American Journal of Applied Sciences 9 (1): 18-23, 2012
ISSN 1546-9239

Impact of Malicious Nodes under Different Route Refresh Intervals in Ad Hoc Network

[1]P. Suganthi and [2]A. Tamilarasi
[1]Mother Teresa Women's University, Kodaikanal,
Tamil Nadu, India
[2]Department of MCA, Kongu Engineering College,
Perundurai Tamil Nadu India

Abstract: Problem statement: Ad hoc networks are formed dynamically by group of mobile devices co operating with each other. Intermediate nodes between source and destination act as routers so that source node can communicate with the destination node even if it is out radio range and thus eliminating the necessity of infrastructure. Co operation of nodes is a very important feature for the successful deployment of Ad hoc networks. The intermediate nodes should not only be involved in the route discovery process but also should be involved in the re transmission of packets as an intermediate between source and destination. **Approach:** Since nodes have to be co operative for successful deployment of Ad hoc networks, the security mechanisms cannot afforded to be stringent which enables malicious nodes to successfully attack the network. The capability of optimized link state routing protocol has been studied extensively for different types of ad hoc networks and has been proved to behave somewhere in between pro active and reactive routing protocols. **Results:** In this study we investigate the impact of malicious nodes on the Optimized Link State Routing (OLSR) protocol under different hello intervals which affects the route discovery process and subsequently investigate the degradation of Quality Of Service (QOS). **Conclusion:** It is observed that the throughput deteriorates when the network is attacked by malicious nodes which selectively retransmit data to some of the destinations. The performance degradation increases as the hello interval time is set beyond 4 sec. Higher hello interval decreases the control packet overheads. It is observed that even with higher hello intervals the network performance is much better than an attack by small group of malicious nodes.

Key words: Ad hoc network, optimized link state routing, malicious node, hello interval, network performance evaluation, routing protocol, Dynamic Source Routin (DSR), multipoint relays

INTRODUCTION

A Mobile Ad-Hoc Network (MANET) is formed by a collection of wireless nodes communicating with each other without the necessity of any infrastructure. Ad-hoc networks are multi hop networks with route being established between source and destination dynamically (Basagni *et al*., 2004; Murugan and Shanmugam, 2010). Since the network is highly dynamic with channel condition varying, regular routing protocols fail. Wireless routing protocols can be broadly classified into pro active routing protocols and reactive routing protocols. In proactive routing protocol, routes are discovered as the network is formed with the routing table continuously being updated over a fixed period as the network dynamic changes. Popular pro active routing protocols are Distance Sequence Distance Vector (DSDV) (Perkins and Bhagwat, 1994) routing protocol, Optimized Link State Routing protocol (OLSR) (Jacquet *et al*., 2001). In reactive routing protocols routes are discovered only when data needs to be transmitted between a source and destination. Popular reactive routing protocols include Ad Hoc on Demand Distance Vector (AODV) routing protocol (Perkins and Royer, 1999), Dynamic Source Routing (DSR) protocol (Johnson and Maltz, 1996). The advantages of proactive routing protocol are the availability of routes between all nodes and hence data can be transmitted immediately between a source and destination without waiting for route discovery. However as the network size increases the overheads in route discovery and maintenance affect the performance of the network.

Corresponding Author: P. Suganthi, Mother Teresa Women's University, Kodaikanal, Tamil Nadu, India Tel: 919894653070

Optimized Link State Routing Protocol (OLSR) was designed to perform effectively for large and dense ad hoc network and is an optimization of link state protocol. OLSR eliminates some of the disadvantages of Distance Sequence Distance Vector (DSDV) routing protocols by using the concept of Multipoint Relays (MPR) flooding technique to reduce the topology broadcast packets. OLSR consists of two types of control message for establishing communication between nodes: Hello message and Topology Control (TC) message. Hello messages are always transmitted one hop and are used to identify the node's neighbour and link status. Topology control messages are used for broadcasting neighbour and MPR selector list. Only MPR hosts are capable of forwarding TC messages and also the data throughout the network. In OLSR the routing table entries include the destination address, next address, number of hops and address. Routing tables are updated when new neighbour link appears or when a link disappears, whenever a two hop neighbour is created or removed.

Ad hoc network are more vulnerable to security issues compared to wired network due to its physical channel being wireless and the co operative nature of the nodes to form a successful network. Security vulnerabilities can occur in all the layers of the OSI model. Attacks can be classified based on the mode of operation and generally falls under one of the following category: Black hole attack, Flooding attack, Spoofing attack, Detour attack, Rushing attack and falsified route error generation attack. In black hole attack (Hu and Perrig, 2004) the routing information is modified so that packets are diverted to a malicious node and then the packets are dropped. In flooding attacks (Milanovic *et al*., 2004) the intermediate nodes burn their battery resources as malicious nodes use these intermediate nodes to forward flooded packets and this can also lead to blow out of the routing table as a result of overflow. In spoofing attack (Yang *et al*., 2002) the malicious node uses the identity of legitimate node to transmit data and control packets. In detour attack (Nallathambi *et al*., 2011) the packets are diverted to take a sub optimal route and hence increasing the network overheads. Rushing attacks (Hu *et al*., 2003a) are caused by route suppression techniques where the malicious node responds to a route request before the legitimate node can reply. In falsified route error generation attack, the source node is forced to rediscover the route due to false control messages generated by the malicious node Worm whole attacks are tunnelling attacks where the malicious node prevents the legitimate node from successfully discovering the route (Hu *et al*., 2003b).

Dhillon *et al*. (2004) proposed a Public key infrastructure (PKI) to improve security in a Mobile Ad hoc Network (MANET) running on OLSR routing protocol using a fully distributed Certificate Authority (CA). The proposed solution improves the control traffic load compared to using a centralized CA. However malicious nodes with proper credentials could not be identified.

Chriqi *et al*. (2009) proposed the Secure Clustering based OLSR (SC-OLSR). The mail goal of their research was to increase the life time of ad hoc networks in the presence of selfish nodes. The proposed algorithm effectively reduced the percentage of MPR nodes and thus reducing the traffic overhead. It provided a mechanism to select cluster heads and MPR nodes based on the residual energy and the connectivity index. The proposed incentive mechanism was able to motivate nodes to cooperate under the threat that better network services will be provided only on accumulation of reputation

Wang *et al*. (2005) describe security threats to the OLSR MANET routing protocol. A semantic based intrusion detection solution was presented. The semantics properties are based on semantic properties implied in the OLSR routing behavior. However the proposed solution did not address conflicts resolution and verification procedure for intruders.

Babu *et al*. (2008) investigate the collusion attack in a MANET using OLSR protocol. During the presence of collusion attack the Packet Delivery Ratio (PDR) falls to 0% on the targeted node. To overcome this attack OLSR was enhanced by adding two new messages, Trust Request (TREQ) and Trust Reply (TREP). Implementation of these additional control overheads was able to detect collusion attack and subsequently improved the PDP. The proposed improvement on OLSR does not require time synchronization or location improvement.

Suresh *et al*. (2010) investigated collusion attack in MANET based on OLSR. They proposed a method Forced MPR switching (FMS-OLSR) which observes symptoms of attack and temporarily blacklist potential attackers. Once backlisted, the algorithm forces recomputation of its MPR set thus avoiding attacks.

Kannhavong *et al*. (2008) proposed a unique acknowledgement between two hop neighbors whenever the control traffic is successfully received. The proposed methodology was able to protect the network from link spoofing, worm hole attack without requiring location information or the full topology of the network. The proposed system was able to achieve higher packet delivery ratio compared to standard OLSR.

MATERIALS AND METHODS

Simulation was carried out using 20 nodes acting as client and one node acting as server. All the nodes run client/server application over TCP/IP or UPD/IP network. Fast recovery was enabled in TCP with receive buffer size of 8760 bytes. The maximum acknowledgement delay for TCP in each node was set at 0.2 sec with slow start initial count at 2. The transmit power of each node is 0.005 watts and reception power threshold set at -95dBm. The data rate of the wireless network was uniformly set at 11Mbps. All nodes were programmed to have a random trajectory. FTP traffic was generated randomly.

Three scenarios under the same network conditions were considered. In the first scenario the network does not contain any malicious nodes. Hello interval messages were set at 2, 4 and 8 sec respectively. In the second scenario three of the nodes are made malicious with two of the nodes selectively retransmitting packets and one node rejecting all packets that is not destined for it. Simulations were conducted with Hell interval of 2, 4 and 8 sec. Simulations were run for 15 min and the network performance observed.

RESULTS

In each scenario the throughput, the neighbor additions and the total control packets sent and received were measured. Figure 1-5 show the network performance when there is no attack in the network.

It is observed that as the hello interval time increases the number of additions and deletions increase which increases the overall control overheads.

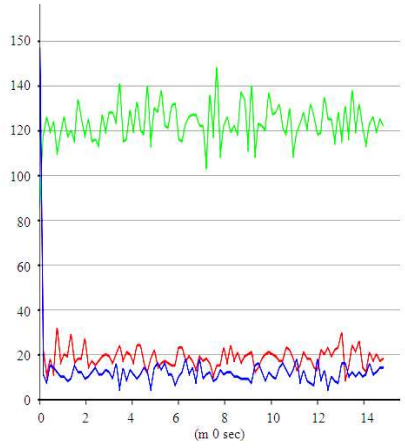

Fig. 1: Neighbor additions for hello interval of 2, 4 and 8 sec (blue, red and green respectively) in network without malicious nodes

The network throughput also decreases as the Hello interval increases. However for small network with normal random mobility it is seen that increasing the Hello interval from 2-4 sec does not affect the network performance. Figure 6-10 shows the performance of the same network under attack.

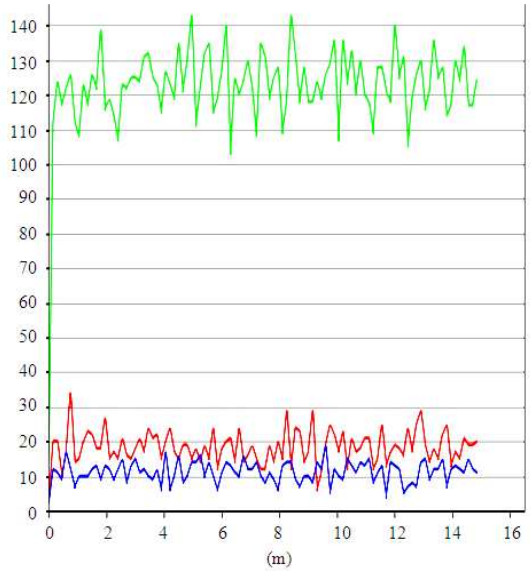

Fig. 2: Neighbor deletions for hello interval of 2, 4 and 8 sec (blue, red and green respectively) in network without malicious nodes

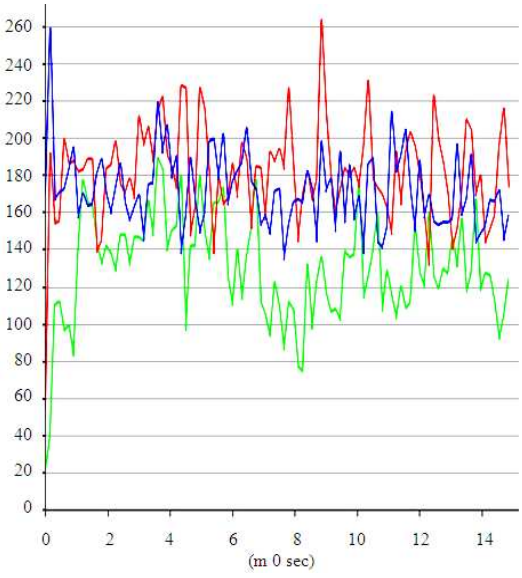

Fig. 3: Routing traffic received in packets/sec in network without malicious nodes for hello interval of 2, 4 and 8 sec (blue, red and green respectively)

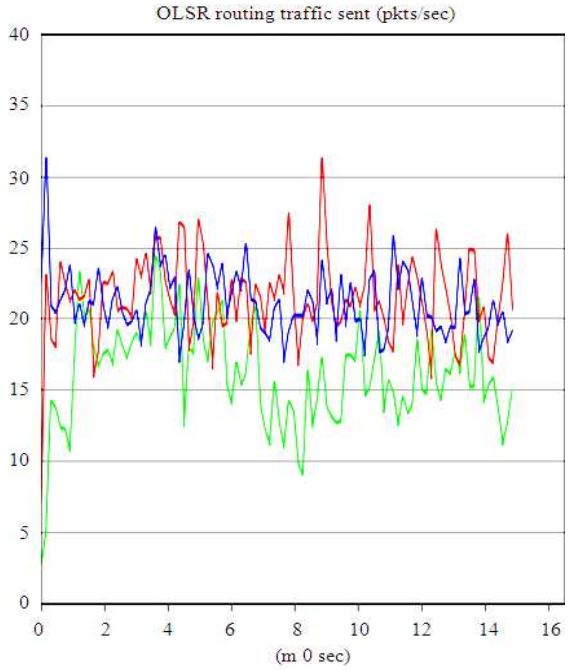

Fig. 4: Routing traffic sent in packets/sec in network without malicious nodes for hello interval of 2, 4 and 8 sec (blue, red and green respectively)

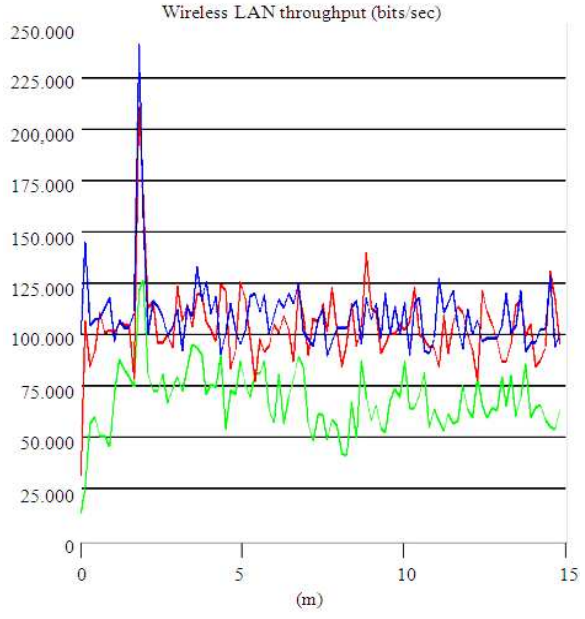

Fig. 5: Throughput of the network in bits/sec when no malicious node is present nodes for hello interval of 2, 4 and 8 sec (blue, red and green respectively)

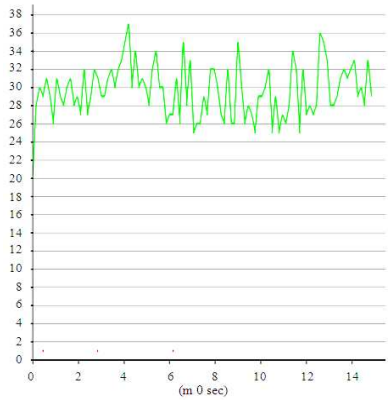

Fig. 6: Neighbor additions for hello interval of 8s in network with malicious nodes

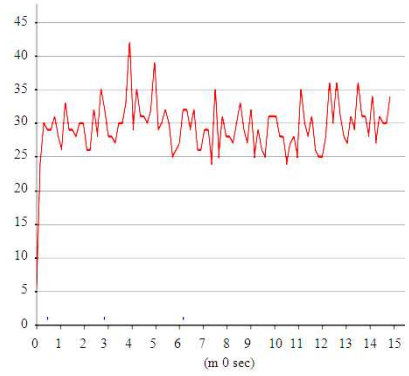

Fig. 7: Neighbor deletions for hello interval of 8 sec in network with malicious nodes

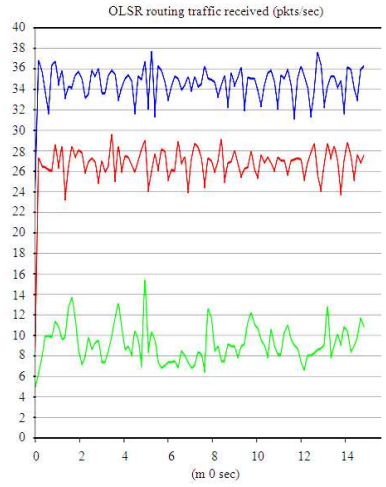

Fig. 8: Routing traffic received in packets/sec in network with malicious nodes for hello interval of 2, 4 and 8 sec (blue, red and green respectively)

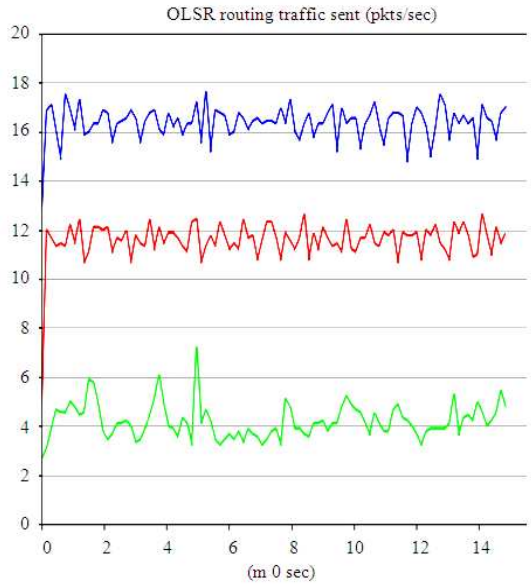

Fig. 9: Routing traffic sent in packets/sec in network with malicious nodes for hello interval of 2, 4 and 8 sec (blue, red and green respectively)

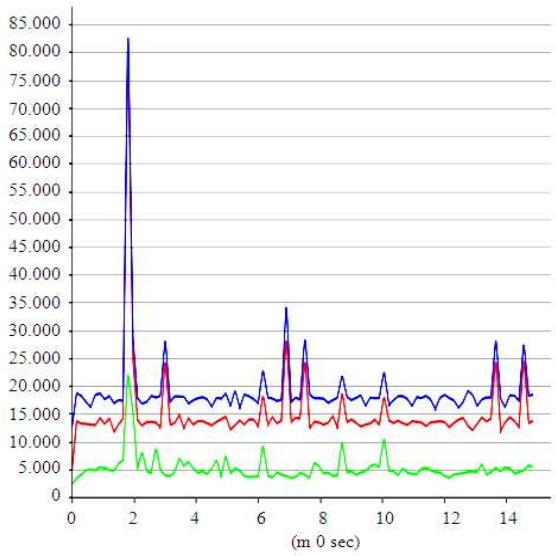

Fig. 10: Throughput of the network in bits/sec when malicious node is present nodes for hello interval of 2, 4 and 8 sec (blue, red and green respectively)

CONCLUSION

In this study we investigate the performance of an adhoc network using OLSR routing protocol under normal co operative conditions with different hello interval and a network consisting of malicious nodes with different hello intervals. From Fig. 5 and 10 it is observed that the throughput deteriorates when the network is attacked by malicious nodes which selectively retransmit to the destination. The performance degradation increases as the hello interval time is set beyond 4 sec. Higher hello interval decreases the control packet overheads. It is observed that even with higher hello intervals the network performance is much better than an attack by small group of malicious nodes. Further investigations need to be done to detect different types of malicious nodes and propose mechanism to alleviate the performance degradation.

REFERENCES

Babu, M.N.K, A.A. Franklin and C.S.R. Murthy, 2008. On the prevention of collusion attack in OLSR-based Mobile Ad hoc Networks. Proceedings of the 16th IEEE International Conference on Network, Dec. 12-14, IEEE Xplore Press, New Delhi, pp: 1-6. DOI: 10.1109/ICON.2008.4772578

Basagni, S., M. Conti, S. Giordano and I. Stojmenovic, 2004. Mobile Ad Hoc Networking. 1st Edn., John Wiley and Sons, IEEE Press, Piscataway, NJ., ISBN: 0471373133, pp: 461.

Chriqi, A., H. Otrok and J.M. Robert, 2009. SC-OLSR: Secure clustering-based OLSR model for ad hoc networks. Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Oct. 12-14, IEEE Xplore Press, Marrakech, pp: 239-245. DOI: 10.1109/WiMob.2009.48

Dhillon, D., T.S. Randhawa, M. Wang and L. Lamont, 2004. Implementing a fully distributed certificate authority in an OLSR MANET. Proceedings of the IEEE Conference on Wireless Communications and Networking, Mar. 21-25, IEEE Xplore Pres, pp: 682-688. DOI: 10.1109/WCNC.2004.1311268

Hu, Y.C. and A. Perrig, 2004. A survey of secure wireless ad hoc routing. IEEE Security Privacy, 2: 28-39. DOI: 10.1109/MSP.2004.1

Hu, Y.C., A. Perrig and D.B. Johnson, 2003a. Efficient security mechanisms for routing protocols. Proceedings of the Network and Distributed System Security Symposium (NDSS'03), San Diego, USA., pp: 57-73.

Hu, Y.C., A. Perrig and D.B. Johnson, 2003b. Packet leashes: A defense against wormhole attacks in wireless networks. Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies, Mar. 30-Apr. 3, IEEE Xplore Press, pp: 1976-1986. DOI: 10.1109/INFCOM.2003.1209219

Jacquet, P., P. Muhlethaler, T. Clausen, A. Laouiti and A. Qayyum *et al*., 2001. Optimized link state routing protocol for ad hoc networks. Proceedings of the IEEE International Multi Topic Conference Technology for the 21st Century, IEEE Xplore Press, pp: 62-68. DOI: 10.1109/INMIC.2001.995315

Johnson, D.B. and D.A. Maltz, 1996. Dynamic source routing in ad hoc wireless networks. Mobile Comput., 353: 153-181. DOI: 10.1007/978-0-585-29603-6_5

Kannhavong, B., H. Nakayama and A. Jamalipour, 2008. SA-OLSR: Security aware optimized link state routing for mobile ad hoc networks. Proceedings of the IEEE International Conference on Communication, May 19-23, IEEE Xplore Press, Beijing, pp: 1464-1468. DOI: 10.1109/ICC.2008.283

Milanovic, N., M. Malek, A. Davidson and V. Milutinovic, 2004. Routing and security in mobile ad hoc networks. IEEE Comput., 37: 61-65. DOI: 10.1109/MC.2004.1266297

Murugan, R. and A. Shanmugam, 2010. A combined solution for routing and medium access control layer attacks in mobile ad hoc networks. J. Comput. Sci., 6: 1416-1423. DOI: 10.3844/jcssp.2010.1416.1423

Nallathambi, E.E., R. Sankararajan, V. Sundaram and G. Sheeba, 2011. A secure routing protocol to eliminate integrity, authentication and sleep deprivation based threats in mobile ad hoc network. J. Comput. Sci., 7: 924-936. DOI: 10.3844/jcssp.2011.924.936.

Perkins, C.E. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computer Systems and Applications, Feb. 25-26, IEEE Xplore Press, pp: 90-100. DOI: 10.1109/MCSA.1999.749281

Perkins, C.E. and P. Bhagwat, 1994. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers. ACM SIGCOMM Comput. Commun. Rev., 24: 234-244. DOI: 10.1145/190809.190336

Suresh, P.L., R. Kaur, M.S. Gaur and V. Laxmi, 2010. Collusion attack resistance through forced MPR switching in OLSR. IFIP Wireless Days, 1-5. DOI: 10.1109/WD.2010.5657700

Wang, M., L. Lamont, P. Mason and M. Gorlatova, 2005. An effective intrusion detection approach for OLSR MANET protocol. Proceedings of the 1st IEEE ICNP Workshop on Secure Network Protocols, Nov. 6, IEEE Xplore Press, pp: 55-60. DOI: 10.1109/NPSEC.2005.1532054

Yang, H., X. Meng and S. Lu, 2002. Self-organized network-layer security in mobile ad hoc networks. Proceedings of the 1st ACM Workshop on Wireless Security, Sept. 28-28, Atlanta, GA, USA., pp: 11-20. DOI: 10.1145/570681.570683