SECURE ROUTING IN WSN

Rachid Haboub and Mohammed Ouzzif

RITM laboratory, Computer science and Networks team.
ENSEM - ESTC - UH2C, Casablanca, Morocco.

rachidhaboub@hotmail.com and ouzzif@yahoo.com

ABSTRACT

The growing diffusion of wireless sensors and the recent advances in Wireless Sensor Networks (WSNs) open new scenarios where sensors can be rapidly deployed without any existing infrastructure. Such networks are useful in many fields, such as emergency rescue, disaster relief, smart homes systems, patient monitoring, industrial applications, health monitoring, environmental control, military applications, etc. However WSN presents many challenges. These networks are prone to malicious users attack, because any device within the frequency range can get access to the WSN. There is a need for security mechanisms aware of the sensor challenges (low energy, computational resources, memory, etc.). Thus, this work aims to provide a secure WSN by changing the frequency of data transmission. This security approach was tested, and the results shows an interesting decreased of throughput from malicious node when the number of frequency used is increased, that way the WSN will not waste it's resources treating malicious packets.

KEYWORDS

Security, Wireless Sensor Networks (WSN), routing protocols.

1. INTRODUCTION

WSN's are a challenging topic and promise to change the concept of computer science and its role in every day's life. A WSN consists of several battery-powered computing units communicating with each other through radio messages and interacting with the environment through sensors. A wireless sensor network is a special network with many challenges compared to a traditional computer network. Due to these constraints it is difficult to directly employ existing security approaches to the area of WSN.

WSNs were initially proposed in domains where ordinary networks (not necessarily wired) are not convenient, either because of the missing infrastructures, or when numerous nodes (in the order of hundreds) are needed to achieve the assigned task. Examples of such domains are military applications (figure 1). WSNs can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems. The rapid deployment, self-organization and fault tolerance characteristics of sensor networks make them a very promising sensing technique for military.

Since sensor networks are based on the dense deployment of disposable and low-cost sensor nodes, destruction of some nodes by hostile actions does not affect a military operation as much as the destruction of a traditional sensor, which makes sensor networks concept a better approach for battle fields. Some of the military applications of sensor networks are monitoring friendly forces, equipment and ammunition, battle field surveillance, recognition of opposing

DOI : 10.5121/ijdps.2011.2624

forces and terrain, targeting, battle damage assessment, and nuclear, biological and chemical attack detection and recognition.

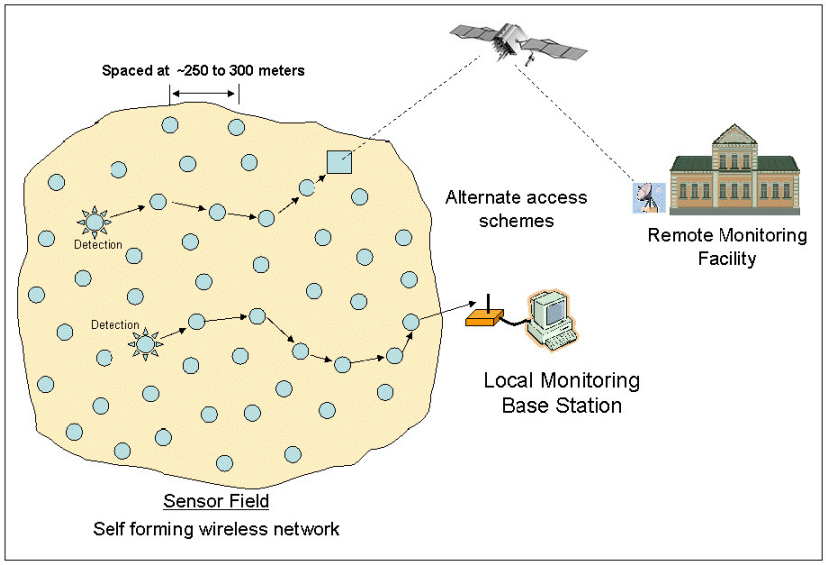

Figure 1. WSN application

However, for motion detection, security of all the WSN components is primordial. For example, if we consider a monitoring WSN to protect a specific area where there is no pre-existing infrastructure, the enemy may attack a set of sensing nodes, in order to get access to a specific area. Existing security approaches uses mainly encryption keys, which need too much resources. And as we know, WSN resources are limited [13]. In this paper we use a security approach, to improve the AODV (Ad-hoc On-demand Distance Vector) [10] routing protocol, in order to be protected from the resource exhaustion attack, by periodically changing the packet transmission frequency.

This paper is organized as follow: section two gives some related works. Section three show how a WSN can be attacked. Section four present a useful approach for the resource exhaustion attack, section five gives a simulation of the security approach. Finally the last section gives a conclusion.

2. PROBLEMATIC

Now a day, WSN are used in many critical fields such as emergency, military, etc. In such networks, security is very important, in order to be protected from malicious nodes attacks. There are many kinds of attacks: node outage, link layer jamming, collision attack, traffic manipulation and resource exhaustion [20].

Node outage consists of stopping the functionality of the WSN's components, such as a sensor node or a cluster-leader, by physically or logically damaging the network. Link layer jamming consist of finding data packet and to jam it [7], this kind of attack can cause colliding packets during transmission, exhausting nodes' resources and confusions.

Collision attacks consist of creating interferences in the network, by changing packet's fields and altering the “Ack message”. This may causes a corruption, a cripple and discarding the transmitted packets. It can also cost an energy exhaustion which is cost effective [9].

Traffic manipulations consist of regular monitoring transmissions and computing some parameters based on affected MAC protocol carefully, by doing a time adjustment, in order to transmit messages just at the moment when normal nodes do so. This decrease the signal quality, network availability and WSN performance, it also breaks the protocols operations, destroy the traffic and create confusions. This kind of attack is similar to the collision attack.

Resource exhaustion attack (in which we are interested) consists of doing repeated collisions and continuous retransmission out-of-date, dead and corrupted packets until the sensor node death. We consider as a scenario of WSN of 24 nodes and a malicious one (node 25). If the malicious node wants to do a resource exhaustion attack on node 0, it will at first search how to reach it.

In order to send malicious packets, the malicious node begins by broadcasting a RREQ (Route REQuest) message, to find a path leading to node 0 (figure 2).

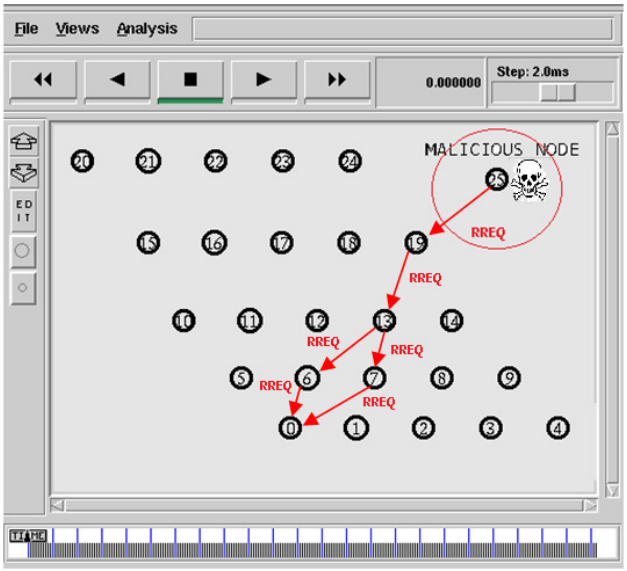

Figure 2. Malicious node sending Route REQuests to get access to node 0.

Next, a RREP (Route REPly) message will be received by the malicious node with the destination paths to node 0 (figure 3).

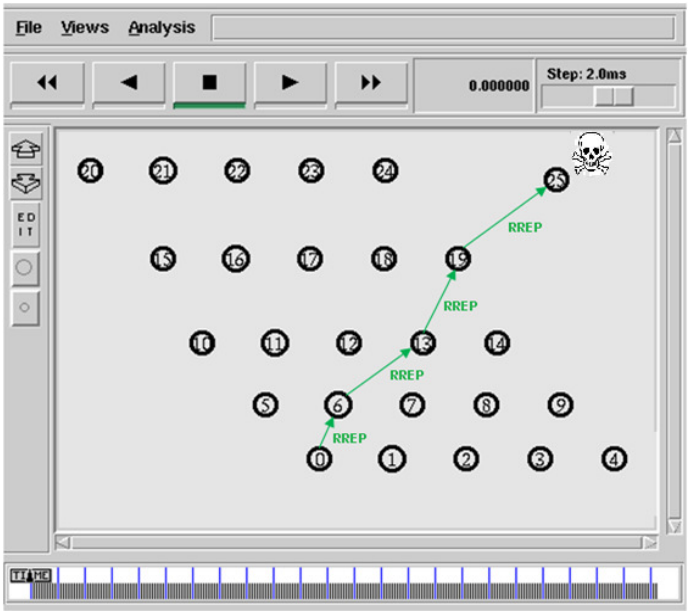

Figure 3. RREP message from destination to malicious node.

Once node 0 is localized and the path to reach it is defined, the malicious node will be able to send his malicious packets to node 0 (figure 4).

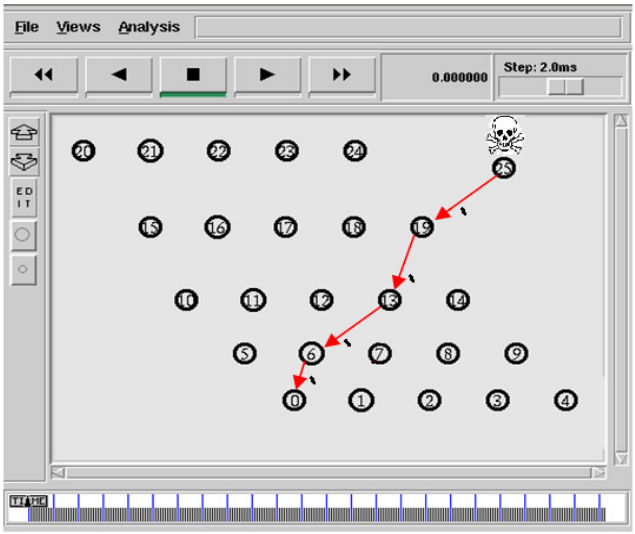

Figure 4. Malicious node trying to do a resource exhaustion attack to node 0.

3. RELATED WORKS

There are a lot of attacks types described in [5]. We are interested in the "Resource Exhaustion" attack. Existing security approaches require a certain amount of resources, including data memory, energy, etc. However, currently these resources are very limited in a tiny wireless sensor. The most common security mechanism is encryption techniques [1] which require using security keys and encrypting data, which consume the memory storage space inside the device. Wood and Stankovic [3] define a kind of denial of service attack as "any event that diminishes or eliminates a network's capacity to perform its expected function", denial of service attacks are not a new techniques, although this is still an open problem to the network security community. Unfortunately, wireless sensor networks cannot afford the computational overhead necessary in implementing many of the typical defensive strategies. LEAP [15] establishes different security requirements for each type of message, therefore, it uses four types of keys for each sensor node, and nodes need more storage capabilities, each sensor node has to store four types of keys, and it needs efficient mechanisms to update the keys.

4. APPROACH

There are two main categories of routing protocol in WSN (figure 5): proactive and reactive [2]. Proactive protocols maintain fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. Reactive protocols find a route on demand (only when needed) by flooding the network with Route Request packets. We have chosen the second kind of protocols which is suitable for the limited resources of WSN's. We adopt AODV which do not maintain routing information, but depend totally on needs to communicate.

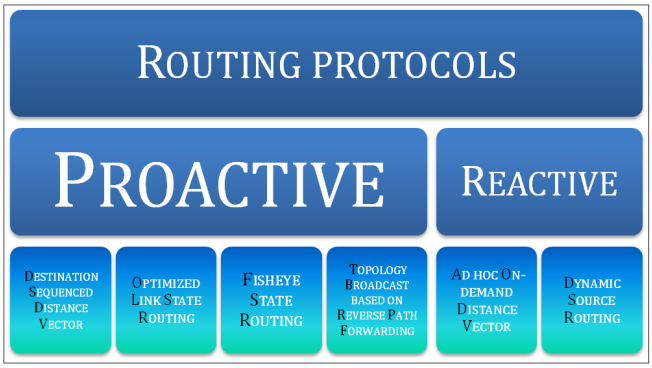

Figure 5. Routing protocols classification

AODV is suitable for the limited resources of WSN. It does not maintain any routing information but totally depends on needs to communicate with its neighbourhood. AODV broadcast discovery packets only when necessary. It is a simplest and widely used reactive routing protocol, which consume low energy, because it searches for a path to reach the destination on demand (only when a node needs to send packets). AODV do not store periodically the paths to destinations in routing tables.

In order to avoid the resource exhaustion attack, we propose to use different frequencies. This technique was suggested in the RFID (Radio Frequency IDentification) systems [6]. We adopt this mechanism in the AODV routing protocol, in order to ensure a secure AODV (SAODV). It is an efficient way to provide security in WSN. If we use for example 30 frequencies and if

intruders get access to the channel, it will only affect a particular channel, and there will be 29 channels still available for data transmission. If the number of frequency used are increased or/and time set of each frequency is random, the probability of intruder accessing the channels will be small.

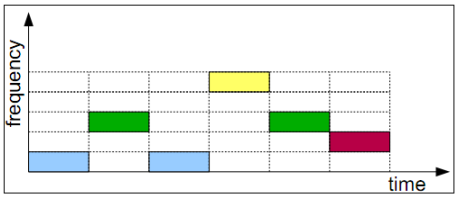

Figure 6. Frequency changing over time

AODV packet format consist of headers and data. There are many types of header available such as common header, IP header, TCP header, RTP header and Trace header. One can add his own header too by creating a new header in the NS2 (Network Simulator). The type of header used in this project is common header. Common header uses many fields to store packets information.

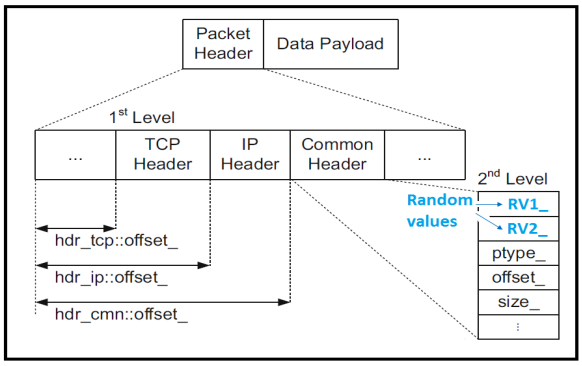

Figure 7. Packet format

In order to implement the security approach, we suggest adding two fields in the common header part of the packet header. This fields store two random values RV1 and RV2 (figure 7), generated before the packet transmission. Those random values allow the receiver to know malicious packets frequency in order to reject them. That way, the receiver will not waste his resources in treating malicious packets.

```
// Creating  two variables to store the random number:
        Double  RV1;
        Double  RV2;

// Setting two random values (the random values are between 0 and 1):
        RV1 = random number;
        RV2 = random number;

// Setting the frequency according to r:
        if (RV1 <= RV2)
        { Send packets using frequency number 1; }
        else
        { Send packets using frequency number 2; }
```

Figure 8. Changing frequency before the packet transmission

We have added in the AODV function which is responsible for packets transmission, the algorithm described in figure 7. This algorithm consists of generating two random values and sending packets in a specific frequency according to them.

Before transmitting a packet, SAODV (Secure AODV) transmission function will set the frequency to either 1 or 2. The variables RV1 and RV2 which has double data type, will keep the random numbers generated, in order to use them at the reception side.

```
//  Verification of the random values:
If (RV1 + RV2 <= 2) && (RV1 + RV2 >= 0)
{
        // Setting the frequency according to the random number r:
        If (RV1 <= RV2 ) { Random_Frequency =1;}
        else             { Random_Frequency =2;}
}

Else { Drop (packet); }

// Checking if the Random_Frequency is the same as the incoming packet
frequency:
If ( Random_Frequency != Incoming packet frequency )
        { Drop (packet); }

Else // Continue with AODV.
```

Figure 9. Frequency verification at the packet reception

When a packet is received, SAODV receiving function will check the random values and the incoming frequency (figure 9). If the packet frequency is not the same as the frequency according to the random number, then the packet will be dropped. If the frequency is the same to the frequency generated by the random numbers, the packet will be accepted.

5. SIMULATION

We use the NS-2 simulator [11]. Figure 10 gives a simplified View of NS-2. NS-2 takes as an input a TCL file (in which we implement the scenario). NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events.

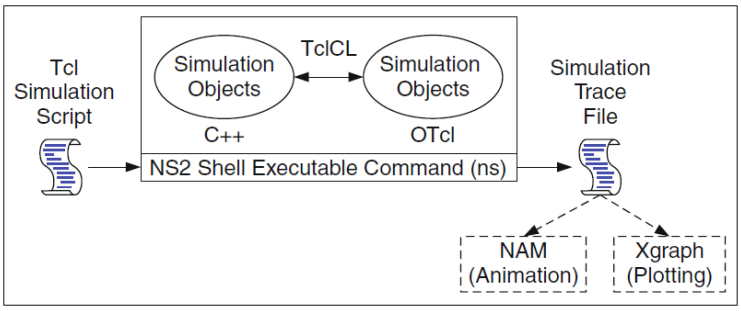

Figure 10. Simplified view of NS-2

After simulation, NS2 outputs a trace file, which can be interpreted by many tools, such as NAM and Xgraph. We create a simulation scenario using NS-2 Scenario Generator [12]. Table 1 shows the network parameter definition in the TCL file. The first parameter tells the simulator that nodes transmits and receives packets through wireless channels. We have used the IEEE 802.15.4 standard, which specifies the media access control and the physical layer. val(nn) is the number of nodes, which is set to 25. val(rp) is set to the SAODV protocol, which represent the routing protocol used in the simulation. val(x) and val(y) are equal to 50 meter. So 50 m² is the simulation area. val(stop) represent the simulation time, and is equal to 50 second.

Table 1. Network parameter definition.

Parameter	Suggested Value	Description
val (chan)	Channel/Wireless Channel	Channel type
val (mac)	Mac/802_15_4	IEEE standard
val (nn)	25	Number of nodes
val (rp)	SAODV	Routing protocol
val (x)	50	Setup topography object
val (y)	50	Setup topography object
val (stop)	50	Simulation time

We use the Java-Trace-Analyzer to interpret the trace file generated by the simulation. Figure 11 shows the NS-2 trace file format. The first field is event, it gives many possible symbols ('r', 'd', etc.). These symbols may correspond for example to received and dropped packets. The second field gives the time at which the event occurs. The third field gives the source node at which the event occurs. The fourth field gives the destination node at which the event occurs. The fifth field shows information about the packet type, whether it's a UDP or a TCP packet. The sixth field gives the packet size. The seventh field gives information about some flags. The Fid field is the flow Id, it can be used for specifying the colour of flow in NAM display. The ninth field is the source address. The tenth field is the destination address. The eleventh field is the network layer protocol's packet sequence number, and the last field shows the unique id of a packet.

Event	Time	Source	Destination	Pkt type	Pkt size	Flags	Fid	Src addr	Dst addr	Seq num	Pkt id

Figure 11. NS-2 Trace File format

The simulation results presented in figure 12 shows that the throughput of dropping packets (coming from the malicious node) at the destination node is low using the AODV protocol. The throughput of dropping packets at the receiving node becomes high using the security approach. This means that using this approach allow rejecting malicious packets. Then malicious node will not be able to do resource exhaustion on the WSN.

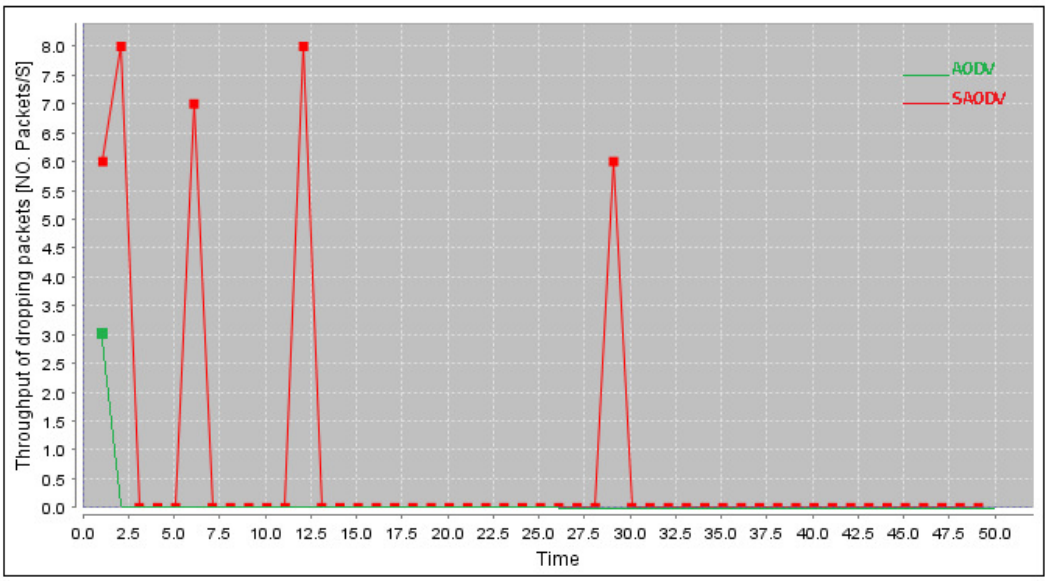

Figure 12. Throughput of dropping packets (coming from the malicious node) at the receiving node

The simulation results presented in figure 13 shows that using SAODV, the victim node will not waste its energy. However, when we use AODV, the victim node wastes all its energy in 60 minutes.

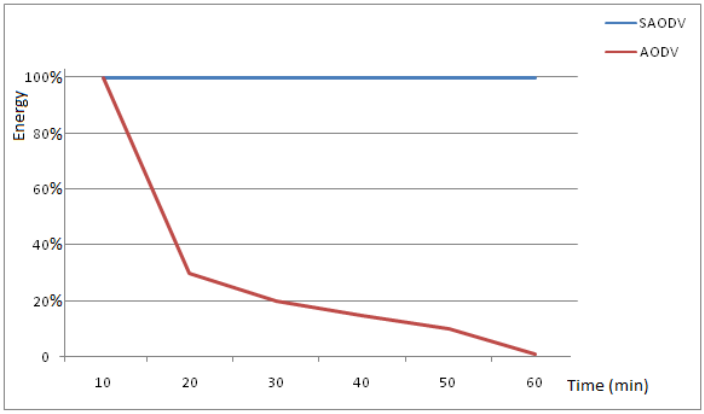

Figure 13. Energy level over time of the victim node

6. CONCLUSION AND FUTURE WORKS

In this paper, we have used an approach based on changing the packet transmission frequency in the AODV protocol, which is a reactive protocol. The goal is to avoid the resource exhaustion attack. We have shown a resource exhaustion attack scenario, which we have simulated using NS-2. Simulation results show that a victim node will not waste its resources treating malicious packets.

Changing the frequency for transmission packets in order to secure a WSN from the resource exhaustion attack, may be useful for many fields, such as in the military.

For future work we intend using the changing frequency approach in another kind of routing protocols in WSN's, then add a switching technique from one protocol to another, based on sensor states (energy, mobility, connectivity, vicinity, etc.). At the end we will have a secure and context aware protocol.

REFERENCES

[1] William Stallings (2003). 3 rd Ed. "Cryptography and Network Security - Principles and Practices". Pearson Education Inc. New Jersey.

[2] José Carlos Castillo, Teresa Olivares and Luis Orozco-Barbosa, "Routing protocols for wireless sensor networks", 2011.

[3] D. Wood and J. A. Stankovic. "Denial of service in sensor networks". Computer, 35(10):54–62, 2002.

[4] Xiuli Ren and Haibin Yu, "Security Mechanisms for Wireless Sensor Networks", International Journal of Computer Science and Network Security, VOL.6 No.3, March 2006.

[5] Dr. Shahriar Mohammadi and Hossein Jadidoleslamy, "A comparison of link layer attacks on wireless sensor networks", Vol.3, No.1, March 2011.

[6] Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels, "RFID Systems and Security and Privacy Implications", Cambridge, Springer 2003.

[7] Saurabh Singh, Dr. Harsh Kumar Verma , "Security For Wireless Sensor Network", International Journal on Computer Science and Engineering, Vol. 3 No. 6 June 2011.

[8] Ritu Sharma, Yogesh Chaba, Yudhvir Singh, "Analysis of Security Protocols in Wireless Sensor Network", International Journal Advanced Networking and Applications, Volume: 02, Issue: 03, Pages: 707-713 (2010).

[9] Jinat Rehana, "Security of Wireless Sensor Network", 2009.

[10] M.Devi and Dr.V.Rhymend Uthariaraj, "Routing with AODV Protocol for Mobile ADHOC Network", International Journal of Technology And Engineering System, Jan – March 2011-Vol2. No1.

[11] Kevin Fall, Kannan Varadhan, "The NS manual", May 9, 2010.

[12] Jia Huang, Hamid Shahnasser, "A preprocessor Tcl script generator for NS-2 communication network simulation", San Francisco State University, USA, pp. 184-187, 5 May 2011.

[13] Kamal Kumar Sharma, Ram Bahadur Patel and Harbhajan Singh, "A Reliable and Energy Efficient Transport Protocol for Wireless Sensor Networks", International Journal of Computer Networks & Communications (IJCNC) Vol.2, No.5, September 2010.

Authors

Haboub is a Ph.D student. He received the Master degree in computer science, assan II University, Ben M'sik faculty of Morocco in 2009. His research spans s communication.

Dr. Mohammed Ouzzif is a professor in the computer science department of the higher school of technology of Casablanca - Hassan II university of Morocco.