Defense Against the Attacks of the Black Hole, Gray Hole and Wormhole in MANETs Based on RTT and PFT

Shahram Behzad, Reza Fotohi, Fathulah Dadgar
Sama technical and vocatinal training colleg, Islamic Azad university, Parsabad moghan, Parsabad, Iran
Sh.behzad173@gmail.com

Department of Computer Engineering, Germi branch, Islamic Azad University, Germi, Iran
Fotohi.reza@gmail.com

Baku State Unıversıty
Dadgar_52@yahoo.com

Abstract

Mobile ad hoc networks are regarded as a group of networks consisted of wireless systems which developing together a network with self-arrangement capability. These networks have no constant communication infrastructure and use central nodes to communicate with other nodes. Despite lots of advantages, these networks face severe security challenges, since their channels are wireless and each node is connected to central node. One of these concerns is the incidence of black hole stacks damaging mobile ad hoc networks routing protocols. Through this process, the Attacker node announces itself as the nearest to destination node; then, network nodes choose it as the central node when transmitting their data packets. As a result, this node can delete its delivered packets rather transmitting. In this paper, for Defense against attacks at the network layer, such as black, gray, hole, wormhole, in Mobil ad hoc network of RTT, PFT test. Simulation results revealed that the proposed method, is compared with DSR and AODV protocol under attack in terms of packet delivery rate, throughput, end to end delay of packets loss and higher efficiency.

Keyword*:* MANETs (Mobile ad hoc networks), DSR (Dynamic Source Routing), Black hole attack, AODV (Ad hoc On-Demand Distance Vector Routing),

I. INTRODUCTION

Mobile Ad Hoc Network is one kind of new wireless network structures. Unlike devices in traditional Wireless LAN solutions, all nodes are movable and the topology of the network is changing dynamically in an Ad Hoc Networks, Similar to other systems, there is a risk of external agent infiltration in the mobile ad hoc networks. These networks are basically no-infrastructure, meaning no routing such as router or switch is used. So, they are highly posed to the risk of various.one the most common attacks in MANET is Black hole attack ,gray hole and worm hole. So, they are highly posed to the risk of damage or exhausting all their common behavior energy. Hence, there is a growing interest towards the methods which can warn the network against the black hole attacks, Gary hole and worm hole attack and external agent infiltration. Routing operation needs collaboration of all nodes to send packets from source node through intermediate nodes to the destination. Hence the, selfish or black hole , gray hole and worm hole behavior of nodes can affect routing and network performance Undesirability. As a result, introducing, evaluating, and analyzing different routing attacks in MANET1s [1] and presenting security mechanisms against them is a challenging field for researchers. Black hole, Gary hole and worm hole attacks is one of the most effective, well-known routing attacks in ad hoc networks. Under

[1] Mobile ad hoc network

such an attack, by misusing routing algorithm packets, attacker node absorbs network traffic and upon receiving packets, instead of forwarding, discards them silently K. (Biswas et al 2007). Black hole attack is investigated, and evaluated in different previous works. However, what is simulated or implemented so far does not represent its most negative effect on dropping data packets. In most of related works (Pegueno et al 2006) (LU et al 2009) absorbing network traffic through malicious node, has been performed using false RREPs[2] in response to received RREQs[3]. The mobile ad hoc networks are not having the fixed network topology due to the reason that mobile nodes are frequently changing their positions and movement. Network topology for the MANET networks is not fixed because of the frequent nodes movement in the network. Mobile ad hoc networks having different types of routing protocols like reactive, hybrid, and proactive protocols type of routing protocols. We can use these protocols with different network scenarios and mobility patterns. The reactive protocols such as DSR4 protocol and AODV5,protocol are frequently used MANET protocols (Refari et al 2005). In this paper, We choose DSR and AODV as a sample example, because it is one of the protocols being considered for standardization for mobile ad hoc networks. There are other routing protocols, and there are parts of mobile ad hoc networks other than routing that need detection black hole attacks , for example medium Achieve control protocols. We believe the main elements of our method would also apply there, but a detailed analysis is for further work. Our emphasis in this paper is Defense Against Black hole, Gary hole and worm hole Attacks in Mobile Ad hoc Networks. For Defense against attacks at the network layer, such as black, gray, hole, wormhole, in Mobil ad hoc network of RTT[4], PFT[5] test. The rest of the paper is organized as follows. Section 2 Related works. Section 3 describes the AODV routing protocol. In section 4 Dynamic source routing (DSR) and its vulnerabilities . Section 5 Attacks in Mobil ad hoc network. Section 6 The Proposed Method against the attacks of the black hole, Gray hole, wormhole. Section 7 Experimental Data and analysis. Finally section 8 concluding .

II. RELATED WORK

MANET is very much popular due to the fact that these networks are dynamic, infrastructure less and scalable. Despite the fact of popularity of MANET, these networks are very much exposed to attacks (Refari et al 2005). Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication (Lu .Li et al 2009). Different kinds of attacks have been analyzed in MANET and their effect on the network. Attack such as gray hole , worm hole, black hole , where the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior (Biswas et al 2007). MANETs routing protocols are also being exploited by the attackers in the form of flooding attack, which is done by the attacker either by using RREQ or data flooding (Marti et al 2005). Design and presentation of different security obstacles and attacks in mobile ad hoc networks as well as finding appropriate solutions against them is a challenging research area for researchers. Black hole attack is one of the famous related attacks. In (Rafaei et al 2005). black hole attack is evaluated in DSR based networks and a solution is proposed to mitigate it, as well. In such papers, fake routes are only suggested in response to RREQ packets. In (Bhalaji et al 2009). and (Palanisamy et al 2010). Black hole attack is assessed in DSR based networks and in (Zhou et al 2010). The method (Bala et al 2009).provides a data learning scheme to detect a black hole attacker. In this scheme, every node has knowledge of the current value of SN by the exchange of route messages such as RREQ and RREP. If a node receives a RREP message with a SN that is much larger than a threshold plus the current SN value, this node will believe that the RREP message is generated by a malicious node. Obviously, this method depends on the value of the threshold and may lead to a high rate of misjudgment. A Bali Proposes a trust based approach (Stoshi et al 2007). using AODV (Bhalaji et al 2011). protocol. But they do not consider the data packets. Instead they

[2] Route Replay
[3] Rout Request
[4] Round Trip Time
[5] Packet Forwarding Table

consider only control packets like RREQ, RRER and RREP and network layer acknowledgement. A black hole can even drop data packets by perfectly transmitting control packets. There the system fails by thinking there is no black hole as the control packets are transmitted without any delay or drop. Many approaches to detect the black hole attack and to defend the MANET from the attack have been proposed (Reza fotohi and shahram behzad et al 2013) (Dang et al 2002). According to the algorithm by Deng et al. (Rubin et al 2002). every node crosses check with its next hop node on the route to the destination on receiving or overhearing a RREP packet. If the next hop node does not have a link to the node that sent the RREP, then the node that sent the RREP is considered as malicious. This solution assumes that there exists at most one malicious node and thus cannot cover the case with two or more malicious nodes, which is quite possible in real situations. An algorithm presented in (Latha et al 2007). claims to detect the black hole attack in a MANET which is based on relationships of a certam trust level among the nodes. However, in the real network, it is very difficult to set an appropriate value for the trust level. In the method (Mohammad et al 2004). every node has a function of learning the traffic flow in the network and evaluating the possibility criterion of black hole attack based on such learning results in order to detect the malicious node. If the value of the criterion is larger than a predetermined threshold, the node judges that there exists a black hole attacker. This method only provides detection of a single black hole attacker and cannot detect a chain of malicious nodes which cooperate with each other. TAODV (Trusted et al 2003). is another protocol based on trust which calculates it on the basis of others opinion. This method uses two additional special messages: (TREQ[6]) and (TREP[7]) and adds addition 3 new fields to the routing table for calculating the trustworthiness of nodes. TAODV use digital signature which is an additional overhead. Opinion of other nodes cannot be trusted as it can also be from malicious nodes itself. This is an extension of basic AODV protocol

III. DESCRIBES THE AODV ROUTING PROTOCOL

The Ad Hoc On-Demand Distance Vector (AODV[8]) routing protocol is an adaptation of the DSDV protocol for dynamic link conditions (Perkins et al 2000). (Charles et al 2003). Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route Request) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route

[6] Trust Request
[7] Trust Reply
[8] Ad Hoc On-Demand Distance Vector

Error) packet to all other nodes that uses this link for their communication to other nodes. This is illustrated in figure 1 and 2.

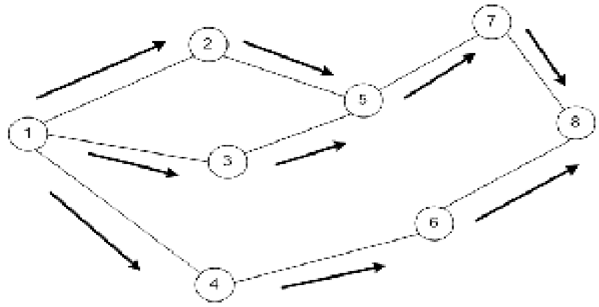


Figure. 1. Broadcast to AODV route discovery

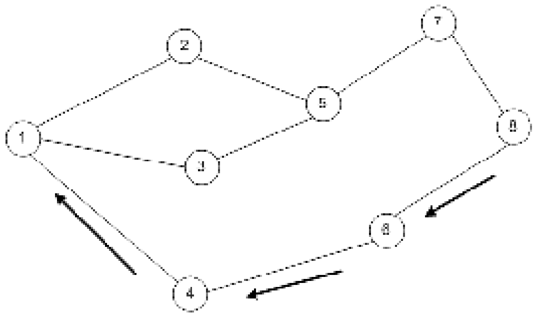


Figure. 2. A sample of route discovery in AODV protocol

IV. DYNAMIC SOURCE ROUTING (DSR) AND ITS VULNERABILITIES

DSR[9] protocol is a reactive routing algorithm designed for mobile Ad hoc network. The process of routing in DSR is composed of two main phases known as route discovery and route maintenance. Routing in DSR3 is completely carried out in an on-demand method (Johnson et al 2007). Route discovery phase is a process under which source node, in order to send data packets, obtains a valid route to the destination node. For this, source node creates a RREQ packet and relays it in the network. Such a packet will be received by all of the sources neighbor nodes. Each RREQ packet contains an identifier and a list of addresses of intermediate nodes which this packet has passed from them. Such a list is initially empty at the time of creating RREQ by the source node. When a node receives a RREQ packet, creates a RREP regarding information included in the list of addresses inside the packet and sends it back to the source node if only it be the destination node itself or have had a route to the destination. Once source node receives such a RREP packet, it first adds this route to its route cache and then starts to send data packets using the route included in the packet. If the receiver of RREQ has not had a route the destination and has not previously received this RREQ packet, appends its address to the list of nodes inside the packet and rebroadcasts that. When the destination node receives a RREQ4, it can create and send back the RREP to the source node using the route which can be computed by inversing the list of addresses inside the RREQ packet. Route maintenance is a mechanism by which, as source node is using a route to send its data packets, can discover changes of topology and send remainder of its packets through an alternative route if it be convinced that the current route has been broken and not usable anymore (Johnson et al 2007).

[9] Dynamic Source Routing

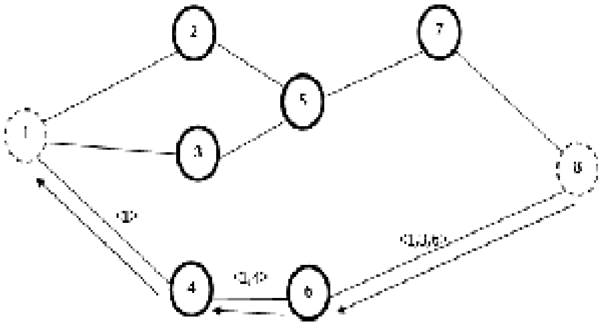


Figure. 3. depicts a discovery route in DSR protocol. (All-over distribution)

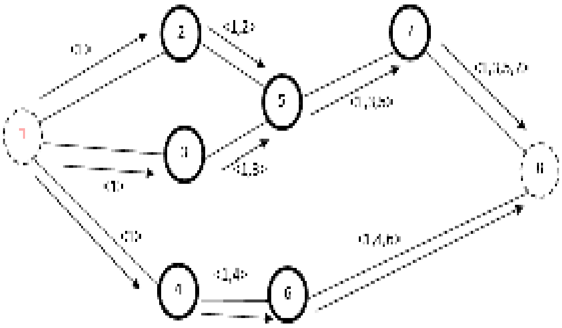


Figure. 3-1. A sample of route discovery in DSR protocol

V. ATTACKS IN MOBIL AD HOC NETWORK

Attacks in mobile ad hoc networks can be in terms of performance In the network layer, which in this section is a brief description of the three Attack on black holes, worm holes, gray hole that most attacks In mobile ad hoc networks is discussed.

5.1 BLACK HOL ATTACK

black hole attack, a malicious node uses its routing protocol in order to With the release of false news, having the shortest path to the destination node or to the packet it wants to avoid the. This black hole node advertises its availability of fresh routes irrespective of checking its routing table. in the attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it (Biswas et al 2007). In protocol based on flooding, the black hole node reply will be received by the requesting node before the reception of reply from actual node; hence a black hole and forged route is created. When this route is establish, now it’s up to the node whether to drop all the packets or forward it to the unknown address (Pegueno et al 2006). (1) The Solution how black hole node Proportional in the data routes varies. Fig. 4 shows how black hole Problems, here node “E” want to send data packets to destination node “D” and The initial process of route discovery. So if node “F” is a black hole node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node “E” before any other node. In this way node “E” will think that this is the active route and thus active route discovery is complete. Node “E” will ignore all other replies and will start seeding data packets to node “F”. In this way all the data packet will be lost consumed or lost.

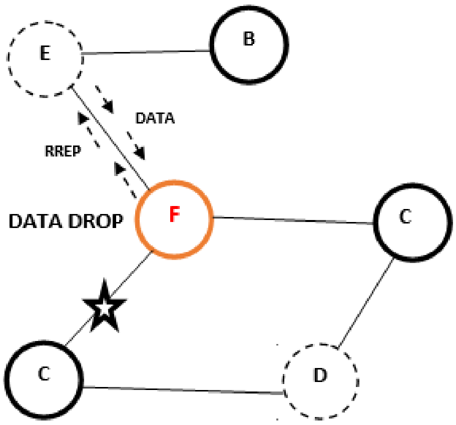


Figure. 4. Problems of black hole attacks

5.2 WORM HOLE ATTACK

wormhole attack which is considered as a severe attack in mobile ad hoc network. Minimum two malicious nodes are required to perform this attack; more than two malicious nodes are also used to perform this attack. In this attack the two malicious nodes resides in the two ends of the network and they form a link between them using an out-of-band hidden channel like wired link, packet encapsulation or high power radio transmission range (Azer et al 2008). After they form a tunnel between them as shown in figure 1, whenever a malicious node receives packets it tunnels them to the other malicious node and in turn it broadcasts the packet there. Since the packet is travelling through the tunnel it reaches the destination speeder than other route and moreover the hop count through this path is going to be less so this path is established between the source and the destination (Reshmi et al 2010). Once the path is established between the source and the destination through wormhole link they can misbehave in many ways in the network like continuously dropping the packets, selective dropping the packets, analyzing the traffic and performing Denial of Service attack. Figure 5 shows an example of this attack.

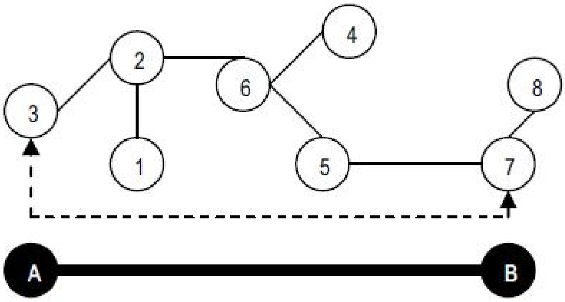


Figure. 5. An example of a wormhole attacks

5.3 GRAY HOLE ATTACK

We now explain the gray hole attack on MANETs. The gray hole attack has two stages. In the first stage, an attacker exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second stage, the node drops the intercepted packets with a certain probability. This attack is harder to detect than the black hole attack where the attacker drops the received data packets with certainly. A gray hole may display its attacker behavior in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A gray hole may also display a behavior which is a combination of the above two, thereby making its detection even more difficult (Pradip et al 2010).

VI. THE PROPOSED METHOD AGAINST THE ATTACKS OF THE BLACK HOLE, GRAY HOLE, VORMHOLE

In this Paper we represent a new way called the protection of navigational protocol in occasional portable networks against black holes, silver holes and worm holes which is consisted of two phases, RTA & Packet forwarding table as it follows. The proposed method not only specifies forged ways but also it adopts prevention criteria against reborn of destructive attacks in the process of route detection phase.

6.1 The First phase: calculating the distance between the inception and destination with RTT

This mechanism which is based on the time and table is used for specifying attacks concerning black holes, silver holes and worm holes, regarding in navigational protocol in the occasional networks, destructive loop always respond to rout reply as quickly as possible and because of this fact that operative loops or the inception doesn't have any valid information about its distance from the destination, they are deceived rapidly by response of these loops, so for preventing from happening this, we must calculate the total round-trip time for all ways available, between the inception and the destination loop until the actual distance between the inception and destination loop is determined and we can make an accurate decision for transmitting information.

A. Calculating round-trip time or RTT:

Round-trip time; middle interval; can be calculated when the inception loop retransmitted "HELLO" message and the moment the response message for "Hello" is received, meaning it has been informed of the neighbors existence. Each individual loop reserves mono-step round-trip time between itself and its neighbors. Aggressor detection mechanism: A typical loop which have a data for transmitting, should at first detect necessary route toward the destination and after that start transmitting data using that route. This method is exclusively used in specifying safe route.

B. Aggressor detection mechanism:

A typical loop which have a data for transmitting, should at first detect necessary route toward the destination and after that start transmitting data using that route. This method is exclusively used in specifying safe route.
In order to do this, the data transmitting loop perform the following mathematics:

1: For each available or detected route, its RTT is calculated from the inception to destination.

2: Then the total amounts RTT for all discovered routes is calculated.

3: Calculating the RTT's average for all discovered routes using the previously mentioned amounts.
4: Now between all available routes, we choose a route that its RTT has a bigger differentiation, in relation to average RTT amount and utilizing that safe route, we send data toward the destination. According to equation (1)

$$\text{Sending time} = \text{value of receive timestamp} - \text{value of original timestamp} \qquad (1)$$

Equation (1) specifies transmitting time course which in fact is a timestamp, representing the differentiation between receiving timestamp with transmitting timestamp.

$$\text{Receiving time} = \text{time the packet returned} - \text{value of transmit timestamp} \qquad (2)$$

Equation (2) specifies receiving time course which in fact is a timestamp, representing the differentiation between transmitting timestamp and receiving timestamp.

Combining equation (1 & 2):

$$\text{Round-trip time} = \text{Sending time} + \text{Receiving time} \qquad (3)$$

In equation (3) we can see round-trip time or RTT. In fact the total time is the sum of receiving time and sending time.As a result when the RTT is calculated for all routs between the inception and destination, the inception loop can easily make an accurate decision regarding its distance from destination and prevents from wrong information, constructed by wormhole loops. Therefore by applying points which have been mentioned previously, we specify the destructive loops and wipe them out from circuit.

6.2 Second Phase: prevention of black holes, silver holes and worm holes incidence, between the inception and destination with the usage of packet forwarding table.

In this Paper we have proposed a new secure method for the detection of loops in black holes, silver holes and worm holes. The way it works is that each loop reserves packet forwarding table for the specification of attacks.We have added a next hop field in the structure of route response packet or RREP. the information of Next step is collected from the route response packet. In our method, before sending data packet, the first arrived packet with the shortest sending route has been revised using middle loop. Availability of the route is revised using the next hop loop from the middle loop toward the destination loop. In the case which no other route exists, the middle loop is determined as destructive loop. Besides the specification of other adverse operations conducted by the misbehave loop in the network, each loop holds a table for the specification of the destructive loop identity (MIT) from the neighboring loop with the purpose of protecting against tracking down receiving, sending and changed packets. The field of this table includes < inception, destination, current loop ID, receiving packets (PR), sending packets (PF) and modified packets (PM). Each loop for the specification purpose of the destructive loop collects information, concerning identity specification table from its neighbors. Initially the counting amount is set to the zero. (PR=PF=PM=0). On the condition the loop successfully receives, sends or changes the packet, the amount of concerned counter will increase one unit. If a loop several times had received the packet triumphantly, but it had not send the packet to its adjacent loops, by this chance it means, that certain loop is considered as a destructive loop. Each loop has buffer memory for temporarily capturing the packet’s contents. While loop A sends the packet to the next packet B, the loop A copies the packet’s contents and oversees the behavior in the adjacent loops of B. sending packet using loop B is compared with buffer memory’s contents of loop A. In the case of any kind of deviation, the PM’s value would get bigger, fair one unit. The following procedure is being used for the detection of adverse operations using the destructive loop.

```
1: For each discovered route calculate RTT between source and destination node.
2: Sum RTT all discovered routes step 1.
3: Avg = Sum / all discovered routes.
4: RTT(route i) - Avg(route)
5: Select the routes that have difference less.
6: Data packet forwarded from selected route in step 5.
7: For each node If   (PR – PF) = 0, there is no packet dropping.
8: Else if
9:          PD   = (PR – PF) > 0, or (PR-PF) < 0, then
10:          there is packet dropping (PD)
11 If  PD > PREDETERMINED_THESHOLD_VALUE, then
12:          the particular node is identified as malicious.
13: If       PM > 0, then
14:          the particular node is identified as malicious.
15:END
```

Figure. 6. Algorithm for the proposed method

If (PR – PF) = 0, no packets have been removed. Or if PD = (PR – PF)>0 and or (PR – PF) <0, then the packet has been removed and we would have (PD).If the specified threshold value < PD, then that certain loop is considered as a destructive loop. If PM>0, then that certain loop is considered as a destructive loop. In this method, those black hole, silver hole and wormhole attacks which have removed or changed the packet are effectively determinable. The second part of this plan concerns separation of the loop for black hole, silver hole and wormhole from the network and improvement of the network. Each loop has either a separation table or it is isolated in which the loop's ID for black hole, silver hole and wormhole is recorded. After that, the ID is broadcasted to the entire network's loops. When the destructive loop, for the second time, with the goal of attracting cooperation, enters to the network, with revising it by the separation table it would be removed.

VII. EXPERMENTAL DATA AND ANALYSIS

This section includes simulation and evaluation of Accurate Black hole attack. NS-2 simulation software is used. In scenarios The proposed method is compared with AODV and DSR under attack The number of nodes in the network 100 and the number of nodes or malicious attacker 4,8,16,32 and 64 is considered. Environmental simulation, 1000*1000, In the simulation of traffic flow We use CBR. In the graphs, the results for performance evaluation protocol AODV and DSR routing under attack by attacking the proposed approach Increase the number of attackers from 4 to 64 and the criteria in terms of packet delivery rate, Throughput, end-to-end delay and packet loss rate were compared.

Table. I
SIMULATION PARAMETRS

Simulator	NS2.35
Area	1000m X1000m
Number OF Mobile Node	100
Routing Protocol	(DSR , AODV)
Transmission Range	250m
Antenna	Omni Antenna
Simulation duration	100,120,140,160,180,200
MAC Layer	802_11
Traffic Type	CBR
Buffer Size	50 Packet
Node placement	Random
Attacker node	4,8,16,32, And 64node

The following performance metrics has been analyzed. Packet delivered ratio. Packet loos, average end to end delay. throughput, and the number of drop packets have been regarded as network parameters.

A. Packet delivery ratio(%)

PDR is the number of packages that are delivered to the destination from the source, divided by the total number of packages in the network. This parameter is also called as success rate of the protocols:

PDR = (Number of Send Packet / Number of recited Packet)* 100

Where PDR is the package delivery rate, Send Packet No is the number of sent packages, and Receive Packet No denotes the number of received packages.

B. Packet loos(%)

Packet loss can be caused by a number of factors including attacker over the network medium due to multi-path fading, packet drop because of channel congestion, corrupted packets rejected in-transit, faulty networking hardware, faulty network drivers, or normal routing routines (among DSR in mobile ad hoc networks),Packet loss can be caused by the black hole attack

C. Throughput

a network can be measured by using the different tools that are available on the different operating systems. This page explains the theory, on which the adjustments of these tools for measurements are based, and the issues related to these measurements. The reason for measurement of the throughput in networks is that, the people often intend to know about the maximum operational power of data in a connection link or network access as expressed by the unit of bit per second. The measurement of this quantity is commonly carried out by transmitting a large size file from one system to another and calculating the required time for complete transmitting or copy of the file. Then, with dividing the file size by that time, the throughput will be achieved in unit of megabit per second, kilobit per second or bit per second. The following formula shows how to calculate the throughput.

Figure 7 shows the number of attackers against throughput. The proposed method is compared with AODV and DSR routing protocol throughput under attack better. When the number of attacks, the throughput of AODV and DSR under attack is much reduced the throughput of the proposed method is slight decrease.

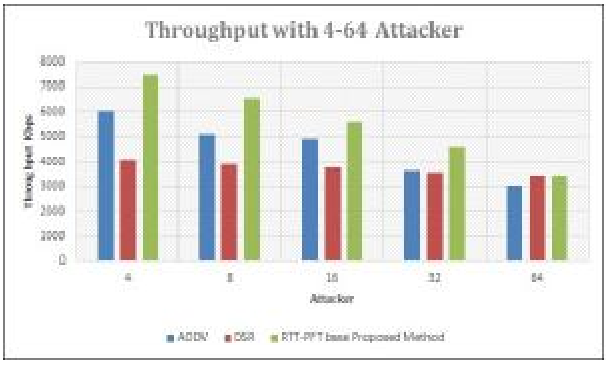


Figure. 7. Throughput In front the number of attackers.

Figure 8 shows assailants in front of the end to end delay. The proposed method is compared with AODV and DSR routing protocol under attack delay is less. Less because of the delay of the proposed method is rapid identification of malicious attackers and to discard they from the cycle of activity on the network.

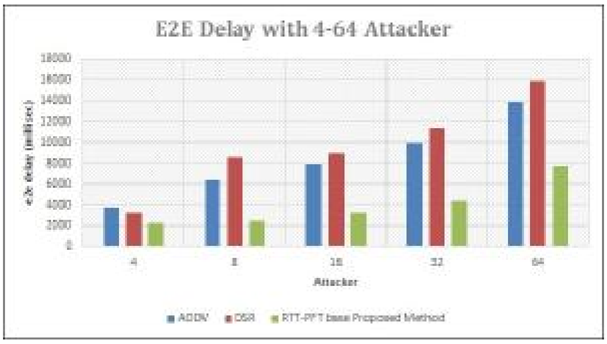


Figure. 8. End to End delay In front the number of attackers

Figure 8 shows the number of attackers in front of the packet delivery rate. The proposed method is compared with AODV and DSR routing protocol packet delivery rate under further attack. When the number of attacks, the packet delivery rate is much lower than AODV and DSR under attack. But the changes in the proposed method is better than good.

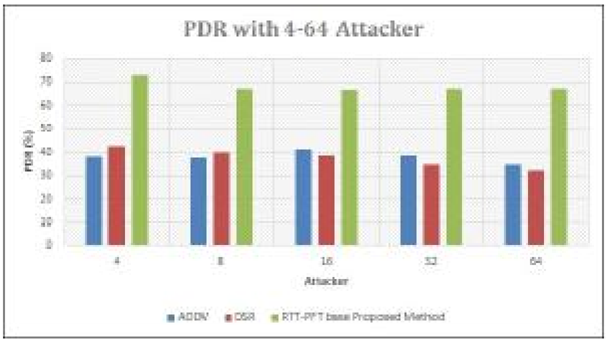


Figure.9. Packet Delivery Ratio In front the number of attackers

Figure 10 shows attackers against packet loss rate. Packet loss rate of the proposed method of routing protocols AODV and DSR under attack less. When the number of attacks, the packet loss rate in AODV and DSR under attack much more. But the changes in the proposed method is less.

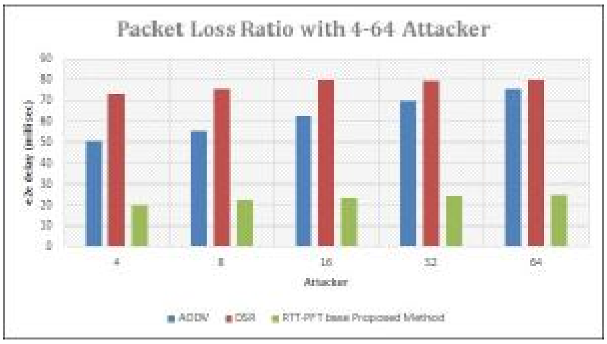


Figure. 10. Packet loss Ratio In front the number of attackers

VIII. CONCLUDING

This paper proposed two techniques namely RTT analysis and PFT based method for detecting and preventing gray hole, wormhole and black hole attacks respectively. To evaluate the performance of proposed techniques, simulation of gray hole, wormhole and black hole attacks along with the simulation of proposed techniques had been done. Simulation of security strategies provides the facility to select a good security solution for routing protocols and gives the knowledge how to use these schemes in hostile and compromised environments. Simulation results show that as the number of nodes increases in the network, the performance of these strategies improves. Nodes mobility affects the performance of routing protocols most. According to simulation results the proposed techniques show superior performance as PDR and throughput increases however, average end-to-end delay and packet loss also decreases. In the analyzed scenario, it is found that the proposed technique has superior performance than AODV and DSR is suitable to detect and prevent black hole, gray hole and wormhole attacks. It improves the PDR under attack conditions, with a minimal decrease in throughput and acceptable increase in end-to-end delay. In this simulation study, it has also been investigated that, proposed method is appropriate to detect and prevent black hole attack. It has high PDR and throughput that makes it suitable for networks prone to black hole attack. It provides these advantages with low end-to-end delay.

References

i. K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007

ii. G. A. Pegueno and J. R. Rivera, “Extension to MAC 802.11 for performance Improvement in MANET”, Karlstads University, Sweden, December 2006

iii. S. Lu, L. Li, K.Y. Lam, L. Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.,” International Conference on Computational Intelligence and Security, 2009.

iv. M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, “A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks,” Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

v. S. Lu, L. Li, K.Y. Lam, L. Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.,” International Conference on Computational Intelligence and Security, 2009.

vi. K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007

vii. S.Marti, T.J.Giuli, K.Lai, M.Baker, “Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks”.

viii. M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, “A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks,” Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

ix. N.Bhalaji, Dr.A.Shanmugam, "Association between nodes to combat blackhole attack in DSR based MANEr", Proc. Int. IFIP Conf. on Wireless and Optical Communications Networks, WOCN '09, India, pp. 1-5,2009.

x. V. Palanisamy, P. Annadurai, S.Vijayalakshmi ,"Impact of Black hole Attack on Multicast in Ad hoc Network (IBAMA)", Proc. In!. IEEE Conf. on Computational Intelligence and Computing Research (ICCIC), India, pp. 1-4,2010.

xi. J. CAl, P. YI, Y. TIAN, Y. ZHOU, N. LIU, "The Simulation and Comparison of Routing Attacks on DSR Protocol", Proc. Int. Conf. on Wireless Communications, Networking and Mobile Computing, WiCom '09, China, pp. 1-4,2009.

xii. A. Bala, M. Bansal, J. Singh,"Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, India, pI41-146, 2009.

xiii. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto: "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Network by Dynamic Learning Method", International Journal of Network Security, Vo1.5, PP.33S-346, (November, 2007)

xiv. N. Bhalaji, A. Shanmugam, “A Trust Based Model to Mitigate Black Hole Attacks in DSR Based Manet”, European Journal of Scientific Research, ISSN 1450-216X Vol.50 No.1,2011

xv. Reza Fotohi, Shahram Jamali, Fateme Sarkohaki, Shahram Behzad,"An Improvement over AODV Routing Protocol by Limiting Visited Hop Count", IJITCS, vol.5, no.9, pp.87-93, 2013. DOI: 10.5815/ijitcs.2013.09.09

xvi. H. Deng, W. Li, and D. P. Agrawal: "Routing security in wireless ad hoc network". IEEE Communications Magazine, pages 70- 75, (2002)

xvii. I. Rubin, A. Behzad, R. Zhang, H, Luo, and E. Caballero, Tbone: "A mobile-backbone protocol for ad hoc wireless networks" , In Proceedings of IEEE Aerospace Conference, volume 6, pages 2727-2740, (2002)

xviii. Latha Tamilselvan, V. Sankaranarayanan: "Prevention of Black Hole Attack in MANEr", The 2nd international conference on wireless, Broadband and Ultra Wideband Communications (January 2007)

xix. Mohanmmad AI-Shurrnan et al: "Black Hole Attack in Mobile Ad Hoc Network", ACMSE' 04, (April 2004)

xx. A Trusted AODV Routing Protocol for Mobile Ad Hoc Networks. PhD thesis, Department of Computer Science and Engineering, The Chinese University of Hong Kong, 2003

xxi. C.E. Perkins, S.R. Das, and E. Royer, "Ad-Hoc on Demand Distance Vector (AODV)", March 2000, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv- 05.txt

xxii. Charles E. Perkins, Elizabeth M. Belding-Royer, Samir R. Das, Mobile Ad Hoc Networking Working Group, Internet Draft, 17 February 2003.

xxiii. D.Johnson, Y. Hu, and D. Maltz, The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, RFC 4728, 2007.

xxiv. K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007

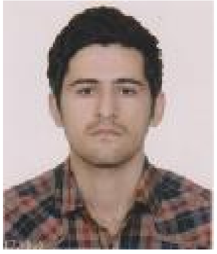
xxv. G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006

xxvi. Azer, M.A., El-Kassas S.M., Hassan, A.W.F., El-Soudani M.S., "Intrusion Detection for Wormhole Attacks in Ad hoc Networks a Survey and a proposed Decentralized Scheme Marianne " IEEE Third International conference on Availability, Reliability and Security, 2008.

xxvii. Reshmi Maulik, Nabendu Chaki "A comprehensive review on wormhole attacks in MANET" International Conference on Computer Information Systems and Industrail Management Applications(CISIM) 2010.

xxviii. Pradip M, Jawandhiy A, "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, vol. 2 no. 9, 2010, pp. 4063-4071.

Authors' Profiles



Shahram Behzad received his B.Sc. in computer engineering from Parsabad University, Parsabad, Iran, in 2008 and his M.Sc. in computer engineering from Azad university of Shabestar branch, Tabriz, Iran, in 2013. His research interests Mobile Ad-Hoc Networks, Performance Evaluation and Optimization algorithms.

Fathulah Dadgar Arablow: Ph.D. Student of computer science in Baku University, interested in multi-media and web mining, mobil ad hoc network and security, Distributed Systems.

Reza Fotohi received his B.Sc. in computer engineering from Shabestar University of Applied Science And Technology, Tabriz, Iran, in 2009, and his M.Sc. in Computer Engineering from Islamic Azad University, Shabestar branch, Tabriz, Iran, in 2013. His research interests include wireless networks, mobile computing and combinatorial optimization.