Sequential Encryption for Multiple Implantable Medical Devices

Taha Belkhouja*, Sameh Sorour*, Mohamed Hefeida*
*Electrical and Computer Engineering Department, University of Idaho, Moscow, ID, USA
Email: belk7517@vandals.uidaho.edu, samehsorour@uidaho.edu, hefeida@uidaho.edu

***Abstract*—Wireless communication became an essential tool for modern Implantable Medical Devices (IMDs) for information exchange. In spite of the many advantages wireless technology has, it puts the patients health in serious danger if no proper security mechanism is deployed. We aim to secure these devices while taking into consideration the limitations these small devices suffer from. IMDs have resources that are relatively simple and sometimes require surgery to be altered. Consequently, common security mechanisms cannot be simply implemented in fear of consuming all the resources dedicated to healthcare needs. A certain balance between security and efficiency must be sought in each IMD architecture. In this work, we propose a sequential and secure encrypted communication scheme for patients with multiple IMDs. We present a model that delivers the information generated by all IMDs in one packet to the final receiver. This information will be encrypted sequentially going from one IMD to the next. This scheme eliminates the need for single IMD authentications with the receiver. Instead of each IMD communicating independently with the same receiver, each device will send its information to a different IMD in a single communication action. Performing this way, the scheme would exploit the inherent properties of the entropy of the physiological signals to randomize the exchanged messages. The scheme succeeded in NIST tests with high rates around 95%. This relieves the IMDs from the need for the encryption in addition to a recovery rate of 100% for the proposed architecture. At the end, the final message will be attack-resistant with length $< 1Kb$ in short handling time in order of 100 ms.**

Keywords*—Implantable Medical Devices, Wireless communication, Sequential encryption, Secure healthcare.

I. Introduction

The global Implantable Medical Devices' market is witnessing a significant increase in these years. The rising number of technological advancements in the field of medical science and treatment is mainly contributing to this expansion. It is is anticipated to be worth 49.8 billion USD by 2024 [1]. Wearable or Implantable Medical Devices (WMD/IMD) contribute significantly to improving patients' quality of life by remotely treating their health issues. They enable easy and efficient diagnostics and monitoring of the patient's health status in real time. Also, they provide more efficient and scalable healthcare as it allows physicians to better utilize their time and be more efficient. They contribute mainly to decrease the burden of medical attention a patient requires, essentially if he/she is suffering from a chronic disease. In addition to the medical performance, an IMD is required to protect the patient: It must be secured from any external hijacking action and able to protect the stored private data. Researchers are aware of the severe limitations of IMDs regarding energy consumption and low resources. For this reason, their goal is to find the best trade-off between efficiency and security. This solution needs to guarantee that access is provided for the patient and any other authorized party, while protecting the user at the same time from any other malicious agent. An adversary may interfere with the regular functions of an IMD and launch different types of attacks. These attacks are mainly categorized into two different types:

- Passive attacks: These attacks are about listening to any communication signals in the network. Therefore, the eavesdropper is able to obtain and store confidential medical logs or personal information. This storage is useful whether for future attacks or for passive knowledge [2].
- Active attacks: These attacks are malicious commands triggered by an adversary to be executed at the IMD level. These commands have different goals: restraining the IMD from functioning, triggering the IMD to execute life-threatening actions or use the IMD as a relay node to access the network [3].

In our previous work [4], we have investigated chaotic generators for the design of a defense mechanism against Man-In-The-Middle attacks. This mechanisms relies on a dynamic signatures that validate the trusted users. Once this trust is built, an attacker cannot interact with the wireless communication. Also, we have reviewed the wireless communication scheme between an IMD and its remote control [5].We have proposed an authentication protocol to ensure the identity of the communicating parties using plain text messages, relying on Diffie-Hillman approach. Furthermore, scanning the literature, one can find some schemes developed for the specific security purposes of IMDs. One idea is to transfer the whole security process to be implemented on an external device, like the example of IMDGuard [6]. These external devices, unlike the IMDs, do not have any resources constraints or limitations. These devices allow the implementation of more robust algorithms but need to be always worn by the patient. In the same context, Gollakota *et al.* [7] explored the feasibility of protecting implantable devices using a physical layer solution which is a personal base station they called ”the shield”. This external device explores a radio design to jam the IMD's messages. This jamming procedure prevents unauthorized commands from reaching the device. Yang *et al.* [8] have proposes a key pairing system for wearable

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

devices. This pairing scheme explores Electromyogram signal's entropy. They have designed a secret key generator scheme that authenticates the different devices' physical proximity and allow a confidential communication. Rasmussen *et al.* [9] proposed a proximity-based access control scheme to secure IMDs. This scheme uses ultrasonic distance-bounding to authenticate the surrounding devices. Li *et al.* [10] treated this issue from a different perspective. They proposed a solution based on Body-coupled communication technology. This solution relies on the closeness of the devices to the human body and on this short communication range.

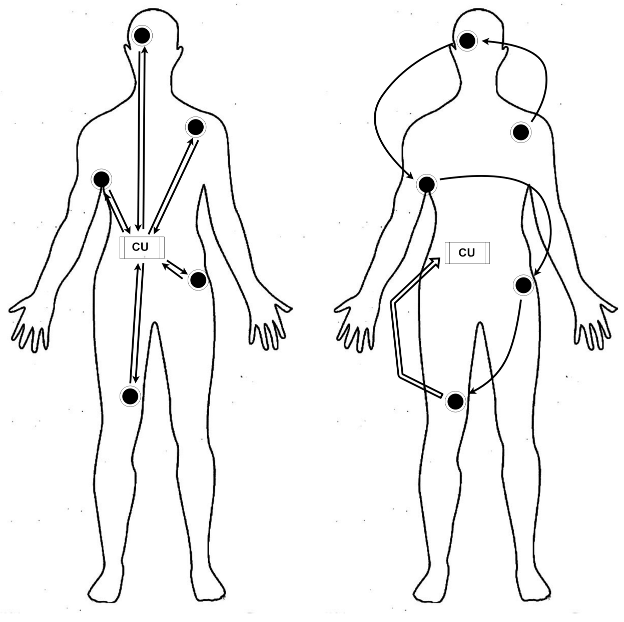
There are multiple IMDs a patient can wear to improve his health status. There is no necessity that these devices are related, or conceived to work together. Each IMD is independent usually. To alleviate this burden and to well protect the patient's privacy, we propose this work to link the different IMDs together while aiming to reduce the overall computational cost. As shown in Fig. 1, we want to alter the conventional communication scheme presented in Fig. 1a. The patient or the doctor uses a centralized device (CU) to collect the different measured data from the body. Therefore, each single IMD needs to undergo an authentication process at least to protect the data's privacy. This work aims to manage the medical data communication of these IMDs while guaranteeing the patient's security and privacy. We propose in this paper a chain architecture to relay the information between all the IMDs in use, as shown in Fig. 1b. We investigate the intrinsic entropy of the physiological data to introduce the secrecy of the information to the deliverable of the IMDs.

The remainder of this paper is organized as follows: Section II explains the communication model we are proposing in this work. Section III explains the architecture details and the IMDs' role partition. Section IV details how this scheme is able to protect the IMDs from malicious attacks. Section V illustrates the performance of the system. Finally, Section VI concludes the paper.

II. Communication Model

We propose for this work a new communication model to send the medical data from the different body sensor to the main Control Unit (CU). The latter is responsible for collecting, analyzing and sending the data of the patient to any other user, e.g, the patient's doctor or nurse. Instead of each sensor sends individually its gathered information to the CU, we propose that these sensors communicate in a chain model. Afterward, the final message, containing all the IMD's information, will be sent to the CU. Fig. 2 shows the proposed communication link between the different nodes. This scheme is beneficial on different points:

- The communication of each IMD will be a single one-way communication. If each node was to communicate directly with the CU, a two-way communication with multiple message exchanges needs to take place. This is to ensure the authenticity and legitimacy of each IMD before the CU accepts the message. In this scheme, each IMD will receive a message, adds its own, and then send it to the next IMD. The security features of the communication will be ensured by the global scheme.
- The communication between the IMD will happen on a Body-Area Communication level. This short-ranged low-power communication will first save on the communication cost of each device. Also, it will save on the computational cost. These communications are very hard to intercept without the patient's knowledge. Therefore, the standard encryption of this communication can be avoided. However, as it will be explained in the following sections, the communication will be encrypted rather than in plain-text. This helps to protect the patient's privacy at a lower cost compared to implementing regular standard encryption [11].
- The information of all IMDs will be more robust to break after passing through each device. The overall authenticity and integrity checks will move the CU part. This will save on the CPU use on the level of the IMDs.



(a) (b)

Fig. 1: Communication Model Used by Multiple IMDs on a Single User.

A. Architecture

We intend through this work to secure the messages generated by the IMD using the possible resources. For this reason, we have proposed the idea of a chain communication between the different IMDs all over the patient's body, before reaching the main device. Relying on the Random aspects of some of the physiological signs, such as Electrocardiographs (ECG) signals [17] and Electromyograph (EMG) signals [8], we are aiming to make the communication more private using simple data dissemination schemes. Section III depicts how each node will build its message based on the one it received. Initially, the architecture shown in Fig 2a was to be used for simplicity. However, we have found that there is a risk that

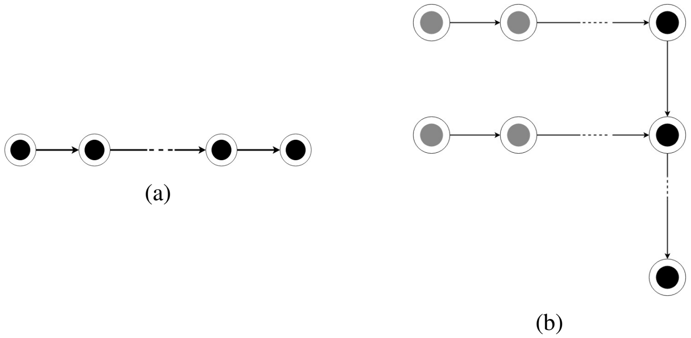


Fig. 2: Proposed Sequential Encryption Model for a Multi-IMD Communication. (a) Full-Sequential Communication Scheme. (b) Multi-row Sequential Scheme.

the final message will be too large that the method will lose interest. For this reason, we are proposing the architecture shown in Fig 2b. The IMDs that are used in each row (gray filled) are IMD characterized by simple reports. These IMDs usually reports physiological signs that only varies in unusual situations. Example of these signals are Blood Oxygen, Blood Pressure and Glucose level. The IMDs that links each row to another (black filled) are the ones that report larger signals. These signals usually require larger messages to report and also vary significantly throughout the day. Blood Glucose level for example, only witnesses a perceivable change on hourly basis. Blood Pressure depends highly on the patient's activity change, otherwise it would remain close to a certain value. However, EMG signals for example would drastically change with a signle muscle flex.

This architecture will improve the final message length required to report all the physiological data than the first one, this will better be explained in Section III.

For the node discovery, we intend to use a secret key agreement with the IMDs in use as an initial step. The CU will share secret keys K_i that will help authenticate the nodes later. The use of the right K_i ensures the identity of the IMD. Moreover, this will help identify which architecture to use, depending on the existing IMDs on the patient's body. The roles of being a "Gray node" or a "Black node" and which comes first in the chain is the role of CU to define. This should only change from one patient to another, or in the infrequent event of adding a new IMD to the system.

III. IMDs' Role Partition

A. Gray-level Messages

These IMDs are characterized by small, slightly-varying physiological signal reports. This can be the example of IMDs reporting Blood Pressure or Blood Glucose. The messages generated by these IMDs will be hidden in the packets generated by the "Black-level" IMDs. We intend to use a simple steganographic [12] technique to insert this message into the final message. If there is more than one "Gray", then the messages will follow the method described in Section III-B.

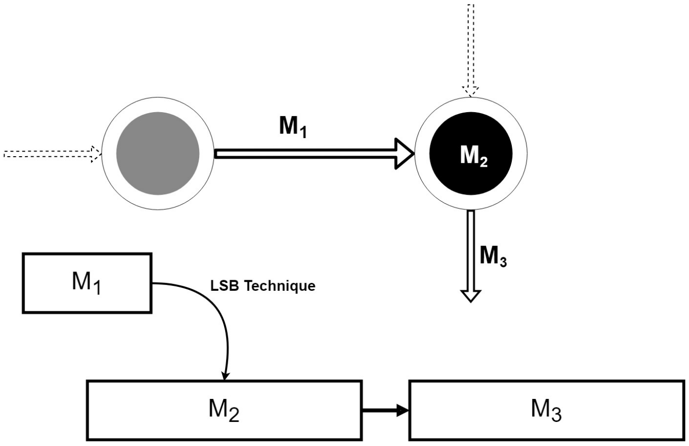


Fig. 3: Message Embedding Between a Gray-level IMD and its Following Black-level IMD

As shown in Figure 3. The message generated by the final Gray IMD will be inserted into what the following Black IMD is intending to send. The insertion will be using the LSB technique. The Least Significant Bit (LSB) [13] steganography is one popular and simple method to embed information usually within images. Steganography techniques are the process of inserting a secret message within a block of useful information that is hard to notice. The robustness of steganography techniques in our scheme will be asserted by embedding the data in an irregular region. This will be the role of shared K_i keys to define the region within each block of the total message. Usually, the gray nodes we are defining will deliver very small information (physiological measurements) that do not require a large packet [19]. However, the defined black nodes require significantly larger packets, essentially if they are monitoring continuous biological signals. Therefore, the LSB technique is useful and practical for this scenario. The technique would not burden the IMD with excessive computational utilization [14].

B. Black-level Messages

To embed the message of the current IMD, we intend to avoid standard cryptography for resource constraints reasons. The IMDs, as implanted in the body, has extreme small size and power constraints. The battery of some IMDs, such as biosensors and ICDs, has to last at least 5-10 years. Any additional computation will decrease drastically the life range of the device. Therefore, the IMD security module should not affect its safety and utility functions. Figure 4 explains the procedure of the message generation of the IMDs in this level. At the first step, the IMD will expand, if needed, its reporting Inf_i to match the message's length of the received message M_{i-1}. Then, it will embed both together. For simplicity, we used the XOR operation in the figure. Afterward, a second part of the message (P2) is generated. This enables CU to reversely read each different Inf_i when receiving the final message of the chain. P2 is a watermark of Inf_i on a pre-set template (TP) using K_i. This technique relies highly on the high entropy of the reported physiological signs to cipher the message [17],

[18]. The need to generate a random key is useless when using physiological signals with random behaviour to create the message to be sent. The watermark we propose is as follows:

$$P2 = Inf_i \times TP_{K_i} + (1 - Inf_i) \times (1 - TP_{K_i}) \qquad (1)$$

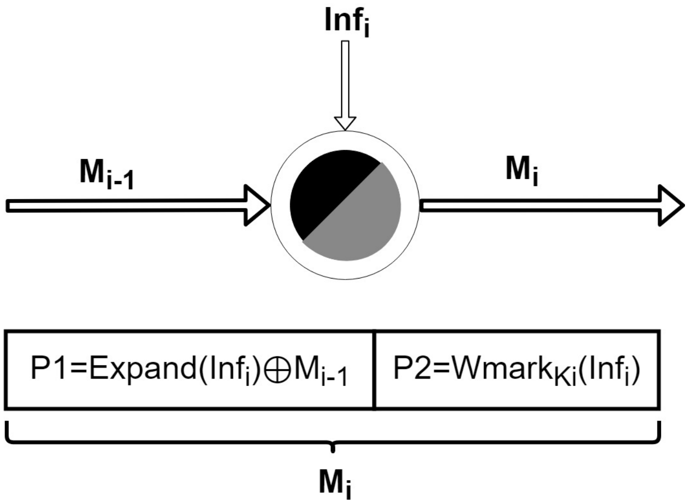


Fig. 4: Message Generation Procedure by an Intermediate Gray-level or a Black-level IMD

TABLE 1: Results of the Randomness Tests on the Black-level Messages

Randomness Test	Average success Rate of M_i
Monobit Test	88%
Frequency Test	93%
Runs Test	96%
DFT	97%

TABLE 2: Correlation Matrix of the Parameters of the Black-level Messages

	K_i	Previous message M_{i-1}	Generated message M_i	Final message
K_i	1	[-0.08,0.1]	[-0.07,0.01]	[-0.05,0.1]
Previous message M_{i-1}		1	[-0.16,0.11]	[-0.12,0.08]
Generated message M_i			1	[-0.03,0.02]
Final message				1

IV. Security Analysis

This protocol is dedicated to patient's that are using multiple IMDs for different purposes. The usual scenario is that each IMD will communicate independently with a central device. To guarantee the privacy of these communications, each IMD must have its own authentication or encryption scheme. In order to alleviate this burden, the proposed scheme is relying on the random variations of certain physiological signals (Electrocardiographs, Electromyograph, Blood Pressure ...) and the sequential communication proposed.
These devices are all implanted in the patient's body. The privacy of communication is ensured using Body Area Communications [15], [16]. This short-ranged communication limits the eavesdropping threat to its minimal. Another advantage of this communication is its low-power use. This makes the use of encrypted communication a low interest. The scheme we have proposed merges the messages generated by the different nodes in a way that the final message is humanly unreadable and hard to recover by an attacker. The authenticity and integrity of the messages are guaranteed by the pre-shared keys K_i. These keys are the parameters that make the final communicated message decipherable. Also, this renders this scheme robust against relay attacks as it will be shown in Section V-A.
This scheme is of real interest to the low-performance IMDs. In our architecture, these IMDs are assigned to be in the level of gray nodes. With no use of standard encryption algorithms, their message is being joined within the different messages. This leads to a harder procedure by any malicious attacker to extract the information. The final message contains all the information generated by the different IMDs. The CU is able to extract sequentially the IMD's messages starting from the last one reaching the first one. The LSB technique guarantees the readability of the information generated by the Gray nodes. The CU is solely knowledgeable about the K_i's. Therefore, it will identify where the messages have been hidden within the Black nodes' messages.

V. Performance Analysis

A. Randomness tests

The security aspects of any key generator relate highly to the randomness of its outputs [20]. The statistical tests for random sequences given by The National Institute of Standards and Technology (NIST) [21] describes procedures that aim to detect any deviation of a given binary sequence from being truly random. The main tests we have used to check on our key generator systems are:

1) Monobit test: This test verifies if the appearance proportions of the bits 0 and 1 are nearly balanced. Thus, there is no bit that is more likely to appear than the other.
2) Frequency Test within a Block: This test is the specification of the previous test on all M-bit blocks individually.
3) Runs test: This test verifies if the oscillation between the bits 0 and 1 in the given sequence is not too quick nor too slow for a random sequence.
4) Discrete Fourier Transform (Spectral) Test: This test looks for periodic features that contradict the assumed

randomness of the bit string. The test applies the Discrete Fourier Transform on the sequence to verify these features.

The results are shown in Table 1. These results were obtained by testing the ”Black-level” IMD’s generated messages after extracting the information to be reported. The information is obtained from different data offered by PhysioNet [22] database.

Table 2 shows the correlation between the different parts of the network. This table shows the absence of any statistical correlation between the messages and the keys received by the intermediate IMDs and those generated at the end. This is enhancing the secrecy of the messages throughout the whole chain.

To test the proposed scheme, we have considered the case of an IMD network of 9 IMDs on the patient body. We have chosen this to test the limitations and the scalability of our proposed idea. It is uncommon for a patient to handle on his body more than this. We intend to test how the architecture of the IMDs’ communication should be when adding a new device. Fig. 5 shows the different possible architecture and repartition of black/gray nodes. Our scheme relies directly on the message lengths and the type of signals for the repartition. A device reporting data that is long and more likely to vary significantly through time, has a tendency to belong to the black-level of IMDs. This data will induce some randomness aspects on the generated message following the scheme in Section III-B. The A device with quasi-static and short reports is more likely to belong to the gray-level of IMDs. Following this, the LSB technique will be efficiently utilized. We need to avoid having a large message to be embedded using LSB technique. Otherwise, there is a risk of information loss, as shown in Table 3. Fig. 6 represents the time needed by the whole architecture to generate the final message and its packet size. This was made under the assumption that all nodes behave likely. Also, under the assumption that the gray-level IMDs generate equal-length messages and the same for black-level messages. We can observe that the structures (b) and (c) performs the best. This is explained by the balanced arrangement of the different IMDs in the network. As one can predict, structure (d) is the worst. All the IMDs are in a sequential order. Also, even the IMDs with small data to report will need to expand their message to meet the communication chain requirement.

TABLE 3: Reliability of the Resulting Message

Architecture	Secrecy Tests	Recovery Rate
Structure (a)	100%	100%
Structure (b)	100%	100%
Structure (c)	100%	98%
Structure (d)	100%	100%
Structure (e)	94%	92%
Structure (f)	63%	86%

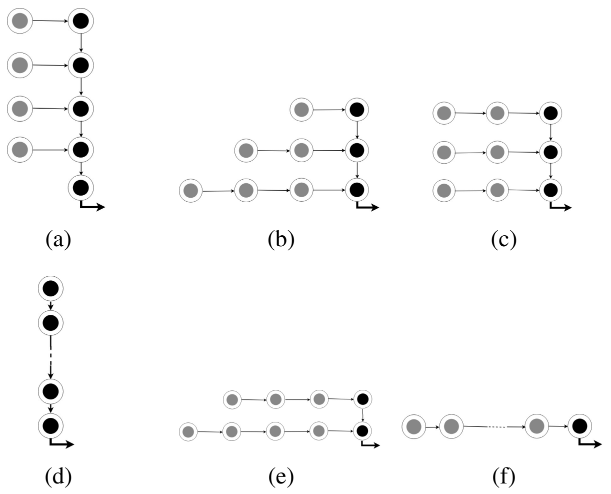


Fig. 5: Illustration of the Tested Different Communication Structures

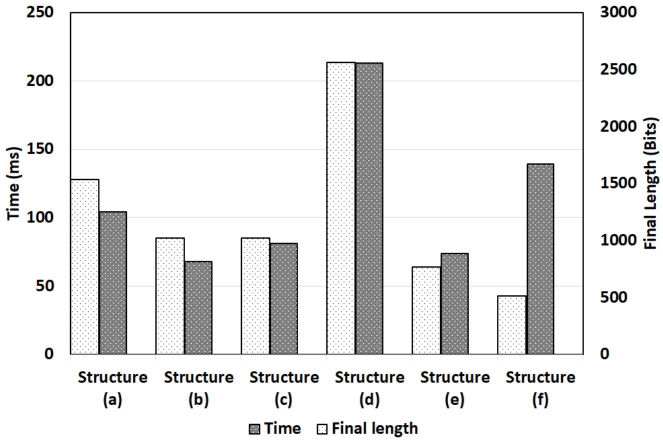


Fig. 6: Time Consumption and Packet Size of the Generation Process of the Final Message Generated by the IMDs

Table 3 shows the average score of the randomness tests (explained in Section V-A) of the message to be sent to the CU and its recovery rate. The smaller the recovery rate is, the more likely the CU will not be able to read all the messages contained within the received messages. This was obtained by testing the CU ability to decipher a large set of generated data by each different structure. We can observe that the structures (e) and (f) have the lowest rate. This is explainable as the gray nodes within the same row are too many that their final message is too large to be carried with LSB technique on the same carrier. For the secrecy score, we can deduce that the more gray-level nodes there are with fewer black nodes in the structure, the less secret the message is. This is mainly due to the fact that those nodes report usually predictable data, whereas the black nodes report data with an interesting random behaviour.

VI. Conclusion

In this work, we have investigated the case of a patient with several functioning Implantable Medical Devices (IMDs). We have proposed in this work a communication scheme between the IMDs to enforce the secrecy of this latter without the use of standard encryption. This helps to improve the security of the data while using the least resources possible of the IMD. This scheme reduces the communication cost and alleviate the need for single node authentication. We have concluded that the proposed system ensures users secure wireless communication for data exchange.

References

[1] Global Implantable Medical Device Market to Reach Valuation of Us$49.8 Bn with Emerging Advancement in Medical Sciences, https://www.transparencymarketresearch.com/,2018.

[2] Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas K, Nadeau E, Piccarreta B, Gabel O'Rourke D, Scarfone K. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. National Institute of Standards and Technology; 2018 Sep 24.

[3] Schwartz S, Ross A, Carmody S, Chase P, Coley SC, Connolly J, Petrozzino C, Zuk M. The Evolving State of Medical Device Cybersecurity. Biomedical instrumentation technology. 2018 Mar;52(2):103-11.

[4] Belkhouja T, Mohamed A, Al-Ali AK, Du X, Guizani M. Light-Weight Solution to Defend Implantable Medical Devices against Man-In-The-Middle Attack. *In2018 IEEE Global Communications Conference (GLOBECOM) 2018 Dec 9 (pp. 1-5). IEEE.*

[5] Belkhouja T, Du X, Mohamed A, Al-Ali AK, Guizani M. New Plain-Text Authentication Secure Scheme for Implantable Medical Devices with Remote Control. *InGLOBECOM 2017-2017 IEEE Global Communications Conference 2017 Dec 4 (pp. 1-5). IEEE.*

[6] F. Xu, Z. Qin, C. C. Tan,B. Wang, Q. Li, IMDGuard, Securing Implantable Medical Devices with the External Wearable Guardian, *Proc. IEEE INFOCOM, 2011.*

[7] S. Gollakota, H. Hassanieh, B. Ransford, D. Dina, K. Kevin, They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices, *Proc. ACM SIGCOMM, 2011.*

[8] Yang L, Wang W, Zhang Q. Secret from muscle: Enabling secure pairing with electromyography. *InProceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM 2016 Nov 14 (pp. 28-41). ACM.*

[9] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, Proximity-based access control for implantable medical devices", *In Proc. of Computer and communications security*, pages 410419, 2009.

[10] Li C, Raghunathan A, Jha NK., Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In2011 IEEE 13th International Conference on e-Health Networking, Applications and Services 2011 Jun 13 (pp. 150-156). IEEE.

[11] Richards D, Abdelgawad A, Yelamarthi K. How Does Encryption Influence Timing in IoT?. In2018 IEEE Global Conference on Internet of Things (GCIoT) 2018 Dec 5 (pp. 1-5). IEEE.

[12] Douglas M, Bailey K, Leeney M, Curran K. An overview of steganography techniques applied to the protection of biometric data. Multimedia Tools and Applications. 2018 Jul 1;77(13):17333-73.

[13] Datta B, Mukherjee U, Bandyopadhyay SK, LSB Layer Independent Robust Steganography using Binary Addition, *Procedia Computer Science. 2016 Jan 1;85:425-32.*

[14] Roy SS, Basu A, Das M, Chattopadhyay A. FPGA implementation of an adaptive LSB replacement based digital watermarking scheme. In2018 International Symposium on Devices, Circuits and Systems (ISDCS) 2018 Mar 29 (pp. 1-5). IEEE.

[15] C. Otto, A. Milenkovic, C. Sanders, E. Jovanov, System Architecture of a Wireless Body Area Sensor Network for Ubiquitous Health Monitoring, *Journal of Mobile Multimedia, 2006.*

[16] A. F. Demir, Z. E. Ankaral, Q. H. Abbasi, Y. Liu, Khalid Qaraqe, E. Serpedin, H. Arslan, R. D. Gitlin, In Vivo Communications: Steps Toward the Next Generation of Implantable Devices, *IEEE Vehicular Technology Magazine, June 2016.*

[17] Belkhouja T, Mohamed A, Al-Ali AK, Du X, Guizani M. Salt Generation for Hashing Schemes based on ECG readings for Emergency Access to Implantable Medical Devices. In2018 International Symposium on Networks, Computers and Communications (ISNCC) 2018 Jun 19 (pp. 1-6). IEEE.

[18] Belkhouja T, Du X, Mohamed A, Al-Ali AK, Guizani M. Biometric-based authentication scheme for Implantable Medical Devices during emergency situations. Future Generation Computer Systems. 2019 Feb 8.

[19] Baura G., Medical device technologies: a systems based overview using engineering standards. *Academic Press; 2011 Sep 28.*

[20] Gupta S, Yadav SK, Singh AP, Maurya KC. A Comparative Study of Secure Hash Algorithms. InProceedings of First International Conference on Information and Communication Technology for Intelligent Systems: Volume 2 2016 (pp. 125-133). Springer, Cham.

[21] National Institute of Standards and Technology, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April, 2010.

[22] PhysioBank Databse, https://physionet.org/physiobank/, 2016.