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,

$$P(k) \propto k^{\alpha} \tag{1}$$

$$\pi_i(p_i, p \quad i) = r_i \quad w \times p_i \tag{2}$$

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,

$$r_i = \frac{q_{ii}(\vec{d}_{ii})p_i}{\frac{1}{B}\sum_{j\neq i} q_{ji}(\vec{d}_{ji})p_j + n_0} \tag{3}$$

Where r_i is the system utility, bandwidth B and corresponding transmission power of node *i, j* are Pi and Pj. The white noise power is mentioned as *n0* and q_{ii} 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,

$$U = \sum_{i=1}^{N} \omega_i g(r_i) \tag{4}$$

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 F_p is defined by an equation:

$$y^2 = x^3 + ax + b$$

Where $a, b \subset F_p$ with a point O at infinity and E (F_p) consists all the points $(x, y), x \subset F_p, yx \subset F_p$. 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 r1 along with the point P1on elliptic curve, from which the requesting code calculated may be asR_c, 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 r2 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_s, which is defined as follows,

$$A_{VER} = r_1 + (r_2 * K_s)$$

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

$$(A_{VER} * P_1) - r_2 * K_p = R_c$$

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 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 m * 20 m square area. All the WBAN (or human) carries a receiver and the transmitters which are placed in a circle of 1 m * 1 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.

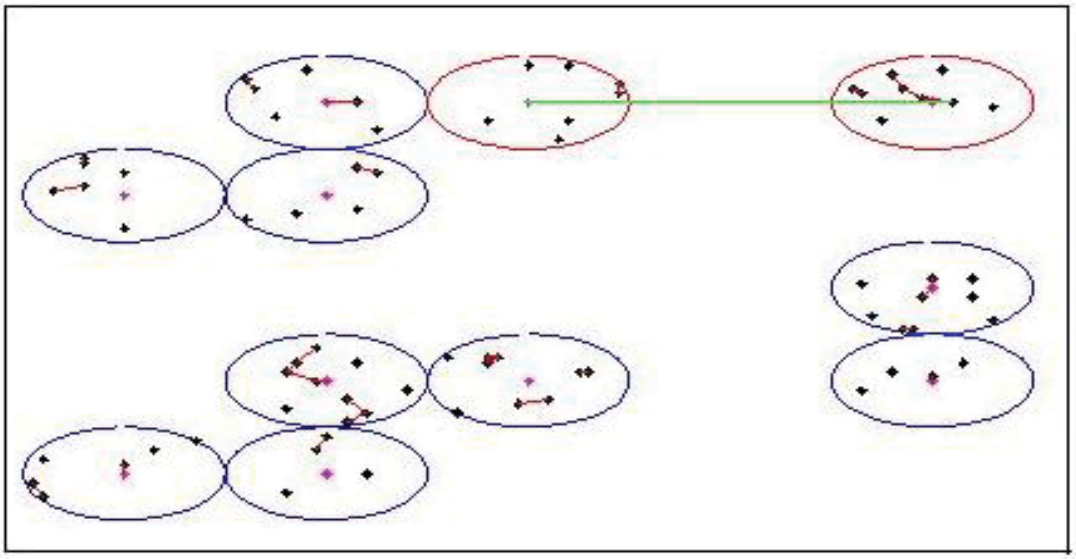

Figure 1: WBAN Nodes Random Placement in Social Interaction Network

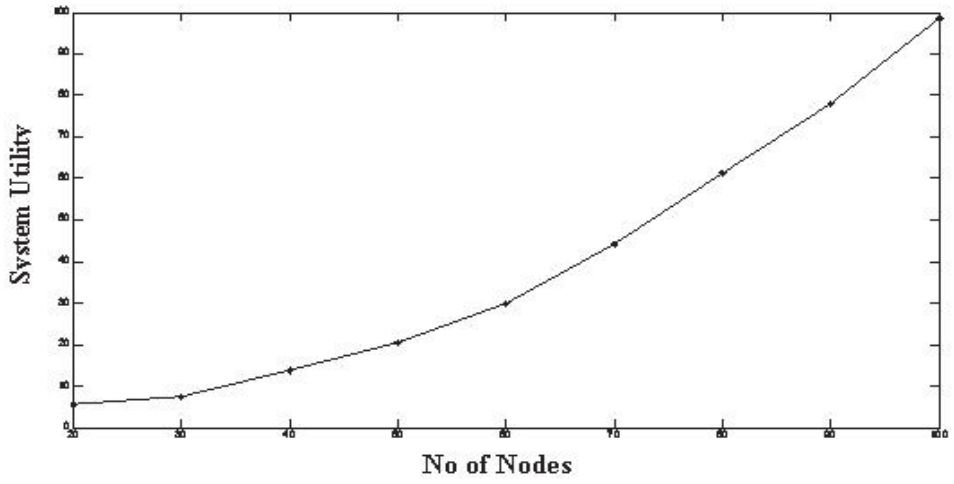

Figure 2: System Utility Based On Number of Nodes in Wireless Network

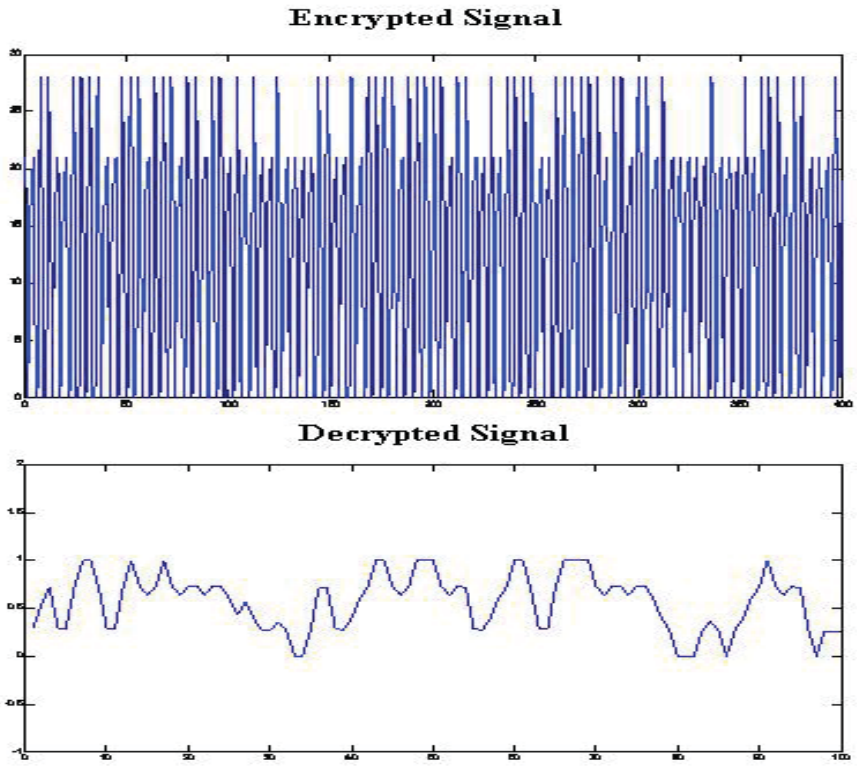

Figure 3: Encrypted and Decrypted sample ECG Signals using Elliptic Curve Cryptography Algorithm

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

[1] K. Wac, R. Bults, B. van Beijnum, I. Widya, V. Jones, D. Konstantas, M. Vollenbroek-Hutten, H. Hermens , “Mobile Patient Monitoring: the MobiHealth System”, 31st Annual International Conference of the IEEE EMBS Minneapolis, Minnesota, USA, September 2-6, 2009.

[2] Aart Van Halteren, Richard Bults, Katarzyna Wac, Nicolai Dokovsky, George Koprinkov, Ing Widya, Dimitri Konstantas, Val Jones, “Wireless Body Area Networks for Healthcare : the MobiHealth Project”, Wearable eHealth Systems for Personalised Health Management, Studies in Health Technology and Informatics Vol. 108, 2004, pp. 121 – 126.

[3] Huasong Cao and Victor Leung and Cupid Chow and Henry Chan, “Enabling Technologies for Wireless Body Area Networks: A Survey and Outlook”, IEEE Communication on Consumer Communications and Networking, pp. 84 – 93, December 2009.

[4] Gengfa Fang, Eryk Dutkiewicz, Kegen Yu, Rein Vesilo and Yiwei Yu, "Distributed Inter-Network Interference Coordination for Wireless Body Area Networks", IEEE Global Telecommunications Conference, pp. 1-5, 2010.

[5] Jitendra Padhye, Sharad Agarwal, Venkata N. Padmanabhan, Lili Qiu, Ananth Rao and Brian Zill, "Estimation of Link Interference in Static Multi-hop Wireless Networks", Internet Measurement Conference 2005.

[6] Kamal Jain, Jitendra Padhye, Venkata N. Padmanabhan, Lili Qiu, "Impact Of Interference On Multi-hop Wireless Network Performance", IEEE Proceedings of the 9th annual international conference on Mobile computing and networking, pp. 66-80, 2003.

[7] Farhad Meshkati, H. Vincent Poor, Stuart C. Schwartz, Narayan B. Mandayam, "A Utility-Based Approach to Power Control and Receiver Design in Wireless Data Networks" , IEEE Transactions On Communications, 2005.

[8] Eitan Altman and Zwi Altman, "S-Modular Games and Power Control in Wireless Networks", IEEE Transactions on Automatic Control, Vol. 48, NO. 5, May 2003.

[9] Cristina Comaniciu, Dandan Wang, Hlaing Minn and Naofal Al-Dhahir, "A Game Theoretic Solution for Exploiting Multiuser Diversity in Cooperative Slotted Aloha", IEEE International Conference on Communications, pp. 6085 – 6090, June 2007.

[10] HyungJune Lee, Hyukjoon Kwon, Arik Motskin, and Leonidas Guibas, "Interference-Aware MAC Protocol for Wireless Networks by a Game-Theoretic Approach", In proceeding of INFOCOM, 28th IEEE International Conference on Computer Communications, 25 April 2009.

[11] Markos P. Anastasopoulos, Pantelis-Daniel M. Arapoglou, Rajgopal Kannan, and Panayotis G. Cottis, "Adaptive Routing Strategies in IEEE 802.16 Multi-Hop Wireless Backhaul Networks Based On Evolutionary Game Theory", IEEE Journal On Selected Areas In Communications, Vol. 26, No. 7, September 2008.

[12] Ming Li and Wenjinglou, Kuiren, "Data security and privacy In Wireless Body Area Networks", IEEE Wireless Communications on Wireless Technologies For E-Healthcare, February 2010.

[13] Steve Warren, Jeffrey Lebak, Jianchu Yao, Jonathan Creekmore, Aleksandar Milenkovic and Emil Jovanov, "Interoperability and Security in Wireless Body Area Network Infrastructures", IEEE Proceedings of the 27th Annual Conference, September 1-4, 2005.

[14] Shu-Di Bao, Yuan-Ting Zhang, Lian-Feng Shen, "A Design Proposal of Security Architecture for Medical Body Sensor Networks", IEEE Proceedings of the International Workshop on Wearable and Implantable Body Sensor Networks, 2006.

[15] Tao Ma, Pradhumna Lal Shrestha, Michael Hempel, Dongming Peng, Hamid Sharif, and Hsiao-Hwa Chen, "Assurance of Energy Efficiency and Data Security for ECG Transmission in BASNs", IEEE Transactions on Biomedical Engineering, Vol. 59, No. 4, April 2012.

[16] Ming Li, Shucheng Yu, Wenjing Lou and Kui Ren, "Group Device Pairing based Secure Sensor Association and Key Management for Body Area Networks", IEEE Proceedings INFOCOM, pp. 1-9, March 2010.

[17] Krishna K. Venkatasubramanian, Ayan Banerjee, and Sandeep Kumar S. Gupta, "PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks", IEEE Transactions on Information Technology in Biomedicine, Vol. 14, No. 1, January 2010.

[18] SK Hafizul Islam, G.P. Biswas, "Design of improved password authentication and update scheme based on elliptic curve cryptography", Information System Security and performance Modeling and simulation for future mobile networks, Elsevier, Volume 57, issues 11-12, pp. 2703-2717, June 2013.

[19] Padma Bh, D.Chandravathi, P.Prapoorna Roja, "Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method", International Journal on Computer Science and Engineering Vol. 02, No. 05, pp. 1904-1907, 2010.

[20] Neal Koblitz, Alfred Menezes, Scott Vanstone, "The State of Elliptic Curve Cryptography", Designs, Codes and Cryptography, 19, 173–193 (2000).

[21] Xu Huang, Pritam Gajkumar Shah, and Dharmendra Sharma, "Multi-Agent System Protecting from Attacking in Elliptic Curve Cryptography", Advances in Intelligent Decision Technologies Smart Innovation, Systems and Technologies, Elsevier, Volume 4, 2010, pp 123-131.

[22] Ding Wang, Chun-guang Ma and Yu-heng Wang, "On the Security of an Improved Password Authentication Scheme Based on ECC", Information Computing and Applications Lecture Notes in Computer Science, Elsevier, Volume 7473, 2012, pp 181-188.

[23] Mark A. Hanson, Harry C. Powell Jr., Adam T. Barth, Kyle Ringgenberg, Benton H. Calhoun, James H. Aylor, and John Lach, "Body Area Sensor networks: Challenges And opportunities", Published by the IEEE Computer Society, 2009.

[24] Aleksandar Milenkovic, Chris Otto, Emil Jovanov, "Wireless sensor networks for personal health monitoring: Issues and an implementation", Elsevier, Volume 29, pp. 2521- 2533, August 2006.

[25] Thomas Guthrie Zimmerman, "Personal Area Networks (PAN): Near-Field Intra-Body Communication" IEEE IBM Systems Journal, Volume: 35, Issue: 3.4, 1996.

[26] Jordi Agud Ruiz and Shigeru Shimamoto, "A Study on the Transmission Characteristics of the Human Body towards Broadband Intra-body Communications", IEEE Proceedings of the Ninth International Symposium on Consumer Electronics, 2005. (ISCE 2005). June 2005.

[27] Namjun Cho, Jerald Yoo, Seong-Jun Song, Jeabin Lee, Seonghyun Jeon, and Hoi-Jun Yoo, "The Human Body Characteristics as a Signal Transmission Medium for Intra body Communication", IEEE Transactions on Microwave Theory and Techniques, Vol. 55, No. 5, May 2007.

[28] Jordi Agud Ruiz, Shigeru Shimamoto, "Experimental Evaluation of Body Channel Response and Digital Modulation Schemes for Intra-body Communications", IEEE International Conference on Communications, 2006. ICC '06. (Volume: 1), pp.349 – 354, June 2006.

[29] Laura Galluccio, Tommaso Melodiay, Sergio Palazzo, Giuseppe Enrico Santagati, "Challenges and Implications of Using Ultrasonic Communications in Intra-body Area Networks", IEE 9th Annual Conference on Wireless On-demand Network Systems and Services (WONS), 2012.

[30] Shamik Sengupta, Mainak Chatterjee, and Kevin A. Kwiat, "A Game Theoretic Framework for Power Control in Wireless Sensor Networks", IEEE Transactions on Computers, Vol. 59, No. 2, February 2010.

[31] Yongkangxiao, Xiuming Shan and Yongren, "Game Theory Models for IEEE 802.11 DCF in Wireless Ad Hoc Networks", IEEE Communications Magazine, Volume: 43, Issue: 3, March 2005.

[32] Sofia Najwa Ramli, Rabiah Ahmad, Mohd Faizal Abdollah and Eryk Dutkiewicz, "A Biometric-based Security for Data Authentication in Wireless Body Area Network (WBAN)", IEEE 15th International Conference on Advanced Communication Technology (ICACT), pp. 27-30, Jan. 2013.

[33] M. J. Morón, J. R. Luque, A. A. Botella, E.J. Cuberos, E. Casilari and A. Díaz-Estrella, "J2ME and smart phones as platform for a Bluetooth Body Area Network for Patient-telemonitoring", 2007.

[34] Zhaoyang Zhang, Honggang Wang, Chonggang Wang and Hua Fang, "Interference Mitigation for Cyber-Physical Wireless Body Area Network System Using Social Networks", IEEE Transactions On Emerging Topics In Computing, Volume: 1, Issue: 1, pp. 121-132, June 2013.,