Secure Medical Data Transmission by using ECC with Mutual Authentication in WSNs

Shashi Kant Shankar, Anurag Singh Tomar, Gaurav Kumar Tak*

Lovely Professional University, Phagwara 144411, India

Abstract

Wireless Body Area Network (WBAN) is a part of Wireless Sensor Network (WSN) which works with medical devices and capable to transmit medical data in run time. It has changed the healthcare industry and proved itself as the best technique in case of emergencies and remote area location. However, WBAN has witnessed several security issues which demand a secure data transmission and user authentication in resource constrained environment. Healthcare devices have resource constraints such as energy constraints, space constraints, etc. Implementing high level security is a daunting task due to those constraints. Proposed scheme implements Elliptic Curve Cryptography (ECC) for secure key distribution and data exchange. ECC provides same level of security by using lesser key size than RSA. Moreover, this scheme has mutual authentication of sink node by base station server and of base station server by sink node. It uses hash value of sink ID, registered random number and timestamp value for two-way authentication. Furthermore, proposed technique uses timestamp value to identify replay attack. Overall, it proves a better security mechanism in case of WSNs for healthcare devices.

Keywords: ECC; WSNs; WBANs; BANs; Mutual Authentication; Medical devices; Secure data transmission.

1. Introduction

Modern healthcare devices are capable to collect medical data such as blood pressure, heart beats rate, brain

* Corresponding author. Tel.: +91-9872431605.
E-mail address: shashi2y22@gmail.com; anuragtomar3105@gmail.com; gauravtakswn@gmail.com
liquid pressure, etc. by using sensors. These data can be transferred wirelessly for further processing and analysis. These medical devices use various sensors to sense medical data and network deployed for data transmission is Wireless Sensor Network (WSN). Wireless Sensor Network for medical devices is also known as Body Area Network (BAN) or Wireless Body Area Network (WBAN). Other applications of WSNs are in Traffic Control, Logistic and Transportation, Home and Office, Security and Surveillance, Tourism and Leisure, Education and Training15, etc. WBAN includes sink nodes and base station. Sink nodes are the sensors which are used inside medical devices. Moshaddique Al Ameen, Jingwei Liu, Kyngsup Kwak, et al.15 describes these medical devices into two categories, one is Implantable devices and other one is Wearable devices. Implantable devices like Brain Liquid Pressure, Endoscopic Capsule, etc. are implanted inside body through surgery. Wearable devices like Blood Pressure Monitor, Heart Beats Rate Monitor, Glucose Sensor, etc. are attached with body. Base stations are always situated at central location including server, motes and transmitter.

Wireless Sensor devices have some constraints like resource and energy constraints3. Issues faced in WSNs can be classified as Security, Privacy and Illegal issues. The major concern of WBAN is Security issues due to high sensitiveness level of medical data17,19. Unauthorized or illegal access of medical data may cause harm, even may lead to death of individuals14. Apart from the above mentioned three issues, other issues are Economic, Political, Psychological, Socio-political, etc. Authors have proposed many security approaches towards secure data transmission in WBAN but those approaches are still needed some improvements and revisions. One of the security techniques implements Elliptic Curve Cryptography (ECC)4,20 for key distribution with any of the available symmetric algorithms for secure data transmission. Although, this approach is unable to resolve replay attack and mutual authentication between sink node and base station. Our proposed scheme is to resolve the above described issues by implementing ECC and some computational steps involved in mutual authentication. It includes registration of every sink node to the central server which generates unique sink ID and a random number. These two parameters with timestamp value is used to generate hash code for two-way mutual authentication. Structure of the remaining paper is as follow: section 2 presents related work, section 3 contains Elliptic Curve Cryptography (ECC), section 4 deals with proposed scheme, section 5 describes system implementation and section 6 discusses analysis, conclusion and future work.

2. Related Work

Now a days, Wireless Sensor Network for medical devices is one the most prominent areas of research16. It includes numerous devices which fall in the category of either Wearable or Implantable devices containing different type of sensors. Those sensors collect different medical data like blood pressure, heart beats rate, arrhythmic rate, brain liquid pressure, etc. JeongGil Ko, Chenyang Lu, Mani B. Srivastava, et al.14 described that those devices are configured to transmit medical data in case of any irregular change which is identified in the pattern of collected data. Transmission of the data is possible by WSNs. Every device transmits its data to its controller module which is available in the mobile phones, PDAs, etc. of patients. These communication devices transmit data further to central location by using carrier medium like GPRS, Edge, etc. Central location set up is in hospital including servers and central repository. It transmits data further to the concerned doctor or designated professionals specific to either patient or data. The overall architecture is technically described as Wireless Body Area Networks (WBANs) or simply Body Area Networks (BANs). This technique is very useful in case of emergencies, remote locations, hilly areas, etc. It helps doctors who can assist their patients based on data without approaching them physically and can save life in case of emergencies. Critical diseases which need ultimate care like Parkinson, Heart Rate Problems, etc. can be easily monitored from home.

WBAN sounds perfectly fine in terms of use but it involves some concerns. Samaneh Movassaghi, Mahyr Shirvanimoghaddam, et al.8 described one of the most important concerns as Physical concern which is related to resource and energy consumption. Devices used in WBANs are very small in size so they can’t hold a big batteries and memory chips. Therefore, powerful and extremely secure applications can’t be injected in those devices. Concerns are mainly grouped into three different categories such as Security, Privacy and Legal issues13,15. Other categories can also exist like social, political, economic, etc. Security issue is the most prioritized issue which needs to be resolved. Security concern covers data transmission problem which includes replay attack, man-in-middle attack, data loss, etc. as described by Da-Zhi Sun, Jian-Xin Li, et al10.
WBAN consists sink nodes, these sink nodes are healthcare devices available to patients and base station (which is responsible for data handling and transmission control). Base station may include central server which may act as central data repository. Data transmission between sink nodes and base station is more vulnerable for different kind of security attacks\(^1,2,6,7,8,9,12\). Although, those known attacks can be restricted if we implement any of the extremely secure and advanced cryptographic algorithms but as we have discussed above, devices have resource constraints which make them unable to process high computation. Therefore, security concern is still an area where we have to find a suitable approach in available resources only\(^1,5,8,11,14\). Young Sil Lee, Esko Alasaarela, et al.\(^4\) and K. Malhotra, S. Gardner, et al.\(^18\) have proposed one approach which is implemented using Elliptic Curve Cryptography (ECC) for secure key distribution and data transmission. ECC resolves the above discussed issues in a resource constrained environment. However, implementation of ECC arise the problem of replay attack and mutual authentication issue between sink node and base station which we have tried to resolve in our proposed work.

3. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is an asymmetric cryptographic algorithm. It is one of the most secure algorithms which includes very few computations and a very small key size, but achieves better security than other algorithms which include heavy computations and large key size. ECC provides same level of security with 112-bit key size in contrast to RSA with 512-bit key size. ECC encodes any message in form of co-ordinates on any plane curve. That plane curve is based on any cubic curve equation. ECC was proposed by Neil Koblitz and Victor Miller in 1985. Common equation of elliptic curve is \(y^2 = x^3 + ax + b\). Computations (which are involved in ECC) follow different steps for compute the results. Addition of two points on the curve is the reflection of intersecting point generated by the straight line passing through those two points. Multiplication is the repeated addition of points. Encoding of message in form of points on curve has powerful security because of computations.

4. Proposed Scheme

Proposed scheme implements Elliptic Curve Cryptography (ECC) for secure medical data transmission and key distribution. It has been proved that ECC is a better asymmetric algorithm than RSA due to level of security achieved by using small key size. Previously, proposed approach\(^4\) has used ECC, but replay attack and mutual authentication was major concern in that approach. Our proposed technique use ECC approach for secure data transmission and resolve these issues.

Replay attack issue can be resolved using time stamp value. This value would enable receiver to identify the status of message. Real message would contain current time whereas replay attack message would contain old time. Apart from replay attack issue, mutual authentication is one of the most important requirements in WBANs due to the privacy and security concern of data. Proposed technique describes that Sink node would authenticate the base station server before actual transmission of medical data and base station server would also authenticate the sink node before any actual reply. However, devices are having resource constraints, so large computations cannot be performed because they may slowdown the overall performance. Our technique involves some computations as in Table 1. It includes two way authentication with time stamp value where every sink node would be registered with the base station.

| Table 1. Mutual authentication steps |
|-------------------------------------|
| **Sink node** | **Base station server** |
| Compute H(ID R) RsK ID and send | Segregate H(ID R), RsK and ID from received message |
| | Fetch R from database based on ID |
| | Compute H(ID R) and compare with received H(ID R) |

| | |
|-----------------|-----------------|
| Compute H(ID R R RsK) | Compute H(ID R R RsK) |
The Notations used in this paper are defined as follows:

| Symbol | Definition                      |
|--------|---------------------------------|
| ID     | Unique ID for every sink node   |
| R      | Registered random number        |
| RsK    | Timestamp value                 |
| H(.)   | Hash Function                   |

4.1. Registration phase

Every medical device would be directly connected, handled and controlled by the application running in patient’s gadget. The application running on any of the gadgets would be registered for every medical device with patient’s unique registration number and every device would have registered sink ID and random number provided by hospital authorities; ex. there is a patient having registration number R001. Doctors prescribe him or her with Blood Pressure Monitor and Endoscopic Capsule. Both the devices are connected to patient’s mobile phone where application is running to handle the devices and medical data. Hospital staff registers both devices with patient’s unique registration number. It generates two pairs of unique sink IDs and random numbers; one pair for Blood Pressure Monitor and another pair for Endoscopic Capsule. Both pairs of data are registered on behalf of single patient registration number R001. Therefore, every device which is used as a sink node gets its own ID and R individually. ID and R is known only to designated sink node and base station server from where it has been generated and registered. This registration process is secure because registration is only possible by authorized staffs of hospital and can be only done within hospital network so, there is no chance of malicious registration. After that whenever sink node wants to communicate with the base station, both have to follow the process of mutual authentication with timestamp value. This process is applied in both cases either sink node is in hospital network or outside hospital network.

Sink node initiates the computation for communication and computes hash value of its ID and R as H (ID || R). Further, H (ID || R) is concatenated with RsK (timestamp value) and ID. After that sink node transfers the overall data (H (ID || R) || RsK || ID) to base station. Base station receives and segregates the received data in three parts as
H (ID || R), RsK and ID. It checks its RsK for validation of message time which helps to identify replay attack. Furthermore, it fetches random number R corresponding to that ID from database. Then, it calculates H (ID || R) and matches it with received H (ID || R), if both are same, means that sink node is authenticated otherwise it would discard the request. After successful authentication of sink node, it computes H (ID || R || RsK) and transfers the same to sink node. On the other hand, sink node also computes H (ID || R || RsK) and compares it with received data, if both are same, means base station server is authenticated.

Sink node is authenticated, it can be determined by server because R is only known to designated sink node during registration. Therefore, same hash value cannot be send by any other node. Moreover, Base station server is authenticated, it can be determined by sink node because R is only known to base station except designated sink node. Other parameter RsK which has been sent by sink node to base station server is also included in hash value returned by base station to sink node so, matching hash value determines that base station server is also authenticated. Implementation of the proposed work is in Fig. 1.

4.2. Key generation and data encryption

Proposed scheme includes ECC for secure key distribution and data transmission. Involved steps in this are shown in Table 2. Number of computational steps involved is very less but security is very high because of message encoding in form of points on curve which is not easy to decode. Let us consider an example with general equation of Elliptic curve as \( y^2 = x^3 + ax + b \). Both sender and receiver will agree on some common parameters and both will select their private key as in Fig. 2. So, suppose Bob is sender and Alice is receiver. Both have agreed on values of a=-1, b=188, prime number=751 and coordinates of base point as x=0 and y=376. Alice and Bob have selected their
private keys as 5 and 8 respectively. So public keys for Alice and Bob has been calculated as (188, 657) and (121, 129) respectively. Next step in ECC is to encode the message on points which are situated on the curve. Encryption of those points with the help of a random number and base point will be processed accordingly. Let us take a message M as 11. By using a random number 20, message M will be encoded on the curve with coordinates (224, 248). After that, point (224, 248) will be encrypted by using another random number 40 and can be decrypted in same manner also. Encryption and decryption can be also analysed from Fig. 3.

Table 2. ECC steps

| User A (Sender) | User B (Receiver) |
|-----------------|-------------------|
| Common Parameters Agreement | Common Parameters Agreement |
| Equation: $y^2 = x^3 + ax + b$ | Equation: $y^2 = x^3 + ax + b$ |
| Prime Number | Prime Number |
| Base Point $B_{(x,y)}$ | Base Point $B_{(x,y)}$ |
| Co-efficient value ‘a’ and ‘b’ | Co-efficient value ‘a’ and ‘b’ |

Key Generation

- Select Private Key $PR_a$
- Calculate Public Key $PU_a$

Where multiplication in Elliptic Curve is repeated addition.

Encoding of Message ‘M’ on Elliptic Curve as $P_a(x,y)$

$x = (M \times k) + i$

where $k$ is any random value and $i$ will vary from 1 to $k-1$

Put value of $x$ in equation $y^2 = x^3 + ax + b$ and find integral value of $y$. If integral value is not found then again calculate $x$ by incrementing the value of $i$.

Encryption of Message $P_a(x,y)$

Select any random value $R$ where $R \in (1, p - 1)$

Cipher Text $CT((x_1, y_1), (x_2, y_2))$ is computed as

$CT = [(R \times B_{(x,y)}) \times P_a(x,y) + R \times P_a(x,y)]$ $CT = R \times P_a(x,y)$

Decryption of Cipher Text $CT((x_1, y_1), (x_2, y_2))$

Compute $P = R \times B_{(x,y)}$ i.e. $(P \times R \times B_{(x,y)})$

Compute $CT(x_1, y_1) \cdot (P \times R \times B_{(x,y)})$ i.e.

$(P \times P_a(x,y) + R \times P_a(x,y)) \cdot (P \times R \times B_{(x,y)})$

Now, $P_a(x,y)$ has been received.

Calculate $M$ as

$M = \text{Floor}(\frac{(x - 1)}{k})$

5. System Implementation

Proposed scheme has been implemented in C# on .NET framework 4.5 using Visual Studio 2012 IDE. We have used Windows Forms Application which is a very lightweight application. SQL Server 2008 has been used as the back-end environment for data management. Connectivity of front-end and back-end has been done by using ADO.NET. The complete snapshots as in Fig 1, 2 and 3 have been taken from same environment and has been also tested on Microsoft ActiveSync Emulator. In that environment this application runs seamlessly. So this implementation also states that it is suitable for resource constraint environment. Underlying hardware used for the above implementation is as follows. 4th Gen Intel i5 Processor with processing capability of 2.50GHz. 4GB RAM with 64-bit Windows 8.1 single-language OS having Microsoft Visual Studio Location Simulation Sensor used for
working of ActiveSync. The proposed application is also able to run on modern smart phones having Windows 8 or above OS windows family.

6. Conclusions and Future Work

It has been observed and analysed from the implementation of ECC and proposed technique that the existing problems (problem of replay attack and mutual authentication) have been resolved. ECC has been proved as the best cryptographic technique for secure data transmission in a resource constrained environment.

Mutual authentication has been proved as the best technique for securing unauthorized access of medical data. Medical data is very sensitive in nature which demands a very secure architecture. 2-way authentication and in just 2 steps has enhanced the overall security architecture of Wireless Sensor Networks for healthcare applications.

In Future work, researchers can propose new scheme which can reduce the included computation of the proposed scheme. As we can see that proposed scheme computes hash value four times. However, it is not too much high as time complexity but still needs some revision for better performance on devices containing less memory. Another aspect which can be done as the implementation of revised approach by using J2ME which is more suitable for such devices.

References

1.  Meng Zhang, Anand Raghunathan, Niraj K. Jha. Trustworthiness of medical devices and body area networks. IEEE; 2014
2.  YataoYang, Shuang Zhang, Jhuming Yang, Jia Li and Zichen Li. Targeted fully homomorphic encryption based on a double decryption algorithms for polynomials. Tsinghua science and technology. Vol-19; 2014
3.  Tao Yang, Dejun Mu, Wei Hu and HuiXiang Zhang. Energy-efficient border intrusion detection using wireless sensors network. Springer; 2014
4.  Young Sil Lee, Esko Alasaarela, Hoon Jae Lee. An efficient scheme using elliptic curve cryptography (ECC) with symmetric algorithm for healthcare system. International journal of security and its applications; 2014
5.  Anurag Singh Tomar, Gaurav kumar Tak, R. Chaudhary. Image based authentication with secure key exchange mechanism in cloud. International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom); 2014
6.  Luhach Ashish Kr., Dwivedi Sanjay k. Designing and Implementing a logical Security Framework for E-commerce System based on Service Oriented Architectures. International journal of Advanced Information Technology; 2014
7.  Luhach Ashish Kr., Jha C. K., Dwivedi Sanjay k. Designing a logical Security Framework for E-commerce System based on Service Oriented Architectures. International journal of Soft Computing; 2014
8.  Samaneh Movassaghi, Mahyr Shirvanimoghaddam, Mehran Abolhasan, David Smith. An energy efficient network coding approach for wireless body area networks. IEEE; 2013
9.  Tsung-Chih Hsiao, Yu-Ting Liao, Jen-Yan Hunag, Tzer-Shyong Chen, Gwo-Boa Horng. An authentication scheme to healthcare security under wireless sensor networks. Springer; 2012
10. Da-Zhi Sun, Jian-Xin Li, Zhi-Yong Feng, Zhen-Fu Cao, Guang-Quan Xu. On the security and improvement of a two-factor user authentication scheme in wireless sensor networks. Springer; 2012
11. Anurag Singh Tomar, CD Jaidhar, S Tapaswi. Secure Session Key Generation Technique for group communication. International journal of information and electronics engineering; 2012
12. Rong FAN, Dao-jing HE, Xue-zeng PAN, Ling-di PING. An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks. JZUS; 2011
13. Gokhroo, M.K., CD Jaidhar, Anurag Singh Tomar. Cryptanalysis of SIP secure and efficient authentication scheme. IEEE 3rd International Conference on Communication Software and Networks (ICCSN); 2011
14. JeongGil Ko, Chenyang Lu, Mani B. Srivastava, John A. Stankovic. Wireless Sensor Networks for Healthcare. IEEE; 2010
15. Moshaddique Al Ameen, JingweiLiu, Kyngsup Kwak. Security and privacy issues in wireless sensor networks for healthcare applications. Springer; 2010
16. G. Virone, A. Wood, L. Selavo, Q. Cao, T. Daon, Z. He, R. Stoleru, S. Lin, and J. A. Stankovic. An advanced wireless sensor network for healthcare monitoring. Department of computer science. University of Virginia; 2009
17. J. A. Stankovic, Q. Cao, T. Doan, L. Fang, Z. He, R. Kiran, S. Lin, S. Son, R. Stoleru, A. Wood. Wireless sensor networks for in-home healthcare: Potential and challenges. Department of computer science. University of Virginia; 2008
18. K. Malhotra, S. Gardner, R Pitz. Implementation of elliptic-curve cryptography on mobile healthcare devices. IEEE; 2007
19. Aleksander Milenkovic, Chris Otto, Emil Jonanov. Wireless sensor networks for personal health monitoring: Issues and implementation. Elsevier; 2006
20. Liu Duo, Song Tao, Dai Yiqi. Isomorphism and generation of Montgomery-form elliptic curves suitable for cryptosystems. Tsinghua science and technology; 2005