Security Guaranteed Event Discovery and Data Transmission under Wireless Body Area Networks

Salif Salih. P.V, M.Tech (CSE),
Mr. Denny Andrews, Assistant Professor,
Department of Computer Science and Engineering,
Cochin Institute of Science and Technology, Ettaipilly, Mannathur P.O. Pampakkuda (via),
Muvatupuzha, Eranakulam District, Kerala, India

Abstract
The mobile health services are constructed with the support of the smart phones and sensor devices. The remote patient care is provided by the mobile health services. The Wireless Body Area Network (WBAN) is constructed with the sensor devices. Patient monitoring and data forwarding operations are carried out with the Wireless Body Area Network (WBAN). The sensor devices are adapted to observe and transmit the blood pressure, Oxygen level and body temperature information. The radio frequency is utilized to support all the data transmission tasks. The device to device (D2D) data transmission process is protected with authentication, confidentiality and data integrity operations.

The Light-weight and Robust Security-Aware (LRSA) D2D-assist data transmission protocol is employed to guarantee the data security and forwarding operations. The Certificateless Generalized Signcryption (CLGSC) technique is employed to provide the security for the D2D data communication. The CLGSC scheme integrates the signcryption, signature and encryption with in single channel. The Network Manager (NM), WBAN Client and Medical Service Provider are the key elements used for the data monitoring and transmission process. All the key management operations are carried out under network manager (NM).

The Wireless Body Area Network (WBAN) data security is build with optimal relay selection and data forwarding policies. The medical data aggregation based query processing is supported in the system. Event detection and decision support operations are integrated with the patient monitoring application. Priority level based data forwarding operations are initiated to control the data transmission overhead. The node security process is enhanced with node anonymization and data privacy models. The data cache and replica schemes are also integrated with the system to support efficient data communication tasks.

1. Introduction
As a special application of Wireless Sensor Networks (WSNs), Body Sensor Networks (BSNs) are deployed on the surface of bodies for periodically monitoring physical conditions. In some cases, especially in emergency or health slight leakage of sensitive data may cause unpredictable damages. Therefore, extensive studies on privacy preservation have been carried out, which is one of the most critical research topics in BSNs.

Usually, data collected, aggregated and transmitted in BSNs contain personal and sensitive private information, which directly or indirectly reveals the condition of a person. If the data cannot be properly preserved, once exposed to the public, the privacy will be destroyed. Therefore, protecting the privacy of sensitive data is of great importance.

In general, traditional methods for protecting privacy and security of big data in BSNs fall into three categories: 1) anonymous techniques, 2) privacy protection rules, and 3) collaborative filtering. However, the above mentioned privacy protection schemes are still suffering from several common problems:
1. Anonymous technologies simply hid or replaced the information such as identity or location. They overlooked the fact that an attacker can identify a certain user based on his background knowledge although an objective user’s identity information is concealed or deleted. Obviously, anonymous technique does not protect the accuracy or availability of data.

2. Privacy protection rules mainly aimed at finding out the underlying relationship among data. However, this method can only cope with a fixed mode of attack.

3. Collaborative filtering schemes loosed degrees of the data set and calculated errors based on similarity. They assumed that the attacker cannot grasp full background knowledge. Such limitations seriously constraints the widespread application based on this scheme.

The mechanism of privacy protection in BSNs provides fundamental contributions in developing network security technology. With the growing demands for wearable devices, privacy protection of big data has become a major concern. As the big data era comes, personal information leakage happens more and more frequently, such as the famous cookies storm happened several years ago, which caused three hundred and sixty users’ information exposed. Therefore, privacy protection of BSNs should be paid close attention.

The security scheme is build to protect the privacy of BSNs based on differential privacy technology. In our scheme, we change the structure of the data set to reduce the sensitivity, and then add noise to the deformation data set, and finally, get the published data set.

2. Related Work

The traditional cryptography technology has been widely used to secure the sensitive medical data collected or transmitted in WBAN system. For example, Identity-based cryptography technology, compared to the traditional PKI technology, has the advantage of identity as the public key and eliminates the trouble of certificate management, so it is widely used in a variety of security protocols. However, due to the existence of key escrow problem, security has been called into question. To solve the key escrow problem in Identity-based cryptography, the certificateless public cryptographic algorithm is proposed. Key escrow problem can be resolved with certificateless cryptography. In certificateless cryptography, the key is generally divided into two parts, generated by the user and the key generation center, respectively. Taking into account the characteristics of weak capacity in processing, storing and bandwidth constraints, certificateless cryptography is more suitable for WBAN. Based on the certificateless cryptography, some authentication protocols have been proposed in WBAN.

In [5], Liu et al. proposed two certificateless authentication schemes for WBAN. However, Zhao [6] found that Liu et al.’s schemes cannot withstand the stolen verifier table attack and proposed an improved scheme to withstand the attack. Later, Wang et al. [7] points that in Zhao’s schemes, the users’ pseudo identities are constant value and the attack could tract the users. Xiong [8] pointed out that Liu et al.’s schemes lack of scalability, forward security and proposed a new certificateless authentication scheme for WBAN. Furthermore, Xiong et al. proposed a revocable and scalable scheme in [9] with tree structure.

A security framework using probabilistic computation is proposed. When the user has an incident but the mobile device fails, the medical sensors will use the probability computation algorithm to request the device's nearby as gateway. In [2], Lee found out that the protocol in [1] has some secure flaws such as user anonymity and mutual authentication. To fix those problems and further improve the computation efficiency of the original protocol, the authors present an improved mobile-Healthcare emergency system based on extended chaotic maps. In [3], a method of medical data
analysis algorithm is proposed. The proposal uses Paillier homomorphic encryption to achieve data privacy. However, it only supports limited styles of analysis operations.

In [4], the authors proposed a cloud-enabled WBAN architecture and its applications in pervasive healthcare systems. They highlight the methodologies for transmitting vital sign data to the cloud server by using energy-efficient routing, cloud resource allocation, semantic interactions, and data security mechanisms. In [10], a secure and privacy-preserving key management scheme for cloud-assisted WBAN in m-healthcare social networks is proposed. In [11], a multi-valued and ambiguous encryption scheme to ensure the data confidentiality has been proposed. Recently, He et al. [12] proposed a certificateless public auditing scheme (CLPA) for cloud-assisted WBAN. However, we found that in their scheme, the cloud server can get user uploaded data directly which will result in the disclosure of users’ medical information. We know that the cloud server can be divided into public cloud, private cloud, and hybrid cloud. Private cloud is for individuals or companies; security can be guaranteed. But public cloud is an open environment, so if the confidentiality of the data is not achieved, the user’s sensitive information will be disclosed to the cloud service providers. So we think that their scheme has security defect.

3. Data Transmission Security for Mobile-Health Systems

The Mobile-Health (M-Health) system has been envisioned as a promising approach to improving healthcare quality and save lives in the aging society. In MHealth systems, the Personal Health Information (PHI) is collected by Body Area Network (BAN) and aggregated by smartphone. Then the data is sent to the healthcare center via cellular networks. With the increasing popularity of mobile healthcare, the medical data sent to base stations may aggravate the already over-burden cellular networks. Fortunately, Device-to-Device (D2D) communications are proposed to be an advantageous solution to meet with the explosive demanding of spectrum because they can be operated on the same time/frequency resources over short distances. Consequently, we propose to transmit the PHI data through D2D communications in M-Health systems.

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. Most of these works mainly focus on either anonymous authentication or privacy-preserving issues while ignoring the security during data transmission. Lin et al. firstly consider this problem by proposing a strong privacy-preserving scheme against global eavesdropping for eHealth systems. These are pioneer works on security-aware data transmission for M-Health systems while they don’t take into account the D2D-assist data transmission scenarios.

Actually, security-aware D2D-assist PHI transmission for M-Health systems is challenging due to the privacy sensitive characteristics of PHI data and the insecure D2D transmission. Specifically, the protocol design should consider the following issues: i) How to guarantee the PHI not to be accessed by the relays while the relays are able to judge whether the data is altered by attackers? ii) How to achieve mutual authentication between the source client of the data and its intended physician without interaction? iii) The proposed protocol should be light weight in the sense that the mobile terminals have energy and storage constraints, i.e., the computational and communication cost should be low. iv) The protocol should be robust enough to face the threat when part of the keys is exposed, i.e., the PHI remains secure even if part of the keys is disclosed.

In order to address the above issues, we use Certificateless public key cryptography
(CLPKC) to achieve the designed security objectives. In CLPKC, the users’ private key is not generated by the Key Generator Center (KGC) alone but a combination of the contributions of the KGC and the user. The KGC does not know the user’s private key but can authenticate its public key. In this way, the key escrow problem of the ID-based public key cryptography is solved. Additionally, the CLPKC avoids the problem of certificate revocation, storage and distribution in certificate-based public key cryptography. Generally, the CLPKC has three techniques, i.e., Certificate less signature, certificate less encryption and certificate less signcryption. The three techniques are usually realized by three different algorithms and are applicable in different application scenarios.

In order to adaptively work as a signcryption scheme, a signature scheme, or an encryption scheme with only one algorithm, a certificate less generalized signcryption (CLGSC) scheme is put forward by Ji et al. Later, the authors propose more efficient CLGSC scheme. However, all the existing CLGSC schemes are realized with pairing operations, which is time consuming and has low computational efficiency. Motivated by the above, we propose a new CLGSC scheme which is low in time consumption cost and proven to be secure in confidentiality and unforgeability.

The new CLGSC algorithm can operate on three modes: signcryption mode, signature mode, or encryption mode adaptively. We use CLGSC to design a light-weight and robust security-aware (LRSA) D2D-assist data transmission protocol for M-Health systems. Firstly, the PHI data is encapsulated with signcryption mode and the source’s identity is encrypted with the encryption mode by the source client, thus achieving data confidentiality and integrity, mutual authentication and contextual privacy. In addition, a session key is introduced in the signcryption algorithm to enhance the security strength. And the session key is updated by a secure hash function at the end of each transmission session to achieve forward security. Moreover, the source client and all the relays sign on the encrypted data to guarantee data integrity. Notably, the proposed LRSA protocol can also achieve anonymity and unlinkability by using the pseudo identity and a random number in the ciphertext of the identity.

We propose a new efficient certificate less generalized signcryption (CLGSC) scheme. The proposed CLGSC is built based on Elliptic Curved Discrete Logarithm Problem (ECDLP) and implemented without pairing. It has the lowest computational cost comparing with the existing CLGSC schemes. Moreover, it is proven to achieve confidentiality and unforgeability in the random oracle model (ROM) under the Discrete Logarithm Problem (DLP) and CDHP (Computational Diffie-Hellman Problem) assumption.

We design a lightweight and robust security-aware (LRSA) D2D-assist data transmission protocol for M-Health systems based on the proposed CLGSC scheme. LRSA achieves data confidentiality and integrity, mutual authentication and contextual privacy by using the proposed CLGSC scheme. Furthermore, anonymity and unlinkability are simultaneously realized by using the pseudo identity and choosing different random numbers at different sessions. Additionally, LRSA has the characteristics of forward security with hash chain of the session key. We analyze security properties of the proposed LRSA and compare it with the other protocols terms of data confidentiality and integrity, mutual authentication, anonymity, unlinkability, forward security and contextual privacy. Moreover, the computational overhead and communication overhead are also compared between our proposed CLGSC algorithm and the other Certificateless generalized signcryption schemes.

4. Problem Statement

The Wireless Body Area Networks (WBAN) is build to collect data from the
patients. The health monitoring applications are constructed with a collection of sensors. The mobile health application collects data from various patients. The data transmission operations are protected with security and privacy features. The Lightweight and Robust Security Aware (LRSA) Device to Device (D2D) assisted data transmission protocol is used for the WBAN data forwarding process. The Medical Service Provider (MSP), Network Manager (NM) and the WBAN client are involved in the mobile health services. The signcryption methods are used for the security process. The event discovery and relay selection operations are also supported in the system. The system is designed with the following objectives.

- To design a mobile health system for remote health services
- To use Wireless Body Area Network (WBAN) for data collection and forwarding process
- To support optimal relay selection for data forwarding operations
- To monitor blood pressure, body temperature and Oxygen level for the patients
- To support event discovery and decision support operations
- To provide aggregation query process on patient information and monitoring process
- To support priority based data forwarding process for health data transmission process
- To provide data cache and replica models for data forwarding process

5. Security Guaranteed Event Discovery and Data Transmission under WBAN

The health monitoring applications are built with the support of the sensor devices. The sensors continuously monitor the body condition of a person and update the data to the centralized system. The Wireless Body Area Networks (WBAN) is constructed to monitor the patients. The data transmission operations are carried out with the mobile communication technology. The WBAN Client, Network Manager and Medical Service Providers are involved in the mobile health monitoring system. The data values are forwarded through the relay nodes. The network managers act as an interface the WBAN client and the medical service provider. The lightweight Certificateless security model is used to provide the security for the data transmission process in mobile health services.

The mobile health service security scheme is enhanced with optimal relay selection and data forwarding policies. The medical data aggregation based query processing is supported in the system. Event detection and decision support operations are integrated with the system. The Priority level based data forwarding, data cache and replica schemes are integrated to support efficient data communication tasks.

The M-Health services are built with D2D data communication security models. Relay selection and query processing operations are improved with data forwarding schemes. Node anonymization and data privacy features are combined to improve the security process. The M-Health system is divided into six major modules. They are Medical Service Provider, WBAN Client, Network Manager, Relay selection and data forwarding process, Privacy and security services and Query Management.

The medical service provider manages the patient health information and health care services. The patient details are collected by the WBAN client application. The network manager is an interface between the WBAN client and medical service provider. Relay selection and data forwarding module is designed to choose the relay node for data transmission process. Node and data values are protected in the privacy and security process. The query management module handles the query processing and event detection operations.

The Medical Service Provider (MSP) application is build to handle the patient health
management services. Patient health information are collected from the Wireless Body Area Network (WBAN) clients. Patient health levels and criticality conditions are continuously monitored by the Medical Service Providers. Medical assistance and services are provided with reference to the patient health information. The Wireless Body Area Network (WBAN) is constructed with the support of the small sensors used for the health monitoring process. The blood pressure, Oxygen level and body temperature information are observed and maintained by the WBAN clients. The health information are transferred to the Medical Service Provider for health care analysis. Data aggregation and event detection operations are carried out through the WBAN clients.

The Network Manager (NM) is the interface between the Medical Service Providers (MSP) and WBAN clients. The network manager maintains the information about the Medical Service Provider and WBAN clients. Initialization and key generation operations are carried out under the Network Manager environment. The key values are distributed to the Medical Service Providers and WBAN clients. The relay nodes are used to manage the data retransmission operation. The optimal relay selection process is carried out with traffic level and coverage details. The data forwarding process is handled with priority information. Data cache and replica schemes are also adapted to improve the data forwarding process.

The Light-weight and Robust Security-Aware (LRSA) D2D-assist data transmission protocol is used for the secure communication process. The data transmission process is protected with Certificate less Generalized Signcryption (CLGSC) technique. Node and data level privacy is provided in the system. The Advanced Encryption Standard (AES), RSA and Secure Hashing Algorithm (SHA) are employed in the data security process. The query management process is adapted to support medical data access process. Data aggregation based query process provides the health data summary details. Event detection and decision operations are managed under the query management process. The query request and response values are protected with privacy and security features.

6. Conclusion

The Mobile Health (M-Health) services are provided with Wireless Body Area Network (WBAN) and Smart phone technologies. M-Health systems are protected with Light-weight and Robust Security-Aware (LRSA) Device to Device (D2D) assist data transmission protocol. The M-Health services are improved with aggregation based query process, optimal relay selection and data forwarding scheme. Priority based data forwarding and event detection operations are supported with data privacy and security features. The Medical Health (M-Health) services are build with lightweight security based Device to Device (D2D) communication process. The optimal relay selection process improves the data forwarding process. Automatic and request based data transmission operations are supported in the system. Data transmission process is improved with cache and replica concepts. The system can be enhanced to protect sensitive data values in the Patient Health Records. The mobile health services data processing load can be managed with the support of the cloud resources.

REFERENCES


