Towards An Improvement of the Security of A WSN Based On Power Management as Part of the QOS

Lamyaa Moulad, Hicham Belhadaoui, Mounir Rifi, Reda Filali hilali

Abstract— Wireless sensor networks (WSN) is tending towards becoming a complete solution in communication protocols, embedded systems and low-power implementations. However, the resource constraints which includes, limited communication range, limited energy, limited computing power, limited bandwidth and the fear of intruders have limited the WSN applications. Since lightweight computational nodes that are currently being used in WSN pose particular challenge for many security applications, the whole research therefore, is the investigation of new security techniques and appropriate implementation for WSN nodes, including various trade-offs such as implementation complexity, security flexibility, power dissipation, and scalability. The goal of this research is to develop a scheme to control the flow through the components of the WSN. This allows to improving the security of WSN by the good management of energy resources, as well as the local management of communications. In this sense, we proposed an improvement of the reactive AODV Routing Protocol [11] under the NS2 Simulator for the security support always as part of Quality of Service .

Keywords— WSN, energy management, security, NS2 Simulator.

I. INTRODUCTION

Wireless sensor nodes are low power electronic devices commonly deployed in remote areas, where batteries cannot be recharged. The complexity of the sensor network increases with power scavenging schemes. Hence, efficient usage of energy becomes a priority. Recently, the demand of wireless sensor networks (WSN) [1] [2] [3].has extended to many real world applications such as health monitoring, emergency evacuations security, soldiers in battlefield, biometric application in airport, etc., where sensitive data is communicated insecurely to the destination node (sink). Thus, WSN can be easily attacked by denial-of-service (DoS) attacks, which sacrifices the information as well as causing large energy expeditious. Therefore, controlling energy consumption is important to secure a WSN .

Manuscript received April. 2013.

L.Moulad is a Ph.D student in ENSEM . She received the Master degree in computer science, from Hassan II University, Ain chock faculty of Morocco in 2011. Her research spans wireless Sensor communication.

M.Rifi is a professor in the computer science department of the higher school of technology of Casablanca(ESTC) - Hassan II university of Morocco and the director of (ESTC).

H.Belhadaoui is a professor in the computer science department of the higher school of technology of Casablanca - Hassan II university of Morocco.

R.Filali Hilali is a professor in the computer science department of the higher school of technology of Casablanca - Hassan II university of Morocco.

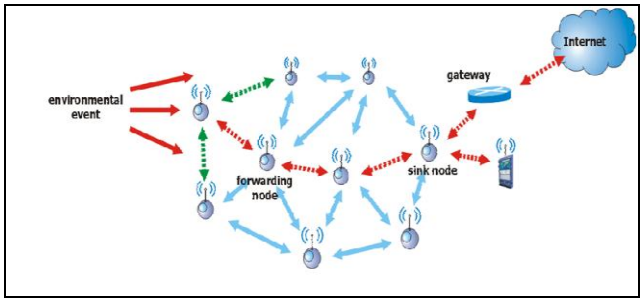

Figure 1: WSN's architecture

Constraints in sensor networks

A WSN is made up of a large number of sensor nodes which are by nature's resources. These nodes have a limited processing capacity, storage very low and constrained communication bandwidth capacity. These limitations are due to limited energy and the physical size of the sensor nodes. Because of these constraints, it is difficult to directly employ traditional security mechanisms in sensor networks. To optimize the conventional security for sensor networks algorithms, you need to be aware on the constraints of sensor nodes (Carman et al., 2000).

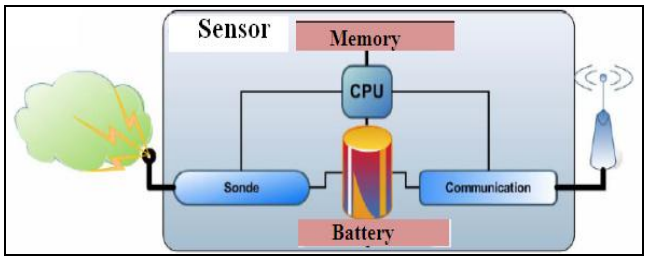

Figure 2: WSN's interne architecture

Energy and sensor networks

In ad-hoc networks, energy consumption was considered a factor decisive but not as energy resources can be replaced by the user. These networks focus more on QoS (Quality of Service) on the consumption of energy. On the other hand, in sensor networks, energy consumption is very important because generally the sensors deployed in inaccessible areas. Thus, it is difficult if not impossible to replace the batteries after their exhaustion. Thus, consumption of energy at the level of the sensor has a great influence on the lifetime of the network it is also considered as a fundamental parameter in a context of availability and security in [08] wireless sensor networks, can be inferred therefore that maximize the lifetime of the network is to reduce the energy consumption of the nodes.

Despite the progress that has been made, these devices battery life continues to be a challenge.

Vulnerabilities of security in sensor networks

Wireless sensor networks are vulnerable to different types of attack. These attacks are primarily of three types (Shi et al. 2004.):

(1) Attacks the availability of the network: the attacks on the availability of WSN are often referred to as DoS attacks.

(2) attacks on the secret and authentication: standard cryptographic techniques can protect the secret and the authenticity of the communication channels against external attacks such as listening, packet replay attacks, and changing or spoofing of packets.

(3) the stealth attack on the integrity of the service: in a stealthy attack, the goal of the attacker is to make the network accepts a value false data. For example, an attacker compromises a sensor node and injects a value of false data by this sensor node.

Security of routing in sensor networks

Routing is a main function in ad hoc networks. It is the mechanism by which the railways are created to route the data to the correct destination through a network. This function is divided into two parts: the routing protocol and routing service.

-The routing protocol is a set of rules that specify the manner with which routers communicate with each other to Exchange topology information enabling them to build their own vision of the network.

-The routing service provides for transmission of data packets using built vision previously.

Indeed without the routing protocol, there is more vision of the network preventing the delivery of data to the destination. Indeed secure routing protocol is to secure the result of this step which is the vision of the network which allows secure routing service. It is important to note that we do not discuss the security of the exchanged data packets but that of routing protocol packets.

II. RELATED WORKS

Many solutions have been proposed to secure WSN routing protocols.

We classify these solutions into two categories: proactive security systems in the direction where the mechanisms are established in advance to ensure the security by strengthening the resilience of the system to the attacks through cryptography-based [7] solutions and reactive security systems that react (adaptation/immediate decision making) according to the behavior of the neighborhood and which is even divided into reputation and trust management solutions.

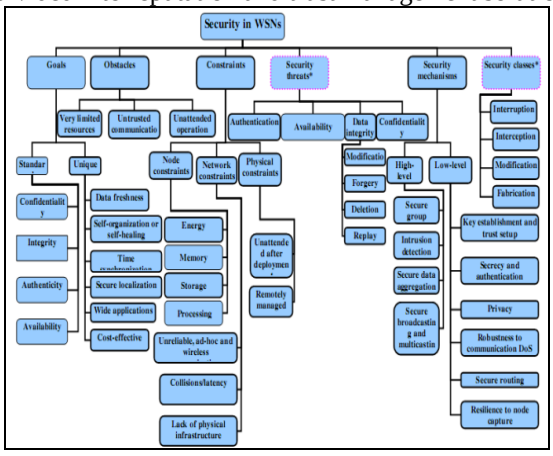

Figure 3: Security in WSN

Sscenario Wireless Sensor Networks are considered to be most active field for research. The security in sensor network also attracts much of attention of researchers towards WSN. The paper in [12] proposed a secure packet transfer between nodes by use of public key cryptographic techniques in packet header. The results suggested that PKC based user access control scheme has got advantage over symmetric key cryptography in terms of memory usage, memory complexity and security resilience.

In [22] an approach proposed for prevention of flooding attack in wireless sensor network in three modules (PMM/RTM/DM) for detecting flooding attack state full signature and rate of transmission are considered as prime criteria's .In order to compensate for energy lost due to integration of these modules, nodes make use of modified LEACH to route the information towards the sink but there is a high probability that the nodes will exhaust .The scheme proposed in [13] proposes concept of duplication of hardware in network at core points. If at some point of time any node gets failed or compromised it is removed from the network without affecting availability and information flow in the network. The problem with this scheme is that total cost of laying the network increases and it does not provide any hard core solution that can prevent the attack.

The scheme in [14, 21] proposes a scheme to prevent path based DoS attacks. In this scheme power of hash functions is used to secure the communication link between the chaining nodes for communication purpose. The technique works well when number of nodes is less .Another setback of this technique is that it cannot handle wide range of DoS attacks.

In [14, 18], a stronger authentication scheme is proposed in which every node who is interested in joining the cluster has to solve a puzzle tossed by head node. The head node tosses puzzle based on reputation of the node. This technique exhausts the resources of legitimate node to some extent too. And. In [15,16] a graph neuron based approach is used. Nodes are named as Graph Neurons. In this approach GN keeps an eye on the network traffic and communicates the findings with other GN nodes. Then the GN uses the flooding rules to construct the traffic flow between GN nodes itself. The, ultimate decision, whether, attack has taken place or not, depends on sink station. The primary problem in concepts proposed in [15, 16] is that both techniques involves lot of computations on incoming packets hence there is high probability that the nodes will exhaust prematurely.

Reference [17] proposed two solutions for detection of flooding attack in which concepts of game theory are used. Here game between attacker and legitimate node is played. Here concept of Nash equilibrium is applied. The algorithm is also restricted by amount of processing time and memory availability. Reference [19] In this approach, on each forwarded packet, the edge of the forwarding path is marked by certain probability and this mark is written in marking field of the packet also. The position relationship of two nodes on attack path is determined for trace back.

III. APPROACH

Routing in ad hoc networks protocols can be divided into two broad classes: proactive(ex OLSR) and reactive(ex AODV), depending on the way in which routes are created and maintained ,a third class can be added, is that of hybrid protocols, which is the combination of the two classes.

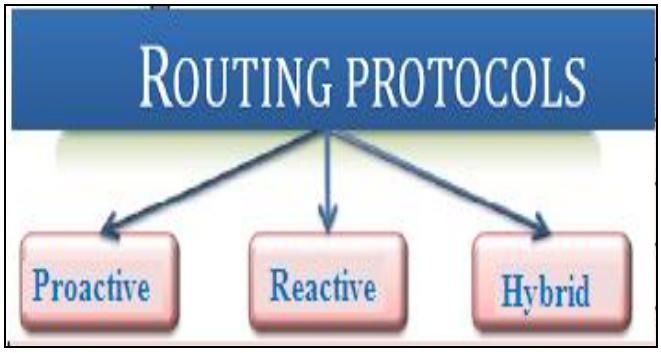

Figure 4: The routing protocols in the WSN

Proactive routing protocols maintain permanently routes to all destinations, these protocols have the advantage of immediate availability of roads. However, an important control traffic is required to update these roads. While the reactive routing protocols establish routes only to the application "On-Demand" consensus protocols do not consume lots of bandwidth of the network. On the other hand, they have more time to looking for itinerary.

We chose the second type of protocols which is suitable for the limited resources of the WSN and taking AODV, which is suitable for the limited resources of WSN. AODV has no routing information, but totally depends on the needs to connect with its neighborhood and the transmission of discovery only packets when necessary. It's a simple reaction and widely used by a routing protocol, which consumes little power, as it seeks a way to achieve the destination on request (only when a node must send packets).

AODV routing with quality of service (Energy for security)

The introduction of the quality of service in AODV is based on the addition of a field in the control RREQ packets, pair this field can be associated with the parameter time, bandwidth setting, energy, etc. Receiving an RREQ message, each mobile verifies that it is able to deliver the requested service, before retransmitting the message.

The AODV with QOS routing protocol is designed to:
• Improve the QOS in ad hoc networks.
• Introduce a metrics more appropriate that the distance (number of hops). Therefore to integrate the service quality in the aodv Protocol is to introduce several extensions in the structure of the routing table in the road (RREQ) request in the response of Road (pair) and in messages Hello to that reservation model described previously is integrated into the AODV protocol.
In our work we are interested in the energy metric and also as we have said that the components of the network must be able to honor the service requested namely energy resources [10] to avoid any unwanted overconsumption and therefore an abnormal failure of the network it comes back so was control the energy level by monitoring the routing of package circulating in network in order to ensure longevity of the WSN we can therefore deduce that our proposal is oriented reputation management since the principle will be based on the consciousness of each the networking component (node,...) which must ensure State in its neighborhood.

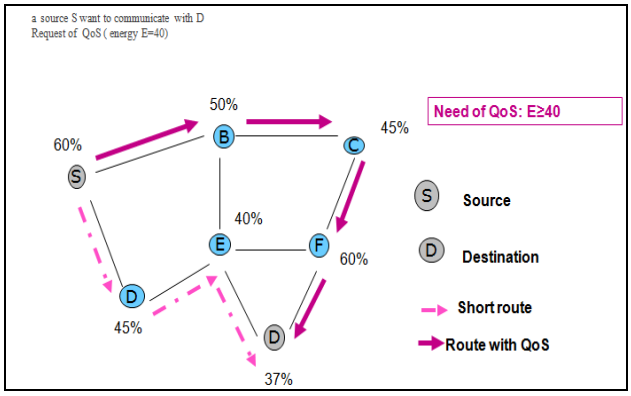

Figure 5: QoS with energy management to control access to node's energy resources

IV. SIMULATION

To test a routing protocol is often used in the simulation. Indeed it would be very expensive if not impossible to put in place a network for the purpose of testing for certain criteria. In our simulation is put to contribution the NS2 to analyze a few properties of the AODV Routing Protocol. The NS2 Network Simulator is a software tool for simulation of computer networks. It is mainly built with the design ideas by objects, modularity and code reuse.

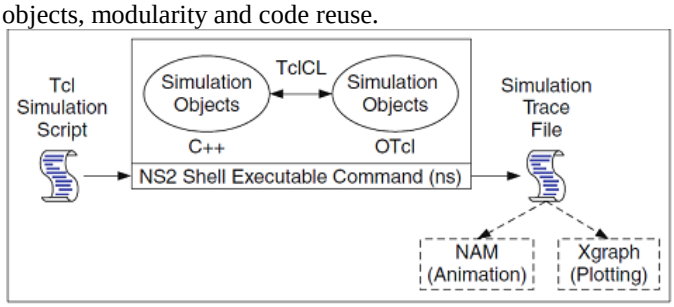

Figure 6 : View of NS-2

Ns2 is written in C++ and uses the OTCL (Object Tools Command Language) language derived from TCL. Through OTCL, the user describes the simulation conditions: the topology of the network, the characteristics of the physical links, protocols, communications taking place. The simulation must be entered as an file that NS will use to produce a file containing the results. But the use of the Otcl also allows the user to create its own procedures.

Simulation environment:

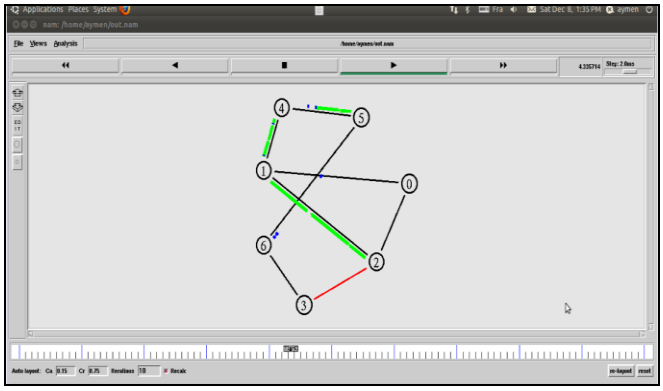

Figure 7: Packet's flow between nodes

Any request abnormal and excessive energy gives a strong indication status of bad behavior, intrusion or attack (we are interested to the resources exhaustion or flooding) [figure 8]the WSN devices, however all the components of the network must be able to honor the service requested namely energy resources [10] to avoid any undesirable overuse.In this context we can thanks to this technique control the flow through the components of the WSN. This allows to reduce the complexity of the routing on a large scale by the good management of energy resources. In this sense, we proposed an improvement of the reactive AODV Routing Protocol [11] under the NS2 Simulator for the quality of service support .

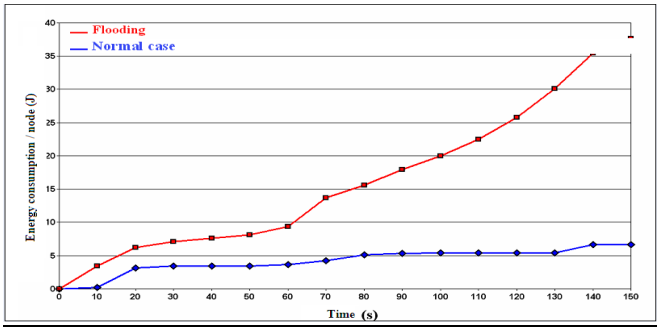

Figure 8:Energy consumption comparison between flooding and normal case

The simulation results presented in figure 9 shows that using QESAODV the victim node will not loses its energy. but when we use AODV, the victim node loses all its energy in 120 minutes.

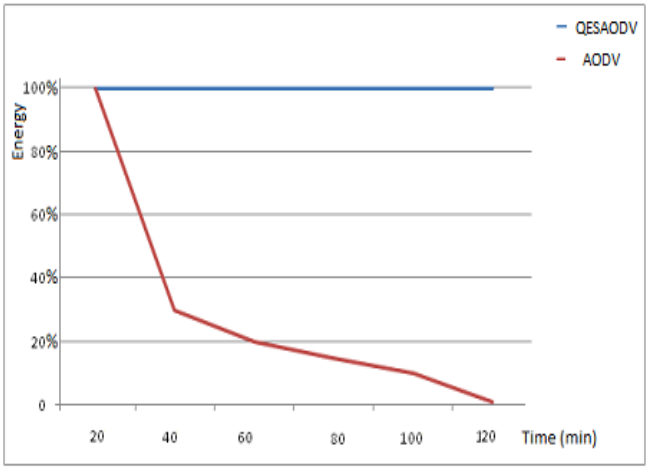

Figure 9: Energy level over time of the victim node

V. CONCLUSION

In a WSN to provide adequate levels of quality of service (QoS). Due to the complexity and the magnitude of the sensors (WSN) wireless networks, quality of service can no longer been seen within the limited perspective of network throughput, the time and bit the error rate / package. system design should encompass other QoS properties such as the energy sustainability (efficiency energy system), dependability (reliability, availability, security, safety and so on), speed (throughput, delay traffic differentiation), scalability, mobility, heterogeneity or profitability.

Although these quality attributes are not new and have already been treated separately, address and satisfy all has not yet been done.

As a future work, we plan identify sources of energy consumption by analyzing the level of the traffic flowing in Wireless sensor networks.

REFERENCES

[1] Houngbadji, Thérence (2009) Réseaux ad hoc : système d'adressage et méthodes d'accessibilité aux données. Thèse de doctorat.

[2] I. F. Akyildiz et al, "Wireless Sensor Networks: a survey, " Computer Networks, Vol. 38, pp. 393-422, March 2002.

[3] H. Karl and A. Willig, "A short survey of wireless sensor networks" Technical Report TKN-03-018, Telecommunication Networks (2004).

[4] andrien Van Den Bossche (2007),proposition d'une nouvelle méthode d'accès déterministe por un reseau personnel sans fil a forte contraintes temporelles.

[5] D.mohammadi & H.jadidoleslamy 'comparison of the attacks on the link layer in wsn ' 2011

[6] JA Stankovic 'DOS in WSN ' .

[7] W. Stallings 'Cryptography and network security' 2003.

[8] Wassim Masri (2009), Dérivation d'exigences de Qualité de Service dans les Réseaux de Capteurs Sans Fil basés sur TDMA.

[9] Cobo Campo, Luis (2011) Gestion de la qualité de service et planification optimale de réseaux de capteurs multimédia sans fil.

[10] Rahim KACIMI ,(Septembre 2009) Techniques de conservation d'énergie pour les réseaux de capteurs sans fil l'Institut National Polytechnique de Toulouse.

[11] Teresa Albero-Albero,(2007) AODV Performance Evaluation and Proposal of Parameters Modification for Multimedia Traffic on Wireless Ad hoc Networks, Universidad Politécnica de Valencia .

[12] Haodong Wang; Bo Sheng; Tan, C.C.; Qun Li; "Comparing Symmetric-key and Public-key Based Security Schemes in Sensor Networks: A Case Study of User Access Control"; Distributed Computing Systems, 2008. ICDCS '08. The 28th International Conference;Year: 2008 , pp: 11 – 18.

[13] Man Wah Chiang; Zilic, Z.; Radecka, K.; Chenard, J.-S.; "Architectures of increased availability wireless sensor network nodes"; Test Conference, 2004. Proceedings. ITC 2005. International, year 2005, pp: 1232 – 1241.

[14] Jing Deng, Richard Han, Shivakant Mishra; "Defending against path-based DoS attacks in wireless sensor networks"; 3rd ACM workshop on Security of ad-hoc and sensor network", Year: 2005.

[15] Meadows, Catherine; "A Cost-Based Framework for Analysis of Denial of Service in Networks", NAVAL RESEARCH LAB WASHINGTON DC CENTER FOR HIGH ASSURANCE COMPUTING SYSTEMS (CHACS), Year:2005.

[16] Baig, Z.A.; Khan, S.A.; "Fuzzy Logic-Based Decision Making for Detecting Distributed Node Exhaustion Attacks in Wireless Sensor Networks "; Future Networks, 2010. ICFN '10. Second International Conference;Year: 2010 , Page(s): 185 - 189.

[17] Z.A.Baig, M. Bager, A.I.Khan;, "A Pattern Recognition Scheme for Distributed Denial of Service (DDoS) Attacks in Wireless Sensor Networks". ICPR '06 Proceedings of the 18th International Conference on Pattern Recognition - Volume 03, Year: 2006.

[18] Agah, A.; Basu, K.; Das, S.K.; "Preventing DoS attack in Sensor Networks: A Game Theoretic Approach"; Communications, 2005. ICC 2005. 2005 IEEE International Conference; Year: May 2005 page(s): 3218 - 3222 Vol. 5.

[19] Mihui Kim; Inshil Doh; Kijoon Chae; "Denial-of-Service(DoS) Detection through Practical Entropy Estimation on Hierarchical Sensor Networks"; Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference; Volume: 3; Year: 2006 , Page(s): 5 pp. – 1566.

[20] Jun Xu; Xuehai Zhou; Feng Yang; "Edge-based Trace back in Sensor Networks"; Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference;Year: 2010 , Page(s): 1 – 4.

[21] Xi Luo; Yi-Ying Zhang; Wen-Cheng Yang; Myong-Soon Park; "Prevention of DoS Attacks Based on Light Weight Dynamic Key Mechanism in Hierarchical Wireless Sensor Networks"; Future Generation Communication and Networking, 2008. FGCN '08. Second International Conference; Volume: 1; Year: 2008 , Page(s): 309 - 312 .

[22] P.Suraksha bhushan,A.Pandey,R.C Triphati "A Scheme for prevention of flooding attach in wireless sensor network", Sience academy publisher,United kingdom, (IJRRWSN) .