Comparison of Hash and Cryptographic Algorithm to Secure Intra-BSN Communication in Wireless Body Area Sensor Networks

T. GayathriMathambigai, R. Rekha and R. Vidhyapriya

Abstract--- Body Sensor Network (BSN) is emerging as one of the main research trends in the telemedicine application. BSN interconnects the biosensors placed in the human body. Since the medical information is sent over the network, the security plays a vital role in the BSN. The solution to this problem is using the biometric approach for securing the keying materials. The conventional biometrics like fingerprint, face recognition cannot be used in the BSN because it is not having high randomness and it is time invariant. Thus novel biometrics can be used. Human body is inherently having the ability to communicate in a secure manner. Thus the physiological characteristics can be captured by the sensors of BSN to generate the entity identifier. The biometrics can be used to distribute the key in a secure manner. The InterPulsed Interval (IPI) of the ElectroCardioGram (ECG) signal has been used as a biometric trait for securing the communication between the nodes in the BSN and to avoid interference. The generation of biokey from the ECG signal and high randomness obtained has been shown using MATLAB V 7.8.0. Biokey has been encrypted with the MD5 and DES algorithm and the results have been shown. The performance of the hash and cryptographic algorithm has been compared.

Keywords--- Biokey, InterPulsed Interval, Security, Wireless Networks.

I. INTRODUCTION

WIRELESS SENSOR NETWORKS are used for various applications such as health monitoring, environmental agriculture, seismic detection etc. The health monitoring is very important to lead a quality life. The health monitoring has to be done periodically for the senior citizens. It is not possible for them to be in hospitals for a long period of time. By using the development in technology, they can take treatment from being in home. Thus the BSN can be used for health monitoring application. Body Area Sensor Networks (BASN) are the networks of wireless medical sensors for monitoring the health of a person continuously in order to avoid any discrepancy. BSN consists of biosensors, which may be implanted inside the human body or a wearable device.

The biosensors are used in the field of biomedicine and biotechnology. They are used to analyze the biological samples to understand about their structure, bio-composition and function. It will collect the data from the human body and transmit it to the medical server through a wireless link. Before transmitting, the data has to be centralized in a hub or any other storage to reduce energy consumption. A BSN proves to be adequate for emergency cases because it autonomously sends data about patients’ health so the physician can prepare for the treatment immediately.

Figure 1: Biosensor to Measure ECG Signal

Wireless Personal Area Network (WPAN) technologies can be used to communicate over the shorter ranges. IEEE classifies the WPAN and created a new standard for the networks that are operating in the human body. IEEE 802.15.6 was formed in the
year 2007 to create a standard for the BAN with the scope of “short range, wireless communication on or inside the human body” [5]. There should not be any interference during the communication between the sensors in the BAN. While transmitting, there are chances for the intruder to get the information and they may attempt to change the profile. On the other hand, the doctors will prescribe the drugs for the patients through the wireless link. At that time, intruder may make changes to the drug dosage details and it may cause harm to the patients’ health.

Thus the main problem that has to be solved in the BSN is the security. The architecture of BASN, its challenges, security requirements and the security methodologies will be discussed detail in the later sessions. The image of a biosensor to record the ECG signal is shown in fig 1.

II. BODY SENSOR NETWORKS

Different types of sensors may be placed on the human body or it is implanted inside the human body and it is termed as Wireless Body Area Sensor Networks (WBASN). BSN can also be termed as BASN or WBASN. The information from the WBASN has been sent to the personal device such as PDA or mobile. Each WBASN will have a base station to which it has to send the medical data. The information from the biosensors can reach the base station either in a single hop or multi hop. Then it will be sent to the medical server or to the physician for treatment. The doctor will prescribe the drugs for the patients.

![Figure 2: Body Area Networks](image)

Fig 2 shows the architecture of Body Sensor Network. WBASN can be used for medical applications like epileptic seizure warning, glucose monitoring and cancer detection. WBASN can also be used for non medical applications. It can be used as assistance to the people who has disabilities. It can be used as muscle tension monitor, blind, speech disability and artificial hands. To implement the WBASN, specific requirements have to be satisfied. Since it is used in the medical application, it has to satisfy the following requirements. The requirements are,

1. The sensors can be placed in the human body in the 2-5 meters distance since it can communicate for a shorter range.
2. The interference should be avoided. The sensors from a WBASN should not interfere with another WBASN during the communication.
3. It must be possible to have more than one type of sensors for different applications.
4. The medical information is transmitted in the network so the transmission speed must be faster in order to save the life of patients’ during the emergency period.
5. The sensor information has to be passed through the human tissue. In the wireless technology, there is a problem of losing the path in the propagation medium. In WBASN, this problem has to be avoided because if there is any loss of information, it will affect the patients’ health.

According to Health Insurance Portability and Accountability Act (HIPAA), the patients’ personal information and medical data should be kept confidential. Security plays a vital role in this application since the persons’ medical data and personal information were being transmitted. The integrity of the data should be maintained. Eavesdropping of the medical information should be avoided in order to secure the patients’ lives. The data should not be sent in a clear form since it may cause harm. The data has to be encrypted by using the cryptographic algorithms.

The WBASN can be divided into three levels of communication. The levels are,

1. Communication between the two nodes of the same WBASN (Intra-BSN)
2. Communication between the node and the base station
3. Communication between the Base station and the medical hub

In WBASN, there may be chance for the nodes of the same BSN to communicate with each other. During this communication, we have to determine whether the node which is requesting for the communication, belongs to the same BSN in order to avoid the interference. Since it is a wireless network, the sensors tend to communicate with the parties which are in the shorter range to it. The medical information are transmitted through the wireless network so more security has to be provided. This is known as Intra...
BSN Communication.

The information has to be transmitted from the node to the base station by using any cryptographic techniques to ensure the security. It is possible for the intruders to get the medical information during the transmission process. Security is the major concern in the medical applications.

The base station will transfer the medical data to the hospital server or medical hub or a back end server. The doctors will monitor the data which has been received and prescribe the corresponding drugs to the patients.

![Figure 3: Levels in BAN](image)

Due to the miniature of the biosensors, there are many constraints in the WBASN. Some of the constraints in the biosensors are experienced by the generic sensors. But the constraints are more for the biosensors.

The constraints are low power, limited memory, low computational complexity, low communication rate.

The data which is sent by the BSN to the network should satisfy requirements like confidentiality, integrity, freshness, availability and authenticity [8]. The eavesdropping of the data has to be avoided.

The BSN can be secured by using the following methods. They are, key distribution, predeployment of keys, pseudorandom numbers. These methods are not applicable to BSN due to drawbacks such as, the same key cannot be generated using pseudo random numbers since the hardware differs. Predeployment of keys is not suitable if any node has to be added or deleted.

So, the inherent properties of the human body can be used as a key for communicating in a secure manner. Thus the possible solution for the security problem is biometrics.

Biometrics is used to identify the individual uniquely by using physiological or behavioral properties. The physiological biometrics is fingerprint, face recognition, voice recognition, iris recognition etc. The behavioral biometrics is signature recognition and keystroke dynamics. It has been proved that the physiological signals of the individuals can be used as a biometric trait for the authentication and security purposes [9]. This method is having many advantages when compared to the previous techniques.

Many physiological features can be used as a biometric trait. They are ElectroCardioGram, PhonoCardioGram (PCG), blood glucose level, blood pressure, etc. The main advantages are time variance, key randomness, universality, and key recoverability.

The conventional biometrics do not depend on the time of it is measurement. But the novel biometrics will vary depending upon the time. Thus it can be used in the BSN for authentication purpose. A good cryptographic key should have high randomness and it should be time variant. Hence the intruder cannot be able to predict the key. Thus ECG can be used in the BSN for the security purposes.

III. RELATED WORK

Cherukari et al., has proposed that the physiological signals can be used for the security purpose. The key has to be committed with the physiological signal and it will be decommitted in another node. The fuzzy commitment scheme can be used to commit and decommit the key. In the commit phase, the entity that has to be protected is c, which is committed with x. RC5 algorithm has been used for encryption and decryption process. The disadvantage of this method is increase in bandwidth due to the large computation. They mentioned that the timing information of the heart beat cannot be used as an entity identifier since it does not have high entropy [9].

C.Y. Poon et al., has proved that the timing information of heart beat can be used as a biometric trait. Fuzzy Commitment scheme has been used to commit and decommit the key with the biometric trait. Thus ECG signal can be used as a biometric trait.
The ECG characteristics have parameters like P, PQR, QT, QS can also be used for securing the data. The problems in this method are it is vulnerable to attacks by the Ultra Wide Band, UWB, Radar and finding the compensation mechanism for asynchrony of different channels [1].

Fen Miao et al., has proposed a method to use cryptographic algorithm for securing the keys in the BSN. S.M.K Raazi et al., does not give any details about securing the keys they have used. Thus the biometric trait can be encrypted by using the block cipher AES. By feeding back the key stream to the AES algorithm it can be considered as a stream cipher. AES operates as a better cipher algorithm when compared to the RC4 algorithm [4].

S. M. K. Raazi et al., has proposed a key distribution scheme known as BARI and here the problem of asynchrony of different channel has been avoided by using the key refreshment schedule. They have used three keys namely communication key, administrative key and basic key. A key refreshment module is used to depict the turn of each node for the key refreshment. The base station is referred here as the personal server which may be any hand held devices like mobiles or laptop. The personal server (PS) issues new key refreshment schedule periodically. Each node refreshes the key in the slot allotted to it. They did not give any details about securing the keys they have used [10].

F. Sufi et al., developed chaos based encryption method. It is used to prevent unauthorized access of ECG signal during transmission from node to the Base Station in WBASN. The Chaos key server will generate the true random numbers and it is known as chaos key. The Chaos key server’s efficiency is dependent on the initial conditions of the server. It is more sensitive. It is known only to the server. The hospital and the patient did not know about the initial conditions. The Diffie Hellman key exchange is used to exchange the chaos key between the base station and node [3].

IV. INTRA-BSN COMMUNICATION

The ECG signal is used as a biometric trait to secure the intra BSN communication. As discussed earlier, the three levels in the BSN has to be secured.

Some considerations have been made for the secure communication between the base station and the external network [6]. The security assumptions are,

1. The back end server is managed by the hospital or medical server. The base station will send all the medical data of the patients to the backend server. Consider that the back end server is physically protected.
2. Access control system has been implemented. So the authorized person can alone access the medical data.
3. The base station and the back end server have securely share the symmetric key to secure the communication between them. Since the medical data is transferred, end-to-end security between the base station and the back end server is necessary.
4. The secure key shared between them may be manually installed or it has been established using the key distribution secure protocol.
5. To avoid the location tracking, the end-to-end channel between the base station and the back end server will be anonymized using the temporary pseudonym.

The InterPulsed Interval (IPI) of the ECG signal is considered as a biometric trait in this system. The IPI is the time interval between the RR peaks in the ECG signal. The main process is generating the biokey from the ECG signal. The biokey can be formed by using the IPI of the ECG signal. The steps in generating the biokey is

1. Geneartating the ECG signal
2. Sampling the ECG signal
3. Finding the maximum amplitude in the ECG signal
4. Calculating the RR Intervals of the detected peaks
5. Converting into binary sequence to form the Biokey of 128 bits
After generating the biokey, the communication between the two nodes in the BSN has to be secured. The step for secure communication between two nodes is shown in fig 4.

Consider Node A needs to communicate with Node B. Node A will measure the ECG signal and the Biokey\textsubscript{A} will be generated. It will send Biokey\textsubscript{A} to the base station. The Node B will also measure the ECG signal and generate its biometric trait Biokey\textsubscript{B}. It will also send its biokey to the base station. The base station will compute the hamming distance between the Biokey\textsubscript{A} and Biokey\textsubscript{B}. S.D. Bao et al., proved that the hamming distance of Heart Rate Variability (HRV) of two identical person will be less than 22 bits and for the different person it will result in the approximately 80 bits or higher difference.

If the Hamming Distance (HD) between them is less than 22 bits, then the nodes are belonged to the same WBSN [7] [2]. The base station will send the value of HD to the node A and sends the NULL value to the Node B. The Node A will xor the HD value and its Biokey\textsubscript{A}

Data Encryption Standard (DES) and MD5 are used to compare the performance of the cryptographic algorithm.

Consider a 64 bit key has been shared between the Node A and Node B in a secure manner. At node A, the xorred value will be encrypted using the DES algorithm. At node B, the biokey will be xorred with the NULL value and it will be encrypted with the DES. The results will be shown in the next session.

Now, the MD5 algorithm is used for morphing the Biokey\textsubscript{A} generated from the Node A. The Node B will xor the NULL value and its biokey. Hence the morphing has to be done for the Biokey\textsubscript{A}.

If the Hamming Distance is approximately greater than 80 bits then it does not belong to the same WBASN and it is discarded. Thus the key has been exchanged securely between the two nodes in the WBASN.

V. EXPERIMENTAL RESULTS

Assume that node A of a person X has to communicate with node B of the same person. The ECG signal of a person X at the node A is shown below.
The node A’s ECG signal is sampled at the rate of 1000 Hz and it is shown in Fig 6.

The detected R peaks are plotted on the ECG signal of Node A (Person X).

The 128 bit length biokey of Node A has been generated (Person X).
The detected R peaks are plotted on the ECG signal of node B of person X.

The 128 bit length biokey of node B has been generated (Person X).

The hamming distance between the biokey of Node A and Node B is calculated to know whether it belongs to same BSN or not. The obtained hamming distance for both the nodes is 16. Thus it belongs to the same BSN.

DES algorithm is used to encrypt the biokey with the inbuilt key to get the shared secret key between node A and Node B. The shared secret key of node A is shown below.

The shared secret key of node B is shown below.
Figure 13: Shared Secret Key of Node B (Person X) using DES
MD5 algorithm has been used for morphing. The shared secret key for node A is shown below.

Figure 14: Secret Key at Node a using MD5 of Person X. The shared secret key for node B is shown below.

Figure 15: Secret Key at Node B using MD5 of Person X
Assume that node B of person Y needs to communicate with the node A of person X. The biokey of both the nodes will be
generated and it will be sent to the base station. The hamming distance between them is 72 and it is shown in fig 16. Thus the
two nodes do not belong to the same BSN.

Figure 16: Mismatch between Node A and Node B of Person X and Y

<table>
<thead>
<tr>
<th>Performance Measured</th>
<th>DES</th>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Size</td>
<td>64</td>
<td>No key</td>
</tr>
<tr>
<td>Block Size</td>
<td>64</td>
<td>512</td>
</tr>
<tr>
<td>CryptAnalysis</td>
<td>Possible if the Key has been known.</td>
<td>Less Possible since hash is used</td>
</tr>
<tr>
<td>Size of Output</td>
<td>64</td>
<td>128</td>
</tr>
<tr>
<td>Number of Rounds</td>
<td>16</td>
<td>64</td>
</tr>
<tr>
<td>Primitive Functions</td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td>Effect of one Bit change in the Plaintext</td>
<td>Output will not have more changes.</td>
<td>50% of the output bits will be changed.</td>
</tr>
</tbody>
</table>

MD5 is better when compared to the DES algorithm in terms of privacy and security. There are less chances to find out the result in MD5 but it is possible in DES if the key has been revealed.

VII. CONCLUSION

Wireless Body Area Networks (WBAN) is an enabling technology for mobile health care. These systems reduce the
enormous costs associated to patients in hospitals as monitoring can take place in real-time even at home and over a longer period. A critical factor in the acceptance of WBAN is the provision of appropriate security and privacy protection of the wireless communication medium. The data travelling between the sensor nodes should be kept confidential and integrity should be maintained. In this work, the secure communication between the sensor nodes has been successfully implemented. MD5 is better when compared to DES algorithm and it is proved. As further work, the communication between the node and the base station will be developed and the morphing algorithm’s performance can be evaluated by using cryptographic algorithms like SHA-1, SHA-512. WBAN is an emerging technology in the real world. If the security issues of WBAN reduce, the patients can take treatment from home. The patient can be monitored ubiquitously without disturbing their daily activities.

REFERENCES


