Improving Security Issues in MANET AODV Routing Protocol

Mahsa Gharehkoolchian[1], A.M. Afshin Hemmatyar[2], and Mohammad Izadi[2]

[1] School of Science and Engineering, Sharif University of Technology, International Campus, Kish Island, Iran
Gharehkoolchian@gmail.com
[2] Department of Computer Engineering, Sharif University of Technology, Tehran, Iran
{Hemmatyar,Izadi}@sharif.edu

Abstract. Mobile Ad-hoc Networks (MANETs) are forming dynamically by joining or leaving the nodes into/from the network without any fix infrastructure. It is also possible that each mobile node act as a host or router. This kind of wireless network is prone to various security threats or attacks due to its unique characteristics like dynamic topology, open medium, lack of central monitoring, etc. So security is a vital scope in MANET to protect communication between mobile nodes. Ad-hoc On-demand Distance Vector (AODV) is one of the on-demand reactive routing protocols in MANET that initially was improved without considering security protection. Significant attempts have been done to secure AODV routing protocol in MANET but there are still critical challenges to overcome. In the present study, after reviewing secured protocols of some previous researches, an improved protocol is proposed to enhance the security of AODV routing protocol against black hole attack. For this purpose, we used a different level of trust for MANET nodes and imposed the limitations based on the nodes' trust level, in order to detect the compromised nodes and malicious behaviors inside MANET; which leads to the low delay and high performance in the network. Finally, we simulated the proposed protocol with NS-2 simulator as a means to validate it and evaluate the results. In fact, the results, demonstrate the efficiency of the presented protocol and its resistance to the black hole attack in comparison to AODV routing protocol.

Keywords: AODV protocol, Black hole attack, MANET, Secure routing, Trust-based technique.

1 Introduction

Accessing network resources from any location makes the wireless networks the most popular networks all over the word. On the other hand, this key feature can increase many problems regarding data security. By increasing the number of mobile hardware and devices, wireless networks' security becomes a big concern issue. MANET is a class of wireless networks that include mobile users which are connected by wireless

N. Mitton et al. (Eds.): AdHocNets 2015, LNICST 155, pp. 237–250, 2015.
DOI: 10.1007/978-3-319-25067-0_19

links with no fixed infrastructure (access point) and are formed on ad-hoc basis. Lack of fixed structures makes MANET more vulnerable to different kinds of attacks in comparison with other types of networks.

MANET does not have typical routers for routing in the network. Instead, each node in the system should function as a router for the other nodes. As a result, malicious behavior from any node can destroy network's function.

One of the most well-known routing protocols in MANET is Ad-hoc On-demand Distance Vector (AODV) protocol, a class of the reactive protocols that finds a route on demand by flooding the network with Route Request packets. This protocol is vulnerable to security threats and attacks. Overall, significant attempts have been done regarding security in MANETs but security issues in a wireless networks still exist.

In this article, first we are going to discuss different security threats and vulnerabilities in MANET and AODV. In next subsections different type of attacks, security attributes and MANET routing protocols are described. Then, the related works, the proposed protocol and achieved results are mentioned.

2 Routing Attacks and Threats in MANET

2.1 Some Attacks against MANET

Networks usually threat by the attackers, different types of attacks are known as flooding attack, gray-hole attack**,** Denial of Service (DoS) attack, impersonation attack, black hole attack, modification attack, etc. At the following section some of them are explained [1], [2]:

1) Wormhole attack: This attack creates a tunnel by attackers who placed themselves in the strategic position of the network; declaring the tunnel as a shortest path of transmission in order to record the traffic or ongoing packets.
2) Black Hole attack: A malicious node realizes a neighbor initiates to send a RREQ packet, it RREP the fake packet with the highest value of sequence number and lowest hop count. Consequently, neighbor node assumes that this malicious node has the best route to the destination. Thus, the source node discards all other RREPs; malicious node drops all the packets as well. In other words, it stops forwarding packets to the right destination [3], [4].
3) Flooding attack: The attacker set up a path between network's nodes to disseminate its unpleasant packets and congest the network.
4) Gray Hole attack: attacker acts as a both malicious and normal node in the network with aim of misleading network, being detected hardly and preventing them to reach the destination [5].
5) Modification attack: both Impersonation and misrouting attacks are including modification attacks.
6) Denial of Service (DoS) attack: a malicious node with the increase of fake RREQs, floods the network. Subsequently, non-malicious nodes cannot work well in the

network while false RREQs imposed the network load. Wastage of bandwidth, extra overhead, network resource exhaustions (like memory or battery exhaustion) are some instances of adverse effects in the network [6].

2.2 MANET Weaknesses

MANET often suffers security attacks more than wired networks because of its nature features such as dynamic topology and open medium. In this section, some of the MANET weaknesses are mentioned.

1) *Lack of centralized administration:* there is no central control, management to monitor the traffic and nodes' functions especially in large scale of networks.
2) *No Boundaries:* nodes can easily join or leave the network, while in a wired network, it is needed to pass firewall or gains physical access to visit the network.
3) *Limited power supply:* selfish problem can be occurred. Selfish nodes don't cooperate with other nodes to provide services while it has enough battery power.
4) *Unpredictable scale:* the protocols and management services should be updated due to frequent change of the network scale.

3 Routing Protocol

3.1 AODV Routing Protocol

AODV protocol is a class of reactive routing protocols or on demand routing protocol, which means that, only by requesting a route – while there is no route to the desire destination – AODV tries to find the best and shortest path to the destination. AODV protocol has three main kinds of control messages during routing processes over UDP, route request (RREQ), route reply (RREP) and route error (RERR) messages.

3.2 AODV Mechanism

The operation of AODV routing protocol can totally be divided into two main stages: route discovery and route maintenance [7]. In route discovery step, source node tries to discover a path to the destination. In the route maintenance mechanism, nodes should be notified if a route is not valid any more due to dynamic network topology.

In MANET, when a source node needs to communicate with a desire destination, which is not existing in routing table, the source node broadcasts RREQ to all its neighbors; each of neighbor nodes rebroadcasts the RREQ as well. This flow is continuing until to finds the destination node or an intermediate node with fresh route to the destination. When the intermediate node gets a RREQ message, it does not need to send RREQ anymore and can have faster replies as it has a valid path into the destination. This RREQ is not only for finding path to the destination, but also it is used for reverse route and informing other nodes about this route to the destination [8]. In continuing, that founded node – destination/ intermediate node – sends a

unicast RREP message to the source node in order to establish the desire route between source and destination. Moreover, In AODV, each node maintains a sequence number in order to identify the freshest route of information; Sequence number counter is increased before dispatching RREQ or RREP messages. So in AODV, nodes update their routing tables' information by finding the highest sequence number. Sequence number is unique 32 bit unsigned integer number, which leads to the great feature of loop-free in AODV routing. Hop-count also should be considered in routing updates, that shows the distance between the source and destination [9].

4 Related Work

In this subsection, several previous researches of securing routing protocol are mentioned and discussed.

Generally, the offered routing algorithm of securing AODV protocol classified into two main types: cryptographic and trust-base technique. Most of the presented secured protocols rely on cryptographic techniques, which can provide the confidentiality and integrity services. One of the cryptographic techniques offered an efficient secure AODV routing protocol named as SAODV [2], [8], [10]. This protocol authenticates non-mutable fields and mutable information (hop count) of the message, using digital signature and hash chain, respectively [10]; They have proven that their proposed routing algorithm has a better level of security and performance in terms of overhead and end-to-end delay; furthermore, SAODV can prevent tampering of control messages and data dropping attacks [2], [8]. However, SAODV only provides the authenticity of the message, not the dependability of the route information or route quality.

Some other articles presented the secured protocols which using cryptographic and trust base technique. Liu et al. is one of the researchers who have done research in this area [11]. Jared Cordasco and Susanne Wetzel have done a high quality of search for comparing SAODV and TAODV, including performance comparison on actual resource-limited hardware. The article addresses routing security based on cryptography and trust techniques [12]. Although their researches are valuable, they are not efficient enough because it needs consecutive monitoring neighbors' nodes and has high cost to implementation.

Some other articles that present trust based technique (such as TCLS, LLSP and RSRP), provide a reliable relation among non-malicious nodes and subsequently lead to low or even no requests for verifying certificates [11], [13], [14]. TCLS protocol uses trust counter and digital signature, to count the forwarded packet and verify the packets in the reverse route process respectively. LLSP protocol uses monitoring techniques to provide the security services at the data link layer. And the RSRP presented an efficient broadcast authentication technique to facilitate instant authentication [13]. Usually, trust based techniques rely on monitoring and packet analyzing mechanism with complicated computation; which leads to significant overhead in networks.

Meka et al. proposed trust-based solution (named as Trust AODV or TAODV), which is isolating malicious nodes, penalizing uncooperative nodes and allowing making decision to identify the best route to the destination by consideration of both node's trust and route trust metrics [11].

In another article trusted routing protocol is suggested against the security problem and selfishness issues. This kind of protocol which is named as TAODV protocol is designed based on trusted frame work and intrusion-detection system (secure protocol). In this model, routing table can be extended with trust information gathering directly from monitoring nodes. Hence great decrease of overhead and routing procedure trustiness can be guaranteed as the results from this model [14]. TAODV still is not completely a perfect protocol because of its some flaw's points. When multiple paths cross each other, it cannot support the trust level synchronization setting on different nodes.

Some researchers have tried to improve the performance of MANETs such as Tactical On-Demand Distance Vector (TAODV) routing protocol [15] and Without Black Hole AODV (WBHAODV) [16]. The introduced protocols significantly reduces the network traffic and increases the performance of network. Although these protocols are well performed, they could be faster and more efficient.

In another work, an optimized protocol is introduced in order to solve the problem of routing in dynamic topology. B-AODV is an example that improves the routing discovery and routing repair of AODV; as a result, it decreases the end-to-end delay and routing overload [17] but extra network traffic could be arisen when nodes have low movements.

In Some researches, solutions for determining the malicious nodes, are presented against black hole attack [1], [3], [4], [18]. In an article [3] a solution of Detection, Prevention Reactive AODV (DPRAODV), unto Black Hole attack is offered; in this protocol, the malicious node can be detected and isolated from data routing by using alarm messages to notify its neighbors. This result in normalize overhead of routing and the minimum increase of the average end to end delay. One of the other given approaches secures nodes by identifying the node's sequence number. Consequently, the routing table information won't be forwarded through the network anymore; so the network will be secured against black hole attack [4]. Another proposed protocol to secure AODV protocol against black hole attack is ERDA (Enhance Route Discovery for AODV). In such a work, ERDA introduces new condition in the routing table update that leads to improvement of network performance. The protocol can isolate the malicious node and decrease the effectiveness of black hole attack with no changes in AODV routing protocol scheme [18]. This protocol can be improved in trusted base for better privacy protection.

In this work, another trust-based solution for black hole attack will be presented using level of trust, which can give more appropriate ideas along implementation, in comparison to previous presented protocols.

5 Proposed Protocol

The present study tries to improve the security performance of the AODV routing protocol against black-hole attack using different level of trust for MANET nodes and impose the limitations based on the nodes' Trust Level (TL) in order to distinguish the reliable and unreliable nodes of network.

In the proposed protocol, each node has a list of its neighbors with their TL values. TL indicates that how much a node can be trusted; higher trust level range of a node represents the more reliability. The range of TL value is determined from -1 to 2. Each node initially has the TL value of 1 by joining to the network, and then maybe gain higher value by acting normally. On the other hand, if a node acts maliciously it would be set to the blacklist immediately with 0 TL value. The detail of each value is shown at the following table.

Table 1. Description of Trust Level values

TL Value	Description
-1	When a node is permanently blocked
0	When a node is in blacklist
1	Initially joined to network or released from blacklist
2	A node can reach to this rate after one trust testing

The improving protocol is described as the following steps:

First step is in the RREQ scope which the source node is broadcasting the RREQ to discover a destination node or an intermediate node with fresh enough route toward a desired destination; this part is same as the original AODV protocol.

Second step is in the RREP scope which uses the TL table, and the trust test technique to distinguish the reliable and unreliable nodes and encouraging or penalizing them respectively. When each node receives the RREP message, initially checks its own TL table. If the sender node of RREP is not a Suspicious Node (SN), TL exists with high enough value (TL= 2) in the TL table of the receiver node (Examiner Node). In this case, EN would evaluate the sender node as a trusted valid node. Then the process would be continued in the fourth step.

Otherwise, when the trust level value of the sender node in the trust level table of EN is equal to 1, then EN has to use trust test technique explained in third step. If the TL value is equal to -1 or 0, then SN has been black listed previously and known as an invalid or malicious node. Hence the RREP of SN would be dropped and never reach the originator.

In third step, we have the trust test technique. In this technique, the receiver node of RREP, sends a test RREQ message with a distinct RREQ ID to SN containing originator IP address (that can be any IP address) and destination IP address, which should be its own IP address; As a result, the reply message of this request would be received by EN itself. If the destination sequence number of the reply packet has the same value with the one that is existing in EN's routing table, SN could be a reliable node. (because as mentioned earlier, the malicious node replies the fake packet with a higher destination sequence number to persuade the originator node to change the

route to itself); In this case, lower hop count between them must be chosen, which leads to have a shorter route. Subsequently, the TL value of the reliable node should be increased in the EN's trust level table; and it continues to the next step.

On the other hand, if the destination sequence number of the reply packet does not have the same value with the one that is existed in EN's routing table, SN would be an unreliable node. In other words, SN fails in trust testing. In this case, SN would be known as a blacklist node and the TL value of SN would be decreased. If TL value becomes 0, the node would be blocked temporary. After a certain time (blacklist timeout) the node would be released, and the TL value would be set as 1. If the node acts maliciously more than 3 times, the node would be blocked permanently as well as changing TL to -1. Blacklist timeout would be doubled at each time, until the node is blocked permanently and not to be able to communicate any more or establish wrong routes.

As an example, Fig. 1 and Fig. 2 assume that EN has no information about SN regarding TL value. So, initially the SN's TL value would be set as 1 in EN's table. Fig. 1 shows that the EN found the SN as a non-malicious node after a trust test, hence the TL value of SN would be increased to 2 and then the RREP would be forwarded toward the source node.

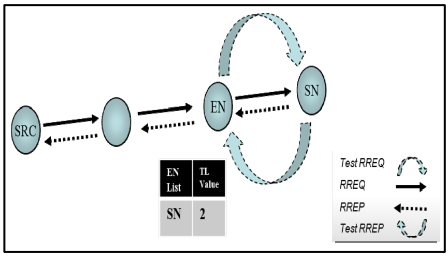

Fig. 1. After testing a non-malicious node

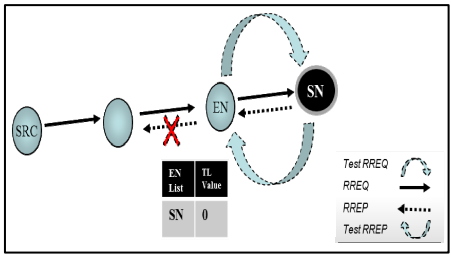

Fig. 2. After testing a malicious node

Fig. 2 shows that EN found the SN as a malicious node, hence the TL value of SN would be decreased to 0 and block the node for the certain block time. The EN node would drop the packet and prevent to establish wrong routes. After block time the SN will be released, and its TL would be set to 1. As mentioned, if SN acts maliciously again, corresponding TL would be set to 0 for the second time, and node should be blocked once more for longer time (doubled time). After releasing, if the node shows malicious behavior for third time, the node will be blocked permanently by changing TL value to -1 therefore, it will not be able to communicate with other nodes anymore.

In fourth step, the receiver node of RREP passes the message to the next hop of its reverse route until RREP reach the source node. So data can be transferred through forwarding tables, which has been made during unicasting RREP message. This action is the same as original AODV.

The general trend of the improved protocol in counter with black hole attack is described by the flowchart shown in Fig. 3.

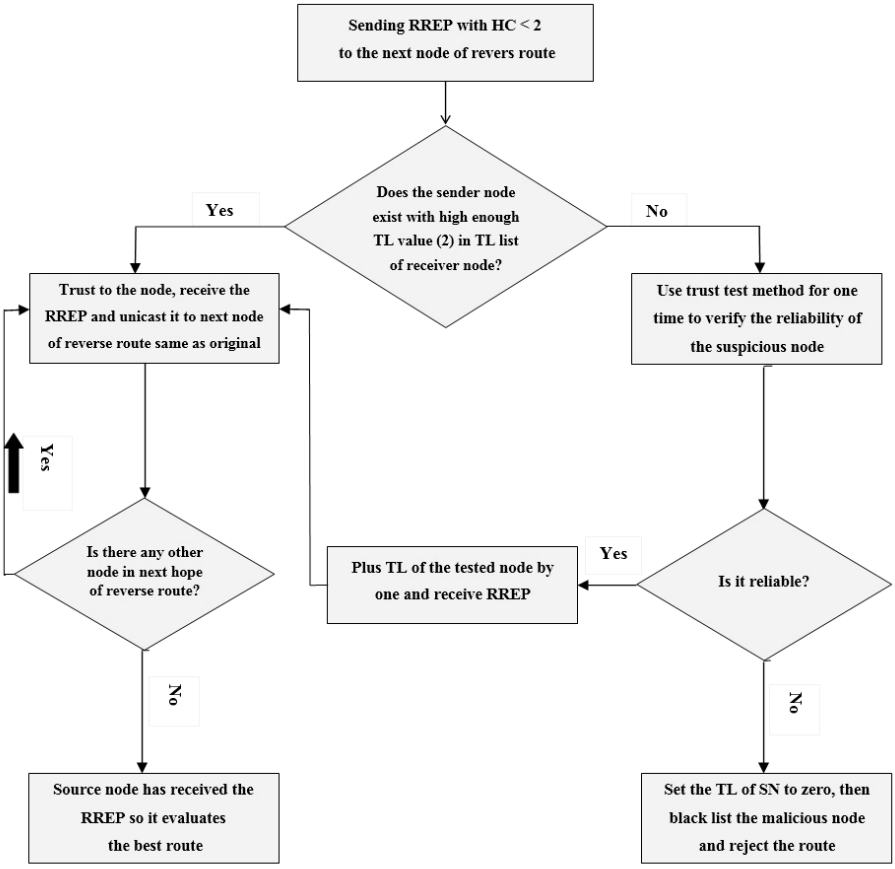

Fig. 3. Flowchart of RREP in the proposed protocol

6 Simulation Results

In this section, the performance of the proposed protocol is evaluated by NS-2 simulator in order to reveal its efficiency.

The following graph compares the total received throughput of network in the proposed protocol and the AODV protocol. Mobility of nodes, forces the AODV protocol to change its route continuously, which leads to give an opportunity to the

attacker nodes to disrupt routing. This can cause a significant fall in the received throughput of network (Fig. 4); however, the proposed protocol has a high received throughput. This advantage is achieved because the proposed protocol can detect the attacker at the initial time of route discovery.

In the proposed protocol, we have to use extra packet controls for trust test technique, which cause the overhead to increase. Although the proposed protocol overhead enhanced initially due to the trust test technique at the start of finding reliable routes through new nodes in a network, after a while the overhead could be reduced to the lowest value as TL values are existing in TL tables and there is no need of trust test technique. Therefore, as graph shows (Fig. 5) the proposed protocol overhead has an upward trend by increasing nodes number, and it almost stays at the higher level of pure AODV protocol.

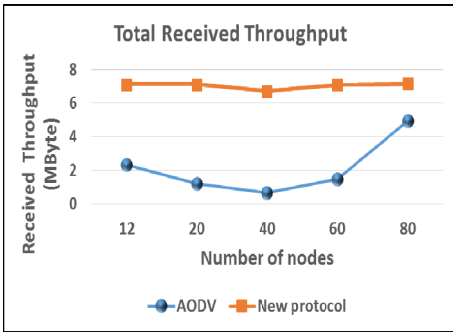

Fig. 4. Total received throughput of network against attackers in different number of mobile nodes (speed 5 to 10 m/s)

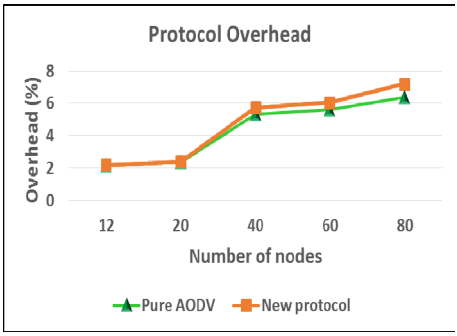

Fig. 5. Protocol overhead of network in different number of mobile nodes

For AODV protocol, the probability of facing to attacker nodes in sparse networks is higher than the dense networks; therefore, networks with a lower number of nodes have lower PDR. However, the proposed protocol detects the attacker nodes in any situation, which leads to appropriate PDR (Fig. 6).

Fig. 7 compares the average end-to-end delay of the proposed protocol and AODV against attackers, whether the network nodes have mobility or not (Mobility speed: 5 to 10 m/s). Regarding to the graph, the average delay of the proposed protocol is almost always stayed at lower rates than the AODV protocol against attackers in either mobile networks or non-mobile networks.

Although by increasing the number of mobile nodes in a network the Average delay of the proposed protocol takes an upward trend, it is much lower than the AODV protocol; and in fact, all the average delay values of the proposed protocol are still lower than the AODV rates which fluctuate greatly.

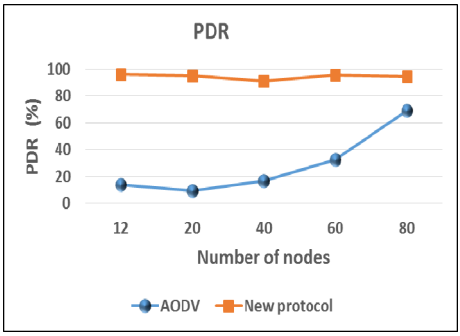

Fig. 6. PDR of network against attackers in different number of mobile nodes

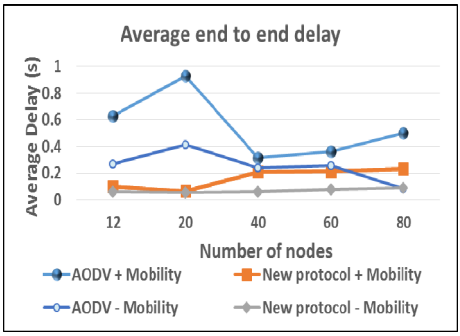

Fig. 7. Comparing average end-to-end delay of the proposed protocol with AODV against attackers in different number of nodes in network

The following graph compares the rate of the average end to end delay of the proposed protocol with pure AODV protocol (no attacker) in a different number of mobile nodes (Fig. 8) in networks. The only main extra delay in the proposed protocol is when the network needs to use trust test technique. As the graph shows, the average delay of the proposed protocol is slightly greater than the pure AODV protocol.

In addition, it can be clearly seen that, increasing number of nodes cause rising of the average end to end delay of network.

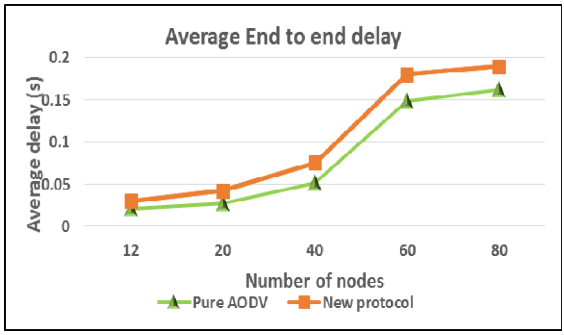

Fig. 8. Average end-to-end delay in different number of mobile nodes in network (Speed of 5 to 10 m/s)

The delay and PDR of some related works are shown in the Table 2. As it is clear, the proposed protocol has an almost better delay in comparison to another trust based techniques (i.e. TCLS, LLSP and RSRP [13]) which is evident in Fig. 9. The PDR of the proposed protocol is much better based on simulation results. This is because of the complicated mechanism of other protocols to find out its reliability. While in the proposed protocol, the unreliable node could be detected at the initial time of routing, which leads to much higher PDR. In comparison to other protocols, it can be clearly seen that the proposed protocol performance is much improved.

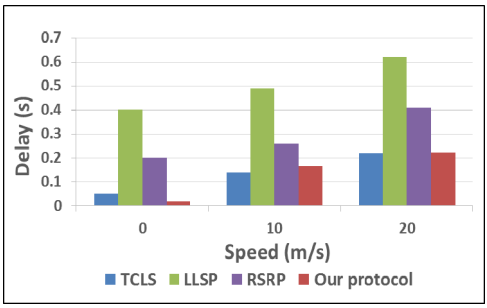

Fig. 9. comparing delay of some trust based techniques vs. speed

Table 2. Comparing different protocols delay and PDR when speed is about 10 (m/s)

Routing Protocols	Delay	PDR (%)
TCLS	0.14	62
LLSP	0.49	50
RSRP	0.26	55
The proposed protocol	0.16	94

Furthermore, there are several substantial advantages in using the proposed protocol comparing with some previous works such as monitoring, packet analyzing and cryptographic techniques. In addition, the comparison of present protocol with some other particular researcher's protocols is given in Table 3.

Monitoring or administration techniques usually cooperate with some extra monitor nodes with intention of collecting all other nodes' reports and subsequently decide in a complex manner about the malicious nodes. This is true that this monitor technique tries to enhance the security, but it causes changing the nature of MANET by adding central manager nodes. In comparison, the proposed protocol does not need any extra nodes whilst supporting the MANET features.

Another offered secured protocol is based on packet analyzing, which always has to suffer the overhead of complex computing. Whereas, in the improved proposed protocol, overhead can be decreased using the trust level technique.

In cryptographic techniques, there is mostly a large packet size because of digital signatures. In contrast, the proposed protocol packets do not use any digital signature and have a default field of AODV packets in trust test.

In some offered previous researches, after sending data packets toward a desired destination, it is found that an error had been occurred by an unreliable node (as the number of received packets is less than it expected), hence it starts to find the problem and detects the malicious node following by sending data packets again. Instead, the proposed protocol detects the malicious node as long as it starts a communication, before sending any actual data packets.

One of the significant advantages of the proposed protocol is that only two trust test packets are done and a TL table, with the aim of evaluating a node as reliable or unreliable. After a while, nodes do not need any more trust test packets with respect to the TL table, which leads to low overhead and faster operation. The efficiency of a network can reach the maximum when each reliable node gets the highest value of TL, and the malicious nodes blacklisted with the lowest TL. In other words, the proposed protocol initially has a light overhead and delay, but after some time, overhead and delay reach the lowest value in comparison to other protocols.

Another advantage of this proposed protocol is that it can stand against mass of attackers, because each node has its own TL table and can decide about the reliability of each node.

Another prominent achievement of the proposed protocol is that it can detect the malicious nodes, whether the attacker playacts as a destination or pretends to have a route to the desired destination. In other words, the attackers would be detected by the proposed protocol, whether the malicious node acts to have the normal RREP or the gratuitous one. At the end, the advantages of the proposed protocol in comparison with some other protocols are demonstrated in Table 3.

Table 3. The advantages of the proposed protocol in comparison with some other protocols

Routing protocol	Technique	Problem	The proposed protocol advantages
SAODV [8],[19]	Cryptographic techniques	Message size is significantly large, mostly because of digital signatures.	It does not need any digital signature
A-SAODV [14]	Threshold mechanism	Large packet size	Packets has an original size, does not need threshold mechanism
B-AODV [17]	BRREQ replace of RREP	Extra network traffic when nodes have low movements	The traffic is lower even in networks with fixed nodes
RAODV [14]	Adding two type of control packet	Used the extra packet controls Still has some flaw points	We just use the original control packets
ARAN [20]	Preliminary certification process	High power consuming and large size of the routing messages at each hop.	Messages obey the original packet size

7 Conclusion

In this article, we have focused on securing AODV routing protocol in combat with black-hole attack in particular. Since the AODV is a weak protocol in a countermeasure to this attack, the performance of network stays at a low level. In consideration of this problem, we proposed an improved protocol as means to enhance the security of AODV routing protocol and revised its flaw points. In the proposed protocol, we used the trust test technique and the TL tables to identify reliable or unreliable nodes in a network. In fact, TL tables considerably help the network performance with the intention of reducing trust-test packets' traffic, which leads to lower delay and higher performance in a network. The efficiency of a network can reach to the maximum when each reliable node gets the highest value of TL, and the malicious nodes blacklisted with the lowest TL. In other words, the proposed protocol initially suffers a light overhead and delay, but after a while it reaches to the lowest value. Lastly, the analysis result of simulation demonstrated that the proposed protocol tends to outperform the AODV routing protocol against black-hole nodes in all cases of performance metrics.

References

1. Agrawal, S., Jain, S., Sharma, S.: A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks. Journal of Computer 3(1), 41–48 (2011)
2. Wadbude, D., Richariya, V.: An Efficient Secure AODV Routing Protocol in MANET. International Journal of Engineering and Innovative Technology (IJEIT) 1(4), 274–279 (2012)
3. Venkatraman, L., Agrawal, D.P.: Strategies for enhancing routing security in protocols for mobile ad hoc networks. Journal of Parallel and Distributed Computing 63(2), 214–227 (2003)
4. Raj, P.N., Swadas, P.B.: Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. arXiv preprint arXiv:0909.2371 (2009)
5. Vasava, M., Patel, H.: Comparison of Different Methods for Gray Hole Attacks on AODV based MANET. International Journal of Engineering Development and Research 2(1), 60–66 (2014)
6. Sanyal, S., Abraham, A., Gada, D.: Security Scheme for Distributed DoS in Mobile Ad Hoc Networks, School of Technology and Computer Science, Tata Institute of Fundamental Research, India, Mumbai University, India (2010)
7. Sarkar, P., Chaki, R.: A cryptographic approach towards black hole attack detection. In: Meghanathan, N., Nagamalai, D., Chaki, N. (eds.) Advances in Computing & Inform. Technology. AISC, vol. 176, pp. 273–278. Springer, Heidelberg (2012)
8. Goswami, J., Dafda, A.: Security aspects with AODV in WMANETs. In: National Conference on Power Systems, Embedded Systems, Power Electronics, Communication, Control and Instrumentation. Department of Electronics & Comm. Engg., L.D. Collage of Engg. Ahmedabad, Gujarat, January 2012
9. Perkins, C.: (RFC) Request for Comments – 3561. Category: Experimental, Network, Working Group, July 2003
10. Zapata, M.G., Asokan, N.: Securing ad hoc routing protocols. In: Proceedings of the ACM workshop on Wireless Security. ACM (2002)
11. Meka, K., Virendra, M., Upadhyaya, S.: Trust based routing decisions in mobile ad-hoc networks. In: Proceedings of the Workshop on Secure Knowledge Management (SKM (2006)
12. Cordasco, J., Wetzel, S.: Cryptographic versus trust-based methods for MANET routing security. Electronic Notes in Theoretical Computer Science 197(2), 131–140 (2008)
13. Simaremare, H., et al.: Secure AODV routing protocol based on trust mechanism. In: Wireless Networks and Security, pp. 81–105. Springer, Heidelberg (2013)
14. Sharma, P.: Trust based secure aodv in manet. Journal of Global Research in Computer Science 3(6), 107–114 (2012)
15. Uddin, M., Rahman, A.A., Alarifi, A., Talha, M., Shah, A., Iftikhar, M., Zomaya, A.: Improving Performance of Mobile Ad Hoc Networks Using Efficient Tactical On Demand Distance Vector (TAODV) Routing Algorithm. International Journal of Innovative Computing, Information and Control 8(6), 4375–4389 (2012)
16. ShafieeNejad Ghahroud, H.: Detection of Malicious Node in Black in Black-Hole Attack on AODV Protocol, Shiraz University of Technology: Hamid Shafiee Nejad Ghahroud (2012)
17. Liu, S., Yang, Y., Wang, W.: Research of AODV Routing Protocol for Ad Hoc Networks1. AASRI Procedia 5, 21–31 (2013)

18. Jali, K.A., Ahmad, Z., Ab Manan, J.-L.: Mitigation of Black Hole Attacks for AODV Routing Protocol. International Journal of New Computer Architectures and their Applications (IJNCAA) 1(2), 336–343 (2011)
19. Masdari, M., Pashaei Barbin, J.: Distributed Certificate Management in Mobile Ad Hoc Networks. International Journal of Applied Information Systems (IJAIS) 4, 33–40 (2012)
20. Sanzgiri, K., et al.: A secure routing protocol for ad hoc networks. In: Proceedings of the 10th IEEE International Conference on Network Protocols. IEEE (2002)