Towards Development of a Remote Charting System for Connected Healthcare

Alex Bodurka
Western Michigan University, ajbodurka@gmail.com

Follow this and additional works at: https://scholarworks.wmich.edu/masters_theses

Part of the Computer Sciences Commons, and the Health Information Technology Commons

Recommended Citation
https://scholarworks.wmich.edu/masters_theses/5175
TOWARDS DEVELOPMENT OF A REMOTE CHARTING SYSTEM FOR CONNECTED HEALTHCARE

by

Alex Bodurka

A thesis submitted to the Graduate College
in partial fulfillment of the requirements
for the Degree of Master of Science
Computer Science
Western Michigan University
December 2020

Thesis Committee:

Shameek Bhattacharjee Ph.D., Chair
Ajay Gupta Ph.D.
Alvis Fong Ph.D.
TOWARDS DEVELOPMENT OF A REMOTE CHARTING SYSTEM FOR CONNECTED HEALTHCARE

Alex Bodurka, M.S.

Western Michigan University, 2020

Health Care Providers play a crucial role in a patient's well-being. While their primary role is to treat the patient, it is also vital to ensure that they can spend adequate time with the patient to create a unique treatment plan and build a personal relationship with their patients to help them feel comfortable during their treatment. Health Care Providers are frequently required to manually record patient data to track their healthcare progress during their hospital stay. However, with hospitals continuously trying to optimize their workflows, this crucial one-on-one time with the patient is often not practical.

As a solution, this thesis puts forward a novel connected healthcare architecture known as Remote Charting System that aims to liberate the Health Care Provider from repetitive manual tasks by automating the process of medical charting, thus enabling them to spend more time with real patient-care, and improve quality of care. Furthermore, this work provides a framework for Remote Charting that automates medical charting activity and puts forward a secure by design framework that addresses authorization and authentication concerns while adhering to the patient privacy and policy constraints that hospitals need to be compliant of.

Specifically, we make the following contributions: First, we propose a communication network of connected medical devices that automates the Health Care Provider's charting duties. Second, we conduct a threat landscape analysis of the remote charting system based on vulnerabilities found in medical devices and under a hospital environment’s unique challenges and constraints. Third, given the challenges, we propose a physical layer hypothesis testing approach towards a HIPAA compliant authorization scheme for medical devices that can be used for a remote charting application. Finally, we provide a theoretical construct of an envisioned security architecture for a remote charting system for connected health where our proposed authorization scheme is one of the modules. Finally, we design a simulated remote charting system to validate our method’s accuracy under varying parameters.
# Table of Contents

## LIST OF TABLES

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>iv</td>
<td></td>
</tr>
</tbody>
</table>

## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>v</td>
<td></td>
</tr>
</tbody>
</table>

## 1 INTRODUCTION

1.1 Challenges ....................................................... 1
  1.1.1 Clinical and Workflow Constraints ................................ 2
  1.1.2 Privacy Policy Constraints .................................... 3
  1.1.3 Safety and Security ....................................... 3
  1.1.4 Device Hardware Constraints ................................. 4
1.2 Contributions of this Work ..................................... 4
1.3 Organization of the Paper ...................................... 5

## 2 Background Literature

2.1 Medical Charting ................................................ 7
2.2 Motivation for Automated Medical Charting .................... 9
2.3 Remote Charting versus Competing Automated Solutions ........ 11
2.4 Security View of the Connected Medical Device Spectrum ...... 12
2.5 Challenges Unique to the Clinical Setting .................... 15
  2.5.1 Regulatory and Compliance Issues ............................ 15
  2.5.2 Clinical Workflow Constraints ............................... 16

## 3 Proposed Architecture of Remote Charting Application

3.1 Building Blocks of Remote Charting System .................... 18
  3.1.1 Network Segmentation ........................................ 18
  3.1.2 Device Classes ............................................... 20
  3.1.3 Actors .......................................................... 21
  3.1.4 Types of Network Connection ................................ 22
  3.1.5 Server Applications ......................................... 22
  3.1.6 Remote Charting Architecture ................................ 23
3.2 Narrowed View of the Remote Charting System ................ 26
3.3 Need for a Novel Authorization Approach ...................... 28
  3.3.1 Current Authorization Approaches in other IoT Systems ...... 29
  3.3.2 Current Authentication Approaches in IoT Environments ..... 30

## 4 Threat Landscape Development for Remote Charting System

4.1 Architectural Weaknesses ....................................... 32
4.2 Operational Weaknesses ......................................... 33
4.3 Categories of Vulnerabilities .................................. 34
  4.3.1 Motives of Attackers ....................................... 34
  4.3.2 Impact of the Attack ....................................... 35
  4.3.3 Method of Manipulation ..................................... 35
4.4 Attack Strategies ............................................... 35
  4.4.1 Spoofing Attacks ............................................ 36
  4.4.2 Fabrication Attacks .......................................... 36
# Table of Contents—Continued

4.4.3 DoS Attacks ................................................. 36

5 Proposed Authorization Framework ........................................ 37
5.1 Device and Resource Constraints ......................................... 37
5.2 Assumptions ..................................................... 38
5.3 Framework Definition .............................................. 40
  5.3.1 Inter BBN - Physical Layer Authorization .......................... 43
  5.3.2 Intra BBN - Physical Layer Anomaly Detection + Device Fingerprinting ........................................... 43
  5.3.3 Primer on Channel State Information (CSI) Data .................. 44
  5.3.4 Anchor Points with Antenna Arrays ................................ 44
5.4 Similar Work .................................................... 48

6 Process for Inter BBN Authorization ...................................... 50
6.1 Group Physical Layer Authorization ..................................... 51
  6.1.1 Process Steps ................................................. 51
  6.1.2 Hypothesis Testing ............................................. 55
  6.1.3 Final Hypothesis Test Procedure at Deployment .................. 67
  6.1.4 Final Voting Decision and Consensus ............................. 73
6.2 Human Assisted Device Assignment ..................................... 74
6.3 Authorization Decision ............................................... 75

7 Process for Intra BBN Authentication and Attack Detection ............ 76
7.1 Compromised Device Detection ........................................ 77
7.2 New Attack Detection ............................................... 77
  7.2.1 Device Placed in BBN Area ...................................... 77
  7.2.2 Removal and Replacement of a Patient-Specific Device ............ 78
  7.2.3 Rearrangement of a Patient-Specific Device ....................... 78
  7.2.4 Stale Data .................................................... 79
7.3 EMR Decision .................................................... 79

8 Simulated Results .................................................... 80
8.1 Setting of System Threshold .......................................... 80
8.2 Proximity Threshold and Error Probability ................................ 83
8.3 Varying Parameters ............................................... 84

9 Threat Analysis ....................................................... 89
9.1 Spoofing Attacks .................................................. 89
9.2 Fabrication Attacks ................................................ 90
9.3 DoS Attacks ....................................................... 90

10 Conclusion .......................................................... 91

References .............................................................. 93
## List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Acuity Level to Caregiver/Patient Ratio</td>
<td>8</td>
</tr>
<tr>
<td>2.2</td>
<td>Patient Data Collection Methods</td>
<td>10</td>
</tr>
<tr>
<td>2.3</td>
<td>CVSS v3.0 Attack Vectors</td>
<td>14</td>
</tr>
<tr>
<td>5.1</td>
<td>Device Constraints</td>
<td>38</td>
</tr>
<tr>
<td>6.1</td>
<td>Relationship between Distance and Errors</td>
<td>63</td>
</tr>
<tr>
<td>8.1</td>
<td>Example False Localization Errors ( P_{fe}(x) )</td>
<td>81</td>
</tr>
<tr>
<td>8.2</td>
<td>Example Missed Localization Errors ( P_{mi}(x) )</td>
<td>81</td>
</tr>
<tr>
<td>8.3</td>
<td>Calculated Localization Errors</td>
<td>81</td>
</tr>
<tr>
<td>8.4</td>
<td>Observation Distributions</td>
<td>83</td>
</tr>
</tbody>
</table>
# List of Figures

3.1 Remote Charting with Security View of Connected Medical Device Spectrum ........................................ 25  
3.2 Narrowed View of Remote Charting System ................................................................. 27  
4.1 Architectural Overview of Bed Bay Device ........................................................................ 33  
5.1 Layout of a BBN ............................................................................................................. 39  
5.2 Defense Flowchart ......................................................................................................... 42  
5.3 System Architecture of [1] ............................................................................................ 45  
5.4 Relative distances: $d^0_T$, $d^0_{00}$ ............................................................................. 48  
6.1 Group Physical Layer Authorization Process .................................................................... 52  
6.2 System Threshold ......................................................................................................... 60  
6.3 Location Accuracy of [1] ................................................................................................. 62  
6.4 Example Sensor Locations ............................................................................................ 63  
6.5 Missed Localization Error .............................................................................................. 65  
6.6 Example Gaussian Distribution: .................................................................................... 72  
8.1 Impact of Higher Cost for False Alarms ........................................................................ 84  
8.2 Impact of Higher Cost for Missed Detections ................................................................. 85  
8.3 Impact of Prior Bias $P_0$ and $P_1$ ............................................................................... 86  
8.4 Impact of mean $m_0$ and $m_1$ ..................................................................................... 87  
8.5 Impact of standard deviation $\sigma_0$ and $\sigma_1$ ............................................................. 88
Chapter 1

Introduction

A large portion of a Health Care Provider’s (HCP) day is spent on documenting sensitive information about patients into a health record. This process is known as medical charting. However, the process of manual medical charting is very time consuming and complex. Several studies have shown that nurses spend up to 26.2–41% of their time charting data received from periodic rounds to each patient [14], [11]. Systems exist that enable this information to be logged for the health care professional (doctors) automatically, but these systems are often expensive and introduce security concerns if networked with other devices to the regular internet.

**Broad Research Hypothesis:** Ideally, a system that could provide continuous real time medical charting would offer the potential for quick and timely healthcare interventions, that will improve quality of healthcare outcomes. To relieve the burden of doctors and nurses from manual medical charting and recording of health records, this thesis presents a vision towards an architectural framework called *Remote Charting System*, that automates the process of medical charting, while adhering to all constraints imposed by clinical workflow, HIPAA privacy policies, healthcare device hardware as well as security and safety concerns. Specifically, this thesis proposes a cyber physical system that connects multiple patient specific medical sensors and actuators in various hospital wards over wireless with the backend application servers that hosts electronic health database. The control decisions are issued by the health care professional either physically or remotely based on contextual factors by accessing the electronic
health database. This thesis also performs a threat assessment of the remote charting system and offer
design considerations that provide a mechanism for authorization of the medical devices without violating
HIPAA constraints, and workflow.

1.1 Challenges

In this section, we present several classes of challenges that exist in the healthcare industry, which
makes the problem of designing a safe remote charting system non-trivial. The challenges can be widely
categorized into the four broad categories: (1) Clinical Workflow (2) Privacy Policy (3) Device Hardware
(4) Safety and Security.

Several challenges arise when it comes to automating the system of remote charting through wireless.
Some of challenges are briefly outlined below, which will be elaborated further in later sections.

1.1.1 Clinical and Workflow Constraints

The envisioned remote charting system should be aware that it cannot negatively change the usual
clinical workflow. Some of the constraints include the following:

(1) Medical sensors and actuators can be switched among multiple different patients based on the
need. Therefore, a single medical device is not permanently tied to a single patient. However, HIPAA
constraints the mapping between patient IDs and device IDs, since the patient IDs are matched with
their health records they must be protected.

(2) A single patient may have multiple new devices assigned at various points of time during their
hospital stay. The remote charting system should be able to ensure that the correct device is being
attached to the correct patient for accurate healthcare delivery. Therefore, the device and patient
mappings cannot be pre-planned.

(3) A hospital ward has multiple beds, each with a patient within the same room. A remote charting
system should be able to reliably distinguish between two different devices belonging to the different
patients versus two different devices from the same patient. This is because healthcare decision is typically
based on inputs from multiple different sensing modalities (for example, the medicine administered to
particular patient should depend on both heart rate, blood pressure, and blood sugar combined).
1.1.2 Privacy Policy Constraints

The patient ID and name mappings are also considered private since knowing a patient ID or device ID can be traced back to a unique patient. This is one of several regulatory and policy constraints under the umbrella term Health Insurance Portability and Accountability Act (HIPAA) in the United States.

In the United States, the FDA provides guidance for the Health Delivery Organization (HDO) and Medical Device Manufacturers (MDM) to follow the rules.

In the European Union, the equivalent of HIPPA, is known as General Data Protection Regulation (GDPR), which is more strict in terms of privacy policy constraints compared to the HIPAA constraints. More details have been elaborated in later sections, about privacy policy constraints.

1.1.3 Safety and Security

Any automated system for remote charting should provide perimeter defense such as basic authorization and authentication of medical devices.

The property of Integrity is defined as the guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity [10]. Integrity can be further broken down into Data and System Integrity:

- **Data Integrity** – The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit [10].

- **System Integrity** – The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental [10].

The sub-properties of Authentication and Authorization will also be covered. Here Authentication and Authorization are defined as

- **Authentication** - Verifying the identity of a user, process, or device [10].

- **Authorization** - The process of verifying that a requested action or service is approved for a specific entity [10].
1.1.4 Device Hardware Constraints

These are challenges and restrictions imposed by the hardware of medical sensors, devices, and actuators.

(1) The authorization approach needs to be aware that multiple devices from different Medical Device Manufacturers (MDMs) are used, and therefore the authorization has to agnostic to the MDM’s device specifics and underlying hardware technology.

(2) The remote charting could only use sensors and actuators that are lightweight and straightforward embedded devices with no computation capabilities and limited memory and cannot deploy additional security mechanisms.

(3) Current medical device market does not have devices that implement hardware-based security. Given the already high healthcare cost, the HDOs are not keen on buying in hardware security embedded devices due to their high cost and the scale at which these sensors and actuators are required for the remote charting across the whole hospital. Typically, all patient-specific medical sensors and actuators should be less than $10.

1.2 Contributions of this Work

The motivation for this work stems from the lack of research and solutions regarding Remote Charting Applications that is fit for real connected healthcare industry needs. With regulatory bodies worldwide starting to focus more on Security and Privacy, designing a system that adheres to these evolving standards while still viable in a clinical setting is of increasing importance.

We propose a framework for implementing a Remote Charting system that can be quickly adopted while still being secure and limiting exposure to regulatory violations. In addition, this paper delivers for the first time, a comprehensive overview of the entire medical device spectrum from a security point of view. Specifically, we make five key contributions:

1. We propose a communication network of connected medical devices that automates the Health Care Provider’s medical charting duties and parts of clinical workflow by seamlessly integrating the patient’s medical sensors and actuators to application servers, electronic health database, and
other clinical apps.

2. We conduct an elaborate threat landscape analysis of the remote charting system based on vulnerabilities found in medical devices and exacerbated under a hospital environment’s unique challenges and constraints.

3. Given the challenges, we propose a physical layer hypothesis testing approach towards a HIPAA compliant authorization scheme for medical devices that are compatible with remote charting systems for connected healthcare and other constraints listed.

4. We provide a complete security requirement specification of the remote charting of an envisioned modularized security architecture for a remote charting system for connected health where our proposed authorization scheme will be one of the modules.

5. We design a simulated remote charting system to validate our method’s accuracy under varying parameters.

1.3 Organization of the Paper

This paper is organized into seven main chapters:

- **Background Literature** - provides detailed information about medical charting, current solutions, various classes of connected medical devices, and challenges that are unique to the remote charting application.

- **Proposed Architecture of Remote Charting Application** - provides an overview of the Connected Medical Device Spectrum before proposing an architecture for implementing a Remote Charting system.

- **Threat Landscape Development for Remote Charting System** - discusses the vulnerabilities and security threats relevant to a Remote Charting System.

- **Proposed Authorization Framework** - provides a list of constraints, assumptions, and an overview of the proposed security framework.
• **Process for Inter BBN Authorization** - explains the decision process for authorizing a new device to join a particular network.

• **Process for Intra BBN Authentication and Attack Detection** - explains the process for detecting new attacks and previously compromised devices.

• **Simulated Results** - provides results for a simulated remote charting system.
Chapter 2

Background Literature

In this chapter, we will first elaborate on the idea of the meaning and current best practices for medical charting in the healthcare industry under Section 2.1. Second, we put forth a discussion on why and how advent of ubiquitous smart devices are enabling smart connected healthcare. Specifically, we also point out how such new devices can revolutionize medical charting by enabling a high level idea of an automated medical charting system known as Remote Charting System and underscore its benefits.

Third, we provide a general description of various classes of connected medical devices and the type of vulnerabilities they fall under using the popular Common Vulnerability Scoring System (CVSS), which motivates security thinking in smart connected health. Finally, we put forward certain medical charting and healthcare specific challenges that are unique to our problem, that prevents us from directly borrowing existing solutions of authentication.

2.1 Medical Charting

As described earlier, the process of documenting sensitive information about patients into a structured health record is known as Medical Charting. Such Medical charts, (aka notes) can be categorized into two sub groups: (i) Nursing Notes; and (ii) Medical notes. While Nursing notes are typically informal and unregulated, Medical Notes are tightly regulated by various government bodies. Formally, these groups is defined as follows:
• **Nursing Note (Chart)** - A nursing note is a medical note that is put into a medical or health record made by a nurse that can provide an accurate reflection of nursing assessments, changes in patient conditions, care provided and relevant information to support the clinical team to deliver excellent care [5].

  1. Not all data is required to be entered in the EHR/EMR

  2. Variety of different formats are possible.

• **Medical Note (Chart)** - is an entry into a medical or health record made by a physician, nurse, lab technician, or any other member of a patient’s healthcare team [5].

  1. All data goes into an Electronic Health Record (EHR) or Electronic Medical Record (EMR)

  2. The file formats are government regulated

The accuracy and comprehensiveness of these charts/notes are crucial for the successful treatment of the patient. The patient parameters and frequency that they need to be retrieved typically depend on the patient’s acuity level. As shown in Table 2.1, the patient’s acuity level is directly proportional to the caregiver to patient ratio. The ratio directly impacts the amount of time the HCP can spend with each patient.

Table 2.1: **Acuity Level to Caregiver/Patient Ratio**

<table>
<thead>
<tr>
<th>Item #</th>
<th>Environment</th>
<th>Acuity Level</th>
<th>Patient Parameters Monitored</th>
<th>HCP to Patient</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Emergency Department</td>
<td>Low + Medium</td>
<td>ECG, SpO2, NIBP, EtCO2, Temp, IBP</td>
<td>1:1</td>
</tr>
<tr>
<td>2</td>
<td>Emergency Department</td>
<td>High</td>
<td>ECG, SpO2, NIBP, EtCO2, Temp, IBP</td>
<td>6:1</td>
</tr>
<tr>
<td>3</td>
<td>Intensive Care Unit</td>
<td>High</td>
<td>ECG, SpO2, NIBP, EtCO2, Temp, IBP</td>
<td>2:1 to 6:1</td>
</tr>
<tr>
<td>4</td>
<td>Med-Surg</td>
<td>Medium</td>
<td>ECG, SpO2, NIBP, EtCO2, Temp</td>
<td>1:6 to 1:8</td>
</tr>
<tr>
<td>5</td>
<td>Med-Surg</td>
<td>Medium to Low</td>
<td>ECG, SpO2, NIBP</td>
<td>1:10 to 1:45</td>
</tr>
<tr>
<td>6</td>
<td>Med-Surg</td>
<td>Low</td>
<td>SpO2, NIBP, Temp</td>
<td>1:10</td>
</tr>
</tbody>
</table>

The procedures the HCP must follow varies depending on the Health Delivery Organization (HDO). A commonly followed procedure requires the HCP to visit the patient every four hours to take patient vitals (HR, RR, BT, BP) and conduct pain assessments. The results of these are either:
• Manually written down (Nursing Note)

• Manually entered to the EHR (Medical Note)

• Automatically entered to the EHR (Medical Note)

2.2 Motivation for Automated Medical Charting

Medical Charting activities is widely viewed as a misuse of time, as it takes time away from the HCP’s ability to tend to their patients and devote time towards deep thinking of the actual treatment strategy. Therefore, several alternative solutions for centralizing and streamlining patient data collection have been proposed to reduce the time for HCP’s in performing medical charting. We show a generalized summary of such alternative solutions in Table 2.2.

All such alternatives conceptualize to leverage the increasingly widespread availability of connected medical devices and proliferation of the Internet of Things and 5G communication abilities. The growth of connected devices in the healthcare industry is rapidly increasing, with the average hospital room containing 15-20 connected medical devices. After including personal devices (i.e., smart-phones, tablets, laptops), a large hospital could have up to 85,000 connected devices on its network [9]. These devices all play an essential role in improving operational efficiency while maintaining a high level of patient care.

This gives credence to the broad idea that these emerging advancements in advanced communication enabled hardware components will allow the possibility of performing medical charting with minimal manual intervention of HCPs. This envisioned broad idea is what we term as a 'Remote Charting System'. Such a 'Remote Charting System' would automatically sense and monitor vital signs of various patients distributed across the hospital, and then disseminate this medical sensory information via an intermediate access network and deposit it in a centralized Electronic Health Record Database in a format that is at least equal or better than a manual HCPs data collection. Doctors, nurses, and technicians can use such collected data at the EHR database to provide better healthcare outcomes and optimal use of the time for all HCPs involved.

While the idea of a remote charting system is exciting at its outset, the apparent criticism by both technology experts and prospective patients is the threat of trusting a digital and automated system for
collecting the correct data and from the correct patients. The problem of guaranteeing a reasonable and trustworthy remote charting system is over-complicated by several regulatory, compliance, and workflow constraints, which makes the positioning of security research in remote charting systems fundamentally different from traditional sensor networks and IoT systems.

Solutions for entering data into the EHR can be grouped into four methods, and each present different challenges, which are explained in more detail in section 2.5.

Table 2.2: Patient Data Collection Methods

<table>
<thead>
<tr>
<th>Item #</th>
<th>Method for Entering into the EHR</th>
<th>Requires remote user access to EHR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Manually Written Nurse Notes</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Manually Entered into EHR with Room Based Device</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Manually Entered into EHR with Mobile Device</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Automatically Entered into EHR with Room Based Device</td>
<td>No</td>
</tr>
</tbody>
</table>

Method 1
The HCP writes down the patient’s data in a Nursing Note (e.g. piece of paper) and enters the data into the EHR at a later time using a computer that’s not physically located in the patient’s room.

Method 2
HCP enters the patient’s data into the EHR using a room based device (e.g. laptop) that’s located in the room. This requires in-room user access to the EHR.

Method 3
HCP uses a mobile device (e.g. smart phone) to enter the patient’s data into the EHR. This requires mobile user access to the EHR.

Method 4
For this method the patient’s data is automatically collected by a room based device (e.g. computer, other device) and entered into to the EHR, without any action by the HCP.
2.3 Remote Charting versus Competing Automated Solutions

As mentioned in method 4 of Table 2.2, some solutions are available for automatically collecting patient data. These solutions are often referred to as health "telemetry" units and are typically only applied to higher acuity patients. These systems typically consist of a Central Station and either a bedside monitor or mobile patient monitor. The patient data is collected by sensors connected to a bedside or mobile monitor. The monitors collect the data and wirelessly transmit it to the Central Station, where the data is reviewed by the HCP and entered into the EMR. These systems are closed and typically manufactured by a single MDM, which drives up cost since the HDO will not be able to source different pieces of the system from multiple MDMs. This also creates the problem of vendor lock-in and may create market monopolies.

While these systems are widely used, they are not designed for a Remote Charting application. Telemetry units are designed to provide real-time data on a patient because of the severity of their condition. While real-time data is necessary for higher acuity patients, it is unnecessary for other patients with lower acuity levels. The real-time requirement of these health telemetry systems increases their complexity and cost. The main benefit of a Remote Charting application is decreasing the amount of time an HCP spends each shift collecting patient data. In the lower acuity levels, the data does not need to be collected in real-time. Thus using an existing Telemetry solution would be overkill and an unnecessary expense for the HDO.

Other issues besides cost arise when using an existing Telemetry system for a Remote Charting application. Systems that use a bedside monitor for collecting the patient’s data require the room to be specifically designed to support the Telemetry system. This implies that there are specific rooms or wards that a patient must be treated. Therefore, if a patient’s condition worsens, they must be transported to a room equipped with a bedside monitor. A workaround for this is implementing a system that uses mobile patient monitors that can be easily transferred from patient to patient. However, this requires the data collected by the monitor to be directly associated with the patient. This presents a potential regulatory violation if patient identifiable information is used to associate the patient to the monitor. Furthermore, if the system requires the HCP to link the two manually, additional risks of human error (i.e., system integrity) arise. For example, a system that requires the HCP to scan a barcode located on
the wrist of a patient. This is done to pair the patient to the data produced by a specific sensor. If the HCP forgets to do this, the data produced by that sensor could be linked to the wrong patient, which can create disastrous health care outcomes.

While existing solutions exist, they are not viable for use in a Medical Charting application because medical charting requires to be (i) more generally applicable to patients of all acuity levels (ii) affordable by their cost (iii) enable a portable solution that allows multiple MDMs to participate, which will decrease cost and potential risks.

2.4 Security View of the Connected Medical Device Spectrum

For heterogeneous connected networks such as remote charting systems and smart connected health in general, a method for grouping various devices is required when attempting to conceptualize the security vulnerabilities presented by this wide variety of connected medical devices. We visualize the following grouping categories of these devices:

- **Device Mobility** - Stationary, Mobile

- **Resource Availability** - Non-Embedded, Embedded

- **Attack Vector** - Adjacent, Local, Physical

- **Security Impact** - Confidentiality, Integrity, Availability

Device Mobility: refers to the device’s ability to be moved from one place to the next. Specific medical devices are not designed to be mobile while others are designed to move from room to room or patient to patient.

Resource Availability: represents the computing resources of the device. This paper loosely defines an Embedded device as one that runs on application-specific hardware and its resources constrained in terms of CPU speed, memory, or user interface. An embedded device will also run using a bare-metal program, embedded OS (real-time/non-real-time), or extremely customized OS. Devices that use generic hardware or run a generic desktop are termed as a non-embedded device. A hospital bed is an example of an
embedded device, whereas a desktop PC that runs Windows is a non-embedded device.

**Attack Vector:** as recommended in the CVSS v3.0 framework [13] is a metric to reflect the context in which a vulnerability exploitation is possible. The metric value depends on how remote (logically, and/or physically) an attacker can be, to use an exploit on that device. Intuitively, it can be therefore concluded that the number of potential attackers of a connected/networked device is more substantial than a device that requires physical access to interact [13]. A summary of these metrics is provided in Table 2.3.

**Security Impact:** refers to the CVSS v3.0 framework’s CIA model of Confidentially, Integrity, and Availability. Where each is defined below:

- **Confidentiality** - Refers to limiting information access and disclosure and system access to only authorized users, as well as preventing access by, or disclosure to, unauthorized parties [13].

- **Integrity** - Refers to the trustworthiness and veracity of information [13].

- **Availability** - Availability refers to the accessibility of information resources [13].

Overtime the CIA triad, has been expanded to include keywords such as authentication, authorization, access control, and non-repudiation, all of which can be indirectly derived from the main CIA triad.
<table>
<thead>
<tr>
<th>Metric Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network (N)</td>
<td>A vulnerability exploitable with network access means the vulnerable component is bound to the network stack and the attacker’s path is through OSI layer 3 (the network layer). Such a vulnerability is often termed &quot;remotely exploitable&quot; and can be thought of as an attack being exploitable one or more network hops away (e.g. across layer 3 boundaries from routers). An example of a network attack is an attacker causing a denial of service (DoS) by sending a specially crafted TCP packet from across the public Internet (e.g. CVE-2004-0230)</td>
</tr>
<tr>
<td>Adjacent (A)</td>
<td>A vulnerability exploitable with adjacent network access means the vulnerable component is bound to the network stack, however the attack is limited to the same shared physical (e.g. Bluetooth, IEEE 802.11), or logical (e.g. local IP subnet) network, and cannot be performed across an OSI layer 3 boundary (e.g. a router). An example of an Adjacent attack would be an ARP (IPv4) or neighbor discovery (IPv6) flood leading to a denial of service on the local LAN segment. See also CVE-2013-6014.</td>
</tr>
<tr>
<td>Local (L)</td>
<td>A vulnerability exploitable with Local access means that the vulnerable component is not bound to the network stack, and the attacker’s path is via read/write/execute capabilities. In some cases, the attacker may be logged in locally in order to exploit the vulnerability, otherwise, she may rely on User Interaction to execute a malicious file.</td>
</tr>
<tr>
<td>Physical (P)</td>
<td>A vulnerability exploitable with Physical access requires the attacker to physically touch or manipulate the vulnerable component. Physical interaction may be brief (e.g. evil maid attack) or persistent. An example of such an attack is a cold boot attack which allows an attacker to access to disk encryption keys after gaining physical access to the system, or peripheral attacks such as Firewire/USB Direct Memory Access attacks.</td>
</tr>
</tbody>
</table>
2.5 Challenges Unique to the Clinical Setting

When attempting to create a secure Remote Charting application, several challenges are unique to a clinical setting. This section explains some of these challenges that impact both the health delivery organizations (HDOs) and medical device manufacturers (MDMs). Such challenges can be broadly divided into two broad categories: (i) regulatory and compliance constraints (ii) Clinical Workflow Constraints.

2.5.1 Regulatory and Compliance Issues

One challenge is that the HDO's and MDMs must adhere to the regulatory and compliance standards imposed by the concerned government of the nation where the HDO is located. These standards come from both local and federal governments. For HDOs that operate in several locations, it can be challenging to enforce global policies that adhere to each of the local government standards. Similarly, for MDMs, it can be tough to design a product that can be used anywhere in the world, as the standards vary dramatically in different countries.

Further complications come when considering liability assignment. As an example, let us consider standards that are relevant to the United States (US). In the US, the Health Insurance Portability and Accountability Act (HIPPA) and the Food Drug Administration (FDA) are relevant when discussing medical devices and the data they produce, consume, or exchange.

HIPPA sets a national standard aimed to protect medical records and other personal health information. HIPPA defines protected health information (PHI) as health information that identifies an individual and must be maintained/exchanged electronically or in a hard copy. Determining what information is considered personally identifiable information (PII) is a common area of confusion and misinterpretation that challenges both HDOs and MDMs. PHI includes information that can be used in a medical context that identify patients, examples include the following attributes:

- Name
- Address
- Birthday
- Credit Card Numbers
• Driver’s License

• Medical records

Additionally, patient ID and name mappings are also considered as private since knowing a patient ID or device ID can be traced back to a unique patient. The FDA provides guidance for the HDOs and MDMs to follow. Regarding cybersecurity, the FDA suggests a shared responsibility model. The FDA provides the following guidance:

• Medical device manufacturers (MDMs) are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity [3].

• Health care delivery organizations (HDOs) should evaluate network security and protect their hospital systems [3].

• Both MDMs and HDOs are responsible for putting appropriate mitigation in place to address patient safety risks and ensure proper device performance [3].

Both the FDA and HIPPA aim to protect the patient and their information. However, it is often challenging for HDOs and MDMs to navigate the guidelines and laws established by both. Determining what information is PHI and who is responsible for securing it is a challenge that is unique to the location of the HDO and each medical device.

When comparing these standards and governance with other countries, it can be easily seen how drastic the differences are from country to country. For example, the EU’s General Data Protection Regulation (GDPR) is much stricter about privacy compared to the US’s HIPPA guidelines, making it difficult for MDMs to manufacture a global product.

### 2.5.2 Clinical Workflow Constraints

Another challenge that arises when designing a Remote Charting application is the clinical workflow of a typical HCP. As previously stated in Section 2.1, the HCP is responsible for several patients at a given point in time; therefore, operational efficiency is of great importance. The tools (i.e., medical devices) used by the HCP must be intuitive and not harm their daily workflow. To further complicate
things, tools are shared throughout the hospital and moved from patient to patient. Therefore, an ideal Remote Charting solution must support mobile devices’ use and be quick to install on a new patient. This also indicates that device and patient mappings are less useful even if not considered for PHI violation. Instead, the more critical challenge is to trust that the correct device is on the intended patient at any point in time.

Referring to the possible solutions outlined in Table 2.2, it is essential to note the tradeoffs for each potential solution approaches. For method 1, where the HCP is manually taking written notes, the HCP must be careful not to write any PII along with the patient’s health data. If both are present, this would be considered PHI and be subject to the rules laid out by HIPPA. This is of great concern to the HDO as there is a high probability of a HIPPA violation occurring from the notes being accidentally viewed by an unauthorized individual. The HCP can avoid writing any PII on their notes, but they are then responsible for remembering which data is associated with which patient, which introduces another issue as the data put into the EHR could be incorrect and affect the patient’s treatment.

In both methods 2 and 3, the HCP manually enters records into a device. The difference is that for method 2, the device is physically fixed to the room (i.e., desktop computer), and in method 3, the device is mobile (i.e., laptop on wheels). For both methods, the probability of data being incorrectly entered into the EHR is decreased since the HCP can enter it immediately. However, unauthorized access to the EHR is still a concern for both.

For method 4, a patient is equipped with a device that monitors the various sensors and automatically enters the data into the EHR. This automatic logging is the ideal solution out of the four, as it removes the possibility of data entry errors and does not require user access to the EHR. However, for this to work, the device must be networked with the EHR in some manner, which is commonly done wirelessly since the device needs to be moved from patient to patient. A method for associating the collected data with a patient is required. Depending on the implementation, the device may contain PHI, which would increase the risk of a HIPPA violation for the HDO.
Chapter 3

Proposed Architecture of Remote Charting Application

This chapter provides an overview of the Connected Medical Device Spectrum, which consists of several networks, actors, and devices. This spectrum is illustrated in Figure 3.1, along with each device’s CVSS metrics. Each component of the spectrum is explained in detail before providing a narrowed view of the spectrum of the components required for the proposed Remote Charting architecture. This chapter concludes with an explanation of the Authorization and Authentication challenges faced by implementing a Remote Charting system. The current solutions for these problems are discussed to illustrate the need for new solutions that meet the requirements of a Remote Charting application.

3.1 Building Blocks of Remote Charting System

The Connected Medical Device Spectrum consists of various subnets, device classes, actors, and types of network communication technologies used, and applications that run on top of the architecture. Below we enumerate each of these aspects sequentially.

3.1.1 Network Segmentation

There are three networks that devices can connect to:
• Bed Bay Network (BBN)

• Room Area Network (RAN)

• Hospital Local Area Network (H-LAN)

3.1.1.1 Bed Bay Network (BBN)

Bed Bay Network (BBN) is a new network proposed in this thesis. We conceptualize this as a decentralized proximity based network for embedded medical devices headed by a Bed Bay Device. The BBN is specific to a particular bed bay found in various rooms in a hospital ward. Depending on the ward, there may be one or more bed bays (and hence BBNs) in any hospital room. Each bed bay holds a single patient for treatments and consists of one bed.

As stated earlier, the BBN consists of a Bed Bay Device that is an edge-device that regulates the connectivity with embedded medical sensors (e.g., heart rate monitors, blood pressure monitors, etc.), actuators (e.g., IV Pole, hand sanitizers), and RFID devices (RTLS badges), and also collects information from such embedded devices.

The proposed Bed Bay Device edge device acts as a decentralized authority for the BBN and should only allow medical devices that are within that BBN to join its network, to maintain the required medical workflow accuracy and integrity. It is capable of communicating with various medical devices and relaying their information back to an application server. The Bed Bay Device is also capable of determining the location of the connected devices.

The Bed Bay Device device has a wired backhaul connection that connects it directly to the nurse call server, this allows the patient to communicate to the HCP. Furthermore, the Bed Bay Device also has a wireless backhaul to a Hospital Wi-fi Access Point that allows communication with the application server.

3.1.1.2 Room Area Network (RAN)

The Room Area Network (RAN) is a room based network for medical devices that do not require direct access to the Hospital LAN.

Commonly found in operating rooms or areas where there is only a single patient, the RAN allows
medical devices to communicate with low latency. A Room Based Device heads the RAN and acts as a gateway to the Hospital LAN. The Room Based Device plays a similar role as the Bed Bay Device does in the BBN. The main difference between a RAN and a BBN is that there can be multiple BBNs for a given room, while there is only one RAN per room.

3.1.1.3 Hospital LAN

The Hospital LAN consists of both medical and non-medical devices. The Hospital LAN allows various actors (doctors, nurses, hospital IT professional, MDM administrator) to interact with remote medical devices and provides access to the internet. Typically the Hospital LAN is available throughout the hospital. However, some hospitals implement separate LANs for a particular ward.

The architecture for the hospital LAN typically consists of multiple servers running various clinical and device management applications. The network consists of wired (Ethernet) devices and multiple access points that allows wireless (Wi-Fi) devices to join the network.

3.1.2 Device Classes

Networked devices in a hospital can be broken down into two classes: Stationary Medical Devices and Mobile Medical Devices.

3.1.2.1 Stationary Medical Devices

Stationary Medical Devices are medical devices that are installed in a particular room and not mobile. Example of this class of devices are Surgical Booms, Monitors, Knee Robots, and Cameras. These are most commonly found in Operating Rooms but some may exist in Acute Care Rooms.

3.1.2.2 Mobile Medical Devices

Mobile Medical Devices are medical devices that are designed to move throughout the hospital. This class includes devices that are attached to the patient for monitoring (e.g. sensors) and treatment (e.g. bed, IV Pole). Additionally, this class also includes devices that are used for entering data into the EMR (e.g. PC on wheels) and devices that help HDO’s in implementing various protocols (e.g. hand sanitizer).
3.1.3  Actors

Several actors exist in the Connect Medical Device spectrum with three different levels of access: Privileged, Normal, and Security Users. Privileged users have full access to either the Device Clinical App, Device Configuration, or Device Server App. Normal users can use the Clinical App to perform actions sanctioned by the HDO’s internal protocols. Security Users are able to configure the Device Server App to adhere to the HDO’s security and network policies.

3.1.3.1  Patients

Patients do not use the medical devices but are the subjects which the medical devices are used upon.

3.1.3.2  Surgeons and Doctors:

Surgeons and Doctors are Privileged users that allow them to assign treatments for a patient and view their EMR data.

3.1.3.3  Nurses

Nurses are Normal users which allow them to view EMR data and assign devices needed to implement the treatments determined by Privileged Users (Surgeons and Doctors).

3.1.3.4  Hospital IT Security Professional

Hospital IT Security Professionals are employees of the HDO that have a Security User access. These individuals are responsible for configuring the Device Server App to meet the security and network policies of the HDO. These users do not have access to the Device Clinical App and therefore cannot access any information in the EMR.

3.1.3.5  MDM Service Administrator

Medical Device Manufacturer (MDM) Service Administrators are Privileged Users that allow them full access to the medical devices, Device Configuration, and Device Server App. This level of access is required for the initial installation of the devices and for troubleshooting issues in the field. It is
important to note that the MDM Service Administrator does not have access to the Device Clinical App, thus avoiding any concern of HIPPA violations.

3.1.4 Types of Network Connection

Devices can communicate to each other over four different mediums: Public Wi-Fi, Private Wi-Fi, Bluetooth, and Wired.

3.1.4.1 Public Wi-Fi

The Public Wi-Fi allows medical devices and HCP’s to wirelessly connect to the hospital’s LAN. This network is not open to patient or visitor’s devices.

3.1.4.2 Private Wi-Fi

Medical Devices that need to run on a Room Area Network, the Private Wi-Fi is used. This medium allows devices in a specific room to communicate to each other but is isolated from the Hospital LAN. Only medical devices in the same room run on this network.

3.1.4.3 Bluetooth

To implement a more localized network that is required for the Bed Bay Network, usage of the Bluetooth protocol is proposed. On this network only mobile medical devices in a particular hospital bed bay may join.

3.1.4.4 Wired

For safety critical operations a wired connection is used. This connection allows a direct line to the Device Clinical App. An example of a safety critical operation is the Nurse Call functionality, where a patient can press a physical button to get the attention of an HCP.

3.1.5 Server Applications

Running on servers on the Hospital LANs are three software applications: Device Clinical App, Device Server App, and Device Configuration.
3.1.5.1 Device Clinical App

The Device Clinical App allows access for HCP’s to view the EMR and assign treatment protocols for a particular patient. This application is managed by the HDO and communicates with the Device Server App to authorize use of a specific medical device for a particular patient. In addition, the Device Clinical App has a wired connection with the Nurse Call Server for implementing safety critical operations (i.e. nurse call).

3.1.5.2 Device Server App

Also running on the Hospital LAN is the Device Server App, which is used to configure network policies and perform server side logic explained in Chapter 5.3. The Device Server App is developed by a Medical Device Manufacturer but is configured by the HDO to meet adhere to their network policies.

3.1.5.3 Device Configuration

The Device Configuration application is used for the initial setup and configuration of the networked medical devices. This is done by service administrators of the various MDMs that have devices on the network.

3.1.6 Remote Charting Architecture

Referring to the Connected Medical Device Spectrum illustrated in Figure 3.1, it is clear that several areas that will undoubtedly be challenging to secure. The Figure 3.1, is depicted in a way such that it combines all the metrics mandated by the CVSS framework, and indicates which devices and communication links are grouped into what category of threats and the severity level according to the CVSS.

The illustration shown below in Figure 3.1 is a broad summary of connected medical devices that are typically found on an HDO’s network. Recognizing that this is not a comprehensive list of devices, it illustrates a standard HDO network.

To better understand how the various components of the spectrum are used, let us consider some example workflows:
3.1.6.1 Operating Room Workflow

In an Operating Room environment the HCP will utilize several wirelessly connected components to treat the patient. The configuration of a surgical boom is unique to the current task on hand. The location of the various devices on the surgical boom (i.e. lighting, monitors, etc..) must be configured to match the heights of the HCP’s operating on the patient. These configurations can be configured over wireless, prior to the beginning of operation to speed up the process.

In some scenarios, a camera and monitor are required to complete the operation. These devices can be wirelessly connected to provide greater flexibility in their use. Furthermore, some procedures benefit from the use of robotics (e.g. knee robot) to assist the surgeon in the operation. These machines must be configured for each operation, often by a remotely connected computer.

3.1.6.2 Acute Care Workflow

For a Acute Care environment let us consider the remote charting workflows that a HCP can use. As discussed in Section 2.5.2, there are three methods for collecting patients data and remotely entering the data into the EHR. For Methods 2 and 3, the HCP will collect the patients data using the various medical devices fixated to the patient and manually enter them into the EHR using either a portable laptop or smart phone. For scenarios where Method 4 is used, the medical devices monitoring the patient are wirelessly connected to the EHR via a Bed Bay Device. The patients data is automatically entered into the EHR and the HCP will view the data remotely via a laptop or smart phone.
Figure 3.1: Remote Charting with Security View of Connected Medical Device Spectrum
3.2 Narrowed View of the Remote Charting System

This thesis's area of focus is the authorization of embedded medical devices in the Bed Bay Network (BBN). As shown in Figure 3.2, our focus is this narrowed view of the Remote Charting System, which is the Bed Bay Network. This includes the Bed Bay Devices, the Hospital Bed, and various medical sensors and actuators that need to be authorized.

The only component outside the BBN that is relevant in this narrowed view is the Applications servers. The MDMs install the Application Servers on the Hospital’s LAN. These servers are maintained by the HDO and typically not accessible outside of the Hospital LAN. The software applications (Device Server App, Device Clinical App) running on these application servers are responsible for receiving data collected from the stationary and mobile medical devices and then storing them into the Hospital's Electronic Medical Record (EMR). The Device Server App and the Device Clinical App are used by authorized medical professionals to deliver treatment.

Downstream from the Application Server is the Bed Bay Device, which is fixed to a particular hospital bay and serves as the edge node connecting the mobile medical devices (the Bed, Patient-Specific Devices) to the Application Servers.

A patient will lay on the Hospital Bed with several actuators and sensors attached, referred to as Patient-Specific Devices. These sensors and actuators represent a wide variety of medical devices used to monitor and treat the patient. The network formed between the edge node and mobile devices is referred to as the Bed Bay Network (BBN). All of the mobile medical devices on a BBN are supposed to be belonging to a single patient.
Figure 3.2: Narrowed View of Remote Charting System: Areas of focus are circled
3.3 Need for a Novel Authorization Approach

The most crucial area for the success of such a concept is the interaction between stationary and mobile medical devices. This interaction is where many different medical device types from various manufacturers need to connect to a single edge device (i.e., Bed Bay Device). If this interaction cannot be secured, the Remote Charting concept will struggle to gain broad adoption.

Additionally, the industry is unlikely to accept the automated Remote Charting concept if the proposed security controls add additional overhead, which may negatively impact the HCP’s daily workflow. Finally, if the security framework’s inherent design demands an increase in the medical device manufacturers’ cost and capabilities, it will be a practical problem that will limit the success of the remote charting system.

The above provides the intuition that host-based and hardware-based security solutions are unlikely to scale for this kind of application. Therefore, one needs to establish a security mechanism that minimally affects the clinical workflow latency, is manufacturer-independent and HIPAA compliant, and does not record patient IDs and device mappings.

There are several potential security threats to the whole Remote Charting system. This thesis’s authorization and authentication approach strictly focuses on threats to the interaction point between the edge node (Bed Bay Device) and the mobile medical devices (Bed, Sensors, Actuators).

The two threats that immediately come to mind relate to Authentication and Authorization. These problems are not unique to the Remote Charting application, as any network is tasked with solving these problems.

1. **Authorization Problem**: Verification that a particular Patient-Specific Device is authorized to perform a specific action within the BBN.

2. **Authentication Problem**: Verification of whether the Patient-Specific Device attempting to join the BBN, should be allowed to join the BBN.
3.3.1 Current Authorization Approaches in other IoT Systems

In the Remote Charting Application, the authorization process for a device to join the BBN involves a risky decision made by the Bed Bay Device. This decision aims to authorize network access to devices that are being used on the patient assigned to the bay in which the Bed Bay Device resides. The obvious question is how the Bed Bay Device will know if a device is being used on the patient?

An easy solution would be to have a human in the loop to perform some sort of local manual pairing process, similar to how a user connects their smartphone to a Bluetooth speaker. However, this would negatively impact the HCP’s workflow, thus not a viable option. Without having a human directly assigning the Patient-Specific Devices to the BBN, the only option is to have the Bed Bay Device capable of autonomously differentiating a device that’s in the patient’s bay and thus can be assumed is for that patient.

As discussed in Section 2.5.1, regulatory bodies enforce the protection of Protected Health Information (PHI). The information must contain Personal Identifiable Information (PII) to be classified as PHI. Therefore, a medical device must not contain PII if it wishes to avoid being classified as a device that produces PHI, making it challenging to map a devices ID to a particular patient. Additionally, device IDs are spoofable, and numerous cyberattacks bear evidence of that. Therefore, these point to the fact that we should go for a physics-based approach that follows laws of nature that is not spoofable. One of these approaches is to use the laws of signal propagation in the physical layer. Therefore, we propose the idea of signal based localization and lateration technique for physical layer authentication of device BBN membership.

To achieve this, the Bed Bay Device must wirelessly determine the location of the Patient-Specific Device. The most common techniques for indoor localization are:

- Received Signal Strength [RSS]
- Channel State Information [CSI]
- Fingerprinting/Scene Analysis
- Angle of Arrival [AoA]
- Time of Flight [ToF] or Time of Arrival [ToA]
• Time Difference of Arrival [TDoA]

• Return Time of Flight [RToF]

• Phase of Arrival [PoA]

In [15], the authors explain the advantages and disadvantages of each technique. Considering the Remote Charting application, the techniques that require line of sight are ruled out because the Patient-Specific Device cannot be assumed to have a clear line of sight with the Bed Bay Device. Thus, the techniques of Tof, TDoA, RToF, and PoA are not suitable for this application. The use of RSS can also be ruled out because of its vulnerability to multipath and environmental noise, which is significant in a hospital environment, and make RSS not accurate enough for the application. Fingerprinting would also not be suitable, as the environment inside a hospital room will change daily, even hourly, and require new fingerprinting every time a new device enters the room. The use of CSI and AoA is the only promising techniques for the Remote Charting application. The solution proposed in this paper relies on using these techniques to design a physical layer authorization for joining the BBN.

### 3.3.2 Current Authentication Approaches in IoT Environments

When considering the process of authenticating a device, the device’s identity can be obtained based on either:

1. Something the device **knows** – e.g., a password or encryption key

2. Something the device **possesses** – e.g., a certificate

3. Something the device **is** (static biometric) – e.g., device fingerprint based on electrical-physical characteristics of the hardware

4. Something the device **does** (dynamic biometrics): recognition of unique patterns generated by the device

The use of obtaining the device’s identity by means of something it "knows" or "possesses" is feasible but not practical for a Remote Charting Application. Both of these would require the HDO to work with the MDMs to establish site-specific information stored on the device. Since medical devices are typically
not manufactured for a single site and are often loaned or sold to other hospitals, this would force both parties to change their current processes dramatically. Also, requiring site-specific data to be entered into the device and tracked by the HDO poses additional vulnerabilities.

Determining a device’s identity based on static biometrics is promising, with the current best approach being the use of Physically Unclonable Functions (PUF). However, PUFs have several drawbacks. They present a manufacturability challenge for the MDMs and have been proven to be vulnerable to Machine Learning attacks [2]. Also, the use of PUFs would require a physical challenge to the device each time it attempted to join the BBN; this implies that the Bed Bay Device would have to have a brief physical connection with the device before allowing it to join the network, which would negatively impact the HCP’s daily workflow.

Authentication based on dynamic biometrics is both feasible and viable for a Remote Charting application. Authenticating the type of device by what it does, allows the devices to move freely across different BBN’s and hospitals without any human intervention for re-authentication. However, by observing its actions, determining a medical device’s type presents its own set of technical and security-related challenges. The following sections discuss these challenges in more detail.
Chapter 4

Threat Landscape Development for Remote Charting System

This chapter discusses the vulnerabilities and security threats relevant to the Remote Charting system shown in Figure 3.2. The system’s three main components, Application Server, Bed Bay Device, and Patient-Specific Devices, all present different vulnerabilities and threats. While this paper proposes a framework for securely implementing an entire Remote Charting system, only vulnerabilities and threats related to the proposed BBN is explored. The reason for this narrowed focus is because the BBN is the only new network introduced to the existing Connected Medical Device Spectrum. The operational and architectural aspects of the BBN will be examined for weakness that attackers can potentially exploit. The relevant threat models and attack strategies will also be discussed.

4.1 Architectural Weaknesses

At the heart of the BBN is the Bed Bay Device. This device is tasked with autonomously determining which Patient-Specific Devices are authorized to join the BBN. The Bed Bay Device must have an awareness of its surroundings to achieve this. This will be based on its local observations and external observations received from other Bed Bay Devices, this is discussed in more detail in 5.3. The Bed Bay Device will also require room-specific configurations and network policies that will be used in granting
authorization to the BBN. Where the room configurations will provide the physical layout of the BBN, and the network policies represent the communication and security protocols used to communicate on the Hospital’s wireless network.

![Diagram](image)

**Figure 4.1: Architectural Overview of Bed Bay Device**

The external observations, room-specific configurations, and network policies will be obtained over the hospital’s wireless network. Therefore, if these external inputs are not authenticated and delivered over a secure channel, there are potential weaknesses in the system. Furthermore, since the Bed Bay Device will be physically accessible to attackers, local observations can be potentially manipulated.

Patient-Specific Devices are mobile and transferred from patient to patient. However, they will be attached to a single patient at any given point in time. The mobility and accessibility of these devices presents plenty of opportunities to be compromised by an attacker. Also, the fact that various manufactures will manufacture them means it will be difficult to enforce any device-level security policies.

### 4.2 Operational Weaknesses

The Bed Bay Devices have to decide if a Patient-Specific Device is physically in range of the BBN to determine if the device is authorized to join the BBN, this requires locating the device by observing the data it transmits. As previously stated in 3.3.1, the only viable solution is a physical layer approach that monitors the phase and amplitude of the transmissions. The Bed Bay Device will make local observations that will be compared to network thresholds to determine if a device is within the BBN range. These thresholds are obtained during the installation process via the Network Policies. These thresholds are an
area of potential weakness as if they are too loose, devices that are not physically attached to the patient may be allowed to join the BBN, which would create a safety risk for the patient as their health data will be incorrectly reported. On the other hand, if the thresholds are too tight, legitimate devices may not be granted access, forcing the HCP to intervene manually. To strengthen this decision’s reliability, the Bed Bay Device will collaborate with other Bed Bay Devices and use their observations with the local observations.

In addition to the network thresholds, the Bed Bay Device will also rely on static room-specific configurations to help determine the location of the Patient-Specific Device. The configurations would contain information such as the physical dimensions of which the Bed Bay Device resides and the distances to other Bed Bay Devices. These configurations rely on the system installer to accurately set the configurations during installation, thus are subject to human error and room modifications and renovations.

4.3 Categories of Vulnerabilities

The outcome of an attack on the BBN is the resulting patient’s health data. This data can be incorrectly reported or not reported at all. Therefore, this paper categorizes the vulnerabilities based on the attacker’s motive, when the impact of the attack is felt and the method of the manipulation.

4.3.1 Motives of Attackers

An attacker’s motive influences the methods an attacker is willing to use to launch an attack. Therefore, the motives of the attacker must be discussed. An attackers motive depends on whether or not the attacker will be directly benefited from the outcome of the attack. Therefore, this dissertation uses the commonly used categorizations of Selfish and Malicious Attacks.

- **Selfish Attacks:** In this type of attack, the attacker is directly benefited from the outcome of the attack. The attacker could benefit financially from the overuse of a particular treatment or death of the patient.

- **Malicious Attack:** The attacker’s motive is to impact others negatively, but it has no direct benefit to them. Here the attacker could be attempting to harm a particular HDO or HCP by
manipulating the patient’s data and creating cases for malpractice.

4.3.2 Impact of the Attack

An attack’s effect can have an immediate impact on its victim, or it can have a delayed impact that is not felt until after the attack has already taken place.

- **Immediate Impact:** Attacks that cause an immediate impact are ones that prevent the patient’s data from being reported. These attacks are designed to deny communication between devices on the BBN or restrict the Bed Bay Device to report the collected data.

- **Delayed Impact:** Attacks whose impact is not felt until a later point in time. These attacks could create compliance and regulatory concerns for the HDO after an audit. The patient’s health could also slowly start to decline after a treatment was chosen based on manipulated data that was previously reported.

4.3.3 Method of Manipulation

An attacker has two primary sources of threats for manipulating the patient’s data that is reported by the Bay Device:

- **Manipulating the BBN Authorization Decision:** An attacker can trick the Bed Bay Device into thinking that a particular Patient-Specific Device is within the BBN range. Here, the attacker would be attempting to manipulate the Bed Bay Devices’ observations by generating signals that would disguise the real location of the device.

- **Manipulating the Patient Data:** An attacker can spoof data to make it appear it came from a device that is already on the BBN. Alternatively, an attacker can compromise a Patient-Specific Device to manipulate the data it sends to the Bed Bay Device.

4.4 Attack Strategies

This section discusses some of the common attack strategies relevant to this application. The three categories for attacks are Spoofing, Fabrication, and Denial of Service (Dos).
4.4.1 Spoofing Attacks

Spoofing attacks are when the adversary pretends to be a valid entity without foiling authentication/authorization. For attacking the BBN, an attacker can spoof the location or data of a Patient-Specific Device.

4.4.2 Fabrication Attacks

An attacker wishing to perform a message integrity attack will attempt to fabricate the message in some manner. Most modern communication protocols have protections in place for most methods of message fabrication. The exception being replay attacks. In this attack, an adversary would observe a message sent by a Patient-Specific Device and replay it later. This replay of stale data could pose a serious health threat to the patient if the data makes it is way into the EMR.

4.4.3 DoS Attacks

DoS attacks are easy to detect and impossible to prevent. An attacker can perform a jamming attack preventing a device from successfully communicating with the BBN. An attacker could also flood the BBN with connection requests, thus making it impossible for other devices to join the network.
Chapter 5

Proposed Authorization Framework

In this chapter we will provide an overview of the security framework for the Remote Charting System. In addition the constraints, assumptions, and a discussion on similar approaches in related areas that inspired the development of our framework will be also explained in detail.

5.1 Device and Resource Constraints

When developing a solution for an industrial application, it is important that all realistic domain specific constraints are applied to ensure a practical approach to the solution is produced.

Apart from the privacy policy constraint imposed by HIPAA regulations (as discussed in the previous chapter), there are certain other system level constraints that relate the components of the remote charting system architecture.

- Manufacturer Agnostic:

- Non-proprietary Communication Protocol:

- Light Weight Sensors and Actuators:

Table 5.1 illustrates the devices of the BBN and their constraints.
Table 5.1: **Device Constraints**

<table>
<thead>
<tr>
<th>Device</th>
<th>Resource Constraints</th>
<th>Communication Constraints</th>
<th>Mobility</th>
<th>Manufacturer</th>
<th>Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bed Bay Device</td>
<td>None</td>
<td>None</td>
<td>Fixed</td>
<td>Single</td>
<td>None</td>
</tr>
<tr>
<td>Hospital Bed</td>
<td>None</td>
<td>None</td>
<td>Mobile</td>
<td>Multiple</td>
<td>None</td>
</tr>
<tr>
<td>Sensors + Actuators</td>
<td>Battery + Computation</td>
<td>COTS non-proprietary Protocol</td>
<td>Mobile</td>
<td>Multiple</td>
<td>Security Related Cost &lt;$5</td>
</tr>
</tbody>
</table>

### 5.2 Assumptions

Several assumptions are made about the three attacks called out in Section 5.3.2.

- Device capable of jamming signal of authorized devices
- Adversary can learn frequency hopping schedule of BBN communication protocol
- Adversary can spoof data of authorized device

Since parts of the proposed framework relies on physical layer attributes of a wireless network, it is necessary to assume a physical layout of the BBN. This is shown in Figure 5.1 below.
Figure 5.1: **Layout of a BBN**: \( AP_{x,y} \) represents anchor point \( x \) of BBN \( y \)

Figure 5.1, a typical hospital setting with two separate rooms, each room containing two BBNs. Each BBN is limited to a 3m x 3m rectangle. The Fig. 5.1 indicates that in a typical hospital setting, each BBN with have at least three or more adjacent BBNs. Two of the BBNs are separated by a physical wall, and another is within the same room.
5.3 Framework Definition

The five basic approaches for securing computer systems are Prevent, Deter, Deflect, Detect and Recover. The framework proposed in this paper utilizes the approaches of both Prevention and Detection to protect a Remote Charting application from Integrity related attacks. To prevent unauthorized devices from joining the BBN, the Bed Bay Device will only allow devices that are within the coordinates of a designated BBN to join the network. Once a device has joined the BBN, the system’s primary defense is detection. The system will monitor the device’s behavior to detect if the device has been compromised or if there’s possibility of an ongoing Spoofing, Fabrication, or DoS attack. If the possibility of an attack is present, the system will alert the HCP of the potential attack. Figure 5.2 provides a high-level flowchart of the proposed framework.

As shown in Figure 5.2, the framework consists of two main processes and four additional sub-processes. Each process requires a decision to be made and concludes with a success or a fail event. There are eight methods for approaching the decision making required for each process: Direct, Assisted, Human Based, Group, Human Assisted, Human Group, Assisted Group, and Human Assisted Group Decision Making.

**Direct Decision Making** A device can directly make a decision without receiving knowledge from another source.

**Assisted Decision Making** A device obtains information from a remote device (i.e. server) to aide in the decision making process.

**Human Based Decision Making** Human (i.e. HCP) input is needed for a device to make a decision.

**Group Decision Making** Decision is made by leveraging information received from adjacent devices.

**Human Assisted Decision Making** Information from a remote device and human input are required to make a decision.

**Human Group Decision Making** Decision relies on information received by adjacent devices and human input.

**Assisted Group Decision Making** Information from both adjacent and remote devices are used
by a device to make a decision.

**Human Assisted Group Decision Making** A decision requires input from a human and information gathered from both adjacent and remote devices.
Figure 5.2: Defense Flowchart
5.3.1 Inter BBN - Physical Layer Authorization

The first layer of the proposed defense is to prevent unauthorized devices from joining the BBN. The HCP will manually assign what ‘types’ of patient-specific medical devices are authorized for a particular BBN, and only devices within the proximity of that BBN are authorized to join the BBN network.

This authorization rule will ensure that devices on the BBN are for the correct patient. To achieve this, the Bed Bay Device will use Channel State Information (CSI) to approximate the distance between the requesting medical device and the Bed Bay Device. The CSI measurement approach was chosen over the more commonly used Received Signal Strength (RSS) because of the increase in robustness to multipath effects and indoor noise, which is achieved by capturing both the amplitude and phase response of the radio frequency. The CSI is also suitable for dynamic RF environments where fingerprinting/scene analysis is not practical.

The Bed Bay Device will be equipped with an antenna array. When a new mobile medical device attempts to join the BBN, its location will be determined, and if it falls within the proximity thresholds of the BBN layout, it will be allowed to join the network.

5.3.2 Intra BBN - Physical Layer Anomaly Detection + Device Fingerprinting

Once a device has successfully joined the BBN, it will be continuously monitored for signs of an attack. The Bed Bay Device will again rely on the device’s CSI metrics to perform a physical layer anomaly detection. There are three events that the Bed Bay Device will be looking for, and reliably detecting these events assures that the patient’s data is accurate and has not been compromised by a new attack:

1. Unauthorized Device Placed in BBN area
2. Removal and Replacement of a Patient-Specific Device
3. Rearrangement of a Patient-Specific Device

For scenarios where a device has been compromised before joining the BBN, the framework will rely on device fingerprinting, but this is a module for future work. The data produced by the Patient-Specific
Devices will be passed on to the Application Servers for a detailed analysis before being sent to the Hospital’s EMR. Each type of Patient-Specific Device will produce data in a predictable manner, which allows the system to authenticate the type of Patient-Specific Device. Deviations to the frequency at which the device produces data or contents of the data indicate that a device may be compromised or malfunctioning.

5.3.3 Primer on Channel State Information (CSI) Data

Before discussing the proposed framework in greater detail, a non-proprietary communication technology standard must be chosen, and additional background information is needed for the CSI data used in the decision-making process. This section discusses the aspect, as mentioned above.

Given the device constraints in Table 5.1, the wireless technology chosen to implement the communications within the BBN is the Bluetooth Low Energy (BLE) standard. While BLE satisfies the constraints, the protocol does not have built-in mechanisms to obtain a received signal’s CSI metrics.

However, a recent work proposed [1] proposed a mechanism to generate CSI metrics from BLE transmissions using antenna arrays on the radio receiver. Also, from prior research in Wi-Fi-Sensing, it is well known that more than one receivers are needed for trilateration and triangulation. Therefore, we put forward the idea of additional anchor points, which are radio transceivers equipped with an antenna array, and the Bed Bay Device itself serves as a virtual anchor point, also equipped with an antenna array.

5.3.4 Anchor Points with Antenna Arrays

The framework requires the use of multiple anchor points that help locate devices. Each BBN consists of four anchor points, one of which is the Bed Bay Device, and each anchor point is equipped with an antenna array consisting of at least four antennas. Information received from adjacent BBNs is required for accurately determining which BBN a Patient-Specific Device is authorized to join.

This framework also requires human (i.e., HCP) interaction for some of the decision making. Therefore, it is assumed that the HDO will provide the necessary personnel and implement appropriate protocols. Furthermore, it is also assumed that each Patient-Specific Devices will produce data in a predictable
manner, and no two types of devices can produce the same class of data. This allows the system to authenticate the type of Patient-Specific Device on the BBN. Lastly, the framework restricts the use of multiple Patient-Specific Devices of the same device type on a single BBN, and the Patient-Specific Device enforces a policy that restricts it being connected to a single Bed Bay Device only. The presence of anchor points and antenna arrays do not require any changes in either the HCP workflow or the constraints on the medical device manufacturer.

The system proposed in [1] involves the use of multiple anchor points to estimate the location of a Patient-Specific Device, with each anchor point having multiple antennas. The system architecture is shown below in Figure 5.3. The Patient-Specific Device establishes a BLE connection to a single anchor point, the Bed Bay Device, referred to as the master. The other anchor points within the BBN calculate the CSI by passively observing the packets exchanged between the Patient-Specific Device and the master. Finally, the likelihood distribution of the Patient-Specific Device’s distance and angle is estimated by combining the observed CSI data from all anchor points.

Figure 5.3: **System Architecture of [1]**

To obtain the CSI data, the algorithm in [1] can be summarized into three steps:
5.3.4.1 Step 1: Estimation of the Distribution of Distances via CSI

The estimation of distance is done using CSI observations between transmitter (target) and the receiver (anchor point) measured across multiple frequencies in the BLE band (there are about 40 frequencies available in the BLE band, each of which offers a bandwidth of 2 MHz). This is possible with BLE standard since, in the connected mode, the master and slave BLE devices hop across the 37 non-broadcast channels (out of the 40 total channels) according to a hop schedule $\delta f$.

Suppose there is a total of $K$ frequencies over which this measurement is done. The phase of a channel frequency is a linear function of distance. Thus, by taking the phase information measured across multiple frequencies, the likelihood of the distance between the two devices can be estimated. The likelihood function of distance is given by the following:

$$Pt(d) = \frac{1}{K} \sum_{k=1}^{K} h_k e^{j \frac{2\pi (\delta f) d}{c}}$$

(5.1)

where $c$ is the speed of light, and $h_k$ represents the wireless channel’s amplitude that was measured on the $k$-th frequency, and $d$ is the distance from the target.

From the likelihood distribution, the maximum likelihood estimate of the mean and standard deviation of the inferred distances can be done.

5.3.4.2 Step 2: Estimation of the Distribution of Angles via CSI:

To estimate the direction, typically an Angle-of-Arrival (AoA) approach is used [1], where the channel measurements are taken at each $i$ of the $N$ antennas on the deployed at each anchor points. By knowing the gap between each antenna ($l$), the likelihood estimate of the signal originating from an angle $\theta$ can then be calculated. The likelihood estimates of the phase angle include mean and standard deviation of the phase angle.

$$Pt(\theta) = \frac{1}{N} \sum_{i=1}^{N} h_i e^{j \frac{2\pi l \sin \theta}{\lambda}}$$

(5.2)

where $\theta$ is the angle between the antenna and the target, $\lambda$ is the signal wavelength.

The two likelihoods can then be combined to give an estimate that the likelihood that a signal
originated from a distance \( d \) and angle \( \theta \): where \( P \) is the total number of paths, and \( i \) is the number of antennas.

\[
P(d, \theta) = \left| \sum_{j=1}^{J} h_{jk} e^{\frac{2\pi i j \sin \theta f_0}{c}} e^{\frac{2\pi i k d}{c}} \right|
\]

(5.3)

where \( c \) is the speed of light, and \( h_{jk} \) represents the wireless channel that was measured on antenna \( j \) and frequency \( k \). For more details see [1].

### 5.3.4.3 Step 3 - Accounting for phase offsets

The BLE protocol does not enforce synchronization between two connected devices. As a result, the experiments done in [1] pointed out that the captured channel measurements need to account for phase offsets, which are a byproduct of the connected devices not being synchronized.

Each anchor point takes measurements of the observed bi-directional communication between the master (leader) localization device and target Patient-Specific Device. A corrected channel measurement can be calculated and used for locating the Patient-Specific Device by combining these measurements.

These corrected channels can then be put into geometric form to replace the channel measurements of 5.3. This produces a new likelihood estimation (5.4), that is free of phase offsets. The likelihood is then calculated for each anchor and added together to produce a joint likelihood of the signals originating from any point.

\[
P_i(d_{ij}^T - d_{i0}^T, \theta) = \left| \sum_{j=1}^{J} \sum_{k=1}^{K} a_{ij} e^{\frac{2\pi i j k}{c}} (d_{ij}^T - d_{i0}^T - d_{i0}^T e^{\frac{2\pi i j \sin \theta f}{c}}) \right|
\]

(5.4)

where \( P_i \) is likelihood of the \( i \) – th anchor, \( d_{ij}^T \) is the distance from the tag to anchor \( i \) antenna \( j \), and \( f \) is the BLE channel frequency. The fixed distance between an anchor \( i \) and the master anchor \( 0 \) is measured during installation and is represented by \( d_{i0}^T \).
5.4 Similar Work

Several of the concepts used in this paper were obtained from other work. While these were not geared toward the same clinical application, their concepts can still be applied to a Remote Charting application. The framework proposed in this paper relies heavily on the use of physical layer attributes for data and system integrity. This concept was also used in [12]. Another concept, obtained from [6], is majority voting. Majority voting is used in 6.1 to reliably decide if a device is authorized to join a BBN.

The authors in [12] propose a data trust framework used by vehicular ad-hoc networks (VANETs) for false data detection and secure vehicle tracking. The proposed approach uses information from a wireless physical layer to verify reported data from another vehicle, where the physical layer attributes of AoA and Doppler Speed are used to verify if a car’s reported actions match its physical actions. These physical layer attributes allow the framework to detect false data without an honest majority from neighboring vehicles. In this paper, wireless physical layer observations are used for system integrity in 6 and data integrity in 7.

In [6], three binary voting algorithms are evaluated for their effectiveness in terms of reliability and security. One of the three algorithms evaluated is a simple Majority Rule algorithm, where all $N$ voters
carry the same weight, and a decision is made when there is one more vote than $N/2$ voters. The authors note that this algorithm achieves high reliability but provides a low level of security benefits. This is sufficient for using the Majority Rule algorithm in 6.1, where a reliable method of detecting a device within the range of a particular BBN is required.
Chapter 6

Process for Inter BBN Authorization

The first process in the proposed framework involves deciding whether or not a device is authorized to join a particular BBN. The Application Server makes the final decision through a Human Group Decision Making approach. This decision requires CSI data of the Patient-Specific Device attempting to join the BBN and for the HCP to manually assign the authorized device type, with the latter ensuring only patient data that has been authorized is collected.

The Inter BBN Authorization process can be broken down into two sub-processes and one decision:

1. Group Physical Layer Authorization

2. Human Assisted Device Assignment

3. Authorization Decision

The first step of this authorization process is to determine if the prospective Patient-Specific Device is within the BBN’s proximity thresholds. Once successfully physically authorized, the Bed Bay Device will communicate to the Application Server to determine if the prospect device’s type has been assigned (i.e., authorized) to this BBN.

The location estimate \([\text{LOC}_i(D_{\text{new}})]\) is used by the BBN to cast it’s vote. However, the location estimate may contain errors and can lead to an incorrect decision (i.e. vote) being made, this is discussed in more detail in Sections 6.1.2 and 6.1.4.

Due to the nature at which RF signals propagate, it cannot be assumed that the Bed Bay Device with
the strongest $RSS_i$ is the correct BBN. Therefore further checks are mandated and described below.

Due to possible localization errors, the Bed Bay Devices will perform a binary majority voting technique to finalize which BBN the prospect device is authorized to join. At this time, it is necessary to note that once a connection is established, the CSI data used to locate a device is done at each Bed Bay Device independently. Each BBN consists of a Bed Bay Device and multiple anchor points, and since the Bed Bay Devices can communicate, each BBN can generate its own localization estimates.

6.1 Group Physical Layer Authorization

This section will first give a detailed description of the Group Layer Authorization process before providing a thorough explanation of the proposed Hypothesis testing and voting mechanism.

6.1.1 Process Steps

As shown in 6.1, there are eight steps of the Group Physical Layer Authorization process:
Figure 6.1: **Group Physical Layer Authorization Process**: when $BBN_1, \ldots, BBN_4$ detected the prospect device $D_{new}$

### 6.1.1.1 STEP 0: Initialization:

Prior to the authorization process being used, the system must be configured with the correct system thresholds based on the hospital’s needs, this is explained in more detail in Section 6.1.2.6. Furthermore, a proximity threshold must be calculated for determining if a device is inside or outside a particular
BBN, which is explained in Section 6.1.3.

6.1.1.2 STEP 1: Join Request:

The process of authorization starts with a sequence of joining requests from a new candidate Patient-Specific Device \( D_{\text{new}} \) that is broadcast over the mandated Bluetooth BLE frequencies, to which all radio receivers on multiple Bed Bay Devices are tuned into by default.

6.1.1.3 STEP 2: RSS Sharing:

Let \( RSS_i(D_{\text{new}}) \) be the received signal strength of the join request calculated at each Bed Bay Device \( i \). The \( RSS_i(D_{\text{new}}) \) is made available to the \( i \)-th BBN directly by the underlying BLE protocol. The Bed Bay Devices share their \( RSS_i(D_{\text{new}}) \) with each other through the hospital’s LAN.

6.1.1.4 STEP 3: Leader Election:

The Bed Bay Device with the highest \( RSS_i(D_{\text{new}}) \) becomes the ‘leader’ Bed Bay Device (denoted by \( BBN-P \)) which initiates the authorization process, with the cooperation of its neighboring (adjacent) set of ‘follower’ Bed Bay Devices (denoted by \( BBN-A_i \)). To conclude, the Bed Bay Device with the strongest received signal strength will establish an initial but temporary connection with the new device to start the process of physical layer authorization. Due to the nature at which RF signals propagate, it cannot be assumed that the Bed Bay Device with the strongest \( RSS_i \) is the correct BBN, therefore further checks are mandated and described in proceeding steps.

\[
RSS_{\text{max}} = \max(RSS_1, \ldots, RSS_i, \ldots, RSS_{\eta(A)}) \Rightarrow BBN_{\text{max}} = BBN - P \tag{6.1}
\]

where \( \eta(A) \) is the number of adjacent BBNs, \( i \in \{1, \eta(A)\} \)

6.1.1.5 STEP 4: Likelihood Estimation via CSI:

After a connection is established, the \( BBN-P \) and each \( BBN-A_i \) will start gathering the CSI \( [\text{CSI}(D_{\text{new}})] \) on that connection. Based on the gathered CSI, the distances are estimated. Based on the likelihood distribution in Eqn 5.4, the maximum likelihood estimate of the mean and standard deviation of the distance distribution can be estimated.
6.1.1.6 STEP 5: Hypothesis Testing for Deciding BBN Membership:

After a distribution of distances have been collected, we propose a hypothesis testing based approach for authorizing a BBN membership or not for each Bed Bay Device (that includes $BBN - P$ and its immediate neighbors). What this step answers is if the target ($D_{new}$) is inside or outside a particular BBN.

6.1.1.7 STEP 6: BBN Membership Voting:

Once each Bed Bay Device decides the membership, each $BBN - A_i$ will send their vote [$V_i$] of whether or not $D_{new}$ belongs to their network, to the $BBN - P$. The vote $V_i$ is the outcome of the hypothesis testing module. A vote of $V_i = 1$ represents the belief that $D_{new}$ belongs to $BBN_i$, while $V_i = 0$ represents the belief that it is not inside $BBN_i$. The $BBN - P$ will tally the votes received from each $BBN - A_i$, along with its own vote to form a location consensus.

6.1.1.8 Step 7: Location Consensus

For a consensus to be reached, the result of the vote tallying ($V_i$) must be 0 or 1.

$$V_{final} = V_P + \sum_{i=1}^{\eta(A)} V_i$$  \hspace{1cm} (6.2)

When $V_{final} = 0$, the prospect device ($D_{new}$) is not within range of any BBN and therefore is not granted authorization, and the process moves to Step 8.

When $V_{final} > 1$, it means that multiple BBN’s have voted that $D_{new}$ should join their network, an alert (audible or visual) is provided by the corresponding Bed Bay Devices ($BBN_i$) that voted $V_i = 1$. This alert informs the HCP/patient that $D_{new}$ needs to be moved closer to the Bed Bay Device. After allowing some time for $D_{new}$ to be re-positioned, the authorization process starts over at Step 1.

When $V_{final} = 1$ and $V_P = 0$, the $D_{new}$ that is temporarily connected to $BBN - P$ should actually be connected to $BBN - A_i$, which voted $V_i = 1$. To achieve this, the connection is terminated with $BBN - P$, and using the hospital LAN, $BBN - P$ notifies the correct $BBN - A_i$ to allow accepting $D_{new}$ to its BBN.

When $V_{final} = 1$ and $V_P = 1$, it implies that $D_{new}$ is within range of $BBN - P$, and a location consensus has been made with all $BBN - A_i$ deciding that it is not in their BBN. The $D_{new}$ is then
determined to be physically authorized for BBN-P.

6.1.1.9 Step 8: Report

The final step is to report when a prospect device is granted physical authorization. The Bed Bay Device of BBN-P is responsible for reporting the successful authorization event to the Application Server. Only successful authorizations need to be reported. The device type, which is communicated by $D_{\text{new}}$, will be included in this event message. Since final authorization is dependent on device assignment, the Bed Bay Device will wait a pre-configured amount of time. If no final authorization has been received at the end of this time, $D_{\text{new}}$ is removed from the BBN. The Application Server is responsible for sending a final authorization to the Bed Bay Device, which is discussed in more detail in Section 6.3.

6.1.2 Hypothesis Testing

Since the BBN voting (Step 6) relies on the accuracy of the CSI metrics, further discussion on this topic is needed. The Figure 6.3 shows the CDF of error localization. The figure implies that 50\% of the tested positions could have a location error ($L_{\text{err}}$) that is $L_{\text{err}} \leq 86\text{ cm}$. The worst case the error can reach is up to $L_{\text{err}} = 3.5\text{ m}$. Where 60\% of the locations tested show an error of 1m or less.

Given these errors, it is clear that there is a nonzero probability ($P_{\text{err}}$) of two or more BBN’s voting ($V_{\text{final}} > 1$) that $D_{\text{new}}$ should join their network, where $P_{\text{valid}} = 1 - P_{\text{err}}$ represents the probability of the networks reaching a consensus ($V_{\text{final}} \leq 1$). Since the proposed action involves the HCP to intervene when consensus cannot be reached, it is important the probability of this occurring is low. Otherwise, it would become a nuisance and impact the clinical workflow. Two types of localization errors can occur:

1. **False Localization Errors** $P_f$: When a $BBN_i$ votes that a Patient Specific Device is within it’s range but is actually physically located outside the $i$-th BBN.

2. **Missed Localization Errors** $P_m$: When a $BBN-P$ votes that a Patient Specific Device is not within range, when it actually is physically within $BBN-P$.

While having any errors in the voting process is not ideal, it is important to note that both errors must occur for a device to join a BBN that it does not physically reside. This statement can be made because of the Consensus Step 7 of Section 6.1.
In order for a device to join an incorrect BBN, the $BBN-P$ must encounter a missed localization error ($P_m$) while an adjacent BBN ($BBN-A_i$) experiences a false localization error ($P_f$). If both of these errors occur during the voting process, a consensus cannot be reached, and the device ($D_{new}$) will not join a BBN.

To reduce the probability of these errors occurring, this framework proposes a commonly used tactic of Hypothesis Testing [7]. For this scenario, each BBN$_i$ has to decide between two hypotheses:

- $H_0$ (null): decision that $D_{new}$ is not within the BBN
- $H_1$ (alternative): decision that $D_{new}$ is within the BBN

### 6.1.2.1 Decision Variables:

Let the decision variable $z \in (H_0, H_1)$ be the two possibilities of the encoded hypothesis. Similarly, let $y$ be the observation, i.e., the estimated output distance and the target device’s angle to be authenticated from the CSI-based algorithm.

### 6.1.2.2 Observation Variable:

The observation is a distance and angle with some noise. The final location will either appear to be inside or outside the concerned BBN. For simplicity, let us denote the observation as $y$, regardless of whether its distance or angle, since the same decision rule procedure applies, regardless of the physical quantity under observation. For every target device, there will be a $n$ number of observations. Therefore, if $y$ denotes distance, we will have a probability distribution of the distance denoted by $P(y)$, parameterized by some mean and variance.

### 6.1.2.3 Need for a Decision Rule:

However, since any observation is noisy and error-prone, especially in wireless systems, we need a decision rule that maps the observations $y$ into a decision of either choosing the null hypothesis $H_0$ or alternative hypothesis $H_1$. A rational decision rule should offer minimal error between our choice of
hypothesis (decision) and the target device’s actual ground truth status.

6.1.2.4 Decision Outcomes:

There are four different combinations of outcomes that are possible in the decision rule involving binary decisions. We need to quantify each decision outcome’s probabilities and costs associated with each possibility before we design a decision rule.

False Alarm \((D_{10})\): is the outcome where the system erroneously decides that a target device is within the BBN when the device is in fact outside the concerned BBN. The instance of a false alarm is also known as Type I error, and this particular outcome’s \((D_{10})\) incurred cost to the system is quantified by \(C_{10}\).

The probability with which a decision rule makes such an error is quantified by the probability of false alarm denoted by:

\[
P_f = P(\text{decide } H_1 | H_0 \text{ is true})
\]  \(6.3\)

Missed Detection \((D_{01})\): is the outcome where the system erroneously decides that a target device is outside the BBN, when the device is in fact inside the concerned BBN. The instance of a missed detection is also known as Type II error, and this particular outcome’s \((D_{01})\) incurred cost to the system, is quantified by \(C_{01}\).

The probability with which a decision rule makes such an error is quantified by the probability of missed alarm denoted by:

\[
P_m = P(\text{decide } H_0 | H_1 \text{ is true})
\]  \(6.4\)

True Positive Detection \((D_{11})\): is the outcome where the system correctly decides that target device is within the BBN, when the device is in fact inside the BBN, and this particular outcome’s \((D_{11})\) incurred cost to the system, is quantified by \(C_{11}\).

The probability of a true positive detection is quantified by:

\[
P_{tp} = P(\text{decide } H_1 | H_1 \text{ is true}) = 1 - P_m
\]  \(6.5\)
**True Negative Detection** \((D_{00})\): is the outcome where the system correctly decides that the target device is not within the BBN, when the device is in fact outside the BBN, and this particular outcome’s \((D_{00})\) incurred cost to the system, is quantified by \(C_{00}\).

The probability of true negative detection is quantified by:

\[
P_{tn} = P(\text{decide} H_0 | H_0 \text{ is true}) = 1 - P_f
\]

\((6.6)\)  

### 6.1.2.5 Hypothesis Testing Decision Rule:

The goal of the hypothesis decision is to minimize the expected risk of the \(i\)-th BBN, denoted by \((E_i)\), and is calculated by the following:

\[
\min(E_i) = C_{00} \cdot P_{tn} + C_{01} \cdot P_{m} + C_{10} \cdot P_{f} + C_{11} \cdot P_{tp}
\]

\((6.7)\)  

Following the theory of binary hypothesis testing rule for the continuous random variables, the method for minimizing the risk of a BBN incorrectly deciding the BBN membership of the device, the Eqn. 6.7 is equivalent to the following decision rule:

\[
\frac{P(y|H_0)}{P(y|H_1)} > H_0 \left( \frac{P_1}{P_0} \right) \left( \frac{C_{01} - C_{11}}{C_{10} - C_{00}} \right)
\]

\((6.8)\)  

where \(P_0\) and \(P_1\) are the prior probabilities of a device being outside or inside the BBN. One very important consideration is the quantity \(\left( \frac{P_1}{P_0} \right) \left( \frac{C_{01} - C_{11}}{C_{10} - C_{00}} \right) = \eta\), which depends on the nature of the BBN layout and inherent risks tied to the remote charting application.

Therefore, intuitively the assignment of various costs \(C_{10}, C_{00}, C_{01}, C_{11}\), and their preference ordering should depend on the relative ease with which a false alarm or a missed detection is inherent in the remote charting system before the system is deployed. The preference ordering of costs can be determined by whether a false alarm or missed detection is inherently equally likely or whether one is more likely than the other. The process of finding the costs is a separate module (discussed later).

Assuming that such a module exists, we can write Eqn. 6.8 as a likelihood-test ratio that can be performed by taking the observations \(P(y|H_1), P(y|H_0)\) and comparing them against a system-dependent
threshold \( (\eta) \) multiplied by any prior probabilities (subjective bias):

\[
P(y|H_0) \geq H_0 \quad \frac{P(y|H_0)}{P(y|H_1)} < H_1 \quad (\eta)
\]  

(6.9)

If the likelihood ratio of the observations is \( > \) the system threshold, than \( H_1 \) should be chosen. The use of the system threshold \( (\eta) \) allows the hospitals to tune their system by assigning higher costs to the localization errors \( (C_{01}, C_{10}) \). This is explained in more detail in the following sections.

6.1.2.6 Approach to Calculation of Suitable Costs and Priors

As motivated previously, we should calculate the designed remote charting BBN layout’s inherent propensity throwing a false alarm or having a missed detection. This information will provide a scientific way of determining priors \( P_0, P_1 \) and the costs \( C_{00}, C_{01}, C_{10}, C_{11} \), rather than just randomly assigning them based on subjective biases.

Note that the inherent propensity of a BBN throwing a false alarm or a missed detection depends on the BBN’s dimensions. If each BBN is big and wide enough, then the errors will decrease. Note the missed detection should not increase even if the BBN’s are larger since the targets are usually placed near the center of a BBN. However, if BBN sizes are smaller, the errors in authorizing a target correctly with its designated BBN will increase, especially the false alarms.

However, the BBN size is not always under the control of the company providing the Remote Charting service. BBN sizes can vary significantly from city to city and across hospitals based on their patient loads and other policies. Therefore, we will consider a hospital ward with multiple BBNs, where each BBN has smaller dimensions found in the real world medical setting. Then, given the localization error in the underlying multi-lateration/triangulation scheme, we will take sample observations to calculate the probability of false alarm and missed detection for several potential target device locations across all BBNs in a hospital ward. The final probability (population measure) of the false alarm or missed detection as a function of the BBN Remote Charting dimensions is calculated as an average across all sample false alarm and missed detection for each candidate location.
Figure 6.2: **System Threshold**: Proposed sensor locations

6.1.2.7 Likelihood of False Alarms:

Any BBN $i$, has a set of adjacent BBNs is represented by $C^{(i)} = \{1, \cdots, c, \cdots, n\}$ such that any neighboring particular BBN, in the set C is represented by $c$. Consider the typical scenario in Fig. 6.2 with two BBNs in a hospital room and two additional BBNs in an adjacent room. During the installation, training target devices are placed in three locations per BBN ($L^{(i)} = L_1, \ldots, L_3$) such that there are twelve candidate locations in the hospital rooms represented by the set $\bigcup_{i=1}^{4} L^{(i)}$. Therefore, for a given BBN $i$, the remaining nine candidate locations will be placed in the adjacent BBNs, that span the
envisioned layout of the hospital room. Thus, these nine locations will be candidates to produce a false alarm for BBN \( i \). Let the cardinality of set \( L^i \) be represented as \( |L| \), such that in the considered scenario, the \( |L| = 3 \).

Suppose \( x \) denotes the estimated location of a target device \( D_{\text{new}} \) at any of the candidate locations. Then the sample false alarm probability, \( P_{f_{ic}}(x) \) is the probability of that a target device (\( D_{\text{new}} \)) at location \( x \) which is in an adjacent BBN\( _c \). The final false alarm rate for the \( i \)-th BBN, denoted by \( P_f(i) \) is an average of sample false alarm probabilities recorded over all candidate locations.

**Sample False Alarm Probabilities (\( P_{f_{ic}}(x) \)):** To calculate the sample false alarm probabilities for a particular BBN, we compute the sample false alarm probabilities per candidate location from all adjacent BBNs, and then take an average of all samples to get the population false alarm probability that is the steady-state likelihood of observing a false alarm in the \( i - th \) BBN. The following procedure does this calculation:

**STEP 1:** Select a sensor location \( x \) from the set \( \bigcup_{i=1}^{4} L^i \).

**STEP 2:** Calculate the shortest distances from this location \( x \) to each of the adjacent BBN\( _c \). The shortest distance is represented by \( Dist_c(x) \), and the set of shortest distances to adjacent BBNs is represented by \( D \).

**STEP 3:** For each such distance \( Dist_c(x) \in D \), find the corresponding localization error mapping \( y = CDF(Dist_c(x)) \) specified by the CSI-BLoC module (specified by the CDF in Figure 6.3)

**STEP 4:** For each \( Dist_c(x) \in D \), find the \( P_{f_{ic}}(x) = 1 - CDF(Dist_c(x)) \)

**STEP 5:** Store all \( P_{f_{ic}}(x) \), such that there are \( |C| \) number of probabilities.

**STEP 6:** Repeat step 1 to 5, for each location \( x \).

The corresponding \( P_{f_{ic}}(x) \) (which is the probability that any device outside \( BBN_i \) is viewed as within \( BBN_i \)) is determined by substituting the calculated distance shortest \( Dist_c \) in the corresponding CDF (\( CDF_c \)) in Figure 6.3, such that where \( P_{f_{ic}}(x) = 1 - CDF_c \).

The physical meaning of the localization error mapping \( CDF(.) \) function is that given any point of
the x-axis, which denotes the error between the true location and the inferred location, the chances that it will happen is less than or equal to the corresponding value in the y-axis.

**Population False Alarm Likelihood** ($P_{fi}$):

$$P_{fi} = \frac{\sum_{L} \sum_{C} P_{f_i}(x)}{|L| \times |C|}$$

(6.10)

where $P_{fi}$ is the population false alarm probability for the i-th BBN, $|C|$ is the cardinality of the adjacent BBN set, and $|L|$ is the cardinality of the set of candidate locations *per BBN*.

![Figure 6.3: Location Accuracy of [1]: Compared to a modern AoA system](image)

Table 6.1 shows an example of this lookup for Sensor1 and Sensor2 that are in positions shown in Figure 6.4. As the sensor moves closer to an adjacent BBN, the probability of a false localization error increases. However, the sensor could be anywhere in the adjacent BBNs, so the final probability of false alarm should be calculated over various target devices’ test positions in the adjacent BBNs.
Table 6.1: **Relationship between Distance and Errors** \( Dist_{c,z} \) to \( P_{f_i} \) matching: Data represents the illustration of Figure 6.4 for BBN\(_i\) when \( CDF_c = 95\% \), \( L_{err} = 2m \), \( c \) is the adjacent BBN, and \( x \) is the location of the sensor. The final probability of missed detection is 36% (0.36) under this given layout.

<table>
<thead>
<tr>
<th>( Dist_{c,z} )</th>
<th>Distance (m)</th>
<th>Sample ( P_{f_x}(x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( Dist_{1,1} )</td>
<td>0.89</td>
<td>0.43</td>
</tr>
<tr>
<td>( Dist_{2,1} )</td>
<td>3.57</td>
<td>0</td>
</tr>
<tr>
<td>( Dist_{4,1} )</td>
<td>3.36</td>
<td>0</td>
</tr>
<tr>
<td>( Dist_{1,2} )</td>
<td>0.52</td>
<td>0.77</td>
</tr>
<tr>
<td>( Dist_{3,2} )</td>
<td>1.30</td>
<td>0.23</td>
</tr>
<tr>
<td>( Dist_{4,2} )</td>
<td>0.52</td>
<td>0.77</td>
</tr>
</tbody>
</table>

Figure 6.4: **Example Sensor Locations**: \( Dist_{c,z} \) represents the shortest distance from BBN\(_c\) to Sensor\(_z\).
6.1.2.7.1 Likelihood of Missed Detection Here, we calculate that given a target device placed in any BBN, what is the inherent propensity that it will be inferred as being outside the BBN. This, of course, is affected by several factors, such as each BBN’s dimensions and the number of BBNs needed to be packed within a hospital room. However, we provide a generic method of capturing such the inherent propensity of a missed detection given a Remote Charting scenario (as in Fig. 6.2).

The first step for determining the likelihood of a Missed Localization Error \( P_{\text{mi}}(x) \) can be understood by Figure 6.5. We know that given the true location of a target BLE device, the BLoc module has a location error, in terms of distance from the target’s actual location, that is quantified by the \( L_{\text{err}} \) in the CDF function. Naturally, we need to estimate the shortest distances to all four sides of a BBN from the location \( x \), \( d^m(i) = d_1, \cdots, d_4 \). For each such distance, calculate \( 1 - CDF(d^m(i)) \) and record only those members of the set \( d^m(i) \) which produce a non-zero \( (1 - CDF(d^m(i)) \). This is because zero will be produced for only those members whose shortest distances to a given BBN side are larger than 3.5m. Since there is 0% chance of the BLoc module, making an error of above 3.5m from the sensor’s true location, these possibilities need not be accounted for in the missed detection. Only non-zero \( (1 - CDF(d^m(i)) \) need to be accounted for.

The easiest way to achieve this is to find the distance for which the \( (1 - CDF(d^m(i)) \) is just zero, which can be easily found from the CDF of the BLoc module. Let this distance be denoted as \( L_{\text{err}}^* \). Draw a circle of radius \( L_{\text{err}}^* \) and determine the area \( (A_{\text{out}}) \) that is outside of the BBN.

One method for calculating \( A_{\text{out}} \) is to use Fig. 6.3 to determine the \( L_{\text{err}} \) (that is the distance that gives a 100% confidence that the actual target is within that boundary), corresponds to a desired CDF \( (CDF_i) \). Then a circle with a radius of \( L_{\text{err}} \) that gives 100% confidence can be drawn around the sensor’s location. There is a \( CDF_i \% \) chance that the sensor’s actual location is within that circle of radius \( CDF_i \). Figure 6.5 below illustrates this.
Figure 6.5: Missed Localization Error

The shaded area of the Figure 6.5 represents $A_{out}$ which is easily calculated using geometry and subtracting the area of the triangle from the circular vector as follows:

$$A_{out} = \sum_{k} A_{outk}$$  \hspace{1cm} (6.12)

where $k$ is the number of shaded regions outside the BBN$_i$.

Then by dividing $A_{out}$ by the total area of the circle, the percentage of the area outside of the area can be obtained. Lastly, by multiplying this percentage by $CDF_i$ provides the probability of a Missed Localization Error ($P_m$) occurring.

$$P_m(x) = \left(\frac{A_{out}}{\pi r^2}\right)(CDF_i(L_{err}))$$  \hspace{1cm} (6.13)

where $x$ represents the location of the sensor.
Calculation of Final Missed Detection Likelihoods \((P_{mi})\): 

\[
P_{mi} = \frac{\sum_{x} P_{mi}(x)}{|L|}
\]  

where \(|L|\) is the number of test locations per BBN. In the given scenario \(|L| = 3\).

**Illustrative Example for Missed Detection Calculation via Eqn. 6.13**

As an example, if \(A_{out} = 1.5m^2\) there is a 11.34% chance of the BBN having a missed localization error. When the sensor is not physically within BBN, \(P_{mi} = 0\), or if the estimated location of the sensor is such that all distances between the edges of that BBN and that location is more than 3.5m, then the probability of the missed detection is zero.

**6.1.2.8 Cost Considerations**

According to our study, two major factors affect cost assignments:

1. The difference between the likelihoods of false alarm and missed detection of that *given dimension and layout of the BBNs in the Remote Charting system*.

2. Perceived risk asymmetry between a false alarm and a missed detection outcome.

One of the factors that determine costs of the various decision outcomes \((C_{00}, C_{01}, C_{10}, C_{11})\) and the priors \(P_0\) and \(P_1\) may be the inherent likelihood of false alarm \((P_{10})\) and missed detection \((P_{01})\) in the system. The closer these two likelihoods are to each other, the lesser should be the difference between the costs \(C_{01}\) and \(C_{10}\) and the priors and vice-versa. This is an important factor because, as evident from the previous Eqn. 6.8, the factor \(\left(\frac{C_{01} - C_{11}}{C_{10} - C_{00}}\right)\), plays a prominent role in the ultimate decision threshold used for converting the observation into a decision.

On the other hand, if these probabilities are very different from each other, the difference in their costs should also be high. For example, although both are erroneous decision outcomes, the more frequent error decision may be provided at a higher cost. This should play a role in the cost assignments in the hypothesis test approach.
Another critical factor affecting the cost is which error, out of the false alarm or missed detection, is riskier? This is evaluated by asking the question as to, regardless of the probabilities of false alarm or missed detection, how much damage occurs for each instance of a false alarm or a missed detection. Suppose, if one false alarm causes 10 units of damage compared to 2 units of damage caused by one missed detection, then even if the false alarm probability is 5 times lower than the missed detection probability, the costs assigned to both outcomes should be equal.

Therefore, in our remote charting system, the perceived risk of a single false alarm and missed detection event by a Bed Bay Device for a given BBN has to be understood from how this decision affects the performance of the voting-based approach that happens between individual decisions among all BBN specific Bed Bay Devices. When a false alarm or missed detection occurs, the resulting decision (Section 6.1.1.6) of whether or not the prospect device is within the corresponding Bed Bay Device’s network will be compromised. This decision is what the Bed Bay Device uses to cast its vote (Section 6.1.1.7) on whether or not that device should join its network. However, the impact of a BBN incorrectly voting is minimized by the requirement of a consensus (Section 6.1.1.8) being reached on the device’s location.

The system threshold ($\eta$) is set by assigning costs of the various decision outcomes ($C_{00}$, $C_{01}$, $C_{10}$, $C_{11}$). We propose this being done during the Remote Charting system’s installation process, which involves placing sensors in twelve locations and calculating the probabilities of localization errors ($P_f$ and $P_m$) for each BBN. Figure 6.2 illustrates this.

### 6.1.3 Final Hypothesis Test Procedure at Deployment

This section puts together the fundamental principles of hypothesis testing, cost considerations, and minimizing expected risk in decision outcomes into one single derivation. This shows that given an observation (which in this case is a distance and an angle), what is the appropriate threshold that the individual Bed Bay Device in a BBN should use to decide its vote of whether the new target device is within the BBN or not. We show this analysis, with the observation as the estimated distance measurement rather than estimated angle measurements. The distance is the most critical distinguishing factor between inter BBN authorization, which establishes whether the target is within the concerned
Bed Bay Device’s BBN or not.

Once this is decided, the angles are essential for understanding whether the target device is in a likely position on the patient or not. While the same analysis applies broadly, we are only showing the distance measurement as the observation to solve the inter BBN authorization problem. The following process is implemented by each Bed Bay Device independently.

As a recap, our hypothesis state space is the following:

- $H_0$ (null hypothesis) - decide that $D_{new}$ is not inside this BBN
- $H_1$ (alternative) - decide that $D_{new}$ is within this BBN

We put forward three key design considerations:

1. Intuitively, the mean distribution of distances measured at the Bed Bay Device, when $H_1$ is true, will be smaller than when $H_0$ is true.

2. Furthermore, when $H_1$ is true, the path between the Bed Bay Device and the target is longer, contains more obstacles and therefore, the variance of this measurement’s distribution under hypothesis $H_1$ is at least equal or greater than the variance in the same measurement’s distribution under the hypothesis $H_0$.

3. Depending on the fading environment inside the hospital, the distribution of the distance measurement can vary. Since Remote Charting systems do not exist yet, and since this is a theoretical piece of work, we assume a Gaussian distributed set of observations consisting of at least 30 samples of distances and angles. In reality, for a given hospital setting, one must replace the Gaussian PDF with the observed PDF of the corresponding parametric family of distribution of distance and angle measurements observed during the installation phase. However, our current assumption of Gaussian is sufficient for the theoretical approach since a large fraction of natural signal processing systems follow a Gaussian distribution. Another option is to use a student’s distribution to give more robust results than the Gaussian distribution. A student’s distribution would be best for removing errors introduced from indirect (reflected signals) or if you the proposed 30 signal observations is not feasible.
In the original formulation of hypothesis tests typically used in radar systems, the null hypothesis is usually a low signal due to the absence of a target. However, our problem is an inverse problem because the observation is a distance measurement, and under the null hypothesis, the observation signal (distance) is larger. Therefore, we switch the specification of the observed signal under each hypothesis such that $H_0$ is parameterized with a distribution with mean $m_0$ and standard deviation $\sigma_0$, while $H_1$ is parameterized with mean $m_1$ and standard deviation $\sigma_1$, where $m_0 > m_1$ and $\sigma_0 \geq \sigma_1$. Formally, it can be represented by the following equations

\[
H_0 : y = m_1 + W_1 \\
H_1 : y = m_0 + W_0 \\
W_0 \approx \mathcal{N}(0, \sigma_0^2) \\
W_1 \approx \mathcal{N}(0, \sigma_1^2) \tag{6.15}
\]

where $W_0$ and $W_1$ are noise sources which are zero mean Gaussian distribution $W_0 \approx \mathcal{N}(0, \sigma_0^2)$, that creates the variation in the distance measurements compared to the true distance. Therefore, the specification of the distribution of the observations (distance) under each hypothesis can be mathematically represented by the following:

\[
P(y|H_1) = \mathcal{N}(m_0, \sigma_0^2) \\
P(y|H_0) = \mathcal{N}(m_1, \sigma_1^2) \tag{6.16}
\]

Referring to Eqn. 6.8, it’s important to note that we ensured that the hypothesis test inequality matched the nature of the problem by having the larger observation being under the null hypothesis.

Therefore, the larger signal is $P(y|H_0)$, whose mean and standard deviation is counter intuitively represented as $m_1$ and $\sigma_1$, respectively. Hence, we write down the Eqn. 6.8 in the following manner:

\[
\frac{P(y|H_0)}{P(y|H_1)} \overset{H_0}{\geq} \frac{P_1}{P_0} \left( \frac{C_{01} - C_{11}}{C_{10} - C_{00}} \right) \tag{6.17}
\]
Replacing the previous section’s Eqn. 6.16, in the Eqn. 6.17, we get

\[
\frac{1}{\sqrt{2\pi \sigma_1^2}} e^{-\frac{(y-m_1)^2}{2\sigma_1^2}} >_{H_0} \frac{P_1}{P_0} \left( \frac{C_{01} - C_{11}}{C_{10} - C_{00}} \right) >_{H_1} \left( \frac{P_1}{P_0} \right) \left( \frac{C_{01} - C_{11}}{C_{10} - C_{00}} \right)
\]

(6.18)

Now let \(\frac{(y-m_0)^2}{2\sigma_0^2} = x_0\) and \(\frac{(y-m_1)^2}{2\sigma_1^2} = x_1\). Therefore, Eqn. 6.18, can be rewritten as:

\[
\left( \frac{\sigma_1}{\sigma_0} \right) \left( \frac{e^{-x_0}}{e^{-x_1}} \right) >_{H_0} \left( \frac{P_1}{P_0} \right) \left( \frac{C_{01} - C_{11}}{C_{10} - C_{00}} \right)
\]

(6.19)

Taking the \(\left( \frac{\sigma_1}{\sigma_0} \right)\) to the R.H.S. of the inequality taking the natural logarithm on both sides, the above equation can be written as:

\[
\frac{(y-m_0)^2}{2\sigma_0^2} - \frac{(y-m_1)^2}{2\sigma_1^2} >_{H_0} \ln \left( \frac{P_1}{P_0} \right) \left( \frac{C_{01} - C_{11}}{C_{10} - C_{00}} \right) \left( \frac{\sigma_1}{\sigma_0} \right)
\]

(6.20)

After solving for \(y\), through some tedious but straightforward algebra, by bringing everything to the right-hand side of the above inequality, it can be shown that solving for \(y\), we get the following:

\[
y >_{H_0} \ln \left( \frac{P_1}{P_0} \right) \left( \frac{C_{01} - C_{11}}{C_{10} - C_{00}} \right) \left( \frac{\sigma_1}{\sigma_0} \right) - \frac{(4\sigma_1^2 \sigma_0^2)(2(\sigma_1^2 - \sigma_0^2))}{-(4(m_1 \sigma_0^2 - m_0 \sigma_1^2)) \pm \sqrt{(4(m_1 \sigma_0^2 - m_0 \sigma_1^2))^2 - 16(\sigma_1^2 - \sigma_0^2) \cdot (\sigma_1^2 m_0 - \sigma_0^2 m_1)}}
\]

(6.21)

The R.H.S of the above equation forms the decision threshold denoted by \(\Gamma_{MAP}\), which can be written as the following:

\[
\Gamma_{map} = \ln \left( \frac{P_1}{P_0} \right) \left( \frac{C_{01} - C_{11}}{C_{10} - C_{00}} \right) \left( \frac{\sigma_1}{\sigma_0} \right) - \frac{(4\sigma_1^2 \sigma_0^2)(2(\sigma_1^2 - \sigma_0^2))}{-(4(m_1 \sigma_0^2 - m_0 \sigma_1^2)) \pm \sqrt{(4(m_1 \sigma_0^2 - m_0 \sigma_1^2))^2 - 16(\sigma_1^2 - \sigma_0^2) \cdot (\sigma_1^2 m_0 - \sigma_0^2 m_1)}}
\]

(6.22)

This complicated looking expression can be denoted as \(\Gamma_{MAP}\) and acts as a decision boundary for the observation \(y\) that we make at the run time. If the \(y > \Gamma_{MAP}\), the Bed Bay Device decides that the target device is not within the BBN. Otherwise, it decides that it is within the BBN.

We need to learn the most generalizable \(\Gamma^*_{map}\). For this, we propose some additional measurements.
at a bed bay device that are taken during the installation process to learn the $\Gamma_{map}^*$. This is done with the following: Here we take two target devices, one near the bed of the correct BBN and one just outside the correct BBN. This is repeated for several candidate training locations, each being a training round containing one location within and one location outside the BBN. Finally, we take the average of all $\Gamma_{MAP}$ testing rounds to report the final $\Gamma_{MAP^*}$, which should be used by the authorization system in the testing/deployment phase. It is important to note that $\Gamma_{MAP^*}$ is the proximity threshold for each BBN.

Plotting an example of these distributions allows us to visualize how the errors ($P_m, P_f$) can be determined:
Figure 6.6: Example Gaussian Distribution:

This illustration shows that the threshold depends on costs, the means of the distributions under the two hypothesis, their variances, and prior probabilities of each hypothesis, as well as the shape of the distribution of the observations that dictate the hypothesis under question.

In this graph, the pure number ($\Gamma_{map}$) separates observations that are missed localization errors ($P_m$, shaded green) from false localization errors ($P_f$, shaded orange). The observation $y_1$ is an example
of when the system infers $H_0$ (i.e., outside the BBN), but this value comes from $H_1$ distribution (i.e., actually inside the BBN), which is an example of a missed localization error ($P_m$). Now that we have a way to visualize the errors, we can calculate the probability of an error ($P_{err}$) occurring

$$P_{err} = P(\text{decide } H_0 | H_1 \text{ is true})P(H_1) + P(\text{decide } H_1 | H_0 \text{ is true})P(H_0)$$

(6.23)

$$P_{err} = P_m P_1 + P_f P_0$$

Lastly, a $Q$ function can be used to calculate the green shaded ($P_m$) and orange shaded ($P_f$) areas of Figure 6.6:

$$P_{err} = P_1 Q\left(\frac{\Gamma_{map} - m_0}{\sigma_0}\right) + P_0 Q\left(\frac{m_1 - \Gamma_{map}}{\sigma_1}\right)$$

(6.24)

Eq. 6.24 represents the probability of a localization error ($P_{err}$) occurring for an observation that are of a Gaussian distribution. Taking the average of $P_{err}$ for the test rounds gives you a system average of $P_{err}^*$ which tells you the expected system performance.

Because of the inversion in the problem, the following is true

$$P_m = Q\left(\frac{\Gamma_{map} - m_0}{\sigma_0}\right)$$

and

$$P_f = Q\left(\frac{m_1 - \Gamma_{map}}{\sigma_1}\right)$$

### 6.1.4 Final Voting Decision and Consensus

In this section, we will summarize how the voting decision (Section 6.1.1.6) is used by the Bed Bay Device in the voting process outlined in Section 6.1.1.7. The output of this vote is then used by the system to reach a consensus (Section 6.1.1.8) on the prospect device’s location.

As discussed earlier in this chapter, in order for a device to receive physical layer authorization, the following must be done:

1. Setting of the System Threshold ($\eta$)

2. Voting Decision made by each BBN$_i$
3. Consensus on the device’s membership.

Before a Bed Bay Device can decide on the BBN membership of a device, the system’s threshold \((\eta)\) must be determined. This process, which is done during the initial installation of the system, allows the Bed Bay Devices to accurately decide whether or not a device is within its authorized jurisdiction since the \(\eta\) takes into consideration the likelihood of localization errors in the given layout (and therefore allows the system to assign appropriate costs) and the uncertainty in the distance and angle observations.

Once the \(\eta\) has been established, the Bed Bay Devices have the information needed to test their location hypothesis on an observed signal. As discussed in Section 6.1.3, each Bed Bay Device will take the observed signal \((y)\) and compare it against a decision boundary \((y > \Gamma^*_{MAP})\). The result of this comparison is the Bed Bay Device’s decision \((z)\) on whether the device is within \((H_1)\) or outside \((H_0)\) its BBN. This decision \((z)\) is then used by the Bed Bay Device in the voting process (Section 6.1.1.7), where \(V_i = z_i\).

Since the votes made by each Bed Bay Device may consist of localization errors (false or missed), the system performs a final analysis (Section 6.1.1.8) to determine if a consensus can be made. The final system decision of granting physical layer authorization, thus allowing a prospect device to join a BBN, is only given if consensus has been made on its location.

6.2 Human Assisted Device Assignment

Before the data generated from a Patient-Specific Device can be entered into the EMR, the device must be assigned to a patient. This is a manual step that must be done by an HCP. As shown in Figure 3.2, the Application Server will be connected to a Clinical App. This Clinical App can be used by an HCP to manually select what data needs to be collected for a patient and assign that patient to a particular room number. Since it is assumed that only one device type can generate a particular class of data (e.g., heart rate), this manual selection will also select the type of Patient-Specific Devices authorized for the patient.

Taking the information received from the Clinical App, the Application Server will then be aware of what device types are authorized for a particular BBN. This can be accomplished by having the Application Server configured in a manner that allows it to link room numbers to a corresponding BBN.
Since a BBN is tied to a Bed Bay Device, which is not mobile, it can be done once during the initial system installation.

6.3 Authorization Decision

The Inter BBN Authorization process’s final step is the decision on whether or not a Patient-Specific Device is authorized to join the BBN. This framework proposes the decision to be made by the Application Server. However, it could also be made by the Bed Bay Device.

When a Bed Bay Device reports a Patient-Specific Device’s physical authorization, the Application Server is responsible for replying with a final Inter BBN authorization event. The Application Server will look at the device type reported by the Bed Bay Device and see if it has been authorized for that BBN by the Clinical App. If previously authorized, it will inform the Bed Bay Device that the reported device is authorized and can remain on the network. Conversely, no authorization is sent back to the Bed Bay Device if it has not been previously authorized. In this scenario, the Bed Bay Device will timeout waiting for final authorization and remove the prospect device from the BBN.
Chapter 7

Process for Intra BBN

Authentication and Attack Detection

After an authorized Patient-Specific Device has successfully joined a BBN, the system must determine if the connected device has been previously compromised and continuously monitor for new attacks. Both tasks are the last line of defense before data is entered into the EMR, potentially impacting both the patient and HDO. If compromised data makes its way into the EMR, it could result in physical harm to the patient or present legal and financial issues for the HDO.

This section explains the process for Intra BBN Authentication and Attack Detection. Assisted Decision Making is used by the Application Server to decide whether data should be passed to the EMR. This process can be broken down into two sub-processes and one final decision:

1. Compromised Device Detection

2. New Attack Detection

3. EMR Decision
7.1 Compromised Device Detection

As previously mentioned in Section 6.1.1.9, the device type identification is obtained directly from the Patient-Specific Device. Therefore, it would not be complicated for a compromised device to bypass this step of the authorization process. It would merely need to inform the Bed Bay Device that it is a device type that is authorized, which can be easily guessed. To prevent compromised patient data from being entered into the EMR, an additional authentication step that verifies the device’s type is required. There are several approaches for authenticating the type of device that was discussed in 3.3.2. However, dynamic biometrics is best suited for a Remote Charting application and the given device constraints of Table 5.1. Due to complexity, the details of an approach has been left for future work.

7.2 New Attack Detection

CSI measurements described in 5.3.3 and data produced by the Patient-Specific Device will be used to look for signs of a new attack. When a new attack is detected, the Application Server will alert the Clinical App to notify the HCP. There are three events that the Bed Bay Device will be looking for:

1. Unauthorized Device Placed in BBN area
2. Removal and Replacement of a Patient-Specific Device
3. Rearrangement of a Patient-Specific Device

7.2.1 Device Placed in BBN Area

The ability to detect and authorize a new device is already built into the proposed framework and is described in 6.1. However, this would not detect a malicious device attacking the BBN without establishing a new connection. To detect this, the BBN must be capable of detecting abnormal transmissions that are within the wireless spectrum of BLE. Each anchor point will continuously monitor the RF environment looking for evidence of signal jamming and if a device appears to be transmitting from multiple locations. If either of these are detected, the Bed Bay Device will send a notification to the Application Server and alert the Clinical App.
7.2.2 Removal and Replacement of a Patient-Specific Device

To differentiate normal behaviors from a potential attack, the proposed framework must be capable of characterizing how a device disconnects from the network, where a normal behavior is defined as the device gradually leaving the range of the BBN. For example, when the patient goes for a walk or is taken out of the room for an X-Ray. When abnormal behavior is detected, the Application Server will inform the Clinical App, which then alerts the HCP. This framework proposes that the HCP follow a device de-assignment process before intentionally powering a device off or removing it from a patient to prevent false alarms being generated. In this simple process, the HCP will use the Clinical App to manually remove the types of data being collected from the patient, thus removing the Patient-Specific Devices from the BBN.

Since the location (i.e., CSI data) of the device is continuously monitored, the BBN can identify a device that is gradually leaving the range of the network. Furthermore, the rate of packet losses in the BLE connection will also indicate the device is leaving the range of the BBN. In this expected behavior, the Bed Bay Device will notify the Application Server that the device has disconnected, and the Clinical App is updated, but no alert needs to be provided to the HCP. However, when a device suddenly disconnects without signs of being physically removed from the room, the BBN will classify this as abnormal behavior, and an alert will be provided to the HCP.

7.2.3 Rearrangement of a Patient-Specific Device

It is common for a patient to rearrange sensors when they are located in positions that are not comfortable. However, this can impact the accuracy of the sensor [4]. Therefore, if a malicious actor wanted to cause harm, they would simply need to rearrange the sensor. To defend against both benign and malicious actions, the proposed framework must be capable of detecting when a sensor has been rearranged. Sensor rearrangement can be detected by combining physical layer information of the sensors’ wireless transmissions with the sensor’s data. When sensor rearrangement is detected, this framework proposes that the HCP goes to the patient’s room and checks to see if the sensor has been rearranged.

Detecting sensor rearrangement can be done by observing the AoA of the sensor’s wireless transmissions, which is required to localize the device. As mentioned in Section 5.3.4.2, the angle at which a
wireless signal originates from can be determined by taking several channel measurements on multiple antennas. When a sensor is moved from one location to another, the relative distance estimated may appear to be unaffected, but the angle at which the direct path arrives will change. This change in angle can be used to identify sensor rearrangement, and the Bed Bay Device will alert the Application Server.

What if the sensor was quickly moved a small distance that results in an identical AoA? To handle this scenario, the data produced by the sensor can be leveraged. A sudden shift in data values indicates that the sensor has been rearranged. As an example, let us consider the scenario where a patient wishes to move a blood pressure cuff, so it is slightly further down their arm. The blood pressure readings will change when the sensor is not physically attached to the patient and could be easily detected by analyzing the data. This data analysis is proposed to be done by the Application Server.

7.2.4 Stale Data

To prevent the possibility of stale data being entered into the EMR, the framework proposes that the data sent from the Patient-Specific Device to the Bed Bay Device is timestamped. Before the data is sent to the Application Server, the Bed Bay Device verifies the correct timestamp. If not, the data is considered invalid. If two or more invalid data packets are received, the Bed Bay Device will terminate the Patient-Specific Device connection and report the event to the Application Server.

7.3 EMR Decision

The Application Server is responsible for making the final decision of allowing data to be sent to the EMR. If the Application Server detects that a device may be compromised or signs of a new attack is detected, an alert will be sent to the Clinical App. It is then assumed that the HCP follows a protocol (enforced by the HDO) that requires them to physically go to the patient’s room and manually check that the data being produced by the sensor is accurate and in the correct location. If no issues are found, the HCP can clear the alarm, and the Application Server will submit the data into the EMR.
Chapter 8

Simulated Results

This chapter provides results for a simulated remote charting system to validate our method’s accuracy under varying parameters. First, using arbitrarily chosen values, we calculate each BBN’s expected risk to evaluate how to assign the system threshold \( \eta \). Secondly, we set the proximity threshold \( \Gamma_{MAP}^* \) and calculate the probability of a localization error occurring for the simulated system. Lastly, we show how changes to the cost assignments and prior bias can impact the system’s performance.

8.1 Setting of System Threshold

To better illustrate the effect of the system threshold \( \eta \), consider observations made during the proposed installation process of Section 6.1.2.6 resulted in the following probabilities of localization errors:

Then using Eqn. 6.10 and Eqn. 6.14 the \( P_{f_i} \) and \( P_{m_i} \) can be calculated for each BBN\( _i \):
Table 8.1: Example False Localization Errors $P_{f_i}(x)$: where $x$ is the sensors location ($L = \{L_1, \ldots, L_{12}\}$)

<table>
<thead>
<tr>
<th>$P_{f_i}(x)$</th>
<th>L1</th>
<th>L2</th>
<th>L3</th>
<th>L4</th>
<th>L5</th>
<th>L6</th>
<th>L7</th>
<th>L8</th>
<th>L9</th>
<th>L10</th>
<th>L11</th>
<th>L12</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_{f_{12}}(x)$</td>
<td>0.03</td>
<td>0.03</td>
<td>0.03</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$P_{f_{13}}(x)$</td>
<td>0</td>
<td>0.03</td>
<td>0.30</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$P_{f_{14}}(x)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$P_{f_{22}}(x)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.03</td>
<td>0.03</td>
<td>0.03</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$P_{f_{23}}(x)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$P_{f_{24}}(x)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.03</td>
<td>0.30</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$P_{f_{32}}(x)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.30</td>
<td>0.03</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$P_{f_{33}}(x)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.15</td>
<td>0.001</td>
<td>0.15</td>
<td>0</td>
</tr>
<tr>
<td>$P_{f_{34}}(x)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.03</td>
<td>0.03</td>
<td>0.03</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 8.2: Example Missed Localization Errors $P_{m_i}(x)$: where $x$ is the sensors location ($L = \{L_1, \ldots, L_{12}\}$)

<table>
<thead>
<tr>
<th>$P_{m_i}(x)$</th>
<th>L1</th>
<th>L2</th>
<th>L3</th>
<th>L4</th>
<th>L5</th>
<th>L6</th>
<th>L7</th>
<th>L8</th>
<th>L9</th>
<th>L10</th>
<th>L11</th>
<th>L12</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_{m_1}(x)$</td>
<td>0.15</td>
<td>0.001</td>
<td>0.15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$P_{m_2}(x)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.15</td>
<td>0.001</td>
<td>0.15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$P_{m_3}(x)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.15</td>
<td>0.001</td>
<td>0.15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$P_{m_4}(x)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.15</td>
<td>0.001</td>
<td>0.15</td>
</tr>
</tbody>
</table>

Table 8.3: Calculated Localization Errors: where $i = \{1,2,3,4\}$ and $x$ is the sensors location ($L = \{L_1, \ldots, L_{12}\}$)

<table>
<thead>
<tr>
<th>Error</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_{f_1}$</td>
<td>0.0840</td>
</tr>
<tr>
<td>$P_{f_2}$</td>
<td>0.0840</td>
</tr>
<tr>
<td>$P_{f_3}$</td>
<td>0.0840</td>
</tr>
<tr>
<td>$P_{f_4}$</td>
<td>0.0840</td>
</tr>
<tr>
<td>$P_{m_1}$</td>
<td>0.1003</td>
</tr>
<tr>
<td>$P_{m_2}$</td>
<td>0.1003</td>
</tr>
<tr>
<td>$P_{m_3}$</td>
<td>0.1003</td>
</tr>
<tr>
<td>$P_{m_4}$</td>
<td>0.1003</td>
</tr>
</tbody>
</table>
In order to evaluate how to assign values for each cost \((C_{00}, C_{01}, C_{10}, C_{11})\), the expected risk of \(i\)-th BBN \((E_i)\) must first be determined using Eqn. 6.7. Assuming the costs of correct decisions are \(C_{00} = C_{11} = 0\), the prior probabilities are not known and thus must add up to 1, \(P_0 = P_1 = 0.5\), and using Table 8.3, the expected risk for each BBN are:

\[
\min(E_i) = C_{00} \cdot P_{tn_i} + C_{01} \cdot P_{m_i} + C_{10} \cdot P_{f_i} + C_{11} \cdot P_{tp_i}
\]

\[
\min(E_i) = 0 \cdot (1 - 0.0840) + C_{01} \cdot (0.1003) + C_{10} \cdot (0.0840) + 0 \cdot (1 - 0.1003)
\]

\[
\min(E_i) = C_{01} \cdot (0.1003) + C_{10} \cdot (0.0840)
\]

note that in this example the \(P_f\) and \(P_m\) are the same for each BBN\(i\).

As previously explained in Section 6.1.2.8, before assigning values for \(C_{10}\) and \(C_{01}\), we must first take into consideration a couple factors. Firstly, the difference between the probabilities of \(P_f\) and \(P_m\), noted as \(P_{diff}\), should be similar to the difference between \(C_{10}\) and \(C_{01}\). Secondly, the damage from a false alarm and missed detection must also be taken into consideration. With this in mind, let us consider a scenario where a hospital has determined that the damage caused from false alarms \((D_f)\) is 2 times higher than the damage of a missed detection \((D_m)\).

With the probabilities of a false alarm and missed detection in this example being very close \((P_{diff} = 0.0163)\), the main factor to consider for assigning the costs is that \(D_f = 2 \cdot D_m\). Therefore, for this example we assign values of \(C_{10} = 2\) and \(C_{01} = 1\) and the expected risk for each BBN\(i\) can be expressed as a finite number:

\[
\min(E_i) = (1) \cdot (0.1003) + (2) \cdot (0.0840) \Rightarrow 0.2683
\]

\[
\text{Eqn. 8.2 allows the hospitals to evaluate if the physical layout of the BBN networks meets their expectations.}
\]

Furthermore, the system threshold \((\eta)\) resulting from these cost assignments will be used by each BBN\(i\) when making the decision on whether or not an observation is within \((H_1)\) it’s network, this is done using Eqn. 6.8.

\[
\eta = \left(\frac{1 - 0}{2 - 0}\right) \cdot 0.5 \Rightarrow \frac{1}{2}
\]
8.2 Proximity Threshold and Error Probability

The performance of the system depends on the probability of a localization error (\( P_{err} \)) occurring. Prior to determining this we must first set the proximity threshold (\( \Gamma_{MAP}^* \)) which the BBNs use to decide if a prospect device is within its BBN.

In Section 6.1.3, we propose that \( \Gamma_{MAP}^* \) is determined at time of installation by taking two target devices, one near the bed of the correct BBN and one just outside the correct BBN. Repeating this for several candidate test locations, and each test round containing one location within and one location outside the BBN. Then by averaging all \( \Gamma_{MAP} \) testing rounds to report the final \( \Gamma_{MAP}^* \), which is used by the authorization system in Section 6.1.1.6.

Now let’s assume the distance means(\( m_0, m_1 \)) and standard deviations (\( \sigma_0, \sigma_1 \)) shown in Table 8.4 are the results of the test rounds. Where \( r \) represents a particular test round. Using Eqn. 6.22 and Eqn. 6.24 we have also calculated \( \Gamma_{MAP_r} \) and \( P_{err_r} \) of each round by using the system threshold in Eqn. 8.3. 6.24

<table>
<thead>
<tr>
<th>Test Round (r)</th>
<th>( m_1_r )</th>
<th>( m_0_r )</th>
<th>( \sigma_1_r )</th>
<th>( \sigma_0_r )</th>
<th>( \Gamma_{MAP_r} )</th>
<th>( P_{err_r} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3.40</td>
<td>0.65</td>
<td>2.00</td>
<td>0.25</td>
<td>0.73</td>
<td>23.6%</td>
</tr>
<tr>
<td>2</td>
<td>4.30</td>
<td>1.30</td>
<td>2.25</td>
<td>0.60</td>
<td>1.19</td>
<td>32.9%</td>
</tr>
<tr>
<td>3</td>
<td>5.20</td>
<td>1.10</td>
<td>2.75</td>
<td>0.50</td>
<td>2.21</td>
<td>7.6%</td>
</tr>
</tbody>
</table>

Taking the averages of \( \Gamma_{MAP_r} \) result in \( \Gamma_{MAP}^* = 1.38 \). This implies that if an observation \( y \) results in a \( \Gamma_{MAP_y} \leq 1.38 \), the corresponding BBN will decide that the target device is within it’s BBN.

Finally we can evaluate the expected system performance by averaging \( P_{err_r} \) to determine the probability of a localization error occurring, which for this simulation resulted in \( P_{err}^* = 21.37\% \). While this may seem high for a medical application, it’s important to recall that for a device to join a BBN that it does not physically reside both errors (\( P_f, P_m \)) must simultaneously occur at different BBNs. This is true because of the Consensus Step 7 of Section 6.1.1.8.
8.3 Varying Parameters

A Remote Charting system that has a 21% chance of an error occurring, may not be suitable for all implementations. In this section we will show how the independent variables of cost ($C_{00}, C_{01}, C_{10}, C_{11}$) and prior bias ($P_0, P_1$) effect the systems performance. Furthermore, we also illustrate the impact of the distance means($m_{0r}, m_{1r}$) and variances ($\sigma_{0r}, \sigma_{1r}$) has on the system’s performance.

Figures 8.1 and 8.2 illustrate the effects of tuning the system to have higher costs for false alarms ($P_f$) or missed detections ($P_m$), respectively.

---

Figure 8.1: **Impact of Higher Cost for False Alarms** Keeping the rest of the parameters in Table 8.4 the same and $C_{10} = n \times C_{01}$ where $1 \leq n \leq 3$ and $C_{01} = 1$
**Figure 8.2: Impact of Higher Cost for Missed Detections** Keeping the rest of the parameters in Table 8.4 the same and $C_{01} = n \times C_{10}$ where $1 \leq n \leq 5$ and $C_{10} = 2$

Looking at Figures 8.1 and 8.2, it is clear that for this simulation, the system will have the lowest probability of localization errors occurring if the cost of false alarms ($C_{10}$) and the cost of missed detections ($C_{01}$) are assigned in manner such that $C_{10} \leq C_{01}$. However, since a hospital may be more concerned about false alarms or missed detections, these figures also show how they system can be easily tuned to decrease a particular type of error.

Another set of independent variables that needs to be explored are the prior probabilities of a device being outside ($P_0$) or inside ($P_1$) the BBN. Figure 8.3 illustrates how $P_{err}$ is impacted by $P_0$ and $P_1$. In this example we use the values of Test Round 3 from Table 8.4.
Figure 8.3: **Impact of Prior Bias** $P_0$ and $P_1$. Using the parameters in Table 8.4 and having $0.3 \leq P_0 < 1$ and $0.1 \leq P_1 < 0.7$.

For this test round, having a higher prior bias of the device being inside ($P_1$) rather than outside, $P_1 > P_0$, results in a lower probability of errors.

Figures 8.4 and 8.5 show how the system’s performance is also dependent on the means of the distance distributions under the two hypothesis ($m_0$, $m_1$) and their variances ($\sigma_0$, $\sigma_1$). In this example we once again use the values of Test Round 3 from Table 8.4. The results show that the system performs best when the mean distance for devices outside the BBN is greater than the mean distance of devices inside the BBN, $m_1 > m_0$. Which makes sense, since devices outside the BBN will typically be at a further distance. Furthermore, the system performs best when the difference in variances ($|\sigma_0 - \sigma_1|$) are higher.
Figure 8.4: **Impact of mean $m_0$ and $m_1$** Using the parameters in Table 8.4 and $1 \leq m_0 \leq 9$ and $0.5 \leq m_1 \leq 6$
Figure 8.5: **Impact of standard deviation \( \sigma_0 \) and \( \sigma_1 \)** Using the parameters in Table 8.4 and 

\[ 1.75 \leq \sigma_0 \leq 3.75 \text{ and } 0.05 \leq \sigma_1 \leq 1.38 \]
Chapter 9

Threat Analysis

In this chapter the proposed framework in 5.3 will be analyzed using the threat model detailed in 4 while under the assumptions of 5.2. The three attacks that will be analyzed are Spoofing, Fabrication, and DoS attacks.

9.1 Spoofing Attacks

To foil the authorization process of 6 an attacker must spoof it’s location to make it appear that is within range of the BBN. However, since this framework uses a physical layer approach for determining the location of a device, it is not possible for an attacker to spoof it’s physical location.

As previously mentioned, the wireless protocol of choice for the BBN is BLE. It has been demonstrated in [8] that BLE is prone to MITM attacks. However, to perform this attack the attacker must connect to both devices in the connection, the Patient-Specific Device and the Bed Bay Device. This additional connection will be easily detected by the Group Physical Layer Authorization steps done in 6.1. For an attacker to successfully perform the MITM attack, the compromised device must be in close physical proximity to the Patient-Specific Device. Furthermore, given the assumption that the Patient-Specific Device cannot connect to more than one device, the attacker must connect to the device before the Bed Bay Device can. Since the BBN is continuously monitoring the RF environment this connection will be detected and will allow the BBN to determine if a prospect device appears to be communicating with another device. In this scenario, the Bed Bay Device will terminate the connection thus preventing the
9.2 Fabrication Attacks

This framework also allows the detection of a replay attack, where an attacker attempts to replay a message previously sent by a Patient-Specific Device. In 7.3, it is stated that the data sent by the Patient-Specific Device is timestamped. This timestamp allows for easy detection of an attacker attempting to replay stale data. In addition, the BBN is monitoring the RF environment looking for abnormal behavior, discussed in 7.2. If an attacker attempts to replay a message it will appear that a device is communicating from multiple locations and thus shows signs a new attack and the HCP will be alerted to come and look for unauthorized devices that could be present in the room.

9.3 DoS Attacks

Like any wireless network an DoS attacks is not possible to prevent. However, since the RF environment is being constantly monitored, an attacker attempting to perform a signal jamming attack will be detected and reported as abnormal behavior, as explained in 7.2. Similarly, if the Bed Bay Device is being overwhelmed with connection requests, which makes it impossible for devices to join the BBN, the Clinical App will indicate that the patient’s data is not being monitored. This allows the HCP to detect an issue with the network.
Chapter 10

Conclusion

This work has discussed the need for a new Remote Charting solution that meets the unique challenges faced in a clinical setting. A first of its kind security view of the connected medical device spectrum was provided. Lastly, a framework is proposed for implementing a Remote Charting application that is secure from integrity-related attacks.

Current Remote Charting solutions discussed in 2.3 have several barriers for entry, mostly due to their high cost and negative impact on the clinical workflow. However, all of these solutions produce data associated with a specific patient, which introduces additional possibilities for regulatory violations if they are compromised. The framework proposed in this work does not require the mobile devices on the network to be associated with a particular patient, thus reducing risks of exposing regulatory controlled patient data. In this framework, the association between a piece of data and a patient is done on an Application Server, which can be located in a secure environment.

We proposed using Bluetooth Low Energy (BLE) for implementing the Bed Bay Network (BBN). In January of 2019, the Bluetooth SIG released version 5.1 of the standard. Introduced in this version was the capability to determine the Angle of Arrival (AoA). This inclusion makes our proposed architecture for a Remote Charting application even more feasible for Medical Device Manufacturers (MDMs) to implement. Since the standard already had Received Signal Strength (RSS) capabilities, this can be combined to generate the Channel State Information (CSI) necessary for implementing our secure by design Remote Charting framework.
To be viable from both a cost and workflow perspective, the proposed framework utilizes techniques and technologies that can be quickly adopted by MDMs and HDOs. The framework allows devices to move freely from patient to patient without negatively impacting the HCP’s daily workflow.
References


