Energy Efficient Aggregation and Reliable Communication for Wireless Body Area Networks (WBAN)

Venkatasubramanian Sivaprasatham[1], Dr. Jothi venkateswaran[2], Dr. Hafidh Taher Ba Omar[3]

[1]Nizwa College of Technology, Nizwa, Sultanate of Oman.
venkatasubramanianphd@gmail.com
[2]HoD, Department of Computer Sciece,
Presidency College, Chennai, TamilNadu, India
[3]Dean, Nizwa College of Technology,
Nizwa, Sultanate of Oman.

***Abstract*- In wireless body area networks (WBAN), the data loss, security and reliability requirements are not handled in the existing literature works. This necessitates the technique that deals with slot allocation scheme, delay and other performance metrics. In order to overcome this issue, in this paper, we propose an energy efficient aggregation and reliable communication for Wireless Body Area Networks (WBAN). Initially, the aggregator nodes are chosen based on the nodes connectivity. During the data aggregation, the encryption key and the verification key is assigned to the nodes while transmitting data to the data aggregator. In order to enhance the reliability of data during transmission, the network coding methodology is considered. By simulation results, we show that the proposed technique enhances the network performance.**

I. INTRODUCTION

A. Wireless Body Area Network (WBAN)

Wireless Body Area Network (WBAN) is an application of wireless sensor network (WSN). In Wireless Body Area Network (WBAN) a number of small sensors are placed in, on and around human body to measure specific physiological parameters of a person and send it to monitoring medical centre or hospital via intermediary devices (like PDAs, Cellular Phones) by wireless communication channel [1], [2]. Normally WBAN is combination of in-body and on-body area networks. An in-body area network allows communication between invasive/implanted devices and a base station. An on-body area network, allows communication between non-invasive/wearable devices and a base station [3].

B. Application of WBAN

There are two types of applications of WBAN, which are Medical [4] and Non- Medical [5]. In medical application, WBAN is used for personal health assistance [6], remote health monitoring for patient [3]. In non-medical application, WBAN is used for various kinds of applications, like gaming, entertainment, lifestyle, medical, health and fitness and intelligent personalization [5].

C. Attacks on WBAN

There are number of key attacks in WBAN which are conducted in different ways, i.e., Denial of Service (DoS) attacks, privacy violation, and physical attacks [11]. Attacks on WBAN can be classified into three main categories: (a) attacks on secrecy and authentication, where an adversary performs eavesdropping, packet replay attacks, or spoofing of packets, (b) attacks on service integrity, where the network is forced to accept false information, and (c) attacks on network availability (DoS attacks), where the attacker tries to reduce the network's capacity. Some attacks are described below [12].

1) Physical Layer Attacks: The main responsibilities of physical layer include frequency selection and generation, signal detection, modulation, and encryption and the medium is radio-based, jamming the network is always possible. The most common attacks are jamming and tampering. Jamming refers to interference with the radio frequencies of the nodes. Nodes in WBAN are deployed in close proximity to the human body, and this reduces the chances of physical tampering [12]

2) Data Link Layer Attacks: Data Link Layer is responsible for multiplexing, frame detection, channel access, and reliability. Attacks on this layer are creating collision, unfairness in allocation, and resource exhaustion. When two or more nodes attempt to transmit at the same time then collision occurs. Unfairness degrades the network performance by interrupting the MAC priority schemes. Exhaustion of battery resources may occur when a self-sacrificing node always keeps the channel busy [12].

3) Network Layer Attacks: In network layer, possible attacks are spoofing, selective forwarding, Sybil, and hello flood. In spoofing, the attacker targets the routing information and alters it to disrupt the network. In selective forwarding, the attacker forwards selective messages and drops the others. In Sybil, the attacker represents more than one identity in the network. The hello flood attacks are used to fool the network [12].

4) Transport Layer Attacks: The transport layers are flooding and de-synchronization. The attacker repeatedly places requests for connection until the required resources are exhausted or reach a maximum limit in flooding. In de-synchronization, the attacker forges the messages between nodes causing them to request the transmission of missing frames [12].

D. Need for Reliable and Secure communication in WBAN

When WBAN is used as health purpose, the collected data is health information which is personal information. It is critical and in the interest of the individual, this information must be safe and not being accessed by unauthorized entities. Non reliable or insecure communication may highly affect health assistance of patient, so the communication must be reliable and secure in wireless body area network (WBAN) [7]. Reliable and Secure communication is also necessary for another application of WBAN.

E. Issues of Secure and Reliable communication in WBAN

There are some issues of Secure and Reliable communication in wireless body area network (WBAN) which are describe below:

1) Data Confidentiality: WBAN Applications need secure data transfer mechanisms, since an opponent can eavesdrop on the traffic and access receptive information of the user.

2) Data Authentication: It is required that only legal nodes of the WBAN are able to participate in the network. Data Authentication ensures the reliability of the received message. Data Authentication allows a receiver to verify that the data really was sent by the claimed sender or from a legal node

3) Data Integrity: When data is transmitted from an authorized sender, an adversary can intentionally modify the message. Due to bad physical conditions of the wireless channel data can also get corrupted.

4) Data Freshness: Data freshness implies that the data received is recent, and it ensures that no adversary replayed old messages in network.

5) Location privacy: Since the nodes in WBAN are worn over the human body the communication between the nodes can help in uniquely identifying a person. So WBAN applications are bound to have inherent Location privacy risks.

6) Contextual privacy: In the breach of contextual privacy, an adversary will be able to co-relate the source and destination, and get the context sensitive information.

7) Access Control: Different users can send and retrieve information to and from WBAN network. It is important to protect private information from unauthorized (may be even for legitimate) parties.

8) Non-repudiation: Repudiation is a threat caused when the sender or receiver denies the responsibility of sending or receiving the messages. So repudiation must be avoided [5].

F. Problem Identification

In the literature review, some of the latest and standard paper are discussed in which, it is found that in [1] there is a problem with data lost, in [2] it need some security features, in [8] it need to be discussed different reliability requirements, in [9] It should be include the design of a stochastic slot allocation scheme, in [10] the delay of signal should be discussed, and overall many performance metrics are not discussed.

Hence in this paper, we propose an energy efficient aggregation and reliable communication for wireless body area networks.

II. LITERATURE REVIEW

A. A Security Suite for Wireless Body Area Networks [1]

In this work, the author addressed data security problem and presented two key management schemes focusing on the independent generation of keys at the sender and the receiver. In this key generation and management schemes, the author removes the need for key exchanges by using mechanisms that enable the sender and the receiver to generate the keys at their end. This ensures that the vulnerability of the communication at the security association phase does not apply when such a system is used. Since only the authorized sender or receiver will have access to the immediately previous medical data (which form the reference frames in case of IAMKeys) and to the periodically refreshed reference frames (in case of KEMESIS), it will be hard for any adversary to make any sense of the sniffed packets. Security increases with updates to the reference frames. The complexity is further improved by changing the encryption keys for each data frame. This ensures that the data frame remains secure under many given circumstances. The performance Metrecs used are overhead; which is reduced and security; which is increased. The author focus on data freshness with removing the need for retransmission of a lost frame, only when more than ten frames are lost or not acknowledged, the sender or the receiver will flag an error, which is not good for emergency medical assistance, because if any data is lost in emergency then it is not good for patient. Optimization of resource utilization is not achieved here.

B. Improving the Reliability of Wireless Body Area Networks [2]

The problem of reliability of wireless body area network is addressed and a highly reliable wireless body area network (WBAN) is proposed. These networks improve upon current WBANs by taking advantage of a new technology, which is Cooperative Network Coding (CNC). Cooperative Network Coding combined with multiple-input multiple- output cooperative techniques at the sinks to achieve high throughput and avoid single points of failure compared to extant wireless body area technologies. The metrics used are Throughput; which is increased, Reliability; which is increased and Latency; which is reduced. The reliability is achieved by author but security is not discussed. Hence, it needs to be added some security feature for secure communication. There is also a problem of interference between signals.

C. An Adaptive Fault-Tolerant Communication Scheme for Body Sensor Networks [8]

The author addressed the problem of reliable data transmission in wireless body sensor network. An adaptive and flexible fault-tolerant communication scheme for BSNs, namely AFTCS, is proposed that adopts a channel bandwidth reservation strategy to provide reliable data transmission when channel impairments occur. For reliability requirements of critical sensors, fault-tolerant priority and queue are employed to adaptively adjust the channel bandwidth allocation. Metrics used are, average transmission latency; which is shorting and packet loss rates; which are lowering. The author discussed that physiological data may have different reliability requirements but do not discuss the method for achieving this.

D. An Emergency Handling Scheme for Superframe-structured MAC protocols in WBAN [9]

Researchers addressed the problem related to immediate and reliable data transmission during an emergency situation. The author proposed an emergency handling scheme for WBAN applications using two mechanisms MP and EP. This scheme can handle emergent data and additional data transmission with low latency. It can be applied to general superframe-structured MAC protocols. The metrics discussed are latency; which is lowering, efficiency and overhead. It should be include the design of a stochastic slot allocation scheme for efficient slot utilization.

E. Energy-aware Topology Design for Wireless Body Area Networks [10]

The topology design problem for wireless body area networks is addressed here. The author proposed a novel and effective model based on mathematical programming that determines the optimal number and placement of relay nodes, the optimal assignment of sensors to relays, as well as the optimal traffic routing, taking accurate account of both the total network cost and energy consumption. The performance metrics used are total energy consumption; which is reduced and network installation cost; which is also reduced. The author worked on energy efficiency but not discussed about the delay of the signal and other performance metric.

III. PROPOSED SOLUTION

A. Overview

In this paper, we propose an energy efficient aggregation and reliable communication for wireless body area networks. Initially, the aggregator nodes are chosen based on the nodes connectivity. During the data aggregation, the encryption key and the verification key is assigned to the nodes while transmitting data to the data aggregator. In order to enhance the reliability of data during transmission, the network coding methodology is considered. During emergency situation that requires immediate and reliable data transmission, crisis management technique is deployed.

B. Energy Efficient Aggregation and Reliable Communication

Our proposed technique mainly concentrates on reliable and energy efficient data aggregation and transmission. It includes following two phases

Phase 1: Secured Data Aggregation

Phase 2: Network Coding

1) Secured Data Aggregation: Fig. 1 demonstrates the proposed architecture of clustered network. C_1 and C_2 represent clusters and CH_1 and CH_2 represents the cluster heads respectively. These cluster heads acts as the aggregator nodes for collecting the information from the sensor nodes and transmitting it to the Base Station (BS).

The clustering process is described below.

The sensor nodes perform the cluster head selection based on the nodes connectivity. The nodes containing the higher connectivity when compared with its 2-hop neighbors are initially chosen as CH_i. The selected cluster heads then broadcast an advertisement message to all its surrounding nodes. The advertisement message includes the cluster-head ID and location information of the cluster head. The non cluster head nodes first record all the information from cluster heads within their communication range.

Each non-cluster head node chooses one of the strongest Received Signal Strength (RSS) of the advertisement as its cluster head and transmits a member message back to the chosen cluster head. The information about the node's capability of being a cooperative node, i.e., its current energy status is added into the message. The message also includes information related to consistency value, consistent sensing count and inconsistent sensing count of the node.

If an advertisement message signal is obtained at a CH_i from another cluster head CH_j, which has the RSS value greater than a threshold then CH_j will be considered as the neighbor cluster head and the ID of j is stored.

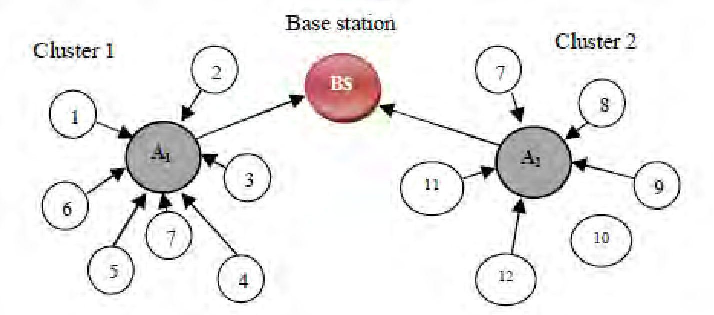

Fig 1 Proposed Architecture

Following the clustering process, the data to be transmitted are injected into encryption phase to improve secured transmission. This is illustrated below

Let N_i represent the sensor network

Let D_i represent the data

Let $Kenc_i$ represent the encryption key

Let $Kver_i$ represent the verification key

Let A_i represent the aggregator node

The steps involved in the encryption of data are as follows

1) Initially N_i is assigned with a one-way hash function y, and proof key $Kver_i$. A_i is assigned with one-way hash function z and aggregator verification keys $Kver_i \oplus Kver_{i+1} \forall$ i. BS stores both hash function of node and aggregator i.e. both y and z and all the verification key Kver for all i.

2) When N_i wants to transmit D_i to A_i, it randomly generates the $Kenc_i$ and encrypts the data with $Kenc_i$, y and $Kver_i$. The encrypted data ($E_i(D_i)$) is represented using the following equation.

$$E_i (D_i) = D_i \oplus y (Kenc_i) \oplus Kenc_i \,||\, Kenc_i \oplus Kver_i \qquad (1)$$

where || indicates data concatenation.

3) Ni then transmits $E_i (D_i)$ to AGG

$$N_i \xrightarrow{E_i(D_i)} A_i \qquad (2)$$

4) In case, A_i wants to transmit the data to BS, it encrypts the data with its verification key $Kver_c \oplus Kver_{c+1} \forall$ c and sends it to BS.

5) BS decrypts the data with the hash function y and z and the respective verification key.

The redundant data packets among n incoming encrypted packets in the A_i can be determined using the following steps

1) Two encrypted data D_i and D_j from the nodes N_i and N_j are transmitted to A_i is shown in Eq. (3) and (4)

$$E_i (D_i) = D_i \oplus y (Kenc_i) \oplus Kenc_i \,||\, Kenc_i \oplus Kver_i \qquad (3)$$

$$E_j (D_j) = D_j \oplus y (Kenc_j) \oplus Kenc_j \,||\, Kenc_j \oplus Kver_j \qquad (4)$$

2) A_i XORs the first parts of these two cipher texts which is shown using Eq. (5)

$$D_i \oplus y (Kenc_i) \oplus Kenc_i \oplus D_j \oplus y (Kenc_j) \oplus Kenc_j \qquad (5)$$

3) As A_i is already assigned with $Kver_i \oplus Kver_{i+1} \forall$ i, the aggregator XORs the last parts of Eq (3) and (4).

$$Kenc_i \oplus Kver_i \oplus Kenc_j \oplus Kver_j \oplus Kver_i \oplus Kver_j \qquad (6)$$

$$= Kenc_i \oplus Kenc_j \qquad (7)$$

A_i can use E_i (D_i) and E_j (D_j) to retrieve $Kenc_i \oplus Kenc_j$, however $Kenc_i$ or $Kenc_j$ cannot be retrieved individually. Hence A_i will not be able to decrypt E_i (D_i) and E_j (D_j).

4) To differentiate whether the encrypted data packets are redundant in the plain text format, a test value ψ is estimated by XORing Eq (6) and (7)

$$\psi_{(i,j)} = D_i \oplus y (Kenc_i) \oplus Kenc_i \oplus D_j \oplus y (Kenc_j) \oplus Kenc_j \oplus (Kenc_i) \oplus (Kenc_j) \oplus D_i(Kenc_i \oplus Kenc_j \qquad (8)$$

$\psi_{(i,j)}$ is further reduced to following Eq format

$$\psi_{(i,j)} = D_i \oplus D_j \qquad (9)$$

5) If $D_i = D_j$,

Then

$\psi_{(i,j)} = D_i \oplus D_j = 0$ and vice versa

End if

The above condition is generalized using the following Eq (10)

$$\text{If } \begin{cases} \psi_{(i,j)} = 0, then\, D_i = D_j \\ \psi_{(i,j)} \neq 0, otherwise \end{cases} \qquad (10)$$

6) If two data packets arriving at A_i is same, then A_i just transmits either E_i (D_i) or E_j (D_j) to BS

7) If two data packets arriving at A_i are different, then A_i transmits $E_i (D_i) || E_j (D_j)$ to BS.

8) When A_i receives n data packets, then first the data are paired. i.e. (E_i, E_j) $\forall$ i. This step is repeated to generate ψ .

9) The generated ψ is used to check if E_i has the same reading as E_j.

10) If $\psi_{(1,2)}\psi_{(2,3)} = ... = \psi_{(n-1,n)}$,

Then

E_1, E_2 ….. E_n has the same reading.

End if

3.2.2 Network Coding: In order to enhance the reliability of data during transmission, we consider the network coding methodology. Initially, the data packets to be transmitted are formatted into a blend packet which is obtained using the following Eq (11)

Let S and D be the source and the destination, respectively.

A blend of data packet is obtained by multiplying each of the (e) original packets with a random co-efficient and then the results are summed:

$$\mathrm{v_i} = \sum_{o=1}^{e} \lambda_{io} u_o \, , i = 1,2,....,e' \qquad (11)$$

where $\mathrm{v_i}$ = coded packets

$\mathrm{u_o}$ = original packets

e' ($\geq$e) = number of combination packets

λ_{io} = randomly chosen from a Galois Field GF (2^q)

GF (2^q) elements = {0, 1, 2, …., 2^q-1)

The random coefficients { λ_{io} } are set in the header of the data packets.

The steps involved in network coding are as follows:

1) When S wants to transmit data packets to D, first it transmits the data to its aggregator node (A_1).
2) A_1 generates the blend packet using Eq. (11) and transmits it towards the nodes in C_2.
3) The nodes in C_2 generate a blend packet from the received packets and transmit it towards the subsequent cluster (i.e. third cluster C_3).
4) Nodes in C_3 receive the combination packets and transmit new combination packets.

The following equation illustrates the method using which N_j in the cluster generates and transmits to nodes in cluster i+1 blend packets from the received blend packets as follows.

$$\mathrm{v_{ij}} = \sum_{o=1}^{e_j} \lambda_{ijo} v_{i-1,o} \, , j = 1,2,....,n_i \qquad (12)$$

where $\mathrm{v_{ij}}$ = transmitted blend packets

$v_{i-1,o}$ = received blend packets

$\mathrm{n_i}$ = number of nodes in cluster i

ej = number of blend packets received by N_j in C1 from the nodes in cluster i-1

λ_{ijo} = randomly chosen from GF (2^q).

Each node in a cluster needs to transmit at least smallest integer greater than or equal to the ratio of the number of original packets (e) and the number of nodes per cluster (n).

5) D receives at least e linearly independent blend packets from nodes in cluster K to be able to recover the original information.

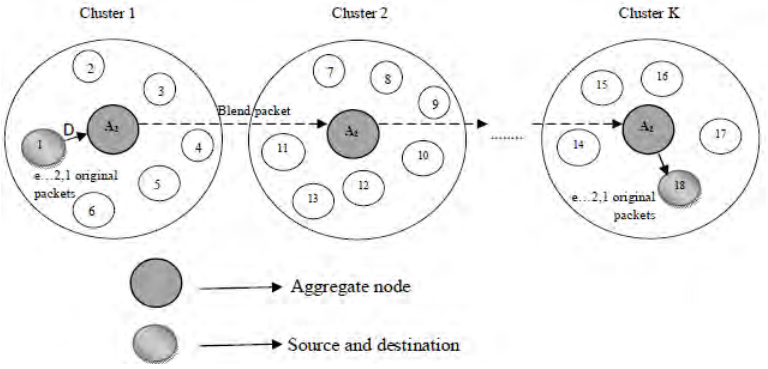

Fig 2 Network Coding

IV Simulation Results

A. Simulation Parameters

To simulate the proposed Energy Efficient Aggregation and Reliable communication (EEARC) NS2 [15] is used. A network area of 50 X 50 m is considered. The IEEE 802.15.4 is used as the MAC layer since it provides reliable communication for the devices. For all types of communications, it provides access to the physical channel. It also supports security features. IEEE 802.15.4 specification uses physical layer (PHY) options based on Direct Sequence Spread Spectrum (DSSS) which uses the frame structure for low-duty-cycle low-power operation containing a 32-bit preamble frame length.

TABLE 3. Simulation Parameters

Total Nodes	60
Area Size	50 X 50
MAC protocol	IEEE 802.15.4
Simulation Time	25 sec
Transmission Range	250m
Routing Protocol	EEARC
Traffic Source	CBR,poisson
Packet Size	512
No. of Keys	50,100,150,200 and 250Kb.
Simulation Time	50 sec.

B.. Performance Metrics

IASCMT scheme is mainly considered for performance comparison. The performance is evaluated based on the following metrics; the Average end-to-end delay, the Average Packet Delivery ratio and the packet drop.

Case 1: (CBR)

1) Based on Rate: In our first experiment, we vary the rate as 50,100,150,200 and 250Kb.

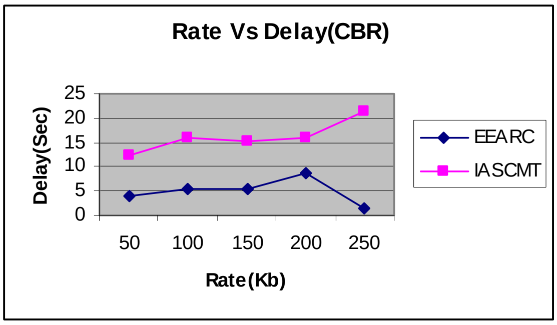

Fig 3: Rate Vs Delay

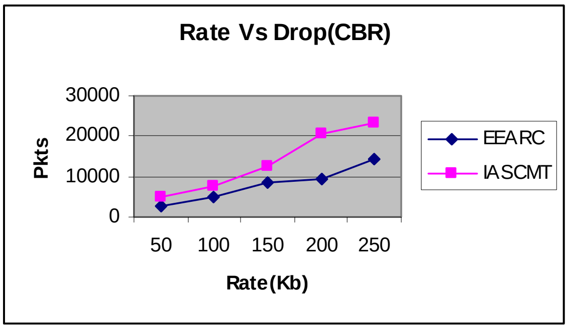

Fig 4: Rate Vs Drop

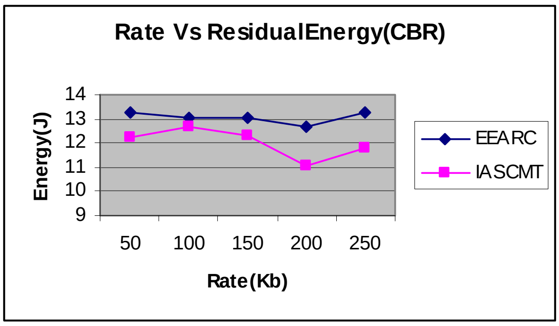

Fig 5: Rate Vs Residual Energy

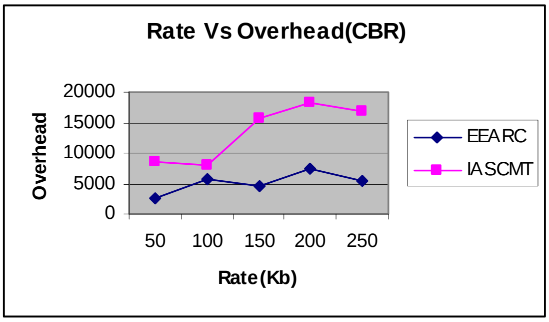

Fig 6: Rate Vs Overhead

Figure 3 shows the delay of EEARC and IASCMT techniques for different rate scenario. We can conclude that the delay of our proposed EEARC approach is 67% less than IASCMT approach.

Figure 4 shows the drop of EEARC and IASCMT techniques for different rate scenario. We can conclude that the drop of our proposed EEARC approach is 41% less than IASCMT approach.

Figure 5 shows the residual energy of EEARC and IASCMT techniques for different rate scenario. We can conclude that the residual energy of our proposed EEARC approach is 8% higher than IASCMT approach.

Figure 6 shows the overhead of EEARC and IASCMT techniques for different rate scenario. We can conclude that the overhead of our proposed EEARC approach is 59% less than IASCMT approach.

Case 2: (Poisson)

1) Based on Rate: In this experiment, we vary the rate as 50,100,150,200 and 250Kb.

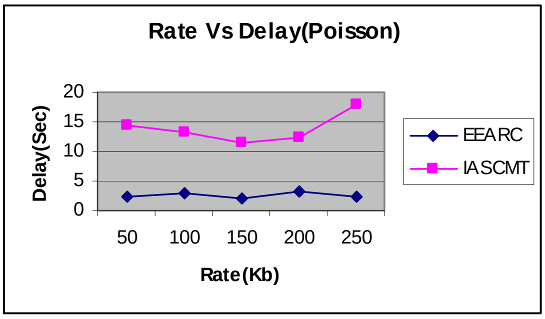

Fig 7: Rate Vs Delay

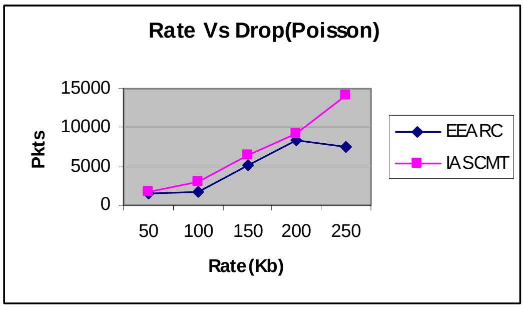

Fig 8: Rate Vs Drop

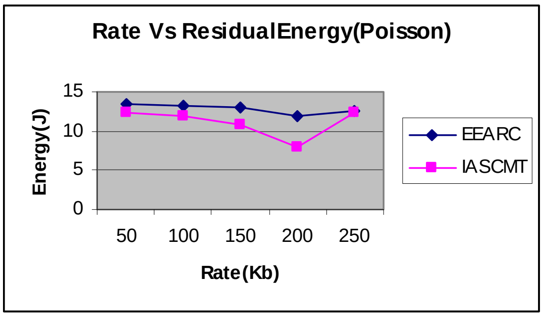

Fig 9: Rate Vs Residual Energy

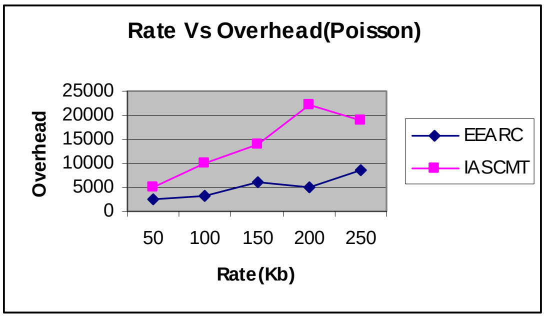

Fig 10: Rate Vs Overhead

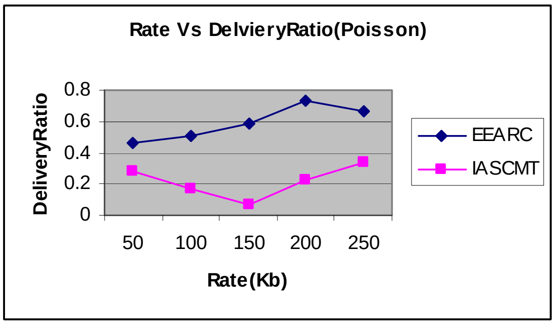

Fig 11: Rate Vs Delivery Ratio

Figure 7 shows the delay of EEARC and IASCMT techniques for different rate scenario. We can conclude that the delay of our proposed EEARC approach is 81% less than IASCMT approach.

Figure 8 shows the drop of EEARC and IASCMT techniques for different rate scenario. We can conclude that the drop of our proposed EEARC approach is 25% less than IASCMT approach.

Figure 9 shows the residual energy of EEARC and IASCMT techniques for different rate scenario. We can conclude that the residual energy of our proposed EEARC approach is 14% higher than IASCMT approach.

Figure 10 shows the overhead of EEARC and IASCMT techniques for different rate scenario. We can conclude that the overhead of our proposed EEARC approach is 61% less than IASCMT approach.

Figure 11 shows the delivery ratio of EEARC and IASCMT techniques for different rate scenario. We can conclude that the delivery ratio of our proposed EEARC approach is 62% higher than IASCMT approach.

V. Conclusion

In this paper, we have proposed an energy efficient aggregation and reliable communication for wireless body area networks. Initially, the aggregator nodes are chosen based on the nodes connectivity. During the data aggregation, the encryption key and the verification key is assigned to the nodes while transmitting the data to the data aggregator. In order to enhance the reliability of data during transmission, the network coding methodology is considered. By simulation results, we have shown that the proposed technique enhances the network performance.

References

[1] Raghav V. Sampangi, Saurabh Dey, Shalini R. Urs and Srinivas Sampalli, "*A SECURITY SUITE FOR WIRELESS BODY AREA NETWORKS*", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012.

[2] Gabriel E. Arrobo and Richard D. Gitlin, "*Improving the Reliability of Wireless Body Area Networks*", 33rd Annual International Conference of the IEEE EMBS Boston, Massachusetts USA, August 30 - September 3, 2011.

[3] Shahnaz Saleem, Sana Ullah and Kyung Sup Kwak, "*A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks*", *Sensors* 2011, *11*, 1383-1395; doi: 10.3390/s110201383.

[4] Jamil. Y. Khan and Mehmat R. Yuce, "*Wireless Body Area Network (WBAN) for Medical Applications*". Domenico Campolo, ISBN 978-953-7619-57-2, published: January 1, 2010 under CC BY-NC-SA 3.0 license.

[5] Ashok Kelur, Anantha Kamath, Neghu Cui and Vishnuvardhan Avula, "*Security and privacy for WBAN Applications*".

[6] Javed Ahmad and Fareeha Zafar, "*Review of Body Area Network Technology & Wireless Medical Monitoring*", International Journal of Information and Communication Technology Research, ISSN 2223-4985 /Volume 2 No. 2, February 2012.

[7] Pervez Khan, Md.Asdaque Hussain and Kyung Sup Kwak, "*Medical Applications of Wireless Body Area Networks*", International Journal of Digital Content Technology and its Applications Volume 3, Number 3, September 2009.

[8] Guowei Wu, Jiankang Ren, Feng Xia and Zichuan Xu, " *An Adaptive Fault-Tolerant Communication Scheme for Body Sensor Networks*", *Sensors* 2010, *10*, 9590-9608; doi:10.3390/s101109590,*28 October 2010.*

[9] BeomSeok Kim, Jinsung Cho, Jongbum Ryou and Ben Lee, "*An Emergency Handling Scheme for Superframe-structured MAC protocols in WBAN*", *ICUIMC'11*, February 21–23, 2011, Seoul, Korea.

[10] Jocelyne Elias and Ahmed Mehaoua, "*Energy-aware Topology Design for Wireless Body Area Networks*", IEEE ICC 2012 - Selected Areas in Communications Symposium.

[11] M. Somasundaram and R. Sivakumar, "*Security in Wireless Body Area Networks: A survey*", 2011 International Conference on Advancements in Information Technology With workshop of ICBMG 2011 IPCSIT vol.20 (2011) © (2011) IACSIT Press, Singapore.

[12] Shahnaz Saleem , Sana Ullah and Kyung Sup Kwak, "*A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks*", *Sensors* 2011, *11*, 1383-1395; doi:10.3390/s110201383.

[13] Shih-I Huang, Shiuhpyng Shieh and J. D. Tygar, "Secure encrypted-data aggregation for wireless sensor networks", National Science Council grants NSC96-3114-P-001-002-Y and NSC96-2219-E-009-013, 7 May, 2009.

[14] Ajay Jangra, Dr. Rajesh Verma and Nitin Goel, "*(ZIA) Zero-Interference Algorithm for Hybrid Wireless Sensor Networks*, ISSN: 2229 - 4333 (Print) | ISSN: 0976 - 8491 (Online) www.ijcst.com IJCST Vol. 2, Issue 1, March 2011.

[15] Network Simulator: http:///www.isi.edu/nsnam/ns