Enhanced BGMM based Lightweight Key Generation and Authentication Method for WBAN

Dharshini S
Vellore Institute of Technology: VIT University
Monicasubashini M (monikanewmail@yahoo.com)
Vellore Institute of Technology: VIT University

Research Article

Keywords: Body Gauss-Markov Mobility model, Lightweight Key Generation, Security, Wireless Body Area Networks

Posted Date: March 31st, 2021

DOI: https://doi.org/10.21203/rs.3.rs-270632/v1

Enhanced BGMM based Lightweight Key Generation and Authentication Method for WBAN

S.Dharshini,Research scholar,Department of ECE,SENSE school,VIT University,Vellore.

dharshini.2016@vitstudent.ac.in

M.Monicasubashini,Associate Professor,Department of E&I ,SENSE school,VIT University,Vellore

monicasubashini.m@vit.ac.in

Abstract: Wireless Body Area Network (WBAN) is one of the best modern inventions that supports medical science significantly. Reliability, Latency, Security and Power consumption are the vital parameters to determine the quality of a WBAN architecture. Security Key Generation and Authentication are the important tasks which impact the vital parameters. A Body Gauss-Markov Mobility model (BGMM) based lightweight key generation and authentication method is introduced in this work to improve the quality of WBAN. Enhanced BGMM, Legacy Key Generator and Idle State Key Manager are the three functional blocks used to construct the proposed system. These new function blocks are introduced in this work to achieve higher throughput, packet delivery ratio and security. The proposed work is also indented to reduce the communication delays and power consumption. Adopting new body sensor nodes and discarding unused or damaged nodes from existing network without affecting other operating nodes is the requirements of modern WBAN as well. The proposed method named as "Enhanced BGMM based Lightweight Key Generation and Authentication method for WBAN" (EBLKGAW) is deigned to manage the network stability during adaptation of new nodes and elimination of existing nodes.

Keywords: Body Gauss-Markov Mobility model, Lightweight Key Generation, Security, Wireless Body Area Networks

1. Introduction

Advancements in communication technology is significantly improved over the last decade. The invention of Internet-of-Things (IoT) enables many tiny electronic devices to communicate with the internet[1]. This cost-effective communication technology reduced the manufacturing cost of many wearable health monitoring devices[2]. The implantable sensor technology is also improved over the time. These wearable and implantable devices are used to monitor several health conditions such as Activities, Breathing, Blood contents, ECG, Heartbeat, Insulin Pump and Temperature. Integration of these health monitoring devices will be a boon used to get the cognitive knowledge about a person's health condition. Connecting wearable and implantable health monitoring devices into a single network is called as Wireless Body Area Network[3].

WBAN has many applications such as Assisted living, Biofeedback, Rehabilitation and Remote Patient Monitoring. Bluetooth, IEEE 802 and Zigbee are some standard protocols used in WBAN. Though these protocols are used to connect over-the-counter wearable devices, a dedicated protocol for WBAN is required to resolve some domain specific chores. Data consistency, Data Management, Interference, Interoperability, Privacy, Sensor Validation and Security are the prime challenges to be considered in the WBAN[4]. After evaluating a vast collection of research works related to WBAN, the latest IEEE 802.15.6. standard is introduced to serve the purpose in a better way. While considering the arrival of new hardware, sensor and communication devices, a constant upgradation to WBAN is required to overcome new security threats.

Wireless body area network devices are battery operated in general. The energy consumption determines the life time of a node. Wearable devices are equipped with rechargeable or replaceable batteries, whereas this facility is not in practice for implantable sensor devices. Since replacing batteries in implantable devices is a complicated process, precise usage of the power source is the vital demand. Applying strong mathematical calculation based key generation procedures for higher security will drain the battery of these devices. Applying low computational complexity security schemes makes sensor nodes vulnerable to intruder attacks[5]. If an intruder triggers a Denial-of-Service (DoS) attack in a compromised sensor node, then that node will utilize maximum power to serve the overload processing and the battery power will be drain much faster. This scenario annihilates the purpose of

applying low computational security schemes[6]. So, they real-time requirement in designing WBAN are power saving and security enhancements. The challenge in WBAN is, while optimizing power usage, security level should be maintained in a decent level as well as while improving security, the power consumption should be kept in control.

2. Existing Methods

There are many attempts carried out by researchers in which most of them are achieved higher security or optimized power consumption. Dual Sink approach using Clustering in Body area network [7], A Novel Framework for Software Defined Wireless body area network [8], Fragmentation in MAC IEEE 801.15.4 to improve Delay Performance in wireless body area network [9] and An Efficient and Reliable Direct Diffusion Routing Protocol in wireless body area networks [10] are taken here for performance analysis. The methodologies used, merits and their limitations are analyzed in this section to identify the problem statement for a new work.

2.1. Dual Sink approach using Clustering in Body area network (DSCB)

Clustering based on Line-of-Sight (LoS) and Non-Line-of-Sight (NLoS) communications is performed in this work. The concept of two sink nodes is introduced to improve the network stability and node lifetime. In DSCB, one predefined fixed cluster head is allocated and operates as the sink node for member nodes. This cluster head is responsible for data aggregation and communication with the gateway. A forwarder node is selected for each cluster using cost function, Signal-to-Noise Ratio and link quality. This Forwarder node acts as the second sink node to the cluster. DSCB uses a network topology with five different phases, they are Initialization phase, cluster formation phase, Data sensing phase, Forwarder selection phase and Routing and Energy consumption phase. DARE and SIMPLE protocols are compared with the DSCB protocol for performance comparison through simulationsin terms of throughput, end-to-end delay, Energy consumption and Network lifetime. The security is not discussed in this work which is found to be the limitation of DSCB work.

2.2. A Novel Framework for Software Defined Wireless body area network (NFSDW)

NFSDW introduces a new framework for applying Software Defined Network (SDN) in wireless body area network applications. It also enables to use sensors manufactured by different vendors. The application based static nature is converted into dynamic nature while using this network. Node mobility, Traffic priority, Traffic flow are handled in a better way than in the static wireless body area networks. The conceptual framework introduced a Packet Dissemination Model in data, control and application planes. Simple Network Management, Vendor selection independence, Prioritization of data, Enhanced Patient monitoring, Mobility, Accurate Location Tracking, Energy efficiency and security are the advantages of NFSDW method. NFSDW totally depends on Software Defined Radio (SDR) concept and limited to SDN applications. Though the security is improved than some other existing methods, many SDR nodes are vulnerable to intruder attacks due to Over-the-Air (OTA) configuration updates [11][12].

2.3. Fragmentation in MAC IEEE 802.15.4 to Improve Delay Performance in WBAN (FMIDPW)

FMIDPW operates by fragmenting data packet in WBAN environment and decrementing the slot time of MAC IEEE 802.15.4 protocol. FMIDPW works with the 30 Bytes data packet in WBAN to reduce the transmission delay. The default time slot of IEEE 802.15.4 Slotted Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The initial values of Back-off, Back-off Exponent and Contention Window are changed towards optimum values by measuring Back-off time expiration, 1st Clear Channel Assessment (CCA1) and 2ndClear Channel Assessment (CCA2). The data fragmentation method of FMIDPW is performed in MAC IEEE 802.15.4 protocol. Larger data packets are fragmented into several smaller data packets to reduce the MAC and PHY layer payloads. FMIDPW is implemented and validated using OMNeT++ simulator. Standard evaluation metrics such as Throughput, Average Delay and Packet Delivery Ratio are measured for performance analysis. Security and Energy consumption is not discussed in this work which is crucial for Wireless Body Area Network environment. The packet size limitation is also an encumbrance for modern medical data streaming devices [13].

2.4. An Efficient and Reliable Directed Diffusion Routing Protocol in WBAN (ERDDRP)

The main theme of ERDDRP work is to ensure the lower energy consumption in IEEE 802.15.4 protocol. A new Gradient concept is introduced to track records about the direction, rate of data transmission and hop counts. Each node is aware of the nearest neighbors' gradient information along with the shortest path information. ERDDRP work starts with the introduction of a new naming mechanism scheme followed by gradient establishment, probe data transmission and reinforce path determination. Network Simulator 2 is used to evaluate the ERDDRP method. End-to-End delay, Packet loss rate and Energy consumption are measured during the simulation. As per the results, the power consumption of ERDDRP is more optimized than the other existing procedures. Throughput and security are not discussed in this work which are stated as the real-time limitations of this work.

A brief summary about the methodologies used, merits and limitations of these existing systems are tabulated and given below.

Author	**Work**	**Methodology**	**Advantages**	**Limitations**
Zahid Ullah et al.	DSCB: Dual sink approach using clustering in body area network	Dual Sink Node	Increased Throughput and network lifetime	Low Security
K. Hasan et al.	A Novel Framework for Software Defined Wireless Body Area Network	Software Defined Network - Packet Dissemination	Vendor selection independency	Low Security
Wan Aida Nadia Wan Abdullah et al.	Fragmentation in MAC IEEE 802.15.4 to Improve Delay Performance in Wireless Body Area Network (WBAN)	Packet fragmentation and Clear Channel Assessment	Reduced communicatio n delays	High Energy consumption
J. Mu et al.	An Efficient and Reliable Directed Diffusion Routing Protocol in Wireless Body Area Networks	Gradient concept path determination	Low Energy conception	Low throughput and security

Table 1: Existing methods' advantages and limitations

3. Related Works

The proposed system uses some of the fundamental functionalities of Random Gaussian Markov Mobility model (RGMM), Body Gauss-Markov based Mobility Model (BGMM)[14]and Biometric based Cryptographic Key Generation (BCKG)[15]. Therefore, mandatory elements of these related works are explained here in this section.

3.1. Random Gaussian Markov Mobility model(RGMM)

Random Gaussian Markov Mobility model is used to calculate the speed and direction of a randomly moving particle or node. The velocity of a node at n^{th} instance can be predicted using $(n-1)^{th}$ instance by RGMM. The formula to calculate the velocity is given below in Equation 1.

$$v_n = \alpha v_{n-1} + (1-\alpha)\mu + \sigma\left(\sqrt{1-\alpha^2}\right)w_{n-1} \quad \text{Equation (1)}$$

Where the memory level α gets the value $0 < \alpha < 1$, μ is the velocity mean, σ is the standard deviation and w_{n-1} is the uncorrelated Gaussian process at n^{th} instance.

The speed is calculated using equation 2 and the direction is determined as on equation 3 – given below

$$|v_n| = \alpha|v_{n-1}| + (1-\alpha)\mu_v + \sigma_{|v|}\left(\sqrt{1-\alpha^2}\right)w_{|v_{n-1}|} \quad \text{Equation (2)}$$

$$\theta_n = \alpha\theta_{n-1} + (1-\alpha)\mu_\theta + \sigma_\theta\left(\sqrt{1-\alpha^2}\right)w_{\theta_{n-1}} \quad \text{Equation (3)}$$

Where $w_{|v_{n-1}|}$ is the uncorrelated Gaussian process which is independent of $|v_{n-1}|$ and $w_{\theta_{n-1}}$ is uncorrelated Gaussian process which is independent of θ_{n-1}.

The position of a node is calculated using Equations 4 and 5.

$$x_n = x_{n-1} + |v_{n-1}| \cos \theta_{n-1} \quad \text{Equation (4)}$$

$$y_n = y_{n-1} + |v_{n-1}| \sin \theta_{n-1} \quad \text{Equation (5)}$$

3.2. Body Gauss-Markov based Mobility model (BGMM)

BGMM is constructed over the RGMM model with the initial assumptions such as the chest is the center of movements which is the horizontal center of the sink node, the movement radius is not more than 2 meters, nodes on the arms and legs have more possibilities to change the network topology than the nodes in head and chest, sensor nodes are placed in a symmetrical way, the velocity of the node movements is in between 0 to 10 m/S and the node placements are in elbows and legs. The BGMM model node placements are given in Figure 1.

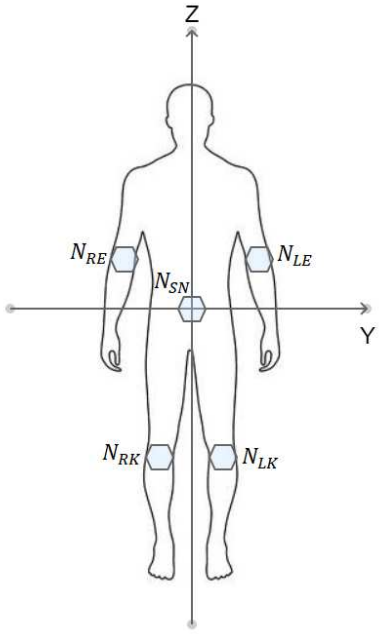

Figure 1: Node Placements

In the picture (Figure 1) N_{RE}, N_{LE}, N_{RK}, N_{LK} and N_{SN} are referring Right Elbow Node, Left Elbow Node, Right Knee Node, Left Knee Node and Sink Node respectively. The two-dimensional coordinates of the five nodes are $(0, y_{RE}, z_{RE})$, $(0, y_{LE}, z_{LE})$, $(0, y_{RK}, z_{RK})$, $(0, y_{LK}, z_{LK})$ and $(0, y_{SN}, z_{SN})$ in order. A three-dimension matrix is constructed using the two-dimensional coordinates using the equation 6

$$S_0 = \begin{bmatrix} x & y & z \\ 0 & 0 & 0 \\ 0 & y_{LE} & Z_{LE} \\ 0 & -y_{LE} & Z_{LE} \\ 0 & y_{LK} & -Z_{LK} \\ 0 & -y_{LK} & -Z_{RK} \end{bmatrix} \quad \text{Equation (6)}$$

Where the rows are given in order SN, LE, RE, LK and RK. The total number of wearable sensors will be represented as η.

The state transfer activities of walking and slow running will change the placements of the sensor nodes which can be represented as H matrix – refers the variations on node locations from sink node. H Matrix is constructed as in Equation 7.

$$H = \begin{bmatrix} x & y & z \\ 0 & 0 & 0 \\ \sigma_E \cos\gamma_n \cos\theta_n & \sigma_E \cos\gamma_n \sin\theta_n & \sigma_E \sin\gamma_n \\ -\sigma_E \cos\gamma_n \cos\theta_n & \sigma_E \cos\gamma_n \sin\theta_n & \sigma_E \sin\gamma_n \\ -\sigma_K \cos\gamma_n \cos\theta_n & \sigma_K \sin\gamma_n \sin\theta_n & \sigma_K \sin\gamma_n \\ \sigma_K \cos\gamma_n \cos\theta_n & \sigma_K \sin\gamma_n \sin\theta_n & \sigma_K \sin\gamma_n \end{bmatrix} \quad \text{Equation (7)}$$

Where $\sigma_E \in [\sigma_{Emin}, \sigma_{Emax}]$ is the magnitude variation,$\sigma_K \in [\sigma_{Kmin}, \sigma_{Emax}]$ is the step variation, γ is the angle between velocity and xy plane, θ is the angle between velocity and yzplane

The state transfer matrix B is calculated as $B = S_0[n] + H[n]$, where $n = 0,1,2 \ldots$ Equation (8)

Where

$$S_0(n) = \begin{cases} S_0(0), n = 4i \pm 2, (i = 1,2,3 \ldots); \\ S_0(1), n = 4i + 1, (i = 0,1,2 \ldots); \\ S_0(2), n = 4i + 3, (i = 0,1,2 \ldots); \end{cases}$$

3.3. Biometric based Cryptographic Key Generation (BCKG)

BCKG proposed a new method to generate cryptographic key from fingerprints. The first phase of BCKG is the feature extraction part. Core Point, Delta point and Minutiae points are extracted from the input finger print. Let P be the set of minutiae represented as $P = \{P_1(x_1, y_1), P_2(x_2, y_2) \ldots P_k(x_k, y_k)\}$ where k is the number of minutiae points. Let $C_P(x_c, y_c)$be the core point where x_c and y_c are the x and y coordinates. Similarly, $D_P(x_d, y_d)$ be the core point where x_c and y_c are the x and y coordinates of the detected delta point. The fingerprint data I is represented as

$$I = \begin{pmatrix} I_{11} & I_{12} & \ldots & I_{1q} \\ I_{21} & I_{22} & \ldots & I_{2q} \\ \ldots & \ldots & \ldots & \ldots \\ I_{p1} & I_{p2} & \ldots & I_{pq} \end{pmatrix} \quad \text{Equation (9)}$$

Let F_B is the set of lengths (l) and angles (a) if straight lines formed by minutiae points, F_c is the lengths (l') and angles (a') of core points and F_D is the lengths $(l'')$and angles (a'') of delta points. Let z^b_{max}, z^c_{max} and $z^d_{max}$are the maximum sizes of sets F_B, F_C and F_D. Then the complete representation of the sets are as follows.

$$F_B^{max} = \left\{(l_1, a_1), (l_2, a_2), \ldots, \left(l_{z^b}, a_{z^b}\right), \left(0_{z^b+1}, 0_{z^b+1}\right), \ldots, (0_{z^b_{max}-z^b}, 0_{z^b_{max}-z^b})\right\} \quad \text{Equation (10)}$$

$$F_C^{max} = \left\{(l'_1, a'_1), (l'_2, a'_2), \ldots, (l'_{z^c}, a'_{z^c}), (0_{z^c+1}, 0_{z^c+1}), \ldots, (0_{z^c_{max}-z^c}, 0_{z^c_{max}-z^c})\right\} \quad \text{Equation (11)}$$

$$F_D^{max} = \left\{(l''_1, a''_1), (l''_2, a''_2), \ldots, \left(l''_{z^d}, a''_{z^d}\right), \left(0_{z^d+1}, 0_{z^d+1}\right), \ldots, (0_{z^d_{max}-z^d}, 0_{z^d_{max}-z^d})\right\} \quad \text{Equation (11)}$$

$$F^{max} = \{F_B^{max} \| F_C^{max} \| F_D^{max}\} \quad \text{Equation (12)}$$

F^{max} is the concatenated set which is further obfuscated using binary X-OR operation to generate the cryptographic keys. The similarities of the matrices in Equation 7 and Equation 9 makes it possible to use BCKG in BGMM with some modifications – addressed by the proposed method EBLKGAW.

4. Enhanced BGMM based Lightweight Key Generation and Authentication method for WBAN

EBLKGAW model provides a way to connect more number of wireless senor nodes to a single network which is a primary requirement is modern WBAN environments. IoT and cloud developments are improving Implantable sensor nodes and Wearable sensor nodes crates more possibility to connect more than 5 WBAN nodes[16]. EBLKGAW consists three sub-modules, they are, Enhanced BGMM (EBGMM), Legacy Key Generator (LKG) and Idle State Key Manager (ISKM). The functionalities are explained below in detail.

4.1. Enhanced BGMM (EBGMM)

EBGMM adopts the base working principle of the BGMM. The omni-direction movement measurement and tracking are added in EBGMM. More node adoptability is also adopted by adding more rows in processing matrix. Implantable sensors are used to measure the primary vital parameters such as Body temperature, Heart rate, Respiratory rate, Oxygen saturation, Blood glucose level and Blood pressure, whereas wearable sensors are used for the same with lesser accuracy and they are equipped with better activity movement tracking components. WBAN implantable and wearable node placements are illustrated in Figure 2 – given below to explain the process of EBGMM.

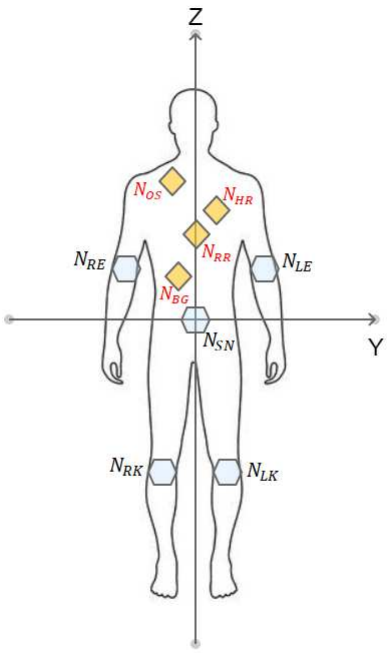

Figure 2: Implantable and Wearable node placements

In Figure 2, Oxygen Sensor Node N_{OS}, Heart Rate sensor Node N_{HR}, Respiratory Rate sensor N_{RR} and Blood Glucose Sensor N_{BG} are the implanted sensors. Similarly, Right Elbow Node N_{RE}, Left Elbow Node N_{LE}, Right Knee Node N_{RK}, Left Knee Node N_{LK} and Sink Node N_{SN} are the wearable wireless sensor nodes. The implantable nodes are treated as a set and represented as $\Xi = \{\xi_0, \xi_1 \dots \xi_{\Xi_{max}}\}$ where ξ_0 refers the alternate sink node $N_{RR}$and Ξ_{max} is the number of implanted sensors.

The initial assumption of EBGMM is that the intra distance mobility between the implanted sensor nodes are lesser then the wearable sensor nodes. This assumption copes with all WBAN environments because implanted sensor nodes cannot get the Euclidean distance which is greater than the maximum body part mobility. Therefore, the measured data of implanted nodes are substituted for the physical movements to get more stochasticity. The

BGMM model is used to construct the mobility matrix with the modification of using measured context of the implanted nodes are used as the input instead of physical movements. The measured 16-bit value's most significant bits (MSB) are substituted for the y-axis movement data (δ_y) and least significant bits (LSB) are substituted for the z axis movement data (δ_z) as given in Figure 3. By this way every implanted wireless sensor node $\xi_i$will have a coordinate data $(0, \delta_{y_i}, \delta_{z_i})$

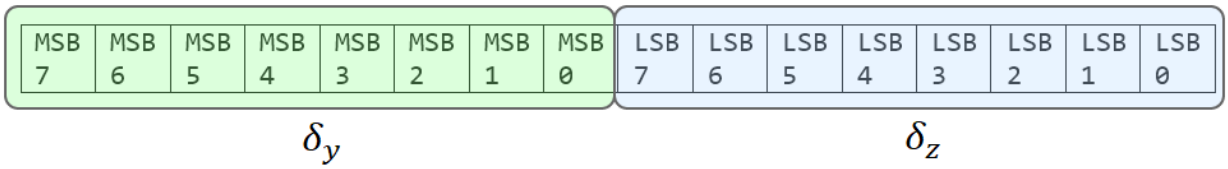

Figure 3: Implantable nodes' coordinate data

The purpose of EBGMM is to generate the security keys with more randomness thus movement measurement accuracy is not concentrated here.N_{RR} will be assigned as the sink node in the WBAN environments where there are no wearable devices are used, N_{SN} will be the standard sink node otherwise. The three-dimension state matrix construction based on Equation 6 is given below as Equation 13.

$$S_0 = \begin{bmatrix} x & y & z \\ 0 & \delta_{y_0}\delta_{z_0} \\ 0 & \delta_{y_1}\delta_{z_1} \\ 0 & \delta_{y_2}\delta_{z_2} \\ 0 & \delta_{y_3}\delta_{z_3} \\ 0 & 00 \\ 0 & y_{LE}z_{LE} \\ 0 & -y_{LE}z_{LE} \\ 0 & y_{LK}-z_{LK} \\ 0 & -y_{LK}-z_{RK} \end{bmatrix} \quad \text{Equation (13)}$$

Where the rows refer N_{RR}, N_{OS}, N_{HR}, N_{BG}, N_{SN}, N_{LE}, N_{RE}, N_{LK} and N_{RK} in order.

By Equation 7, the EBGMM H Matrix is constructed as below in equation 14

$$H = \begin{bmatrix} x & y & z \\ \sigma_{\xi_0}\cos r_{\xi_0}\cos\theta_{\xi_0} & \sigma_{\xi_0}\cos r_{\xi_0}\sin\theta_{\xi_0} & \sigma_{\xi_0}\sin r_{\xi_0} \\ \sigma_{\xi_1}\cos r_{\xi_1}\cos\theta_{\xi_1} & \sigma_{\xi_1}\cos r_{\xi_1}\sin\theta_{\xi_1} & \sigma_{\xi_1}\sin r_{\xi_1} \\ \sigma_{\xi_2}\cos r_{\xi_2}\cos\theta_{\xi_2} & \sigma_{\xi_2}\cos r_{\xi_2}\sin\theta_{\xi_2} & \sigma_{\xi_2}\sin r_{\xi_2} \\ \sigma_{\xi_3}\cos r_{\xi_3}\cos\theta_{\xi_3} & \sigma_{\xi_3}\cos r_{\xi_3}\sin\theta_{\xi_3} & \sigma_{\xi_3}\sin r_{\xi_3} \\ 0 & 0 & 0 \\ \sigma_E\cos\gamma_n\cos\theta_n & \sigma_E\cos\gamma_n\sin\theta_n & \sigma_E\sin\gamma_n \\ -\sigma_E\cos\gamma_n\cos\theta_n & \sigma_E\cos\gamma_n\sin\theta_n & \sigma_E\sin\gamma_n \\ -\sigma_K\cos\gamma_n\cos\theta_n & \sigma_K\sin\gamma_n\sin\theta_n & \sigma_K\sin\gamma_n \\ \sigma_K\cos\gamma_n\cos\theta_n & \sigma_K\sin\gamma_n\sin\theta_n & \sigma_K\sin\gamma_n \end{bmatrix} \quad \text{Equation (14)}$$

Where $\forall i \coloneqq 0 \rightarrow \Xi_{max}, \sigma_{\xi_i}$ refers the measured data value of implanted wireless sensor node ξ_i. Since four implanted wireless sensor nodes taken here for example, the value of Ξ_{max} is assigned as 3.

Since the state transfer calculations are not required to generate the cryptographic key generations process, this H Matrix will be directed to the next phase of the process.If there is enough mobility sensed by the wearable sensors, then the key generation will be per formed by the LKG module, otherwise ISKMwill generate the keys.

4.2. Legacy Key Generator (LKG)

Legacy Key Generation module functions in a similar way as the BCKG. The BGKG gets the input data matrix from a fingerprint scanner. The Hmatrix output from EBGMM module is given as the input matrix for the LKG module. By substituting the values from Equation 14 into Equation 9, the following input matrix is formed to proceed with LKG.

$$I = \begin{bmatrix} x & y & z \\ I_{11} & I_{12} & I_{13} \\ I_{21} & I_{22} & I_{23} \\ I_{31} & I_{32} & I_{33} \\ I_{41} & I_{42} & I_{43} \\ I_{51} & I_{52} & I_{53} \\ I_{61} & I_{62} & I_{63} \\ I_{71} & I_{72} & I_{73} \\ I_{81} & I_{82} & I_{83} \\ I_{91} & I_{92} & I_{92} \end{bmatrix} \quad \text{Equation (15)}$$

Since the taken physical coordinate dimension is limited to 3, the input matrix I is split into several 3×3submatrices $\left(m_1^{sub}, m_2^{sub}, \ldots m_{\left\lceil \frac{\eta+\Xi_{max}}{3} \right\rceil}^{sub}\right)$to reduce the computational complexity. If the value of $\eta + \Xi_{max}$ is not divisible by 3, then number of 0s will be added to the last submatrix to match the 3×3size. Then even number submatrices will be transposed for further obfuscation to improve security. Post execution sub matrices will be as follows

$$m_1^{sub} = \begin{bmatrix} I_{11} & I_{12} & I_{13} \\ I_{21} & I_{22} & I_{23} \\ I_{31} & I_{32} & I_{33} \end{bmatrix}$$

$$(m_2^{sub})^T = \begin{bmatrix} I_{41} & I_{51} & I_{61} \\ I_{42} & I_{52} & I_{62} \\ I_{43} & I_{53} & I_{63} \end{bmatrix}$$

$$m_3^{sub} = \begin{bmatrix} I_{71} & I_{72} & I_{73} \\ I_{81} & I_{82} & I_{83} \\ I_{91} & I_{92} & I_{93} \end{bmatrix}$$

The cryptographic key construction is performed based on the Expansion-Permutation as in equation 16 - given below

$$K = EP[\{m_1^{sub} \| (m_2^{sub})^T \| m_3^{sub} \| (m_4^{sub})^T \ldots \varepsilon_T\}] \quad \text{Equation (16)}$$

Where K is the cryptographic key, ε_T is the end term determined using equation 17

$$\varepsilon_T = \begin{cases} m_{\left\lceil \frac{\eta+\Xi_{max}}{3} \right\rceil}^{sub} \; if \; (\eta + \Xi_{max}) \; is \; divisible \; by \; 3 \\ \left(m_{\left\lceil \frac{\eta+\Xi_{max}}{3} \right\rceil}^{sub} \right)^T \; otherwise \end{cases} \quad \text{Equation (17)}$$

Selected Key K is further used to encrypt and decrypt the data transferred between WBAN nodes. The Sink Node N_{SN} or N_{RR} knows the physical movements as well as the measured values from the sensors, it can safely exchange information among the nodes with the initial session key K. Annihilation of existing key and conception of new key takes place periodically or on demand [17]based on the normal process or intrusion detection.

4.3. Idle State Key Manager (ISKM)

ISKM is used when there are no significant physical movements sensed by the wearable sensors. ISKM excludes the wearable sensor devices while there are no or less inputs from them. Implanted sensors continue to work by measuring the essential parameters which will be included in the H matrix to calculate the cryptographic keys. By Equation 14, the H matrix of ISKM will be as follows

$$H = \begin{bmatrix} x & y & z \\ \sigma_{\xi_0} cos\gamma_{\xi_0} cos\theta_{\xi_0} & \sigma_{\xi_0} cos\gamma_{\xi_0} sin\theta_{\xi_0} & \sigma_{\xi_0} cos\theta_{\xi_0} \\ \sigma_{\xi_1} cos\gamma_{\xi_1} cos\theta_{\xi_1} & \sigma_{\xi_1} cos\gamma_{\xi_1} sin\theta_{\xi_1} & \sigma_{\xi_1} cos\theta_{\xi_1} \\ \sigma_{\xi_2} cos\gamma_{\xi_2} cos\theta_{\xi_2} & \sigma_{\xi_2} cos\gamma_{\xi_2} sin\theta_{\xi_2} & \sigma_{\xi_2} cos\theta_{\xi_2} \\ \sigma_{\xi_3} cos\gamma_{\xi_3} cos\theta_{\xi_3} & \sigma_{\xi_3} cos\gamma_{\xi_3} sin\theta_{\xi_3} & \sigma_{\xi_3} cos\theta_{\xi_3} \end{bmatrix} \quad \text{Equation (18)}$$

The LKG Input matrix will have only 4 rows from I_1 to I_4. Therefore, the submatrices will be constructed as follows

$$m_1^{sub} = \begin{bmatrix} I_{11} & I_{12} & I_{13} \\ I_{21} & I_{22} & I_{23} \\ I_{31} & I_{32} & I_{33} \end{bmatrix}$$

$$(m_2^{sub})^T = \begin{bmatrix} I_{41} & 0 & 0 \\ I_{42} & 0 & 0 \\ I_{43} & 0 & 0 \end{bmatrix}$$

The cryptographic session key is calculated by Equation 16 as follows

$$K = EP[\{m_1^{sub} \| (m_2^{sub})^T\}]$$

ISKM also maintains the security by improving the hamming distance of the two subsequent session keys by applying Left-Shift operation and One's complement operation. The key modification algorithm is given below.

Key modification Algorithm

Inputs: Previous session key K_P and Current session key K

Output: Current session key with hamming distance $\psi > 2$

Step 1: Let c be the counter with initial value 0

Step 2: Calculate $K_T = K_p \oplus K$

Step 3: $\psi = Count1bits(K_T)$

Step 4: if $(\psi > 2)$ return K

Step 5: if $(c > 1)$ go to Step 9

Step 6: Increment c by 1

Step 7: $K = K \ll 1$ (Left-Shift by 1)

Step 8: Go to Step 2

Step 9: Return $\sim K$ (1's compliment)

By this way ISKM generates diversified keys even in idle state, that is less or no mobility in the wearable WBAN nodes.

The overall flow diagram of EBLKGAW is given below as Figure 4.

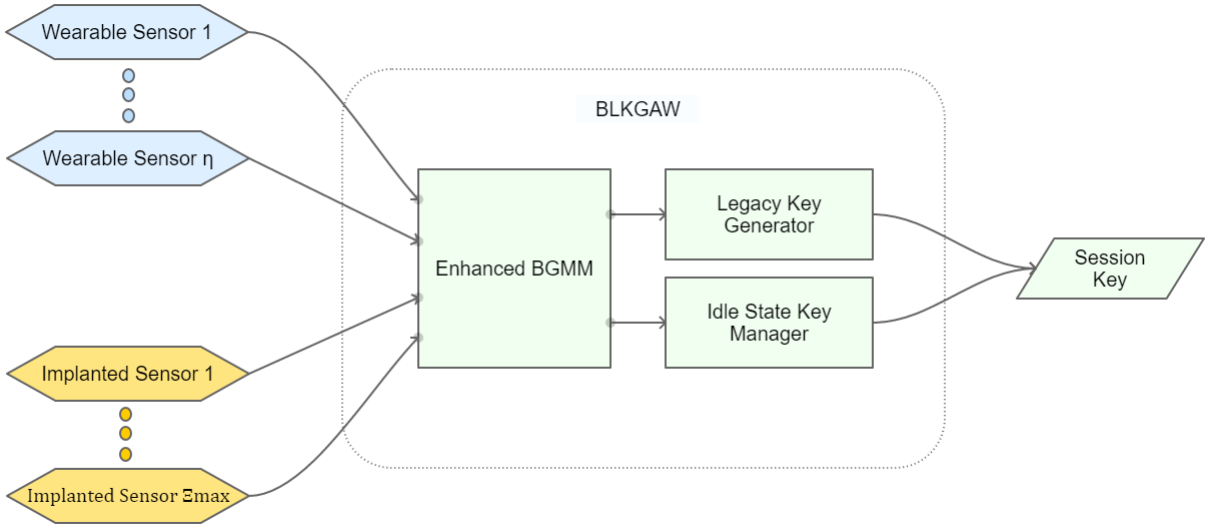

Figure 4: EBLKGAW Flow Diagram

5. Experimental setup

OPNET[18][19][20]– a leading industrial network simulation tool is used to analyze the performance of the existing and proposed method. OPNET is a complete network simulation tool which provides access to all level network components from node to base-station. It has the random network generation facility to evaluate new network architectures and protocols. OPNET can be configured using many familiar programming languages such as C and C++. The configuration of nodes, their placements, permitted network protocols and customized user defined network entities are loaded into OPNET to measure their performance. It also has a built-in mechanism with random triggered network attacks to measure the security level of a network architecture or protocol. Visual Studio IDE [21][22]is used to write the code to create the OPNET interface and evaluation results are captured as tables and graphs.

OPNET Wireless sensor nodes are configured to emulate the TELOSB Mote TPR2420 sensors[23][24]. This wireless sensor device is capable of handling IEEE 802.15.4 and IEEE 802.15.6 standards. This mote node is equipped with high data rate radio up to 250 kbps. The brain of this sensor node is MSP430 microcontroller works in 16-bit RISC architecture from Texas Instruments. Tiny OS – an open source operating system us used to operate this device. TRP2420's radio operates in 2.4 to 2.4835 GHz frequency range with Power -24 dBm to 0 dBm.Twenty sensor nodes are divided in to two equal body area networks. Each BAN contains 10 number of sensor nodes. Eight number of sensor nodes are used to collect and communicate healthcare data, one is dedicated to operate as Control Unit and the remaining node is used as an intruder to measure the stability of the existing and proposed Network Schemes. A Computer with Intel® Core ™ i5-7200 CPU @ 2.5GHz to 2.7 GHz Turbo boost processer and 8GB RAM is used to run the simulations in Windows 10 64-bit operating system.

6. Results and Analysis

Simulation is performed to measure various benchmark parameters of body area network like Throughput, End-to-End delay, Packet Delivery Ratio, Memory consumption, Power Consumption and Security. These parameters are measured for existing methods DSCB, NFSDW, FMIDPW, DRDDRP and for proposed method EBLKGAW. Simulation is performed for 1-hour real world time duration and parameters are logged in 12 minutes equal interval.

6.1. Throughput

Throughput: The amount of data communicated by a network system is referred as throughput with the unit bits-per-second. Throughput is measured for discussed network protocols are measured using OPNET and the results are given in Table 2. It is also represented in graph given in Figure 5 for clear comparison.

Throughput (bps)					
Time stamp (Minutes)	**DSCB**	**NFSDW**	**FMIDPW**	**ERDDRP**	**EBLKGAW**
12	83038	88229	87485	81808	91331
24	82718	87526	88558	81834	91009
36	83913	88059	88665	81747	90029
48	82638	86544	88472	81050	90918
60	84362	88210	87600	80624	90938

Table 2: Throughput (bps)

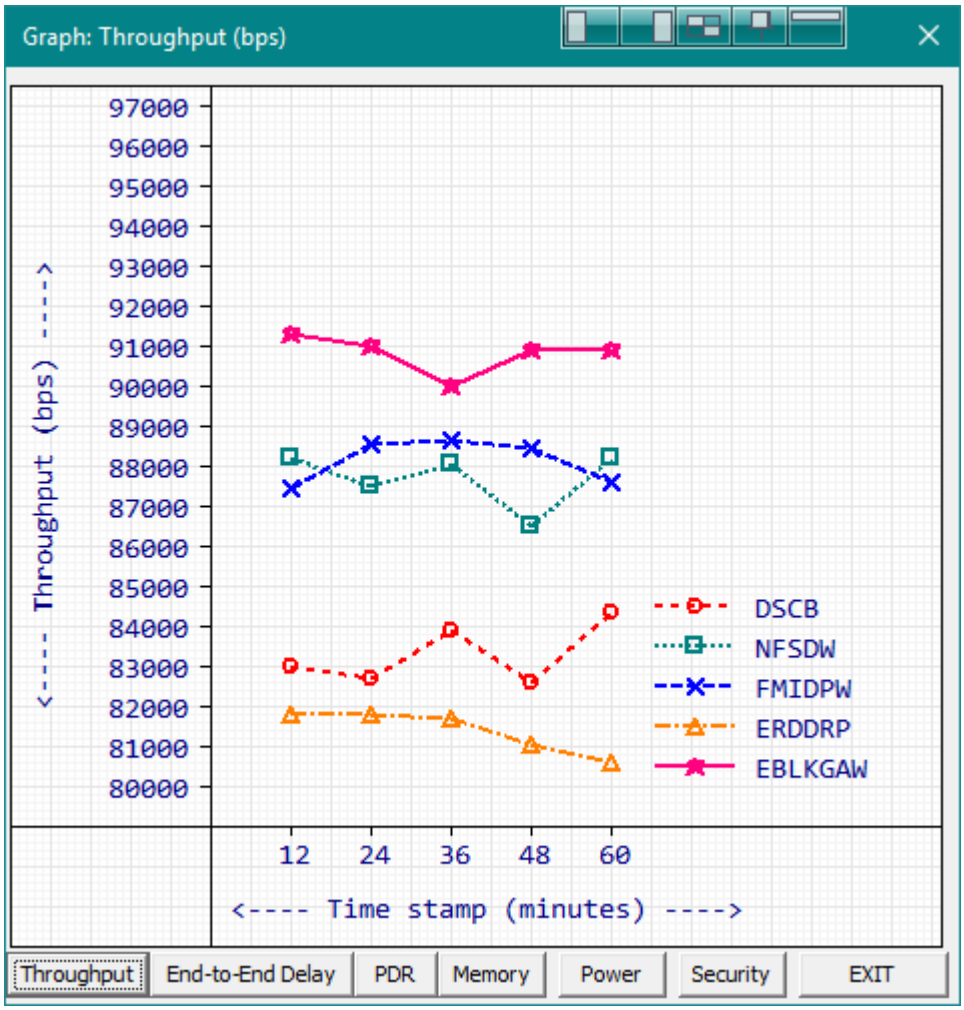

Figure 5: Throughput

EBLKGAW scores the throughput range from 90029 to 91331 bps with the average value of 90845 bps in 5 different timestamp measurements which is higher than other existing methods. The nearest competitor FMIDPW scored the throughput between 87485 and 88665 bps with the average of 88156 bps.

6.2. End-to-End Delay

The total time taken to transmit a packet from a source to destination is represented as End-to-End delay and measured in milliseconds(mS) unit. It is the accumulated value of System delay, Latency, IP-Delay and Jitter values. Lesser End-to-End delay value indicates the higher data transmission and the quality of the network. End-to-End delay values for the existing and proposed systems are measured by the simulator and logged in every 12 minutes interval. Logged End-to-End delay values are tabulated and given in Table 3. Table values are plotted as graph and given in Figure 6.

End-to-End Delay (mS)					
Time stamp (Minutes)	**DSCB**	**NFSDW**	**FMIDPW**	**ERDDRP**	**EBLKGAW**
12	521	392	393	573	320
24	513	391	404	568	330
36	509	397	409	568	324
48	518	396	395	581	325
60	510	405	401	568	325

Table 3: End-to-End Delay (mS)

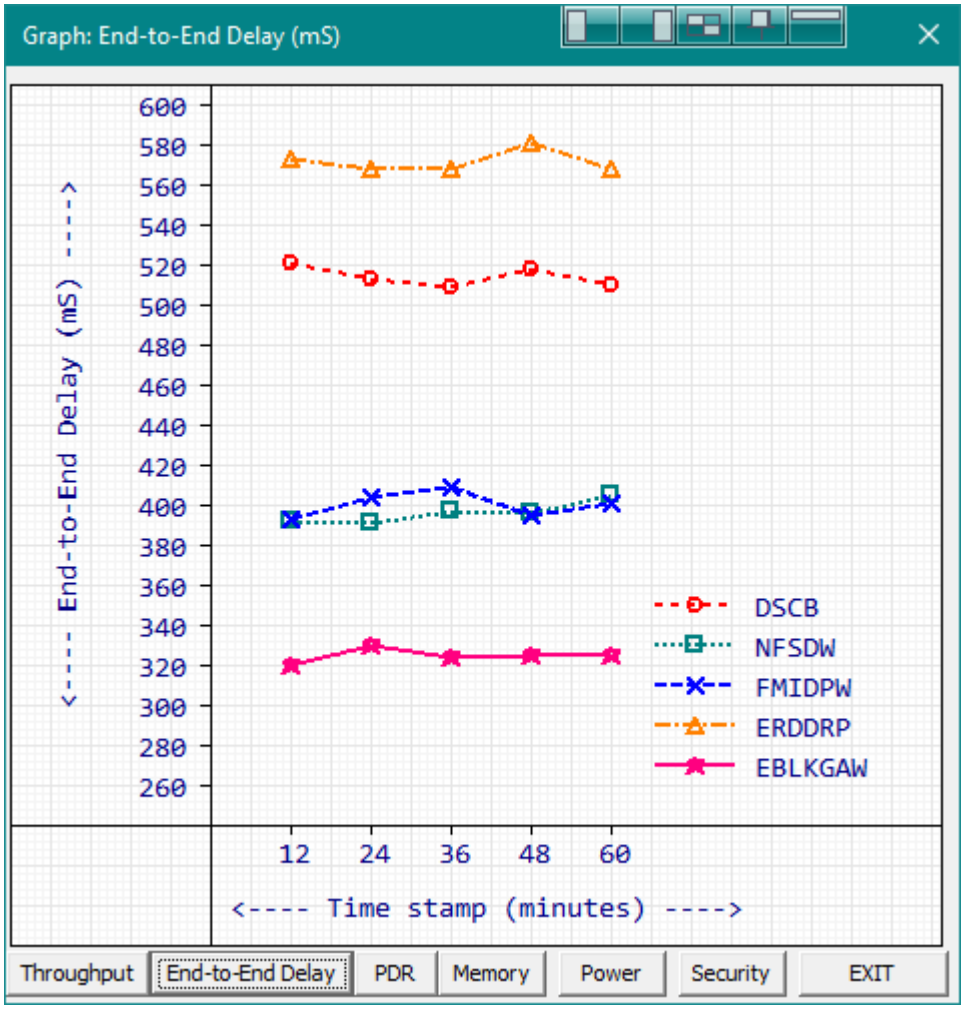

Figure 6: End-to-End Delay

The average end-to-end delay of proposed EBLKGAW is 325 mS which is lesser than the values 514mS, 396mS, 400mS and 571mS of DSCB, NFSDW, FMIDPW and ERDDRP in order. The minimum end-to-end delay 320 mS is achieved my EBLKGAW in the first 12 minutes timestamp.

6.3. Packet Delivery Ratio

The ratio between number of transmitted packets and the number of received packets is defined as Packet Delivery Ratio. Various network barriers like data collision, insufficient buffer memory and channel inaccessibility are causing packet drops. A good quality network architecture has minimum number of Packet drops whereas middling quality network architectures suffer in lot of packet drops. Packet Delivery radio is calculated throughout the simulation period by OPNET. The observed packet delivery ratio values for DSCB, NFSDW, FMIDPW, DRDDRP and EBLKGAW are given in Table 4. Comparison graph is plotted and given in Figure 7.

Packet Delivery Ratio (%)					
Time stamp (Minutes)	**DSCB**	**NFSDW**	**FMIDPW**	**ERDDRP**	**EBLKGAW**
12	90	92	94	82	94
24	89	93	93	82	95
36	89	93	93	81	96
48	91	92	92	82	95
60	90	94	93	81	95

Table 4: Packet Delivery Ratio (%)

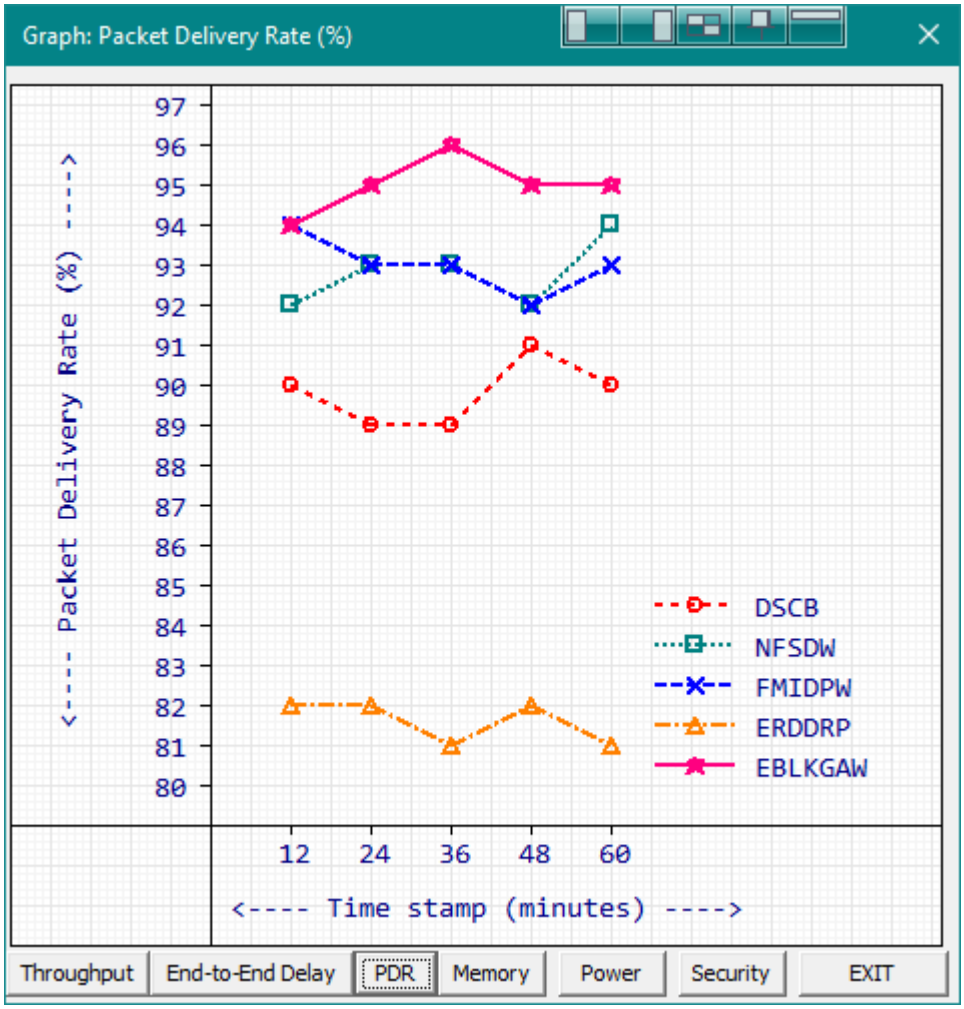

Figure 7: Packet Delivery Ratio

EBLKGAW achieved 95% of maximum average packet delivery ratio with the range between 94% and 96%. Existing DSCB, NFSDW, FMIDPW and ERDDRP are getting 90%, 93%, 93% and 82% of packet delivery ratio respectively.

6.4. Memory consumption

Wireless sensor nodes are embedded devices with limited memory. Their elementary intent is to sense and stream environmental data to another node or to a control unit. Hence these devices are manufactured with limited memory to reduce the size and cost. Providing intelligent routing and secured communication system with this limited memory is a challenging task. In a secured communication, calculating and updating security keys are essential process. To improve the security and other communication improvements, consuming a little higher memory within the availability will not affect the performance of the system. Memory consumptions for security key calculation and revocation by the procedures DSCB, NFSDW, FMIDPW, DRDDRP and EBLKGAW are measured by the simulator. These values are given in Table 5 and comparison graph is given in Figure 8.

Memory (B)					
Time stamp (Minutes)	**DSCB**	**NFSDW**	**FMIDPW**	**ERDDRP**	**EBLKGAW**
12	2476	2999	2985	2594	1661
24	2463	2974	2962	2582	1661
36	2463	2964	2983	2555	1685
48	2483	2963	2966	2588	1668
60	2469	2979	2973	2570	1658

Table 5: Memory Consumption

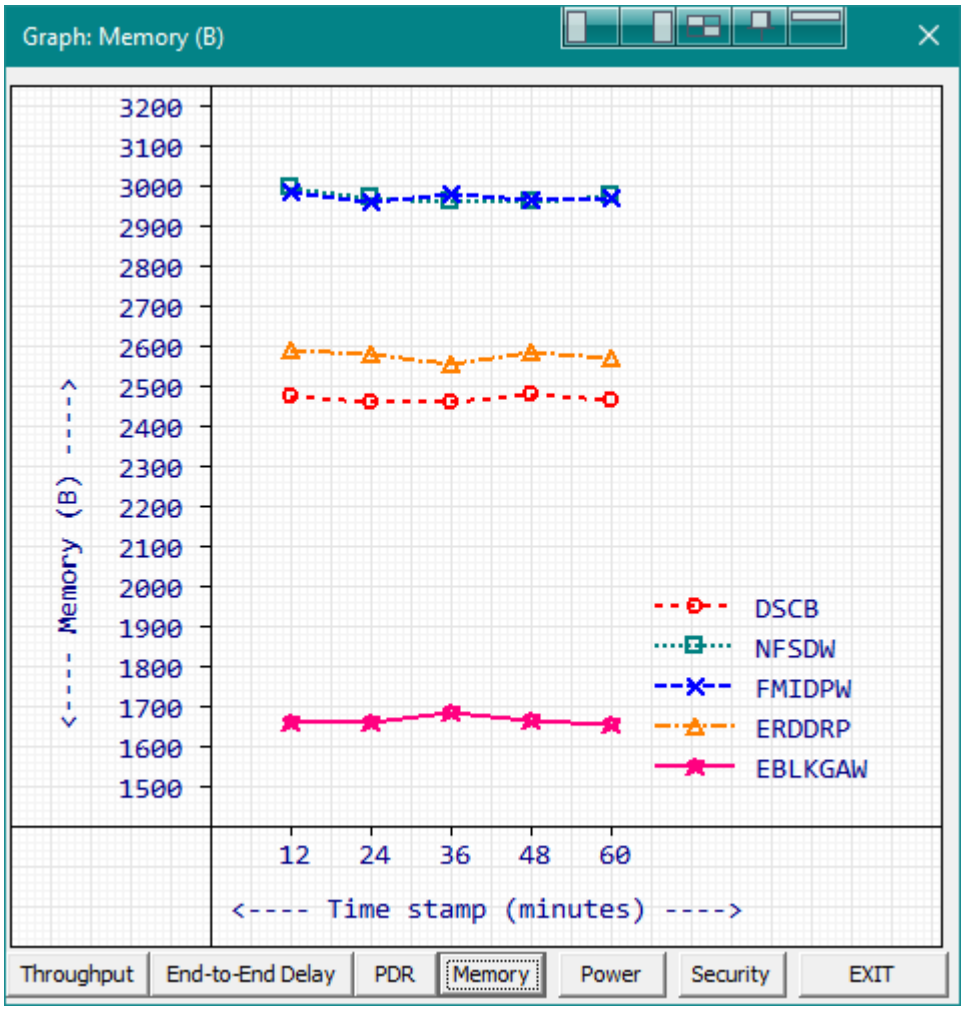

Figure 8: Memory Consumption

EBLKGAW consumed the memory average of 1667 Bytes to generate and annihilate a session key.

6.5. Power Consumption

Wireless sensor nodes are depending battery power to function. Higher power consumption will drain the battery swiftly and the overall operation period of the nodes will be reduced by this. A better network system should use the limited power wisely to extend the life span of the network. Power consumption of existing and proposed methods are measured by the simulator and given in Table 6. Comparison graph is given in Figure 9.

Power (mW)					
Time stamp (Minutes)	**DSCB**	**NFSDW**	**FMIDPW**	**ERDDRP**	**EBLKGAW**
12	40	63	66	38	27
24	44	64	64	36	30
36	43	62	62	37	27
48	42	65	62	38	28
60	41	62	64	35	30

Table 6: Power Consumption (mW)

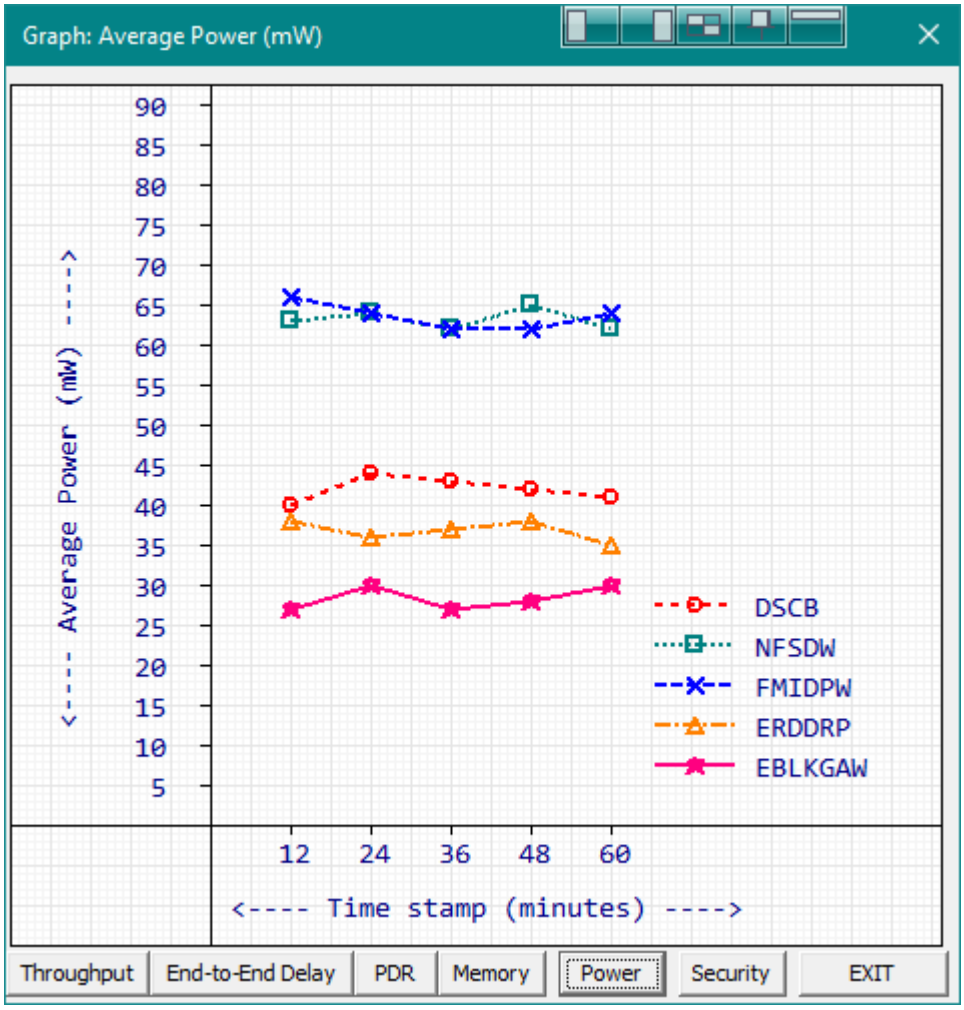

Figure 9: Power Consumption

EBLKGAW consumed the power consumption average of 28mW to generate and annihilate a session key which is lesser than 42mW, 63mW, 63mW and 37mW of DSCB, NFSDW, FMIDPW and ERDDRP in order. The minimum power required to calculate a session key by EBLKGAW is 27mW and the maximum power consumption is 30mW. The average power consumptions for key calculation of EBLKGAW for Timestamp 1 to 5 are 27mW, 30mW, 27mW, 28mW and 30mW.

6.6. Security

Wireless Body Area Network mainly deals with healthcare data which is delicate and should be handled with privacy. An intruder can get advantage if he gets access for some personnel healthcare data. Therefore, Security is one of the prime concerns in BAN. Security is measured by the simulator by adding intruder nodes in to the simulation. Metered security values are tabulated and given in Table 7. Comparison graph is provided in Figure 10.

Security (%)					
Time stamp (Minutes)	**DSCB**	**NFSDW**	**FMIDPW**	**ERDDRP**	**EBLKGAW**
12	80	88	87	79	95
24	81	87	88	79	95
36	81	87	87	79	94
48	82	88	88	79	94
60	82	88	87	81	95

Table 7: Security (%)

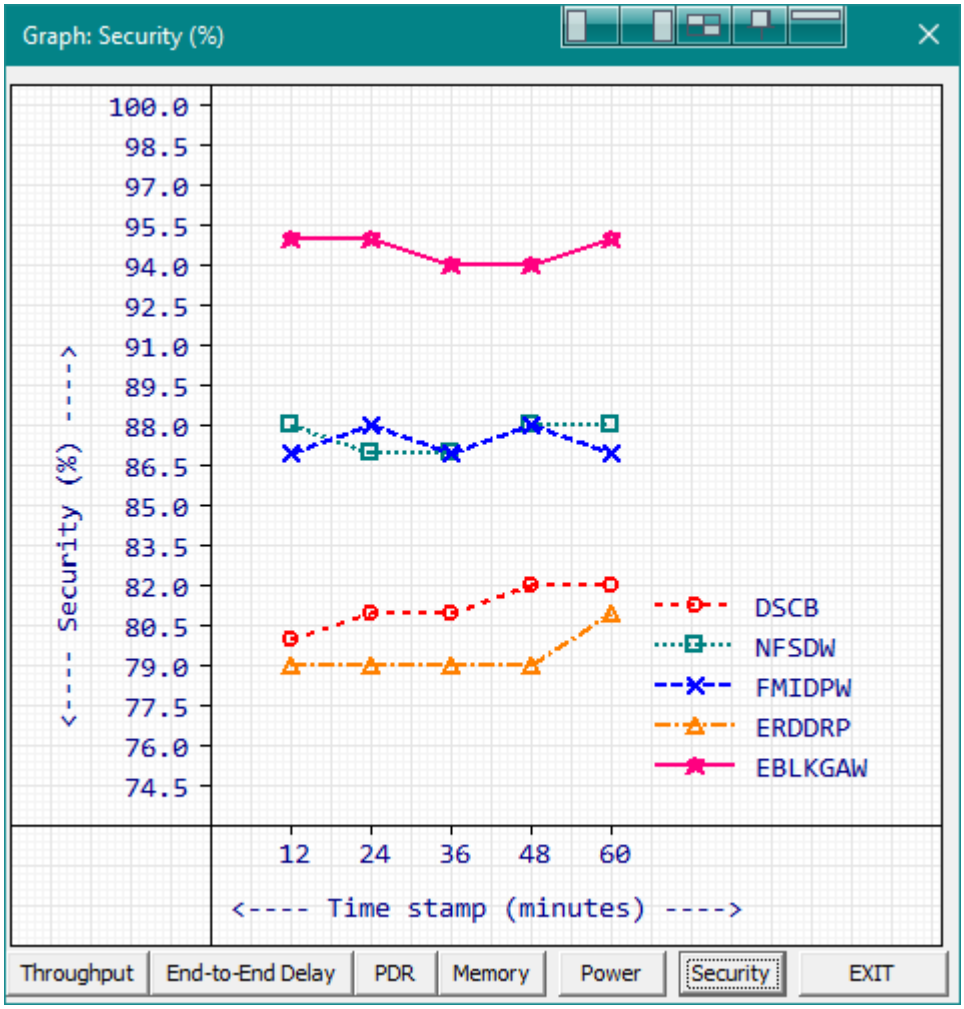

Figure 10: Security

The Security level average of EBLKGAW is 94.6%. The maximum vulnerability occurred at 3rd and 4th timestamps where EBLKGAW secured 94% of security level which is higher than other maximum-security levels 82%, 88%, 88% and 81% of DSCB, NFSDW, FMIDPW and ERDDRP. The security level averages of DSCB, NFSDW, FMIDPW and EEDDRP are 81.2%, 87.6%, 87.4% and 79.4% respectively. The observed results show that the proposed EBLKGAW method is more reliable that other methods in security aspect.

7. Conclusion

Power saving and security are the prime factors to decide the quality of a wireless body area network. Improved Throughput and reduced communication delays are other supporting factors of the networks. Achieving higher security without increase in power consumption is the challenging task of any network. Key generation and authentication play vital role in improving security and dealing with power consumption. A balanced lightweight key generation procedure EBLKGAW that provides higher security levels with reduced power consumption without affecting other parameters is proposed and evaluated in this work. The proposed key generation procedure goes well with both WBAN IEEE 802.15.6. and IoT IEEE 802.11 b/g/n standard security schemes. Therefore, this work will serve the purpose of handling wearable and implanted heterogeneous wireless body area network nodes in an efficient way by improving the network lifetime with adequate security levels.

8.Funding

There is no funding information.

9.Conflict of interest

There is no conflict of interest.

10.Availability of data and material

There is no availability of data and material.

11.Code availability

There is no code availability.

References:

[1] Simon EliasBibri, "The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability" in Sustainable Cities and Society Volume 38, Elsevier 2018, Pages: 230-253

[2]Huseyin Yildirim and Amr M.T.Ali-Eldin, "A model for predicting user intention to use wearable IoT devices at the workplace" in Journal of King Saud University - Computer and Information Sciences online version, Elsevier 2018, Pages: 1-9

[3] M. S. Darweesh, T. Ismail and H. Mostafa, "On RF Telemetry for Implantable Medical Devices: A Communication Theory Perspective" in Networks & Digital Signal Processing (CSNDSP), IEEE 2018, Pages: 1-6

[4] Sabri Khssibi, Adrien Van Den Bossche, Hanen Idoudi, Leila AzouzSaidane and Thierry Val, "Enhancement of the Traffic Differentiation Architecture for WBAN Based on IEEE 802.15.4" in Wireless Personal Communications Volume 101 Issue 3, Springer 2018, Pages: 1519–1537

[5] Inayat Ali, Eraj Khan and Sonia Sabir, "Privacy-preserving data aggregation in resource-constrained sensor nodes in Internet of Things A review" in Future Computing and Informatics Journal Volume 3 Issue 1, Elsevier 2018, Pages: 41-50

[6] F. S. Chowdhury, A. Istiaque, A. Mahmud and M. Miskat, "An implementation of a lightweight end-to-end secured communication system for patient monitoring system" in Emerging Trends in Electronic Devices and Computational Techniques (EDCT), IEEE 2018, Pages: 1-5

[7] Zahid Ullah, Imran Ahmed, Kaleem Razzaq, Muhammad Kashif Naseer and Naveed Ahmed, "DSCB: Dual sink approach using clustering in body area network" in Peer-to-Peer Networking and Applications Volume 12 Issue 2, Springer 2019, Pages: 357–370

[8] K. Hasan, X. Wu, K. Biswas and K. Ahmed, "A Novel Framework for Software Defined Wireless Body Area Network", International Conference on Intelligent Systems - Modelling and Simulation (ISMS), IEEE 2018, Pages: 114-119

[9] Wan Aida Nadia Wan Abdullah, NaimahYaakob, R. Badlishah, Mohamed ElshaikhElobaid, Siti Asilah Yah, and I.Zunaidi3, "Fragmentation in MAC IEEE 802.15.4 to Improve Delay Performance in Wireless Body Area Network (WBAN)" IOP Conference Series: Materials Science and Engineering Volume 557, IOPC 2019, Pages: 1-7

[10] J. Mu, X. Yi, X. Liu and L. Han, "An Efficient and Reliable Directed Diffusion Routing Protocol in Wireless Body Area Networks", in IEEE Access volume 7, IEEE 2019, Pages: 58883-58892

[11] Q. Zhang, T. H. Loh, W. Zhang, Y. Yang and F. Qin, "Proof of Concept Experiment for Single Probe MIMO OTA Measurement System", European Conference on Antennas and Propagation (EuCAP), IEEE-2019, Pages: 1-5

[12] Mehrdad Hessar, Ali Najafi, Vikram Iyer and ShyamnathGollakota,"TinySDR: Low-Power SDR Platform for Over-the-Air Programmable IoT Testbeds" in Electrical Engineering and Systems Science - Signal Processing, Cornell University 2019, Pages: 1-16

[13] T. Chang, T. Watteyne, X. Vilajosana and P. H. Gomes, "Constructive Interference in 802.15.4: A Tutorial", in IEEE Communications Surveys & Tutorials volume 21, IEEE 2019, Pages: 217-237

[14] Y. Liu, D. Liu and G. Yue, "BGMM: a body gauss-markov based mobility model for body area networks", in Tsinghua Science and Technology Volume - 23 Issue 3, IEEE 2018, Pages: 277-287

[15]GaurangPancha and DebasisSamanta, "A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security" in Computers & Electrical Engineering Volume 69, Elsevier 2018, Pages: 461-478

[16] Adeniyi Onasanya and Maher Elshakankiri, "Secured Cancer Care and Cloud Services in IoT/WSN Based Medical Systems" in International Conference on Smart Grid and Internet of Things SGIoT: Smart Grid and Internet of Things, Springer 2018, Pages 23-35

[17] Steven Myers and Adam Shull "Practical revocation and key rotation" in Cryptographers' Track at the RSA Conference CT-RSA 2018: Topics in Cryptology – CT-RSA, Springer 2018, Pages 157-178

[18] N. I. Sarkar, S. Gul and B. Anderton, "Gigabit Ethernet with Wireless Extension: OPNET Modelling and Performance Study" in International Conference on Information Networking (ICOIN), IEEE 2019, Pages: 216-221

[19]M. Pahlevan and R. Obermaisser, "Evaluation of Time-Triggered Traffic in Time-Sensitive Networks Using the OPNET Simulation Framework" in 26th Euromicro International Conference on Parallel - Distributed and Network-based Processing (PDP), Cambridge, IEEE 2018, Pages: 283-287

[20] C. Kamyod, "End-to-end reliability analysis of an IoT based smart agriculture" in International Conference on Digital Arts, Media and Technology (ICDAMT) Phayao, IEEE 2018, Pages: 258-261

[21] T Kahlert and K Giza, "Visual Studio Code: Tips & Tricks Vol.1", Microsoft Publications 2018, Pages: 1-26

[22]Pengzhan Chen, Wei Chu and Junchao Wang, "A Human Body Motion Capture System Using a Wireless Inertial Sensor" in Proceedings of the 2019 International Conference on Wireless Communication, Network and Multimedia Engineering, WCNME 2019, Pages: 1-4

[23] Neha Fotedar and Poonam Saini, Performance Analysis of Time Synchronization Protocols on Different Commercial Mote Platforms" in Procedia Computer Science Volume 125, Elsevier 2018, Pages: 888-894

[24] F. Luo, S. Poslad and E. Bodanese, "Kitchen Activity Detection for Healthcare using a Low-Power Radar-Enabled Sensor Network" in ICC 2019 - 2019 IEEE International Conference on Communications (ICC) Shanghai China, IEEE 2019, Pages: 1-7

Figures

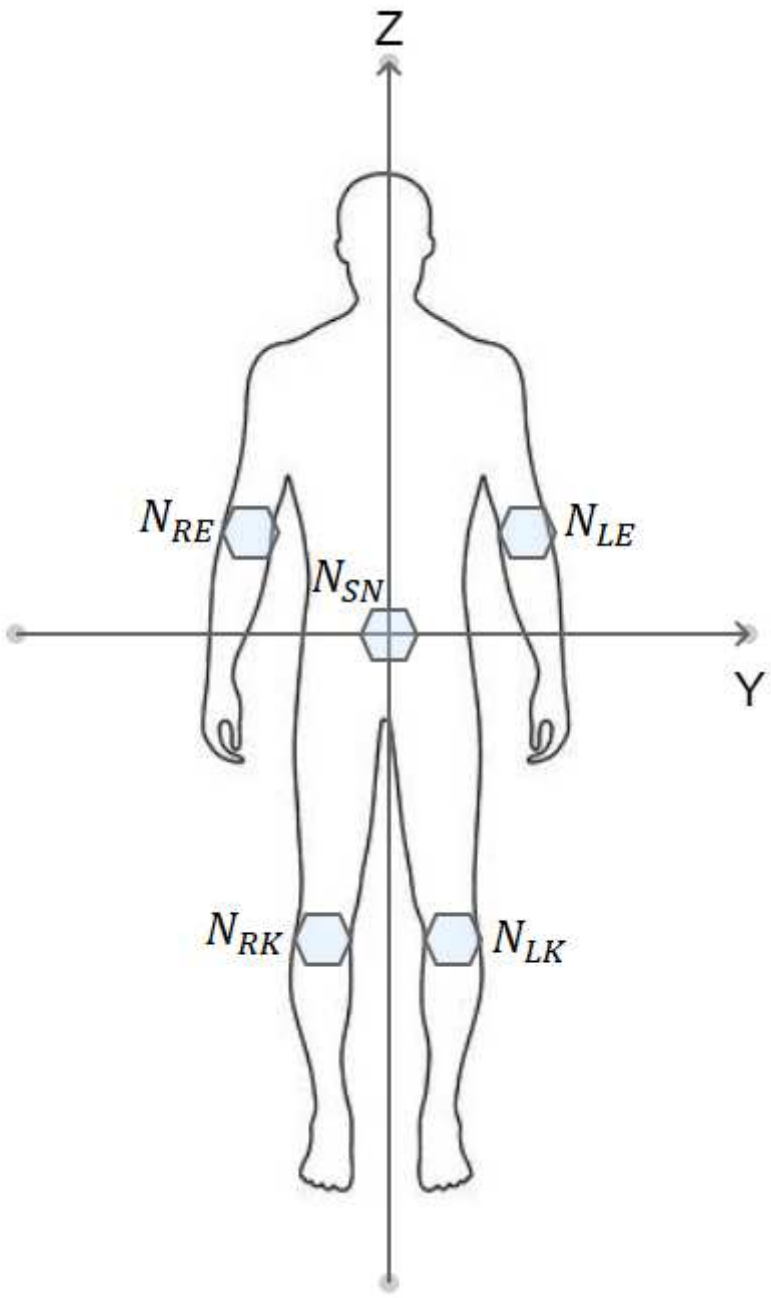

Figure 1

Node Placements

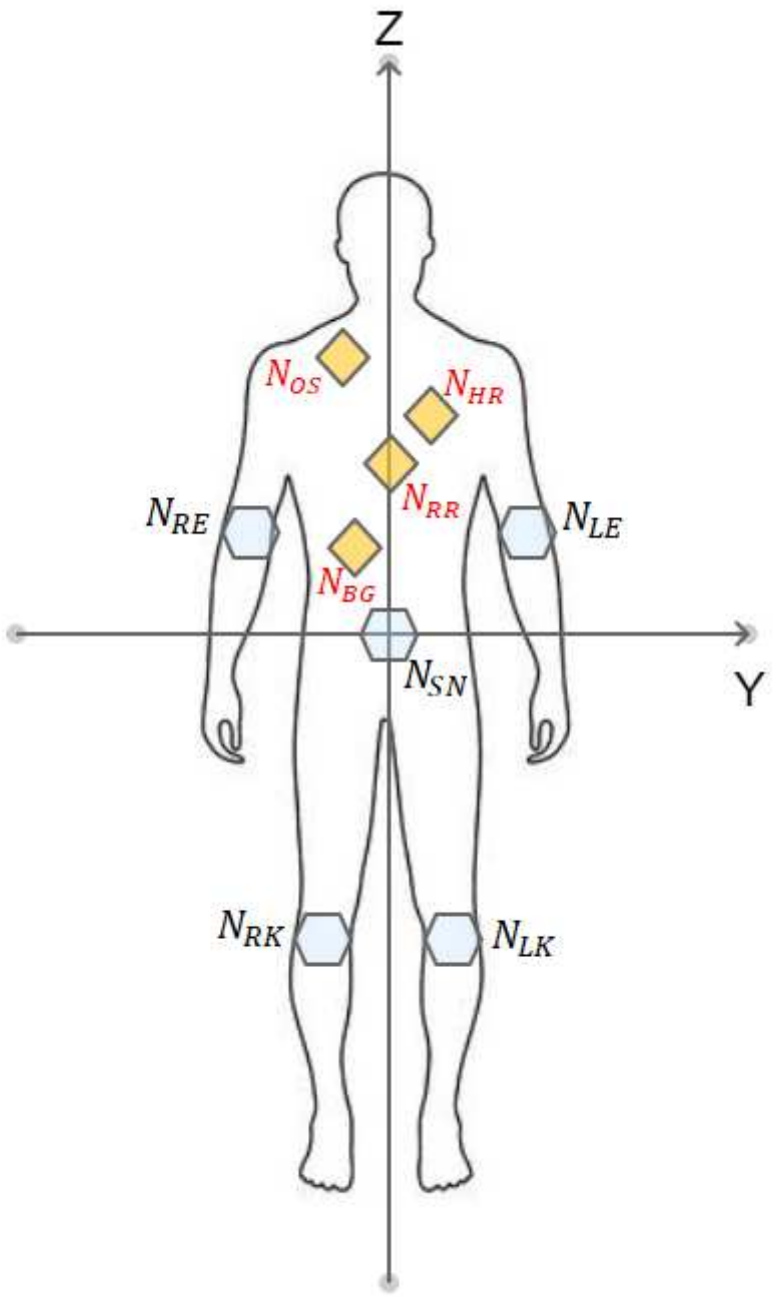

Figure 2

Implantable and Wearable node placements

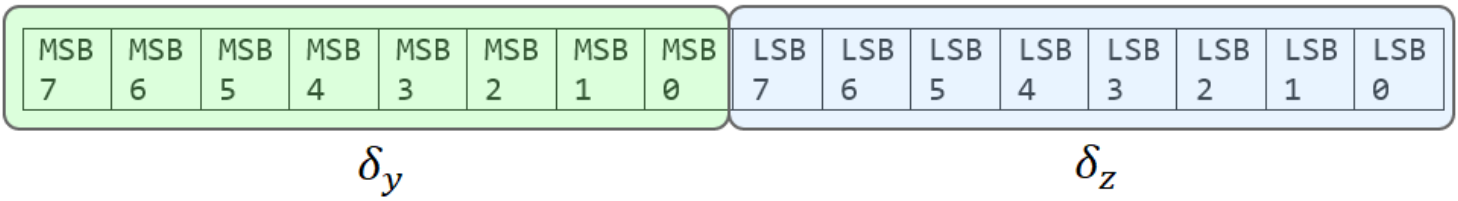

Figure 3

Implantable nodes' coordinate data

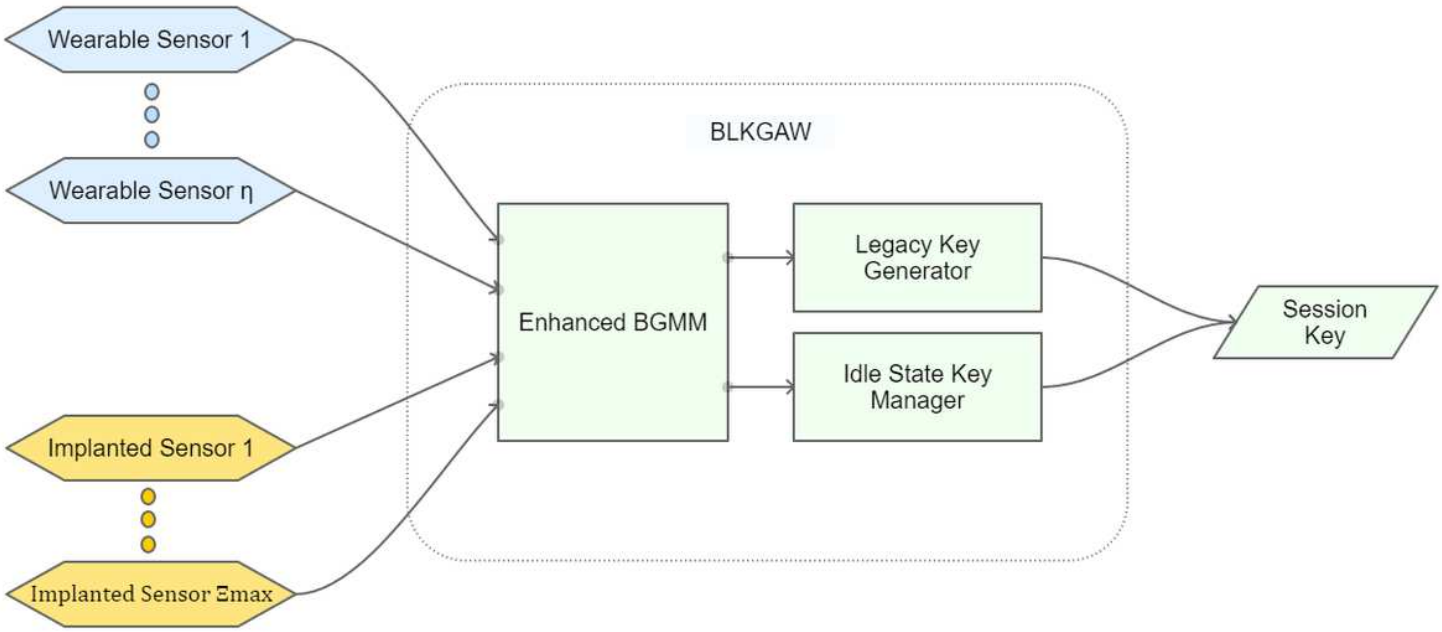

Figure 4

EBLKGAW Flow Diagram

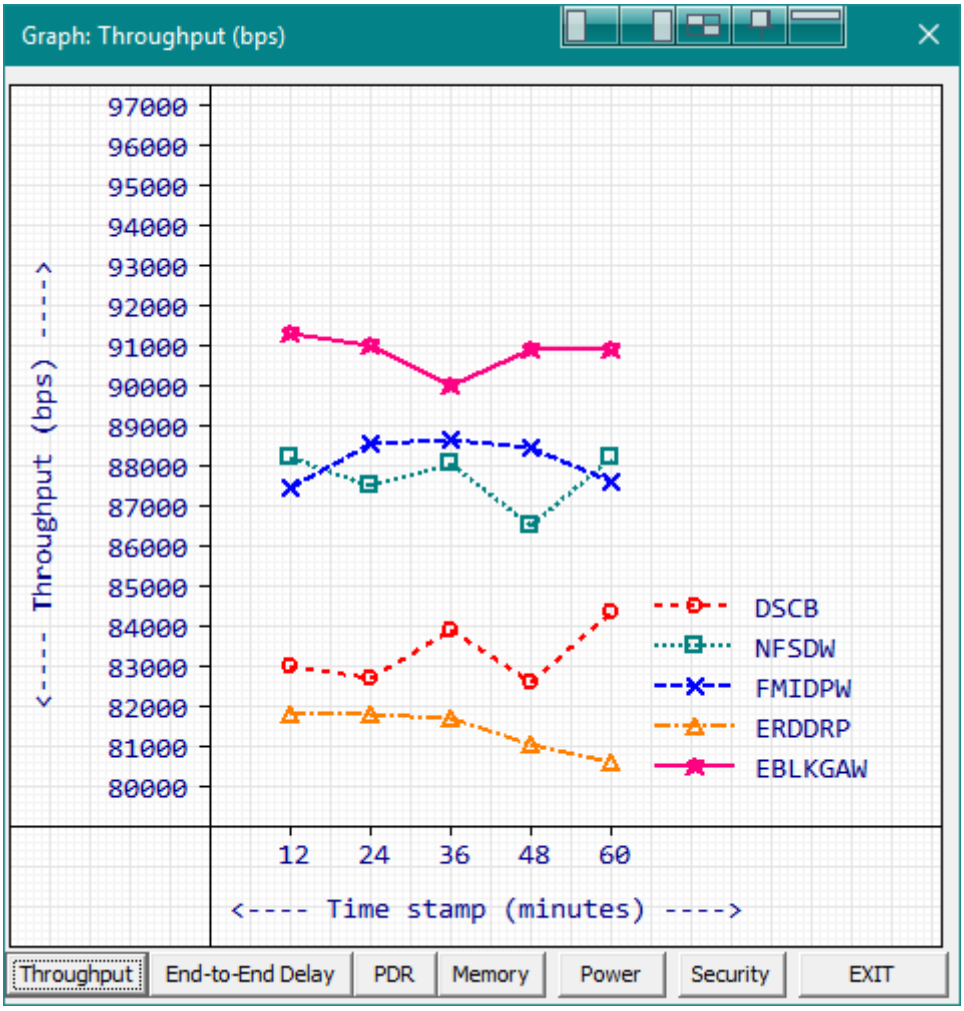

Figure 5

Throughput

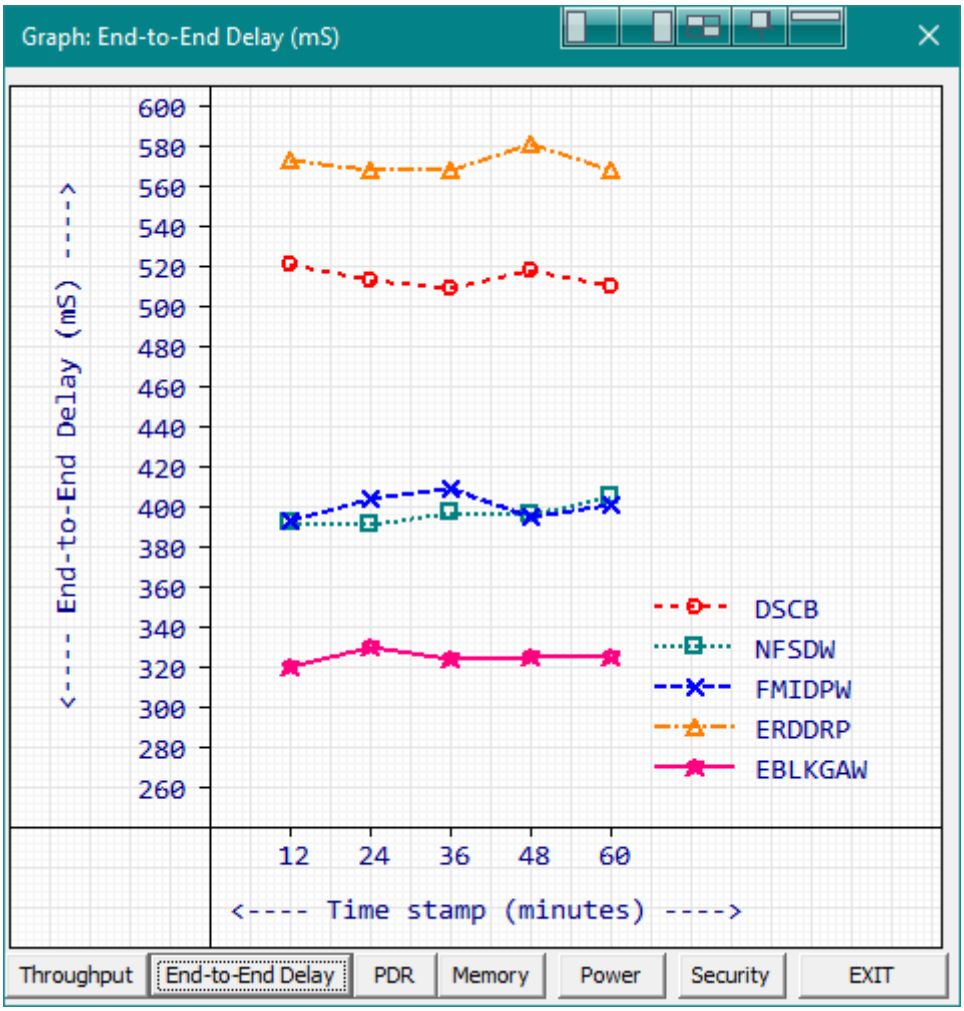

Figure 6

End-to-End Delay

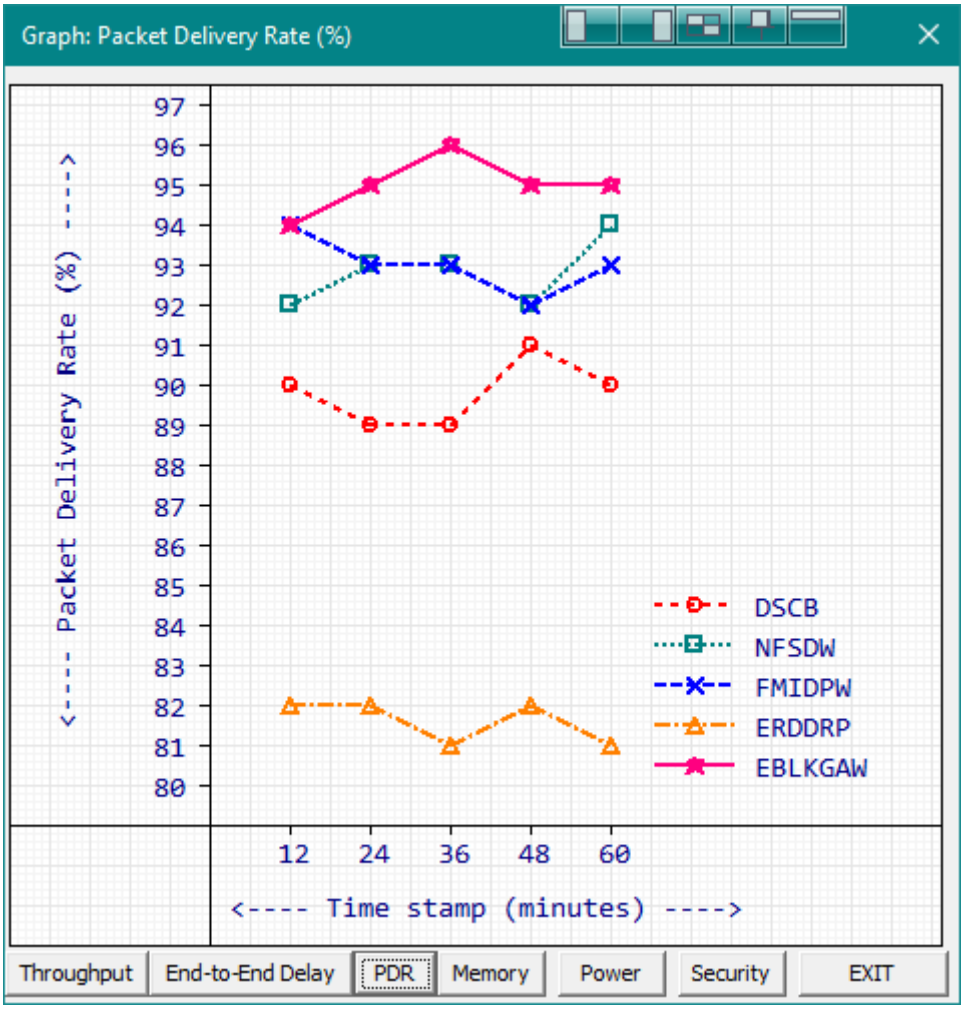

Figure 7

Packet Delivery Ratio

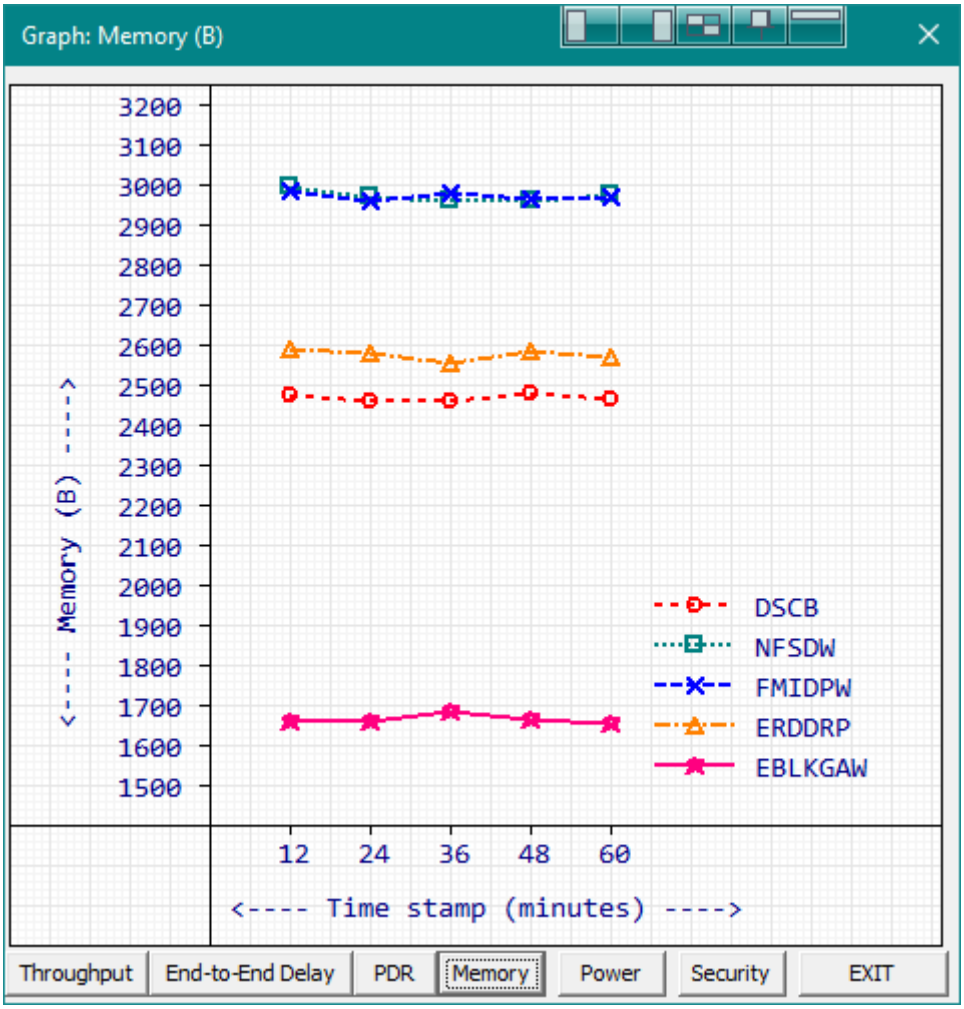

Figure 8

Memory Consumption

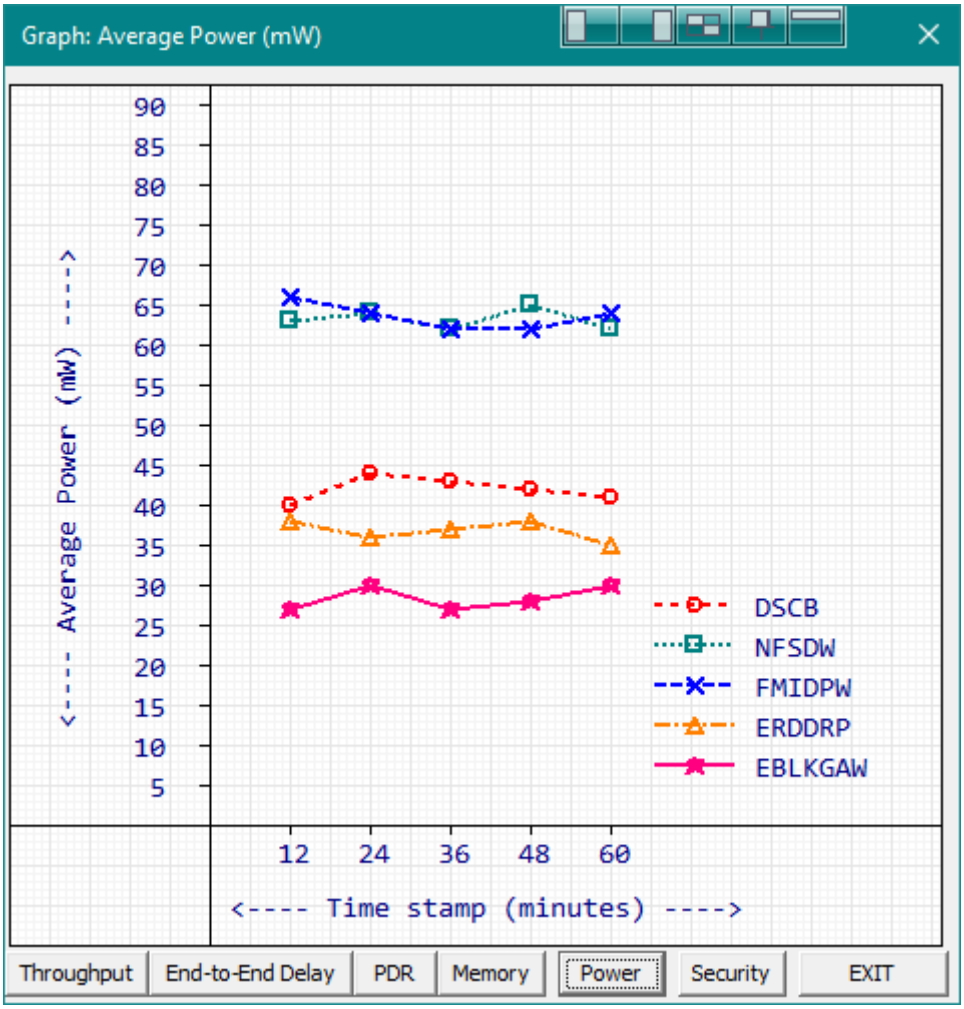

Figure 9

Power Consumption

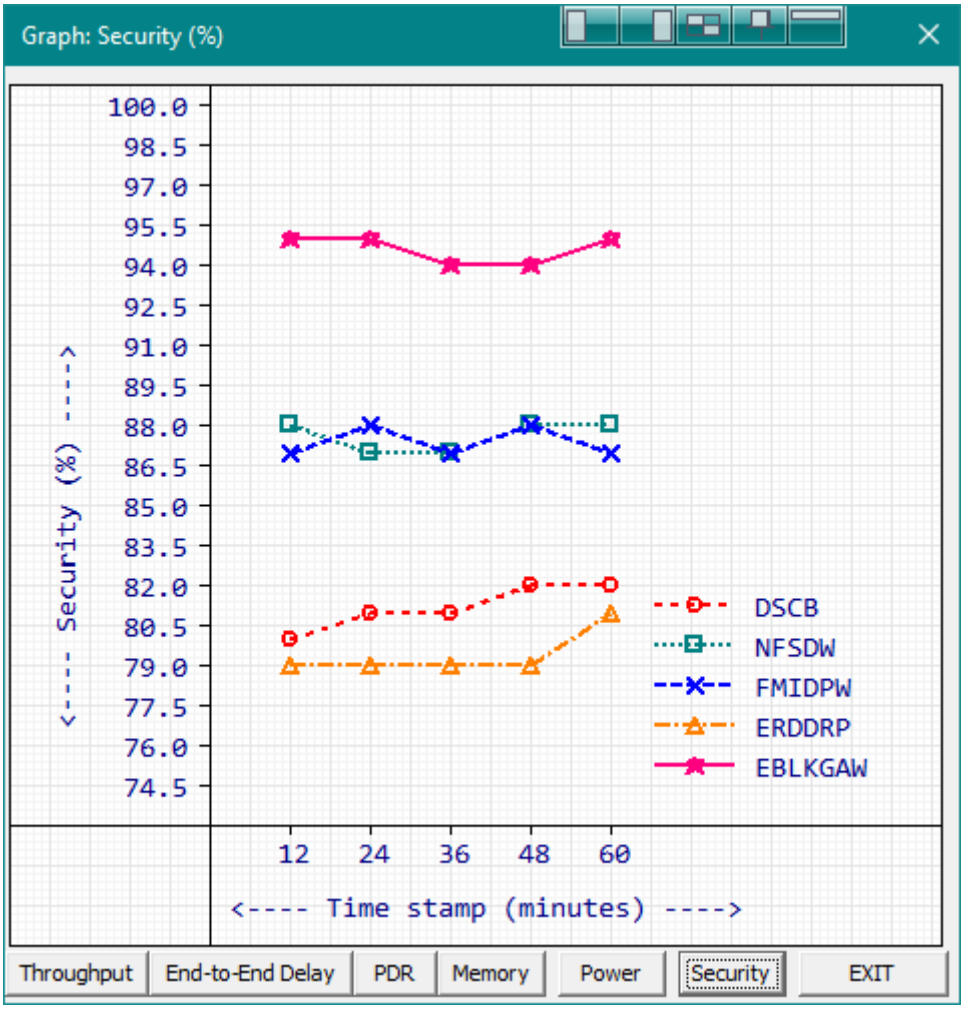

Figure 10

Security