Lightweight Trusted Authentication Protocol for Wireless Sensor Network in e-Health

Nazhatul Hafizah Kamarudin, Yusnani Mohd Yussoff, Habibah Hashim
Department of Computer Engineering, Faculty of Electrical Engineering,
University Technology MARA Shah Alam, Malaysia.
yusna233@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 such as in e-Health application. However, due to its ability to work without human intervention, the sensor nodes are susceptible to clone nodes types of attacks. These will then lead to worst consequence which is a false message. Therefore, secure communication is no more enough in e-health environment. This paper presents a rigorous research work in the development of a lightweight trusted authentication protocol for wireless embedded devices in the e-Health environment. The term trust in this research work is based on Trusted Computing Group definition and therefore the development is started from the sensor node itself. Based on that, an IBE_TRUST e-health authentication protocol is presented and analyzed. Conceding the energy constraint of the e-health environment, analysis on the power and energy consumption is conducted to ensure its practicality. This proposed authentication protocol will protect the e-health communication system from node cloning attack and replay attack. By integrating the trusted authentication protocol in mobile health monitoring system, it suggests a great assistance in patient-doctor interaction and protects the security of the e-health data network.**

***Index Terms*—Wireless Sensor Network; Authentication; Trust; IBE.**

I. Introduction

E-health communication system is currently being developed due to the enhancement of the Internet of Things (IOT). Protecting the wireless sensor network of e-health system should be taken as a serious issue in handling the e-health security aspects such as sensor node authenticity and data confidentiality. The designing phase for e-health sensor network should consider these aspects and a secure authentication phase should be implemented since e-health system consists of wireless sensor nodes that transmit highly sensitive data and thus extremely susceptible to security attacks. There are lots of research discussing on the importance of sensor network security and focusing on the possible vulnerabilities of WSNs [2][3]. However, with the implementation of sensor node in a patient body that are mostly left unattended by the health personnel, authenticating valid sensor nodes or trusted nodes in the network system is also an important issue to be considered.

According to Trusted Computing Group (TCG) [1] requirement, attestation is the fundamental phase of trusted computing platforms. The user has to authenticate the property of a sensor node by providing confirmation of the integrity of its hardware or software over the network. There are two major components for this attestation which are Integrity Measurement Architecture (IMA) and remote attestation protocol. It is to ensure system integrity and to check whether the system has been changed since it is last been turned off. Then, remote attestation protocol is to determine the identity of a sensor node or a program.

Nevertheless, in order to integrate this attestation into the e-health wireless sensor network system, power energy and computation capability are the core issues due to energy constraint in the e-health sensor node [4]. Therefore, IBE_Trust [5] is proposed to this e-health authentication protocol and then power analysis and cryptography process analysis are being evaluated throughout this paper.

The idea of identity-based encryption (IBE) [6] was first introduced by Shamir because of the security issues in Public Key Infrastructure (PKI). IBE eliminates the need for a third party certificate by using the identity of the base station to generate private key and encrypt the message data transmitted [7]. Authorized users can only decrypt the message data. On the other hand, the use of elliptic curve cryptography (ECC) algorithm in IBE can reduce the computational cost since the key size is shorter than RSA authentication protocol [8][9][10] and IBE is an efficient authentication protocol [11].

IBE_Trust is an improved version of the existing IBE protocol that is reliable to apply in the e-Health authentication environment. A trusted sensor node first needs to successfully boot-up and authenticate with the mobile device during the login process. The meaning of trust sensor here has to comply with the TCG specifications of the trusted platform. The integrity of the software in the sensor node will be measured through a secure boot process in a trusted platform and if it passes, a non-regenerated unique identity of the sensor node is produced and then will be installed in the mobile device. Then, it will go through the IBE_Trust e-health authentication protocol that will be discussed later throughout this paper. Mobile device and e-health base station can detect mischievous coding installed in the sensor node through this secure boot process. Using a formal analysis software, AVISPA [18], IBE_Trust authentication protocol is recognized and it is secured from security attacks specifically node impersonation and replay attack.

This paper discusses the implementation of IBE_Trust e-health authentication protocol on mobile health monitoring system and evaluates its feasibility in terms of wireless sensor network application. The outline of this paper is: Section 2 presents the related works for IBE-Trust and existing e-Health authentication protocol, the following Section 3 describes the overall experimental test bed for the authentication protocol, Section 4 presents the results and analysis of the proposed authentication protocol and finally in Section 5 clarifies the conclusion and future research that can be developed from this research.

II. Related Works

There are lots of e-health monitoring applications that have been developed using wireless sensor network recently. Most authentication schemes in e-health currently are using username and password for identity authorization which is susceptible to security attacks such as replay attack and masquerade attack. In [12,13,14], basic authentication scheme were proposed where a user need to successfully verify their identity in the system by log in their username and password to the mobile e-health network. Then, it will automatically direct the user into the e-health system. The use of username and password in authentication protocol has been exposed to security attacks such as packet sniffing where a perpetrator can listen to the network traffic and get an illegal authorization to the data access. Even though we have built most of cryptographic and security protocols to eliminate these attacks, username and passwords still can be cracked using debuggers and dissemblers [14]. Therefore, additional security mechanism should be implemented in the network system besides using only password for authentication to enhance the security of e-health system [15].

On the other hand, involvement of an e-health service provider or a third-party user in mobile e-health current architecture will reduce the reliability of the e-health authentication system. Privacy and confidentiality are the important aspects in e-health systems and in general, people should not expose their private data to any third party except for trusted authorities [16,24]. For instance, patient mobile device will connect first to a third-party database server or to the e-health service providers and then connect to the e-health base station [17].

IBE_Trust e-health authentication protocol is an identity-based authentication protocol that confirms data confidentiality, integrity and authenticity. This protocol will verify that a sender is a trusted sensor node and behave in the expected manner in the network. It comprises of two compulsory stages which are pre-registration phase and registration phase. This proposed authentication protocol also suggests seamless authentication with the base station without a need for a third-party server. Therefore, it can eliminate a security hole of the network system.

III. Methodology

A. Full Hardware Setup

The whole system is setup by connecting a pulse sensor to a mobile device through Bluetooth application. Since the e-health environment is between body area sensor networks with a patient mobile device, it is more secure to use Bluetooth for its smaller range area covered in order to avoid interference attack. Some programming codes are used to transmit and receive message through sensor node, mobile device and e-health base station [20]. IBE_Trust e-health authentication protocol is performed in the e-health base station in order to generate common parameters, master key and private key. After successful authentication between sensor node and mobile device, the mobile device will send a login request to the e-health base station. IBE_Trust e-health authentication protocol will be implemented in the system to establish common session key agreement.

B. Proposed Protocol

The development of IBE_Trust e-health authentication protocol comprises of two main stages which are the generation of the sensor node identity in a trusted platform and the e-health authentication protocol. This trusted computing system ensures that it boots and generates only authenticated and genuine code for the non-regenerated sensor node identity. Therefore, a secure boot process has to be done first prior to the deployment of the e-health authentication protocol to achieve trusted environment. Each component of the hardware and software for the sensor node is validated from the lowest layer to the upper layer. Secure boot process has been discussed thoroughly in [19]. Through the secure boot process, a non-regenerated unique identity of the sensor node is produced which will be used as node's identity in the e-health authentication protocol. This unique identity is almost impossible to be cloned or to be regenerated. thus it protects the whole system from masquerade node cloning attack. This IBE_Trust protocol works as a biometric concept where we use human physical features as the unique identity but for a wireless embedded hardware system authentication, a unique identity of the sensor node is generated. Figure 1 shows the process flow for unique sensor identity generated followed by IBE_Trust e-health authentication protocol.

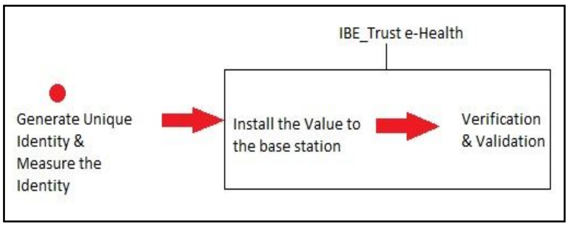
IBE_Trust e-Health
Generate Unique Identity & Measure the Identity
Install the Value to the base station
Verification & Validation

Figure 1: Process flow of IBE_Trust e-health authentication

After installation of the unique sensor identity value in the mobile device or base station, the system will go through the IBE_Trust e-Health authentication protocol. It has four phases which are pre-registration phase, registration phase, login phase and authentication phase. List below states the symbols that will be used in the IBE_Trust authentication equations algorithm.

||=concatenation
⊕= XOR operation
SNi = sensor node identity
ID_{mobile}= mobile device identity
s = master key
a, b, M= random nonce
K= e-health base station public key
P_k= e-health base station private key
* = input value

a. Pre-registration phase

Pre-registration phase is done in offline mode by the healthcare personnel in order to generate a sensor node and mobile device unique identity upon connection to the e-health network system. It mainly consists of a secure boot process that generates the unique identity and also generates common system parameters and public key. This information will be installed in the sensor node and mobile device before registration phase.

b. Registration phase

In the registration phase, the sensor node will reboot to generate its unique identity value as well as generating nonce. The non-regenerated unique identity value and the nonce will be hashed using security algorithm and then the sensor will submit the value to the mobile device. Upon receiving the message from the sensor node, the mobile device will firstly be installed with the sensor node unique identity given at the pre-registration phase.

Sensor node selects random number, a and computes = A_i which is a hash value of sensor node identity concatenated with a.

$$Ai = H(SNi|\,a) \tag{1}$$

Mobile device then computes F_i after receiving Ai from the sensor node.

$$F_i = A_i \oplus s \tag{2}$$

where s is a master key generated by the e-health base station.

Mobile device will then generate its unique identity together with a nonce value, b and compute B_i. B_i is then will be stored in the e-health base station.

$$B_i = H(b \oplus ID_{mobile}) \tag{3}$$

The value of ID_{mobile} and B_i will be stored in the base station. The e-health base station will then compute security parameter C_i.

$$C_i = B_i \oplus H(s) \oplus s \tag{4}$$

c. Login phase

The user turns on the sensor node and connects to the mobile device. The sensor will submit SN_i^* to the mobile device. The mobile devices computes:

$$F_i^* = A_i^* \oplus s \tag{5}$$

and then compare the value F_i^* with the value F_i in its memory to verify the legitimacy of the sensor node identity. After verification, mobile device generates random nonce value, M and computes:

$$CIDi = Bi^* \oplus H(x) \oplus H(s) \oplus M \tag{6}$$

where x is a random value chosen by the e-health base station. Then, mobile device computes:

$$Ri = EK\,(M| \oplus IDmobile^* \tag{7}$$

The unique identity of mobile device and the nonce are encrypted with the base station public key, K which is the server ID to prevent the login information from being exposed. The mobile device then sends a login request <R_i, CID_i> to the e-health base station.

d. Authentication phase

After receiving the login request from the mobile device, the e-health base station will firstly verify the mobile device unique identity given at the pre-registration phase. The e-health base station then decrypts R_i using the e-health base station private key, P_k and verifies the received unique identity value with the one existed in the trust list. If the identity is not equal, the login request is rejected and the session will be terminated.

$$DK\,(Ri) = obtain\ IDmobile^* \tag{8}$$

The e-health base station checks $ID_{mobile}^* = ID_{mobile}$, if authentic, it computes

$$Ci^* = CIDi \oplus M \oplus H(s) \oplus s \tag{9}$$

Then, the e-health base station checks $C_i^* = C_i$. The equivalency authenticates the legitimacy of the sensor node and the mobile device. Thus the login request is accepted and a secure session key has established.

IV. Result Analysis

This section analyzes the performance of IBE_Trust e-Health protocol. The analysis focuses on the energy and power consumption during the sensor node authentication process.

In RSA-1024, a client can transmit 490 bytes of data and a server can transmit up to 314 bytes [8]. Following body sensor node 802.15.4 specifications [20] which allow transmission up to 100 bytes , RSA requires 5 packets data from sensor to base station and 4 packets data from base station to sensor. Thus, overall number of packet that is required for RSA authentication is 9. For ECC authentication, sensor node and base station transmit 138 bytes of data, which add up to 4 packets. IBE_Trust e-health authentication protocol on the other hand requires only 3 packets data from sensor to base station and 1 packet data from base station to sensor.

For that reason, by analyzing packets data which is then converted into energy consumption, we can see that IBE_Trust protocol is more efficient and lower energy consumption compared to RSA and ECC protocol. It is due to the transmission of username and password in their authentication scheme which require large key size and high energy. Because of the large key size, RSA authentication protocol utilizes the highest energy. In contrast, ECC consumes the lowest energy during the transmission since this protocol does not have pairing algorithm and IBE_Trust on the other hand requires pairing algorithm in order to successfully authenticate. But IBE_Trust e-health authentication protocol uses the lowest power at receiving since the sensor node has to receive only 2 bytes of packets data from the e-health base station.

Figure 2 displays the comparison between RSA, ECC and IBE_Trust protocol in terms of energy analysis throughout the communication system.

For Bluetooth with 48-bit computing [25], sensor node is able to send up to 100 bytes of packets data and 25 bytes packets header. Thus, the total size of packets data communication from sensor to base station is 355 bytes, and 27 bytes from base station to sensor node.

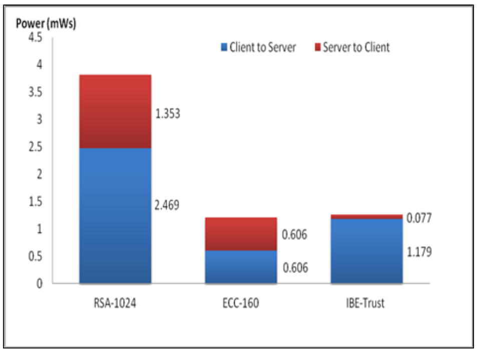

Figure 2: Energy analysis

In order to transmit the packets data, it only takes about 0.1985 seconds or 8.072µWs per bit using Bluetooth transceiver. Nevertheless, in order to receive the same packets data, it takes about 58.616µWs which is 6.5 times longer. We can conclude that, sensor node uses a low amount of energy to transmit the packets data compared to the energy used in the e-health base station. This explains that IBE_Trust protocol is efficient and applicable to use in the e-health sensor network authentication.

Figure 3 shows the analysis on the encryption and decryption process. The decryption process uses 17.412W of energy utilization which is 68 percent higher compared to the encryption process that uses only 5.472W. Since the decryption process will be done by the e-health base station, the IBE_Trust decryption process does not depend on the sensor node requirement as the e-health base station has high processing capability with no power constraint.

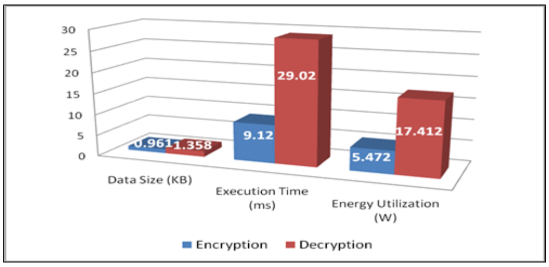

Figure 3: Performance analysis during encryption and decryption process in IBE_Trust

Additionally, Figure 4 shows the energy decomposition for IBE_Trust e-health authentication protocol. Cryptography process which consists of encryption and decryption use the most energy consumption. Lots of researches [8][21][22] show that public key cryptography process dominates the energy consumption in the network system. For that reason, IBE_Trust e-health authentication protocol has minimized the cryptography algorithm especially at the sensor node process.

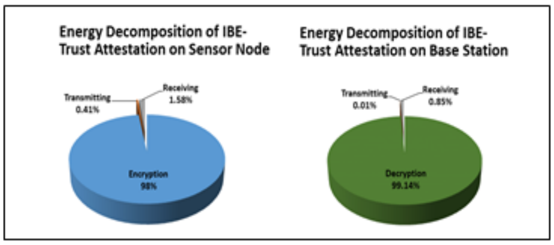

Figure 4: Decomposition of energy for IBE_Trust protocol

V. Conclusion

In summary, the proposed authentication technique is reliable and secure to be implemented in the e-health communication environment. It focuses on a trusted and secure communication in the e-health network system which consists of sensor node, mobile device and e-health base station. A prototype has been set up in the laboratory using a pulse sensor node, developing an e-health application in a smartphone, and setting up a database server. The critical issue concerning the e-health data security is basically the authentication of a sensor node with the mobile device and e-health base station. This proposed IBE_Trust e-health authentication protocol has ensured that the data received to the owner of the mobile device are their own sensor data and the e-health base station can only get connected with the registered mobile device since the non-regenerated unique identity has been installed in the system. There are lots of mobile health research has been initiated throughout the developing countries and these works have demonstrated many researches on the e-health authentication issues.

We believe that this issue should be handled by a proper and secured authentication of the sensor nodes. Basically there are several ways to authenticate the body sensor node to the mobile device and base station such as password, biometrical method and MAC address. However, works on trust establishment between sensor and mobile device are more reliable and secure. 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. Thus it will provide a better personal health management together with a trusted monitoring health system.

This proposed IBE_Trust e-health authentication protocol has contributed to a new method in authenticating a sensor node in e-health where a unique and non-regenerated value from the sensor trusted platform is used to authenticate the sensor node [23]. With this non-regenerated unique identity, it is almost impossible to clone the sensor node and therefore it can avoid masquerade attack in the e-health system. Moreover, secure key distribution mechanism is no longer needed since the pre-distribution keys has already be done in the pre-registration phase.

Acknowledgement

The authors would like to thank MOSTI for e-science under grant 100-RMI/SF 16/6/2 (11/2013) project of trusted remote medical telemonitoring attestation model, Research Management Institute (RMI) of University Technology MARA, and members of Computer Engineering (INSTIL) research, Faculty of Electrical Engineering.

References

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

[2] Padmavathi G., 2009. A Survey of Attacks , Security Mechanisms and Challenges in Wireless Sensor Networks. *Journal of Computer Science*. 4(1):1–9.

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

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

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

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

[7] Boneh D. and Franklin M. 2003. Identity-Based Encryption from the Weil Pairing. Computer. 32(3). 586–615.

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

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

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

[11] Moises Salinas, Gina Gallegos Garcia and Gonzalo Duchen Sanchen. 2009. Efficient Message Authentication Protocol for WSN. *WSEAS Transactions on Computers*. 6(8). June 2009.

[12] Bai G. and Guo Y. 2010. Activity Theory Ontology for Knowledge Sharing in E-health. *IEEE Int. Forum on Information Technology and Appication*. July 2010. 39–43.

[13] Ghazizadeh E., Zamani M., Ab Manan J., and Alizadeh M.. 2014. Trusted computing strengthens cloud authentication. *The Scientific World Journal*. 2014.

[14] Zhang R. and Liu L. 2010. Security Models and Requirements for Healthcare Application Clouds. *2010 IEEE 3rd Int. Conf. Cloud Computing*. 268–275.

[15] Fernández-Alemán J. L., Señor I. C., Lozoya P. Á. O., and Toval A. 2013. Security and privacy in electronic health records: a systematic literature review. *Journal on Biomedical. Informatic*. 46(3):541–62.

[16] Dong N., Jonker H., and Pang J. 2012. Challenges in ehealth: from enabling to enforcing privacy. FHIES'11 Proc. First Int. Conf. Found. *Health Informatics Engineering. System.* 195–206.

[17] Bai G., Guo Y. 2011. A General Architecture For Developing A Sustainable Elderly Care e-Health System. IEEE International Conf. *On Service System and Service Management (ICSSM)*June 2011. 1-6.

[18] Avispa T. and Document T. 2006. AVISPA v1 . 1 User Manual, 2006. [Online].From:ww.avispaproject.org/package/user-manual.pdf. [Accessed: September 2015].

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

[20] Yusnani M. Yussoff, Rosli R. 2014. Analysis of Remote Attestaion Protocol in Wireless Sensor Network (WSn). *WSEAS Advances in Computer Science*. Lisbon Portugal.

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

[22] Tiwari A., Ballal P., and Lewis F. L. 2007. Energy-efficient wireless sensor network design and implementation for condition-based maintenance. *ACM Transactions on Sensor Networks.* March 2007. 3(1).

[23] Nazhatul Hafizah Kamarudin, Yussoff Y.M., Hashim H. 2015. IBE_Trust Authentication for e-health mobile monitoring system. *IEEE Computer Applications & Industrial Electronics (ISCAIE) 2015.* Langkawi Malaysia. 12-14 April 2015. 160-164.

[24] Nazhatul Hafizah Kamarudin, Yussoff Y. M., Hashim H. 2014. Two-tier e-Health Monitoring System. *WSEAS Applied Computational Science (ACACOS) 2015* Kuala Lumpur, Malaysia. 23-25 April 2014.

[25] Curt Franklin, Julia Layton. How Bluetooth Works [Online]. From:http://www.ocmboces.org/files/folder1273/HowStuffWorks%20_How%20Bluetooth%20Works_.pdf [Accessed on 20 August 2015].