OPTIMAL RELAY SELECTION AND DATA FORWARDING STRATEGIES FOR SECURE MOBILE HEALTH MONITORING SERVICES

Ms. M.Devi¹ and Dr. G.Kesavaraj²

¹M.Phil Full time Research Scholar, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women (Autonomous), Tiruchengode, Tamilnadu, India.
²Head of the Department, PG and Research Department of Computer Science Vivekanandha College of Arts and Sciences for Women (Autonomous), Tiruchengode, Tamilnadu, India.

Abstract-The Wireless Body Area Networks (WBAN) are used to support health monitoring services. The mobile health services are provided to assist health care monitoring services. The Light-weight and Robust Security-Aware (LRSA) D2D-assist data transmission protocol is constructed for M-Health systems. 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 within a single channel. The mobile health system is built with three elements Network Manager (NM), WBAN Client and Medical Service Provider. The network manager handles the initialization and key generation operations for the WBAN clients and Medical Service Providers. 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. Priority level based data forwarding operations are initiated to control the data transmission overhead. Node anonymization and data privacy features are combined to improve the security process. The data cache and replica schemes are also integrated with the system to support efficient data communication tasks.

Keywords-Medical Health Services, Wireless Body Area Networks, Medical Service Providers, Relay Selection and Data Forwarding Process

I. INTRODUCTION

Recent advances in wearable and implementable of wireless sensors in health domain attracted the attention of the research community ranging from theory to practice. These tiny devices with low computing power and limited life, deployed in/on or around a human body, are able to detect and collect the physiological phenomena of the human body and further transmit this information to a collector point that will process it, take decisions, alert or record.

To address the increasing use of sensors in this area, a new technology called WBAN (Wireless Body Area Networks) has emerged in response to the various disadvantages associated with wired sensors commonly used to monitor patients in hospitals and emergency rooms. The mess of wires attached to a patient is not only uncomfortable for patients, leading to a very limited mobility and making patients anxious, but it is also difficult to manage for staff. Voluntary or involuntary disconnections of sensors are very common and reintegrating these sensors properly is difficult if not impossible. WBAN is a promising technology for various applications and it shall be increasingly necessary for monitoring, diagnosing and treating populations. Recent medical reports predict that the number of people using home health technologies will enormously increase from 14.3 to 78 million.
consumers from 2014 to 2020, respectively. Additionally, body sensors shipments will hit 3.1 million units every year.

WBANs could hence represent a true advance in digital patient care. Thus, the communication between the different wireless nodes deployed in a compact spatial region can be single-hop or multihop. Previous research, confirms that the multi-hop communication is considered as the most appropriate for WBAN networks due to the absorption nature of energy by the human body, entail a very low Signal-to-Noise-Ratio (SNR). Since in the WBANs, the stored data related to a patient plays a critical role in medical diagnosis and treatment, ensuring the security of pertinent information and the privacy of patients is a crucial task. If not securely protected, an adversary may eavesdrops the patient related data and reveal them to social networks or to insurance companies.

II. RELATED WORK

Utilizing mobile devices for remote health care has gained momentum due to its potential for enhancing the quality of life and reducing the load on classic health-care systems [10]. However, only recently has the cost aspect surfaced due to its importance to under-served communities and direct impact on the much needed scalability of mHealth services beyond pilot systems. In [7], the authors survey wireless communications standards and architectures in telehealth systems. The smart home care concept and architecture have been introduced in [6]. However, the cost, among other tradeoffs, associated with data transfer was out of the scope. Recently, the work in [3] uses off-the-shelf Wi-Fi enabled mobile phones to monitor breathing rate.

The CodeBlue project [8] uses a number of medical devices, e.g., pulse oximeter and ECG connected to Zigbee transmitters [4]. These sensors publish relevant information while physicians subscribe to the network via multicasting. Physicians can specify the information needed, such as the identification of patients of interest and vital signs. Exploits the smartphone accelerometer for elderly activity monitoring. On-body sensors are distributed to transmit positions through radio devices to a computer which issues a warning in case of emergency. The system adaptively analyzes body posture and determines the injury level for rescue and treatment purposes.

Focusing on the user experience, the concept of always best connected (ABC) was originally proposed in 2003 where the user is allowed to choose the best available access network and device at any point of time. Although selecting a wireless network interface to upload data is one of the prime objectives of this work and is somewhat related to the ABC concept, it is considerably different since it brings the transfer cost as a major design parameter along with data size, modality and delay tolerance. We target an extensible mHealth system that not only utilizes access technologies, opportunistically, but also accommodates mobile phone sensors as well as on-body medical devices, e.g., pulse oximeter and blood pressure monitor. In addition, we leverage the proximity of mobile phones to minimize the cost of disseminating public health and other advisories. Although having multiple wireless interfaces onboard smartphones today opens room for simultaneously using them, based on the multihomed terminals technology. In this paper, we focus on deciding the least cost interface and leave the possibility of multihoming to future work. The work has studied the similar problem of wireless interface selection on smartphones, yet, with focus on energy-delay tradeoffs. Deng et al. [9] proposed a wireless interface selection scheme where the user objectives are defined in terms of throughput and delay as well as the overall social utility. Furthermore, [11] characterizes the power and throughput tradeoffs of Wi-Fi and Bluetooth radios in smartphones, revealing interesting insights, yet, with no focus on cost issues. The work in [1] exploits multihop communications to facilitate data dissemination in mobile social networks with the objective of relieving the cellular network congestion through mobile data offloading. The second part of this paper aims to reduce the cost for the health-care provider (HCP) in order to disseminate advisory messages among a group of users, subject to a delay constraint.
The cost and consumption of data plans have started to receive attention recently, yet, with different objectives. For instance, [2] proposes a cost–benefit model to decide when to prefetch user data. The objective is to minimize the application response time through prefetching, while meeting budget constraints for battery lifetime and cellular data plan usage. Unlike our work, focuses on prefetching decisions. In addition, [5] proposes a system for data plan sharing among users with limited-quota data plans. The system targets smartphone users with dynamic network usage, where users may over/underuse their data plans. The objective is to allow users with remaining quota to help others who fully consumed their quota. This immediately yields cost savings to borrow users, avoiding high “beyond quota” rates.

To the best of the authors’ knowledge, none of the systems proposed in the open literature targets mHealth with prime focus on cost. This brings about a plethora of new research challenges attributed to pricing. For instance, choosing the least cost radio interface is an open question depending on the cost of the data plan and SMS, size and type of data and the availability of public Wi-Fi. It is worth noting that the proposed system can be extended along the lines of the IEEE 802.21 Standard allow handover and interoperability between heterogeneous networks for seamless upload in case of mobility. This extension is a subject of future research. In addition, sending advisory messages from the HCP to patients, in a cost- and resource-efficient manner, is another research direction presented in this paper.

III. MOBILE-HEALTH SERVICES

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 in this paper.

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 weigh 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 are exposed, i.e., the PHI remains secure even if part of the keys are 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., Certificateless signature, certificateless encryption and certificateless 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 certificateless 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 certificateless 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 ontextual privacy. Moreover, the computational overhead and communication overhead are also compared between our proposed CLGSC algorithm and the other Certificateless generalized signcryption schemes.

IV. SECURITY ISSUES ON MOBILE HEALTH SERVICES

The Light-weight and Robust Security-Aware (LRSA) D2D-assist data transmission protocol is constructed for M-Health systems. 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 mobile health system is build with three elements. They are Network Manager (NM), WBAN Client and Medical Service Provider. The
network manager handles the initialization and key generation operations for the WBAN clients and Medical Service Providers. The WBAN client collects and transfers the health information from the patients. The Medical Service Provider (MSP) analyzes the patient health information collected from the WBAN clients. The following security issues are discovered from the current mobile health services.

- Relay node selection and data transmission scheduling is not optimized
- Data and node level privacy is not provided
- Query processing and event detection operations are not supported
- Data transmission priority levels are not considered

V. OPTIMAL RELAY SELECTION AND DATA FORWARDING STRATEGIES

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 build 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 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 Certificateless 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.

VI. EXPERIMENTAL ANALYSIS

The mobile health services are constructed with Wireless Body Area Networks and Medical Service Providers. Lightweight Robust and Security Aware Device to Device (LRSA) scheme is built with Certificateless Signcryption communication scheme. Optimal Relay Selection based Data Forwarding (ORS-DF) technique is used to support data communication with relay selection process. The system is analyzed with three parameters.

They are Average Throughput, Average Delay and Relay Consumption Rate. The data transmission speed is estimated with the average throughput parameters. The average throughput is estimated with the messages that are transferred through the relay nodes. The relay consumption rate analysis between Lightweight Robust and Security Aware Device to Device (LRSA) and Optimal Relay Selection based Data Forwarding (ORS-DF) is shown in figure 6.1. The Optimal Relay Selection based Data Forwarding (ORS-DF) technique increases the average throughput 20% than the Lightweight Robust and Security Aware Device to Device (LRSA) technique. The average delay is estimated with the data request and data response interval time periods. The Average Delay is estimated with the messages that are transferred through the relay nodes. The relay consumption rate analysis between Lightweight Robust and Security Aware Device to Device (LRSA) and Optimal Relay Selection based Data Forwarding (ORS-DF) is shown in figure 6.2. The Optimal Relay Selection based Data Forwarding (ORS-DF) technique reduces the Average Delay 25% than the Lightweight Robust and Security Aware Device to Device (LRSA) technique. The relay consumption rate is estimated with the messages that are transferred through the relay nodes. The relay consumption rate analysis between Lightweight Robust and Security Aware Device to Device (LRSA) and Optimal Relay Selection based Data Forwarding (ORS-DF) is shown in figure 6.3. The Optimal Relay Selection based Data Forwarding (ORS-DF) technique reduces the Relay Consumption Rate 35% than the Lightweight Robust and Security Aware Device to Device (LRSA) technique.

![Average Throughput Analysis between LRSA and ORS-DF schemes](image)

Figure no.6.1 Average Throughput Analysis between LRSA and ORS-DF schemes
VII. CONCLUSION AND FUTURE WORK

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.

REFERENCES

[1] B1. Han, P. Hui, J. Shao and A. Srinivasan, “Mobile data offloading through opportunistic communications and social participation,” IEEE Trans. Mobile Comput., May 2012.
[2] B. D. Higgins, J. Flinn, C. Peplin and D. Watson, “Informed mobile prefetching,” in Proc. 10th Int. Conf. Mobile Syst. Appl. Serv., 2012.
[3] H. Abdelnasser, K. A. Harras and M. Youssef, “UbiBreathe: A ubiquitous non-invasive WiFi-based breathing estimator,” in Proc. ACM Mobihoc, 2015.
[4] Youssef Khazbak, Mostafa Izz, Tamer ElBatt, Arsany Guirguis and Moustafa Youssef, “Cost-Effective Data Transfer for Mobile Health Care”, IEEE Systems Journal, 2016.
[5] T. Yu, Z. Zhou, D. Zhang, X. Wang, Y. Liu and S. Lu, “INDAPSON: An incentive data plan sharing system based on self-organizing network,” in Proc. INFOCOM, 2014, pp. 1545–1553.
[6] L. M. S. Morillo, L. Gonzalez-Abri, J. A. O. Ramirez and M. A. A. de la Concepcion, “Low energy physical activity recognition system on smartphones,” Sensors, vol. 15, no. 3, 2015.
[7] E. Warpenius, E. Alasaarela, H. Sorvoja and M. Kinnunen, “A mobile user-interface for elderly care from the perspective of relatives,” Informat. Health Social Care, vol. 40, no. 2, 2015.
[8] R. S. Istepanian, “M-health: A decade of evolution and impact on services and global health,” Brit. J. Healthcare Manage., vol. 20, no. 7, pp. 334–337, 2014.
[9] S. Deng and H. Balakrishnan, “All your network are belong to us: A transport framework for mobile network selection,” in Proc. 15th Workshop Mobile Comput. Syst. Appl., 2014.
[10] J. M. Beer and L. Takayama, “Mobile remote presence systems for older adults: Acceptance, benefits and concerns,” in Proc. 6th Int. Conf. Human–Robot Interact., pp. 19–26,2011.
[11] R. Friedman, A. Kogan and Y. Krivolapov, “On power and throughput tradeoffs of WiFi and Bluetooth in smartphones,” IEEE Trans. Mobile Comput., vol. 12, no. 7, Jul. 2013.