Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 7 (2017) pp. 2095-2117

http://www.ripublication.com

Reputation based Incentive Scheme for Secured Data Privacy in Wireless Body Area Network Communication

Ms. I.Shanmugapriya[1] and Dr. K.Karthikeyan[2]
[1]PhD Scholar, Assistant Professor, Dr.SNS Rajalakshmi College of Arts and Science (Autonomous), Coimbatore-49, Tamil Nadu, India.

[2] Head Department of Computer Science, Government Arts and Science College, Karambakudi, Pudhukottai (Dt) Tamil Nadu, India

Abstract

Secure communication over wireless body area network (WBAN) is significant issue because it lacks security and privacy level of data while performing transmission. To improve the security and privacy of wireless body area network communication, Repute Derivative Incentive and Sparse Sampled Data Aggregation (RDI-SSDA) scheme is proposed. The RDI-SSDA initially used Repute Derivation Based Incentives scheme to identify the trustworthy users in network over a period of time using second order derivative for secured data communication and improving the throughput. Next, RDI-SSDA scheme used Preferential Sparse Sampled Data Aggregation for collecting sensed data of sensor nodes in WBAN. The Preferential Sparse Sampled Data Aggregation considers a tolerance delay factor that refers the maximum delay a packet can support before its delivery. With this tolerance delay factor, the RDI-SSDA scheme selects data packets with minimum tolerance delay for aggregating the data at aggregators and therefore improves the data aggregation efficiency. Finally, compressed sensing is performed for each aggregated data through sensing matrix in which encryption and decryption is performed to improve the privacy of data transmission in WBAN. The RDI-SSDA scheme conducts the experimental works on parameters such as data privacy level, throughput and data aggregation efficiency. The experimental results show that the RDI-SSDA scheme is able to improve the privacy level of data and data aggregation efficiency when compared to state-of-the-art works.

Keywords: trustworthy users, reputation, incentive, data aggregation, tolerance delay compressed sensing, sensing matrix

1. INTRODUCTION

In a wireless body area sensor network (WBAN), sensor nodes are placed around a patient's body for monitoring their body functions and the neighbouring environment. With the help of a WBAN, a patient's health related information like temperature, respiration, heart rate, blood pressure, blood sugar, and pH are remotely monitored. The monitored data about patients are collected and transmitted to the sink node i.e. doctor for analysing patient current disease status. The security and privacy are major problem is to be solved in WBAN while performing the data transmission. Therefore, a new scheme is designed for improving the security and privacy of wireless body area network communication.

Recently, many research works have been designed for ensuring the security and privacy in WBAN. For example, an attribute-based encryption and signature scheme was introduced in [1] to secure data communications among wearable sensors and the data consumers by using Cipher text-Policy Attribute Based Encryption. This protocol improves the data security and reduces energy consumption and communication/computation overhead. A privacy-preserving and multifunctional health data aggregation (PPM-HDA) mechanism was developed in [2] for guarding users' privacy against many threats and lessening the communication overhead. Though, fault tolerance in the framework of health data aggregation was not considered.

A secure and privacy-preserving key management scheme was presented in [3] that preserve patient's identity privacy, sensor deployment privacy and location privacy through exploiting the blinding technique and embedding human body's symmetric structure into Blom's symmetric key mechanism with modified proactive secret sharing. However, the data privacy rate was not at required level. An elliptic curve cryptography-based public key cryptosystem was designed in [4] that allowed the user to authenticate at the sensor node within a WBAN under certain access privileges. This cryptosystem improves security with the lower communication and computational costs. But, the security level of data packet transmission was not sufficient.

A lightweight and confidential data discovery and dissemination protocol was developed in [5] that employed low-complexity symmetric cryptographic techniques for achieving data confidentiality in WBAN. This protocol improves authenticity and integrity of the disseminated data. But, trustworthiness remained unsolved. Revocable and Scalable Certificateless Remote Authentication Protocol with Anonymity was intended in [6] to make sure the security and privacy of the patient's health status in WBAN.

An Energy-efficient cluster-based security mechanism was designed in [7] for intra-WBAN and inter-WBAN communications for healthcare applications and improving the network lifetime. However, privacy of data transmission was remained unaddressed. The Multi-valued and Ambiguous Scheme was designed in [8] to attain data confidentiality and secure data communications in WBAN. But, the data delivery rate was lower.

A multi-hop topology formation game (MTFG) was designed in [9] for addressing the problem of optimizing multihop transmission in WBAN. The MTFG improves PHY security and reduced end-to-end delay. But, data privacy level was poor. A lightweight multilayer authentication protocol based on ECC encryption was employed in [10] to safeguard the integrity, confidentiality, and authenticity of the data in WBANs. However, security and privacy related issues were remained unaddressed.

In order to overcome the above mentioned existing issues in WBAN, Repute Derivative Incentive and Sparse Sampled Data Aggregation (RDI-SSDA) scheme is developed. The research objective of RDI-SSDA scheme is formulated as follows,

- To identify the trustworthy users in WBAN for improving the security of data communication with higher throughput rate, Repute Derivation based Incentive is employed in RDI-SSDA scheme.
- To improve the performance of data collection in WBAN with higher data aggregation efficiency, Preferential Sparse Sampled Data Aggregation is used in RDI-SSDA scheme.
- To enhance the privacy of aggregated data, compressed sensing is performed through sensing matrix in RDI-SSDA scheme.

The rest of this paper is organized as follows. Section 2 explains Repute Derivative Incentive and Sparse Sampled Data Aggregation (RDI-SSDA) scheme with the aid of architecture diagram. Section 3 and Section 4 presents the experimental section with detailed performance analysis. Section 5 explains the related works. Finally, Section 6 concludes this paper.

2. REPUTE DERIVATIVE INCENTIVE AND SPARSE SAMPLED DATA AGGREGATION SCHEME

The Repute Derivative Incentive and Sparse Sampled Data Aggregation (RDI-SSDA) scheme is designed with the objective of improving the security and privacy of data transmission in WBAN for health monitoring. In RDI-SSDA scheme, repute derivation based incentive algorithm is designed with aiming at identifying the trustworthy users in WBAN for achieving secure data communication and enhancing the throughput. Besides, Preferential Sparse Sampled Data Aggregation is performed in RDI-SSDA scheme for enhancing the performance of data collection with higher data aggregation efficiency. Further, compressed sensing is performed in RDI-SSDA

scheme through sensing matrix in order to enhance the privacy of aggregated data. The architecture diagram of Repute Derivative Incentive and Sparse Sampled Data Aggregation (RDI-SSDA) scheme for Secured data Privacy is shown in below,

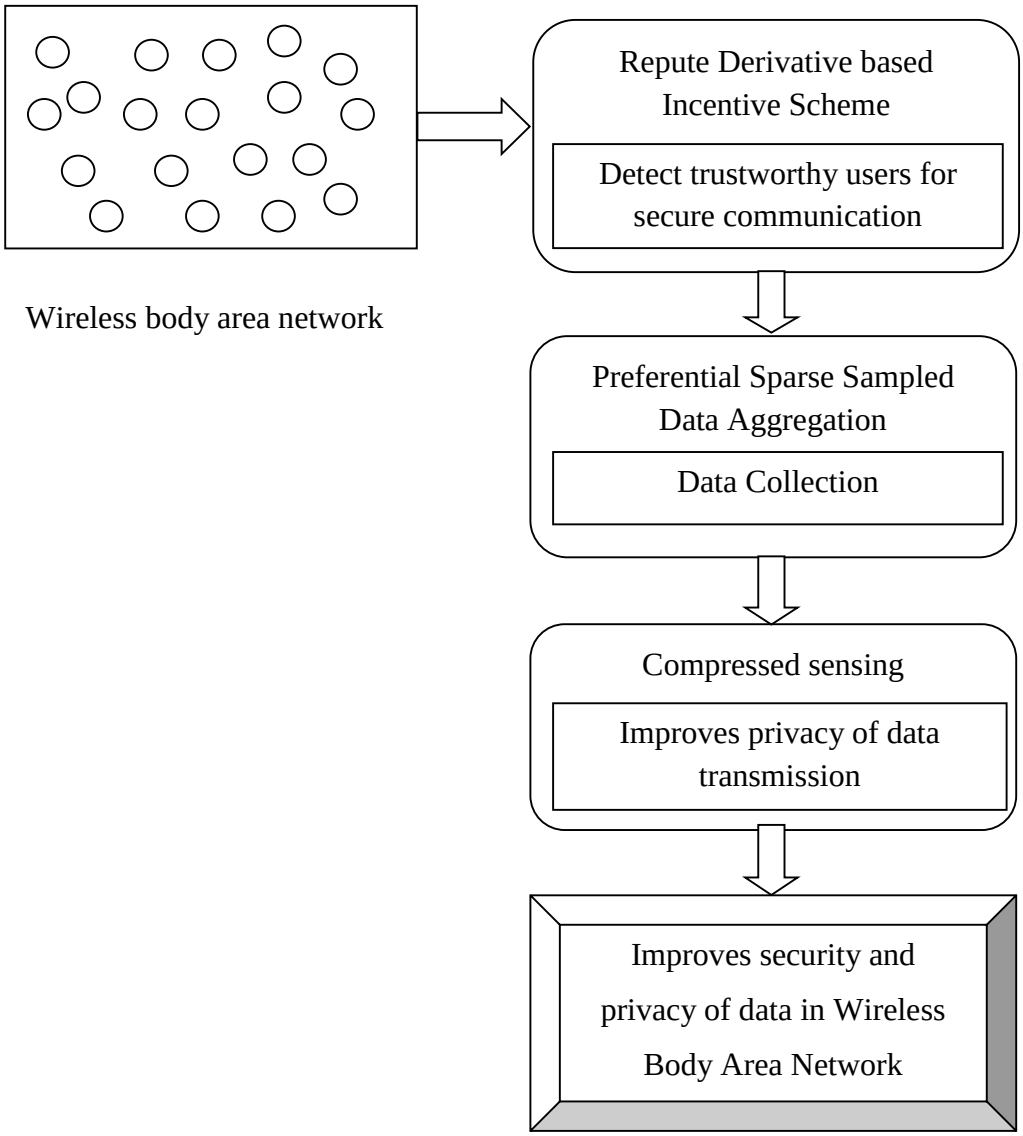

Figure 1. Architecture Diagram of Repute Derivative Incentive and Sparse Sampled Data Aggregation scheme for Secured data Privacy

As shown in Figure 1, RDI-SSDA scheme initially detects the number of trustworthy users in WBAN with application of Repute Derivative based Incentive algorithm. This Repute Derivative based Incentive algorithm enhances the security of data communication and therefore improves the throughput rate in WBAN. Next, RDI-

SSDA scheme accomplish Preferential Sparse Sampled Data Aggregation for collecting the data sensed form and the sensor node with higher data aggregation accuracy. At last, compressed sensing is carried out for each aggregated data to improve the privacy of data transmission in WBAN. The detailed explanation about the RDI-SSDA scheme is described in forthcoming sections.

2.1 Repute Derivation Based Incentive for Identifying Trustworthy User

In WBAN, detecting the trustworthiness users is significant in order to improve the security of data communication. The RDI-SSDA scheme selects the trustworthy users for securely transmitting the data packets to sink node by using the incentive value of sensor nodes. Let consider the WBAN consisting of many sensor nodes like $SN_i = SN_1, SN_2, SN_3, \ldots SN_n$. The incentive value is provided to every sensor nodes based on their reputation i.e. past history of data packet forwarding. Thus, RDI-SSDA scheme computes the reputation value for each the sensor nodes in network through considering the past history of data packets delivery for identifying the trustworthy users for data packet dissemination. Based on measured reputation value, trustworthy users in WBAN are detected for secured data packet dissemination. Then incentive value is given to trustworthy users based on the reputation. The reputation of sensor node is defined as the mean differentiation between the successful data packets delivery and the data packets dropped to the total number of data packets transmitted.

The initial incentive value of all trustworthy users is initialized as 1. On the process of communication in the network, the incentive value of trustworthy users may get increment (+1) depend on the packets being forwarding to the next corresponding node in the route path. By measuring the reputation value, RDI-SSDA scheme identifies the number of trustworthy users and malicious users in the network in order to enhance the security of data communication in WBAN. The trustworthy users in WBAN are good sensor node which broadcasts the data packets to the neighbouring sensor node without any data packet loss. The malicious users drop the every data packets that have received from the source node.

The reputation value of a sensor node is calculated by using following mathematical formula,

$$R_{SN_i} = \frac{(DP_T - DP_D)}{DP_N} \quad (1)$$

From the equation (1), DP_N represents the total number of data packets that the sensor node received and DP_T designates the number of data packets that sensor node successfully transmitted to neighbouring node and DP_D is number of data packets that the sensor node dropped. The reputation value (R) of a sensor node is measured over a period of time t by using second order derivatives which is formulated as,

$$f^{"} = \frac{d}{dt}\left(\frac{dR_{SN_i}}{dt}\right) \quad (2)$$

$$f^{"} = \frac{d^2R_{SN_i}}{dt^2} \quad (3)$$

By using the equation (2) and (3), reputation value for each sensor node is determined over a period of time. With the aid of determined reputation value, RDI-SSDA scheme detects the trustworthy users and malicious users in WBAN. If the detected node is trustworthy user, then the incentive is given to node. Otherwise no incentive is given. On the process of communication in the network, the incentive value of trustworthy user is gets incremented (+1) based on reputation value. The Repute Derivation based Incentive scheme for detecting the trustworthy users in WBAN is shown in below Figure 2,

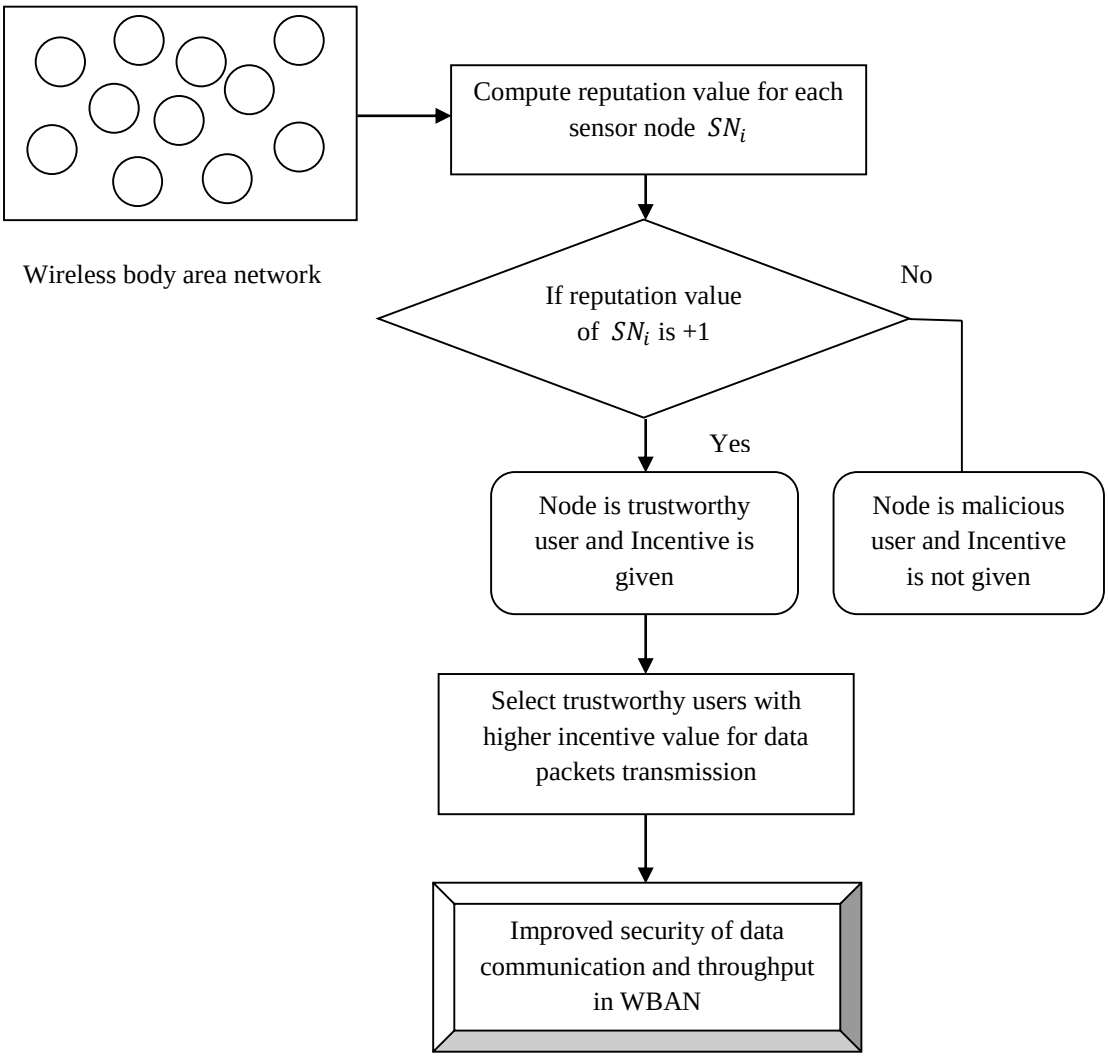

Figure 2 Repute Derivation Based Incentive Scheme for Detection of Trustworthy Users

As shown in Figure 2, RDI-SSDA scheme improves the security of data communication through selecting the trustworthy users with higher incentive value for data packets transmission which resulting in enhanced throughput in WBAN. The algorithmic process of Repute Derivation based Incentive is shown in below,

// Repute Derivation based Incentive Algorithm

Input: Sensor nodes '$SN_i = SN_1, SN_2, SN_3 \ldots, SN_n$',

Output: Improved throughput

Step 1:Begin

Step 2: **For** each sensor node SN_i

Step 3: Measure reputation value over a period of time using (3)

Step 4: **if** $R_{SN_i} = +1$

Step 5: $SN_i$is a trustworthy user

Step 6: **else if** $R_{SN_i} = -1$

Step 7: $SN_i$is a malicious user

Step 8: **end if**

Step 9: **if** $SN_i$is trustworthy user then

Step 10: the incentive is given to node

Step 11: **else**

Step 12: the incentive is not given to node

Step 13: **end if**

Step 14: The trustworthy user with higher incentive value is selected for transmitting data packets in WBAN

Step 15: **End for**

Step 16: End

Algorithm 1 Repute Derivation based Incentive Algorithm

By using the above algorithmic process, RDI-SSDA scheme finds the trustworthy users in communication route path for improving the security of data transmission in WBAN. The Repute Derivation based Incentive Algorithm initially computes reputation value for all the sensor nodes in network. By using reputation values, then this algorithm identifies the number of trustworthy users and malicious users in

WBAN. Subsequently, Repute Derivation based Incentive Algorithm assigns incentive value for trustworthy users. The incentive value of trustworthy users is gets incremented or decremented according to their reputation value on the process of communication. Finally, RDI-SSDA scheme chooses trustworthy users with higher incentive value in network for enhancing security data communication. This helps for improving the throughput in WBAN in an efficient manner.

2.2 Preferential Sparse Sampled Data Aggregation

The Preferential Sparse Sampled Data Aggregation is an essential operation in WBAN where the sensed data of the dissimilar sensor nodes are collected and transmitted to the sink. The data aggregation process in WBAN is shown in below Figure 3.

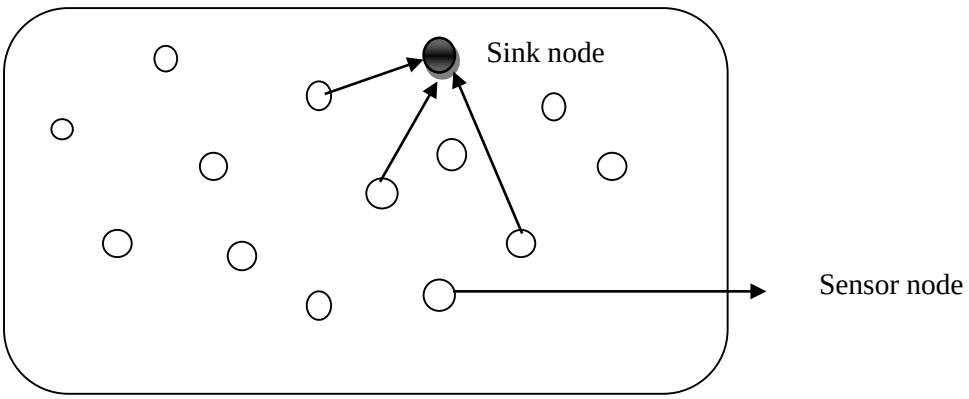

Figure 3 Data Aggregation Process

As shown in Figure 3, the sensor nodes in WBAN sense the information. The sensed information of multiple sensor nodes are collected at the aggregator node i.e. sink and then transmitted to the corresponding users. The Preferential Sparse Sampled Data Aggregation defines a tolerance delay factor for each data packets sensed form the sensor nodes that refers to the maximum delay a packet can support before its delivery. Therefore, a tolerance delay factor is defined as the time from a packet's first transmission until its successful arrival at the sink. By measuring this tolerance delay factor, the RDI-SSDA scheme selects data packets with minimum tolerance delay among collection of data packets for performing data collection. Therefore RDI-SSDA scheme improves the data aggregation efficiency in WBAN. The Preferential Sparse Sampled Data Aggregation for data collection is shown in below.

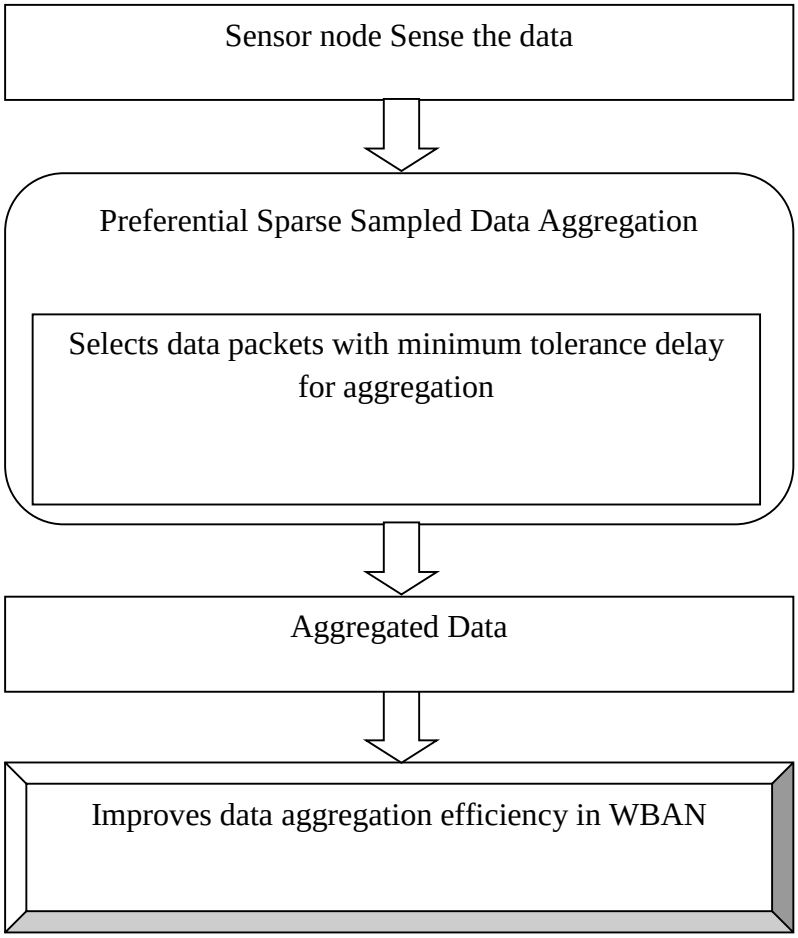

Figure 4. Process of Preferential Sparse Sampled Data Aggregation

Figure 4 shows the process of Preferential Sparse Sampled Data Aggregation for performing data collection in WBAN. Let assume $\tau_i$is the tolerance delay of data packet from node i to sink. Besides consider the network delay which denotes the more time required for all nodes in the network completes its single transmission to the sink. Thus, the network delay is represented as N_{delay}. In network delay model, there are h intermediate nodes from the source node i to the sink. Let P_i represent one routing path from node i to the sink in which $P_i = \{n_0^i, n_1^i, n_2^i, \dots n_h^i\}$. Here n_h^i designate the node whose distance to the sink is h hops in the routing path of node i. The delay caused at each hop while performing data transmission and aggregation processing is represented as,

$$\tau_i^T = [\tau_0, \tau_1, \tau_2, \dots . \tau_h] \quad (1)$$

Therefore, the tolerance delay for a data packet transmitted to sink form node i is

measured by using mathematical formula

$$\tau_i = \sum_{k=0}^{h} \tau_k \quad (2)$$

From the equation (2), tolerance delay of data packet is measured in which $k = 0,1,..h$ denotes h hops from the source node i to the sink. Thus, minimum tolerance delay (MTD) for a data packet transmitted to sink form node i is determined by using mathematical representation,

$$MTD = \min\{\tau_i\} \quad (i = 1,2,3,\dots) \quad (3)$$

By using equation (3), Preferential Sparse Sampled Data Aggregation model collets data packets with minimum tolerance delay among all the data packets sensed from the sensor node. This in turn helps for improving the data aggregation efficiency in an effective manner. The algorithmic process of Preferential Sparse Sampled Data Aggregation is shown in below,

// Preferential Sparse Sampled Data Aggregation Algorithm

Input: : Sensor nodes '$SN_i = SN_1, SN_2, SN_3 \dots, SN_n$',

Output: Improved data aggregation efficiency

Step 1: Begin

Step 2: **For** each sensor node SN_i

Step 3: Sensor node sense the information

Step 4: Measure tolerance delay for each data packet sensed from the sensor node i to the sink using (2)

Step 5: Compute minimum tolerance delay of a data packet transmitted to sink form node i using (3)

Step 6: Select data packet with minimum tolerance delay for data aggregation

Step 7: **End for**

Step 8:Ends

Algorithm 2 Preferential Sparse Sampled Data Aggregation Algorithm

By using the above algorithmic process, RDI-SSDA scheme efficiently performs the data collection process which resulting in enhanced data aggregation efficiency. After performing the data collection, compressing sensing is carried out to improve the privacy of data transmission in WBAN.

2.3 Compressed Sensing

With the aggregated data, compressed sensing is performed through sensing matrix for providing privacy. The compressed sensing encrypts the aggregated data D using sensing matrix. The sensing matrix reduced the space complexity and computational time of aggregated data for transmission with higher privacy rate. Therefore sensing matrix $\emptyset$ is constructed by using following mathematical formula,

$$\emptyset = \prod_{i=1}^{L} \emptyset_i \tag{4}$$

From the equation (4), sensing matrix $\emptyset$ is created which consisting of set of binary matrices $\emptyset_1, \emptyset_2, \ldots . \emptyset_L$. These matrices are used to form the sensing matrix. The aggregated data D is encrypted with sensing matrix $\emptyset$ which is mathematically represented as below,

$$y = \emptyset D \tag{5}$$

From the equation (5), y is the encrypted data and $\emptyset$ is the sensing matrix which is known to the compressed sensing algorithms for recovering the original data. The compressed sensing algorithms employ the sensing matrix to recover the original data D. The encrypted data y is transmitted over a network for corresponding users in WBAN. For an obtained encrypted data at a receiver, the original signal is reconstructed as a solution to the convex optimization problem which is formulated as,

$$\min_{\hat{x}} ||\hat{x}||_1 \ \ subject\ to\ y = \emptyset D \tag{6}$$

From the equation (6), the original aggregated data is obtained at the receiver. The process of compressed sensing for improving privacy of data in WBAN is shown in below Figure 3.

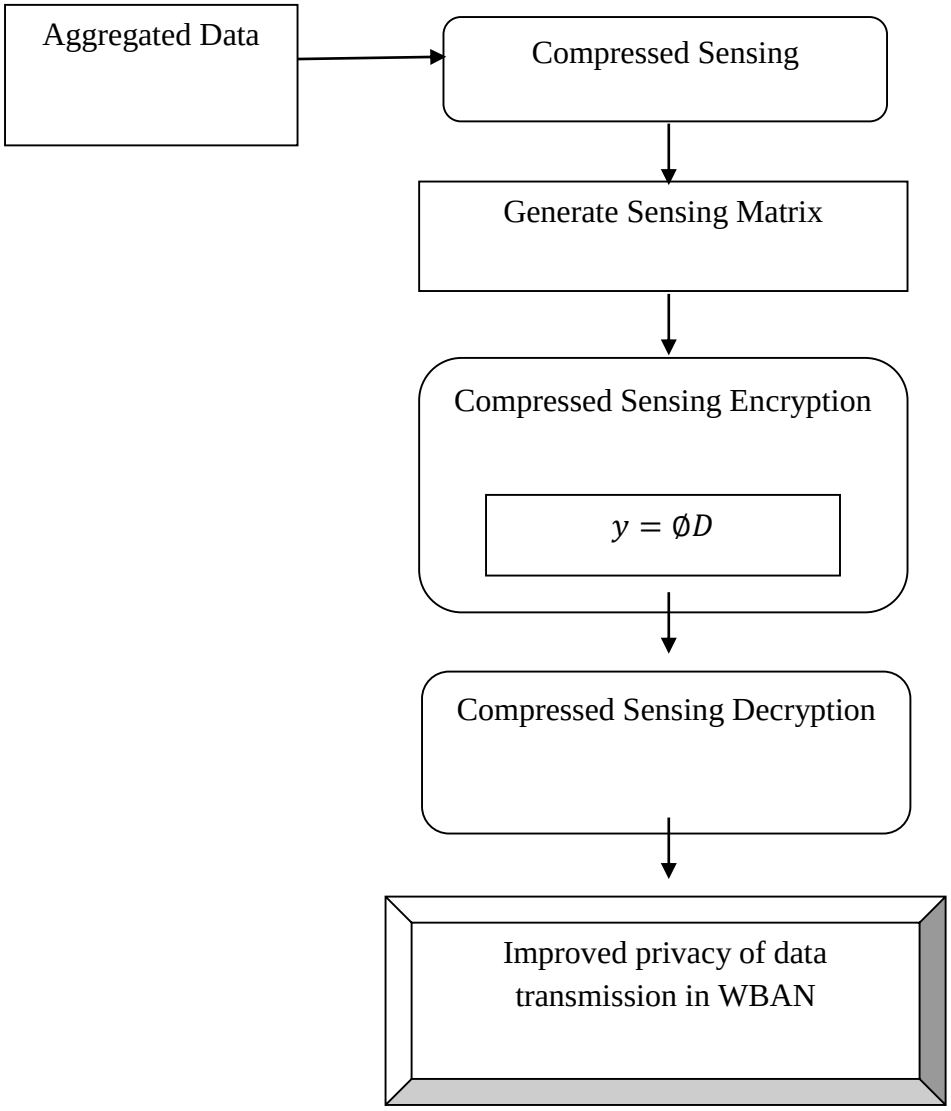

Figure 3. Process of Compressed Sensing For Improving Privacy of Data in WBAN

As shown in Figure 3, compressed sensing process initially takes aggregated data as input and then create sensing matrix for each aggregated data in order to perform encryption. Next, compressed sensing encryption and decryption is carried out with aiming at improving the privacy rate of data transmission. The algorithmic process of compressed sensing is shown in below,

// Compressed Sensing Algorithm

Input: Aggregated Data

Output: Enhanced Data Privacy

Step 1:Begin

Step 2: **For** each aggregated data

Step 3: Construct sensing matrix using (4)

Step 4: Aggregated data is encrypted with sensing matrix using (5) and then transmitted to the corresponding users in WBAN

Step 5: The original data is obtained in receiver side using (6)

Step 5: **End for**

Step 6: End

Algorithm 3 Compressed Sensing for Improving Privacy of Data in WBAN

By using the above algorithmic process, RDI-SSDA scheme enhance the privacy rate while data transmissions in WBAN.

3. SIMULATION SETTINGS

In order to evaluate the efficiency of proposed, Repute Derivative Incentive and Sparse Sampled Data Aggregation (RDI-SSDA) scheme is implemented in NS-2 simulator with the network range of 1500*1500 m size. The sensor nodes are placed in patient's to monitor the activities of patient and analyze the medical data with high security level. In Random Way Point (RWM) model, each sensor node moves to an arbitrarily selected location. Table 1 shows the simulation parameters used for performing the experimental work.

Table 1. Simulation parameters

Parameter	Value
Node density	50,100,150,200,250,300,350,400,450,500
Network area	1500*1500m
Transmission range	250m
Packets	10,20,30,40,50,60,70,80,90,100

Simulation period	600s
Minimum node speed	2m/s
Maximum node speed	25m/s
Node pause time	0 – 300 seconds
Routing protocol	Dynamic source routing protocol (DSR)

The RDI-SSDA scheme used Dynamic Source Routing (DSR) protocol as routing protocol. The performance of RDI-SSDA scheme is compared against with the existing attribute-based encryption and signature scheme [1] privacy-preserving and multifunctional health data aggregation (PPM-HDA) [2]. The RDI-SSDA scheme conducts experimental works on the factors throughput, data aggregation efficiency and data privacy level.

4. RESULT AND DISCUSSION

In this section, the result analysis of RDI-SSDA scheme is evaluated. The performance of RDI-SSDA scheme is compared against with exiting two methods namely, attribute-based encryption and signature scheme [1] privacy-preserving and multifunctional health data aggregation (PPM-HDA) [2]. The performance of RDI-SSDA scheme is evaluated along with the following metrics with the help of tables and graphs.

4.1 Measure of Throughput

In RDI-SSDA scheme, throughput determines the successful rate data packets delivery over a period of time interval in WBAN. Therefore, throughput rate is defined as the ratio of data packets sent by the source node and the data packets received by the destination node. The throughput is measured in terms of percentage (%) and mathematically expressed as,

$$Throughput = \frac{DP_r}{DP_s} * 100 \quad (11)$$

From the equation (11), throughput rate is measured in which 'DP_s' denotes the data packets sent and 'DP_r' is data packets received respectively. While the throughput rate is higher, the method is said to be more efficient.

Table 1. Tabulation for Throughput

Number Of Data Packets	Throughput (%)		
	Attribute-Based Encryption And Signature Scheme	PPM-HDA	RDI-SSDA scheme
10	52.12	61.52	73.65
20	53.87	62.91	74.15
30	55.16	65.12	76.81
40	57.64	67.82	77.36
50	60.11	69.13	80.15
60	61.92	70.82	82.16
70	63.47	73.65	83.91
80	65.17	74.18	84.30
90	66.95	76.96	86.33
100	68.24	79.61	88.15

Table 1 demonstrates the comparative result analysis of throughput based on different number of data packets in the range of 10-100 using three methods. The RDI-SSDA considers the framework with different number of data packets and sensor nodes for conducting the simulation work. From the table, it is expressive that the throughput using RDI-SSDA scheme is higher when compared to existing attribute-based encryption and signature scheme [1] and PPM-HDA [2].

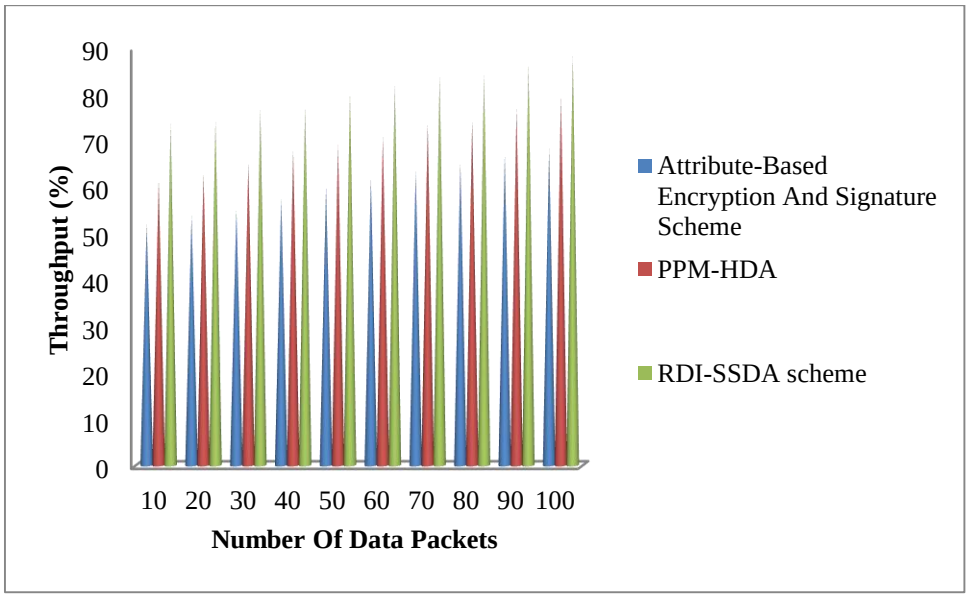

Figure 5. Measurement of Throughput

Figure 5 depicts the impact of throughput is achieved with respect to the different number of data packets. As exposed in figure, RDI-SSDA scheme is provides better throughput when compared to existing attribute-based encryption and signature scheme [1] and PPM-HDA [2]. Besides while increasing the number of data packets for dissemination, throughput rate is also increased using all the three methods. But comparatively, the throughput using RDI-SSDA scheme is higher. This is due to the application of repute derivation based incentive algorithm in Repute Derivation based Incentive to identify the trustworthiness users for secured data communication in WBAN. By using this algorithmic process, Repute Derivation based Incentive choose the trustworthy users with higher incentive for transmitting the data packets in WBAN. This in turn helps for improving the throughput in an effective manner. As a result, RDI-SSDA scheme improves the throughput by 34% when compared to attribute-based encryption and signature scheme [1] and 15% when compared to PPM-HDA [2] respectively.

4.2 Measurement of Data Aggregation Efficiency

The data aggregation efficiency (DAE) is defined as the ratio of number of data packets that are collected at the aggregator to the total number of data packets sensed form the sensor node. The data aggregation efficiency is measured in terms of percentages (%) and mathematically expressed as,

$$DAE = \frac{number\ of\ data\ packets\ that\ are\ collected\ at\ the\ aggregator}{total\ number\ of\ data\ packets} \qquad (12)$$

From the equation (12), data aggregation efficiency is obtained. While the data aggregation efficiency is higher, more efficient the method is said to be.

Table 2. Tabulation for Data Aggregation Efficiency

Number Of Data Packets	**Data Aggregation Efficiency (%)**		
	Attribute-Based Encryption And Signature Scheme	**PPM-HDA**	**RDI-SSDA scheme**
10	63.49	71.45	85.17
20	67.12	74.18	87.51
30	68.90	75.86	88.92
40	70.32	77.51	89.79
50	71.35	79.38	90.15

60	73.28	80.17	91.78
70	74.91	82.36	93.12
80	76.16	83.67	94.68
90	77.64	84.95	95.13
100	78.81	85.63	97.65

The data aggregation efficiency with respect to diverse number of data packets in the range of 10-100 using three methods is presented in Table 2. From the table, it is clear that the data aggregation efficiency using RDI-SSDA scheme is higher when compared to existing attribute-based encryption and signature scheme [1] and PPM-HDA [2].

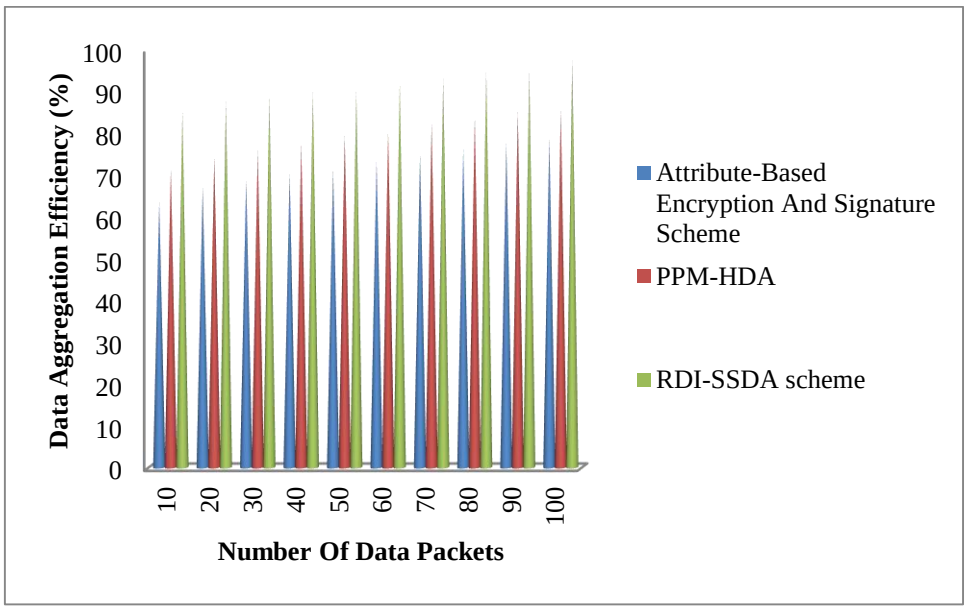

Figure 5. Measurement of Data Aggregation Efficiency

Figure 5 portrays the impact of data aggregation efficiency versus different number of data packets. As revealed in figure, RDI-SSDA scheme is provides better data aggregation efficiency when compared to existing attribute-based encryption and signature scheme [1] and PPM-HDA [2]. As well while increasing the number of data packets, data aggregation efficiency is also increased using all the three methods. But comparatively, the data aggregation efficiency using RDI-SSDA scheme is higher. This is owing to the application of Preferential Sparse Sampled Data Aggregation in

RDI-SSDA scheme. The Preferential Sparse Sampled Data Aggregation deploys a tolerance delay factor which indicates the maximum delay a packet can support before its delivery. By using this, the RDI-SSDA scheme provides preferential for a data packet with minimum tolerance delay for aggregation. This in turn supports for improving the data aggregation efficiency in a significant manner. Therefore, RDI-SSDA scheme improves the data aggregation efficiency by 27% when compared to attribute-based encryption and signature scheme [1] and 15% when compared to PPM-HDA [2] respectively.

4.3 Measurement of Data Privacy Level

In RDI-SSDA scheme, data privacy level (DPL) is defined as the rate at which the data packets transmitted is only be accessed and used by the authorized users. The data privacy level is measured in terms of percentage (%) and mathematically formulated as,

$$DPL = \frac{number\ of\ data\ packets\ that\ are\ correctly\ accessed\ by\ authorized\ user}{total\ number\ of\ patient\ data\ send} * 100 \qquad (14)$$

From the equation (14), privacy level of different data is measured. When the data privacy level is higher, the method is said to be more efficient.

Table 4. Tabulation for Data Privacy Level

Number of data packets	Data Privacy Level (%)		
	Attribute-Based Encryption And Signature Scheme	PPM-HDA	RDI-SSDA scheme
10	68.25	74.35	81.14
20	70.15	76.13	82.88
30	71.68	77.82	84.11
40	72.80	80.34	85.90
50	74.65	81.86	87.36
60	75.96	82.47	88.14
70	76.80	84.38	90.25
80	78.36	85.16	91.13
90	80.19	87.21	94.18
100	82.47	88.05	95.91

Table 4 explains the comparative result analysis of data privacy level for three methods with respect to dissimilar number of data packets in the range of 10-100. From the table, it is descriptive that the data privacy level using RDI-SSDA scheme is higher when compared to existing attribute-based encryption and signature scheme [1] and PPM-HDA [2].

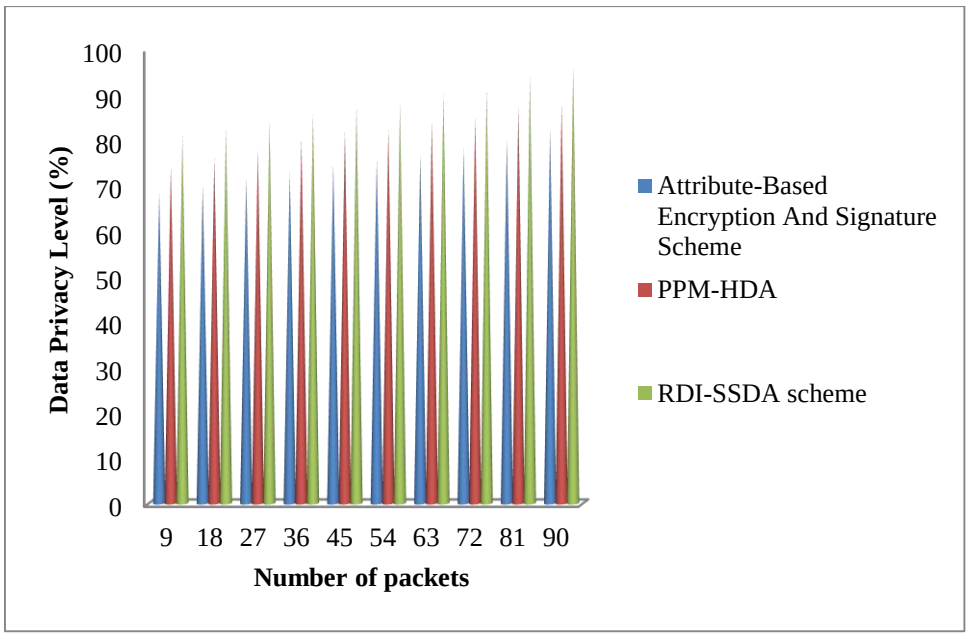

Figure 6. Measurement of Data Privacy Level

Figure 5 depicts the impact of data privacy level versus dissimilar number of data packets in the range of 10-100. As illustrated in figure, RDI-SSDA scheme is provides better privacy level for data transmission when compared to existing attribute-based encryption and signature scheme [1] and PPM-HDA [2]. Also while increasing the number of data packets, data privacy level is also increased using all the three methods. But comparatively, the data privacy level using RDI-SSDA scheme is higher. This is because of application of compressed sensing is performed in RDI-SSDA scheme. The compressed sensing generates sensing matrix for each aggregated data. Then, aggregated data is encrypted with the sensing matrix with objective of improving the privacy level. Thus, RDI-SSDA scheme improves the data privacy level by 17% when compared to attribute-based encryption and signature scheme [1] and 8% when compared to PPM-HDA [2] respectively.

5. RELATED WORKS

A novel anonymous authentication scheme was designed in [11] for improving the security of data transmission in WBAN. An enhanced secure sensor association and

key management protocol was intended in [12] based on elliptic curve cryptography and hash chains to afford secure and correct association of a group of sensors with a patient and assure the requirements of data confidentiality and integrity in body area networks. This protocol achieves lower computation and communication cost for authentication and key derivation.

A secure protocol was developed in [13] to achieve confidential transmission in star two-tier WBAN topology and to satisfy the essential security requirements. Though, this secure protocol improves the security but data privacy rate was not sufficient. The security and inter-node transmission energy for biosensors in a wireless body area sensor network (WBASN) system was analysed in [14] providing for inter-node communication security. But data aggregation process was remained unsolved.

The physical layer security method was designed in [15] depends on the observation of the user's behavioural fingerprint through radio channel characteristics to provides high level of security against false authentication attacks in WBANs. This physical layer security method was appropriate for low power WBAN applications containing highly sensitive private data. An energy efficient method was introduced in [16] for achieving secure and reliable data transmission in WBAN with aid of RelAODV. This energy efficient method enhances the overall QoS of the system. However, the performance of secure and reliable data transmission was not efficient which lacks the level of security.

A secured electrocardiogram (ECG) signal transmission scheme was developed in [17] to enhance the security of data transmission in WBAN. A privacy-enhanced and multifunctional health data aggregation scheme (PMHA-DP) was designed in [18] to preserve the privacy of aggregated data from cloud servers. The PMHA-DP attains data privacy. But, data aggregation performance was not effectual.

A Data Privacy Protective Mechanism was intended in [19] to assure the security and privacy of users' data in the environment of WBAN. Game Theory with Stackelberg Security Equilibrium (GTSSE) mechanism was designed in [20] to obtain the patient's information with higher security in WBAN. This mechanism improves the security of data transmission and reduces the formation loss rate in WBAN.

6. CONCLUSION

An effective Repute Derivative Incentive and Sparse Sampled Data Aggregation (RDI-SSDA) scheme is developed to enhance the security and privacy of wireless body area network communication for health monitoring. At first, RDI-SSDA scheme employed Repute Derivation Based Incentives scheme to discover the trustworthy users in network over a period of time with the aid of second order derivative for achieving secure data communication. Therefore, RDI-SSDA scheme improves the

throughput in WBAN. After that, RDI-SSDA scheme carried out Preferential Sparse Sampled Data Aggregation for collecting the sensed data of different sensor nodes with higher data aggregation efficiency. At last, compressed sensing is accomplished for each aggregated data through sensing matrix where the data is encrypted with sensing matrix with aim of improving the data privacy of level of transmission in WBAN. The performance of RDI-SSDA scheme is measured in terms of throughput, data aggregation efficiency and data privacy level and compared with two exiting methods. With the simulations conducted for RDI-SSDA scheme, it is observed that the privacy level of data transmission provides more accurate results as compared to state-of-the-art works. The simulations results shows that RDI-SSDA scheme provides better performance with an improvement of data privacy level and data aggregation efficiency when compared to state-of-the-art works.

REFERENCES

[1] Chunqiang Hu, Hongjuan Li, Xiuzhen Cheng, Xiaofeng Liao, "Secure and Efficient data communication protocol for Wireless Body Area Networks", IEEE Transactions on Multi-Scale Computing Systems, Volume 2, Issue 2, Pages 94 - 107, 2016

[2] Song Han, Shuai Zhao, Qinghua Li, Chun-Hua Ju and Wanlei Zhou, "PPM-HDA: Privacy-preserving and multifunctional health data aggregation with fault tolerance", IEEE Transactions on Information Forensics and Security, Volume 11, Issue 9, Pages 1940 – 1955, 2016

[3] Jun Zhou, Zhenfu Cao, Xiaolei Dong, Naixue Xiong, Athanasios V. Vasilakos, "4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks", Information Sciences, Elsevier, Volume 314, Pages 255–276, 2015

[4] Santanu Chatterjee, Ashok Kumar Das, Jamuna Kanta Sing, "novel and efficient user access control scheme for wireless body area sensor networks", Journal of King Saud University – Computer and Information Sciences, Elsevier, Volume 26, Pages 181–201, 2014

[5] Daojing He, Sammy Chan, Yan Zhang and Haomiao Yang, "Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks", IEEE Journal of Biomedical and Health Informatics, Volume 18, Issue 2, Pages 440-448, March 2014

[6] Hu Xiong and Zhiguang Qin, "Revocable and Scalable Certificateless Remote Authentication Protocol With Anonymity for Wireless Body Area Networks", IEEE Transactions On Information Forensics And Security, Volume 10, Issue 7, Pages 1442-1455, July 2015

[7] Aftab Ali and Farrukh Aslam Khan, "Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications", EURASIP Journal on Wireless Communications and Networking, Springer, Volume 216, December 2013

[8] Nguyen Dinh Han, Longzhe Han, Dao Minh Tuan, Hoh Peter In, Minho Jo, "A scheme for data confidentiality in Cloud-assisted Wireless Body Area Networks", Information Sciences, Elsevier, Volume 284, Pages 157–166, November 2014

[9] Hussein Moosavi and Francis Minhthang Bui, "Delay-Aware Optimization of Physical Layer Security in Multi-Hop Wireless Body Area Networks", IEEE Transactions on Information Forensics and Security, Volume 11, Issue 9, Pages 1928 – 1939, 2016

[10] Jian Shen, Shaohua Chang, Jun Shen, Qi Liu, Xingming Sun, "A lightweight multi-layer authentication protocol for wireless body area networks", Future Generation Computer Systems, Elsevier, Pages 1-25, 2016

[11] Libing Wu, Yubo Zhang, Li Li, Jian Shen, "Efficient and Anonymous Authentication Scheme for Wireless Body Area Networks", Journal of Medical Systems, Springer, Volume 40, Issue 134, Pages 1-12, 2016

[12] Jian Shen, Haowen Tan, Sangman Moh, Ilyong Chung, Qi Liu, and Xingming Sun, "Enhanced Secure Sensor Association and Key Management in Wireless Body Area Networks", Journal Of Communications And Networks, Volume 17, Issue 5,Pages 454-462, October 2015

[13] Maged Hamada Ibrahim, Saru Kumari, Ashok Kumar Das, Mohammad Wazid, Vanga Odelu, "Secure anonymous mutual authentication for star two-tier wireless body area networks", computer methods and programs in biomedicine, Volume 135, Pages 37–50, 2016

[14] Chukwunonyerem, A.M. Aibinu, A.J. Onumanyi, O.C. Ugweje, E.N. Onwuka, C. Alenogbena, N. Ezechia, "Development of key generation algorithm using ECG biometrics for node security in wireless body area sensor network", European Research in Telemedicine / La Recherche Européenne en Télémédecine, Elsevier, Volume 5, Issue 4, Pages 137–144, December 2016

[15] Nan Zhao, Aifeng Ren, Fangming Hu, Zhiya Zhang, Masood Ur Rehman, Tianqiao Zhu, Xiaodong Yang and Akram Alomainy, "Double Threshold Authentication Using Body Area Radio Channel Characteristics", IEEE Communications Letters, Volume 20, Issue 10, Pages 2099 – 2102, 2016

[16] Kanaga Suba Raja, Usha Kiruthika, "An Energy Efficient Method for Secure and Reliable Data Transmission in Wireless Body Area Networks Using

RelAODV", Wireless Personal Communications, Springer, Volume 83, Issue 4, Pages 2975–2997, August 2015

[17] Hansong Xu and Kun Hua, "Secured ECG signal transmission for human emotional stress classification in wireless body area networks", EURASIP Journal on Information Security, Springer, Volume 5, Pages 1-12, 2016

[18] Hao Ren, Hongwei Li, Xiaohui Liang, Shibo He, Yuanshun Dai and Lian Zhao, "Privacy-Enhanced and Multifunctional Health Data Aggregation under Differential Privacy Guarantees", Sensors, Volume 16, Pages 1-27, 2016

[19] GuangXia Xu, QunWu, Mahmoud Daneshmand, Yanbing Liu and ManMan Wang, "A data privacy protective mechanism for wireless body area networks", Wireless Communications and Mobile Computing, Volume 16, Issue 13, Pages 1746–1758, September 2016

[20] M. Somasundaram, R. Sivakumar, "Game Theory Based Security in Wireless Body Area Network with Stackelberg Security Equilibrium", Hindawi Publishing Corporation, the Scientific World Journal, Volume 2015, Article ID 174512, Pages 1-9, 2015