ISSN (e): 2250 – 3005 || Vol, 04 || Issue, 4 || April – 2014 ||
International Journal of Computational Engineering Research (IJCER)

Performance Evaluation of Energy Consumption of Ad hoc Routing Protocols

Mohamed Otmani[1], Abdellah Ezzati [2]
[1] PhD student, Faculty of Science and Technology Settat, Morocco
[2] Asst. Professors, Faculty of Science and Technology Settat, Morocco

Abstract:
In wired networks there are different physical devices routing the traffic centrally, by consequence we can create paths in the network by using multiple management rules, but in Ad-Hoc network nodes must do this work in an autonomous way. For that there are three types of routing protocol proactive, reactive and hybrid. The first one continuously calculates the possible paths to be available at the time of transmission. The second one create the roads only when are needed. And the last one is a combination between the two methods. In this study we will focus on three routing protocols AODV, OLSR and ZRP; and compare their performance in terms of Routing Power, Throughput, Energy Consumed in Transmit mode, Energy Consumed in Receive Mode, End-to-End Delay..

Keywords: *AODV; OLSR; ZRP; ADHOC*

I. INTRODUCTION

Mobile ad-hoc network (MANET) is the network of mobile nodes that requires no infrastructure or centralized management in order to communicate. This type of network allows to create and deploy a wide field of communication quickly, and that's what we need in several cases such as a natural disaster or 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, due to distributed nature of the wireless nodes and lack of energy resource this type of network must have specifics protocols.

In MANET network the nodes must the routing in an autonomous way, in this order there are three types of routing protocol proactive, reactive and hybrid. Every type of architecture or protocol has some advantages and disadvantages in this paper we will put this three types in test.

II. PROTOCOLS ANALYSED

The following protocols are considered for analysis:
• AODV
• OLSR
• ZRP

A. 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.

1) 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.

2) 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 Symetric 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 momment from the node; we say is a lost link or a dead link.

3) 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 Symetrical 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.

c) 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).

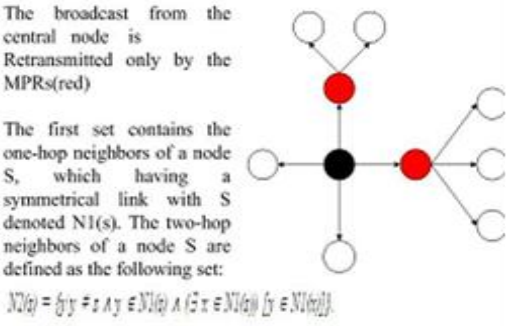

Figure 1. OLSR MPR

B. Overview of ZRP Protocol

The ZRP protocol [9] implements simultaneously, a proactive routing and reactive routing, in order to combine the advantages of both approaches. To do so, it passes through a cutting concept network into different zones, called "routing areas". A routing area for a node is defined by its "radius zone". This radius corresponds to the maximum number of hops that can exist between two nodes.

1) Architecture ZRP

An example of area is given in Fig. We note that for a radius of area equal to two, the routing area of the node S is constituted by all the nodes around the node S is a maximum of two hops between them. Are included in the routing area, all the neighbors of node S and all the neighbors of these neighbors.

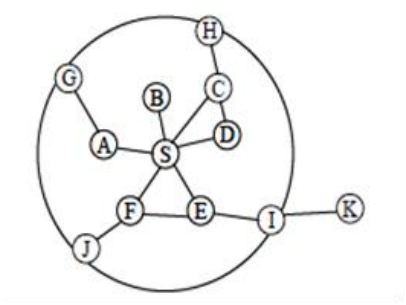

Figure 2. Example zones

2) Routing within ZRP

Routing within a zone is proactively via IARP protocol (intra-zone Routing Protocol) routing to external nodes of the zone is reactively through the IERP (Interzone Routing Protocol). In addition to these two protocols, ZRP uses the BRP (bordercast Routing Protocol). To build the list of devices nodes it is to an area and roads to reach them, using data provided by the topology IARP protocol. It is used to propagate search queries IERP roads in the network. Figure illustrates the necessary implementation of ZRP protocol network components.

A search path is as follows: we first checks if the destination node is in the area of the source node, in which case the path is already known. Otherwise, a request is initiated route RREQ to all peripheral nodes. These check if the destination exists in their areas. In the case of an affirmative answer, then the source will receive a RREP packet containing the path to the destination. Otherwise, the edge nodes broadcast the request to its own edge nodes which, in turn, perform the same processing.

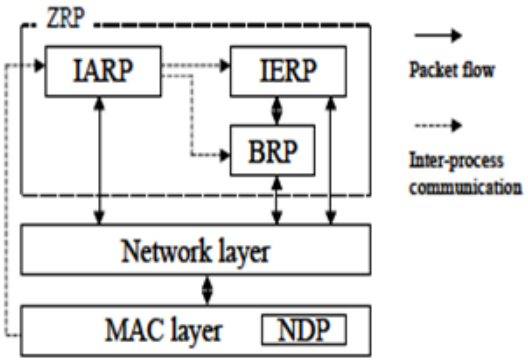

Figure 3. Components

- ✓ The routing protocol IERP: IERP is respondable management hosts that are present beyond the routing area. IERP collecting routing information reactively through bordercast queries that contain accumulations of routes from the source. When receives an IP data packet for an unknown destination (that is to say that it is not listed in the routing table in the interzone or intra-area routing table), is interrupted IERP. He responds by initiating a search for a solution ("route discovery") and bordercast a route request.

- ✓ The routing protocol IARP: IARP depends on the services of a separate protocol (referred to herein as the "Neighbor Discovery / Maintenance Protocol) to provide information about the neighbors of the host. At a minimum, this information contains the IP addresses of all neighbors. IARP can be configured to support additional information on neighbors, such as the cost of a link.

- ✓ The routing protocol BRP: The interface of the upper layer of BRP is implemented to be compatible with any IP-based application. However, we assume that the hierarchy of the routing area is visible only to entities ZRP protocol.

C. Overview Of AODV 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.

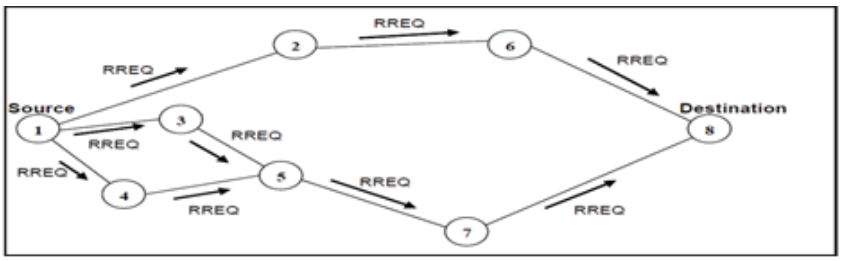

Figure 4. RREQ message

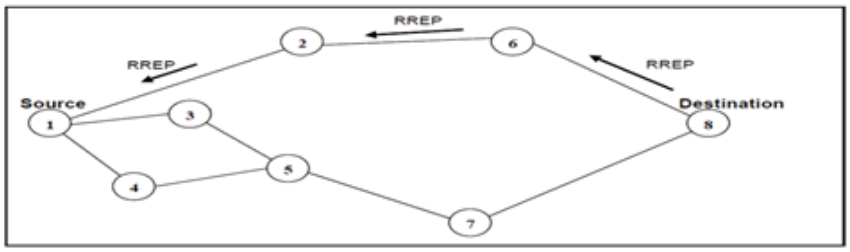

Figure 5. RREP message

1) Messages

a) 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.

b) 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 mean that the destination is ready to accept information and the rout is working correctly.

c) 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.

III. SIMULATION ENVIRONMENT

The simulation process of MANET is implemented using simulator Qualnet. QualNet is network simulation and modelling software that predicts performance of networks through simulation and emulation. QualNet run on a vast array of platforms, including Linux, Windows XP, and Mac operating systems, it can run both 32- and 64-bit computing environments.

Table 1.Simulation Parameters

Simulator Parameters	
Mac Type	IEEE 802.11
Protocols under studied	AODV,OLSR,ZRP
Node movement model	Random
Traffic type	CBR
Node Speed	10m/s
Scenario Parameters	
Topology area	1000x1000
Simulation time	30 Seconds
Packet Size	256 bytes
Generic energy model Parameters	
Energy Model	Generic
Energy Supply Voltage	6.5 Volt
Transmit Circuitry Power Consumption	100.0 mW
Receive Circuitry Power Consumption	130.0 mW
Idle Circuitry Power Consumption	120.0 mW
Sleep Circuitry Power Consumption	0.0 mW

A. Snapshot of Simulation

The simulations of energy model were performed using QualNet Simulator 5.0.1. The traffic sources are CBR. The source-destination pairs are multiplying randomly over the network. The mobility model uses random waypoint model in a rectangular filed of 1000m x 1000m and deploys 50 nodes. During the simulation, each node starts its journey from a source node to destination node. This process repeats throughout the simulation, causing continuous changes in the topology of the underlying network. Fig.6 Shows the running simulation of snapshot when we applying CBR (1- 40) nodes and AODV routing protocol.

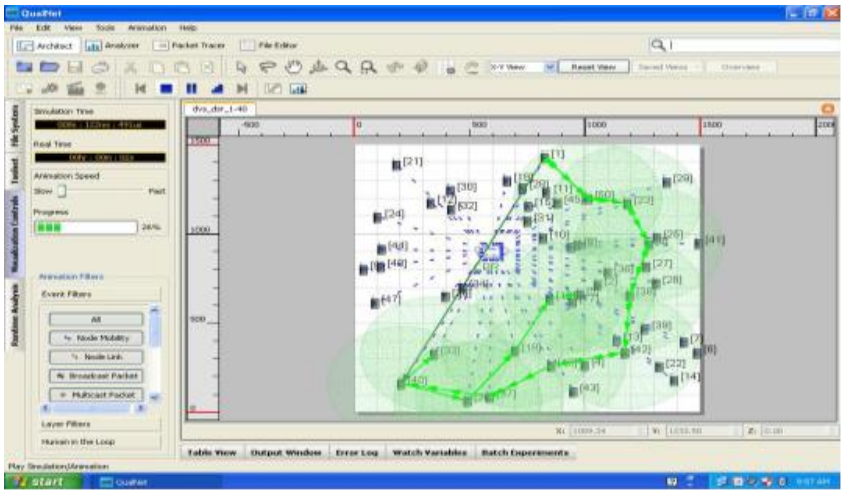

Figure 6.Snap shot of Qualnet Animator in Action

We obtained the number of scenarios in QualNet simulator with varying 10, 20, 30, 40 and 50 nodes selected randomly over a 1000X1000 topology area and taking different routing protocols which we are consider in our simulation. These protocols are AODV, OLSR and ZRP. The node speed is 10 m/sec and each simulation lasted 30 seconds simulation. We evaluate the performances metrics in Application and Physical layers of designed scenarios. The performance matrices are given below.

- Routing Power
- Throughput
- Energy Consumed in Transmit mode
- Energy Consumed in Receive Mode
- End-to-End Delay

IV. RESULT ANALYSIS

A. Throughput

The throughput of the protocols can be defined as percentage of the packets received by the destination among the packets sent by the source .The throughput is measured in bits per second (bit/s or bps).

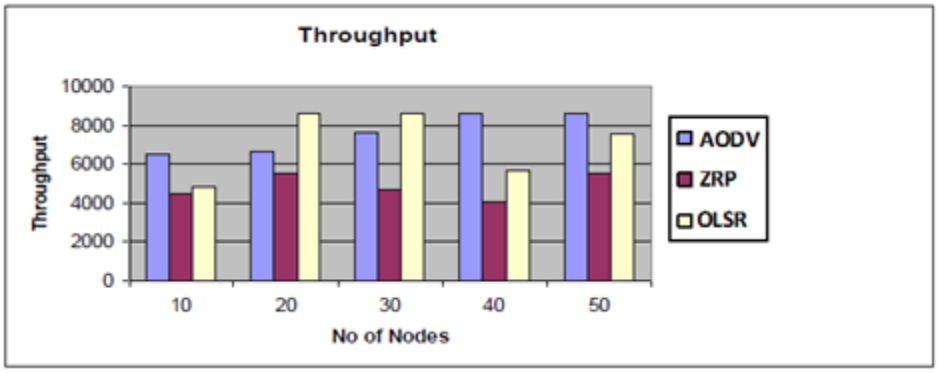

Figure 7.Throughput

Impact on Throughput: Throughput performance is high for AODV and OLSR. ZRP performance is very poor.

B. End-to-End delay

This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination.

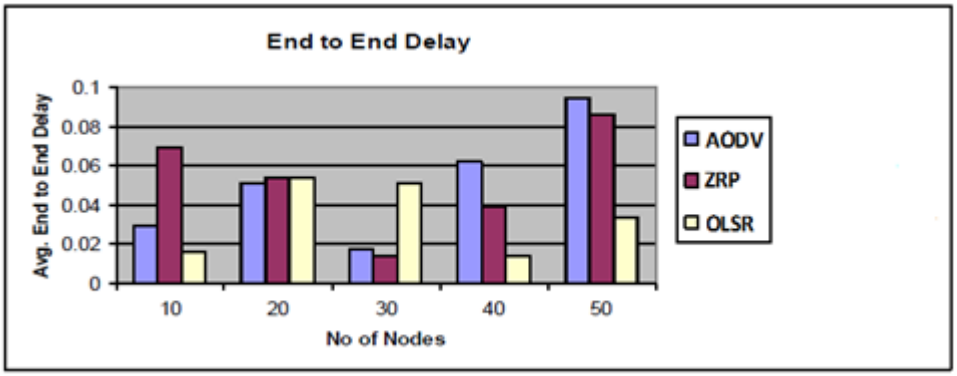

Figure 8. End-to-End delay

Impact on Average End to End delay: From the graph the average End to End delay is low for OLSR while using less nodes as well as more nodes. AODV has high.

C. Data packet delivery ratio

The data packet delivery ratio is the ratio of the number of packets generated at the source to the number of packets received by the destination.

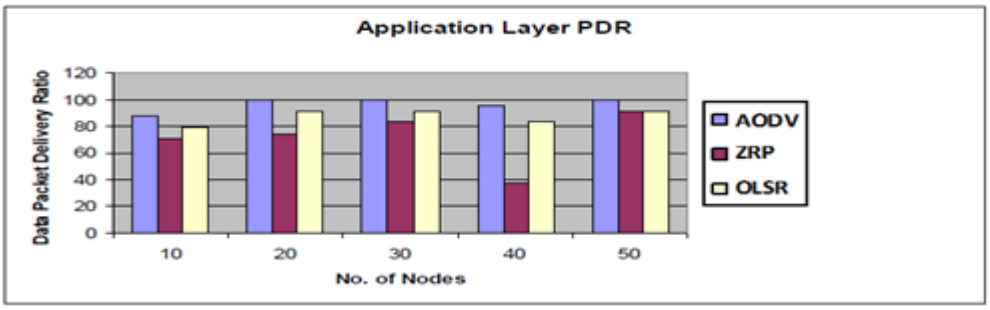

Figure 9. Data packet delivery ratio

Impact on Data packet delivery ratio: Data Packet Delivery Ratio is high for AODV when compared to ZRP and OLSR protocol. Which increases the life time of the entire network for AODV.

D. Energy consumed in transmit mode

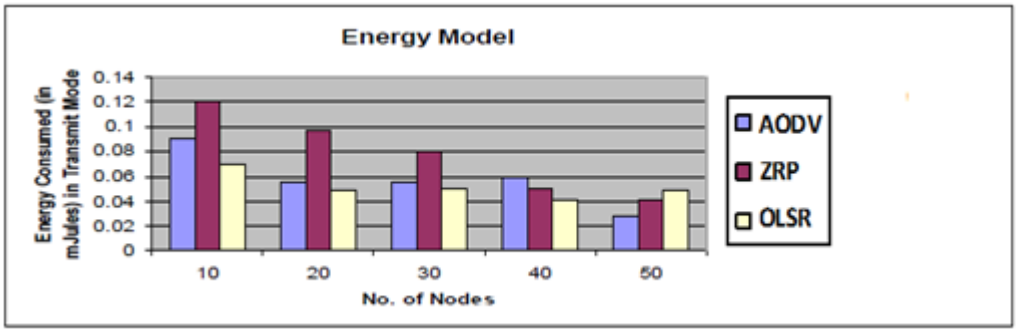

Figure 10. Energy Consumed in transmit mode

Impact on Energy consumed in transmit mode: Fig. 10 shows the total energy consumed in transmit mode is very low for OLSR protocol when compared to the other two.

E. Energy Consumed in Receive Mode

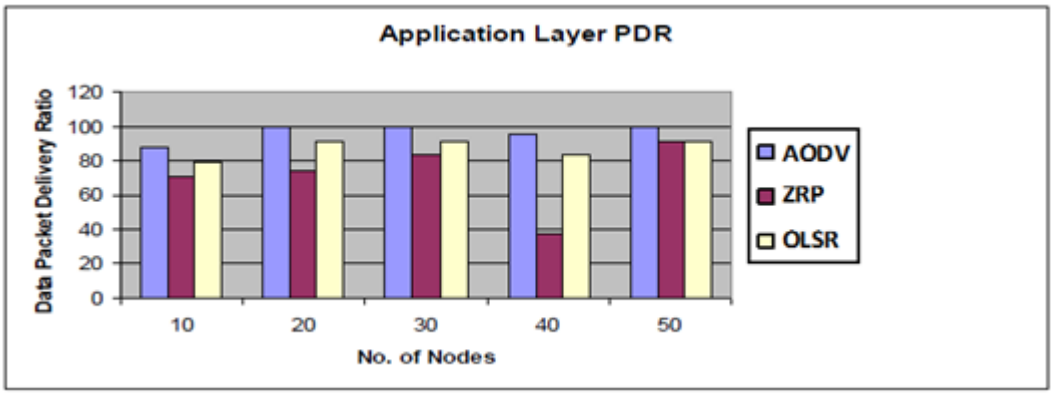

Figure 11. Energy Consumed in Receive Mode

Impact on Energy consumed in receive Mode: ZRP routing protocol consumes less power than other protocols in receive mode.

F. Routing Power

Routing Power = Throughput / Avg.End-to-End Delay

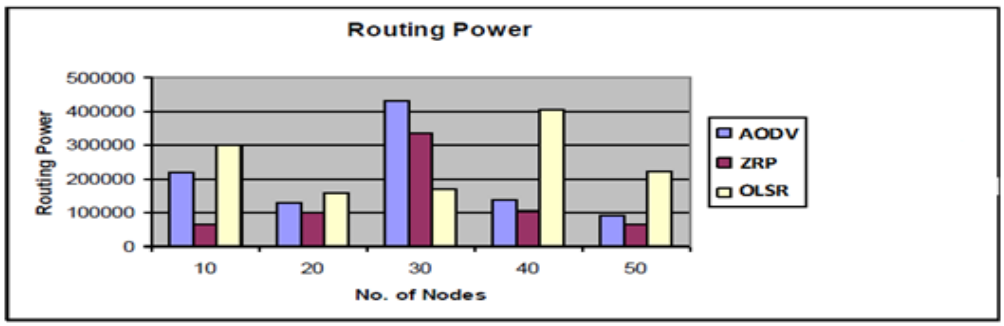

Figure 12. Energy Consumed in Receive Mode

Impact on Routing Power: The routing power effect on AODV routing protocols more as compare others, but as on average routing power of AODV protocol is reduced.

V. CONCLUSIONS

We observed that Energy saving is very important optimization objective in Manet, the energy consumed during communication is more prevailing than the energy consumed during processing because of Limited storage capacity, Communication ability, computing ability and the limited battery are main restrictions in sensor networks. By the observations we compare that the impact of energy constraints on a nodes in physical layer and application layer of the networks that AODV offers the best combination of energy consumption and throughput performance. AODV gives better throughput, packet delivery fraction, average jitter and delay performance compared to ZRP followed by OLSR. If we increased numbers of nodes also increase maximum energy consumption in OLSR followed by ZRP then AODV due to routing control packets in the network. Future work, we can reduce the waste energy consumption of the nodes by reducing the number of routing control packets and reducing the energy consumed by nodes in a large network to increase the life time of network.

REFERENCES

[1] C T. Clausen, P. Jacquet, "RFC3626: Optimized Link StateRouting Protocol (OLSR)", Experimental, http://www.ietf.org/rfc/rfc3626.txt

[2] Raffo, D., Adjih, C., Clausen, T., and Mühlethaler, P. An advanced signature system for OLSR. In Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04)

[3] Hu, Y.-C., Perrig, A., and Johnson, D. B. "Packet leashes : A defense against wormhole attacks in wireless networks" In Proceedings of INFOCOM, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies (April 2003).

[4] Wang, M., Lamont, L., Mason, P., and Gorlatova, M. "An effective intrusion detection approach for olsr manet protocol".

[5] T. Clausen, U.Herberg, "Security Issues in the Optimized Link State Routing Protocol Version 2 (OLSRv2)", International Journal of Network Security and its Applications, 2010.

[6] Céline Burgod, "Etude des vulnérabilités du protocole de routage OLSR" 2007.

[7] Djallel Eddine Boubiche, «Routing protocol for wireless sensor networks, "Memory Magister, University of l'Hadj Lakhdar, Batna, Algérie, 2008.

[8] Wendi Beth Heinzelman, «Application-Specific Protocol Architectures for Wireless Network », IEEE Transactions on Wireless Communications, Massachusetts Institute of Technology, June 2000.

[9] Z. J. Haas – « A new routing protocol for the reconfigurable wireless networks», dans Proc. 6th IEEE Int'l Conf. on Universal Personal Communications (ICUPC'97) (San Diego, CA, USA), vol. 2, 1997, p. 562–566.