A Design of Secure and Reliable Wireless Transmission Channel for Implantable Medical Devices [1]

Lake Bu, and Mark Karpovsky
Reliable Computing Laboratory, Electrical and Computer Engineering
Boston University, Boston, USA
{*bulake, markkar*}*@bu.edu*

Keywords: implantable medical devices, security, eavesdropping, hijack, tampering, replay, man-in-the-middle, encryption, authentication, AES, AMD, error control codes.

Abstract: Implantable medical devices (IMDs) have increasing impact in people's life nowadays. With the development of electrical and computer engineering, the IMDs are of great convenience to patients by their small sizes and portable wireless monitors or controllers. However, because of the insecure wireless communication between the devices and their controllers, it makes way for attackers to passively and actively attack the devices and so the patients. Unlike other attacks which target on victims' information or property, the medical attacks threat victims' life directly. Up to now there are few efficient solutions to those attacks which balance security, reliability, and power consumption. In response to the situation, this paper proposes a scheme against the existing and potential attacks to IMDs while keeping a low overhead in hardware and power consumption.

1 INTRODUCTION

Implantable medical devices (IMDs) such as insulin pumps, pacemakers, and self-powered biosensors are widely used to save and extend people's life. These devices are embedded inside patients' bodies and communicate through wireless transmissions with their controllers or monitors, depending on whether it is open-loop or closed-loop.

However, these wireless transmissions usually are not protected due to the consideration of saving battery life, and capability of allowing the third-party devices' connection at emergency. This makes it possible for attackers to maliciously apply remote attacks to the IMD users. Since all these attacks are applied on the channel between the devices and the controllers or monitors, we categorize them into Man-In-The-Middle (MITM) attacks.

Moreover, since the medical data transmitted through the wireless channel are highly repetitive or in a regular pattern such as heart beats or glucose in the blood, it is not too difficult to predict the information even if it is encrypted, which makes the IMDs more vulnerable to attacks.

Eavesdropping is one of the most commonly seen passive attacks to wireless channels. The attackers simply listen to the unencrypted transmissions and acquire the knowledge of the health of the targeted patients or victims. Since there is no malicious tampering to the transmission, it is hard to detect. There are software and hardware means to eavesdrop the IMDs' channel. Researches on this type of passive attacks have been made by (Halperin et al., 2008), (Li et al., 2011), and (Paul et al., 2011) etc.

If eavesdropping is only the stealth of the victims' medical information, then active attacks such as hijack or replay are more lethal to the victims' health and even life. The attackers can use radio transmitters to simply generate commands to the devices implanted inside patients' bodies. They can either send their own forged commands, or replay a legal command eavesdropped and stored previously, if the transmission is encrypted. These types os attacks have been explored by (Halperin et al., 2008) over pacemakers and (Roberts, 2011) over insulin pumps. Both resulted in a fatal attack in simulation.

As a matter of fact, many IMD manufacturers actually integrated the Advanced Encryption Standard (AES) in their devices. However, they are not activated due to the concern of increasing power consumption or authentication of the third party devices (InfoSec, 2014).

Moreover, even if the AES module is activated,

[1]This work was sponsored by the NSF grant CNS 1012910.

the transmission is encrypted but not properly authenticated. Thus there are still potential threats it is vulnerable to: replay and known-plaintext attacks.

Therefore in this paper we propose a design of secure and reliable wireless transmission channel using authenticated encryption against both passive and active MITM attacks. The major contributions are:

- It uses encryption on transmitted messages against eavesdropping. It also randomizes the message to avoid known-plaintext attacks;
- It checks the authenticity of each transmission against forged messages. The attack misdetection probability is almost 0 in a device's lifespan;
- All encrypted legal messages are valid for only once in a device's lifespan, so that a prior legal message cannot be stored and replayed to pass authentication;
- It provides strong reliability to restore the transmission from random errors;
- When the pre-installed AES module on device is enabled, the proposed authenticating process adds less than 5% additional power consumption over it, which is much less than that of other conventional methods.

The rest of the paper is organized as the following. Section 2 briefly explains the several IMD transmission models. Section 3 illustrates the existing and potential attack models against current IMDs. Section 4 explains the criteria of the protection against such attacks. Section 5 introduces the proposed protection scheme and its work flow, as well as the theoretical estimation of its security level. Section 6 evaluates the proposed design by experiments and overhead comparison with other possible schemes.

2 IMD COMMUNICATION MODELS

There are a number of various types of wireless IMDs. They are characterized by different communication protocols and power supplies. Upon different types of IMDs, different attacks may apply.

2.1 Closed-loop IMDs

Closed-loop IMDs are self-monitored and self-managed. They receive wireless transmission from the sensor inside the patients' bodies and the actuator determines what therapy to deliver accordingly. The most commonly seen closed-loop IMDs are pacemakers and implantable cardiac defibrillators (ICDs) (Burleson et al., 2014).

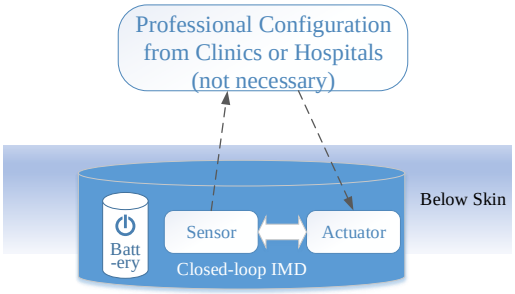

Figure 1: Closed-loop IMDs manage themselves based on the communication between the sensor and the actuator. Although they have no access for the patients to control them, they do allow configurations from professionals. The communication is not encrypted. The battery is usually not chargable and the replacement takes a surgery.

Since the transmissions are not encrypted, the transmitted messages are plainly from the medical sensors. Thus it is not too difficult to eavesdrop and acquire the knowledge of the patient. Based on the acquired information, the attackers will be able to replay some of the messages to the monitor, inducing the device to react in a certain way. In 2008, (Halperin et al., 2008) conducted their research on the vulnerabilities of pacemakers and ICDs. They successfully listened and understood the wirelessly transmitted information of the patient. They even reused the stored messages to disable the device, which may cause fatal accident to the patients in real life.

Besides, the power consumption is another major issue in these IMDs. Usually pacemakers or ICDs are designed to last for 5 to 7 years. Once the battery runs out of power, it takes a surgery to replace it. Hijacking the transmission channel by eavesdropping and replay can also result in a quick drain of battery by making the device working in a high-power mode.

2.2 Open-loop IMDs

Open-loop IMDs such as insulin pump systems can be more assailable. They receive wireless transmission from the devices' sensors inside patients, who are able to respond with remote controls. For example, a patient can issue pumps themselves according to reading of his/her glucose.

Since the communication involves control signals, the attackers can take advantage of it to apply more direct and harmful attacks to the victims. Furthermore,

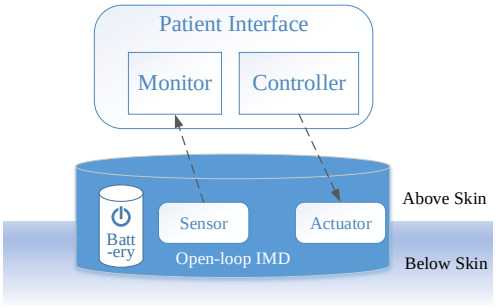

Figure 2: Open-loop IMDs usually come with a monitor and a controller. The patients monitor their health status based on the data from the sensor. They are able to issue commands (such as a dose of medicine or an insulin pump) by their judgement. The communication is not encrypted.

these IMDs' communications are not encrypted or authenticated, making it even less complicated to eavesdrop the transmission or forge malicious commands.

(Li et al., 2011) have studied the case on insulin pump systems. They were not only able to acquire the encrypted information from the device, but also managed to forge false glucose readings to the monitor. Finally, they successfully sent their own commands to the pump due to its lack of authentication process.

Moreover, other researchers such as (Radcliffe, 2011) and (Takahashi, 2011) claimed that they have gained full control to some of the insulin pump systems because these devices accept unauthorized radio signals or commands.

2.3 Biosensors

Biosensors are different from the two types above in several ways. Firstly they are usually self-powered inside human bodies. Secondly they are purely transmitters and receive no commands. Biosensors are widely used to detect glucose, lactate, or cholesterol etc. The receiver (patches) serves as the middle station which powers the sensor while sending the data to a higher level of monitors or analysts. However, both the monitor and the patch give no feedbacks in the form of commands.

The major threat to biosensors will be eavesdropping although it is not easy to implement because of their short communication distance. Other precise and practical threat models are yet to be developed (Burleson et al., 2014).

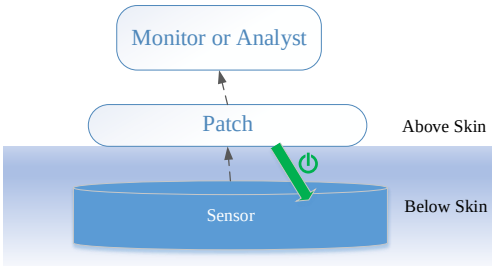

Figure 3: Biosensors send measurement to the patch and are powered by it. The patch then sends the measurement to monitors for analysis.

3 EXISTING AND POTENTIAL ATTACKS TO IMDS

As mentioned in the previous section, for IMDs with wireless communication, eavesdropping and channel hijack are two most frequently reported attacks. Also many IMDs are equipped with AES but have not enabled the encryption process. Even if they have, this can only prevent the attackers from eavesdropping and understanding the patients' health information. Those devices may still be vulnerable in certain ways under active Man-In-The-Middle (MITM) attacks such as hijack and replay.

According to the existing reported IMD attacks, they usually have the following preconditions:

1. The attacker is able to eavesdrop the victim's wireless IMD transmission between the sensor and the monitor/controller (Rostami et al., 2013);
2. Given the device' serial number, the attacker is able to use a programmed radio to send forged or stored commands to the victim's actuator (Rushanan et al., 2014);
3. The medical signals such as heart beats or glucose in the blood are in a regular pattern. Meaning they are possible to predict (Yury, 2014).

Given the assumptions above, the following subsections will describe the existing and potential attacks to ordinary IMDs and AES protected IMDs.

3.1 IMDs with AES Disabled

As mentioned in Section 2, most IMDs have their AES disabled, leaving the transmission channel entirely unprotected. Once the attackers eavesdrop and analyze the transmitted messages, they are capable to apply various attacks such as replay or spoofing commands. The results can be leakage of patients' health information, increase of battery power consumption,

overdose of the medicine, and malfunction or termination of the implanted devices etc.

3.2 IMDs with AES Enabled

Even if the IMDs activate their AES module to have each transmitted message encrypted (InfoSec, 2014), there still can be many potential ways to attack.

3.2.1 Eavesdropping and Known-plaintext Attacks

Eavesdropping is a type of passive attacks that the attacker listens to the unencrypted wireless transmission silently. The attacker does not necessarily apply any malicious modifications to the transmitted messages. Usually the goal of eavesdropping is to acquire the victim's important health information.

The Advanced Encryption Standard (AES) (Daemen and Rijmen, 2013) is a well-known solution that prevents the attackers from understanding the message transmitted even if they record it. However, if the encrypted cipher can be listened, and the attackers are able to predict or make a proper guess of the victim's health data (precondition 3.), with both the cipher and plaintext it is possible to apply known-plaintext attacks. This can lead to severe information leakage such as the secret keys (Bogdanov and Isobe, 2014). This will be disastrous since the attacker then will be capable to decrypt and understand any ciphers of the health data. Moreover, the attacker will have the sufficient knowledge to forge the measurement of health data to spoof the sensor.

3.2.2 Hijack and Replay

As (Rushanan et al., 2014) have pointed out, some IMDs have no authentication of the incoming radio signals. Thus the attackers and establish anonymous transmissions to either the implanted device or the monitor/controller.

This gives attackers opportunities to take over the transmissions between legal sensors and controllers. The attacker can firstly eavesdrop and record the legal transmitted ciphers without any understanding of the health data. Then he/she can replay some of the stored legal ciphers to IMD. Even if every transmitted message is encrypted and authenticated, the replayed ciphers will still be considered as legal. Moreover, if the attacker is able to apply known-plaintext attack and acquires the information of the secret key, he/she can choose to inject certain ciphers to harmfully affect the IMD. For example, very high glucose measurements can be frequently sent to the patient's monitor, inducing overdose of insulin pumps. Or commands of persistent large electric shocks can be sent to the defibrillator or pacemaker, causing deadly aftermath.

Depending on which AES mode a IMD is quipped with, the replay attacks will have different effects.

If it is AES in ECB mode, then there is a one-on-one pairing between the plaintext (health data) and cipher as shown in the figure below. This makes it extremely easy for attackers to choose ciphers to inject into the hijacked channel according to their malicious purposes.

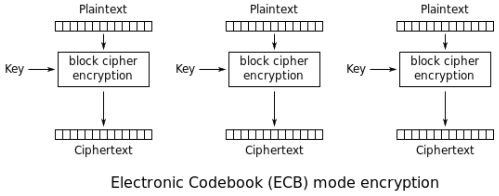

Figure 4: In ECB mode the cipher is a function of the secret key and the plaintext, whose mapping is unique and predicatble.

If it is AES in CBC mode, which is considered as much more secure than the ECB mode, the current plaintext will be randomized by the previous cipher and then sent for encryption. Thus the decrypted texts are beyond the control of the attackers. However, since the health data are usually generated from microprocessors and sensors of 8 bits, 12 bits, or 16 bits (Chede and Kula, 2008) (McDonald et al., 2011), it makes the replayed cipher from attackers decrypted to another legal numeric value with a high probability.

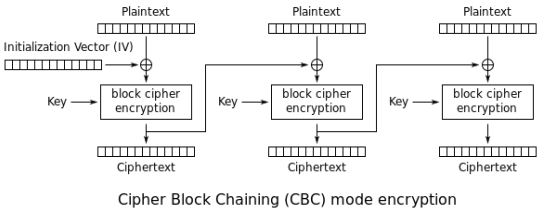

Figure 5: In CBC mode the cipher is effectively randomized by a function of the secret key, the current plaintext, and the previous cipher.

Example 3.1: In a 128-bit AES-CBC protected insulin pump IMD system with a 128-bit IV (in hexadecimal):

$$IV = \{0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06,$$
$$0x07, 0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f\}$$

And a 128-bit secret key (in hexadecimal):

$$key = \{0x60, 0x3d, 0xeb, 0x10, 0x15, 0xca, 0x71, 0xbe, 0x2b, 0x73, 0xae, 0xf0, 0x85, 0x7d, 0x77, 0x81\}$$

This insulin pump generates 16-bit measurement data of glucose in the blood. From a previous eavesdropping, the attacker has acquired the legal cipher of a sensor's measurement of glucose at moment t_0 as:

$$cipher(t_0) = \{0x17, 0x71, 0x98, 0x42, 0xac, 0x9c, 0x9e, 0xe8, 0x87, 0xc6, 0xed, 0x71, 0xd1, 0x1a, 0x78, 0x24\}$$

After a meal at the moment t_1 the patient's IMD microprocessor transmits the cipher text for '200 mg/dL" high level glucose in the blood to his monitor:

$$cipher(t_1) = \{0x0e, 0x11, 0x43, 0x4e, 0x23, 0xb1, 0x32, 0xf2, 0x4c, 0x12, 0x0a, 0x6d, 0x2c, 0x03, 0x87, 0x1e\}$$

Then the attacker uses his own programmed radio to send the pre-stored $cipher_0$ soon after, although he has no knowledge of the plaintext that this cipher relates to. According to the CBC mechanism, by the secret key and the previous $cipher(t_1)$ the decryption gets the following plaintext at moment t_2:

$$plaintext(t_2) = \{0x00, 0x8c, 0xe2, 0x41, 0xf2, 0x5f, 0x42, 0x07, 0x28, 0x59, 0x2a, 0x44, 0x52, 0xe2, 0x43, 0x5c\}$$

where the measurement bits are $\{0x00, 0x8c\}$ which happens to be "140" at the normal range, resulting in a skip of medication. Similar technique also works for closed-loop devices such as defibrillators.

3.2.3 Bit-flipping Attacks

Another type of attack taking advantage of the CBC mode is bit(byte)-flipping. By maliciously flipping some of the bits in the previous cipher, the next decrypted plain text will be altered in exactly the same bits.

Even if there is no leakage of the secret key, according the the precondition 3, as long as the attacker can listen to the channel and has a proper guess of the incoming message, the attack is highly probable to succeed.

According to the AES-CBC decryption procedure, a bit-flipping attack can be applied as the following chart (Swepsie, 2014).

For wireless IMD communications, even if the attacker is not able to modify the legal cipher in the channel, if he/she can predict the coming message (a command or a health data measurement), a carefully selected forged cipher can be injected before the next legal cipher. Then the plaintext decrypted from the next legal cipher will be affected by the previously injected forged cipher in certain bits by XOR operation.

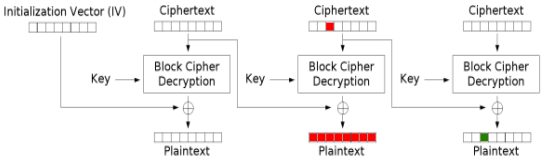

Figure 6: If a previous cipher is flipped by XOR operations to some bits, the next plain text will be flipped accordingly by XOR operations in the same bits.

Example 3.2: In a 128-bit AES-CBC protected insulin pump IMD system, the 128-bit IV and secret key are the same as *Example 3.1*. The system encodes and decodes 16-bit commands including issuing an injection $\{0x00, 0x80\}$, turning on the device$\{0x80, 0x00\}$, and turning off the device $\{0x08, 0x00\}$ etc.

After the patient finishes his meal and the glucose reading is at a high level, and the patient will be ready to issue a command of insulin injection which is $\{0x00, 0x80\}$. And if the attacker can predict this event, he can simply inject a forged command cipher at moment t_0 as:

$$cipher(t_0) = \{0x08, 0x80, 0x35, 0xf6, 0x88, 0x28, 0x6e, 0xc1, 0x3a, 0xd0, 0x87, 0x60, 0x10, 0x90, 0xd5, 0xe0\}$$

This forged command itself does not fall into any legal command. However, as the patient sends a following command of insulin injection, after decryption in the CBC mode at moment t_1 the command becomes:

$$plaintext(t_1) = \{0x00 \rightarrow 0x08, 0x80 \rightarrow 0x00, 0x60, 0x3d, 0xeb, 0x10, 0x15, 0xca, 0x71, 0xbe, 0x2b, 0x73, 0xae, 0xf0, 0x85, 0x7d\}$$

And this is the command to turn off the device instead of insulin injection.

As for closed-loop devices such as defibrillators, this type of attack is not that straightforward but still possible. Since those IMDs only accepts professional configuration from a clinic or a hospital, it demands the attackers to have access to those locations. However once the attackers can be physically close to the configuration, this bit-flipping attack can still work in a similar way. This causes even grave danger to turn a defibrillator off.

4 SYSTEM DESIGN CRITERIA

The goals of the proposed security system are to protect the IMD wireless channels from all the MITM attacks mentioned above while keeping low power consumption overhead. In addition, the design should modify the current secure scheme (AES-CBC) on IMDs as less as possible, so that it can be smoothly adopted by the current IMD manufacturers.

4.1 Data Block Size

We assume that the current IMDs equipped with AES will enable the encryption module in either 128 or 192-bit mode, where the 128-bit mode is the most common used and the 256-bit mode is an overkill to both security and power consumption and thus much less applied. Each health data or command packet is encrypted into a 128 or 192-bit data block. We aim not to increase the number of blocks or the size of blocks needed for each packet.

4.2 Against Eavesdropping and Known-plaintext Attacks

The current AES-CBC scheme is sufficient against eavesdropping. It takes hundreds of years to decrypt(understand) the patient's encrypted health data or command by brute force without the security key.

However it is not sufficient against known-plaintext attacks in the case of IMDs. As stated in preconditions 1, it is possible for an attacker to eavesdrop and store a number of legal ciphers. Precondition 3 suggests that an attacker is also able to make a proper guess of the encrypted health data or commands (plaintexts), since they are usually in highly regular patterns. For example, the glucose level is usually between 70 to 200 mg/dL, and cardiac rhythms are known to be the biological signatures of each person. The packet formats of the commands of controllers are even easier to find from their technical specifications. Then the attackers can pair up the ciphers and plaintexts to implement known-plaintext attacks. Since the plaintexts are predictable, they should be properly randomized. However, even if they are in the CBC mode (by XORing the current health data or command bits with and the previous cipher), the attackers still can analyze them since the ciphers have already been eavesdropped.

Therefore a more sophisticated randomization should be involved so that even with a record of ciphers and plaintexts, the attack is still not able to pair them up for known-plaintext attack.

4.3 Against Hijack, Replay, and Bit-flipping Attacks

Firstly the transmission should be authenticated, so that unauthorized or replayed radio signals should not be accepted as a legal sensor reading or commands. AES itself does not provide this feature and extra modules for authentication is required.

There are various ways for authentication. Keyed-hash Message Authentication Code (HMAC) provides strong security but requires a huge amount of extra bits for the digest, which contradicts with the first design criterion by bringing considerable modification (each data packet uses more than one blocks) to the current AES-CBC scheme. Here we propose to use the Algebraic Manipulation Detection (AMD) codes which is a light weight keyless message authentication code (Wang and Karpovsky, 2011b). Unlike HMAC which has a fixed length over 160 bits, it is very flexible to work on different sizes of data packets by which its security level is determined. Moreover, the AMD codes bring in a random vector so that the plaintext is randomized even if the health data or commands are non-uniformly distributed, which efficiently prevents the known-plaintext attacks.

Secondly, each authenticated cipher should be valid only once in a lifetime. It indicates that even if the attacker stores all the authenticated and encrypted transmissions, he/she will not be able to reuse any of them in future. Thus it is necessary to use a self-incrementing timestamp in each transmission as part of the authentication process. The system always keeps track of the latest timestamp. If an incoming message has a timestamp smaller or equal to the highest one known by the system, it is illegitimate.

The medical devices usually use low frequency sensors with sampling rates from 1Hz to 1kHz. And an IMD can last from 1 to 10 years. The security module should guarantee that within these years under the health data sampling rate, not a single replay or bit-flipping attack can succeed. Therefore based on these parameters, the attack mis-detection probability should be at least 2^{-32} for IMDs working under low frequency of up to 10Hz and at least 2^{-40} for higher frequency of up to 1kHz.

4.4 Against Random Errors

Random errors are not attacks. They are usually caused by unstable transmissions or minor change of voltages etc. Upon the presence of random errors the readings of health data might be imprecise or the commands might be distorted. The reliability against random errors can be enhanced by applying error con-

trol codes (ECC) to the plaintexts (Burleson et al., 2014). In this design we will use double error correction codes which is more than enough for the channel.

4.5 Power Consumption

Since wireless IMDs are mostly battery powered (except the self-powered biosensors), the design should also aim for low power consumption overhead comparing with other possible methods.

5 SYSTEM DIAGRAM AND WORKFLOW

The proposed protection scheme uses authenticated encryption with timestamps. Its encoding procedure is MAC-then-Encrypt (MtE). In this way the IMD's information part (health data from sensors or commands from controllers), the timestamp, and the authentication signature can be wrapped all under 128 bits or 192 bits depending on the demand. As a result, it adds no extra transmission overhead to the current IMDs equipped with 128 or 192-bit AES in CBC mode. Although MtE is not considered as the most generically secure in all authenticated encryption modes, it has been proved to be secure with the AES-CBC mode (Krawczyk, 2001).

5.1 Notations

To help describe and evaluate this protection mechanism, we introduce the following notations.

5.1.1 Finite Field Operators

We denote the Galois finite field by GF, and the numbers of bits in each data packet by b. Then $\cdot$ is the multiplication in the $GF(2^b)$ finite field, $\oplus$ the addition in $GF(2^b)$, namely bitwise XORs, and $\bigoplus$ as the accumulated sum operator. $||$ represents concatenation of two vectors.

5.1.2 Elements in Data Packets

The information part carrying the health data from sensors or commands from controllers is denoted by k, and r is the ECC redundancy to protect k from random errors. $y = k||r$ is the concatenation of both. The self-increment timestamp is denoted by i, the random vector by x, and the AMD code's signature by ω.

5.1.3 Attacks

e represents the injected error by attackers to each data packet and so $e = \{e_\omega, e_y, e_i, e_x\}$. Any packet tampered by e is marked by $\tilde{}$. The attack misdetection probability is denoted by P_{miss}.

5.1.4 Random Error Correction

The ECC's check matrix H is used with $\tilde{y}$ to compute the syndrome S for random error correction.

5.2 AMD Codes

The AMD codes have been known as a class of low weight but highly secure attack detecting codes against strong attacks, where the attackers have proper knowledge of the information part, the encoding scheme, and are able to issue any modifications to the message in channel. It often cooperates with cryptographic systems as a keyless authentication code (Wang and Karpovsky, 2011a). Because of its random vector x, AMD codes performs excellently with uniform security even under non-uniform distribution of the information part, which covers the vulnerability of the highly repetitive health data or commands.

Construction 5.1: Let the random variable $x = \{x_1, x_2, \cdots, x_t\}$, and the information part $y = \{y_1, y_2, \cdots, y_t\}$, then the AMD codes are constructed by (Luo et al., 2013):

$$\omega = \bigoplus_{j=1}^{t} (x_j \cdot y_j \oplus x_j^3); \quad \omega, x_j, y_j \in GF(2^b). \tag{1}$$

If the error e_y on y is non-zero (for an attack to make sense), then the term x_j^3 can be omitted. For the proposed protection scheme, $t = 1$ since $y = k||r$ is in one packet. y can be robustly combined with the self-incrementing timestamp i by $y \cdot i$ (K.J.Kulikowski et al., 2005), where $\cdot$ is the finite field multiplication. The signature ω of the AMD code is computed by:

$$\omega = y \cdot i \cdot x = (k||r) \cdot i \cdot x; \quad i, x, y \in GF(2^b). \tag{2}$$

If the injected errors to each component is represented as e_ω, e_y, e_i and e_x, the error masking equation will be:

$$\omega \oplus e_\omega = [(k||r) \oplus e_y] \cdot (i \oplus e_i) \cdot (x \oplus e_x). \tag{3}$$

It has been verified that the right-hand side of the equation is always a non-zero polynomial of x of degree 1. It is easy to prove that for a certain message and an error e, the error missing probability is at most:

$$P_{miss} = 2^{-b}. \tag{4}$$

b should be at least 32 or 40 to ensure that no attack will succeed in an IMD's lifetime.

5.3 Error Correction Codes for Random Errors

Usually there is little error correcting code's (ECC) redundancy added to information part of the IMD sensors or controllers to restore the message from random errors. Since the proposed scheme should be encoded into at least 32-bit packets and the information part is at most 16 bits, the rest of the bits can be allocated for the ECC's redundancy.

To ensure fast decoding and low hardware complexity, we propose to use the Orthogonal Latin Square Codes (OLSCs) (Yalcin et al., 2014). The error correction procedure is:

$$H \cdot (\tilde{k}||\tilde{r}) = S \tag{5}$$

where $\tilde{k} \in GF(2^{16})$ or less and $\tilde{r} \in GF(2^{16})$ are distorted information part and redundancy, H is a 16×32 binary matrix, and S is a 16-bit binary vector which is used for one-step majority voting error correction (Bu and Karpovsky, 2016) of up to 2 random errors in k.

5.4 System Diagram

As stated prior this section, the proposed scheme is structured by authenticated encryption with MAC-then-Encrypt work flow. The AES-CBC encryption process will protect the system from eavesdropping on k the health data or commands. The ECC's redundancy r enables correction of up to 2 random errors in k. The timestamp i will guarantee that each transmitted cipher can never be replayed again to spoof a legal command or health data. The random vector x randomizes the plaintext $((k||r)||i||x||\omega)$ so that the attackers cannot apply known-plaintext attacks even if they have a proper guess of the patient's medical data as stated in the precondition 3 (Kulikowski et al., 2008). The AMD authenticating finally signature ω verifies if the message is authentic or not.

For IMDs working under lower sampling frequency of up to 10Hz, the block size is 128 bits and each data packet 32 bits. For IMDs working under frequency up to 1kHz, the block size should be 192 bits and data packet at least 40 bits. However since each block includes 4 packets, each packet can be made to 48 bits to fully utilize the space while enhancing the security lever.

The diagram of the lower frequency system is shown in Figure 7. The system firstly encodes the 16-bit health data from the sensors or commands from the controller k into the 32-bit information part y, with a double-error correcting OLSC code's redundancy r. Secondly they are encoded with the timestamp i and random vector x into ω by the message authentication code AMD. Then the 128-bit $((k||r)||i||x||\omega)$ will serve as the randomized plaintext to be encrypted by the 128-bit AES under CBC mode. The Man-In-The-Middle attacks occur in the wireless transmission channel by eavesdropping, hijack, replay, and bit-flipping. On the receiver end, the AES firstly decrypts the plaintext and the first 32 bits are sent to the OLSC decoder for random error correction. Then it checks if the timestamp i is larger than the previous one. Finally the entire plaintext is verified by the AMD decoder for attack detection.

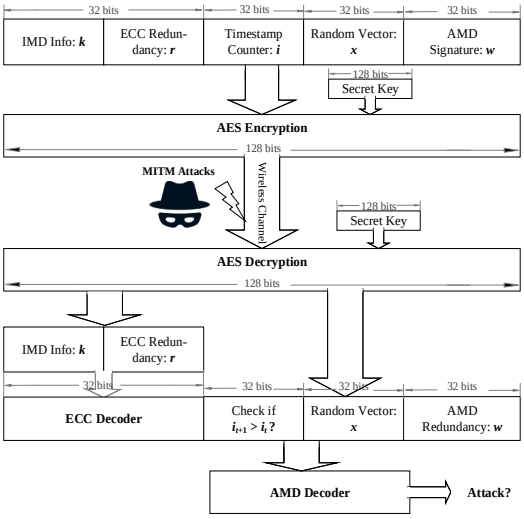

Figure 7: The lower frequency secure system's diagram. The higher frequency system has the same workflow except the block size is 192 bits and packet size 128 bits.

6 EVALUATIONS

In this section the proposed scheme's security and power consumption overhead will be evaluated.

6.1 Error Mis-detection Probabilities

To verify this probability we have run through tests on over 3 billions simulated IMD radio transmissions of sensor's health data and controller's commands, which is about the total number of an ordinary IMD's transmissions in 10 years under a lower frequency of 10Hz. During the simulation the system mimics an IMD sending and receiving messages, and the attacker applying hijack, replay, and bit-flipping attacks alternatively in every around, while the receiver verifying the timestamps and the AMD signatures.

Since the 32-bit and 48-bit system provides so strong security that not a single attack was missed in our experiment, we apply various sizes of data blocks (from 8 to 48 bits) due to AMD codes' flexibility to observe how much the experimental error mis-detection probability matches $P_{miss} = 2^{-b}$ in (4).

Table 1: P_{miss} under 3,154,043,200 Active MITM Attacks

Missing \ b	8	16	32	48
Missed Errors in Experiments	12,321,649	48,032	0	0
Experimental P_{miss}	3.91e-3	1.52e-5	0	0
Theoretical $P_{miss} = 2^{-b}$	3.91e-3	1.53e-5	2.33e-10	3.55e-15

[I] Under 3 billions MITM attacks modeled in Section 3, not a single error was mis-detected by the 32-bit and 48-bit packet-sized systems.

The experimental result not only shows that the proposed protection scheme works well according to the theoretical estimation of 2^{-b} error mis-detection probability precisely, but also demonstrates that the 32-bit and 48-bit schemes are secure enough for missing 0 attack under 3 billions of malicious hijack, replay, and bit-flipping attacks, providing sufficient security during the IMD's lifespan.

6.2 Power Consumption Overhead

As mentioned above, AMD codes are light weight message authentication codes. With the AES enabled in the IMDs, the AMD encoding and authentication add minimum power consumption overhead while providing the security demanded. This is critical to the power sensitive IMDs such as defibrillators whose battery replacement takes a surgery.

The following overhead comparison was made based on the implementation on Xilinx Vertex 4 FPGA and Cadence SOC Encounter.

Table 2: Power Overhead Comparison Based on AES enabled

	P_{miss}	Extra Bits Over AES	Area (um^2)	Energy (nJ)
Proposed Scheme (32-bit packets)	2^{-32}	0	3093.6	2.10
AES (128 bits)	N/A	N/A	57520.3	67.03
Proposed Scheme (48-bit packets)	2^{-48}	0	4765.9	4.05
AES (192 bits)	N/A	N/A	66732.7	91.36

[I] The proposed authentication module adds only 3.1% energy to the 128-bit AES encryption module, and 4.4% to the 192-bit AES module, resulting in an ignorable energy consumption overhead while providing sufficient security.

On another hand, one alternative approach is AES + HMAC + timestamps. However the popular HMAC requires at least 160 bits to provide 2^{-80} mis-detection probability which is an overkill to the security required and brings too much modification to the existing AES based systems.

As for the 32-bit and 48-bit AMD code and timestamp based scheme, since all computations are done in the 32-bit or 48-bit finite field, it saves largely the transmission overhead, hardware area, and power consumption over the HMAC authentication method. Even if the scheme upgrades x and ω to 80 bits to achieve the same P_{miss} as the HMAC based scheme, it still saves tremendously the power consumption.

Table 3: Transmission and Power Overhead Comparison

	P_{miss}	Extra Bits Over AES	Area (um^2)	Energy (nJ)
Proposed Scheme (32-bit packets)	2^{-32}	0	3093.6	2.10
Proposed Scheme (48-bit packets)	2^{-48}	0	4765.9	4.05
Proposed Scheme (80-bit packets)	2^{-80}	128	6274.8	7.49
HMAC Based (160 bits)	2^{-80}	128	58813.7	58.06

[I] Even when the authentication process is brought up to error mis-detection probability of 2^{-80} which is the same as HMAC, the energy cost is only 12.9% of the later, making the proposed lightweight scheme an economic choice for the IMDs.

7 CONCLUSION

This design is proposed under the motivation of the existing and potential Man-In-The-Middle attacks to the IMDs with wireless communication. We have proved by theory and experiments that by authenticated encryption with a random vector and a timestamp encoded by AMD codes, it mis-detected 0 errors in a device's lifespan. Moreover, the proposed authentication module's energy consumption is merely $3 \sim 4\%$ of the pre-installed AES module's. Also comparing with other authentication techniques such as HMAC, it consumes only 13% energy of the later while providing the same security level. These advantages make the proposed scheme a secure and reliable solution to the IMDs against MITM attacks, while extending the lifespan of IMDs by saving their batteries.

The power analysis of this paper is based on the AES module that has already been integrated in IMDs. However AES is not the best choice in an energy efficient design. Since the AMD message authentication code is lightweight itself, it is recommended to also use a lightweight encryption scheme to have a better saving of the battery life in IMDs.

REFERENCES

Bogdanov, A. and Isobe, T. (2014). How secure is aes under leakage. *International Conference on the Theory and Application of Cryptology and Information Security*.

Bu, L. and Karpovsky, M. G. (2016). A hybrid self-diagnosis mechanism with defective nodes locating and attack detection for parallel computing systems. *IEEE International On-Line Testing Symposium (IOLTS)*.

Burleson, W., Clark, S. S., Ransford, B., and Fu, K. (2014). Design challenges for secure implantable medical devices. *Springer New York*.

Chede, S. and Kula, K. (2008). Design overview of processor based implantable pacemaker. *Journal of Computers*.

Daemen, J. and Rijmen, V. (2013). The design of rijndael: Aes-the advanced encryption standard. *Springer Science and Business Media*.

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., and Maisel, W. H. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. *Proceedings of the 29th IEEE Symposium on Security and Privacy*.

InfoSec (2014). Hacking implantable medical devices. `http://resources.infosecinstitute.com/hcking-implantable-medical-devices/`. [Online].

K.J.Kulikowski, G.Karpovsky, M., and A.Taubin (2005). Robust codes for fault resistant cryptographic hardware. *Proc of Int. Workshop on Fault Detection and Tolerance in Cryptography*.

Krawczyk, H. (2001). The order of encryption and authentication for protecting communications (or: How secure is ssl?). *Springer Berlin Heidelberg*.

Kulikowski, K., Wang, Z., and Karpovsky, M. G. (2008). Comparative analysis of robust fault attack resistant architectures for public and private cryptosystems. *IEEE 5th Workshop on Fault Diagnosis and Tolerance in Cryptography*.

Li, C., Raghunathan, A., and Jha., N. K. (2011). Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. *Proceedings of the 13th IEEE International Conference on e-Health Networking, Applications, and Services*.

Luo, P., Z.Wang, and M.G.Karpovsky (2013). Secure nand flash memories resilient to strong fault-injection attacks using algebraic manipulation detection codes. *Proc. Int. Conference on Security and Management, SAM*.

McDonald, J., Dean, S., Niewolny, D., Garcia, D., Chhabra, N., and Chang, L. (2011). *Integrated Circuits for Implantable Medical Devices*.

Paul, N., Kohno, T., and Klonoff., D. C. (2011). A review of the security of insulin pump infusion systems. *Journal of Diabetes Science and Technology*.

Radcliffe, J. (2011). Hacking medical devices for fun and insulin: Breaking the human scada system. *Black Hat Conference*.

Roberts, P. (2011). Blind attack on wireless insulin pumps could deliver lethal dose. `https://threatpost.com/blind-attack-wireless-insulin-pumps-could-deliver-lethal-dose-102711/75808/`. [Online].

Rostami, M., Burleson, W., Koushanfar, F., and Juels, A. (2013). Balancing security and utility in medical devices? *Proceedings of the 50th Annual Design Automation Conference*.

Rushanan, M., Rubin, A. D., Kune, D. F., and Swanson, C. M. (2014). Sok: Security and privacy in implantable medical devices and body area networks. *2014 IEEE Symposium on Security and Privacy*.

Swepsie (2014). Bypassing encrypted session tokens using cbc bit flipping technique. `http://swepssecurity.blogspot.com/2014/05/bypassing-encrypted-session-tokens.html/`. [Online].

Takahashi, D. (2011). Excuse me while i turn off your insulin pump. `http://venturebeat.com/2011/08/04/excuse-me-while-i-turn-off-your-insulin-pump`. [Online].

Wang, Z. and Karpovsky, M. G. (2011a). Algebraic manipulation detection codes and their applications for design of secure cryptographic devices. *IEEE 17th International On-Line Testing Symposium (IOLTS)*.

Wang, Z. and Karpovsky, M. G. (2011b). Manipulation detection codes and their application for design of secure cryptographic devices. *Proc of International Symposium on On-Line Testing (IOLTS)*.

Yalcin, G., Islek, E., Tozlu, O., Reviriego, P., Cristal, A., Unsal, O. S., and Ergin, O. (2014). Exploiting a fast and simple ecc for scaling supply voltage in level-1 caches. *IEEE International On-Line Testing Symposium (IOLTS)*.

Yury, C. (2014). Your heartbeat may soon be your only password. `http://wired.com/insights/2014/06/heartbeat-may-soon-password/`. [Online].