Detection And Elimination Of Denial Of Service Attack In OLSR Protocol Using Fake Nodes

Akhil S[1], Amalkanth P Raveendran[2], Vishnu S N[3], Aby Abahai T[4], Surekha Mariam Varghese[5]

[1,2,3]Students,Dept of computer science and engineering Mar Athanasius College of Engineering,
[4]Assistant Professor, Dept of computer science and engineering Mar Athanasius College of Engineering,
[5] Professor and HOD Dept of computer science and engineering Mar Athanasius College of Engineering

---

Abstract— *With the main focus of research in routing protocols for Mobile Ad-Hoc Networks (MANET) geared towards routing efficiency, the resulting protocols tend to be vulnerable to various attacks. Over the years, emphasis has also been placed on improving the security of these networks. Different solutions have been proposed for different types of attacks, however, these solutions often compromise routing efficiency or network overload. One major DOS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack occurs when topological knowledge of the network is exploited by an attacker who is able to isolate the victim from the rest of the network and subsequently deny communication services to the victim. In this paper, we suggest a novel solution to defend the OLSR protocol from node isolation attack by employing the same tactics used by the attack itself. Proposed method can successfully prevent most of the node isolation attacks prevalent in OLSR protocol.*

***Key Words*: OLSR, DOS, MANET, Ad-hoc, NS2, TCL**

INTRODUCTION

With the rise of networking, need for efficient and effective protocols emerged. Two type of protocols are static and dynamic protocols. Static protocol stores manually created routes and is used for routing. Dynamic routing protocol uses routing table which is updated dynamically based on the specific protocol used. Distance vector and link state routing protocols belong to dynamic routing protocols. Distance vector means that routes are advertised by providing two characteristics. They are Distance, which identifies how far is the destination network and Vector which Specifies direction of the next hop router or exit interface. Examples of distance vector protocols are RIP and EIGRP. In contrast to distance vector routing protocol, a link state routing protocol can create a complete view or topology of a network by gathering information from all other routers. For example OSPF and OLSR.

Idea of proactive and reactive routing protocols created two categories of protocols. Proactive routing protocols (Table driven protocols) keeps a record of list of all possible destination nodes and routes towards each destination nodes. Requirement of a mobile AD-hoc network is the ability to recognize the nodes by other participant nodes in motion. Mobile Ad-hoc network can undergo frequent topology changes due to its mobile nature. Intermediate node can break the routes between two nodes during transition.

Basic idea behind the working of a link state routing protocol is the cooperation between the nodes. Each nodes shares the basic details of themselves with other neighboring nodes, which can then be used to find the best path to destination and then send packets via those routes. A new routing protocol called optimized link state routing protocol was developed later which works in a much efficient way, overcoming the drawbacks of its predecessors. OLSR protocol being a widely used protocol can have less tolerance to attacks. Various kind of attacks were found to be successful on an OLSR network namely, link spoofing, flooding, worm hole, denial of service etc.

OLSR PROTOCOL

Optimized link state routing protocol is an optimized form of link state routing protocol. Link state routing protocol is also a proactive routing protocol, but it uses the technique of flooding to communicate with other nodes. A node sends message to all of the nearby nodes resulting in wastage of bandwidth and many other factors. OLSR protocol on the other hand selectively retransmit messages based on a set of rules. Here comes the idea of Multi point relays (MPR). MPR of a sender is the set of nodes in the 1-hop of the sender which are connected to a maximum number of 2-hop neighbors of the sender. Moreover, the sender should be able to contact all of its 2-hops via the nodes listed as its MPR.

Both hello packets and data packets are send via the MPR network so that duplication can be avoided and at the same time maintains a network wide coverage. Two types of messages used to maintain topology control are HELLO messages and Topology Control (TC) messages.

Hello messages carrying the information about the environment are broadcast to all nodes via MPR nodes of the sender. Any node that can hear the broadcast and reciprocate back to the sender is classified as a 1-hop neighbor. Consequently, each node acquires its local topology up to a 2-hop range. In addition, OLSR requires that all nodes selected as MPRs periodically advertise a TC message listing all nodes that have selected the sender as its MPR. These control messages are only propagated through the MPR super-network, reducing overall network traffic.

Network topology is maintained using these messages and calculate the shortest or best path to the MPR of the destination node.

Node isolation attack, which is a specific denial of service attack, being a major attack on such protocols can be identified and eliminated using the internal knowledge about network topology stored in each nodes. Basic idea used by the attacker node itself is used here to identify the attacker node and eliminate the attacker node from routing tables.

NODE ISOLATION ATTACK IN OLSR

In [15], Kannhavong et al. proposed a Denial of Service (DOS) attack against OLSR called node isolation attack. In this attack, an attacker exploits the fact that the victim prefers a minimal MPR set in order to hide the existence of the victim in the network. The attacker, which must be located within broadcast distance of the victim, advertises a fake HELLO message claiming to be in close proximity to all of the victim's 2-hop neighbors. In addition, a fictitious node is advertised, giving the attacker an advantage over other possible legitimate candidates for MPR selection. Knowledge of the victim's 2-hop neighbors is readily available by analyzing TC messages of the victim's 1-hop neighbors, a list of which can be constructed directly from the HELLO message broadcast by the victim himself. MPR selection rules would cause the victim to exclusively select the attacker as its sole MPR, as it is the minimal set that allows for coverage of all of the victim's 2-hop neighbors (including the fictitious node). DOS is now straightforward. The attacker can isolate the victim simply by not including the victim in its TC message.

In essence, the attacker refrains from notifying the network that the victim can be reached through it, and because no other node advertises a path to the victim, it is isolated. Other nodes, not seeing link information to the victim, would conclude that it has left the network, and remove its address from their routing tables. Although nodes 1- and 2-hops from the victim would continue to exchange information with it, they will not propagate that information further as they were not designated as its MPR.

The node isolation attack is illustrated by Figure 1. Assume all nodes within broadcast distance have an edge connecting them, that node x is the attacker, that Fx is a fictitious node, and that node b is the victim. The cloud in the Figure represents the rest of the network. OLSR rules state that x should have advertised a legitimate HELLO message containing {b; f}. Instead, it sends a fake HELLO message that contains {b; f; g; Fx}. This list contains all of b's 2-hop neighbors, as well as one non-existent node, Fx. b would now innocently select x as its sole MPR, setting the ground for node isolation. By not advertising b in its TC message, x effectively isolates b from the rest of the network.

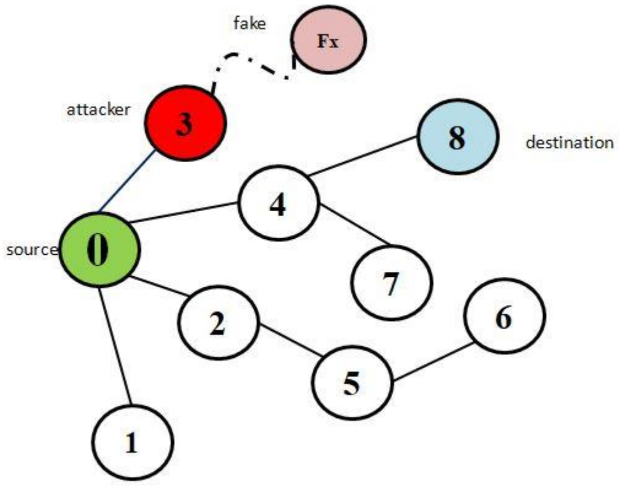

Fig -1: Node Isolation Attack in OLSR

RECOVERY

To prevent the attack the sender (0) in made to run in a secure mode. In this secure mode all 1-hop neighbors of the sender creates fake nodes (F2, F3, F4) to itself (as 2-hop to the victim node) and advertises to all other nodes. While the attacker (3) enters the communication, it identifies the 2-hope nodes of the victim and enters the same in its 1-hope neighbour tuple. But in the secure mode the attacker will also add the fake nodes created by sender's 1-hop. When the attacker publishes its information with any fake nodes created by sender's 1-hop we can identify the node as an attacker and deny the same node from participating in MPR selection and in routing table and thus by choosing an alternative route with secure communication.

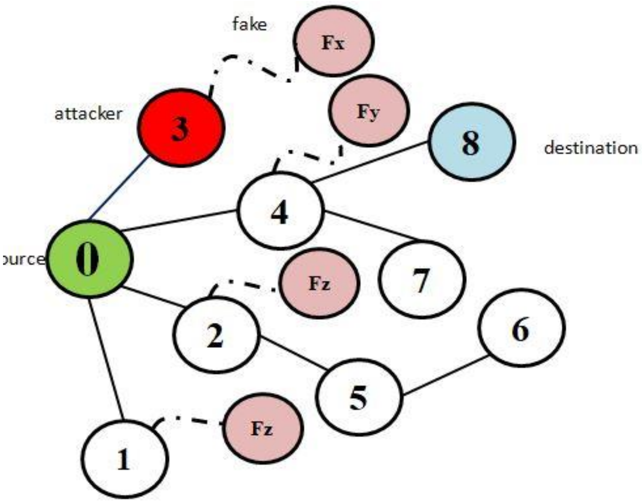

Fig -2: Recovery Of DOS Attack In OLSR

ANALYSIS

Attack and recovery phases are simulated in ns2 and the result is analysed using graphs, throughput and drop .Analysis is done in 3 stages. At the first stage a normal OLSR protocol is implemented. In the second stage a dos attacker is added to the topology and in the final stage sender is made to run in secure mode. At each stage the throughput of the destination node (8) and drop by attacker node (3) is calculated and graphs are plotted for the same.

Ns2 is a network simulation tool which can be used to simulate various networking scenarios. It contains various tools, network animator and Xgraph used to animate a simulated network. Xgraph is used to plot the graph which shows the final result of analysis. The output from ns2 is a trace file which contains large amount of data. Required information is extracted from this trace file using scripting languages like awk and perl. Three stages of analysis of a network topology implementing OLSR protocol is as follows.

Stage 1: Normal OLSR

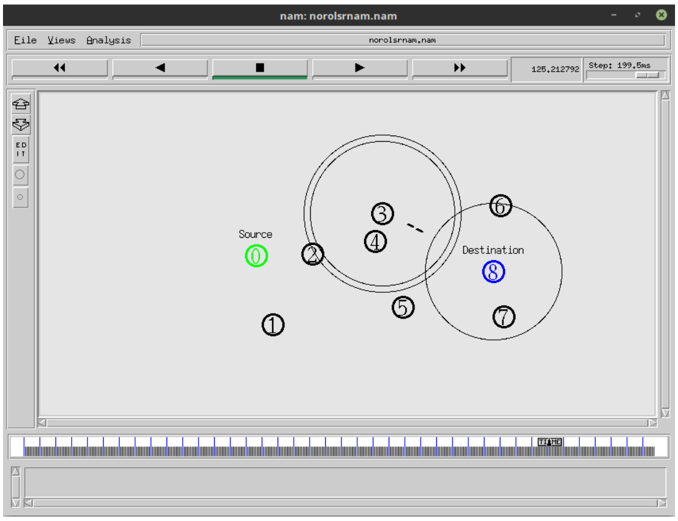

Fig -3: Nam Output of Normal OLSR

In figure 3 a topology is created in which OLSR protocol is implemented, CBR packets are sent from node 0 to node 8. At this stage node 3 is a normal node and acts as an intermediate hop for the communication. Here, node 0 which is the sender selects node 3 as its MPR to reach node 8 using OLSR protocol's MPR selection properties. Any node that can hear the broadcast and reciprocate back to the sender is classified as a 1-hop neighbour. Consequently, each node acquires its local topology up to a 2-hop range. In addition, OLSR requires that all nodes selected as MPRs periodically advertise a TC message listing all nodes that have selected the sender as its MPR. These control messages are only propagated through the MPR super-network, reducing overall network traffic. Network topology is maintained using these messages and calculate the shortest or best path to the MPR of the destination node

Throughput of the destination node (8) is given by figure 4 with time in ms along x axis and throughput in Mbps along y axis. Throughput value obtained in the case of normal OLSR is 163.265 Mbps in a time span of 150ms.

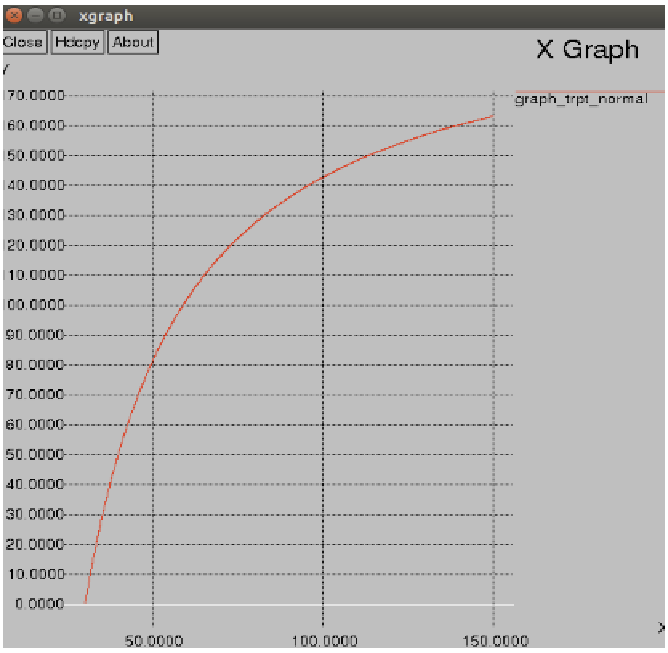

Fig -4: Throughput of destination node plotted in Xgraph

Stage 2: Attacker Introduced

In this topology represented in figure 5 node 0 is the sender and node 8 is the destination. Node 3 is an attacker node which when introduced into the network act as a MPR of the sender and receives all packets from the victim node. Attacker node does not forward any of the received packets to destination. Hence it act as a black hole node [7].

Throughput of the destination node (8) plotted in Xgraph is given in figure 6 with time in ms along x axis and throughput in Mbps along y axis. Throughput value obtained is 0 Mbps in a time span of 150ms. Which implies that none of the packets were received by the destination node.

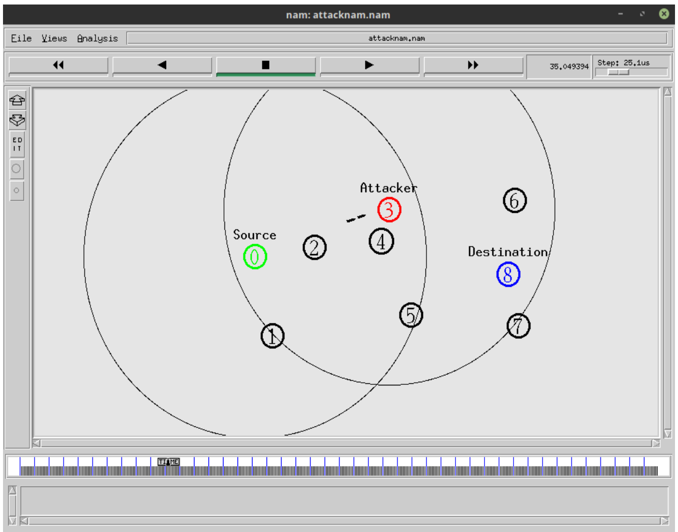

Fig -5: NAM output of DOS attack in OLSR

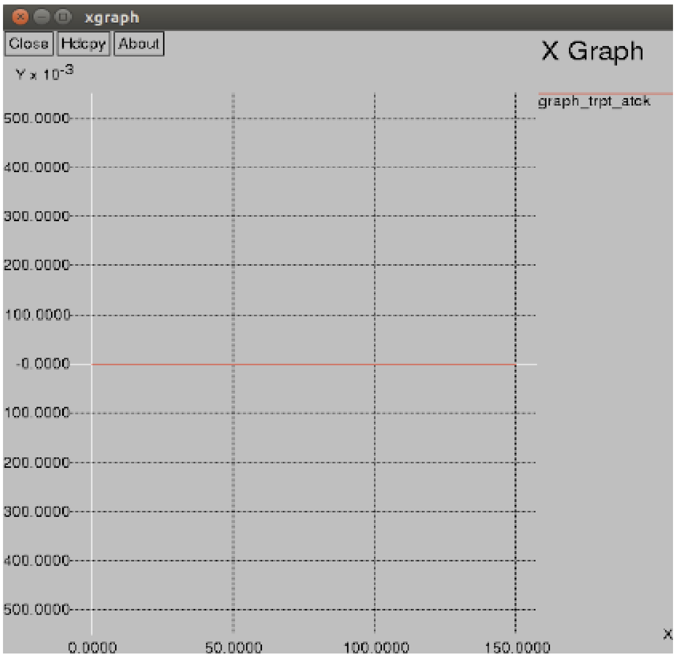

Fig -6: Throughput of destination node

Drop of packets by the attacker node (3) is given by figure 8 with time in ms along x axis and number of packets dropped in each 1000 packets along y axis. Total number of packets dropped by the attacker node is obtained as 1500 which implies that none of the packets has reached the destination.

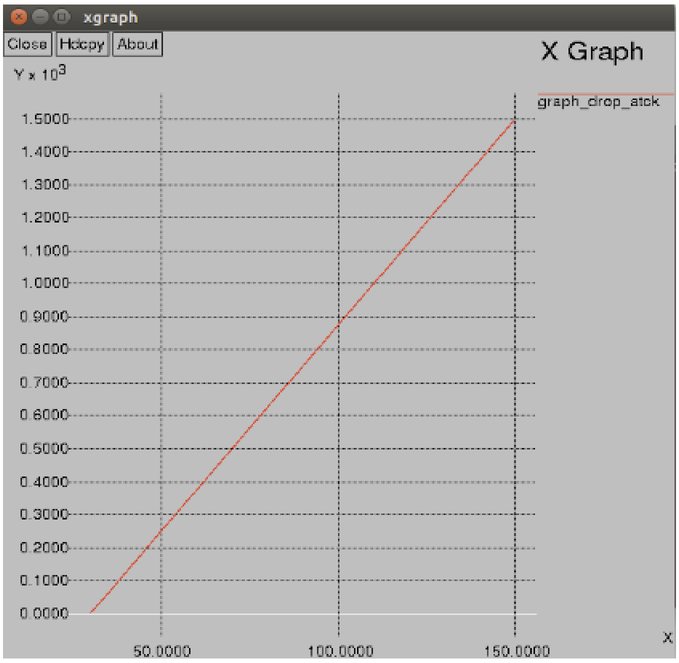

Fig -7: Packets dropped by attacker against time

Stage 3: Sender Run in Secure Mode

Figure 8 shows the sender node run in secure mode. Hence 1-hops of the sender creates a secure path for communication between source and destination. In the above topology packets from node 0 does not reach attacker node (3) instead they are redirected through node 4

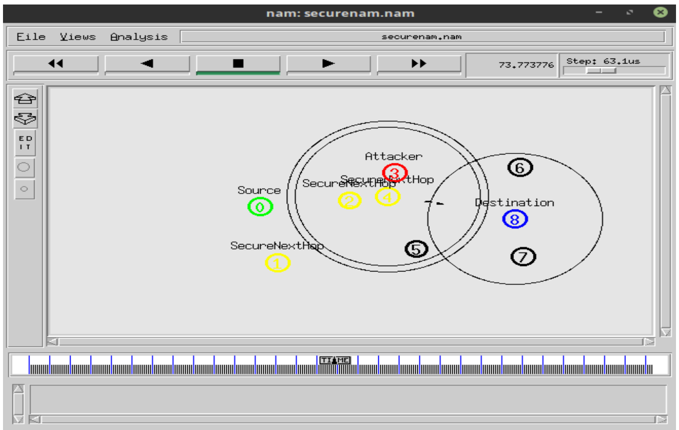

Fig -8:NAM output of sender running in secure mode

Throughput of the destination node (8) is given by figure 9 with time in ms along x axis and throughput in Mbps in y axis

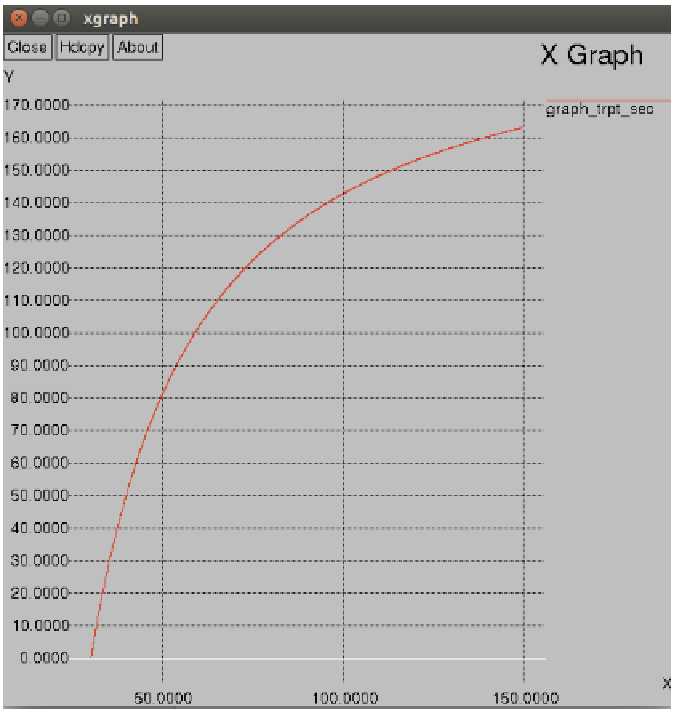

Fig -9: Throughput of destination node

From figure 9 it is clear that the throughput of destination node brought back to its previous value of 163.265 Mbps

Drop of packets by the attacker node (3) is given by figure 10 with time in ms along x axis and number of packets dropped along y axis

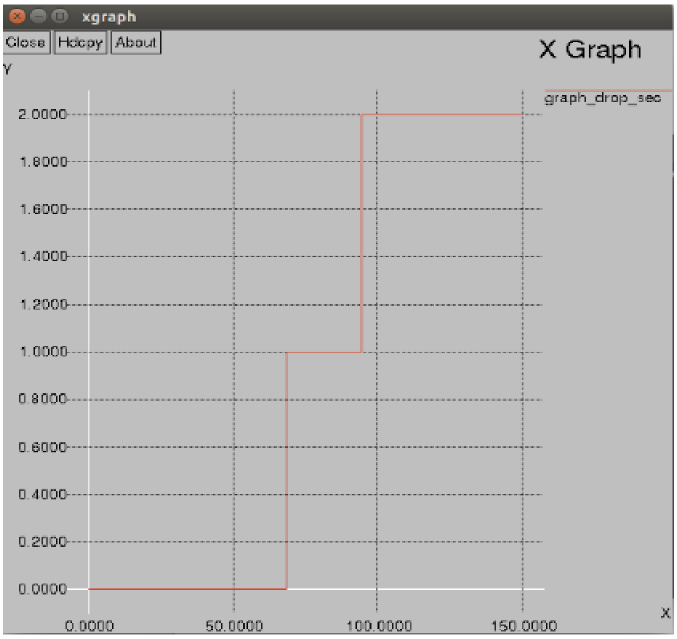

Fig -10: Packets dropped by attacker

Result:

Simulation of a number network topologies which uses OLSR protocol shows that the proposed method to detect and eliminate DOS attack is effective. Proposed method belongs to prevention based approach, since it prevents attack by not appointing the attacker as MPR. Each simulation was tested with and without attack to find the difference in number packets dropped by attacker and the throughput of the destination. For small networks the addition of fake node adds an overhead to the OLSR protocol but as node density increases the average number of fictitious nodes required decreases.

From the analysis of the network simulation number of packets dropped by the attacker node is reduced from 1500 packets to 2 packets in 150 ms. And also the throughput of the destination node was brought back to 163.265 Mbps. When the topology was simulated with normal OLSR protocol, the drop was absent. Second stage of the work introduced an attacker node which dropped all of its packet and the value of drop was raised to 1500 packets and throughput was drastically reduced. Third stage of work introduced a mechanism for identifying the attacker node using the same tactic followed by the attacker node and later traffic was successfully rerouted to next node in the MPR set of sender. This step successfully restored the throughput and reduced the drop to 2 packets in a time span of 150 ms.

CONCLUSION:

In this paper, we have presented a solution to identify and eliminate DOS attacker nodes in a network which uses OLSR protocol. It prevents the node isolation attack in which the attacker manipulates the victim into appointing the attacker as its MPR, giving the attacker control over the communication channel. This method makes use of the tactic followed by the attacker itself to gain control over the network. By learning local topology and advertising fictitious nodes, a node is able to deduce suspect nodes and refrain from nominating them as MPR, thus overcoming the attacker's attempt to gain control over network.

REFERENCES:

[1] S. Mclaughlin, D. Laurenson, and Y. Tan, "Mobile ad-hoc network," Aug. 10 2006, uS Patent App. 11/351,777. [Online]. Available:
http://www.google.com/patents/US20060176829

[2] C. E. Perkins and P. Bhagwat, "Highly dynamic destination sequenced distance-vector routing (dsdv) for mobile computers," in Proceedings of the Conference on Communications Architectures, Protocols and Applications, ser. SIGCOMM '94. New York, NY, USA: ACM, 1994, pp. 234–244. [Online]. Available: http:
//doi.acm.org/10.1145/190314.190336

[3] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International, 2001, pp. 62–68.

[4] T. Clausen and P. Jacquet, "RFC 3626 - Optimized Link State Routing Protocol (OLSR)," p. 75, 2003. [Online]. Available: http:
//www.ietf.org/rfc/rfc3626.txt

[5] D. Johnson, Y. Hu, and D. Maltz, "Rfc: 4728," The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPV4, 2007.

[6] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, Feb 1999, pp. 90–100.

[7] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tolle,"Detecting black hole attacks in tactical manets using topology graphs," in Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on, Oct 2007, pp. 1043–1052.

[8] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the olsr protocol," in Proceedings of Med-Hoc-Net,2003, pp. 25–27.

[9] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," Wireless Communications, IEEE, vol. 14, no. 5, pp. 85–91, October 2007.

[10] D. Dhillon, J. Zhu, J. Richards, and T. Randhawa, "Implementation & evaluation of an ids to safeguard olsr

integrity in manets," in Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing, ser. IWCMC '06. New York, NY, USA: ACM, 2006, pp. 45–50. [Online]. Available: http://doi.acm.org/10.1145/1143549.1143560

[11] D. Raffo, C. Adjih, T. Clausen, and P. Mühlethaler, "An advanced signature system for olsr," in Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks, ser. SASN '04. New York, NY, USA: ACM, 2004, pp. 10–16. [Online]. Available: http://doi.acm.org/10.1145/1029102.1029106

[12] C. Adjih, D. Raffo, and P. Mühlethaler, "Attacks against olsr: Distributed key management for security," in 2nd OLSR Interop/Workshop, Palaiseau, France, 2005.

[13] Y.-C. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks," Selected Areas in Communications, IEEE Journal on, vol. 24, no. 2, pp. 370–380, Feb 2006.

[14] B. Kannhavong, H. Nakayama, and A. Jamalipour, "Nis01-2: A collusion attack against olsr-based mobile ad hoc networks," in Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE, Nov 2006, pp.1–5.

[15] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Analysis of the node isolation attack against olsr-based mobile ad hoc networks," in Computer Networks, 2006 International Symposium on, 2006, pp. 30–35.

BIOGRAPHIES:

Akhil.S is currently pursuing B.Tech in Computer Science and Engineering in Mar Athanasius College of Engineering. His areas of interests are Network Security and Datastructures.

Amalkanth P Raveendran is currently pursuing Engineering in Mar Athanasius College of Engineering. His areas of interests are computer networks, network security, cloud computing

Vishnu S N is currently pursuing B.Tech in Computer Science and Engineering in Mar Athanasius College of Engineering. His areas of interests are network security, data structures and algorithms, Artificial intelligence

Aby Abahai T is currently assistant professor at Department of Computer Science and Engineering, M.A. College of Engineering, Kothamangalam, Kerala, India. He received his B-Tech Degree in Computer Science and Engineering in 1999 from Calicut University, and M-Tech from NIT Suratkal in 2009. He is a lifetime ISTE member, AICTE affiliation committee member and NBA accreditation committee member. His research interests include Data Structures and Algorithms, Machine Learning. He has published several papers in international journals and international conference proceedings.

Surekha Mariam Varghese is currently heading the Department of Computer Science and Engineering, M.A. College of Engineering, Kothamangalam, Kerala, India. She received her B-Tech Degree in Computer Science and Engineering in 1990 from College of Engineering, Trivandrum affiliated to Kerala University and M-Tech in Computer and Information Sciences from Cochin University of Science and Technology, Kochi in 1996. She obtained Ph.D in Computer Security from Cochin University of Science and Technology, Kochi in 2009. She has around 25 years of teaching and research experience in various institutions in India. Her research interests include Network Security, Database Management, Data Structures and Algorithms, Operating Systems, Machine Learning and Distributed Computing. She has published 17 papers in international journals and international conference proceedings. She has been in the chair and reviewer for many international conferences and journals.