ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Security Ensured Data Gathering and Decision Support Framework for Remote Health Services

[1]T. Revanth, [2]K. Manimekalai, [3]S. Ananda vignesh, [4]Mr. P. Sathishkumar
[1-3]UG Student, Department of Computer Science and Engineering,
K.S.Rangasamy College of Technology, Tiruchengode
[4]Assistant Professor, Department of Computer Science and Engineering,
K.S.Rangasamy College of Technology, Tiruchengode

Email id: revktr@gmail.com

Abstract

The smart phones and sensor devices are used to build the mobile health services. The mobile health services provides remote health monitoring process. The sensor devices are adapted to observe and transmit the blood pressure, Oxygen level and body temperature information. The Wireless Body Area Network (WBAN) is constructed with the sensor devices. The radio frequeny is employed 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 mobile health systems are secured with the support of the Light-weight and Robust Security-Aware (LRSA) D2D-assist data transmission protocol. 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 Network Manager (NM), WBAN Client and Medical Service Provider. All the key management operations are carried out under network manager (NM).

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.

Index Terms: Wireless Body Area Networks, Remote Health Services, Device to Device (D2D) Communication, Network Manager and Data Communication Security.

1. Introduction

Human health monitoring has significantly benefited from the current developments in sensor technology and wireless communication, which enabled the utilization of sensor to aid in recording biometric information remotely. The inactive lifestyles have increased the threat of possibly fatal medical circumstances like diabetes, cardiac disease, and high blood pressure and the lack of healthcare have contributed to increase in their risk. Provided the unpredictable nature of deterioration of such conditions, continuous and systematic monitoring considers high priority.

Wireless body area networks also known as Body Sensor Networks (BSN) are a special kind of wireless sensor networks, where a collection of sensors are positioned on the human body measure certain physiological factors of a person and forward it to the monitoring hospital or medical centre. This transmission happens through internet or some kind cellular networks utilizing personal digital assistance or any other devices [5]. The typical body sensor network architecture. Thus, BSN seem to be a favourable solution to the issue of continuous health monitoring. Here, the patients' health information travels through an open wireless channel in order to arrive at the intermediary devices and finally at the monitoring station. This, combined with the fact that the therapeutic decisions are carried out based on the information

received, a substantial focus on the research of BSN has gained significant consideration.

The security in BSN is of vital importance because of coupling the medical information with the resource constrained individual body sensors that require lightweight solutions. Security must be offered between the patients and the physicians via key management solutions. Basically, security solutions provided for body sensor network must satisfy the following security features. The medical information must be accessible only by the specific patient and their doctors thereby ensuring confidentiality. To avoid medical information from getting in to the hands of unauthorized persons, the information must be authenticated. Thus, the information must be encrypted before transmitting and storing at the server. Encryption is one of the powerful for securing medical information. In this paper, lightweight block cipher based on Fiestel Cipher structure has been proposed for encrypting the medical information and key management is achieved using Attribute Based Key-Exchange (ABKE).

2. Related Works

Several research works has been carried out for securing the medical inf network. Cryptographic keys are generated from the electrocardiogram (ECG) signals and are used for encrypting the communication between pair of sensor nodes in BSN. In this work, the ECG values are obtained for a specific interval of the signal and the fast Fourier transform is employed to extract the coefficients. Then feature vectors are generated based on these coefficients that are used for generation of keys. The derived key is then used to encrypt the communication. The aim of this work is to secure the inter sensor communication. The key generated using this approach is different for various people since the ECG value is different for each people.

In [8] a two-tier authentication scheme is used for securing healthcare information's of the BSN. Here, security is achieved in two phases: In the first phase a unique key is generated in a decentralized manner and is used to encrypt the information [4]. In the second phase, the key is utilized as a session key for authenticating data aggregation node from the sensor node. This approach provides security, authorization and confidentiality of the healthcare information.

A hybrid authenticated key agreement through rekeying has been proposed for body sensor networks [9]. The approach is based on symmetric cryptography and elliptic curve for the purpose of key agreement. [10] uses a Elliptic Curve Cryptography (ECC) for generating keys that is used to encrypt the communication between the sensor node and the base station. In this approach, RC5 block cipher is used for encryption and decryption process. This process ensures data integrity and confidentiality.

In [1] security in body sensor network is achieved by employing cryptographic techniques. Here, the ECG signals are utilized to generate keys. In this work, encryption is performed using Advanced Encryption Standard (AES). The Public Key Cryptography (PKC) with re-keying approach has been utilized for key establishment [2]. RSA and DHECC parameters are utilized for key agreement protocol that provides rekeying features. A particular routing algorithm has been used in the agreement phase for achieving resilience, scalability and memory efficiency. But the RSA and DHECC as well as PKC increases the computational cost of the BSN.

A novel chaos based encryption technique has been developed [3] for avoiding unauthorized access of ECG signal in inter- body sensor network communication. Here true random numbers are used for deriving the chaos key. This approach uses Diffie Hellman key exchange algorithm for exchanging the key between the node and the base station.

In [7] EKG is used as physiological measures to generate cryptographic keys for securing inter sensor communication. First the communicating sensor nodes sense EKG values and then hashing and watermarking approaches are applied to exchange values to generate public key for communication also utilizes biometric measures as symmetric keys as they as random. In this framework, key refreshment concept is utilized where the server provides key refreshment schedule to all the nodes of the BSN. This schedule exchanges the key allocated to it for communication. Here three keys namely, communication key, administrative key and basic key are utilized.

3. Secured Data Transmission Protocol 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., Certificateless signature, certificateless 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 certificateless generalized signcryption (CLGSC) scheme is put forward by Ji et al. Later, the authors propose more efficient CLGSC scheme. 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.

4. Issues on Secured Data Transmission Protocol

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. 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.

5. LRSA Protocol

In this section we design a lightweight and robust securityaware (LRSA) D2D-assist data transmission protocol based on the proposed CLGSC scheme. Due to generalized property of CLGSC, the proposed protocol is able to effectively achieve various security and privacy protection requirements at source, relays and destinations. Firstly, we give an overview of the proposed protocol. Then the protocol is described in details. For simplification of expression, we may use "client" to denote "WBAN client". The "pseudo identity" of the client is presented as "identity".

In order to achieve the design goals, certificateless signcryption, Certificateless encryption and certificateless signature are jointly introduced into the protocol. Firstly, at the system initialization step, the clients and physicians register to the NM to generate their full private keys and public keys. Meanwhile, the clients connect to his physicians and generate the initial session key with him through key agreement protocol. Then, the source client with pseudo identity S collects its PHI m and formulates the information as $M = (\mu S||e^{S}{}_{H}||e^{H}{}_{N})$, where μS is the signcryption of m performed by the source client, i.e., $\mu S = CLGSC(S,H,m)$. It can only be decrypted and verified by the intended physician H with his full private key. The identity of the source client is encrypted by S with the public key of the physician using certificateless encryption mode, i.e., $e^{S}{}_{H} = CLGSC(H, S)$. Meanwhile, the identity of the intended physician is also encrypted with the public key of the NM, i.e., $e^{H}{}_{N} = CLGSC(\_,N,H)$. Notably, $e^{S}{}_{H}$ and $e^{H}{}_{N}$ protect the identity privacy of source and destination for the PHI to guarantee contextual privacy.

During data transmission process, the packet M is treated as a whole before getting the NM and is signed by the relays to guarantee data integrity. Specifically, the source S signs on m as $\sigma_S = CLGSC(S, \Phi, M)$ and appends it with the data. The relays verify the signature and forward the data with their signatures. The messages passing through the path. Note that the NM parses the data to get eHN and decrypt it for the intended physician of the data. Upon receiving the data $(\mu^{S}||e^{S}{}_{H})$ from the NM, the physician firstly decrypts eS0 H to obtain source WBAN client's pseudo identity S. Then the physician decrypts and verifies μ_S with its full private key and S's public key for accessing the PHI and providing the corresponding services.

The proposed LRSA protocol is composed by the following four phases: System initialization, data formulation, data transmission and data receiving.

5.1. System initialization. System parameter generation.

Given the security parameter k, the network manager NM generates two primes p and q such that $q|p-1$. P is a generator of cycle group G, which is on ECC with order q. Moreover, the NM randomly selects $x_N \in Z^{*}{}_{q}$ as the master private key and computes the public key XN = xNP. The NM additionally chooses four secure hash functions: $H_0 : Z*q \rightarrow Z*q$, $H_1 :\{0, 1\}* XG$ XG XG $\rightarrow Z*q$,H_2: G ->$Z*qXZ*q \rightarrow Z*q$,H3 : $Z*qXZ*qXZ*q \rightarrow \{0, 1\}*$. The system parameter is published as params = (p, q, P,XN,H_0,H_1,H_2,H_3).

Registration. Both the WBAN clients and physicians (named "user") register to the NM for joining the system. The WBAN clients use pseudo identity, denoted by C, for anonymity while the physicians use real identity H.

• The user $D \in \{C,H\}$ randomly selects $xD \in Z* q$ as the secret value and computes $X_D = x_D P$ as its partial public key.

• The user sends its identity and partial public key (D,X_D) to the NM for registration.

• The NM randomly selects $y_D \in Z* q$ and computes $Y_D = y_D P$, $z_D = yD+xNH1(D, Y_D,X_D,X_{N)}$ for the register D with partial public key X_D.

• The partial private key z_D is sent to the register through secure channel and the public key (X_D, Y_D) is stored in the public tree by the NM.

The full private key of user D is (x_D, z_D). Note that D may judge the validity of the partial private key by checking whether $Y_D + H_1(D, Y_D, X_D, X_N)X_N = z_D P$.

Initial session key agreement. When a WBAN client and a physician establish client/server relationship, they should negotiate an initial symmetric session key for their coming data transmission. They may generate the symmetric key at both sides via a secure key agreement protocol, i.e., Diffie- Hellman key exchange. Substantially, the main purpose of this process lies in constructing a consensus between the WBAN client and his physician for their first communication event. The security of their successive communications are realized based on their former session key, i.e., $K_D i^{t+1}$ is a function of K_D^i t . The corresponding session key is refreshed after each transmission.

5.2. Data formulation.

This step is performed by the source client with identity S. Firstly, S selects his intended physician H for receiving the PHI m and refers to its key record table for the session key with H, denoted by K_t, at current session t. Then S runs certificateless signcryption algorithm CLGSC(S,H,m) on m as follows:

• S randomly chooses $r \in Z* q$ and computes h1 $=H_1(ID_H, Y_H, X_H, X_N)$;
• Computes $f_1 = r_P$, $f_2 = r/(x_S + z_S + f_3)$, $f_3 = H_2(f_1, I_{DS}, m)$;
• Computes $m' = H_3(v_1, v_2, K_t) \in$
m, where $v1 = rX_H, v_2 = r(Y_H + h1X_N)$;
• Return $\mu_S = (f_1, f_2, f_3, m')$ as the ciphertext.
The signcryption of S for H on m is presented as $\mu_S = (f_1, f_2, f_3, m', t)$.

Moreover, the source client performs certificateless encryption on his identity S and intended physician identity H for contextual privacy. $I \in \{H,N\}$ denotes the entity NM or the physician and $D \in \{S,H\}$ denotes the identity of S or H. The certificateless encryption algorithm CLGSC(_, I,D) is performed as follows

• S randomly picks $r \in Z*q$ and computes $f_1 = r_P$, $f_3 = H_2(f_1, I, D)$;
• Computes $D' = H3(v_1, v_2) \in D$,
where $v_1 = rXI$, v2 =r(YI + XNH1(I, YI ,XI ,XN)).D is encrypted as eDI= (f1, f3,D′) with the public keyof entity I. Specifically, e_H is an encryption on S with H's public key, which can only be decrypted with H's private key. e^N His an encryption on H with N's public key, which can only be decrypte with N's private key. the source S. Before sending the data out, the source client signs on the data by implementing certificateless signature algorithm CLGSC(S, Φ,M) as follows:

• S randomly chooses $r \in Z*q$;
• Computes $f_1 = r_P$, $f_2 = r/(x_S + z_S + f_3)$, $f_3 = H_2(f_1, S, M)$.
The signature of S on M is $\sigma_S = (f_1, f_2, f_3)$. The client S sends the data M, his signature and his identity in the formate data = $(M||S||\sigma_S)$ to the predetermined relay R_1.Simultaneously, S updates his key record table by refreshing its session key with H as $K_{t+1} = H_0(K_t)$.

5.3. Data transmission

After receiving the data from the source S, R1 parses the sender's identity S and signature σ_S from data. Then, R1 searches the public tree for the sender's public key (XS, YS) and verifies the signature as follows:
Computes $f_1 = f_2(X_S + Y_S + H_1(S, Y_S, X_S, X_N)X_N + f_3 P)$, where $f_3 = H_2(f_1, S, M)$ and checks $f'_1 = f_1$.

If the equation holds, R1 accepts the data. Before sending M to the next relay R_2, R_1 also signs on M by performing algorithm CLGSC(R_1,Φ,M) with his private key (xR_1 , zR_1) and generates its signature σR_1 . Similarly, R_1 appends M with his identity and signature, formulating data = $(M||R_1||\sigma R_1)$ and sends it to the next relay R_2. All the other relays forward the data in the same way, i.e., verifying the signature of the sender, generating his signature on M, sending it to the next relay. When the data arrives at the NM, the NM firstly checks the validity of the sender's signature as the relays have done. Then, the NM parses M as $(\mu_S||e^S_H||e^H_N)$ and decrypts $e^H_N = (f_1, f_3, H')$ by computing $v'_1 = x_N f_1$, $v_2 = zN_{f1}$, $H = H_3(v'_1, v'_2) \in H'$.If $H_2(f_1, N, H) = f_3$ holds, the NM sends $(\mu S||e_{SH})$ to the corresponding physician H.

5.4. Data receiving and processing.

Similar to the NM, the physician H decrypts eS H with his private key after receiving the data μS||eS H and obtains the source identity S of the PHI. Then, H accesses the public tree for the source's public key (X_S, Y_S) and refers to his session key record table for the session key Kt with S. H decrypts and verifies $\mu_S = (f_1, f_2, f_3, m', t)$ as follows:
• Computes $v'_1 = x_H f_1$, $v'_2 = z_H f_1$, m $=H_3(v'_1, v'_2, Kt) \in m'$;
• Checks $H_2(f_2(X_S + Y_S + h'1X_N + f_3 P), IDS_m) = f_3$.
If the equation holds, the message m is accepted. Additionally, the physician H refreshes its session key with S as $K_{t+1} = H_0(K_t)$.

6. Security Ensured Data Gathering and Decision Support Framework

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 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 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.

7. Performance 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 build 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 Average Delay parameter.

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 average delay analysis between Lightweight Robust and Security Aware Device to Device (LRSA) and Optimal Relay Selection based Data Forwarding (ORS-DF) is shown in figure 7.1. 1..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.

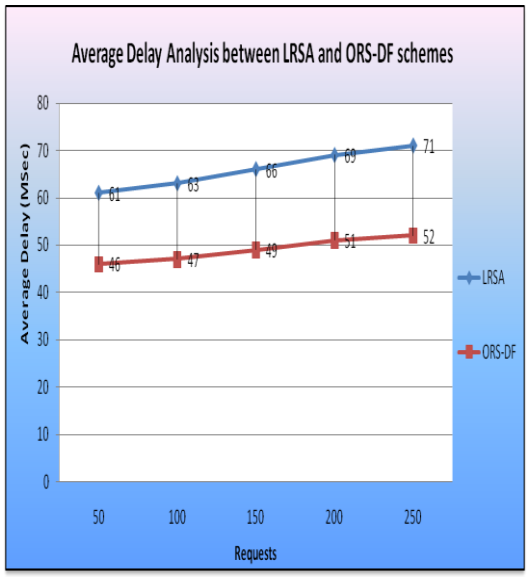

Figure no.7.1. Average Delay Analysis between LRSA and ORS-DF schemes

8. 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 mobile health monitoring services can be improved with intrusion detection schemes.

References

[1] Liu, J. W., Zhang, Z. H., Rong, S., & Kwak, K. S. (2012). Certificateless remote anonymous authentication schemes for wireless body area networks. Proceedings of the IEEE International Conference on Communications (ICC).

[2] Eldefrawy, M. H, Khan, M. K., & Alghathbar, K. (2010). A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography. Proceedings of the IEEE International Conference on Anti-Counterfeiting Security and Identification in Communication.

[3] Sufi, F., Han, F., Khalil, I., & Hu, J. (2010). A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications. Security and Communication Networks.

[4] A. Siva Sangari, J. Martin Leo Manickam, "Secure Communication over BSN Using Modified Feather Light Weight Block (MFLB) Cipher Encryption", Journal of Software Volume 10, Number 8, August 2015

[5] Guanglou Zheng, Gengfa Fang, Rajan Shankaran, Mehmet A. Orgun, Jie Zhou, Li Qiao and Kashif Saleem, "Multiple ECG Fiducial Points based Random Binary Sequence Generation for Securing Wireless Body Area Networks", IEEE Journal of Biomedical and Health Informatics, 2016.

[6] Haipeng Peng, Ye Tian, J¨urgen Kurths, Lixiang Li, Yixian Yang and Daoshun W, "Secure and Energy-Efficient Data Transmission System Based on Chaotic Compressive Sensing in Body-to-Body Networks", IEEE Transactions On Biomedical Circuits And Systems, 2017.

[7] Aftab, A., & Farrukh, A. K. (2010). An improved EKG-based key agreement scheme for body area networks. Proceedings of the International Conference on Information Security and Assurance.

[8] Kanjee, M. R., Divi, K., & Liu, H. (2010). A two-tiered authentication and encryption scheme in secure healthcare sensor networks. Proceedings of the International Conference on Information Assurance and Security.

[9] Amin, N., Asad, M. N., & Chaudhry, S. A. (2012). An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem. Proceedings of the IEEE International Conference on Networking, Sensing and Control.

[10] Malasri, K., & Wang, L. (2009). Design and implementation of a secure wireless mote-based medical sensor network. Sensors.