Mobility Maintenance in Wireless Body Area Network

Manisha Mittal

Department of Electronics and Communication Engineering
NIU, Greater Noida, U.P., India

Dr. D.K. Chauhan

Director Technical
NIU, Greater Noida, U.P., India

Abstract — A WBAN is predicted as a valuable technology being used in many applications, especially in medical application for monitoring and detection of possible problems of patients. Some of the issues are addressed in WBANs, in which the critical issues need to be solved are energy saving and security along with inter-WBANs interference. To evade the inter-WBANs interference along with the control the transmission power on WBAN system, this paper presents a cooperative based power control game algorithm which is utilized with the social interaction information model. In order to manage the WBAN with the security measures to transmit the patient data throughout the system an Elliptic Curve Cryptography (ECC) algorithm is used for authentication before initiating the transmission. The performance of the proposed approach is evaluated along with the increased number of nodes while the occurrence of an interference problem is also rigorous. The proposed approach provides the better results where the power is increased to maximize the system life time of WBAN communication through power game approach, which also mitigates the interference problem efficiently. The WBAN system uses ECC algorithm to perform authentication, encryption and decryption, which yield better security of patient data to establish the communication between the numbers of WBAN.

Keywords — Interference, system utility, WBAN, ECC, Game-theory, Social interaction.

I. INTRODUCTION

One of the issues generated in WBANs is interference due to the short range of frequency usage for communication i.e. one WBAN may overlap with another. Interference is a major problem is generated by other signals from the nearest device or body area operating very close in frequency that disrupts the preferred signals of the body area network. Interference should affect the system performance by dropping packets during the communication. Inter WBANs interference is the most severe concern during communication that diminishes the system performance by affecting the power, signal to interference plus noise ratio (SINR) and throughput degradation. Thus, an effective manner should be explored to deal with the inter WBANs interference along with handling the power of sensor nodes to improve the system life time. The interferences between nearby wireless networks have been analyzed by researchers in [4] [5].

Inter body interference is the key problem [6], which is occurred when two or more WBAN is close to each other. Interference in WBAN is considered as a social interaction carried between people, in which interactions are lost for a few times, and several interactions do not vary in the next time period. This scenario helps to circumvent the interference over WBAN networks. The other challenge is the power control during the interference mitigation in WBANs. An innovative scheme utilized is the cooperative based Game-theoretic approach [7]-[11], which is the optimal solution for power control and interference mitigation in social interaction based WBAN system. The proposed work carries the social contact network based WBAN and power game theoretic approach for the above addressed issues.

II. EFFECTIVE APPROACH FOR ENHANCING THE TRANSMISSION POWER

The main contribution of this paper work is to improve the system performance when the interference occurs between the nodes which are participated in the communication. Thus, the objective function of our work is to avoid
the interference, improve the power after each transmission and high system utility. A cooperative based game theory approach is used to resolve the power control problem to progress the system's utility at the same time it helps to improve the power for transmission and provide better life time of the system. The power control game is usually played if N transmission links between the transmitters and the corresponding receivers established in the N WBANs then they are acting as N players in the game. Initial transmission power is revealed for each N player should be less than the power used for the whole communication P. All players participated in the game are assumed to be cooperative, and there will be a price for each player where the price function is the divergence between weighted utility and weighted power.

The price function is calculated, when the system utility and power is determined as follows,

\[ P(k) \propto k^k \]  
\[ \pi_i(p_i,p_j) = r_i \propto p_i \]  

Before that the SINR is need to discuss here because due to overlapping of nodes this can happen in most scenarios. SINR is described as below,

\[ \Gamma_i = \frac{\sum \mu_i \delta_i p_i}{\sum \sum Z_j p_j q_j u_j \Gamma_j p_j + n_0} \]

Where \( r_i \) is the system utility, bandwidth B and corresponding transmission power of node \( i, j \) are \( P_i \) and \( P_j \). The white noise power is mentioned as \( n_0 \) and \( q_{ij} \) is the channel gain between transmitter \( i \) and receiver \( i \) and \( q_{ji} \) is the channel gain between transmitter \( j \) and receiver \( i \). when the interference distance is calculated then the interference channel gain should be determined.

By using this system utility (U) can be detected as mentioned below,

\[ U = \prod_{i=1}^{N} \mu_i \Gamma_i \]

The power game design is based on the social interaction information. Where the social interaction information helps to mitigate the interference and improve the system utility

III. EXPERIMENT AND RESULT

A secure communication system contains should satisfy the characteristics such as Confidentiality, integrity and authentication. Authentication is an effective action being used for establishing or validating something or someone as genuine [18] or to ensure the identity of the peer node for communicating with facilitated node. Privacy protection is accomplished by authentication, which makes sure verification and validation of one another earlier than revealing any secret information. In this paper, a skilled authentication based on Elliptic curve Cryptography is utilized that suggests realistic security with lesser key length. A point which is taken in an elliptic curve process may be defined as an ordered pair of scalars conforming to the elliptic curve equation considered for verification and validation. ECC is a relative of discrete logarithm cryptography where an elliptic curve E over the finite set of point \( \mathbb{F}_p \) is defined by an equation:

\[ y^2 = x^3 + ax + b \]

Where \( a, b \in \mathbb{F}_p \) with a point \( O \) at infinity and \( E(\mathbb{F}_p) \) consists all the points \( (x,y), x \in \mathbb{F}_p, y \in \mathbb{F}_p \). Basic Elliptic Curve operations are point addition and point doubling where elliptic curve cryptographic primitives
have need of scalar point multiplication. Multiplication is defined by repeated addition where an addition operation is performed over elliptic curves that include pairs of non-zero integers modulo a prime number \( q \). Multiplication is done if a given a point \( P(x, y) \) on an Elliptic Curve, then needs to compute \( kP \), where \( k \) is a positive integer which is like a series of addition of \( P \).

The authentication is initiated by sending the request to the nodes for communication and if there is a response from the corresponding node, then it verifies the authentication of the requested node. The initial process is to exhibits a key pair generation from which the nodes can obtains a private and public key and then it will be preceded for the authentication process. The verification and validation condition will be satisfied only if the private key, public key and the generating point are same otherwise the condition will be false. After checking the authentication of the other node, the prior node will start its message transformation. Most of them discussed ECC algorithm for authentication and security purposes [17]-[20].

For example, if the request is assumed a random number \( r_1 \) along with the point \( P_1 \) on elliptic curve, from which the requesting code calculated may be as \( R_c = (r_1 * P_1) \), which is defined as follows,

\[
R_c = (r_1 * P_1)
\]

The requesting code is then forwarded to the corresponding nodes for exchanging the information. The corresponding node receives the request and generates a random number \( r_2 \) and sends it back to the requested node. Then authentication verification \( A_{VER} \) is needed, which is calculated based on the private and public key belongs to the requested node by its private key \( K_p \), which is defined as follows,

\[
A_{VER} = r_1 + (r_2 * K_p)
\]

Then the condition used to verify and validate the nodes based on its public key \( K_P \) is described by the following manner,

\[
(A_{VER} * P_L) - r_2 * K_p = R_c
\]

If the above-mentioned condition illustrated in equation is satisfied, then the node wishes to participate in the communication are promoted as a valid one and are not an eavesdropper. After that the node will start its message transformation by performing an encryption and decryption using the corresponding public and private key pairs.

IV. EVALUATION RESULTS

The simulated network is constructed as a scale free network with \( P_i/ n_0 = 40 \text{ dB} \) and \( B=128 \). The WBAN nodes are placed randomly over the network area based on the Social Interference Network algorithm in which the area is \( 20 \text{ m} * 20 \text{ m} \) square area. All the WBAN (or human) carries a receiver and the transmitters which are placed in a circle of \( 1 \text{ m} * 1 \text{ m} \) centered on the appropriate receivers. The centers are receivers, and the transmitters are randomly placed in the corresponding circles. This representation is mention in figure 3 as social interaction network with random distributed WBAN nodes. The center nodes are always the receiver, and each WBAN node consists of more transmitters. In that representation, two red circles initiate the communication in which the link describes the communication establishment between two nodes. The interference distance is calculated based on the channel gain between the transmitter and receiver where each user is initialized with a random transmitting power, and then it updates the power according to the price after applying power game theory.

Figures illustrates the system utility where the total utility of the network is increased when there are more nodes in the network.
Figure 1: WBAN Nodes Random Placement in Social Interaction Network

Figure 2: System Utility Based On Number of Nodes in Wireless Network
The graph plotted in figure 3 shows the average and total power variation after each transmission is updated in order to improve the system life time. The results effectively prove that the proposed game-theoretic approach is successfully carried out the interference mitigation and power control even the number of nodes is increased in the network. Channel gain and SINR are calculated to measure the system utility and price, power function.

V. CONCLUSIONS

In our WBAN node of the communication scheme, ECC algorithm is applied where the receiver node is meant to receive the information, and the transmitter node is meant to transmit the information to a valid data server. As discussed earlier, there are lots of possibilities for hacking the medical information when there are no securities and authentication measures are used to protect the communication. Using the ECC based algorithm when there is a request for initiates the communication then that are allowed to verify and validate them before transmission. Figure 9 shows the encrypted and decrypted signal using ECC which significantly proven that the WBAN communication enabled in our scheme is the secure and effective communication approach. The future work will mainly concentrate to the more effective secure mechanisms along with improved interference detection schemes.

REFERENCES


