# CHAPTER – 8

# Implementation and Analysis

## 8.1. Implementation

We implemented the entire protocol to provide a proof of concept using C# programming language and XML. The prototype implementation demonstrated the suitability of our proposed solution. We have developed the prototype which is explained below:

Network Switch that simulates a wireless environment and broadcasts the received data to all the devices present in the network. The UI for the Network Switch is shown in Fig. 8.1.

Device Selection Screen which can be used to select a number of IMDs and a number of ED which are registered with the Proxy. It is compulsory to start the Proxy as the Proxy Device is heart of the proposed security model. The screen shot shown in Fig. 8.1 shows the UI for device selection. It shows the Device ID, Device Type, Name, Description, configuration file.

The configuration file is an XML file storing the details of the device. The Topic Management, device management and role management is implemented as XML files.

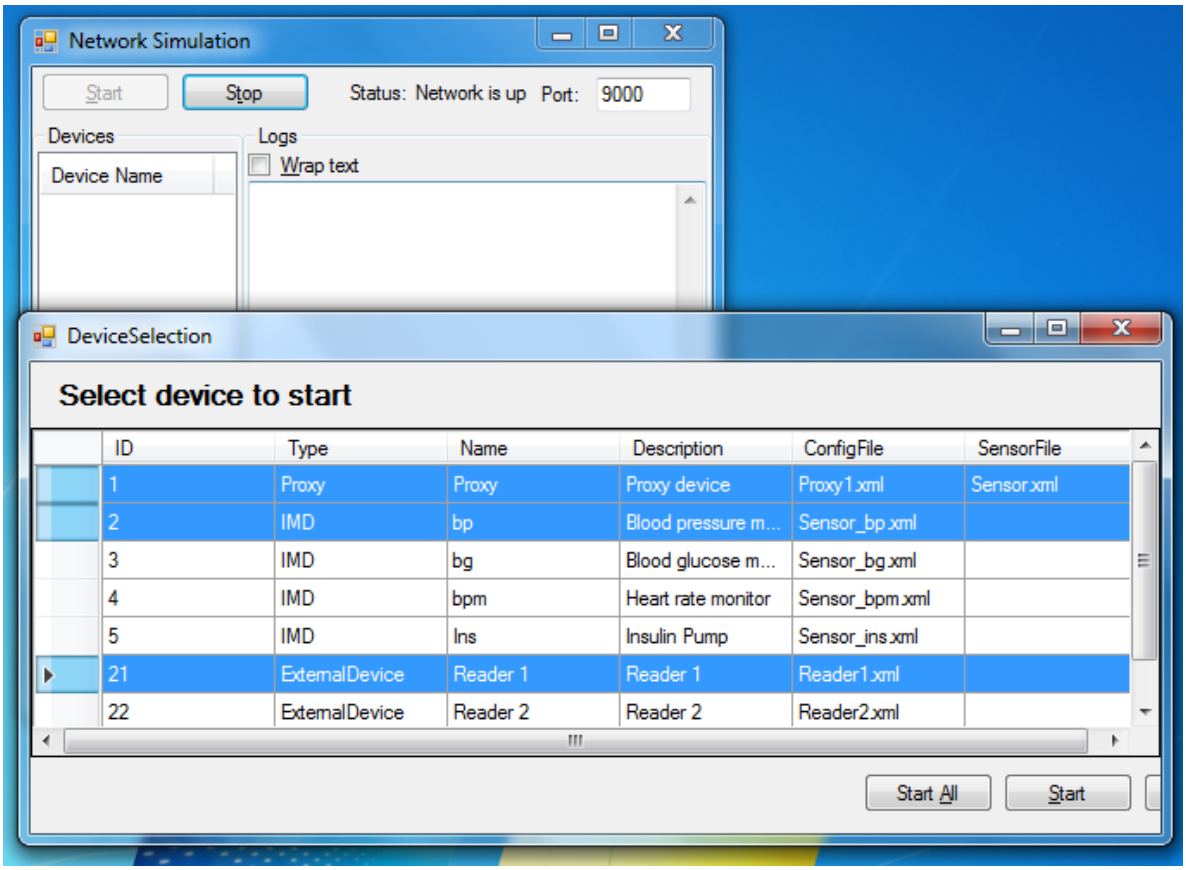


**Figure 8.1 Network Switch Screen and Device Startup Screen**

Once the Proxy device has started, secure request-response protocol is executed on click of Connect button of Proxy Device. The request-response protocol for Proxy initiating communication is described in Chapter 7. Mutual authentication between IMD and Proxy is shown in Fig 8.2. If one or more EDs are available, secure publish-subscribe communication protocol as described in Chapter 7 is executed by the Proxy.

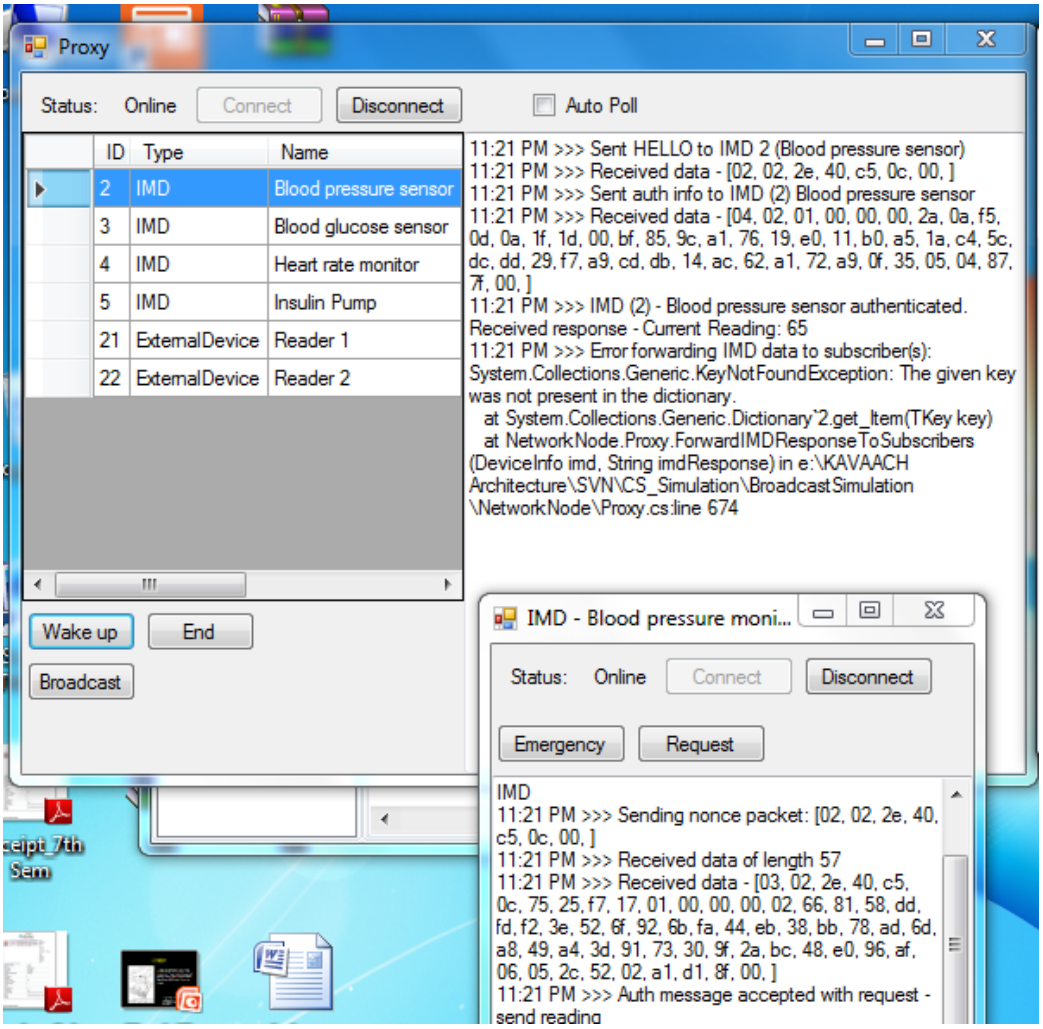


**Figure 8.2 Mutual Authentications between IMD and Proxy.**

A Registered External device can send a join request to the Proxy following which a mutual authentication protocol is executed by the Proxy and ED. The screenshot of External device sending join request to the proxy is given in Fig. 8.3.

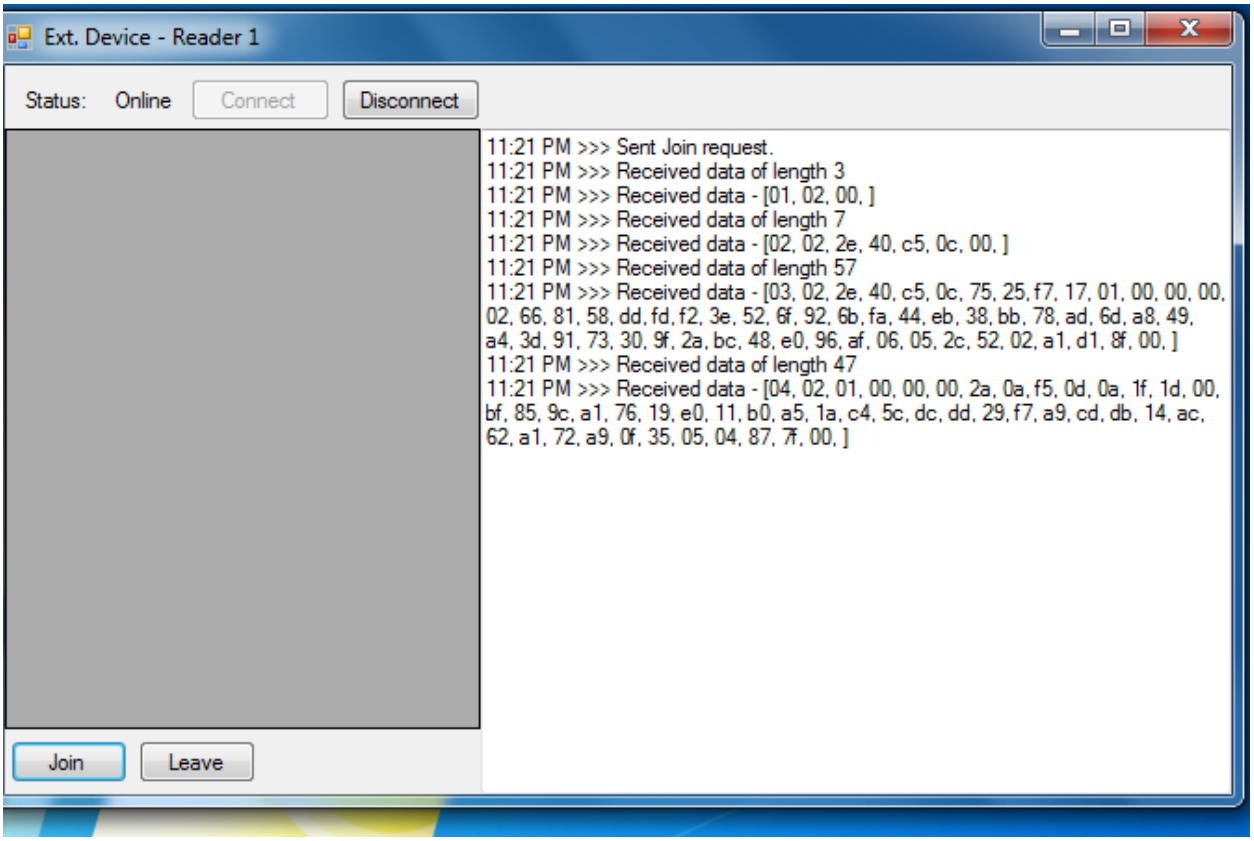


**Figure 8.3 External device sending join request to Proxy**

One the devices have started and mutual authentication phase is over. IMD and ED can communicate securely via the proxy device. A subscribe message from an external device for which IMD is the publisher is send by the proxy to the corresponding IMD as a request for data, The response obtained from the IMD is transformed into a publish message and a notified to the subscriber device. Similarly, when an external device or IMD publishes data for a topic, the subscriber IMD or external device is notified. The proxy communicates simultaneously with the IMDs and also with the EDs as shown in Fig. 8.4**.**

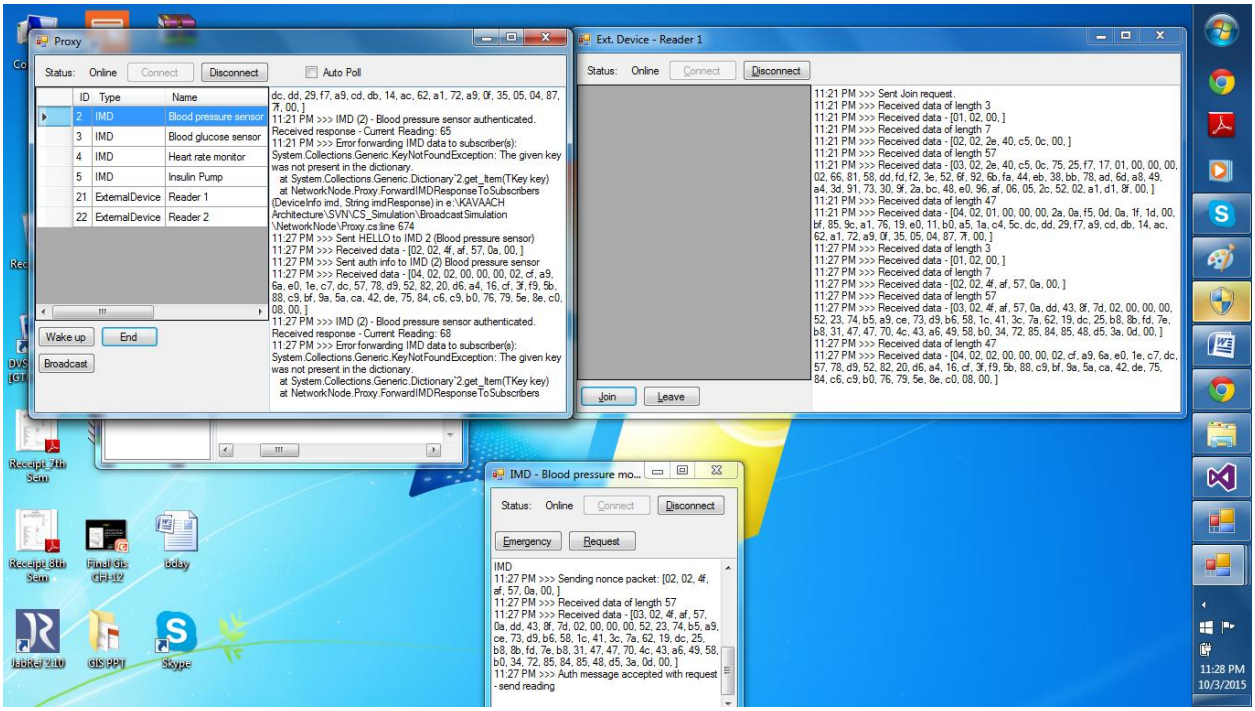


**Figure 8.4 Communications between Proxy, IMD and EDs.**

The data related to the topics, devices and access control policies is maintained by the proxy device in XML files. Thus all required information is present in the XML files. The Proxy communicated with the IMD using request response protocol in a secure manner. We have implemented the mutual authentication protocol proposed in chapter 7 which also required generation of nonce. For message encryption and decryption AES-GCM is used. We have implemented the formation of IV, and algorithm for incrementing the counter to check for message freshness.

## 8.1. Security Analysis

In this section we measure the security strength of the proposed model explained in chapter 7 with respect to some well know attacks:

1. **Denial of Service Attack:** The proposed security model has highly resistant to denial of service attack. The use of an additional Proxy device minimizes the load of performing security transformations. Use of symmetric cryptography for mutual authentication, and for data confidentiality between IMD and Proxy reduces energy consumption. Use of authenticated mode of encryption provides data integrity and authentication. The packets are designed in a manner to reduce the transmission overhead.

2. **Man in the Middle Attack (MITM):** The proposed security model uses a mutual authentication protocol which helps to thwart the man in the middle attacks.

3. **Replay Attack:** Involves passive capture of data messages or commands and then their retransmission. As we are making use of counter to detect packet freshness such attack can be detected.

4. **Masquerade Attack:** A rouge device can pretend to be an IMD or a proxy by capturing authentication sequences and replaying. Such attacks can be thwarted by the mutual authentication by making use of nonce.

5. **Message Modification:** Alteration in message can be detected by the recipients due to use of authenticated mode of encryption.

6. **Known-Ciphertext Attack:** In this attack adversary tries to deduce a plaintext or key from a set of known ciphertexts. GCM uses a pseudo random function to generate a unique key before performing encryption therefore adversary cannot deduce any information about the key or plaintext from the ciphertext.

7. **Known-Plaintext Attack:** In this attack adversary has one or more plaintext-ciphertext pairs formed with the secret key from which it tries to deduce the key of the plaintext. The encryption scheme chosen is resilient to such attack. The secret key shared between IMD and Proxy is not known to external device therefore our model is secure.

## 8.3. Conclusion

Through our prototype implementation we developed a proof of concept which confirms that the proposed two tier based security framework is possible to be implemented with wireless IMDs which are networked in and IWBAN. The security analysis with respect to various attacks shows that our scheme is resilient to security attacks which are most critical for IMDs.