International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 6 (2018) pp. 3449-3460

QOS Based Data Privacy Using Pearson Correlation for Secured Wireless Body Area Network

Ms. I.Shanmugapriya[1] and Dr. K.Karthikeyan[2]

[1]PhD Scholar, Department of Computer Science, Dr.SNS Rajalakshmi College of Arts and Science (Autonomous), Chinna vedam Patti, Saravanam Patti(PO), Coimbatore-49,Bharathiar University, Tamil Nadu, India.

[2] Assistant Professor, Department of Computer Science, Government Arts and Science College, Palladam, Tiruppur (Dt), Tamil Nadu, India.

Abstract

Wireless Body Area Networks (WBANs) provides efficient communication to the omnipresent health care systems. A small sensor is inserted into the human body and monitors an individual's health and collects the data, store and transmits a health care center over wireless links. During the transmission, better quality of service based secured communication is the major issues for achieving data privacy. Recently many research works has been designed for secured communication but it still not provides the better quality of services for enhancing the security of sensed data. In order to provide secured QoS for sensed data, Data privacy based Pearson Correlation Coefficient (DP-PCC) scheme is introduced. DP-PCC scheme is used for channel assignment to obtain better QoS for secured communication in WBAN. Initially, Sensed data are classified as emergency constrained or normal data based on data transfer rate. After that, bandwidth availability is measured in traffic conditions to send the data packet over a network. Then the Pearson correlation is used to measure the relationship between the available bandwidth and data packet to assign the priority. Then the channel is allocated to higher priority for effective transmission. With the allocated channel, Elliptic curve cryptography is applied for secured data packet transmission in such a way to provide better QoS in WBAN. The simulation is carried out to analyze the performance of proposed DP-PCC scheme with the parameters such as throughput, delay, Sensed data privacy level and data loss with number of data packets and size.

Keywords: Wireless Body Area Networks (WBANs), Quality of service, data privacy, Pearson correlation Coefficient, emergency constrained data, normal data, data transfer rate, bandwidth availability, Elliptic curve cryptography.

INTRODUCTION

In WBAN, the multiple sensor nodes are used for monitoring the data. These sensed data are sending to the base station and guaranteeing the privacy against multiple traffic conditions. During this condition, the Quality of services plays a vital role for improving the data transmission in WBANs. Therefore, the several research works has been established in WBAN and it explained with the help of literature.

In [1], an attribute-based encryption and signature scheme was developed to secure data communications between the sensor nodes with the help of Cipher text-Policy Attribute Based Encryption. However, the quality of services during secure communication was not achieved. A multi-hop topology formation game (MTFG) framework was developed in [2]for improving the transmission of a WBAN with higher PHY security with end-to-end delay management. However, privacy was not ensured during the data communication.

An augmenting Compressed Sensing with Wireless Physical Layer Security was designed in [3] to provide a reliable and secured model in WBANs. But, QoS based secured communication was not performed. A secure IoT based healthcare system was introduced in [4] for improving the data privacy and integrity. But the reliability of data communication was not addressed.

In order to improve reliable health care monitoring, a lightweight anomaly detection technique for medical WSNs was developed in [5]. However, it failed to analyze the data in normal or critical traffic. A cloud-based secure framework was introduced in [6] for mobile healthcare system that focuses on inter-sensor communication security and patients' data security as well as privacy. However, it failed to allocate the efficient channel for data communication.

A QoS profile named delay, reliability, and throughput (DRT) based channel access mechanism was introduced in [7] for providing a high reliability of data transmission with minimum latency. But, it failed to handle both QoS and data privacy. The different QoS issues were addressed in [8] for handling real time data transmission system, data rate, end-to-end data transmission, data transmission accuracy rate, latency, delay time, jitter, low power data transmission, and so on. But the security of data transmission was not performed.

In [9], a cluster-based hybrid security framework was developed for effective intra-WBAN and inter-WBAN communications. However, secured channel allocation was not performed in traffic conditions. In order to guarantee the security and privacy of user's data, a Data Privacy Protective method was developed in [10] for WBAN. But, the bandwidth and throughput of the data communication remained unsolved.

The certain issues are identified from above said existing methods such as lack of privacy, failed to allocate the channel, less throughput, lack of reliability, failed to support differentiated quality of service (QoS) for traffic in a WBAN. In order to overcome such kind of issues, Data privacy based Pearson correlation Coefficient (DP-PCC) scheme is introduced.

Contribution of the paper is described as follows,

- Data privacy based Pearson correlation Coefficient (DP-PCC) scheme is introduced for secured wireless body area network communication. The sensed data packets from sensor node are identified as emergency or normal data. After that, the bandwidth availability is measured based on original bandwidth and consumed bandwidth for data packet transmission in traffic circumstances.
- Priority based channel allocation is performed using Pearson correlation coefficient to measure the relationship between the bandwidth availability and data packet in normal or emergency constrained. The coefficient provides the positive correlation and it has high priority. The negative correlation has low priority. After that, channel is allocated for higher priority to perform efficient communication.
- The Elliptic curve cryptography is applied for secured communication using private and public key. The data packet (i.e. plain text) is encrypted at the sender. Then the decryption is performed at the receiver with their private key to obtain the original data packet. This helps to improve the reliable data transmission and sensed data privacy level. Moreover, the throughput is increased with minimum delay and data loss.

The rest of the paper is arranged in a following manner. In Section 2, Data privacy based Pearson Correlation Coefficient (DP-PCC) scheme is explained with neat diagram. In Section 3, Experimental evaluation is presented and the simulation results are discussed in section 4. In Section 5, related works are reviewed and discussed briefly. Finally, the conclusion of the research work is presented in section 6.

DATA PRIVACY BASED PEARSON CORRELATION COEFFICIENT SCHEME FOR SECURED COMMUNICTION

In WBAN, the sensor nodes are used to sense the data and it is transmitted into the base station (i.e. sink node). The continuous data transmission in WBAN contains minimum delay, data loss due to higher network traffic and higher throughput for efficient data transmission. This helps to obtain better quality of services for secured communication in WBAN. In order to handle QoS challenges and issues in WBAN, Data privacy based Pearson correlation Coefficient (DP-PCC) scheme is developed. The DP-CCC scheme is explained by starting with a system model for improving the proposed system quality.

SYSTEM MODEL

A system model for DP-PCC scheme is explained in this section. Let us consider a rectangular sensing area 'MXN' and the connectivity graph, '$G = (V, E)$', where 'V' denotes a number of sensor nodes $V \in SN_1, SN_2, \dots, SN_n$ in the network, and 'E' denotes an edges representing the communication links between the nodes. The data packets are represented as $DP = DP_1, DP_2, \dots, DP_n$' for sensing and transmitting to the sink node. The channel is assigned for data packets transmission based on their priority. The problem is to develop an efficient QoS aware secured data communication in WBAN. Therefore, a DP-PCC scheme is introduced for improving the QoS based data privacy of wireless body area network communication.

Data privacy based Pearson correlation Coefficient scheme

DP-PCC scheme is employed for achieving the better QoS based secured communication. Quality of service (QoS), and reliability are significant objectives in WBANs. Different sensor nodes are deployed to collect critical (i.e. emergency constrained data) and non-critical information (i.e. normal data), and send them to the sink node. Therefore, low delay, high reliability and throughput are considered for secure data communication in WBAN. The Flow processing diagram of DP-PCC scheme is illustrated in figure 1.

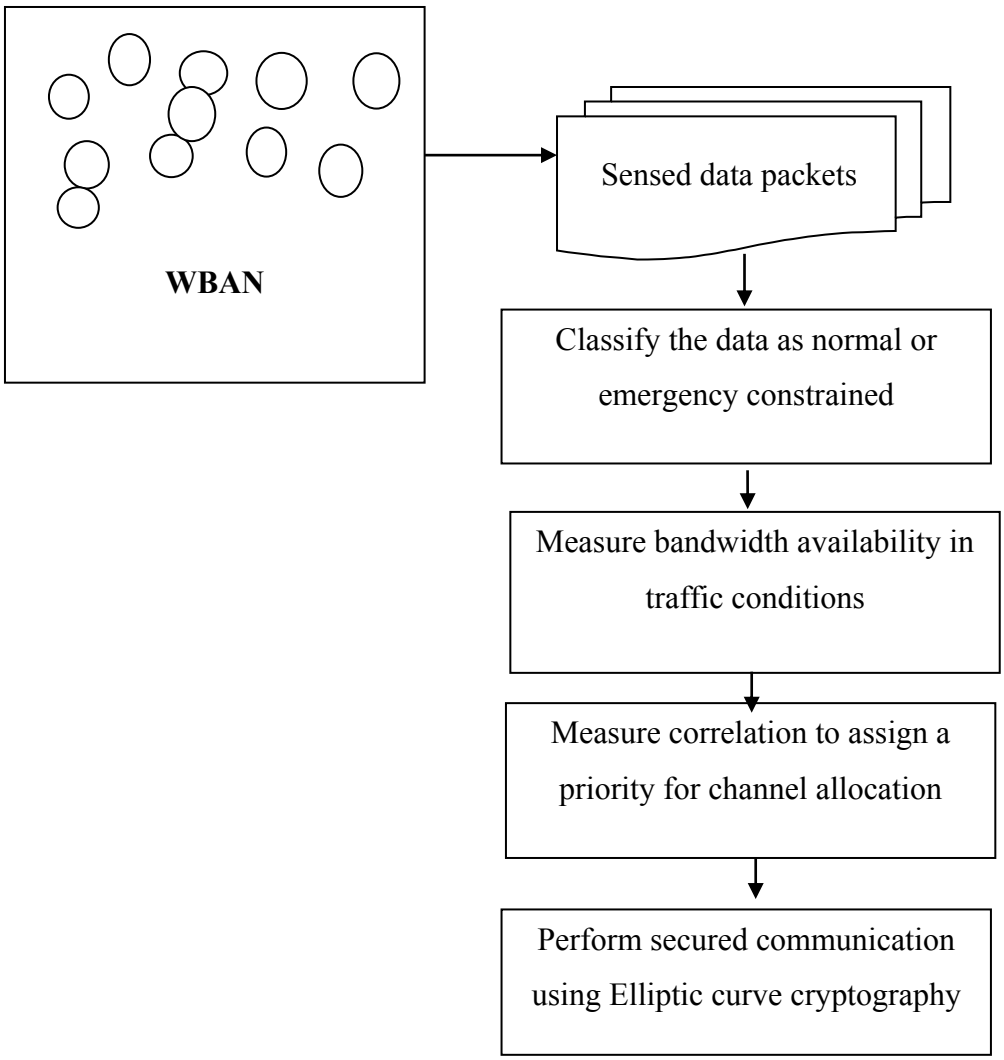

Figure 1. Flow processing Diagram of Data privacy based Covariance correlation Coefficient scheme

Figure 1 shows the flowprocessing diagrams of the Data privacy based Pearson correlation Coefficient (DP-PCC) scheme for secured communication in WBAN. The DP-PCC scheme considers the following processes for achieving higher security in WBAN communication. Initially, sensed data from the sensor nodes are transmitted and it is classified as emergency or normal data for channel allocation based on Data transfer rate. After that, bandwidth availability is measured in traffic scenario. Then, the correlation is measured to assign the priority for channel allocation. Finally the secured data communication is performed using Elliptic curve cryptography. The brief description of DP-PCC scheme is presented in the following subsections.

Data packet classification

Initially, the number of sensor nodes is deployed to perform effective communications. The data are collected from the sensor node to be transmitted to the sink node. Let us consider the number of data packets $DP = DP_1, DP_2, \ldots, DP_n$. During the data transmissions, quality of service is essential for effective communication. Therefore, the quality of service based data privacy is achieved using DP-PCC scheme. Initially, the sensed data (i.e. incoming data) are classified as normal or emergency constrained.

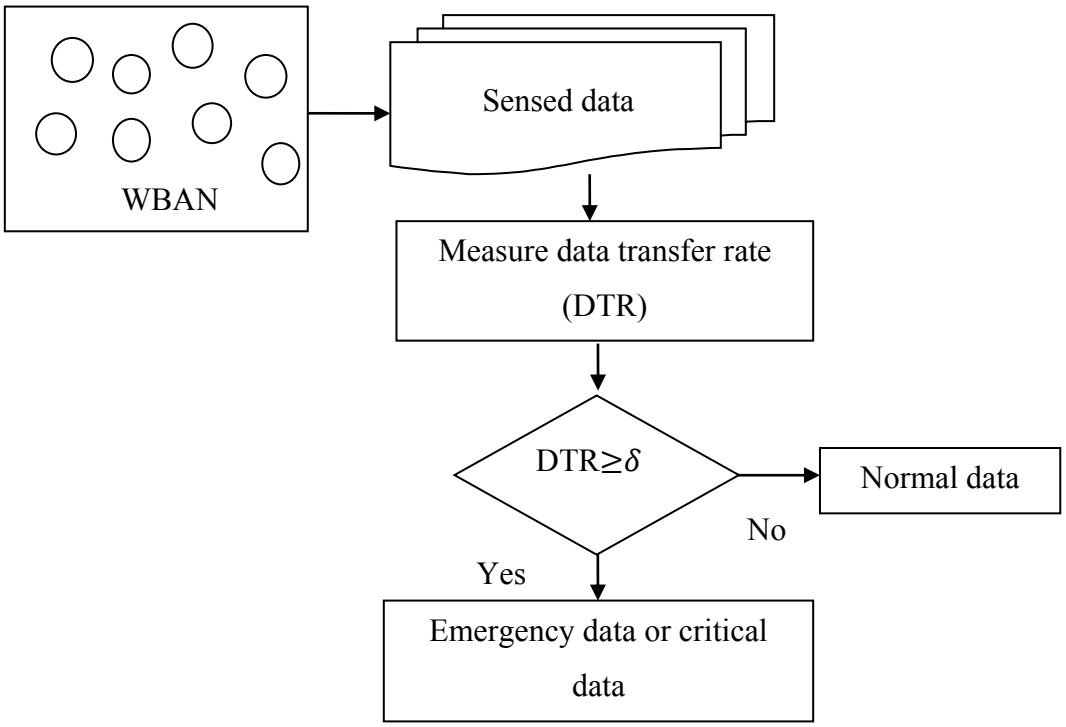

Figure 2 Flow processing diagram of data packet classification

Figure 2 illustrates the flow processing diagram of data packets for achieving a QoS in WBAN. The main objective of DP-PCC scheme is to reduce the end to end delay and improving the throughput. The data transfer rate is a speed with which data packet is to be transmitted from one node in a time to another in a network. Data rates are measured in megabits per second and it is measured as follows,

$$DTR = \frac{Speed\ of\ data\ transmission}{specific\ time} \quad (1)$$

From (1), where DTR denotes a Data packet transfer rate. The data transfer rate of each WBAN sensor nodes is measured and compared with Data Rate Threshold value (δ). If the data transfer rate is greater than are equal to threshold value, then the data packet is said to an emergency constrained. Otherwise it is said to a normal data packet.

Due to large data communication, the traffic is occurred over the network. Traffic is the amount of data packet transferring across a network at a certainperiod of time. In traffic scenario, where multiple routes are available from source to destination, the key challenges in the network is bandwidth to establish the quality of services. Bandwidth is defined as the amount of data packet transmitted in a specified period of time. From that, the available bandwidth in traffic scenario is measured as follows,

$$BA = B_{Initial} - B_C \quad (2)$$

From (2), where BA denotes a Bandwidth availability, $B_{Initial}$ denotes anoriginal channel bandwidth and B_C represents a consumed bandwidth.Therefore, the bandwidth availability is effectively measured to allocate the channel for efficient transmission through the priority assignments.

2.2.1.1 Priority based channel allocation

The design of DP-PCC scheme is a Channel allocation based on priority assignment along with their traffic conditions. Channel assignment means allocating the channels to radio interfaces for efficient communication. In network traffic scenario, the priority is assigned based on the correlation between the data packet in emergency or normal conditions and the bandwidth availability. Correlation is used to measure the mutual relationship between two variables (i.e. bandwidth availability and data packet in normal or emergency constrained).Therefore, the Pearson correlation coefficient is measured as follows,

$$r = \frac{\sum ab - \frac{(\sum a)(\sum b)}{n}}{\sqrt{\left(\sum a^2 - \frac{(\sum a)^2}{n}\right)(\sum b^2 - \frac{(\sum b)^2}{n})}} \quad (3)$$

From the (3),$n$denotes the number of data packets to be transmitted, a and b denotes a two cases (i.e. data packet in emergency constrained or critical condition) and bandwidth availability,$\sum ab$ refers the sum of cross product of a and b, $\sum a$ is the set of differential relationships with respect to b. $\sum b$ is differential relationship of b with respect to a. From (3), 'r' denotes a Pearson correlation coefficient. As a result, the correlation between the two cases is identified. The Pearson correlation coefficient $'r'$ value is ranges between -1 and +1.The coefficient values are ranges from 0 to 1 provides better correlation. It means that the data packetsin emergency conditions and the availability of bandwidth is less. The coefficient values are ranges from -1 to 0 provides less correlationit denotes a data packets in normal conditions and the availability of bandwidth is more. Based on correlation value, the priority is assigned. The better correlation value has

higher priority whereas the low correlation value has low priority. Finally, the channel is allocated for higher priority first than the lower priority to perform communication.

Channel allocation is used for assigning the channels in a network to perform effective communications. Generally, there are three channel assignments are presented such as fixed channel assignment, dynamic channel assignment and hybrid channel assignment. In fixed channel assignment, a set of channels is allocated to every data packet in the network permanently. A dynamic channel assignment is not allocated the channel previously. It only allocatesthe channel when a data packet arrived. The hybrid allocation is a combination of both fixed and dynamic channel assignment. The DP-PCC schemeuses a dynamic channel allocation model to improve the quality of service communications.As a result, the channel allocation implemented with this dynamic assignment during the data packet transmission of the networks. The Priority based channel allocation algorithm is described as follows,

Input: : Sensor nodes'$SN_i = SN_1, SN_2, SN_3 \ldots, SN_n$', data packets$DP_1, DP_2, \ldots, DP_n$

Output: Priority based channel allocation

Step 1: Begin

Step 2: For each sensed data packet

Step 3: Measure data transfer rate (DTR) using (1)

Step 4: If (DTR≥δ) then

Step 5: Emergency data or critical data

Step 6:else

Step 7: Normal data

Step 8: end if

Step 9: Measure bandwidth availability in traffic conditions using (2)

Step 10: Measure Pearson correlation between data and the bandwidth availability using (3)

Step 11: If Pearson correlation coefficient 'r' value from 0 to 1 then

Step 12: Provides better correlation and it has higher priority

Step 13: else if ('r' values from -1 to 10) then

Step 14: Provides negative correlation and it has lowpriority

Step 15: End if

Step 16: End if

Step 17: end for

Step 18: End

Algorithm 1 Priority based channel allocation

The algorithm of Priority based channel assignment is described to allocate the efficient channel for effective communication. For each incoming sensed data packets, the data transfer rate is measured to classify normal data or emergency constrained data. Then the bandwidth availability is measured for assigning a channel.The correlation between the data and their bandwidth availability is measured using Pearson correlation coefficient. The coefficient values are ranges from 0 to 1 provides better correlation and it has higher priority. Otherwise, the coefficient values -1 to 0provides perfect negative correlation which has low priority. Then the channel is allocated for high priority for effective communication.

Elliptic curve cryptography based secured channel communication

Once the channels are allocated, the sensor node sends the data packet through the allocated communications channels. The intruder may interrupt the communication channel and it affects the secured transmission. Therefore, the security plays a major role for achieving secured communications. By using cryptography techniques, the DP-PCC scheme avoids the unauthorized node enter into the encrypted packets and the major challenge is to prevent from interruption. Therefore the necessity of the Prevention System is introduced.

The DP-PCC scheme is to construct efficient security for communication channel during data packet transmission within the network. The helps to prevent the intruder who's affects the transmitted data. In order to provide the secured communication, Elliptic curve cryptography is used. The key generation is a significant part for encryption in which the both public key and private key are generated. Elliptic curve cryptography process is shown in figure 3.

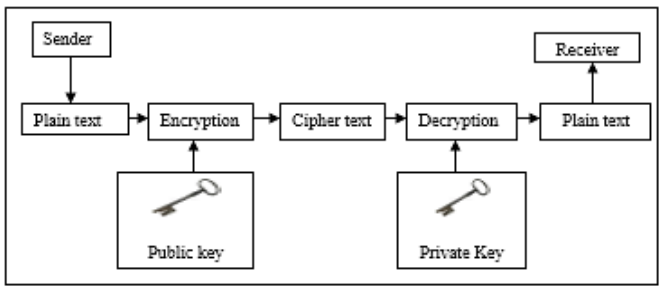

Figure 3. Block diagram of Elliptic curve cryptography

Figure 3 shows the Block diagram of Elliptic curve cryptography systems with two types of keys for efficient data packet transmission from sender to receiver. Both the sender (i.e. source node) and receiver (i.e. base station) use the key for achieving high security over the network. In Elliptic curve cryptography, an encryption is a kind of symmetric encryption in which the private key and public is generated. The Elliptic curve cryptography encrypts the data packet (i.e. plain text) into the cipher text by generating the private key and public key. The private key provides individual use of purpose and

the public key is provided to access the individual's information. These two keys are generated as follows,

$K = R * X$ (4)

From (4), K denotes public key and R denotes a random number (i.e. private key) that selected in the range of $(1\ to\ n-1$)'X' denotes a point on the elliptic curve. The sender encrypts the data packet with receiver's public key. This helps to obtain secure communication. Let us consider the emergency data packets 'DP' (i.e. plain text) on the curve and the two cipher texts C_1 andC_2which is mathematically formulated as below,

$C_1 = a * X$ (5)

$C_2 = DP + a * K$ (6)

From the equation (5) and (6), two cipher texts C_1 andC_2 is obtained.Data packets 'DP' are encrypted to obtain a cipher text with a public key'K' andrandomly selects 'a' from (1 – (n-1)).After encrypting the data packet, the decryption is done to attain the original data (i.e. plain text). The decryption is described as follows,

$D = C_2 - R * C_1$ (7)

Using (5) and (6), $D = DP + a * K - R * a * X$ (8)

Using (4)$D = DP + (a * R * X) - (R * a * X)$ (9)

$D = DP$ (10)

From (10), DP original data packet is obtained after decrypting the original data packet. This result provides better quality of service to the communication system. Also it makes a secure channel allocation over the network. Elliptic curve cryptography based encryption and decryption algorithm is described as follows,

Input: Data Packets '$DP_i = DP_1, DP_2, \ldots, DP_n$, K denotes public key, R denotes a private key, C_1andC_2 cipher text,

Output: Secured channel communication

Step 1: Begin

Step 2: For each data packet DP_i

Step 3: Generate the key using (4)

Step 4: Perform encryption to create the two cipher text using (5) (6)

Step 5: Perform decryption using (10)

Step 6: If (the key is matched at the receiver) then

Step 7: Obtain original data packet

Step 8: End if

Step 9: Secured transmission is performed

Step 10: End for

Step 11: End

Algorithm 2 Elliptic curve cryptography based encryption and decryption

The above algorithm of Elliptic curve cryptography based encryption and decryption is clearly described for secured channel communication from source node to sink node in WBAN. The proposed DP-PCC scheme uses Elliptic curve cryptography is to improve the throughput and reduce the delay for attaining the better quality of services. The data packets are encrypted to transmit the data through the allocated channel. Then the receiver side decrypts the encrypted data with their private key. This helps to obtain reliable data transmission and avoids the unauthorized user access the data packets.

As a result, Data privacy based Pearson correlation Coefficient (DP-PCC) scheme is introduced. DP-PCC scheme is used to achieve better QoS for secured communication in WBAN.

SIMULATION SETTINGS

An efficient Data privacy based Pearson correlation Coefficient (DP-PCC) scheme is implemented in NS2.34 network simulator. In WBAN, the sensor nodes are inserted into patient's body and connected wirelessly in health care applications. These sensor nodes are used for continuous monitoring of the patient's data such as heart rate, temperature, blood pressure, electrocardiograms (ECGs), electroencephalography (EEG) and so on. Totally 500 sensor nodes deployed in WBAN over the network range 1500 m*1500 m size. The DSR routing protocol is used for experimental evaluation for efficient communication.The Random Way Point (RWM) model is used to move the mobile nodes arbitrarily. Table 1 shows the simulation parameters used for performing the experimental work.

Table 1 Simulation parameters

Parameter	Value
Sensor nodes	50,100,150,200,250,300,350,400,450,500
Network area	1500*1500m
Transmission range	250m
Number of data Packets	10,20,30,40,50,60,70,80,90,100
Data packet size	10KB-100KB
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)

RESULTS AND DISCUSSION

Result analysis of DP-PCC scheme is discussed and compared with two existing methods Attribute-based encryption and signature scheme [1] and Multi-hop topology formation game

(MTFG) framework [2]. In order to evaluate the performance of DP-PCC scheme, different parameters such as throughput, delay, sensed data privacy level and data packet loss taken for simulation. The performance of DP-PCC scheme is described with the help of tables and graphs.

Measure of Throughput

Throughputis defined as thesuccessful data packets received at the base station with certain time period. Throughput rate is defined as the ratio of number of data packets (i.e. patient data)received by base station (i.e. doctors)and number of data packets sent by source node. Throughput is measured as follows,

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

From the equation (11), 'DP_s' denotes the data packets sent and 'DP_r' represents data packets received respectively. It is measured in terms of percentage (%).

Performance of throughput with respect to number of data packets being sent from source node to base station is described in table 2. The number of data packet is varied from 10 to 100. The throughput is significantly increased using DP-PCC scheme compared to Attribute-based encryption and signature scheme [1] and MTFG framework [2]. Simulation results of DP-PCC scheme is shown in figure 4.

Table 2. Tabulation for Throughput

Number of data packets	Throughput (%)		
	DP-PCC	Attribute-based encryption and signature scheme	MTFG
10	80	52	60
20	82	54	62
30	83	55	64
40	84	58	68
50	86	60	70
60	87	62	71
70	88	63	73
80	90	65	75
90	92	67	78
100	94	68	82

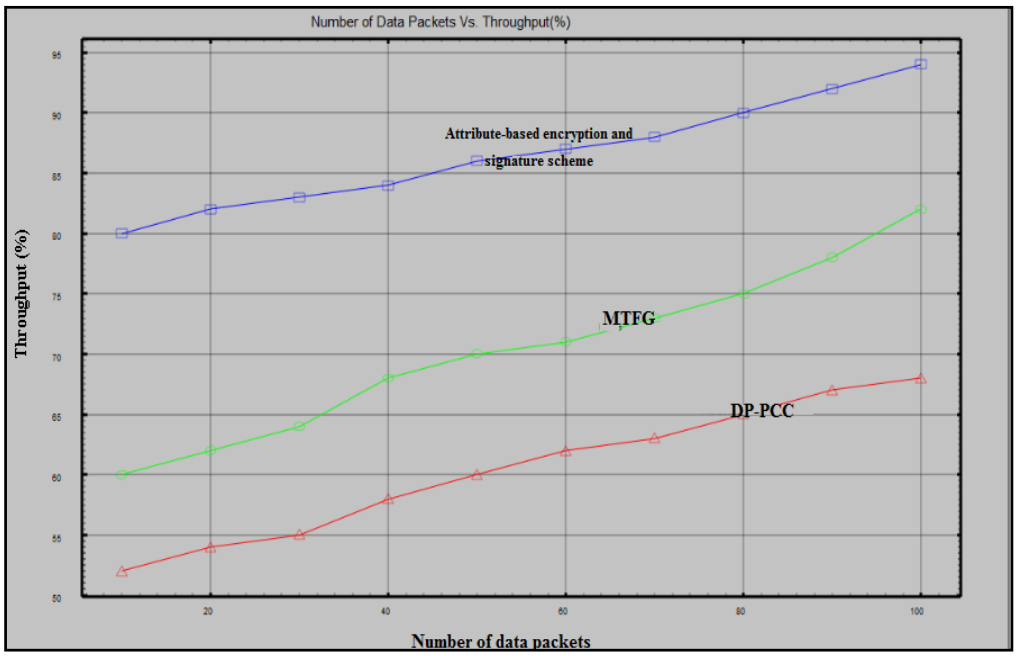

Figure 4. Simulation result of throughput

Figure 4 illustrates the simulation result of throughput with respect to number of data packets (i.e. patient's data). Throughput is measured according to the number of data packet correctly received at the base station. The throughput is increased using DP-PCC scheme than the existing methods. This is because, the Priority based channel allocation is performed to assign the channel. This helps to assign a set of channels for each data packets for improving the communication rate. Due to minimum availability of bandwidth, the emergency data are not effectively flow. During this condition, channel is allocated dynamically to improve the quality of service communications. In addition, the Elliptic key cryptography is used to provide the secured channel communication to improve the data delivery. As a result, the proposed DP-PCC scheme considerably improved the throughput by 44% and 24% when compared to existing Attribute-based encryption and signature scheme [1] and MTFG framework [2] respectively.

IMPACT OF DELAY

Delay is defined as the difference between the average time taken by a data packet to arrive at the base station and time for sending the data packet in the source node. The delay is measured as follows,

$$Delay = T(DP_R) - T(DP_S) \quad (12)$$

From (12),DP_R denotes a Data packets received and DP_S represents a data packet sent. 'T' denotes a Time. Delay is measured interms of milliseconds (ms).

Table 3. Tabulation for Delay

Number of data packets	Delay (ms)		
	DP-PCC	Attribute-based encryption and signature scheme	MTFG
10	13	25	22
20	15	28	25
30	18	32	28
40	22	35	31
50	24	38	33
60	28	41	36
70	32	44	40
80	35	48	42
90	38	50	44
100	41	52	48

Table 3 describes performance of delay with respect to number of patient's data being sent from source node. It is measured based on difference between transmitting and receiving time of data packet. Performance of Delay is reduced using DP-PCC scheme than the existing Attribute-based encryption and signature scheme [1] and MTFG framework [2]. The simulation result of delay is shown in figure 5.

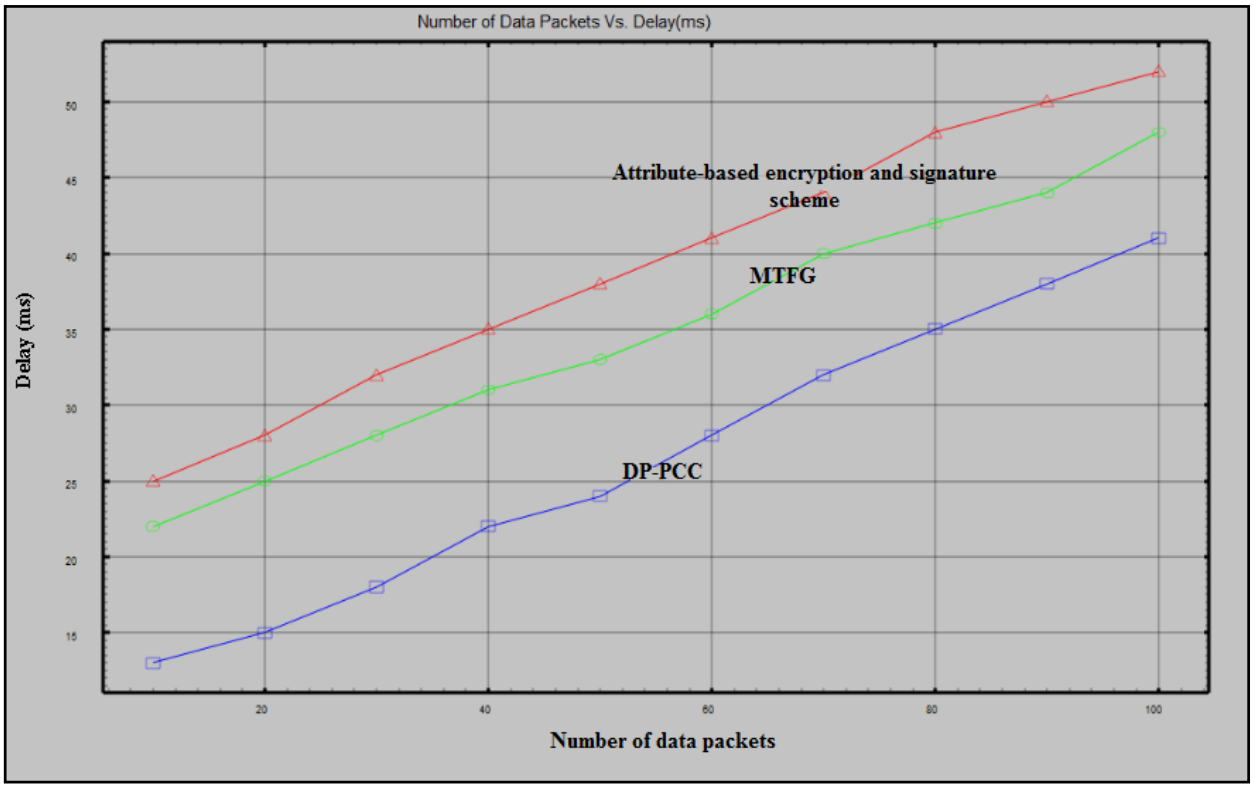

Figure 5. Simulation result of delay

Figure 5 depicts the simulation result of delay with respect to number of data packets varied from 10 to 100. From the figure, it is clearly evident that the proposedDP-PCC scheme reduces the delay during the data packet transmission between source node to base station. The delay of a network identifies how long the base station receives a patient's data to travel across the network from source node. The node sends an emergency patient's data rapidly. If the channel becomes extremely busy in traffic conditions, the DP-PCC scheme performs channel allocationbased on the priority assignmentto improve the data packet transmission. Followed by, the patient's data effectively transmitted to the base station. This helps to reduce the delay of data packet communication. Therefore, the delay is significantly reduced by 34% and 26% compared to existing Attribute-based encryption and signature scheme [1] and MTFG framework [2] respectively.

IMPACT OF SENSED DATA PRIVACY LEVEL

Sensed dataprivacy level (SDPL) is defined as the ratio of the number of data packets accessed by the authorizeduser to the number of data packet being sent from source node. The sensed data privacy level is described as,

$$SDPL = \frac{Number\ of\ DP_R\ correctly\ accessed\ by\ authorized\ user}{Number\ of\ DP_S} * 100 \quad (13)$$

From the equation (13), where DP_R represents data packet received andDP_srepresents data packet sent. The sensed data privacy level is measured in terms of percentage (%).

Table 4. Tabulation for Sensed Data privacy level

Number of data packets	Sensed Data privacy level (%)		
	DP-PCC	Attribute-based encryption and signature scheme	MTFG
10	83	68	72
20	84	70	75
30	86	72	78
40	87	73	80
50	88	75	82
60	90	76	84
70	91	77	85
80	93	78	87
90	95	80	89
100	96	82	90

Table 4 describes a Sensed Data privacy level with three different techniques DP-PCC scheme than the existing Attribute-based encryption and signature scheme [1] and MTFG framework [2]. For different number of data packets in the range of 10 to 100, the Sensed Data privacy level is significantly improved using DP-PCC scheme when compare to existing methods.

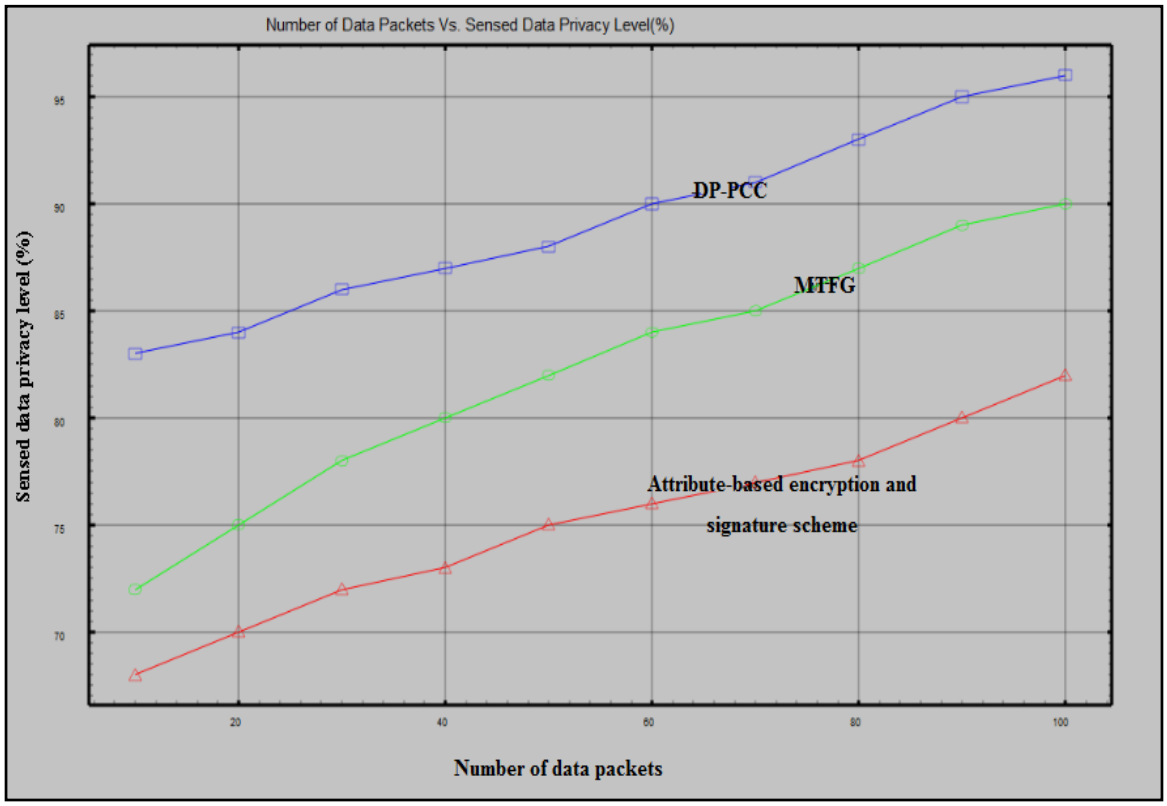

Figure 6. Simulation result of sensed data privacy level

Figure 6 describes simulation results of sensed data privacy level with number of data packets. As shown in figure, the sensed data privacy level is considerably increased using DP-PCC scheme than the existing methods. The sensed data from the patient's are transmitted in a secured manner. This is obtained by DP-PCC scheme allocating the channel for effective communication based on the bandwidth availability and data transfer rate. If the data transfer rate is higher than the threshold value, then it is said to an emergency constrained data. These data is transmitted over the network but the channel is in busy condition. The relationship between data and bandwidth availability are performed by using Pearson correlation coefficient. The coefficient value provides the positive correlation which is said to be higher priority and the channel is allocated.Then the data is transmitted through the allocated channel. During this transmission, the security is provided by using elliptic key cryptography. The sender encrypts the data and transmitted through the channel with their public key and receiver decrypts the cipher text to attain original data packet. This helps to avoid the unauthorized access of patient's data. The authorized users only access the data to improve the reliable data transmission. As a result, the DP-PCC scheme improves the sensed data privacy level by 19% and 9% when compared to existing Attribute-based encryption and signature scheme [1] and MTFG framework [2] respectively.

Impact of dataloss

Data loss is defined as the difference between the amount of data packets sent from source node and amount of data packets received at sink node. The data loss is measured in Kilo Bytes (KB) and it is formulated as.

$$DL = DP_S - DP_R (14)$$

From (14),where DL denotes a Data Loss, DP_S and DP_Rrepresent s amount of data packet sent and data packet received respectively.

Table 5. Tabulation for data loss

Data packet size (KB)	Data loss (KB)		
	DP-PCC	Attribute-based encryption and signature scheme	MTFG
10	3	5	4
20	4	7	5
30	5	8	6
40	8	11	7
50	10	13	12
60	11	15	13
70	12	16	15
80	13	18	17
90	15	20	22
100	18	21	24

Table 5 clearly shows an impact of Data loss with respect to data packet size. Data packet size is ranges from 10 KB to 100 KB. Data loss is reduced using DP-PCC scheme when compared to existing Attribute-based encryption and signature scheme [1] and MTFG framework methods [2] respectively.

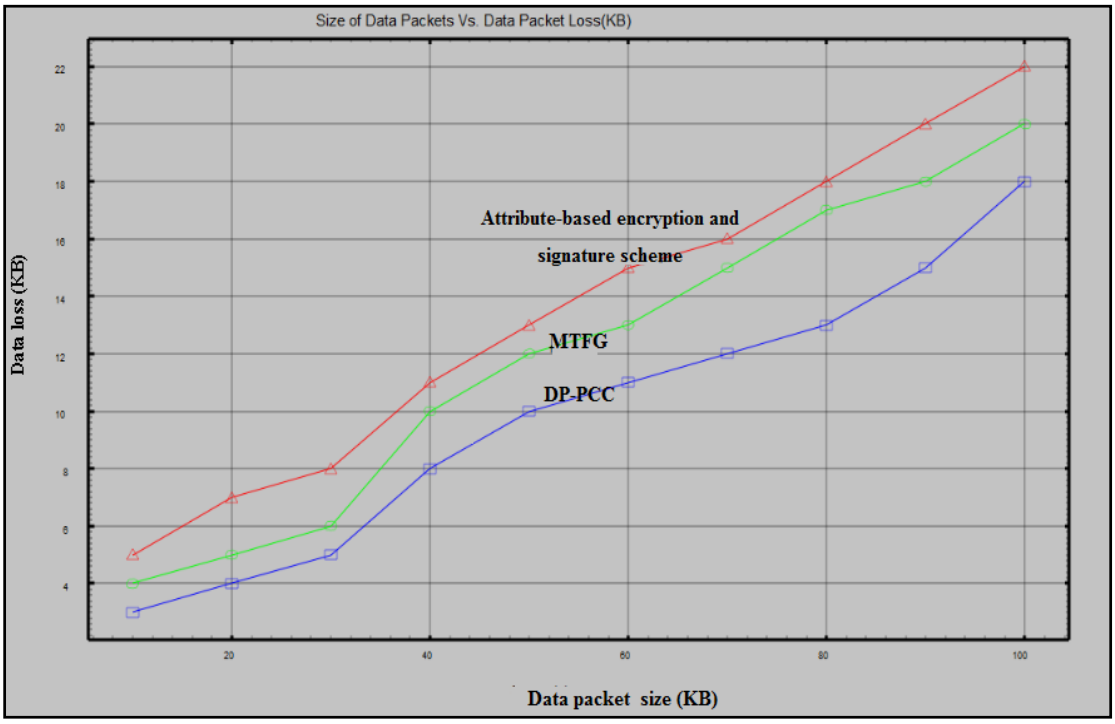

Figure 7. Simulation result of data loss

Figure 7 illustrates the simulation result of data loss with respect to data packet size to be sent. From the figure, it is clearly evident that the data loss is reduced in proposed DP-PCC scheme by varying the data packet size. The proposed DP-PCC scheme uses the Elliptic key cryptography to avoid the unauthorized user access for increasing the data privacy level. By using cryptography technique, the sender and receiver use the key for secured communication and the authorized node receives the data. This in turn reduces the data loss in communication. Moreover, DP-PCC scheme reduces the data loss by improving the throughput and data privacy level. Let us consider 10KB of data packet being sent, the 7KB of data successfully received at the destination and the remaining 3KB is lost. This shows the significant improvement of DP-PCC scheme than the existing methods. As a result, proposed DP-PCC scheme considerably reduces the data loss by 29% and 18% compared to Attribute-based encryption and signature scheme [1] and MTFG framework methods [2].

RELATED WORKS

QoS-based network management system was developed in [11] that contains two parts namely, QoS monitoring and admission control. However, security was not considered. DP-PCC scheme efficiently handles both QoS and security in WBAN communication.

A flexible quality of service model was introduced in [12] for improve data transmission in WBAN networks. But, it failed to use QoS services for smart healthcare monitoring applications in terms of data transmission rate. DP-PCC scheme improves the Quality of service communication to improve the data transmission rate in healthcare monitoring system.

A reliable, and power efficient routing protocol was designed in [13] for achieving high throughput for WBAN. However, end to end delay was high. The DP-PCC scheme improves the throughput with minimum delay.

Priority-based Allocation of Time-Slots (PATS) algorithm was introduced in [14] for healthcare data transmission. But,buffering delays of successive transmission was high. DP-PCC scheme allocate the channel based on the priority assignment which results in reduces the delay.

A MAC protocol was introduced in [15] with multi-constrained QoS provisioning for different traffic classes in WBANs. However, data privacy level was not measured to achieve high security. DP-PCC scheme increases the sensed data privacy level for secured communication in WBAN.

Priority-based traffic load adaptive medium access control (MAC) protocol was introduced in [16] for diverse QoS requirements, such as delay, reliability and throughput in Body sensor networks (BSNs). However, data loss during the transmission remained unaddressed. DP-PCC scheme reduces the data loss.

Fritchman model was introduced in [17] to allocate the dynamic channel fading for human body communication (HBC). But, the security based channel allocation was not performed. DP-PCC scheme improves the security based channel allocation using Elliptic key cryptography.

Fuzzy Attribute-Based Signcryption (FABSC) technique was developed in [18] for providing a tradeoff between security and flexibility. However, it failed to secure the inter-sensorcommunications within a WBAN. DP-PCC scheme improves encryption and decryption for improving the security. Publish-subscribe architecture for WBAN was designed in [19] with Security and privacy in medical wireless body area networks (WBANs). But Qos aware secured communication remained unaddressed. DP-PCC scheme effectively improves the Qos aware secured communication.

A novel secure protocol was designed in [20] to recognize the anonymous joint certification and confidential transmission for star two-tier WBAN topology. However, the performance of secure and reliable data transmission was not efficient using multi-tier WBANs. DP-PCC scheme improves the secure and reliable data transmission.

CONCLUSION

A new scheme called Data privacy based Pearson correlation Coefficient (DP-PCC) is developed to provide QoS based data privacy for secured wireless body area network communication. Initially, data transfer rate is measured for classifying the dataas emergency or normal data. After that, emergency data is transmitted through the network. If the channel is busy condition, the bandwidth availability is measured in traffic circumstances. Then the correlation between the data and the bandwidth availability is measured using Pearson correlation coefficient. Based on the correlation coefficient value, the priority is assigned for channel allocation. Then the sensor node transmits sensed data through the allocated channel in a secured manner. The security is obtained by using Elliptic curve cryptography toimprove the effective communication between source node and sink node in WBAN. The simulation is carried out to analyze the performance of proposed DP-PCC scheme with the parameters such as throughput, delay, sensed data privacy level and data loss. The performance result shows that the DP-PCC scheme increases the factor on throughput and data privacy level with minimum delay and data loss compared to state-of-art methods.

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] 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, 2016, Pages 1928 – 1939

[3] Ruslan Dautov and Gill R. Tsouri," Securing while Sampling in Wireless Body Area Networks with Application to Electrocardiography", IEEE Journal of Biomedical and Health Informatics, Volume 20, Issue 1, 2016, Pages 135 - 142

[4] Prosanta Gope, Tzonelih Hwang, "BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network", IEEE Sensors Journal, Volume 16, Issue 5, 2016, Pages 1368 – 1376

[5] Osman Salem, Yaning Liu, Ahmed Mehaoua, and Raouf Boutaba, "Online Anomaly Detection in Wireless Body Area Networks for Reliable Healthcare Monitoring", IEEE Journal Of Biomedical And Health Informatics, Volume 18, Issue 5, 2014, Pages 1541-1551

[6] Farrukh Aslam Khan, Aftab Ali, Haider Abbas, Nur Al Hasan Haldar, "A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks", Procedia Computer Science, Elsevier, Volume 34, Pages 511 – 517, 2014

[7] Muhammad Sajjad Akbar, Hongnian Yu, and Shuang Cang. "Delay, Reliability, and Throughput Based QoS Profile: A MAC Layer Performance Optimization Mechanism for Biomedical Applications in Wireless Body Area Sensor Networks", Journal of Sensors, Hindawi Publishing Corporation, Volume 2016, November 2015, Pages 1-17

[8] Shah Murtaza Rashid Al Masud, "QoS Taxonomy towards Wireless Body Area Network Solutions", International Journal of application or Innovation in Engineering and Management (IJAIEM), Volume 2, Issue 4, April 2013, Pages 221- 234

[9] 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

[10] 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, 2016, Pages 1746–175

[11] Carlos Abreu, Francisco Miranda, Manuel Ricardo and Paulo Mateus Mendes, "QoS-based management of biomedical wireless sensor networks for patient monitoring", Springer plus, Volume 3, Issue 239, 2014, Pages 1-13

[12] Yangzhe Liao Mark S. Leeson, Matthew D. Higgins, "Flexible quality of service model for wireless body area sensor networks", Healthcare Technology Letter, Volume 3, Issue 1, 2016, Pages 1-15

[13] Nadeem Javaid, Ashfaq Ahmad, Qaisar Nadeem, Muhammad Imran, Noman Haider, "iM-SIMPLE: iMproved stable increased-throughput multi-hop link efficient routing protocol for Wireless Body Area Networks", Computers in Human Behavior, Elsevier, Volume 51, 2015, Pages 1003–1011.

[14] Sudip Misra and Subhadeep Sarkar , "Priority-Based Time-Slot Allocation in Wireless Body Area Networks During Medical Emergency Situations: An Evolutionary Game-Theoretic Perspective", IEEE Journal of Biomedical and Health Informatics , Volume 19, Issue 2, 2015, Pages 541 - 548

[15] Muhammad Mostafa Monowar, Mohammad Mehedi Hassan, Fuad Bajaber, Musaed Al-Hussein and Atif Alamri, "McMAC: Towards a MAC Protocol with Multi-Constrained QoS Provisioning for Diverse Traffic in Wireless Body Area Networks", Sensors, Volume 12, 2012, Pages 15599-15627

[16] Iffat Anjum, Nazia Alam,Md. Abdur Razzaque, MohammadMehedi Hassan, and Atif Alamri, "Traffic Priority and Load Adaptive MAC Protocol for QoS Provisioning in Body Sensor Networks", International Journal of Distributed Sensor Networks, Hindawi Publishing Corporation, Volume 2013, February 2013, Pages 1-9

[17] Zedong Nie, Jingjing Ma, Zhicheng Li, Hong Chen and Lei Wang, "Dynamic Propagation Channel Characterization and Modeling for Human Body Communication", Sensors, Volume 12, 2012, Pages 17569-17587

[18] Chunqiang Hu , Nan Zhang ,Hongjuan Li , Xiuzhen Cheng , Xiaofeng Liao, "Body Area Network Security: A Fuzzy Attribute-Based Signcryption Scheme", IEEE Journal on Selected Areas in Communications, Volume 31, Issue 9, 2013, Pages 37 – 46

[19] Pablo Picazo-Sanchez, Juan E. Tapiador , Pedro Peris-Lopez and Guillermo Suarez-Tangil, "Secure Publish-Subscribe Protocols for Heterogeneous Medical Wireless Body Area Networks", Sensors, Volume 14, 2014, Pages 22619-22642

[20] 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, Elsevier, Volume 135, 2016, Pages 37-50