The Impact of Black-Hole Attack on ZRP Protocol

CHAHIDI Badr
Mathematics and Computer Science Dept, LAVETE Laboratory Faculty of Sciences and Technical Settat, Morocco

EZZATI Abdellah
Mathematics and Computer Science Dept, LAVETE Laboratory Faculty of Sciences and Technical Settat, Morocco

***Abstract*—lack of infrastructure in ad hoc networks makes their deployment easier. Each node in an ad hoc network can route data using a routing protocol, which decreases the level of security. Ad hoc networks are exposed to several attacks such as the blackhole attack. In this article, a study has been made on the impact of the attack on the hybrid routing protocol ZRP (Zone Routing Protocol). In this attack a malicious node is placed between two or more nodes in order to drop data. The trick of the attack is simple, the malicious node declares to have the most reliable way to the destination so that the wife destination chooses this path.**

In this study, NS2 is used to assess the impact of the attack on ZRP. Two metrics measure, namely the packet delivered ratio and end to end delay.

Keywords—ZRP; Blackhole; security; Routing

I. INTRODUCTION

Wireless sensor networks are composed of a set of independent nodes capable of communicating with each other via radio waves. Communications can be direct or through other nodes called relay allowing others outside to communicate. Each node acts as a terminal and as a routing point so that each node can send packets or receive packets or re-route packets if they belong to another node.

Putting a number of radio range nodes causes the appearance of a rapidly deployed network and adapts to a number of situations where the infrastructure mode is too expensive, too long or sometimes impossible.

Ad hoc mode differs from the infrastructure mode where the nodes communicate via an access point, which can be connected to a fixed network. This type of network (Ad-hoc) which is characterized by a lack of infrastructure is used in various fields such as industrial fields for monitoring the pressure flow or others such as the military for surveillance of the battlefield or in the civil field during disasters by rescue services.

So we are dealing with ad hoc networks that use specific routing protocols where the big problem is security, because that they are designed to run in an environment of trust. Arguably the MANET is susceptible to attacks, whether active or passive.

To secure an ad hoc network, you must consider the following attributes: availability, confidentiality, integrity and authentication. Most of the research has been done with the aim of reducing energy consumption without taking into account different attacks such as the attack Black Hole.

In this section, the security requirements are presented as well as principles of routing, and the impact of the attack on the Black Hole ZRP protocol. The simulation is performed on NS-2 and the simulation results are analyzed on various parameters such as the rate of delivered packages and the time from start to finish.

In this article, a detailed explanation of the new routing protocol where it has implemented the attack black hole. The simulation was made under NS2, in the objective of studying the impact of the attack on the networks Manet. Metric two were measured to know the rate of lost packets and the end-to-end delay. As expected a decrease in performance was noted mainly in the case where the number of nodes sources is high.

Our paper is organized as follows: the second part describes the principle of routing in ad hoc networks. In the third part there is a classification of attacks. The fourth part gives more information on security in ad hoc networks and the implementation of the attack in the Protocol ZRP. The simulation of the attack and the discussion of the results are shown in Part 5. We conclude the section in Part 6.

II. ROUTING IN AD HOC NETWORKS

The routing protocols in different categories, and this according to the itinerary discovery method, according to the information exchange method or how the nodes share the job of routing them.

A. Routing classification

Given their specific characteristics (absence of fixed infrastructure, limited source of energy and ability to calculate non-secure communication links), ad hoc networks CANNOT use the WIRED NETWORK ROUTING PROTOCOL. New protocols were born with the aim to meet their needs.

These protocols can be divided into three categories according to the update method of the routing table. The first so-called proactive where each node maintains its updated routing table via a regular exchange with its neighbors. OLSR [1] (Optimized link state routing) is one of the most popular routing protocols for this category.

The second category is called REACTIVE; each node performs a demand routing. When a node wants to communicate with another, it sends the route request requests to all nodes, and expects the recipient's response, a response that contains the path to take. Among the reactive protocols it there's the AODV (Ad-hoc On-demand Distance Vector).

The last category includes the proactive and reactive, it is called Hybrid. Each node wants to send data verified the

presence of the destination within the zone using the reagent. Out of the proactive area is used to derive the road. ZRP [3] is a hybrid routing protocols known for this category.

Each category has different strengths and weak. The proactive routing consumption of bandwidth due to the regular exchange of packets for the regular updating of the routing table. As against the problem of reactive protocols is latency, due to the discovery route to each request.

B. Routing Data

To understand the attacks in Ad hoc networks can be said that each node wants to send a message checks for the destination in its routing table. If it does not exist, it starts the route discovery process is broadcast on the network a route request message type. When an intermediate node receives this packet, and it is not also the recipient and the destination is not present on the table it in turn generates a road type of packet request containing its identifier.

In the event that the route to the destination is present in the routing table, a route reply message type is returned to the source indicating the way. Figure 1 shows the route discovery process.

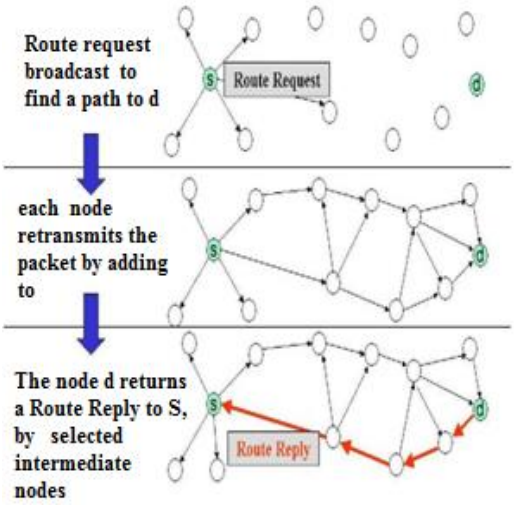

Fig. 1. route discovery process

When receiving the request reply packet from the source node, an update is made to its routing table to find out list of intermediate nodes to the destination and the associated cost. The cost is to choose between two routes to the same destination.

C. ZRP

The Zone Routing Protocol or ZRP [3], combines the advantages of both proactive and reactive approaches in a hybrid plan, taking advantage of proactive discovery in the local vicinity of a node, and using a reagent protocol for communication between the zones.

ZRP is proposed with the aim of reducing checks messages for proactive protocols and latency for reactive protocols. It is suitable for networks with a wide range and diverse patterns of mobility. For each node a routing area is defined separately. In the routing area, routes are available immediately, but outside the zone ZRP uses the route discovery process.

ZRP in each routing area comprises nodes that are a distance of max n jumps of reference node. There are two types of nodes for a routing area in ZRP [10]:

- Peripheral nodes
- Interior nodes

The nodes whose distance from a central node is less than the radius of an area are internal nodes while the node in the distance is exactly equal to the radius ρ are peripheral nodes. In Fig. 2, peripheral nodes E, F, G, K, M and Interior nodes B, C, D, H, I, J. The node is outside the node routing area A.

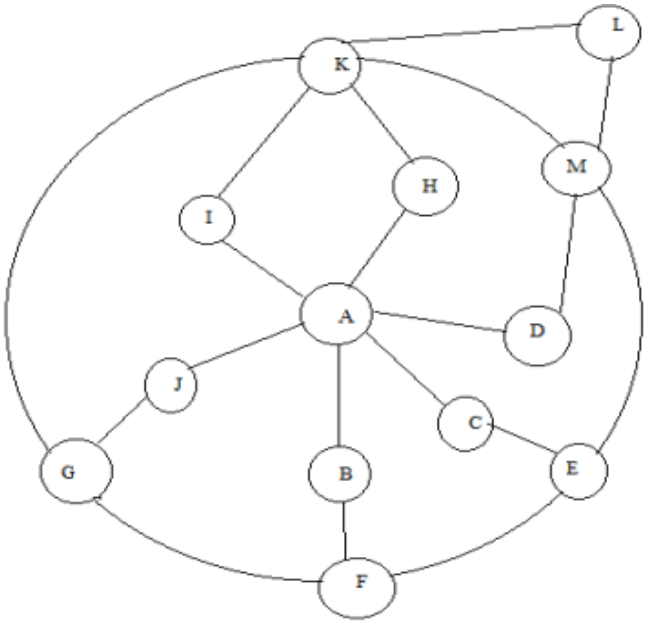

Fig. 2. Node Routing Area A with a radius = 2 jump

The source node sends a route request to the device nodes of its zone.la Route request contains the source address, destination address and a unique sequence number. Each device node checks if the destination is in its local area. If the destination is not a member of this local area, the boundary node adds its own address to the route request packet and sends it to its own device nodes.

If the destination is a member of the local area, it sends a response on the reverse path to the source. The source node uses the path recorded in the response packet to send data packets to the destination.

By adjusting the node transmission power, the number of nodes in a routing area can be controlled. Lowering the power reduces the number of nodes whose direct reach and vice versa. [10] ZRP uses both proactive and reactive routing strategies. In a routing area, the proactive strategy is used, while the reagent is used between the zones. ZRP refers to intra-zone Proactive Routing Protocol in local routing (IARP). The reactive routing is called inter-zoneRouting Protocol [12]. Its architecture is shown in Fig 3. IARP maintains nodes routing information existing in the node a routing area. The

discovery and maintenance of road is offered by IERP. If the topology of the local area is known, IERP can be used to reduce traffic.

Instead of broadcasting a package, ZRP uses the concept of broadcasting. [10] The broadcasting service is provided by the broadcasting Resolution Protocol (BRP).

BRP [11] uses an extended routing map provided by IARP, to build broadcast trees through which request packets are directed.

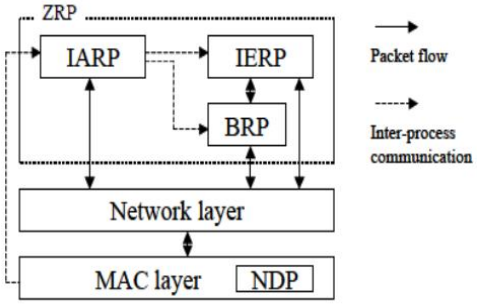

Fig. 3. Architecture ZRP [11]

III. Classification of Attacks

Before Routing protocols are exposed to various attacks that impact that this differs. Some attacks can cause the shutdown of a node by consuming their energies. Other attacks lead to a connectivity outage which influence on the packet rate issued and the time from start to finish.

Attacks in Ad hoc networks can be classified according to several criteria, such as the intelligence of the attack, its objective, the location of the attacker node, the impact of the attack on the network, etc...

- Impact of the attack: an attack can have a passive impact is to say that there's a network traffic analysis, surveillance of communications without modification of data or network operation and also without no injection of information in the network, all this in order to use this information in other attacks, such as the collection of passwords. It can be inferred that the main objective of such an attack is to know and understand how the nodes communicate with each other, and how they come together in the network. This attack is known as the "sniffing attack". [6] Another type of impact, called active, is a result of active attacks. This type of attack requires an injection of information in the network, or interacts with other nodes. Among active attacks include the attack "sleep deprivation" [7], which is to work the target in order to exhaust its battery.
- The objective of the attack: the target of the attack to a direct relationship with the type of striker. There are two types of attacker: the rational and the irrational. The first type of striker prepares his attack in order to take a direct or indirect benefit of the results of the attack. However, the objective of the second type of attack is to disrupt the proper functioning of the network. These attacks can be distinguished attack "jamming" [5]
- The intelligence of the attack: This type of attack is based on one or more layers of the OSI model. There are several types of attacks that are either of the attacks based on network layer attacks that exploit the failure of routing algorithms. The attack black hole (black Hole) is an attack that offers a shorter wrong path [8] it is based on the network layer.
- Location of the attack: the location of the attack is a very important parameter. An attack can be launched depending on the target location in the network. For example, a node that has a strategic location that provides network connectivity can be a target for an attacker seeking to isolate the network is to switch it off.

A. The BlackHole attack

An ad hoc network is susceptible to many security attacks. The blackhole is among the most known attacks. It is defined simple but effective, an attack that is based on the insertion of a malicious node having the capacity to take the identity of valid nodes on an ad hoc network since there is no physical barrier. This insertion leads to disturbances in the network and that due to the participation of all the nodes in the routing.

During this attack a malicious node exploits the vulnerability and claims to have the most reliable path to the destination. The source node takes one consideration that path is sending data to the malicious node which leads to loss of data. The main aim of such attack is to drape the packages, and to break the communication between nodes is diverting traffic to a non-existent node. . Fig 4 describes a blackhole type attack.

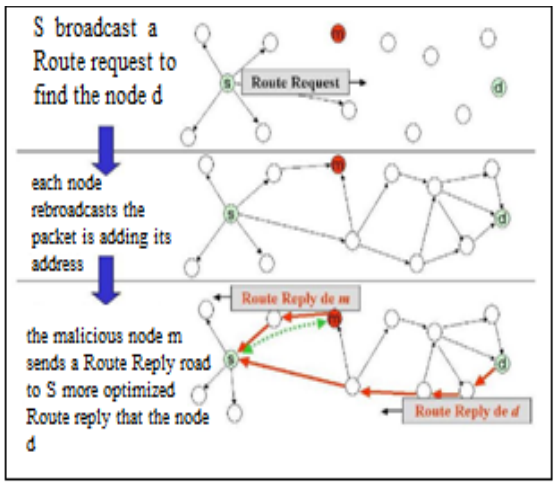

Fig. 4. Attack blackhole

When a source node wants to send data to a destination, it launches the route discovery mechanism is sending a RREQ message type. When receiving such a message by a malicious node, it responds immediately by sending a fake RREP post where he mentions he has the correct path to the destination requested with high sequence number. After receiving such a message by the source, it stops the process of discovery and ignores other RREP messages and begins sending packets to the malicious node. In turn it absorbs all the packets from

other nodes and thus the source node is attacked and its data are lost.

B. The Wormhole attack

This attack is based on two strikers who are interconnected via a link known as the tunnel. The first node in a striker this side of the network, receives packets from a legal node, the encapsulated then transmit using the tunnel to the second malicious node located in the other side of the network. The striker said node having the shortest route to the destination with the objective that it becomes the relay node. Fig 5 shows an example of a Wormhole attack [4], where two malicious nodes A and B that communicate through a tunnel which can be wired or wireless types. In this figure the nodes 3 and 7 respectively represent the source and destination. When the source wants to send given to the destination that is to say the node to node 3 and 7 in the absence of malicious nodes will be the path taken with a number 3-2-6-5-7 jump equal to 3.

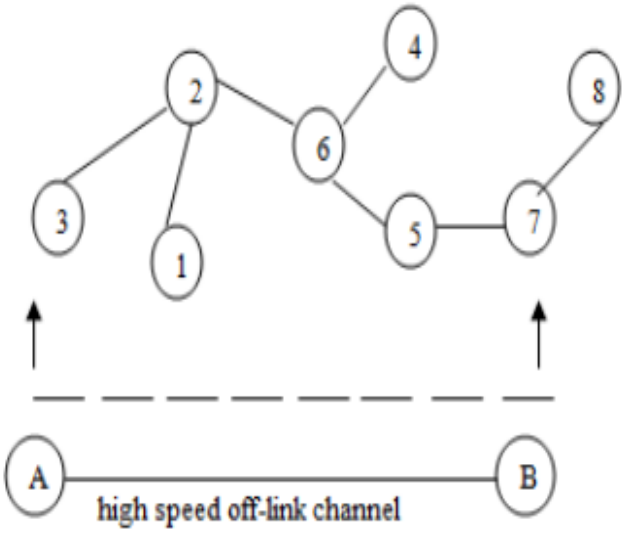

Fig. 5. Example Wormhole attack

In the case of presence of a Wormhole attack, the two nodes A and B will be activated where the transmissions take place between 3 and 7 via both malicious nodes A and B is using the Wormhole tunnel.

C. The attack RUSHING

In a type of attack Rushing [9] the malicious node responds as quickly as possible on RREQ type messages with the aim that the road through either retained him. If the proposed path is chosen, it will be to absorb all or part of the packets passing through it. Due to the high transmission speed, packets sent by the attacker will reach the destination first, pushing the source accepted her packages and throw the others. This way the attacker can easily access the communication between the transmitter and receiver.

D. Location disclosure

In the case of location disclosure attack, the malicious node role for collecting information on the location of the nodes, the set of paths and nodes involved and also other information useful on the network.

IV. Security in Ad Hoc Networks

The safety requirements for Ad hoc networks are almost identical for the wired or wireless networks with infrastructure. The security services are based on three concepts: authentication, confidentiality, data integrity and non-repudiation of users.

A. Authentication

The first concept is that authentication controls the identification of a node or entity in the network. Authentication ensures control of access to network resources. With the lack of authentication, malicious nodes can easily assume the identity of another with the aim to attack or take the privileges assigned to that node.

B. Confidentiality

Confidentiality ensures protection of information against threats that may lead to the disclosure of information. Confidentiality ensures private communication between nodes; is based on encryption. Encryption that can be applied to different levels of protocol layers. Encryption algorithms require encryption keys before sending it to the destination. However at the destination one must have the decryption key to decrypt the message.

C. Integrity

Integrity ensures protection against the traffic without prior authorization modification during transmission. Arguably, it is made to secure the system against threats that can cause change in the configuration of the system or data. This concept can be applied in a indirect way with protocols that confidentiality or authentication.

D. Nonrepudiation

Non-repudiation is made to ensure the identity of the sender and receiver. The non-repudiation of the issuer proves that the data was sent, and the non-repudiation of the receiver verifies and confirms receipt. This concept is reached on using the technology of the digital certificate.

V. Simulation of Blackhole Attack on ZRP

A. Simulation environment

In this part a study has been made on the impact of blackhole attack on the ZRP hybrid routing protocol, the NS 2.33are chose for simulation. The attacker is known in advance and simulation parameters are shown in Table 1.

Two performances are evaluated in order to infer the influence of the attack on the ZRP protocol namely the packet rate issued and the time from start to finish.

The mobility scenario is one generated using the random way point method, a method that generates a scenario in a random manner ie speed and nail mobility.

To implement the attack on NS 2 changes are made at the source code of the ZRP protocol in order to generate the new clone ZRP Protocol integrating the attack. This new protocol will be used by the attacker node while other nodes use the standard protocol ZRP.

TABLE I. SIMULATION PARAMETER

Parameter	Value
Nbr. Sources node	5, 20, 30
mobility	Absent
routing protocol	ZRP
Simulation time	200s
Packet size	512
Traffic	CBR
Network size	1000 X 1000
Total of node	50

B. Scenarios Simulations

To assess the impact of the attack on the black hole routing protocol ZRP different scenarios have been proposed:

- 1st scenario: In this first scenario simulation, all nodes using ZRP as the communication protocol are fixed, including the attacker node.
- 2nd scenario: In the second scenario, the fixed mobility is kept for all nodes; and increasing the number of node addressing two.
- 3rd scenario: In this third scenario simulation all nodes using the ZRP routing protocol for communication are mobile except attacking node.
- 4th scenario: The simulation in the fourth and final scenario simulation is the same as the third, it is made with mobile nodes except instead of an attacker node using two nodes.

This after a discussion of the results obtained in the simulation of the attack on the black hole ZRP protocol, checking the two parameters ie the rate of packets delivered and the time from start to finish. The results are as graphs and four scenarios are used to test the performance.

1) packet rate issued

The results obtained from the simulation of the attack black hole on hybrid routing protocol ZRP we see the influence of the attack.

Fig 6 illustrates the variation of the lost packet rate based on the number of source nodes, and also in different scenarios. Based on the results we see that the attack Black Hole has an impact on the ZRP protocol considered especially in cases where the number of source nodes is high. Also the rate of delivered packets decreases from the fixed case we note that in the case of mobility, which is logical as mobility increases the rate of lost packets according to the results previously obtained.

The reduction of packages delivered in the mobile case rate is not 100% on the attack, but also the mobility that has a significant impact on this metric.

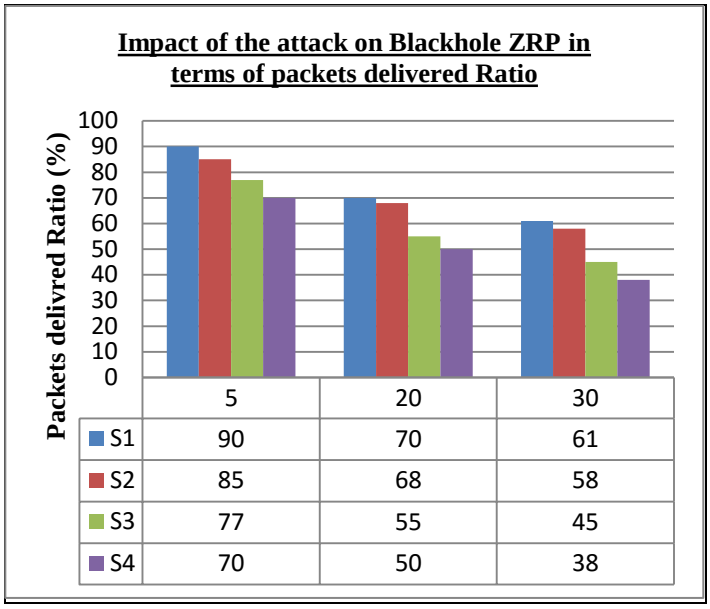

Fig. 6. Variation packets delivered ratio

2) End to End delay

Fig 7 shows the time from start to finish in different scenarios depending knew many nodes sources. From the results obtained it can be inferred that the attack has an effect on this metric especially in the case where the number of source nodes is as high in the presence of mobility.

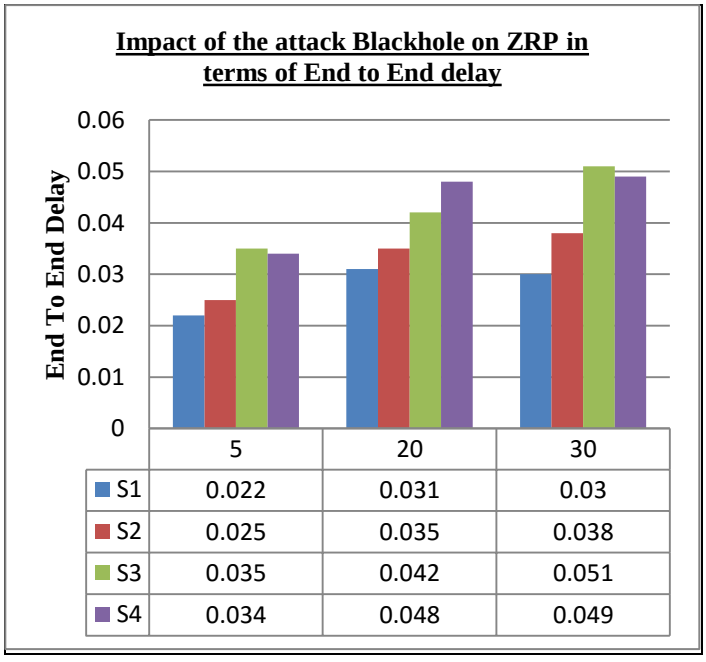

Fig. 7. Variation End to End Delay

VI. CONCLUSION

Ad-hoc networks are characterized by the absence of infrastructure, also by devices with limited capabilities in terms of calculated and energy. The lack of infrastructure is considered a strong point for this type of facility since the implementation network in an environment with minimal cost.

Each node in its network can simultaneously be a capture unit as a routing device, all this makes them vulnerable to a Manet set of security attacks; attacks that can be active or passive and influence on the confidentiality, integrity and availability of data.

These attacks found the attack Black Hole (Black Hole); a powerful attack that influence on Ad hoc networks. This attack can cause a complete network failure is absorbing the traffic as it can isolate part.

In this study we investigated the impact of the attack black hole on hybrid ZRP protocol, for we have created a clone of the protocol where we implemented the attack, the new protocol will be called by the attacker in order drape traffic.

According to the results we see that the attack has an impact on the protocol is in the fixed or mobile network case. As the rate of packets delivered decreases with increasing the number of source nodes; one can also deduce that the high number of packets lost in the case of mobility is not at 100% of the attack but also because of the mobility of the network.

For the second metric (time from start to finish), he was also influenced by the attack and in the same time by mobility, which makes sense from the results found previously.

To conclude, in such an attack traffic is diverted to a specific station or the malicious node influence on the whole of the network which induces to the injury of the MANET. The detection of such a nodes is difficult in this type of network.

REFERENCES

[1] Institute of Electrical and Electronics Engineers. IEEE Std 802.15.1-2005, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifi-cations for Wireless Personal Area Networks (WPANs), 14 June 2005. URLhttp://standards.ieee.org/getieee802/download/802.15.1-2005.pdf

[2] Institute of Electrical and Electronics Engineers. IEEE Std 802.15.4-2006, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifi-cations for Low-Rate Wireless Personal Area Networks (WPANs), 8 Septem-ber 2006.

[3] IEEE Std. 802.11a, "High-Speed Physical Layer in the 5 GHz Band," 2000.

[4] S. Upadhyay and B. K. Chaurasia, "Impact of wormhole attacks on MANETs", International Journal of computer science & Emerging Technologies (E-ISSN: 2044-6004) vol. 2, no. 1, (2011) February.

[5] Y. Z. T. W. W. Xu, W. Trappe, 2005. The feasibility of launching and detecting jamming attacks in wireless networks. Dans les actes de ACM international symposium on Mobile ad hoc Networking and Computing, 46–57.

[6] K. K. Z. Trabelsi, H. Rahmani et M. Frikha, 2004. Malicious sniffing systems detection platform. Dans les actes de International Symposium on Applications and the Internet, 201–207.

[7] V. N. P. M. M. K. M. Pirretti, S. Zhu et R. Brooks, 2005. The Sleep Deprivation Attack in Sensor Networks : Analysis and Methods of Defense. International Journal of Distributed Sensor Networks 2-3, 267–287.

[8] S. P. M. Al-Shurman, S. M. Yoo, 2004. Black hole attack in mobile Ad Hoc networks. Dans les actes de 42nd annual Southeast regional conference, 96–97.

[9] Y.C. Hu, A. Perrig, and D.B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In Proc. of the 2nd ACM workshop on Wireless security, page 40. ACM, 2003.

[10] G. Barrenetxea, F. Ingelrest, G. Schaefer, and M. Vetterli, "SensorScope: Out-of-the-Box Environmental Monitoring," in ACM/IEEE IPSN , 2008 Baydere, S.,Safkan, Y., and Durmaz, O. 2005.

[11] Lifetime Analysis of Reliable Wireless Sensor Networks. IEICE Transactions on Communications E88-B, 6, 2465-2472

[12] L. Selavo, A. Wood, Q. Cao, T. Sookoor, H. Liu, A. Srinivasan, Y. Wu, W. Kang, J. Stankovic, D. Young, and J. Porter, "LUSTER: Wireless Sensor Network for Environmental Research," in ACM SenSys , 2007.