Performance Evaluation for the DIPDAM schemeon the OLSR and the AODV MANETs Routing Protocols

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

***Abstract*—the DIPDAM scheme is a fully-distributed message exchange framework designed to overcome the challenges caused by the decentralized and dynamic characteristics of mobile ad-hoc networks. The DIPDAM mechanism is based on three parts 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. The DIPDAM scheme was fully tested on the OLSR routing protocol. In order to prove the efficiency of DIPDAM scheme on detection and isolation packet dropping attackers, DIPDAM is applied to another routing protocol category, AODV. AODV represents different concepts in routing path calculation and it is widely adopted. The comparison between the two routing protocol is tested onsmart attackers. The goal from this comparison is to prove that the DIPDAM scheme can be applied to a different routing protocols category.**

Keywords—Ad hoc networks; AODV; Computer network management; IDS;MANETS; OLSR

I. INTRODUCTION

A mobile ad-hoc network (MANET) is categorized under infrastructure less network where a number of mobile nodes communicate with each other without any fixed infrastructure between them. Furthermore, all the transmission links are established through wireless medium [1].

The DIPDAM scheme [2, 3, 4] is a fully-distributed message exchange framework designed to overcome the challenges caused by the decentralized and dynamic characteristics of MANETs.

The collaboration of a group of neighbor nodes is used to make accurate decisions. Eliminating misbehavior node(s) enables the source to select another trusted path to its destination. In order to lower message exchange overhead aswell as to achieve scalability, message exchange is triggered only when new detection is observed, and only occurs with local neighbors.

DIPD AM scheme enables routing protocols to detect packet dropping frauds. In fact, source nodes in the network independently monitor the behavior of their own data when transferring through routing path, however, they need to collaborate in order to identify and isolate the intruders. This scheme is based on the reputation concept.

In this paper the DIPDAM scheme is tested on two different MANETs routing protocols, the OLSR and the AODV. The scheme is evaluated using four different performance metrics. Furthermore, the detection accuracy and false positive rate are calculated for the two routing protocols.

II. PREVIOUS WORK

For Mobile Ad-hoc Networks, the general function of anIntrusion Detection Systems (IDS) is detecting misbehaviors by observing the networks traffic in a Mobile Ad-hoc [5]. Most of recent researches focused on providing preventive schemes to secure routing in MANETs [6-10]. Key distribution and an establishment of a line of defense defined in [6], [6] based on mechanism in which nodes are either trusted or not and if trusted they are not compromised. Also contribution in [8], [10] 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 [11]. In [12] a survey of different network layer attacks on MANET was provided and compared the existing solutions to combat single or cooperative black hole attack.

A feedback mechanism to secure OLSR against the link spoofing attacks was provided in [13, 14]. 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.

The proactive protocols are Table-Driven protocols in which each node maintains up-to-date routing information about every other node in a routing table and routes are quickly established without any delay [15].

Researchers in [16, 17] describes an explicit security issue on AODV Routing Protocol Suffering from Black Hole Attack. Source node sends the routing information to the nasty node which essentially cannot have a path to destination node

in its own routing table. It thinks that fake route reply and it ignores the message without passing to destination. Authors also include the exact method to overcome the Black Hole Attack by providing a new method called Secured AODV (SAODV). It provides an additional procedure to AODV algorithm by requesting source node to broadcast the Secured Route Request along with random sequence number to destination. Destination checks whether source request sequence number from two or more path are the same.

III. COMPARING AODV AND OLSR PROTOCOLS

AODV and OLSR protocols are compared with respect to resource usage, mobility, and route discovery delay. Being a proactive protocol, OLSR imposes large control traffic overhead on the network. Maintaining up-to-date routing table for the entire network calls for excessive communication between the nodes, as periodic and triggered updates are flooded throughout the network. The use of MPR's reduces this control traffic overhead, but for small networks, the gain is minimal. The traffic overhead also consumes bandwidth. The creativeness of AODV is more sensitive to resource usage than OLSR. As control traffic is only emitted during route discovery, most of the resource and bandwidth consumption is related to actual data traffic.

A. Resource usage

Since information about the entire network needs to be maintained at all times, OLSR requires relatively much storage complexity and usage. Hence, there is a greater demand for storage capacity of nodes in such networks.

Also, the control overhead adds to the necessary processing in each node, hence increasing the battery depletion time. Another downside to OLSR is that it must maintain information about routes that may never be used.

AODV, on the other hand, only stores information about active routes at a node, which considerably simplifies the storage complexity and reduces energy consumption. The processing overhead is also less than OLSR, as little or no useless routing information is maintained.

B. Mobility

OLSR and AODV have different strengths and weaknesses when it comes to node mobility in MANETs. Unlike wired networks, the topology in wireless ad-hoc networks may be highly dynamic, causing frequent path breaks to ongoing sessions. When a path break occurs, new routes need to be found. As OLSR always have up-to-date topology information at hand, new routes can be calculated immediately when a path break is reported. In comparison, since AODV is a reactive protocol, this immediate new route calculation is not possible, so a route discovery must be initiated. In situations where the network traffic is sporadic, OLSR offers less routing overhead due to having found the routes proactively. AODV, on the other hand, will need to discover a route before the actual information can be transmitted. This calls for extensive control overhead per packet. In cases where the network traffic is more or less static (i.e., the traffic has a long duration), however, AODV may perform better, as the amount of control overhead per packet decreases.

TABLE I. AODV VS. OLSR ROUTING PROTOCOLSCOMPARISON.

Parameters	AODV routing protocols	OLSR routing protocols
Availability of routing	Available as required	Always available
Periodic route updates	Not required	Required
Dealing with Link	Use route discovery	Propagate information to neighbors to maintain consistent routing table
Routing overload	Increases with mobility of nodes	Independent of traffic and mostly greater than On-demand protocols

C. Route discovery delay

When a node in a network running the OLSR protocol needs to find the route to a host, it is only required to do a routing table lookup, whereas in a AODV network, a route discovery process need to be initialized unless no valid route is cached.

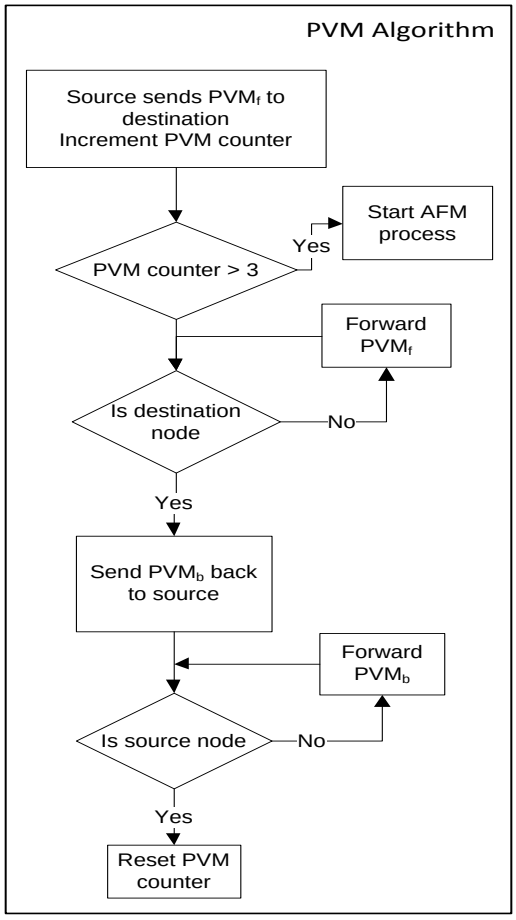

Fig. 1. Flow chart for Path Validation Message (PVM) algorithm

1 Source sends AFM_f to Destination and starts a waiting time
2 **If** receiver node = destination **then**
3 Send AFM_b back to source
4 **Else**
5 Forward AFM_f to destination
6 Send AFM_b back to Source with information about next-node-to-destination(NNTD) and availability of route to destination in the routing table
7 **End if**
8 **If** Source received AFM_b came from Destination **then**
9 No attacker detected, start advanced detection
10 Cancel AFM wait timer
11 Send PVM to each node in path to D
12 **If** Source receive PVM from intermediate node **then**
13 Node is trusted
14 **Else**
15 Malicious node of type-N2 is detected.
16 Add to blacklist table and end AFM process
17 **End if**
18 **Else**
19 Last NNTD known by S is suspected as type-N1 attacker
20 Send PVM to NNTD
21 **If** PVM received **then**
21 NNTD is a trusted node
22 **Else**
23 NNTD is confirmed as an attacker
24 **End if**
25 **End if**

Fig. 2. Attacker Finder Message (AFM) algorithm.

It goes without saying that a table-lookup takes less time than flooding the network, making the OLSR protocol performance better in delay-sensitive networks. Table 1 summarizes basic differences between the two protocols classes.

IV. Detection And Isolation Of Packet Dropped Attackers In Manets (DIPDAM)

New 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 [18]. 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 scheme, 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.

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.

To evaluate the robustness of DIPDAM scheme we tested MANETs under different attacker types [19].

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.

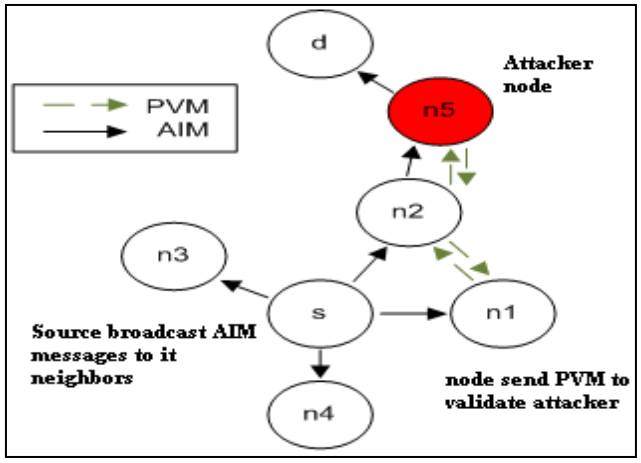

Fig. 3. Attacker Isolation Message (AIM) process.

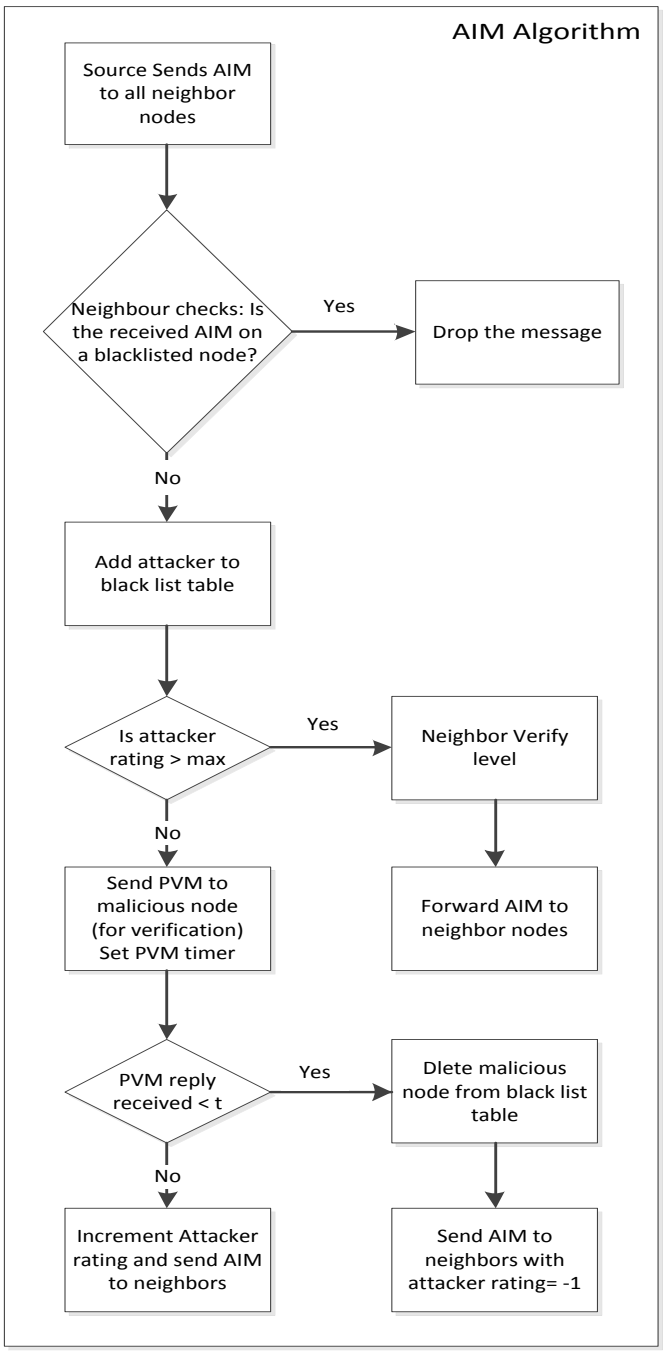

Fig. 4. Flow chart for AIM algorithm.

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 N1typeand N2 type. N3type selfish nodes will be detected only when they behave similar to N1or N2type 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.

Network Simulator program

The NS-2 simulation tool [20-21] consists of two kinds of scenarios; 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 way point 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 2.

TABLE II. 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:-

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.

Average Packet Delivery Ratio (Rating):

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

Average end-to-end delay:

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

A. *Percentage of Overhead*

The first performance metric used in comparison is the percentage of average overhead. Fig..5illustrates the percentage of average overhead in both routing protocol (OLSR & AODV) versus the number of attackers.

From Fig.5, it is clear that when the attacker numbers is relatively small AODV protocol achieve better average overhead than OLSR.

Increasing the number of attackers leads to an increasing in the average overhead in AODV, with the rate higher than OLSR. When the number of attackers is increased more, the OLSR achieves better percentage of average overhead than AODV.

The increase of the attacker numbers leads to the increase of lost links, then AODV will produce more control messages (like RREQ and RREP). These control messages will be broadcasted throughout the network nodes to create an alternative routing path causing the overall overhead to increase rapidly. These results are expected as OLSR is more stable than AODV and it is less affected with network changes than AODV.

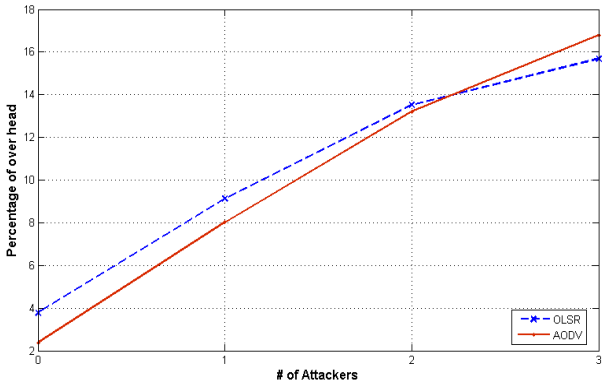

Fig. 5. Percentage of overhead vs. number of attackers.

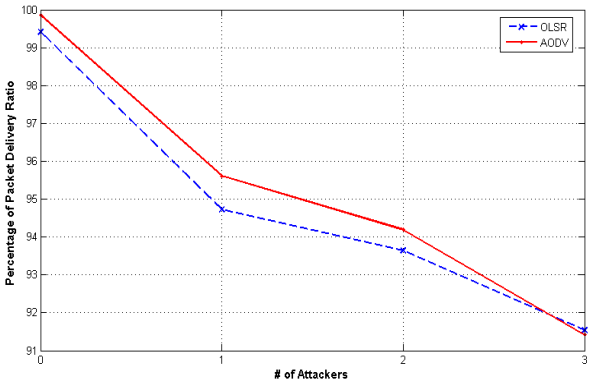

Fig. 6. Percentage ofPacket Delivery Ratio vs. number of attackers.

B. *Percentage of Packet Delivery Ratio*

The average packet delivery ratio performance metric in both routing protocol (OLSR & AODV) is showed in Fig..6. The results presented in the figure show that the AODV routing protocol achieves better average packet delivery ratio than OLSR routing protocol, especially when the number of attackers are relatively small. As the number of attackers increase, the average packet delivery ratio in AODV decreases at a rate higher than OLSR. When a certain number of attackers is reached (about 10% from the total nodes) the OLSR will perform better than the AODV.

The average packet delivery ratio in OLSR is slightly higher than that in AODV when the number of attackers is large. AODV needs to recalculate the routing path because the routing path expires if it is not used for a certain time or if the path is broken. During the recalculating process, the source node will not be able to send its data. The higher the number of attackers makes the recalculation process take more time, which affects the average packet delivery ratio.

C. *Percentage of Dropped packets*

The percentage of average dropped packet performance parameter in both routing protocols (OLSR & AODV) is plotted against the number of attackers as shown in Fig.7.

Fig. 7 results show that the value of the percentage of average dropped packets recorded is remarkably small when no attacker is found in the networks. The percentage of

average dropped packets in the OLSR protocol increaseslinearly with the number of attacker, but the increasing is nonlinear in the AODV protocol .

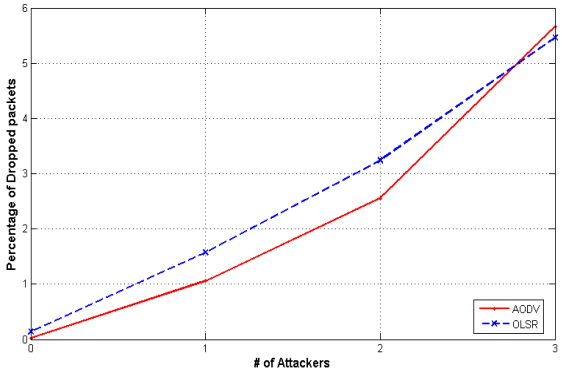

Fig. 7. Percentage of Dropped packets vs. number of attackers.

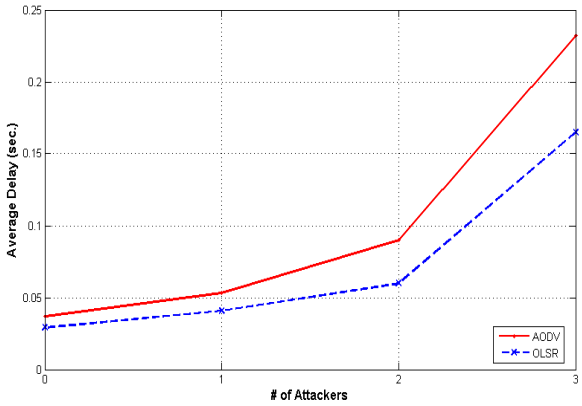

Fig. 8. Average End to End delay (sec.) vs. number of attackers.

Fig.7 results show that the value of the percentage of average dropped packets recorded is remarkably small when no attacker is found in the networks. The percentage of average dropped packets in the OLSR protocol increases linearly with the number of attacker, but the increasing is nonlinear in the AODV protocol .

The results obtained from Fig.7 show that the percentage of dropped packets in AODV is always less than OLSR when the number of attackers is relatively less than 10% of the total network nodes .

When the number of attackers approaches nearly 10% of the total nodes, the ADOV averaged dropped packet value exceeds the OLSR value. The greater the number of attackers leads to greater lost links. The recovery time in AODV is slower than OLSR because OLSR protocol maintains its routing paths periodically while AODV recalculates its path when the source needs to send data. The recalculation process requires more computational process and time.

D. Average End-to-End delay

The fourth performance metric measured is the average end to end delay. The results against the number of attackers in both routing protocol is shown in Fig. 8.

It is noticed from Fig.8 that the values of average End-to-End delay produced by OLSR protocol is always less than the values of AODV. The routing path in OLSR is always available irrespective of the source needed to transmit data or not. AODV calculates the routing path only if the source needs to send data to its destination. The data remains waiting until the routing path calculation is completed, and then the data is forwarded to its destination. That led to the OLSR achieving a better average End-to-End delay than AODV. Since lost links in AODV need extra computational time to recalculate the routing path, the End-to-End delay in OLSR was less than AODV when the number of attackers becomes larger. In OLSR, the routing path is always ready, and there is no need to calculate it.

TABLE III. DETECTION RATE AND FALSE POSITIVE RATE

Routing Protocols	Detection rate	False Positive rate
OLSR	99.42 ±0.5%	1.1±0.01%
AODV	98.96±0.5%	1.21±0.012%

VI. DETECTION ACCURACY AND FALSE POSITIVE VALIDATION TESTS

To validate the DIPDAM scheme two more factors are measured for OLSR and AODV routing protocols: detection accuracy and false positive rate are calculated. Experimental results showed that DIPDAM in both OLSR and AODV achieved high performance with remarkably low false positives, and very high detection rate in any environment with high mobility, as shown in Table 3.

VII. DISCUSSION

From the performance metrics figures, it is obvious that the DIPDAM scheme can be considered as an effective scheme to detect and isolate any number of attackers from routing paths, irrespective of the routing protocol type.

AODV routing protocol achieved better performance metrics when the number of attackers is relatively small to the network size. On the other hand the OLSR seemed to be a more stable routing protocol in larger networks and achieved better performance than AODV, especially when the number of attackers was large.

It is clear that the AODV is more flexible for security solutions than the OLSR in small networks. Performance metrics of AODV protocol highly depends on the number of attackers, but OLSR protocol keeps the network performance the same, irrespective of the number of attackers.

DIPDAM performed efficiently with the validation tests performed. The scheme achieved high detection ratewith impressive low false positives on both the OLSR and the AODV protocols.

VIII. CONCLUSION

DIPDAM has been successfully implemented in OLSR and AODV. Experimental results show that DIPDAM in both

OLSR and AODV has low message overhead and low detection delay. This achieves higher performance with remarkably low false positives, and remarkably high detection rate in an environment with high mobility. Also, DIPAM proved to be a practical, scalable, and effective solution for securing both OLSR and AODV.

The simulation results showed that DIPDAM scheme was able to detect and isolate any number of attackers, while keeping a reasonably low overhead in terms of network traffic. The four performance metrics of the experiment demonstrate that the DIPDAM system can detect packet dropping attacks in both routing protocols (OLSR and AODV) with low message overhead, low detection delay, high rating under message loss and mobility conditions.

According to the simulation results, AODV protocol will perform better in networks with static traffic and relatively small numbers of attackers for the same network size of OLSR.AODV uses lower resources than OLSR, because the control message size used in AODV is kept small and requires smaller bandwidth for maintaining the routes. The AODV routing protocol maybe used in resource critical environments.

IX. FUTURE WORK

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

The same scheme can be tried on different MANETs protocols from other categories, like multicast protocols. DIPDAM scheme can be upgraded to detect both types of attackers, data packet attackers and routing packets attackers.

REFERENCES

[1] F.Tseng, L. Chou, and H. Chou. “A survey of Black Hole Attacks in wireless mobile ad-hoc networks”, Human-centric Computing and Information Sciences, 2011

[2] A.Abdalla, I. Saroit, A. Kotb, and A.Afsari. “An IDS for Detecting Misbehavior Nodes in Optimized Link State Routing Protocol”, International Journal of Advanced Computer Science, 1 (2), pp. 87-91, 2011

[3] A. Abdalla, I. Saroit, A. Kotb, and A. Afsari. “Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol”, World Conference on Information Technology. Procedia Computer Science,3, pp. 115–121, 2011

[4] A. Abdalla, A.Almazeed, I. Saroit, A. Kotb, and A.Afsari. “Detection and Isolation of Packet Dropping Attacker in MANETs”, International Journal of Advanced Computer Science and Application, 4 (4), pp. 29-34, 2013

[5] A. Fourati, and K. AlAghha.“An IDS First Line of defense for Ad Hoc Networks”, in Proceeding of IEEE WCNC, 2007

[6] Y. Hu, A. Perrig, and D. Johnson.“Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks”, Proc. of the MobiCom, Atlanta, Georgia, USA, 2002.

[7] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo. “Securing the OLSR protocol”, Proc. of Med-Hoc-Net, Mahdia, Tunisia, June 25, 2003.

[8] D. Dhillon, T.Randhawa, M. Wang and L. Lamont. “Implementing a Fully Distributed Certificate Authority in an OLSR MANET”, IEEE WCNC2004, Atlanta, Georgia USA, 2004.

[9] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler.“An Advanced Signature System for OLSR”, Proc. of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 04), Washington, DC, USA, 2004.

[10] C. Adjih, D. Raffo, and P. Muhlethaler. “Attacks Against OLSR: Distributed Key Management for Security”, 2nd OLSR Interop/Workshop, Palaiseau, France, 2005.

[11] P. Glaus. “Locating a Black Hole without the Knowledge of Incoming Link, Algorithmic Aspects of Wireless Sensor Networks”, Lecture Notes in Computer Science, Vol. 5304. 128, 2009.

[12] N.Kaushik, and A.Dureja.“A comparative study of black hole attack in MANET” , International Journal of Electronics and Communication Engineering & Technology (IJECET) 4(2), 2013.

[13] J.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, 2007.

[14] J.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, 2006.

[15] P.Jaiswal, and R. Kumar.“Prevention of Black Hole Attack in MANET”, International Journal of Computer Networks and Wireless Communications (IJCNWC), 2(5), 2012.

[16] K. Lakshmi, S. Manjupriya, A. JeevaRathinam, K. Ram, and K. Thilagam. “Modified AODV Protocol against Black hole Attacks in MANET”, Proc, on International Journal of Engineering and Technology, 2(6), pp. 444-449, 2010.

[17] K.Taneja, and M. Rachna.“Security Issue on AODV Routing Protocol Suffering From Black holeAttack”. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE),1(7), 2012.

[18] 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.

[19] S. Sen. “Evolutionary Computation Techniques for Intrusion Detection in Mobile Ad Hoc Networks”, doctoral diss., University of York Department of Computer Science, 2010.

[20] The Vint Project, “The Network Simulator –ns-2”. March 2005,www.isi.edu/nsnam/ns/index.html.

[21] F. J. Ro. (2005).“UM-OLSR Documentation”, University of Murcia. March 2005, http://masimum.dif.um.es/um-olsr/html