BLACK HOLE ATTACK DETECTION IN MOBILE AD-HOC NETWORK: A CASE STUDY

Kavita T. Markad and Veeresh G. Kasabegoudar
P. G. Dept., MBES College of Engineering, Ambajogai, India.

ABSTRACT
An ad hoc network is a collection of mobile nodes that dynamically form a temporary network and are infrastructure less. Black hole attack is an attack in network layer which degrades the network performance by dropping packets. This paper identifies black hole attack against Optimized Link State Routing (OLSR) protocols, one of the four standard routing protocols for MANETs. We used Topology Graph Based Anomaly Detection (TOGBAD) a new centralized approach using topology graphs to identify nodes attempting to create a black hole. It is used to gain knowledge about the network topology and use this knowledge to perform plausibility checks of the routing information propagated by the nodes in the network. When a node generates fake (malicious) routing information or when plausibility checks fail, an alarm is triggered. This paper gives the corresponding simulation results in NS2. It also demonstrates detection process when the attempt to create a black hole before the actual impact occurs.

KEYWORDS: *Black Hole Attack, TOGBAD, Optimized Link State Routing Protocol.*

I. INTRODUCTION

In wireless networks, computers are connected and communicate with each other not by a visible medium, but by emissions of electromagnetic energy in the air. An ad hoc-network or MANET is a network composed only of nodes with no Access Point (AP). Messages are exchanged and relayed between nodes [1]. A MANET in general has the characteristics which are dynamic topology due to node mobility, limited bandwidth due to wireless communication, limited energy resources due to battery powered devices, and limited security against eavesdropping, since communication is done across an intrinsically open medium [2-20].
In this paper, we use Topology Graph Based Anomaly Detection (TOGBAD) which is a new centralized approach, using topology graphs to identify nodes attempting to create a black hole.
Section 2 presents routing protocols for ad hoc networks. Section 3 presents the basic optimized link state routing protocol. TOGBAD architecture is presented in Section 4. Simulation results in NS2 have been presented in Section 5 followed by conclusions in Section 6.

II. ROUTING PROTOCOLS FOR AD HOC NETWORKS

For the nature and challenges found in designing an ad hoc network routing protocol, a large amount of work has been done in the research community to find a perfect routing protocol for wireless ad hoc networks. The research has resulted to a number of routing protocols which can be classified as topology-based routing protocols and position-based routing protocols as shown in Figure 1. Topology based routing protocol uses the traditional routing concept such as maintaining a routing table or distributing link state information. Position based routing protocol uses the geographical physical position of the mobile nodes to route the data packets to the destination. Topology based Routing protocols can be classified into the following categories: reactive, proactive, and hybrid.

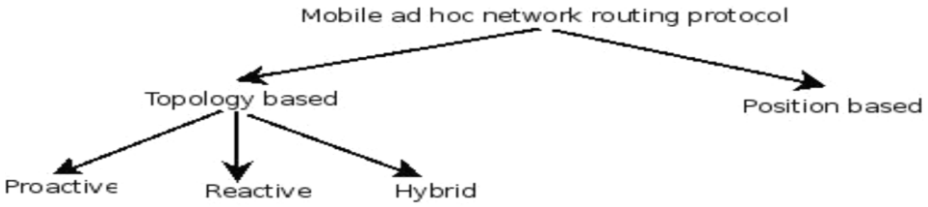

Figure 1: Classification of mobile ad hoc network routing protocols.

Under a reactive (also called on-demand) protocol, topology data is given only when needed. For example, A Dynamic Source Routing (DSR) protocol, and Ad hoc On-demand Distance Vector routing (AODV) protocol are reactive protocols [4-12].
In contrast, proactive (also called periodic or table driven) protocols are characterized by periodic exchange of topology control messages. Nodes periodically update their routing tables. Therefore, control traffic is more dense but constant, and routes are instantly available. OLSR (Optimized Link State Routing) is one of the reactive protocols. Hybrid protocols have both the reactive and proactive nature. ZRP (Zone Routing Protocol) and CBRP (Cluster Based Routing Protocol) are the example of hybrid protocol [13].

III. THE OPTIMIZED LINK STATE ROUTING PROTOCOL

The Optimized Link State Routing (OLSR) protocol is a proactive link state routing protocol for ad hoc networks. The core optimization of OLSR is the flooding mechanism for distributing link state information, which is broadcast in the network by selected nodes called Multipoint Relays (MPR) [14].

3.1 OLSR Message and Packet Format

OLSR control messages are communicated using a transport protocol defined by a general packet format. Each packet encapsulates several control messages into one transmission. Control traffic in OLSR is exchanged through two different types of messages: HELLO and TC (Topology Control) messages. HELLO messages are exchanged periodically among neighbour nodes, in order to detect links to neighbours and to signal MPR selection. TC messages are periodically flooded to the entire network, in order to diffuse link state information to all nodes. The other OLSR control messages are MID (Multiple Interface Declaration) and HNA (Host and Network Association). MID and HNA messages are emitted [15-17].

3.2 MPR Selection

The core optimization in OLSR is done by the selection of multipoint relay (MPR) nodes. Each node in the network independently selects a set of neighbours which retransmit its packets. This minimizes the broadcast of packets in the network by reducing the duplicate transmission of control messages in the same region. The set of selected neighbour node is called multipoint relays (MPRs) of that node [10].

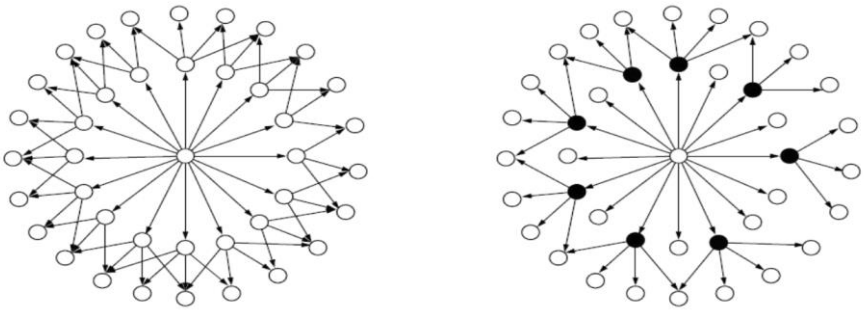

Figure 2: The broadcast from the central node is transmitted: (a) by all its neighbours and in (b) by its MPRs only denoted by solid black circles.

Figure 2(a) illustrate the same broadcast domain without the use of MPRs. Figure 2(b) shows a typical selection of MPRs around the central node covering all its two-hop neighbours in its radio transmission range. The solid circle represents the multipoint relays which will only broadcast the control messages [11].

3.3 Incorrect Traffic Relaying and Black Hole Attack

Network communications coming from legitimate, protocol-compliant nodes may be polluted by misbehaving nodes. An attacker can drop received routing messages, instead of relaying them as the protocol requires, in order to reduce the quantity of routing information available to the other nodes. This is called *black hole attack* by Hu et al [19] and is a "passive" and a simple way to perform a Denial of Service. The attack can be done selectively (drop routing packets) for a specified destination, a packet every η packets, a packet every t seconds, or a randomly selected portion of the packets or in bulk (drop all packets), and may have the effect of making the destination node unreachable or downgrade communications in the network.

IV. TOPOLOGY GRAPH BASED ANOMALY DETECTION

TOGBAD is a centralised topology graph based approach. It consists of three parts. Part one consists of creation of a topology graph and the number of neighbours of a node according to this topology graph is calculated. (Figure 3; steps 1-3) In part two, the number of neighbours a node claims to have in its HELLO messages is determined (Figure 3; steps 4 and 5). Finally, in part three, for each HELLO message, the originator's number of neighbours according to the message is checked for plausibility against the number of neighbours according to the topology graph (Figure 3; step 6). A significant difference between the two values triggers an alarm [20].

4.1 Number of Neighbours Calculated

The topology graph is obtained by using a modified version of the Cluster-Based Anomaly Detector (CBAD).There are two modifications to CBAD which lead to the construction of a topology graph, i.e. a graph containing complete topological information of the network.

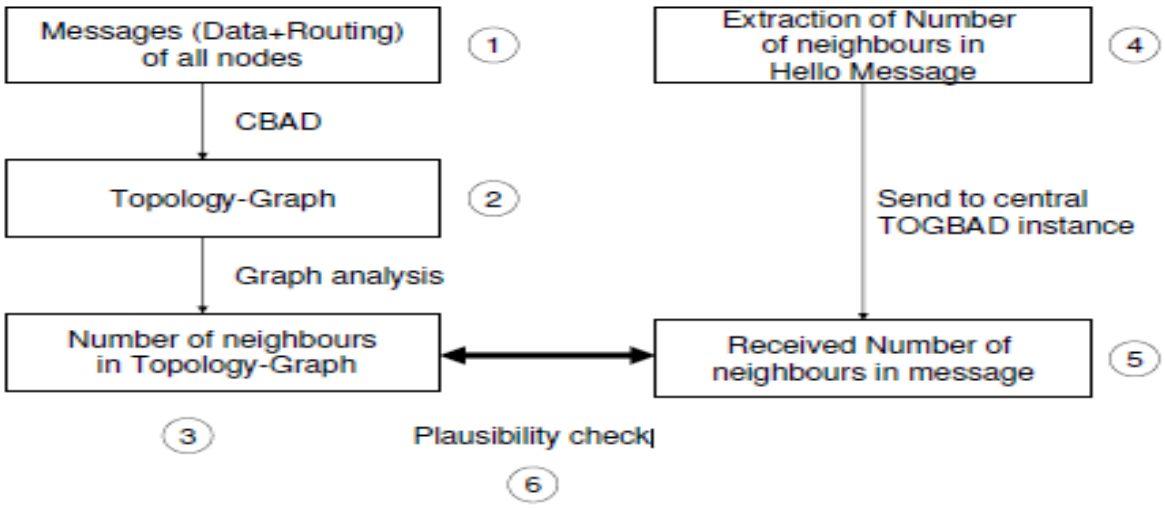

Figure 3: Algorithm of TOGBAD.

a) Consideration of routing and data packets b) Consideration of all hops (Figure 3; step 1).

In the topology graph, each network node is represented by a node and each link is represented by an edge. Therefore, the degree of each node is the number of neighbours looking for (Figure 3; step 3). The number of neighbours claimed in propagated HELLO messages is determined in the following way: Every network node extracts the number of neighbours from a received HELLO message (Figure 3; step 4) and sends the information to the central TOGBAD instance running on a supervising node.

4.2 Detecting Misbehaviour

The core part of TOGBAD is responsible for detecting routing misbehaviour. If the central TOGBAD instance receives a message from one of the network nodes, it extracts the number of neighbours for the originator of the HELLO message from the Topology Graph (Figure 3; step 3) and checks the plausibility (Figure 3; step 6) by comparing this number to the number of propagated neighbours (Figure 3; step 5). A significant difference between propagated neighbours and neighbours in the graph is classified as an attack attempt and an alarm is triggered. TOGBAD uses two formulae for detecting misbehaviour. Let o be the originator of a routing message, then
t(o) = node degree in topology graph and
m(o) = number of neighbours in routing message.
Under ideal circumstances,

$$t(o)=m(o) \quad (1)$$

Taking into account the dynamic nature of MANETs, assume

$$t(o)=m(o)+\delta \quad (2)$$

where δ represents the deviation due to node movement.
If TOGBAD discovers t(o) significantly smaller than
$m(o) + \delta$

$$t(o)<<m(o)+\delta \quad (3)$$

an alarm is triggered. When a deviation is "significantly" smaller then use a threshold based approach. Let

$$diff:=m(o)+\delta-t(o) \quad (4)$$

If diff > threshold
an alarm is generated. The threshold determination strongly depends on the specific network. It may be based on several metrics, e.g. average of previous diff values or maximum of previous diff values.

V. SCENARIO AND SIMULATION ENVIRONMENT

The simulation results were obtained using version 2.29.3 of the network simulator NS-2. A total of 20 nodes on a 700 m x 700 m area have been considered for this study. Each node has a transmission range of 250m. The total simulation time is 500 seconds, after an initial phase of 50 seconds, four senders and four corresponding receivers are randomly chosen. The traffic is constant bit rate with each sender transmitting one packet every 0.51 seconds starting at 0.1 seconds of simulation time. One node attempts to launch a black hole attack at simulation 170.94 time seconds and stops at 350.1 seconds. During this time, it sends fake HELLO messages. Before and after acting as black hole, the node behaves correctly. In the static scenario, the nodes are randomly distributed over the simulation area. Node 0 launches a black hole attack. In the mobile scenario, the nodes move according to the random waypoint model with a minimum speed of 0.5 m/s and a maximum speed of 2.0 m/s approximating pedestrian speed. Again, node 0 launches a black hole attack. The implemented TOGBAD is in OLSR protocol in the NS-2 simulation environment.

5.1 Static Scenario PDF

Figure 4 shows the average packet delivery fraction (pdf) of the static scenario. The pdf is calculated and it remains near about 100% until the black hole attack is launched. A few seconds after the black hole node starts sending fake routing information the average pdf drops to 50% and remains at about 50% percent until the black hole is switched off again. Approximately 15 seconds after the black hole attack is switched off, the pdf raises back to near about 90%. Additionally, due to the random node distribution the position of the black hole is randomly based.

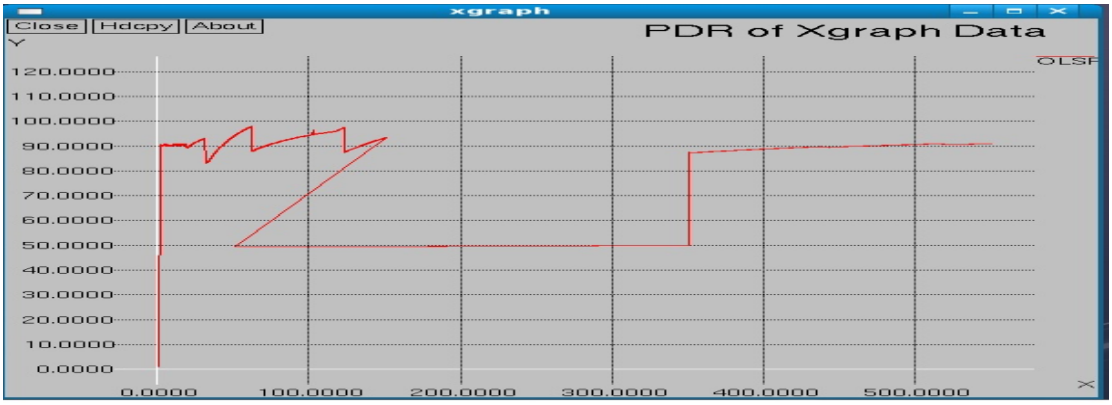

Figure 4: Packet delivery fraction (PDF) in static scenario.

5.2 Mobile Scenario PDF

The Figure 5 shows the packet delivery fraction for the mobile scenario. Without black hole the average pdf stays mainly at about 90%. Compared to the static scenario the pdf stays at a lower value due to the mobility of the nodes. This is due to node movement and to the local impact of a black hole attack already seen in the static scenario. Nevertheless, the average pdf drops to about 50% and after few seconds the average pdf drops to about 60% when the black hole is switched on.

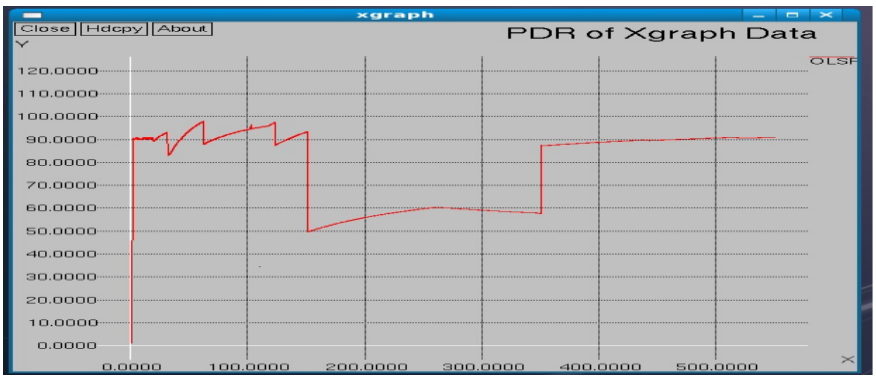

Figure 5: Packet delivery fraction (pdf) in mobile scenario.

Furthermore, the average pdf again drops (increases) about 15 seconds after the black hole is switched on (off), similar to the static scenario. This is caused by the time necessary for spreading the fake (valid) routing messages.

5.3 Different Values in Mobile Scenario

Figure 6 presents the diff values of the mobile scenario. While the black hole attack is active, the average diff values of the black hole node are larger than 15. Thus, for the entire duration of the black hole attack the diff value of the black hole node is significantly larger than the maximum over all non-black hole nodes.

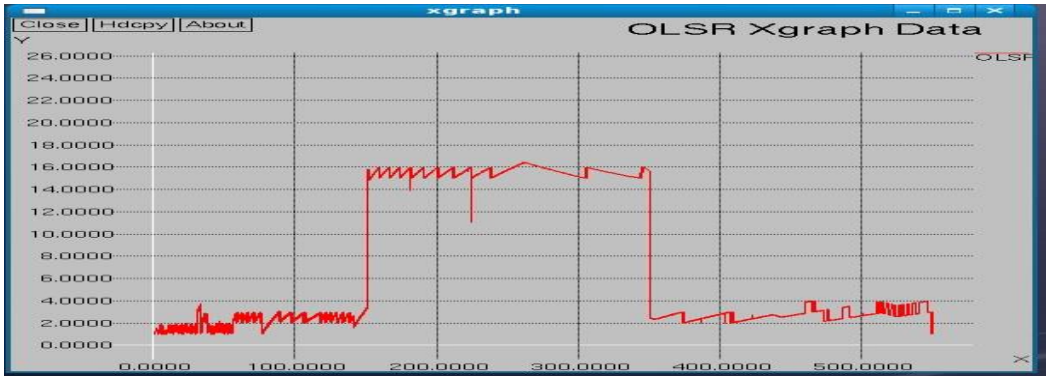

Figure 6: Difference value in mobile scenario.

5.4 Different Values in Static Scenario

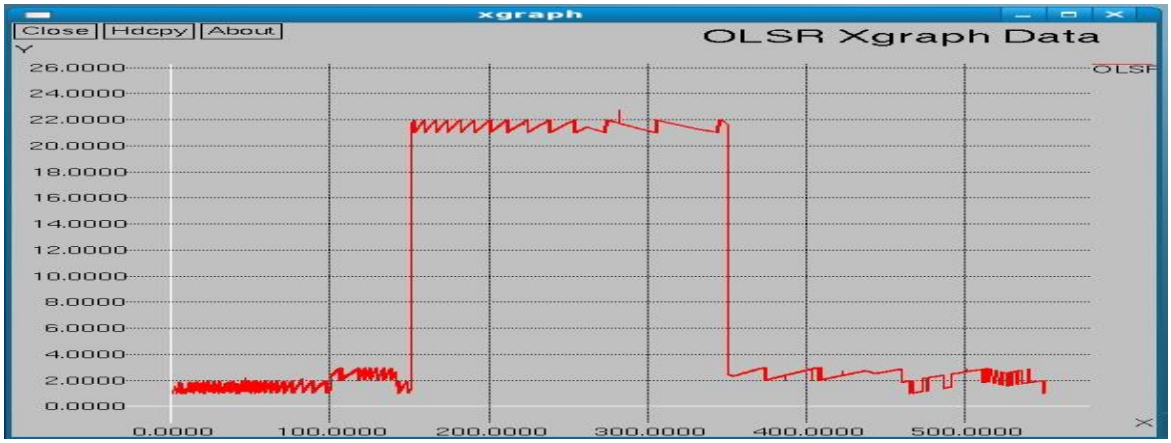

Figure 7: Difference value in static scenario.

In Figure 7, the difference values over time in the static scenario are shown. Since there is no mobility in this scenario, the network topology does not change. Therefore, the maximum diff. values for non-black hole nodes remain very small. After the black hole attack is launched, the black hole node has an average diff value of nearly 21 until the attack is switched off again.

5.5 Performance Parameters

There are different kinds of parameters for the performance evaluation of the routing protocols. These have different behaviors of the overall network performance. These parameters are delay, network load, throughput, and packet delivery ratio for protocols evaluation. These parameters are important in the consideration of evaluation of the routing protocols in a communication network. These protocols need to be checked against certain parameters for their performance. To check protocol effectiveness in finding a route towards destination, how much control messages sent by the source is important. It gives the routing protocol internal algorithm's efficiency. These parameters have great influence in the selection of an efficient routing protocol in any communication network.

5.6 Normalized Routing Load

It is calculated as the ratio between the no. of routing packets transmitted to the number of packets actually received (thus accounting for any dropped packets). A routing protocol offering low network load is called efficient routing protocol. The Figure 8 shows normal OLSR has high NRL than attack OLSR.

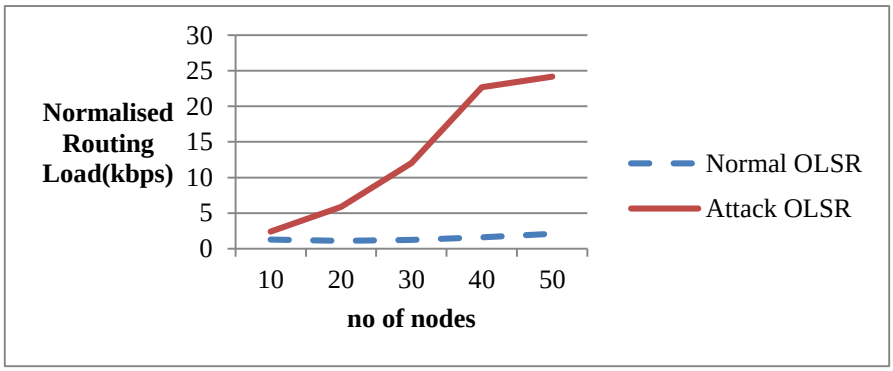

Figure 8: Number of nodes vs. normalized routing load.

5.7 Throughput

Throughput is defined as; the ratio of the total data reaches a receiver from the sender. The time it takes by the receiver to receive the last message is called as throughput. The throughput as it represents the successful deliveries of packets in time. If a protocol shows high throughput so it is the

efficient and best protocol than the routing protocol which have low throughput. Figure 9 shows the high throughput than OLSR protocol under black hole attack.

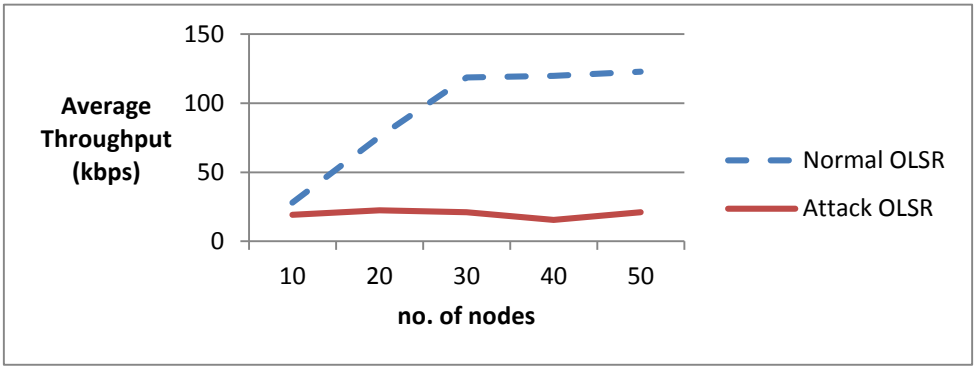

Figure 9: Number of nodes vs. throughput.

5.8 Packet Delivery Ratio

The PDR is defined as: Packet Delivery Ratio= Σ Number of packets sent at source / Σ Number of packets received at destination x 100%.The Figure 10 shows packet delivery ratio high for normal OLSR.

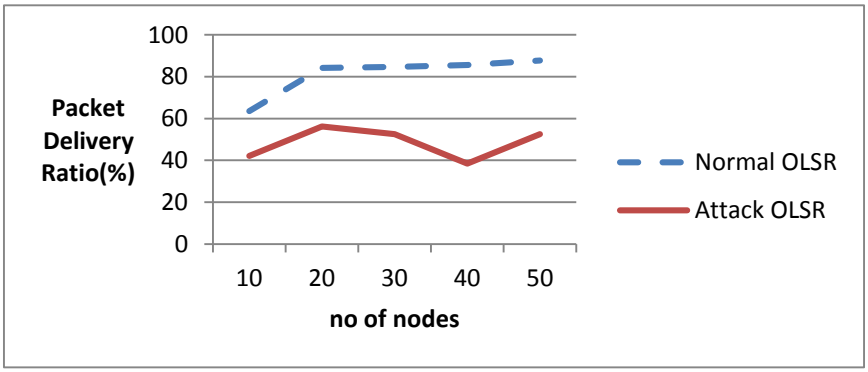

Figure 10: Number of nodes vs. packet delivery ratio.

5.9 Delay

The packet end-to-end delay is the time of generation of a packet by the source up to the destination reception. So this is the time that a packet takes to go across the network. This time is expressed in sec. If the routing protocol gives much end to end delay so probably this routing protocol is not efficient as compare to the protocol which gives low end to end delay. Figure 11 shows low end to end delay for normal OLSR as compared to OLSR protocol under black hole attack.

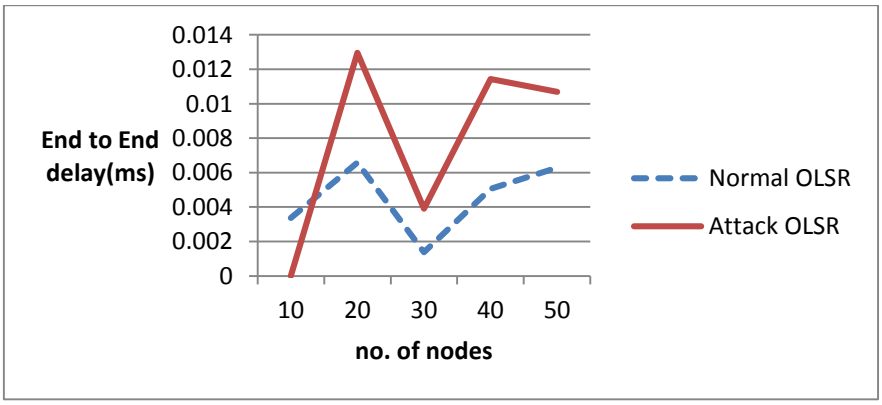

Figure 11: Number of nodes vs. end to end delay.

VI. CONCLUSIONS AND FUTURE WORK

TOGBAD is used for detecting routing attacks in tactical MANETs. Topology information is gained and represented in topology graphs. Based on this, plausibility checks for propagated routing messages are performed. The simulation results presented here show the potential of our approach and various performance parameters are measured.

Future work includes attacks against TOGBAD itself have to be considered. For example, malicious nodes sending spoofed messages or nodes modifying messages. Additionally, the black hole may influence the messages needed to build the topology graph, because for these messages routes are needed. Also, we will evaluate this approach, especially involving realistic mobility and traffic models suitable for tactical MANETs. In addition, the development of a robust metric to determine whether a diff value leads to the creation of an alarm is necessary. Furthermore, we plan to evaluate TOGBAD using routing protocols other than OLSR

REFERENCES

[1]. F Kargl, Mobile Ad hoc Networking, PhD Thesis, University of Ulm. Ulm, Germany, 2003.
[2]. S. McCanne and S. Floyd, "NS Network Simulator," 2006. Available (online): http://www.isi.edu/nsnam/ns.
[3]. C.S.R.Murthy and B.S.Manoj, Ad Hoc Wireless Networks, Pearson Education, 2008
[4]. G.Kaur, "Performance Analysis of AODV routing protocol in Manets", *International Journal of Engineering Science and Technology (IJEST)*, vol. 4 no.8, 2012.
[5]. Kuppusamy, P., Thirunavukkarasu, K. and Kalaavathi, B. ," A study and comparison of OLSR, AODV and TORA routing protocols in ad hoc networks", *3rd International Conference on Electronics Computer Technology (ICECT)*, 2011
[6]. FahimMaan, NaumanMazhar "MANET Routing Protocols vs. Mobility Models: Performance Analysis", pp. 179-184, 2011.
[7]. J. Hubaux, L. Butty´an and S. Capkun, "The quest for security in mobile ad hoc networks," *Proceedings of the 2nd ACM International Symposium on Mobile ad hoc Networking & Computing*, 2001.
[8]. Mohit Kumar and Rashmi Mishra "An Overview of MANET: History, Challenges and Applications", *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 3, 2012.
[9]. Daniele Raffo, Cédric Adjih, Thomas Clausen, Paul Mühlethaler, "An advanced signature system for OLSR," *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks* October 25-25, 2004.
[10]. Dilpreet Kaur,Naresh Kumar,"Comparative Analysis of AODV, OLSR, TORA, DSR and DSDV Routing Protocols in Mobile Ad-Hoc Networks",*IJCNIS*, vol.5, no.3, pp.39-46, 2013.
[11]. David B. Johnson and David A. Maltz. "Dynamic Source Routing in ad hoc wireless networks," In Imielinski and Korth, editors, Mobile Computing, volume 353, pp. 153–181. Kluwer Academic Publishers, 1996.
[12]. David B. Johnson, David A. Maltz, and Yih-Chun Hu, "The Dynamic Source Routing protocol for mobile ad hoc networks (DSR)," July 19, 2004.
[13]. Mingliang Jiang, Jinyang Li, and Y. C. Tay, "Cluster Based Routing Protocol (CBRP)",August 14 1999.
[14]. Thomas Heide Clausen, Gitte Hansen, Lar Christensen, and Gerd Behrmann, "The Optimized link state routing protocol evaluation through experiments and simulation," *Proceedings of the IEEE Symposium on Wireless Personal Mobile Communications*, September 2001.
[15]. Philippe Jacquet, Paul Mühlethaler, Thomas Clausen,Anis Laouiti, Amir Qayyum, and Laurent Viennot.Optimized, "Link state routing protocol for ad hoc networks,"*Proceedings of the IEEE International Multitopic Conference (INMIC 2001)*, Pakistan, 2001.
[16]. J. Cai, P. Yi, J. Chen, Zh. Wang, N. Liu, An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network, Proc. *Int. Conf. on Advanced Information Networking and Applications. Singapore*, pp. 775-780, 2010.
[17]. T. Clausen, U. Herberg, Security Issues in the Optimized Link State Routing Protocol Version 2 (OLSRv2), International Journal of Network Security and its Applications, 2010.
[18]. Pooja Singh, Anup Bhola and C K Jha. Article: Simulation based Behavioral Study of AODV, DSR, OLSR and TORA Routing Protocols in Manet. *International Journal of Computer Applications* 67(23):23-26, April 2013. Published by Foundation of Computer Science, New York, USA.
[19]. Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "A secure on-demand routing protocol for ad hoc networks," *Proceedings of the 8th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '02)*, September 2002.

[20]. E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tolle, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs," *Proceedings of the 32nd IEEE Conference on Local Computer Networks*, LCN 2007, pp. 1043-1052, 2007.

AUTHORS

Kavita T. Markad received the bachelor's degree from Nagpur University, Nagpur, in 2010, and currently pursuing her Master's degree from the College of Engineering Ambajogai. Since June 2012, she has been working as Lecturer in Pratap Institute of Management and Technology, Washim, India. Her research interests include Computer Networks, Wireless Networks and Mobile Ad hoc Networks.

Veeresh G. Kasabegoudar received the Bachelor's degree from Karnataka University Dharwad, India, the Masters degree from the Indian Institute of Technology (IIT) Bombay, India, and the Ph.D. degree from the Indian Institute of Science (IISc), Bangalore, in 1996, 2002, and 2009, respectively. From 1996 to 2000, he worked as a Lecturer in the Electronics and Telecommunication Engineering Department, College of Engineering, Ambajogai, India, where, from 2002 to 2006, he worked as an Assistant Professor and, since 2009, he has been a Professor and Dean of PG Department. He has published over 20 papers in technical journals and conferences. His research interests include wireless networks & mobile Ad-hoc networks, microstrip and CPW fed antennas, microwave filters, and image/signal processing.