CHAPTER – 9

Conclusion, Major Contributions and Further Work

9.1 Objectives Achieved

This thesis addressed several challenging issues related to secure wireless communication of Implantable Medical Devices (IMDs). Solutions provided make use of an additional proxy device.

The contributions of our work, while trying to achieve the main goal of providing two-tier solution, are the following:

1. Firstly we performed a thorough Literature survey and threat modeling for security issues prevalent in wirelessly communication IMDs.
2. Secondly, we surveyed and analyzed all the available security solutions proposed by researchers.
3. Thirdly, we worked on providing a solution to detect active attacks for IMDs and also worked on providing emergency aware access control.
4. Fourthly, we proposed Buddy system solution for IMDs communicating with external devices.
5. Finally, we proposed a two tier based security model and designed communication protocol for various scenarios. We also implemented the protocol to provide a proof of concept.
6. Our solution based on two-tier model is intended to support heterogeneous co-existing IMDs on a human body and external devices like reader and programmer with widely varying capabilities when it comes to communication and computation

speeds and resource availability. The senders and receivers of data are decoupled. This allows the IMD to go back to sleep state once information has been relayed to proxy which can cache the data and save IMDs battery power.

7. The solution supports adjustments of frequency of probes that are performed on the IMD depending on the battery power, patient health condition etc.
8. The solution proposed is flexible and scalable providing a balance by using light-weight request-response protocols at one end and asynchronous publish-subscribe protocol at the other end.

9.2. Major Contributions

1. We proposed an IWBAN framework for securing wireless access of IMDs by providing end-to-end security at the application layer for intra-body as well as extracorporeal communication.
2. In the proposed security framework, we use an additional hand held proxy device (like PDA) as a mediator between external devices and different types of IMDs. This allows our defence system to offload security related processing and storage from the medical device thus conserving IMDs energy and memory. This offloading helps in reserving medical device resources only for medical functions.
3. In the proposed security framework we use secure and light-weight request-response communication protocol between IMD and proxy to provide mutual authentication, confidentiality, integrity and message freshness, for to and fro communication. These security services are provided by use of symmetric encryption and message authentication technique using 128-bit secret key, random nonces and counters. The secret keys required for symmetric encryption is exchanged between proxy and IMD during registration. For each IMD, a set of requests/response messages are defined and a list of Topics is defined with respect to the requests and responses, role (Publisher/Subscriber) of the IMD for each Topic is defined.
4. In the proposed security framework we use Publish-Subscribe communication protocol between proxy and external devices (readers and programmers) that are registered with the proxy and their public keys are stored for future authentication. A user interface is provided for selecting the available Topics and role

(Publisher/Subscriber) of the external device for each topic which further constitutes the access control list. Once external devices are registered with Proxy, they can securely publish or subscribe to the topics. Such communication provides mutual authentication, confidentiality, integrity, message freshness, and access control.

5. In the proposed security framework we use Proxy Device for secure dissemination of received telemetry data from IMDs to other IMDs or external devices which are registered as subscribers for the topic pertaining to the telemetry data.
6. In the proposed security framework we use Publish-Subscribe paradigm in the Proxy Device for secure collection of Published telemetry data for a specific Topic by IMDs or external devices which are registered as publishers and forward it to the relevant subscribers for that topic.
7. In the proposed security framework we provide a centralized security solution to communication pertaining to heterogeneous IMDs and other external medical devices which may either act as publisher or subscriber for a particular topic.
8. In the proposed security framework we use symmetric encryption techniques to secure communication between IMD and Proxy Device.
9. In the proposed security framework we use both symmetric encryption and asymmetric encryption techniques to secure communication between Proxy Device and other external device.
10. In the proposed security framework we provide a mechanism for peer-to-peer, end-to-end, multicast and broadcast wireless communication in a secure manner.
11. In the proposed security framework we provide a mechanism for asynchronous communication between IMDs and other external devices.
12. In the proposed security framework we provide resilience to Denial of Service attacks by using light-weight authentication and external proxy device.

9.3 Comparison of proposed Security Model with Existing Solutions

Our solution described in chapter 7 can be compared with [153] in which secure architecture is proposed based on publish-subscribe paradigm to guarantee confidentiality and access control.

Table 9.1 Comparison of proposed solution with [153]

Parameters	**[153]**	**Our Approach**
Use of Additional Device	Message Bus	Proxy Device
Communication model	Publish-subscribe	Request-response between IMD and Proxy Publish-subscribe between Proxy and ED
Confidentiality	Ciphertext policy attribute-based encryption (CP-ABE)	AES-GCM for authenticated encryption.
Access Control	Lattice-based access control (LBAC). Access control policies managed by IMD.	Device Role and Topic based. Access Control policies managed by proxy.
Access Control policies	Set on the IMDs therefore cannot be modified later.	Managed by Proxy device, therefore can be managed easily.
Perfect Forward Security (PFS)	No assurance of forward and backward security	Assurance for forward and backward security.
Support for Authentication	No	Yes
Overhead	Use of CP-Abe for encryption of symmetric key. Use of another algorithm for data encryption	IMD require use of AES-GCM encryption.
Usability	Secure Communication amongst IMDs	Secure Communication amongst IMDs and also with external devices.
Replay resilience	Not provided	Provided
DOS resilience	Not provided	Provided
Paradigm	Publish-Subscribe	Request-response and Publish-subscribe

The other available work with which our proposed solution can be compared are the ones which also make use of an external device to provide security. A comparison with such security schemes are given the table 9.2

Table 9.2 Comparison of proposed solution with solutions proposing use of external device

Comparison Parameters	**H2H [81]**	**Cloaker [80]**	**IMD Shield [84]**	**IMD Guard [86]**	**Medmon [45]**	**Our Approach**
Design Approach	Use of PVs	Trusted External Device	Trusted External Device	Trusted External Device (PVs)	Trusted External Device	Trusted External Device
Invasive Approach	Y	Y	N	Y	N	Y
Confidentiality	Y	Y	Y	Y	N	Y
Data Integrity	Y	Y	Y	Y	N	Y
Authentication	Y	Y	Y	Y	Y	Y
Message Freshness	N	N	N	N	N	Y
Replay Resilience	N	N	N	N	N	Y
Access Control	N	N	N	Y	Y	Y
Fail-open system?	N	Y	Y	Y	N	N
Secure IMD-IMD communication?	N	N	N	N	N	Y
Secure IMD-ED communication?	Y	Y	Y	Y	Y	Y

9.4 Possible Further Work

1. More investigation is required regarding the commands the IMD receives from a valid device or from other IMDs.
2. Secure software upgrades for IMDs needs to be analyzed further.
3. More complex access control policies can be derived for our security model.
4. Key exchange techniques between IMDs and external devices have a scope of further analysis. Cross layer security solutions need to be studied.
5. Implementation in simulators and analysis of energy expense and efficiency of the communication protocol for IMDs required to be studied further.
6. The current work on access control can be enhanced by including context awareness in the security model.