Lightweight Trusted Authentication Protocol for Wireless Sensor Network (WSN)

YUSNANI MOHD YUSSOFF, NAZHATUL HAFIZAH KAMARUDIN, HABIBAH HASHIM
Faculty of Electrical Engineering, Universiti Teknologi MARA (UiTM)
40450 Shah Alam, Selangor Darul Ehsan, Malaysia
yusna233@salam.uitm.edu.my, azzfie@gmail.com, habib350@salam.uitm.edu.my

Abstract— Wireless Sensor Network is a network consisting of tiny and limited power sensor nodes communicate wirelessly and being deployed at any random places. The unique feature of Wireless Sensor Networks that enable continuous data collection and monitoring has accelerate the development of sensor network related applications ranging from non-sensitive to highly sensitive data applications. However, due to its ability to work without human intervention, the sensor nodes are susceptible to clone nodes types of attacks. These will then leads to worst consequences which is false message. Therefore secure communication is no more enough in Wireless Sensor Network Environment. This paper present a rigorous research work in the development of a lightweight trusted authentication protocol for wireless embedded devices in the Wireless Sensor Networks environment. The term trust in this research work is based on trusted Computing Group definition and therefore the development start from the sensor node. Following that, a remote attestation protocol name as IBE_Trust is presented and analyzed. Acknowledging the energy constraint faced by the target devices, analysis on the power consumption is conducted to ensure its feasibility. Finally, this paper suggests the application in e-health mobile device authentication for wireless sensor network. By integrating the trusted authentication protocol in mobile health monitoring system, it will propose a great assistance in patient-doctor interaction since it is required to protect the security of the data network.

Key-Words: - Trust; Performance; Cryptography; Transmission; IBE; WSN

1 Introduction

Securing the network of wireless sensors is no more a secondary issues. The security aspects such as data confidentiality, node authenticity and integrity should be considered at the very beginning of the designing stage. Several papers have discussed on the important of securing the sensor networks by discussing the vulnerabilities and attack on WSNs [2][3]. However, with the nature of wireless sensor nodes that are mostly left unattended for a period of time, confirming valid sensor nodes or trusted node in the network is another important issue to be considered.

According to Trusted Computing Group (TCG) [1], attestation is the core function of trusted computing platforms. It is a method whereby attester authenticates the properties of a target by providing evidence of the integrity of its hardware or software or both over the network. Integrity Measurement Architecture (IMA) and remote attestation protocol are two major components of the architecture of remote attestation. The former is used to guarantee integrity, to ensure the system was not tampered with since it was last turned off and also to confirm the execution of programs will not be tampered with. While the latter, is to ascertain the identity of a remote party or program.

However, in merging attestation into WSNs related applications to form a trusted platform of WSNs, energy and computation capability are issues that need to be considered due to the constrained in power[4] of the sensor node. To solve this problem without compromising the security, IBE-Trust [5] is proposed and the performance of cryptography processes and communication are measured and analyze.

IBE [6] was designed by Shamir to overcome some of the problems in conventional Public Key Infrastructure (PKI). It removes the need for third party certificate issuance to obtain recipient's public key by only using recipient's unique identity (ID) (e.g. an email address) to generate private key and encrypt message for the given entities [7]. Only legitimate entities can then decode the message. Furthermore, the use of Elliptic Curve Cryptography algorithm in IBE gives extra advantage in reducing the computational cost which is due to shorter ECC key size as compared to RSA [8][9][10]. It is also can be considered as efficient authentication protocol as discussed by Moises Salinas in his paper [11].

IBE_Trust is basically a modified version of IBE protocol that is used by base station and sensor nodes in the attestation process. A node is considered as trusted when it successfully boot-up and pass the authentication process with the base station. In order to use the word Trust, the development of the protocol has comply with the TCG specifications of the trusted platform. Referring to Fig. 1, the process started with the boot-up of the sensor node followed by the IBE_Trust protocol. A secure boot process design in the trusted platform will measure the integrity of the software images in the sensor node and if pass, will generate a unique management value for the sensor node to authenticate with the base station using IBE_Trust protocol. This process will help the devices to detect malicious codes installed in it. By using a formal analysis software, AVISPA [11], IBE_Trust was proven to be secured from attacks such as node impersonation.

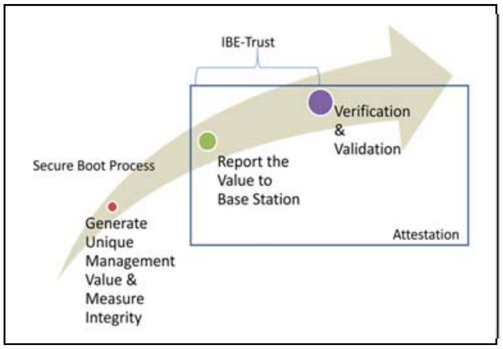
IBE-Trust
Verification & Validation
Report the Value to Base Station
Secure Boot Process
Generate Unique Management Value & Measure Integrity
Attestation

Figure 1. Process flow of trusted sensor node.

This paper presents the implementation of IBE_Trust protocol on real world implementation and analyzes its performance comprehensively. The layout of this paper is outlined as follow: Section II presents the related works to this paper which are secure boot process and IBE-Trust, the following Section III explains the methodology and presents the overall experimental test bed set up for the protocol, Section IV presents the performance results and analysis, finally in Section V and VI state the conclusion and future work that can be expand from this research.

2 Trusted Sensor Node

As presented in Fig. 1, the development of a Trusted Sensor Node comprises of two main stages which are the trusted platform and the authentication protocol.

2.1 Trusted Platform

The underlying principle of a trusted computing system is the assurance that it boots and executes the only authenticated or genuine code. Thus, secure boot process is a must in accomplishing a trusted system environment. By sealing a chain of trust, each component of hardware and software is validated from the lowest layer to the upper layer. The detail of the secure boot process is discussed in Adnan et. al. [12] paper where ARM11 32 bit processor with on-SoC memory and TrustZone is used in the development. The chain of trust begins from Level 0 (*L_0*) at 1st boot loader until Level 2 (*L_2*) at operating system (OS) layer. Fig. 2 illustrated the flow of secure boot process.

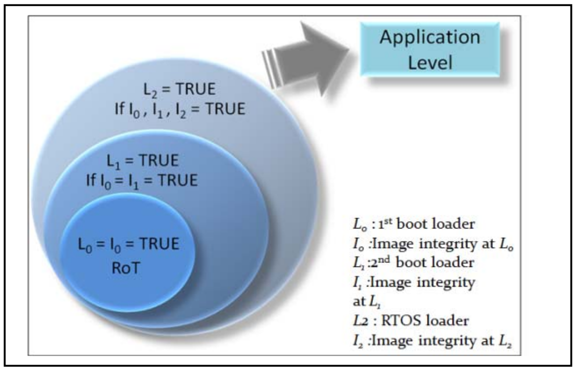

Figure 2. Secure boot process.

The outcome from the secure boot process is a unique value identifying the node which is later used as node's identity. This value is almost impossible to be regenerated by any other nodes and therefore has significantly reduced the possibility of having a masquerade node in the network and subsequently prevents the development of exactly the same sensor node in the node cloning attack. The idea of integrating certain component's serial number in the generation of node's identity comes from the biometric concepts where the uniqueness of human comes from its physical features.

2.2 Authentication Protocol - IBE-Trust

IBE-Trust is an identity-based attestation protocol that confirms data confidentiality, integrity and authenticity. The protocol will verify that a sender is a trusted node and behave in the expected manner in the network. This protocol comprises of two compulsory stages which are pre-deployment and deployment.

Pre-deployment Stage:

Pre-deployment is conducted off-line with the intention to prepare sensor nodes with enough information for secure and trusted communication upon joining the network. It's basically consisting of secure boot process that generates node's identity and trust value and identity base process that generate global system parameters and public key. This information is stored in every sensor node prior to joining the network.

Deployment Stage:

In the deployment stage, the sensor node will again reboot to generate its trust value as well as generating nonce. The trust value and the nonce are *encrypted* with base station public key to prevent the information being exposed. Next, sensor node sends the encrypted value with its ID to the base station for attestation process. Upon receiving the message from the sensor node, the base station will firstly verify the sensor node unique identity with the trust list given at the pre-deployment stage. Packet will immediately be discarded for invalid or unknown identity.

For valid identity, the base station then, *decrypt*s the cipher text, and verifies the received trust value with the one existed in the trust list. Again, if the trust value is not valid, the packet will be discarded.

Finally, the base station responds to the sensor node to inform that authentication is successfully completed by generating a new nonce based on the nonce that it received earlier from sensor node. Once the new sensor node passes the attestation, the base station sends the sensor node identity to member in the group. The members in the group do not need to re-authenticate or attest this newly joining node as it's has been done by base station.

Due to availability of trust list in each sensor, subsequent communications between sensors are very much simplified. Receiving sensor node will authenticate the sender based on the sender ID and upon success, the receiver will locally generate session key using pre-installed key derivation function (KDF) and random nonce value, and this is sent together with the authentication message. To utilized common parameters installed in the sensor node at pre-deployment stage, the Authenticate Key Exchange (AKE) protocol is proposed to be used in subsequent communications between sensor nodes in the network. The generation of the session key between Node A and B that utilized symmetric bilinear pairings is explained in the following paragraph. The steps involved are:

Node A:Picks random number $r \in Z_q$, computes

$$R= rQ_A \tag{1}$$

where Q_A is public key of node A. Z is set of natural numbers while q denotes prime order. Therefore $Z_q = \{0,1,\ldots\ldots q-1\}$. Node A will then send R value sized 64 bytes to node B over public channel. Following that, Node A then computes the shared secret as:

$$K_{AB} = e((r+h)S_A,Q_B) \tag{2}$$

Where e is bilinear map, S_A is the private key of node A that is securely kept in the On-SoC ROM, Q_B is public key of Node B and finally h that is computes by both parties is define in eq. (3). H_1 and H_2 are hash algorithms installed in the sensor node in the pre-deployment stage.

$$h = H_2(R, ID_A||ID_B) \tag{3}$$

Node B then, computes shared secret as:

$$K_{BA} = e(R + hQ_A, S_B) \tag{4}$$

Finally the session key computed by A is $\kappa(K_{AB})$ and by B as $\kappa(K_{BA})$ where κ is key derivation function. The idea towards this implementation is adopted from ID-based one-pass AKE technique [14] and the only difference is in the authentication value where, in [14] authentication is performed using sender public key while here it is performed using sender ID. Other issues regarding key distribution techniques and optimize routing protocol in WSN are discussed by Wangke Yu and Jasmine Norman in [15] and [16] respectively.

Finally, total transmission data sizes from sensor node to base station, during online stage are 280 bytes of payload. The 280 bytes of payload consisted of 3 bytes of sensor node's ID, 259 bytes of key file and 18 bytes of chipertext. While total transmission data size from base station to sensor node are 2 bytes payload of nonce.

3 Experiment & Test Bed Result

Following section briefly discuss on the test bed set up in the laboratory. The test bed was set up to enable real-time analysis on the IBE_Trust protocol.

3.1 Test Bed Set-up

Each two XBee 802.15.4 transceiver is connecting with two HP workstations acting as a sensor node and a base station. Serial port programming written in C++ language is used to write and read message from XBee. *IBE_Trust* program is executed in base station to generate global parameters, master key and private key.

The clock function determines the processing time in *CLOCKS_PER_SEC*. It is then used to measure the energy for each process. Eq. *5* shows the relationship between volt (*V*), current (*I*), time (*t*) and energy (*E*). Volt (*V*) and current (*I*) can be found at XBee Series I specification. Table I shows the specifications of XBee transceiver 802.15.4 [15].

$$E=V*I*t \quad (5)$$

TABLE 1: SPECIFICATION OF ZIGBEE TRANSCEIVER

RF Data Rate	250 Kbps
Interface Data Rate	Up to 115.2 Kbps
Transmit Current	35 mA @ 3.3VDC
Receive Current	50 mA @ 3.3VDC

3.2 Energy Analysis on Encryption and Decryption Process

Figure 3 presents the details on the encryption and decryption process. With the data size more than 41% compared to encryption, decryption process as predicted consume higher energy compared to encryption. However, the energy is 68% higher than encryption process and 27% more than the percentage of data. This shows that, decryption process utilizes more energy as compared to encryption process. However, in this implementation, it (decryption process) does not affect sensor node's life time as it is performed by base station that is assume to have better processing capability with no constraint in power.

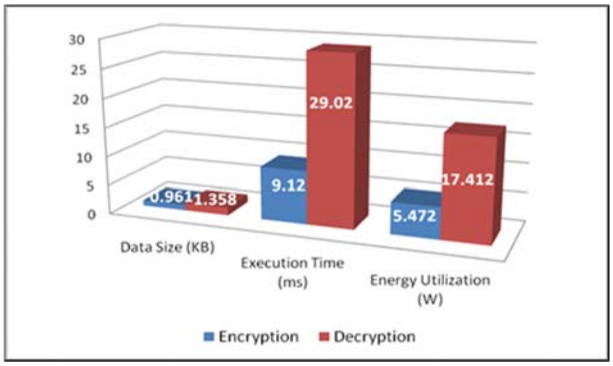

Figure 3. Data Size (KB), Execution Time (ms) and Energy Utilization (W) during Encryption and Decryption of IBE-Trust.

3.3 Energy Energy analysis during communication

As mentioned earlier in Section II B, the sensor node transmits 280 bytes of payload to base station, while, the base station transmits 2 bytes of payload to the sensor node. For X-Bee Series 1 with 64-bit addressing [19], node is capable to send up to 100 bytes of payload and 25 bytes of header. Hence, the total size of data transmission from sensor to base station is 355 bytes, and 27 bytes from base station to sensor node.

XBee transceiver takes around 0.1985 seconds to transmit 355 bytes of data from sensor node to base station or 8.072μWs for a bit. However, it takes around 6.5 times longer to receive the same amount of data which is close to 58.616μWs per bit. Figure 4 presents the energy distribution for communication between sensor node and base station during the on-line stage of IBE_Trust protocol. It is clear that total energy used by sensor node is 27% lower as compared to the total energy used at the base station. This indirectly shows the practicality of IBE_Trust protocol for sensor node.

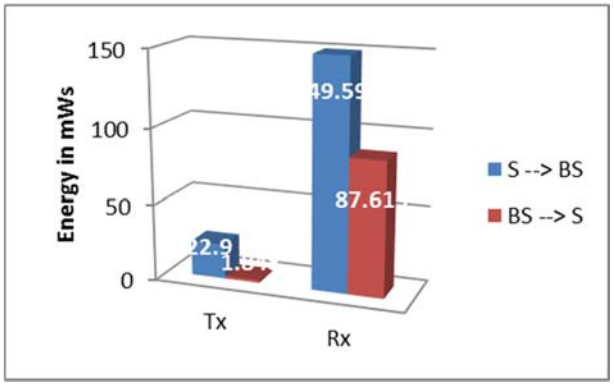

Figure 4. Energy distribution for communication between sensor node and base station.

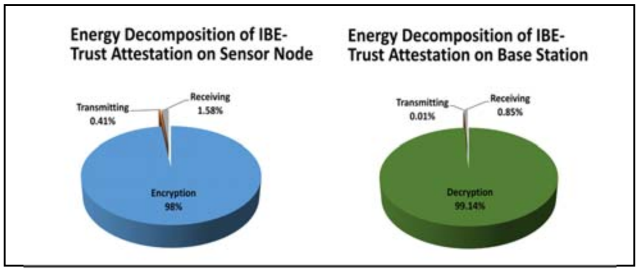

Figure 5. Decomposition of energy for IBE_Trust protocol

Further, Figure 5 shows the decomposition of energy for IBE_Trust protocol, where cryptography processes which are encryption and decryption utilize most of the energy. Therefore, the design of IBE_Trust protocol tries to minimize the cryptography process at the sensor node especially. Few other papers [8][20][21] that discussed on performance of wireless sensor nodes also showed that public key cryptosystem overshadows other processes in term of energy consumption.

4 Performance Analysis

This section discuss the performance of IBE_Trust protocol by means of comparison with other closely related work. The analysis however focuses only on energy consumption during transmitting and receiving.

In [8] , the authors stated that RSA-1024 requires a client to transmit 490 bytes of payload and a server to transmit 314 bytes of payload. Considering XBee 802.15.4 specifications [22] that allows up to 100 bytes payload at one time, RSA-1024 requires 5 packets of data client to server and 4 packets from server to client. Total number of packet that is required for RSA authentication is 9. ECC-160, client and server transmit 138 bytes of payload each, which add up to 4 packets of data. Finally, IBE-Trust attestation needs 3 packets from node to base station and 1 packet in the opposite way.

Figure 6 shows the comparison between RSA, ECC and IBE_Trust protocol concentrating on the number of packets (converted into energy) involve in the communication. It shows that the performance of IBE_Trust in term of total energy consumption during the communication is almost comparable with ECC protocol. RSA protocol as predicted consumed the highest energy due to the large key size. ECC on the other hand, utilize lowest energy during the transmission because this protocol does not require pairing algorithm, whereas IBE_Trust needs Tate pairing to successfully compute. However, at receiving, IBE_Trust used lowest power as sensor node only needs to receive 2 bytes of packet consisting nonce value from base station. ECC on the other hand requires 138 bytes of data for SSL handshake.

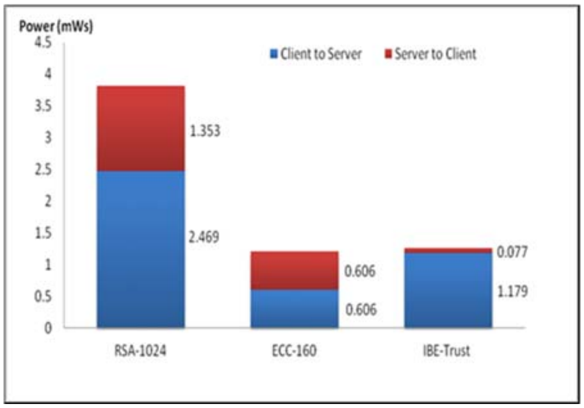

Figure 6. Comparison between RSA, ECC and IBE_Trust protocol

5 Proposed Application

Based on the promising results, the proposed technique is currently being analysed on its feasibility in the remote e-health communication. The work focused on trusted and secure communication between ubiquitous sensors which might be attached to human body or located at any electronic home appliances to personal devices and finally to medical database which is located in the hospital. A test bed consisting of wireless sensor nodes, smart phone and server is being set up in the laboratory to enable advance analysis on the IBE _Trust Protocol. Further secure communication from the smart phone to the medical database will be made available. Figure 7 depicts the architecture of the test-bed.

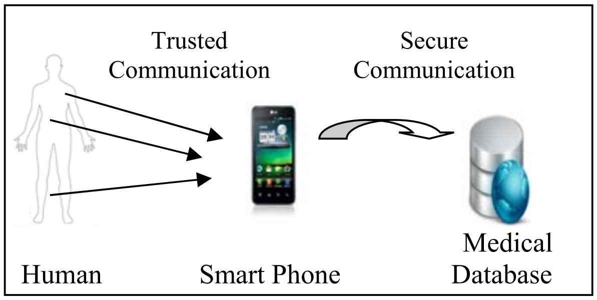

Figure 7. E-Health Test Bed

Referring to Figure 7, one main issue concerning the data security that arise is authentication of sensor node with mobile devices. The system has to ensure that the data received at the owner of the mobile device are their own data and should not be confused with other sensors surrounding them. The possibilities of having this problem will rise with the increased acceptance of mobile e-health related applications. There are lots of mobile health research has been initiated throughout the developing countries and these works have demonstrated great assistances in patient-doctor interaction including increased access to the healthcare information mostly in remote populations.

We believe that this issue should be handled by proper authentication of the sensor nodes. Basically there are several ways to authenticate the body sensor to the mobile device such as password, biometrical method and MAC address. However, works on trust establishment between sensor and mobile device are hardly found. This work aims at enabling password-less authentication between sensor nodes and mobile device for seamless operation. With this connection, it is now becoming more feasible than before to use mobile technology for medical applications. A user can simply connect a wireless sensor on their body to a mobile device in order to monitor their health data. This application is intended to provide a better personal health management and a trusted monitoring health system.

6 Conclusion

This paper firstly shows the importance of having a trusted sensor node in the network of wireless sensor. It then discusses on the methods and procedures involve toward trusted sensor node. Acknowledging the constraint in power experience by almost all sensor nodes, the presented work is analyzed by means of energy to confirm its feasibility. First part of analysis proves the feasibility of presented work toward having a trusted sensor node. On the other hand, the second part of the analysis confirms that the proposed work consumed reasonable energy as compared to available work. The developed authentication protocol contributes to a new method in authenticating newly joining nodes in the WSNs environment where a unique generated value from the trusted platform is used to authenticate the new nodes. With non-regenerated unique platform identity, the possibility of node cloning attack by adversaries is almost impossible. In addition, demand for secure key distribution mechanism needed in PKC mechanism is no longer necessary due to the existence of pre-distribution keys in the pre-deployment stage. Next, proposed application in the e-health authentication system that will integrate the wireless sensor network authentication with mobile device system for secured communication is presented and discussed.

Acknowledgement

The authors would like to thank the Ministry of Science, Technology and Innovation (MOSTI) for providing the grant 100-RMI/SF 16/6/2 (11/2013). Authors would also like to thank Faculty of Electrical Engineering, UiTM Shah Alam, Research Management Institute (RMI) and member of Information Security and Trusted Infrastructure Laboratory (InSTIL), Computer Engineering Department for supporting the research work.

References:

[1] "Copyright ©2011 Trusted Computing Group (www.trustedcomputinggroup.org.) All Rights Reserved," *Group*, 2011. [Online]. Available: http://www.trustedcomputinggroup.org/files/static_page_files/BDEACD8E-1A4B-B294-D06D2F15D16238AE/TCG FACTSHEET_rev Jan 19 2011 (3).pdf.

[2] G. Padmavathi, "A Survey of Attacks , Security Mechanisms and Challenges in Wireless Sensor Networks," *Journal of Computer Science*, vol. 4, no. 1, pp. 1–9, 2009.

[3] Y. M. Yussoff, H. Hashim, R. Rosli, and M. D. Baba, "A Review of Physical Attacks and Trusted Platforms in Wireless Sensor Networks," *Procedia Engineering*, vol. 41, Iris, pp. 580–587, Jan. 2012.

[4] A. Forster, D. Puccinelli, and S. Giordano, "Sensor node lifetime: An experimental study," *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pp. 202–207, Mar. 2011.

[5] Y. M. Yussoff, H. Hashim, and U. T. Mara, "IBE-Trust : A Security Framework for Wireless Sensor Networks," in *Internet Security (WorldCIS), 2011 World Congress on*, 2011, pp. 171–176.

[6] A. Shamir, "Identity-Based Cryptosystems and signature schemes," in *Proceedings of CRYPTO 84 on Advances in cryptology*, 1984, pp. 47–53.

[7] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *Computer*, vol. 32, no. 3, pp. 586–615, 2003.

[8] A. S.Wander, N. Gura, H. Eberle, and Vipul Gupta, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," in *PERCOM '05 Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*, 2005, pp. 324–328.

[9] K. Piotrowski, P. Langendoerfer, F. Oder, S. Peter, and D. S. Engineering, "How Public Key Cryptography Influences Wireless Sensor," in *SASN '06 Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, 2006, pp. 169–176.

[10] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy Analysis of Public-Key Cryptography on Small Wireless Devices," in *Pervasive Computing*, 2005, pp. 324–328.

[11] Moises Salinas, Gina Gallegos Garcia and Gonzalo Duchen Sanchen, "Efficient Message Authentication Protocol for WSN," in *WSEAS TRANSACTIONS on COMPUTERS*, 2009, Issue 6, Volume 8, June 2009.

[12] T. Avispa and T. Document, "AVISPA v1 . 1 User Manual," 2006. [Online]. Available: www.avispa-project.org/package/user-manual.pdf. [Accessed: 30-Apr-2013].

[13] L. H. Adnan, Y. M. Yussoff, and H. Hashim, "Secure Boot Process for Wireless Sensor Node," in *Computer Applications and Industrial Electronics (ICCAIE), 2010 International Conference on*, 2010, ICCAIE, pp. 646–649.

[14] M. C. Gorantla, C. Boyd, and J. M. G. Nieto, "ID-based One-pass Authenticated Key

Establishment," in *Australasian Information Security Conference, AISC'08 Australia*, 2008, pp. 39-46.

[15] L. H. Adnan, H. Hashim, Y. M. Yussoff, and M. U. Kamaluddin, "Root of Trust for Trusted Node Based-on ARM11 Platform," in *Conference on Communications (APCC), 2011 17th Asia-Pacific*, 2011, no. October, pp. 812–815.

[15]Wangke YU, Shuhua WANG, "Key pre-distribution using combinatorial designs for wireless sensor networks," in *WSEAS TRANSACTIONS on MATHEMATICS*, vol. 12, 2013.

[16] Jasmine Norman, "Optimized Routing for Sensor Networks using Wireless Broadcast Advantage," in WSEAS TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS, vol. 5,2013.

[17] "MIRACL Reference Manual." [Online]. Available: https://wiki.certivox.com/display/EXT/MIRACL+Reference+Manual#MIRACLReferenceManual-1MIRACLReferenceManual. [Accessed: 30-Apr-2013].

[18] M. Hebel, G. Bricker, and D. Harris, "Getting Started with XBee RF Modules." [Online]. Available: http://www.parallax.com/portals/0/downloads/docs/prod/book/122-32450-xbeetutorial-v1.0.pdf. [Accessed: 30-Apr-2013].

[19] "XBee® 802_15_4 - Digi International." [Online]. Available: http://www.digi.com/products/wireless-wired-embedded-solutions/zigbee-rf-modules/point-multipoint-rfmodules/xbee-series1-module#specs.

[20] Rickard Söderlund, "Energy Efficient Authentication in Wireless Sensor Networks," in *Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on*, 2006, pp. 1412 – 1416.

[21] A. Tiwari, P. Ballal, and F. L. Lewis, "Energy-efficient wireless sensor network design and implementation for condition-based maintenance," *ACM Transactions on Sensor Networks*, vol. 3, no. 1, Mar. 2007.

[22] "Sending data through an 802_15_4 network latency timing_Knowledge Base Article - Digi International." .

[23] G. Ferrari, P. Medagliani, S. Di Piazza, and M. Martal, "Wireless Sensor Networks : Performance Analysis in Indoor Scenarios," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, pp. 41–54, 2006.