International Journal of Engineering Research and Reviews ISSN 2348-697X (Online)
Vol. 6, Issue 4, pp: (17-24), Month: October - December 2018, Available at: www.researchpublish.com

Incentive Based Energy and QoS Efficient Algorithm for Wireless Body Area Networks

Niraj Korde[1], Urmila Deshmukh[2]

[1,2] Indira College of Engineering and Management

Abstract: **To solve the current research problem for dynamic WBAN communications, we proposed novel opportunistic communication protocol for WBANs with aim to solve the research challenges not only the energy efficiency and network management cost reduction but also solves the problem non-reliable nodes data dissemination. First we proposed a novel energy-efficient and distributed network management cost minimization framework for dynamic connectivity and data dissemination in opportunistic WBANs. Then proposed the pricing based approach for reliable node data dissemination. We introduced a pricing based approach to optimize the network management cost for opportunistic WBANs. Concurrently, the behaviours of WBANs are taken into the consideration (i.e., critical and normal condition) to provide reliable services. We proposed algorithms: (1) energy efficient prioritized opportunistic communications algorithm, (2) optimal network cost reduction algorithm.**

Keywords: **Cost Management, Energy Management, reliable data dissemination, WBAN.**

I. INTRODUCTION

Wireless Body Area Networks (WBAN)/Wireless Body Area Sensor Network (WBASN) consist of sensor nodes attached in and around the human body to monitor the bio signals of human being for a variety of applications such as patient monitoring, gaming etc. This term has been first coined by Van Dam et al (2001) and received the interest of several researchers. Due to the advancements in MEMS and wireless communication technologies, WBAN has undergone a technical boom in the last decade. The schematic overview of differences between Wireless Sensor Networks and Wireless Body Area Networks is given by [1]. There are significant points to be noted in the Wireless body area network. As opposed to the wireless sensor network, the WBAN monitoring environment is restricted to the human body, heterogeneous data rate, the requirement of biocompatible sensor devices and more variable network topology due to body movement.

The communication in the Body sensor network is categorized into two types, in body communication is the RF communication between invasive sensor nodes implanted inside the human body and on body communication is the communication between wearable sensor nodes. The MICS (Medical Implantable Communication Service) band – 402-405 MHz should be used for in body communication (Sana Ullah et al 2010a). ISM or UWB can be used for on body communication.

A WBAN provides real-time electronic healthcare services to medically emergent patients in a cost effective manner. In a WBAN, several body sensor nodes are implanted on/in the human body to sense the physiological signals of patients. After sensing the physiological signals, the sensor nodes send the sensed data to the Local processing Unit (LPU). Subsequently, the LPU transmits the aggregated data to the local access points (APs), which, in turn, send them to the medical servers [3], [4]. The body sensor nodes transmit the medical data to LPUs at wide range of data rates from 10 Kb/s to 10 Mb/s [5]. Also, the energy consumption rates of sensor nodes are restricted to certain limits, as the battery power of these nodes is limited. To minimize energy consumption, the sensor nodes use a one-hop star topology to send their medical data [6]. However, mobility, body postures, and environmental obstacles increase the dynamism in WBANs, which frequently changes the network topology, which, in turn, decreases the network QoS. Additionally, the link-quality between nodes in WBANs varies as a function of time due to various body movements, which also affects the inter-node connectivity [7].

Due to body movements and mobility of WBANs [6], the link qualities of intra-BAN and inter-BAN communication units degrade significantly, which increases the packet loss rate and decreases the life-time of the body sensor nodes. Further, the above also disrupts data dissemination. Therefore the QoS management cost in the network increases in order to maintain fair QoS among WBANs. As the network connectivity establishment and QoS management costs increase in the network, we need a network management cost minimization framework to provide reliable and cost effective service to WBANs. We introduced energy efficient and QoS efficient communication protocol for WBAN based on energy management cost minimization and QoS management cost minimization with reliable data dissemination.

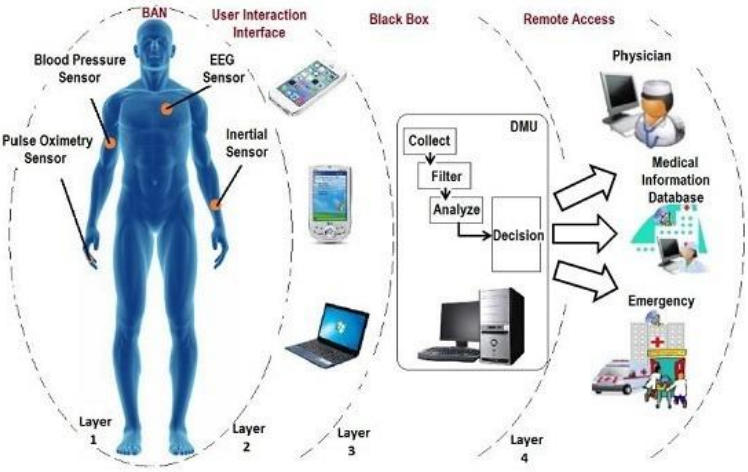

Figure 1: WBANs working scheme

II. RELATED WORKS

In this section, we represent the review of research works on practical communication protocol and energy consumption techniques for WBANs.

Samanta et al. [8], [9] investigated that link-quality-mindful asset assignment cum load adjusting plan for the hub in WBANs. In this system, the researcher has used two sub-issues dynamic resource portion and link-quality measurement in WBANs. These research works manage the adaptability of WBANs they don't examination the progression of network organization cost within the sight of body/ limb action in WBANs, in light of which the aggregate whole of network cost raising and the QoS of WBANs.

Elias at al. [10] innovated that an energy mindful ideal plan of energy successful and furthermore, financially savvy WBANs. This framework analyzed a financially savvy way; the analyst does not inspect the outcomes of dynamically exists and opportunistic information diffusing in WBANs. This raising the deferment and packet killed of the network.

Zhao et al. [11] investigated a network price minimization scheme for information fragmentation in WSNs. In the first place, this procedure does not inspect the required record of WBANs in the best way to deal with the survey the therapeutic state of the WBAN- devices patients, which is one of the extraordinary qualities of WBAN-based Deliberation.

Energy-effective and dependable Deliberation are essential requests of WBANs; these are supplies touchy therapeutic data because of shadowing and disappear outcomes inside the network, the energy utilization rate of sensor focus points increments, what's more, the trustworthiness in bits of knowledge transmission lessons, intermittently. To explosion the power execution and immovable quality in bits of knowledge transmission recently wide variety of strategies reported.

Yousaf et al. [12] investigated that, another three-level helpful transferring plan for WBANs. As casing sensor hubs deliver clinical insights at a variable charge, their relating activity design is unverifiable in nature. Subsequently, within the sight of negative hyperlink-agreeable, the parcels drop the charge the network and the power confirmation of body sensor focus point expands.

Andreagiovanni and Nardin [13] analyzed that vigorous approach for combine streamlining of energy correctness and information rate in WBANs under development absence of value. In this advancement work, the bundle transmission rate of body sensor center is thought to be homogenous in nature; regardless, in the province of WBANs, the packet transmission rate of body sensor focus points is heterogeneous.

Huang and Cai [14] researched proposed a concern conscious booking plan for utilized by a WBAN inside the presence of more than one coinciding WBANs. To grow the group throughput of WBANs, a nonlinear development trouble is portrayed, while thinking about the demands between WBANs. This work is obliged to handiest the stress mindful booking of WBANs inside the closeness of impedance between matching WBANs. Notwithstanding, they do never again think about the elevated network association value inside seeing impedance.

Ibarra et al. [15] investigated a combined power and QoS control structure to plans of energy and got the best QoS in WBANs. The base paper techniques are analysis the difficulty traffic ministry for the information transference system. Be that as it may, this method isn't utilized for a wide range of traffic administration in the network.

Similarly, Seyedi at al. [16] evolved one-of-a-kind energy efficient data transmission scheme for WBANs. As a way to provide power-green statistics transmission, the tradeoffs among energy admission and packet mistakes possibility are implanted into the sensor center points. This frame neglects to offer QoS to WBANs inside sight of community dynamics, on due of flexibility.

Also, Seyedi et al. [17] researched that a Markov-chain depend analytical approach for energy aggregate hub in WBANs, in which the probability of circumstance hardship is examined to see the energy hardship circumstance of the body sensors center point. Ren et al. [18] explored an approach which secures higher network throughput for synchronize WBANs. The base paper works does not fulfil to supplies robustness in the network management approach for WBANs.

III. PROPOSED DESIGN

To optimize the reliable data communication approach, we design the pricing technique in this paper. The pricing method rewards the nodes that relay others' packets and charges those that send packets. The trust system evaluates the nodes' competence and reliability in relaying packets in terms of multi-dimensional trust values. The trust values are attached to the nodes' public-key certificates to be used in making routing decisions. We develop routing technique to transmit the data via those highly-trusted nodes having sufficient energy to minimize the probability of breaking the route. This proposed technique can maintain route stability and report correct battery energy capability. This is because any loss of trust will result in loss of future earnings. Moreover, for the efficient implementation of the trust system, the trust values are computed by processing the payment receipts. Figure 1 shows the architecture for the proposed pricing based data dissemination in WBANs.

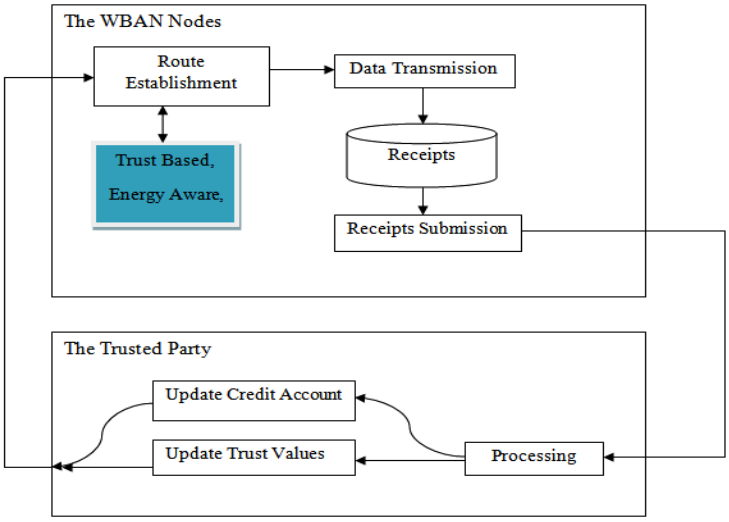

Figure 2: Pricing based data transmission

The working of trust based model is explained in below sections:

Below sections are discussing the key terminologies of proposed routing methods.

A. Data Transmission Phase

Let the source node NS send messages to the destination node ND through a route with the intermediate nodes NX, NY, and NZ. For the ith data packet, NS computes the signature $\varepsilon_s(\mathrm{i}) = \{H(H(m_i), t_s, r, i)\}K_{s+}$ and sends the packet $< R, t_s, i, m_i, \varepsilon_s(i) >$ to the first node in the route. R, ts, and mi are the concatenation of the identities of the nodes in the

route (R=IDS, IDX, IDY, IDZ, IDD), the route establishment time stamp, and the ith message, respectively H (d) is the hash value resulted from hashing the data d using the hash function. H (). {d}Ks+ is the signature of d with the private key of NS. The purpose of the source node's signature is to ensure the message's authenticity and integrity and secure the payment by enabling TP to ensure that NS has sent i messages. Each intermediate node verifies $\varepsilon_s(i)$ and stores $\varepsilon_s(i)$ and $H(m_i)$ for composing the receipt. It also removes the previous ones $(\varepsilon_s(i-1)$ and $H(m_i-1)$ because $\varepsilon_s(i)$ is enough to prove transmitting i messages. Signing $H(m_i)$ instead of mi can reduce the receipt size because the smaller-size $H(m_i)$ is attached to the receipt instead of mi.

The destination node generates a one-way hash chain by iteratively hashing a random value hS S times to obtain the hash chain {hS, hS-1,…,h1, h0}, where hi-1= H (hi) for 1 ≤ i ≤ S and h0 is called the root of the hash chain. The node signs h0 and R to authenticate the hash chain and link it to the route, and sends the signature to the source node in route establishment phase. In order to acknowledge receiving the message mi, the destination node sends ACK packet containing the preimage of the last released hash chain element or hi. Each intermediate node verifies the hash chain element by making sure that hi-1 is obtained from hashing hi, and saves hi for composing the receipt and removes hi-1. The underlying idea is that $\varepsilon_s(i)$ and hi are undeniable proofs for sending and receiving i messages, respectively.

Each node in the route composes a receipt and submits it when it has a connection to TP to claim the payment and update its trust values. A receipt is a proof for participating in a route and sending, relaying, or receiving a number of messages. A receipt contains R, ts, i, (mi), h0, hi, Cm, and an undeniable cryptographic token for preventing payment manipulation. Cm is data that depends on the used routing protocol, such as the number of messages the intermediate nodes commit to relay. The cryptographic token contains the hash value of the last source node's signature and Auth_Code. Auth_Code is the authentication code that authenticates the hash chain and the intermediate nodes to hold them accountable for breaking the route. If i messages are delivered, the format of the receipt is <R, ts, i, (mi), h0, hi, Cm, H ($\varepsilon_s(i)$, Auth_Code)>, $\varepsilon_s(i)$ and Auth_Code are hashed to reduce the receipt's size.

B. Update Credit Account and Trust Values

Once TP receives a receipt, it first checks if the receipt has been processed before using its unique identifier (R, ts). Then, it verifies the credibility of the receipt by computing the nodes' signatures (j(i) and Auth_Code) and hashing them. The receipt is valid if the resultant hashes value is identical to the receipt's cryptographic token. Below equations are used for trust values during the routing phase.

Let the source node NS send messages to the destination node ND through a route with the intermediate nodes NX, NY, and NZ. For the ith data packet, NS computes the signature $\varepsilon_s(\mathrm{i}) = \{H(H(m_i), t_s, r, i)\}K_{s+}$ and sends the packet $< R, t_s, i, m_i, \varepsilon_s(i) >$ to the first node in the route. R, ts, and mi are the concatenation of the identities of the nodes in the route (R=IDS, IDX, IDY, IDZ, IDD in Fig. 2), the route establishment time stamp, and the ith message, respectively H (d) is the hash value resulted from hashing the data d using the hash function. H (). {d}Ks+ is the signature of d with the private key of NS. The purpose of the source node's signature is to ensure the message's authenticity and integrity and secure the payment by enabling TP to ensure that NS has sent i messages. Each intermediate node verifies $\varepsilon_s(i)$ and stores $\varepsilon_s(i)$ and $H(m_i)$ for composing the receipt. It also removes the previous ones $(\varepsilon_s(i-1)$ and $H(m_i-1)$ because $\varepsilon_s(i)$ is enough to prove transmitting i messages. Signing $H(m_i)$ instead of mi can reduce the receipt size because the smaller-size $H(m_i)$ is attached to the receipt instead of mi.

The destination node generates a one-way hash chain by iteratively hashing a random value hS S times to obtain the hash chain {hS, hS-1,…,h1, h0}, where hi-1= H (hi) for 1 ≤ i ≤ S and h0 is called the root of the hash chain. The node signs h0 and R to authenticate the hash chain and link it to the route, and sends the signature to the source node in route establishment phase. In order to acknowledge receiving the message mi, the destination node sends ACK packet containing the preimage of the last released hash chain element or hi. Each intermediate node verifies the hash chain element by making sure that hi-1 is obtained from hashing hi, and saves hi for composing the receipt and removes hi-1. The underlying idea is that $\varepsilon_s(i)$ and hi are undeniable proofs for sending and receiving i messages, respectively.

Each node in the route composes a receipt and submits it when it has a connection to TP to claim the payment and update its trust values. A receipt is the proof for participating in a route and sending, relaying, or receiving a number of messages. A receipt contains R, ts, i, (mi), h0, hi, Cm, and an undeniable cryptographic token for preventing payment manipulation. Cm is data that depends on the used routing protocol, such as the number of messages the intermediate nodes commit to relay. The cryptographic token contains the hash value of the last source node's signature and Auth_Code. Auth_Code is

the authentication code that authenticates the hash chain and the intermediate nodes to hold them accountable for breaking the route. If I messages are delivered, the format of the receipt is <R, ts, i, (mi), h0, hi, Cm, H ($\varepsilon_s(i)$, Auth_Code)>, $\varepsilon_s(i)$ and Auth_Code are hashed to reduce the receipt's size.

$$\text{TP} \rightarrow N_K: Cert_K = ID_K, t_e, t_j, K_K-, \tau_K, \{H(ID_K t_e, t_j, t_i, K_K-, \tau_K)\}K_{TP+}, \quad (1)$$

$$\tau_K^{(2)} = 1 - \frac{\text{NO.of sessions broker in the last } \omega \text{ sessions}}{\omega} \quad (2)$$

$$\tau_K^{(1)} = \frac{\text{NO.of packets that are relayed in the last } \omega \text{ sessions}}{\text{Total No.of incomin packets the last } \omega \text{ sessions}} \quad (3)$$

$$\tau_K^{(3)} = \frac{\text{NO.of sessions that } N_K \text{relayed at least } \delta \text{ packets}}{\omega} \quad (4)$$

$$\tau_K^{(4)} = \frac{\text{NO.of swssions } N_K \text{participated in the period t}}{M} \quad (5)$$

C. Route Establishment Phase

In this phase two methods utilized called the Load balanced shortest reliable route (LB-SRR) and the load balanced best available route (LB-BAR). LB-SRR establishes the shortest route that can satisfy the source node's trust, energy, and route-length requirements, but the destination node selects the best route in the LB-BAR protocol. The routing protocols have three processes: 1) route request packet (RREQ) delivery; 2) Route selection; and 3) route reply packet (RREP) delivery.

LB-SRR: To establish a route to the destination node ND, the source node NS broadcasts RREQ packet and waits for RREP packet. The source node embeds its requirements in the RREQ packet, and the nodes that can satisfy these requirements broadcast the packet. The destination node establishes the shortest route that can satisfy the source node's requirements. The rationale of the LB-SRR protocol is that the node that satisfies the source node's requirements is trusted enough to act as a relay. The protocol is useful to establish a route that avoids the low-trusted nodes as well as achieve the load balancing.

IV. SIMULATION RESULTS

In this area, we display the present outcomes utilizing the network simulator NS2. We evaluated the methods using the ns-2.34 version. The network parameters and techniques represented in table 1. The proposed RNCDM method is compared with two state-of-art methods in this section such as OPS [19] and NCMD [19].

Table 1: Network Simulation Parameters

Network Area	1000 x 1000
Type of Network	WBAN
Number of Nodes	50-350
Velocity	1.5 m/s
MAC	802.11
Simulation Time	30sec
Initial Energy	0.5 J
Transmitter energy consumption	16.7 nJ
Receiver energy consumption	36.1 nJ

There are five performance metrics evaluated in this paper such as:

- Energy Consumption vs. Number of WBANs
- Data Dissemination delay vs. Number of WBANs
- Network Throughput vs. Number of WBANs
- PDR vs. Number of WBANs
- Number of packet drops vs. Number of WBANs

Table 2: Average throughput performance evaluation

WBANs	OPS	NCMD	RNCMD
50	250	260	270
100	253	262	271
150	261	275	293
200	272	285	300
250	288	303	321
300	305	316	327
350	311	327	342

Table 3: PDR performance evaluation

WBANs	OPS	NCMD	RNCMD
50	67.5	70	73
100	68	71	74
150	72.5	75	78
200	76	79	82
250	79	82	85
300	83	86	88
350	85	88	91

As showing in the performance of throughput and PDR, the proposed RNCDM technique improves the performance due to the effective strategies designed for the optimum opportunistic routing. The RNCDM is based on NCDM technique.

Table 4: Average energy consumption performance evaluation

WBANs	OPS	NCMD	RNCMD
50	0.072	0.079	0.095
100	0.075	0.08	0.097
150	0.081	0.09	0.102
200	0.1	0.109	0.122
250	0.12	0.129	0.142
300	0.142	0.15	0.163
350	0.163	0.17	0.19

Table 5: Number of packets drop performance evaluation

WBANs	OPS	NCMD	RNCMD
50	590	540	490
100	575	525	475
150	500	450	400
200	425	375	325
250	375	325	275
300	310	260	210
350	260	260	160

Table 6: Data dissemination delay performance evaluation

WBANs	OPS	NCMD	RNCMD
50	1.79	1.7	1.62
100	1.35	1.3	1.23
150	0.8	0.79	0.78
200	0.48	0.46	0.44
250	0.39	0.38	0.38
300	0.28	0.25	0.22
350	0.18	0.17	0.16

Similarly, the delay and average energy consumption performance is optimized using the proposed solution for the varying WBANs. The throughput and PDR performances are increasing with increased number of WBANs.

V. CONCLUSION AND FUTURE WORK

In this research, we proposed the network management cost reduction approach for the opportunistic WBANs in order to manage the increased cost of network management. We first designed the joint distributed network management cost reduction algorithm and energy-efficient algorithm for the dynamic data dissemination process in the opportunistic WBANs. Then we introduced pricing based data transmission for the reliable and stable route selection. The simulation results prove that proposed solution outperforms the existing routing protocols for WBANs. For future work, it will be interesting to investigate the variations in other important parameters of WBAN such as mobility speed, packet rate etc.

REFERENCES

[1] Benoit Latre, Bart Braem, Ingrid Moerman, Chris Blondia & Piet Demeester 2011, „A Survey on Wireless Body Area Networks", Journal of Wireless Networks, vol. 17, no. 1, pp. 1-18.

[2] Kyung Sup Kwak, Sana Ullah & Niamat Ullah 2010, "An Overview of IEEE 802.15.6 Standard", 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), 7-10 Nov. 2010 Rome, Italy, pp. 1-6.

[3] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung, "Body Area Networks: A Survey," Journal of Mobile Networks and Applications, vol. 16, no. 2, pp. 171–193, 2011.

[4] S. Moulik, S. Misra, and A. Gaurav, "Cost-Effective Mapping Between Wireless Body Area Networks and Cloud Service Providers Based on Multi-Stage Bargaining," IEEE Transactions on Mobile Computing, vol. PP, no. 99, pp. 1–1, 2016.

[5] K. M. S. Thotahewa, J. Y. Khan, and M. R. Yuce, "Power Efficient Ultra Wide Band Based Wireless Body Area Networks with Narrowband Feedback Path," IEEE Transactions on Mobile Computing, vol. 13, no. 8, pp. 1829–1842, 2014.

[6] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, "A Comprehensive Survey of Wireless Body Area Networks," Journal of Medical Systems, vol. 36, no. 3, pp. 1065–1094, 2012.

[7] "IEEE Standard for Local and Metropolitan Area Networks - Part 15.6: Wireless Body Area Networks," IEEE Std 802.15.6-2012, pp. 1–271, 2012

[8] A. Samanta, S. Bera, and S. Misra, "Link-Quality-Aware Resource Allocation With Load Balance in Wireless Body Area Networks," IEEE Systems Journal (DOI: 10.1109/JSYST.2015.2458586), vol. PP, no. 99, pp. 1–8, 2015.

[9] Samanta, S. Misra, and M. S. Obaidat, "Wireless Body Area Networks with Varying Traffic in Epidemic Medical Emergency Situation," in Proceedings of IEEE International Conference on Commumications, 2015.

[10] J. Elias, "Optimal Design of Energy-efficient and Cost-effective Wireless Body Area Networks," Ad Hoc Networks (Elsevier), vol. 13, pp. 560–574, 2014.

[11] M. Zhao, D. Gong, and Y. Yang, "Network Cost Minimization for Mobile Data Gathering in Wireless Sensor Networks," IEEE Transactions on Communications, vol. PP, no. 99, pp. 1–1, 2015.

[12] S. Yousaf, N. Javaid, Z. A. Khan, U. Qasim, M. Imran, and M. Iftikhar, "Incremental Relay Based Cooperative Communication in Wireless Body Area Networks," Procedia Computer Science, vol. 52, pp. 552–559, 2015.

[13] F. D. Andreagiovanni and A. Nardin, "Towards the Fast and Robust Optimal Design of Wireless Body Area Networks," Applied Soft Computing, vol. 37, pp. 971–982, 2015.

[14] S. Huang and J. Cai, "Priority-Aware Scheduling for Coexisting Wireless Body Area Networks," in Proceedings of International Conference on Wireless Communications Signal Processing, 2015, pp. 1–5.

[15] Ibarra, A. Antonopoulos, E. Kartsakli, J. Rodrigues, and C. Verikoukis, "QoS-Aware Energy Management in Body Sensor Nodes Powered by Human Energy Harvesting," IEEE Sensors Journal, vol. 16, no. 2, pp. 542–549, 2016.

[16] A. Seyedi and B. Sikdar, "Energy Efficient Transmission Strategies for Body Sensor Networks with Energy Harvesting," IEEE Transactions on Communications, vol. 58, no. 7, pp. 2116–2126, 2010.

[17] ——, "Modeling and Analysis of Energy Harvesting Nodes in Body Sensor Networks," in Proceedings of International Summer School and Symposium on Medical Devices and Biosensors, 2008, pp. 175–178.

[18] Z. Ren, X. Qi, G. Zhou, H. Wang, and D. Nguyen, "Throughput Assurance for Multiple Body Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. PP, no. 99, pp. 1–1, 2015

[19] Amit Samanta, Student Member, IEEE, Sudip Misra, "Energy-Efficient and Distributed Network Management Cost Minimization in Opportunistic Wireless Body Area Networks", IEEE Transactions on Mobile Computing, 2017