABL, a backup route is created by overhearing the reply messages and data packets, and local repair will be used as required. In AODV-BFABL, the source and destination nodes are able to transmit the data to each other. In this method, the best overheard backup route enters into the table. In AODV-AR, instead of eliminating the data packet, it will be transmitted through an alternative route.

3. The Proposed Method

In order to reduce the control overhead, the researchers used the ideas in AODV-ABL and AR-AODV protocols. That is, the whole routing operation turns into two phases. First, there is the similar idea of AR-AODV algorithm, which uses the alternative route in data packet or node, and if it does not find any alternative route or if the alternative one has expired, it goes to the second phase. The second phase is based on the ABL protocol's idea, which has local repair (LR) or uses the alternative route's neighbors at a distance of one hop (ABR). In this case, sending control messages is avoided as far as possible.

The idea of AODV-BFABL protocol can be used for real-time table updating. That is, nodes are forced to overhear the packets which are sent by their neighbors located in their communication distance. However, in the proposed method, one routing table is used instead of two, just like ABL protocol.

In the proposed method the source node starts the route request process by broadcasting a RREQ. Then each node broadcasts the RREQ to its neighbor. The destination has two RREPs. Nodes listen to both RREPs and put the best one in main route table and the other one goes to alternate route table. Then it will compare the overheard information with the main route table and if the information was better, then the routing entry will transfer from main table to the alternative one and the past alternate route entry will be deleted. So eventually the new discovered route will be put in the main route table. But if the route breaks, the local repair will happen and it tries to find an alternate route.

Overhearing every data packet, the node is convinced to pay attention to hop counts to source and destination as well as the sequence number of source and destination. Then, this information is compared with the corresponding information in the routing table and if the new information is optimal, it will be transferred from alternate table to the main one—the former alternate element is removed. Afterwards, the newly

Table 1: Comparison of discussed methods.

Scholar	Protocols	Features	Advantages	Disadvantages
Lai et al. [5]	AODV-BR	It will not try to repair the broken path, so it will need lesser hops. There is expiration time possibility.	Low delay: it needs less hops.	Low throughput: if the speed goes high, the backup routes that had been made in reply phase will fail.
Lai et al. [5]	AODV-LR	It uses local repair.	It has a better throughput rather than BR and ABR and also has a wide repair searching range.	It has more hops and high delay (because of increment in the path hops).
Lai et al. [5]	AODV-ABR	If it detects a link failure then a handshake process will be used. AODV-BR has hop control signals such as BRRQ and BRRP. It can select a backup route.	It is adaptive towards network topology. It has less control overhead and less delay than AODV-LR. It avoids collision and congestion issues.	It has average throughput (less than LR and more than BR).
Lai et al. [5], Zhou and Li [8]	AODV-ABL	It is an adaptive backup routing protocol which uses local repair. It works in a promiscuous mode (overhear the packets). This method has main and alternative routes.	It has BRRQ and BRRP. The packet delivery ratio is high. It has a MAX_Repair_TTL threshold.	It is possible to drop some alternative routes only with one hop distance to thedestination. It cannot update the main route in time to adjust with dynamic topology. There are a lot of hop counts. It has control overhead and throughput is almost low.
Zhou and Li [8]	AODV-BFABL	It merges the main routes with alternative ones. It can update the routes during the data transmission. It is suitable for bidirectional traffics and is based on ABL.	It improves adaptability. The packet delivery ratio is higher than ABL. Its delay and overhead are lower than ABL. It can avoid link failure with one hop distance to destination by packet overhearing.	—
Patil et al. [7]	AR-AODV	It has two route replies. Also it has a local repair scheme and is able to dominate link failure.	It improves the packet delivery ratio, protocol operations, and mobility. It reduces routing load and end-to-end delay.	—

discovered direction will immediately be replaced with the corresponding element in the main table.

The goal of this study is to provide a secure routing protocol in MANET. The proposed protocol is based on overhearing the neighbors and constant comparison of the information of main and alternative tables. Considering the fact that there are some methods like neighbors overhearing (NEVO) and Packet Travel Time (PTT) [9–11], which have some similar fields, such as overhearing and comparison of hops and information, with this proposed method, the proposed protocol was assumed to be safe and some attacks were tested on it. NEVO did not use the clock drift and had a slight change in network layer. In PTT, by overhearing the nodes it will discover the wormhole attack [10]. It should be mentioned that no security solutions were added to this method and the proposed method itself could resist against black hole and wormhole attacks in the simulated situations.

4. Simulation and Results

The proposed method was simulated by NS 2.34 in the Linux environment. During this process, the network was first considered without any intended attack, with three mentioned protocols in two different scenarios which were based on different pause times and different number of nodes. Then, the results were evaluated.

4.1. Parameters and Simulation Metrics. In order to evaluate and compare the performance of listed protocols, three metrics were considered: packet delivery ratio, end-to-end delay, and control overhead. Table 2 shows the parameters in this simulation which were selected based on researches in [5, 8, 12].

4.2. Simulation Results of First Scenario. The results of the first simulation scenario depend on pause time. As can be seen in Figure 1, in the proposed protocol (M-AODV),

Table 2: Simulation parameters.

Parameter	Value
Simulation time	500 and 1000 sec
Simulation environment	1000 m ∗ 1000 m
Number of nodes	40, 50, 60, 70, 80, 90, and 100
Bandwidth	10 Mbps
Packet size	512 bytes
Mobility model	Random way point
Pause time	0–400 sec
Traffic type	CBR
Protocol type	UDP

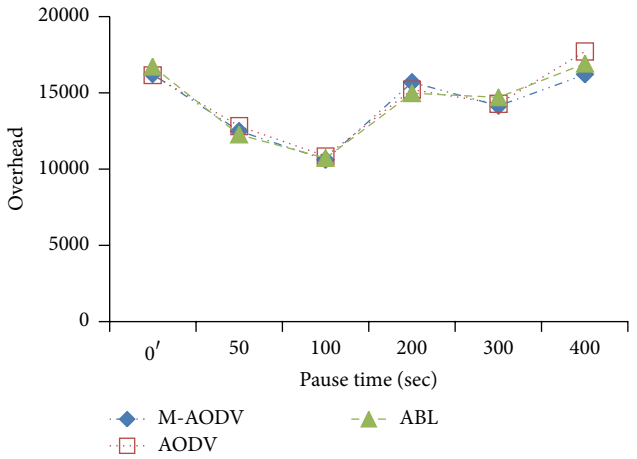

Figure 1: Control overhead in first scenario.

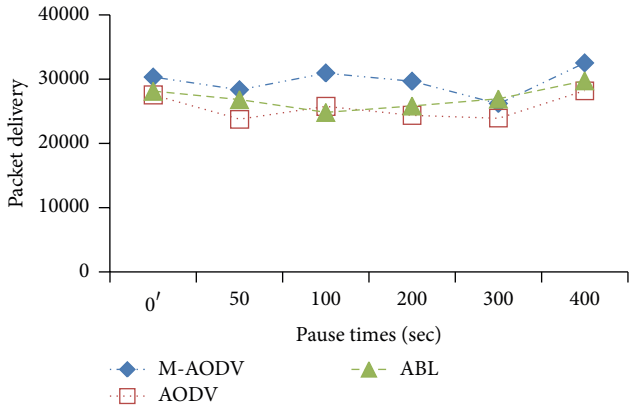

Figure 2: Packet delivery ratio in first scenario.

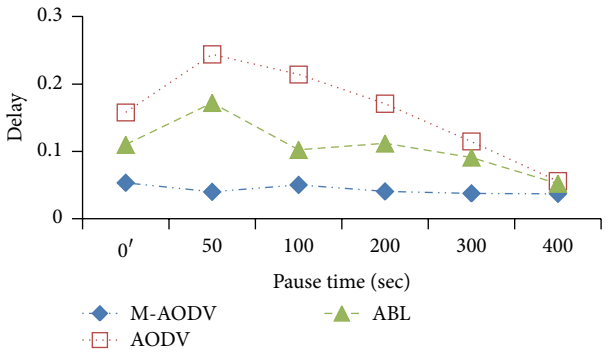

Figure 3: End-to-end delay in first scenario.

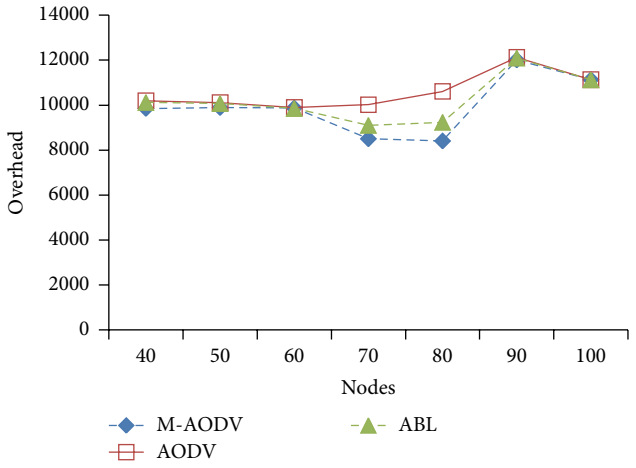

Figure 4: Control overhead in second scenario.

the average control overhead is improved compared with other two protocols (AODV and AODV-ABL). The average improvement rate is about 1 percent more than AODV and AODV-ABL.

In Figure 2, in the proposed protocol (M-AODV), the number of received packets versus the pause time has improved compared with the other two protocols (AODV and AODV-ABL). This plot is almost linear but has a few critical points. However, packet delivery ratio is higher than AODV and AODV-ABL. The average improvement rate for M-AODV is 13% more than AODV and 8% more than AODV-ABL, respectively.

Based on Figure 3, it is clear that the amount of delay versus pause time in the proposed protocol (M-AODV) has been improved compared with both AODV and AODV-ABL. M-AODV diagram is relatively linear. The average improvement rate for M-AODV is approximately 67% compared to AODV and about 55 percent compared to AODV-ABL, respectively.

4.3. Second Scenario Simulation Results. In the second scenario, a different number of nodes have been selected. Simulation results in Figure 4 show that, in the proposed protocol (M-AODV), overhead has been improved compared to both AODV and AODV-ABL protocols. In this simulation, in 90-node situation, overhead suddenly goes high in all three protocols, and this is probably due to random encounters and movements among nodes. The average improvement rate for M-AODV is about 1% more than AODV and about 4 percent more than AODV-ABL, respectively.

Based on Figure 5, it can be seen that the number of received packets versus the number of nodes has been improved in M-AODV compared with both AODV and AODV-ABL protocols. The average improvement rate is 20%

Table 3: Evaluation of simulation results.

Scenario	Received packets	Delay	Overhead
First scenario towards pause time	M-AODV has the highest received packets. Then ABL and finally AODV had good behavior.	AODV had the most delay, then ABL, and at the end M-AODV had the lowest delay.	Except at the 200th sec, the most overhead belonged to ABL, then AODV, and at the end to M-AODV.
Second scenario towards the number of nodes	M-AODV had the best results in packet received category. ABL had almost better results than AODV.	AODV had the most delay. M-AODV had the least. AODV-ABL was in between.	Overhead in the simulation with 60 and 90 nodes was almost equal. In other situations AODV had the most overhead, then ABL, and finally M-AODV.

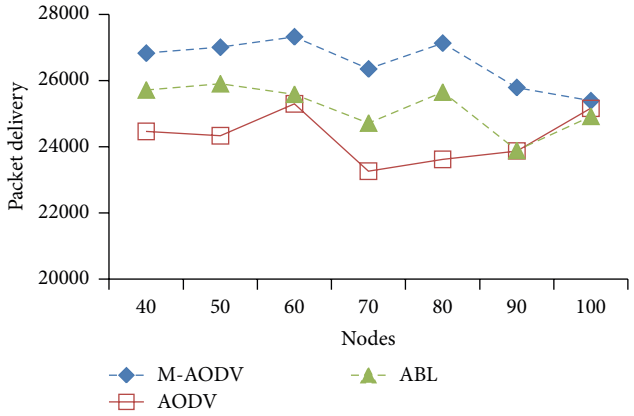

Figure 5: Received packets in second scenario.

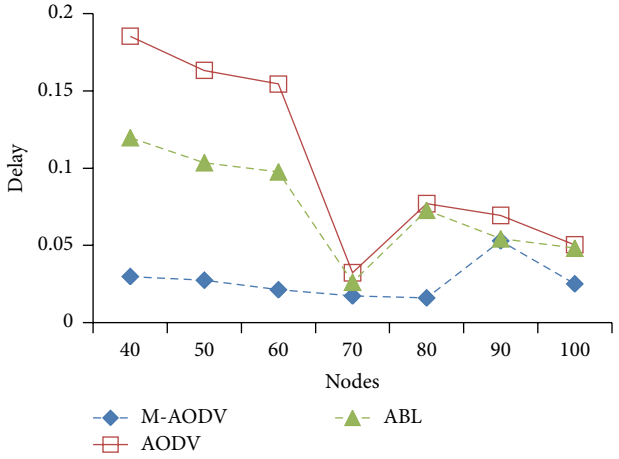

Figure 6: End-to-end delay in second scenario.

compared with AODV and about 5% compared with AODV-ABL.

Average end-to-end delay in the proposed protocol (M-AODV) has been improved compared to both AODV and AODV-ABL. Figure 6 shows that the delays of other two protocols are very critical and not stable. The average improvement rate for M-AODV is almost 64% compared with AODV and about 55% compared with AODV-ABL, respectively.

4.4. Evaluating the Results of the Two Scenarios. Results of these two scenarios are gathered in Table 3 and the operation of proposed protocol (M-AODV) is compared to AODV and AODV-ABL protocols. All the metrics calculated in both simulated scenarios are put in this assessment. Looking at the table, it can be seen that the proposed method (M-AODV) performs better than the other protocols.

4.5. Simulation of the Proposed Network under Attack. In this section, the network is examined and compared under wormhole and black hole attacks. It should be mentioned that no security solution was used. Since the features of the proposed method are almost like neighbor overhearing (NEVO) and Packet Travel Time (PTT) [9–11] and both of these methods resist wormhole attacks, this method may also resist, under special circumstances. In NEVO algorithm it will reduce the wormhole attack's effect through overhearing the broadcasted packets by their neighbors and with the help of overhearing time of transferring packets. In PTT algorithm, the nodes are able to listen to their neighbors, so they can discover the attack and they will not send the data through the suspected wormhole path.

Therefore, the proposed method was investigated with different numbers of nodes under wormhole and black hole attacks. The results and diagrams are compared with AODV under attack and obviously our protocol still has a better performance.

It had been tried to use the same parameters during the simulation of attacks, as far as possible; however, since this simulator works randomly, it was necessary to change a few parameters, such as the number of nodes, to get the best results. In Table 4, the simulated parameters, being similar to [5, 8, 9], are gathered.

4.6. Simulation Results under Wormhole Attack. In Figure 7, in the proposed protocol (M-AODV), the number of received packets versus nodes is improved compared with AODV protocol during the attack. The average improvement rate for M-AODV is about 13% more than AODV.

Based on Figure 8, in the proposed protocol (M-AODV), the average delay over the number of nodes during the attack, by simulating with 20 nodes, is more than AODV, but in other cases, the delay is approximately equal to or lower than AODV protocol. The average improvement rate for M-AODV is about 17% more than AODV.

Table 4: Simulation parameters under attack.

Parameter	Value
Simulation time	500 sec
Simulation environment	1000 m ∗ 1000 m
Number of nodes	20, 30, 40, 50, and 60
Bandwidth	10 Mbps
Packet size	512 bytes
Mobility model	Random way point
Traffic type	CBR
Protocol type	UDP

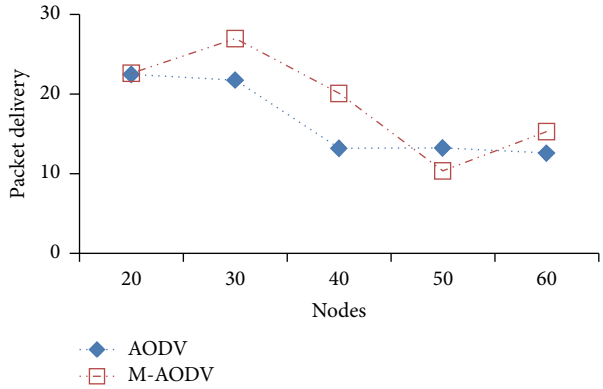

Figure 7: Packet delivery under wormhole attack.

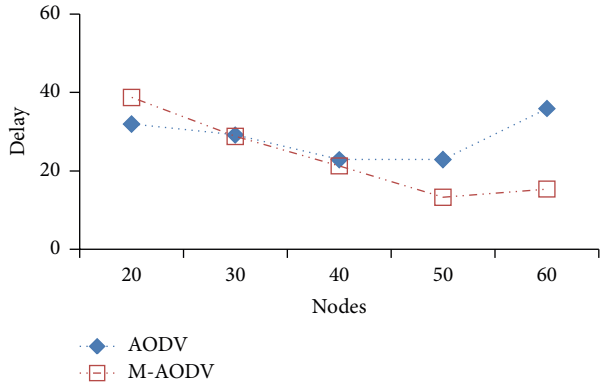

Figure 8: Delay under wormhole attack.

In the proposed M-AODV protocol in Figure 9, overhead is compared to the number of nodes under wormhole attack and it is found to be slightly higher than AODV protocol; that is, it is about 4% more than AODV.

4.7. Simulation Results under Black Hole Attack. Simulation results in Figure 10 show that, during the black hole attack, the proposed protocol (M-AODV) has less delay up to 60 nodes, but the delay is almost equal to AODV in simulation with 60 nodes. This might indicate that more attacks could have happened in this case or the simulation conditions were not

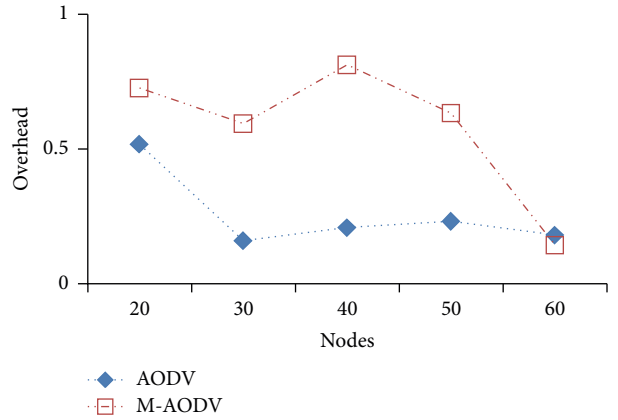

Figure 9: Overhead under wormhole attack.

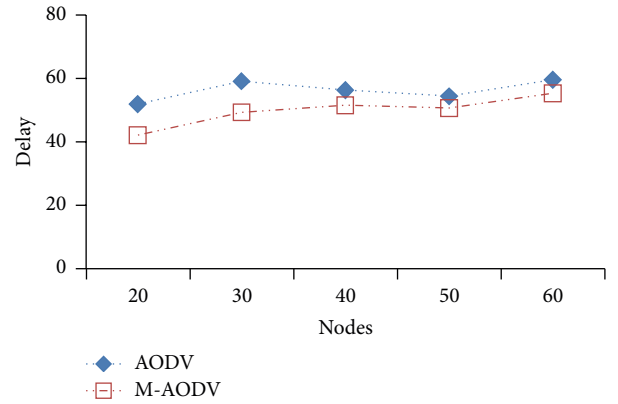

Figure 10: Delay under black hole attack.

as favorable as before. The average improvement rate for M-AODV is about 13% more than AODV.

Based on Figure 11, from the simulation results under black hole attacks, it can be seen that, in cases with 20 and 30 nodes, packet delivery ratio in M-AODV is almost the same as AODV. With more nodes, however, we had better packet delivery ratio than AODV. The average improvement rate for M-AODV is almost 7%.

Simulation results in Figure 12 show that, in the proposed protocol (M-AODV) during the black hole attack, overhead amounts in 20, 30, and 60 nodes are almost the same as those of AODV. With 40 and 50 simulated nodes, however, it performs better than AODV. The average improvement rate for M-AODV is about 3% more than AODV.

4.8. Evaluating the Results of the Simulation under Attack. Results of the proposed protocol (M-AODV) under attack scenario for both black hole and wormhole attacks are put in Table 5 and compared to AODV protocol under attack. The results show the overall success of the proposed procedures under simulated situation. It should be noted that these random results are obtained under these conditions.

Table 5: Evaluation of the results under attack.

Scenario	Overhead	Delay	Packet delivery ratio
Black hole attack scenario	Under black hole attack, the overhead was almost the same.	*In this attack, delay will increase when there are more nodes.*	The most packet delivery ratio belonged to M-AODV.
Wormhole attack scenario	Under wormhole attack, M-AODV had higher overhead.	Under wormhole attack, M-AODV delay has been improved compared to AODV.	Under wormhole attack except in the situation with 50 nodes, the most packet delivery ratio belonged to M-AODV.

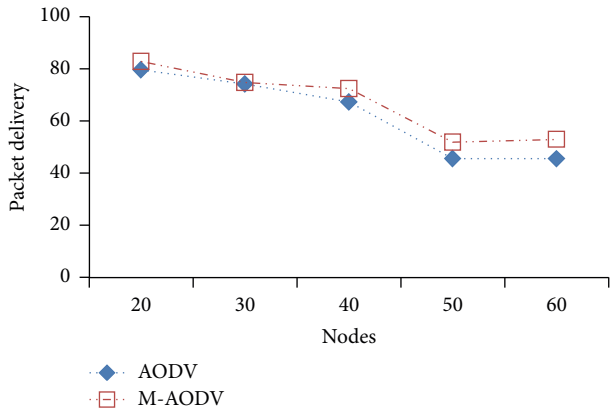

Figure 11: Packet delivery ratio under black hole attack.

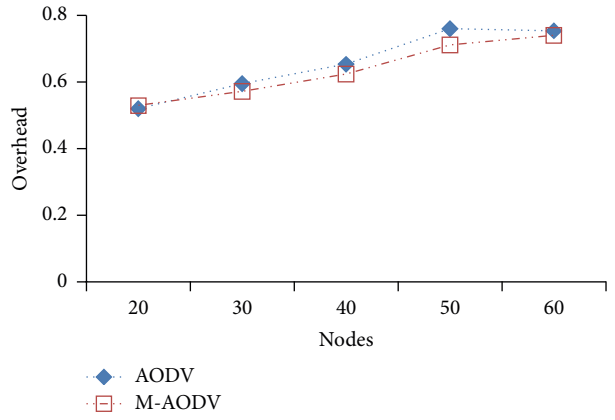

Figure 12: Overhead under black hole attack.

5. Conclusions and Suggestions for Future Work

The results of these simulations proved that the proposed M-AODV protocol improved the quality and security of networks. In various pause time scenarios for this protocol, therefore, it was seen that it had been improved between 55 and 67% in terms of delay reduction, 1% in terms of overhead reduction, and between 8 and 13% in terms of packet delivery ratio. In the scenario with different number of nodes, the delay reduction metric had been improved between 48 and 57%, the overhead reduction had been improved between 4 and 9%, and packet delivery ratio had been improved between 5 and 25%.

When security measures were taken, the proposed method had attributes such as overhearing, immediate updating, local repair, and two routing tables. It was assumed that the proposed protocol may act like some other secure methods, such as neighbor overhearing (NEVO) and Packet Travel Time (PTT), which have some of these features as well and may be secure against some attacks. Thus, in simulations with and without attack, the proposed method was proved to be secure against wormhole and black hole attacks. However, while it had a small raise in overhead, the number of delivered packets increased and delay did not change significantly. Also it can be considered that perhaps with the combination of this proposed method with NEVO or PTT algorithms they can work against black hole attack as well. It is clear that NEVO does not use the clock drift and makes some changes in network layer, so maybe with the proposed method there will not be any need to do that.

There are two parameters (power consumption and electromagnetic interference) which can affect the results of this simulation but the resources for this study were not enough to consider them, so it is a good idea to resimulate these situations in other different scenarios with these theories as well in the future.

In the future, other types of attacks, such as malicious node, gray hole, and flooding, can be applied to this protocol so as to try to improve its performance. Another idea is to combine the basis of this protocol with other protocols derived from AODV and introduce a new protocol. Other types of parameters, then, can be applied to it.

Conflict of Interests

The authors (Elham Zamani and Mohammadreza Soltanaghaei) declare that there is no conflict of interests regarding the publication of this paper.

References

[1] D. L. Denovic, "Mobile ad hoc network security," in *Proceedings of the 5th International Scientific Conference on Defensive Technologies (OTEH '12)*, Belgrade, Serbia, September 2012.

[2] S. D. Ubarhande, "Performance evolution of AODV and DSR routing protocols in MANET using NS2," *International Journal of Scientific & Engineering Research*, vol. 3, no. 5, pp. 1–5, 2012.

[3] P. Jawandhiya, "A survey of mobile Ad Hoc network attacks," *International Journal of Engineering Science and Technology*, vol. 2, no. 9, pp. 4063–4071, 2010.

[4] K. Sivakumar and G. Selvaraj, "Analysis of worm hole attack in MANET and avoidance using robust secure routing method,"

International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 1, 2013.

[5] W. K. Lai, S. Hsiao, and Y. Lin, *Adaptive Backup Routing for Ad-Hoc Networks*, Elsevier, 2007.

[6] G. M. Lee, "AODV-BR: backup routing in ad hoc networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '00)*, Chicago, Ill, USA, September 2000.

[7] V. P. Patil, K. T. Patil, A. R. Kharade, and D. Gote, "Performance enhancement of reactive on demand routing protocol in wireless Ad Hoc network," *International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN)*, vol. 1, no. 4, 2012.

[8] P. Zhou and W. Li, "A bidirectional backup routing protocol for mobile ad hoc networks," in *Proceedings of the 2nd International Conference on Business Computing and Global Informatization (BCGIN '12)*, pp. 603–606, IEEE, Shanghai, China, October 2012.

[9] X. Su and R. Boppana, "Mitigating wormhole attacks using passive monitoring in mobile ad hoc networks," in *Proceedings of the IEEE Global Telecommunications Conference*, pp. 1–5, IEEE, New Orleans, La, USA, November 2008.

[10] R. Siwach and V. Kaul, "Mitigating large propagation delay by mitigating wormhole attack in mobile Ad Hoc network," *International Journal of Science and Research Publications*, vol. 3, no. 6, 2013.

[11] A. Hassan, S. Ahsan, S. Alshomrani, and A. Alshamrani, "Packet travel time based mechanism for detection and mitigation against wormhole attack in AODV for MANET," *Life Science Journal*, vol. 11, pp. 636–641, 2014.

[12] Z. Feng, L. Wang, and X. Gao, "An improved routing protocol ad-AODV based on AODV," in *International Conference on Information Science and Computer Applications (ISCA '13)*, Atlantis Press, 2013.