IAMKeys: Independent and Adaptive Management of Keys for Security in Wireless Body Area Networks

Raghav V. Sampangi[1], Saurabh Dey[2], Shalini R. Urs[2], and Srinivas Sampalli[1]

[1] Faculty of Computer Science, Dalhousie University, Canada
[2] International School of Information Management, India
raghav.vs@ieee.org, saurabh@isim.net.in, shalini@isim.ac.in, srini@cs.dal.ca

Abstract. Wireless Body Area Networks (WBANs) have gained a lot of research attention in recent years since they offer tremendous benefits for remote health monitoring and continuous, real-time patient care. However, as with any wireless communication, data security in WBANs is a challenging design issue. Since such networks consist of small sensors placed on the human body, they impose resource and computational restrictions, thereby making the use of sophisticated and advanced encryption algorithms infeasible. This calls for the design of algorithms with a robust key generation / management scheme, which are reasonably resource optimal. This paper presents IAMKeys, an independent and adaptive key management scheme for improving the security of WBANs. The novelty of this scheme lies in the use of a randomly generated key for encrypting each data frame that is generated independently at both the sender and the receiver, eliminating the need for any key exchange. The simplicity of the encryption scheme, combined with the adaptability in key management makes the scheme simple, yet secure. The proposed algorithm is validated by performance analysis.

Keywords: body area networks, body area network security, wireless network security, key management, encryption.

1 Introduction

Recent advances in wireless communication and sensor technologies have meant that sensors can be used efficiently in human health monitoring. With sedentary lifestyles already having increased the risks of potentially fatal medical conditions such as high blood pressure, cardiac diseases, diabetes, and the like, and given the unpredictable nature of worsening of any such condition in a person, regular and continuous monitoring assumes high priority.

Wireless Body Area Networks (WBANs) [1] are a type of wireless sensor networks, where a group of sensors placed on the human body measure specific physiological parameters of a person and relay it to the monitoring medical center or hospital. This relay happens via the Internet or a cellular network, using

N. Meghanathan et al. (Eds.): CCSIT 2012, Part III, LNICST 86, pp. 482–494, 2012.

personal digital assistants (PDAs) or cellular phones as intermediary devices. Thus, WBANs seem to be a promising solution for the problem of continuous health monitoring. However, with a patient's personal health data travelling in the open, typically in a wireless channel, to reach the intermediary device and then the monitoring station, securing this data becomes critical. This, coupled with the fact that medical decisions are made based on the data received, assumes significant focus in the research on WBANs.

To achieve security in any network, the messages to be transmitted are encrypted using specialized encryption schemes and a special encryption key, and decrypted at the receiver end. Many advanced encryption algorithms, which are used for securing wireless networks, however, cannot be used in WBANs, given that they have severe power constraints and resource constraints since they are small sensor devices residing on a person [1]. Thus, it becomes crucial to design algorithms that are simple in computation and resource utilization, yet achieve the desired security. At the heart of any encryption algorithm is the successful management of the special encryption key. The key generation scheme must also be computationally inexpensive yet secure.

This paper presents a dynamic key generation/management scheme for encryption of data in a WBAN, with focus on security in the part of the network from the central controller node of the WBAN to the receiver at the monitoring station. This scheme makes use of the random nature of the physiological parameters and the simplicity of stream-cipher encryption scheme to achieve efficient encryption of sensor recorded data in the WBAN.

The rest of this paper is organized as follows: Section 2 presents the related work. Section 3 describes the proposed algorithm. Section 4 presents the performance analysis of the algorithm, while Section 5 provides a brief discussion on the scheme and its limitations. In Section 6, we conclude the paper and present a glimpse of the future work.

2 Related Work

A comprehensive description of WBANs, with a detailed description of the system architecture, construction and tested prototypes, is provided in the work by Otto et al [1]. In their work, they present the implementations of an activity sensor that detects an organ's activity, a motion sensor that detects the motion of the person, and a personal server (PS), with a network controller. Though the authors have described in detail the implementation aspects, they have very briefly described a possible security protocol for ZigBee. Data recorded and communicated by WBANs have a direct impact on the decisions made concerning a person's health and well-being. Thus, ensuring the reliability and security of this data assumes a central role in such a system.

Tan et al [2] present an identity-based encryption (IBE) scheme called IBELite for security in WBANs. In this scheme, a sensor generates a public key dynamically using an arbitrary string, but the sensors cannot create secret keys. They, thus, use a trusted third party to ensure security of data in WBAN.

Moving away from the conventional key generation schemes and capitalizing on the inherent random and time variant nature of biometric data, Venkatasubramanian et al [3] present a scheme where the electrocardiogram (EKG) signals of a person are used to generate cryptographic keys between two nodes in a WBAN. The sensors in the network agree upon a common key, generated based on the EKG reading of the patient, to secure inter-sensor communication. Mana et al [4,5] also use EKG signals to secure keys between sensor nodes and the base station, thereby focusing on securing the end-to-end communication, as well as communication among the nodes. On the other hand, Raazi et al [6] propose a scheme where any one of the recorded biometrics is used as the encryption key and is periodically communicated by the personal server to the nodes, as key refreshment schedules.

The proposed algorithm in this paper focuses on exploiting the random nature of physiological data and by introducing additional randomness dynamically. With an underlying distinction of the physiological data between people, this work aims to exploit these characteristics to implement a simple key generation scheme for securing data in a WBAN.

3 The Proposed Algorithm: IAMKeys

We consider the WBAN illustrated in Figure 1 for the purposes of this work. It includes sensors to measure the heart rate (S1), the blood pressure (S2) and the blood glucose (S3) of a patient. The sensors send their recorded data (after basic filtering to remove the noise) to the WBAN Central Controller Node (WCC), which is marked as the sensor node SC in the figure. SC acts as the sink node for receiving the data on the body. The WCC then aggregates the readings in a data frame, along with a sequence number and a timestamp. Figure 2 illustrates the data frame structure. The WCC encrypts the data frame and forwards it to the medical monitoring station, via the intermediate personal device, which in our example is a cellular phone. We consider securing the portion of this WBAN system beginning at the WCC and culminating at the monitoring station.

Resource restriction in WBANs is one of the primary reasons that led us to develop a customized encryption and key management algorithm. Since the network is deployed on the human body, frequent maintenance activities, such as replacement of batteries, would prove highly inconvenient for patients. In case we manage to strike a balance between the computational expense and the algorithm, the next concern to be addressed is that of key exchange. In other proposals, any encryption key that is generated (or refreshed) is exchanged between the sender and the receiver. If an adversary were to eavesdrop on such a conversation, the entire communication between the sender and the receiver will be jeopardized and vulnerable to attacks.

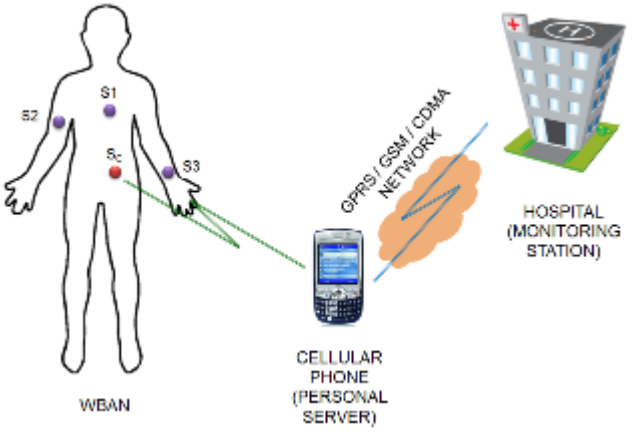

Fig. 1. WBAN used for the purposes of this work

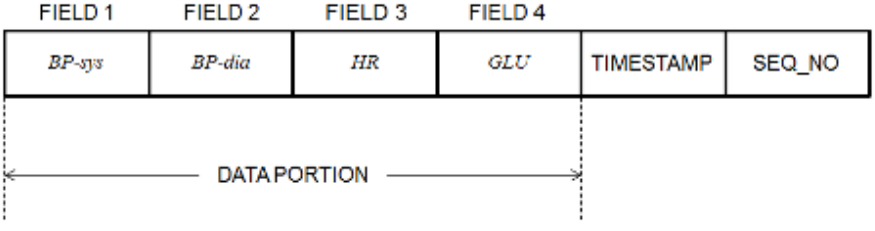

Fig. 2. Data frame format considered in this work

An obvious solution to such an impasse is the use of symmetric cryptography. However, the key being constant in such schemes poses a threat to the system in question. Our work revolves around a scheme that:

- Nullifies the need for key exchange;
- Enables independent generation of keys at both sender and receiver;
- Ensures sender authentication;
- Simplifies the encryption process; and,
- Prioritizes freshness of data

To ensure the successful operation of such a scheme, we make the following assumptions:

- An administrator at the monitoring station (typically, a hospital) deploys the WBAN on the patient.
- At the time of installation, the administrator loads five “dummy” reference frames into both the WCC and the monitoring station data receiver.
- The receiver acknowledges every successful transmission.
- The sender receives the acknowledgement within the transmission of three subsequent frames.

- The study of the effects of radiation of the sensors on the human body has not been considered in this work.

Figure 3 illustrates the proposed scheme in brief. Each data frame is encrypted using a stream cipher based encryption scheme, with a key that is a pseudorandom number. A pseudorandom number generator (PRNG) generates the key using one of the randomly chosen data fields of one of the randomly chosen reference frames as the seed. The encrypted frame is then transmitted.

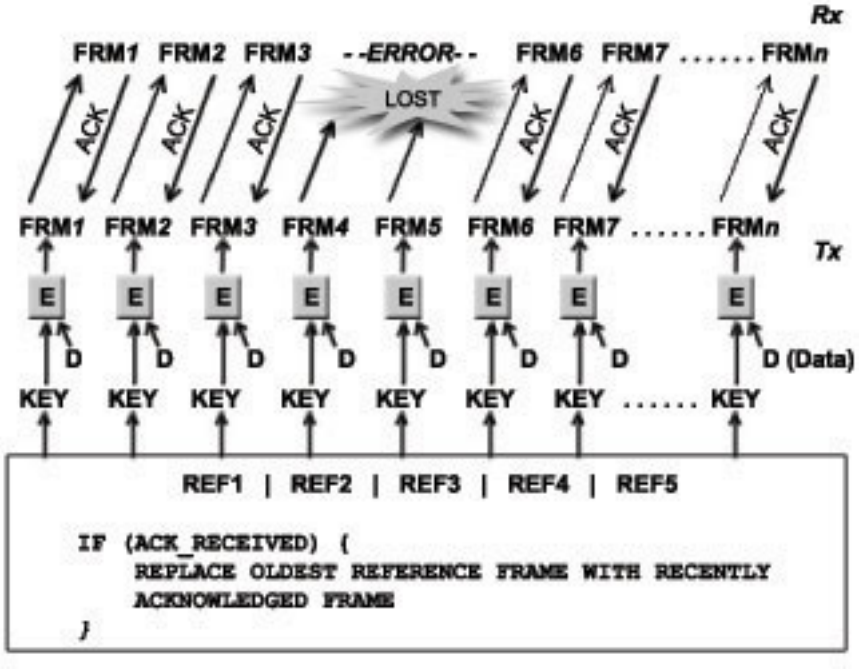

Fig. 3. Overview of the proposed scheme

Upon reception, the receiver verifies the identity of the sender, and on successful authentication, generates the key independently to decrypt the data. Following this, the receiver sends an acknowledgement to the sender (WCC). Upon receiving the acknowledgement, the WCC updates the reference frame list by replacing the oldest reference frame (indicated by the sequence number) with the currently acknowledged data frame. This is a gist of the operation of the presented scheme. In the following sub-sections, we describe the constituents of the scheme in detail.

3.1 Reference Frames

A crucial component of this scheme is the list of five reference frames that are a stored both at the sender and the receiver. During the WBAN deployment, the administrator loads these reference frames with identical dummy values at both the WCC and the monitoring station data receiver. When the receiver successfully receives the sent data frame, it sends an acknowledgement (ACK) to the WCC, along

with the sequence number. Then, the receiver waits for one more reception, and updates its reference frame list. Upon reception of the ACK, the WCC proceeds to update its reference frame list. The reference frame list is updated as follows. The sender (or, receiver) checks for the oldest reference frame in its list. This is assumed to be the frame with the oldest sequence number. The system then replaces this reference frame with the acknowledged frame.

3.2 Sender Authentication and Tone

Each encrypted data frame that is transmitted is appended with the sequence number of the reference frame used for generating the key, the field number in this reference frame whose value is used as the seed, a "Tone" value, and a sender authentication code.

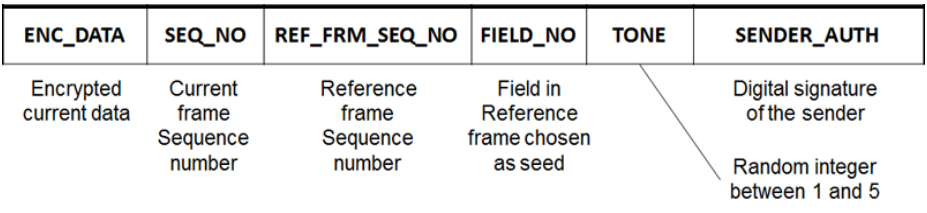

Fig. 4. Structure of the transmitted frame

The transmitted frame is as illustrated in figure 4. The tone is a random number between 1 and 5, generated for each data frame. To generate the sender authentication code, the reference frame that was chosen to generate the encryption key is hashed the number of times indicated by the Tone value of that frame. This is analogous to generating a digital signature of the sender on the fly for each transmitted frame. The receiver repeats this process by retrieving the reference frame pointed by the reference-frame-sequence-number that was received as part of the transmitted message to authenticate the sender. The value of the tone has a minimum value of 1so as to ensure that the reference frame is hashed at least once, and has a maximum value of 5 to ensure that the hashing process does not become increasingly computationally expensive.

3.3 Key Generation and Management

After aggregating values for the data frame, the WCC proceeds to generate the keys for encrypting the current frame. It begins by randomly choosing one of the five reference frames, and one of the data fields of the chosen frame. The value of this field will be used as the seed for the PRNG, whose output will be the key, K1, which is logically inverted to generate key, K2. To avoid exchange of the keys, the WCC appends the sequence number of the reference frame and the field number in this frame as REF_FRM_SEQ_NO and FIELD_NO, respectively, in the transmitted frame. The receiver, after authenticating the WCC, initiates the key generation process by first retrieving reference frame sequence number, followed by the field

number. The receiver then retrieves the value of the particular field from its reference frame list, and uses this value (could be any biometric value in the reference data frame) as the initial seed for the PRNG to generate K1 and inverts it to obtain K2. The key generation operations are summarized in equations (1) and (2). These are the two keys that are used for the encryption and decryption processes, and are independently generated at both the sender and the receiver.

$$K1 = PRNG\ (SEED) \tag{1}$$

$$K2 = INVERT\ (K1) \tag{2}$$

where,

PRNG () = Pseudorandom number generator

SEED = Value of the field pointed by FIELD_NO, in the reference frame pointed by REF_FRM_SEQ_NO

INVERT () = Logical inversion operation

3.4 Data Encryption

Once the keys are generated, the WCC proceeds to encrypt the data. The encryption process is a combination of the concepts of block and stream ciphers, to ensure a simple encryption process that is also slightly complex. This proceeds as follows. At the time of data aggregation, the WCC assembles data as blocks of k bits. This is to avoid the additional computation required to divide the aggregated frame into blocks of the specified size. The k bit blocks of data and the keys, K1 and K2, are then divided into equal halves.

The encryption involves two rounds, one for each key. In the first round, the left half of the data is encrypted (XORed) with the right half of K1 to yield the right half of the intermediate frame, and the right half of the data is encrypted with the left half of K1 to yield the left half of the intermediate frame. The intermediate frame is the output of the first round of encryption. In the second round, the same logic as above is applied to the intermediate frame with K2. The left half of the intermediate frame is XORed with right half of K2 to yield right half of the encrypted frame, and the right half of the intermediate frame and left half of K2 are XORed to yield left half of the encrypted frame. Thus, after two rounds of encryption, the order of the data is preserved, but data is encrypted using a complex mechanism. Figure 5 summarizes the encryption process, and the operations are summarized in equations (3) and (4).

$$E1 = [\ XOR\ (RHD, LHK1) \mid XOR\ (LHD, RHK1)\ ] \tag{3}$$

$$E2 = [\ XOR\ (RHE1, LHK2) \mid XOR\ (LHE1, RHK1)] \tag{4}$$

where,

E1, E2 = Encrypted frames after round 1 and round 2, respectively

XOR () = The logical XOR function, that performs exclusive OR operation on its arguments

LHD, RHD = Left and Right halves of the Data frame

LHE1, RHE1 = Left and Right halves of the Intermediate encrypted frame (after round 1)

LHK1, RHK1, LHK2, RHK2 = Left and Right halves of the keys, K1 and K2, respectively.

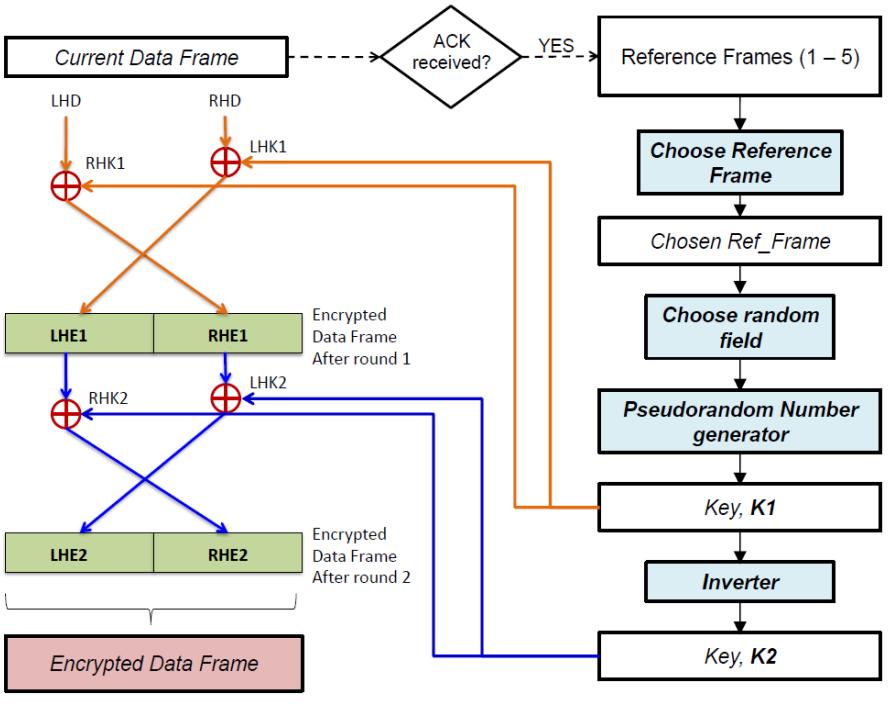

Fig. 5. Illustration of the Encryption process

3.5 Acknowledgements and Data Freshness

In applications that employ WBANs, such as healthcare, freshness (or recentness of data) is of utmost importance. Thus, even if a couple of frames are lost in transmission, and the WCC does not receive the corresponding acknowledgements, it continues to generate keys using the existing reference frames, and transmits the latest data frame encrypted using the keys generated. The concept of re-transmission of a lost data frame is not considered in such a scenario, with data freshness assuming priority. However, one needs to monitor the number of frames, which have not been acknowledged by the receiver. This is to avoid a case of lost connection between the WCC and the monitoring station, when several continuous frames are lost.

To address this, the WCC maintains a count of the number of frames, which have been transmitted since the transmission of a frame, say x1. If the acknowledgement is not received from the receiver within the transmission of 10 subsequent frames, the connection between the WCC and the monitoring station receiver is considered to be lost, and an alarm is raised. Meanwhile, if the receiver does not receive 10 consecutive frames, it considers the connection to be lost. In such a scenario, the administrator has to reset the connection.

4 Performance Analysis

Preliminary analysis of proposed algorithm was done with a java program to emulate the desired operation.

All the values/ sensor readings were randomly generated using predefined mathematical random functions in java packages. In their work, Venkatasubramanian et al [3] present an analysis of randomness, time-variance and distinctiveness characteristics of the keys generated as performance analysis, based on which we present an analysis of our scheme.

Randomness is the unpredictable nature of the keys used. In the proposed scheme, randomness of the keys generated by the PRNG is dependent on the seed, which is a function of three parameters—the chosen reference frame, the field in the reference frame, and the value of the field (physiological data). Since each of these values are randomly chosen for each data frame being encrypted, the randomness property of the seed, and hence the key, is preserved. We generated 100 frames of data, and noted the values of the offsets of randomly chosen reference frames and fields. Figure 6 illustrates the randomness of the reference frames and the field number values that were generated. *Distinctiveness* refers to how different the keys are when compared to different individuals. We observed from our simulation that keys are only identical for a person if the readings are exactly identical and the random reference frame or field values generated are the same, which is highly unlikely.

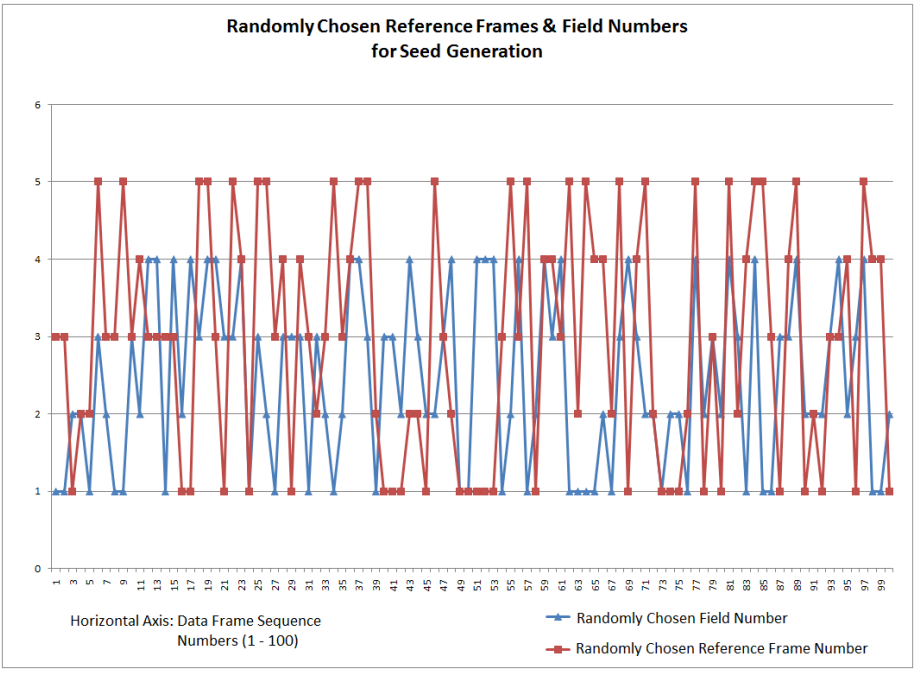

Fig. 6. Simulation of reference frames and field numbers

Time-variance of the keys implies that different instances of time should produce different keys. Not all sensor readings would vary drastically between intervals, and

any drastic variation would indicate that the patient might be in distress. The time-variant nature of the keys is a function of the randomness property, and since the keys generated are random, we can say that they are time-variant as well.

We analyze the complexity of the algorithm by determining the number of logical operations performed in the encryption and decryption of one data frame. However, for analysis purposes, we make the following assumptions:

Table 1. Number Of Logical Operations In Key Generation And Encryption / Decryption Of One Frame In IAMKeys

Operation	Encryption #	Decryption #
Random number generation Encryption: choice of reference frame, field in the reference frame, K1 generation, tone generation Decryption: K1 generation	4	1
Inversion Encryption & Decryption: Generation of K2	1	1
Exclusive OR (XOR) Encryption of each half of data in two rounds; and, Decryption of each half of data in two rounds.	8 x 4	8 x 4
Addition (or, increment) ## Encryption: Sequence number, ACK monitor counter, addition of data fields in reference frame for hashing Decryption: transmitted frame monitor counter, addition of data fields in reference frame for hashing	8 x 5 x (2 + α)	8 x 5 x (1 + α)
Hash operation Encryption & Decryption: dependent on the tone value in the reference frame	β	β
Reference frame refresh Encryption & Decryption: 0, if no ACK 1, if ACK received	γ	Γ
Frame transmission Encrypted frame and Acknowledgement frame transmission	1	1
Total	**118+40α+ β+ γ**	**75+40α+ β+ γ**

Addition and XOR operations are multiplied by 8, since they are bitwise operations.
Since 5 logical operations are performed per bit addition, we multiply the factor by 5.

- Data in each field of the frame is 8-bits.
- The PRNG is implemented using 8-bit Linear Feedback Shift Registers (LFSR).
- Reference frame and field numbers are randomly identified by numbers generated using 4-bit LFSRs.
- For addition operation, we consider the use of a *full adder* circuit for adding each bit, which employs 2 XOR gates, 2 AND gates and 1 OR gate. Hence, each bit addition will contribute to 5 logical operations [8].
- For sender authentication, hash operation is performed on the sum of all data values in the reference frame. If $\alpha+1$ is the number of fields in the frame, then, there will be α extra additions during encryption/decryption.
- We have assumed that reference frame list refresh and frame transmission do not count as logical operations, and thus, have not included these numbers in the calculations in table 2.
- Hash operation is assumed to be one-bit circular left shift operation, contributing to one logical operation.

Table 1 highlights the various logical operations in key generation and encryption/decryption of one frame. Table 2 presents the total number of logical operations, with calculations based on assumed values for α, β and γ listed in table 1. The major contributing factor to the total logical operations is the sender authentication, which decides the value of β.

Table 2. Number of logical operations in IAMKeys, with calculations based on assumed values of α, β and γ

Operating Scenarios	Total number of logical operations	
	Encryption	***Decryption***
Best case scenario (4 data fields => $\alpha = 3$; Tone value = $\beta = 1$; ACK received => $\gamma = 1$)	240	197
Average case scenario (4 data fields => $\alpha = 3$; Tone value = $\beta = 3$; ACK received => $\gamma = 1$)	242	199
Worst case scenario (4 data fields => $\alpha = 3$; Tone value = $\beta = 5$; ACK received => $\gamma = 1$)	244	201

5 Discussion

With the primary objective of a WBAN being transmission of patient data with as little delay as possible, and such transmission being fool-proof, security and data freshness assume highest priority. In this algorithm, we focus on data freshness with removing the need for retransmission of a lost frame. Instead of retransmission, the

algorithm transmits the frame with the latest data values, hence, maintaining the data fresh. In case more than ten frames are lost or not acknowledged, the sender or the receiver will flag an error, and the administrator will need to check the communication link.

IAMKeys focuses on independently generating keys at both the sender and the receiver. The keys generated will be random for the encryption of each frame, due to the following reasons:

- Randomly, one reference frame out of the five in the list is chosen.
- A random data field is chosen in this reference frame.
- Even though the data may not be very random, the fact that such a data field is chosen randomly from a random reference frame, in addition to refreshing the list of reference frames, induces a sense of randomness in the keys generated.

With security assuming high priority, optimizing resource utilization becomes a challenge. Tables 1 and 2 indicate that the resource utilization varies mainly based on the value of β, which differs for each frame based on the randomly chosen reference frame. However, the actual implementation of hash operation and its complexity will vary the number of operations significantly. This gives the first limitation of this approach, where the complexity is not constant.

One of the important forms of attacks that we need to consider to analyze the security of such a system is man-in-the-middle (MITM). If an adversary were to listen to every conversation occurring in the system and modify the data as required, it would constitute MITM attack. Since randomness of the keys generated in this scheme is a function of three parameters, the proposed scheme has the property of dynamically changing encryption keys, which are not exchanged.

Another important attack that can be considered is the session hijacking, where the adversary initially becomes a part of the network, and gains control of the communication by assuming the role of either of the communicating entities. The decryption of each frame depends on the earlier successfully transmitted frames, which act as reference frames. Further, since reference frames also authenticate the sender, it would be impossible for the adversary to pose as a sender with the absence of the refreshed reference frame list, thereby keeping data secure. However, he may pose as the receiver, since the receiver is not acknowledged in the current implementation. This improves security of such a WBAN system and reduces the probability of an adversary taking control of the conversation.

One of the other limitations of the proposed scheme is relying on humans to ensure the randomness of the dummy (or initial) reference data frames. This can be avoided using an automated program to randomly assign dummy reference frames during the initial set up in the hospital. The second limitation of this scheme is that it if the acknowledgement frame were lost, then, there would be no way for the monitoring station to know if the acknowledgement failed, and no way for the WCC to know that the monitoring station received the transmitted could, however, be avoided if there were two-way acknowledgement, where the transmitted frame would also contain the acknowledgement of the previously acknowledged frame by the receiver. Though the proposed algorithm has some notable limitations, the chaotic nature that it imposes on key generation keeps the algorithm stable and efficient, and less prone to attacks.

6 Conclusion and Future Work

In this paper, we presented a novel algorithm that randomly generates and uses keys for encrypting each data frame in a WBAN. The algorithm randomly picks one of the random frames and one of the random sensor readings from it, and uses this value to generate a pseudorandom number sequence as the key to encrypt the message. The encryption process uses a combination of the concepts of block and stream ciphers, and uses blocks of the data frame being encrypted using simple XOR as in stream ciphers. The division of a data frame into blocks before encryption ensures the security of data by confusion and diffusion, as in block ciphers. The use of XOR encryption as in stream ciphers ensures that single bit errors remain single bit errors and do not propagate. The algorithm exploits the distinct nature of readings among people and the induced randomness of the keys to ensure efficiency. To ensure that the sender is genuine, a hash function-based (or a dynamic digital signature) authentication is employed. As discussed in the previous section, the proposed algorithm achieves confidentiality, integrity, authentication, and non-repudiation, which are a part of the generic security goals of any network.

Future work on this algorithm involves addressing the two limitations listed in the previous section, followed by validation using further simulation exercises. This will be followed by implementation of the algorithm on actual hardware, and the evaluation of the overall system.

References

1. Otto, C., Milenkovic, A., Sanders, C., Jovanov, E.: System Architecture of a Wireless Body Area Sensor Network for Ubiquitous Health Monitoring. Journal of Mobile Multimedia 1(4), 307–326 (2006)
2. Tan, C.C., Wang, H., Zhong, S., Li, Q.: Body Sensor Network Security: An Identity-Based Cryptography Approach. In: Proc. WiSec 2008, March 31-April 02 (2008)
3. Venkatasubramanian, K.K., Banerjee, A., Gupta, S.K.S.: EKG-based Key Agreement in Body Sensor Networks. In: Proceedings of IEEE INFOCOM Workshops 2008, pp. 1–6 (April 2008), doi:10.1109/INFOCOM.2008.4544608
4. Mana, M., Feham, M., Bensaber, B.A.: SEKEBAN (Secure and Efficient Key Exchange for Wireless Body Area Network). International Journal of Advanced Science and Technology 12, 45–60 (2009)
5. Mana, M., Feham, M., Bensaber, B.A.: Trust Key Management Scheme for Wireless Body Area Networks. International Journal of Network Security 12(2), 71–79 (2011)
6. Raazi, S.M.K., Lee, H.: BARI: A Distributed Key Management Approach for Wireless Body Area Networks. In: Proceedings of 2009 International Conference on Computational Intelligence and Security, pp. 324–329 (December 2009), doi:10.1109/CIS.2009.186
7. Robshaw, M.J.B.: Stream Ciphers, in RSA Laboratories Technical Report TR-701, version 2.0 (July 1995)
8. Mano, M.M., Ciletti, M.D.: Combinational Logic. In: Digital Design, 4th edn., pp. 135–196. Pearson Prentice Hall, New Delhi (2008)