The Caspian Sea Journal
ISSN: 1578-7899

Volume 10, Issue 1, Supplement 4 (2016) 398-406

Providing a New Algorithm to Improve AODV Protocol Security and Performance of Ad Hoc Networks against Black Hole Attacks

Samad Soltanzad,
Faculty of engineering, Payame Noor University, Tehran, Iran
Reza Askari-Moghadam, *Ph.D.*
Faculty of New sciences and technologies, University of Tehran, Tehran, Iran
Corresponding Author Email: r.askari@ut.ac.ir

ABSTRACT─ Because of some Ad hoc network properties such as dynamically network structure changing, node's reliance in each other, lack of the fixed infrastructure to investigate the nodes behaviors and performance and lack of certain defensive lines, these networks are not supported against destructive node's attacks. The one of these attacks is black hole attack in which destructive nodes absorb and destroy data sets at network. Then providing an algorithm to detect and encounter the black hole attacks in Ad hoc networks are seems necessary both in terms of security and network's performance. In this article a new algorithm had been suggested which improve the AODV routing protocol security against black hole attacks in Ad hoc networks. Considering the node behaviors in network we attempted to identify the destructive nodes and delete them from routing process. Suggested algorithm simulated by NS2. Simulation results show the considerable improvement in end to end delay and packet delivery ratio in the suggested algorithm compared to the original version of AODV protocol which had been attacked.
KEYWORDS: Ad hoc network, AODV routing protocol, security, black hole attack.

Introduction

During the recent years widely user's accessibility to wireless communication and manual devices caused increasing research on Ad hoc networks which are not require a predetermined infrastructure. Ad hoc networks are designed to correlate remote devise such as cell phones, laptops and pocket computers to each other's. Developing and application of Ad hoc networks are owed to radio technology development and its most important purpose is success on civil applications. At first, the concept of these networks was separate from networks with fixed infrastructure and Internet and this is why the Ad hoc networks technology was not used in most people's lives. In Ad hoc networks, node's mobility may alter the path between two nodes. This is why these networks are different from other wireless networks. Beside the Ad hoc networks advantages, providing and maintaining the security of these networks confronted many problems. Applying radio signals instead of wires and cables, and indeed without borders covering at the network structure, hackers will be able to show themselves as a member of these networks if the security obstacles in these networks had been removed, and so the accessibility to vital information, attack to organization and society service providers, information destruction, creating confusion in networks node's communication to each other, providing false and misleading data, misusing the network effective wide band and other destructive activities will be occurred [1]. Ad hoc networks are composed from independent wireless nodes which manage the network without any infrastructure themselves and can attach or leave the network easily everywhere and every time dynamically. The relationship between the nodes in this network is somewhat base on reliance and cooperation between the nodes. In these kinds of network, every node sends the packets not only as a host, but also as a router. The most important properties in these networks are presenting a dynamic and Variable topology which is because of node mobility [2]. Wide applying the Ad hoc networks in military environments and other sensitive security application had made the security as a fundamental requirement since introducing these networks. Since all of the communication done wirelessly it could be heard or changed. Also since these nodes contribute to the routing, then a destructive node in routing could leads to network destruction. In these networks, it is difficult to imagine a contribution unit or universal key infrastructure. Since these networks are made often without any preprogramming and they need a short time to security. Then the security discussed in these networks separately [3]. In suggested algorithm, the purpose is to be able to identify the destructive nodes and delete them from routing with considering the node's behavior in the network. In this algorithm, to identify the destructive nodes it also applied some rules and also IDSAODV protocol which had changed, which leads to obtaining the new rules to identify the destructive nodes. Applying this algorithm, improves AODV protocol security and performance against black hole attack and also the percentage of identifying the destructive nodes. Following, we refer to conducted studies and then investigate the problem and providing a suggested strategy and finally the results will be presented.

Conducted works

Many studies had conducted to improve the security in Ad hoc network against black hole attack. This method focused on many conducted studies related to black hole on AODV protocol of Ad hoc networks [4]. There are some suggestions to discover and decline the black hole attacks at Ad hoc networks. Although most of the solutions do not work properly single black hole attacks and they failed at discovering the bulk black hole attacks. The author had provided a comparison between existing solutions, but this method is not reliable because most of the solutions do have long delay, big network's overflowing is because of new introduced packets and mathematical calculations. Then the author suggests that applying the mixed techniques can be suitable to discover the bulk black hole attacks. In another way, primary credit of middle nodes which send the respond's message, but the confirmation from destination received from destination will be evaluated [5]. If confirmation doesn't receive by the destination, this middle destructive node's background will be saved at black list judge in the future CL parameter is a calculator which shows the bad middle node's behavior while they send an incorrect routing respond. If CL be more than 3 for every node, that node will be introduced as a destructive node and it will be avoided from introduced route by this node. In next work, we want to induct the simulation and compare recommended model to pilot results. Perhaps when the node does not receive the confirmation from destination node at a determined time it will be a false discovery. The next step to decline the discovery ratio is false to obtain a short prevention method against black holes attack. In another research Latha Tamilselvan had recommended a solution to improve the main AODV protocol [6]. This idea had designed by chronometer at Rimer Expired Table as long as this request is received, the requests will be gathered from other nodes. The packet sequence number and delivery time saved in a collection routing response table (CRRT), the delay value is calculated based on the time of first time delivery of routing request, after that judges calculated the route based on threshold value. The author had simulated this solution by GlomoSim software and the results show that the ratio of packet delivery improves by delay and low over flow. In a research by Djenouri and Badache, a method presented to monitor, discover and solve the black hole attack's problem in Ad hoc networks [7]. At the first step (monitoring), an effective method was applied which consists of random couple jumps. Authors applied Bayesian method to charge the nodes to disable the nodes release before judgment. The advantage of this method is to prevent accessibility of false charge attacks and declining the false properties which occurred via node's dynamic and channel's conditions. This method can be used to all released packet's kinds, self- centered and malfunction nodes which caused black hole attack. This solution can identify the attacker when the packets are released. Authors used Glomosim to simulate this method and conclude that random double sump is considerable as a very effective method compared to ordinary double jump to discover the low mistake and high fact and very low over flow more than ordinary double jump. This method had applied base tester proof, although it cannot prevent the multiple malfunction nodes and group black hole attacks. In another research Ming- Young Su suggested an identifier method to prevent the black hole attacks called anti-black hole [8]. In this method, some of the nodes applied as the node's identifier. They act in sniffing position to evaluate the mistrust ratio to the other neighbor. When the mistrust ratio increase from a burden an obstructive packet will be distributed via the nodes with identifier, nodes will be aware all over the network to preserve the destructive nodes at quarantine. Simulation with NS2 shows a good discovery ratio, but end to end delay had increased. In this study, a new solution had presented which prevent the group black hole attacks [9]. In this method an accuracy table used to counter the black hole attacks in which every node does have an accuracy ratio which considered as the confidence level for that node. In the confidence level of a node be zero, this means that this node is a hostile node called black hole which should be discarded. The origin node sends the Rout request to its neighbors. Then origin will be waited as TIMER to gather the rout responds. In every one of the received rout's responds, the level of responder's node accuracy is determined. For every one it the level of its next step's accuracy will be evaluated. If there are two or more than two roust with equal accuracy level, then the rout with lower level will be selected, otherwise the more accuracy Level will be selected. Receiving the information packets, end node sends a confirmation message to origin to increase the middle nodes accuracy level, if acknowledgment is not received then middle node's accuracy level will declined.

Study basis of suggested method in [9] are as follow:

Respond gathering:

- Origin address
- Destination address
- Steps number
- Next step
- Life long
- The number of destination series

Choosing a response between received responses, search the responder's node accuracy levels and its next step. If their average level be more than threshold, then the node considered reliable. If you get several responses, the response with the highest accuracy level will be selected. If accuracy levels be equal for two nodes. The node with fewer steps will be selected.

- Accuracy table updating
- Black holes deleting.

In the other research a method had introduced to identify the group black hole attack [10].
This protocol is a few modified version of AODV protocol conducted by data routing information table (DRI), routing request message and route response. Every node preserves a routing information table. DRI pursues, if node exchanges its neighbors. In this table there is an entry for every neighbor. DRI shows that if the node sent via this neighbor and also if the node had received the data neighbor's or not. In this study a solution had suggested to black hole attack [11].In this method, when a node sends the destination response, a survey process performs around that node. Then base on notified views from node's neighbors it is determined of the node is destruction or not. Alternatively, a new solution to discover attacks black hole is provided that uses the analysis neighbors. If a new neighbor introduced to the node at the first step, current node will be suspicious to black hole, and statically analysis will started by some of the nodes in a suspicious position to attack. It supposed in this method, that by making the black hole, close neighbor to second enemy node (black hole destination) will increased. The one of the main disadvantages of this method is that a new node added to the network, statically analyzes should be conducted certainly and it is possible to there is a false black hole in this position.In this study a new method had suggested to discover the group black hole at AODV routing [13]. In this method, origin node by finding more than one destination confirm the node credit which had started the routing response- origin node waits to receive the routing response's packet more than two nodes. when origin node receive the routes responses, if there is a common steps to destination in the routes, origin node can determined The secure rout to the destination.

Problem explanation

Because of some Ad hoc networks properties such as dynamically network structure changing, node's reliance in each other and lack of fixed infrastructure to investigate the behaviors and performances and lack of certain defensive lines, these networks are exposed to many attacks compared to the other networks. One of these attacks is black hole attack. At first, black hole attacker needs to enter the contribution delivery group to can separate data packets from multi contributions session. Attacker node pretends itself as the shortest route to reach the packets to the destination node to make the sender of packet to deliver its own packet to destination via this false node. Then easily starts to destroy all the pass packets. In this kind of attack, some or all of the received Packages delete instead of delivery and this causes the results of packet delivery ratio be very low [14]. Black hole attack is divided to two groups: single and group black hole attacks. Single Black hole attack is performed via one of the exiting nodes at network, but there is more than one destructive node at group's black hole attack which cooperate at attacking, and in other words, black hole nodes can work just like a group and this means more than one black hole node work collectively to conduct the other nodes falsely. This kind of attack called group black hole attack. The node which performs the black hole attack will wait to receive a request route packet from neighbor nodes. By receiving the packet of rout request, immediately and without evaluating the routing table, responds to the route request by delivering a packet of false route response. In other word, destructive node, regardless its own routing table and if there is a route to destination node or not, sends a suitable route response to received route request packet and this causes declining the route of response packet comparing the other nodes. Attacker node put the highest order number and lowest steps number in route response packet and then deceives the route requester's node. The node had the route request packet supposes had discovered the best route by receiving this packet of route response. Then it considered this node as a proper and short route to send the packets and delivered its own packets via the route of this node. The black hole had created and the node known as black hole instead of sending the packets to receive information or throwing them out. Since the destructive node not investigate its own routing table, then response the requester node before the other nodes. If destructive node introduces itself as the proper route to all of the network's nodes and it can receive all the network's traffic, and then causes losing all of the network's packets and preventing the attack to service [15, 16]. Figure 1 shows a view of black hole attack.

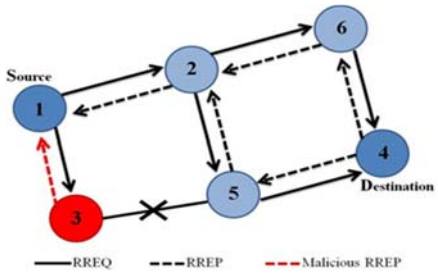

Figure 1: Black hole attack

Suggested algorithm

Suggested algorithm had conducted on AODV protocol. In this algorithm have been attempted, considering the node's behavior in the network destructive nodes identified and deleted from rotting. By increasing the destructive nodes, identifying the destructive nodes will be more difficult. Then rate of packet delivery declined by increasing the destructive nodes. Then by identifying more destructive nodes can decrease delay and increase the ratio of packet delivery.

Destructive nodes are the nodes which respond the route request packet by sending the false route respond packets. Many data packets delivered them but any packets or a few packets delivered by them to destination or neighbor nodes. When a node received packets of route response from its own neighbor node, then if the responder node be a middle node and not a destination node it investigates if it is not one of the nodes in quarantine. If the node be a destructive node, the route response packet threw out. Otherwise voting process conducted around responder node to obtain all the expected node's activities. Then base on received information, investigate the expected node accuracy based on the rules to determine the destructive node at origin node, and if it is a destructive node, a danger message contributed in the network to put that node in quarantine. Suggested algorithm basis is as follow:

1. Related information to the node activity is saved and investigated. The communication between the nodes in Ad hoc networks based on reliance and cooperation between the nodes. Two nodes which are not in radio span of each other applied the relationship of the other exiting nodes in the network. Then existing nodes in the networks conduct some activities to make relationship between two nodes, to save and investigate these activities. These activities consist of the number of data which receive the middle node from origin node, the number of middle nods which are delivered to destination node and the number of responses which sent the middle node to the origin node.
2. The request packet of neighbor views related the node which delivered the packet of route request will be sent. In Ad hoc network, because there is some network's node which related to each other, the neighbors of that's node can be applied to receive the information related to destructive node which delivers the packet of route response to origin node. Then to receive the information related to the node which delved the packet of route response, the request packet of the view will sent its neighbors nodes, saved information in neighbor nodes related to sender node will receive the packet of route response.

After delivering the packet of views request related to the node which delivered the packet of route response, neighbor nodes deliver their information and views about being that's node a destructive one to the origin and origin node receive and save the Information.

3. Receivedinformation and the attitude about being a destructive node is evaluation. After origin node receives the information from neighbor nodes this information is investigated to find the accuracy of the node which delivered the packet of route request.
4. A danger packet to quarantine the destructive node delivered and contributed all over the network, if obtained information from neighbor nodes be the node which delivered the packet of route response, Base on determined rules, it is known as destructive node, the packet of danger will be broadcasted all over the network to inform the other network's nodes from being destructive of that's node and quarantine.
5. The nodes inside the quarantine deleted from routing process. After broadcasting the dangers packet all over the network, destructive node is put in the quarantine. In routing process, existing nodes are removed from routing in quarantine and then they do not send the delivered packets at the route of these nodes [13].

In suggested algorithm following rules are applied to identify destructive node:

1. The node which delivers faster than the other network's nodes to the sender node of the route request a packet of route response, it could be a destructive node.

Because destructive node, regardless the its own routing table and if there is a destination node's routing or not, send packet of suitable route request base on received route from origin node, this can decline the path of the packet of route response to the other nodes; In other word because destructive node does not evaluate the routing table, responds to the route requester node before the other nodes.

2. The node with highestorder number and lowest step number can be destructive node. As mentioned above in black hole attack, attacker node put the highest and equal order number with the lowest step number in this case, route requester' s node supposed by receiving this packet of route response. As a consequence, this node (destructive node) considered as the suitable and short own packets from the route of the node.
3. The node which sends some packets to the nodes can be also a destructive one. Destructive node can received at first some packets from origin node and send them to destination or neighbor nodes to cheat the network nodes and after delivering some packets, destructive node starts instead of delivering the packets to destination to receive their information and / or throw them out.
4. The node that received more packets and delivered just one packet is a destructive node. If anode had received many packets from origin node but only one packet had delivered, it a destructive node. Destructive node deletes the received packets instead of delivering and this causes the results packet's delivery ratio decreased very much.
5. The node that received many packets and had not delivered them is certainly destructive. Destructive node pretends itself as the shortest way to take the packets to destination, makes the origin node to take its own packets via this false node. Then destructive node does not deliver the received packets to destination and as a sequence, starts to destroy all passing packets.

Simulation results

Simulation's environment

NS2 simulator software applied to simulate. This software is suitable both of wired and wireless networks, and many protocols support software. Its primary basis is Linux but it can be installed on different windows too. Ns2 is the standard simulation software at network researches field. Different parameters had applied in simulation to evaluate the suggested algorithm performance as follow:

- End to end delay: The average delay between the sending time by origin nodes to the receiving time by destination nodes which includes all the created delays such as routing, buffering and processing at middle nodes etc.

- The ratio of packet delivery: The ratio between the number of delivered data packets by origin nodes and the number of received data packets at final destination.
- The ratio of packet losing: The ratio of all data packets that are deleted because of crowd and the destructive nodes, to all the data packets which are delivered.
- Through put: All the received information at a time span.

The number of existing nodes at the network is 20 nodes. These nodes set at random position. There is one destructive node which performs the black hole attack. The simulation environment is considered 700* 700 meters. The packet size is 512 bits. Simulation performs at 200, 400, 600, 800 and 1000 seconds. In different scenarios, suggested protocol had compared to AODV protocol which is attacked. The results of simulation had shown at following schemes. In the schemes, AODV is a standard protocol which poetical which could identify the attacker nodes in black hole correctly.

Table 1: Simulated environment by NS2

Simulator software	**NS2**
Simulated time	**200s-1000s**
Network's nodes count	**20**
Destructive nodes count	**1**
Simulated environment	**700*700**
Routing protocol	**AODV**
Type of traffic	**CBR**
Ratio of sending	**10kb**
Size of packet	**512b**

Simulation results

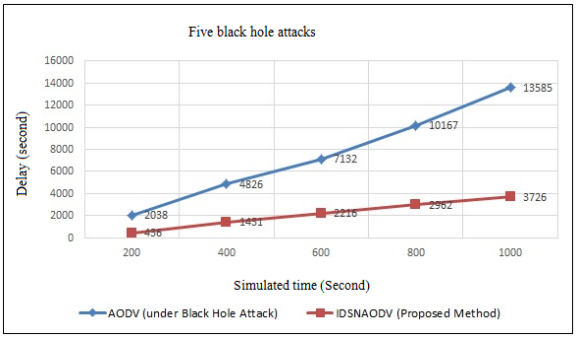

Figure 2: End to end delay

In figure 2, the influence of increasing the simulation time on end to end delay had shown. When there are destructive nodes in the network, suggested algorithm with fewer end to end delays identify the destructive nodes and inform the other nodes, but AODV doesn't can do this. So it has more end to end delay. Because sendingof lower general requests, suggested algorithm does have lower end to end delay compared to AODV protocol. At 200 seconds of simulation time, because of very low delay at end to end, the ratio of packet delivery is so high, but gradually when the time span increased the suggested algorithm end to end delay will increased and the ratio of packets delivery will declined.

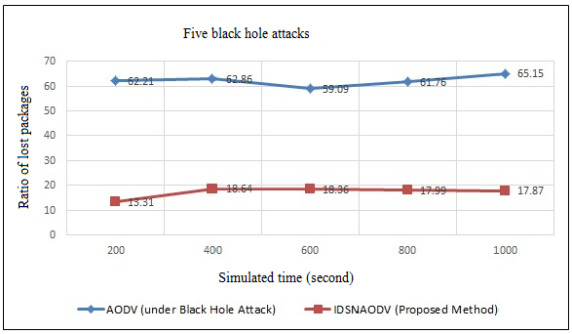

Figure 3: Ratio of lost packets

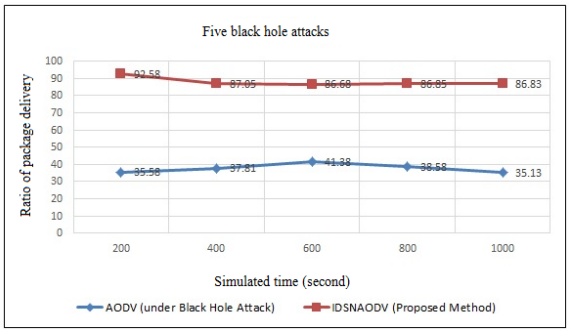

Figure 4: Ratio of packet delivery

In figure 3, the influence of increasing the simulation time on lost packet ratio had shown. AODV protocol losses more packets compared to suggested algorithm and this show the successful being the attacker nodes at performing black hole attack on this protocol. In suggested algorithm at 200 to 1000 seconds, the ratio of lost packets was between 10 to 20 percentages. But in AODV protocol, the ratio of lost packet was between 59 to 66%. In general, the ratio of packet losing in suggested algorithm is lower than AODV protocol and this is because of rules and calculations of suggestion method to identify the destructive nodes.

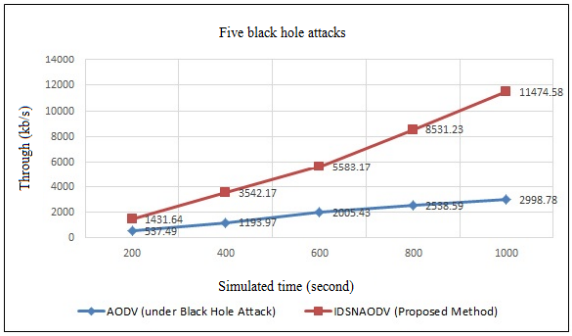

Figure 5: Throughput of protocols

In figure 4, AODV and IDSNAODV protocols had compared in terms of the ratio of packet delivery. As it is shown the ratio of packet delivery had improved at suggested algorithm compared to AODV protocol, and this is because of better performance of suggested algorithm at identifying the destructive nodes and then making them quarantine and deleting them from routing. The ratio of packets delivery at 200 to 1000 seconds was 85 to 93% at suggested algorithm, but at AODV protocol, the ratio of packets delivery between 35 to 42%. Figure 5 shows two protocol's through put, since suggested algorithm in identifying attacker nodes does have more ability and the ratio of packets delivery increased, them throughput in suggested algorithm increased compare AODV protocol. Throughput for two protocols increased by increasing the simulation time, but at 200 to 1000 second

span time, throughput of algorithm was between 1400 and11500 and the throughput for AODV protocol was between 500 and 3000.

Comparison

In [43] a method presented to encounter the group black hole attack, in which a response table applied to gather the received response to origin node and also a table called accuracy table kept by all the nodes, and accuracy levels of the network's nodes are saved. The way to select the route in this method is somewhat different compared to AODV protocol. In this method with updating and broadcasting of accuracy table, the nodes which perform group black hole attack are identified by origin node and preempted in routing. Route discovery process in this method is similar to AODV protocol. In this way, the origin node waits by a timer after broadcasting the route request. After this time, numbers of responses are delivered to origin node. These responses are stored in a table called response table. To determine the black hole attack, the accuracy level is assigned to each node. Accuracy levels are saved in a table called accuracy table. The source node increases or decreases accuracy levels depending on the participation of the faithful in delivering data packets to the destination node. This method is similar to AODV protocol, from the received responses is chooses response with the highest sequence number and if there are multiple responses with the same sequence number in the table, a response with fewer steps is selected. Before sending the accuracy level and the next step of responder node are considered. If one or both of them was zero, selected response is discarded and the response is the second largest destination number.This method is simulated by NS2 software. The network includes 30 nodes. The simulation environment is considered 1000*1000 meters. Packet size is 512 bytes. The simulation duration is 300 seconds. In the schemes, BAODV means AODV protocol which is attacked and BPM is suggested protocol [18] and IDSNAODV is my suggested protocol. The measured criteria to compare the network performance include end to end delay and the ratio of packet delivery.

In method [19] when the origin node does not receive ACK from destination or PREP had come from black hole nodes with highest order number, routing does not repeated and applied RPEP with second highest order number that usually is the response of an honest node and it is effective at declining the end to end delay. BAODV protocol loses many packets which show the black hole node's success in performing the group black hole attack. Improving the ratio of packet delivery in [19] method is more than 50% in comparing with BAODV protocol which the success of [19] method in identifying and deleting the black hole nodes from routing.

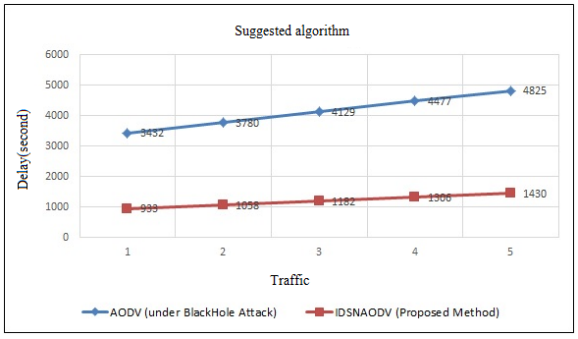

Figure 6: End to end delay in suggested algorithm

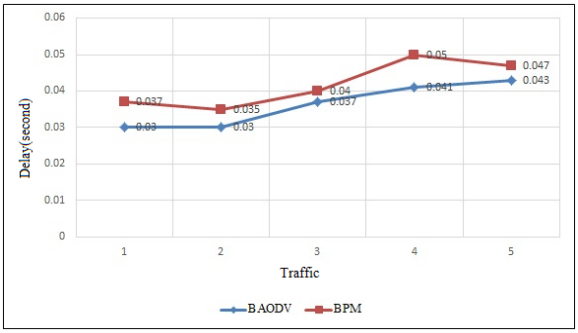

Figure 7: End to end delay in method [19]

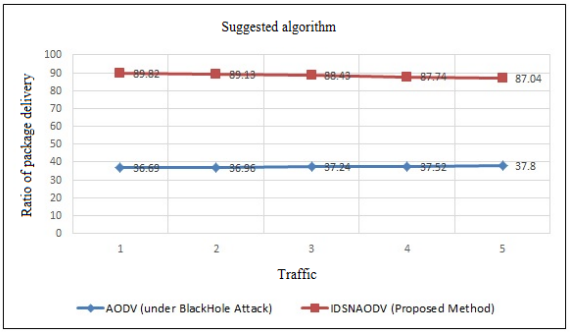

Figure 8: Ratio of packet delivery in suggested algorithm

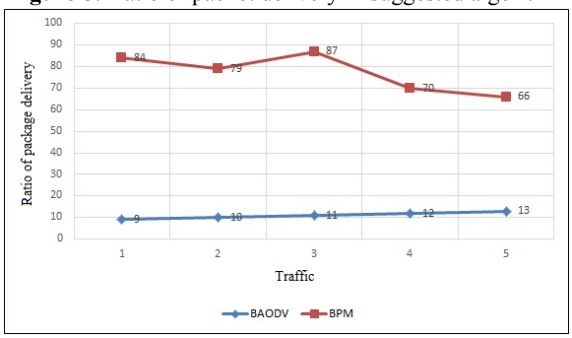

Figure 9: Ratio of packet delivery in method [19]

Conclusion

All of the wireless networks are vulnerable against security attacks, and dealing with them is one of the main challenges for these network's developers. Like the other networks, providing security in Ad hoc networks is one of the important problems in designing these kinds of networks and during the last year, many methods had suggested to solve this problem. Considering the dynamic and variable no true of these networks, data and information security is so important. In this study, at first we studied the influence of black hole attack on suggested algorithm performance and the main version of AODV protocol which is attacked. In the following, suggested algorithm was investigated. The aim of this algorithm is that with considering the node's behavior in the network and identifying the destructive nodes we delete them from routing. Some new rules had applied to identify the destructive nodes. In the following, suggested algorithm performance was evaluated in terms of end to end delay, rate of packets delivery, rate of packet losing and throughput. As it was observed, during the five black holes with 200,400, 800 and 1000 seconds time span of simulation, ratio loss of packets and end to end delay in suggested algorithm declined considerably compared to AODV and also the ratio of packet delivery and through put increased AODV protocol. Generally considering the obtained results, we can say the suggested algorithm performs better than AODV protocol against attacker's nodes. Then we can conclude that a certain algorithm perform better than the others and various conditions should be considered in terms of node's mobility, traffic ratio and type, network size, end to end delay, the rate of packet delivering

References

[1] N.Marchang, R.Datta "Light-Weight trust-based routing protocol for mobile adhoc networks", IET Journals & Magazines, Vol.6, Issue.2, pp-77-83, 2012.

[2] M.Lima, A.dos Santos, G.Pujolle "A Survey of Survivability in Mobile Ad Hoc Networks", IET Journals & Magazines, Vol.11, No.1, pp-66-77, 2009.

[3] Nguyen, Hoang.L. Nguyen, Uyen.T, "A study of different types of attacks on multicast in mobile ad hoc networks", Ad Hoc Networks, Vol.6, pp.32–46, 2008.

[4] Amin Mohebi, Dr. Simon Scott, "A survey on mitigation methods to Black hole Attack on AODV routing protocol", ISSN 2224-610X (Paper) ISSN 2225-0603 (Online), Vol.3, No.9, 2013.

[5] TANYA KOOHPAYEH ARAGHI, MAZDAK ZAMANI, AZIZAH BT ABDUL MANAF, SHAHIDAN M.ABDULLAH, HODA SOLTANIAN BOJNORD, SAGHEB KOHPAYEH ARAGHI, "A Secure Model For Prevention Of Black Hole Attack In Wireless Mobile Ad Hoc Networks", ISBN:978-1-61804-171-5, 2013.

[6] Mahmood Salehi and Hamed Samavati.(2011).Simulation based Comparison of Ad hoc Reactive and Proactive Algorithms Under the Effect of New Routing Attacks.2012 Sixth International Conference on Next Generation Mobile Applications, Services and Technologies.6 (2), p100-105.

[7] Hesiri Weerasinghe, 2011, on Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks Proceedings of the IEEE International Conference on Communications, Jun.24-28.
[8] Anita, E.A.M.and V.Vasudevan, Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining.International Journal of Computer Applications.2010.1 (12):p.22-29.
[9] Latha Tamilselvan, Dr.V Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in AD HOC", JOURNAL OF NETWORKS, VOL.3, NO.5, MAY 2008.
[10] Hesiri Weerasinghe, Huirong Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", International Journal of Software Engineering and Its Applications Vol.2, No.3, July, 2008.
[11] Mehdi Medadian, M.H.Yektaie and A.M Rahmani, Combat with Black Hole Attack in AODV routing protocol in AD HOC, 2009, AH-ICI 2009.First Asian Himalayas International Conference, pp:1-5, 3-5 Nov 2009.
[12]Tassos Dimitriou, Athanassios Giannetsos, "Local black hole detection and prevention in wireless networks", 2010.
[13] M.medadian, KH.Fardad, I.Barazandeh," Discovered and removed a mass black hole attacks on mobile networks Ad Hoc", 1st National Conference on Soft Computing and Information Technology,Iran, Jan 2011.
[14] Vaithiyanathan, S.R.Gracelin, E.N.Edna, S.Radha "A Novel Method for Detection and Elimination of Modification Attack and TTL Attack in NTP Based Routing Algorithm", IEEE Conference, pp-60-64, 2010.
[15] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto, Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method, International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov.2007.
[16] K.S.Dhurandher, M.S.Obaidat, K.Verma, P.Gupta "FACES: Friend-Based Adhoc Routing Using Challenges to Establish Security in AD HOCs Systems", IEEE Journals & Magazines, Vol.5, No.2, pp-176-188, 2011.
[17] N.SHANTHI, DR.LGANESAN, DR.K.RAMAR," STUDY OF DIFFERENT ATTACKS ON MULTICAST MOBILE AD HOC NETWORK", Journal of Theoretical and Applied Information Technology.2005 - 2009 JATIT.
[18] Maryam Forokhi Nematolahi, Faegheh Najafzadeh Moghadam, Marzieh Forokhi Nematolahi, "Using the technology of mobile agents in intrusion detection systems to prevent attacks black hole in the mobile networks", the first National Conference on Computer and Information Technology, 6-1, vocational schools Kerman unit Sama, 1390.[In Persian]
[19] Iman Zanganeh,Mehdi Sadeghzadeh, syed Javad MirAbdini, " A Novel Method for detecting and removing mass black hole attack in AODV protocol in wireless network", First National Conference on Electrical and Computer southern Iran, 8-1, Islamic Azad University Khormoj, Persian date ordibehesht 1392.[in Persian]