Injection and Evaluation of New Attacks on Ad hoc Proactive Routing Algorithms

Mahmood Salehi, Hamed Samavati
Sama Technical and Vocational Training College, Islamic Azad University, Karaj Branch
Karaj, Iran

Abstract

Providing security of communications in Mobile Ad hoc Networks (MANETs) is one of the most significant fields for researchers. In order to provide security, the first step is to recognize vulnerabilities and examine different implementable attacks regarding such networks. Secure routing is one of the most important security blind spots regarding MANETs. Security of routing in MANETs can be endangered by uncooperative behavior of nodes. Uncooperative behavior can be done selfishly by refraining from participation in routing or maliciously in the form of an attack against network. One of the most famous and devastating routing attacks regarding MANETs is Black hole. In Optimized Link State Routing (OLSR), as one of the most well-known proactive routing algorithms, Black hole attack can be implemented in different methods. In this paper, effects of different selfish behaviors and different implementations of Black hole on OLSR based MANETs is studied. In order to evaluate network parameters, network simulator (NS-2) tool has been used. Simulation results demonstrate that a special implementation of Black hole, compared to other implementations and selfish nodes, has had more destroying effects on the network. Furthermore, such an attack results in a reduction in routing overhead and delay in transmitting packets compared to basic OLSR.

Keywords-Mobile Ad hoc Network; Black hole Attack; Selfish Node; OLSR

1. Introduction

Mobile ad hoc networks are a subset of wireless networks having no fixed infrastructure. Various applications as well as low establishment costs has led to performing a large amount of research in different challenging problems of such networks. MANET is a set of wireless mobile nodes in which each node would be able to send and receive network packets with regard to its limited transmission range. In order to exchange information with the world outside of its transmission range, network nodes need collaboration of other nodes to route and forward packets to their destinations in a multi-hop manner [1]. Lack of centralized control system and limited battery power necessitates routing algorithms of MANETs to operate with distributed behavior and divide routing overhead among all network nodes. Routing algorithms of MANETs can be classified into two main categories named proactive and reactive methods. In reactive or on-demand routing protocols, source node first tends to discover a route to the destination node before sending its data packets. After route discovery phase, source node sends its data packets through one of the obtained routes to the destination. In proactive or table-driven algorithms, on the other hand, each node maintains tables containing latest information regarding current network topology. Such tables are updated periodically and, as a result, at the time of sending data packets, there is no need performing route discovery operations.

In both proactive and reactive algorithms, routing needs collaboration of all nodes to send packets to their destinations and routing quality depends on the amount of cooperation of all network nodes. One aspect of cooperation is forwarding source node's generated data packets through intermediate nodes to the destination node. Therefore, selfish or malicious behavior of nodes can adversely affect routing and network performance. Consequently, with regard to their innate features, MANETs are always susceptible to different routing attacks through attacker nodes. Hence, introducing, evaluating, and analyzing different routing attacks in MANETs and presenting security mechanisms against them is a challenging field for researchers.

OLSR is one of the most famous proactive routing algorithms which reduces network overhead dramatically by restricting diffusion of control packets across the network. OLSR's functionality is highly bound with the transmission of HELLO and Topology Control (TC) messages. Such messages are periodically diffused in the network by all nodes and allow recipient nodes to update their related tables using related information. Consequently, information content of HELLO and TC messages forms the basic operation of OLSR protocol [6].

Black hole is one of the most effective, well-known, and devastating routing attacks in ad hoc networks. Under such an attack, with regard to routing algorithm behavior and by misusing routing packets, attacker node tries to situate itself in different routes of data packets. On the other hand, it proceeds to absorb network traffic towards itself. Afterwards, upon receiving packets, instead of forwarding, discards them silently [2].

Black hole attack can be implemented in different forms in OLSR based MANETs; therefore, analysis of the effects of such an attack has remained as a challenging area of study.

The purpose of this paper is to evaluate, simulate and compare different Black hole attack implementations and introduce the most effective one which is considered in this paper for the first time.

In the second section of paper, related works are presented. After that, section 3 consists of an overview of OLSR protocol. OLSR routing attacks are explained in section 4. Simulation, evaluation, and analysis of the effects of attacks in an OLSR based MANET can be found in section 5. Conclusion is added in 6th section. Sections 7 and 8 include references and acknowledgement, respectively.

2. Related works

Black hole attack has been studied and evaluated in different related works. However, operation of this attack regarding fake routes advertisement in reactive protocols differs from proactive ones and, as a result, effects of that on network parameters are different, as well. In most of related works in case of reactive routing algorithms [3], [4] traffic absorption has been performed by Black hole nodes through sending unreal Route Reply packets in response to received Route Request packets. In our previous paper [5], we introduced a more destroying Black hole attack which suggests fake routes not only in response to received Route Request packets, but also using overheard Route Reply packets. Traffic attraction of Black hole in proactive routing algorithms, however, is done through manipulating routing control packets before propagating them. Black hole nodes in an OLSR based network, in order to absorb and silently discard network data packets, advertise false information by modifying each of the HELLO or TC packets or both of them simultaneously [7].

Different OLSR routing attacks have been designed and studied in different related papers. Node isolation attack and a method of its prevention has been introduced in [8]. Malicious nodes collusion attack and a countermeasure against that has been studied in [9] and [10]. In [11], [12], and [13] a definition of different attacks against MANETs and a description of their operation has been explained. In [7], different Black hole attacks in OLSR have been introduced; however, evaluation of Black hole has been considered only based on modification of HELLO messages. In [14], a solution to nullify and isolate Black hole nodes in MANETs has been suggested. In different related works regarding implementation of Black hole attack in OLSR, such an attack has been considered only based upon manipulating HELLO messages and other implementations have not been studied yet.

In this paper, different aspects of selfish behavior of nodes and Black hole nodes in an OLSR based MANET have been studied and evaluated. Implementation of false route advertisement through Black hole nodes has been simulated using NS2 based on modification of HELLO, TC, and combination of both HELLO and TC messages. The goal of this paper is to examine and assess effects of a malicious or selfish node in a MANET with proactive routing algorithm like OLSR. In our previous work [5], such an evaluation has been done for a MANET with reactive routing algorithm.

3. An overview of OLSR

OLSR protocol is a proactive routing algorithm related to ad hoc networks. OLSR routing process depends on sending periodic control messages to maintain latest network topology information [6].

OLSR is an optimized routing protocol which reduces propagation of control packets using the concept of multipoint relay (MPR) nodes. In order to decrease routing overhead, each node in the network selects a subset of its neighbors as its MPRs. MPR node is responsible to rebroadcast control packets of nodes which have just selected this node as their MPR. Other Non-MPR neighbor nodes receive and process packets; however, they do not relay them. A key point in selecting MPR nodes is that the set of MPR nodes for each individual node, which is composed amongst level-1 neighbors of that node, should be elected on condition that they cover all of the level-2 neighbors of that node. Furthermore, the smaller MPR set of a node, the higher performance of the routing protocol. The reason is that, as the number of MPR nodes of an individual node becomes smaller, the number of rebroadcasts of control packets for that node will decrease, as well [6]. Fig. 1 represents the role of MPR nodes in reducing routing overhead of the network.

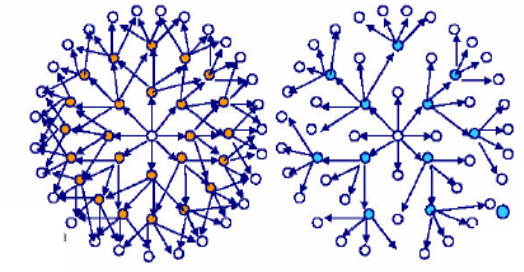

Figure 1. The role of MPR nodes in OLSR

In the left side image, it is observed that after propagation of a control message by a network node, all of the receiving neighbors rebroadcast this packet which results in an increase in routing overhead. However, in the right side image, which represents operation of OLSR protocol, only a subset of neighbor nodes, the MPR set of that node, rebroadcast control packets. It is remarkable that MPR set nodes are level-1 neighbors which cover all level-2 neighbors.

As mentioned before, OLSR contains two kinds of control messages named HELLO and TC messages. Such messages are periodically transmitted in the network. Each node contains a table including information about its current neighbors and HELLO messages are created using such information. By means of sending HELLO messages, each node propagates information regarding its neighbors and the state of link between itself and its neighbors. Upon reception of HELLO messages, other nodes can derive information concerning their level-1 and level-2 neighbors and they can also tend to select their MPR set. Furthermore, through receiving a HELLO message, nodes can create or update their MPR Selector list. MPR Selector list demonstrates nodes which have currently selected this node as their MPR. Upon

creation of such an important list, nodes start to send TC messages in the network. HELLO messages are processed by neighbor nodes; they are never relayed by them, however. TC messages actually contain the list of MPR Selectors of a node and each entry of this list represents existence of a link from this node, which has been selected as MPR and has sent TC message, to the MPR Selector node. Other nodes, which contain a table named topology table, after receiving a TC message, update their topology table with information of this TC message and propagate it on condition that they have been selected as MPR node for the sender of TC message. Therefore, all of the neighbor nodes receive and process TC messages; however, among them, just MPR nodes relay such messages. Finally, each node, with regard to information of its topology table, would be able to extract current detectable routes of current network topology. Nodes store such routes in an individual table called Routing Table. At the time of sending data packets to a destination node, each node uses routes of its routing table and tends to send data packets through such routes [6].

4. OLSR routing attacks

In first part of this section, some OLSR routing attacks are introduced and in the second part, Black hole attack and its different implementations are especially explained.

4.1. Important OLSR attacks

This subsection consists of a brief description of important attacks concerning OLSR protocol.

4.1.1. Selfish behavior. Selfish behavior of a node can be carried out by refraining from forwarding data or control packets. In actual words, a selfish node participates in all of the network activities; however, when it comes to packet forwarding, for some reason, for example in order to conserve its battery power, it prevents from forwarding such packets [15].

4.1.2. Collusion attack. In collusion attack, some of the malicious nodes collude with each other and manipulate routing information of one or a number of other nodes such that those nodes will not be accessible in the network anymore [9], [10].

4.1.3. Black hole Attack. In Black hole attack, attacker node propagates unreal information in the network and tries to direct network traffic towards itself. Traffic absorption would be possible through suggesting optimized fake routes to other nodes of the network. Therefore, a considerable amount of network traffic would be absorbed by attacker node. Afterwards, Black hole node can misuse received information or discard them silently [2], [5], [7], [12].

4.1.4. Gray hole attack. Gray hole attack is a special form of Black hole in which after absorbing the network traffic, in some cases attacker node behaves like the other trusty nodes and forwards packets according to the routing algorithm; whereas in other cases, it drops received packets [2].

4.1.5. Worm hole attack. One of the serious and sophisticatedly designed attacks against MANETs is Worm hole attack. Two colluding attacker nodes compromise with each other under Worm hole attack. One of them records packets from one point of the network and transmits them using a private high speed link to another point of the network which the second attacker is located. After receiving packets, second attacker rebroadcasts them in the second point of the network. As a result, incorrect routing information will be propagated in the network and routing tables of the network nodes will be updated by such incorrect information. Routing can be faced with serious problems under Worm hole attack [16], [17].

4.1.6. Replay Attack. In ad hoc networks, because of nodes mobility, network topology changes frequently. It means that current routing information will be expired and not valid in the near future. In Replay attack, a malicious node records control messages of other nodes and injects them again to the network in the future when they have been expired. Consequently, incorrect and expired information will be recorded in the routing tables of network nodes which results in various routing problems [11].

4.1.7. MPR-Flooding Attack. According to OLSR protocol, when a node receives a control message, should retransmit it on condition that it has been selected as MPR by that node. MPR-Flooding can be performed by propagating received TC messages by means of an attacker node which has not been selected as MPR. Therefore, in the next steps of propagation, it is possible that such retransmitted packets be ignored by real MPR nodes; because real MPR nodes have recently received related packets from another node (attacker node) and it leads to network routing obstacles [11].

4.2. NEW Black hole Attack in OLSR

Black hole is a denial of service (DOS) attack. As mentioned in section 4, a Black hole attacker tries to absorb network traffic towards itself and upon receiving packets, discards them silently. In this section, a description about implementation details of different Black hole attacks based on OLSR protocol is presented.

In OLSR protocol, establishment and advertisement of valid routes is carried out by transmitting HELLO and TC messages. Therefore, attacker node can modify each of the HELLO, or TC messages or both of them simultaneously to advertise false routes. Consequently, three cases of Black hole attack can be implemented in OLSR which we have named them as: TC-Black-Hole, HELLO-Black-Hole, and TC-HELLO-Black-Hole.

4.2.1. TC-Black-Hole Attack. Attacker node in this attack tries to advertise false routes by modifying TC messages. In order to perform modification, malicious node claims that all nodes of the network have selected this node as their MPR. It means that attacker node propagates and advertises address of all network nodes in its TC messages. Such false information is received and processed by neighbor nodes and relayed in the whole network through attacker's MPR nodes. As a result, network nodes update their topology tables by this fake information and make forgery routes using such information while establishing and recording their routes. Finally, at the time of sending data packets, it is possible for source node to send its data packets through the route which attacker node has advertised to create that. This scenario results in dropping data packets by attacker node. Implementation and evaluation of TC-Black-Hole attack has been carried out in this paper for the first time.

4.2.2. HELLO-Black-Hole attack. This attack operates based upon manipulating HELLO messages. In this case, at the time of sending HELLO messages, attacker node embeds address of all network nodes into the message and broadcasts that [7]. In actual words, attacker node claims that all of the nodes in the network are its neighbors and they have a bi-directional link with it. After reception of such a message, in their MPR selection process, neighbor nodes note that their level-2 neighbor set are contained in the attacker node's advertised HELLO message. In other words, attacker node claims that it covers all of the level-2 neighbors of all of its level-1 neighbors. On the other hand, in OLSR protocol nodes always try to minimize the number of their MPRs. Consequently, all of the attacker node neighbors select it as their only MPR. Afterwards, as soon as the Black hole node was selected as MPR by its neighbors, according to OLSR protocol sends TC messages in the network containing list of its MPR Selectors. Actually, by sending TC messages, Black hole node advertises a list including all of its neighbors and propagates such a list in the whole network by means of its own MPRs. It means that all of network nodes update their topology and routing tables using information of such fake TC messages. As a result, when a node wants to send a data packet to one of the attacker neighbors, if the destination node does not be the level-1 or level-2 neighbor of the source node, it uses a path to send its data packets which passes from attacker node in its last hop. Finally, all of the data packets with the destination of attacker neighbors are received and silently dropped by Black hole node.

4.2.3. TC-HELLO-Black-Hole attack. Third Black hole attack is composed as combination of both TC-Black-Hole and HELLO-Black-Hole attacks. Under TC-HELLO-Black-Hole attack, malicious node modifies not only HELLO, but also TC messages. Therefore, similar to HELLO-Black-Hole, attacker would be selected by all of its neighbors as MPR and, similar to TC-Black-Hole, would propagate much fake links using fake TC messages. As a result, Black hole node will be able to advertise unreal routes more strongly and absorb more network traffic towards itself and finally drop all of the received packets mutely. TC-HELLO-Black-Hole attack has been simulated and evaluated in this paper for the first time.

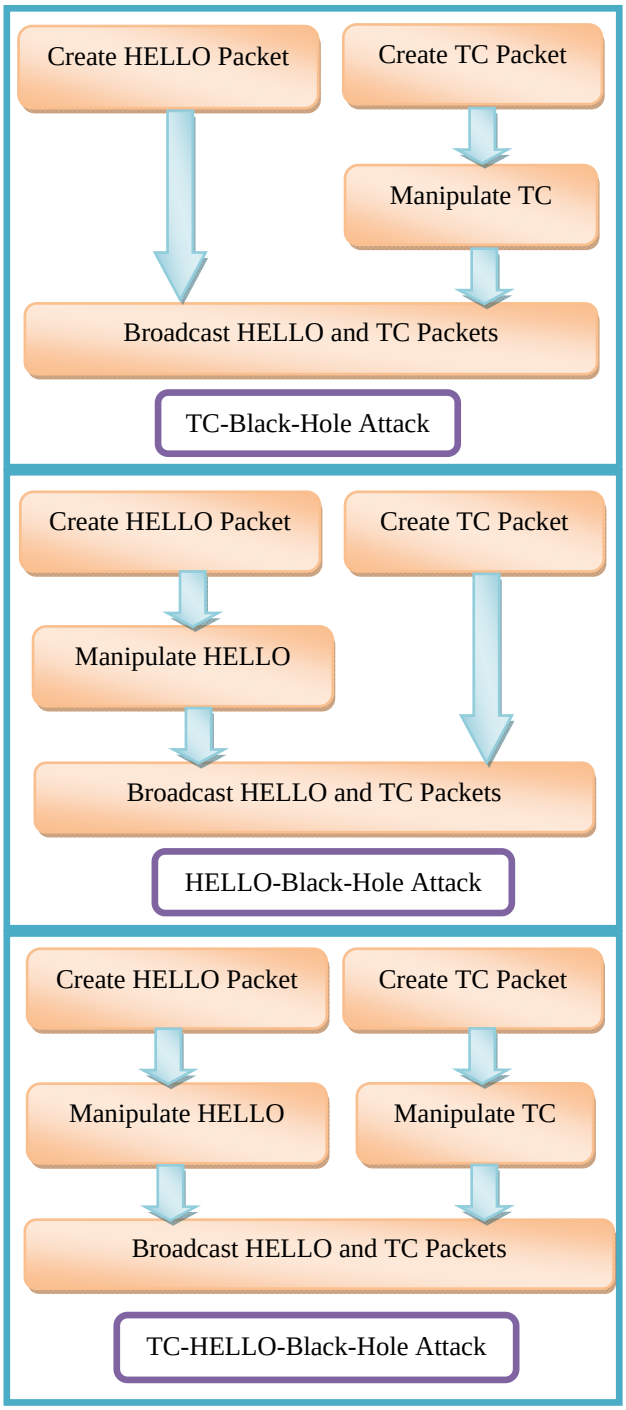

Figure 2. Implementation of different Black hole attacks in OLSR

Fig. 2 represents the operation of different Black hole attacks which can be implemented in OLSR protocol.

5. Simulation

This section includes simulation and evaluation of TC-HELLO-Black-Hole attack. For this purpose, such an attack has been compared with other Black hole attacks (TC-Black-Hole and HELLO-Black-Hole), selfish nodes, and basic OLSR. When it comes to selfish nodes, two different selfish behaviors have been considered which have been labeled as Selfish Nodes and Very Selfish Nodes in the plots. A Selfish Node is a node which prevents from forwarding data packets and discards them. A Very Selfish Node is a Selfish Node which refrains from forwarding control packets, as well. Simulations have been done using NS-2.34 [18] and simulation parameters have been listed in Table 1. Each point in plots has been calculated as average of 10 simulation runs.

Table 1. Simulation Parameters

Parameter	Value
Routing Protocol	OLSR
Mac Layer	802.11b
Simulation Time	600 seconds
Region	1000*1000 m^2
Number of Mobile Nodes	40 nodes
Transmission Range	250 m
Movement Model	Random Waypoint
Pause time	10 seconds
Max speed	0 to 20 m/s
Traffic Type	CBR
Data payload	512 bytes
Rate	2 packets/seconds
Number of connections	10
Number Attacker nodes	1 node
Target of Attacks	All nodes
Buffer Size	50 packets

In order to assess effects of nodes mobility on the network, speed of nodes has risen from 0 to 20 meters per second for the mentioned scenario. Packet drop ratio, average end-to-end delay, throughput, and the number of routing packets have been regarded as network parameters to evaluate different attacks. Three different figures for each parameter have been plotted. The first plot compares the operation of selfish nodes and basic OLSR, the second one compares the operation Black hole attacks, and the last one compares all attacks with each other.

5.1. Packet Drop Ratio

5.1.1. Selfish Nodes. Packet Drop Ratio for selfish nodes has been illustrated in the first plot of Fig. 3. It is evident that the amount of dropped packets for both Selfish Nodes and Very Selfish Nodes is less than basic OLSR. The reason is that uncooperative nodes refrain from forwarding received packets. The amount of dropped packets for Very Selfish Nodes is not meaningfully comparable with Selfish Nodes. It means that by dropping received control packets, Very Selfish Nodes cannot absorb and drop more data packets.

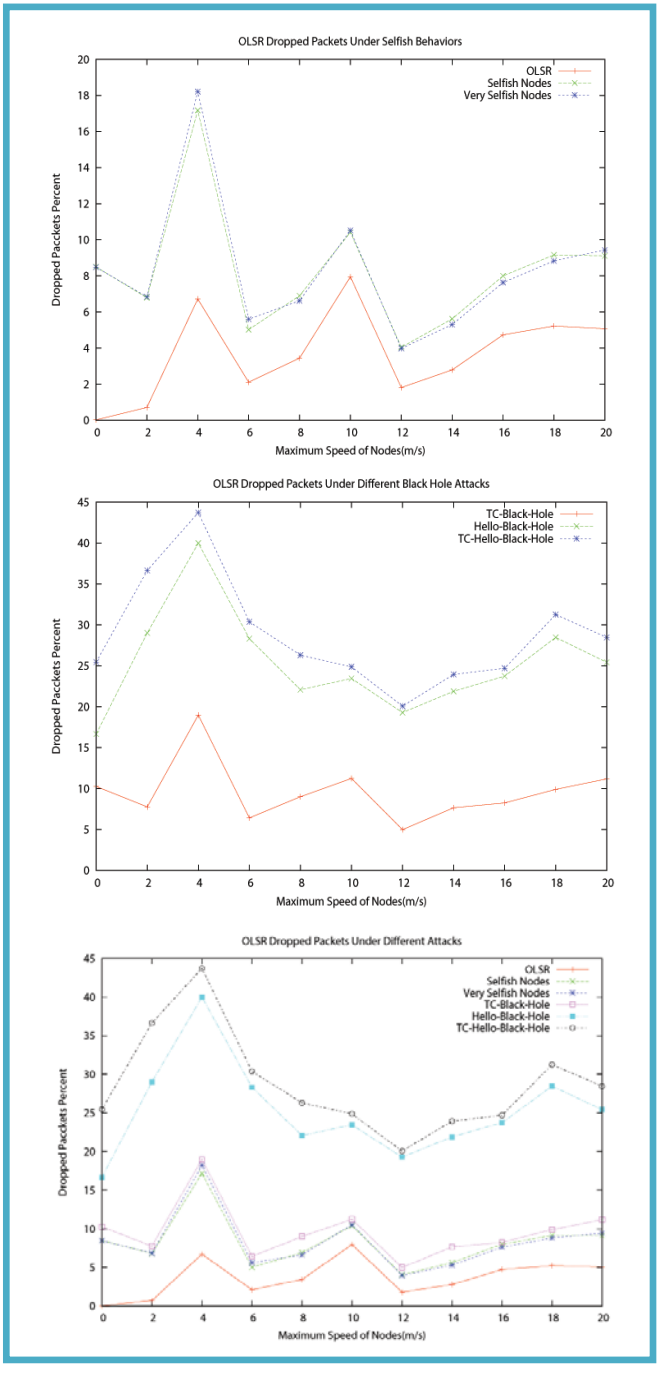

Figure 3. Packet Drop Ratio

5.1.2. Black hole attacks. Second plot of Fig. 3 represents packet drop ratio for Black hole attacks. The figure represents that packet drop ratio in TC-HELLO-Black-Hole and HELLO-Black-Hole is by far more than TC-Black-Hole attack. The reason is that in both prior attacks, Black hole node is selected as the only MPR for all of its neighbors. It means that, with a high probability, all of the routes with the length greater than 2, to any of the Black hole node neighbors should pass from Black hole node; because this is the only node which generates TC messages for all of its neighbors. However, in TC-Black-Hole, attacker node does not play any extra role in the phase of MPR selection compared to basic OLSR. It only advertises fake links in its TC messages. Packet drop ratio for TC-HELLO-Black-Hole demonstrates higher proportion than HELLO-Black-Hole. The reason is that TC-HELLO-Black-Hole node not only captures routes to its neighbors, but also advertises a higher number of unreal links to all of the network nodes by means of transmitting TC messages. In this case, the possibility of composing fake routes in routing tables of network nodes and, as a result, packet drop ratio increases.

5.1.3. All attacks. Packet drop ratio for all attacks has been depicted in the third plot of Fig. 3. It is shown that Black hole attacks, for the reason of fake route advertisement, have had more destructing effects compared to both selfish behaviors. It is due to their effective fake route advertisement which leads to absorbing more network traffic and dropping more data packets by Black hole nodes.

5.2. Throughput

5.2.1. Selfish nodes. Throughput ratio is directly bound with drop ratio. As demonstrated in the first plot of Fig. 4, the proportion of throughput for basic OLSR is reasonably more than both selfish behaviors. What's more, the amount of packet throughput for both Selfish Nodes and Very Selfish Nodes is nearly the same similar to their packet drop ratio.

5.2.2. Black hole attack. Throughput for Black hole attacks is represented in the second plot of Fig. 4. The figure reasonably shows a dramatic decrease for HELLO-Black-Hole and especially TC-HELLO-Black-Hole compared to TC-Black-Hole attack. As mentioned before, it is because of more packet dropping by TC-HELLO-Black-Hole and HELLO-Black-Hole than TC-Black-Hole.

5.2.3. All attacks. As shown in the last plot of Fig. 4, throughput of Black hole attacks is less than both selfish behaviors. Furthermore, it can be concluded that by increasing the speed of nodes, average throughput of packets for all of the algorithms almost decreases, conversely. The proportion for basic OLSR is the most and for TC-HELLO-Black-Hole attack is the least.

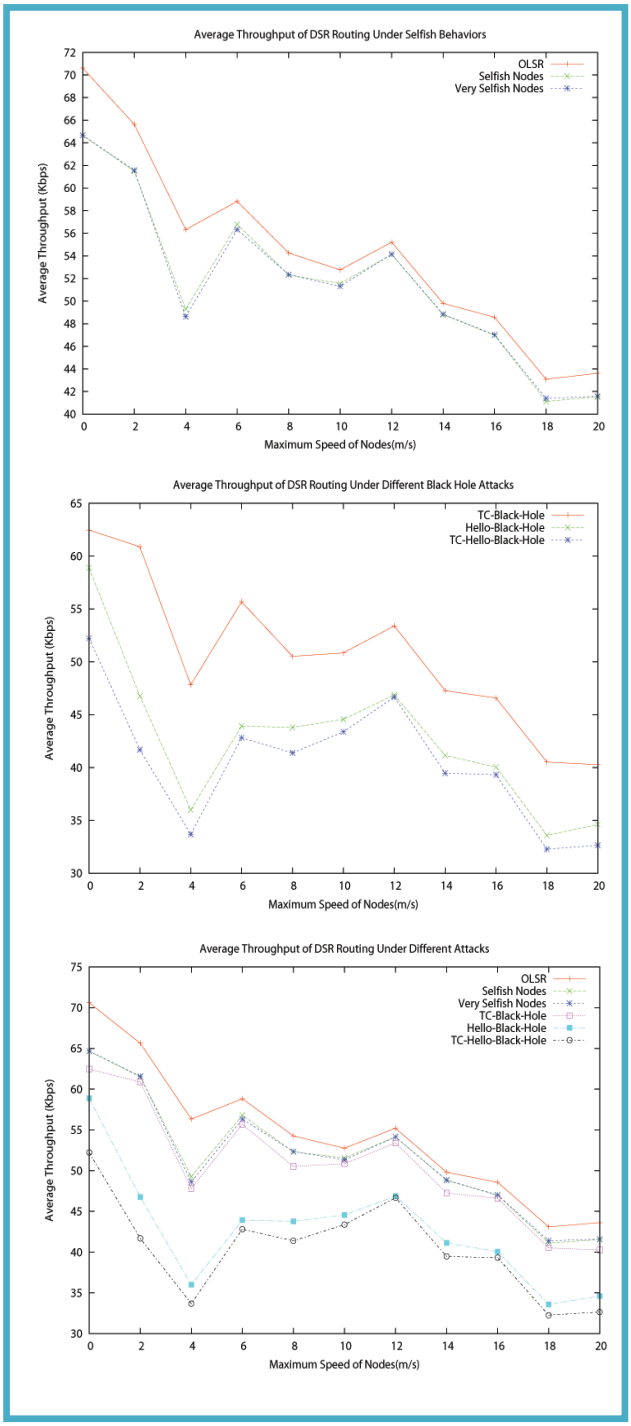

Figure 4. Average Throughput

5.3. End-to-end delay

5.3.1. Selfish Nodes. The amount of end-to-end delay for selfish nodes is illustrated in the first part of Fig. 5. The proportion for Very Selfish Nodes is higher than Selfish Nodes. It is due to the fact that Very Selfish Nodes, which drop TC messages, lessen the probability of establishing many of routes and network nodes have to establish

alternative routes related to information of their topology table. Such routes may be longer than regular routes and this brings about an increase in the amount of delay. The proportion for basic OLSR is almost more than both selfish behaviors.

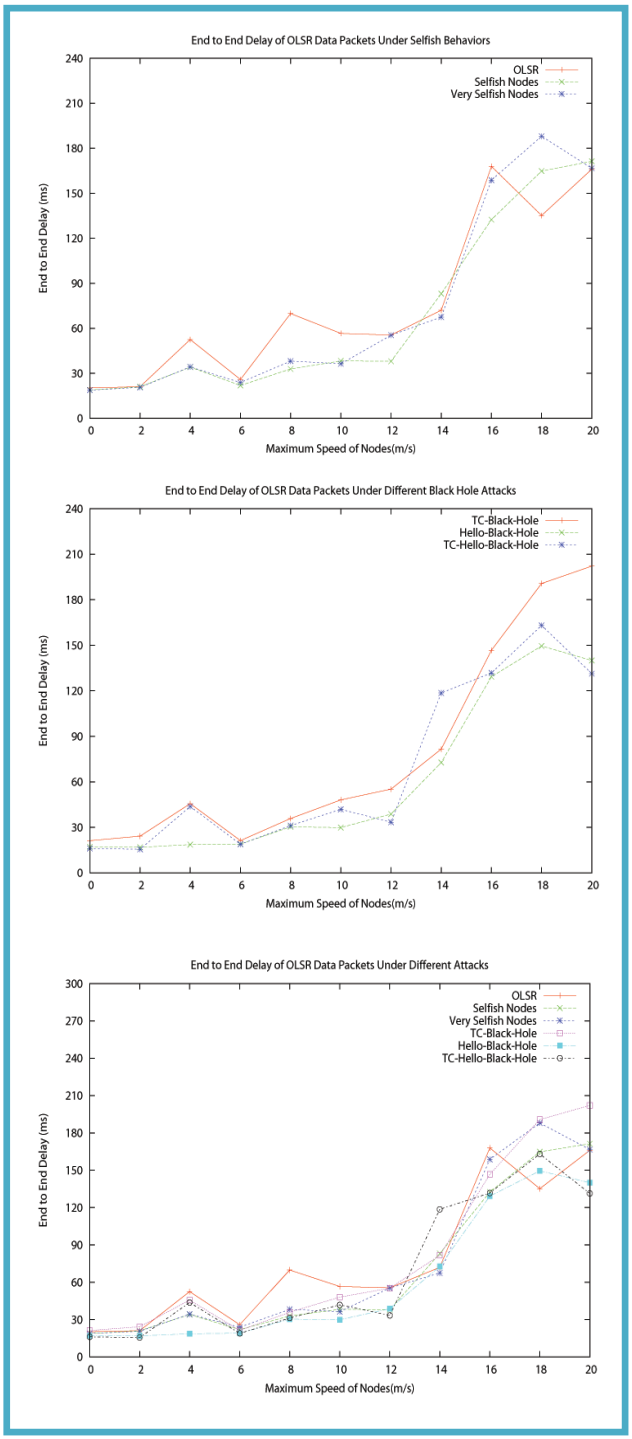

Figure 5. End-to-end delay

5.3.2. Black hole attacks. Second plot of Fig. 5 represents the amount of end-to-end delay for Black hole attacks. The proportion for TC-Black-Hole is more than other Black hole attacks. The reason is that HELLO-Black-Hole and TC-HELLO-Black-Hole attacks absorb and discard more network traffic rather than TC-Black-Hole. In order to calculate end-to-end delay, it is important to emphasize that no delay is calculated for dropped packets. As a result, packets which have reached to their destination and have not been dropped by Black hole nodes possibly have used short routes and Black hole node, with its effective fake route advertisement scheme, has not been able to be placed in such routes. For example, fake route advertisement does not affect sending data packets to level-1 or level-2 neighbors of the source node in OLSR.

5.3.3. All attacks. In the last plot of Fig. 5, end-to-end delay is plotted for different attacks. As represented, by increasing speed of nodes in the network, the amount of end-to-end delay rises for all of the algorithms. The reason is that as nodes move faster, the number of broken routes increases and packets have to wait until nodes obtain up-to-date routes. Additionally, it can be observed that end-to-end delay for basic OLSR, which consists of the least drop ratio, is almost the most.

5.4. Number of routing packets

5.4.1. Selfish Nodes. The number of routing packets for selfish behaviors and basic OLSR has been plotted in the first plot of Fig. 6. As shown, the number of routing packets for Very Selfish Nodes is less than Selfish Nodes and basic OLSR; because Very Selfish Nodes does not rebroadcast received TC messages which results in fewer number of routing packets. The proportion for Selfish Nodes and basic OLSR is nearly the same. The reason is that selfish nodes does not change the behavior of routing operation and it just drop received data packets.

5.4.2. Black hole attacks. According to the second plot of Fig. 6, HELLO-Black-Hole and TC-HELLO-Black-Hole impose by far fewer number of routing packets compared to TC-Black-Hole. This is due to the fact that in prior attacks neighbors of the attacker node do not transmit much TC messages to the network. The reason is that attacker node is the only MPR for all of its neighbors and is the only node which almost sends TC messages among its neighbors. As a result, participation of attacker's neighbors in routing decreases.

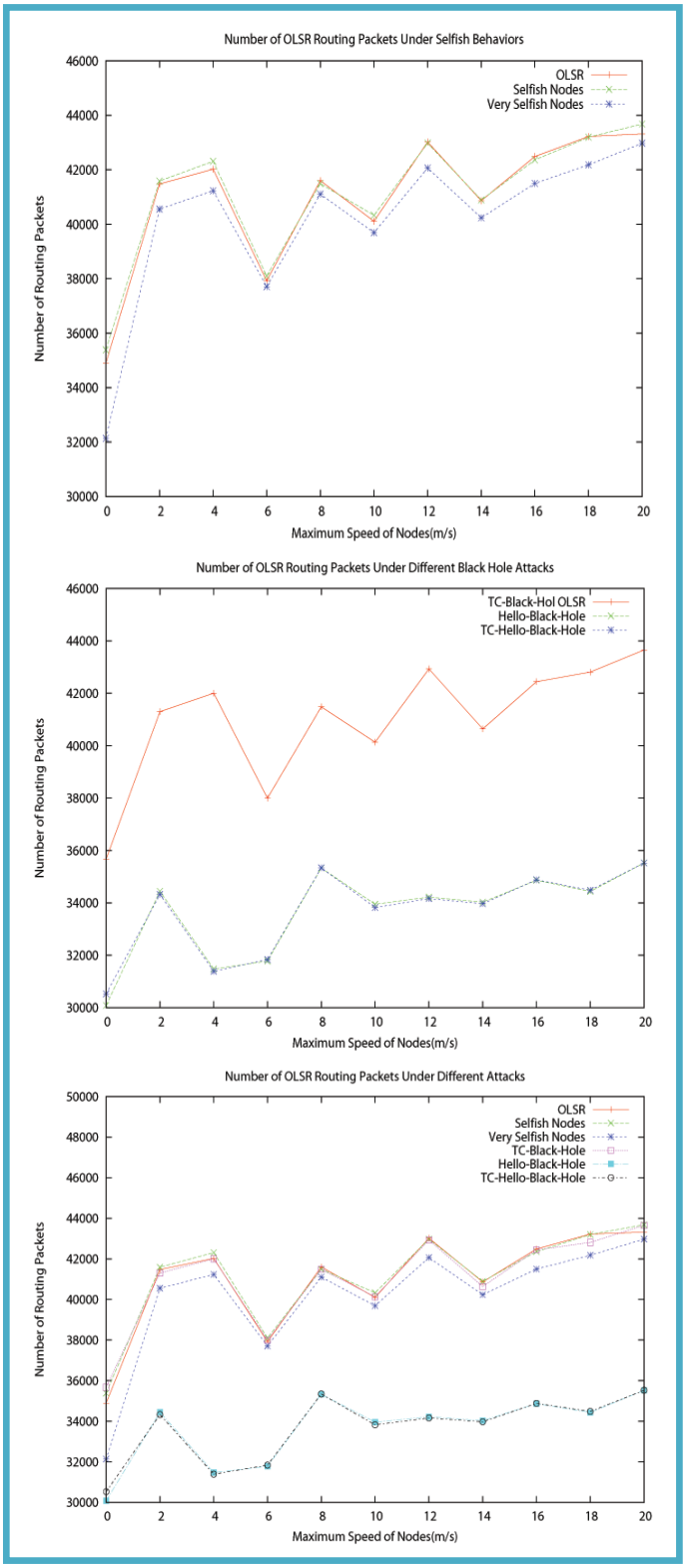

Figure 6. The number of routing packets

5.4.3. All attacks. As represented in the third plot of Fig. 6, the number of routing packets almost increases as the speed of nodes rises. HELLO-Black-Hole and TC-HELLO-Black-Hole impose nearly the same number of routing packets to the network. The reason is that both of such attacks follow the same procedure in transmitting routing packets. Similarly, TC-Black-Hole, Selfish Nodes, and basic OLSR follow the same mechanism in case of sending routing packets. Consequently, the number of routing packets for all of the mentioned three protocols is nearly equal to each other. The only difference for Very Selfish Nodes compared to above-mentioned three protocols is dropping received TC messages which leads to fewer number of routing packets.

6. Conclusion

One of the most important vulnerability points of MANETs is routing. In this paper, routing attacks of OLSR protocol are introduced and different implementations of Black hole attack are especially examined. Simulation results and evaluation of a special kind of Black hole which we introduced in this paper for the first time and called it as TC-HELLO-Black-Hole, compared to other implementations of such an attack represented that effects of this attack on network parameters can be more destructive than what has been considered in the past related works. TC-HELLO-Black-Hole especially reduces packet drop ratio and, as a result, average throughput of the system. Whilst, according to simulation results, with only one Black hole node in the network, in average about 29 percent of data packets have been dropped which means a considerable damage on the network connectivity. As a result, nodes will not be able to efficiently communicate with each other. Meanwhile, end-to-end delay in delivery of the packets and the number of routing packets will decrease, as well.

7. References

[1] J. Sarangapani, “Wireless Ad Hoc and Sensor Networks Protocols, Performance, and Control”. CRC Press Taylor & Francis Group, pp. 24-35, 2007.

[2] J. CAI, P. YI, J. CHEN, Zh. WANG, N. LIU, “An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network,” *Proc. Int. Conf. on Advanced Information Networking and Applications*. Singapore, pp. 775-780, 2010.

[3] D. Mishra1, Y. K. Jain, S. Agrawal, “Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET)”, *Proc. Int. Conf. on Advances in Computing, Control, and Telecommunication Technologies*. Singapore, pp. 775-780, 2009.

[4] Sh. sharma, R. gupta, “simulation study of blackhole attack in the mobile ad hoc networks”, Journal of Engineering Science and Technology, School of Engineering, Taylor’s University College, Vol. 4, No. 2, pp 243 – 250, 2009.

[5] M.Salehi, H.Samavati, M.Dehghan, “Performance Assessment of DSR Protocol under a new Black hole Attack”, *Accepted in Third Int. Conf. on Intelligent Networking and Collaborative Systems*, INCoS-2011, FUKUOKA, JAPAN, 2011.

[6] T. Clausen and P. Jacquet, “RFC 3626 Optimized Link State Routing Protocol (OLSR),” 2003.

[7] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, J. Tolle, “Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs”, *Proceedings of the 32nd IEEE*

Conference on Local Computer Networks, LCN 2007, Ireland, pp. 1043-1052, 2007.

[8] K.URMILA VIDHYA, M. MOHANA PRIYA, "A NOVEL TECHNIQUE FOR DEFENDING ROUTING ATTACKS IN OLSR. MANET", 2010 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2010, India, 2010.

[9] M. N. Kishore Babu, A. Antony Franklin, and C. Siva Ram Murthy, "On the Prevention of Collusion Attack in OLSR-based Mobile Ad hoc Networks", *16th IEEE International Conference on Networks*, ICON 2008, India, 2008.

[10] P. Lalith Suresh, Rajbir Kaur, M. S. Gaur, V. Laxmi, "Collusion attack resistance through forced MPR switching in OLSR", *In Proceedings of Wireless Days'2010*. pp.1-5, Venice, Oct. 2010.

[11] C. Adjih, D. Raffo, P. Muhlethaler, "Attacks Against OLSR: Distributed Key Management for Security", 2nd OLSR Interop / Workshop, France, 2005.

[12] B. KANNHAVONG, H. NAKAYAMA, Y. NEMOTO, AND N. KATO, A. JAMALIPOUR, "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS", IEEE Wireless Communications, Vol 14, No 5, pp. 85-91, October 2007.

[13] T. Clausen, U.Herberg, "Security Issues in the Optimized Link State Routing Protocol Version 2 (OLSRv2)", International Journal of Network Security and its Applications, 2010.

[14] P. Agrawal, R. K. Ghosh, S. K. Das, "Cooperative black and gray hole attacks in mobile ad hoc networks", *Proceedings of the 2nd ACM international conference on Ubiquitous information management and communication, ICUIMC '08,* pp.310-314. USA, 2008.

[15] P. Michiardi and R. Molva. "Simulation-based analysis of security exposures in mobile ad hoc networks". *In Proceedings of European Wireless Conference*, 2002.

[16] F. Na¨ıt-Abdesselam, B. Bensaou, and T.Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks", IEEE Communications Magazine, Vol 46, No 4, pp. 127-133, April 2008.

[17] M. A. Ferrag, M. Nafaa, "Securing the OLSR routing protocol for Ad Hoc Detecting and Avoiding Wormhole Attack", *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, pp. 51-58, April Edition, 2011.

[18] K. Fall; K. Varadhan, NS notes and documentation, The VINT Project, UC Berkely, LBL, USC/ISI, and Xerox PARC, 1997.

8. Acknowledgment

This work was supported by Sama technical and vocational training college, Islamic Azad University, Karaj branch, Karaj, Iran.

