Lightweight Security and Privacy Scheme for Wireless Body Area Network in E-Health System

Oladayo O. Olakanmi

University of Ibadan, Dept. of Electrical & Electronic Engineering.
Ibadan, Nigeria. Tel: +2348068730815. e-mail: olakanmi.oladayo@ui.edu.ng

Abstract—Low computational power of wireless sensors and the multicast form of transmission exhibited by WBAN make it susceptible to several security and privacy issues. Due to these, many security and privacy preservation approaches had been proposed to secure and preserve privacy of wearable WBAN systems. However, the inherent low computational power which characterises WBAN nodes made most of these approaches inefficient for the networks.

This paper proposes a lightweight two-way but coordinated perturbation scheme for obfuscating both the identities and measurements of the sensor in the wearable WBAN system. The coordinated generation of perturbs eliminates security and privacy problems associated with reconstruction by the receiver. The propose scheme was analysed and its estimated speed was compared with five state of the art schemes proposed in [39], [40], [41], [42]. The results showed that the scheme outperforms these schemes in terms of computational overhead. The scheme was also evaluated by simulating the scheme using digital ECG sensors as WBAN nodes. The simulation results not only confirm the estimated speed but also showed that the scheme left no semantic pattern in the transmitted data.

Keywords—Sensor network, Ehealth, Electrocardiography, Wireless Body Area Network (WBAN).

1. Introduction

Acquisition of accurate health knowledge of human anatomy and condition is the major operation that helps health-care professionals or doctors in handling health related issues of their patients. Most of the major health complications can easily be averted if useful information are readily available for health-cares professionals. The wireless body area network has emerged as a new technology for healthcare delivery. It monitors and communicates patients vital body parameters and movements through small wearable or implantable sensors over short-range wireless communication. Although, WBAN easily solves the problem of timing and non-availability of patients health information in health-care system, however wireless communication is not secured. This subjects health information to different forms of attacks. Preservation of identity and securing data transfer from the user to the server or sensors data stored in the server are the major challenges of WBAN. Examples of these security challenges are snooping, routing attacks and spoofing which affect the data confidentiality, data integrity, data availability and privacy of the sensor node. Several schemes had been proposed to secure health information in resources constraint WBAN. However, most of these schemes are either network specific or based on public or private key infrastructure which requires considerable memory and computational resources. These make them unsuitable for resources constraint network such as WBAN. In view of this, a lightweight but efficient security and privacy mechanism is required for WBANs routing protocol in order to protect sensitive data and wearer privacy during data transfer.

2. Literature Review

Wireless Body Area Network, as shown in Figure 1, is a set of sensor with wireless communication capabilities placed on human body for physiological monitoring of some of the body quantities to prevent complications and prompt diagnosis of health conditions. Sensor nodes are characterised with low power and computational capacity. Therefore, it must be subjected to low power and computational tasks in order to carry out its operation for a considerable period of time. The current developments and future direction of research on wearable WBAN systems for continuous monitoring of out and in-patients are inherently showing the need to improve on the security and privacy of sensor. Also, there is considerable increase in the number of the security threats on WBANs [27] [28]. These security threats affect the confidentiality, integrity, privacy, and availability on WBAN.

Many works had been done on how to secure data and preserve privacy of nodes on WBANs. For example, authors in [3] argued that sensor network routing protocols are not designed with security as a goal. They showed the effect of crippling attacks against major routing protocols for sensor networks and concluded that these protocols were not designed with security as a goal, and the used of them in WSN may compromise the networks. They further affirmed that they can be secured by incorporating security mechanisms after design has completed. Ferng et al in [4] proposed an energy-efficient secure routing protocol for WSNs to take care of the security lapses in the WSN routing protocol. In [5], a scheme was proposed to secure cardiography information by using a lightweight encryption framework to augment compression during sampling by using the measurement matrix as a symmetric key for encryption and decryption. The symmetric key was extracted from Received Signal Strength Indicator (RSSI) values which was used as seed to feed a Linear Feedback Shift Register (LFSR) to generate an m-sequence. This would be reorganised to form CS sensing matrix by the receiver and transmitter. However, this method is sensor dependent, that is, it is built around analog sensors which output must be converted to binary data before transmission. Also, the authors in [29] paper proposed a new user access control scheme for a WBAN. Their proposed scheme made use of a group-based user access ID, an access privilege mask, and a password. An elliptic curve cryptography-based public key cryptosystem was used to ensure that a particular legitimate user can only access the information for which he/she is authorized.

Authors in [33] presented the survey of WSN topologies, data sharing mechanisms, cryptography and attributes-based encryption in privacy preserving. In their work, some cryptography issues such as storage or computational overhead, the trade-off between the security and elasticity, trust assurance against the attacks were discussed. They made it clear that the secure data transfer from the user to the server is the major issue against the network adversaries. They highlighted the major cryptography operations such as key generation, encryption, and decryption as the main sources of storage and computational overheads and delegation issues in data preserving. Apart from security issues associated with data transmission in WBAN, authors in [32] also highlighted some security issues on WBAN data in the storage. Another research efforts where computation cost reduction was tackled was presented in [37]. The authors proposed a lightweight and robust security-aware data assist data transmission protocol for M-health systems by using a certificateless generalized signcryption to secure data Their certifcateless generalized signcryption scheme consists of three cryptographic primitives: signcryption, signature, or encryption, within one single algorithm. In [36], authors proposed a healthcare system framework that collected medical data from WBANs, transmits them through an extensive wireless sensor network infrastructure and finally publishes them into wireless personal area networks (WPANs) via a gateway. They engaged the groups of send-receive model scheme to implement both key distribution and secure data transmission, and homomorphic encryption based on matrix to ensure privacy.

In order to reduce the computation cost incurred by some WBAN schemes, a certificateless public auditing scheme with privacy preserving and revocation in group sharing data model was proposed in [35]. Although their scheme supports properties of multi-user sharing data, public auditing, forward security and revocation of illegal group members. However, the amount of computation cost required will overwhelm WBAN. Another lightweight scheme for WBAN was proposed in [38]. In this work, authors presented a secure lightweight and energy efficient authentication scheme called BANZKP. The scheme was based on cryptographic protocol, Zero Knowledge Proof (ZKP) and a commitment scheme. They used ZKP to confirm the identity of the sensor nodes while the commitment scheme was used to deal with replay attacks. Information retrieval in WBAN is another issues which are being addressed to improve the operations in ehealth. One of the research efforts in this direction is the work in [36]. The authors proposed the similarity search tree structure to enhance the hit rate of multikeyword ranking search. They also developed dynamic interval clustering algorithm in the cloud storage.

There are other schemes which address the privacy and security challenges faced in e-health network systems, however, most of them are network-oriented and required high computational power due to the complexity of their crypto-operations. Some of these schemes adopted Attribute Based Encryption (ABE) to provide access control to patient health record in the cloud [12] [17][18][19][20][21]. Attribute-based encryption is in two forms: Key Policy Attribute Based Encryption (KP-ABE) and Ciphertext-policy attribute-based encryption (CP-ABE). For data in the cloud like Patient Health Record (PHR), CP-ABE is the most suitable as patient can decide an access policy using attributes and encrypts data based on the corresponding attributes. In [9], the authors proposed a patient-centric and fine-grained data access control in multi-owner settings. To achieve fine-grained and access control control of PHR, they implemented KP-ABE to encrypt patient's PHR. Also, to achieve reduced key distribution problems, they divided the system into multiple security domains with each domain manages only a small number of users. Their revocation scheme involves computing a re-key by updating the ciphertexts of all the affected attributes. However, the use of KP-ABE results in higher key management complexity and cost of computation because users have to posses many attributes from different authorities to guarantee security of PHR, thus unfit to secure WBAN. Ramesh et al in [17] also proposed multi-authority scheme based CP-ABE with attribute revocation for cloud data storage. However, their scheme requires high computational power. Attribute-based access control scheme with efficient revocation in cloud computing was proposed in [43]. The authors introduced an access controller and designed an escrow-free generation protocol between the attribute authority and the access controller. Nevertheless, their scheme also resulted in higher computational cost.

Apart form ABE, data aggregation and perturbation are another ways employed in preserving privacy and reduced bandwidth [25][26][43]. The most common and non-complex technique used in privacy preservation of limited computational power nodes network is perturbation. The use of perturbation to hide or obfuscate data is not new, it has been used in many resources-constraint networks to secure and preserve privacy [6][7][8][43][23][24]. For example, authors in [7] proposed simple but efficient cryptographic privacy techniques for spatial aggregation of the smart meters data. They also considered temporal aggregation of multiple data for a single smart meter in order to prevent sniffing of consumers' energy profile. Although, their scheme is capable of achieving spatial and temporal aggregation of consumers data however, their scheme is not resistant to pre-target attack whereby adversary use the knowledge of the NAN topology and direction of aggregation to launch attack on a specific node. Apart from this, their perturbation technique is not only prone to sniffing but reconstruction is too easy for an attacker. Also, in [8] authors showed that it is possible to effectively and efficiently track the correlation and autocorrelation structure of multivariant streams and use it to perturb the stream data to preserve privacy. However, there is limitation on the size of the noise which can be used in their scheme, therefore such scheme can not be enough to map data into oblivion space.

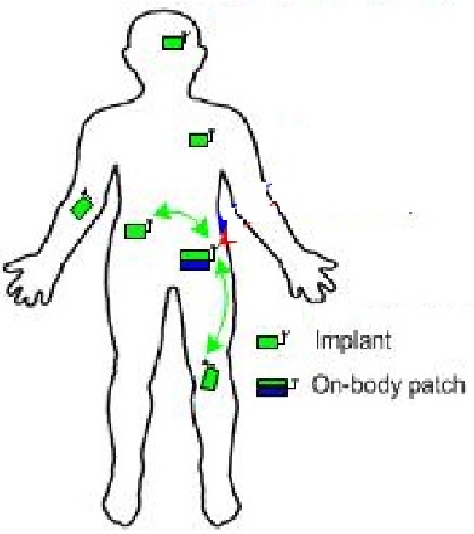

Fig. 1. Wireless Body Area Network

3. Problem Formulation

In this work two problems were formulated in order to address the security and privacy issues in WBAN. These are how to secure data in resource-constraint WBAN, and an efficient 2-way coordinated perturbs generation technique to secure data and preserve the privacy of wearers in WBAN.

Problem 1: Securing data in resource-constraint WBAN environment. *For any WBAN using sink to send measurements out of the network, assuming the possibility of gleaning and modification of these measurements. Securing the measurements of each sensor such that gleaning will be impossible and any attempted data modification will be easily detected by the user (Intelligent Diagnostics Server, Care-Giver and Medical Center) is a security challenge.*
In this work, we propose a 2-way coordinated perturbation scheme which obfuscates sensors' data through additive noise that can be re-constructed only by authorised receiver(s).

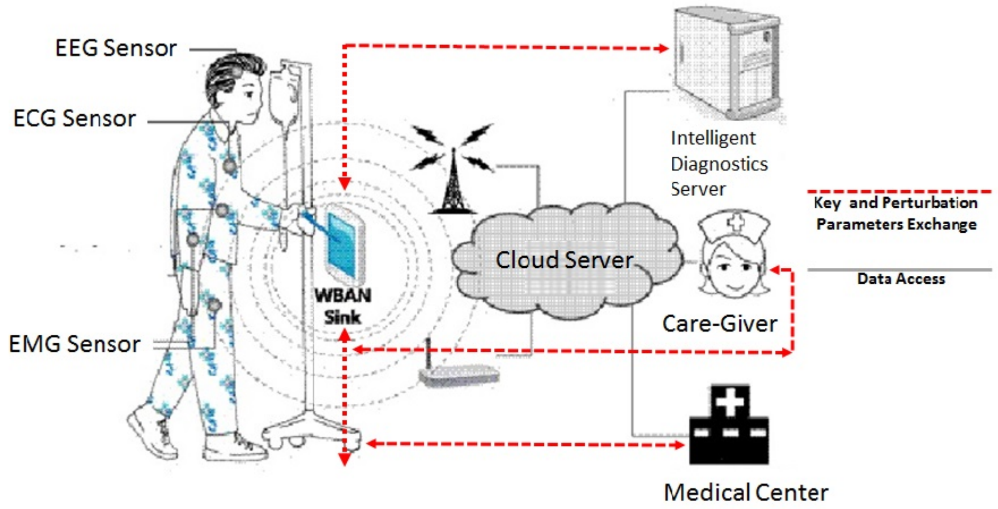

Fig. 2. System Model of the Enhanced Security and Privacy Oriented WBAN for E-health System

Problem 2: Formulation of coordinated 2-way perturbation parameters. *The major issue in data obfuscation using perturbation is how to generate perturbs such that each sensor's perturb can be regenerated only by the authorised receiver without compromising its knowledge to the adversary. That is, there must be a form of authentication and exchange feature(s) inherent in the perturb generation procedure otherwise reconstruction of data by receiver will not be possible. In most perturbation schemes, this coordination is a weak link through which adversary launches attacks.*
In this work, a set of cryptography operations which allow sensor to create root parameters for any authorised users to unperturb any of its perturbed measurements is used.

4. System Model

The system model, as shown in Figure 2, consists of the following entities:

1 Patient: This is the wearer of WBAN. The WBAN has an access point called sink through which information leaves and enters the WBAN. Sink performs registration on behalf of each sensor in the network.

2 User: This entity makes use of sensors' measurements on real time and non real time modes. This may be Intelligent Diagnostic Server, Care Giver and Medical Center as shown in Figure 2.

3 Cloud Server: This stores the past and present measurements of each sensors in WBAN for authorise users' immediate or future needs.

5. Threat Model

All the threats listed below are considered as likely threats to the propose scheme.

1 **Spoofing**: In this threat, it is assumed that adversary is capable of launching sybil attacks on source node in order to obtain perturbation parameters of the targeted user.

2 **Theft Identity:** In this threat, adversary may want to steal identity of either the sender or user in order to generate a set of perturb for reconstruction of both the past and current

data.

3 **Repudiation**: This involves wearer denying measurements generated from her WBAN.

4 **Information Disclosure**: This involves cloud server conniving with adversary to spoof on patients by leaking out their identity or health information.

5 **Denial of Services**: Denial of service (DoS) attack denies services to valid users.

6 **Elevation of privilege:** User may want to maliciously use previously generated perturbation parameters to generate perturb for sensors' measurements for which it does not have access right.

6. Primitives

In the scheme the following primitives are used to achieve the security and privacy preservation of the propose scheme; The elliptic curve E/F_q, where F_q is a finite field with prime order, $E : y^2 = x^3+ax+b$ and $4a^3 + 27b^2(modP) \neq 0$, where, $a, b \in \mathbb{F}_q$ is used. The point P is the generator of E/F_q, and $H\{0,1\}^* \leftarrow \mathbb{G}$ is a one-way collision resistance hash function. Elliptic Curve Discrete Logarithm Problem (ECDLP) is more difficult to break than the factorization of RSA and discrete logarithm on a multiplicative group G such that $(Z/pZ)^*$ [43],[44], [45].

7. Security and Privacy Orientation Scheme for WBAN

The data perturbation involves the use of additive noises to hide data without prior exchange of the noises between the source and destination. Choosing an efficient perturbation technique for sensor in WBAN requires consideration of computational power limitation of WBAN. This is the major weakness of some of the existing security and privacy schemes developed for WBAN. In light of this, the propose scheme engages a few exponential operations for data and identity obfuscation. Data perturbation and transmission are done through the WBAN gateway (sink). The WBAN is modelled such that registration and parameters exchange are between WBAN sink and authorise users. During registration, the sink and user obfuscatory exchange their session identities and time-stamp using the propose novel obfuscatory exchange method used in registration and 2-way coordinated perturb generation phases. Then, sink initiates 2-way coordinated perturb generation by generating perturbation parameters P_s, blinds and sends it to the user. This procedure is repeated by user by generating its own perturbation parameter P_a, blinds and sends it to sink. Each of them unblind the received perturbation parameter to compute the session perturb P_t. The source node perturbs its message with P_t and sends it to the user for a real time use or stores it in cloud server for future use. Since user has P_t, it can reconstruct message from perturbed message anytime.The scheme consists of three phases; registration, 2-way coordinated perturbs generation and obfuscation, and reconstruction phases as described in the subsequent subsections.

7.1. Registration Phase

Every new user registers with the patient through the WBAN sink by obscurely submit its identity U_{id} and receive the serial number of its desire sensor's data through the following steps:

Step 1: For each sensor i desired by user d, the sink obfuscately sends the session time stamp $tstamp$ and serial number of the sensor i through these steps:

- For sensor node i user d randomly generates k_d, computes and publishes $\alpha_d = k_d P$

- Sink then randomly generates k_1 and k_{sink} for each sensor i
  - Computes both $\beta_1 = k_1 P$; and $\beta_2 = k_{sink} P$ and publish β_1 and β_2
  - Computes $\digamma_i = k_1 \alpha_d + serial\_of\_sensor_i$
  - Computes $tstamp_i = k_1 \alpha_d + ts_i$
  - Sends $\{\beta_1, \digamma_i, tstamp_i\}$ to the user d

User U_d retrieves the obfuscated serial number of the sensor i and time stamp as:
$serial\_of\_sensor_i = \digamma_i - k_d(\beta_1)$
$ts = tstamp_i - k_d \beta_1$

Step 2: User d also sends her obscure identity U_{id} to sink by:

- Randomly generating k_2 and computes $\digamma_d = k_2 \beta_2 + U_{id}$; $\beta_3 = k_2 P$
- Sends pair $\{\beta_3, \digamma_d\}$ to the sink.

WBAN sink retrieves the user U_{id} as: $U_{id} = \digamma_d - k_{sink} \beta_3$

7.2. 2-way Coordinated Perturb Generation

Both the user d and sink have three parameters in common $\{U_{id}, serial\_of\_sensor_i, ts\}$ obtained through obfuscatory exchange technique described in registration phase. These parameters are used to generate perturbs in this phase. This phase consists of two stages; perturb generation and perturbation stages.

7.2.1. Perturb Generation

Before data perturbation, both sink and user must generate and exchange the perturbation parameters. The serial number of sensor i and identity of user d are used to generate a 2-way coordinated perturbs P_i^t at time t by following these steps:

Step 1: For each sensor i, sink randomly generates large number a_i and performs the following:

- Computes $Ps_i = (U_{id} \bigoplus ts \bigoplus a_i)$, where ts is a unique time-stamp for each session, $a_i \in Z$ and i is index of the sensor.
- It then blinds Ps_i as $Ks_i = Ps_i \bigoplus serial\_of\_sensor_i \bigoplus ts$,

Step 2: Sends Ks_i to the user d.
Step 3: User d also randomly generates large number b_i such that $b_i \in Z$ and performs the following:

- Computes $Pa_i = (serial\_of\_sensor_i \bigoplus ts \bigoplus b_i)$
- It then blinds Pa_i as $Ka_i = Pa_i \bigoplus U_{id} \bigoplus ts$,
- Sends Ka_i to the sink.

Sink then unblinds the received Ka_i to obtained its perturbation parameters Pa_i as:
$Pa_i = Ka_i \bigoplus U_{id} \bigoplus ts$
$Pa_i = Pa_i \bigoplus U_{id} \bigoplus U_{id} \bigoplus ts \bigoplus ts$ and
User d also unblinds the received Ks_i to obtained its own perturbation parameters Ps_i as:
$Ps_i = Ks_i \bigoplus serial\_of\_sensor_i \bigoplus ts$
$Ps_i = Ps_i \bigoplus serial\_of\_sensor_i \bigoplus serial\_of\_sensor_i \bigoplus ts \bigoplus ts$

7.2.2. Perturbation

Once the perturbation parameters had been exchanged between the user and sink, then the perturb P_i^t for sensor i at time t can be independently generated by the sink and user, d as:
$P_t^i = Ps_i \bigoplus Pa_i$
The generated perturb, P_t^i is then used by sink to perturb the sensor i data m_i^t at time t as:
$M_i^t = m_i^t + P_t^i$ where M_i^t is the corresponding perturbed data. The signature δ_i^t of m_i^t is also obtained by generating the message authentication

code of m_i^t as: $\delta_i^t = H_{Ps_i}(m_i^t)$
Then, the pair $\{M_i^t, \delta_i^t\}$ is sent to the user for an immediate use or store in the cloud server for future use. This is repeated for other sensor nodes in the WBAN at every time t.

7.3. Reconstruction

Authorise user d reconstructs the received perturbed M_i^t message by unperturbing M_i^t as follows: $m_i^t = (M_i^t - P_t^i)$. Then confirms the authenticity of the message by generating: $\delta_d^t = H_{Ps_i}(m_i^t)$ since it has Ps_i. If the user d generated signature δ_d^t is similar to the received signature δ_i^t then the received message is accepted otherwise rejected.

7.4. Security Analysis

This section contains the formal security analysis which shows that the propose scheme is secure against all the threats described in the threat model. The scheme security and functionality depend solely on one way hash function used in the message authentication, elliptic curve discrete logarithm problem introduced in the key parameters exchange and in perturbation parameters exchange phases. For this purpose, the formal definitions of these primitives are defined to show the strength of the proposed scheme against some of the possible attacks:
Definition 1: *(Elliptic Curve Discrete Logarithm Problem ECDLP). Here the elliptic curve discrete logarithm problem which the registration and perturbation parameters exchange phases of the scheme depend on can be formally defined as related to the scheme as follows:*
Suppose E is an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$ and $P \in E(\mathbb{Z}/\mathbb{Z}_p)$, given a multiple Q of P , the Elliptic Curve Discrete Logarithm Problem (ECDLP) is to find $n \in \mathbb{Z}$ such that $nP = Q$.
In the registration phase, both the sink and authorise user exchange their obscure identities and sessional time stamp using the propose obfuscatory technique which relies on ECDLP.

For example, in the registration phase, $\alpha_d = k_dP$, $\beta_1 = k_1P$, $\beta_2 = k_{sink}P$, and $\beta_3 = k_2P$ introduced elliptic curve discrete problem to hide k_d, k_1, k_2, and k_{sink} from unauthorise entities, an hardest problem than integer factorization problem and discrete log problem on multiplicative group. Discrete log problem on the multiplicative group $(Z/Z_p)^*$ can be reduced to factorization problem and solved for small prime number. However, elliptic curve discrete problem for small key size has been proved to be hard, and for now unbreakable. That is, for most elliptic curves, there is no known analogue of index calculus attacks on the discrete log problem. That is, given P the discrete log problem in $E(Z/Z_p)$ it is much harder than the discrete log problem in the multiplicative group $(Z/Z_p)^*$. This shows that by using an elliptic curve-based cryptosystem, as used in the registration phase, instead of one based on $(Z/Z_p)^*$, equivalent security with much smaller numbers will be achieved. The two random oracles which are made difficult by ECDLP are described below.
$Oracle_1$: This oracle unconditionally outputs k_d from given points P and $Q = k_dP$; k_1 from given points P and $\beta_1 = k_1P$; k_{sink} from given points P and $\beta_2 = k_{sink}P$, in an elliptic curve $Ep(a, b)$.
$Oracle_2$: This oracle also outputs the user identity U_{id} from $\digamma_d = k_2\beta_2 + U_{id}$, serial number of sensor $serial\_of\_sensor_i$ from $\digamma_d = k_2\beta_2 + U_{id}$, and t_s from $tstamp_i = k_1\alpha_d + ts_i$ with the help of the relevant public parameters.
The harder the ECDLP is, the more impossible for adversary to obtain the k_d, k_1, k_2, k_{sink}, actual sessional identities and time-stamp, and the more difficult it becomes for adversary to launch attack on the system.

Definition 2: *(One-way hash function). There exists a secure one-way hash function $H : X \to Y$, where $X = 0, 1^*$ and $Y = Z_p^* = \{a|0 < a < p$ and $\gcd(a, p) = 1\}$ satisfying the following requirements:*

1 *For a given $y \in Y$, it is hard to find an $x \in X$ such that $H(x) = y$.*
2 *For a given $x \in X$, it is hard to find another $x' \in X$, with $x' \neq x$, such that $H(x') = H(x)$.*
3 *It is hard to find a pair $(x, x') \in X \times X$, with $x' \neq x$, such that $H(x') = H(x)$.*

7.4.1. Elevation of privilege and repudiation attacks through signature forging

In the scheme, elevation of privilege and repudiation attacks are taken care by a simple signature $\delta_i^t = H_{Ps_i}(M_i^t)$ using a commonly agreed upon key Ps_i which is generated by the sender. Since Ps_i is generated by the sink for sensor i which is known only by authorised user and sink for that session, and the requirements stated above hold for H, therefore it is impossible for any adversary to forge signature δ_i^t and impossible by wearer to repudiate its message m_i^t.

That is, for a message m_i^t signed as $H_{Ps_i}(m_i^t)$, if an adversary A, whose intention is to modify m and generate $\delta_i^{t'}$ such that $\delta_i^t = {\delta'}^t{}_i$ then:

$A_{H_{Ps}}(m) = Pr[(m, m') \Leftarrow RA : m \neq m', H_{Ps}(m) = H_{Ps}(m')]$

where $Pr(L)$ denotes the probability of a random attack on message m through signature δ, and $(m, m') \Leftarrow RA$ denotes the pair (m, m') is selected randomly by A. If the adversary success rate in finding collision for $A_{H_{Ps}}(m) \leq 0$, then hash function is collision resistant and the scheme is secured against any message authentication related attacks such as repudiation, elevation of privilege, modification etc.

7.4.2. Sniffing of perturbation parameters

The Elliptic Curve Discrete Logarithm Problem (ECDLP) with XOR symmetric encryption introduced in 2-way coordinated perturb generation phase secure the scheme against perturbation parameters' sniffing threat. Inasmuch ECDLP is hard to solve and ts collision is avoided during parameters blinding and exchange then perturbation parameters are secured against sniffing. This problem with the respect to how its introduction secures the scheme against sniffing are describe as follows:

Inasmuch oracle 1 and 2 hold, and collision of either a_i, b_i or ts is avoided then the perturbation parameters exchange technique cannot be compromised. That is, even if adversary get both Ks_i and Ka_i the discrete log problem with the mutual exclusiveness of XOR operator would make it difficult for him to get the actual perturbation parameters pair Pa_i, Ps_i. Therefore, probability of data gleaning by unauthorised users is impossible.

7.4.3. Spoofing on the user and sensor identities and session parameters

The elliptic curve discrete logarithm problem introduced during identity and parameters exchange in registration phase secures the scheme against identity and session parameters spoofing. The harder the problem is the more secure the scheme becomes. This is shown in the definition 1.

7.4.4. Gleaning through semantic pattern of the data

Semantic insecurity of perturbed data is another threat considered. This form of insecurity on the perturbed data is usually caused by the semantic pattern which is inherent in the sensor data. For example, if the variation in the data sizes are wide some level of information could be gleaned by adversary despite being perturbed. Semantic issue is addressed in the scheme through the generation of large size perturb for perturbation of sensor data before being transmitted so as to completely mask off the uneven variation of the data set. This is done through the exclusive OR of serial number of the sensor or user identity, randomly generated large number a_i, b_i and time stamp to produce a large but unique perturb $P^i_t = Ps_i \bigoplus Pa_i$. This would not only make the perturbed data to be uniformly distributed to the oblivious space but gives each perturbed data a linkable identity to the sensor node and user through through Ps_i and Ps_i.

7.5. Performance Evaluation

Performance evaluation of the proposed scheme was done based on computation cost and obfuscation efficiency of the scheme as described below.

7.5.1. Obfuscation Efficiency Analysis

The obfuscation efficiency analysis was based on effective obfuscation of the granular measurements through perturbation phase of the scheme. Digital ECG samples of a patients were used to determine the efficiency of our scheme against gleaning. A simulator was developed based on the proposed scheme. The two different set of ECG samples were

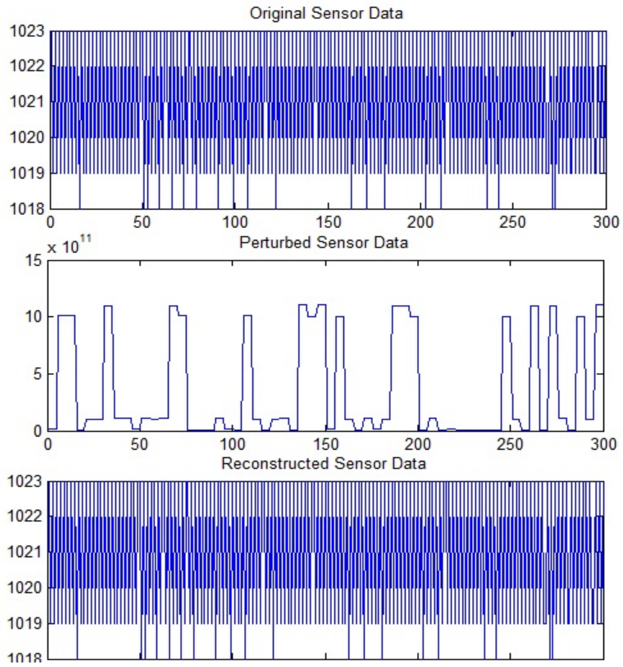

Fig. 3. Obfuscation Efficiency Test 1

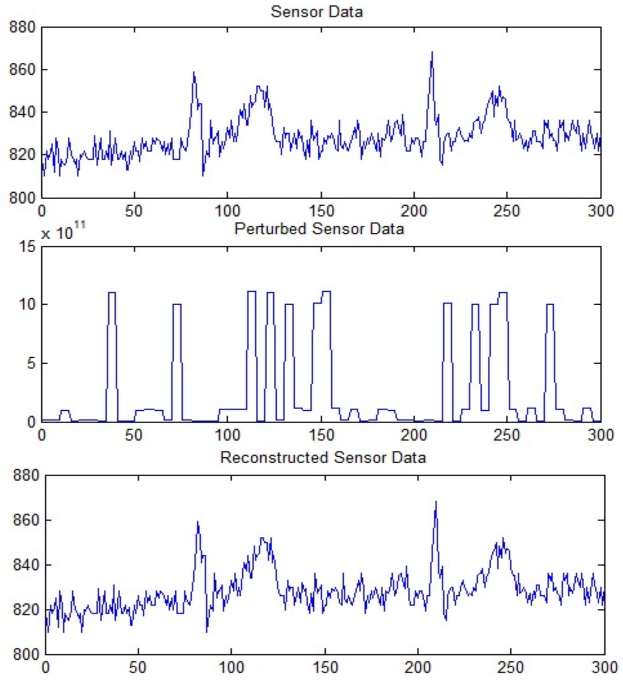

Fig. 4. Obfuscation Efficiency Test 2

passed into the simulator to obtained corresponding set of obfuscated samples as shown in Figure 3 and 4. Row 1 of the Figure 3 and 4 represents the ECG samples, row 2 is the corresponding perturbed ECG samples, and Row 3 is the unperturbed ECG samples reconstructed from the received perturbed samples. The perturbed waveforms are totally different from the waveforms of the unperturbed ECG samples. This shows that the perturbation successfully obfuscated the measurements with no semantic pattern. Meanwhile, the unperturb sample obtained after reconstruction is the same with original sample, which indicates that the scheme gives a perfect reconstruction of the original data from the perturbed data.

7.5.2. Computation Cost Analysis

In this section, the proposed scheme is compared with 4 different certificateless WBAN schemes in terms of computational overhead. As the operations on pairing, exponentiation, hashing, XOR and multiplication dominate the computational overhead in the schemes, these operations are therefore considered in determining the computation overhead. We denote T_{exp} the time consumed for one exponentiation operation, T_{ecm} the time consumed for one scalar multiplication in E, T_{hash} the time for one way keyed hash function SHA256, T_{pair} the time for one pairing operation, and T_{exc} the time for one exclusive OR operation. In [30]], where the operations were implemented on an Intel PIV processor at 3GHz, the running time are $T_{exp} = 2.19ms$, $T_{ecm} = 0.6ms$, $T_{pair} = 4.5ms$, $T_{hash} = 1.17ms$, and $T_{exc} = 1ns$. The cost analysis was done for the four schemes using the similar settings. The estimated computational time of the four schemes are shown in Table 1. The propose scheme takes 2 hash operations to compute and verify the signature, 4 elliptic multiplication operations for obfuscatory transfer, and 21 exclusive OR operations in perturbation phase. The computation costs in Table 1 show that the propose scheme requires lowest computation time, confirmation of its lightweightness than other three certificateless state of the art schemes for wireless sensor networks.

TABLE 1
Computation Cost Analysis

Schemes	Operations	Estimated Time(ms)
Aiqin et al [37]	$15T_{ecm} + 15T_{hash}$	26.55
Ji et al [39]	$10T_{exp} + 5t_{ecm} + 5T_{pair}$	47.40
Kushwah et al [40]	$7T_{exp} + 13T_{ecm} + 4T_{pair}$	41.06
Zhou et al [41]	$2T_{exp} + 11T_{ecm} + 14T_{pair}$	73.98
Shi et al [42]	$16T_{exp}$	35.04
Propose scheme	$2T_{hash} + 4T_{ecm} + 21T_{exc}$	4.74

8. Conclusion

In this work, a lightweight scheme for securing data and preserving the privacy of wearer of WBAN in e-health is proposed. The scheme is resilient to malfunction associated with computation power, energy consumption and with no semantical pattern in the transmitted data. Compare to the other WBAN security schemes, the proposed scheme outperforms the other state of the art schemes in terms of computational overheads and capable of securing data with no semantic pattern.

References

[1] V. Agrawal. ”Security and privacy issues in wireless sensor networks for healthcare”. In Internet of Things, User-Centric IoT, LNICST 150, Springer, Cham, pages 223-228, 2015.

[2] P. Gong, T. Chen, and Q. Xu. ”ETARP: An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks”. Journal of Sensors, 2015(1), pages 1-10, 2014.

[3] C. Karlof, and D. Wagner. ”Secure routing in wireless sensor networks: attacks and countermeasures”. Journal of Ad Hoc Networks, 1(2003), pages 293-315, 2003.

[4] F. Huei-Wen, and D. Rachmarini. ”A secure routing protocol for wireless sensor networks with consideration of energy efficiency”. In IEEE Network Operations and Management Symposium (NOMS), pages 105-112, 2012.

[5] D. Ruslan and R. Gill. ”Securing While Sampling in Wireless Body Area Networks With Application to Electrocardiography”. IEEE Journal of Biomedical and Health Informatics, 20(1), pages 1-7, 2016.

[6] A. Matthew, and S. Thomas. ”General Deviants: An Analysis of Perturbations in Compressed Sensing”. IEEE Journal of Selected Topics in Signal Processing, 4(2), pages 342-349, 2010.

[7] Z. Erkin and G. Tsudik. ”Private Computation of Spatial and Temporal Power Consumption with Smart Meters”. Proceedings of the 10th international conference on Applied Cryptography and Network Security, LNCS 7341, pages 561-577, 2012.

[8] F. Lei, J. Sun, S. Papdimitriou, G. Mihaila, and I. Stanoi. ”Hiding in the Crowd: Privacy Preservation on Evolving Streams through Correlation Tracking”. Proceeding of IEEE 23rd International Conference on Data Eng. (ICDE), pages 1-10, 2007.

[9] M. Li, S. Yu, K. Ren, and W. Lou. ”Securing Personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings”. International Conference on Security and Privacy in Communication Systems, LNICST 50, pages 89-106, 2010.

[10] K. Zhang, R. Lu, X. Liang, J. Qiao, and X. Shen. ”PARK: A privacy-preserving aggregation scheme with adaptive key management for smart grid”. In Proceedings of IEEE/CIC International Conference on Communications in China (ICCC ’13), pages 236-241, 2013.

[11] J. Ni, k. Zhang, X. Lin, and X. Shen. ”EDAT: Efficient data aggregation without TTP for privacy-assured smart metering”. In Proceedings of Communication and Information Systems Security Symposium, pages 1-6, 2016.

[12] L. Guo, C. Zhang, J. Sun and Y. Fang. ”PAAS: A privacy-preserving attribute-based authentication system for eHealth networks”. 32nd IEEE International Conference on Distributed Computing Systems, pages 224-232, 2012.

[13] Y. Lee, S. Han, B. Chung, and D. Lee. ”Anonymous authentication system using group signature”. IEEE Proceedings of International Conference on Complex, Intelligent, and Software, pages 1235-1239, 2009.

[14] D. Boneh and B. Lynn, and H. Shacham. ”Short signature from the weil pairing”. Journal of Cryptology, 17(4), pages 297319, 2004.

[15] D. He, M. Khan, and N. kumar. ”A new handover authentication protocol based on bilinear pairing functions for wireless networks”. International Journal of Ad hoc and ubiquitous computing, 18(2), pages 67-74, 2015.

[16] C. Rong, H. Cheng. ”Authenticated Health Monitoring Scheme for Wireless Body Sensor Networks”. Proceedings of 7th International Conference on Body Area Networks, pages 31-35, 2012.

[17] D. Ramesh, and R. Priya. ”Multi-authority scheme based CP-ABE with attribute revocation for cloud data storage”. International Conference on Microelectronics, Computing and Communications (MicroCom), pages 1-4, 2016.

[18] X. Zhihua, L. Zhang, and D. Liu. ”Attribute-based access control scheme with efficient revocation in cloud computing.” China Communications, 13(7), pages 92-99, 2016.

[19] V. Goyal, O. Pandey, A. Sahai, and B. Waters. ”Attribute-based encryption for fine-grained access control of encrypted data”. Proceedings of the 13th ACM conference on Computer and communications security, pages 89-98, 2006.

[20] M. Chase, and S. Chow, ”Improving privacy and security in multi-authority attribute-based encryption”. Proceedings of the 16th ACM conference on Computer and communications security, pages 121-130, 2009.

[21] X. Mao, J. Lai, Q. Mei, K. Chen, and J. Weng. ”Generic and efficient construction of attribute-based encryption with verifiable outsourced decryption”. IEEE Transactions on Dependable and Secure Computing, 13(5), pages 1-14, 2016.

[22] K. Nomura, M. Mohri, and Y. Shiraishi. ”Attribute Revocable Attribute-Based Encryption for Decentralized Disruption-Tolerant Military Networks.” IEEE Third International Symposium on Computing and Networking (CANDAR), pages 491-494, 2015.

[23] Z. Erkin, J. Troncoso-Pastoriza, R. Lagendijk, and F. Perez-Gonzalez. ”Privacy-preserving data aggregation in smart metering systems: an overview”. Signal Processing Magazine, 30(2), pages 75-86, 2013.

[24] H. Lin, W. Tzeng, S. Shen, and B. Lin. ”A practical smart metering system supporting privacy preserving billing and load moitoring”. In Proceedings of the 10th International Conference on Applied Cryptography and Network Security, pages 544-560, 2012.

[25] Z. Shi, R. Sun, R. Lu, L. Chen, J.Chen, and X. Shen. ”Diverse grouping based aggregation protocol with error detection for smart grid communications”. IEEE Transaction on Smart Grid, 6(6), pages 2856-2868, 2015.

[26] L. Min, Z. Shi, R. Lu, R. Sun, and X. Sherman. ”PPPA: A practical privacy-preserving aggregation scheme for smart grid communications”. IEEE/CIC International Conference on Communications in China (ICCC), pages 692-697, 2013.

[27] L. Shinyoung, T. Oh, Y. Choi, and T. Lakshman. ”Security issues on wireless body area network for remote healthcare monitoring”. IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), pages 327-332, 2010.

[28] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, S. Shamshirband. ”Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications”. Egyptian Informatics Journal, 18(2), pages 113-22, 2017.

[29] S. Chatterjee, A. Das, J. Sing. ”A novel and efficient user access control scheme for wireless body area sensor networks”. Journal of Computer and Information Sciences, 26(2), pages 181-201, 2014.

[30] M. Scott. ”Efcient Implementation of Crypto-

graphic Pairings". [Online]. Available: http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf

[31] K. Manoj. "Security issues and privacy concerns in the implementation of wireless body area network". In International Conference on Information Technology (ICIT), pages 58-62, 2014.

[32] M. Li, W. Lou, K. Ren. "Data security and privacy in wireless body area networks, IEEE Wireless Communications". 17(1), pages 51-58, 2010.

[33] D. David, A. Jeyachandran. "A comprehensive survey of security mechanisms in healthcare applications". International Conference on Communication and Electronics Systems (ICCES), pages 1-6, 2016.

[34] H. Haiping, T. Gong, and N. Ye. "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System". IEEE Transactions on Industrial Informatics, 13(3), pages 1227-1237, 2017.

[35] S. Li, Z. Hong, and C. Jie. "Public Auditing Scheme for Cloud-Based Wireless Body Area Network". IEEE/ACM 9th International Conference on Utility and Cloud Computing (UCC), pages 375-381, 2016.

[36] L. Yao, J. Gu, and M. Tang. "Privacy Protection Based Retrieval on WBAN Big Data". IEEE 18th International Conference on High Performance Computing and Communications, pages 876-882, 2016.

[37] A. Zhang, L. Wang, X. Ye, and X. Lin. "Light-Weight and Robust Security-Aware D2D-Assist Data Transmission Protocol for Mobile-Health Systems". IEEE Transactions on Information Forensics and Security, 12(3), pages 662-675, 2017.

[38] N. Khernane, M. Potop-Butucaru, C. Chaudet. " BANZKP: A Secure Authentication Scheme Using Zero Knowledge Proof for WBANs". IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), pages 307-315, 2016.

[39] H. Ji, W. Han, and L. Zhao. "Certificateless generalized signcryption", Cryptology eprint Archive, [Online]. Available: http://eprint.iacr.org/ 2010/204.pdf.

[40] P. Kushwah and S. Lai. "An efficient identity based generalized signcryption scheme", Cryptology eprint Archive, Tech.,[Online]. Available: http://eprint.iacr.org/ 2010/346.pdf.

[41] C. Zhou, W. Zhou, and X. Dong. "Provable certificateless generalized signcryption scheme". Journal of Design, Codes Cryptography, 71(2), pages 331-346, 2014.

[42] W. Shi, N. Kumar, P. Gong, and Z. Zhang. "Cryptanalysis and improvement of a certificateless signcryption scheme without bilinear pairing". Frontiers Computer Science, 8(4), pages 656-666, 2014.

[43] Z. Liping, S. Tang, and H. Luo. "Elliptic curve cryptography-based authentication with identity protection for smart grids." PloS one, 11(3), pages 1-15, 2016.

[44] B. Michael, and S. Meiser. "Differentially private smart metering with battery recharging". In Conference on Data Privacy Management and Autonomous Spontaneous Security, Springer, Berlin, Heidelberg, pages 194-212, 2014.

[45] X. Li, Y. Zhang, X. Liu, J. Cao and Q. Zhao. "A Lightweight Roaming Authenticaton Protocol for Anonymous Wireless Communication". IEEE Global Communications Conference (GLOBECOM), pages 1029-1034, 2012.