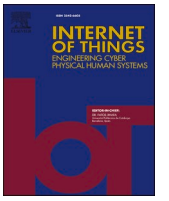
Internet of Things 22 (2023) 100717

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.sciencedirect.com/journal/internet-of-things



Research article

# A lightweight and secure sensing model for body area networks in the Internet of Things in biological warfare applications

Sobhan Esmaeili [a,*], Raziyeh Shamsi [b]

[a] Department of Computer and IT Engineering, Tehran North Branch, Islamic Azad University, Tehran, Iran
[b] Department of Mathematics, Evaz Center, Islamic Azad University, Evaz, Iran

ARTICLE INFO

*Keywords:*
Internet of Things
Body area networks
Lightweight and secure sensing
Energy
Biological warfare

ABSTRACT

In the era of communicational technologies, body area networks (BAN) provide useful and applicable devices for monitoring soldiers' health, of paramount importance for the governments and countries' security. However, BANs face two main challenges of security and energy, due to limitations in energy, memory, and process of the utilized sensors. Despite the developments of many solutions to tackle the stated challenges, the simultaneous consideration of energy and security has been overlooked in the majority of them. Besides, in some of the recommended solutions, the energy consumption is not optimum, resulting from discarding information content in data sampling. In addition, another group of the current methods is not practical, not guaranteeing security, given the high computational costs and the entropic inefficiency of encryption keys. Therefore, in the present study, a lightweight and secure sensing model is recommended for BANs, applicable in biological warfare. In the proposed model, the data are sampled according to their entropies, then compressed and encrypted simultaneously considering their sparsity levels, aiming at reducing energy consumption and boosting security. To synchronize two functions of compression and encryption, a measurement matrix, a type of sub-Gaussian matrix, is used. Furthermore, the biological data associated with the under-care soldier is encrypted using a key, guaranteeing the secure transfer of data to the smart healthcare center. In this process, the key is generated from the time interval calculated from the heart rate of the under-care soldier. The simulation data reveal that the proposed sensing model causes a reduction in energy consumption while providing security, compared to the previous methods.

## 1. Introduction

Nowadays, body area networks are utilized vastly in several applicational fields [1]. They have been designed to provide remote monitoring and treatment for smart healthcare systems as key infrastructure [2]. These networks have been hired in the military, thanks to their care-oriented approach as well as the importance of military health care to governments. With the outbreak of Covid-19, this application started to play a key and vital role in controlling and decreasing the epidemic. Covid-19 is a highly contagious virus, capable of spreading rapidly and infecting even physicians with slight negligence.

Regarding the origin of the Covid-19 virus, two theories have widely been published in the East and the West as follows [3]: In the first theory developed in the East, the United States was claimed to be responsible for the production and early development of the

* Corresponding author.
*E-mail address:* dr.sobhan.esmaeili@hotmail.com (S. Esmaeili).

https://doi.org/10.1016/j.iot.2023.100717

Available online 18 February 2023

Covid-19 virus. On the contrary, in the second theory stated in the West, the Wuhan China Biological Laboratory was recognized as the primary center of the Covid-19 virus epidemic. However, the common line in both theories is the attempt to create a biological weapon. These claims are groundless based on the available scientific evidence. Nevertheless, the expansion of such conspiracy theories reveals the continuing long and destructive trend of spreading distrust, biological warfare threats, bioterrorism, and the accidental leakage of deadly viruses from real and growing laboratories. In the meantime, BANs can be used as a technology addressing the threats caused by biological warfares. Nonetheless, the efficient application of BANs requires accurate administration, solving the challenges, and removing the obstacles associated with them [4–7].

Although a variety of solutions have been proposed to promote security and decrease energy consumption in BANs, the majority of them have failed to simultaneously address two stated challenges. High capacity of BANs in data generation leads to the insufficient observation of the large amounts of the produced data. The lack of attention to the informational content in data sampling causes the samples to have considerable unnecessary information less bits beside the bits with useful information. The mentioned obstacle results in an increase in both mean transmit delay and utilized bandwidth. Furthermore, it causes the energy consumed in each sensor and the whole BAN to increase. Likewise, despite the sensitive and vital nature of data, the applicable methods capable of guaranteeing security have not been proposed, making BANs challenging and limiting the use of smart healthcare systems. Thus, if a new approach can decrease energy consumption and increase the security level in BANs, it will win the attention and enthusiasm of the researchers interested in this field, ultimately leading to their widespread popularity.

In the model presented in the current study, data are sampled based on their entropies and then compressed and encrypted according to their sparsity level. Besides, to synchronize compression and encryption functions, a measurement matrix, a type of sub-Gaussian matrix is used. In addition, in the present model, the sampled data is aggregated in the sink node, in the encryption domain. Then, the aggregated data is encrypted with the normal key and sent to the smart care center. In this process, the normal key is generated from the time interval calculated from the heart rate of the under-care soldier, extracted using a piezoelectric sensor. In this model, the measurement matrix and the Message Authentication Code (MAC) mechanism are used to retrieve and pair the smart healthcare center's normal key. Next, the received data is decrypted utilizing the normal key of the smart care center and the biological data associated with the soldier under care is extracted. Here, the biological data is used to serve the soldier under care.

The present study is organized as follows: related works are presented in the 2nd section. Then, in the 3rd section, a brief explanation of the system's general model and its components including the network's schematic, radio model, and the assessment model used for the analysis of the proposed scheme is presented. The details of the proposed scheme are described in the 4th section. The 5th section outlines the used dataset, assumptions and settings of parameters in the simulation to evaluate the performance of the proposed sensing model. In the 6th section, the simulation results obtained in the 5th section are analyzed and assessed. Finally, the 7th section, while offering a conclusion, considers the future tasks.

## 2. Related works

The section of the bibliographic review is divided into two subsections: In the 1st subsection, the schemes proposed for security promotion in BANs are summarized. In the 2nd subsection, the optimization of energy consumption in BANs is considered, while evaluating the associated schemes.

### *2.1. The schemes proposed for promoting security*

In [8], a scheme based on selective encryption is proposed for effective data transmission in BANs. The recommended scheme includes essential components of "authentication" based on the Hidden Markov Model and a "mechanism" based on selective encryption using biometric information for distribution (shared key). This scheme has less energy consumption, thanks to a lower need for memory and computational power, compared to the conventional encryption peers. However, the energy consumption is not optimized in it, due to the use of the Nyquist sampling method and discarding information content, justifying the necessity of further works. Furthermore, in contrast to conventional encryption schemes, it shows low successful key-recovery percentages and low accuracy.

In [9], an encryption approach based on authentication is developed for BANs, in which sensing nodes compute the general keys via applying a Hash function to a desired number of the self-generated keys. The self-generated keys are saved in the memory of the sensors to be used, if necessary, to execute encryption or decryption of elliptic curve using Elliptic Curve Digital Signature Algorithm (ECDSA). In the method proposed in [9], energy consumption is not optimal due to the high computational overhead. Besides, the described method is not practical given high execution time and a need for vast saving space for saving the keys.

In the paper [10], a priority-aware lightweight secure sensing model is presented for body area networks with clinical health care applications in the Internet of things (PALWSS). In the presented model, the data is encrypted using compressed sensing theory beside simultaneous compression, ensuring their safe transmission to the smart care center with minimal delay and bandwidth consumption. However, the model presented in [10] does not perform well for non-sparse data or data with inconsiderable sparsity, having a high computational cost and a long reconstruction time. In addition, if the presented model does not use random methods to build the measurement matrix, it is overwhelming to build a complex measurement matrix and implement it in hardware.

### *2.2. The schemes proposed for the optimization of energy consumption*

In the paper [11], a priority-based energy efficient, delay and temperature-aware routing Algorithm (PEDTERRA) is presented for

**Table 1**
Comparison of evaluated routing algorithms in body area networks.

| Year | Research | Sampling method | | Algorithm type | | Advantages | | | | | | Compared |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Compressed sensing | Nyquist | Mathematical-based | Bio-inspired algorithm | Energy consumption | Bandwidth consumption | End-to-end delay | Security | Throughput | Network lifetime | |
| 2020 | [8] EEPRS | | ✓ | ✓ | | ↓ | | ↓ | | | | IM-SIMPLE |
| 2020 | [9] DE2-LB | | ✓ | ✓ | | ↓ | | ↓ | | ↑ | ↑ | DEEAC |
| 2020 | [10] PALWSS | ✓ | | ✓ | | ↓ | ↓ | ↓ | ✓ | | ↑ | DSCB |
| 2021 | [11] PEDTARA | | ✓ | | ✓ | ↓ | | ↓ | | ↑ | ↑ | TAEO |
| 2019 | [12] DSCB | | ✓ | ✓ | | ↓ | | ↓ | | ↑ | | IM-SIMPLE |
| 2021 | [13] AHP-TOPSIS | | ✓ | ✓ | | ↓ | | ↓ | | ↑ | ↑ | AHP |
| 2021 | [14] EERP-DPM | | ✓ | ✓ | | ↓ | | ↓ | | ↑ | ↑ | PCRP |
| 2020 | [15] DE2-LB | | ✓ | ✓ | | ↓ | | ↓ | | ↑ | ↑ | DEEAC |

vital data transmission in WBANs. PEDTERRA algorithm utilizes an advanced optimization algorithm called Multi-Object Genetic Chaotic Spider Monkey Optimization (MGCSMO) to select the forwarding node from the nodes with the lowest heat and optimal path based on energy, queue length, link reliability, and path loss. Besides, this algorithm benefits from incorporating the advantages of chaotic and genetic operators to improve the position-updating function of the enhanced spider monkey optimization algorithm. In the PEDTERRA algorithm, to do the prioritized routing, patient data is categorized into 3 groups: normal, on-demand, and emergency data. Then, these data are sent via the shortest optimal path routing, energy efficient emergency routing, and faster but priority-verified routing, respectively. Although the routing algorithm presented in the article [11] outperforms the traditional routing models presented for SDN-Based WBANs, the energy consumption, transmission delay, bandwidth consumption and the amount of heat generated in the sensor nodes of this routing model are not optimal due to overlooking the information content of the sent data and using the Nyquist sampling method, still needing further work. On the other hand, in this routing model, security, adverse environmental factors, and mobility issues in the practical environment have not been considered.

To increase network lifetime and power efficiency, the authors in [12] have proposed a routing algorithm titled Dual Sink approach using Clustering Body area network (DSCB). Two sink nodes, as fixed cluster heads, are employed in DSCB to aggregate the received data from the sensor nodes and transfer it to the nearest gateway. In the protocol, data is sent directly or is transmitted indirectly through a forwarder node, which is selected based on minimum nodal distance from the sink, maximum residual energy, and maximum transmission power. Various performance metrics such as residual energy, power efficiency, and end-to-end delay are measured for the DSCB scheme to compare its performance with DARE and Improved Sable Increased-throughput Multi-hop

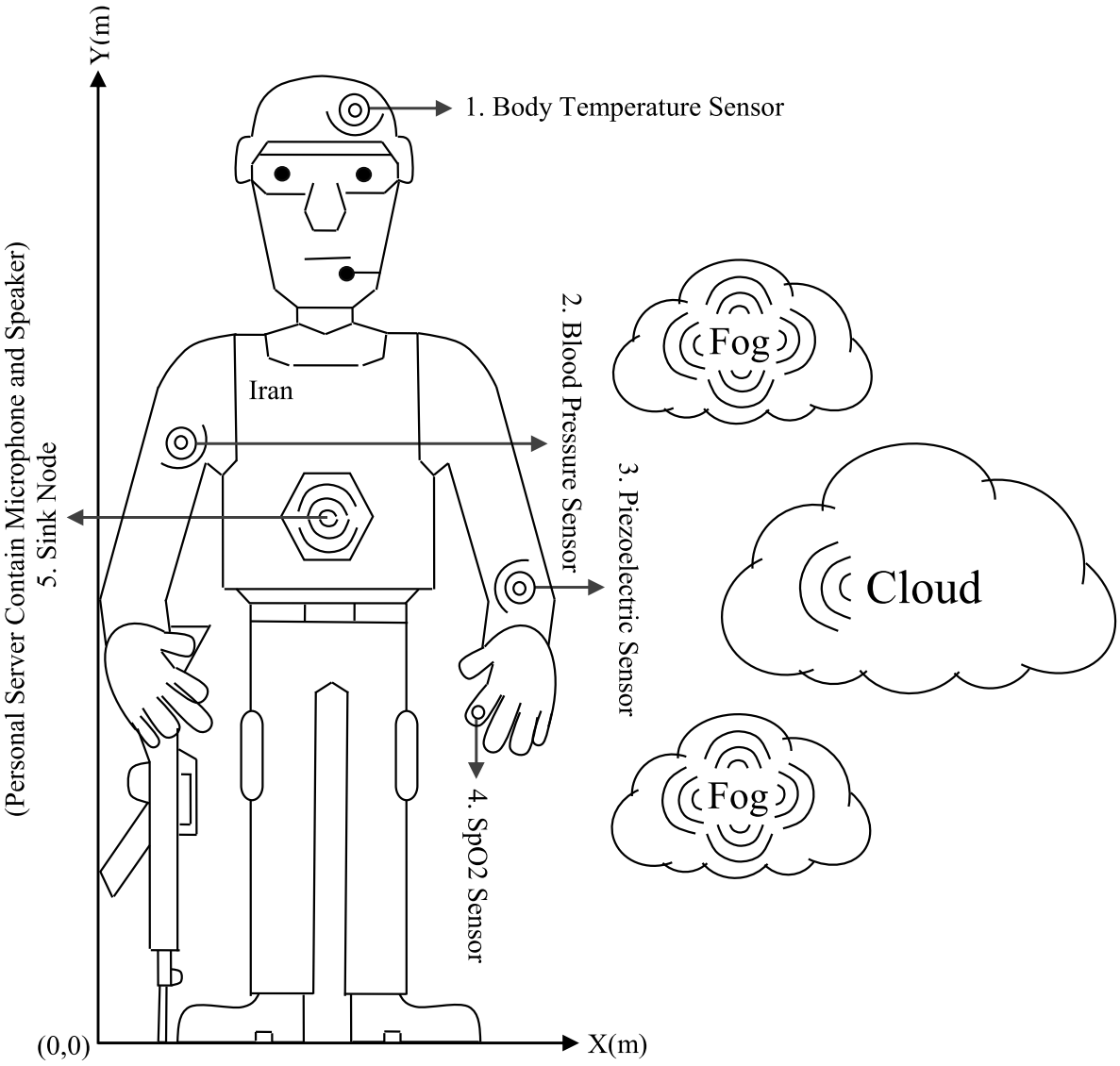



**Fig. 1.** The network topology in the proposed scheme.

Link-Efficient (IM-SIMPLE) routing protocols. MATLAB simulations show that the DSCB scheme provides better network stability, network lifetime, power efficiency, and end-to-end delay and outperforms the two other schemes. Again, despite the improvement in power consumption, security and privacy issues are not addressed by the DSCB method.

In the article [13], an energy-efficient relay node selection scheme is presented for sustainable wireless body area networks. In the presented scheme, a hybrid of the analytic hierarchical process (AHP) and a technique for order preference based on similarity to the ideal solution (TOPSIS) is utilized to choose the relay node. In this technic, nodes are ranked considering different parameters such as residual energy, traffic load, signal-to-noise ratio, and Euclidean distance, and then a first-ranked node is chosen as a relay node. However, according to the evaluated results, the selection of the relay node according to the Hybrid AHP-TOPSIS method increases both efficiency and stability of the network. Yet, the energy consumption in the plan presented in [13], due to disregarding the information content and Spatio-temporal correlation of the sensed data, and transferring a large amount of redundant data, is not optimal and still needs extra work.

In the paper [14], an energy-efficient routing protocol, using a dual prediction model, with health care application in the Internet of Things is presented. In this protocol, if the predictions match the readings or the sensed data values are beyond the lower and higher limits of the threshold value and are recognized as critical, the double prediction mechanism is used to reduce the energy consumption caused by data transmission from the sensor nodes to the medical server. The results of evaluating the performance of the proposed model confirm that the model presented in [14], in addition to reducing energy consumption and end-to-end delay, increases reliability and throughput.

In [15], an opportunistic energy-efficient routing algorithm with load balancing (DE2-LB) is introduced. In this method, network lifetime increases via the application of a load-balancing algorithm eliminating the effect of data-aggregation delay and routing loops. In the DE2-LB protocol, the nodes switch following the commands and computations between active and sleep status, aiming at decreasing energy consumption and increasing nodes' survival time. However, the protocol suffers from high overhead and transmission delay, despite its success in the reduction of energy consumption.

After reviewing the routing protocols of body area networks of the research area, in Table 1, we have compared them in terms of the sampling method, algorithm type and advantages. In this table, (↑) and (↓) refer to increase and decrease, respectively.

## 3. System model

In this section, we introduce the model of the system and its components, including network topology, radio model, and sensing model, which are used to analyze the proposed scheme.

### 3.1. Network topology

To investigate the impact of the proposed sensing model on enhancing the security and efficiency of BANs, a simple network topology is introduced, on which the performance of the proposed scheme is evaluated. In this topology, 4 sensor nodes are used to monitor the physiological data of the body, and 1 sink node is used to monitor and aggregate the sensed data by the sensor nodes. The sensor nodes with the same computational power equipped with 0.3 J initial energy are fixed at particular locations of the body and transfer their data to the sink node using a single-hop direct communication. Moreover, the sink node with higher energy and processing resources than sensor nodes is located in the center of the body and the lumbar region. It dynamically accesses sensor node information including the amount of remaining energy, the identity, location, and distance of each sensor node. Fig. 1 depicts the described schematic.

Besides, Table 2 represents the type and location of nodes in the topology shown in Fig. 1.

### 3.2. Radio model

The radio model describes the amount of energy consumed by the electronic system of sensor nodes and sink nodes used in the soldier's body. In our proposed scheme, the first-order radio model and the single-chip low-power transceiver of Nordic nRF2401 are utilized. The used transceiver operates in 2.4 GHz bandwidth, and its radio parameters are given in Table 3. In this model, the energy consumption of the transceiver of each sensor implanted in the body of a male soldier with 182 cm height, 70 kg weight, 79 cm waist circumference, and 3.20 dB Body Path Loss (BPL), and located with a distance d from another sensor or sink node for transmuting and receiving k data bits in a single-hop communication is given by Eqs. (1) and (2) [15,16].

**Table 2**
The type and coordinates of the nodes in the described network topology.

| Node number | Description | Width coordinate (m) | Length coordinate (m) |
|---|---|---|---|
| 1 | Body temperature Sensor | 0.22 | 1.74 |
| 2 | Blood Pressure Sensor | 0.06 | 1.12 |
| 3 | Piezoelectric Sensor | 0.36 | 0.85 |
| 4 | Blood oxygen level Sensor | 0.33 | 0.61 |
| 5 | Sink Node | 0.20 | 0.97 |

**Table 3**
Radio parameters of Chipcon CC2420 transceiver used in the proposed sensing model.

| Parameter | Value |
|---|---|
| DC Current (TX) | 10.5 mA |
| DC Current (RX) | 18 mA |
| Supply Voltage (Min) | 1.9 V |
| $E_{tx-elec}$ | 16.7 nJ/bit |
| $E_{rx-elec}$ | 36.1 nJ/bit |
| $E_{amp}$ | 1.97 nJ/bit/$m^2$ |
| $BPL$ | 3.20 dB |

$$E_{tx-i}(k,d,BPL) = (E_{tx-elec} \times k) + \left(E_{amp} \times k \times BPL \times d^{BPL}\right) \quad (1)$$

where $E_{tx-i}(k, d, BPL)$ is the amount of energy consumed in direct communication (single hop) to send k bits of data from the transmitter of the $i^{th}$ sensor to a receiver located at distance d in body transmission media with an energy loss coefficient of BPL. Moreover, $E_{tx\text{-}elec\text{-}i}$ is the amount of energy consumed by the electronic circuit of the $i^{th}$ transmitter sensor for transmitting one bit while $E_{amp\text{-}i}$ is the amount of energy consumed by the circuit of the amplifier circuit of the $i^{th}$ sensor for transmitting one bit.

$$E_{rx-i}(k) = (E_{rx-elec-i} \times k) \quad (2)$$

where $E_{rx\text{-}i}(k)$ is the amount of energy consumed by the receiver of the $i^{th}$ sensor in direct communication (single hop) to receive k bits of data from the transmitter. Besides, $E_{rx\text{-}elec\text{-}i}$ is the amount of energy consumed by the electronic circuit of the receiver of the $i^{th}$ sensor for receiving one bit. Here, d means the distance between the sensor node and the sink node, calculated according to Eq. (3). In addition, $X_{SRC}$ and $X_{DST}$ are the width coordinate of the source and destination nodes, respectively, and $Y_{SRC}$ and $Y_{DST}$ denote length coordinate of the source and destination nodes, respectively.

$$d = \sqrt{(X_{SRC} - X_{DST})^2 + (Y_{SRC} - Y_{DST})^2} \quad (3)$$

### 3.3. Sensing model

In the proposed sensing model, the energy consumed in a sensor node can be attributed to two processes of sensing and radio communication. Section 3.2 discusses the radio model and the calculation of the energy caused by the communication. In this section, the sensing model is outlined, describing the amount of energy consumed due to the sensing data in the proposed sensing model. The energy consumed due to the sensing contains the energy consumed for sensing the data through the secure and lightweight sensing method as well as the energy consumed in the background, calculated according to Eq. (4).

$$E_{Sensing} = E_{LWS-Sensing} + E_{Background} \quad (4)$$

where $E_{Sensing}$ is the energy consumed due to the sensing process, $E_{LWS-Sensing}$ is the energy consumed for sensing data by the lightweight secure sensing method, and $E_{Background}$ is the energy consumed in the background. Here, forasmuch as, in the secure and lightweight sensing, after sensing the data normally, the data is sensed according to the information content of the data and M random mapping operations of the analog signal instead of N measurement operations. An n-dimensional signal, using a measurement matrix and M operations of measurement is sampled. Therefore, the energy consumed for sensing the data through secure and lightweight sensing is an aggregation of energy consumed by normal sensing, N operations of reading, M operations of writing, MN operations of multiplication, (MN—N) operations of addition, and computational cost, calculated by Eq. (5).

$$E_{LWS-Sensing} = E_{Normal-Sensing} + NE_{Mrd} + MNE_{Mul} + (MN - N)E_{Add} + ME_{Mwr} \quad (5)$$

where N is the number of samples; $E_{Mrd}$ is the energy required to read a bit of data from memory; M is the number of measurements; $E_{Mul}$ is the energy required for a multiplication operation; $E_{Add}$ is the energy needed for a sum operation; $E_{Mwr}$ is the necessary energy to write a bit of data in memory; and $E_{Normal-Sensing}$ is the energy consumed for the normal sense of data, calculated according to Eq. (6).

$$E_{Normal-Sensing} = N \times P_{Acquisition} \times T_{Instruction-Execution} \quad (6)$$

where E_(Normal-Sensing) is the energy consumed for the normal sense of N-bit data, N represents the number of samples and P $_{acquisition}$ is the power consumed for sensing data by both processor and the sensor circuit. P $_{acquisition}$ is 66.3 mW for the AquisGrain sensor [17]. In addition, $T_{Instruction\text{-}Execution}$ is the time required to execute an instruction. Here, since the operating frequency of the Atmel Atmega 128 L processor is equal to 7.4 Mhz, capable of executing 7.4 machine instructions per second, the execution time of each instruction is calculated based on Eq. (7). Note that in the Atmel Atmega 128 L processor, the majority of instructions are executed in one clock cycle of the processor [18] and the processor access to different peripherals does not take a longer time than other instructions [18].

$$T_{Instruction-Execution} = \frac{1}{F_{Instruction-Execution}} \tag{7}$$

where $T_{Instruction-Execution}$ is the time required to execute an instruction, and $F_{Instruction-Execution}$ is the frequency of instruction execution. On the other hand, in Eq. (4), the energy consumed in the background is the energy consumed by different sources required for the platform operation. It is almost identical in different signal processing techniques and calculated according to Eq. (8).

$$E_{Background} = P_{Background} \times I_{LWS} \times T_{Instruction-Execution} \tag{8}$$

where $E_{Background}$ is the background consumed energy; $P_{Background}$ is CPU power consumed in the inactive mode; $T_{Instruction-Execution}$ means the time required to execute an instruction; and $I_{LWS}$ represents the number of instructions required to sense the data using the lightweight secure sensing method, calculated as follows:

$$I_{LWS} = N + MN + (MN - N) + M \tag{9}$$

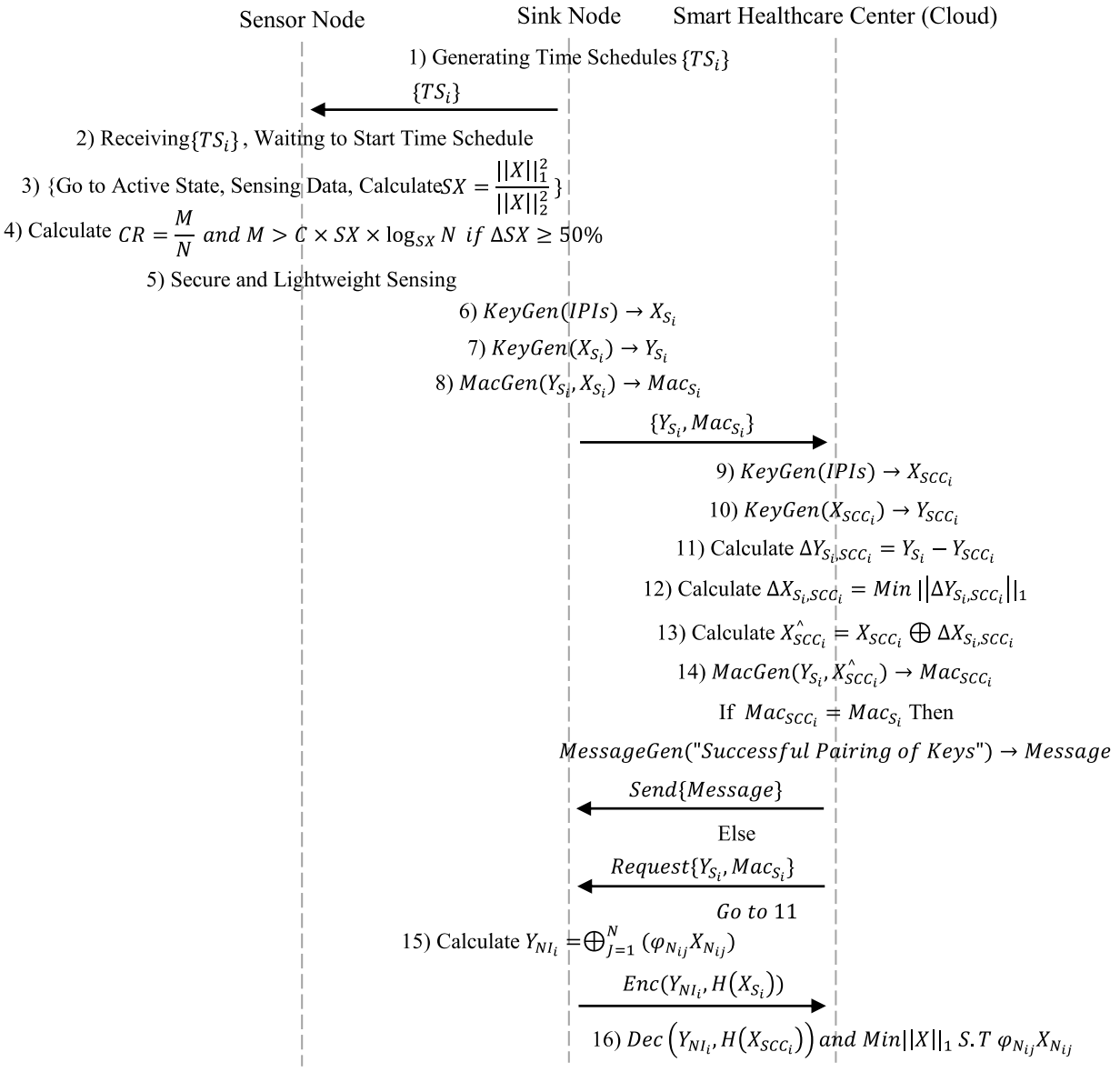



**Fig. 2.** Steps of the proposed sensing model.

## 4. Proposed scheme

To provide a solution to the problem described in Section 1, this paper proposes a scheme called a lightweight and secure sensing model for BANs in the Internet of Things in biological warfare applications, discussed in more detail in the following. Fig. 2 shows the steps of this design.

### 4.1. Generating and allocating time schedules

In the proposed scheme, to decrease the energy consumption of the nodes as well as the unpredictable effect of wireless communication between them, the channel mutation-based time slice mechanism is used. The channel mutation-based time slice mechanism can be considered as a combination of the multiple-access mechanism with time division, and the multiple-access mechanism with frequency division. The reason is that it employs variation in time and frequency to provide a reliable access control solution. In this mechanism, each sensor node sends its schedule to the sink node. After investigating and removing the interference caused by the overlapping of the time schedules with each other, the sink node informs each node of the final schedule and the activity interval related to itself and other nodes. Moreover, in this mechanism, by changing the frequency of the communication carrier for each transmission, the effect of multipath fading is be overcome. Fig. 3 describes the channel mutation-based time slice access control mechanism.

### 4.2. Receiving a schedule and waiting to start the activity intervals

At this step, each node, after receiving its schedule, waits until the beginning of its interval activity in a sleep state. Then, with the start of its relevant activity interval, it senses data.

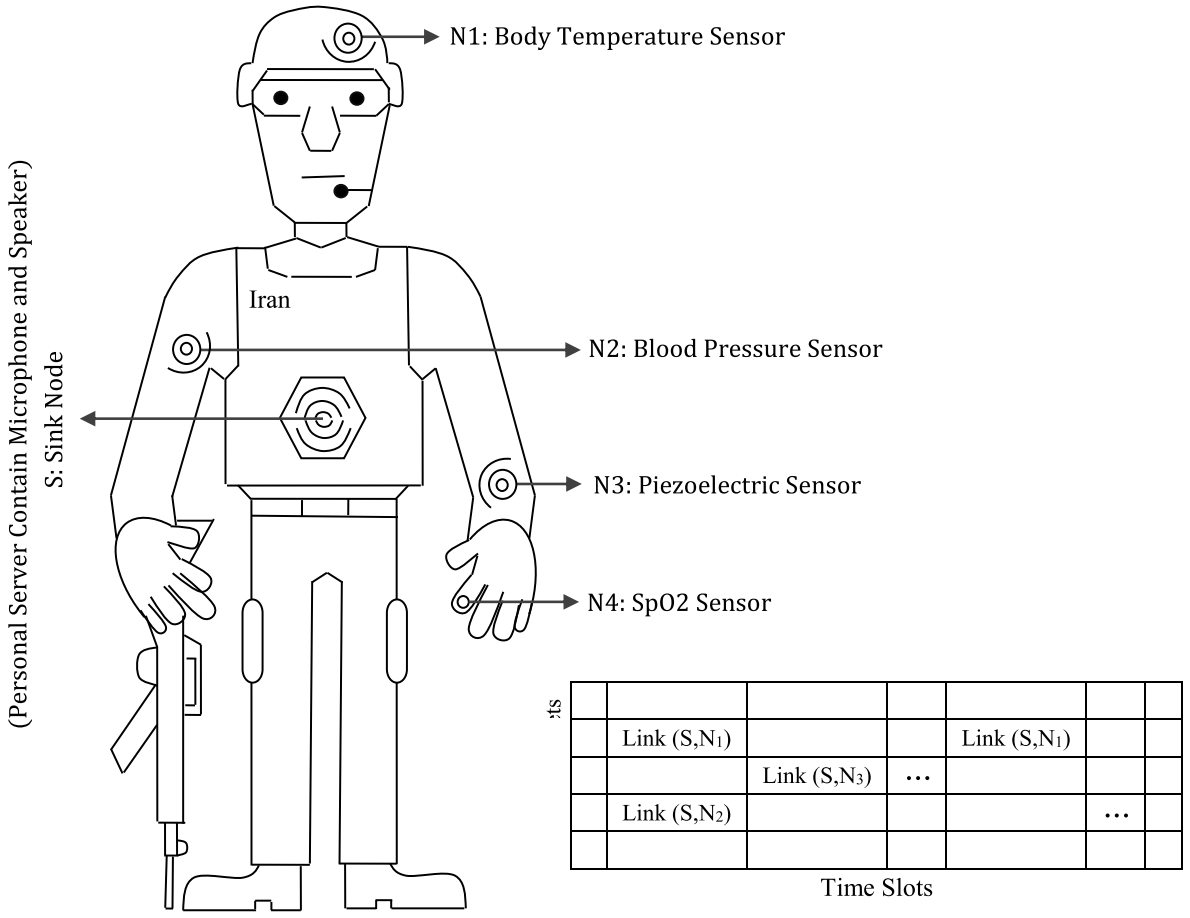



**Fig. 3.** The mechanism for allocating the activity intervals in the proposed scheme.

### 4.3. Sensing data and calculating the sparsity level of the sensed data

In this step, when the activity interval starts, the sensor node switches from sleep to active state and continuously computes the sparsity level of the sensed data by Eq. (10) [9].

$$SX = \frac{||X||_1^2}{||X||_2^2} \tag{10}$$

where $SX$ is the sparsity level of the sensed data; $||X||_1^2$ is the squared one-norm of the sensed data vector $X$, the summation of the absolute value of the elements of $X$; and $||X||_2^2$ is the squared two-norm of $X$, obtained by the Euclidean norm equation.

### 4.4. Calculation of compression coefficient according to the amount of sparsity level of sensed data

Obtaining up-to-date information on the sensed data helps us adjust and select the optimal value of the compression ratio. Hence, according to Eq. (11), when the changes of sparsity level of sensed data are equal to or over 50%, the sensor node uses the number of calculated measurements to update the compression ratio [16]. When the changes of the sparsity level are less than 50% and have no considerable time variation, the default compression ratio is used. Here, the number of accomplished measurements defining the compression ratio depends on the sparsity level of the sensed data.

$$\begin{cases} R = CR_{Default} \;\; if \;\; 0 \le SX < 50\% \\ CR = \dfrac{M}{N} \;\; and \;\; M > C \times SX \times \log_{10}\dfrac{N}{SX} \;\; if \;\; \Delta \mathrm{SX} \ge 50\% \end{cases} \tag{11}$$

where $CR$ is the compression ratio; $CR_{Default}$ is the default compression ratio; $\Delta SX$ is the changes in the level of the sensed data sparsity; $M$ is the number of measurements; $N$ is the number of samples; and $C$ is a constant, whose value is set to 2 for a Gaussian measurement matrix.

### 4.5. Secure and lightweight sensing

The secure and lightweight sensing provides a way to securely retrieve a sparsity signal at a large scale from a small number of measurements. Upon secure and lightweight sensing, data reduction is carried out using non-adaptive measurements in a way that the approximation error in data reconstruction becomes proportional to the approximation error in data reduction in an adaptive manner. The secure and lightweight sensing can be expressed using Eq. (12). In lightweight and secure sensing, unlike the conventional method, where the sensed data are sampled, the data are measured. The measure is a linear combination of several samples. In lightweight and secure sensing, the SX number of the non-zero coefficient is coded indirectly by M operations of signal measurement ($M < N$), each one of which is equal to the mapping of signal on the M number of measurement vector. In this process, without extracting data from all sensors, one can achieve the important coefficients having most of the information and sample the sensed data with helpful information while ignoring the rest of the sensed useless data. Thus, upon the secure and lightweight sensing, the data are sampled based on their information rate rather than the Nyquist rate. Thus, the number of measurements required for data retrieval is far less than that of samples required for data retrieval in the traditional method based on the Nyquist theorem [19].

$$Min\left|\left|X_{N_{ij}}\right|\right|_1 \;\; S.T \; Y_{N_{ij}}[M \times \; 1] = \varphi_{N_{ij}}[M \times N] \times X_{N_{ij}}[N \times \; 1] \tag{12}$$

where $Y_{N_{ij}}$ represents the data vector sensed by sensor node j in the $i^{th}$ round after secure and lightweight sensing; $\varphi_{N_{ij}}$ means the measurement matrix generated by sensor node j in the $i^{th}$ round; and $X_{N_{ij}}$ is the vector of sensed data by sensor node j in the $i^{th}$ round. Moreover, in this step, by considering special conditions in the design of the measurement matrix and smartly choosing the elements of the measurement matrix, it is also possible to secure the sensed data while improving the measurement and making data retrieving possible. Here, to keep confidential the sensed data and reduce the total number of encryptions and consequently reduce the computations, a sparse matrix is used, including the set of permitted keys of the sensor, sink nodes, and cloud. This sparse matrix which is somehow a sub-Gaussian matrix is created by Eq. (13), and its set of keys is generated by a random seed, owned by the sensor nodes, sink node, and cloud.

$$\begin{cases} P\left(\varphi_{N_{ij}} = k\right) = \dfrac{1}{2SX_{N_i}} \\ P\left(\varphi_{N_{ij}} = 0\right) = 1 - \dfrac{1}{2SX_{N_i}} \end{cases} \tag{13}$$

where $\varphi_{N_{ij}}$ is the measurement matrix generated by sensor node No. j in the $i^{th}$ round and $SX_{N_i}$ represents the amount of sparsity level of the sensed data by sensor node No. j in the $i^{th}$ round. Here, when the value of $\varphi_{N_{ij}}$ is zero, no encryption occurs, and when the value of $\varphi_{N_{ij}}$ is equal to k, the sensor node No. j projects its $i^{th}$ round sensed data over its related j column of the $i^{th}$ round measurement matrix, to obtain its measurement result. The measurement result is encryption-domain data based on the $i^{th}$ round measurement matrix, and

the intruder cannot read it. To recover the encryption-domain data, the receiver or allowed entity should have the $i^{th}$ round measurement matrix. In the end, the encryption-domain data are sent to the sink node for encryption-domain aggregation.

### 4.6. Generating the normal key of the sink node using the IPIs measured from the heart rate

In the proposed scheme, a piezoelectric sensor is employed to extract the heart signal and calculate the Interpulse Interval (IPIs). The piezoelectric sensor is an electromechanical system responding to applied forces and mechanical strains and then converting them into electrical signals. It contains a very high natural frequency, linear over a wide amplitude range. Besides, this sensor is not sensitive to electromagnetic fields and radiation and can measure in harsh conditions. The piezoelectric sensor is self-excited and does not require any power supply to operate. Furthermore, the piezoelectric sensor is smaller, lighter, more efficient, and cheaper than the ECG sensor. It can sense the vibrations generated by the heart without needing skin contact if there is skin sensitivity in the person. Meanwhile, due to the low SNR of the heart signal extracted by the piezoelectric sensor, the key generation rate is around 2.9 bit/IPI. This rate is 50% better than the key generation rate of methods by which the heart signal is extracted using the ECG sensor [17]. After extracting the heart signal using the piezoelectric sensor, since the output signal contains significant random noise, we pass the extracted signal through a Savitzky Golay filter. It is a digital filter employed to increase the precision of the data without distorting the signal tendency. This is performed in a process called convolution by fitting successive subsets of adjacent data points with a low degree polynomial using the method of linear least squares. The use of the Savitzky Golay filter allows us to decrease the noise effect without changing the location of the R peaks in the signal and calculate IPI values accurately. This process has a great impact on increasing the entropy of the extracted IPIs and the quality of the key generated from the IPIs. Fig. 4 exhibits the heart signal extracted using the piezoelectric sensor and optimized with the Savitzky Golay filter.

After extracting the ECG signal and passing it through the Savitzky Golay filter, the R peaks of the QRS wave are extracted by applying the script written on the ECG signal and obtain the timestamp of each R peak. Then, using Eq. (14), the time interval between each pair of consecutive R peaks of the ECG signal is calculated, called IPI in short.

$$IPI_{i,i+1} = T_{R_{i+1}} - T_{R_i} \tag{14}$$

where $IPI_{i,i+1}$ denotes the time difference between two successive peaks of $R_i$ and $R_{i+1}$, $T_{R_i}$means the timestamp of peak $R_i$, and $T_{R_{i+1}}$refers to the timestamp of peak $R_{i+1}$. Fig. 5 shows how to calculate the IPI from two successive peaks of the ECG signal, and the IPIs read by the piezoelectric sensor.

Here, to use IPIs calculated of the heart rate as a secret source and generate a normal key, the extracted IPIs must meet two conditions of randomness and proximity [18]. Moreover, the symmetric key must have a uniform distribution, and it should be generated independently to ensure security in the intended applications. The entropy value of each bit of the IPIs calculated from the ECG signal must be high enough to meet the randomness condition. For this reason, after calculating the IPIs from the ECG signal, the entropy of each bit of the calculated IPIs is calculated. Then, a threshold of 0.80 is set for the entropy of each bit of the IPIs to ensure the

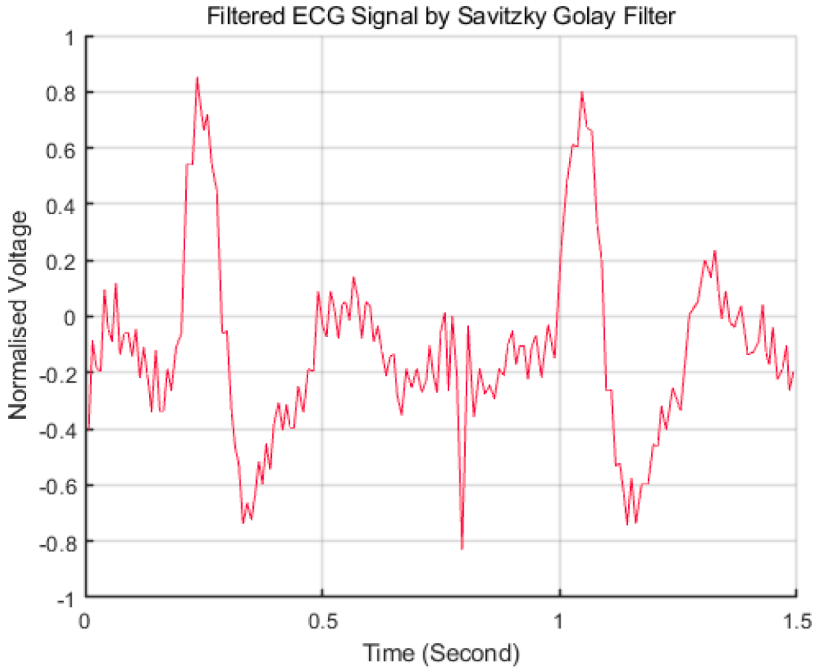



**Fig. 4.** ECG signal extracted from the piezoelectric sensor and filtered by the Savitzky Golay filter.

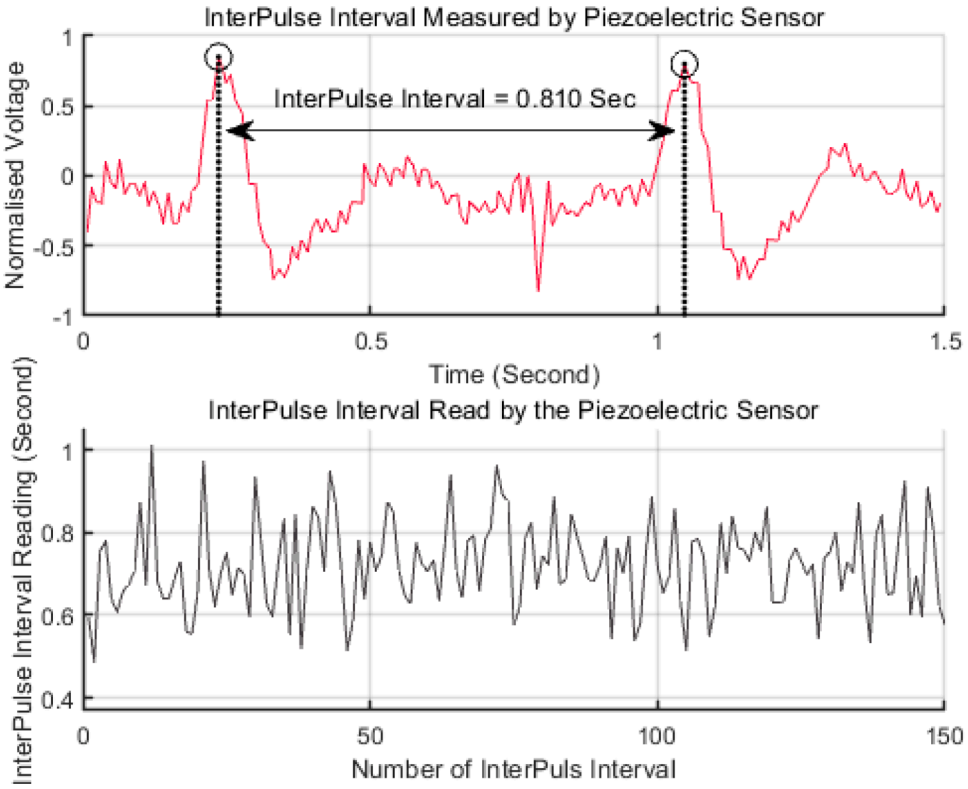



**Fig. 5.** Calculating the IPI of the ECG signal extracted from the heart and the IPIs read by the piezoelectric sensor.

quality of the generated key from the IPIs. On the other hand, to meet the proximity condition, the mismatch rate of each bit of the calculated IPIs must be low enough. In this regard, we consider a mismatch rate of more than 25% unqualified to generate a key with the quality. Table 4 lists the entropy and mismatch rate of the IPI bits calculated from the ECG signal extracted from the heart rate using the piezoelectric sensor.

As seen in Table 4, the entropy of the 7th bit of the calculated IPIs is zero. Thus, the entropy of the 7th bit of the calculated IPIs must be increased before using for generating the key. On the other hand, in the proposed method, to ensure the uniform distribution of the generated key, after extracting the heart signal and calculating the IPIs, the type of distribution of calculated IPIs was examined using the descriptive method. In this technic, the histogram, normal probability, and two criteria of Kurtosis coefficient and Skewness coefficient are examined.

Here, the data have a uniform distribution in the 5 following states: A) the value of the skewness coefficient is positive, and the mean of the data in the histogram is skewed to the left. B) the value of the skewness coefficient is negative and the mean of the data in the histogram is skewed to the right. C) the data in the normal probability diagram deviate significantly from the straight line. D) The value of the kurtosis coefficient is positive, the data scatter is low around the mean, and the drawn histogram diagram is tall. E), the value of the kurtosis coefficient is negative, the data scatter is high around the mean, and the drawn histogram diagram is lying down. But if, both the skewness and kurtosis coefficients are zero or with a slight error value close to zero or their histograms are bell-shaped and symmetrical, the distribution of IPIs is normal. Fig. 6(a) and (b) show the normal probability diagram and the histogram diagram obtained for the IPIs calculated from the heart signal.

As seen in Fig. 6(a) and (b), the IPIs calculated from the ECG signal fluctuate around a moderate value and follow a normal

**Table 4**
Entropy and mismatch rate of IPI bits calculated from ECG signal.

| Mismatch rate (Percentage) | Entropy (Bits) | Bit number |
|---|---|---|
| 48.54 | 0.999535 | 0 |
| 55.18 | 0.999931 | 1 |
| 49.80 | 1 | 2 |
| 51.17 | 0.999006 | 3 |
| 48.44 | 0.998544 | 4 |
| 50 | 0.99977 | 5 |
| 45.51 | 0.940522 | 6 |
| 0 | 0 | 7 |

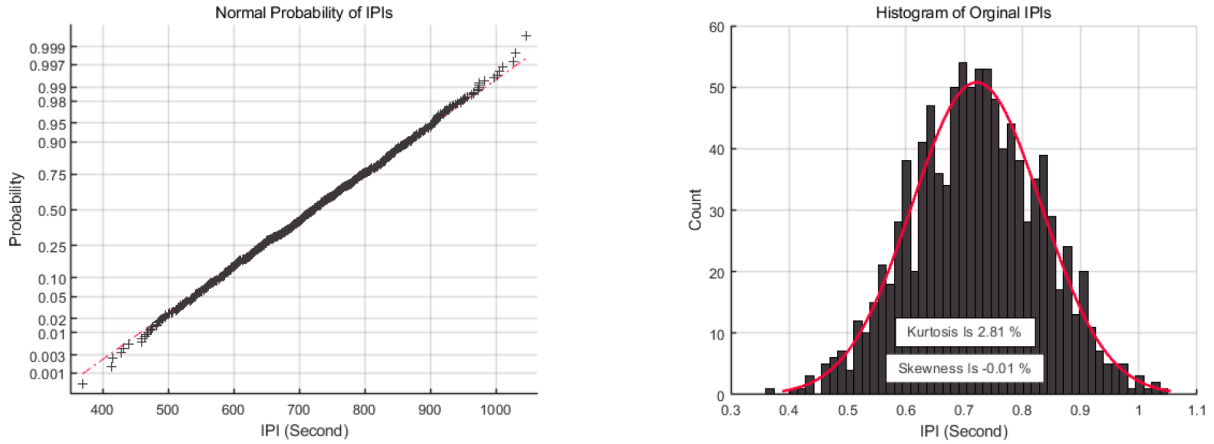



**Fig. 6.** (a). Normal probability diagram of IPIs calculated from the extracted ECG signal. Fig. 6. (b). Histogram of the IPIs calculated from the extracted ECG signal.

distribution. Meanwhile, investigating the entropy and mismatch rates of the IPI bits calculated from the extracted ECG signal reveals that the calculated IPIs are not random. Hence, they are not a good candidate to generate a symmetric quality key, and an attacker with statistical analysis can get a huge deal of information about the generated keys. Thus, to solve this problem, it is necessary, using several steps, to convert the set of calculated IPIs into a set of data with uniform distribution and prepare the necessary conditions for generating a quality key with increasing their entropy rates while decreasing their mismatch rates. For this purpose, we use a quantile function. The quantile function is defined by Eq. (15).

$$Q(P) = inf\{x \in R : \ P \leq F(x)\} \tag{15}$$

The quantile function, shown by $Q(P)$, acts the opposite of the cumulative probability function. The cumulative probability function, shown by $F_X(x)$ and defined by Eq. (16), represents the probability of having values less than or equal to x of the random variable X.

$$F_X(x) := Pr(X \leq x) = P \tag{16}$$

Here, if the probability of having values less than or equal to x of the random variable X is defined as P, the quantile function produces a threshold like x, the lowest value of x with the cumulative function greater than P. Now, assuming that the set X contains a set of IPIs calculated from the heart signal via a normal distribution, we can specifically divide this set into a set of discrete values with an equal probability of$\frac{1}{n}$. Here, we can easily calculate different threshold values using Eq. (17) as follows:

$$Threshold_i = Q(P) \ and \ P = \left(\frac{1}{n}, \frac{2}{n}, \ldots, 1\right) \tag{17}$$

Here, the value of n is determined by the number of quantizations that correspond to the total entropy of the IPI values, so that the entropy of the extracted keys does not exceed the entropy of the source in theory. Eq. (18) shows how to calculate the value of n

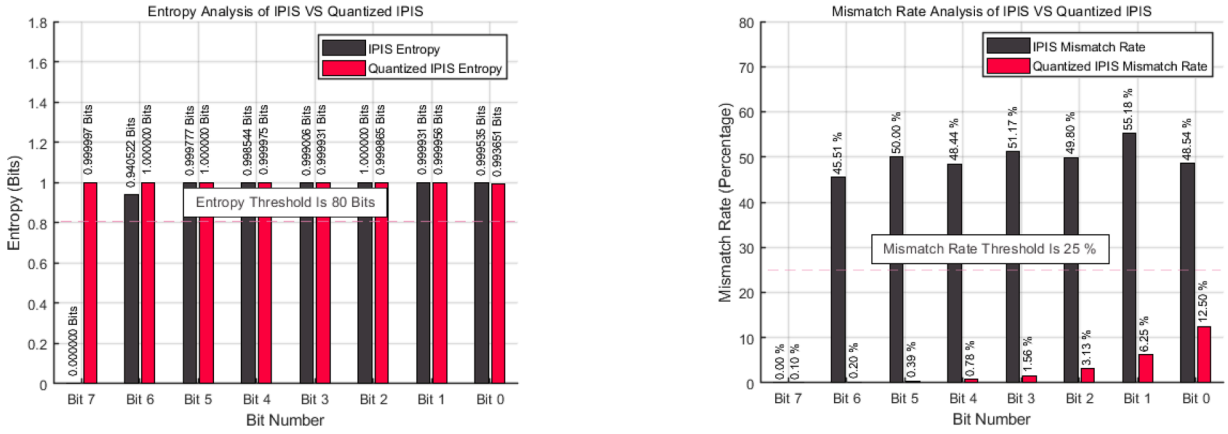



**Fig. 7.** (a). Entropy diagram of the original IPIs in comparison to the entropy of the quantized IPI. Fig. 7. (b). Diagram of the mismatch rate of the bits of the original IPI in comparison to the quantized IPI.

concerning the entropy of IPI values.

$$n = 2^{\lfloor H(X) \rfloor} \tag{18}$$

where H (X) is the entropy of the IPI values and ⌊H(X)⌋ is the largest integer number smaller than H (X). After obtaining various threshold values, the original IPI values falling into the $i^{th}$ segment are quantized by i-1. For instance, the original IPI values in the first segment are quantized by 0, whereas the original IPI values falling into the second segment are quantized by 1. In the end, we use the gray code to encrypt the quantized IPI values and then show each IPI value with a bit string of 0 and 1. Then, we merge all bit strings produced by the IPIs to generate the sink node's normal key. Fig. 7(a) shows a comparison between the entropy diagrams of the original IPIs and those of the quantized IPIs along with the threshold set for entropy that guarantees the quality of the extraction key. Likewise, Fig. 7(b) compares the diagrams of the mismatch rate of the bits of the original IPIs to the quantized IPIs, while showing the threshold set for mismatch rate guaranteeing the extraction key's quality.

According to Fig. 7(a) and (b), after quantizing the extracted IPIs, the entropy and mismatch rate of their bits were improved. Hence, they meet the threshold value set to meet the two conditions, randomness and proximity, and can be used as a secret source to generate a quality key. On the other hand, according to Fig. 8(a) and (b), the quantized IPIs follow a uniform distribution, guaranteeing the necessary security in the intended application. Fig. 8(a) and (b) illustrate the distribution of the IPIs calculated from the ECG signal after the quantization operation.

### 4.7. Generating the encryption domain key of the sink node from the normal key of the sink node

The normal key of the sink node generated in step 5 is transmitted to the smart healthcare center through a public channel that may be insecure. Therefore, to provide security and prevent unauthorised access, the normal key of the sink node is transferred to the encryption domain using Eq. (19), and then a key is generated known as the encryption domain key of the sink node.

$$\mathrm{Min}||X_{S_i}||_1 \quad \mathrm{S.T}\ Y_{S_i} = \varphi_{S_i} \times X_{S_i} \tag{19}$$

In Eq. (19), $X_{S_i}$ is the normal key of the sink node in the encryption-domain aggregation of the $i^{th}$; $Y_{S_i}$ denotes the encryption domain key of the sink node in the encryption-domain aggregation of the $i^{th}$; and $\varphi_{S_i}$ represents the measurement matrix generated in the encryption-domain aggregation of the $i^{th}$ on the side of the sink node. This sparse matrix, a kind of sub-Gaussian matrix, transfers the normal key of the sink node to the encryption domain with the least possible calculations. This matrix is created using Eq. (20), and its set of keys is generated by a random seed, owned by the sensor nodes, sink node, and cloud.

$$\begin{cases} P(\varphi_{S_i} = K) = \dfrac{1}{2SX_{S_i}} \\ P(\varphi_{S_i} = 0) = 1 - \dfrac{1}{2SX_{S_i}} \end{cases} \tag{20}$$

Here, when the value of $\varphi_{S_i}$ is zero, no encryption occurs, and when the value of $\varphi_{S_i}$ is equal to K, the sink node projects its $i^{th}$ aggregated data over its related $\varphi_{S_i}$ matrix columns to obtain its measurement result. The sink node measurement result is the sink node encryption domain key based on the $\varphi_{S_i}$ matrix and the intruder cannot read it. To recover the sink node encryption domain key, the smart healthcare center must generate the $\varphi_{SCC_i}$ matrix by the agreed random seed.

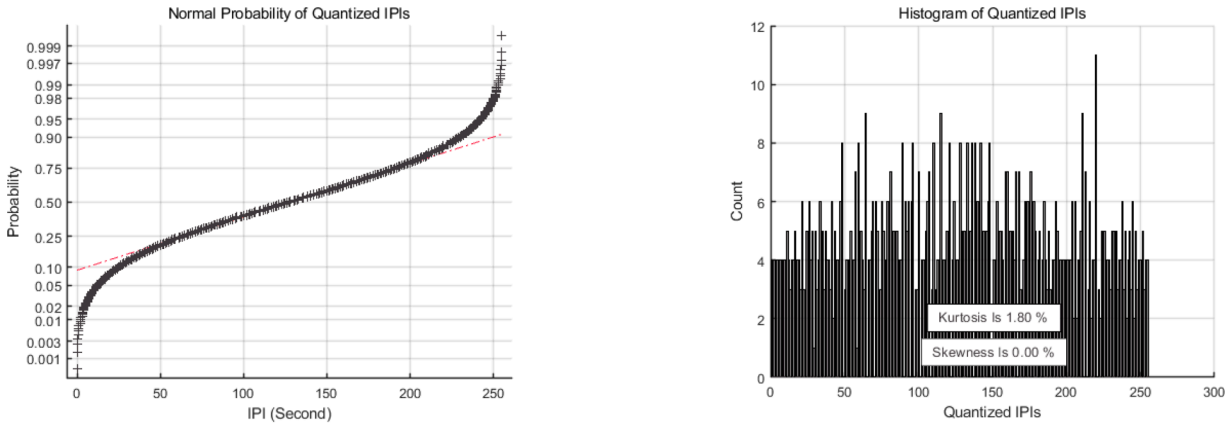



**Fig. 8.** (a). Normal probability diagram of quantized IPIs. Fig. 8(b). Histogram of quantized IPIs.

### 4.8. Generating message authentication code from encryption domain key of the sink node using the normal key of the sink node

In this step, according to Eq. (21), a message authentication code is generated from the sink node encryption domain key using the sink node normal key. Then, the message authentication code is sent to the smart healthcare center along with the sink node encryption domain key. The generated message authentication code is utilized to verify the authenticity of the key generated on the smart healthcare center.

$$\begin{aligned} &MacGen(Y_{S_i}, X_{S_i}) \rightarrow Mac_{S_i} \\ &Send\ \{Y_{S_i}, Mac_{S_i}\}\ to\ Cloud \end{aligned} \tag{21}$$

where $Y_{S_i}$ is the encryption domain key of the $i^{th}$ round of the sink node, $X_{S_i}$ is the normal key of the $i^{th}$ round of the sink node, and $Mac_{S_i}$ is the generated message authentication code of the sink node encryption domain key using the sink node normal key.

### 4.9. Generating the normal key of the smart healthcare center from IPIs calculated from the soldier's heart data record

In this step, similar to the process mentioned in Section 4.6, the smart healthcare center calculates the soldier-related IPIs using the soldier's heart data record and generates the normal key of the smart healthcare center. The generated normal key is utilized in the key pairing process to produce the retrieved normal key of the smart care center.

### 4.10. Generating the encryption domain key of smart healthcare center from the normal key of the smart healthcare center

In this step, generated the normal key of the smart healthcare center in steps 5–8 is transferred to the encryption domain by Eq. (22) and generated the encryption domain key of the smart healthcare center.

$$\mathrm{Min}||X_{SCC_i}||_1 \ \ \mathrm{S.T}\ Y_{SCC_i} = \varphi_{SCC_i} \times X_{SCC_i} \tag{22}$$

where $X_{SCC_i}$ is the normal key of the $i^{th}$ round of the smart healthcare center and $Y_{SCC_i}$ is the encryption domain key of the $i^{th}$ round of the smart healthcare center. Besides, $\varphi_{SCC_i}$ is the measurement matrix of the $i^{th}$ round, generated in the smart care center, in a process similar to the one discussed in Section 4.6 and based on the seed agreed with the sink node and Eq. (23).

$$\begin{cases} P(\varphi_{SCC_i} = K) = \dfrac{1}{2SX_{SCC_i}} \\ P(\varphi_{SCC_i} = 0) = 1 - \dfrac{1}{2SX_{SCC_i}} \end{cases} \tag{23}$$

### 4.11. Calculating the difference between the encryption domain key of the sink node and the encryption domain key of the smart healthcare center

In this step, the difference between the encryption domain key of the sink node and the encryption domain key of the smart care center is calculated using Eq. (24).

$$\Delta Y_{S_i,SCC_i} = Y_{S_i} - Y_{SCC_i} \tag{24}$$

where $Y_{S_i}$ is the encryption domain key of the $i^{th}$ round of the sink node; $Y_{SCC_i}$ is the encryption domain key of the $i^{th}$ round of the smart healthcare center; and $\Delta Y_{S_i,SCC_i}$ is the difference between the encryption domain key of the $i^{th}$ round of the sink node and the encryption domain key of the $i^{th}$ round of the smart healthcare center.

### 4.12. Calculating the difference between the normal key of the sink node and the normal key of the smart healthcare center

In this step, the difference between the normal key of the sink node and the normal key of the smart healthcare center is calculated using the calculated $\Delta \mathbf{Y_{S_i,SCC_i}}$.and Eq. (25)

$$\Delta X_{S_i,SCC_i} = \ \mathrm{Min}\left|\left|\Delta Y_{S_i,SCC_i}\right|\right|_1 \tag{25}$$

where $\Delta X_{S_i,SCC_i}$ is the difference between the normal key of the $i^{th}$ round of the sink node and the normal key of the $i^{th}$ round of the smart healthcare center. Besides, $||\Delta Y_{S_i,SCC_i}||_1$ is the one-norm of the difference between the encryption domain key of the $i^{th}$ round of the sink node and the encryption domain key of the $i^{th}$ round of the smart healthcare center.

### 4.13. Calculating retrieved normal key of the smart healthcare center

In this step, according to Eq. (26) and using the direct sum of the normal key of the smart healthcare center and the difference between the normal key of the sink node and the normal key of the smart care center, the retrieved normal key of the smart care center is generated.

$$X^{\wedge}_{SCC_i} = X_{SCC_i} \oplus \Delta X_{S_i,SCC_i} \tag{26}$$

where $X_{SCC_i}$ denotes the normal key of the $i^{th}$ round of the smart healthcare center; $\Delta X_{S_i,SCC_i}$ is the difference between the normal key of the $i^{th}$ round of the sink node and the normal key of the $i^{th}$ round of the smart healthcare center; and $X^{\wedge}_{SCC_i}$ is the retrieved normal key of the $i^{th}$ round of the smart care center.

### 4.14. Generating MAC from encryption domain key of the sink node using the retrieved normal key of the smart healthcare center and comparing it with the MAC generated from the encryption domain key of the sink node using the normal key of the sink node

In this step, according to Eq. (27), a message authentication code (MAC) is generated from the encryption domain key of the sink node using the retrieved normal key of the smart healthcare center. Then, the generated MAC ($Mac_{SCC_i}$) is compared with the MAC generated in Section 4.8 ($Mac_{S_i}$). Here, if the result of the comparison is positive, a message containing a successful pairing of the keys is sent to the sink node and then the process shown in the Fig. 2 is continued. Otherwise, a message containing the re-request of the encryption domain key of the sink node along with $Mac_{S_i}$ is sent to the sink node, and the process is continued from step 11 of the Fig. 2.

$$\begin{aligned}
&MacGen\left(Y_{S_i}, X^{\wedge}_{SCC_i}\right) \rightarrow Mac_{SCC_i}\\
&If\ Mac_{SCC_i} = Mac_{S_i}\ \ Then\\
&MessageGen(Successful\ Pairing\ of\ Keys) \rightarrow Message\\
&Send\{Message\} to\ Sink\ Node\\
&Else\\
&Request\{Y_{S_i}, Mac_{S_i}\} From\ the\ Sink\ Node\\
&Go\ to\ 11
\end{aligned} \tag{27}$$

### 4.15. The aggregation of the encryption domain of the sensed data and sending the aggregated data of the encryption domain, encrypted with the hash of the normal key of the sink node, to the smart care center

In this step, according to Eq. (28), the received encryption domain data in the $i^{th}$ round are aggregated in the encryption domain in the sink node. Then, the aggregated data of the encryption domain is encrypted by the hash of the normal key of the ith round of the sink node and sent, via the fog, to the cloud of the smart care center. In this approach, security is guaranteed as all of the received data are in the encryption domain, and all network aggregations are performed in the encryption domain.

$$Y_{NI_i} = \oplus_{j=1}^{N}\left(\varphi_{N_{ij}} X_{N_{ij}}\right)\ and\ Send\ Enc(Y_{NI_i}, H(X_{S_i}))\ to\ Cloud \tag{28}$$

where $Y_{NI_i}$ is the encryption domain data aggregated in the $i^{th}$ round, $X_{N_{ij}}$ is the sensed data of the $i^{th}$ round by sensor node No. j, $Enc(Y_{NI_i}, H(X_{S_i}))$ is an encrypted data with the hash of the normal key of the $i^{th}$ round of the sink node, and $\varphi_{N_{ij}}$ identifies the related column of the sensor node No. j in the measurement matrix of the $i^{th}$ round.

### 4.16. Retrieving and decrypting the received data and completing the therapy processes at the smart care center

In this step, first, the smart healthcare cloud receives the data sent by the sink node and generates the measurement matrix of the $i^{th}$ round based on the random seed agreed with the sink node. Then, the normal key of the smart care center is retrieved and the received data are decoded and retrieved according to hash of the normal key. After that, therapy processes are completed at the smart care center. Here, in the decryption and recovery process in the cloud, we seek the sparsest solution, which satisfies all the measurements. This solution is obtained by problem $P_0$ in Eq. (29), where the zero-norm of the sensed data is minimized. However, the number of samples and the search space in the problem $P_0$ are very large, and consequently, $P_0$ is NP-Hard. Therefore, instead of $P_0$, the alternative problem $P_1$ in the Eq. (30) is solved by relaxing the zero-norm [20].

$$P_0 : Min\ ||X||_0\ S.T\ Y_{M\times 1} = \varphi_{M\times N} \times X_{N\times 1} \tag{29}$$

$$P_1 : Min||X||_1\ \ S.T\ Y_{M\times 1} = \varphi_{M\times N} \times X_{N\times 1} \tag{30}$$

In Problem One, we employ the 1-norm to minimize the taken samples. Norm 1 is the closest convex release to zero-norm. If the condition described in Eq. (31) is true in terms of the number of measurements, the solution of the zero-problem will be the same as problem one.

$$M > C \times SX \times Log_{10}^{\frac{N}{SX}} \tag{31}$$

Moreover, in data recovery, considering the number of measurements as the number of equations, and the number of taken samples as the number of variables, if the number of samples is greater than that of measurements (the number of variables is greater than the number of equations), our set will not have a unique solution. Thus, the system of equations has infinite solutions, that by assuming the sparsity assumption, we can choose the sparsest solution from the available solutions for the optimum data recovery.

## 5. The used dataset, assumptions, and setting of parameters in the simulation to evaluate the performance of the proposed sensing model

In the present research, to examine the obtained results, the real dataset of "vital signs" of the smart medical care center of the University of Queensland is used. The dataset includes data obtained from 18 women and 32 men aged between 35 and 45 years with different skin colors plus a wide range of patient-monitoring data and vital signs collected from the patients anesthetized at the Royal Adelaide Hospital during 50 surgeries and recorded. In this dataset, raw monitoring data is recorded as comma-separated data with a sampling rate of 11 ms. The dataset comprises features such as time, relative time (ms), heart rate, systolic blood pressure, body temperature, blood oxygen saturation percentage, blood pressure, and other vital features. This 5-GB dataset can be accessed via the official website of this university at www.eait.uq.edu.au. In Fig. 9, the characteristics of heart rate, systolic blood pressure, body temperature, and blood oxygen saturation percentage of this dataset related to 50 investigated patients are deicted beside the regular values of each feature for a healthy individual. Moreover, in this paper, to obtain accurate results, all experiments and simulations were performed in a fair environment on a system with Intel Core i3 2.5 GHz ® processor specifications and 4096 MB of memory and 64-bit Windows 7 operating system. To simulate the proposed sensing model and the DSCB comparison method [12], MATLAB R2019b simulator software was employed. Besides, in the simulation, the body environment is implemented as 2D in the dimensions of 1.82 $m$ $\times$ 0.79 m. Then, the sensor nodes and the sink node are located in a fixed form at the coordinates predetermined according to Table 2, with the initial energy of 0.3 J and 0.525 J, respectively. Furthermore, in the simulation, some assumptions are considered following the item presented in Table 5.

Note that in the analysis, data with an entropy level of 0.915 bits were considered. Besides, the number of default measurements was 209. In addition to the aforementioned issues, details of the setting of other parameters used in the simulation are presented in Table 6.

## 6. Analyzing and evaluating the results

This section deals with investigating the results of applying the proposed sensing model in comparison with the PALWSS [10], PEDTARA [11] and DSCB [12] methods on the network topology described in Section 3, using simulations and experiments conducted within the framework of five experiments.

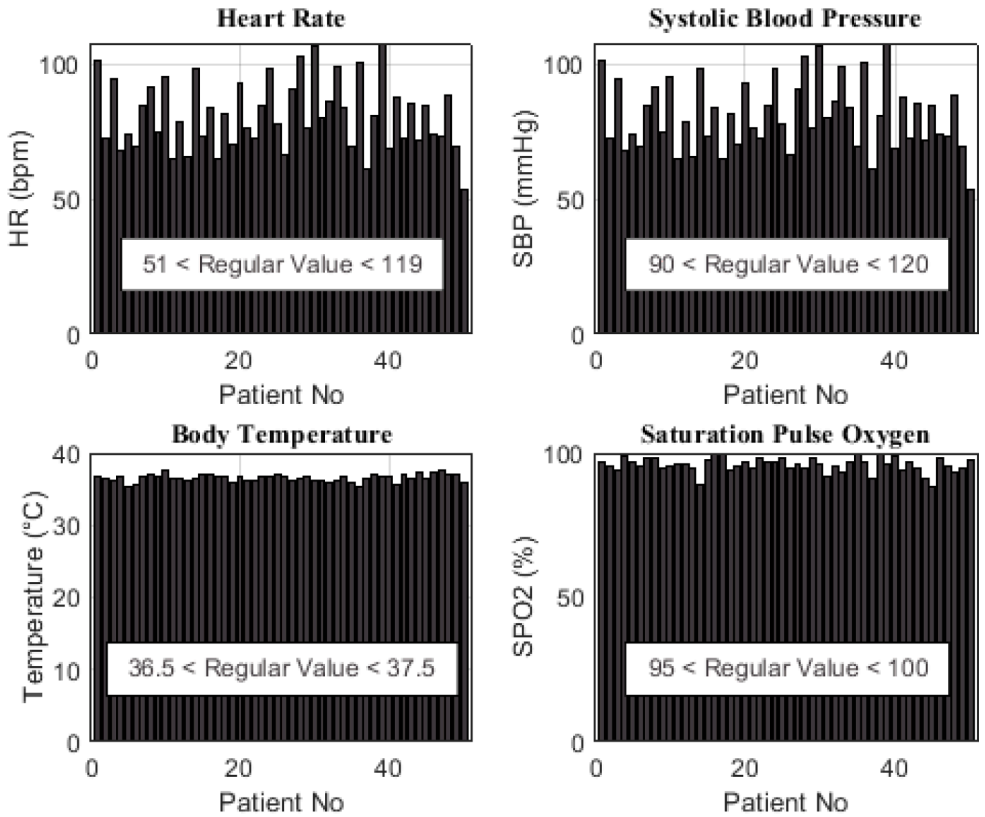



**Fig. 9.** Visual representation of heart rate, systolic blood pressure, body temperature, and percentage of oxygen saturation propeties of the dataset associated with the 50 investigated patients beside the regular values of each feature for a healthy individual.

**Table 5**
Experiment's assumptions.

| No. | Assumption |
|---|---|
| 1. | Each node knows its residual energy and location. |
| 2. | The sink node is different from other sensor nodes and has more resources (energy, memory, processing power, and transmission power) compared to them. |
| 3. | There is no null message in the data sensed by the sensor nodes. |
| 4. | The sensor and sink nodes are fixed at given locations. |
| 5. | The channel is collision-less. |
| 6. | Any signal is sparse in the linear-transform domain. |
| 7. | The measurement is linear. |
| 8. | The number of measurements is equal to or more than twice the sparsity level of the sensed data. |
| 9. | The measurement matrix $\varphi$ has Restricted Isometry Property (RIP) and is suitable for the recovery of sparse or compressed data. |
| 10. | The number of data sensed by the sensor nodes is infinite. |
| 11. | The sparsity level of the sensed data is not fixed over time and changes for different data types sensed by the sensor nodes. |
| 12. | $X$ is uniformly distributed over $x$. |
| 13 | $SX_{\Delta_{S_i,SCC_i}} \times \log_2 \frac{N}{SX_{\Delta_{S_i,SCC_i}}} < M < Min(SX_{S_i}, SX_{\Delta_{S_i,E}})$ |

**Table 6**
Parameter settings in the simulations.

| Proposed method<br>Parameter symbol | Parameter description | Value |
|---|---|---|
| $M_{Default}$ | Number of Default Measurements | 209 |
| $t_{Distributing\ Activity\ Intervals}$ | Time of Distribution of Activity Intervals | 0.32 ms |
| $CR_{Default}$ | Default Compression Ratio | 0.8164 |
| N | Total Number of Unknowns in $R^N$ | 256 |
| $t_{Lightweight\ Secure\ Sensing}$ | Time of Lightweight Secure Sensing | 0.0145 s |
| $E_{Usage\ Energy\ Lightweight\ Secure\ Sensing}$ | Usage Energy of Lightweight Secure Sensing | 0.028 mj |
| $E_{Add}$ | Energy dissipation for addition | 3.3 nj |
| $E_{Mrd}$ | Memory Read Energy Dissipation | 0.26 nj |
| $E_{Mwr}$ | Memory Write Energy Dissipation | 4.3 nj |
| $E_{Mul}$ | Multiplication Energy Dissipation | 9.9 nj |
| $E_{Sft}$ | Shift Energy Dissipation | 3.3 nj |
| $E_{Cmp}$ | Comparison Energy Dissipation | 3.3 nj |
| $SX_{Default}$ | Number of Nonzero Coefficients (Default Sparsity Level) | 17 |
| $P_{Acqired}$ | Sensing Power Consumption | 66.3 mW |
| $t_{Instruction\ Execution}$ | Instruction Execution Duration | 0.135 $\mu s$ |
| $t_{Active\ Listening\ Period}$ | Active Listening Period | 0.02 s |
| $f_{Operation}$ | Operation Frequency | 7.4 MHZ |
| $PS_{Activity\ Intervals}$ | Packet Size of Activity Intervals | 48 bit |
| $t_{Normal\ Sensing}$ | Time of Normal Sensing | 0.346 ms |
| $E_{Usage\ Normal\ Sensing}$ | Usage Energy of Normal Sensing | 0.5 $\mu j$ |
| $P_{BCK}$ | Background Power Consumption | 9.6 mW |
| $P_{ACQ}$ | Sensing Power Consumption | 15.01 mW |
| $t_{DSCB\ Sensing}$ | Time of DSCB Sensing | 0.0180 s |
| $E_{Usage\ DSCB\ Sensing}$ | Usage Energy of DSCB Sensing | 1 mj |

### 6.1. Evaluation criteria

Here, the performance and security of the proposed scheme are evaluated using various evaluation criteria such as the average energy consumption of sensor nodes, average packet delivery delay, the quality of the recovered signal, mutual information, the principle of recovery in secure and lightweight sensing, and normalized mutual information.

#### 6.1.1. Average energy consumption of sensor nodes

One of the parameters used in this paper to assess the performance of the proposed sensing model is the average energy consumption of the sensor nodes. In evaluating the efficiency of the proposed sensing model in comparison with the PALWSS [10], PEDTARA [11] and DSCB [12] methods, the average energy consumption of the sensor nodes is calculated using Eq. (26) as follows:

$$E_{Usage-Average} = \frac{\left[\sum_{j=1}^{N}\left(E_{Usage-Sensing_j} + E_{Usage-Communication_j}\right)\right]}{N} \tag{32}$$

where $E_{Usage-Average}$ is the average energy consumption of the sensor nodes; N denotes the total number of sensor nodes; $E_{Usage-Communication_j}$ is the energy consumed by the $j^{th}$ sensor node to transfer sensed data to the sink node; and $E_{Usage-Sensing_j}$ is the amount of energy consumed by the $j^{th}$ sensor node to sense data using the proposed sensing model or sensing model used in PALWSS

[10], PEDTARA [11] and DSCB [12] methods. It included the energy consumed for sensing data in raw form, the energy used for compressing and securing the sensed raw data, and the energy consumed for the background processing. Fig. 10 depicts the performance analysis of the proposed sensing model in terms of average energy consumption in each sensor at different levels of entropy and dynamic compression rates in comparison to the PALWSS [10], PEDTARA [11] and DSCB [12] methods.

As indicated in Fig. 10, the average energy consumption in sensor nodes in the case of using the proposed sensor model improved compared to the PALWSS [10], PEDTARA [11] and DSCB [12] methods. For instance, the average energy consumption of sensor nodes is improved respectively by 2.18%, 6.32% and 7.63% when the entropy level of the sensed data is 0.9150 bits. This improvement in sensed data with lower entropy is more dramatic, and sensor nodes survive in more rounds. There is a difference between the average energy consumption of sensor nodes in the proposed sensing model and the PALWSS [10], PEDTARA [11] and DSCB [12] methods, which increases with decreasing the level of entropy of the sensed data. The reason can be the sampling and compression of the sensed data with the number of dynamic measurements and the dynamic compression rate based on the amount of information content and the sparsity level of the data. It causes the data sensed in the proposed sensing model and PALWSS method [10], with the same size as the data sensed in the PEDTARA [11] and DSCB [12] methods, to be sent with fewer bits and lower energy consumption than the PEDTARA [11] and DSCB [12] methods.

### 6.1.2. Analysis and evaluation of the average packet delivery delay

The average time taken for delivering the packets sent by sensor nodes to the sink node is called the average packet delivery delay. Minimizing the delay is a very important factor in the BANs with limited energies to increase the survival time of nodes. Therefore, in this paper, we consider the average packet delivery delay as another important parameter to assess the performance of the proposed sensing model compared to the PALWSS [10], PEDTARA [11] and DSCB [12] methods. It is calculated using Eq. (33) as follows [12]:

$$PDD_{Average} = \frac{\left[\sum_{i=1}^{N} t_{Activity-Interval} + \left(2 \times \frac{L_j}{R}\right) + \frac{d_j}{C}\right]}{N} \tag{33}$$

where $L_j$ is the size of the packet sent by the j$^{th}$ sensor node; R represents data transfer rate; $d_j$ is the distance between the j$^{th}$ sensor node and sink node; and $t_{Activity-Interval}$ denotes the time allotted by the sink node to the sensor node at which the sensor node can be active and sense the data. In addition, the constant value C is $3 \times 10^8$ for wireless connection, equaling the light speed. Fig. 11 illustrates the proposed sensing model compared to the PALWSS [10], PEDTARA [11] and DSCB [12] methods in terms of the average packet delivery delay at various entropy levels when the data transfer rate is 0.25 Mbps.

As indicated in Fig. 11, the average packet delivery delay when the proposed sensing model is used and the level of entropy of the sensed data is 0.9150 bits, is reduced respectively by 1.32%, 5.35% and 11.80% compared to that when using the PALWSS [10], PEDTARA [11] and DSCB [12] methods. This is due to the sampling and dynamic compression of the sensed data based on the information content and their sparsity level, causing the sensed data to be sampled with fewer measurements and transmitted with fewer bits. Therefore, with a constant data transfer rate and a constant value of both C and the distance between the sensor nodes and the sink

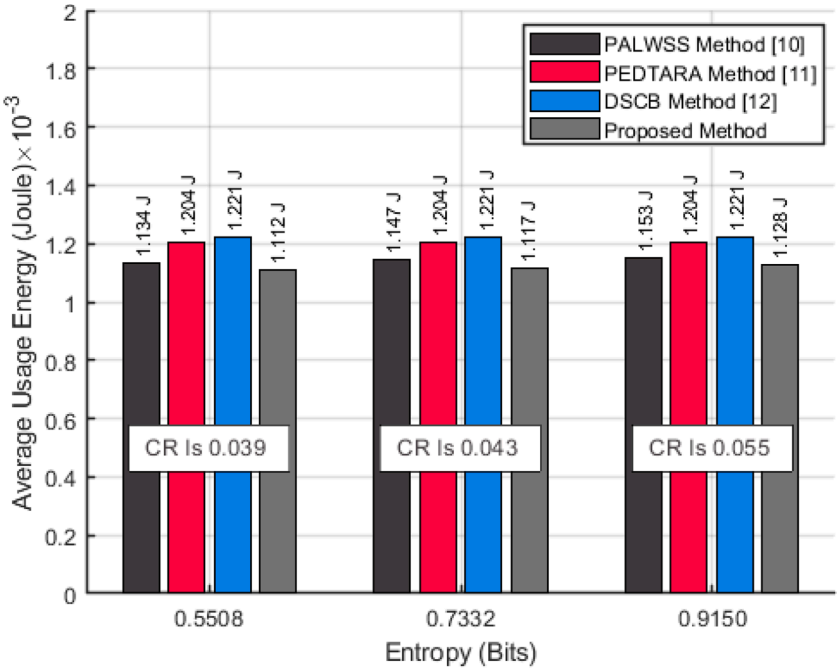



**Fig. 10.** Calculating diagram of average energy consumption in sensor nodes at various entropy levels and compression rate.

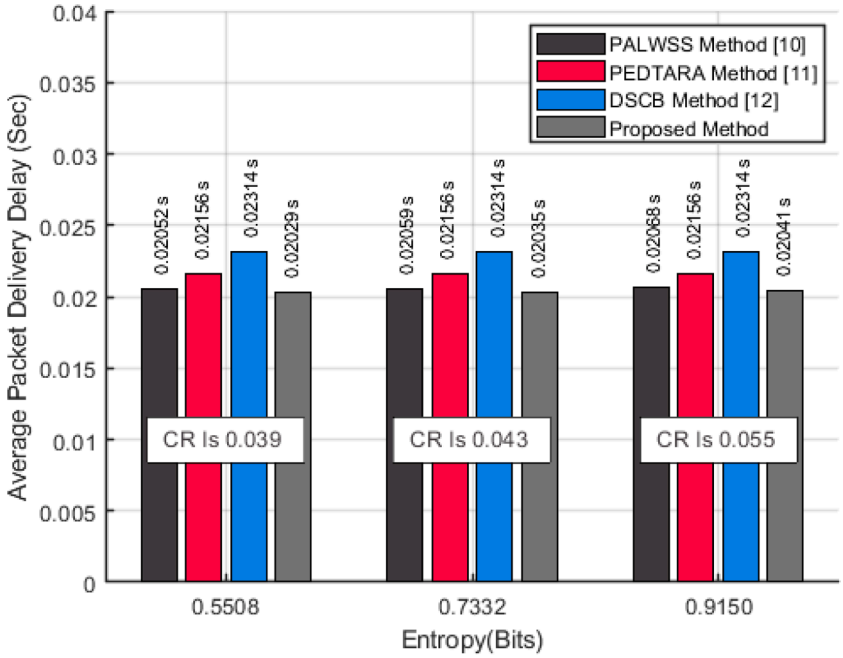



**Fig. 11.** Diagram of average packet delivery delays at various entropy levels and compression rates.

node, the average packet delivery delay decreases. Here, packet delivery delay decreases directly, attributable to the reduced level of entropy of sensed data, and this decrease is more dramatic in sensed data with lower levels of entropy.

*6.1.3. Analysis and evaluation of the quality of the recovered signal*

To evaluate the performance of the proposed sensing model, the signal-to-noise (SNR) ratio indicator of the recovered signal at various entropy levels is employed. Entropy is one of the fundamental concepts in information theory, used as a criterion to measure uncertainty and information content. In a signal, entropy determines the degree of compressibility of the signal coefficients over a given range. In the performed simulation, the entropy level of the signal is calculated based on the Shannon standard using Eq. (34),

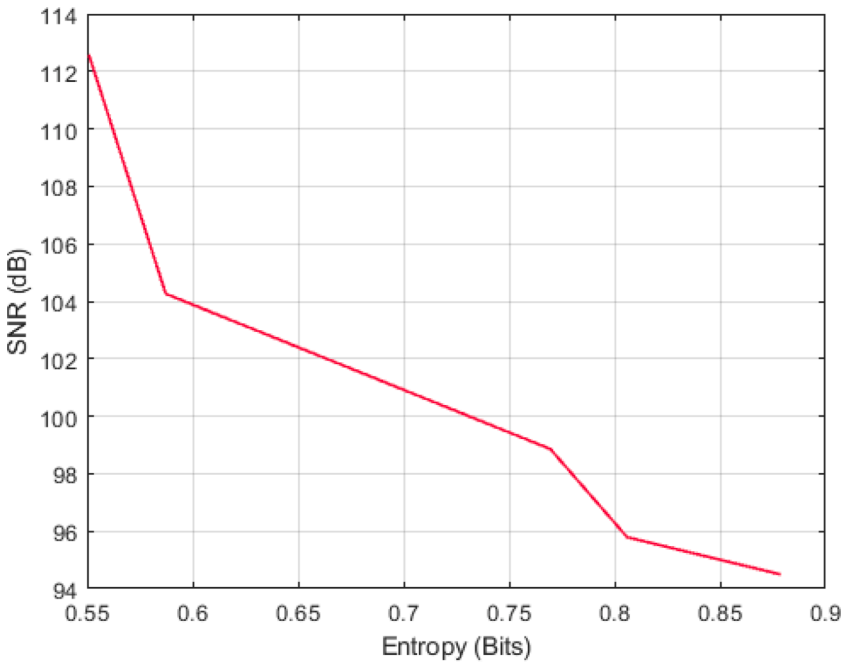



**Fig. 12.** Quality of the recovered signal at various entropy levels.

and the signal-to-noise (SNR) ratio is calculated according to Eq. (35) [21,22].

$$H(X) = -\sum_{i=1}^{N} P(X_i)\log_2 P(X_i) \tag{34}$$

$$SNR = 10\log_{10}\left(\frac{\| X \|_2^2}{\| X^{\wedge} - X \|_2^2}\right) \tag{35}$$

In Eq. (34), N is the number of samples, $P(X_i)$ is the probability of occurrence of the $i^{th}$ sample and $H(X)$ is the entropy of the sensed data vector. In Eq. (35), X represents the original signal, $\hat{X}$ denotes the recovered signal, and SNR is the signal-to-noise ratio of the recovered signal. Fig. 12 depicts the performance of the proposed sensing model in the conducted experiment in terms of the quality of the recovered signal based on the signal-to-noise ratio criterion at various entropy levels.

As shown in Fig. 12, in the recovery done using the lightweight secure sensing Model, the signals recovered from low entropy signals have a higher signal-to-noise ratio and quality than those recovered from high entropy signals. This is because only the sparsity signals can be retrieved simply by secure and lightweight sensing and the sparsity signals have low entropy.

### 6.1.4. Analysis and evaluation of the security in the proposed sensing model

In analyzing and evaluating the security of the proposed sensing model in terms of confidentiality, we assume that a powerful attacker is present with complete information about the system and control of the communication channel. In this section, we first prove the security of the proposed sensing model based on the approach of Shannon Information Theory. After that, we discuss 3 attack scenarios where the attacker tries to extract the key.

*6.1.4.1. Security of the proposed sensing model in terms of Shannon information theory.* According to the assumptions described in lines 3, 8, 9, and 12 of Table 5 in Section 5, since the measurement matrix has a limited isometric property based on the assumptions, there is no data in the vacant space of the measurement matrix. Since there is no empty message in the sensed data, we have no encrypted data of $y = 0$. Moreover, as the number of measurements is equal to and larger than twice the sparsity level of the sensed data, each sensed data vector of x has a unique mapping, and each sensed data from X with a unique encrypted equivalent belonging to Y is encrypted. Hence, y has a uniform distribution on Y. Hence:

$$H(y|x) = \log_2|T| - \log_2|T| = 0$$

So, the Perfect security is available as follows:

$$I(x,y) = H(y) - H(y|x) = \log_2|T| - \log_2|T| = 0$$

*6.1.4.2. Analysis of resistance against active eavesdropping attack.* An active eavesdropping attack is an attack upon which an inactive attacker understands the mechanism of key generation and tries to generate a key based on his heart rate information and then utilizes it to pair with one or more legitimate devices. For example, the attacker uses $Y_E$ to calculate $\Delta Y_{S_i,E}$, and then recovers the normal key value of the sink node following Eq. (3), using $\Delta X_{S_i,E}$ instead of $\Delta X_{S_i,SCC_i}$ and $Y_{S_i,E}$ instead of $Y_{S_i,SCC_i}$. Here, given that in the proposed sensing model after quantization of the sink node normal key, 50% of the sink node normal key elements are zero, and the rest of the elements are non-zero, the normal key of the sink node is not sparse. Hence, based on assumption No. 13 of Table 5, performing this process is difficult and almost impossible for the attacker, and the attacker cannot retrieve the normal key of the sink node and the difference between the normal key of the sink node and himself.

$$\Delta X^{\wedge}_{S_i,SCC_i} = Min \ \| \Delta X_{S_i,E} \|_1 S.T \ \| \Delta Y_{S_i,E} \oplus \varphi \Delta X_{S_i,SCC_i} \|_2 < \varepsilon, \Delta X_{S_i,SCC_i} \tag{36}$$

where $\Delta X^{\wedge}_{S_i,SCC_i}$ is the difference between the retrieved normal key of the $i^{th}$ round of the sink node and the retrieved normal key of the $i^{th}$ round of the smart healthcare center; $\Delta X_{S_i,E}$ is the difference between the normal key of the $i^{th}$ round of the sink node and the normal key of the attacker; $\Delta Y_{S_i,E}$ refers to the difference between the encryption domain key of the $i^{th}$ round of the sink node and the encryption domain key of the attacker; $\varepsilon$ is noise.

*6.1.4.3. Analysis of resistance against brute force attack.* In the proposed sensing model, the sensed data can only be retrieved by access to the measurement matrix. Hence, in analyzing and evaluating the security of the proposed sensing model, we have simulated some scenarios for a brute force attack on the communication between the sensor nodes and the sink node to generate the measurement matrix. In the proposed scenario, the attacker employs the brute force attack along with the trial and error method on the received data to obtain the measurement matrix. Here, if the $\varphi_E$ denotes the measurement matrix used by the attacker to retrieve the signal sensed by the sensors, the expression $\varphi_E = \varphi$ must be true so that the attacker can fully retrieve the data sensed by the sensors. If not, the retrieved data will have a lot of noise, making it impossible to use. In addition, since the measurement matrix is generated randomly in each round, even if the attacker generates a measurement matrix for one round, this matrix is unusable for the next round.

Here, $T_r$ is defined as the number of the identical rows in the main measurement matrix ($\varphi$) and the measurement matrix obtained by the attacker ($\varphi_E$). Besides, $\tau$ is used to show the ratio of the identified rows by the attacker to the total number of rows in the main measurement matrix. In this condition, mutual information test can be employed to determine the security of the proposed sensing

model against the brute force attack. In this experiment, we assume that the dimensions of the signal sensed by the sensor nodes and the sparsity level of the signal are known to the attacker. Thus, only the attacker does not have complete information about the measurement matrix $\varphi$. Here, if "I" is defined as the mutual information between the signal sensed by the sensor node and the signal retrieved by the sink node and $I_E$ is defined as the mutual information between the original signal and the signal retrieved by the attacker, the Normalized Mutual Information (NMI) can be calculated using Eq. (37).

$$I_{Normalization} = \frac{I_E}{I} \tag{37}$$

Fig. 13 exhibits the NMI for various values of $\tau$ for the signals obtained from the sensor nodes.

As can be seen in Fig. 13, in the high compression rate producing high-quality results, the mutual information between the signal sensed by the sensor node and the signal recovered by the sink node is 2 to 3 times more than that between the main signal and the signal recovered by the attacker. The results clearly show that the information decrypted by the attacker is marginal and useless, and therefore, the attacker is not able to exploit the encrypted signal.

*6.1.4.4. Analysis of resistance against passive attack.* Upon a passive attack, the attacker, using his heartbeat data, strives to pair his key with a key utilized by an authorized user. In the analysis, we used the seismocardiogram signal measured from the same body parts of two different users (their chests) and the bit agreement rate metric to assess the probability of creating the same keys. The bit agreement rate is the fraction of matching bits on all bits of a key. The result obtained from the stated study is shown in Fig. 14.

In Fig. 14, the bit agreement rate is depicted versus the cumulative distribution function. Obviously, at most 70% agreement rate can be obtained in the passive attack. Therefore, since a successful key generation process requires the generation of a symmetric key with an agreement rate of 100%, the attacker is not able to pair his key with the key utilized by the authorized user using the heartbeat data of his own.

## 7. Conclusions and future works

In the present study, while focusing on two important challenges of energy consumption and security in BANs, a sensing model applicable in biological warfare is proposed. For this purpose, in the proposed sensing model, the biological data of the cared soldier are sampled according to the information content. A dynamic compression mechanism is utilized in which the compression coefficient is calculated according to the sparsity level of data. In this model, after aggregation of the sampled data in the sink node in the encryption domain and their encryption with a normal key, they are sent to the smart care center. In this process, the time interval calculated from the heart rate of the under-care soldier and extracted using a piezoelectric sensor is utilized to generate the normal key. Then, the message authentication code mechanism and the measurement matrix are utilized to retrieve and pair the normal key of the smart care center, targeted at making it possible to access the biological data and serve the soldier under care using the normal key of the smart care center. After that, we compare this sensing model and the PALWSS [10], PEDTARA [11] and DSCB [12] methods based

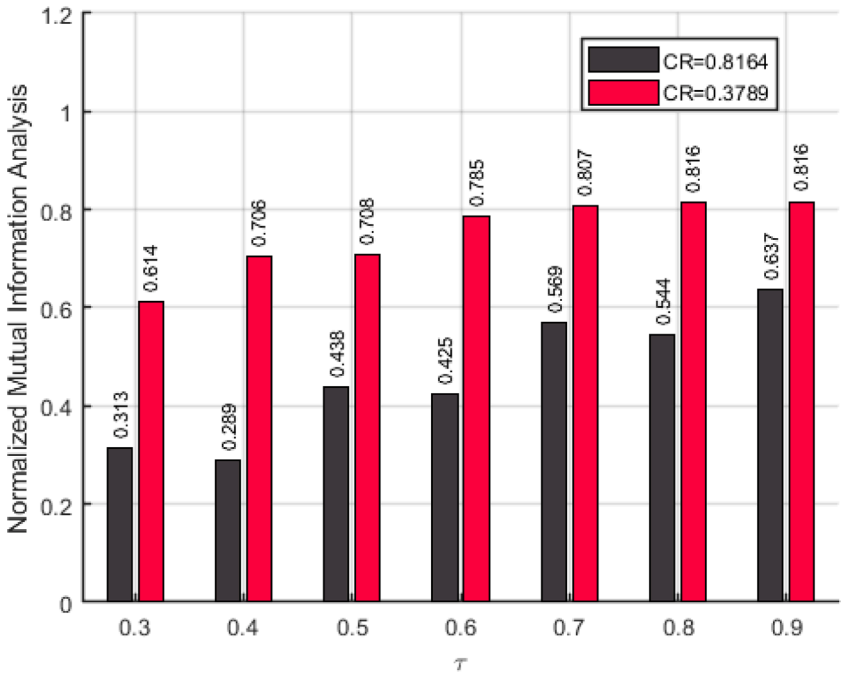



**Fig. 13.** Normalized mutual information (NMI) versus the ratio of rows known for the attacker to the total rows of the main measurement matrix.

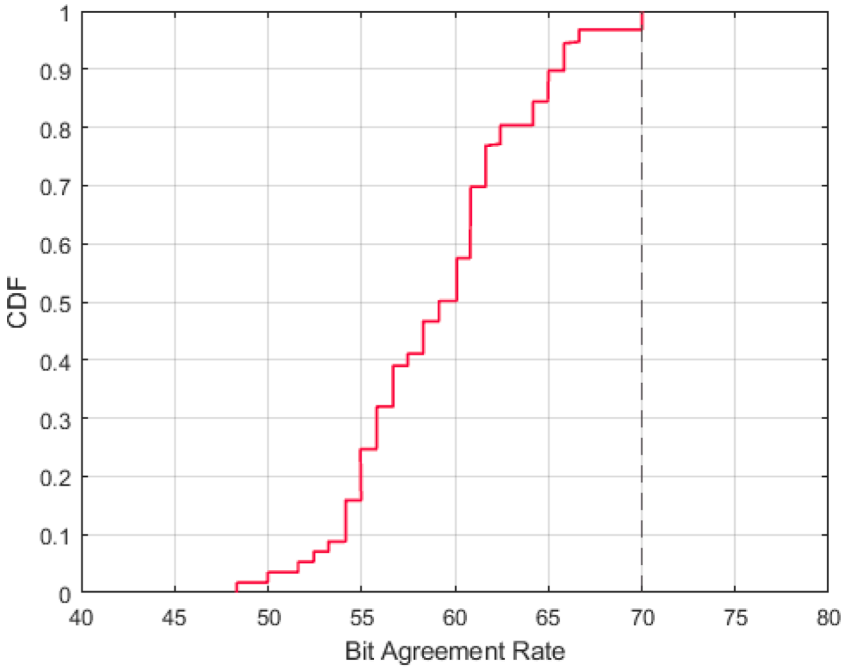



**Fig. 14.** Bit agreement rate versus cumulative distribution function.

on the specific criteria using simulation in terms of the performance of sensed data sampling and its retrieval [12]. Besides, we evaluate the proposed sensing model in 3 attack scenarios, where the attacker tries to extract the key. Then, it is indicated that with the uniform distribution over the data sensed by the sensor nodes and limiting the number of measurements, this model, in addition to achieving the Shannon definition of perfect security, is resistant to both aforementioned attacks. Furthermore, it is shown how the proposed sensing model could improve the quality of the recovered signal and the performance of the BAN in terms of average packet delivery delay and average node energy consumption. In this paper, some experiments are conducted at various levels of entropy for a variety of measurements, taking into consideration the retrieval error. It is obvious that by increasing the number of measurements to approach the total number of signal samples, the retrieved signal will be closer to the original signal. However, in our analysis, it is found out that the signal quality does not play a key role in medical diagnosis and a medium-quality recovered signal enables the doctors to make a correct diagnosis. On the other hand, increasing the number of measurements makes the illegal recovery of the main signal complicated for the intruder. Therefore, we tried to adjust the number of measurements to preserve the signal quality, guarantee security, and improve other quality of service parameters. Nonetheless, the proposed sensing model cannot compress and recover the slightly sparse signals or the signals that are not sparse, with good quality, and has a complex computational cost and long retrieval time. Thus, in the continuation of this research and as future work, we intend to implement the proposed sensing model in a multi-bit manner and with a special and optimal design of the measurement matrix where a unique biological feature is used to generate the measurement matrix. Therefore, the compression and recovery of signals with a low level of sparsity, in a more reasonable computational cost and low recovery time, will be possible.

In the present study, while focusing on two important challenges of energy consumption and security in BANs, a sensing model applicable in biological warfare is proposed. For this purpose, in the proposed sensing model, the biological data of the cared soldier are sampled according to the information content. A dynamic compression mechanism is utilized in which the compression coefficient is calculated according to the sparsity level of data. In this model, after aggregation of the sampled data in the sink node in the encryption domain and their encryption with a normal key, they are sent to the smart care center. In this process, the time interval calculated from the heart rate of the under-care soldier and extracted using a piezoelectric sensor is utilized to generate the normal key. Then, the message authentication code mechanism and the measurement matrix are utilized to retrieve and pair the normal key of the smart care center, targeted at making it possible to access the biological data and serve the soldier under care using the normal key of the smart care center. After that, we compare this sensing model and the PALWSS [10], PEDTARA [11] and DSCB [12] methods based on the specific criteria using simulation in terms of the performance of sensed data sampling and its retrieval [12]. Besides, we evaluate the proposed sensing model in 3 attack scenarios, where the attacker tries to extract the key. Then, it is indicated that with the uniform distribution over the data sensed by the sensor nodes and limiting the number of measurements, this model, in addition to achieving the Shannon definition of perfect security, is resistant to both aforementioned attacks. Furthermore, it is shown how the proposed sensing model could improve the quality of the recovered signal and the performance of the BAN in terms of average packet delivery delay and average node energy consumption. In this paper, some experiments are conducted at various levels of entropy for a variety of measurements, taking into consideration the retrieval error. It is obvious that by increasing the number of measurements to approach the total number of signal samples, the retrieved signal will be closer to the original signal. However, in our analysis, it is found out that

the signal quality does not play a key role in medical diagnosis and a medium-quality recovered signal enables the doctors to make a correct diagnosis. On the other hand, increasing the number of measurements makes the illegal recovery of the main signal complicated for the intruder. Therefore, we tried to adjust the number of measurements to preserve the signal quality, guarantee security, and improve other quality of service parameters. Nonetheless, the proposed sensing model cannot compress and recover the slightly sparse signals or the signals that are not sparse, with good quality, and has a complex computational cost and long retrieval time. Thus, in the continuation of this research and as future work, we intend to implement the proposed sensing model in a multi-bit manner and with a special and optimal design of the measurement matrix where a unique biological feature is used to generate the measurement matrix. Therefore, the compression and recovery of signals with a low level of sparsity, in a more reasonable computational cost and low recovery time, will be possible.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References

[1] G. Dini, M. Tiloca, ASF: an attack simulation framework for wireless sensor networks, in: 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2012, pp. 203–210.
[2] M.R. Yuce, Implementation of wireless body area networks for healthcare systems, Sens. Actuators A: Phys. 162 (2010) 116–129.
[3] J.-.B. Nie, In the shadow of biological warfare: conspiracy theories on the origins of COVID-19 and enhancing global governance of biosafety as a matter of urgency, J. Bioeth. Inq. 17 (2020) 567–574.
[4] D.K. Altop, et al., Deriving cryptographic keys from physiological signals, Pervasive Mob. Comput. 39 (2017) 65–79.
[5] M. Cicioğlu, A. Çalhan, Energy-efficient and SDN-enabled routing algorithm for wireless body area networks, Comput. Commun. 160 (2020) 228–239.
[6] F. Ullah, et al., An energy-efficient and reliable routing scheme to enhance the stability period in wireless body area networks, Comput. Commun. 165 (2021) 20–32.
[7] J.J. Hathaliya, S. Tanwar, An exhaustive survey on security and privacy issues in healthcare 4.0, Comput. Commun. 153 (2020) 311–335.
[8] G. Yang, et al., Energy-efficient protocol for routing and scheduling in wireless body area networks, Wirel. Netw. 26 (2020) 1265–1273.
[9] A.S. Raj, M. Chinnadurai, Energy-efficient routing algorithm in wireless body area networks for smart wearable patches, Comput. Commun. 153 (2020) 85–94.
[10] S. Esmaeili, et al., A priority-aware lightweight secure sensing model for body area networks with clinical healthcare applications in Internet of Things, Pervasive Mob. Comput. 69 (2020), 101265.
[11] O. Ahmed, et al., PEDTARA: priority-based energy efficient, delay and temperature aware routing algorithm using multi-objective genetic chaotic spider monkey optimization for critical data transmission in WBANs, Electronics (Basel) 11 (2021) 68.
[12] Z. Ullah, I. Ahmed, K. Razzaq, M.K. Naseer, N. Ahmed, DSCB: dual sink approach using clustering in body area network, Peer-to-Peer Netw. Appl. 12 (2019) 357–370.
[13] N. Bilandi, et al., Energy-efficient relay node selection scheme for sustainable wireless body area networks, Sustain. Comput.: Inform. Syst. 30 (2021), 100516.
[14] F.A. Almalki, et al., EERP-DPM: energy efficient routing protocol using dual prediction model for healthcare using IoT, J. Healthc. Eng. 2021 (2021).
[15] A.S. Raj, M. Chinnadurai, Energy efficient routing algorithm in wireless body area networks for smart wearable patches, Comput. Commun. 153 (2020) 85–94.
[16] F. Salahdine, et al., One-bit compressive sensing vs. multi-bit compressive sensing for cognitive radio networks, in: 2018 IEEE International Conference on Industrial Technology (ICIT), 2018, pp. 1610–1615.
[17] F. Xu, et al., IMDGuard: securing implantable medical devices with the external wearable guardian, in: 2011 Proceedings IEEE INFOCOM, 2011, pp. 1862–1870.
[18] S. Cherukuri, et al., Biosec: a biometric-based approach for securing communication in wireless networks of biosensors implanted in the human body, in: 2003 International Conference on Parallel Processing Workshops, 2003. Proceedings, 2003, pp. 432–439.
[19] R.G. Baraniuk, Compressive sensing [lecture notes], IEEE Signal Process. Mag. 24 (2007) 118–121.
[20] M. Hyder, K. Mahata, An approximate l0 norm minimization algorithm for compressed sensing, in: 2009 IEEE International Conference on Acoustics, Speech and Signal Processing, 2009, pp. 3365–3368.
[21] T. Cover, J. Thomas. Elements of Information Theory, John Wiley and Sons, Inc, NY, 1991, pp. 33–36.
[22] A. Lavrenko, et al., On the SNR variability in noisy compressed sensing, IEEE Signal Process. Lett. 24 (2017) 1148–1152.