Secure Routing Protocol: Affection on MANETs Performance

Shervin Ehrampoosh Ali Mahani

Abstract— **In mobile ad hoc networks, the absence of infrastructure and the consequent absence of authorization facilities impede the usual practice of establishing a practical criterion to distinguishing nodes as trusted and distrusted. Since all nodes in the MANETs would be used as router in multi-hop applications, secure routing protocols have vital rule in the security of the network. So evaluating the performance metrics of secure routing protocols and calculating the overhead of security design is very important in network engineering. In this paper the effects of Black hole attack on two different types of routing, OLSR as proactive routing protocol and AODV as reactive routing protocol are considered. In addition, the performance metrics of ordinary routing protocols (AODV and OLSR) are compared with a new secure routing protocol MAODV, in which neighbors of node help him to distinguish a trusted node. Finally, the simulation results depict the end-to-end delay of a network under black hole attack with different type of routing protocols, AODV, OLSR and MAODV. The simulation results illustrate good comparison of network performance parameters for different conditions such as node mobility and number of nodes.**

Index Terms— **Mobile Ad Hoc network (MANET), wireless network, security, OLSR, AODV.**

I. INTRODUCTION

MOBILE Ad Hoc networks (MANET) are self configuring networks in which mobile devices connected by wireless links. These networks classify into infrastructure less networks, where the network communication is established without any fixed infrastructure, such as battlefields, military applications and other emergency disaster situations. Obviously, security is a critical issue in such areas [1, 2]. Network architecture with shared wireless medium, resource constraints, and highly dynamic topology, lead to various challenges of the security design. Since the wireless channel is accessible to both legitimate users and malicious nodes so various forms of attacks such as passive eavesdropping, active signal interference, and jamming could be hampered the network. The cooperative nature of Ad Hoc routing protocols makes it more vulnerable to data tampering, impersonation, and denial of services (DoS). MANETs architecture causes the inefficiency of some conventional security solutions, such as a public key infrastructure (PKI), and the intrusion detection system [3, 4].

Some of the standard terms about security concepts of networks are message non-repudiation, Isolation and Trust. Message non-repudiation means that the sender cannot deny transmitting a packet. Isolation requires that protocol be able to identify misbehaving nodes and render them unable to interfere with routing. Alternatively, the routing protocol should be designed to be immune to malicious nodes.

One aspect of mobile ad hoc networks that complicates the design of a secure routing protocol is in-network aggregation. A secure routing protocol is typically only required to guarantee message availability and message integrity and confidentiality are handled at a higher layer by an end-to-end security mechanism such as SSH or SSL. In an ideal world, we would like to guarantee the confidentiality, integrity, authenticity and availability of all messages in the presence of resourceful adversaries.

In such an environment, there is no guarantee that a path between two nodes would be free of malicious nodes that would not comply with the employed protocol and would attempt to harm the network operation. The mechanisms currently incorporated in routing protocols cannot cope with disruptions due to malicious behavior. For example, any node could claim that it is one hop away from the sought destination, causing all routes to the destination to pass through itself. Constructing security for the first time may not be so difficult, maintaining trust and handling dynamic changes seem to need more effort. So many routing protocols in mobile ad hoc network to guarantee the security of network increase the control packets [12, 23]. Hence, the overhead of packet transmission, and also the end-to-end delay would be increased. The overheads are very important in network planning and a fair comparison between secure routing and conventional protocols lead to designing optimum routing protocol.

In this paper the performance metrics of routing protocols are simulated. The results are depicted for different protocols and finally a secure protocol is compared with AODV and OLSR. The rest of the paper is organized as follows. In Section II, routing protocols are reviewed. The effects of black hole attack in AODV, OLSR, and new approach called MAODV are discussed in section III. Simulation results of

Shervin Ehrampoosh is an M.Sc. student at Faculty of Electrical and Computer Engineering, Kerman Graduate University of Technology (KGUT), Kerman, Iran (e-mail: s_ehrampoosh@yahoo.com).

Ali Mahani is with the Department of Electrical Engineering, Shahid Bahonar University, Kerman, Iran.
(e-mail: amahani@uk.ac.ir)

performance metrics are described in section IV and the paper is concluded in section V.

II. ROUTING PROTOCOLS

The first classification of routing protocols is:

1. Single phase routing approach
2. Two phase routing protocols

The single-phased approach embeds data into the routing process, while the two-phased approach sends data over established routes.

In another classification the routing protocols of ad hoc networks are classified into two main categories, proactive and reactive. In a proactive (sometimes-referred to as table-driven) routing protocol, nodes periodically exchange routing information with other nodes to update their routing information. The Optimized Link State Routing (OLSR) [8] protocol is a well-known proactive routing protocol. In a reactive (sometimes-referred to as source-initiated) protocol, a route from source to destination would be established only when the source node has a packet to send to the destination [5]. Dynamic Source Routing (DSR) [6] and Ad Hoc On-Demand Distance Vector (AODV) [7] are two main samples of reactive routing protocols. Nevertheless, unfortunately there is no common standard routing protocol in MANETs.

A. AODV Protocol

When a node "A" as a source node try to initiates a connection to destination node "D", it will generate a route request message (RREQ). This message is transmitted through a limited flooding to their neighbors. In the second hop the message is forwarded to the neighbors of neighbors and would be continued till to finding destination node or finding a node that has a fresh route to the destination. Then a new control message, route reply message (RREP), is replied to the source node. When RREP reaches the source node, a route is established between the source node "A" and destination node "D". Once the route is established between "A" and "D", the communication would be started. Fig. 1 depicts the exchange of control messages between source node and destination node.

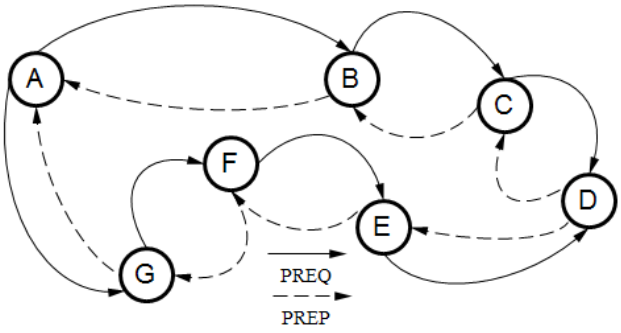


Fig. 1 AODV Route Discovery

If the route between source and destination is broke, the RERR message is sent to the source and destination nodes separately. The scheme of sending RERR message in a network s shown in the Fig. 2.

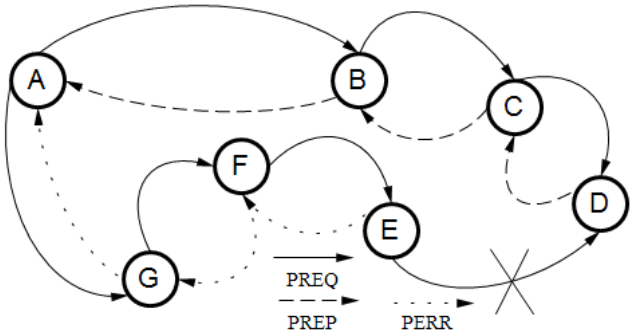


Fig.2 Route Error Message in AODV

B. OLSR protocol

OSLR protocol is a proactive protocol used in mobile ad-hoc networks. It is often called table-driven protocol as it maintains and updates its routing table frequently. OLSR has also three types of control messages that are describe bellow.

1) Hello
2) Topology Control (TC)
3) Multiple Interface Declaration (MID)

Hello message is transmitted for sensing the neighbor and multi-point distribution relays (MPR) calculation. Topology control is link state signaling that is performed by OLSR.
MPRs are used to optimize theses messaging. MID messages contains the list of all IP addresses used by any node in the network. All the nodes running OLSR, transmit these messages on more than one interface.

OLSR exchanges the topology information always with other nodes. Few nodes are selected as MPRs (Multi point relays). MPRs are responsible for transmission of broadcast messages during flooding and generating link state information. MPRs technique used in OLSR protocol will reduce the message overhead and even minimize the number of control messages flooded in the network (Fig 3).

Nodes maintain the information of neighbors and MPR's, by sending and receiving HELLO messages from its neighbors. This will help in determining the link formation illustrated in Fig 4.

1) Node X transmits the HELLO message to node Z and then the message received by node Z from node X that can be called asymmetric link.
2) Even if The node Z transmits the HELLO message to node X then the resulting link retransmits this HELLO message called asymmetric link.
3) Finally, the resulted bidirectional link is known as a symmetric link.
4) Symmetric link formation will help the nodes to choose

MPRs.

5) MPRs will send the topology control (TC) messages containing the information about link status and MRP node information [9].

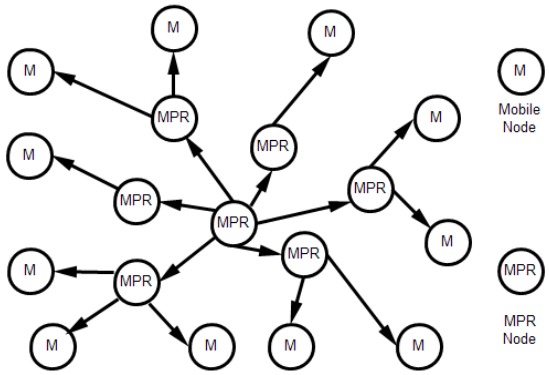


Fig.3 Flooding Packets Using MPR

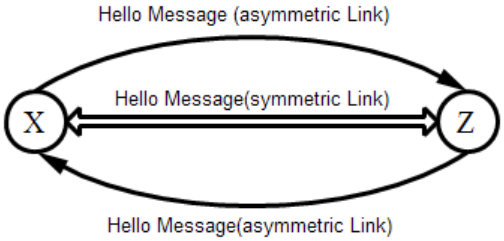


Fig.4 OLSR Symmetric link formation (Hello Message Exchange)

III. SECURE ROUTING PROTOCOLS

As mentioned above MANETs often suffer from security attacks because of their specification such as open medium, dynamic topology, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battlefield situation for the MANET against the security threats [10]. The attacks could be classified based on:

- The behavior of the attack (Passive vs. Active)
- The source of the attacks (Internal vs. External)
- The processing capacity of the attackers (Wired vs. Mobile)
- The number of the attackers (Single vs. Multiple)

Current ad hoc routing protocols are basically exposed to two different types of attack: active attacks and passive attacks. The active attacks occur when the malicious node bears some energy costs in order to perform the threat, whereas passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly.

Malicious nodes can disrupt the functions of a routing protocol by modifying its information or by sending false routing information through the entire network.

Also according to the position of attacker, the attacks are divided into four categories, which are shown in figure 5. These categories are Interception, Interruption, Modification and Fabrication.

In black hole attack as an active attack, the malicious node waits for the neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does notallow forwarding any packet anywhere. This attack is called a black hole as it swallows all objects; data packets [11].

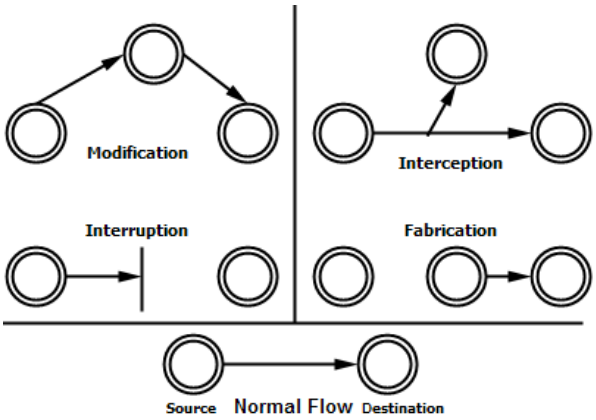


Fig.5 Security Threats

In Fig 6, source node S wants to send data packets to a destination node D in the network. Node M is a malicious node that acts as a black hole. The attacker replies with false reply RREP having higher modified sequence number. So data communication initiates from S towards M instead of D. In OLSR black hole attack, a malicious node forcefully selects itself as MPR. Malicious node keep its willingness field to will always constantly in its HELLO message. Therefore, in this case, neighbors of malicious node will always select it as MPR. Hence, the malicious node earns a privileged position in the network that it exploits to carry out the denial of service attack. The effect of this attack is much harmful when more than one malicious node is present near the source and destination nodes.

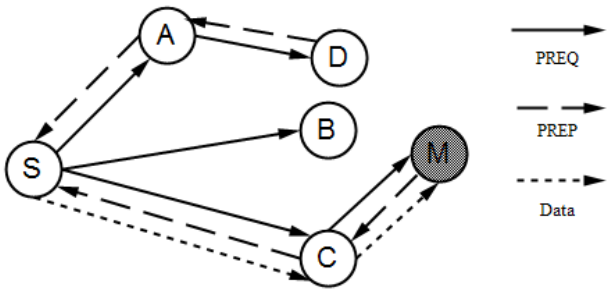


Fig.6 Black hole attacks in MANETs

Therefore, black hole attacks are non-single attacks; since multiple malicious nodes could be acting as a group of attacker.

A. Mitigation Techniques against Black Hole Attack

In MANET, attacks that modify routing messages can be provoked by the use of source authentication. Digital signature, message authentication code (MAC) and hashed MAC (HMAC) can be used. Up to certain level of security can be attained at network layer in internet by the use of IPSec. Authenticated Routing for Ad-Hoc Networks (ARAN) is another routing protocol that provides the protection from Black Hole attack where there is threat to the changes in sequence number, hop count modification, source routing changes and spoofing of destination addresses [12].

The protocol implement in [13] proposed Secure Ad-Hoc On-Demand Distance Vector Routing (SAODV), which verifies the destination node by exchanging random numbers. SAODV effectively prevents Black Hole attack in Mobile Ad-hoc network and it is better than AODV in terms of security and routing efficiency.

Authors of [14] are focused on the requirement of a source node to wait unless the arrival of RREP packet from more than two nodes. When it receives multiple RREPs, the source node check that there is any share hops or not. The source node will consider the routed safe if it finds the share hops. Its drawback is the introduction of time delay that it has to wait for the arrival of multiple RREPs before authenticating a node.

In [15], the authors proposed route confirmation request message (CREQ) and route confirmation reply (CREP) in order to avoid Black Hole attack. So when an intermediate node sends RREPs to the source node also it send CREQ to its next hop node in direction of destination node. After receiving CREQ, the next hop look for route in its destination in cache. If a CREP is received during this time it will confirm the validity of path in RREP and in CREP. Upon matching the source node will recognize the route being correct. Its drawback is that it cannot detect multiple Black Hole attacks.

In [16], the author showed that malicious node should increase the sequence number of destination to assure the source node of its route. The author proposed a statistics based detection for Black Hole that is based on the difference between destination sequence numbers of received RREP's. Its drawback is the false positives approach because of the nature of anomaly detection.

B. MAODV Protocol

As discussed in previous section, such malicious nodes can also create new routing messages and advertise nonexistence links provide incorrect link state information and flood other nodes with routing traffic thus inflicting failures on the system.

In this section, we use an approach that has been proposed in [17] to combat black hole attack in AODV routing protocol. In this approach, numbers of rules are used to inference about honesty of replier. The proposed method is based on this principle that the activity of a node in a network shows its honesty. Each node for participating in data transfer process, must be demonstrate its honesty. Early of simulation, all nodes are able to transfer data; therefore, they have enough time to show its truth. If a node is the first receiver of a RREP packet, forwards that packets to source and initiates judgment process about replier. The judgment process is based on opinion of network's nodes about replier. Neighbors of each node store the activities of that node. So during the judgment process the neighbors send their opinion about a node. When the node collects all opinions of neighbors, it decides about honesty of that node. The decision is based on the following rules which are used to judge about honesty of a node.

Rule 1: *If a node delivers many data packets to destinations, it is assumed as an honest node.*

Rule 2: *If a node receives many packets but do not sent same data packets, it is possible that the current node is a misbehavior node.*

Rule 3: *When the rule2 is correct about a node, if the current node has sent many RREP packets; therefore surely the current node is misbehavior.*

Rule 4: *When the rule2 is correct about a node, if the current node has not sent any RREP packets; therefore the current node is a failed node.*

IV. SIMULATION RESULTS

Our simulation model was carried out using the OPNET Modeler software platform. It is a useful research tool for achieving good simulation results. Mobility scenarios are generated by using a Random waypoint model by varying 20 to 80 nodes moving in a terrain area of 1000m x 1000m. Each node independently repeats this behavior and mobility is changed by making each node stationary for a short period. The simulation parameters are summarized in Table I.

The simulation results could be used to analyze the performance metrics of the network. The metrics are:

1) ***Packet Delivery Ratio***: *The ratio of the data delivered to the destination to the data sent out by the source.*
2) ***Average End-to-End delay***: *The difference in the time it takes for a sent packet to reach the destination. It includes all the delays, in the source and each intermediate host, caused by the routing discovery, queuing at the interface queue etc.*

3) ***Routing Overhead:*** *the total number of routing exchanged packets during the simulation in terms of total number of packets transmitted*

Main network variables, which are considered to simulate the effects of security on the performance metrics, are:

Network size: *variation in the number of mobile nodes.*
Traffic load: *variation in the number of sources.*
Mobility: *variation in the maximum speed.*

Each simulation scenario is repeated 10 times and the average of simulation results are depicted in figures 7, 8 and 9.

Figure 7(a) and 7(b) show that under black hole attack the PDR (Packet Delivery Ratio) of MAODV is improved by 40-60% than AODV under attack with Average-End-to-end delay almost same as normal AODV. In addition, we find that the difference between OLSR under attack and MAODV is 30-60%.

Figure 7(c) illustrates the overhead of MAODV and AODV. As we expect the routing overhead of AODV is less than MAODV. The figure shows that the MAODV routing overhead follows the overhead of AODV through variation of traffic load with at most 10% difference.

Figure 8(a) and 8(b) conclude the simulation based on the effect of mobility on the MAODV compared to normal AODV. The PDR stays within acceptable limits almost 5-20% lower than it normally expected.

As shown in figure 8(a) the PDR of MAODV is reduced through growing the node mobility. By growing the mobility of nodes, the neighbors of a node move faster and the expected rate of control packets in MAODV is growth rapidly so the routing overhead is increased. Consequently the PDR of MAODV is less than AODV and OLSR. The PDR of MAODV under attack shows that this protocol has a good robustness against mobility in comparison with AODV and OLSR under attack. But the Average-End-to-End delay almost same as normal AODV.

Figure 9(a) considers the network size as a variable, so the PDR (Packet Delivery Ratio) of MAODV improves by approximately 40% than AODV under attack.

The PDR diagrams of this figure lead us to conclude that the MAODV is a robust routing protocol against network size. In other words the modified AODV keeps it's throughput from small to large networks.

As shown in Figure 9(b) and 9(c) the average end to end delay and routing overhead of modified AODV and normal AODV both is increased by enhancing the network size.

As we expect the PDR of MAODV under attack is better than AODV and OLSR under attacks through increasing traffic load, mobility and network size.

It means that the modified AODV is in top situation in comparison with OLSR and AODV under attack. Additionally increasing the average end to end delay and routing overhead of the MAODV in comparison with normal AODV is very small and could be neglected in all situation.

TABLE I
SIMULATION PARAMETERS

Parameter	***Value***
Simulator	OPNET 14.5
Routing Protocol	AODV, OLSR and MAODV
Simulation Time (sec)	1000
Number of Nodes	20-80
Simulation Area (m × m)	1000 × 1000
Packet Size (bit)	Exponential(1024)
Minimum Mobility (m/s)	10
Maximum Mobility (m/s)	60
Transmission Range (m)	250
Traffic Model	TCP
MAC Protocol	IEEE 802.11
Packet Size (bit)	1024
Mobility Model	Random Way Point (RWP)
Pause Time in RWP (sec)	50
Message TTL (sec)	100
Data Rate (Mbs)	11
Transmit Power (mW)	5
No. of Malicious Node	5
No. of Source Node	1-6

V. CONCLUSION

In this paper the effects of Black hole attack in MANET using both Proactive routing protocol and Reactive routing protocol such as OLSR and AODV are considered. The impact of Black Hole attack on the performance of MANET is illustrated finding out which protocol is more resilience against traffic load, mobility and network size. Additionally, a secure routing protocol, which is proposed in [17], is considered and the impacts of security design on the network performance metrics are simulated. As we expect the Simulation results show that the secure protocol has more end-to-end delay comparing with the AODV and OLSR, but it provides better performance in terms of packet delivery ratio than the conventional routing protocols in presence of Black holes attack.

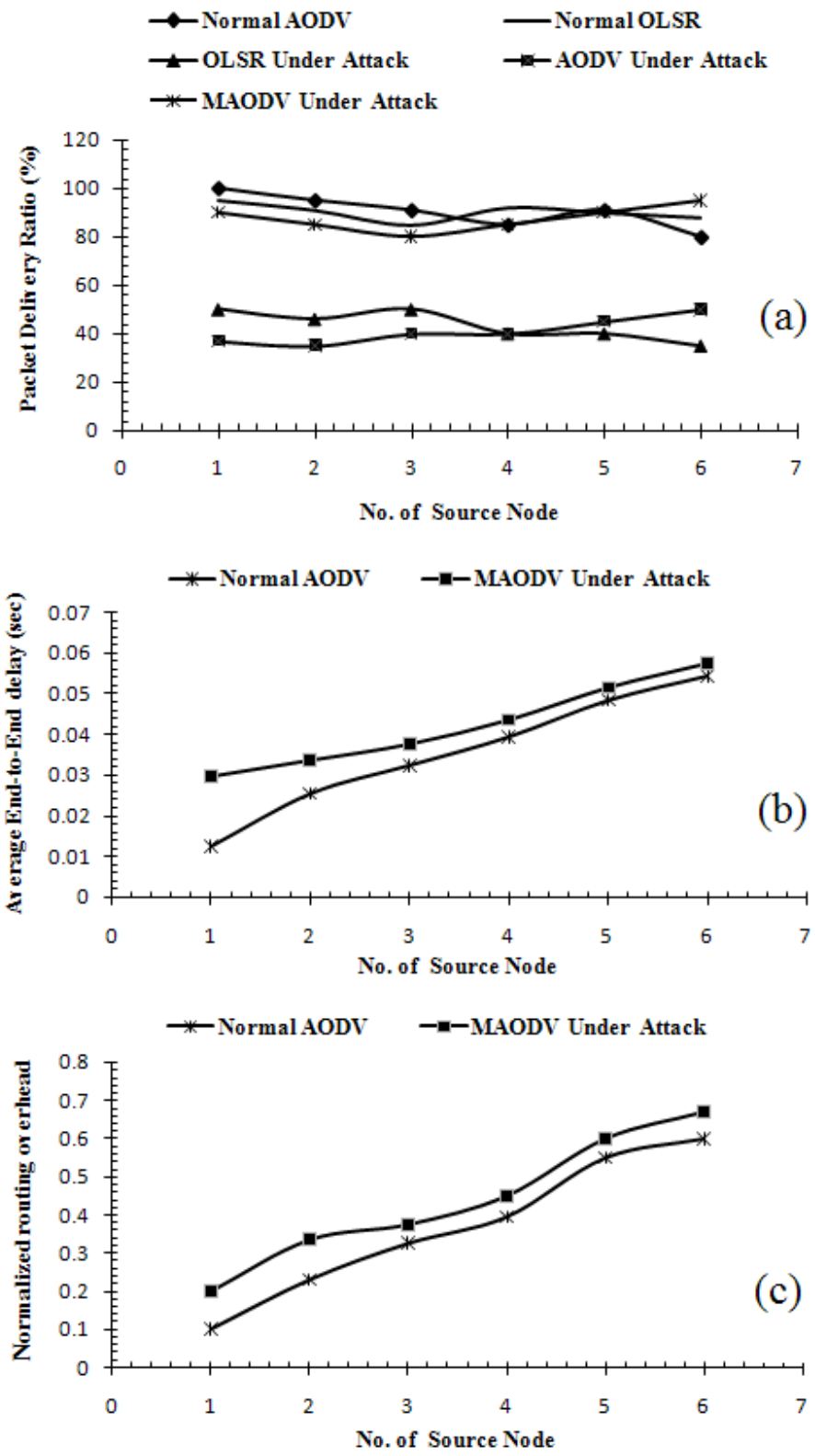


Fig.7 Influence of traffic load on the performance metrics, (a) Packet delivery ratio, (b) Average End-to-End Delay, (c) Normalized routing overhead

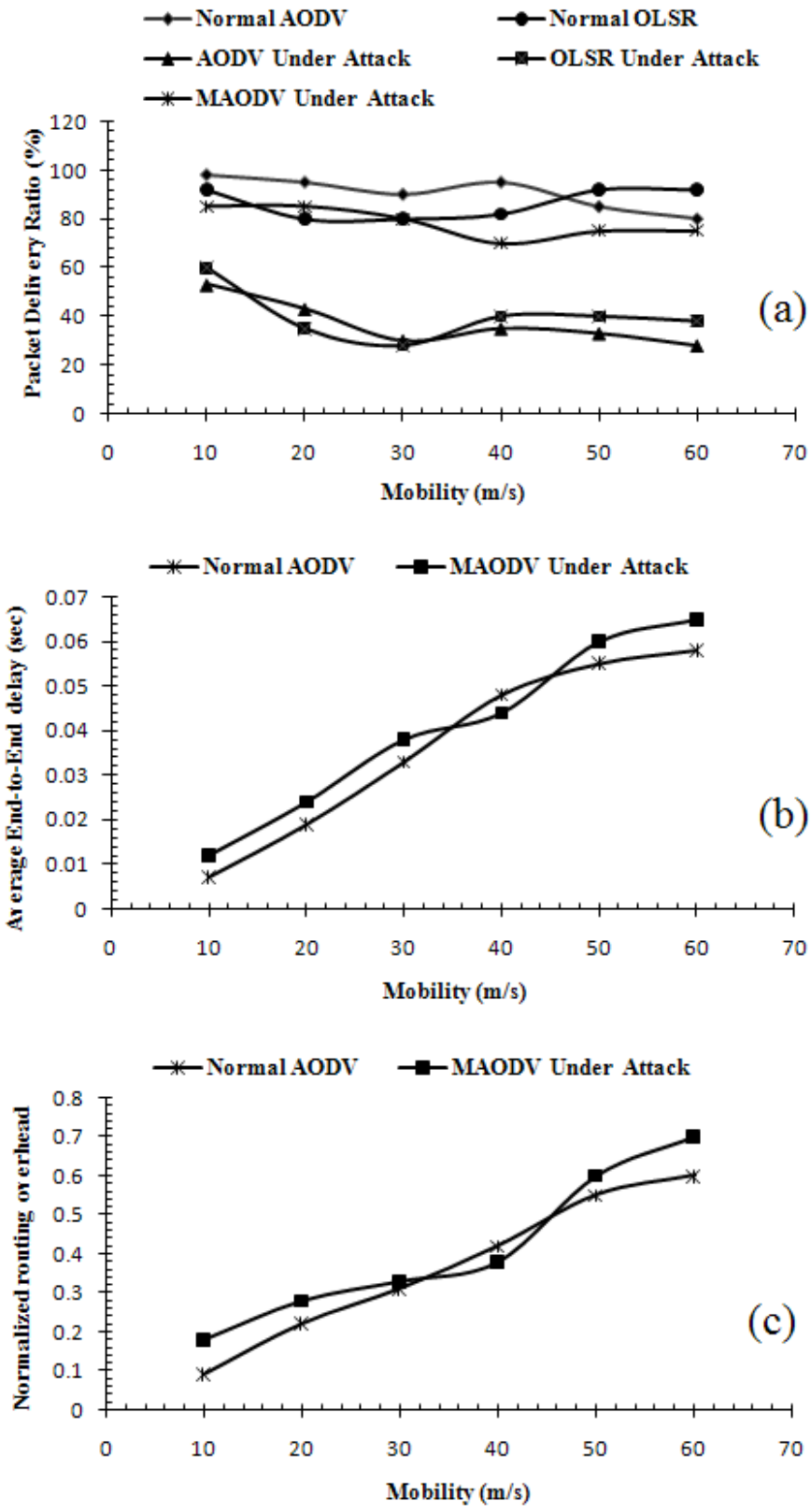


Fig. 8 Network Performance metrics versus node mobility

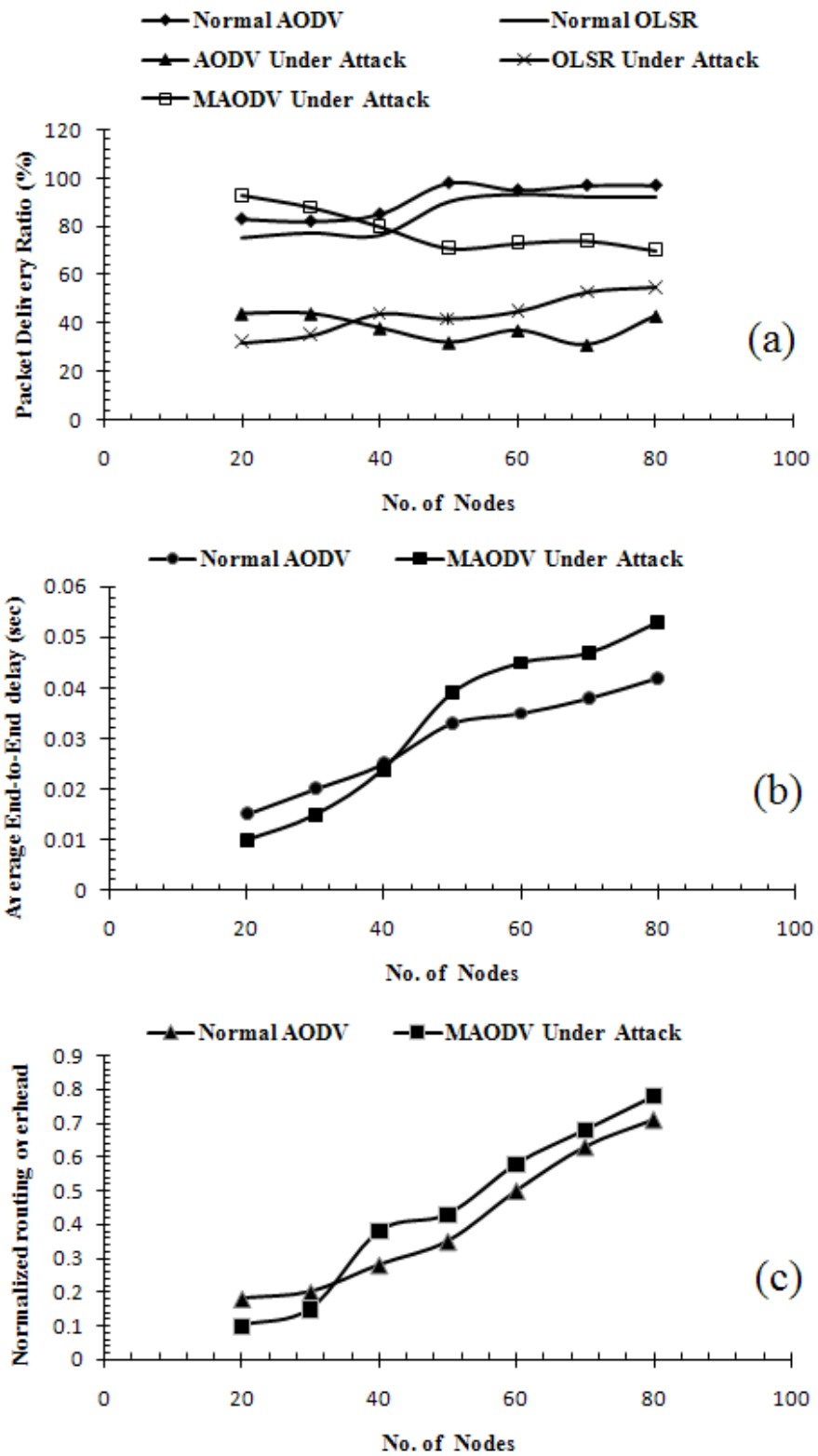


Fig.9 The effects of Network size on the performance metrics

REFERENCES

[1] Todd R. Andel, Alec Yasinsac, "Surveying Security Analysis Techniques in MANET Routing Protocols", IEEE Communications Surveys, 4th Quarter, No.4, 2007.

[2] N.H Saeed, M.F Abbod, H.S Al-Raweshidy, "Modeling MANET Utilizing Artificial intelligence", Second UKSIM European Symposium on Computer Modeling and Simulation, EMS '08, Page(s):117–122, 8–10 Sept. 2008.

[3] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks", Proc. of IEEE INFOCOM, 2002.

[4] A. Menezes, P. Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[5] A. Kush, C.J Hwang, "Proposed Protocol for Secured Routing in Ad Hoc Networks", International Association of Computer Science and Information Technology Spring Conference, IACSITSC '09, Page(s):76–81, April 2009.

[6] M. Bouhorma, H. Bentaouit, A. Boudhir, "Performance comparison of ad-hoc routing protocols AODV and DSR.", International Conference on Multimedia Computing and Systems, 2009. ICMCS '09, Page(s):511–514, April 2009.

[7] Y. Hu, A. Perrig, and D. Johnson, Ariadne, "A Secure On-Demand Routing for Ad Hoc Networks.", Proc. of MobiCom 2002, Atlanta, 2002.

[8] Zhan Huawei, Zhou Yun, "Comparison and Analysis AODV and OLSR Routing Protocols in Ad Hoc Network", 4th International Conference on Wireless Communications, Networking and Mobile computing 2008, WiCOM '08, Page(s):1 – 4, 12-14 Oct. 2008.

[9] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot, " Optimized Link State Routing Protocol", IEEE INMIC Pakistan 2001.

[10] Irshad Ullah, Shoaib Ur, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols.", Master Thesis at School of Computing, Blekinge Institute of Technology, 2009.

[11] Dokurer, Semih. "Simulation of Black hole Attack in Wireless Ad-hoc Networks.", Master's thesis, Atılım University, September 2006.

[12] H. Deng, W. Li, D.P. Agrawal, "Routing security in wireless Ad-Hoc networks" Cincinnati University, Ohio, USA, IEEE Communications Magazine, Vol.40, page(s):70-75, Oct. 2002.

[13] 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.

[14] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad-Hoc Networks.", ACM Southeast Regional Conf. 2004.

[15] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET.", Master Thesis at Karlstads University, Sweden, December 2006.

[16] S. Kurosawa et al., "Detecting Black hole Attack on AODV-Based Mobile Ad-Hoc Networks by Dynamic", IEEE Military Communications Conference, Vol. 2, page(s):1054-1059, Oct 2003.

[17] Mehdi Medadian, M.H. Yektaie, A.M Rahmani, "Combat with Black hole attack in AODV routing protocol in MANET ", First Asian Himalayas International Conference on Internet, page(s) 1-5, 3-5 Nov. 2009 .

[18] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks", IEEE Network Journal, No. 6, page(s):24–30, 1999.

[19] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-demand Secure Routing Protocol Resilient to Byzantine Failures", Proceedings of the ACM Workshop on Wireless Security, page(s):21–30, 2002.

[20] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks", Proc. of 8th ACM Mobile Computing and Networking (MobiCom'02), page(s):12–23, 2002.

[21] Z. Haas and M. Pearlman, "The Performance of Query Control Scheme for The Zone Routing Protocol", ACM/IEEE Transactions on Networking, pages:427–438, August 2001.

[22] Yang Xiao, Xuemin Shen and Ding-Zhu Du, "Wireless Network Security.", Springer, 2007.

[23] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, "Secure routing protocol for Ad Hoc networks",10th IEEE International Conference on Network Protocols, Dept. of Computer Sciences, California University, Santa Barbara, CA, USA. Page(s):78-87, 2002.