Design of a Novel Proactive Link State Routing Approach to Defense against Node Isolation Attack in MANETs

Anurath Mane, Deepali Vora, Shailendra Kelkar,

Abstract— Routing protocols designed for MANETs are, in general, highly vulnerable to various forms of security attacks. A routing protocol is vital to the functioning of a wireless ad hoc network, and hence, security needs to be present to negate any potential malicious influences. However, providing efficient security mechanisms for such routing protocols is still viewed as being a considerable challenge. In this paper, the focus lies on the Optimized Link State Routing (OLSR) protocol, a proactive protocol which relies heavily on broadcast transmissions. This paper investigates end-to-end security mechanisms for the OLSR protocol, with specific interest in the denial of service attack. This paper proposes an extension to the standard OLSR approach called Enhanced OLSR (EOLSR) to overcome the DOS attack by using route reply messages in addition with route request messages.

Keywords: MANETs, Node isolation attack, OLSR, EOLSR, and MPR.

1 INTRODUCTION

A mobile ad hoc network (MANET) sometimes called a wireless ad hoc networkor a mobile mesh networkis a wireless network, comprised of mobile computing devices (nodes) that use wireless transmission for communication, without the aid of any established infrastructure or centralized administration such as a base station or an access point [1]. Unlike traditional mobile wireless networks, mobile ad hoc networks do not rely on any central coordinator but communicate in a self-organized way. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those far apart rely on other nodes to relay messages as routers. Applications of ad hoc network range from military operations and emergency disaster relief, to commercial uses such as community networking and interaction between attendees at a meeting or students during a lecture. Most of these applications demand a secure and reliable communication. Most of the previous research on ad hoc networking has been done focusing only uponthe efficiency of the network. There are quite a number of routing protocols proposed [3, 4] that are excellent in terms of efficiency. However, they were generally designedfor a non-adversarial network setting, assuming a trusted environment; hence no securitymechanism has been considered.Mobile wireless networks are generally more vulnerable to information and physicalsecurity threats than fixed wired networks. Vulnerability of channels and nodes, absence of infrastructure and dynamically changing topology, make ad hoc networks security adifficult task [2]. In addition to this, the security of routing protocols in theMANET dynamic environment is an additional challenge.

Designing a foolproof security protocol for ad hoc routing is a challenging task due to the unique network characteristics such as, lack of central authority, rapid node mobility, frequent topology changes, insecure operational environment, shared radio channel and limited availability of resources. A number of protocols have been proposed in the literature for secure routing. Most of these protocols are either proactive or reactive in approach. However, both the approaches have their own limitations [4, 5]. Optimized link state routing (OLSR)routing protocol which is a proactive routing protocol [6] offerspromising performance in terms of bandwidth and trafficoverhead but it does not incorporate any security measures. Asa result, OLSR is vulnerable to various kinds of attacks [7], [8]such as flooding attack, link withholding attack, replay attack,denial-of-service (DOS) attack [9] and colluding misrelay attack.

This paper proposes an enhanced optimized link state routing approach (EOLSR) to provide the security for MANETs from the denial of service attack called node isolation attack. Node isolation attack is occurred for the target node by the attacker after observing the network activity. The proposed EOLSR enhances the security by verifying the hello packets from all of its neighboring nodes coming from a new node before selecting it as a multi-point relay (MPR) node for forwarding the packets.

The remainder of this paper is organized as follows: section 2 gives the complete details about the earlier approaches proposed on the security issues of OLSR. Section 3 gives the details of OLSR approach and the proposed EOLSR is described in section 4. Section 5 gives the illustration about numerical evaluation of proposed EOLSR and finally conclusions are provided in section 6.

2 RELATED WORKS

In earlier there are so many approaches are proposed to provide and to enhance the security of OLSR. Among them few approaches are discussed here.

A hybrid secure approach for OLSR was proposed in[10]. It's using The Hash Chain for providing the security to the

- *Anurath Mane is currently pursuing masters degree program in computer science engineering in Vidyalankar Institute of Technology,Wadala(E)Mumbai,India, E-mail:anurathmane@gmail.com*
- *Deepali Vora is currently Working as Asst Prof. in Vidyalankar Institute of Technology,Wadala(E)Mumbai,India, E-mail: deepali.vora@vit.edu.in*
- *Shailendra Kelkar Ex Assoc Prof. in Vidyalankar Institute of Technology,Wadala(E)Mumbai,India E-mail:shailendra.kelkar@gmail.com*

routing protocol. [10]Calculates the Hash of some Initial value up to total no of Hop count and distribute it to the entire network. And the sender node sends the one time hash of initial value to the next neighbour which is MPR of it. Now the intermediate node calculate the difference of TTL and Hop count and doing the hash of received hash value up to calculated difference time. If both the value is same then there is no malicious node changed the value in between them. If both the value is not same then there is some malicious node and it changed the value of Hop count and TTL for making the path to itself.

Another secure approach for OLSR based on signature scheme was proposed in [11] and the signature scheme and the approach provide the authentication between the two nodes. For providing the signature the approach uses the two functions. To prevent malicious nodes from injecting incorrect information into the OLSR network, the originator of each control generates an additional security element called signature message and transmitted with the control message. A timestamp is associated with each signature in order to estimate message freshness. Thus, upon receiving the control message, a node can determine if the message originates from a trusted node, or if message integrity is preserved. Signatures are separate entities from OLSR control traffic: while OLSR control messages perform the purpose of acquiring and distributing topological information, signatures serve to validate information origin or integrity.

[12] Proposed a secure OLSR approach in two stages, encryption and hash chain. According to [12] when a node is identify in the routing table then it send the encrypted nonce (a fixed length input) to that node if the node respond back with correct nonce that it is the node which have the encrypted else a node which have not the key can't send back the response, and if the node receives the correct response than mark it as symmetric node. Hash chain is used in the OLSR routing protocol for security from other attacks.

[13]Proposed an efficient OLSR routing approach by incorporating a security solution that defends the network against malicious nodes by rewarding proper routing behavior and thus assuring effective cooperation between communicating parties. The main novelty of [13] is the ability to correlate two sources of traffic information: (1) the (unreliable) monitoring of whether neighbors relay packets sent to them and (2) the paths traversed by successfully delivered packets. It argues that the latter increases the network's ability to detect misbehaving nodes. Although the proposed approach analysis of these security issues, which includes a thorough review of related work and taxonomy of system vulnerabilities, is mainly focused on the OLSR protocol, the described problems and the proposed solutions are equally applicable to other common routing protocols for MANETs.

[14] Proposed an OLSR routing approach is to identify and formalize trust assumptions that are implicitly used by the standard OLSR protocol. One of the goals of [14] is to propose extensions to OLSR in order to make it more flexible to the variations of the environment and more resistant against security treats, while avoiding excessive restrictions on the auto-organization capacities and the dynamics of the network. For this purpose, this begins from the idea of trust classification, which consists of a delimitation of the circumstances where a trust relationship is established, and it analyzes the classes of trust present in OLSR. Initially, [14] present the language used to formally express trust clauses and the definition of trust subjacent to this language. Then, it exposes the general characteristics of the OLSR protocol and its security problems. Finally, it presents the OLSR implicit trust clauses and analyzes the attacks against this protocol according to these implicit clauses.

3 OPTIMIZED LINK STATE ROUTING & DOS ATTACK

3.1 OLSR

OLSR is a table-driven pro-active protocol. As the name suggests, it uses the link-state scheme in an optimized manner to diffuse topology information. In a classic link-state algorithm, link-state information is flooded throughout the network. OLSR uses this approach as well, but since the protocol runs in wireless multi-hop scenarios the message flooding in OLSR is optimized to preserve bandwidth. The optimization is based on a technique called Multi-Point Relaying (MPR). OLSR defines three basic types of control messages, HELLO, TC (topology control) and MID (Multiple Interface Declaration). A HELLO messageis the message that is used for neighbor sensing and MPR selection. In OLSR, each node generates HELLO message periodically(every HELLO INTERVAL). A node's HELLO messagecontains its own address and the list its 1-hop neighbors.A TC message is the message that is used for route calculation.In OLSR, each MPR node advertises TC message periodically(every TC INTERVAL).

OLSR uses flooding of packets to diffuse topology information throughout the network. Flooding, in its simplest form, means that all nodes re-transmit received packets. To avoid loops, a sequence number is usually carried in such packets. This sequence number is registered by receiving nodes to assure that a packet is only retransmitted once. If a node receives a packet with a sequence number lower or equal to the last registered retransmitted packet from the sender, the packet is not retransmitted.

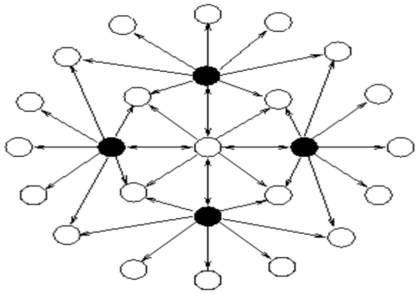

Fig.1. Flooding a packet in a wireless multi-hop network from the center node using MPRs(black). The arrows show all transmissions.

OLSR uses a very simplified version of a neighbor discovery session using HELLO messages. A first sends an empty HELLO message. B receives this message and registers A as an asymmetric neighbor due to the fact that B cannot find its own address in the HELLO message. B then sends a HELLO declaring A as an asymmetric neighbor. When A receives this message it finds its own address in it and therefore sets B as a symmetric neighbor. This time A includes B in the HELLO it sends, and BregistersA as a symmetric neighbor upon reception of the HELLO message.

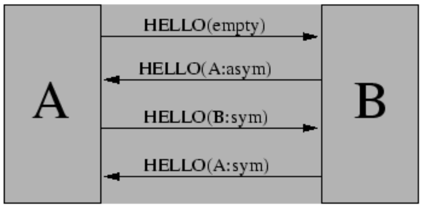

Figure 2: A typical neighbor discovery session using HELLO messages

OLSR protocol performs the link state advertisement with the help of TC messages. TC messages are flooded using the MPR optimization. This is done on a regular interval, but TC messages are also generated immediately when changes are detected in the MPR selector set. In OLSR the flooding process itself is optimized by the usage of MPRs.

3.2 NODE ISOLATION ATTACK

Here we present a node isolated attacks which can results in denial-of-service against OLSR protocol. The goal of this attack is to isolated a node from communicating with other node in the network more specifically this attack prevent the victim node from receiving data packets from other node in to the networks. The idea of this attack is that attackers prevent link information of a specific node, the group of nodes. From being spread to the whole network. Those other node who could not receive the link information of the target node will not be able to build a route to the target node and hence will not able to send data to these nodes.

In this attack, attackers create a virtual link by sending fake HELLO message including the address list of target nodes 2-hop neighbors. (The attacker can learn its 2-hop neighbors by analyzing the TC message of its 1-hop neighbors.) According to the protocol, the target node will select attacker to be its only MPR. Thus the only node that must forward and generate TC message from the target node is the attacking node. By drooping TC message received from the target node and not generating the TC message for the target node, the attacker can prevent the link information of the target node for being disseminated to the whole network. As a result, other node would not be able to receive link information of a target node will conclude that a target node doesn't exist in the network. Therefore, a target node's address will be removed from the other node's routing tables. Since in OLSR, through HELLO message each node can obtain only information about its 1-hop and 2-hop neighbors, other node that are more than 2-hopes away from the target node will not be able to detect the existence of the target node. As a consequence, the target node will be completely prevented from receiving data packets from nodes that are three or more hops away from it.

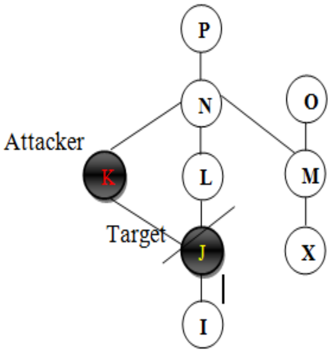

Figure .3. Node Isolation Attack (a) Topology Perceived by Node P before the Attack

In Figure 3 Node K is attacking node, and Node J is target node. Instead of sending correct HELLO message {J,N} in neighbors address list the attacker send a fake Hello message that contains{J,N,O,A} which include the target nodes all 2-hop neighbors {N,O} and one non-existing node {A}. According to the protocol, the target Node J will select the attacker K as it's only MPR being Node J's the only MPR, the attacker refuse to forward and generate a TC message for Node J. since the link information of the Node J is not propagated to the entire network. Other nodes whose distance to Node J is more than two hopes (e.g., Node P) would not be able to build route to Node J as show in figure 4. As a result, other node would not be able to send data to Node J. despite being in the network, and the target Node J will be isolated from the network. An attacker can launch this attack, as long as the target node is within its transmission range.

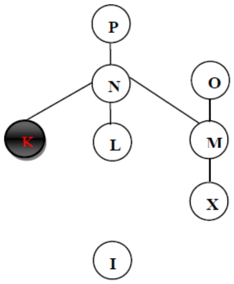

Figure 4. Topology Perceived by Node P after the Attack

An attacker can launch this attack, as long as the target node is within its transmission range.

4. PROPOSED APPROACH

In previous work (EOLSR) node isolated attack is detected but we cannot prevent it from choosing the same attacker node as MPR in future. So we proposed a further improved technique for Enhanced OLSR using the trust based system. Initially all the nodes are assigned high trust value (1.0). Each node maintains the trust value based on the trust value of its neighbors. Then trust value of the nodes is varied according to the activity of the nodes in the network. MPR node is selected based on the trust value of the node. Once the node is detected as attacker using EOLSR, its trust value is reduced to half of its initial value (0.5). Hence in future, selection of attacker as MPR node is prevented since all the nodes will select only high trust node as MPR node. Our method uses HOP_INFORMATION table, 2-hop request and 2-hop reply. Generally, OLSR nodes trust all information that received from its 1-hop neighbor. Here we analyze the pattern of Hello message of the node that advertise all 2-hop neighbors as its 1-hop neighbors and verify whether that node is malicious or not. If we found it as malicious then we will assign its trust value as zero. In OLSR, TC and HELLO message are used to select MPR and route calculation. Each node must broadcast periodically HELLO message to indicate its existence. In this mechanism, each node maintains HOP_INFORMATION Table which contains of HELLO message sender and its 2-hop neighbors. In Figure 5, I selects J, K and L as MPR to broadcast packets to M, N, and O and maintains HOP_INFORMATION table show in Table 1.

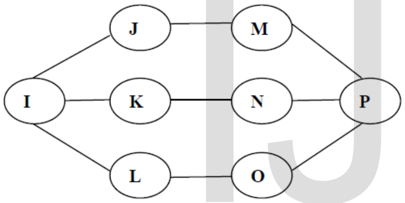

Figure.5. OLSR Nodes, I Selects J,K,L as MPR

TABLE 1
HOPS INFORMATION

HELLO message sender	2-hop neighbors
J	M
K	N
L	O

In Figure 6, if new node Z sends HELLO message as shown in table 5.2 advertising all the target node's 2-hop neighbors as its 1-hop neighbors along with a new neighbor A. then I add Z's 1-hop information in I's HOP_INFORMATION Table as show in Table 3.

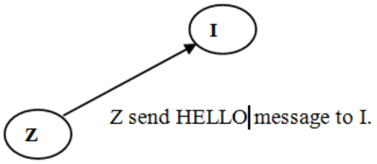

Figure 6. Z advertise its Neighbor to I

TABLE 2
Z's HELLO MESSAGE

Originator	Neighbors
Z	M,N,O,A

TABLE3
I'S HOP_INFORMATION TABLE AFTER RECEIVING Z'S HELLO MESSAGE

HELLO message sender	2-hop neighbors
J	M
K	N
L	O
Z	M,N,O,A

After including Z's information, (Figure 7) A send 2-hop request to its 1-hop neighbors J,K,L and then the node J,K and L forward 2-hop request to their 1-hop neighbor M,N,O to verify whether node Z in its HOP_INFORMATION Table.

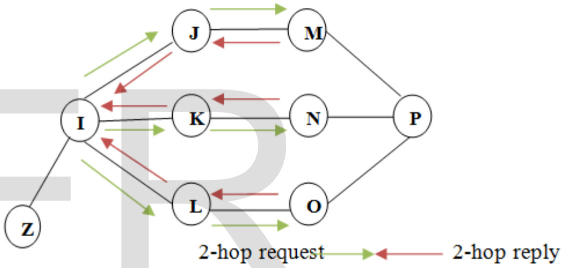

Figure.7. I Send 2-hop Request to J, K, L then J, K, L Send Request to M,N,O and M,N,O Send 2-hop Reply to I Through J,K,L.

If node Z founds in the table, then M,N,O sends 2-hop reply to I through J,K,L indicating Z is its 1-hop neighbor. If so, I will select Z as a MPR and broadcast through Z. otherwise I add Z in Blacklist and discard its HELLO message. Node I then informs about the presence of malicious node Z to the network through HELLO and TC messages.In other case, if node Z is actually be in the coverage area of M,N,O nodes, then the target node I queries about the existence of node Z in the networks through the NEQ message forwarded through its current MPR nodes. If any designated MPR node in the network confirms the existence of node Z, then node Z will be selected as MPR, otherwise, it will be confirmed as a malicious node.

5. SIMULATION RESULTS

This section gives the complete details about the simulation results of the proposed approach. Simulation was performed using NS-2 (network simulator). The performance of proposed approach is measured by evaluating throughput, packet loss and control packets with varying number of attackers. The proposed work was also compared with EOLSR with respect to all above mentioned performance parameters. Simulation results obtained are shown below:

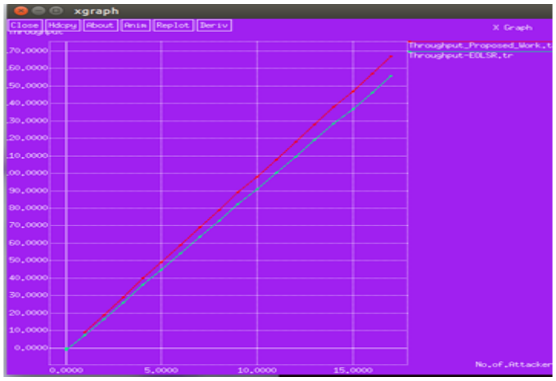

Fig. 8.Number of attacker's v/s throughput

The above plot shows the through performance of proposed approach with varying number of attackers. Form the above figure it is clear that, for a given number of attackers, the throughput of the proposed approach is better than EOLSR.

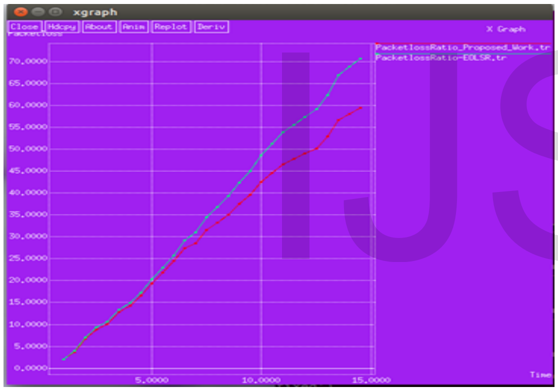

Fig.9. Time versus packet loss

The above plot shows the packet loss performance of proposed approach with varying time. Form the above figure it is clear that, for a given time, the packet loss of the proposed approach is less compared to EOLSR.

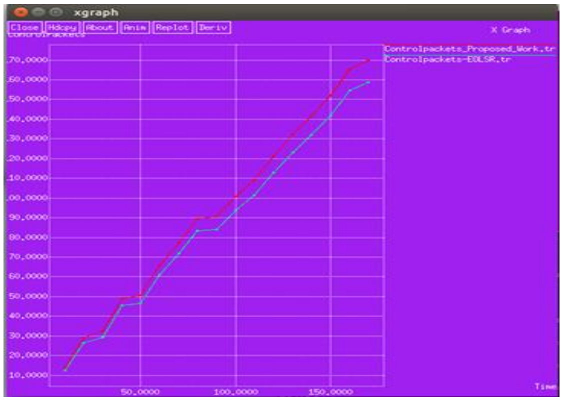

Fig.10. Time versus control packets

The above plot shows the control packets performance of proposed approach with varying time. Form the above figure it is clear that, for a given time, the control packets of the proposed approach are high compared to EOLSR.

6 CONCLUSIONS

This paper proposed a protocol that provides a defense mechanism against the DOS attack in OLSR MANET protocol.The proposed work aims at preventing the network from this attack by means of verification scheme of hello packets coming from neighbor nodes to detect the malicious nodes and by maintain the trust values for each node in the network. The experiment results show that the percentage of packets received through the proposed work is better than OLSRin presence of multiple attacker nodes.Compared to other related works, the proposed protocol has more merits; the most important merit is that it achieves degradation in packet loss rate without any computational complexity or promiscuous listening.

REFERENCES

[1] Stefano Basagni, Macro Conti, Silvia Giordano and Ivan Stojmenovic, "Mobile Ad Hoc Networks" , IEEE press, A john Wily & Sons, INC. publication, 2003

[2] ImrichChlamtac, Marco Conti, Jenifer J.-N. Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges", Elsevier Network Magazine, vol. 13, pages 13-64, 2003

[3] E.M. Belding-Royer and C. K. Toh, "A review of current routing protocols for AdHoc mobile wireless networks", IEEE Personal Communications Magazine, pages 46–55, April 1999.

[4] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-SequencedDistance-Vector Routing (DSDV) for Mobile Computers," Comp. Commun.Rev., Oct. 1994, pp. 234–44.

[5] D.B. Johnson, D.A. Maltz, "Dynamic source routing in adhoc wireless networks",in: T. Imielinski, H. Korth (Eds.), Mobile Computing, Kluwer AcademicPublishers, Dordrecht, 1996, pp. 153–181.

[6] T. Clausen and P. Jacquet, "IETF RFC3626: Optimized link state routing protocol (OLSR)," Experimental, 2003.

[7] T. Clausen and U.Herberg, "Security issues in the optimized link staterouting protocol version 2 (OLSRv2)," Int. J. Netw. Security Appl., 2010.

[8] B. Kannhavong, H. Nakayama and A. Jamalipour, "A study of routingattack in OLSR-based mobile ad hoc networks," Int. J. Commun. Syst.,2007.

[9] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour,"Analysis of the node isolation attack against OLSR-based mobile ad hocnetwork," in Proc. ISCN, 2006, pp. 30–35.

[10]. A.M.Hagland, P.Spilling, L.Nilsen and Q.Kure; "Hybrid Protection of OLSR", Electronic Notes in Theoretical Computer Science 2006.

[11]. AmanpreetKaur, GurpreetKaurDeol; "Secure Optimized Link State Routing Protocol", 2006.

[12] M.Sathyam Reddy, " Quantitative Study and Comparison of Secure OLSR Routing Protocol", S Tamilarasan et al,Int.J.Computer Technology &Applications,Vol 3 (2), 632-638

[13] Joao P. Vilela and Joao Barros, "A Cooperative Security Scheme for Optimized Link State Routing in Mobile Ad-hoc Networks".

[14] AsmaaAdnane, Rafael Timoteo de Sousa Jr, Christophe Bidan, and Ludovic Me, "Analysis of the implicit trust within the OLSR protocol".