Virtual platform for power and security analysis of wireless sensor network

A. Diaz, J. Gonzalez-Bayon, P. González de Aledo Marugán, P. Sanchez
University of Cantabria
{ adiaz, javiergb, pabloga, sanchez }@teisa.unican.es

ABSTRACT

Wireless Sensor Networks (WSNs) include low-power and low-cost devices (nodes) with demanding power requirements (long autonomous lifetime). The nodes have to use the available battery carefully and avoid expensive computations or radio transmissions. Therefore, effective simulation mechanisms that allow the developer to obtain estimations at the early stages of the WSN design, prior to deployment, are necessary. Power consumption is not the only important concern in this design but security is becoming a real problem too, since some WSNs process sensitive data. Thus, it is necessary to ensure that the processed data are tamper-proof. This paper proposes a framework for network simulation and embedded SW performance analysis that focuses not only on time and power estimation but also on two new metrics: the "entropy security-oriented metric" provides information about the security encryption used in WSN transmissions and the "heterogeneity metric" provides information to help avoid "replication attacks". All this information will aid in the whole WSN deployment design, providing useful metrics about power and security.

Keywords: Wireless Sensor Network, power consumption, security analysis

1. INTRODUCTION

The complexity of Wireless Sensor Networks (WSNs) is growing with the need for these devices to perform more complex operations over long periods of time. One of the biggest problems of this requirement is the battery of the nodes as its performance is limited. Another important requirement nowadays [1-2] is to guarantee appropriate security levels in its usual working, especially transmissions. Therefore, it is also critical to decide which encryption method should be used. This is not only because confidentiality and authentication must be performed when sending or receiving sensitive data but also because it is critical that the consumption should not increase significantly compared to a typical non-secure use.

In this scenario, due to the high impact of the information contained and managed or the importance of the monitored zones, it is necessary to guarantee the integrity of the data exchanged/processed and to react effectively against attacks. One of the biggest problems of these types of networks is their vulnerability to being attacked in a huge number of different ways. These networks are often deployed in an insecure environment. For this reason, it is of great importance, in the design phase, of taking into consideration the weaknesses of the sensor network.

Thus, it is desirable to use a software virtual simulator to simulate and estimate the security against these attacks. The technique used in this paper extends the performance analysis tool explained in [4]. This work focuses on proposing novel metrics in a software virtual simulator that facilitates the decision about which encryption should be used in each network and how to avoid replication attacks. This is particularly relevant because a good tradeoff between security and power consumption implies an important effort for the sensor network designer.

In order to be competitive, it is essential to shorten development time. To reduce this time-to-market and to increase the efficiency of the devices, it is necessary to perform fast accurate simulation of the WSN and its nodes. Doing simulations in the early stages of development helps to detect potential problems in the nodes and the network. It allows the number of complications in future stages of development to be reduced. An early detection of potential problems reduces the time and cost of the development. Fast and accurate simulation can provide information to the developer that enables the modification of the algorithms or the architecture of the network in order to avoid or minimize attack effects. As is explained later, the estimation of the system consumption is very important in this kind of system. One of the critical constraints in the WSN is its battery life. In this type of network, the death of a node may cause the isolation of a part of the network.

Current WSN simulator tools do not offer the possibility to estimate impact due to the cryptographic functions used. References [4] [5] and [6] reflect the state of the art of WSN simulation frameworks. NS-2 [7] and OMNET++ [8] are discrete event network simulators. GloMoSim [9] is a simulation environment for wireless and wired network systems. Another framework, TOSSIM [10], is a bit-level discrete event simulator and emulator of TinyOS [11]. Avrora [12] provides a clock-cycle accurate execution of programs that are executed in the WSN node. As far as we know, there is no previous work that provides real-time Operating System support or power and execution time estimation for WSNs. Power consumption estimation is one of the critical aspects of WSNs.

Some research works have analyzed the impact of encryption methods for WSN. In [13], the authors perform a wide-ranging analysis on the cost of using symmetric and asymmetric cryptographic algorithms and hash chain functions but the work is focused on handheld devices. In [14] there is a comparison between different symmetric cryptographic algorithms. In [15], a novel key management scheme is presented. It is oriented to wireless sensor network security and it is based on a public key method. The paper in [15] focuses on a methodology to create and share the keys for encryption but there is a lack of practical results confirming the suitability of the proposed scheme. In [16], authors provide results of experiments with AES and RC4, two symmetric key algorithms that are commonly suggested or used in WLANs. However, nowadays the use of RC4 is not so extended as triple DES thus the comparison is not complete. In [17], a survey of security issues in WSNs is presented. First, the constraints, security requirements and typical attacks with their corresponding countermeasures in WSNs are outlined. Then, a holistic view of security issues is presented. One of the conclusions from this paper is that symmetric key cryptography is superior to public key cryptography in terms of speed and energy. However, the key distribution schemes based on symmetric key cryptography are not perfect. Efficient and flexible key distribution schemes need to be designed. In [18], comprehensive cryptography algorithms suitable for WSN are evaluated. This survey only includes symmetric algorithms such as RC4, AES, in a similar way to previous papers. It proposes taking into account the factors that may affect algorithm choice, such as clock cycles, code size, SRAM usage, and energy consumption, but results are only focused on a few of them.

This paper is organized as follows. In Section 2, the virtual simulator used to measure security is presented. The proposed security metrics are described in Section 3. The results are presented in Section 4. Finally, the conclusions are drawn in Section 5.

2. VIRTUAL SIMULATOR

A WSN node is typically based on a System-On-Chip (SoC). Most of the WSN nodes are composed of typical components, such as processors, memories or caches, plus two important hardware components, the transceiver and the sensor.

2.1 HW/SW Co-Simulation

The co-Simulation methodology used in this paper is based on the native simulation approach explained in [3]. This approach consists in the execution of annotated software code in an environment that models the platform hardware details. The original environment supports the execution of the software application over the hardware model.

2.2 Wireless Network Simulator

The virtual simulator framework has some important features that enable an accurate simulation and estimation of security. The first feature is power consumption estimation, which is one of the most critical constraints in these kinds of networks. Another important feature of the simulator is that it executes the same software code that will be executed in WSN networks. This is important because most of the previous simulator frameworks obtain their network traffic from external functions, not from real traffic. Without real traffic information, it is not possible to perform accurate simulation of the firmware of the nodes or security.

The proposed framework supports classical WSN RTOS such as FreeRTOS [19]. Moreover, it enables a node-level simulation. Due to this, we obtain independent results for nodes. It enables conflicting nodes to be identified along with strategies that will help to improve network and node performance. Another important advantage of the simulator is that it enables heterogeneous networks to be estimated, with different hardware and software for each node.

2.3 Wireless Network Model

Figure 1 represents an example of node architecture and how the network model is included in the schema. This network model will be explained below.

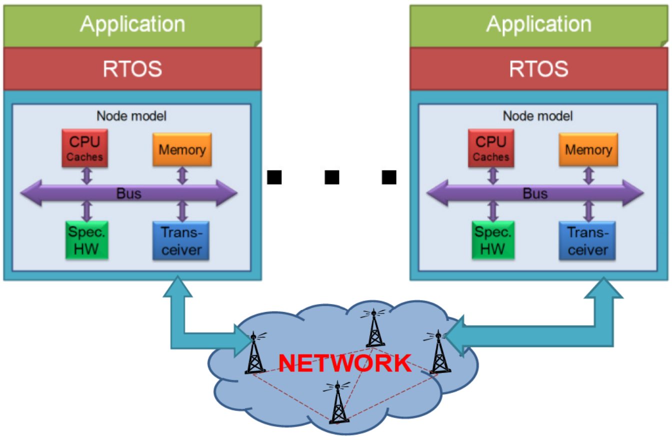


Figure. 1. Simulation of a Wireless Network

In a wireless network, the physical channel between two nodes is a shared channel, with noise and interference, in which it must be taken into account that the range of the node is limited. As a consequence, developers need to determine the visibility and the probability of a successful reception of a packet sent between nodes. For this, and with the goal of performing accurate simulation, the developer must study the WSN deployment zone and define a matrix with the probability of packet loss among all nodes. This probability must include the probability of loss due to noise. This probability data may be calculated by electromagnetic propagation simulation, for example the computer tool Cindoor [20]. Cindoor is an engineering tool for the effective implementation of wireless systems. With these probabilities, the simulator can find out the effectiveness of the links between nodes. If the developer defines a link as 100, it means that the sending node range is not enough to reach the destination directly. Meanwhile, if the developer defines the link as 0, all the packets transmitted through that link reached its destination. In contrast, if the link is defined by any other number between 0 and 100, this number indicates the probability of the packet reaching its destination. For example, in Figure 2, the link between node 0 and node 1 is defined as 3%; it indicates that for every 100 packets sent through that link only 97 packets reach their destination. In the case of the link between node 4 and node 3, the network discards 12 packets of every 100. These probabilities can be seen in Figure 2 represented as “Node Link” (Radio link between node 1 and node 4).

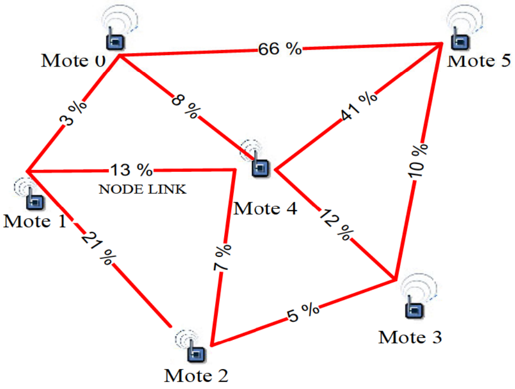


Figure. 2. Wireless Network Model

3. SECURITY METRICS

The security metrics proposed are integrated in the WSN simulator. In this work, we propose two levels of entropy measurements. In the first level, the encryption security is measured and compared with the increase in consumption of the whole network. This provides important information about the confidentially of the packets sent over the network and the power consumption increase related to the encryption method used.

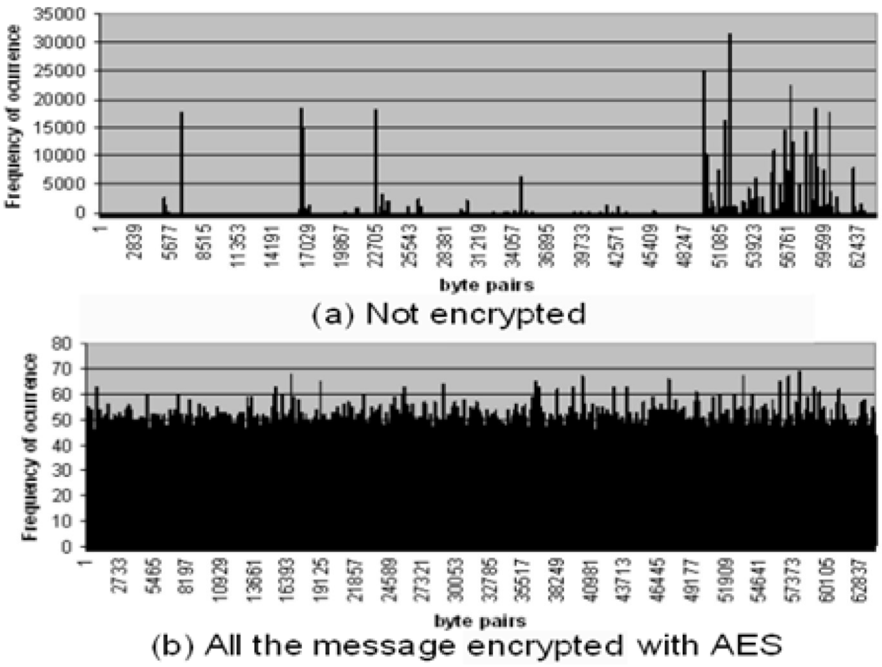
The second level measures the heterogeneity of the messages sent over the network. This is important because some attacks use replication techniques, so they are more dangerous if the same packets are sent repeatedly. Thus this second level of measurement provides information about how secure the network is against these attacks.

3.1 Evaluation of WSN encryption methods

One of the aims of this work is to propose a new measurement provided by the virtual simulator that helps to identify what security is obtained with a encryption method. This facilitates not only the comparison of existing encryption schemes but also the evaluation of new proposals. This is really important for low-power devices such as WSNs in which it is necessary to save power without losing efficiency. For these systems, security is an open research area and, depending on the deployment scenario or sensor purposes, it can have different focuses: security or low consumption. Therefore, it is very important to show the security level achieved with a single number.

To demonstrate the new metric, a simple example with state-of-the-art encryptions is proposed. This work focuses on AES or TDEs symmetric encryption because of its relatively low power consumption compared to asymmetric encryption algorithms.

The goal is to measure the "entropy" obtained with different encryptions, thus providing an idea of which one is more secure. An encryption of a file containing a text from a book is used, which has 256 different possible characters (bytes). A way of observing the entropy obtained with the message encrypted is to observe how the distribution of the characters is encrypted. Figure 3 shows the pair-byte frequency distribution from the example file. It shows the percentage of all the possible 65536 pair-bytes (256x256). It is also possible to show the percentage of single-bytes or trio-bytes but, from previous experiments performed in this work, it was observed that pair-bytes was the best choice for performing a simulation with good tradeoff between accuracy and time consumption.



(a) Not encrypted

(b) All the message encrypted with AES

Figure. 3: "Entropy" for a non-encrypted and an encrypted message

As is observed in Figure 3a, when there is no encryption some pairs-bytes are more frequent than others. Thus, an easy deduction of the pair-bytes can be obtained even if the text is randomized. On the contrary, when an encryption procedure such as AES is used, this frequency is highly similar between the pairs as is shown in Figure 3b.

However, the results shown in Figure 3 are not practical for measuring the level of security obtained for a specific cryptography scheme. Thus, in this work the use of the standard deviation of the metrics shown in Figure 3 is proposed for use as the “entropy measure”. Figure 4 shows this measure for the main symmetric encryptions. The term AES-“KeySize” is related to the size of the key used. As can be observed, the “entropy measure” matches the level of security of the different cryptography schemes. AES-256 is the most secure scheme and it obtains the lowest value of “entropy measure”. It is also known that TDES obtains worse security performance than any AES and this is also shown with the proposed metric since the “entropy measure” is higher than any AES. Finally, if there is no encryption the “entropy measure” is clearly higher than with any encryption method.

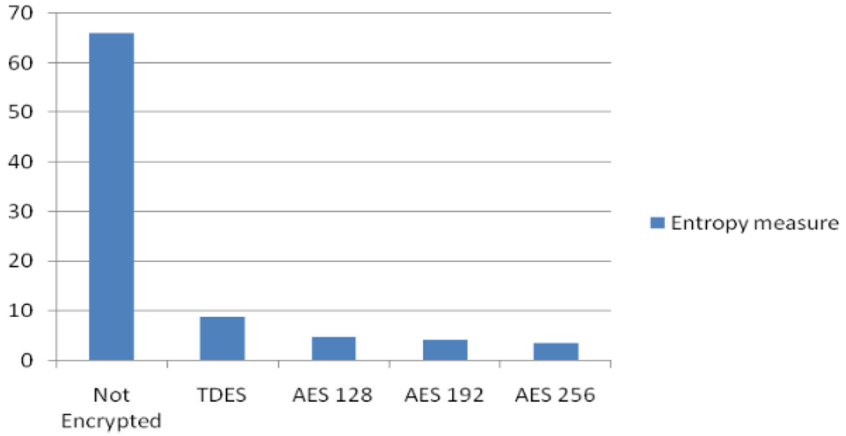


Figure 4: “Entropy measure” for the main symmetric encryptions

3.2 Evaluation of WSN Heterogeneity

The packets transmitted through the network nodes can be captured by an attacking device. A cryptographic algorithm must be strong, but if the packets transmitted by a node are always the same, a replication attack is easy to perform. A strong encryption ensures the protection of the data, but if a node sends the same messages repeatedly, the network is vulnerable. This is why the entropy related to the content of the packets must be measured to provide an idea of the heterogeneity of the message network.

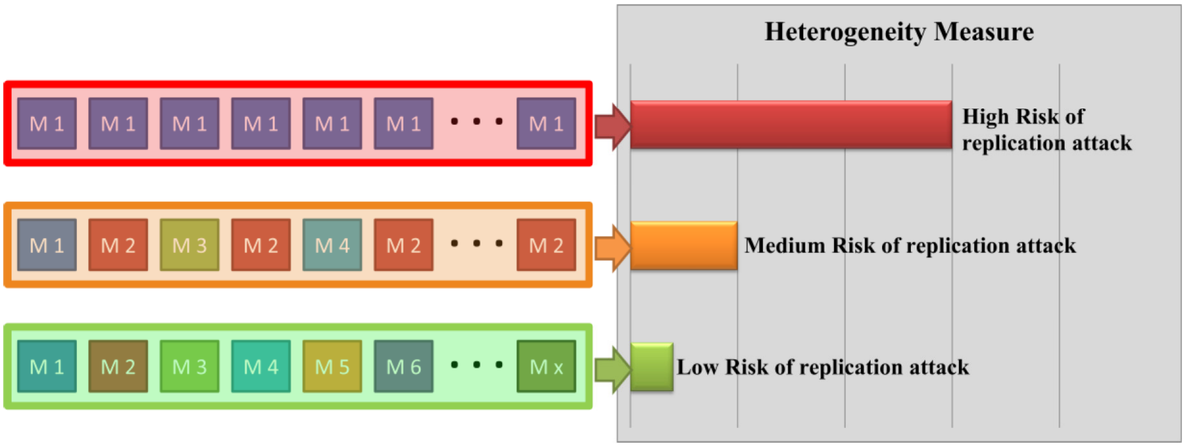


Figure 5 Heterogeneity measure

As can be observed in Figure 5, the transmission of repeated messages (M1, M1, …M1) reduces the security against some attacks. Even if the packets are transmitted with an unbreakable encryption and the attacker cannot read the information contained, the attacker can use a copy of the packet to send it to a node and impersonate another node. Because of this, it is important to develop applications that send heterogeneous packets to avoid these attacks. Figure 5 shows how the heterogeneity in the transmission packets reduces the risk of replication attacks due to the increased difficulty for the attacker to find a pattern in the messages.

4. **RESULTS**

The "entropy measure" proposed in section 3.1 was validated with results from state-of-the-art symmetric cryptography methods. Several encryption proposals for low consumption are explored. They are TDES, AES-128, AES-192 and AES-256. In addition the increased cost that each of these encryption techniques introduces per node is shown.

The "entropy measure" and the power consumption are both measured by the virtual simulator. These results are shown in Figure 6. As can be seen in Figure 6, the least secure encryption is TDES. Furthermore, its consumption is the highest so its use in a WSN is not recommended. Therefore, AES appears to be a most realistic option. Among the different key sizes, AES-256 is the most secure but it is also the one that consumes most. AES-128 is the most suitable regarding the battery life problem since its consumption is the lowest. The measurements provided by the virtual tools allow the designer to identify and evaluate numerically this consumption/security tradeoff.

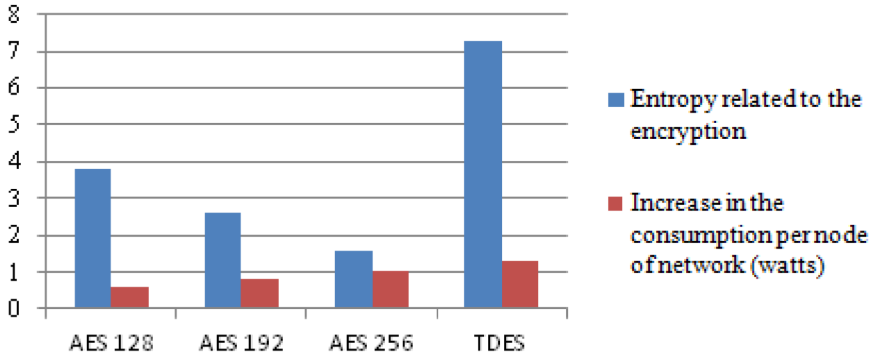


Figure. 6: Entropy measure for different encryption choices

In addition, the virtual simulator was used to measure the WSN heterogeneity described in section 3.2. Three different cases were simulated. In case 1 all the nodes send the same packet, in case 2, several packets are sent in a repeated pattern, and in case 3 all the packets are different. The idea is to show how this heterogeneity measure varies in different WSN scenarios. The measures for these cases are shown in Figure 7. As can be observed the most secure WSN is in Case 3, since the "heterogeneity measure" is the lowest of all the three cases.

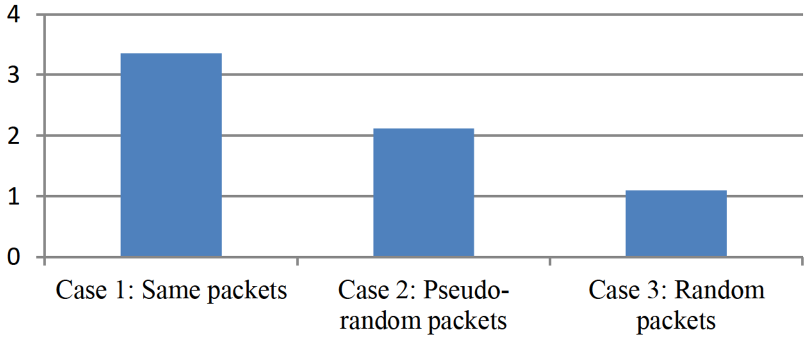


Figure 7: Heterogeneity measure for different transmission cases

5. CONCLUSIONS

This paper presents two new security-oriented metrics for Wireless Sensor Networks. An “entropy measure” is proposed in this work that provides a mathematical value for the security achieved by any encryption scheme. The other metric is based on the heterogeneity of the packets transmitted over the network. These measures are implemented in a WSN virtual simulator. With this virtual simulator, it is possible to obtain realistic power consumption measures for Wireless Sensor Networks. This enables the designer to establish which level of power consumption relates to a specific encryption technique.

The developers can take accurate decisions with the estimations obtained from simulations in order to optimize the application software and the network deployment at early design stages. Through these estimations, the developer may provide greater security to WSN and, furthermore, may shorten the time-to-market. In addition, because of these metrics, the nodes can avoid expensive encryption computations and risky radio transmissions.

ACKNOWLEDGMENTS

This work was funded by the Spanish MICINN through the EUI2010-04255 and TEC2011-28666-C04-02 projects.

REFERENCES

[1] Al-Jarrah, O., Saifan, R., “A novel algorithm for defending path-based denial of service attacks in sensor networks”, International Journal of Distributed Sensor Networks, 2010.

[2] Portilla, J.a , Otero, A.a , De La Torre, E.a , Riesgo, T.a , Stecklina, O.b , Peter, S.b , Langendörfer , “Adaptable security in wireless sensor networks by using reconfigurable ECC hardware coprocessors”, International Journal of Distributed Sensor Networks, 2010.

[3] Posadas, H., Castillo, J., Quijano, D., Fernandez, V., Villar, E., & Martinez, M. (2010). SystemC Platform Modeling for Behavioral Simulation and Performance Estimation of Embedded Systems. In L. Gomes, & J. Fernandes (Eds.), Behavioral Modeling for Embedded Systems and Technologies: Applications for Design and Implementation (pp. 219-243). Hershey, PA: Information Science Reference. doi:10.4018/978-1-60566-750-8.ch009

[4] M. Mekni, B. Moulin, "A survey on sensor webs simulation tools", Proceedings of the 2008 Second International Conference on Sensor Technologies and Applications, 2008, pp. 574-579.

[5] Calibrating and Comparing Simulators for Wireless Sensor Networks. : Andriy Stetsko, Martin Stehlík, and Vashek Matyas. In: MASSIEEE (2011), p. 733-738.

[6] D. Curren, “A survey of simulation in sensor networks”, University of Binghamton project report for subject CS580.

[7] NS-2, “The Network Simulator”, 2007

[8] OMNeT+-, "www.omnetpp.org" 2012

[9] X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: a library for parallel simulation of large-scale wireless networks," presented at Twelfth Workshop on Parallel and Distributed Simulation, 1998.

[10] Levis P., Lee N., "TOSSIM: A Simulator for TinyOS Networks", pal@cs.berkeley.edu, September 17, 2003

[11] http://www.tinyos.net 2012

[12] Titzer, B. L., Palsberg, J., and Lee, D. K. Avrora: Scalable sensor network simulation with precise timing. In Fourth International Conference on Information Processing in Sensor Networks (2005).

[13] Helena Rifa-Pous and Jordi Herrera-Joancomartí, “Computational and Energy Costs of Cryptographic Algorithms on Handheld Devices”, Journal Future Internet, 2011

[14] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, “New Comparative Study Between DES, 3DES and AES within Nine Factors”, Journal of Computing, 2010

[15] Eldefrawy, M.H.; Khan, M.K.; Alghathbar, K. , “A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography”, International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID), 2010.

[16] Prasithsangaree, P.; Krishnamurthy, P. , “Analysis of Energy consumption of RC4 and AES algorithms in wireless LANs”, IEEE Global Telecommunications Conference 2003

[17] Yong Wang; Attebury, G.; Ramamurthy, B., “A survey of security issues in wireless sensor networks”, IEEE Communications Surveys & Tutorials, 2006.

[18] Wei Liu; Rong Luo; Huazhong Yang, “Cryptography overhead evaluation and analysis for wireless sensor networks”, International Conference on Communications and Mobile Computing, 2009.

[19] http://www.freertos.org 2012

[20] Torres, R.P., Valle, L., Domingo, M., Loredo, S., Diez, M.C. "CINDOOR: An engineering tool for planning and design of wireless systems in enclosed spaces" (1999) IEEE Antennas and Propagation Magazine, 41 (4), pp. 11-21