CHAPTER – 4

A Buddy System for Securing Wireless IMDs

This chapter's contributions are:

1. A trusted external device called Buddy Device is used to authenticate external devices on behalf of IMDs to prevent resource-depletion. Buddy Device is a resource rich device supporting RSA based certificates for mutual authentication and temporary key exchange over wireless link.
2. Buddy Device allows IMD to emit a session key and performs friendly jamming to convey the session key only to an authenticated external device.
3. Following exchange of session key IMD and external device can indulge in secure wireless communication.
4. Allows Perfect Forward Security (PFS) as the session key is renewed for every session.
5. This solution can be explicitly use for IMD to external device communication as such communication is more vulnerable to attacks.

4.1. Introduction

As explained in Chapter 1, unauthenticated communication may force IMD to exhibit unpredictable behavior which may threaten a patient's life [38, 52, 88]. It is highly desirable to block unauthorized wireless communication attempts of an adversary while allowing seamless communication between IMD and authorized external device for immediate diagnosis and treatment. Typical IMDs are battery powered devices capable of running for five to seven years [48]. Their batteries cannot be charged unless surgerically removed from the body. Also due to miniaturized size and unique placement in human body, IMDs lack memory and computational skills unlike modern day wireless devices. Moreover putting stringent security policies may render the device inaccessible in case of an emergency for the healthcare personal who do not have the access credentials [89]. For a security scheme to work in presence of these limitations following requirements should be satisfied:

1. Energy, storage, computation, communication overhead induced should be minimized.
2. Support for real time generation and sharing of renewable and secure credentials should be provided.
3. Adherence to Perfect Forward Secrecy (PFS) requirement which means compromise of a session key will lead to disclosure of only the data encrypted by that key and not any subsequent data or key.
4. Support for security services viz. Confidentiality, Integrity and Availability for IMDs should be provided.
5. Support for rendering Authentication and Access Control for all communications with reader/programmer.
6. Access during emergency situations should also be controlled to a certain extent.
7. The scheme should provide security to any IMD in general and to a specific IMD in particular.
8. Support for scalability to cater to security requirements of multiple IMDs implanted for a patient.
9. The scheme should be minimally invasive requiring minor changes in existing IMDs.
10. The scheme should make use of standard algorithm rather than relying on security through obscurity.

4.2. Proposed Solution: The Buddy System

We provide a solution to this problem by introducing an external device called a Buddy Device which secures patient IMDs and enforces authenticated communication for the IMDs. It performs authentication of external devices on behalf of IMDs thus conserving scarce resources of IMD for critical therapeutic functions. Using our system, an external device obtains access to IMD provided it successfully passes the stringent authentication and access control policies rendered by the Buddy Device. When a reader seeks access to an IMD, Buddy Device initiates an authentication session which once successful leads to sharing of a temporary key between Buddy Device and authenticated external device. Buddy Device requests IMD to transmit the one time session key and simultaneously jams

the channel to bard other devices in vicinity from interpreting the key while allowing authenticated reader to interpret the key as it is in possession of the temporary key which can be used to cancel the jamming signal and derive the session key. The session key is renewed for every new session between IMD and external device. An important facet of our scheme is forward security and replay attack resilience as for every session a new session key is generated and used for encipherment of telemetry data. IMD supports session key generation by using time-varying biometric, known as physiological value (PV). Any PV can be used by an IMD to generate session key, one such example is use of the waveform produced by the heart, known as an ECG (electrocardiogram). MEMS Microcontrollers used for IMDs today allow it to perform only lightweight cryptography. Our scheme requires invocation of Ultra light weight cipher like PRESENT-80[90, 91] or MISTY1[70]. The Buddy Device performs following roles:

1. **Mutual authentication and temporary key generation:** The Buddy Device and external devices exchange RSA based Public Keys on prior basis. It authenticates external device (ED) on behalf of IMDs and a temporary key is generated.
2. **Access Control:** It provides a role based access control for IMD resources based on a configurable Access Control List (ACL) available with the Buddy Device.
3. **Jamming:** It requests IMD for one time session key generation and transmission to the external reader while simultaneously jamming the channel.

The proposed scheme is minimally invasive as the IMD only needs to generate session key and transmit it and later use it for encryption and decryption of telemetry data. The session key generation is lightweight procedure as IMD uses random bits from the sensed data to form a session key. This aims to provide a technique for sharing of secret session keys between implanted device and reader by use of friendly jamming which is controlled by temporary key in presence of adversary. This makes the session key unpredictable to adversary but as the authenticated reader is aware of the master key; it can remove the jamming signals and recover the key send by IMD. Once key is shared with authenticated external device, all communication between IMD and external device is encrypted by the session key ensuring message confidentiality and integrity. This scheme can also be used for securing multiple IMDs worn by a patient. To make session key generation light-weight, we propose use of Physiological values (PVs). PVs are sensed by IMDs as a part of their functionality. Therefore no extra overhead of pseudo random number generator (PRNG) or

Round Function is incurred. As described in [81], it is possible to extract four high-grade truly random and uncorrelated bits per IPI from processed ECG source. We propose use of such random bits for session key generation as they provide the required entropy.

From the literature survey in chapter 3, we found a lack of appropriate key sharing mechanisms, the use of pre-shared keys makes them vulnerable to cryptanalysis attacks, biometric [77] or physiological value (PV) [81] based key exchange requires closer assessment to be used in practical and also external device to be able to measure a PV. The solutions given in literature [84], [14, 29, 48] exhibit some or the other limitations like authentication using pre-shared keys which cannot be renewed even when compromised; use of invasive techniques which call for a major design change in current IMDs. Moreover encryption and authentication protocols used are vulnerable to battery depletion and denial-of-service attack. Fail-open access in case of emergency increases vulnerability; also the device specific nature of security solution makes them unusable for other implanted devices.

4.3 Features of Buddy Device

We propose the Buddy Device as trusted external device similar to shield [84] but differing in following aspects:

1. While the shield [84] act as a jammer-cum-receiver to jam the IMD messages and unauthorized commands, our Buddy Device uses jamming only for secure exchange of session key between IMD and external reader.
2. When present, our Buddy Device is also capable of using fast jamming techniques as shown in [6] to jam the frames which are directly addressed to IMD. This strategy prevents attacks like Denial-of-Service and battery depletion. No such attempt was made in [84].
3. When the shield [84] sends reader's commands to the IMD, confidentiality is not warranted. While in our case IMD and external reader communication is secured by use of session keys.
4. Shield [84] is vulnerable to attacks in presence of an adversary with two receiving antennas as shown in [50] we make an effort to mitigate this problem by use of temporay key as also proposed in ally friendly jamming [50].

4.4. Proposed Architecture using Buddy Device

Here we describe the proposed architecture which deviates from the from the normal communication pattern by introduction of a device called Buddy Devise. The Buddy Device based architecture is shown in Fig 4.1.

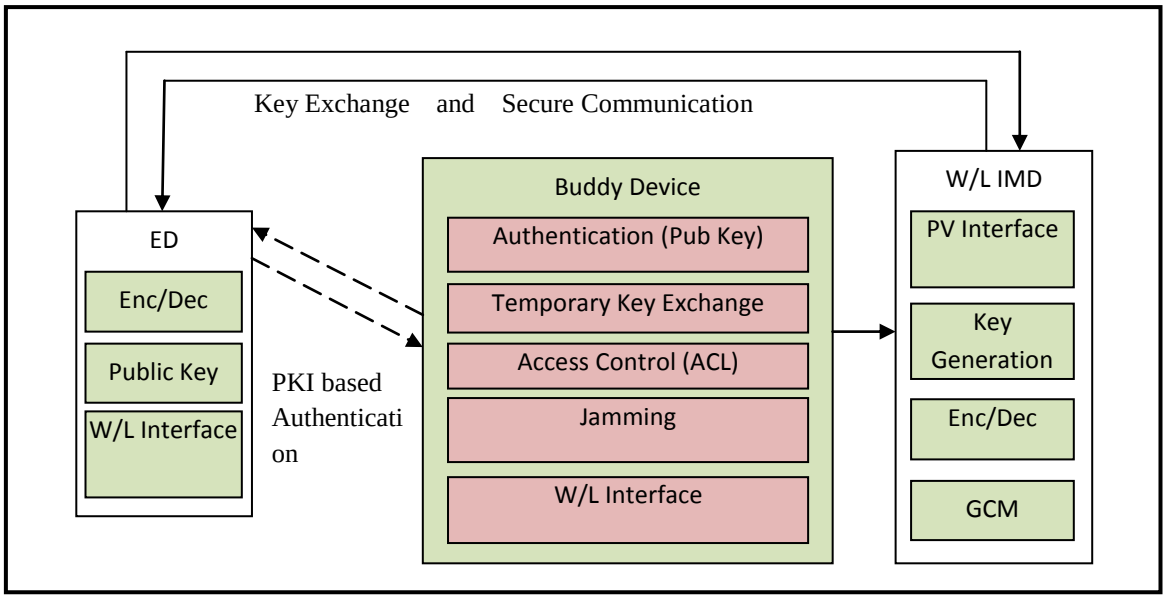

FIGURE 4.1 Architecture of Proposed Security Scheme using Buddy Device

The essential modules for working of the proposed solution are explained below

4.4.1 Buddy Device

Buddy Device is securely paired with IMD during IMD installation. This allows only the Buddy Device of the patient to request an IMD for session key generation and transmission while simultaneously jamming the channel. It contains following modules:

1. **Authentication:** By use of prestored RSA based Public Keys, Buddy Device and ED perform mutual authentication and a temporary key exchange. Buddy encrypts the generated temporary key by Public Key of ED and sends. ED decrypts the temporary key using its own Private Key.
2. **Access Control:** It uses a pre-configured access control list(ACL) to provide role based access control to IMD resources by the external devices.
3. **Jamming:** Three particular situations that require use of jamming are firstly when the session key is being transmitted by IMD to the external reader to avoid eavesdropping attempts of an attacker. Secondly, when an adversary bypasses the Buddy Device to communicate with IMD. Thirdly, when the proxy is unable to jam the adversary and finds IMD responding to the adversary.

4.4.2 Implantable Medical Device

This is a regular IMD which includes all the components that are already in existence like battery (provides power), memory (stores collected data and therapy settings), sensor (for sensing medical parameters), actuator (for giving therapy), microcontroller (which manages the IMD operation) and communication interface along with transreceiver. In addition for our scheme, IMD will have following components:

1. PV Interface:This is used to extract a PV and output random bits with sufficient entropy.
2. Session Key Generation: This is used for generation of random, unpredictable session keys by use of PV bits as seed.
3. Encryption/Decryption: Ultra light weight cipher called PRESENT-80[91] or MISTY 1[70] can be used for encryption. When used in combination with GCM, integrity is also assured.

4.4.3 Enhanced External Device (ED)

This is a regular external reader/programmer that is used for wireless communication with IMD. In the proposed work, we require such external device to undergo Public Key based authentication procedure at the end of which it tends to exchange a temporary key with Buddy Device. This key is used to cancel the jamming signals to derive the one time session key. It also makes use of symmetric encryption while communicating with IMD using a secure request-response communication protocol.

4.5 Secure Communication Protocol

In this section we discuss the communication protocol for securing IMD by use of Buddy Device. The sequence diagram of communication protocol which uses Buddy Device is illustrated in Fig. 2. The protocol is explained below:

4.5.1 MD-Buddy Device Pairing

The Buddy Device needs to be paired with one or more IMDs of a patient for the very first time. This pairing can be done in a restricted environment like hospital. Once the devices

are paired, the Buddy Device needs to be configured with the information about authenticated external readers and the Access Control List (ACL). As the Buddy Device is configurable, external device information like Public Key can be added or removed as per need.

4.5.2 Reader Authentication

The Buddy Device listens for a communication request by an external device, on receiving request; it first authenticates the reader and then authorizes the type of request according to the ACL. Since all the communication to IMD should pass through Buddy Device, if a communication request is directly addressed to IMD, it uses fast jamming technique [97] to jam the signal. If it is unsuccessful in jamming the readers signal and it somehow reaches the IMD to which IMD starts responding then it immediately jams the IMDs response signal using slow jamming technique[86] .

4.5.3 Buddy Device-IMD Communication

The buddy device sends a request to the IMD in response to which the IMD generates one time session key by using random bits of PVs. When session key, X_{IMD} is transmitted by IMD, buddy device jams the communication. For jamming, it makes use of a PRNG with temporary key K_{temp} as the seed to continuously emit jamming signals X_{Buddy}. In our technique, authenticated external device can employ proper signal processing techniques to cancel out the jamming signals from the received mixed signals with the help temporary key, K_{temp} to derive the session key XIMD. In contrast, the unauthorized device does not have the secret keys, and cannot remove the interference introduced by Buddy's jamming signals. For an unauthorized device E, the signals received will be the mixture of both X_{IMD} and some portion of X_{Buddy}. This results into distortion of the IMD signal, X_{IMD}. As a result, unauthorized device E is unable to receive the session key. However, since R has access to temporary key K_{temp}, it can regenerate the same jamming signals X_{Buddy}. Once it finds out which portion of X_{Buddy}. is mixed with X_{IMD}, it can subtract this portion of X_{Buddy} to get a clean copy of X_{IMD}.

4.5.4 IMD-External Reader Communication

Once X_{IMD} is shared, telemetry messages are encrypted using light weight schemes like PRESENT-80 [77] or MISTY 1 [55]. Once a session is over, one time session key is discarded and cannot be reused so as to avoid replay attacks.

4.5.5 Emergency Access

To tackle emergency access when an authenticated device is not around, access can be granted to a doctor or ambulance staff by switching off the Buddy Device so that no authentication or jamming is performed. When IMD senses the unavailability of Buddy Device, during emergency, it transmits the session key to which no jamming is performed by Buddy due to its absence. The external device can capture the session key and communicate with the IMD. But once the session is over the session keys will no more be usable and Buddy Device can again take control of the IMDs. Thus, our scheme provides a controlled access during emergency for a very short duration.

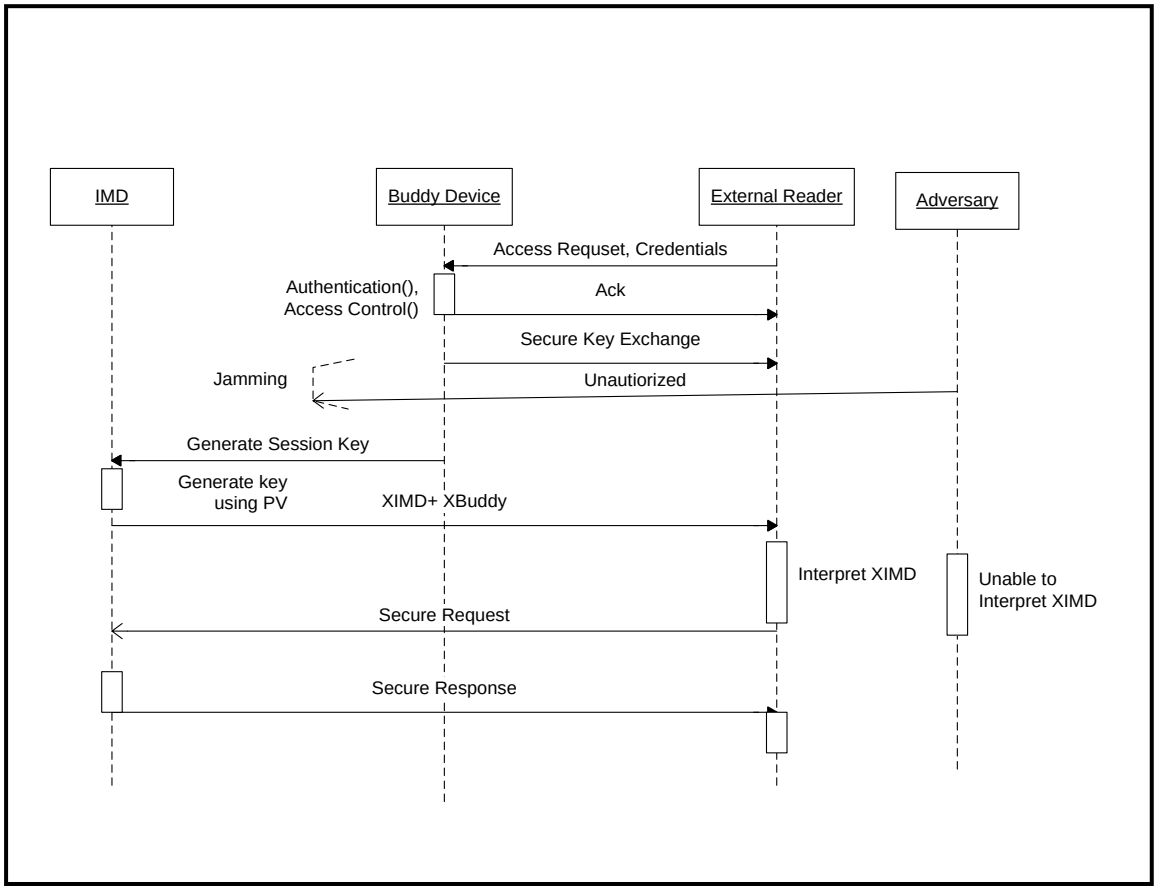

FIGURE 4.2 Sequence Diagram for Buddy Device based communication protocol

4.6 Conclusion

In this paper we proposed a Buddy Device which is used to grant secure access to IMD resources. Key based jamming technique is used to share session key at runtime. Our security protocol allows us to enforce Confidentiality, Integrity, Authentication and Access Control and also enforces Perfect Forward Secrecy (PFS). It protects the IMD against replay attacks. It is also successful in preventing resource depletion attack. As the jammer Buddy Device works as a mediatory it can be topped up with powerful access control policies, generation of audit logs and many other security features. Although this scheme enforces the patient to carry another device, these features can be integrated into the patients Smartphone itself. As a part of future work we explore the possibility of implementing the proposed security protocol on Android based Smart phones.