Applied Mathematics & Information Sciences **5**(3) (2011), 655-667
– An International Journal

Study of key pre-distribution schemes in wireless sensor networks: case of BROSK (use of WSNet)

A. Jemai[1,2], A. Mastouri[2] and H. Eleuch[1,3]

[1]Institut National des Sciences Appliques et de Technologie (INSAT),
University of Carthage, BP676, 1080 Tunis Cedex, Tunisie
Email Address: : abderrazak.jemai@insat.tn

[2]Laboratoire LIP2, Facult des Sciences de Tunis, 1060 Belvedere Tunis, Tunisie

[3]Institute for Quantum Science and Engineering and Department of Physics and Astronomy,
Texas A&M University, TX 77843, USA

Wireless sensor networks are composed of small entities with limited memory, computation and communication capabilities. These entities role is to detect process and transmit information. Therefore, they are considered as embedded systems. Wireless sensor networks are deployed in many hostile environments and face many security issues. Sensor nodes are also resource-constrained. To achieve security in wireless sensor networks, many key management (distribution and share) schemes have been proposed. In this paper we aim to study these key distribution schemes and implement one of them (BROSK) and look at its behaviour in terms of energy consumption and the construction of shared keys using a wireless sensor network simulator (WSNet).

Keywords: wireless sensor networks, embedded systems, key pre-distribution schemes, WSNet.

1 Introduction

Distributed sensor networks are deployed in many fields and applications (environment, military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environments, etc...). Sensors are randomly spread over the terrain under security [24]. To secure these networks from threats [7] (eavesdropping, message injection, message modification, message replay, impersonation DOS, etc...) [11, 25, 26], symmetric cryptography is used. Its more adequate for WSN with low powered sensors [3, 20, 22].
Key distribution is a serious problem in wireless sensor networks conception [12]. Its done before the nodes deployment; nodes construct the network using their secret keys after

they are deployed: when they reach their targets [16]. Many key pre-distribution schemes have been proposed [2, 4, 15, 17, 23, 24]. In this paper, the operation of one of these schemes (BROSK) is studied by implementing and simulating it, using a wireless sensor network simulator (WSNet). BROSK (BROadcast Session Key) is based on constructing session keys between communicating nodes. Results obtained are exploited to evaluate its functionalities.

2 Related works

Wireless sensor networks are composed of sensors with small sizes, low power and cost deployed in a space to monitor the environment. Thus, security is very important when WSN are deployed in hostile environment. Sensitive data have to be protected to ensure authenticity, confidentiality and integrity. Resources constraint is the principle WSN limitation [12].

Notation

- A, B: Communicating nodes.
- BS: Base Station
- ID_A, ID_B: Identifiers (Names) of nodes A and B.
- N_A, N_B: Nonces of nodes A and B (generated randomly by nodes A and B).
- $MAC(K, M)$: Message Authentication Code of data M created by key K.
- $M1|M2$: Concatenation of data $M1$ and $M2$.
- $A \rightarrow B : node\mathrm{A}unicastsamessagetonodeB.$
- K_{AB} : shared key between A and B.

- K_{enc}: encryption key.

- K_{mac}: MAC key.

Different key pre-distribution schemes were proposed. Echenauer and Gligor proposed a random key pre distribution scheme in [16], this scheme is based on a probabilistic key sharing among nodes of a random graph [11, 15]. It consists of three phases: key pre-distribution, shared key discovery and path key establishment. Before deployment, every node selects a subset of keys from a large size key pool and stores them in its memory [13, 14]. The key discovery process is done to exchange information with a node neighbours after deployment. If two neighbour nodes share one or more common keys in their memory, they can establish a secure communication link between them. The path key establishment process is done when two communicating nodes need to communicate with an intermediate node.

Zhu et al. introduced in [23] a Localised Encryption and Authentication Protocol (LEAP).The authors of this scheme support the idea that a unique key pre- distribution mechanism cant guarantee secure communications in wireless sensors networks. Thats why they propose the establishment of four types of keys: individual key shared between the node and the base station, group key used by the base station to encrypt its communications with WSN nodes, cluster key shared by a node and all its neighbours and pairwise key shared by a node and its immediate neighbours.

Perring et al. proposed in [2] SPINS (Security Protocols for Sensor Networks). This scheme is presented as a set of sub-protocols. The set is composed of two protocols: SNEP and TESLA. The first one provides confidentiality, authenticity, integrity and data freshness however the second offers authenticity when transmitting data [6].

SNEP [17, 26] describes basic primitives providing confidentiality and authenticity between two communicating nodes. It uses a shared counter. Every text block is encrypted with a counter using a block cipher in counter mode algorithm. The receiver/sender increments the counter after each block [2]. Theses counters offer an order and freshness to data. The secured message exchanged between A and B is: $A \rightarrow B : E(Kenc, C) + M, MAC(K_{mac}, (M|E(K_{enc}, C) + M))$

The second sub-protocol ν TESLA (ν Timed Efficient Streaming Loss tolerant Authentication Protocol) -which ensures authenticated transmissions- consists of several phases: sender set up, broadcasting authenticated packets, bootstrap a new receiver, authenticating broadcast packets and nodes broadcast authenticated data.

In the first step, the sender node generates a sequence of m keys by randomly selecting the last key Km and applying a one way function to generate the remaining keys of the chain. The second step is to broadcast authenticated packets, in every time interval, the sender

uses a key from the chain to compute the MAC of the packets to send in this interval. The sender reveals the key after a delay of d intervals after the end of the interval.
For the bootstrapping of a new receiver phase, one receiver having the authenticated value of K_j can easily authenticate a K_{j+1} by verifying $K_j = F(K_{j+1})$. Every receiver node must have an authenticated key from the key chain. The receiver broadcasts a nonce in the message to send to the sender, which replies with a message containing the following components: T_s: the current time of the sender, K_i: a key in the one way key chain, T_i: starting time, T_{int}: duration of time interval, and δ: disclosure delay.
$A \rightarrow B : N_A$
$B \rightarrow A : (T_S|K_i|T_i|T_{int}|\delta), MAC(K_{BA}, N_A|T_S|K_i|T_i|T_{int}|\delta)$

The sender has to be sure that the packet has been sent by an authenticated sender and by an adversary (authenticating broadcast packets). This is achieved through loose synchronization of the sender and receiver. If the packet is legal, the receiver stores it; if it is spoofed, it is dropped. Once the receiver verifies the key, it authenticates the packets with the key and replaces that new key with the key it already has.
Blundo et al. [8] suggested the $PDKD$ protocol (Perfectly-Secure Key Distribution for Dynamic Conferences). In a set of n user, the protocol permits to a sub-set of t users to establish a group key resisting to coalition of $d = n - t$ users. In other words, even if d users collect the information they have, they cant discover the key [14]. SNAKE [6] is another protocol proposed for the establishment of session keys. A node A issues a request to node B. Node B will reply with a message as a challenge to node A which receives the message, authenticate it and resends it to A. its a mutual challenge and authentication procedure. Nodes A and B will use K_{AB} as their shared session key:

1. $A \rightarrow B : request|N_A$;
   K master key shared by all the nodes

2. $B \rightarrow A : M = (ID_B|ID_A|N_A|N_B)|MAC(K, M)$;

3. $A \rightarrow B : ID_A|N_B|MAC(K, ID_A|N_B)$;

4. $K_{AB} = MAC(N_A|N_B)$;

Blom et al. proposed in [14, 21]the matrix based scheme. In this scheme [14], two matrices G and D are constructed by the base station [24]. It then computes a matrix A:

$$G = (\lambda + 1) + n$$
$$D = (\lambda + 1) + (\lambda + 1)$$
$$A = (D.G)^T$$

λ is the threshold provided to compromise the secret
G is considered as public information so every node (even an adversary) can have an idea on what it contains while D is considered as private information and must not be revealed.
Keys used by pairs of nodes are:
$K = (D.G)^T.G$

A pair of nodes (i, j) will use K_{ij}, (line i and column j of K). K is a symmetric matrix ($K_{ij} = K_{ji}$) therefore if node i knows line i of K and j knows column j they have a common key.

3 BROadcast Session Key Negotiating Protocol

In protocol BROSK, session keys are constructed between nodes. Every node can broadcast a key negotiation message to its neighbours [4, 6, 26]. The establishment of the shared keys is done before the network deployment so that communication between nodes sharing keys is secure and authenticated.
The message sent by a node A is as follow:

$ID_A|N_A|MAC(K, ID_A|N_A)$

Another node B will broadcast the same message

$ID_B|N_B|MAC(K, ID_B|N_B)$

The shared key is obtained by generating the MAC of the two nonces by one node (A or B):

$$K_{AB} = MAC(K, N_A|N_B)$$

The Method Authentication Code (MAC) is used to ensure authentication of the transmitted message and a nonce is unique for every node, its a random character chain generated by one node. Nodes then will use these shared keys to secure the exchanged messages.

4 Simulation (WSNet)

To implement BROSK, a wireless sensor network simulator (WSNet) is used. Its a simulator that has been developed in CITI laboratory of INSA Lyon. WSNet is a modular event-driven wireless network simulator [1, 9]. Several blocks define the functionalities of the nodes and the radio medium. WSNet is based on modules that are either provided by the simulator or by users [19]. To simulate the protocol BROSK, we have used some modules provided by the simulator and developed other modules. To set a simulation, WSNet uses an XML file that sets the wireless sensor network parameters. The parameters used in our simulations are flexible as we will make many tests with different values of the parameters.

First of all, we have defined the network topology; nodes are randomly deployed in a square area of $400x400$m. Then, the simulation duration also vary with tests. For the propagation model we have chosen the range model which means that a signal broadcasted by a node wont be abated since it didnt exceed the range value. The range is a ray surrounding the node; so it communicates with nodes being in this disk, these nodes are named neighbours.

Tests are done with different values of the parameters to permit the evaluation of the scheme. First, we use different values of the network size and of the range. Then, we focus on the results concerning the number of constructed keys, the number of a node neighbours and the number of isolated nodes, simulation time, consumed energy and the remaining energy per node.

5 Simulation results

The first test concerns the number of constructed keys in function of the size of the network. These tests were done with different values of the range. Recalling that the range is the ray that surrounds the node and that presents the transmission scope of one node. Nodes existing in this disc can communicate with the previous node and are called neighbours.

When the range is 20m, we can note that the number of shared keys is growing with the size of the network, so it depends on the size of the network. Our tests include also the number of one node neighbours [10] which is increasing when the number of nodes of the network achieves 400. The number of isolated keys will decrease in the same way to achieve 0, which means that the network is completely connected. We can see that the number of the shared keys is twice what should be. In fact, in the optimal case, if n is the number of nodes in the network and d the number of one node mean number of neighbours, the mean number of the shared keys is nxd whereas in our case, the number

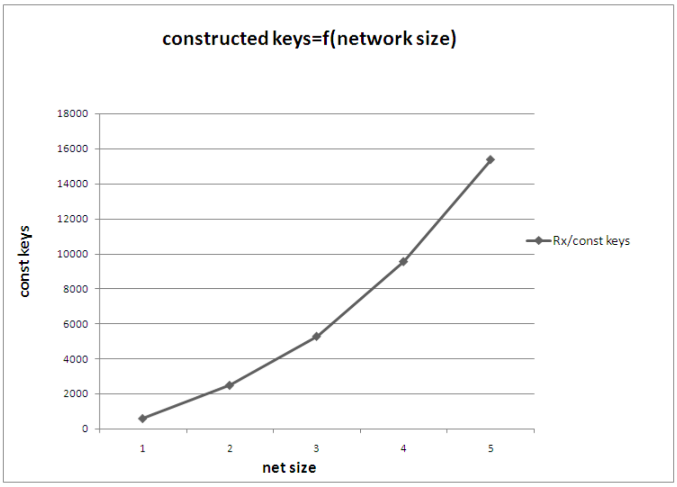

Figure 5.1: Number of constructed keys=f(net size)

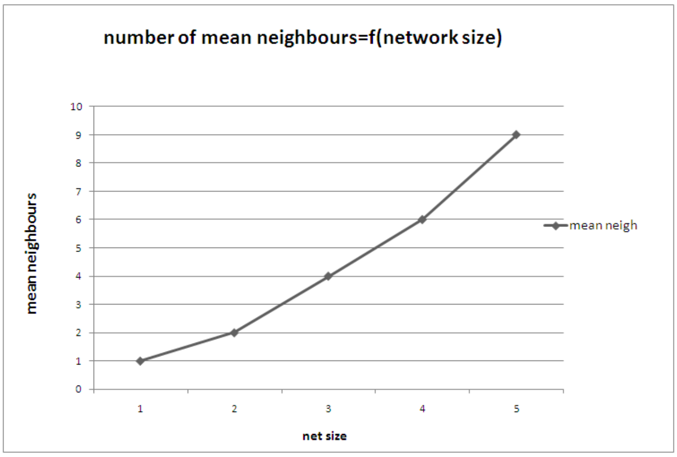

Figure 5.2: Number of mean neighbours =f(net size)

of shared keys is $2nxd + \epsilon$. This fact means that, when Tx is the sent messages and Rx is the received messages, one Rx was sent for every received broadcast. So, the number of created keys is not optimal and corresponds to the creation of all the possible keys in the network. The only solution to decrease this number is to pre-organize the network via an auto- set phase.

In our tests, we have also focused on the attitude of the network with the energy representing a critical point. The consumed energy curve has an increasing shape while the remaining energy curve is decreasing which is totally ordinary, because the activity of the node consumes energy. But, this value doesnt achieve 80 percent of the total energy of

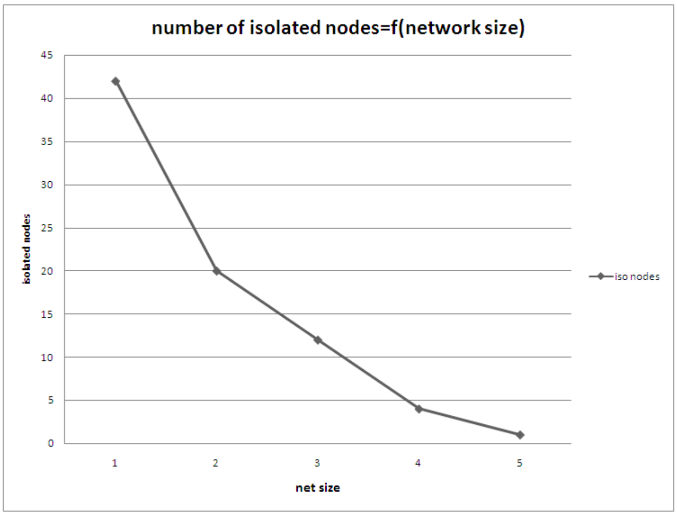

Figure 5.3: Number of isolated nodes =f(net size)

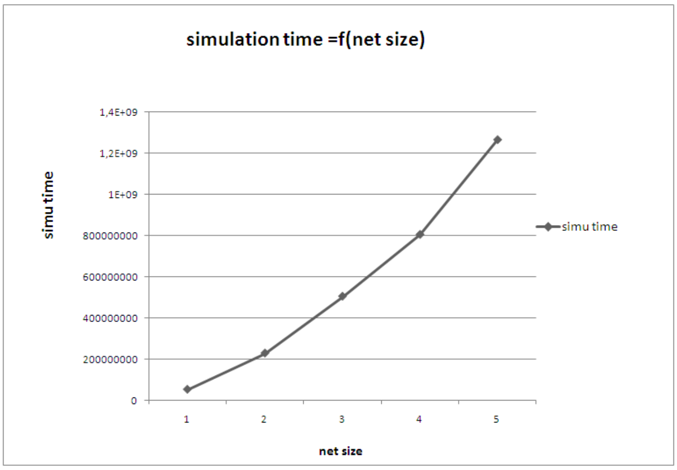

Figure 5.4: Simulation time=f(net size)

the battery. So, we can say that the construction of the shared keys doesnt consume all the energy of the node which permits to lengthen the duration separating two updates of one node. We note also that the simulation time (time to construct a shared key) is growing with the number of the network nodes.

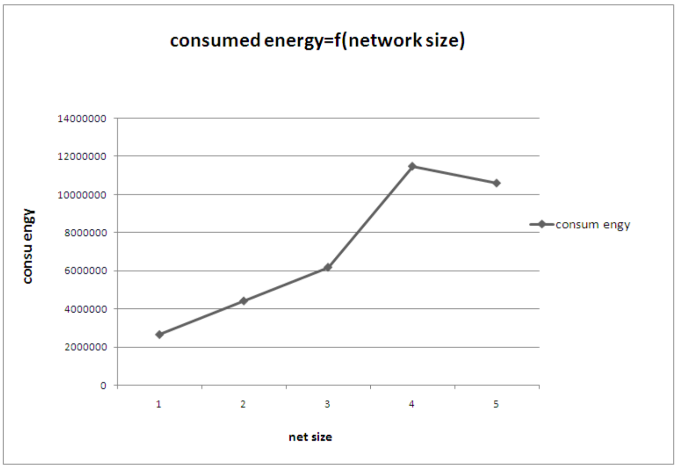

Figure 5.5: Consumed energy=f(net size)

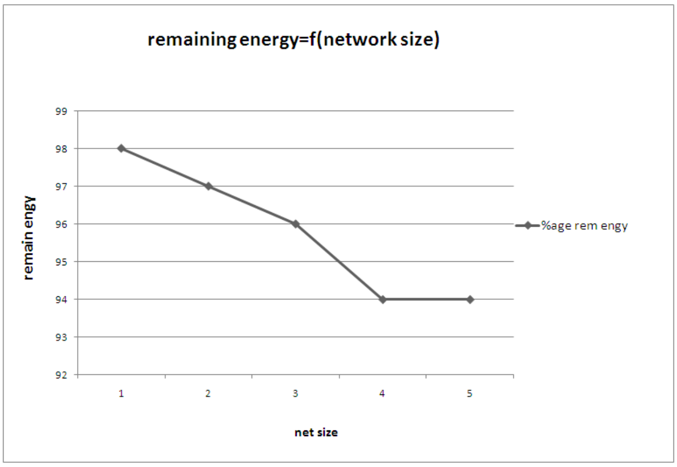

Figure 5.6: Remaining energy=f(net size)

6 Conclusion and future works

We have presented BROSK (BROadcast Session Key), a pre distribution scheme. We simulated it with a wireless sensor network simulator (WSNet) and tested its reactions in different conditions. Results of tests show that one of the characteristics of BROSK is its dependency on the network size and on the range value which represents one node transmission scope. In fact, the number of isolated keys is 10 for a network of 200 nodes and a range of $30m$, it decreases to zero when the network size is 600. We can note also that the mean number of one node neighbours is increasing with the value of the range, one node communicates with 1, 2 or 3 neighbours for a network with a range of 10m. The

number of isolated key varies between 94.5percent and 0.47 percent because actually, by increasing the number of nodes in the same space, the number of isolated keys decreases and one node communicates with more than one neighbour.
We notice also that the energy consumption is widely dependent on the size and the range of the network. The explanation of such results is that one node consumes energy when it communicates also by raising the number of the network nodes, the energy consumption will rise. On the other hand, the energy consumption decreases when the range value is minimal but it doesnt achieve a low value and the battery doesnt exhaust. Then, it respects the sensors constraints (energy, memory size, etc) which increase network life duration. Our perspective for the future works is to integrate in WSNet new performance estimation functionalities so we could evaluate other characteristics of a protocol.

References

[1] A. Fraboulet, G. Chelius, and E. Fleury, Worldsens : development and prototyping tools for application specific wireless sensors networks. In IPSN 07 : *Proceedings of the 6th international conference on Information processing in sensor networks*, New York, NY, USA. ACM, 2007, 176-185.

[2] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler, Spins : security protocols for sensor networks, *Wirel. Netw.* 8(5), 2002, 521-534.

[3] A. Seyit, Camtepe and B. Yener, Key distribution mechanisms for wireless sensor networks : a survey, 2007.

[4] A. Seyit Camtepe and B. Yener, Combinatorial design of key distribution mechanisms for wireless sensor networks. *IEEE/ACM Trans. Netw.*, 15(2), 2007 :346-358.

[5] B. Lai, S. Kim, and I. Verbauwhede, Scalable session key construction protocol for wireless sensor network. In *IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES)*, 2002.

[6] B. Lai, S. Kim, and I. Verbauwhede. Reducing radio energy consumption of key management protocols for wireless sensor networks. In *ISLPED 04 : Proceedings of the 2004 international symposium on Low power electronics and design*, New York, NY, USA. ACM, 2004, 351-356.

[7] B. Levente. and J-P. Hubaux, Security and cooperation in wireless networks Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing. Cambridge University Press, 2007.

[8] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, Perfectly-secure key distribution for dynamic conferences. *Lecture Notes in Computer Science*, 1993,740:471-486.

[9] E. Ben Hamida et G. Chelius. WSNet : Simulation configuration Tutorial, 2007.

[10] E. Ben Hamida, G. Chelius, and E. Fleury, Revisiting neighbour discovery with interferences consideration. In *PE-WASUN 06 : Proceedings of the 3rd ACM international workshop on Performance evaluation of wireless ad hoc, sensor and ubiquitous networks*, New York, NY, USA. ACM, 2006, 74-81.

[11] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *SP 03 : Proceedings of the 2003 IEEE Symposium on Security and Privacy*, 197, Washington, DC, USA,IEEE Computer Society, 2003.

[12] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, Wireless sensor networks : a survey. Comput. Netw. 38(4), 2002,393-422.

[13] Lee, J.C. and Leung, V.C.M. and Wong, K.H. and Jiannong Cao and Chan, H.C.B. Key management issues in wireless sensor networks: current proposals and future developments.*Wireless Communications, IEEE,*, vol 14, n5, 2007, 76.

[14] J.Jeong, and Haas, Z.J. Predeployed secure key distribution mechanisms in sensor networks: current state-of-the-art and a new approach using time information. *Wireless Communications, IEEE*, vol 15, n 4, 2008,41–51.

[15] J . Hwang, and Y. Kim, Revisiting random key pre-distribution schemes for wireless sensor networks. In *SASN 04 : Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks* , New York, NY, USA. ACM, 2004, 43-52.

[16] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *CCS 02 : Proceedings of the 9th ACM conference on Computer and communications security* , New York, NY, USA.ACM, 2002, 41-47.

[17] L. Tobarra, D. Cazorla, and F. Cuartero. Formal analysis of sensor network encryption protocol (snep). *IEEE Internatonal Conference onMobile Adhoc and Sensor Systems, MASS 2007*, 8-11, 2007,1–6.

[18] N. Fournel. Estimation et optimisation de performances temporelles et nergitiques pour la conception de logiciels embarqus. PhD thesis, cole normale suprieure de Lyon, 2007.

[19] N. Fournel, A. Fraboulet, G. Chelius, E. Fleury, A. Allard, and O. Brevet, Worldsens : from lab to sensor network application development and deployment. In *IPSN 07: Proceedings of the 6th international conference on Information processing in sensor networks*, New York, NY, USA. ACM.48, 2007 551-552.

[20] O.G, Morchon, and H. Baldus, and D.S. Sanchez, Resource-efficient security for medical body sensor networks.*International Workshop on Wearable and Implantable Body Sensor Networks*, 2006. BSN 2006. 4th edition, 2006, 83.

[21] R. Blom. An optimal class of symmetric key generation systems. In *Proc. of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques* , New York, NY, USA. Springer-Verlag New York, Inc, 1985, 335-338.

[22] S. Rajasegarar and C. Leckie and M. Palaniswami, Anomaly detection in wireless sensor networks, IEEE, Wireless Communications, vol 15, n 4, 2008, 34–40.

[23] S. Zhu, S. Setia, and S. Jajodia, Leap : efficient security mechanisms for large-scale distributed sensor networks. In *CCS 03 : Proceedings of the 10th ACM conference on Computer and communications security,*New York, NY, USA.ACM, 2003, 62-72.

[24] W. Du, J. Deng, S. Yunghsiang Han, and K. Pramod Varshney. A pairwise key predistribution scheme for wireless sensor networks. In *CCS 03 : Proceedings of the 10th ACM conference on Computer and communications security,* New York, NY, USA. ACM, 2003, 42-51.

[25] W. Znaidi, J-P. Babau and M. Minier, Detecting wormhole attacks in wireless networks using local neighborhood information. *IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008.*Volume , Issue , 15-18 Sept. 2008,1–5.

[26] Y. Xiao, V. Krishna Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, A survey of key management schemes in wireless sensor networks. Comput. Commun., 30(11-12), 2007, 2314-2341.

Abderrazak JEMAI received an Engineer degree from the University of Tunis, Tunisia in 1988 and the DEA and Doctor degrees from the University of Grenoble, France, in 1989 and 1992, respectively, all in computer sciences. From 1989 to 1992 he prepared his thesis on simulation of RISC processors and parallel architectures. Since 1993, his interests are focused on high level synthesis and simulation at behavioral and system levels within AMICAL and COSMOS at TIMA Laboratory in Grenoble. Dr Jemai became an assistant professor at the ENSI university in Tunis in 1993 and a Maitre-Assistant Professor at the INSAT university in Tunis since 1994. He was the principal investigator for the Synthesis and Simulation of VLSI circuits project at the ENSI/Microelectronic group. He was the principal investigator of the simulation module in AMICAL at TIMA in Grenoble. He is also the principal investigator for the Performance evaluation of MPSoC project in LIP2/FST Laboratory in Tunis. Dr Jemai is also working on Security of embedded systems.

Abir Mastouri received a master degreee in computer sciences from Sciences University of Jendouba in Tunisia in 2008. Her interestes are focused on Performance evaluation of MPSoC under the directions of Dr. Abderrazak Jemai.

Dr. Hichem Eleuch received electric and electronic engineering diploma from Technical University of Munich in Germany. He obtained his Ph. D. in Quantum Physics from Kastler Brossel Laboratory at Ecole Normale Suprieure de Paris and Universit Pierre-et-Marie-Curie in France. in France in 1998. Recently, he spent two years in USA as researcher at the Institute for Quantum Science and Engineering Institute for Quantum Studies, Texas A&M University as well as visiting scientist at Princeton University. Now he is a Guest Scientist at Max Planck Institute of Physics for Complex Systems and a professor at National Institute of Applied Science and Technology (University of Carthage, Tunis). Furthermore, he is an associate member at the International Centre of Theoretical Physics in Trieste. His research interest is related to quantum optics, nonlinear optics, stochastic processes and Complex Systems.