Body Sensors Network Management Protocol

Ahmad Y. Alhusenat
Department of Network Engineering and Security
Jordan University of Science and Technology
Irbid, Jordan
ayalhusenat18@cit.just.edu.jo

Baha' A. Alsaify
Department of Network Engineering and Security
Jordan University of Science and Technology
Irbid, Jordan
baalsaify@just.edu.jo

***Abstract*—Body Sensors Network (BSN) can be defined as a group of sensors attached to a patient's body and form a network in order to acquire physiological data. BSN can play a major role in enhancing human healthcare. However, personal data obtained from the BSN needs to be secure as the privacy of the patient is a main concern. In this work, we propose a lightweight algorithm for BSN management protocol, where we can send patents data and update the security key at the same time. The proposed algorithm is based on one-time pad (OTP) principle. The data exchange is encrypted using a dynamic key.**

***Index Terms*—Lightweight, BSN, One-time pad, Privacy, Dynamic key**

I. Introduction

Recently and with the emerging of Internet of Things (IoT) technology the development of wireless wearable devices with sensors for clinical applications has been accelerated [1].

The term BSN – Body Sensor Networks was introduced by Prof Guang-Zhong Yang of Imperial College in the early 2000's [2 website]. BSN is designed to provide monitoring of physical, physiological, and biochemical parameters in any environment and without activity restriction and behavior modification. The main challenge facing the implementation of BSN is achieving practical and functional interconnection between the sensors and the data receiver. Wireless techniques are the most suitable and practical techniques to form unobtrusive networks between physically discrete sensors and the data receiver [3]. However, wireless connection is highly secured and thus requires networking protocols to avoid interference and improve data security.

Recently, Xi Tian et. al [4] has proposed clothing structured with conductive textiles termed metamaterial textiles to enable wireless signals emitted by standard devices to efficiently and securely propagate around the body. However, the cost of such clothing structured can be as serious obstacle in its implementation. Lin Guo et al [5] has introduced a transmission scheduling and energy harvesting strategy to manage energy supply and consumption and build several dynamic models to capture the stochastic processes in BSN. However, they have not proposed a practical solution for data security and information privacy. Indeed, the majority of current research articles in BSN focus in minimize energy consumption and optimize the transmission order and transmission duration [3-5].

978-1-7281-6535-6/20/$31.00 ©2020 IEEE

Biometrics cryptosystem using the ECG frequency is proposed by [6] to generate keys and to use AES for Encryption. However, the presented approach in [6] still needs data management and synchronization technique. Key exchange technique has also been used by [7-9] where encryption standard was used for integrity without any management from the user. C. Tan et. al [10] have added limited management data for patient with elliptic curve cryptography (ECC) and made comparison between AES, RSA and their scheme. However, still their approach needs large number of keys and storage requirement. Indeed, less attention has been given to develop comprehensive management protocol to assure data security and thus patient privacy and data control.

The OneTime Pad (OTP) is the strongest secure cipher that is cannot be broken, unless the truly random key is used; which is extremely difficult as the random key must be used one time and it must be equal or at least the same size of the plaintext to be encrypted [11].

The proposed approached in this paper uses the human natural data as the random key. Thus the use of this random key of one time and the same size for next data is needed to be encrypted. However, in case the encoding sensors data encrypted, we propose that data to be sent and decrypt to decoding it as shown in Figure 1 using dynamic OTP key. The Dynamic OTP key approach uses one secret key which is easy to exchange and safe. Moreover this will give the patient the power to manage his/her data, with secure light weight protocol.

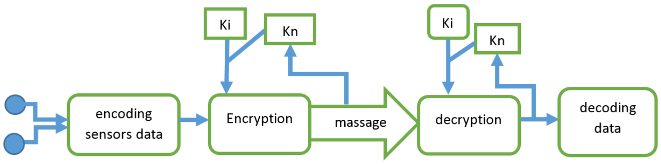


Fig. 1. Dynamic OTP key.

In this work we propose lightweight encryption and management protocol for collected data from BSN, that can guarantee security and privacy demands for the patient.

The goals that we intend to achieve here are as follow:

1) The proposed work presents an improved secure algorithm at which the data can be sent, and updated while the key is exchanging.

2) The patient has the full power of managing his/her data and can change and select who, when, where, and what the receivers can know about his/her data.

3) Minimizing the power consumption by minimizing the message size and using two main light operation (Xor, Hash(.)) in the lightweight algorithm.

4) Minimize the algorithm time complexity to O(n) in both sides.

The remainder of this paper is organized as follows: In Section II, the problem formulization is discussed; where security requirements, system Module and Encryption Techniques are described in detail. Section III proposes the BSN security solution including enhance security requirement, and dynamic algorithm solution. In section IV Algorithm Transaction Example is discussed in detail also Power Consumption and Complexity Analysis. Section V provides conclusions and future work.

II. Problem formulization

In this section the main security requirements are discussed, then the system module and the encryption technique will be introduced.

A. SECURITY REQUIREMENTS

In this subsection we describe the BSN system security requirements and the approach algorithm proposed solution as shown in Figure 2.

1) The privacy: Privacy of patents data is main concern in applying BSN system. The only authorized identity i.e. the Authentication doctor can know and use the patient information. To assure the privacy of the patents their data must be transmitted between the sensors and the receiver in secure way. Thus, we propose the following algorithm to ensure data security. This algorithm relies in applying the onetime pad key principle. In the onetime pad key principle enhance the collected data from the group of sensors that coming from natural environment (human body) is changed randomly. Since all massages has the same limited size it can be used as key for the next massage by simple xor operation, as will be explained in detail later.

2) The Integrity and Authentication: Changing patient's data or manipulating the data can cause critical threat for patient's life; so it must be eliminated. We propose the use of specific ID for administrator and specific ID for the server to get Authentication. Then we proposed the use of Hash function with massage to get integrity, between the patient and doctor.

3) Replay attack: We propose the use of sequential number generated randomly by server that can be sent back to administrator with acknowledge massage. Then the Sequence number can be used for next massage generation; just one time to ensure updating the data, which is very important to protect the patient life and system usability.

B. System Module

Multiple Body sensors are attached to patient body in many way and for various purposes such as thermometer, Electrocardiogram (ECG), Electromyography (EMG), Electroencephalography (EEG), Blood Pressure (BP), etc. [7]. This data should be sent from sensors to administrator where the administrator gather all data from the sensors then manage the data by grouping it and send each group of sensors data to server; where their destination authentication doctor can see the patient information and interact with the patient situation.

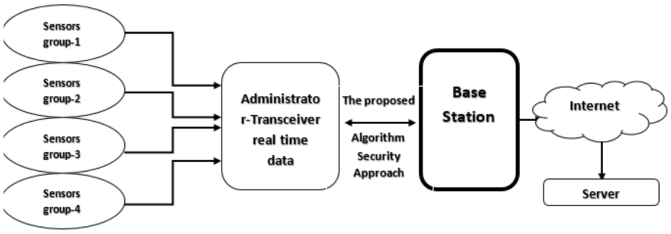


Fig. 2. BSN- Management system

For example the BSN attached to a patient provides data for three groups. The first one for heart where there are four sensors collecting data of the heart health. This information must be available for doctor x, and not available for anybody else. The second group, for physical body data, where there are five sensors collecting physical data, and these group of physical data available for doctor y. The last group for emergency situation that need to send all data for doctor z. Where the administrator can also send the data with patient localization to a police station or nearest emergency center.

The administrator manage the data based on criteria that is selected and programmed in advance based in patient and doctors demand and request. Moreover, our protocol gives the ability to the patient to add some category for family or emergency response station., These option can be added manually by user to eliminate who, when, where and what data receives.

C. Encryption Techniques

In the presented technique we proposed dynamic stage that change and updated the key every time the data is being sent. This will improve the ability to exchange key between the administrator and server without using any additional algorithm. This will improve algorithm security. Then data can be sent, updated and the key can be exchanged at the same time.

This algorithm technique gives the patent powerful management, so he/she can change and select who, when, where, what the receives can know about his/her data. Moreover, the patent can add special case where all his/her data can be sent through initial key. This initial key can be used on the first contact and in emergency situation or de-synchronization.

If we use the Advanced Encryption Standard (AES) encryption for our BSN- Management system, then we need to store all keys for all posable scenario, which made key exchange a serious problem [10].

In case of the use of RSA (Rivest–Shamir–Adleman) encryption for our BSN- Management system, the single public key

TABLE I
ABBREVIATIONS AND CRYPTOGRAPHIC FUNCTIONS

K_i	Initial key
ID_a	Administrator identity
ID_s	Server identity
S	data sensor
D	data group
M	massage
Seq	Sequence number
Ak	Acknowledgment
$hash(.)$	One-way hash function
$\bigoplus$	Exclusive-OR operation
$//$	Concatenation operation

can be used for each group to encrypt data in administrator. Moreover, there will be a need for single private key to decrypt data using by the doctor for particular group. However, if the doctor used his/her private key mystically the patient data can be decrypted. Indeed, there is a limit for the storage space for the public keys and private keys and this will lead to the same issue of key exchange as in AES [10].

III. Proposed Solution

In this section how to achieve the required security using our Dynamic Algorithm approach is discussed.

A. Enhance Security Requirement

In this paper new BSN- Management protocol is proposed to achieve the required security demands as discussed before in section II. The ultimate goal is to assure that patient can send data securely. The requirement and control management BSN system abbreviations and cryptographic functions used in the proposed algorithm are defined in the Table I.

The initial key was exchange using Diffie–Hellman key exchange technique, In [12] they proposed key exchange protocol enables server and administrator to securely agree on a secret initial key.

The developed protocol is divided into two sides. The first side is administrator and the other side is for server as shown in Figure 2. In addition to that, the protocol is divided into three stages.

1) *Initial stage:* That is used at first contact between patient and the doctor. In emergency cases or de-synchronization, the administrator send $(k_i \bigoplus D_1)$ where the two sides have the secret initial key as shown in Figure 3.

2) *Normal stage :* Where data is grouped by the administrator. In this stage the administrator can acknowledge the last massage sent from the server as key. This is important as the server side just can know the key and decrypt the massage using last data received.

Then the protocol uses hash $(ID_a \bigoplus D_1)$ in the first stage from the patient side as a part of massage to ensure the integrity and Authentication in the server side. Then massage from server side can be acknowledged and included in hash $(seq_1 \bigoplus ID_a)$ that allows the patient to control the integrity and Authentication to his/her doctor.

To prevent reply attack, it is proposed the use the acknowledgment massage $(seq_1 \bigoplus D1)$, then the administrator use the hash $(seq_1 \bigoplus ID_a)$ to update the data and send it back along with the next massage to the server, as indicated in Figure 3.

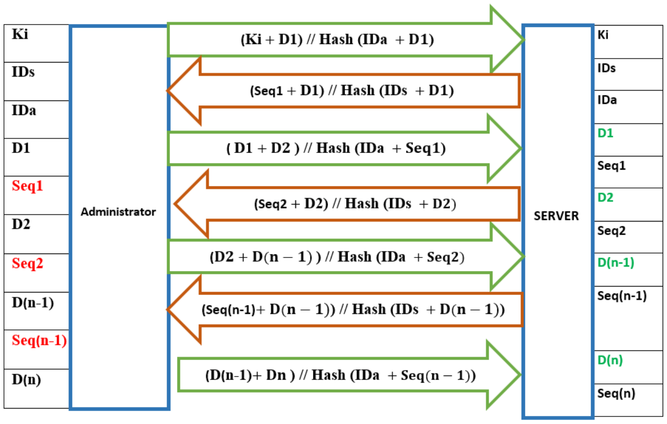

Ki
IDs
IDa
D1
Seq1
D2
Seq2
D(n-1)
Seq(n-1)
D(n)
Administrator
(Ki + D1) // Hash (IDa + D1)
(Seq1 + D1) // Hash (IDs + D1)
(D1 + D2) // Hash (IDa + Seq1)
(Seq2 + D2) // Hash (IDs + D2)
(D2 + D(n − 1)) // Hash (IDa + Seq2)
(Seq(n-1)+ D(n − 1)) // Hash (IDs + D(n − 1))
(D(n-1)+ Dn) // Hash (IDa + Seq(n − 1))
SERVER
Ki
IDs
IDa
D1
Seq1
D2
Seq2
D(n-1)
Seq(n-1)
D(n)
Seq(n)

Fig. 3. Protocol stages

3) *Dynamic stage :* The main point of using dynamic stage technique is to update and exchange the key between patient and doctors. Therefore, the massage can be used as next key to decrypt the data from the administrator side. Moreover, the server side can use the previous massage as the key to decrypt the data as shown in Figure 3, In this aspect, the patient can as act as administrator side to manage the BSN system.

The administrator then can select a specific group of sensors and combine the sensor data $S_1//S_2//S_3$. This will increase the randomness of the data. These data then will be used as group data D that will be sent to doctor receive D securely. The same data then will be used to decrypt next massage. Thus, the patient can choose a group of sensors, and change between them any time he/she wants. This will allow the patient to act as the administrator and use the previous massage as key which has been exchanged already with Authenticated doctor before.

B. Dynamic Algorithm Solution

proposed in this work a protocol with three stage, between two sides is proposed. These three stages do not need to store plenty of keys or stick in one key. Indeed, it is just required to store one secret key and use it in the initial stage. This key will be updated in the dynamic stage after finishing the normal stage automatically and dynamically. This action will depend on the data collected from group sensors chosen.

1) *Initial Stage Algorithm:* The Initial Stage Algorithm is the first contact between the administrator and the server. In this stage the patient can select the group sensors data he/she wants to send to the doctor and then the administrator will collect the data from sensor and set the size for the needed initial key.
The initial key full size will be equal to the total data size from all sensors together. The localization data can be used once needed in emergence situation.

Algorithm 1 Algorithm Initial Stage Administrator Side

```
Input: Select group of sensors from 1 to n
    collect the data group D= data combines from sensors group chosen
Output: send $M_i//hash(D_1 \bigoplus ID_a)$
calculate $M_i = D_1 \bigoplus K_i$
calculate $hash(D_1 \bigoplus ID_a)$
then send the $M_i//hash(D_1 \bigoplus ID_a)$
```

Algorithm 2 Algorithm Initial Stage Server Side

```
Input: $M_i//hash(D_1 \bigoplus ID_a)$
Output: send $(Ak//hash(Seq_1 \bigoplus ID_s))$
Calculate $D_1 = D_1 \bigoplus k_i$
Calculate $hash(D_1 \bigoplus ID_a)$
if the same result $hash$ received then
    accept the massage Authenticated
    Set $K_d = D_1$
    generate random $Seq_1$
    calculate $Ak = Seq_1 \bigoplus D_1$
    calculate $hash(Seq_1 \bigoplus ID_s)$
    send $(Ak//hash(Seq_1 \bigoplus ID_s))$
    Else discard the massage not Authenticate
end if
```

2) Normal Stage Algorithm: In the Normal Stage Algorithm, the key is synchronized and used the sequence to update the data, If Acknowledge massage is missed the key will be re-synchronized by resending the data using the initial key, and checking the emergency situation.

Algorithm 3 Algorithm Normal Stage Administrator Side

```
Input: $Ak//hash(Seq_1 \bigoplus ID_s)$
    collect the data group $D_2$= data combines from sensors group chosen
Output: send the $M_1//hash(Seq_1 \bigoplus ID_a)$
calculate $M_1 = D_2 \bigoplus D_1$
calculate $hash(ID_a \bigoplus Seq_1)$
send the $M_1//hash(Seq_1 \bigoplus ID_a)$
```

3) Dynamic stage Algorithm: In the last Stage, the Dynamic Algorithm, the administrator encrypts the group data by using dynamic key, and then the server decrypts the data by using the dynamic key. Then both sides update the key. If there is emergency or de-synchronization problem the administrator will use the initial key to encrypt the data. The server will check this action and re-synchronize again by getting back to the initial stage. In case the sensors group is changed by the patient the administrator will use a reasonable initial key size and back to initial stage.

IV. Discussion

In this section algorithm transaction example is discussed, Then, system power consumption and complexity analysis will be discussed.

Algorithm 4 Algorithm Normal Stage Server Side

```
Input: $M_1//hash(Seq_1 \bigoplus ID_a)$
Output: send $(Ak//hash(seq_2 \bigoplus ID_s))$
Calculate $D_2 = D_1 \bigoplus M_1$
Calculate $hash(Seq_1 \bigoplus D_a)$
if the same result $hash$ received then
    accept the massage Authenticated
    Set $K_d = D_2$;
    generate random$Seq_2$
    calculate$Ak = Seq_2 \bigoplus D_2$
    calculate $hash(Seq_2 \bigoplus ID_s)$
    send $(Ak//hash(seq_2 \bigoplus ID_s))$
    Else
    Calculate $D_2 = D_2 \bigoplus K_i$
    Calculate $hash(D_2 \bigoplus ID_a)$
    if the same result $hash$ received then
        accept the massage Authenticated
        Set $K_d = D_2$
        generate random $Seq_2$
        calculate$Ak = Seq_2 \bigoplus D_2$
        calculate $hash(Seq_2 \bigoplus ID_s)$
        send$(Ak//hash(seq_2 \bigoplus ID_s))$
        Else discard the massage not Authenticate
    end if
end if
```

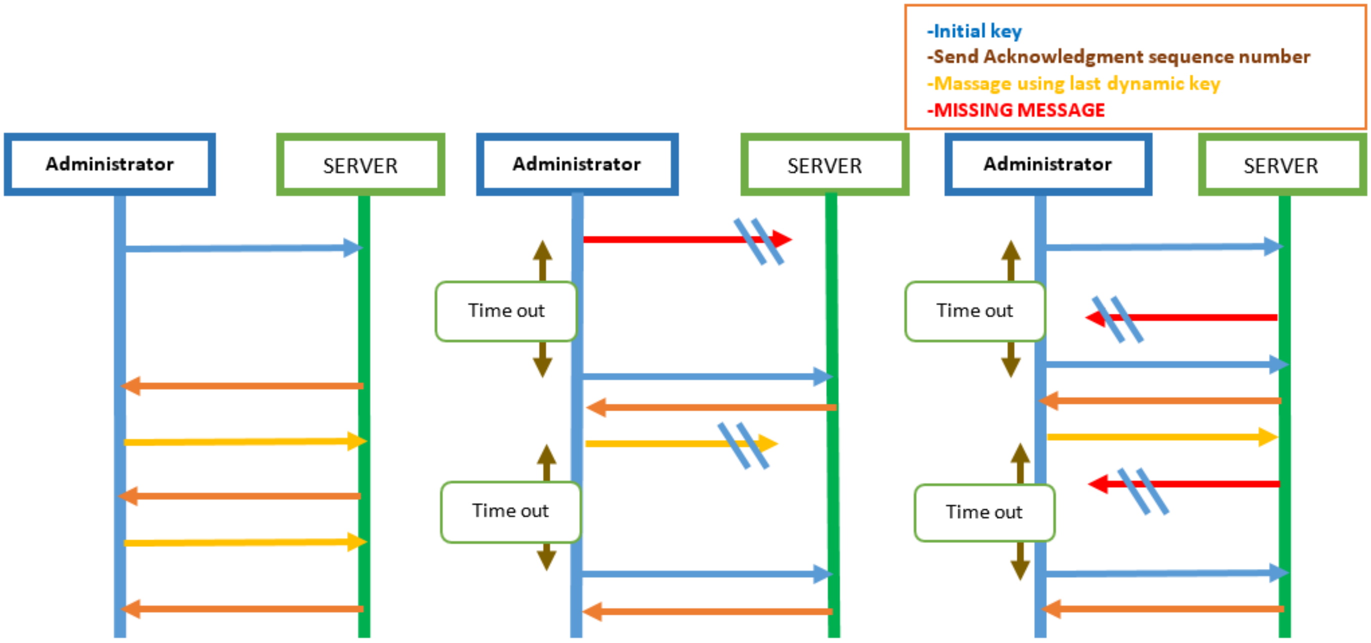
Algorithm 5 Algorithm Dynamic Stage Administrator Side

```
Input: $Ak//hash(Seq_2 \bigoplus ID_s)$
    collect the data group $D_n$= data combines from sensors group chosen
Output: send $M_{(n-1)}//hash(Seq_{(n-1)} \bigoplus ID_a)$
calculate $M_{(n-1)} = D_n \bigoplus D_{(n-1)}$
calculate $hash(ID_a \bigoplus Seq_{(n-1)})$
send the $(M_{(n-1)}//hash(Seq_{(n-1)} \bigoplus ID_a)$
```

A. Algorithm Transaction Example

In this subsection, the proposed three parts of BSN- Management protocol will be discussed. These three parts are the Initial stage, Normal stage and Dynamic stage. Each stage has multiple massages between the administrator and server. Figure 4 shows the action needed if massage is missed in the three stages or/and in case of emergency situation will be discussed.

1) Initial stage protocol: In this stage the patient can select the group of sensors and use part of the initial key to encrypt the data. The server side will use the initial key to decrypt the massage and authentication. Then a sequence for next massage synchronization will be generated and sent with acknowledgement massage to administrator. In case the first data in Figure 4.(b), or the acknowledgment massage will not be received the Administrator will wait for out time then recollect new data and send it again to server side as seen in Figure 4.(c).



(a) without missing massage.

(b) with missing massage

(c) with missing Acknowledgment massage

Fig. 4. Stage protocol. (a) without missing massage. (b) with missing massage. (c) with missing Acknowledgment massage.

Algorithm 6 Algorithm Dynamic Stage Server Side

```
Input: $M_{(n-1)}//hash(Seq_{(n-1)} \bigoplus ID_a$
Output: send $(Ak//hash(seq_n \bigoplus ID_s))$
Calculate $D_n = D_{(n-1)} \bigoplus M_{(n-1)}$
Calculate $hash(Seq_{(n-1)} \bigoplus ID_a)$
if the same result$hash$ received then
    accept the massage Authenticated
    Set $K_d = D_n$
    generate random $Seq_n$
    calculate$Ak = Seq_n \bigoplus D_n$
    calculate $hash(Seq_n \bigoplus ID_s)$
    send$(Ak//hash(seq_n \bigoplus ID_s))$
    Else
    Calculate $D_n = D_{(n-1)} \bigoplus K_i$
    Calculate $hash(D_n \bigoplus ID_a)$
    if the same result $hash$ received then
        accept the massage Authenticated
        Set $K_d = D_n$
        generate random $Seq_n$
        calculate $Ak = Seq_n \bigoplus D_n$
        send$(Ak//hash(seq_n \bigoplus ID_s))$
        Else discard the massage not Authenticate
    end if
end if
```

2) Normal Stage Protocol: In this stage the first massage will be sent and encrypted with the data by first data as a key$(D_2 \bigoplus D_1)$. Then the seq_1 will be used to prevent replay attack. Sarver will decrypt the M_1 by $\bigoplus$ with last data D_1 and then will achieve D_2. Then a new sequence number will be generated for the next massage. If data or acknowledgment massage is missed between server and administrator, the initial stage will be activated with newest data as shown in Figure 4.(b) and Figure 4.(c) respectively.

3) Dynamic Stage protocol: In this stage it is assumed that the group sensor will not be changed and a regular situation is taken place with good synchronization between administrator and server. Thus, the massage will be sent with previous data as a key, where the server can decrypt the data and update his key and generate the new seq for next massage smoothly. In emergency situation, or if a massage is missed as shown in Figure 4. (b and c), which cause de- synchronization, the initial stage will be reactivated then the initial key will be used to encrypt and decrypt the massage.

B. Power Consumption and Complexity Analysis

1) Power Consumption: It has been concluded by [12] that the size of the massage (mainly increasing the size of message) in the algorithm instructions is the main factor affect the power consumption. In our approach, we use the lightweight Algorithm, with two main light operation (Xor, Hash(.)) to minimum massage size. Moreover, updating the key periodically is proposed to enhance data security.

2) Complexity Analysis: Given n Massages $M = (M_1, \ldots M_n)$, the time complexity using algorithm for three stage is O(n), where every Massage needs for O(1) for encryption. In this paper to minimize the algorithm time complexity we store and update new dynamic key is stored and updated in the Administrator side. In the server side, the same complexity time is needed for decryption O(n), Where O(1) is needed for every Massage and thus O(n) are needed to generate sequence number. One initial secrete key is needed for every doctor or reserve, where the initial key size should be equal to the size of all sensors data together at least.

V. CONCLUSION AND FUTURE WORK

We are proposing a light weight management BSN protocol to enhance the security between the administrator machine and server. Where the sensitive data of the patients could be threatening in case of eavesdropping, data modification attack, impersonation attack, and replay attack. As the proposed solution we proposed a dynamic key exchange protocol to ensure the security and privacy of the BSN patient data. In our proposal the protocol have a low power consumption feature which will enhance the node size as well as it's battery. The proposed protocol does not need high computational power which will facilitate the implementation and distribution of the BSN. As a future work some enhancement could be provided to secure the communication and data between the sensors and the administrator machine and providing a real environment to implement the solution.

REFERENCES

[1] D. Sehrawat and N. Gill, "Smart Sensors: Analysis of Different Types of IoT Sensors", 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019.

[2] G-Z. Yang, Body sensor networks, Springer, 2006.

[3] P. Gope and T. Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network", IEEE Sensors Journal, vol. 16, no. 5, pp. 1368-1376, 2016.

[4] X. Tian, X. Yang and J. Ho, "Energy-efficient and Secure Wireless Body Sensor Networks with Metamaterial Textiles", 2019 IEEE Biomedical Circuits and Systems Conference (BioCAS), 2019.

[5] L. Guo, Z. Chen, D. Zhang, J. Liu and J. Pan, "Sustainability in Body Sensor Networks With Transmission Scheduling and Energy Harvesting", IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9633-9644, 2019.

[6] F. Miao, L. Jiang, Y. Li and Y. Zhang, "A Novel Biometrics Based Security Solution for Body Sensor Networks", 2009 2nd International Conference on Biomedical Engineering and Informatics, 2009

[7] S. Yoo and F. Castro De La Gruz, "Enhanced BSN-Care: Cryptanalysis of BSN-Care and proposal of improved authentication system", 2016 IEEE International Symposium on Robotics and Intelligent Sensors (IRIS), 2016

[8] Shu-Di Bao, Yuan-Ting Zhang and Lian-Feng Shen, "A Design Proposal of Security Architecture for Medical Body Sensor Networks", International Workshop on Wearable and Implantable Body Sensor Networks (BSN'06).

[9] S. Chang, S. Ji, J. Shen, D. Liu and H. Tan, "A Survey on Key Management for Body Sensor Network", 2015 First International Conference on Computational Intelligence Theory, Systems and Applications (CCITSA), 2015.

[10] C. Tan, Haodong Wang, Sheng Zhong and Qun Li, "IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks", IEEE Transactions on Information Technology in Biomedicine, vol. 13, no. 6, pp. 926-932, 2009.

[11] A. Brisson, "Deterministic random number generation for one time pads: Creating a Whitenoise super key", 2017 IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computed, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2017.

[12] M. Sibahee, S. Lu, Z. Hussien, M. Hussain, K. Mutlaq and Z. Abduljabbar, "The Best Performance Evaluation of Encryption Algorithms to Reduce Power Consumption in WSN", 2017 International Conference on Computing Intelligence and Information System (CIIS), 2017.

[13] Taparia, A., Panigrahy, S., Jena, S., 2017. Secure key exchange using enhanced Diffie-Hellman protocol based on string comparison. 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET).