CHAPTER – 6

Detection of Active Attacks on wireless IMDs using Proxy Device and Localization Information

6.1 Introduction

While passive attacks on IMD can be addressed using encryption techniques, active attacks like replay attacks, massage injection and MITM attacks needs more innovative techniques to be identified to handle with. To address the problem of Active Attacks, we advise the use of RF-signal based localization technique which leverages multi-antenna Proxy Device to profile the directions in which Reader/Programmer signal arrives and use the triangulation technique to generate a signature that uniquely identifies authorized external device. This technique is an extension of Secure Angle **[106]** which was proposed for wireless networks to improve security.

While security mechanisms like authentication and encryption is must, they alone are unable to fight active attacks like Man-in-the-Middle, Replay and Message Injection and require use of some extra technique. As IMDs are themselves resource constrained many researchers have proposed to shift the security related processing to an external proxy device which acts as an intermediary [80, 84, 86]. In this chapter, in order to prevent active attacks we propose to use a multi-antenna Proxy Device which securely pairs with IMD and relays messages from external device to and fro IMD.

In this model reader/programmer transmits an RF signal in order to communicate. The Proxy Device which is in listening mode, receives the transmitted signal and tries to estimate the Time Difference of Arrival (TDoA), Received time of flight (RTOF), phase of arrival (POA) and angle of arrival (AOA).These parameters depend on the location from which signal is being transmitted. We assume an authentication mechanism in place for differentiating an authorized reader from an unauthorized one. Once the authentication stage is over, then in the second step, the accumulation of the estimated parameters is applied to bring forth a unique signature which is utilized to differentiate authorized external device from an un-authorized one by the Proxy Device. We assume that the proxy device is capable of deriving these values from the received signal.

Our work is different from the work proposed in [106] as they have used AoA signature in general wireless environment to prevent MAC spoofing attacks. Whereas we are using the AoA signature to prevent active attacks specific to Implantable Medical Devices using a Proxy Device. Information derived by use of Triangulation Techniques can be used by multi-antenna Proxy Device to drop frames from unauthorized reader/programmers by verifying its AoA signature. Thus, unauthorized requests will be refrained from being sent to IMDs hence saving its expensive resources. The techniques to mitigate active attacks on wireless telemetry between IMD and reader/programmer require extra energy, computation and bandwidth from the medical device Therefore we use a Proxy Device which mediates the communication.

6.2 RF based localization techniques

Wireless location based sensing systems for indoor applications are presented in [108] . Triangulation is one such technique that uses the geometric properties of triangles to estimate the target location. It has two derivatives: lateration and angulation. Lateration is used to estimate the position of an object by measuring its distance from multiple reference points by measuring Time of Arrival (ToA), Time Difference of Arrival (TDoA): and Received Signal Strength Indicator (RSSI). Angulation is used to locate an object by measuring the angles relative to multiple reference points and is called.Angle of Arrival(AoA). These techniques are described below:

6.2.1 Time of Arrival (ToA)

The ToA is the time taken by a signal to arrive at the receiver and is calculated as the sum of the transmitting time and the propagation delay. Once the one-way propagation time is measured, it is used to calculate the distance of the transmitter. It requires the devices to possess synchronized clocks and presence of a timestamp in transmitted signal for receiver to calculate the distance, signal has travelled. Its accuracy is affected by non-line of sight.

6.2.2 Time Difference of Arrival (TDoA)

In order to determine relative position of transmitter, the difference between several signal arriving times is used. The signal is received by multiple receivers are synchronized in time. Its accuracy is affected by non-line of sight.

6.2.3 Received Signal Strength Indicator (RSSI)

It is measured as voltage value representing the power present in radio signal of the receiver unit [109]. RF-signals are subject to multipath attenuations due to barriers.

6.2.4 Angle of Arrival (AoA):

Here the direction of a signal is used to calculate precise object locations. The result is obtained from the intersection of several pairs of angle direction lines, each formed by the circular radius from antennas of various devices [108]. Therefore the angle of the arriving signal is detected by using sensor arrays. At each sensor element a signal arrives with a path difference. These differences can be used to calculate the angle of arrival . The location estimate degrades as the mobile target moves farther from the measuring units. While in our proposed system, we make use of AoA, better results can be obtained by using a combination of techniques.

6.3 Overview of components

6.3.1 System Configuration

Our model consists of three components, the IMD, the multi-antenna Proxy Device and reader/programmer. The IMD is implemented in the body to perform therapeutic functions. The programmer/reader is interested in wireless communication IMD to read telemetry data or send commands. The Proxy Device is a multi-antenna device with more power and resources for security related transformations and is rechargeable. Proxy Device is tightly coupled with IMD. Proxy authenticates the reader/programmer on IMDs behalf. Once IMD and Proxy are paired, IMD acts only on those requests that are sent through the Proxy

6.3.2 Assumption

We use AoA technique not to find the exact location of a transmitting device, but to use AoA information to generate a unique signature to identify the communicating device. We assume the authenticated reader / programmer is in close proximity to Proxy Device and that adversary does not possess information to get authenticated.

6.3.3 Proxy Device Overview

When an authorized reader starts communicating with Proxy device, it indirectly measures the distance between an incoming signal's arrival at each antenna and calculates the angle of arrival (AoA). It generates a signature from AOA that is unique to the reader/programmer. The proxy can recalculate the AOA at random intervals to identify forged devices. In order to forge the signature, the attacker needs to know the locations of the communicating devices and all obstacles in the vicinity The combined direct path and reflection path AoA unique signature can be generated as in [4]. This signature can be used in conjunction with other security techniques like encryption and authentication. When a reader moves or a barrier moves, the angle of arrival may change and therefore it needs to be recalculated. The proxy device is calibrated as mention in [106] to generate AoA signature.

6.4 Signature Generation and Verification

The proxy device authenticates the External Device, and measures TDOA, RTOF, POA and AOA. The resultant value is fed into a secure hash function, like SHA-256.

S= Hash (TDOA || RTOF POA|| AoA) ---------------From [122]

This value easily verifies if the party transmitting is actual IMD or MIMT. Figure 6.1 shows the flowchart for Proxy Device performing signature verification.

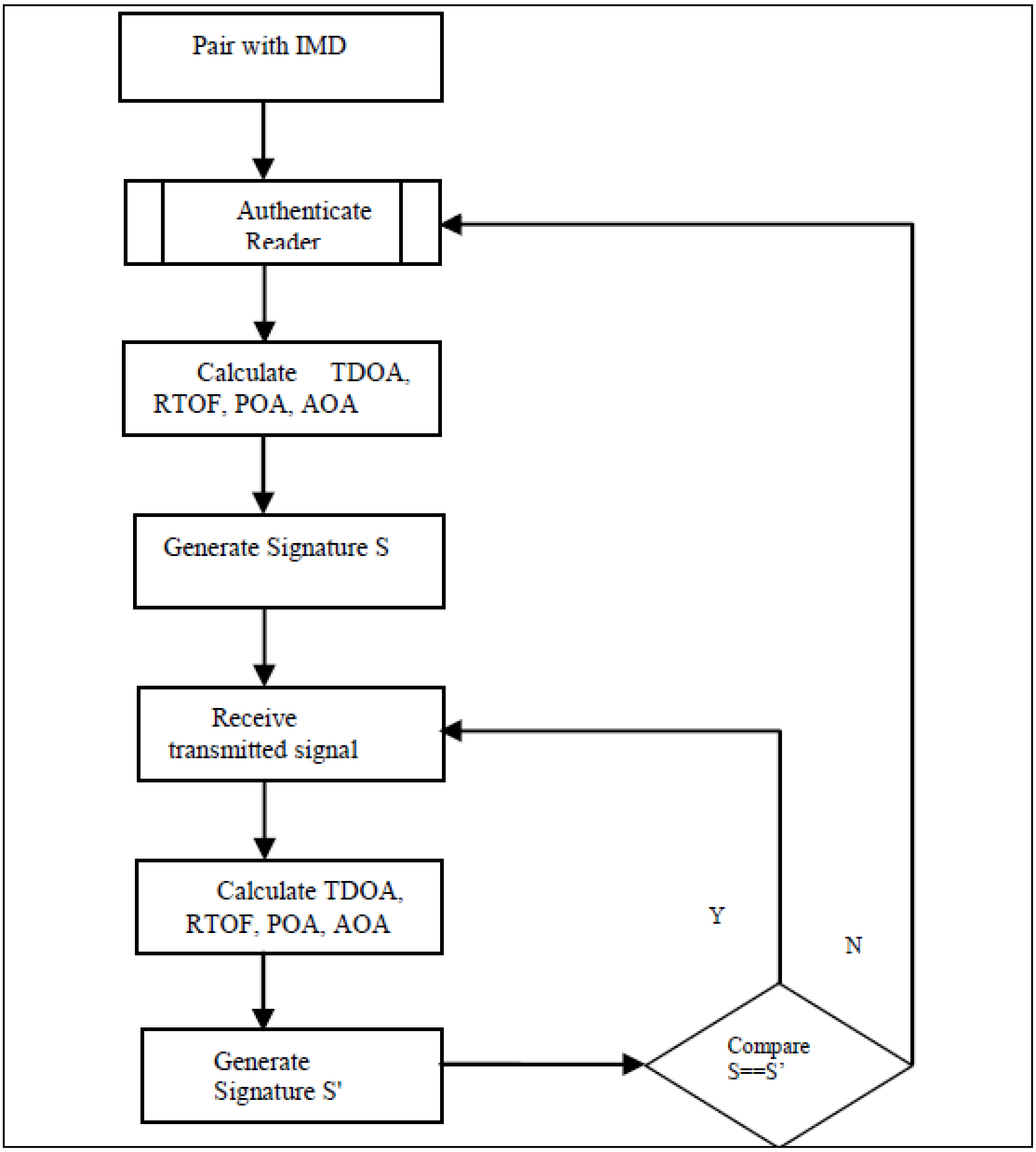

FIGURE 6.1 Signature Verification [122]

6.5 Proposed Proxy based Protocol

We assume that the IMD and Proxy Device are securely paired. Proxy Device (A) receives request from reader/programmer (B) for communication with IMD. Table 6.1 sums up the notations used. A after authenticating B, generates B's triangulation based signature S_B and stores it and grants access to the IMD. For every request from B or after random time intervals, A recalculates the AOA based signature and compares it with stored signature $S_{B.}$ If there is a significant discrimination in the signature, A asks B to get authenticated (as either B or obstacle has changed position or a forged request is received). If B successfully gets authenticated, it is granted access and its triangulation based signature is changed to the new value i.e. S_B'. Instead of B, if T sends a request to proxy the signature generated is S_T, which will not match with stored S_B and this will activate the authentication process during which T will be denied access. This technique is successful in preventing active attacks as any message from T will not get accepted unless either the device or the triangulation based signature is verified. As noted earlier, it is very difficult for T to spoof the triangulation based signature of B as T needs to induce the positioning data of both authorized reader/programmer and Proxy device, and also needs to forge the direct path AoA and all multipath AoA as an example. FIGURE 6.2 shows the sequence diagram for the signature verification based protocol.

TABLE 6.1 Table of Notation [122]

A	Proxy Device
B	Authenticated Reader/Programmer
T	Adversary Reader/Programmer
S_B	AoA Signature of B
S	AoA Signature calculated for each request
$S_{B'}$	Modified AoA Signature of B
S_T	AoA Signature of T

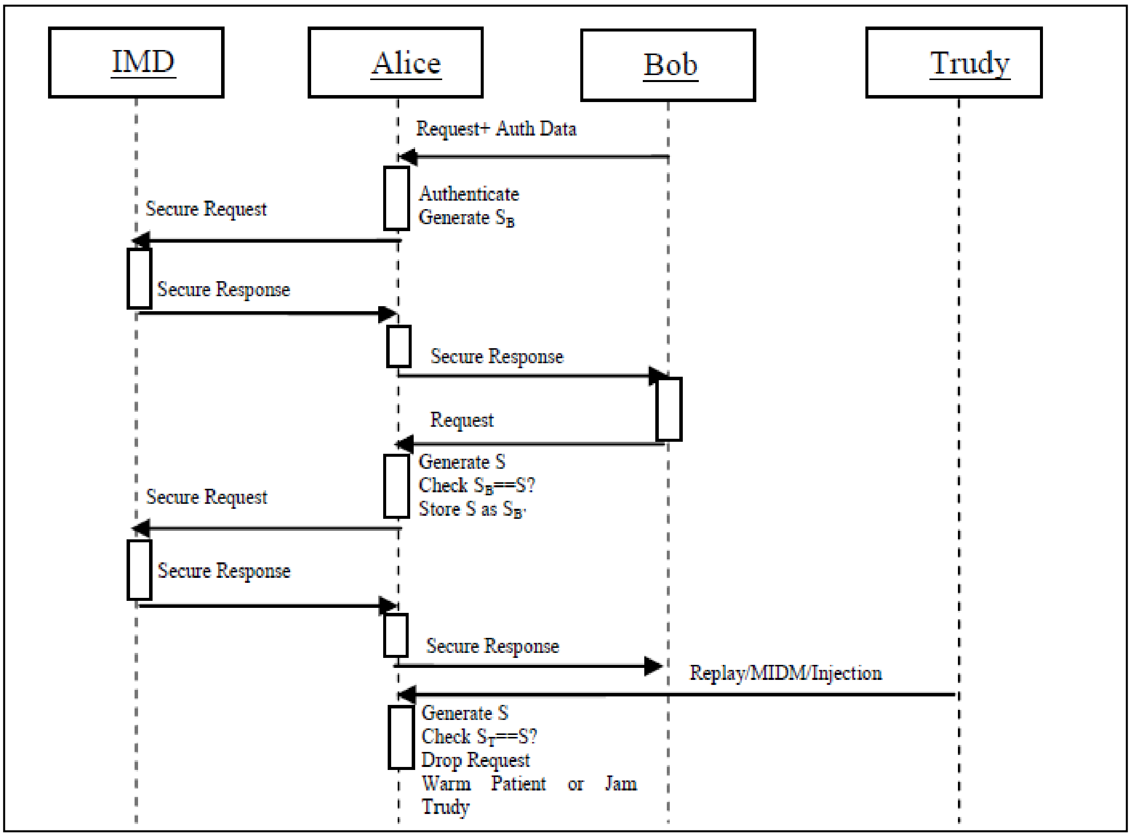

FIGURE 6.2 Sequence Diagram for Signature Verification Protocol [122]

6.6 Conclusion

In this chapter we made use of triangulation technique to generate a unique signature of the authorized external device and use it for detection of active attacks like MITM, Replay or Message Injection.