Detection and Isolation of Packet Dropping Attacker in MANETs

Ahmed Mohamed Abdalla, Ahmad H. Almazeed
Electronics Department, College of Technological Studies,
The Public Authority for Applied Education and Training,
P.O.Box 42325, Shuwaikh 70654, Kuwait

Imane Aly Saroit, Amira Kotb
Information Technology Department, Cairo University, 5
Dr. Ahmed Zewail St, Orman,
Giza 12613, Egypt

***Abstract*—Several approaches have been proposed for Intrusion Detection Systems (IDS) in Mobile Ad hoc Networks (MANETs). Due to lack of MANETs infrastructure and well defined perimeter MANETs are susceptible to a variety of attacker types. To develop a strong security mechanism it is necessary to understand how malicious nodes can attack the MANETs. A new IDS mechanism is presented based on End-to-End connection for securing Optimized Link State Routing (OLSR) routing protocol. This new mechanism is named as Detection and Isolation Packet Dropped Attackers in MANETs (DIPDAM). DIPDAM mechanism based on three ID messages Path Validation Message (PVM) , Attacker Finder Message (AFM) and Attacker Isolation Message (AIM).**

DIPDAM mechanism based on End-to-End (E2E) communication between the source and the destination is proposed.

The simulation results showed that the proposed mechanism is able to detect any number of attackers while keeping a reasonably low overhead in terms of network traffic.

Keywords—MANETS; IDS; OLSR; DIPDAM

I. INTRODUCTION

A Mobile ad hoc Network (MANET) is a distributed and highly dynamic network environment. Mobility and unreliable wireless channels are the result of an unpredictable-dynamic network topology. Due to the fully distributed network, establishing a centralized node which can collect all of the network traffic is not feasible. In addition, mobile nodes have relatively limited power and bandwidth constraints, so they cannot carry high overhead security protection.

An ideal intrusion detection model in MANET should first have a reliable, distributed, low-overhead, message collecting, and exchanging mechanism. The mechanism should also adapt to changes in the network topology and tolerate message loss.

Second, the model should be affordable for low computation power devices. Third, the model should perform real-time protections since the routing topology may change very quickly and the attack damage may also propagate relatively quickly. Finally, the model should not generate high false positives and negatives with respect to new routing attacks.

The main goal in this paper is to detect successfully and isolate the data packet dropping attackers from routing path in OLSR routing protocol for MANETs.

In this paper, a new IDS mechanism is presented based on End-to-End connection for securing OLSR routing protocols. This new mechanism DIPDAM is based on three ID messages Path Validation Message (PVM) enables E2E feedback loop between the source and the destination, Attacker Finder Message (AFM) to detect attacker node through the routing path, and Attacker Isolation Message (AIM) to isolate the attacker from routing path and update the black list for each node then trigger to neighbors with updated information [1-2].

To save nodes resources, DIPDAM avoids monitoring every node at all times. DIPDAM is a fully distributed detection approach. DIPDAM is a scalable approach and allows the source to monitor its data messages with minimal overhead.

According to simulation results, It can be stated that DIPDAM mechanism can detect and isolate many types of misbehavior node(s) through the path between the source and the destination..

II. PREVIOUS WORK

Intrusion detection is defined as the method to identify “any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource”. [3]

Intrusion detection system (IDS) is a practical approach to enhance the security of existing networks. Briefly, an intrusion detection system monitors activity in a system or network in order to identify, to detect, and then to isolate current attacks.

There are three main components of an IDS:

- The collection of data.
- The analysis of collected data (Detection).
- The response of an alert when a threat is detected.

For Mobile Ad hoc Networks, the general function of an IDS is detecting misbehaviors by observing the networks traffic in a Mobile Ad hoc [4]. Most of recent researches focused on providing preventive schemes to secure routing in MANETs [5-9].

Key distribution and an establishment of a line of defense defined in [5], [6] based on mechanism in which nodes are either trusted or not and if trusted they are not compromised. Also contribution in [7], [9] considers the compromise of trusted nodes. It assumed a public key infrastructure (PKI) and a timestamp algorithm are in place. However, the above approaches cannot prevent attacks from a node who owns a legitimate key.

It is necessary to understand how malicious nodes can attack the MANETs. A model to address the Black Hole Search problem algorithm and the number of agents that are necessary to locate the black hole without the knowledge of incoming link Developed in [10]. Watchdog and path-rater are discussed in [11]. Their drawback is the increase of the percentage of overhead significantly with the percentage increase of misbehavior nodes. Ex-watchdog [12] suggests modifying the previous system to decrease the percentage of overhead. [13] Introduces IDS which formulate the problem of distributed collaborative defense against coordinated attacks as a dynamic game problem. The same group extends their work in [14] by proposing detection schemes that are suitable to detect in-band wormhole attacks. The first detection scheme uses the Sequential Probability Ratio Test (SPRT) is discussed in [15]. The SPRT has been proven to be an optimal detection test when the probability distributions of both normal and abnormal behaviors are given.

A feedback mechanism to secure OLSR against the link spoofing attacks was provided in [16], [17]. The solution assesses the integrity of control messages by correlating local routing data with additional feedback messages called CPM sent by the receivers of the control messages.

Another formal approach to harden the Multi Point Relay (MPR) selection and thwart the attacks against OLSR suggested in [18]. This approach validates the routing table and the topology information using trust based reasoning. Hence, each node can verify the validity of the received HELLO and TC messages simply by correlating the information provided by these messages. A technique to detect attacks by discussing a collusion attack model against the OLSR protocol was presented in [19].

III. Detection and Isolation of Packet Dropped Attackers in MANETs (DIPDAM)

New existing solutions for detecting data packet dropping in ad hoc networks work by monitoring individual nodes. Other solutions used so far for protecting these networks are authentication and encryption [20]. Most of these mechanisms are not considerably appropriate for MANETs resource constraints, i.e., bandwidth limitation and battery power, since they result in heavy traffic load for exchanging and verification of keys.

In DIPDAM mechanism, each source node in the network monitors its own packets (data packets or routing packets) by using a Path Validation Message (PVM) as shown in fig. 1. If a misbehavior node is detected, the other neighboring nodes are informed in order to help them in protecting themselves. Each source node monitors the behavior of its neighborhood instead of making each node in the networking doing this job which consumes nodes resources.

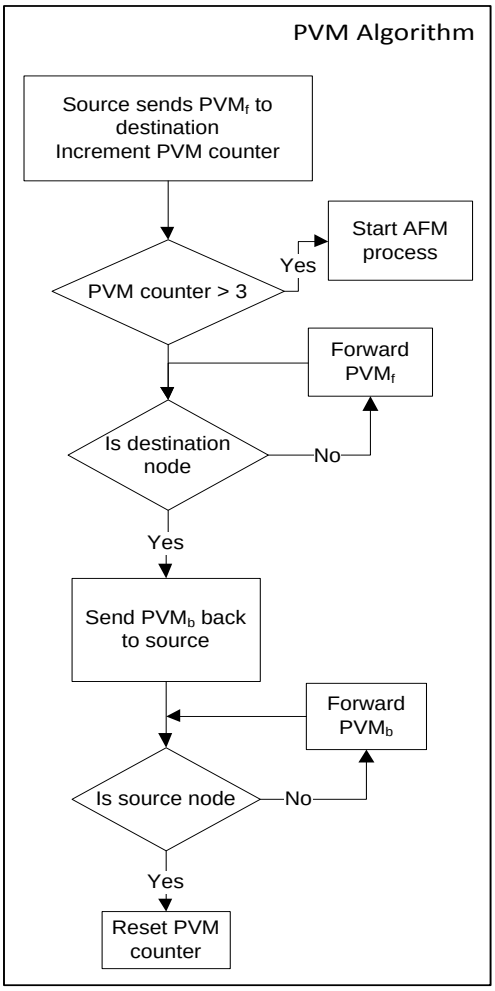

Fig.1. Flow chart for Path Validation Message (PVM) algorithm

A failure to get a reply for an N PVM messages sent (N is set to 3 in the flow chart), DIPDAM algorithm will trigger an Attacker Finder Message (AFM) algorithm shown in fig. 2.

The detector node needs to share the information about the detected attacker with other nodes in the network. This is accomplished by flooding the network with Attacker Isolation Messages (AIMs) [2]. It is noticed that nodes can be incorrectly detected as attackers due to network malfunction during a certain period. Such nodes would be wrongly isolated for the lifetime of the whole network.

A verification step is added to ensure that nodes are correctly detected and isolated. The process is illustrated in fig. 3. Fig. 4 shows a flow chart for the AIM algorithm.

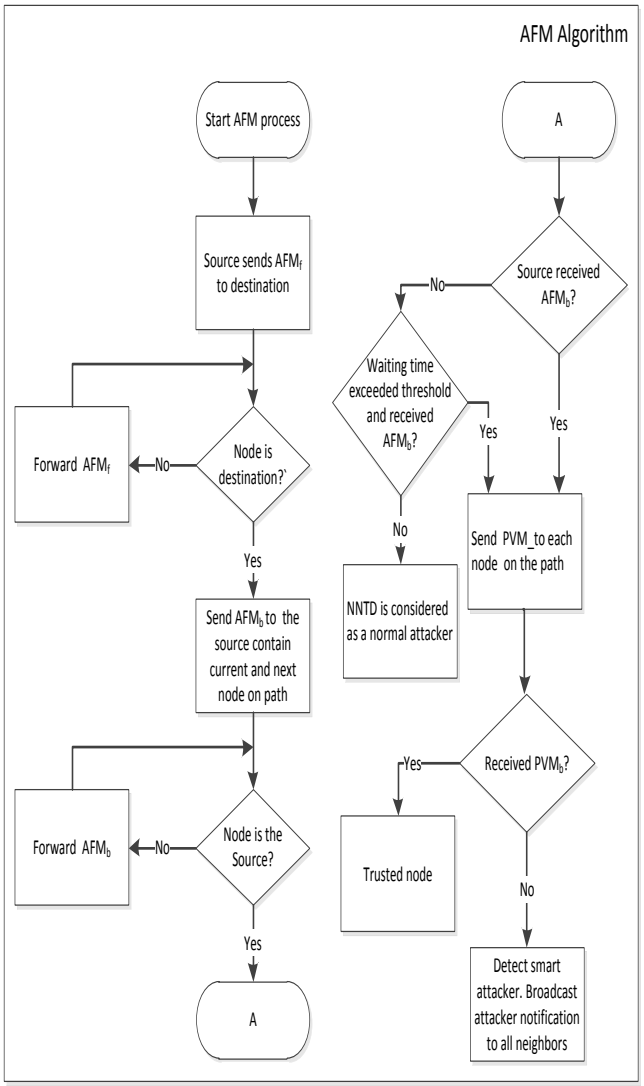

Fig.2. Flow chart for Attacker Finder Message (AFM) algorithm.

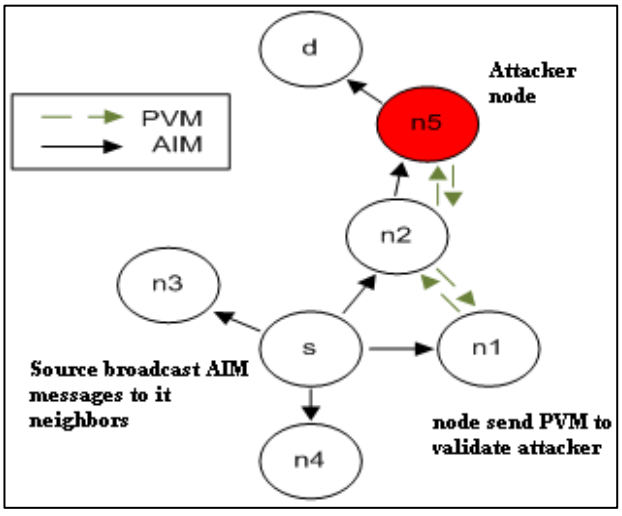

Fig.3. Attacker Isolation Message (AIM) process.

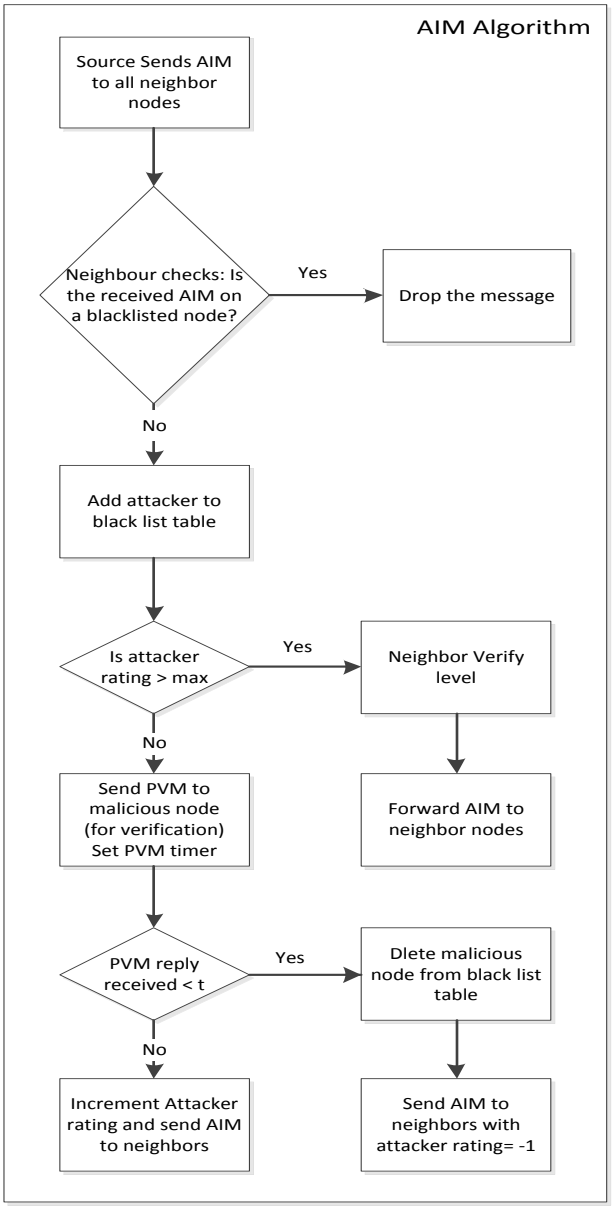

Fig.4. Flow chart for AIM algorithm.

To evaluate the robustness of DIPDAM mechanism we tested MANETs under different attacker types [21].

N1 nodes take contribution in the route discovery and route maintenance processes but refuses to forward data packets to protect its resources. This attack type can reduce network throughput, but does not affect any of the network traffic unless it is routed through selfish nodes, selfish nodes refuse to forward or drop data packets, this attacker type will be named as smart attacker.

N2 nodes neither contribute to the route discovery processes nor data-forwarding processes. Instead they use their resources only for transmissions of their own packets which are called selfish nodes. An attacker with this criterion will be named normal attacker.

N3 nodes behave properly if its energy level lies between full energy-level and certain threshold T1. They behave like node of type N2 if energy level lies between threshold T1 and another threshold T2 and if energy level falls below T2, they behave like node of type N1.

N1, N2, and N3 nodes are risky to routing protocols. These nodes suspend the data flow by either dropping or refusing to forward the data packets thus forcing routing protocol to select an alternative available route which it may again contain some malicious nodes, resulting in the new route also to fail. This process form a loop which enforce source to conclude that data cannot be further transferred.

The proposed work is designed to detect and isolate N1 type and N2 type. N3 type selfish nodes will be detected only when they behave similar to N1 or N2 type nodes.

Dropping any packets affects the network performance by causing the retransmission of data packets many times. Furthermore, it can prevent the end-to-end communications between nodes.

IV. NETWORK SIMULATOR PROGRAM

The NS-2 simulation tool [22-23] consists of two sets of scenario; topology scenario and traffic generation pattern. The topology scenario defines the simulation area and the mobility model of randomly distributed mobile nodes over the simulation time. The traffic pattern defines the characteristics of data communications, data packet size, packet type, packet transmission rate and number of traffic flows. Each node is assumed to be equipped with a wireless transceiver operating on 802.11 wireless standards. The physical radio frequency characteristics of each wireless transceiver such as transmit power, the antenna gain, and signal to noise and interference ratio, are chosen with a bit rate of 2Mb/sec and a transmission range of 250 meters with an omni-directional antenna.

The simulation scenarios consist of two different settings. First, the impact of network density or size is assessed by varying the number of mobile nodes placed on an area of a fixed size of 1500m x 300m. The second simulation scenario investigates the effects of node mobility on the performance of route discovery by varying the maximum speed of mobile nodes placed on a fixed area of 1500m x 300m.

Each node participating in the network is transmitting within the 250m transmission range, and each simulation runs for a period of 900sec. The above settings could represent a MANET scenario in real life; like a University campus. Note that the number of mobile nodes could be larger than the one presented in these scenarios and the operational time could be longer; the values chosen are to keep the simulation running time manageable while still generating enough traces for analysis. Flows of Constant Bit Rate (CBR) unicast data packets, each with size 512 bytes.

In this study, mobile nodes move according to the widely used random waypoint mobility model where each node at the beginning of the simulation remains stationary for pause time seconds, then chooses a random destination and starts moving towards it with a speed selected from a uniform distribution [0, V max]. Other simulation parameters used in this research study have been widely adopted in existing performance evaluation studies of MANETs and are summarized below in Table 1.

TABLE I. SYSTEM PARAMETERS USED IN THE SIMULATION EXPERIMENTS.

Simulation Parameter	Value
Simulator	NS-2 (v.2.31)
Transmitter range	250 meter
Bandwidth	2 Mbps
Traffic type	CBR
Number of Nodes	30
Topology size	1500m x 300m
Packet size	512 bytes
Simulation time	900 sec

V. PERFORMANCE METRICS

In order to evaluate the performance of our proposed Intrusion Detection System DIPDAM, we will focus mainly on evaluating four performance metrics:-

a) Average overhead:

The average overhead is defined as the total number of data packet and routing control packets normalized by the total number of received data packets.

b) Average Packet Delivery Ratio (Rating):

It is the ratio of the number of packets received successfully to the total number of packets transmitted.

c) Average Packet dropping:

The average packet dropping is the average percentage of data packet dropped to all data and control packets sent from the sources to the destinations.

d) Average end-to-end delay:

The end-to-end-delay is the average overall delay measured from the sources to the destinations.

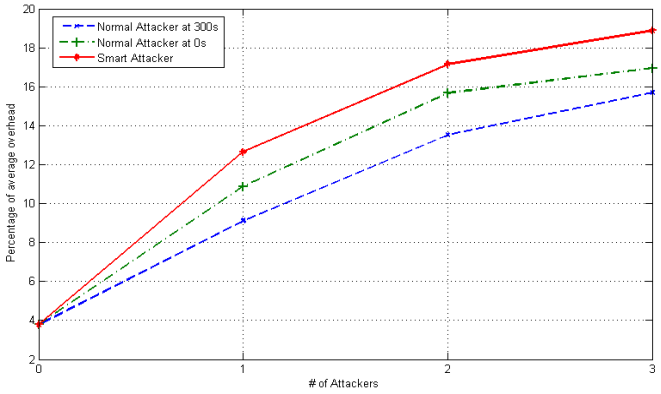

Fig.5. Average percentage of overhead vs. numbers of attackers.

Figure 5 shows that the average overhead increases directly with the numbers of attackers. The increase in the percentage

of overhead compared to the original OLSR came from three major reasons. Firstly, PVM messages inserted within data packet to monitor the path between the source and the destination. Secondly, due to AFM messages used to find attackers through the transmission path. Finally, because of AIM messages needed to isolate the attacker from the routing path.

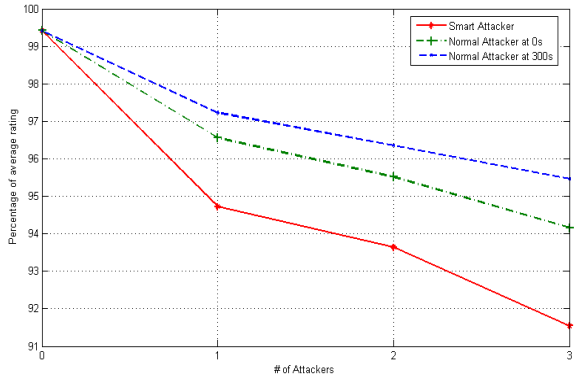

Fig.6. Percentage of average rating vs. numbers of attackers.

As shown from figure 6 the percentage of average rating almost decreases linearly with the increase of the number of attackers. The decrease is due to the dropped data attacker found in routing path.

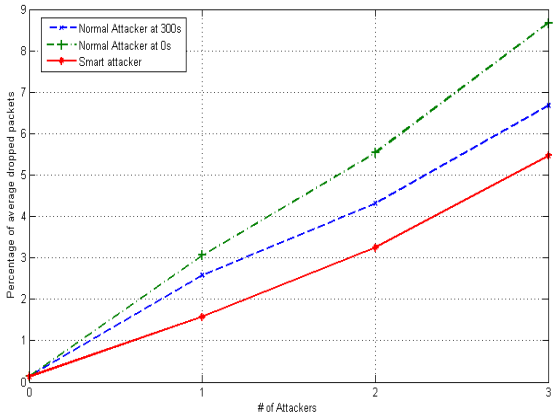

Fig.7. Percentage of average dropped packets vs. number of attackers.

As shown in figure 7, the percentage of average dropped packets almost increases linearly with the increase of the number of attackers. The increase in is due to the dropped data attacker found in routing path.

Average End-to-End delay versus the number of attackers is shown in fig. 8.

Results obtained in the above figure illustrate an increase in the average delay as the number if attackers increase. The increase of E2E delay comes from two major reasons.

Firstly, the network takes some time to detect and isolate the attacker. Secondly, since the attacker damaged the routing path, the process to recalculate an alternative routing path needs extra time which results in the increase of the average E2E delay time

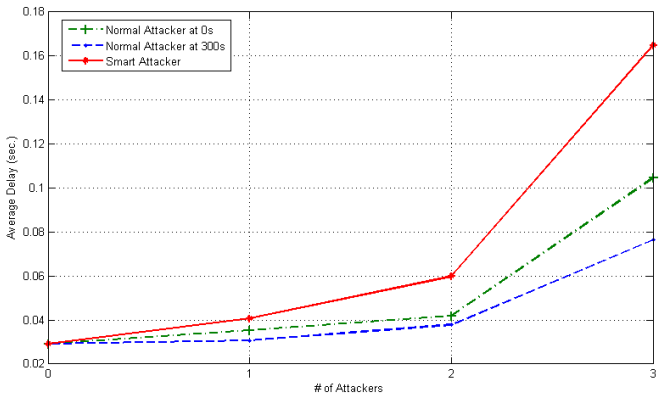

Fig.8. Average End to End Delay vs. number of attackers.

Table 2 shows a sample from the detection process results. The table contains the attacker detector node, transmission path, attacker node, and the attacker type. Table 2 shows that source nodes 13, 19, and 28 were able to detect the attacker's nodes 12, 14, and 21 successfully when present in the path. The results show that the accuracy of detection is independent of the path length or the location of the attacker in respect to the detector. The detection procedure also can detect different types of attackers found in the network at the same time

TABLE II. SAMPLE LIST OF ATTACKERS DETECTED.

Detector	Path	Attacker	Attacker type
28	28.12.23.26.26.23.0	12	Normal
28	28.1.14.0	14	Smart
28	28.21.5.0	21	Normal
19	19.16.9.12.0	12	Normal
19	19.7.14.23.0	14	Smart
19	19.21.13.0	21	Normal
13	13.21.4.0	21	Normal

VI. DISCUSSION

From the above figures, It can be concluded that DIPDAM mechanism achieved better performance metrics when the attacker is a normal attacker and its attacking action after certain amount of time from the beginning of the simulation test.

On the other hand the smart attacker type take larger time, higher overload, more dropping packet, and worst average rating compared to other attacker types discussed. It is expected that this result is due to deep processing to detect and isolate the smart attackers.

VII. CONCLUSION

We have presented IDS mechanism based on End-to-End connection for securing OLSR routing protocol. DIPDAM mechanism can detect and isolate many types of misbehavior node(s) through the path between the source and the destination

then a blacklist of misbehavior nodes is created and broadcasted to 1-Neighbors IDS mechanism was proposed for Detection and Isolation of Packet-Dropped Attacker in MANETs (DIPDAM).

DIPDAM, a fully-distributed message exchange framework designed to overcome the challenges caused by the decentralized and dynamic characteristics of MANETs.

DIPDAM performance was inspected using different comparable performance metrics to show its reliability and efficiency in detection and isolation many types of misbehavior nodes.

Three ID messages are proposed to implement DIPDAM Path Validation Message (PVM) enables E2E feedback loop between the source and the destination, Attacker Finder Message (AFM) to detect attacker node through the routing path, and Attacker Isolation Message (AIM) to isolate the attacker from routing path and update the black list for each node then trigger to neighbors with updated information.

VIII. FUTURE WORK

Our mechanism must be tested in real MANETs with different conditions like variation on mobility, size, network traffic type, and node density.

DIPDAM mechanism may be upgraded to detect both types of attackers, data packet attackers and route packets attackers.

The same mechanism can be tried on different Manet's protocols from other categories.

REFERENCES

[1] Ahmed M. Abdalla, Imane A. Saroit, Amira Kotb, Ali H. Afsari,"An IDS for Detecting Misbehavior Nodes in Optimized Link State Routing Protocol", International Journal of Advanced Computer Science, Vol. 1, No. 2, Pp. 87-91, Aug. 2011.

[2] Ahmed M. Abdalla, Imane A. Saroit, Amira Kotb, Ali H. Afsari," Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol", World Conference on Information Technology. Procedia Computer Science volume 3, 2011, pages 115–121.

[3] Y. Huang and Wenke Lee, "Attack analysis and detection for ad hoc routing protocols", In Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pages 125-145. Springer, 2004.

[4] A. Fourati, K. Al Aghha "An IDS First Line of defense for Ad Hoc Networks", in Proceeding of 2007 IEEE WCNC.

[5] Y-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks," in Proceedings of the MobiCom 2002, Atlanta, Georgia, USA, September 23-28, 2002.

[6] C. Adjih, Th. Clausen, Ph. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the OLSR protocol," In Proceedings of Med-Hoc-Net, Mahdia, Tunisia, June 25, 2003.

[7] D. Dhillon, T.S. Randhawa, M. Wang and L. Lamont, "Implementing a Fully Distributed Certificate Authority in an OLSR MANET," IEEE WCNC2004, Atlanta, Georgia USA, March 21-25, 2004.

[8] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "An Advanced Signature System for OLSR," in Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 04), Washington, DC, USA, October 25 2004.

[9] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks Against OLSR: Distributed Key Management for Security," 2nd OLSR Interop/ Workshop, Palaiseau, France, July 28-29, 2005.

[10] [Peter Glaus, "Locating a Black Hole without the Knowledge of Incoming Link", Algorithmic Aspects of Wireless Sensor Networks, Lecture Notes in Computer Science, Volume 5304. Springer-Verlag Berlin Heidelberg, 2009, p. 128, http://www.springerlink.com/index/h8424573040077v5.pdf

[11] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Network", in 6th International Conference on Mobile Computing and Networking, MOBICOM'00, p255-265, Aug 2000.

[12] Nidal Nasser, Yunfeng chen, "Enhanced Intrusion Detection System for Discovering Malicious Node in Mobile Ad hoc Networks", Communications, 2007. ICC '07. IEEE International Conference on Publication Date: 24-28 June 2007, page(s): 1154-1159.

[13] Baras, John S. Radosavac, Svetlana Theodorakopoulos, George Sterne, Dan Budulas, Peter Gopaul, Richard " Intrusion Detection System Resiliency to Byzantine Attacks: The Case Study of Wormholes in OLSR", Military Communications Conference, 2007. MILCOM 2007. IEEE Publication Date: 29-31 Oct. 2007, page(s): 1-7, Orlando, FL, USA.

[14] Shanshan Zheng Tao Jiang Baras, J.S. Sonalker, A. Sterne, D. Gopaul, R. Hardy, R. "Intrusion detection of in-band wormholes in MANETs using advanced statistical methods", Military Communications Conference, 2008. MILCOM 2008. IEEE Publication Date: 16-19 Nov. 2008, page(s): 1-7, San Diego, CA.

[15] M.T. Refaei, Yanxia Rong, L. A. DaSilva, and Hyeong-Ah Choi, "Detecting Node Misbehavior in Ad hoc Networks", Communications, 2007. ICC '07. IEEE International Conference on Publication Date: 24-28 June 2007, page(s): 3425-3430, Glasgow.

[16] J.P. Vilela and J. Barros, "A Feed Reputation Mechanism to Secure the Optimized Link State Routing Protocol", The 3rd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks, Nice, France, September 2007.

[17] J.P. Vilela and J. Barros, "A Cooperative Security Scheme for Optimized Link State Routing in Mobile Ad-hoc Networks", Proc of the 15th IST Mobile and Wireless Communications Summit, Mykonos, Greece, June 2006.

[18] Asmaa Adnane , Rafael T. de Sousa, Jr., Christophe Bidan, Ludovic Mé, " Autonomic trust reasoning enables misbehavior detection in OLSR", Proceedings of the 2008 ACM symposium on Applied computing, Pages 2006-2013.

[19] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "A Collusion Attack Against OLSR-based Mobile Ad Hoc Networks", in Proceeding of 2006 IEEE GLOBECOM.

[20] Y. Rebahi, V. Mujica, C. Simons, and D. Sisalem, "SAFE: Securing pAcket Forwarding in ad hoc nEtworks", In 5th Workshop on Applications and Services in Wireless Networks 2005.

[21] Sevil Sen, "Evolutionary Computation Techniques for Intrusion Detection in Mobile Ad Hoc Networks", PhD Thesis, University of York Department of Computer Science, March 2010.

[22] The Vint Project, "The Network Simulator –ns-2," http://www.isi.edu/nsnam/ns/index.html

[23] F. J. Ro, "UM-OLSR Documentation," University of Murcia, March 2005, http://masimum.dif.um.es/um-olsr/html