Cost Effective Security Solutions for Mobility in Wireless Body Area Networks

Manisha Mittal
PhD Scholar, Department of Electronics and Communication Engineering
Noida International University,UP, India

Dr. D.K.Chauhan
Director Technical
Noida International University,UP, India

Suryakant
Assistant Professor
Noida International University,UP, India

Abstract- Body Sensor Network (BSN) that is linked by a wireless network interface roams from one coverage zone to another then interference between wireless-body-area-networks (WBAN) created, which can cause serious throughput degradation, Scattering of WBAN and Remote Base Station (RBS) will not be in range. When a wireless body area network become mobile then problem arises of inter process interference A necessity appears for efficient WBAN monitoring information extraction, high spatial reuse, dynamically fine tuning the monitoring process to suit the data quality. This paper proposes an optimized BSN handover strategy, and hop by hop method to reach RBS (Sink), and a method to maximize the network throughput by using stable routes to avoid inter- and intra-flow interferences based on mobility prediction.

Keywords – Watermarking, Haar Wavelet, DWT, PSNR Body Sensor Network (BSN), wireless-body-area-networks (WBAN), RBS (Remote Base Station) RASS (Real-Time, Accurate, and Scalable System), VMISO (Virtual Multiple Input Single Output), Inter-WBAN scheduling (IWS), PS (Personal Server). ***Interference, system utility, WBAN, ECC, Game-theory, Social interaction***

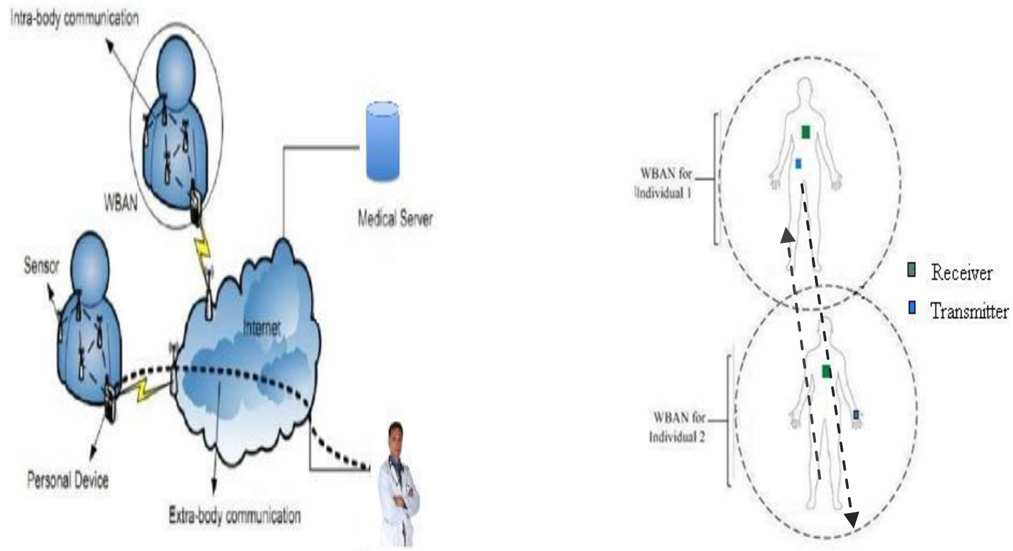
I. INTRODUCTION

With the evolution of inexpensive and lightweight of sensors, most of the applications are encouraged to utilize them where one of the key mechanisms is a Remote Health Monitoring by Wireless Body Area networks (WBAN). WBAN initiates the communication by sensors attached on the human body that helps to take decisions for treatment through effective monitoring by an external medical representative. Due to the short frequency range of bio-sensors, WBANs is influenced with an interference problem that degrades system performance by clashing the medical data. With the aim of avoiding communication interference in WBANs, social interaction based network is designed to detect the interference between one WBAN to another body area. When try to evade the interference problem the key issue has to consider is the power control of sensors to maintain the system utility. To improve the system utility a game-theoretic approach is enabled along with that an Elliptic Curve Cryptography approach is adopted with WBAN for authentication and secure communication between sensors of body area. The results show the effectiveness of the proposed secure power aware scheme of WBAN.

Wireless body area networks (WBANs) grow to be a promising technology due to the diversity manner along with the miniaturization of devices used for communication and monitoring [1] [2]. Recently, WBANs emerged as a significant evolution to offer opportunities to move in tele-medicine, which facilitates the effective consultation between the patient and medical representatives. In order to continuously monitoring and sensing the patient health and provide corresponding information to the respective medical personal WBANs consist of various low cost sensors, which are deployed on the human body. The wearable and commonly used small sensor devices in medical applications are ECG, EEG, etc., which can communicate with a network and helps to monitor the patient conditions such as measuring heartbeat, body temperature and so on [3]. The monitoring signals and data are then collected from the appropriate sensors by a personal device i.e. a smart phone that transmits the collected information to the healthcare professional for health monitoring.

WBAN should establish a secure communication with another WBAN to protect patient's privacy and prevent hacking into the network and periodically updates the user's medical record. When dealing with medical applications, it is imperative that a system should provide great security and authenticity [12]-[16] between users or personal devices in WBAN to make an effective system. A unique challenge for secure communication in WBAN is the communication between nodes, which should not share any sensitive information, especially access to patient data must be strictly limited only to authorized users. In order to accomplish the system security and to facilitate the authentication process, the cryptographic based approach is utilized, which is an Elliptic Curve Cryptography (ECC) algorithm [17]-[22] is enabled in this paper.

II. INTERENFERENCE BASED WBAN SYSTEM DESIGN AND ARCHITECTURE



(a) WBAN Communication

(b) Interference problem in WBANs

Figure 1: System Architecture

Every human carries a WBAN, which consists of a central node which is assumed as a receiver and several sensor nodes within the body area is assumed as a transmitters which are used to initiate the communication. In WBAN system, the sensors attached on the body can communicate with other body sensor nodes and personal devices through either Zigbee or Bluetooth technology due to most mobile phones enabled with Bluetooth receivers. When the communication is taken place between the nodes presented in WBAN, there will be an interference occurrence because human sensors are nearly close to other sensors of body area.

Inter-body and extra body communications are carried out in WBAN system (see figure 1 (a)) where interference is also appeared which are described in figure 1(b) in which the arrow indicate the interference link and the circle represents the coverage area. The interference is referred as from the links between one person's transmitter and other receivers. Thus when person A's receiver receives the message from person B's transmitter and the transmitter of person A send message to person A's receiver at the same time, then interference occurs between B's transmitter to A's receiver. The interference distribution and interference distance is calculated which are the significant role to find the noise and mitigate the interference between the nodes.

A WBAN system is initially designed as an inter-network interference model where the nodes satisfy power law distribution similar to a social contact network model [34].The system constructs a scale free network which satisfies the power law exponent in which the nodes level does not change based on the size of the network. Based on power law distribution [34], the nodes should have k neighbors as $P(k)$ is proportional to $K^{-\propto}$ for a large value of k is denoted as below;

$$P(k) \propto k^{\propto} \quad (1)$$

The social interference network algorithm is based on the power law exponent.

III. EVALUATION RESULTS

After applying the power game theory the work observes the performance of the power control game with the number of the nodes increasing from 20 to 100. If there are more nodes in the network, the interference increases and most of the nodes need to reduce their power to reduce the interference according to the power control game. Figure 4 illustrates the system utility where the total utility of the network is increased when there are more nodes in the network.

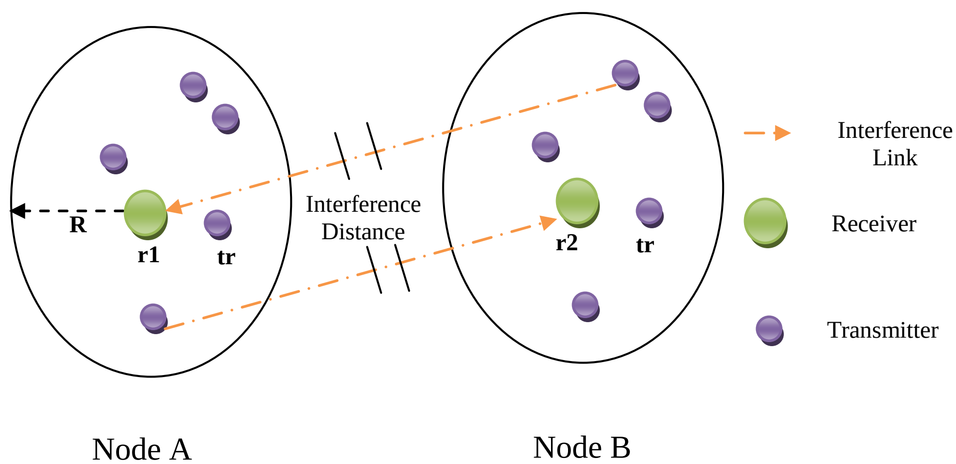


Figure 2: Interference link and distance

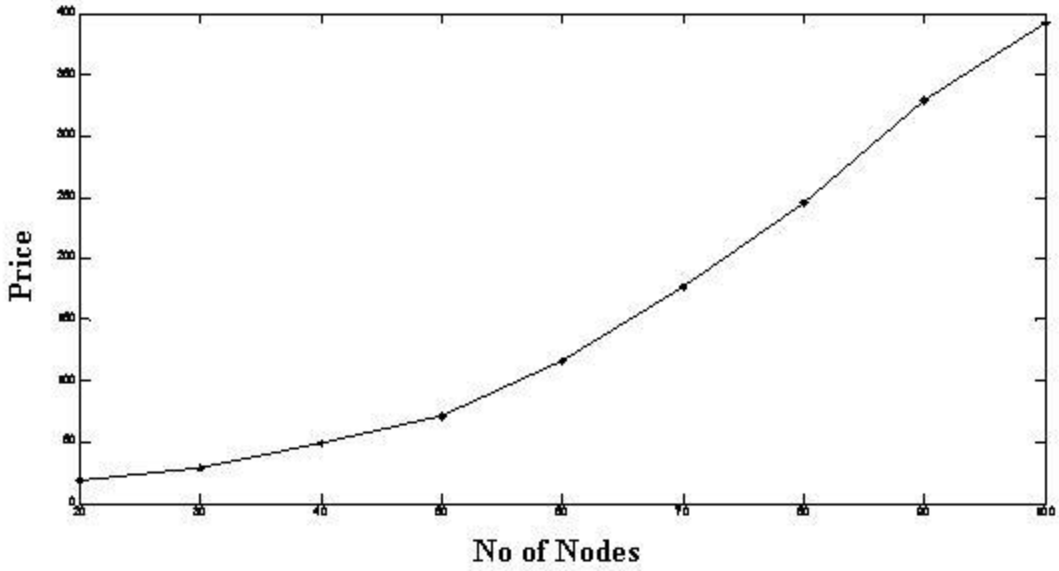


Figure 3: Total Price according to the Number of Nodes in the Network

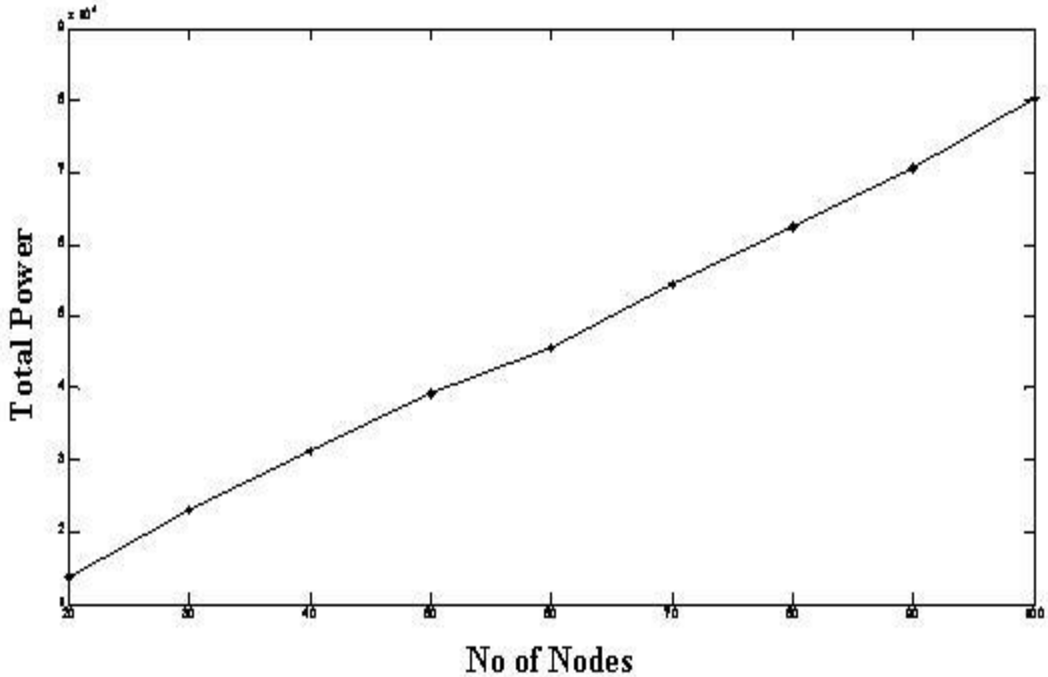


Figure 4: Total Power vs. Number of Nodes in the Network

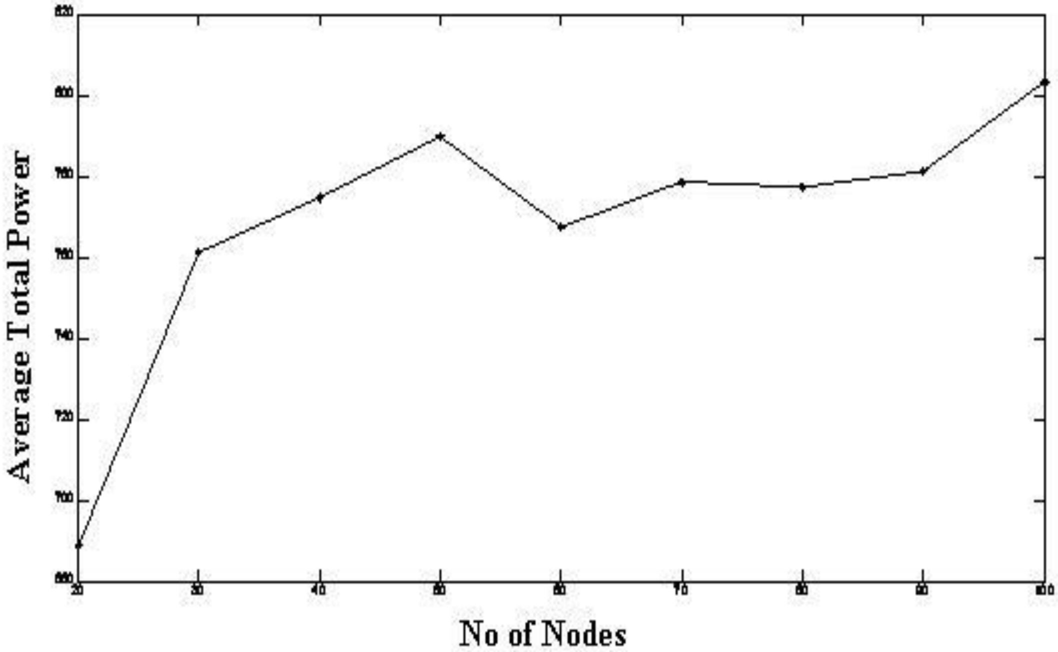


Figure 5: Average Total Power vs. Number of Nodes in the Network

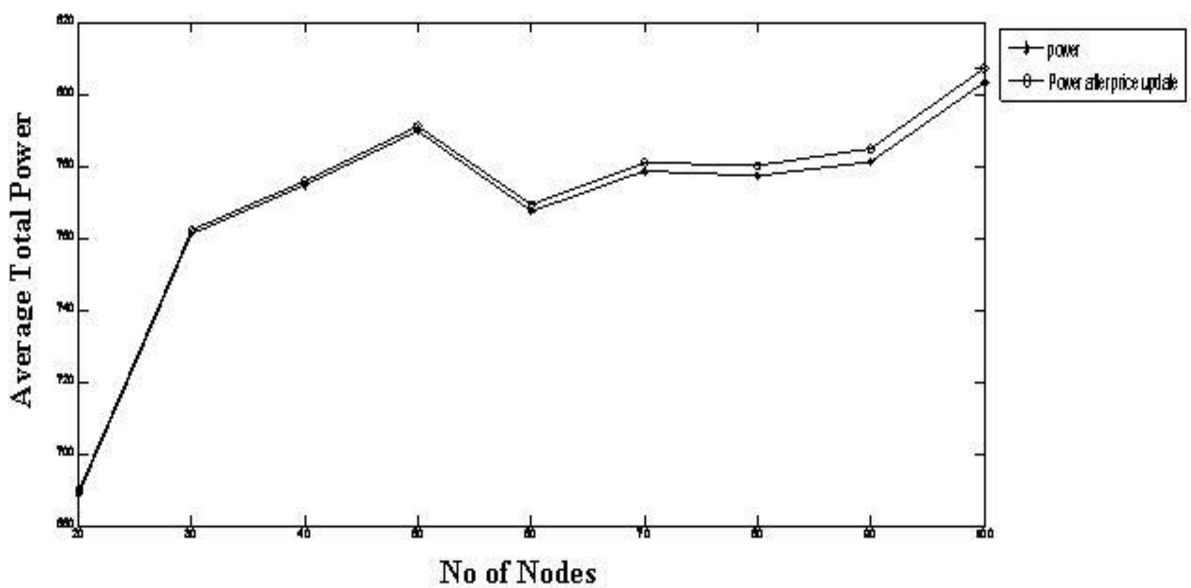


Figure 6: Average Total Power and Power after Price update while Number of Nodes in the Network

The graph plotted in figure 5 and 6 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.

IV.CONCLUSION

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

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.,