I J C T A, 9(15), 2016, pp. 7317-7324

Attenuate Black Hole Attack using Zonal Routing Protocol with Fictitious nodes

T. Peer Meera Labbai (T. Vigneshwar)*

ABSTRACT

In MANETs (Mobile ADHOC networks) routing protocols are vulnerable to transfer the data across networks. To improve MANET security against different types of attacks, we use the nodal structures. There are numerous nodes in MANET routing. The existing technique does not isolate the node that has been attacked. Thus, the intruder can create a fake node. This fake node can malfunction and misfit among the native nodes of the MANET network. To avoid the fake node in the DOS attacks and specifically in Black hole Attack, we improve the security of the system by using ZRP, Zonal Routing Protocol where it identifies and segregates the node that has been attacked by the intruder.

1. INTRODUCTION

The MANET environment sends the data's to the base nodes through a broadcast process. Each and every sensor node sends directly to the base node which is energy consuming and traffic intense. The network is divided to some sub-networks because of the limited wireless communication range. Sensors deployed in a building may not be able to communicate with the sensors which are placed in the neighboring buildings. Therefore, limited communication range may pose a challenge for data collection from all sensor nodes. The MANET consumes the energy from the sensors. While an intruder attacks, the fake node that has been created amidst the nodes can consume more energy, resulting in the high energy obtainment in the network.

2. A OVERVIEW ON MANET

A Mobile Ad-hoc network is a wireless ad-hoc network which is used for data transfer to forward and transfer the packets. It will work as self configuring dynamic network of mobile devices connected by wireless links in a hostile environment without any pre-fixed infrastructure. The protecting in a MANET is constituted by intrusion prevention systems like cryptography and authorization have some limitations.

2.1. MANET Features

a) Light Weight: The function of node will act as both host/router.

b) Distributed Operations: There is no fixed structure for controlling and managing the network.

c) Multi-hop routing: Packets delivered via one or more nodes.

d) Dynamic network topology: As the network varies rapidly, the movable nodes dynamically establish routing among themselves.

2.2. Routing Protocols in Manets

MANET Routing Protocols are mainly categorized in to three different ways they are

* Assistant Professor (S.G) Department of Computer Science and Engineering Vigneshwar Thiyagarajan Post Graduate Student SRM UNIVERSITY Chennai-603202, India, *Email: mailtovigneshwart@gmail.com*

1. Proactive Protocol
2. Reactive Protocol
3. Hybrid Protocol.

2.1.1. Proactive Routing Protocols

Proactive MANET protocol is based on table-driven technique and will actively monitor the layout of the network. Table-driven technique maintains consistentency ,latest routing information from every node .Proactive protocol requires to maintain table for each node and to store the routing information, then they respond to changes in network topology propagating updates throughout the network in order to maintain a consistent network view. Example for proactive routing protocol is table-driven technique is Dynamic State Distance Vector Protocol(DSDV). Routing (OLSR), Destination-Sequenced Distance Vector (DSDV), Landmark Routing Protocol (LANMAR)[ref], Cluster head Gateway Switch Routing Protocol (CGSR) all are Proactive Routing Protocols.

2.1.2. Reactive Routing Protocols

Reactive protocols will be working on the basic of on- demand, creates only when desired by source nodes.When requirement is there to send a data via nodes the it initiates the route to destination. Once the data is reached to destination automatically the route will be disabled. Best Examples of reactive MANET protocols is Dynamic Source Routing (DSR).

2.1.3. Hybrid Routing Protocols

Combination of both proactive and reactive protocol is Hybrid protocol. Since proactive and reactive routing protocols work on different scenarios, there is good reason to develop hybrid routing protocols, which use a mix of both proactive and reactive routing protocols.

The idea of hybrid routing protocols is to use proactive routing in some places and Reactive routing in some places. Based on the situation the routing mechanism the protocol need to be selected. Best Example of hybrid is Zonal Routing Protocol (ZRP).

3. BLACK HOLE ATTACK

Black hole attack is also known as packet loss attack. This attack is that whitout any prior knowledge of user there will be a packet loss or intruder will delete the packet without any prior intimation.

Packet loss can be only realized with comparing data when the data is sended from source and which the data is recived by the destination. With comparison we come to know whether the packet is loss is there or not. The unknown router can also accomplish this attack, e.g. by dropping packets for a particular network destination, at a certain time of the day, a packet every *n*packets or every *t* seconds, or a randomly selected portion of the packets. This is also called a gray hole attack.

3.1. Architecture Diagram

4. PROPOSED SYSTEM

4.1. Network Formation

Each node sends “hello” message to other nodes which allows detecting it. Once a node detects “hello” message from another node (neighbor), it maintains a contact record to store information about the neighbor. Using multicast socket, all nodes are used to detect the neighbor nodes.

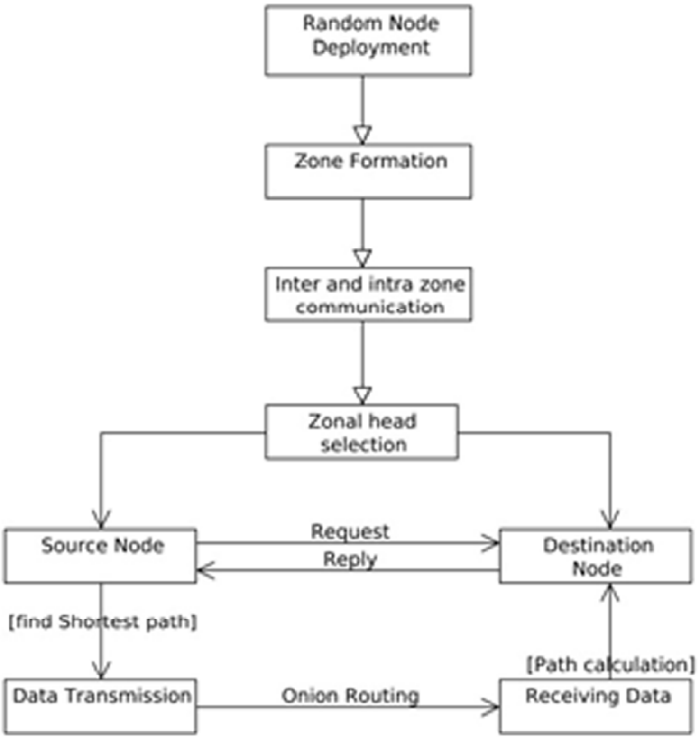

Figure 1:

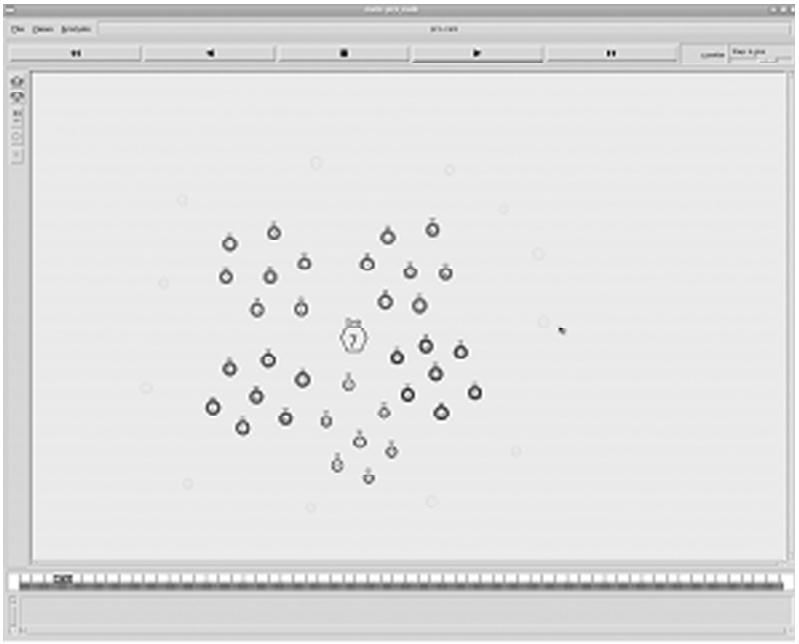

Figure 2:

4.2. Zone formation And Key Distribution

In a cluster, each monitored component is monitored by *n* sensing nodes and it can communicate with each other nodes. We assign the cluster name to each cluster and each sensing node stores its cluster name. Each cluster can communicate with the help of forwarding sensors. Each sensing nodes can sense the data and forward the data to the forwarding sensors. Then the measured data can be forwarded to the controller with the help of forwarding nodes. Each sensing node stores the stores the check polynomial of other clusters. Data can be validated by using this check polynomial.

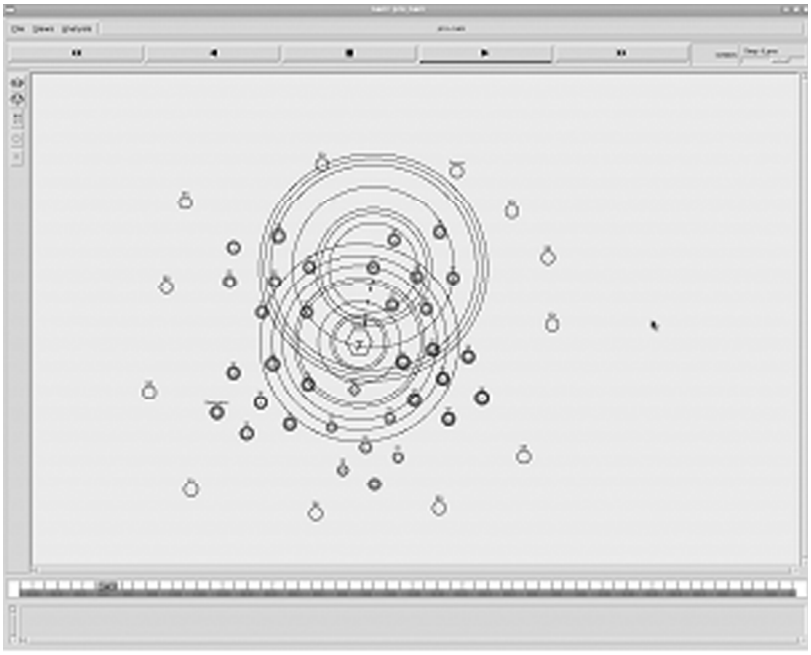

Figure 3:

4.3. Domain

Is a set of related devices that can be connected directly or through Domain Router.

4.4. Domain Router (DR)

Domain Server that performs the following functions:

1) Routing the messages among its clients.
2) Resolve the problem of Domains merging.

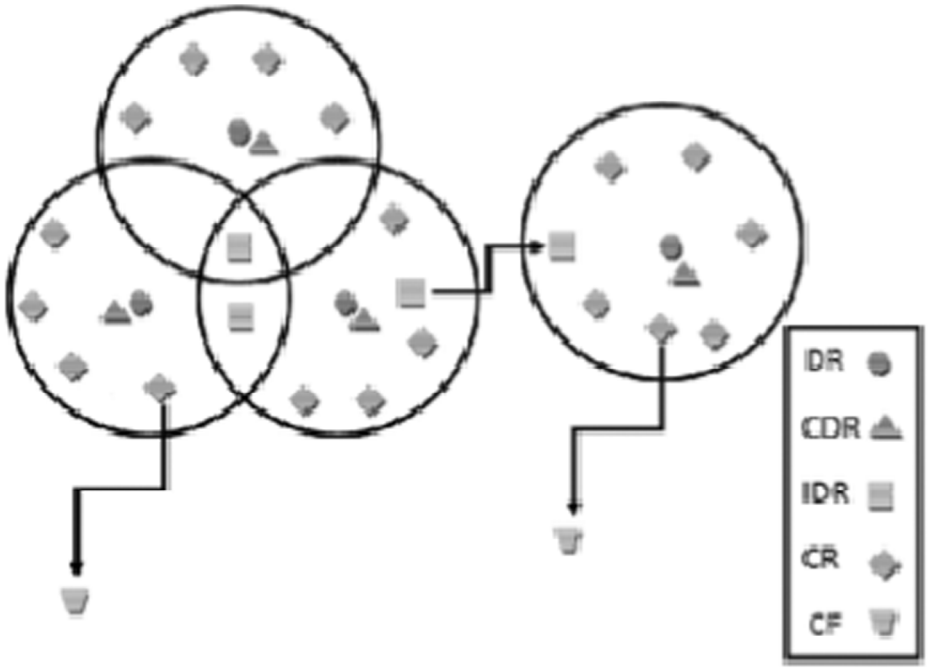

Figure 4:

3) Forwards the messages to neighbor domains.
4) Resolve the IP conflict.
5) Limiting the Domain boundaries.

4.5. Co-Domain Router (CDR)

It's the nearest device to DR, it is s elected by DR . CDR should be capable of performing the same function as DR. CDR used to enhance the stability of MANET topology and to minimize the domain formation processes messages.

4.6. Onion Routing Protocol

Onion routing protocol is the mechanism in which the sender and the receiver nodes communicate with other anonymously by means of some intermediate nodes. The encrypted data is transmitted through a series of network nodes called onion routers, each of which "peels" away a single layer, uncovering the data's next destination. When the final layer is decrypted, the message arrives at its destination. The sender remains anonymous because each intermediary knows only the location of the immediately preceding and following nodes.

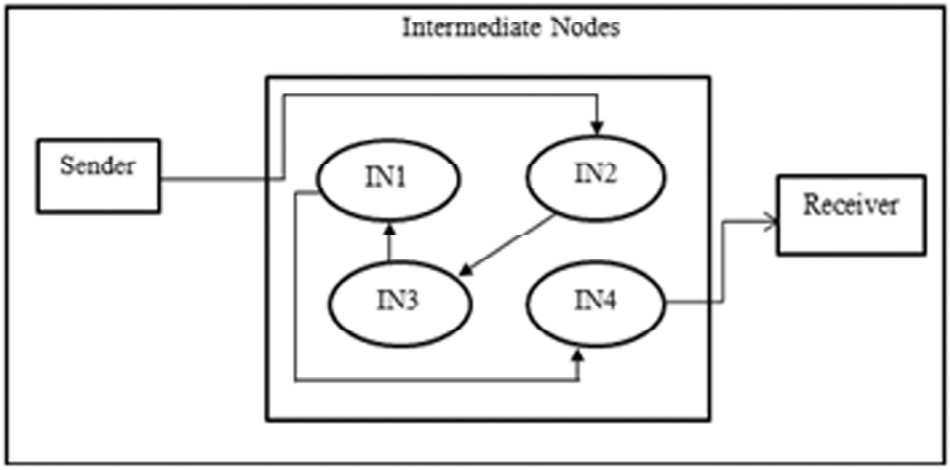

Figure 5:

4.6.1. Steps

1. Defining a route.
2. Constructing an anonymous connection.
3. Moving data through an anonymous connection.
4. Destroying the anonymous connection.

4.7. Zonal Routing Protocol

Zonal routing protocol (ZRP) is mainly used to reduce the latency time. Hybrid routing protocol has been used to reduce the control overhead of proactive routing protocol and decrease the latency caused by route discovery in reactive routing protocol.

In ZRP proactive routing protocol is Intra-Zone Routing Protocol(IARP) used inside the routing zones, reactive routing protocol is Inter-Zone Routing Protocol (IERP) used between routing zones.ZRP is the combination of proactive and reactive routing protocol.In ZRP the message is directly transferred from the source to destination if the destination node presents inside the zone of the source node.

5. SIMULATION

5.1. Packet_Loss

Packet Lost is that the total number of packets dropped during the simulation. Packet lost is that the data send to the destination and the data which is received by the destination. Where the difference between two data is the packet lost while receiving the data in the receiver end.

Packet lost = Number of packet send – Number of packet received .

In this graph i have compared the Packet loss with the OLSR and ZRP protocol with onion routing. When we use Zonal routing protocol the data transfer with out any data loss percentage is less when it compared to OLSR protocol.

5.2. Delay

End-to-end Delay : the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

In the graph i have compared the delay which happen while using OLSR Protocol which is used in a base paper and compared with ZRP. With the graph comparison we can analyze the delay time is very low compared to the OLSR protocol.

5.3. Channel

In wireless network, the packets are transmitted through channel at the physical layer. The channel invokes a shared medium with support for contention mechanisms. The channel (wireless channel) allows the MAC to implement carrier sense, contention and collision detection.

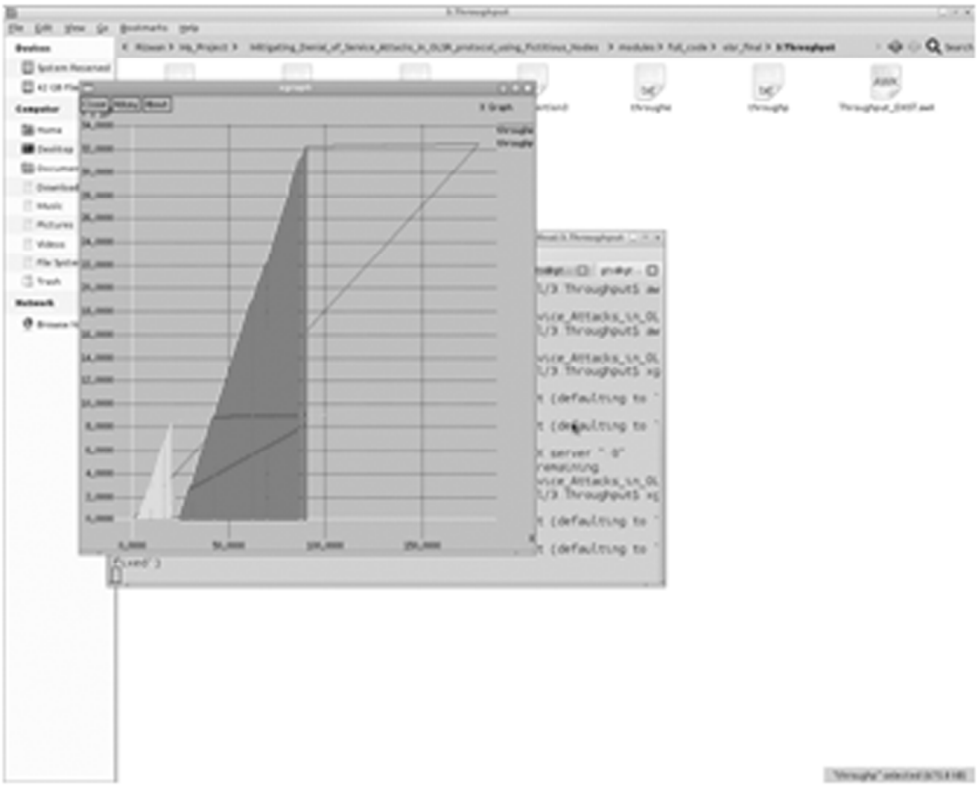

Figure 6:

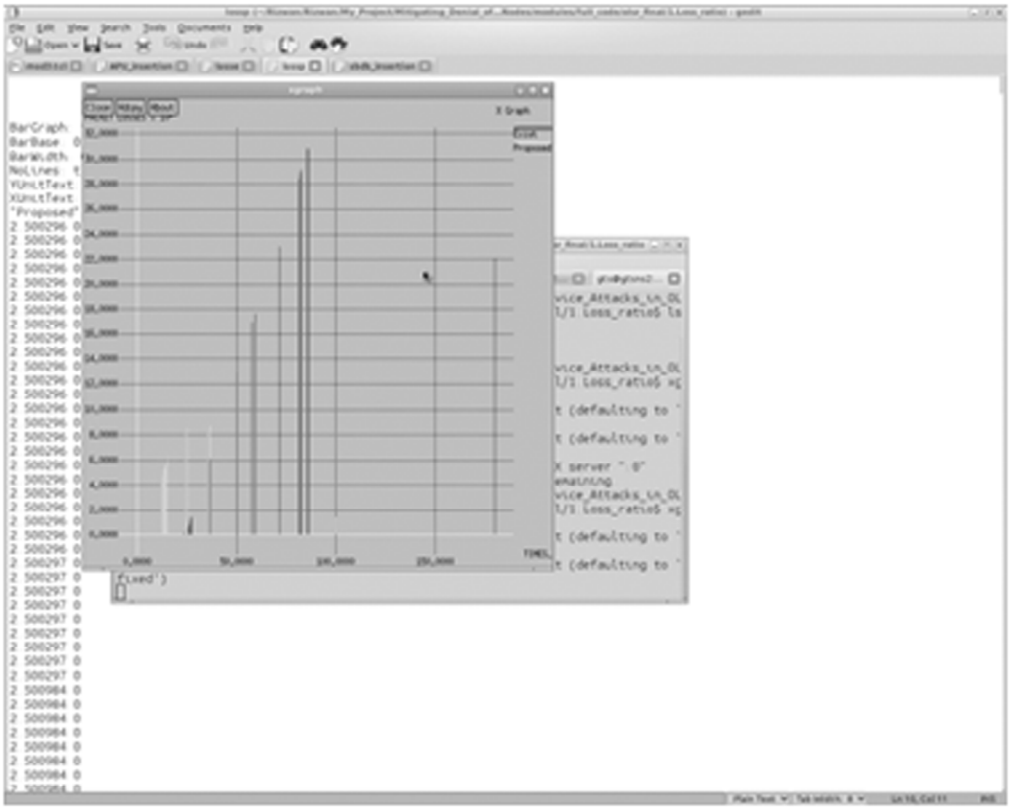

Figure 7:

5.4. Throughput

Packet delivery ratio : the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

5.5. Drop_nodes

Each and every nodes individual performance of packet delivered ratio.

6.CONCLUSION

In this paper, we have presented a solution for Secure MANET routing to prevent from a Black hole attack while transferring data in which the attacker manipulates the victim into appointing the attacker as a fictitious node, giving the attacker control over the communication channel. Then the attack is prevented by using onion routing algorithm where the attacker the ability to follow the victim around. ZRP with onion routing is unique in that all the information used to protect the MANET stems from the victim's internal knowledge, without the need to rely on a trusted third party.

Simulation shows that ZRP with onion routing successfully prevents the attack, specifically when number of nodes are are high and complex. In addition, it was discovered that as node population increases in density and size, the closer ZRP overhead is to OLSR. Given that ZRP functions best in dense large networks, ZRP can function without real additional cost. I expect that with only minor adjustments, ZRP with Onion routing can protect other family of attacks such as node isolation attack, gray hole and wormhole attacks). We leave this for future work.

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 destinationsequenced 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].