Faculty of Information and Communication Technology

AN ELECTROCARDIOGRAM-BASED AUTHENTICATION PROTOCOL IN WIRELESS BODY AREA NETWORK

Sofia Najwa binti Ramli

Doctor of Philosophy

2016

AN ELECTROCARDIOGRAM-BASED AUTHENTICATION PROTOCOL IN WIRELESS BODY AREA NETWORK

SOFIA NAJWA BINTI RAMLI

A thesis submitted
in fulfillment of the requirements for the degree of Doctor of Philosophy

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2016

DECLARATION

I declare that this thesis entitled "An Electrocardiogram-based Authentication Protocol in Wireless Body Area Network" is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ……..

Name : SOFIA NAJWA BINTI RAMLI
……..

Date : ……..……

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in term of scope and quality for the award of Doctor of Philosophy.

Signature	:	……..
Supervisor Name	:	PROF. DR. RABIAH BINTI AHMAD ……..
Date	:	……..……

DEDICATION

To my beloved husband and parents

ABSTRACT

In the past few years, the applications of Wireless Body Area Network (WBAN) have improved the ability of healthcare providers to deliver appropriate treatments to the patients either in hospitals or at homes. Precisely, biomedical sensors in a WBAN collect physiological signal from human's body to enable remote, continuous and real-time network services. As the signal contains highly sensitive medical information about the patient and communicates through an open wireless environment, securing the information from unauthorized access and tampering are critically needed. One of the most crucial components to support security architecture in WBAN is its key management as it serves as the fundamental of authentication and encryption, but the overheads are enormous in dealing with key generation, exchange, storage and replacement. In response to such issue, the most promising solution for key management is the use of biometrics so that the involved parties can agree on a key to provide the authenticity of medical data in WBAN. However, the existing models are inappropriate to achieve optimal security performance and the required lightweight manners due to the sensor's resource constraints in terms of power consumption and memory space. Therefore, this thesis presents a new authentication protocol model that utilizes Electrocardiogram (ECG) signal as biometric as well as cryptographic key to ensure that the transmitted data are originated from the required WBAN. The proposed model is developed and simulated on Matlab based on an improved fuzzy vault scheme with a lightweight error correction algorithm to reduce the computational complexity when compared to previous work. To validate the proposed ECG-based authentication protocol model, the FAR and FRR analysis is done and then followed by the complexity analysis. The result of FAR and FRR analysis demonstrates that choosing a definite degree and tolerance level can achieve optimal security performance required in WBAN communications. In complexity analysis, based on t-test, the result shows that there is a significant difference with 5% significant level in the computational complexity between the proposed authentication model and the previous protocol called ECG-IJS scheme and the proposed model requires fewer overheads in terms storage and communication overheads. To enhance the overall performance, this thesis also evaluates the uniqueness and the stability of ECG signal using Independent Component Analysis (ICA) and fast Fourier Transform (FFT) algorithm respectively as the signal is applied as inputs of the proposed ECG-based authentication protocol model. The experimental result of ICA algorithm exhibits that each ECG signal is unique to each other as each signal is composed strongly from each different independent component and approximately zero relative to other independent components. While the result of FFT algorithm summarizes that the number of the common FFT peak location index for sensors on the same subject is significantly higher compared to the number of common feature for sensors on different subjects.

ABSTRAK

Dalam beberapa tahun yang lepas, penggunaan Rangkaian Kawasan Badan Tanpa Wayar (WBAN) telah meningkatkan keupayaan staf kesihatan untuk menyediakan rawatan kepada pesakit-pesakit sama ada di hospital ataupun di rumah. Ianya adalah dengan sensor bioperubatan di dalam WBAN mengumpul isyarat fisiologi daripada badan pesakit untuk membenarkan penggunaan rangkaian WBAN dari jauh secara berterusan dan langsung. Memandangkan isyarat fisiologi mengandungi maklumat perubatan yang sulit tentang pesakit dan dihantar melalui rangkaian tanpa wayar yang terbuka, keselamata maklumat perubatan adalah sangat diperlukan terhadap akses yang tidak dibenarkan dan yang diubah. Salah satu komponen untuk menyokong keselamatan maklumat dalam WBAN adalah pengurusan kunci rahsia kerana ia adalah asas kepada pengesahan dan penyulitan maklumat, tetapi kos operasi adalah besar dalam penjanaan, pertukaran, penyimpanan dan penggantian semula kunci rahsia, Sebagai tindakbalas terhadap isu tersebut, penyelesaian yang paling terjamin adalah dengan penggunaan biometrik supaya pihak yang terlibat bersetuju dengan satu kunci rahsia untuk pengesahan data perubatan dalam WBAN. Walaubagaimanapun, model-model yang sedia ada adalah tidak sesuai untuk mencapai penilaian keselamatan yang optimum dan ringkas berikutan kekangan sumber sensor dari segi penggunaan tenaga dan ruang memori. Oleh itu, tesis ini mempersembahkan satu model protokol pengesahan maklumat yang baru menggunakan isyarat ECG sebagai biometrik juga kunci kriptografi untuk memastikan bahawa maklumat yang dihantar adalab berasal dari WBAN yang sepatutnya. Model ini direka dan disimulasi menggunakan aturcara Matlab berdasarkan satu skim kebal kabur dengan satu algoritma pembetulan ralat yang ringkas untuk mengurangkan kerumitan pengkomputeran apabila dibandingkan dengan model yang sedia ada. Untuk mengesahkan model protokol pengesahan berasaskan ECG, analisis FAR dan FRR dilakukan dan diikuti oleh analisis kerumitan. Hasil analisis FAR dan FRR menunjukkan bahawa memilih tahap toleransi yang betul boleh mencapai prestasi keselamatan optimum yang diperlukan dalam komunikasi WBAN. Dalam analisis kompleks, berdasarkan t-test, hasilnya menunjukkan bahawa terdapat perbezaan yang signifikan dengan tahap signifikan 5% dalam kerumitan pengkomputeran antara model yang dicadangkan dan protokol sedia ada yang dipanggil skim ECG-IJS dan model yang dicadangkan memerlukan kos penyimpanan memori dan komunikasi yang kurang. Untuk meningkatkan prestasi keseluruhan, tesis ini juga menilai keunikan dan kestabilan isyarat ECG menggunakan ICA dan FFT algoritma masing-masing kerana isyarat yang digunakan adalah input model protokol pengesahan berasaskan ECG yang dicadangkan. Hasil eksperimen algoritma ICA adalah bahawa setiap isyarat ECG adalah unik antara satu sama lain kerana setiap isyarat terdiri daripada setiap komponen bebas yang berbeza dan kira-kira sifar berbanding dengan komponen bebas lain. Manakala hasil daripada algoritma FFT meringkaskan bahawa bilangan indeks puncak lokasi FFT untuk sensor pada subjek yang sama adalah lebih tinggi berbanding dengan bilangan indeks puncak lokasi FFT untuk sensor pada subjek yang berbeza.

ACKNOWLEDGEMENTS

In the name of Allah, the Most Gracious, the Most Merciful.

Firstly, I would like to express my sincere gratitude to my supervisor, Prof. Dr. Rabiah binti Ahmad and co-supervisor, Assoc. Prof. Dr. Faizal bin Abdollah for the continuous support of my Ph.D study and related research, for their patience, motivation, and immense knowledge. Their guidances helped me in all the time of the research and writing this thesis. I could not imagine having better advisors and mentors for my Ph.D study. Besides them, I would like to thank my fellow colleagues who shared their technical knowledge, stimulating discussions, insightful comments and encouragement.

Also, this thesis would not be realized without the continuous loves, prayers and supports from my husband, Dr. Mohd. Aifaa bin Mohd Ariff, my great parents, my brothers and my sister. They are the symbol of love and giving, who never stop giving themselves in countless ways, lead me through the edges with hope and support, and stand by me when things look bleak. I dedicate this thesis to all of you.

Last but not least, thank you to Faculty of Information and Communication Technology, all the administration staff for their friendly helps and supports throughout this journey in Universiti Teknikal Malaysia Melaka. Besides, this research would not be accomplished without the funding from Ministry of Higher Education Malaysia under the Exploratory Research Grant Scheme (ERGS) and MyBrain 15 (MyPhD) Scholarship program. Thank you to all of you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF SYMBOLS

A	-	The mixing matrix
a	-	High coefficients of the monic polynomial
b	-	Low coefficients of the monic polynomial
C	-	The modified unknown sources, in P ICA algorithm
E	-	Encrypted message
FA	-	The number of false acceptance
FR	-	The number of false rejection
f	-	Feature vector at the sender site
f'	-	Feature vector at the receiver site
$f(x)$	-	A monic polynomial constructed by the sender
$f_h(x)$	-	The polynomial with degree $s-t$ to $s-1$
$f_l(x)$	-	The polynomial with degree 0 to $s-t-1$
$f_{\max}$	-	Maximum resolvable frequency
$f_{Nyquist}$	-	Nyquist frequency
f_s	-	Sampling frequency
H	-	Hash function
ID_{BAN}	-	The information of WBAN's controller in which the transmission is active

ID_R	-	The address information of the receiver
ID_S	-	The address information of the sender
K	-	The cryptographic key
m	-	The number of signals correspond to the number of patients
N	-	The number of samples
n	-	The number of independent components
P	-	The modified unknown sources, S
Q	-	The modified mixing matrix, A with positive peak values
S	-	Row vectors of unknown sources, $s(t)$
s	-	The degree of the monic polynomial
$s(t)$	-	A vector of independent component
SN	-	The sign of the dominant peak of every column in the mixing matrix, A
T	-	The normalized mixing matrix, Q
T_0	-	The period of the sampled signal
TC	-	The total number of client accesses
TI	-	The total number of imposter accesses
t	-	The coefficients of the monic polynomial/ number of errors
u	-	The element of feature vector, f'
V	-	The whitened data
v	-	The value of $f_h(x)$ on all points u

w	-	The element of feature vector, f
$w(t)$	-	Window function
$X(t)$	-	Row vectors of the recorded ECGs signal, $x(t)$ in time domain
$X'(f)$	-	The Fourier transform of the periodic function, $x'(t)$ in frequency domain
$x(t)$	-	The amplitude of the recorded ECG signal of a patient in time domain
$x'(t)$	-	A periodic function with a period of T_0
$y(t)$	-	The sampled data function in time domain
$\delta(t)$	-	Impulse function
$\phi(t)$	-	The inverse Fourier transform of the frequency sampli function
α_n	-	The component of Fourier transform
Δ_i	-	Normalizing the element in a vector to unity
Δf	-	Frequency solution
ΔT	-	Sampling interval

LIST OF ABBREVIATIONS

BSS	-	Blind Source Separation
DFT	-	Discrete Fourier Transform
DNA	-	Deoxyrebonucleic acid
ECC	-	Elliptic Curve Cryptography
ECDH	-	Elliptic Curve Diffie-Hellman
ECG	-	Electrocardiogram
EDB	-	European ST-T Database
FAR	-	False Acceptance Rate
FFT	-	Fast Fourier Transform
FRR	-	False Rejection Rate
HIPAA	-	Health Insurance Portability and Accountability Act
HR	-	Heart rate
HTER	-	Half Total Error Rate
IC	-	Independent component
ICA	-	Independent Component Analysis
IEEE	-	Institute of Electrical and Electronics Engineering
IJS	-	Improved Juels Sudan method
IMD	-	Implantable Medical Devices
IPI	-	Interpulse Interval

LTSTDB	-	Long Term ST Database
MAC	-	Message Authentication Code
MITDB	-	MIT-BIH Arrhythmia Database
NSRDB	-	Normal Synus Rhythm Database
PDA	-	Personal Digital Assistant
PPG	-	Photoplethysmography
PSKA	-	Physiological signal-based key agreement
QoS	-	Quality of Services
QTDB	-	QT Database
RF	-	Radiofrequency
RSA	-	Rivest-Shamir-Adleman
RSSI	-	Received Signal Strength Index
SAR	-	Specific Absorption Rate
SHA-1	-	Secure Hash Algorithm 1
SHA-2	-	Secure Hash Algorithm 2
SpO_2	-	Oxygen saturation
UWB	-	Ultra-wideband
WAN	-	Wide Area Network
WBAN	-	Wireless Body Area Network
WHO	-	World Health Organization
WLAN	-	Wireless Local Area Network
WMAN	-	Wireless Metropolitan Area Network
WPAN	-	Wireless Personal Area Network
WSN	-	Wireless Sensor Network

LIST OF PUBLICATIONS

Ramli, S.N. & Ahmad, R., 2011. Surveying the Wireless Body Area Network in the realm of wireless communication. In *2011 7th International Conference on Information Assurance and Security (IAS)*. pp. 58–61.

Ramli, S.N., Ahmad, R., Abdollah, M.F. & Dutkiewicz, E., 2013. A Biometric-based Security for Data Authentication in Wireless Body Area Network (WBAN). In *Advanced Communication Technology (ICACT), 2013 15th International Conference*. pp. 998–1001.

Ramli, S.N., Ahmad, R. & Abdollah, M.F., 2013. Electrocardiogram (ECG) signals as biometrics in securing Wireless Body Area Network. In *The 8th International Conference for Internet Technology and Secured Transactions*. Ieee, pp. 536–541.

Ramli, S.N., Ahmad, R. & Abdollah, M.F., 2014b. The Applicability of Electrocardiogram (ECG) As Biometrics in Securing the Communication of Wireless Body Area Network Center for Advanced Computing Technology. *Journal of Internet Technology and Secured Transactions (JITST)*, 3(2), pp.246–253.

Ramli, S.N., Ahmad, R. & Abdollah, M.F., 2014a. Hybrid Authentication Protocol Framework Using Wireless Body Area Network (WBAN) for Multiple Concurrent Health Monitoring. *International Review on Computers and Software*, 9(12), pp.1971–1976.

Ramli, S.N., Ahmad, R. & Abdollah, M.F., 2016. A Secure Data Authentication in Wireless Body Area Network for Health Monitoring Using Electrocardiogram-Based Key Agreement. *International Review on Computers and Software (IRECOS)*, 11(7), p.622.

CHAPTER 1

INTRODUCTION

1.1 Introduction

In the past few years, there have been a lot of technological advances in sensors and wireless communications. Sukor et al. (2008) stated that the advanced development in sensors and wireless communications have enabled the design of miniature, cost-effective and smart physiological sensor nodes. One of the approaches in developing these advancements is Wireless Body Area Network (WBAN). Basically, WBAN is a communication network between the humans and computers through wearable or implantable devices. It is found started from existing Wireless Personal Area Network (WPAN) technologies (Jang et al., 2011). WPAN is a personal area network using wireless connections typically within a short range (≤10m). It is used for communication among devices such as telephones, computer peripherals, and personal digital assistants (PDA). Technologies enabling WPAN include Bluetooth, Zigbee and Ultra-wideband (UWB), but the most promising wireless standard for WPAN applications is Zigbee. Zigbee has a low power consumption and low cost technology that is capable of handling large sensor networks up to 65000 nodes.

Technical requirements of WBAN include the requirements of WPAN by rights such as the existing low power wireless sensor network standard, Zigbee. However, the fact that Zigbee does not address majority of core technical requirements of WBAN highlights the need for a standard specifically designed for WBAN. Recognizing the great market potential and rapid technological developments in this sector, the Institute of

Electrical and Electronics Engineering (IEEE) establishes an 802.15.6 standard to develop a communication standard for miniaturized low-power devices that are deployed in or around a human body to serve a variety of medical, consumer electronics and entertainment applications (Ullah et al., 2013). In Figure 1.1, a WBAN is compared with other types of wireless networks. Each type of network has its typical enabling technology, defined by IEEE. A WPAN uses IEEE 802.15.1 (Bluetooth) or 802.15.4 (Zigbee), a WLAN uses IEEE 802.11 (WiFi) and WMAN IEEE 802.16 (WiMax). The communication in a WAN can be established via satellite links.

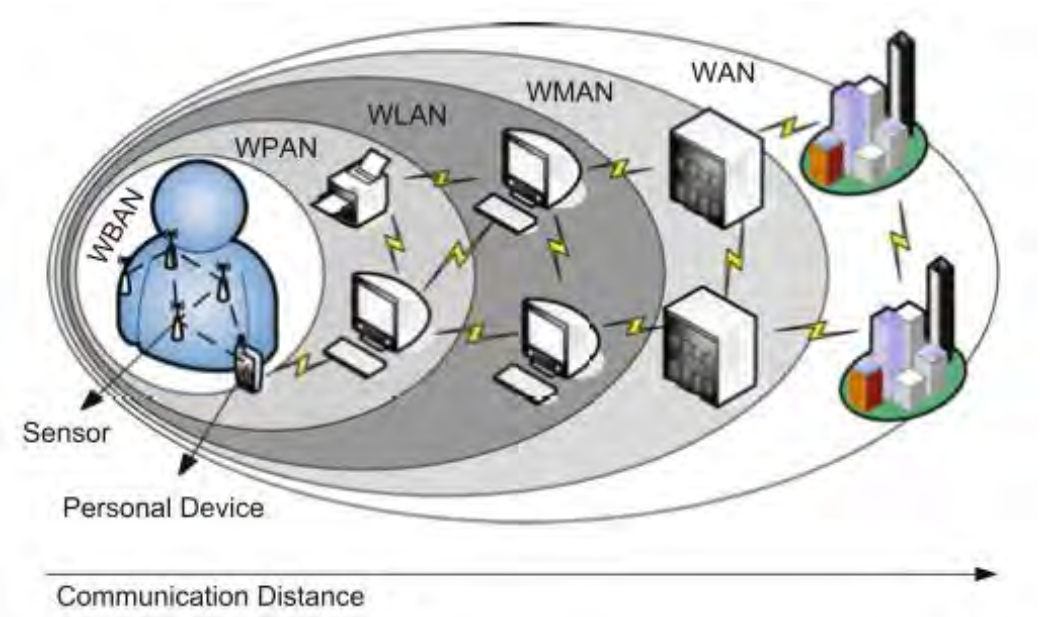

Figure 1.1: A WBAN in the realm of Wireless Network (Latré et al., 2010)

1.2 Characteristics of WBAN

A WBAN system comprises of a set of biomedical sensors attached on, in or around the human body in order to capture a variety of vital sign parameters continuously. A personal hand held device (e.g. PDA or smartphone) that acts as a gateway or

coordinator of data then collects these captured signals and transmits them to the controller (sink node) via Wireless Personal Area Network (WPAN) after the required data processing. The controller transfers the processed data to medical databases, as they need to be accessed and monitored by various users such as healthcare staff, researchers, government agencies, and insurance companies timely and accurately. Figure 1.2 denotes the general architecture of WBAN.

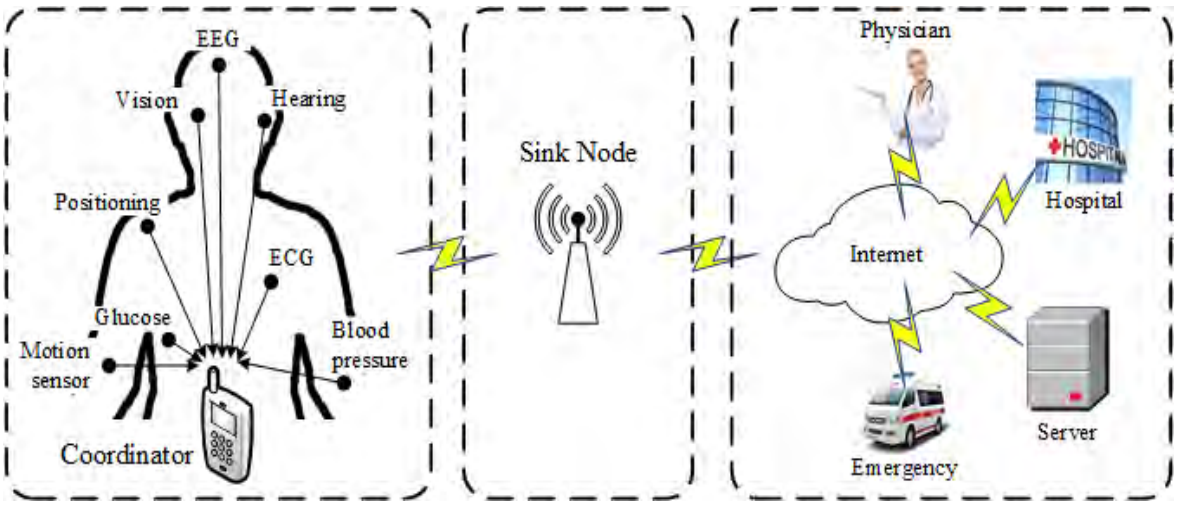

Figure 1.2: The General Architecture of WBAN

As the sensors are intentionally implemented to collect physiological signal from human's body, securing the communication over wireless network is very critical. Health Insurance Portability and Accountability Act (HIPAA) mandates that, as the sensors in WBAN collect the wearer's health data (which is regarded as personal information), care need to be taken to protect it from unauthorized access and tampering (Li et al., 2010; Venkatasubramanian et al., 2010). This is because of the open access environment by various people, which also accommodates attackers. Any point of failure in the security of the WBAN system would cause serious consequences as most of the applications are