www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 10 Oct. 2016, Page No. 18649-18654

Black Hole Attack Detection Using HlA with Optimized Link State Routing Protocol In Wanet

J.JenoMactaline Pears[1], Dr.D.C.Joy Winnie Wise[2]

[1]PG Student of CSE,
piyapears1994@gmail.com

[2]Professor & Head, Department of CSE,
joywinniewise@yahoo.com
Francis Xavier Engineering College, Vannarpettai, Tirunelveli-627003, Tamilnadu, India

Abstract: A wireless ad-hoc network also known as autonomous Basic Service Set which is a computer network in which the communication links are wireless. In ad-hoc network each node can forward data for other nodes and so the determination of which nodes forward data is made dynamically depended on the network connectivity. There are two kinds of sources that providing packet losses are link failure and dropping of packets by adversary activities in multi-hop wireless ad hoc network. While observing a continuous packet losses in the network for determining whether the packet drops are occurred by link errors or by the joined effect of link errors and malicious drop. To improve the detection accuracy of adversary an enhanced Optimized Link State Routing Protocol (OLSR) is used to correctly broadcast the routing protocol control traffic on behalf of other nodes. Homomorphic Linear Authenticator (HLA) based public auditing scheme allows the detector to calculate the truthfulness of the packet loss information informed by nodes. This algorithm is privacy preserving and find the optimal path during transmission.

Keywords*:* packet loss, Attacker detection, Homomorphic Linear Authenticator (HLA), optimized link state routing protocol (OLSR)

1. Introduction

In a multi-hop wireless network the packets transfer from source to destination through nodes. Nodes support in relaying/routing traffic. The malicious node can exploit this cooperative nature to launch attacks. Initially the malicious node, process in a cooperative way until it discover the path from source to destination when it is added into the path, the node starts to loss the packets i.e. upstream node can forward packet via malicious node. But the malicious node stops forwarding nearly all the packets to the downstream node. This type of packet dropping is called as persistent packet dropping. This packet dropping completely reduces the performance of the network. But it is very simple to identify this type of packet dropping.

Selective packet dropping is another type of packet dropping. It is quite different from persistent packet dropping. Here malicious node analyze the importance of various packets and drops those packets that are very essential. This type of packet dropping also reduces the performance of the network. But here the possibility of detecting dropped packet is very lower than the persistent packet dropping. Detecting selective

Packet dropping is more complex in a highly dynamic wireless environment because the hop must be identifiedand also finds whether the packet drop is intentional or unintentional. Intentional packet dropping is caused by attackers node and unintentional packet dropping is caused by harsh channel conditions. The link error always occurs in the open environment. So the attacker may use the harsh channel condition to drop the small amount of packets. The packet dropping rate should be higher than the link error for the accurate detection.

The algorithm helps to find the malicious packet drop. Here detection accuracy is more accurate which is achieved by finding the correlation of lost packets which is done by using the bitmap of packet arrival provided by each node. The packets that are lost help to conclude whether packet loss is caused only because of link error or by the combination of both link error and malicious packet drop.Evaluation of cooperation between the nodes is very important. To ensure the information provided by each node HLA cryptographic primitive [1] is used. This mechanism provides some extra new features which include privacy preservation and reduce overheads between the intermediate nodes. But here frequent changes on topology and link characteristics have not been considered.

To improve the detection accuracy of adversary an enhanced optimized link state routing protocol (OLSR) is used and accurately detectmisbehavior node(s). The OLSR protocol achieves optimization by finding for each node of the network a minimal subset of neighbors, called Multi Point Relays (MPR).Which are able to arrive all 2-hop neighbors of the node. Generally two types of routing messages are used a HELLO message and a Topology Control (TC) message [16-17].

1) HELLO message is periodically transmitted by each node and contains the sender's identity information and three lists:

- List of neighbors of node from which control traffic has been heard.
- List of neighbors of node with which bi-directionality has already committed.
- List of MPR set of originator node.

HELLO messages are interchanged locally by neighbor nodes and are not forwarded again to other nodes. HELLO message

is used for neighbor sensing and also for preference of MPRs nodes

2) TC messages are also released periodically by MPR nodes. TC message includes the list of the sender's MPRSelector set. In OLSR, only MPR nodes are responsible for forwarding TC messages. Upon getting TC

The OLSR function can be given as follows:

Neighbor Sensing: To resolve that each node transmits to its 1-hop neighbors HELLO messages regularly.

MPR Selection: There are two different types of sets

MPRSet:This set contains the nodes from its 1-hop neighbors. When a node sends a routing message, only the nodes forward these messages that are in its MPR set Messages from all of the MPR nodes, each node can Detect Misbehavior Nodes in OptimizedLink State Routing Protocol learns the partial network topology and can build a route to every node in the network. This is used for route calculation

MPR Selector Set. Each node also maintains information about the set of nearby nodes that are selected as MPR which is known as MPR selector set.

Topology Diffusion: Nodes that were selected as MPR must send TC messages to design routing table. TC messages are flooded in the network and only MPRs are allowed to forward TC messages.

2. Related works

Packet dropping and malicious packet attack are the major problems in data transfer in Wireless ad-hoc network. Various packet dropping detection scheme have been proposed. The watchdog detection scheme [12] is a very useful technique for misbehavior node detection during packet transmission. In which, each node has a watchdog agent to store a packet copy before the transmission of that packet.This technique is helpful to finds the packet loss in the transmission. Due to False misbehavior and insufficient transmission power, this technique fails. And it also causes receiver collision problem. To tackle this problem Side Channel Monitoring (SCM) has proposed [13]. Instead of watch dog agent Subset of neighbors is used for monitoring. The information about misbehavior nodes is informed by Alarm channel. It detects packet drops more than the Watchdog Technique but it generates more network traffic and communication overhead.

To reduce the communication overhead TWOACK technique has introduced. In this technique, node can send a data packet and it expected to be received by node it must be two hops away in the path [14].The acknowledgment packets send by the node are called as the TWOACK pack. If the node did not sent a proper acknowledgment then it is considered to be a misbehaving node and that will be eliminated in the next routing. In order to reduce the acknowledgment, overhead selective-TWOACK was proposed. It reduces the overhead, but generate the problem of false alarms to tackle this problem 2ACK is proposed [4] but it has no ability to detect misbehaving node as it finds misbehaving link only and eliminates it.

Most of the recent researches focused on providing preventive schemes to secure routing in Wireless ad-hoc network [18-22]. Key dispensation and establishes a line of protection defined in [18], [19] is based on mechanism for in which nodes are either trusted or not. Also contribution in [20], [22] considers the compromise of trusted nodes. It is considered that a Public Key Infrastructure (PKI) in place. However, the above approaches cannot find attacks from the node. It is necessary to understand how malicious nodes can attack the ad-hoc network. A model to find the Black Hole Search problem algorithm and the number of coordinators that are necessary to locate the black hole without the understanding of incoming link Developed in [23].

Homomorphic linear authenticator (HLA) based public auditing scheme is developed that allows the Auditor to verify the truthfulness of the packet loss information informed by nodes [1]. A packet may be dropped at an upstream malicious node, so a malicious node in downstream does not collect this packet and the HLA signature from the route. However, this attacker can still open a back-channel to provide this information from the upstream malicious node. When being checked, the downstream malicious node can still supply valid proof for the reception of the packet.

So packet losses at the upstream malicious node are not discovered. Such collusion is unique to our problem, because in the cloud computing/storage server scenario, information is uniquely saved at a single server, so there are no other parties for the server to collude with. The new HLA construction is collusion-proof but it will not work in a dynamic environment. Instead of Dynamic Source Routing (DSR) [24], the Optimized Link State Routing protocol (OLSR) is used for finding the optimal path.

3. Proposed detection scheme

3.1 Overview:

Proposed mechanism has developed by adding new routing protocol Optimized Link State Routing Protocol (OLSR) with HLA. It is a proactive or table-driven routing protocol. Therefore it has the ability to quickly find routes when it is needed. During transmission, it reduces the size of the packets and it declares only a selected neighboring node then it minimizes flooding by using only the selected nodes. This technique highly reduces the number of retransmission.

3.2 HLA with Optimized Link State Routing Protocol

In System model assumes P_{sd} be an arbitrary path in a wireless ad hoc network. The path should be as $n_1,\ldots,n_k$, where n_1 is the upstream node of n_k, Routing in mobile ad-hoc network is very difficult because topology can change very rapidly. The proposed scheme of Optimized Link State Routing Protocol (OLSR) with HLA helps to find the packet losses effectively by providing optimal path during transmission.

Figure3.1 illustrates the system design of the proposed scheme. Initially Source node ready to transfer a packet and to find the correct routing path Optimized Link State Routing Protocol [OLSR] and trace route operation can be used by the sender node. During transmission packet losses will occur. At that situation, the receiver node can send a feedback to the sender. After receiving the feedback from the receiver, the sender can call the algorithm to find the unwanted link and the packets that are lost and also ensure the packet loss caused by the malicious attack or link error.

Then it removes the unwanted links and retransmits the packet without any packet dropping.

DOI: 10.18535/ijecs/v5i10.51

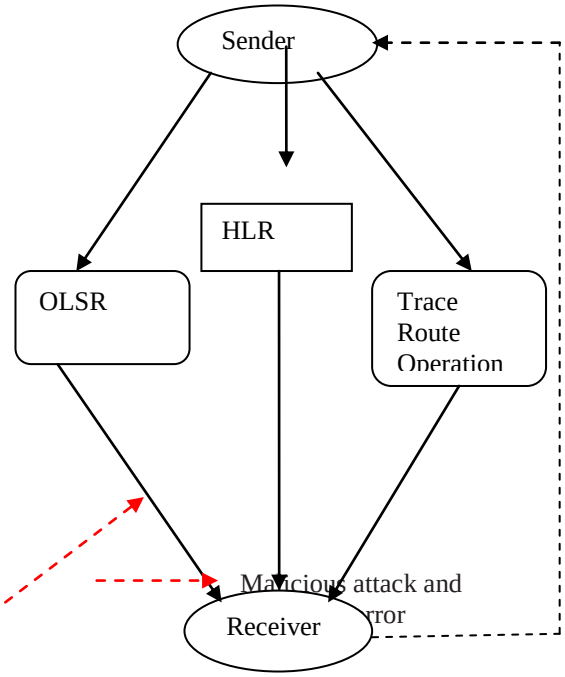

Figure 3.1: System Design

3.3 Path Discovery and replay Process

The Path Discovery Process (PDM) between source (S) and destination (D) under OLSR routing protocol is illustrated in Figure 3.2 Initially, the source broadcasts a PREQ (Path Request) message with a unique identifier to the neighbors of one hop. Then each receiver can rebroadcast this received message to its neighbors until it reaches the destination. The destination can receive the message and updates the sequence number of the source and sends a PREP (Path Reply) message back to its neighbor.

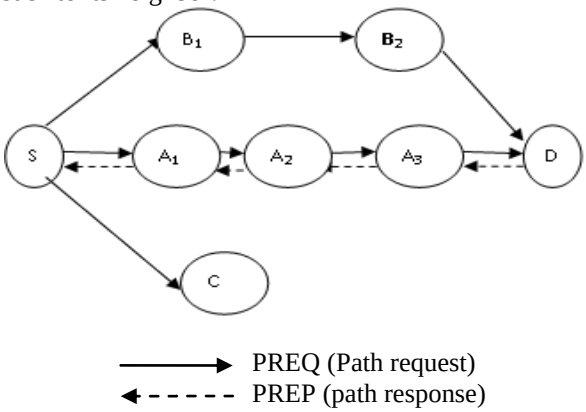

Figure: 3.2 Path Discovery Process

In this proposed scheme, an invalid path is distinguished from valid path therefore the security of the transmission is increased. The invalid path may contain some malicious nodes even though it sends the control packets as the normal intermediate node. Path discovery and reply process help to find the valid path by forwarding PREQ or PREP packets.

ALGORITHM - PDM PROCESSING

Source Send PDM to Destination as Data packets
Increment PDM counter
If PDM counter>3 then
    Start ADMalgorithm
End if
if receiver node = destination then
    Send PDM back to source
Else
    Forward PDM
End if
If receiver node = source then
    Reset PVM counter
End if

In Path discovery process, if the previous node is not a malicious node, it receives the CM packet (a small data packet) and it can be able to send the ACK to the intermediate node. But if it is a malicious node it drops the data packets and it is unable to send ACK to the intermediate node. Sometimes if a node that receives the CM packet fails to reply, then the intermediate node increase the number of count of sending CM packet. If the intermediate node finds there is a malicious node in the transmission path it will forward the information to all other nodes in the network. Then the data packets will be sending via another valid path in the network as shown in the figure3.2

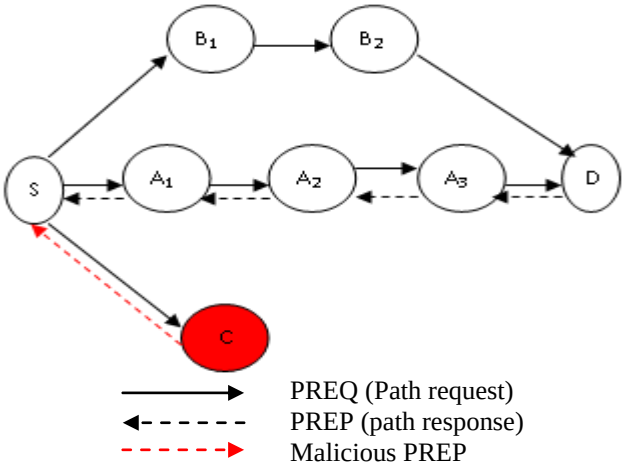

Figure: 3.3 Path Reply Process

3.4Attacker Detection Processing

In Attacker Detection Scheme, the processor can send Attacker Detection Message (ADM) to all nodes in the destination path through adjacent–node-to-destination (ANTD). Intermediates node needs to send an acknowledgment to the source node for a certain time. It updates the potential attacker information. If all the nodes along the path replied back to the source with ADM_b then the source starts the 2nd process of the attacker search. In this process, the source sends a packet to each node and waits for a particular period of time.

The intermediate node should reply back to the source before the interval time, and then only the source sends PDM to the next intermediate node in the path. This process is continued till the destination. If a node fails to reply within the particular interval time then it will be considered as attacker node and added to the black-list. This attacker is considered of type-2 where it was dropping the data packets (PDM) but not the control packets (ADM) an extra step is added to ensure the type-1 attacker is correctly detected. A PDM is sent to the attacker and if it replies back to the source then it is considered a false detection and removed from the black-list sequentially

ALGORITHM - ADP PROCESSING

Source sends ADP_f to Destination and starts a waiting time
If receiver node = destination then
    Send ADP_b back to source
Else
    Forward ADP_b to destination

DOI: 10.18535/ijecs/v5i10.51

Send ADP_b back to Source with information about adjacent-node-to-destination (ANTD) and availability of route to destination in the routing table

End if

If Source received ADP_b came from Destination then

No attacker detected,

start advanced detection

Cancel ADP wait timer

Send PDM to each node in path to D

If Source receive PDM from intermediate node then

Node is trusted

Else

Malicious node of type-2 is detected.

Add to blacklist table and end ADP

Process

End if

Else

Last ANTD known by S is suspected as type-1 attacker

Send PDM to ANTD

If PVM received then

ANTD is a trusted node

Else

ANTD is confirmed as an attacker

End if

End if

4. System Modules

Network Formation

N number of nodes is deployed randomly with 1500 x 1500 in network animator area.The parameters such as, transmission range of each node, maximum speed of a mobile node, the average number of hops from the source node to the destination node.

Packet Transmission Using OLSR

Optimized Link State Routing Protocol (OLSR) is an IP routing protocol optimized for wireless ad hoc networks, OLSR is a proactive link state routing protocol, which hello and topology control (TC) messages to discover and then disseminate link state information throughout the ad hoc networks. The source node sends the information via calculated shortest path routing. In case any failure in link this will disseminate the link failure information to all nodes.

Audit Phase

Auditor Ad is presented in the network. Ad is independent in the sense that it is not associated with any node in PSD and does not have any knowledge of the secrets (e.g., cryptographic keys) held by various nodes. The auditor is responsible for detecting malicious nodes on demand. Specifically, assume Sender S receives feedback from Destination D when Destination suspects that the route is under attack. Such a suspicion may be triggered by observing any abnormal events, e.g., a significant performance drop, the loss of multiple packets of a certain type, etc. The integrity and authenticity of the feedback from D to S can be verified by S using resource efficient cryptographic methods such as the homomorphic linear authenticators.

Detection Phase

Detecting malicious packet drops is a major problem in highly mobile networks, because the fast changes in topology of such networks makes route interference and causes packet losses. In this case, maintaining fixed connectivity between nodes is a greater problem than detecting malicious nodes. The function fc(i) can be calculated using the probing approach. A sequence of M packets is transmitted continuously over the channel. By observing whether the transmissions are successful or not, the receiver obtains a channel state (s1, . . . , sM), where sj € {0, 1} for j = 1, . . . ,M. In this sequence, “1” denotes the successful packet delivery, and “0” denotes the packet was dropped

5. Simulation results and discussions

The simulation results performed using the network simulator ns2 version 2.31.The OLSR protocol implementation follows RFC 3626.

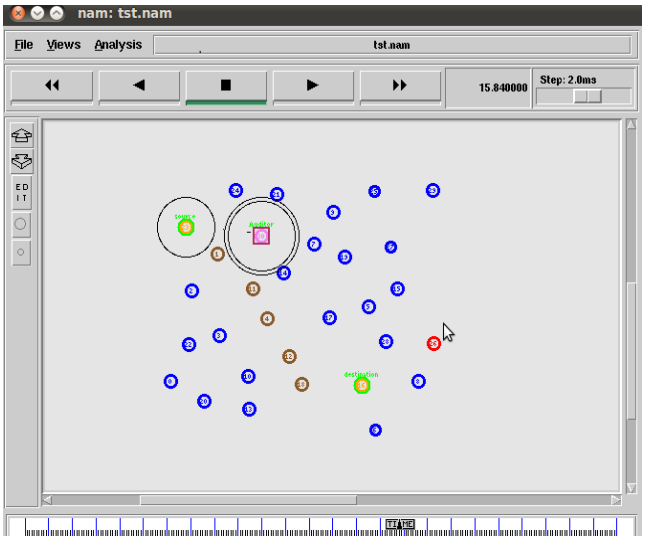

Figure 5.1 Packet losses due to link error

The major objective of simulation is successfully detecting the attackers. Here rectangular shape area is selected for good node scattering and collaboration. Initially, 31 nodes are deployed. The Source node can transmit a data packet through a path as 28.12.23.26.26.23.0. The auditor node can find the misbehaving node (12) by detector node. Detector node is the previous node of the misbehavior node. Then the auditor eliminate that misbehaving node and quickly find the optimal another routing path by OLSR routing protocol. And HLA scheme uses to find the collaboration between the lost packets to find whether the dropping is occurred by link error or malicious attack. Figure 5.1 illustrate the Link error packet dropping. After finding link error optimal route is selected for retransmission.

Table5.1 shows the packet loss bitmap. It maintains the detector and attacker list. In each path detector node is the previous node of the attacker node.

Detector	Path	Attacker
28	28.12.23.26.26.23.0	12

16	19.16.9.12.0	9
13	13.21.4.0	21

Table5.1 packet loss bitmap

Figure 5.1 illustrate the relation between a number of maliciously dropped packets and detection error probability and the detection accuracy is compared with existing algorithm (Maximum Likelihood algorithm) ML scheme. The proposed mechanism of OLSR with HLA improves the detection accuracy of packet dropping. This only utilizes the distribution of the number of lost packets. For given packet-loss bitmaps, the detection on different hops is conducted separately. So, only it is needed to simulate the detection of one hop to evaluate the performance of a given algorithm.

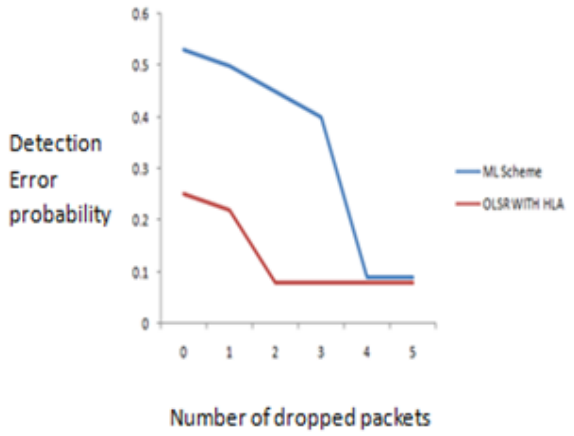

Figure 5.1 Detection error probabilities over number of dropped packets

Optimized Link State Routing protocol improves the probability of false alarm, probability of misdetection, and the overall detection-error probability.

Conclusion

The correlations of lost packet are correctly calculated. To ensure the truthfulness of information send by the nodes HLA based auditing with OLSR is used to provide privacy preserving collision avoidance and low communication storage overheads. And it improves the error probability detection.

Extension to dynamic environments will be studied in future work. Routing in wireless ad-hoc networks is difficult because the topology can change very frequently. By the time new transmission paths are discovered therefore packet losses can occur. Future work focusing on route packets successfully, even if the topology changes very rapidly.

Reference

[1]Tao Shu, Marwan Krunz, "Privacy –Preserving and Truthfull Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks",*IEEE Transactions on Mobile Computing*,April,2015

[2] M. A. Nowak, and K. Sigmund,"Evolution of indirect reciprocity," *Nature*, vol. 437, pp. 12911298,Oct.2005.

[3]4. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 536-550, May 2007

[4] D. B. Johnson, D. A. Maltz, and J. Broch. DSR: "the dynamic source routing protocol for multi-hop wirelessad hoc networks". Chapter 5, *Ad Hoc Networking*,

[5] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "Thefeasibility of launching and detecting jamming attacks in wireless networks*", In Proceedings of the ACM MobiHoc Conference*, pages 46–57, 2005.

[6] G.Ateniese, S.Kamara and J. Katz "proof ofstoragefromHomomorphic Identification protocols inproceedingsof the international conference on the theory and application of cryptology and information security".

[7]. Ramesh, V. Neelima, S. N.Kumar, T. Soujanya and R. S. Prakash, "Optimizing congestion in wireless Ad hoc Networks*", International Journal ofAdvanced Research in Computer Science and Software Engineering*, 2012

[8]Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation-based incentive scheme for adhoc networks," *in Proc. IEEE Wireless Commun. Netw. Conf., 2004*, pp. 825–830.

[9] AnindyaBasu, Alvin Lin, and SharadRamanathan, "Routing using potentials: A dynamic traffic-aware routing algorithm," *in Proceedings of ACM SIGCOMM'03,* Karlsruhe, Germany, August 2003, pp. 37–48

10]Charles E Perkins Elizabeth M Royer ―"Ad-hoc On Demand Distance Vector Routing"‖, 1999

[11] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks", *Proc. 6th Annual Intl. Conf. on Mobile Computing and networking* (MobiCom'00), Boston, Massachusetts, August 2000, pp. 255- 265.

[13] X. Li, R. Lu, X. Liang, and X. Shen, "Side Channel Monitoring: Packet Drop Attack Detection in Wireless Ad hoc Networks*", publication in the IEEE ICC proceedings*, 2011

[14] K. Balakrishnan, D. Jing and P.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", Wireless Communications and Networking *Conference, IEEE, 2005*

15] Changbing Tang, Ang Li, and Xiang Li, "When reputation enforces evolutionary cooperation in unreliable MANETs", Nov. 2014 8(5):579–592, Oct. 2003.

[16] T. Clausen, P. Jacquet, A. Laouati, P. Minet, P. Muhltahler, A. Qayyum, & L. Viennot, "Optimized Link State Routing Protocol," (2003) IETF RFC 3626.

[17] http://www.olsr.or

[18]On-Demand Routing Protocol for Ad hoc Networks," (2002) *in Proceedings of the MobiCom, Atlanta, Georgia, USA, September 23-28.*

[9] C. Adjih, Th. Clausen, Ph. Jacquet, A. Laouiti, P. Muhlethaler, &D. Raffo, "Securing the OLSR protocol," (2003) *InProceedings of Med-Hoc-Net*, Mahdia, Tunisia, June 25.

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

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

[22] C. Adjih, D. Raffo, & P. Muhlethaler, "Attacks Against OLSR: Distributed Key Management for Security," (2005*) 2nd OLSR Interop/ Workshop, Palaiseau, France*, July 28-29.
[23] Peter Glaus, "Locating a Black Hole without the Knowledge of Incoming Link", (2009*) Algorithmic Aspects of Wireless Sensor Networks, Lecture Notes in Computer Science*, vol.. 5304. Springer-Verlag Berlin Heidelberg, p. 128,
[24] D. B. Johnson, D. A. Maltz, and J. Broch. DSR: the dynamic sourcerouting protocol for multi-hop wireless ad hoc networks. Chapter 5, *AdHoc Networking, Addison-Wesley*, pages 139–172, 2001