IJITKM Volume 7 • Number 1 • December 2013 pp. 100-103 (ISSN 0973-4414)

Analysis of ANSN Attack on OLSR based MANETs

Suneel kumar[1], Yogesh Chaba[2]
Department of Computer Science & Engineering
Guru Jambheshwar University of Science and Technology
Hisar-125001, Haryana India
suneelduhan26@gmail.com

Abstract
A MANET is a multi-hop ad-hoc wireless network where nodes can move arbitrary in the topology. The network has no given infrastructure and can be set up quickly in any environment. The Optimized Link State Routing (OLSR) protocol is a route management protocols for such mobile ad hoc networks. This study presents the work of implementing ANSN attack on MANETs based on OLSR routing protocols by any malicious node by carrying out malicious activity within the network, forcing other nodes to change their network topology information with wrong information. The attacks were simulated on NS-3-Dev. The observations are made about the number of TC packets being dropped at all the node in topology in normal condition as well as under attack circumstances.

Keywords: MANET, Security, OLSR, MPR, ANSN Attack

1 Introduction

A Mobile Ad hoc network (MANET) is a collection of mobile nodes organized by wireless links without the aid of any fixed infrastructure or federal access point such a base station. In MANET, each node acts both as a host and as a router to onward message for other nodes that are not within the same radio range. The nodes are free to go and from an random topology. This inherent flexibility makes it attractive for application such as emergency operation, disaster recovery military operation sensor network and so on. These features make it hard to deploy security mechanisms similar to that of in wired network. As a result, MANETs are more susceptible than conventional wired network and are susceptible to various kinds of attacks [1].

1.1 OLSR - core functionality

OLSR is a proactive routing protocol for mobile ad hoc networks. It is an optimization of pure link state protocols; it reduces the size of control packet as well as the number of control packets communication required. Key optimization in OLSR is the use of Multi Point Relay (MPR) nodes are controlled traffic flooding. A MPR is a nodes one-hop neighbor which has been chosen to forward packets. Instead of pure flooding of the network, packets immediately forwarded by a node MPRs.. Because of the use of MPRs, the superior and more dense a network, the more optimized link state routing is achieved. MPR helps providing the shortest path to a destination. The requirement is that all MPRs declare the link information for their MPR selectors [7]. A node transmit it message through the network using standard flooding as show in the figure1 (a) where all neighbors relays message transmitted by left most node and MPR flooding show in the figure 1 (b) where only MPR node relay the message.

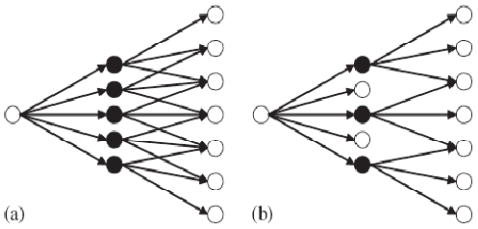

Figure 1 (a) Regular flooding (b) MPR flooding

A node selects MPRs from among its one hop neighbors with "symmetric", i.e., bi-directional, linkages. Therefore, selecting the route through MPRs mechanically avoids the problems linked with data packet transfer over uni-directional links. In OLSR protocol two types of routing message are used, namely, HELLO message and TC message.

A HELLO message is the message that is used for neighbor sense and MPR selection. In OLSR, each node generates HELLO message periodically .A node's HELLO message contains its own address and the list its 1-hop neighbors.

A TC message is the message that is used for route computation. In OLSR, each MPR node advertises TC message periodically. A TC message contains the list of the sender's MPR selector [4].

- Multi Point Relay

In OLSR, only MPR nodes forwarded broadcast traffic. Each node calculates its MPR set by choosing a division of its 1-hop neighbors, such that all its 2-hop neighbor can be reach through this MPR set. Nodes that choose a particular node X as their MPR become MPR selector for X. smaller the MPR set, the lesser is amount of control message traffic generated.

- Neighbor Discovery

HELLO message are generated and transmitted at regular interval to all 1-hop neighbors to get link sensing, neighbor sensing, two-hop neighbor-sensing and MPR selector sensing. Nodes transmit information regarding all know links and neighbors. The node MPR set is also announce link information populates 1 and 2-hop neighbor repositories.

- Link State Declaration

In OLSR, topology information is distributed through the network using topology Control (TC) message. These messages are generated by MPR nodes at regular interval (TC interval) or whenever changes are detected in MPR

selector set. Each MPR nodes advertise links between itself and nodes in its MPR selector set. Advertised Neighbor Sequence Number (ANSN) represents freeness of information contained in the message. MPR optimization is used to flood TC messages in entire network. TC message is used to populates or update topology tuples in TC repository (topology set). After receiving TC message, the topology set is updated as follows:

A. All tuples with seqNo < ANSN are surplus. This is because this information is old. This is the abolition of topology tuples.
B. For every advertised neighbor address received in the TC message: if it's a new updates to already existing information, the validity time of the exiting information is increased. Else, a new tuple is created in the topology set.
C. All tuples past their validity time are removed from the topology set. This is the end of topology tuple.

This paper is organized as follows. First part contains the introduction of MANET's and OLSR routing and different security issues in it. Second section contains the literature survey of different research paper . Third and fourth section contains is about proposed logic and simulation of the work and comparison of result, with existing techniques.

2 Related Work's

Security is an significant feature in MANETs,
especially when they are used in some really critical applications like battlefields or tragedy recovery. Ad-hoc networks are vulnerable to several routing attacks, including address spoofing, alteration of packets, black hole, man-in-the-middle, and dispersed denial-of-service (DdoS).
In most of the previous works on security attacks have mainly focused on Various routing protocols such as OLSR, AODV, DSR etc.

Bounpadith Kannhavong & Abbas Jamalipour [11] and Lalith Suresh [5] have talked about collusion attack against OLSR. it has been presented a technique to detect the attack by utilizing information of two hops neighbors.

Thomas Clausen and Ulrich Herberg, [1] has discussed, Vulnerability Analysis of the Optimized Link State Routing Protocol version 2 problem.

Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharm [2] classifies various types of attacks on MANETs such as Black-Hole, Worm-Hole, Subil, Jellyfish & Rushing attack and their prevention techniques.

Soomro [3] talks about DoS attacks in Ad hoc networks and analytical modeling the scalab-ility of DoS attacks as a function of key performance parameters such as mobility, system size, node density, and counter-DoS strategy. However Very less detail are provided about the practical implementation of attack.

In this paper a detailed studied is presented about an ANSN attacks, the network infrastructure and various observations.

3 Proposed Work

- ANSN Attack

Every TC message has a number called ANSN (Advertised Neighbor Sequence Number). This ANSN number is used to determine the freshness of a TC message. A larger value of ANSN, tells that the information contained by the TC message is latest. As it is well known that in ad-hoc networks the topology keeps changing with time, every time a node generates a new TC message, it puts the ANSN value as 1 additional than the ANSN value of last generated message by this node. This generated ANSN value is kept by the node in order to determine the next ANSN value.

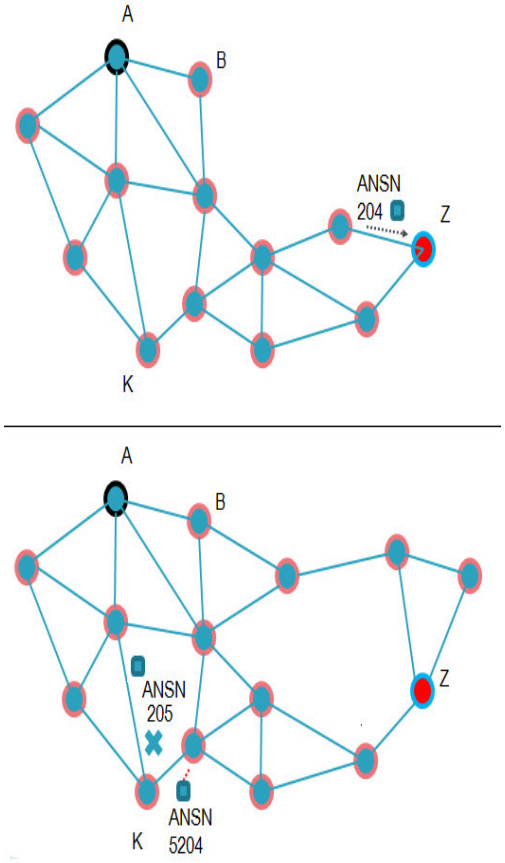

Figure 2: TC message with ANSN 5024 sent by attacker node Z.

Also every node which receives this TC message keeps the ANSN value stored, so that a track of ANSN value received by each node can be kept, which means that every node keeps this information about the latest TC message received from any node in the topology. Though this mechanism is built to reduce redundancy and make OLSR a better routing protocol, there is a loophole in this process. In order to take advantage of this technique, a malicious node Z as show in figure 2 fist listens to a TC message from a particular node

(node A in our case, as per the figure). When it receives the ANSN value, it records the ANSN values (say 204). Now the malicious node will generate a new TC message, which will have its own topology information, but it puts the originator address of node A, from where it received the TC message earlier. Also it puts the ANSN value as much larger (5204) than recorded earlier. It now sends this TC with the spoofed originators address and with an ANSN much larger then recorded. Suppose a node K received this message. Node K will now update the ANSN value corresponding to Node A as 5204. Next time when node A will generate any TC message, it will put ANSN value as 205. But when node K will receive this TC message from node A having ANSN value as 305, it will check with the recorded value against node A. And when it will find that it is very less than recorded one (205<<5204), it immediately discards the TC message. Now any further TC message by the victim node (node A) will be discarded by other nodes having new forged ANSN. As a result wrong topology information will keep on spreading in the network for a long period of time and most of the nodes will update their topology tables with wrong information. As a result there will be a sudden drop in TC messages and data packets would also be dropped as a result. In the following section a simulation of ANSN attack on NS-3-Dev which has OLSR functionality included is described. The major task is to understand the functioning of OLSR, identify the area which are needed to be exploited and make it work according to attack requirements. Basically the primary target was to create a malicious node who would carry out malicious activity. So a manipulation was done in the OLSR in such a way that whenever a particular node will receive any TC message from another nodes, the attacker node would check for the originator address, if it is our desired node (victim), attacker node would record the ANSN value & the originator address. After having received a TC message, OLSR calls a function which creates a new TC message. Here at this point another manipulation was done to put a spoofed originator address and ANSN value much higher than recorded earlier by attacker node. Thus all the surrounding nodes would receive TC message with originator address as victim's address. They would update their routing table as per the incorrect topology information. Now any legitimate TC message from the victim would be discarded in near further as all nodes would have ANSN values in their records much higher than the currently received ANSN value.

In this paper ANSN attack is implemented on MANET having grid topology. Initially starting with 25 nodes and further increasing the grid size up-to 49 nodes. The observation were made of the number of TC packets being dropped at all the node in topology in normal condition as well as under attack circumstances.

4 Results and Discussion

On the basis of the observations made during several runs of the simulated attack, the following results are calculated. The attacks were simulated on NS-3-Dev, with 4, 5, 6, 7 grid topology of size 16, 25, 36 and 49 nodes. All the nodes were having a range of 500 meter. Default packet size was set as 500 byte. Packet sending interval was 1 second. With the help of tables and graphs below, the statistics about the simulation are explained.

Node	TC Drop
16	69
25	73
36	136
49	287

Table 1: TC Packet Drop, time = 100 seconds

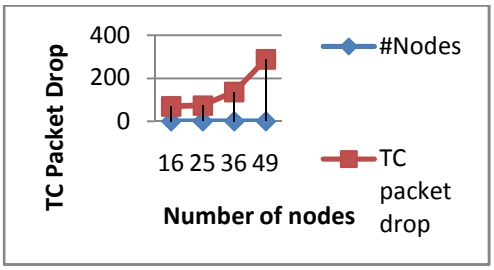

Figure 3: No. of TC packet drops, time =100 seconds

It was observed that for smaller topologies, the impact of attack is less in comparison with larger topologies. Table 1 and figure 3 above show that for 16 and 25 nodes TC drops are less however a significant increase in TC drops is clearly visible for larger topology.

Node	Attack
16	0
25	49
36	73

Table 2: Data Packet drop, Time=100 seconds

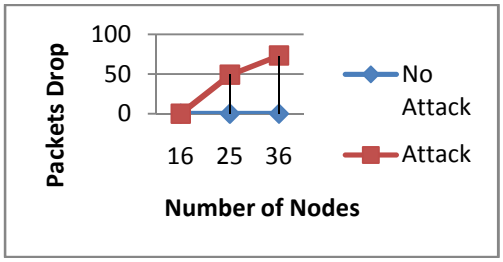

Figure 4: Data Packet drop, time=100 seconds

Figure 4 shows the comparison between attack and normal scenario for 16, 25 and 36 nodes topology. It is clear from the graph that in normal scenario there are no data packet lost, while in attack condition packets drop increase with increase in the size of topology.

Node	Total TC	TC Drop	Attack Performance
25	504	73	14.48
36	768	136	17.7
49	1080	287	28.19

Table 3: Attack Performance, time=100 seconds

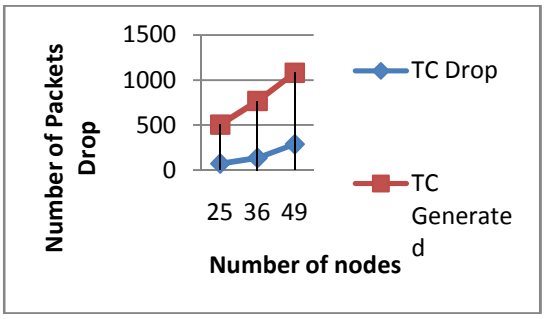

Figure 5: Attack Performance, time=100 seconds

In figure 5 one can see that with increase in size of topology, attack gets severe. The larger the topology better is the attack performance.

5 Conclusion

On the basis of the above results and observations, it is found that significant difference in number of TC packets being dropped in both the condition (attack scenario and normal scenario) was observed.

Hence it is conclusive enough that during the ANSN attack the number of drop of TC packets increase. Also with increasing number of nodes in the topology, number of drops increase accordingly. If number of nodes are increased, then the number of data packet drop increases accordingly. The above data clearly show the effect of ANSN attack on a network consisting of grid topology, based on MANETs.

6 **References**

[1] Thomas Clausen and Ulrich Herberg, "Vulnerability Analysis of the Optimized Link State Routing Protocol version 2", *Proc. in insitut national de recherché en informatique et en automatique,, {ISSN-0249-6399},* pp.1-17,February 2010.

[2]Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharm, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks" *Paper published in Journal of Computing, { ISSN-2151-9617},* pp. 41-48, January 2011.

[3] Safdar Ali Soomro, Sajjad Ahmed Soomro, "Denial of Service Attacks in Wireless Ad hoc Networks", *Journal of Information & Communication ISSN-Technology Vol.-4,Issue-2,* pp.68-71, January 2010.

[4] David Johnson and Gerhard Hancke, "Comparison of two routing metrics in OLSR on a grid based mesh network" *Published in Elsevier science Direct, Journal of Ad-Hoc Network, Vol.-7*, pp.374-387, 2009.

[5] Lalith Suresh, Rajbir Kaur, M.S.Gaur, "Collusion Attack Resistance Through Forced MPR Switching in OLSR", *Proceeding in IEEE, 978-1-4244-9228,Vol.-2/10* ,2010.

[6]. Djahel, F. Nat-Abdesselam, Z. Zhang, and A. Khokhar, "Defending against packet dropping attack in vehicular ad hoc networks," pp.245–258, 2008.

[7] Bounpadith Kannhavong, Hidehisa Nakayama,"A Collusion Attack Against OLSR-based Mobile Ad Hoc Networks," *Proceeding in IEEE GLOBECOM,1-4244-0357-x/06*, 2006.

[8] Rachid Abdellaoui and Jean-Marc Robert "SU-OLSR: A New Solution to Thwart Attacks against theOLSRProtocol",*People.scs.carleton.ca/gcevia/olsr/2009.*

[9] Atul Patel Ruchi Kansara Dr. Paresh Virparia, "A Novel Architecture for Intrusion Detection in Mobile Ad hoc Network", *International Journal of Advanced Computer Science and Applications, Special Issue on Wireless & Mobile Network*, Vol. {ISSN.2156-5570}, pp. 68-71,2011.

[10]Ruiliang Chen*, Michael Snow*, Jung-Min Park*, M. Tamer Refaei, "Defense against Routing Disruption Attacks in Mobile Ad Hoc Networks". *Laboratory for Advanced Research in Information Assurance and Security (ARIAS).*

[11]Bounpadith Kannhavong, Hidehisa Nakayama, Abbas Jamalipour "Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad Hoc Networks" *Proc. 7th IEEE International Symposium on Computer Network,* pp 30-35, 2006.

[12] Network simulator 3. http://www.nsnam.org.