Indonesian Journal of Electrical Engineering and Computer Science
Vol. 11, No. 1, July 2018, pp. 256~262
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v11.i1.pp256-262

Robust Security for Health Information by ECC with Signature Hash Function in WBAN

G. Sridevi Devasena, S. Kanmani
Indian Maritime University, Chennai Campus, India
Department of Information Technology, Pondicherry Engineering College, Puducherry, India

Article Info

Article history:

Received Dec 04, 2017
Revised Jan 11, 2018
Accepted Apr 15, 2018

Keywords:

Elliptical curve cryptography
Hash function
Key management
One time password
Security
WBANs

ABSTRACT

Wireless Body Area Networks (WBANs) are fundamental technology in health care that permits the information of a patient's essential body parameters to be gathered by the sensors. However, the safety and concealment defense of the gathered information is a key uncertain problem. A Hybrid Key Management (HKM) scheme [13] is worked based on Public Key Cryptography (PKC)-authentication scheme. This scheme uses a one-way hash function to construct a Merkle Tree. The PKC method increase the computational complexity and lacking scalability. Additionally, it increases expensive computation, communication costs and delay. To overcome this problem, Robust Security for Protected Health Information by ECC with signature Hash Function in WBAN (RSP) is proposed. The system employs hash-chain based key signature technique to achieve efficient, secure transmission from sensor to user in WBAN. Moreover, Elliptical Curve Cryptography algorithm is used to verifies the authenticate sensor. In addition, it describes the experimental results of the proposed system demonstrate the efficient data communication in a network.

Corresponding Author:

G. Sridevi Devasena,
Indian Maritime University, Chennai Campus, India
Email: sridevigphd@gmail.com

1. INTRODUCTION

Wireless Body Area Networks (WBANs) are expected to play a significant role in the field of patient-health monitoring, which gains tremendous attention amongst researchers in recent years. One of the challenges is to establish secure communication architecture between sensors and users, while addressing the common security and privacy concerns [1]. Unfortunately, patients concerns on potential leakage of personal health records (PHRs) are the biggest stumbling block. In current eHealth/mHealth networks, patients' medical records are usually associated with a set of attributes like existing symptoms and undergoing treatments based on the information collected from portable devices [2]. To guarantee the authenticity of those attributes, PHRs should be verifiable. However, due to the linkability between identities and PHRs, existing eHealth systems fail to preserve patient identity privacy while providing medical services. However, due to the intrinsically open nature of wireless communications and dynamics of cellular networks, D2D communications are vulnerable to security attacks such as eavesdropping, fake message, privacy violation, etc. Currently, security for M-Health systems has attracted extensive attentions [5].

A Secure Medical information communication [3] equipment ECC for protected key sharing and data exchange. ECC offers the same level of security by using lesser key size than RSA. Secure logging of events [4] by gathering in a safe and reliable way all information at one central point. The system assures the sequential order of logged events sent by the different sensors. This protocol is responsible for the secure logging and the secure transmission of medical information.

Ciphertext-Policy Attribute Based Encryption (CP_ABE) [5] and signature to store the data in ciphertext format at the data sink, hence ensuring data security. This scheme provides the security between sensors and the doctors. However, this system creates additional communication, computation overhead, and it expensive method in a WBAN. Lightweight and Robust Security-Aware (LRSA) [6] data communication protocol for M-Health systems by using the certificateless signcryption technique. An efficient Certificate Less Generalized SignCryption (CLGSC) scheme that can adaptively work as one of the three cryptographic primitives: signcryption, signature, or encryption. However, it cannot function well in M-Health systems.

Secure Authentication technique [7] to recognize the security issues in the existing authentication protocols for patient monitoring and presents a lightweight public-key-based authentication protocol for MSNs. The sensor nodes are reported about the human body and actuators that receive commands from the medical staff and perform actions. The Rabin authentication algorithm improved signature signing process and it suitable for delay-sensitive MSN applications.

Certificateless Remote Anonymous Authentication scheme [8] used to enable remote WBAN users to anonymously healthcare service. The certificateless signature (CLS) scheme provides security against forgery on adaptively chosen message attack in the network. The network manager that serves as a private key generator in the authentication protocols, is prevented from impersonating legitimate users. Privacy-preserving attribute-based authentication system [9] leverages users verifiable attributes to authenticate each other while preserving attribute and identity privacy. Lightweight encryption framework [10] provides secure information based on the use of the measurement matrix as an encryption key. It eliminates the need for a separate encryption algorithm as well as the pre-deployment of a key. This scheme provides legitimate communication is reliable and secure given that the eavesdropper is located at a reasonable distance from the sensor-node and the access point.

Mutual Authentication and Key Agreement Scheme [11] demonstrated session key and protests many attacks. However, it has security failings. The security of the session key established between user and SNs is imperfect due to lack of forwarding secrecy and session-specific temporary information leakage attack. Additionally, it creates extra computational overhead and it does not work user-friendly due to an absence of user anonymity and require of password change facility.

1.1. Contribution of the Work

a. The main objective of RSP method is to access the patient information from the authenticated sensor and communicates the original patient information to the user.
b. In RSP, identify the authenticated sensors using ECC key verification based on wierstrass equation.
c. It proposes a hash-chain based key signature technique protects the data from the Denial of Service attack, thereby reducing communication overhead.

2. RESEARCH ROBUST SECURITY FOR HEALTH INFORMATION BY ECC WITH SIGNATURE HASH FUNCTION IN WBAN

Here, the sensor nodes are disseminating the patient health information to the user. This system consists of three entities such as a patient, user, System Administrator (SA), record table, and a mobile phone. Figure 1 shows that the architecture of the RSP scheme.

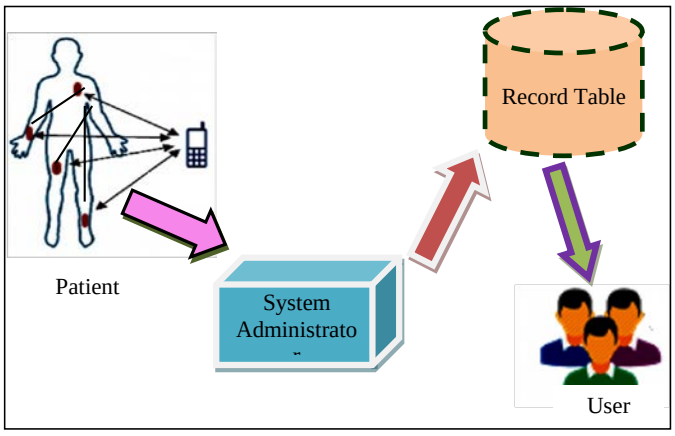

Figure 1. Architecture of RSP Scheme

Patient: The patient consists of the number of sensors for measure the blood pressure, sugar, temperature, ECG, pulse, oxygen and so on. *System Administrator (SA):* SA is an important unit in the network system owing to it act as a key distribute centre. It contains the public and private key of a sensor node for security purpose. The sensor node gets or sends the information to next sensor using these keys. *User:* user represents the doctor, nurse or particular person. These members registered to the SA before serving the patient.

The patient sensor needs to reports his Protected Health Information to user whereas it is not capable of achieving SA straightly. So the sensor sends the information via the number of relay node to reach the user. Thus, provide the security for forwarding PHI information is the significant factor in WBAN because of eavesdropper hack the patient health status and modified. To solve this problem, we propose Robust Security for Protected Health Information in WBAN to provide data confidentiality and data integrity. In this scheme, data privacy to protect Health Information from informative the source secrecy information when data integrity to make sure the information is not modified throughout the data communication in the WBAN. If the eavesdropper is available in this system, the algorithm is providing the security to the health information.

The Elliptic Curve Cryptography (ECC) is a better approach to public-key cryptography method to verify the node authentication and Hash function [12] with OTP method to achieve strong robustness against eavesdropping attacks. The proposed scheme contains 3 steps such as Registration phase, Sensor Node Verification, and Data Transmission Phase.

2.1. Registration Phase

In this scheme, the SA acts as the authorized person. Initially, the sensor node and user register to the SA for connecting the network. Then the SA assigns the sensor to a corresponding to a user. The user has the privilege to access its sensor node. The SA stores the sensor Id and location in a record table.

2.2. Sensor Node Verification Phase

The sensor verification function is used to detect the malicious sensor in BAN. In this phase, the SA verifies the sensor node based on ECC algorithm utilizing the wierstrass equation. The ECC utilized the wierstrass function is given below. Regard the coordinate points of the source S and System administrator R and another point K that forms a line.

$$v^2 = u^3 + au + b$$

$S+R=K$ where $S \neq R$ and $\square\ S, R, \epsilon, E$

Here (x_s, y_s), $(x_R, y_R)(x_k, y_K)$ are the coordinates of the source S, System administrator R and K points making an Elliptic curve. The coordinates (x_k, y_K) received from the following equations

$$x_K = \gamma^2 - x_S - x_R$$

$$y_K = \gamma(x_S - x_K) - y_S$$

Where $\frac{y_R - y_S}{x_R - x_S}$

The commutative law is defined as,

$S+R=R+S$

2.3. ECC Algorithm

```
ECC_Check ()
{
Source sends REQ to the next Relay node R
Source S computes forward key FK←S+R;
R replies with computing RK←R+S
if (FK!=RK){
    Eliminate R from neighbour list
    Disseminate R is 'malicious' to all nodes
 Else {
    Source sends the data to R
```

} end
The source computes the Forward Key FK computation is given below.
F_K= S+R
The SA calculate the Reverse key calculation is given below
R_k= R+S

These two keys are match, the SA stores the record table otherwise, it broadcast the notification message to the network.

2.4. Data Transmission

The sensor wants to transmit the data to user, and it protects the data from the Denial of Service attack, the OTP key is added to the signature packet. The OTP, Rn is attached to the payload of the signature packet d||sign (H(d)). Next employed the hash function to the payload of the signature packet d||sign (H(d))|| Rn|| OTP and it sends to the SA.

The OTP computation equation (1) is given.

$$OTP = \log_2 S_{ID}^{R_n} \quad (1)$$

Where: R_n=random number
S_{ID}=Sensor Identity

The SA gets the message from the source and it verifies the OTP. If it matches, the SA sends the information to the particular user. The user obtained the message from the SA and it checks the sensor signature. The signature is valid it accepts the message otherwise it discard.

Figure 2 shows that the flowchart of the proposed scheme. This scheme initially, sensors and users registered to the SA. The sensor wants to transmit the patient data to user, the SA first check the sensor forward key and reverse key, if the key is the match then the sensor is authenticated. Otherwise, that sensor is malicious and SA sends a notification message to all sensor nodes. The authenticated sensor sends the signature payload data to user via SA then verified the sensor OTP. The OTP is valid, the SA send the data to user else discard the packet. The user gets the sensor message and checks the signature. If the signature matches accept the sensor data and proceed the treatment process otherwise it rejects the sensor data.

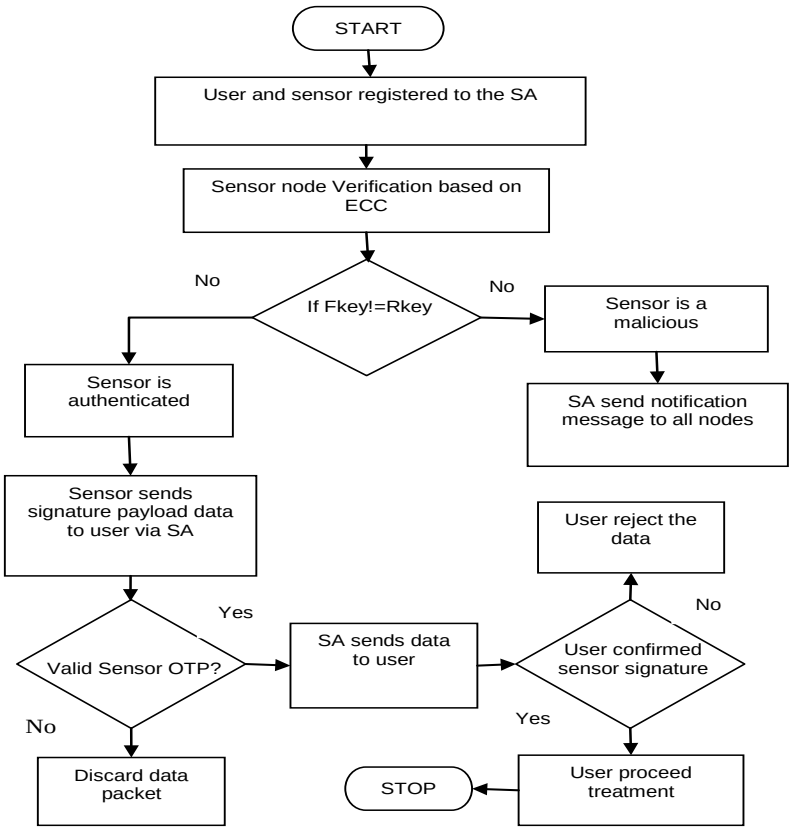

Figure 2. Proposed System Flowchart

3. RESULTS AND ANALYSIS

The simulation analysis is done using the Network Simulator tool (NS-2). The existing scheme HKM and the proposed RSP scheme are analysed and compared with the simulation results. The network traffic in the simulation prototype is handled using traffic model Constant Bit Rate (CBR). The parameters used for the simulation of the proposed scheme are tabulated below. The performance of the proposed scheme is evaluated by the metrics packet delivery rate, delay, packet loss rate and throughput.

Table 1: Simulation Parameters of RSP

Variable	Speed (rpm)
Channel Type	Wireless Channel
Simulation Time	100s
Number of Nodes	15
MAC Type	802.11
Traffic Model	CBR
Simulation Area	500x500
Transmission Range	10m
	WirelessPhy

3.1. Packet Delivery Rate

Packet delivery rate is defined as number of packets reached by the destination to the total packet sent by the source node. PDR can be measured using the equation (2).

$$PDR = \frac{Packets\ Rcvd\ in\ total}{Total\ Packets\ sent} \quad (2)$$

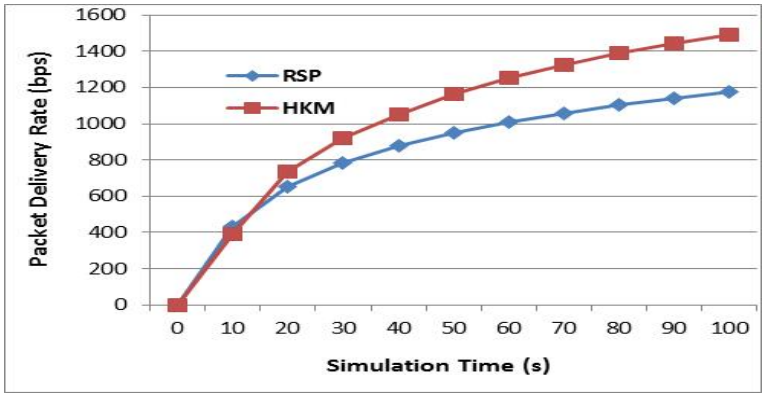

Figure 3. Packet Delivery Rate

The packet delivery rate of the proposed scheme RSP is higher than the packet delivery ratio of the existing methods HKM which is shown in the Figure 3. The more prominent estimation of packet delivery rate implies the better execution of the protocol. It shows that the proposed scheme RSP has 26.75% better PDR when compared to the existing HKM.

3.2. Packet Loss Rate

Packet Loss Rate (PLR) is the ratio between the packets dropped to the packet sent and it can be measured using the equation (3)

$$PLR = \frac{Packets\ dropped\ in\ total}{Total\ Packets\ sent} \quad (3)$$

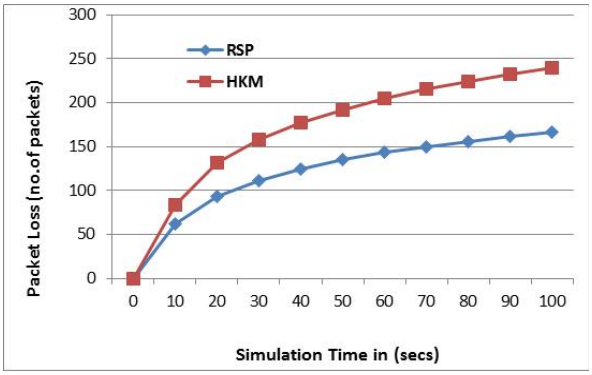

Figure 4. Packet Loss Rate

The packet loss rate of the proposed scheme RSP is lower than the existing HKM method which shown in Figure 4. Lower the packet loss proportion demonstrates that higher execution of the network. Figure 4 indicates that PLR of RSPis greater by 43.97% when compared to that of HKM.

3.3. Average Delay

The delay is defined as the time contrast between the present packets received and the previous packet received. It is calculated by the equation (4).

$$Delay = \frac{\sum_{0}^{n} PktSendTime - Pkt\,\mathrm{Re}\,cvTime}{Time} \quad (4)$$

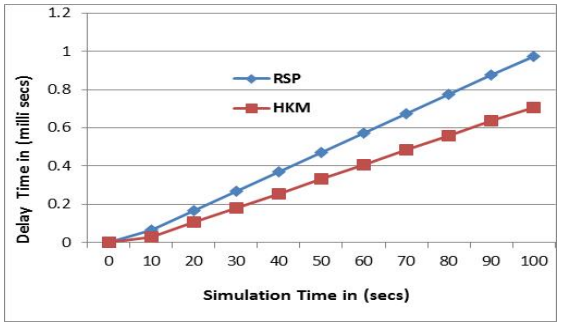

Figure 5. Average Delay

The delay value is low for the proposed scheme RSP than the existing method HKM is shown in Figure5. The base estimation of delay implies that higher estimation of the throughput of the system. The graph reveals that the RSP has 37.16% lower delay for a node when compared to the HKMscheme.

3.4. Throughput

Throughput is characterized as the average of successful or effective messages delivered to the destination. The average throughput is estimated using equation (5):

$$Throughput = \frac{\sum_{0}^{n} PktsReceived(n) * PktSize}{1000} \quad (5)$$

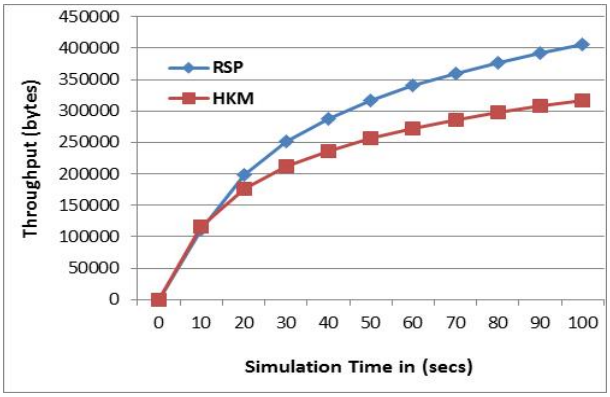

Figure 6. Throughput

The proposed scheme RSP has higher average throughput when compared to the existing scheme HKM is shown in Figure.6. It can be observed from the graph explains that the number of packets received successfully for every 1000 packets for RSP is greater than 21.89% compared to that of the HKM mechanism.

4. CONCLUSION

Robust Security for Health Information by ECC with signature Hash Function in WBAN (RSP), is proposed in this paper. It significantly developed to eliminate the eavesdropping attack and access the patient information from the authenticated sensor. The Elliptical Curve Cryptography algorithm is used to verify the authenticated sensor. Especially, this scheme using hash-chain based key signature technique to achieve efficient, secure transmission from sensor to user in WBAN. Our simulation results explain that the RSP protocol can reduce packet loss rate by up to 43.9 % when compared to the HKM protocol. Also RSP improves the network throughput and packet delivery rate in a network. Thus the RSP protocol provides data confidentiality, authentication and secure data transmission in a WBAN.

REFERENCES

[1] Xie Z, Huang G, He J, Zhang Y, "A clique-based wban scheduling for mobile wireless body area networks". *Procedia Computer Science*. 2014; 31:1092-1101.
[2] Al-Janabi, S, Al-Shourbaji, Shojafar M, Shamshirband S, "Survey of main challenges security and privacy) in wireless body area networks for healthcare applications", *Egyptian Informatics Journal*.2016.
[3] Shankar S K, Tomar AS, Tak G K. "Secure medical data transmission by using ECC with mutual authentication in WSNs". *Procedia Computer Science*, 2015; 70: 455-461.
[4] Braeken A, De La Piedro A, Wouters K. "Secure event logging in sensor networks". In *European Public Key Infrastructure Workshop*. Springer Berlin Heidelberg.2011: pp. 194-208.
[5] Hu C, Li H, Huo Y, Xiang T, Liao X. "Secure and efficient data communication protocol for wireless body area networks". *IEEE Transactions on Multi-Scale Computing Systems*, 2016; 2(2): 94-107.
[6] Zhang A, Wang L, Ye X, Lin X., "Light-weight and robust security-aware d2d-assist data transmission protocol for mobile-health systems". *IEEE Transactions on Information Forensics and Security*, 2017; 12(3): 662-675.
[7] Hayajneh T, Mohd B, Imran M, Almashaqbeh G, Vasilakos A. "Secure Authentication for Remote Patient Monitoring with Wireless Medical Sensor Networks". *Sensors*. 2016; 16: 424: 1424-8220.
[8] Liu J, Zhang Z, Chen X, Kwak K S. "Certificateless remote anonymous authentication schemes for wireless body area networks". *IEEE Transactions on Parallel Distributed Systems*. 2014; 25(2); 332-342.
[9] Guo L, Zhang C, Sun J, Y. Fang. "A privacy-preserving attribute-based authentication system for mobile health networks". *IEEE Transactions on Mobile Computing*, 2014; 13(9):1927-1941.
[10] Dautov, R., &Tsouri, G. R., "Securing while sampling in wireless body area networks with application to electrocardiography". *IEEE journal of biomedical and health informatics*. 2016; 20(1): 135-142.
[11] Kumari S, Li X, Wu F, Das A K, Arshad H, Khan M. K. "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps". *Future Generation Computer Systems*, 2016; 63: 56-75.
[12] He D, Chan S, Tang S, Guizani M. "Secure data discovery and dissemination based on hash tree for wireless sensor networks". *IEEE transactions on wireless communications*, 2013; *12*(9), 4638-4646.
[13] Meharia P, Agrawal D P. "A hybrid key management scheme for healthcare sensor networks". *IEEE International Conference on Communications (ICC)*, 2016*:* 1-6.