International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp.63-70
http://dx.doi.org/10.14257/ijsia.2014.8.3.07

An Efficient Encryption Scheme using Elliptic Curve Cryptography (ECC) with Symmetric Algorithm for Healthcare System

Young Sil Lee[1, 2], Esko Alasaarela[2] and Hoon Jae Lee[1]

[1]*Department of Ubiquitous IT, Dongseo University Graduate School, 47 Jurye-ro, Sasang-gu, Busan, Rep. of Korea*
[2]*Department of Electronic Engineering, University of Oulu FI-90014, Oulu, Finland*
youngsil.lee0113@gmail.com, esko.alasaarela@ee.oulu.fi, hjlee@dongseo.ac.kr

Abstract

Wireless Body Area Networks (WBANs) has been recognized as one of the promising wireless sensor technologies for improving healthcare service thanks to its capability of seamlessly and continuously exchanging medical information in real time. However, the lack of a clear in-depth defense line in such a new networking paradigm would make it potential users worry about the leakage of their private information, especially to those unauthenticated or even malicious adversaries. In this paper, we present efficient encryption method based on Elliptic Curve Cryptography (ECC) to protect patient's medical data in WBANs. This method used the symmetric cipher algorithms (i.e., DES, modified Feistel algorithm, etc.) to encrypt or decrypt some sensitive patient's medical data, and then use ECC to manage the key's distribution, update and revocation.

Keywords: *We would like to encourage you to list your keywords in this section*

1. Introduction

The wearable medical devices (WMDs), which aim at collecting an individual's medical data unobtrusively and ubiquitously, are becoming more and more important and popular. With WMDs, the vital physiological parameters of a patient could be continuously and remotely collected from a few sensing nodes attached to his body, through wireless communication channels. Consequently, the patient's normal daily life is not disturbed by those annoying wired devices. In addition, with the collected data, the patient's health conditions could be monitored and medical professionals could react much more quickly and efficiently to some critical situation, such as a heart-attack. With the above mentioned advantages, the medical model is shifting from the traditional therapy-centered model to a pre-diagnose model at lower cost [1].

ISSN: 1738-9976 IJSIA

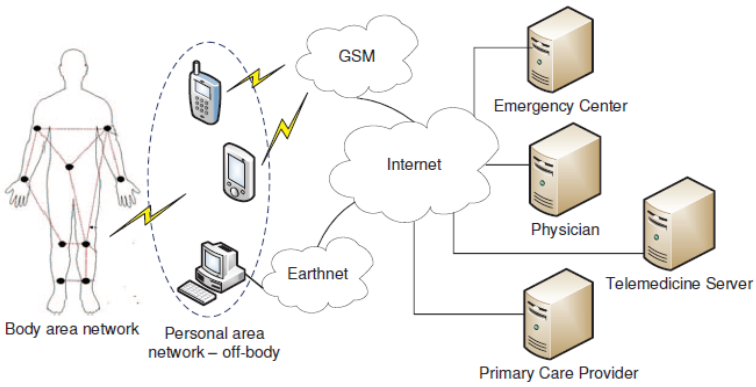

Figure 1. A WBAN Example for Healthcare [2]

Figure 1 illustrates one typical medical application scenario of WBAN, where biological information of concern like electrocardiogram (ECG) and blood pressure (BP), oxygen level (SpO2) and activity recognition *etc.*, are gathered by the sensors around the body (in-body networks) and transmitted to body area network (BAN) controller nodes (out-body networks), such as PDA and smart phones, which serve as gateway for anonymously accessing the services provided by external networks and servers.

Such a system consists of some wearable heterogeneous sensors spreading over the entire body and is capable of measuring and communicating a myriad of health-related stimuli. These wearable healthcare monitoring systems are either called body sensor networks (BSN), wearable wireless body/personal area network or body area sensor networks (BASN). The development of the BASN/BSN/WSN is imperative for modern telemedicine, PEMS and m-health.

However, the development of all the previous healthcare monitoring systems is mainly focused on the implementation of system functions and the security issues are often neglected. In fact for the development of a healthcare monitoring system, the security issue is critical to the successful application of such a system. The vital signals in wireless communications by nature are vulnerable to being eavesdropped. What's worse, the ill-minded invader could actively modify, inject or spoof the sensitive data. Therefore the importance of protecting the privacy and security of medical data is obvious because sensitive medical information must be protected from unauthorized use for personal advantages and fraudulent acts that might be hazardous to a person's life [3].

The privacy and security requirements for medical care are complex and scenario dependent. In addition to the general requirements of security in WSN, there have been three challenges to medical data security, briefly proposed in literature as follows [4]:

- How to ensure the privacy and integrity of the medical data, given that the wireless channel is easily subject to many forms of attack?
- How to ensure that only authorized people can access the data? The solution should scale to a large number of users (medical professionals, patients or relatives) and accommodate changes in the users.
- How to prevent someone from using captured sensors to recover sensitive medical information or inject false information?

This paper focuses on these challenges and intends to provide some contributions to solve the problem. In order to these problems, we choose the Elliptic Curve Cryptography (ECC)

which is one of the most famous asymmetric cryptographic algorithms. It has attracted considerable with the other widely used asymmetric cryptographic algorithm RSA. An elliptic curve Cryptosystem using a 160-bits key can provide the same security level with a 1024-bits RSA key [5]. We have applied symmetric algorithm to encrypt or decrypt some sensitive physiological data, and also use ECC to manage the key's distribution, update and revocation.

The rest of this paper is organized as follows. Section II presents the related work and in Section III, also presents about ECC cipher algorithm. In Section VI, we introduce our proposal scheme and VII discuss some analysis and conclusion.

2. Related Works

Evolution of wireless, medical and computer networking technologies have merged into an emerging horizon of science and technology called Wireless Body Area Networks (WBANs). However, applications of WBANs are not limited to medical field only. WBANs are also considered as an important branch of Wireless Sensor Networks (WSN) due to its appliances. In WBANs and WSNs, energy efficiency, mobility and localization of sensor nodes is an eye-catching issue to achieve better optimization of WSNs [6]. Also for security application, choosing best algorithms in terms of energy-efficiency and of small memory requirements is a real challenge because stringent resource-constrained devices such as WBANs and WSNs, the RAM space is very limited resource.

There is lot of work done on BSN authentication and key agreement schemes. Pan J. L. *et al.*, [7], has two modified Feistel algorithms called Simplified Feistel with no S-Box (SF_noSBox) and Simplified Feistel with S-Box (SF_Sbox) are applied to encrypt and decrypt the sensitive medical information. Also, includes compared these two algorithms with Data Encryption Standard (DES) in [1]. The results of experiments show that the SF_noSBox has poor avalanche effect for the reason of no S-Box operations, but SF_Sbox has the same avalanche effect as DES. Also two algorithms are much faster than DES because the procedures of encryption and decryption of SF_noSBox and SF_Sbox need only four-round computations but DES needs 16-rounds.

Pre-loaded symmetric shared keys are used in large scale sensor networks for geographical region observation [8-9]. In these techniques, a certain key is loaded in each node and used to derive a shared secret key. In [10] a secure-limited channel (*e.g.*, infrared) was used to exchange public-keys between parties before to the authentication process. However, the key management is difficult once these symmetric cipher methods are used. For such approach we need high memory and computational power which may not be always available in small device of BSN as explained above.

In [11] self-certified keys (SCK) and Elliptic Curve Cryptography (ECC) was used to establish asymmetric keys for authentication. Here KDC was used for key generation. Protocol called SNAP [4] also makes uses of ECC to set up pair-wise keys between nodes and the gateway. For which every sensor has biometric device which can authenticate the patient and shared secret is used for communicating with the base station. But, it does not set up any group keys. Lot of work has been done about ECC-based public-key cryptography [12]. It is best suitable for resource constrained devices.

3. Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) was proposed independently by Miller and Koblitz in the 80's [13]. In this paper, the prime finite field p is selected and an elliptic curve is defined as a set of points which satisfy $y2 = x3 + ax + b$, where $4a3 + 27b2 \neq 0$. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation

plus a point at infinity lies on the elliptic curve. For example, in the curve shown below in Figure 2, we have a = -4 and b = 0.67. The equation of curve now becomes y2 = x3 – 4x + 0.67.

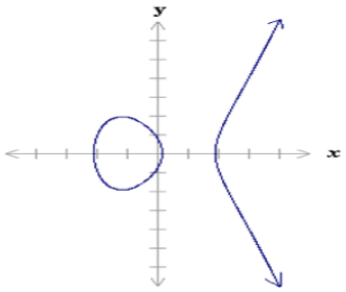

Figure 2. Elliptic Curve Graph for the Equation $y^2 = x^3 - 4x + 0.67$ [14]

ECC is one of the public key cryptography and the public key of ECC is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC. One main advantage of ECC is its small key size and a 160-bits key in ECC is considered to be as secured as 1024-bits key in RSA. It has attracted researchers' attention in recent years due to its shorter key length requirement comparing with RSA, especially in the domain of embedded systems where devices have limited computing power.

4. Proposed Scheme

A new encryption method based on ECC is presented in Figure 3. This method tries to use some symmetric algorithm to encrypt or decrypt some sensitive patient's medical data, and also use ECC to manage the key's distribution, update and revocation. This method combines the advantage of symmetric and asymmetric encryptions into a total scheme to fix the security issues in WBANs.

4.1. Notations and Assumptions

Table 1. Notations

$T=(P, a, b, G, n, h)$	P : The finite field in the elliptic curve a and b : elements in the finite field that the define the elliptic curve equation G : a point of the elliptic curve n : the order of the point G h : the divider of the number of elements of elliptic curve by n
K_{SB}	The secret key of base station
K_{PB}	The public key of base station
K_{SN}	The secret key of sink node
K_{PN}	The public key of sink node
KDF	Key derivation function
$HMAC$	MAC function
K_S	Parse the first left S-bits from KDF
K_M	Parse the right t-bits from KDF
M	Message
E	Encryption
D	Decryption

Table 2. Assumptions

The 6-tuple T is shared by sink node and base station in WBANs.
Base station establishes the Key Derivation Function (KDF), for KDF we use PBKDF2 with the option SHA-1.
Base station establishes the MAC scheme, which is HMAC with the option SHA-1.
Base station establish symmetric encryption scheme such as modified Feistel algorithm [7].
A sink node has more computational and communication ability than normal sensor node and it is a trusted and non-compromised node at which all legal sensors have to identify by it in advance.
A sink node obtain in an authentic manner the selection made by base station that are the elliptic curve domain parameters T, key derivation function, the HMAC scheme and the symmetric encryption scheme.

4.2. Second-order Headings

The sink node encrypts messages using ECC using the keys and parameters and the detailed procedures of encrypting and decrypting are explained in Figure 3.

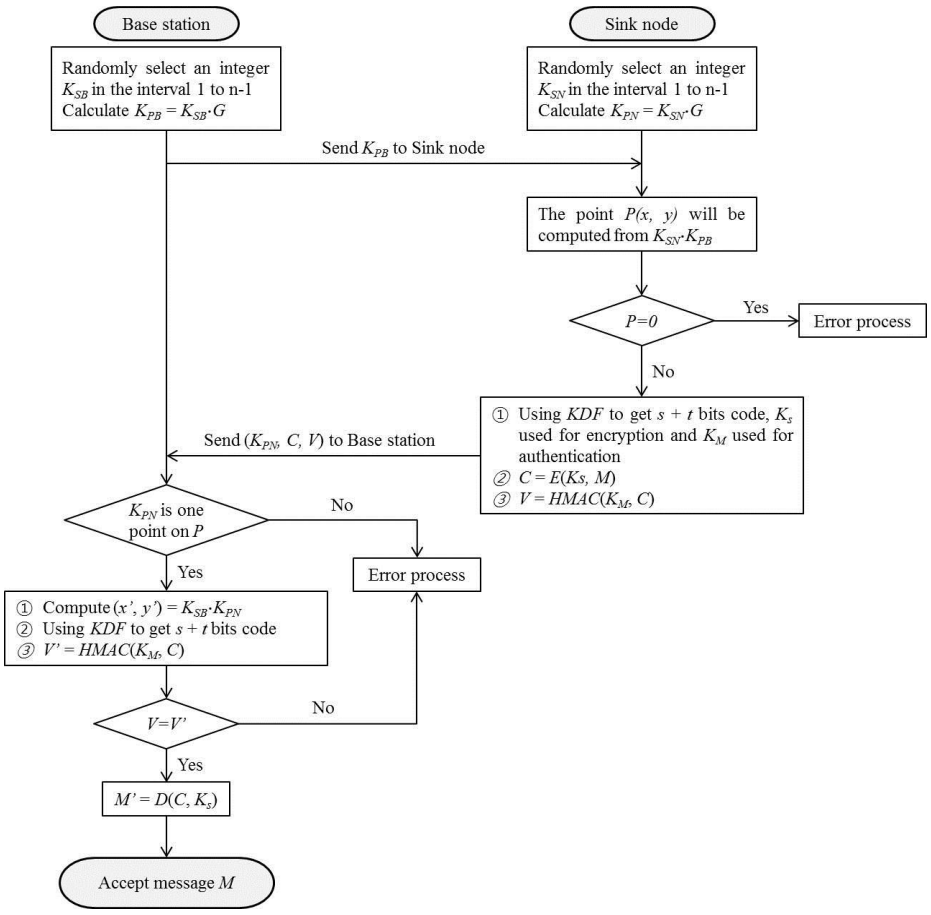

Figure 3. Flow Chart of Proposed Protocol

5. Analysis and Discussion

Ensure that information is not altered by unauthorized persons. If the cipher text has been altered by unauthorized user from C to C' and then in decryption process the value is

calculated other than D'. This alteration can be found at the time of verification process and the cipher text has been denied by base station to accept and hence integrity is ensured. To prevent man-in-the-middle attack, the sink node does not send the message containing his identity directly but in encrypted form of the data. So an adversary cannot decipher the text since he/she does not have private key of receiver which key pairs could be generated. Non-repudiation is the assurance that someone cannot deny something. That is sink node cannot deny that encrypted text is not sent by it. Any trust party or receiver himself can check that it is sent by the sink node by running the verification procedure through MAC code before decrypt the cipher text.

Also, after using encryption and decryption algorithms, the outside eavesdropping can be prevented by transmitting cipher text and the inside attacker cannot modify, inject and spoof any fault message into the networks easily. However, the problem of replay attacks remains to be solved as a focus of future work.

6. Conclusion

In this work, efficient encryption method based on elliptic curve cryptography (ECC) to protect patient's medical data in WBANs is proposed. This method used the symmetric cipher algorithm such as DES or modified Feistel algorithm to encrypt or decrypt sensitive patient's medical data and then use EDD to manage the key's distribution, update and revocation. ECC provides greater security and more efficient performance than the other cryptography techniques. Even though ECC which were used in our solution provide some valuable advantage s over other cryptosystems as RSA, the number of slightly different versions of ECC included in the standards may obstruct the adoption of ECC.

In our future work, we try to update overall process which includes digital signature and mutual authentication phase detail. In addition, we will find some solution for secure communication between the wearable heterogeneous sensors and the sink node.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant number: 2013-071188) and it also supported by the BB21 project of Busan Metropolitan City.

References

[1] J. Pan, S. Li and Z. Xu, "Security mechanism for a wireless-sensor-network-based healthcare monitoring system", IEEE Commun., vol. 6, no. 18, **(2012)**, pp. 3274-3280.
[2] L. Liu, Z. Zhang, X. Chen and K. Sup Kwak, May, "Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks", IEEE Transaction on Parallel and Distributed Systems, **(2013)**.
[3] N. Li, N. Zhang, S. K. Das and B. Thuraisingham, "Privacy preservation in wireless sensor networks, A state-of-the-art survey", Ad Hoc Networks, **(2009)**, pp. 1501-1514.
[4] K. Malari and P. Wang, "Addressing security in medical sensor networks", First ACM SIGMOBILE int. Workshop Systems and Networking Support for Healthcare and Assisted Living Environments, San Juan, Puerto Rico, (2007), pp. 7-12.
[5] N. Gura, A. Patel, A. Wander, H. Eberle and S. Shantz, "Comparing elliptic curve cryptography and rsa on 8-bit CPUs", Cryptographic hardware and embedded systems-CHES 2004: 6th International workshop, Cambridge, MA, USA, August 11-13, 2004: proceedings, Springer-Verlag New York Inc., vol. 6, **(2004)**, pp. 119.
[6] N. Javaid, S. Hayat, M. Shakir, M. A. Khan, S. H. Bouk and Z. A. Khan, "Energy Efficient MAC Protocols in Wireless Body Area Sensor Networks – A survey", Journal of Basic Applied Scientific Research (JBASR), **(2013)**.

[7] J. L. Pan, S. P. Li and D. Y. Zhang, "A Study of two algorithms based on feistel cipher in wireless medical sensor networks (in Chinese)", Chinese J. Sens. Actuators, vol. 23, **(2010)**, pp. 1030-1036.
[8] D. Liu, P. Ning and R. Li, "Establishing pair-wise keys in distributed sensor networks", ACM Trans. Inf. Sys. Secur. 2005, vol. 8, **(2005)**, pp. 41-77.
[9] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks", Proceedings of the 9th ACM conference on Computer and Communication Security, Washington, DC, USA, **(2002)**.
[10] D. Balfanz, D. Smetters, P. Stewart and H. Wong, "Talking to Strangers: Authentication in Ad-hoc Wireless Networks", Proceeding of Network and Distributed System Security Symp, San Diego, CA, USA, **(2002)**.
[11] C. Jiang, B. Li and H. Xu, "An efficient scheme for user authentication in wireless sensor networks", Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops, Niagara Falls, Canada, **(2007)**.
[12] H. Wang, B. Sheng and Q. Li, "TelosB Implementation of Elliptic Curve Cryptography over Primary Field", Technical Report WM-CS-2005-12, Williamsburg, VA, USA, **(2005)**.
[13] Y. Shou, H. Guyennet and M. Lehsaini, "Parallel Scalar Multiplication on Elliptic Curves in Wireless Sensor Networks", ICDCN, Mumbai, India, **(2013)**.
[14] B. Tiwari and A. Kumar, "Physiological Value Based Privacy Preservation of Patient's Data Using Elliptic Curve Cryptiography", Health Informatics – An International Journal (HIIJ), vol. 2, no. 1, **(2013)**.
[15] C.-T. Li, M.-S. Hwang and Y.-P. Chu, "An Efficient Sensor-To-Sensor Authentication Path-Key Establishment Scheme for Secure Communications in Wireless Sensor Networks", International Journal of Innovative Computing, Information and Control, ISSN: 1349-4198, **(2009)**.
[16] R. Markan and G. Kaur, "Literature Survey on Elliptic Curve Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 9, **(2013)**.
[17] K. Chok, M. Kim and K. Chae, "Secure and Lightweight Key Distribution with ZigBee Pro for Ubiquitous Sensor Networks", International Journal of Distributed Sensor Networks, article ID 608380, **(2013)**.
[18] Standards for Efficient Cryptography, SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV), version 1.0, **(2013)**.

Authors

Young Sil Lee, Lee received her B.S degree in Electrical engineering and the M.S. degree in Electrical engineering, both from the Dongseo University, Busan, South Korea in 2006 and 2010, respectively. Her research area covers security including healthcare system, RFID or WSN technologies. She is currently a Doctoral student of Ubiquitous IT at the Dongseo University, South Korea. She works also regularly as a Doctoral student at University of Oulu, Oulu, Finland.

Esko Alasaarela, received M.Sc. and Ph.D. degrees in Electrical Engineering from the University of Oulu, Oulu, Finland in 1975 and 1983, respectively. His research area covers biomedical engineering including wireless technologies. He is currently a Professor of Health and Wellness Measuring at the University of Oulu, Finland. He works also regularly as a Visiting Professor at Dongseo University, Busan, South-Korea. In addition, he is a founding partner in ZEF Solutions Ltd. and Domuset Ltd., innovative Internet service companies in Finland. Formerly he has also served as Research Director at the University of Jyvaskyla, and founder of Moistic Ltd. and High Technology Center Ltd. He is a member of the Finnish Association of Biomedical Engineering and Physics (since 1990).

Hoon Jae Lee, received the B.S., M.S. and Ph.D. degree in Electrical Engineering from Kyungpook national university in 1985, 1987 and 1998, respectively. He had been engaged in the research on cryptography and network security at Agency for Defense Development from 1987 to 1998. Since 2002 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor. His current research interests are in security communication system, side-channel attack, USN & RFID security. He is a member of the Korea institute of Information security and cryptology, IEEE Computer Society, IEEE Information Theory Society and etc.