Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.1167 – 1173

RESEARCH ARTICLE

Secure Platform for Wireless Sensor Network

Mohamed Otmani[1], Abdellah Ezzati[2]

[1]Faculty of Science and Technology Settat, Morocco
[2]Faculty of Science and Technology Settat, Morocco
[1] simo.otmani@gmail.com; [2] abdezzati@gmail.com

Abstract— ***A mesh, ADHOC and MANET networks can be used in several cases. In this paper we try to focus on two routing protocols in ADHOC in order to use one in real cases and without too much difficulty in implementation and securing. In this order we start by introducing the two routing protocols, then we create a mesh network using one of them as routing protocol with laptops, android, ARM based computer and smart phones as end-devices, then we implement a passive and active attack in order to collect data exchanged between nodes then we secure the communications with virtual private network tunneling and connect the end devices to the cloud.***

Keywords— AODV; OLSR; ADHOC

I. INTRODUCTION

Wireless sensor network can introduce a new life style to the world by using it in order to create smart cities, monitor and detect natural disaster or in battlefield surveillance where there is no centralized infrastructure and all nodes are capable of movement and must be connected to each other dynamically and arbitrary. However this concept is rarely used due to security problems, routing technology, energy and open platform for the test. In this study we will create a secure WSN test platform with OLSR.

II. OVERVIEW OF OLSR PROTOCOL

The basic principal of link-state routing is the complete knowledge of the network topology; each node performs a discovery of its neighbors and informs the others. To do that several messages are exchanged and different types of link are established.

A. Messages

- ✓ HELLO. Allows the discovering of the network and sends the information about the state and the type of link between the sender and each neighboring node.
- ✓ Topology Control .Allows determining the routing table by forwarding the list of the neighbors who has been selected as MPR by another MPR.
- ✓ Multiple Interface Declaration .Declare the presence of more than one interface in the node.
- ✓ Host and Network Association. To announce the gateway to a specific network like an Ethernet network.

B. Links

- ✓ UNSPEC link. A link with no specific information about his current state.

- ✓ Asymmetrical link. We say that a link is asymmetric if a node receives a message from another but there is no confirmation that the first one has been heard. It can be called unidirectional link.
- ✓ Symmetrical link. A link is called Symmetric if the two nodes hear each other.
- ✓ Lost link. When a link has been reported as symmetrical or asymmetrical, but there is no message received for the moment from the node; we say is a lost link or a dead link.

C. Neighbors

In order to discover the neighbors, each node periodically sends in the HELLO messages information about neighboring, the nodes that are selected as MPR and the list nodes that are declared by that node as asymmetric. We can say that there are three types of neighbors, and two different sets.

a) Types of neighbors.

- ✓ Not Neighbor : the node has no Symmetrical link.
- ✓ Symmetrical Neighbor : The node has at least one Symmetrical link.
- ✓ MPR Neighbor : the node has been selected as an MPR by the sender neighbor.

b) Sets.

The first set contains the one-hop neighbors of a node S, which having a symmetrical link with S denoted N1(s). The two-hop neighbors of a node S are defined as the following set: $N2(s) = \{y | y \neq s \wedge y \notin N1(s) \wedge (\exists x \in N1(s)) [y \in N1(x)]\}$.These two sets N1(s) and N2(s) of each node S are built by the trading of HELLO messages. This allows all nodes to have a vision for 1-hop and 2-hop topology of the network and have all the information needed to build paths between a source and a destination.

D. Multipoint relays (MPR)

Even that all neighbors can read the packet already sent by a node; however in order to minimize retransmissions of packets, OLSR introduces the principle of MPR. Every node can choose from its neighbors a set of MPR, these MPR are the only ones can retransmit the broadcast packets. Each node S selects a subset of MPR from N1(s) that allows it to be joined by all nodes in N2(s).

E. SECURITY ISSUES

In OLSR the nodes are trusted to generate and forward the routing information, if a node betrays that trust by doing some routing misbehaviors the whole network can be paralyzed.

In this section we will specify the different attacks on OLSR. Those attacks can be differentiated by the nature of their handling the network, either by generation or by relaying.

a) Incorrect traffic generation.

In this section we describe one of the most used attacks on OLSR which generating wrong control traffic, an intruder can generate what does appear a correct traffic but in fact it's misleading.

- HELLO.

As we know the HELLO messages are generated periodically by a node to send information about the state of the node, and to discover the neighborhood. However an outsider node can generate the same messages.

- ✓ Identity spoofing: an intruder node can generate HELLO messages with Originator Address of another node, which cause several perturbations in the network. First of all the neighbors of the intruder may announce a link state to the node with Originator Address in their HELLO and TC messages. Secondly the intruder choose from its neighbors a set of MPRs, those MPRs announce that they are at one-hop distance from the Originator Address. In HELLO messages there is an field called Willingness where OLSR specify the desire of a node to carry, forward the traffic and being chosen as MPR, an intruder can put in this field the value of "WILL_NEVER" with Originator Address of another node, this last one will be never chosen as MPR by its neighbors which may cause a loss of connectivity.
- ✓ Link spoofing : In HELLO messages a node advertises the neighbors that it have and the type of link. A hostile node can signalize a wrong or incomplete set of neighbors in the HELLO messages with wrong link code value, which cause wrong selection of MPRs and determination of the shortest path.

- Topology control (TC).

In OLSR specifications only the MPRs are allowed to generate and manage the TC messages, but an intruder node can do the same thing because there is no mechanism to control this specification.

- ✓ Identity spoofing : The fact that a node can steal the identity of another and use it to send TC messages advertising a wrong Neighbor Main Address can lead to lost of the connectivity, wrong calculation of the paths and loss of messages. In order to know the most recent message from the oldest OLSR uses the sequence number ANSN, an intruder node can use this specification to send TC messages with higher ANSN then the original node which mean that all TC messages coming from it will be ignored by the receivers.
- ✓ Link spoofing : in the case where a malicious node is selected as an MPR from the other nodes, it can choose to generate TC messages with incomplete routing information which may cause lost of connectivity or wrong choice of the shortest path.
- ✓ Multiple Interface Declaration / Host and Network Association . The generation of MID and HNA by a node declaring the presence of interfaces, either by pretending being another node or just by link spoofing, can cause wrong route calculation, lost of connectivity and lost of messages.

b) Incorrect traffic relaying.

- *MPR attack*.

In the default forwarding algorithm of OLSR the fourth step involves that if the final sender is not a MPR selector the message will not be retransmitted. In the MPR attack an intruder can receive a message and retransmit it even that it's not been selected as MPR, which cause that the real MPRs will not do their work because it considered done.

- *Wormhole attack.*

The object of this attack is the redirection of packets between two areas. Suppose a set of nodes denoted N building an Ad-Hoc network. N1 and N2 are two nodes belonging to N,N1 and N2 are geographically separated, now if we add another node N3, which in the field of communication of N1 and N2, it takes control over all traffic between N1 and N2 by creating a virtual link between these two. This type of attack can be performed by several malicious nodes, exchanging control messages between them and the targets in purpose of creating the virtual link.

- *Blackhole attack.*

A malicious node that was selected by its neighbors as MPR may reject all received packets from its neighbors. This type of attack causes a loss of connectivity and degradation of the communication.

- *Replay attack.*

This type of attack involves snorting on the network and save the control messages and retransmitted later with a higher sequence numbers. This attack causes a false determination of the existing topology, as a result a large routing problem.

III. OVERVIEW OF AODV ROUTING PROTOCOL

AODV (Ad hoc On-Demand Distance Vector) is a reactive routing protocol used to find a route between a source and a destination, and allows mobile nodes to obtain new routes for new destinations in order to establish an ad hoc network. In this order several messages are exchanged, different types of link are established, and many information can be shared between the participants' nodes. In AODV protocol we find hello message and three others significant type of messages, route request RREQ, route reply RREP and route error RERR. The Hello messages are used to monitor and detect links to neighbors, every node send periodically a broadcast to neighbors advertising it existent ,if a node fails to receive an hello message from neighbor a link down is declared. In order to communicate every node must create routes to the destinations, to achieve that the source node send a request message RREQ to collect information about the route state; if the source receives the RREP message the route up is declared and data can be sent and if many RREP are received by the source the shortest route will be chosen. Any nodes have a routing table so if a route is not used for some period of time the node drop the route from its routing table and if data is sent and a the route down is detected another message (Route Error RERR) will be sent to the source to inform that data not received.

A. MESSAGES

- ✓ Route Request (RREQ) Message. This type of message is used by AODV at first in order to locate a destination; this message contains identification of request, sequence number, destination address and also a count of hop started by zero.
- ✓ Route Reply (RREP) Message.This type of message contains the same fields like Route Request (RREQ) Message, and it sent in the same route of reception of RREQ message. When the source received this message it means that the destination is ready to accept information and the rout is working correctly.
- ✓ Route Error (RERR) Message. Sometimes a node detect a destination node that not exists in network, in this scenario another message (Route Error RERR) is sent to the source informing that the data is not received. RERR is like an alert message used to secure table of routing.

B. SECURITY ISSUES

AODV protocol is exposed to a variety of attacks, the impact of these attacks on AODV protocol are not the same. Some of these attacks can cause a breakdown of the network connectivity, increasing the end-to-end delay, increasing the number of the loss packets, or shutting down some nodes by consuming all the energy left in there batteries.

- *Black hole attack.*

In black hole attack a malicious node must be placed between two or more nodes and begin dropping all the traffic. This attack exploits the vulnerability of the route discovery packets of the routing protocol by modifying this last one in order to control all traffic that circulates between nodes. Wormhole attack.

- *Wormhole attack*

In this type of attack, an attacker saves the packets generated in one location of the network and redirects it to another and replays it. This type of attack can be performed by several malicious nodes in same time.

- *Byzantine attack*

In this type of attack, individually or cooperatively a malicious nodes carry out attacks such as creating routing loops and forwarding packets through non-optimal paths.

- *Rushing attack*

Rushing attacker forwards data and messages very quickly by skipping some of the routing processes. So, in on-demand routing protocol such as AODV, the route between source and destination include rushing nodes.

- *Resource consumption attack*

In this type of attack, an attacker attempts to consume battery life of other nodes to take it down.

- *Location disclosure attack.*

In this type of attack, the related information to the structure of network is revealed by attacker nodes.

IV. THE DAMAGE DUE TO TWO DIFFERENT TYPES OF ATTACKS

A. Passive attack

The nodes in mobile networks communicate by wireless with shared media (CSMA / CA) access, which allow to an attacker to capture and analyze all transmissions by setting its own communication interface in promiscuous mode. In this order and with all the analyzed transmissions the attacker will be able to perform stronger attacks.

To achieve the passive attack we need to send malicious Arp massages in order to interpose the attacker between the nodes and capture information, for that we will apply arpspofing attack using our backtrack system.

we did test the ARPSPOFING attack on an mesh network that use olsr as routing protocol, and we did collect the information calculated by the sensors.

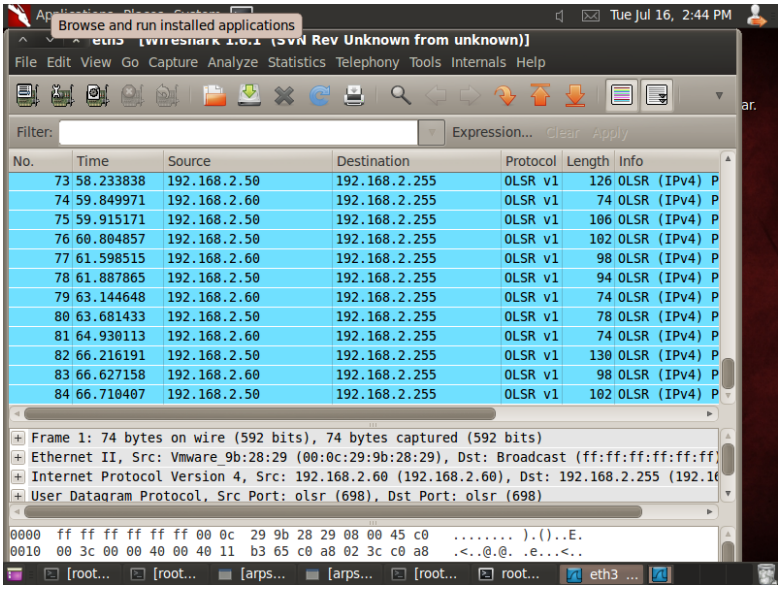


Fig. 1 Passive attack

B. Active attack

Active attacks can be performed on different Layer of the OSI model (mac layer, network, transport, application) the difference between active and passive attack is that in an passive attack the attacker can only retrieve information (login, password ...) unlike in the active attack the attacker can even add modify delete information in the packets.

- *Example of active attack.*

The main objective of black hole attack is to drape packets and break communications between nodes, all the network's traffic is redirected to a specific node which does not exist at all. Black hole node work with two scenarios, in the first one the node exploits all the vulnerability that exists in an ad hoc network such as announcing itself having a valid route to a destination node; the Second one, the node drupes and controls all the intercepted packets. The Black hole attack in AODV protocol can be classified into two categories: black hole attack caused by RREP and black hole attack caused by RREQ.

In our simulation of the Black hole attack, we did use Ns2 as a simulator and we fixed some cases where we will study the impact of the attack on AODV protocol.

In order to simulate a Black hole behavior we did integrate a new protocol in NS2 using the source code of AODV protocol and adding the black hole algorithm in it by modifying the AODV functions.

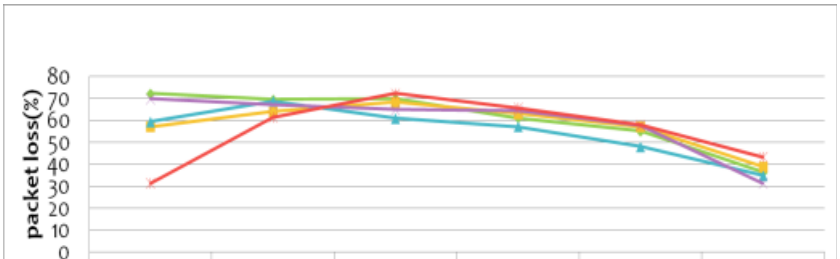
TABLE I

SIMULATION PARAMETERS

Simulator	Ns2.34
Time	500s
Pause Time	1.0
Max speed	20 m/s
Number of nodes	5 , 10 , 15 , 20 , 25 , 30
Flat space	750 * 750 m

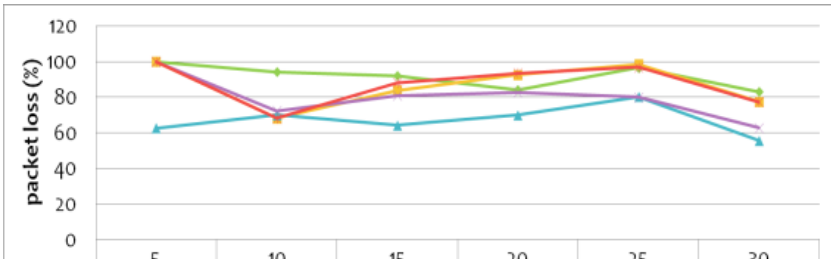
- Scenario 1: we simulate with mobile nodes that use AODV as routing protocol and one non-mobile node with the behavior of a black hole attacker.
- Scenario 2: we simulate with mobile nodes that use AODV as routing protocol and one non-mobile node and another mobile node with the behavior of black hole attackers.
- Scenario 3: we simulate with mobile nodes that use AODV as routing protocol and one mobile node with the behavior of a black hole attacker.

- Scenario 4: we simulate with mobile nodes that use AODV as routing protocol and two mobile nodes with the behavior of black hole attackers.
- Scenario 5: we simulate with mobile nodes that use AODV as routing protocol and two non-mobile nodes with the behavior of black hole attackers.
- Scenario 6: we simulate with non-mobile nodes that use AODV as routing protocol and one non-mobile node with the behavior of a black hole attacker.
- Scenario 7: we simulate with non-mobile nodes that use AODV as routing protocol and two non-mobile nodes with the behavior of black hole attackers.
- Scenario 8: we simulate with non-mobile nodes that use AODV as routing protocol and one mobile node with the behavior of a black hole attacker.
- Scenario 9: we simulate with non-mobile nodes that use AODV as routing protocol and two mobile nodes with the behavior of black hole attackers.
- Scenario 10: we simulate with non-mobile nodes that use AODV as routing protocol, one non-mobile node and another mobile node with the behavior of black hole attackers.



	5	10	15	20	25	30
S1	72,36	69,6	70,08	61,2	55,3	36,57
S2	57,25	64,15	68,4	63,2	57,26	39
S3	59,57	68,81	61,03	57,19	48,13	35,06
S4	69,95	67,21	65,02	64,55	57,9	31,4
S5	31,49	61,52	72,35	65,81	58,05	43,41

Fig. 2. Simulation results for the first five scenarios where the AODV nodes are mobile. X number of nodes, Y % of packet loss.



	5	10	15	20	25	30
S6	99,88	94,13	92,12	84,1	96,6	83,15
S7	99,88	68,2	83,84	92,6	98,57	77,45
S8	62,69	69,9	64,3	69,95	80,28	55,6
S9	99,94	72,24	80,97	82,7	80,1	62,89
S10	99,86	68,14	88,1	93,42	96,93	77,28

Fig. 3. Simulation results for the last five scenarios where the AODV nodes are non-mobile. X number of nodes, Y % of packet loss.

The Black hole is one of the most powerful attacks on an Ad hoc network, it can cause a complete failure of the network by dropping all the traffic specially when the nodes are non-mobile. And with passive attack we can see all the traffic and get critical information.

V. BUILDING WIRELESS SENSOR NETWORK WITH OLSR AND RASPBERRY

In this study we did use three sets of tools:

- raspberry-PI-B, sagem usb wireless and huawei 3g usb modem. Linux Raspbian wheezy as an operating system with OLSRD, Openvpn, Iptables and different types of sensors.
- Laptops with Windows or linux as operating systems
- Samsung Galaxy android phones.

A. Raspberry-PI-B

Raspberry-PI-B is a one single-board-computer with an ARM processor, 512 MB a Memory (SDRAM), one Ethernet port and two USB ports; powered with 5v via Micro-usb port with Power ratings 700 mA (3.5 W in normal case).

B. OLSRD

Olsr daemon is an implementation of olsr protocol that support windows OS, LINUX OS, BSD OS, MAC OSX and ANDROID. OLSRD implements also an optional link quality extension plus the normal multipoint relaying for optimized message flooding in OLSR standardization, with very little CPU time thus saving battery power.

C. Implementation

After doing the basic configuration of wireless 2.4 connection, 3g dongle for internet connection and send sms notifications, olsrd and open vpn server on raspberry , we did implement iptables as fire wall with forwarding options; and finally create and configure 30 clients.

D. E-lab

After creating mesh/MANET network with olsr and sensors we did create an open e-lab with tightvnc, no vnc for desktop on browser and ssh; witch permeate to student the full access to the platform and doing there tests on olsr for routing and sensors. WE need to introduce in the future a centralized authentication and reservation platform for the students outside the faculty.

VI. CONCLUSION

The mean objective of this study is to create a secure wireless sensor network platform for education propose with open source software and available hardware. We did see also how an attacker can damage the full network or use it for his own interest in order to collect information and that the radical solution for the most popular attacks is VPN tunneling but it reduce the bandwidth capacity and increase the consummation of energy which we will try to monitor it in the future and introducing from 3W to 40W solar panel for independent raspberry.

REFERENCES

[1] H. Deng, W. Li, and D. P. Agrawal, “Routing security in ad hoc networks,” IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.

[2] C T. Clausen, P. Jacquet, “RFC3626: Optimized Link State Routing Protocol (OLSR)”, Experimental, http://www.ietf.org/rfc/rfc3626.txt

[3] Y. A. Huang and W. Lee, “Attack analysis and detection for ad hoc routing protocols,” in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID’04), pp. 125-145, French

[4] Charles E. Perkins and Elizabeth M. Royer, “Ad-hoc On-Demand Distance Vector Routing ,” 2nd IEEE workshop on mobile computing systems and applications, New Orleans, Louisiana, USAp. 90-100, Feb. 1999

[5] Seung Yi and Prasad Naldurg, “Security-aware ad hoc routing for wireless networks ,” 2nd ACM international symposium on Mobile ad hoc networking & computing, MobiHoc'01, 2001,p. 299 - 302

[6] Charles Perkins and Elizabeth Royer, “ Ad hoc On-Demand Distance Vector (AODV) Routing ,” RFC 3561, 2003, p. 1-37

