# A Multi-Radio Interface for Dependable Body Area Network Communications

by

Yasmin Hovakeemian

A thesis

presented to the University of Waterloo

in fulfillment of the

thesis requirement for the degree of

Master of Applied Science

in

Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2011

# Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

# Abstract

Body Area Networks (BANs) are emerging as a convenient option for patient monitoring. They have shown potential in improving health care services through a network of external or implanted biosensors and actuators collecting real-time physiological data. Advancements in wireless networking and sensor development are expediting the adoption of BANs. However, real-time patient monitoring still remains a challenge due to network failures and congestion. In order to improve channel loss resilience and thus link availability, a multi-radio systems approach is adopted incorporating Bluetooth and Wi-Fi.

In this work, we propose a multi-radio interface designed for a BAN to improve end-to-end communications. A multi-radio BAN controller is introduced to interface between the two wireless protocols (Wi-Fi and Bluetooth), control inter-radio handovers, manage a shared transmission buffer, and overall, route data accordingly through the protocol stacks. Simulations are conducted to study the performance of the system by adjusting handover timing and its effect on link availability. Advancing a handover has the benefit of a higher throughput at the cost of an increase in power consumption and timing overhead. Furthermore, various human mobility models, AP placement arrangements, and network densities are simulated to evaluate the performance of the BAN multi-radio interface. Sparse networks were found to have the most gain from the addition of the secondary Bluetooth radio system, as primary AP coverage was already very limited. Simulation results for various combinations of simulation parameters are presented to illustrate the improvement in BAN dependability through a multi-radio interface.

# Acknowledgements

I would first like to extend my sincere appreciation and gratitude to my advisor, Dr. Sagar Naik for all of his advice, guidance and time throughout this process. He was always encouraging and willing to share all of his ideas. His support and patience was truly crucial to my progress. I would also like to extend a thank you to my reviewers Professor Mahesh Tripunitara and Professor Pin-Han Ho for your time and contributions. Finally, I would like to acknowledge the support of Kuwait Ministry of Higher Education.

I am truly indebted to Walid Henawy for all of his motivation, support and 'sanity check' phone calls/visits throughout the duration of my Masters. Thank you so much for putting up with my complaints and deadlines and helping me push through this 'life event'. Last, but certainly not least, I would like to extend a huge thank you to my family who are my greatest supporters! To my mom, Wahiba, for all your much needed phone call distractions and recipes! To my dad, George, for always challenging me and reinforcing that there is always a time to work and play! To my brother and sister, Basil and Sara, for calling to make sure I was alive and making sure I was having fun once in a while! And finally, to Mr. Pico, for his company and entertainment in the final stages. Love you and miss you all!

*To my family…*

# *Table of Contents*

# *List of Figures*

# *List of Tables*

# *List of Abbreviations & Acronyms*

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| ACK | Acknowledge |
| ACL | Asynchronous Connectionless Link |
| AES | Advanced Encryption System |
| AP | Access Point |
| BAN | Body Area Network |
| BASN | Body Area Sensor Network |
| BN | Body Network |
| BP | Blood Pressure |
| BS | Base Station |
| BSN | Body Sensor Network |
| BSS | Basic Service Set |
| CBC | Cipher Block Chaining |
| CCM | CTR and CBC Mode |
| CSMA/CA | Carrier Sense Multiple Access/ Collision Avoidance |
| CTR | Counter |
| CTS | Clear to Send |
| DCF | Distributed Coordination Function |
| DIFS | DCF Interframe Space |
| DL | Downlink |
| ECG | Electrocardiogram |
| EEG | Electroencephalogram |
| EMG | Electromyography |
| ESS | Extended Service Set |
| FFD | Full-Function Device |
| FHS | Frequency Hopping Synchronization |
| FHSS | Frequency Hopping Spread Spectrum |
| FIFO | First In, First Out |
| HSPA | High Speed Packet Access |
| IBSS | Independent Basic Service Set |
| I/O | Input/Output |
| LAN | Local Area Network |
| LLC | Logical Link Control |
| LR-WPAN | Low-Rate Wireless Personal Area Network |
| LTE | Long Term Evolution |
| MAC | Medium Access Control |
| MMO | Metal Metal Oxide |
| MS | Mobile Station |
| PAN | Personal Area Network |
| PC | Point Coordinator |
| PCF | Point Coordination Function |
| PHY | Physical Layer |
| QoS | Quality of Service |

| | |
|---|---|
| RAN | Radio Access Network |
| REQ | Request |
| RFD | Reduced-Function Device |
| RSP | Response |
| RTS | Request to Send |
| SCO | Synchronous Connection-Oriented Link |
| SIFS | Short Interframe Space |
| UL | Uplink |
| UMTS | Universal Mobile Telecommunications System |
| UWB | Ultra Wide Band |
| WAN | Wide Area Network |
| WBAN | Wireless Body Area Network |
| Wi-Fi | Wireless Fidelity |
| WLAN | Wireless Local Area Network |
| WPAN | Wireless Personal Area Network |
| WSN | Wireless Sensor Network |

# Chapter 1
# Introduction

Healthcare is seeing dramatic increases in cost and reductions in quality of service (QoS) globally [1]. Additionally, the number of healthcare workers per patient is decreasing [2]. With both of these issues escalating, the need to cut costs and maximize professional health resources is necessary. A trend that is emerging is alternate care delivery [1] or non-conventional models of care. One such alternative brings added convenience to both patients and healthcare professionals alike with the hopes of alleviating the stress and burden on healthcare systems. This is the idea of Home Health aided by innovative e-healthcare, tele-health, and m-health (mobile-health) ideas. By employing tele-monitoring and home monitoring techniques, healthcare can be brought into the home of the patient achieving consistent care and assisting with national goals for early diagnosis, disease prevention, and preserving healthcare resources.

Significant research has been conducted to miniaturize semiconductors and scale back costs. Additionally, wireless and energy technologies have seen similar advances [3]. With this, pervasive networks, and more specifically wireless sensor networks (WSNs), are becoming a wide spread reality. A range of applications for WSNs has been proposed, however, one of the most significant and likely to have a huge benefit to our quality of life is that of Body Area Networks (BANs). They are also known as Body Sensor Networks (BSNs), Body Area Sensor Networks (BASN) or simply, Body Networks (BN). Sensor nodes are placed in, on, or around a patient to monitor his or her physiological, behavioral and contextual data [3][4]. These interconnected sensors together form the BAN and give health care professionals the opportunity to remotely monitor their patients.

Recent studies have shown that Home Health applications will be growing at a significant rate of 180% annually and will become a multi-billion dollar industry over the course of a few short years [5]. With the added emerging healthcare reforms, research in BANs will only continue to develop. However, there still exist a number of issues that require attention in order for BANs to be widely accepted and widely adopted. These include the following [4]:

1. Design elements of BANs
    a. Network Design
    b. Wearability Design
2. Data and Sensor Integration
3. Reliable Communications
4. Patient Privacy

Not only do technical elements have to be addressed (i.e.: Sensor design, energy demands) but also that of patient comfort. BANs are meant to continuously monitor the health of patients. As such, BANs will be an integral part of a patient's lifestyle. In order for patients to accept such a technology, BANs will need to be minimally invasive and intrusive biologically and physically. They should have a minimal effect on patient behaviors and activities. Additionally, when considering healthcare, one is dealing with sensitive and confidential information. Additional security measures will need to be adopted to ensure this privacy.

However, looking beyond the sensor and actuators nodes in the BAN, one arrives at the link between the BAN and the healthcare server, hospital, emergency services, etc. (or Issue 3 - Reliable Communications). Patient monitoring can be a very time sensitive application when dealing with acutely or chronically ill, elderly, or remote patients. A continuous communication link ensures that the data received by health care services is not delayed. Delays in physiological information can have severe consequences and in some cases, even fatal. For example, if a chronically ill patient has a medical emergency, his or her BAN can notify emergency services. With any delays in communication of this information, the patient may not receive care in time. In this thesis, we investigate the use of a multi-radio communications protocol connecting a BAN to external communication infrastructure to achieve a higher connectivity time.

The rest of the introduction is grouped into sections highlighting each of the following: Outline of BANs, Research and Motivation, Definition of Dependability and the Organization of Thesis.

## 1.1 Outline of BANs

Very similar to WSNs, recent advancements in wireless technologies have prompted researchers and industries to take notice of BANs. Advancements in biosensors have further made the realization of BANs more feasible [6]. While much research has been conducted for WSNs, BANs still face unique issues. To further understand this, a BAN model and the differences between WSN and BAN are outlined.

***Table 1.1: Examples of Sensor and Actuators for BANs***

| Sensors/Actuators [7] [8] | Physiological Parameter |
|---|---|
| Accelerometer | Movement, Position |
| Blood Pressure (BP) | Systolic, Diastolic BP |
| $CO_2/O_2$ Sensor | Respiration and Oxygen Concentration |
| Drug Delivery | Drug injection (specific to ailment) |
| ECG | Heart Activity |
| EEG | Electrical Brain Activity |
| EMG | Electrical Muscle Activity |
| Glucometer | Blood Glucose |
| Gyroscope | Movement, Position |
| MMO pH | Body and Blood pH |
| Pulse Oximetry | Respiration |
| Thermistor | Body Temperature |

A BAN consists of a network of small sensor or actuator nodes either implanted or attached to the body. Each of these sensor nodes is then capable of establishing a link – wired or wireless – with other nodes. Some examples of these sensor and actuators nodes and the physiological parameter they monitor are presented in Table 1.1. They are strategically placed and chosen to monitor a patient's health status and movements. Each of these sensors generates physiological data at different data rates. For example, an accelerometer or gyroscope would have a high data rate to reflect constant human movement whereas a thermistor would have a lower rate, as body temperature does not fluctuate as much. To some degree, some of the sensors and actuators in a BAN are

controllable and/or programmable. For example, a cardiologist will regulate a cardiac pacemaker to select the optimized heart rate for the patient. Similarly, drug delivery systems can be adjusted to control timing and dosage.

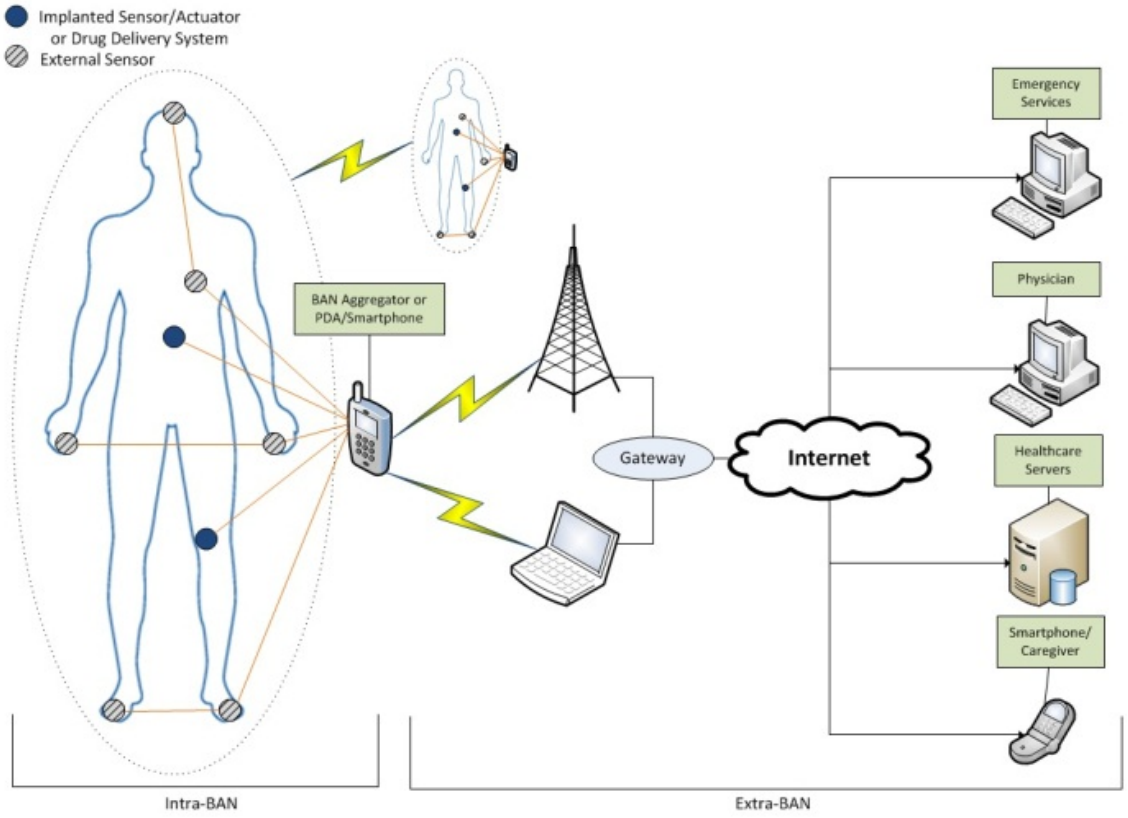


***Figure 1.1: General BAN Architecture with Communications Systems***

Once the sensors collect the patient's information, the data is sent through a radio or wired interface to a personal BAN Aggregator or Smartphone. Depending on the long-range communication capability of the sensor devices, the aggregator can be bypassed and the sensors can forward their information directly to radio Access Points (APs). The aggregator acts as the as the gateway between the Intra-BAN and Extra-BAN networks and local base for security (encryption, authentication) and data fusion techniques [7]. Figure 1.1 illustrates an overall structure of a BAN including sensors and/or actuators, BAN aggregator and external communication infrastructure similar to the generic models

presented in [7] and [9]. The Intra-BAN network consists of the inter-networked implanted or external sensor nodes and the aggregator device. Typically a short-range, low-rate, ubiquitous communication standard, like Zigbee (supported by IEEE 802.15.4), is used for Intra-BAN communications [7]. The extra-BAN network includes all communication infrastructure connecting the BAN aggregator to a destination healthcare provider, server, or device. This division of the structure into the Intra and Extra-BAN networks allows for simpler analysis of each sub-section or the system as a whole.

The wide range of applications for WSNs include environmental and equipment monitoring, industrial and structural monitoring, and military or remote location exploration [3]. However, the human body poses unique challenges for BANs in the medical application context. When compared to a WSN, a BAN differs in the following different ways [3], [7]:

1. *Density:* BAN nodes are usually limited and are placed throughout and on the body. This introduces new issues such as body shadowing and biocompatibility. WSN nodes are usually deployed in large numbers to cover a larger area. There are often redundant sensor nodes to achieve higher levels of accuracy with nodes failures.
2. *Dynamics:* Once deployed, WSNs are usually stationary whereas a BAN is as mobile as its user. Additionally, WSNs can be subjected to extreme weather or noise conditions. BANs are kept in the same environment that humans are exposed to. This working environment is much more limited than that of a WSN. However, the human body poses new environmental challenges for BAN developers.

3. *Security:* Patient information is highly sensitive and requires encryption and authentication schemes to protect it.
4. *Data Transfer:* WSNs usually deploy a high number of redundant nodes to record events that can occur at random times. BANs, on the other hand, have fewer nodes to maintain data accuracy and are usually recording physiological parameters continuously with stable monitoring rates.
5. *Power:* Depending on the application, WSN nodes can be deployed with the intent of not being recovered or in an accessible environment. Consequently, power demand and supply can vary. Replacing power supplies on BAN nodes is easier with the exception of implanted sensors.

A number of applications, especially home health or mobile health applications [10], have a lot to gain from BANs. This can also include military, gaming and fitness applications [7]. When considering these possible aplications, data transfer latency is not usually acceptable in BANs. Real-time monitoring is critical to the user or health of the patient. A dependable BAN should provide reliable and secure data transfers.

## 1.2 Definition of Dependability

A dependable system is one that a user can trust and rely on. We define a system as dependable if it is reliable or consistently operating in the same fashion [11-12]. The six aspects that create a foundation for dependable behavior are [13]:

- Reliability
- Availability
- Maintainability
- Safety

- Confidentiality
- Integrity

These can be summarized as a conjunction of three main facets of dependability: security, availability and reliability. A BAN needs to be able to maintain a continuous connection, prevent faults or recover from an outage in a timely fashion while still maintaining high security for sensitive patient or user data.

Increasing the dependability of BANs is addressed in various different ways. Dependability solutions or improvements can extend throughout the entire BAN structure illustrated in Figure 1.1 or within the Intra/Extra-BAN network. Various exemplary dependability schemes that cover security, availability and reliability will be outlined in Chapter 2.

## 1.3 Research and Motivation

BANs have significant opportunities for advancements in a number of domains including sensor miniaturization, signal processing, context aware processing, communications and storage [14]. With respect to communications, by enabling the sensors with long-range communication capabilities to bypass the aggregator, a single-hop link between each sensor and AP is established, but at the cost of power consumption. When sensors communicate with the local aggregator, this creates a shorter communication distance required by the sensors and preserves power. This smaller transmit power is also advantageous to prevent any harmful effects of electromagnetic radiation. However, the aggregator becomes the single point of contact between the Intra- and Extra-BAN networks. Smartphones and/or PDAs can serve as aggregator and have the added benefit of multiple radio interfaces. Through this multi-radio interface, one can

increase the path diversity [15]. With respect to the BAN structure outlined in Figure 1.1, if one link from the aggregator to the extra-BAN network fails or is unavailable, a secondary radio may provide a communication link or path to its destination.

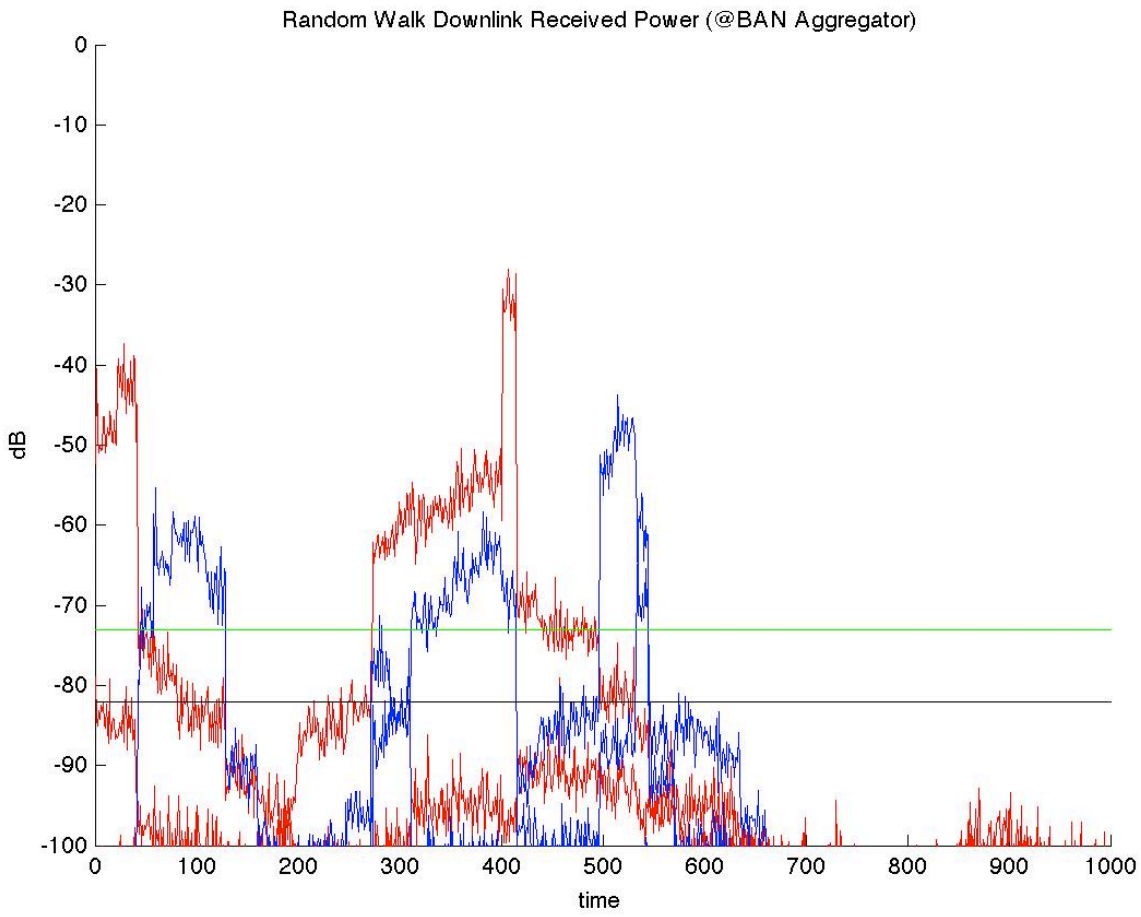


***Figure 1.2: Single Simulation DL Received Power***

*Wi-Fi Received Power at Aggregator in red with corresponding green receiver sensitivity, Bluetooth received Power in Blue with corresponding black receiver sensitivity at the Aggregator. This plot shows some exemplary times when the system can profit from a second radio. For example, at approximately times 50-100 and again at about 500-550.*

Our research is motivated by the idea of multi radio diversity in an aggregator to provide a continuous wireless communication link between the Intra- and Extra-BAN networks. The contributions of this thesis will be a multi-radio protocol that switches between a primary Wi-Fi (IEEE 802.11) and secondary Bluetooth (IEEE 802.15.1) at an aggregator node to increase the availability of a wireless link for a BAN. A variety of

different variables will be explored and simulated such as walk patterns, switching thresholds, and AP placement in Chapter 3.

## 1.4 Thesis Organization

The remaining portions of this thesis are organized as follows. Chapter 2 will provide background information on communication standards used for design of the contributed protocol (Wi-Fi and Bluetooth) as well as other potential standards. Additionally, related works on multi-radio diversity and interfacing and some schemes on increasing dependability in BANs will be presented. Chapter 3 will outline the potential and selected models used for simulation of the network behavior required. This will include human mobility models, wireless link models, AP placement and the inter-radio handover model. With that, an overall simulation system model will be presented. Chapter 4 will analyze all simulation results for varying parameters and simulation networks. Finally, future directions for research and a conclusive summary will be presented in Chapter 5.

# Chapter 2
# Background & Related Works

In order to introduce the idea of improving dependability of BANs through a multi-radio aggregator interface, background and related works are presented in this chapter. First, an overview of different wireless protocols is reviewed. Second, some technical schemes to improve the dependability (security, reliability or availability) of BANs are mentioned and classified. Last, related works on the use of multi-radio interfaces in wireless communications is presented. As a whole, these introduce the main goals of this thesis as presented in Chapter 1.

## 2.1 Wireless Protocol Overview

Wireless networking is a fast growing field enabling significant mobility and flexibility in user devices, sensors and various other technologies. A number of different protocols are readily available and have become the norm in wireless networking. These range in application due to their variation in range, security, capacity, and power

consumption [16]. Long-range communications include satellite and cellular communications. Cellular communications have recently encompassed data networks including the more traditional voice networks. These include such protocols as GSM, CDMA, LTE, HSPA, etc. On the other hand, short-range communications include more localized networks. They are predominately one of four different protocols: Wi-Fi, Bluetooth, Zigbee, and Ultra Wide Band (UWB) [16].

Within the short-range and long-range categories, different protocols can operate in different frequency bands all determined by the corresponding IEEE working groups and standards. This helps to minimize the interference these communication protocols may have on one another. This also lends itself well for multi-radio interfacing if a given connection is experiencing interference, cross talk or noise. This will be further discussed in Section 2.3. The remainder of this section will provide overviews of these protocols, their differences, and our motivation for their selection for the simulation.

### 2.1.1 IEEE 802.11: Wi-Fi

Wi-Fi or Wireless Fidelity is a set of standards to establish a Wireless Local Area Network (WLAN). It is primarily a substitute for cabled LANs and for quick connectivity for mobile and notebook devices [17]. This makes it a convenient option for home, business and public networks for Internet connectivity.

The IEEE working standard for 802.11 defines the MAC and PHY layers for transmissions in the 2.4GHz and 5GHz range with varying signal rates[18]. A Wi-Fi network could be ad-hoc or structured. An ad-hoc network would be considered an Independent Basic Service Set (IBSS) and include a few Wi-Fi enabled stations with no added or supporting communication infrastructure. A structured network or Basic Service

Set (BSS) would include mobile stations, access points (APs) and any other various communication structures. Each BSS would be the equivalent of a cell and these cells can be interconnected to form an Extended Service Set (ESS). Through a distribution system, whether a supportive cabled or wireless network, the BSSs form a wider ESS network. The distribution system connects the APs of each of the BSSs to each other. Through this, mobile users can migrate throughout the wider network with only having to reassociate to another AP. Within the ESS there can also be portals to link the WLAN to separate cabled LAN to increase the breadth of the network [17].

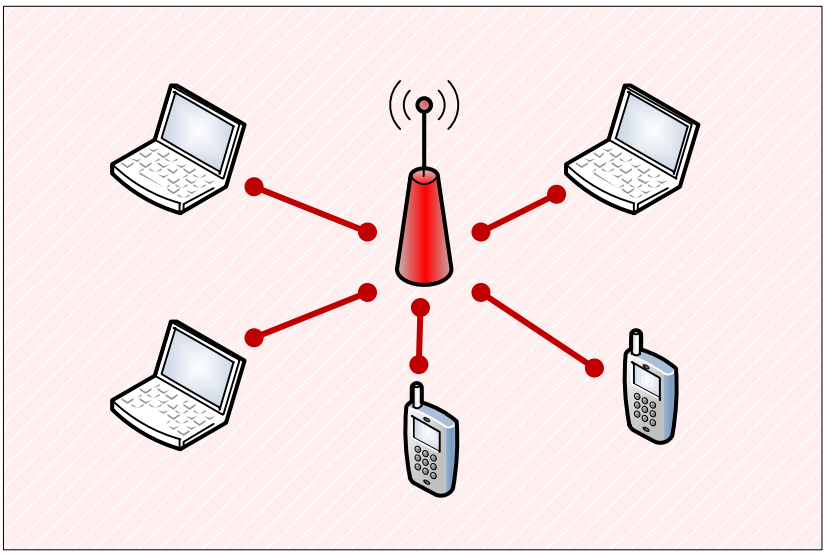


***Figure 2.1: A Wi-Fi BSS or Basic Service Set***

A Distributed Coordination Function (DCF) dictates the accessibility of the transmission medium in IEEE 802.11 [16][17][22]. The number of available channels on a given bandwidth is limited (as is the case for more wireless standards) and needs to be

regulated and multiplexed for optimal usage. The DCF function employs the following [18]:

1. Collision Avoidance using Carrier Sense Multiple Access (CSMA/CA): In an effort to prevent collisions, the DCF function employs CSMA/CA to ensure non-overlapping transmissions. When a mobile or fixed station in a service set wants to transmit, it listens to a channel for a predefined amount of time (DIFS). If the channel is busy, the station waits a random Backoff Time before reattempting. If the channel is available, if continues with its transmission.
2. Request and Clear to send (RTS, CTS): The RTS and CTS frames are exchanged between communication stations in the service set prior to the actual data frame. This, in a sense, 'announces' to nearby stations that the channel medium is in use. While this can seem like extraneous overhead for smaller data frames, it does provide a collision and transmission path assurance prior to transmitting longer frames. It is also an optional feature to implement.
3. Positive Acknowledgement (ACK): When a data frame is received, the destination station sends a positive acknowledgement message to the source.

An additional and optional Point Coordination Function (PCF) for infrastructured WLANs uses a Point Coordinator (PC) to control the communications. Contention is avoided by the PC polling each station for data in the service set. Therefore, it is a more centralized scheme with the PC having continuous access to the channel mediums.

When a station enters a network. It begins by sending Probe REQs to identify nearby stations and APs. Once an appropriate network is found, the station then associates and authenticates through the exchange of a series of REQ and RSP frames. Once associated with a network, the station is now connected and data exchange can

begin subject to the functions established by the DCF. If for any reason (interference, movement away from AP, etc.) the station loses it's connection, it can reassociate to the same network as dictated by the distribution system by probing for a new AP to connect to. There are intermittent beaconing frames sent out in a BSS by the APs to maintain synchronicity within the cell. Finally, a station can go into a power save mode or completely disassociate from the network if need be.

***Table 2.1: Wi-Fi Frame Categorization and Rates***

| Frame Type | Includes… | Data Rates (Mbps) |
|---|---|---|
| Control | RTS, ACK, CTS | 1, 2 |
| Management | Association, Authentication, Beacon, Reassociation, Disassociation, Deauthentication, Probe | See IEEE 802.11 Rate Table (Table 2.2) |
| Data | Data to and from BAN | See IEEE 802.11 Rate Table (Table 2.2) |

***Table 2.2: IEEE 802.11 Rate Table***

| Standard | Data Rates (Mbps) |
|---|---|
| IEEE 802.11a | 6, 9, 12, 18, 24, 36, 48, 54 |
| IEEE 802.11b | 5.5, 11 |
| IEEE 802.11g | 6, 9, 12, 18, 24, 36, 48, 54 |
| IEEE 802.11n (20MHz) | 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 |
| IEEE 802.11n (40MHz) | 15, 30, 45, 60, 90, 120, 135, 150 |

The link setup is managed by the MAC and Logical Link Control (LLC) layers in the Wi-Fi Protocol stack [18]. Therefore, this makes for the easier reassociations as mentioned earlier [17].

### 2.1.2 IEEE 802.15.1: Bluetooth

Unlike Wi-Fi, Bluetooth is intended for even shorter-range communication and low power devices. Bluetooth connectivity is becoming a standard in mobile devices, automobiles, computers, and various other household and consumer gadgets.

Bluetooth operates in the 2.4GHz band and at distances ranging from 1m to 100m depending on the class of device [16] [17] [19] [20]. A Bluetooth device connects to a piconet (or a network of up to 8 devices – 1 master with 7 active slaves) as a master or a slave. A number of different piconets can form a scatternet with a single station serving as a master in a maximum of 1 piconet. It can remain in slave mode in several other piconets. Multi-hop connections can then link several stations together wirelessly or a Bluetooth AP station can serve as a gateway into another type of network.

There are two different types of links that can be established via Bluetooth. These are Asynchronous Connectionless Links (ACLs) or Synchronous Connection-Oriented Links (SCOs) [17]. SCOs, typically used for information such as voice and streaming, provide direct master to slave (point-to-point) link with a constant data rate (synchronous). The master and slave then transmit their data on reserved time slots preventing any collisions. ACLs, on the other hand, are unreserved. A master can then exchange packets with any slave on a need basis. A connection is always explicitly established for an ACL link and is disconnected after a default 20-second timeout period. To maintain integrity, an automatic retransmission would be initiated if no ACK signal were received during an ACL transmission.

When a station enters a network, it can operate as a master by establishing a piconet or join an existing piconet as a slave device. If it assumes the role of a master device, it begins sending out inquiries to nearby devices to respond. If it is in slave mode, it will listen for these inquiries. This inquiry request and response is an exchange of addresses between the two devices. Following the inquiry stage, the master then pages a device to begin link setup. A slave responds to a page from a master device with it's own

unique address identifier in it. The master then sends an FHS packet with vital master clock information. Once the slave acknowledges the FHS packet, the two devices are connected. If the slave does not receive the FHS packet after a timeout duration, they return to the paging state [19].

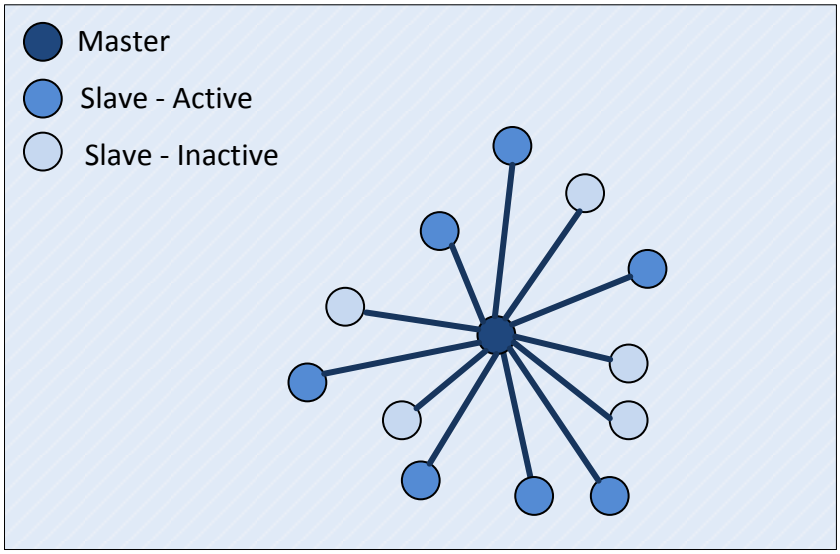


***Figure 2.2: Bluetooth Piconet with single Master and various Slave devices***

Once connected, the master then schedules data transmissions according to whether or not the link established is an ACL or SCO link and both follow a Frequency Hopping Spread Spectrum (FHSS) for channel access. This FHSS pattern is dictated by a sequence generated in part by the master clock and address. When not active, the devices can go into one of three power saving modes:

1. Park: When a device is 'parked', it still remains synchronized to the piconet. However, they do surrender their unique addresses prior to going into this power save mode.

2. Sniff: A device in sniff mode remains synchronized within the piconet. However its duty cycle is lowered and thus activity within the piconet is lowered.
3. Hold: The hold power save state is generally used when there are 'black-out' periods with no data or voice to transfer for a certain period of time.

Bluetooth makes for a convenient standard for various Input/Output (I/O) devices (such as mice and keyboards) and mobile phone headsets. However, its long device discovery time can be a disadvantage.

### 2.1.3 Other Standards (Zigbee, UWB, WAN)

Zigbee is an emerging wireless standard focused on low-cost, low-rate, and low-power devices. It's designed to work within a nominal range of approximately 10m and hence suited for Wireless Personal Area Network (WPAN) or Low Rate WPAN (LR-WPAN or IEEE 802.15.4) applications [16]. Within the context of a BAN, this could include the Intra-BAN network of sensor nodes placed on or implanted in the human body.

Like Bluetooth, Zigbee also operates on the global 2.4GHz frequency band at a maximum rate of approximately 250 kbps [21]. Within a Zigbee network, there are two different types of devices: a Full-Function Device (FFD) and Reduced-Function Device (RFD). An FFD can serve as a PAN Coordinator, a simple coordinator, or as an active device. A PAN Coordinator may establish it's own network, control devices entering the network, and provide synchronization control to coordinators and RFDs in the network. There can be at most one PAN Coordinator per network. Because of these tasks, a PAN Coordinator is usually the most computationally capable device especially considering the simplicity of devices using the Zigbee protocol [16]. An RFD device may only

communicate with a single FFD device. For this reason, RFDs are usually very simple low-rate devices such as a thermistor or pH sensor in a BAN.

Ultra Wide Band, or IEEE 802.15.3, is another standard for WPANs with a higher data rate. With the current need for multi-media streaming, UWB is emerging as a potential standard for short-range, high-rate communications [16]. In contrast to some of the other wireless standards presented, UWB operates in a wide frequency band from 3.1-10.6GHz and has one of the highest maximum signal rates at 110 Mbps. However, this comes at a nominal range of 10m, which is well within the personal operating range. Similar to Bluetooth, UWB using a FHSS to prevent collisions and builds a piconet of up to 8 devices (including a single master device).

Long-range communications are becoming more important in daily lives as people become more mobile and connected. Telecommunication networks are becoming more sophisticated to handle higher data rates for mobile and wireless broadband applications. A number of criteria need to be considered when designing a mobile network. These include high data rates, low latency, adequate coverage, and QoS [23]. Dropped or blocked connections need to be minimized in order to maintain a high QoS. One way that mobile protocols have been increasing data rates is by using higher order modulation schemes. Advanced antenna systems have also enabled higher coverage areas and higher network capacity.

An emerging protocol that is becoming commercially available and implemented is High Speed Packet Access (HSPA) [23]. HSPA, or 3.5G, is an upgrade to an already available UMTS network offering Downlink (DL) and Uplink (UL) data rates of up to

approximately 14Mbps and 5.76Mbps respectively. However, with all cellular or mobile networks, voice calls take precedence over data transfers.

### 2.1.4 Comparison & Simulation Selection

The following table outlines the protocols described in the previous section for a discussion about similarities and differences [16] [17] [18] [19] [21] [23].

***Table 2.3: Protocol Overview and Comparison***

| Protocol | Wi-Fi | Bluetooth | Zigbee | UWB | W-CDMA HSPA |
|---|---|---|---|---|---|
| ***Standard*** | IEEE 802.11n | IEEE 802.15.1 | IEEE 802.15.4 | IEEE 802.15.3a | 3GPP – Release 7 |
| ***Frequency Band*** | 2.4 / 5 GHz | 2.4 GHz | 2.4 GHz | 3.1-10.6 GHz | UL 1885-2025 MHz<br>DL 2110-2200 MHz |
| ***Number of Channels*** | 14 | 79 | 16 | 1-15 | 98 |
| ***Channel Bandwidth*** | 20/40MHz | 1MHz | 2MHz | 500 MHz – 7.5GHz | 5MHz |
| ***Nominal Range*** | 100m | Class 1 100m<br>Class 2 10m<br>Class 3 1m | 10m | 10m | 1-10km* |
| ***Nominal Transmit Power*** | 10-20dBm | 0-10dBm | -25 – 0 dBm | -41.3 dBm/MHz | ~20dBm with 0.5,1,1.5,2 dB power control steps ** |
| ***Maximum Data Rate*** | 20MHz 300Mbps<br>40MHz 600Mbps | 1Mbps | 250Kbps | 110Mbps | UL 5.76Mbps<br>DL 14Mbps |
| ***Basic Cell*** | BSS | Piconet | Star | Piconet | RAN (MS, BS) |

** The range of a cellular base station depends on surrounding terrain and interference. A typical cellular station will get several of kilometers of coverage.*
*** Power Steps for Class 4 Mobile Device (typical to common cell phones and smartphones)*

When selecting two wireless protocols for this thesis, a number of criteria needed to be met. First off, we wanted to select two protocols that operate in different frequency bands. If both interfaces were operating in the same band, interference could potentially

affect both. For example, if Bluetooth and Zigbee were selected and the 2.4GHz band were subject to significant interference for a period of time, both interfaces would be useless hence eliminating the benefits of a multi-radio interface. Second, we wanted to select protocols that were common in mobile devices today. This includes Wi-Fi, Bluetooth and HSPA (or another cellular data interface). However, most people have access to Wi-Fi networks within their home or workplace, which is where they spend most of their time. So we select Wi-Fi as the primary interface. For the sake of having a secondary low-power, low-rate interface, Bluetooth is a convenient option. Also, there exist some mobile entertainment devices, vehicles, and household goods that do not necessarily have cellular capabilities, but do have Bluetooth capabilities.

A BAN equipped with a single-radio interface will continually transmit physiological data over the primary wireless interface (in this case, Wi-Fi) until the signal is lost. At this point, the BAN has lost its end-to-end connection with its destination. All data accumulated during that time would buffer at the aggregator waiting for the link to be re-established. However, by doing this, real-time patient monitoring is lost for a potentially long duration. A dual-radio or multi-radio interface would offer a secondary option for the BAN aggregator to transmit data thus increasing the throughput and maintaining the real-time monitoring.

## 2.2 Dependability in BANs

Referring back to section 1.2, the definition of dependability can be summarized as a system that consistently behaves in a manner to provide reliable and secure communications with a high level of availability. With real-time patient monitoring, the ideal situation would be to have an end-to-end BAN to destination connection available

100% of the time. But considering how mobile users are and how dynamic communication networks can be, 100% availability becomes increasingly difficult to achieve.

This section will be devoted to identifying and classifying potential failure modes in BANs and presenting related works dedicated to improving dependability in one or more of the categories identified in Section 1.2 (reliability, availability, maintainability, safety, confidentiality, and integrity).

### 2.2.1 BAN Modes of Failure

Depending on the application context of the BAN, certain properties of dependability may be more significant than others [24]. For example, a patient who relies on a BAN for automating insulin delivery to regulate their diabetes may need an extremely secure and powerful network. Any device failure in the drug delivery system could have disastrous effects. A BAN designed for monitoring athletes however may not need the same scrutiny in the design but may require advanced context processing and be more susceptible to motion changes causing changes in topology or interference.

A BAN can fail in numerous different ways that can be classified into two categories: permanent or transient failures [25]. Permanent failures are just that – failures that a BAN cannot recover from. Transient failures can occur numerous times and gradually with the potential for recovery. A BAN mode of failure is any type of failure within the entire system (Figure 1.1) that causes a disturbance in information access, security, and/or end-to-end communications [26]. The following are the definitions and effects of the different modes of failure [24] [26]:

1. Node Failure

   A node failure can be either a permanent or transient failure. A node that has had a hardware or software failure preventing it from operating altogether would be considered a permanent failure. Whereas an unresponsive node or a node on standby could respond in the future which then categorizes this as a transient failure. Within WSNs, node failures are usually resolved by initiating a new path discovery. Alternatively, if redundant paths exist, the WSN can recover from a node failure by finding an alternate route to the destination. However, with a BAN, there are usually only very few (sometimes even one) nodes monitoring a single physiological parameter. This is due to a design decision to keep the BAN minimally intrusive on the patients' lifestyle. Due to this fact, a node failure could then result in the loss of necessary and vital physiological information.

   With WSNs and BANs alike, a node failure usually results in topology and path changes if there are multi-hop paths from node-to-node in WSN and node-to-aggregator in BAN. With this comes the potential for isolating nodes or parts of the network if a critical path node should fail. However if other paths do exist, they may come at the expense of longer delays.

2. Node Removal

   Node removals are always permanent failures within a BAN. Sensor nodes may fall of if they are not secured to the patient properly. On the other hand, nodes may be intentionally removed if they are no longer needed. In both cases, whether removal is intentional or not, a node removal has similar effects as a node failure. A loss of physiological information, potential for isolating nodes and longer delays can occur as a

result.

3. BAN Compromise / Lack of Security

   Because of the nature of BANs, an attack (whether passive or active, permanent or transient) could cause serious harm. A passive attack is one in which the attacker may just collect or monitor data from the BAN. An active attack is a much more serious one. The attacker may re-route data transmissions, modify information, or even seek to control actuators by sending appropriate signals. Patient health is extremely sensitive and adequate security measures need to be put in place before a BAN is deployed.

   With either type of attack, we have confidential information leaking to an unauthorized third party. This is unacceptable by any health information standards. However, a more serious consequence is that of physiological harm. If an attacker takes an active approach to controlling actuators within a BAN, they can cause the patient fatal harm. Any control over a drug delivery system, cardiac pace maker, or similar actuator would have serious effects. Alternatively, an attacker can modify physiological information sent to a healthcare database, physician or emergency services provoking any unnecessary alarm, neglect or emergency response.

4. Limited or Failed BAN Aggregator

   In Figure 1.1, the BAN aggregator serves two main purposes: it is the central processing unit of the intra-BAN network and serves as the single point of contact between intra-BAN and extra-BAN networks. A limited aggregator could be one that has less processing capability than needed or an inadequate transceiver for data transmission causing data loss. A failed BAN could be one with a hardware or software failure. In both cases, the failure or lack of capability would be a permanent problem. A limited or failed

BAN could then create serious bottleneck situations or a single point failure isolating the patient from their healthcare providers. An aggregator with lower capability than needed, can also affect the system from a security standpoint. With lower processing capability, less complex security mechanisms can be used which may make the BAN vulnerable to attacks.

5. Sensor Interference

   Interference remains a critical issue with any type of wireless communications. Within a BAN, sensor devices can affect each other unintentionally. A congested intra-BAN network and neighboring high power sensors can both cause interference. This can cause data integrity issues as well as packet disruptions, delays or losses as sensors continually try to retransmit. However, this can be considered a transient failure as it can pass with time.

6. Environmental Interference

   Not only can neighboring sensors interfere with each other, but certain environments can disrupt signal transmissions within the BAN. Similar to sensor interference, other high power devices within the region of the BAN could cause data integrity issues. Additionally, signal attenuation, obstructions, and fading are always a factor when dealing with wireless communication. Perfect line of sight communication is never a reality and obstacles must be accounted for. One of these obstacles within the intra-BAN network is actually the human body. The human body challenges wireless BAN designers by posing two main challenges: movement and signal attenuation [14]. The body has the property to attenuate and even absorb RF signals and the added movement only adds more variability to this path loss.

7. Limited or Loss of Power

   Power sources and batteries are usually the heaviest portion of a mobile node [27]. However, there is a tradeoff between the weight of a battery and the power supply available to the node. Having a smaller battery may seem lighter and more convenient, but having to frequently charge or replace the batteries may cause a nuisance. Additionally, a lot of power is consumed by transceivers. Wireless communications do expend significant power for the sake of having no interfering wires or cables. Charging batteries may not be an inconvenience for external sensors, however, with the lack of access posed by internal or implanted sensors, it is up to the doctor and patient to form a rigorous battery management schedule to replace critical power sources before failure.

   If a device in the BAN fails due to power, this can be classified as a permanent failure under the assumption that in the near future, the device will not be charged. Once this happens, we can also say that this would cause the same effects as node removal because essentially this is the similar to unintentionally removing a node from the network. If that node happened to be the aggregator, one could be facing more serious effects of signal point failure as pointed out in Issue 4. Otherwise, with the loss of a node comes the loss of necessary physiological information. The network dynamics also change as it undergoes topology changes and potentially isolate segments of the network.

8. Loss of Connectivity/Network Failure

   End-to-end communications are essential for real-time monitoring in BANs. Path diversity is important to maintain this idea. However, loss of connectivity should always be accounted for due to the fact that BAN user mobility can be highly variable. A user may move into a region where no access points are within range or in the line of sight. This can isolate the intra-BAN network from the extra-BAN network causing the loss of

data and real-time monitoring. At this point, the Aggregator would have to search for another path to transmit the data or resort to buffering the information and prioritizing critical packets once communications are resumed. While this is a transient failure, transceiver damage or failure can cause longer and more permanent failure. Furthermore, network interruptions (such as scheduled maintenance) can also cause longer periods of failure.

9. Overload or Network Congestion

   Some biosensors have higher than usual sampling data rates. These sensors usually are monitoring a highly variable physiological parameter such as brain activity through an ECG monitor. This has the potential for creating huge amounts of data leading to an overloaded aggregator. When the aggregator has to deal with large amounts of data, this can cause delays in transmission and buffer overflows if transmissions are not scheduled accordingly. Furthermore, a larger number of intra-BAN transmissions could also be causing more collisions in the overloaded network. While it is important to monitor physiological parameters, it is also just as important to realize the capabilities of the BAN and not over-commit any of the resources as it can have counter-productive effects.

10. Compatibility, Interoperability, and Sensor Heterogeneity

    The IEEE 802.15 is a working group dedicated to the standardization of WPANs. Within this is the IEEE 802.15.6 task group focusing on BAN technologies [28]. While not a lot of information is readily available for this task group, the lack of harmonious standards, regulations, and licensed bands is deterring users from adopting BANs. With a number of wireless standards such as Bluetooth, Wi-Fi, Zigbee, etc. all operating within the same unlicensed band, interference becomes a major obstacle to overcome.

### 2.2.2 Techniques to Improve Dependability in BANs

While BANs do fit under the category of a WSN, certain existing mechanisms for higher dependability in for WSNs and even other wired/wireless networks may not apply. BANs are as dynamic as a human in motion and vary from WSNs in the five ways outlined in Section 1.1 – density, dynamics, security, data-transfers and power. This section will outline some exemplary attempts to increase dependability in BANs by addressing one or more of the BAN modes of failure. Each issue will be addressed individually again with the exception of Node Failure and Removal and Network Congestion and Failure. They are grouped together as solutions to each are typically applicable to the other.

1. Node Failure and Removal

   The small radius of the intra-BAN network surround the body spans approximately 2 meters. This small distance already facilitates creating path diversity within the intra-BAN network. Because sensors are generally very close to one another and the aggregator, isolating nodes due to node failure or removal can be rare. However, strategic placement of sensor nodes can overcome this. But when a node fails, the loss of the physiological data retrieved from that node becomes an issue. The easiest way to overcome this is the use of redundant sensors [3] [29] [31]. Not only can they serve as a second source of critical information, using multi-sensor data fusion techniques, the information generated from redundant sensors can be averaged together for higher sensing accuracy and precision. This added benefit comes at two significant costs. The first being the monetary cost of the additional sensors. Depending on the type of sensor, this cost can be expensive. The second cost is related to convenience. Additional sensors mounted externally or implanted within a patient add extra weight burden and can hinder

movement. This can affect the patients' lifestyle. Therefore there is a subtle balance between designing a BAN for a patients' lifestyle and to gather all necessary information.

One way to work around additional sensors is by using already available sensors. Mobile devices (especially smartphones) are being equipped with more and more sensors each day, including GPS modules and gyroscopes and accelerometers for gaming [30]. Local and context processing can easily be integrated within a BAN aggregator equipped with similar sensors. This leaves the high rate motion monitoring to a more capable aggregator. This does add an extra power burden on the aggregator. However, an aggregator is an external device and the patient can easily charge the device making this a feasible option.

2. BAN Compromise/Lack of Security

Safety and privacy are crucial for BANs, especially those dealing with healthcare patients. Similar to the previous section, additional sensors would protect a BAN if one of the nodes happened to be compromised [29]. The redundant sensors would provide a backup should this happen. Similarly, data replication (at a different node other than the one that created the information) could also serve as a backup [32].

However, when backing up data at the cost of extra hardware is not an option, more elaborate techniques such as frequency hopping [31], encryption and authentication [7] [31] [32] [33], and biometrics and/or RFID [6] [7] could be implemented. Similar to that employed in Bluetooth, frequency hopping protects data transmission by switching channels according to a pseudorandom sequence. This sequence is known by only the transmitter and receiver and, in essence, is their protection. The biggest challenge when employing frequency hopping is the synchronization between both communicating nodes.

This can be done with an extra message exchange during establishing a link if both nodes have frequency hopping tables to follow. If this is not an option, it may take extra time for the both nodes to locate each other by randomly selecting the same channel.

Encryption and authentication requires additional steps as well but then provides assurance for both data integrity and node integrity. In [33], three common security mechanisms are proposed. AES or Advanced Encryption System is an encryption standard used globally that protects data by combining non-linear substitutions, shifts and transformations. For encryption only, AES-CTR is used which uses a counter to create the encrypted data (or cipher text) using the various transformations on blocks of data. For authentication only, AES-CBC can be used. CBC or cipher block chaining is another transformation on node data that uses previous node data to encrypt current data. Last, if both encryption and authentication are required, a combination AES-CCM (CTR and CBC Mode) can be employed at the cost of additional complexity.

A non-conventional approach to security is that of integrated biometrics and RFID [6] [7]. Biometrics recognizes a user by a physical trait such as a fingerprint or retina scan. For authentication through biometrics, additional hardware is required and can sometimes be extremely costly. While not perfect yet, they still are potential options for security in BANs.

In order to best understand threats to security on BANs, one can entice attacks. By using ‘honeypots’ [12], one lures an attacker into an unprotected network to expose weak points in the system. While not a solution to a security problem, it can help with validating new ideas and discovering new threats.

3. Limited or Failed BAN Aggregator

An aggregator usually serves two purposes as mentioned earlier: single point between intra-BAN and extra-BAN networks and a point for data fusion, security, and any other computationally complex processing. However, an aggregator may have a limited processor, power supply or transceiver. One way to overcome this challenge is by implementing a star-mesh intra-BAN network topology [9]. This can limit the communications from the aggregator to only nodes that are cluster heads. These cluster head nodes would then need sensing and minor aggregating capabilities to run application middle-ware [13].

Another option is managing and scheduling transmissions from the aggregator [7] [31]. With transmission scheduling, the aggregator would manage when to transmit data depending on the priority. Time sensitive information would be transmitted right away whereas less critical information would be held for a period of time to schedule an efficient transmission. This may eliminate the real-time monitoring aspect of a BAN, but could be feasible with lower data rates.

4. Sensor Interference

When signals are being disrupted in the intra-BAN network due to sensors, the easiest way to recover is by a limited number of retransmissions [3]. However, this can overload the network causing more and more collisions. One option would be to eliminate the 'wireless' aspect of the intra-BAN network. In [7] and [9], a wired network of sensors is used to eliminate any interference or security threats. Wires are obstructive and are not hassle-free especially when trying to monitor a moving patient. However, current systems such as MITHrill [7] and SMART [7] already employ this technique. One way to alleviate the hassle of dealing with loose wires is to contain them. In Smart Textiles [9],

sensors and wires are sewn into clothing. Ensuring proper placement of sensors becomes crucial, as it would be difficult to reposition them. Some users may find this convenient but others may not due to the sensitive nature of the garment.

5. Environmental Interference

   Environmental interference can be handled the same way as sensor interference with a limited number of retransmissions [3] or by creating 'closer' multi-hop paths similar to the star-mesh topology with sensor cluster heads proposed for handling a limited aggregator [9]. This idea of creating a closer path can also be applied in the hop between the aggregator and AP. The addition of multiple access points within a frequented region could help by limiting the transmission distance [34] [35]. This option can be very expensive and not very practical.

   UWB (presented in section 2.1.3) has also been proven to be an employable standard for the intra-BAN network. From an interference standpoint, it has been shown to maintain high QoS mostly due to its large and unique operating frequency band [6]. Alternatively, considering that the human body is the major obstacle with the intra-BAN network, body coupled-communication [6] [9] or a low power communications channel through the body can achieve direct paths to the aggregator. When dealing with even shorter ranges, near field magnetic induction has also been shown to be a potentially feasible solution [9].

6. Limited or Loss of Power

   Power continues to be a bottleneck for most mobile devices and their applications. With BANs, sensor miniaturization and increased complexity are calling for more advancements with battery technologies. If real-time monitoring is not critical, power

management can be an option [27]. Lower sampling data rates on sensor nodes [9] and low-power sleep or standby states [6] [7] would also help with power conservation. Power at the aggregator can also be conserved with the transmission scheduling technique mentioned previously [7] [31]. One variation of transmission scheduling can include on-node storage [9]. If nodes, including the aggregator, were capable of gathering more data before a power consuming transmission, it would help reduce the number of times the transceiver is used.

Newer and innovative ideas for energy sources are also becoming a reality. With the addition of energy converting devices and transducers, energy harvesting is becoming a reality not only for BANs [9]. Potential energy sources include sun, wind, thermal and mechanical energy from the surrounding environment or movement and vibrations from the BAN user. Wireless energy transmission or wireless charging is also emerging in the world of mobile devices [7]. Additionally, low-weight super-capacitors and carbon nano-tubes are being developed for high power and long life options when compared to standard batteries [9].

7. Loss of Connectivity/Network Failure or Congestion

   There are basically two ways to address the issue of connectivity. First is to modify the network itself (APs and communication infrastructure). Referring to Figure 1.1, this would be modifications to the extra-BAN network. The second option is to modify the interactions the aggregator has with the extra-BAN network (by expanding network options or efficiently utilizing resources).

   Improving or adding additional communication infrastructure to the extra-BAN network is usually expensive and time consuming which is why it is probably the more difficult

option between the two. The addition of more access points and/or gateways would definitely increase the coverage area and capacity of a given network [34].

One can consider that the wireless link between the aggregator and the extra-BAN network is probably one of the more dynamic and vital links in the BAN network. As such, a loss of connectivity there would isolate the intra-BAN from the extra-BAN network eliminating any patient monitoring data from reaching its destination. To improve the performance of the BAN and lower data losses if outages occur at this point, one can use some previously mentioned techniques (limited retransmissions [7], on-node storage [9], and transmission scheduling [6] [7] [31]). Similar to transmission scheduling, asynchronous MAC mechanisms can take advantage of idle channels to schedule transmissions and overall prevent network congestion and contention for channel access [7]. However, equipping the aggregator with more than one radio interface would, in essence, give BAN more APs to connect to, thus increasing the coverage area and path diversity [15][39]. The idea of multi-radio transceivers will be discussed in Section 2.3.

8. Compatibility, Interoperability, and Sensor Heterogeneity

Throughout the world, different standards can operate on designated frequency bands or share a common unlicensed band. Because of the sensitive nature of healthcare and health informatics, a lack of standards and regulations for BANs may deter some users. While there exists the IEEE 802.15.6 task group whose main goal is standardizing BAN communications, no standards exist to this day [36] [37]. When a BAN enters a network it is not compatible with, no communications can occur, which leaves the aggregator with excess data. The aggregator can store this information until a viable connection is re-established [6] or, in other words, the aggregator uses a store-and-forward technique. While a BAN developer may not have control over this, task groups and frequency band

regulators should allocate a band for medical applications for BANs. These harmonious frequency standards may attract more developers and users alike.

## 2.3 Related Works with Multi-Radio Interfaces

With the advancement of wireless technologies, we are seeing more day-to-day devices equipped with some standard interfaces. Automobiles, cell phones, televisions, computers, routers, and much more are coming standard with wireless capabilities built in due to small and inexpensive wireless interfaces [46]. A diverse set of standards is also emerging for WLAN, WPAN and WAN networks. These include IEEE 802.11 a/b/g/n, Bluetooth, Zigbee, UWB, 3G and 4G cellular networks.

BANs are highly mobile networks with a high need for continuous end-to-end communications for real-time monitoring. Designing a BAN that is resilient to human mobility would need to incorporate multiple radio transceivers. This directly increases the path diversity of a given BAN and coverage area of wireless APs[15]. A human may walk through different regions covered by different wireless standards in a given period of time. It is becoming more economically feasible to incorporate multiple radio transceivers into mobile devices making this a reality [46].

To begin, Farago and Basagni study the gain in network connectivity by introducing the notion of multi-radio transceivers from a theoretical standpoint [46]. They model network topologies representing all the hops and paths through a graph. A graph is devised for each radio interface separately at first (random geometric graphs are generated to represent each of the wireless networks as they are the most frequently used models for study). Next, they merge each of the graphs for all radio interfaces to create a multigraph sum. This multigraph sum is representative of all the paths and connections

within the network that are created by the superposition of two or more radio interfaces. The authors then demonstrate that the connectivity (or the multigraphs' edge connectivity) cannot be smaller than the cumulative sum of each of the components. This they define as the multigraph advantage and illustrate the solid return on investment in multi-radio interfaces on connectivity.

The benefits of a multi-radio system are also illustrated in [39]. Bahl et al. argue that collaborative multi –radio interfaces improve the overall performance and flexibility of the system. They also provide guidelines for multi-radio system design. The three governing principles according to the authors are:

1. Design for Choice: This guideline is reinforced by the concept of radio diversity. Selecting radios for interfaces with different properties (such as range, transmit power, frequency band, etc.) is key.
2. Design for Flexibility: Flexibility, in this case, refers to the ease of switching between different radios in a multi-radio system. To the application layer, this should be a seamless transition.
3. Design for Separation: This entails using different radio transceivers for different system tasks.

Three multi-radio strategies are also presented for use on a commercially available phone with built in Wi-Fi capabilities. In the first approach, a secondary radio is used to monitor Wake requests. When a wake request is received, the device resumes communications with the more power-consuming primary Wi-Fi radio. However, energy conservation is key here, as the secondary link remains active during scanning phases. The second approach is similar to the first with a fine tuned wakeup scheme. In last

approach, the system hands over some of the data transmissions that would normally be sent over the primary Wi-Fi radio to the secondary radio thus reducing the energy consumption even more. With energy being so critical to mobile devices, these three approaches show promise for future applications.

Similar to the works of Bahl et al. mentioned previously, Pering et al. devise a multi-radio system that interfaces between Wi-Fi and Bluetooth to reduce power consumption [43]. The CoolSpots algorithm developed in this work uses a switching policy that trades off energy consumption and available bandwidth accordingly. The policy activates a switch to Wi-Fi when the established communication link is lacking in bandwidth. Similarly, the policy activates a switch to Bluetooth when there is excess bandwidth or not enough power. Continuously switching will also draw a lot of energy, thus the switching policies also consider the implications of a switch.

While Pering et al. have devised switching policies for energetic performance in multi-radio systems, Caporuscio et al. take a more theoretical approach to understanding an optimal multi-radio system [44]. By forming a graphical representation of a multi-radio system, the authors developed an integer programming optimization problem to minimize energy consumption. Some of the constraints used are: (1) only a single radio on at a single time, (2) nodes must have adequate power available to use certain radios, (3) two connected nodes must share at least one radio interface, and (4) nodes must provide adequate bandwidth to all their neighbors. The optimization problem was shown to be extremely complex which can in turn imply that multi-radio systems have a higher degree of network management complexity when compared to its single-radio counterpart. However, the careful approximation can lead to better energy consumption.

Gummeson et al. take the works of Pering et al. and Bahl et al. to the next level by substituting switching policies and optimizations for a Q-learning (or reinforcement learning) based switching protocol [45]. The learning algorithm monitors the channel during operation; more specifically this would include the channel variations due to mobility and distance away from the AP. The algorithm would then make a decision to switch or not based on past performance and their respective decisions. The idea was then tested in hardware (mote-class sensor network) and compared to its single-radio counterpart. The dual-radio system showed up to 52% energy savings with the same degree of mobility.

Energy conservation is a powerful concept in mobile devices; however, bandwidth is an emerging issue with new high rate mobile applications. Chebrolu et al. design a multi-radio system to increase the overall system bandwidth [40] [42]. Unlike the previously mentioned multi-radio systems, power consumption is not a major consideration for the authors. With multiple radio interfaces, using all radio resources available can increase the throughput of the system. The idea of Bandwidth Aggregation is employed here. First, available bandwidth is approximated and a scheduling algorithm is used to distribute data packets onto each of the 'paths' created by the multiple radio interfaces. The scheduling algorithm considers packet reordering when distributing the data packets. However, this is a much more complex process to ensure minimal out of order packets received at the destination. Secondly, due to the fact that reordering cannot be avoided, a buffer is used at the client-side to hide the effects. Through simulations, the authors have shown an exemplary system to increase throughput with multi-radio systems.

Another novel idea is that of using one radio interface to seek out a connection with another radio interface. Ananthanarayanan et al. present a multi-radio system called Blue-Fi that uses Bluetooth to seek out a Wi-Fi connection [41]. The idea uses a log entry system in which each mobile device in the network logs the network signals it encounters in a localized record. If a Bluetooth device has had a recent log entry including a Wi-Fi AP, then a connection is available. However, due to mobility of the devices, this may not always be true. Therefore, the potential for the existence of a Wi-Fi connection is based on a sample of the most recent entries in a Bluetooth device. If most of those entries include a Wi-Fi AP, then a Wi-Fi connection is available. The advantages of such a system relate to the energy consumption benefits of previously mentioned works. Bluetooth, being a low-rate and low-power interface, saves significant amounts of energy when compared to Wi-Fi AP probing and scanning.

# Chapter 3
# Multi-Radio Interface for BANs

This chapter highlights the system model and detail of the multi-radio interface for BANs to facilitate higher dependability through continuous end-to-end communications. Referring back to Section 2.2.1, this system hopes to alleviate the loss of connectivity or network failure issue through radio diversity.

The focus for the proposed interface is the single hop wireless link between the BAN aggregator and the wireless AP. This wireless link is one of the most dynamic in the BAN system model due to the mobility of the BAN user. This chapter introduces the details of the system and suggested multi-radio protocol as follows:

1. In Section 3.1, the overall system model is presented. Furthermore, the individual models (mobility, AP Placement, wireless link, etc.) are considered and selected for use.

2. Section 3.2 outlines the multi-radio protocol from an algorithmic perspective. It outlines the framework for switching between the two radio interfaces and the handover procedure.
3. Finally, with all the system models in place, Section 3.3 assembles it all together for a complete picture including simulation parameters and network assumptions.

## 3.1 System Model

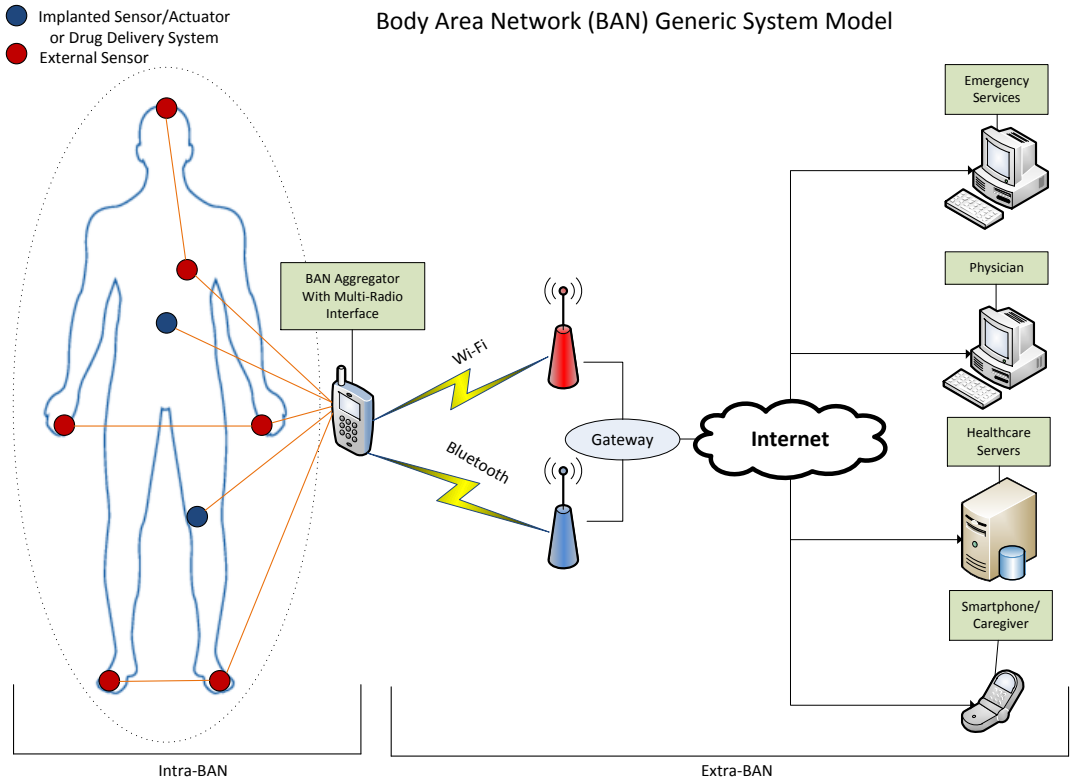


***Figure 3.1: Multi-Radio System Model and Surrounding Infrastructure***

Figure 1.1, the original overall BAN system model, is adjusted in figure 3.1 to reflect the two wireless interfaces – Wi-Fi and Bluetooth – selected for the suggested multi-radio system proposed. The BAN aggregator collects and fuses data collected for the sensor nodes in the intra-BAN network. This data is then sent regularly and in a timely fashion through the multi-radio interface to a Wi-Fi or Bluetooth AP. The goal is

to achieve a higher connectivity by connecting to either one of the interfaces. The primary interface here is the Wi-Fi interface due to higher range and bandwidth capabilities. If unavailable, the protocol will then switch to the low-power secondary Bluetooth interface (if available) to maintain connectivity.

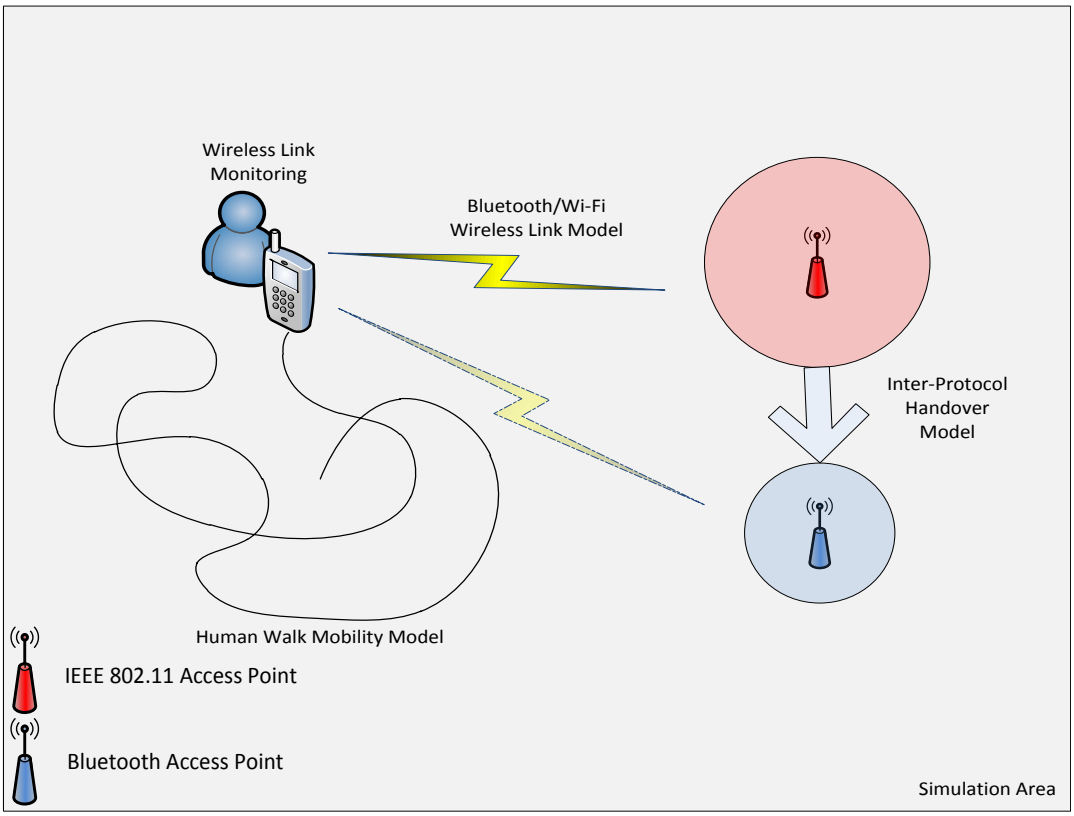


***Figure 3.2: Breakdown of system model into individual behavioral models***

In order to simulate the single hop wireless interface, we must narrow down the system model to focus on the behaviors from that scope. In figure 3.2, this single hop connection is illustrated between the BAN aggregator and wireless APs. Furthermore, in order to simulate the performance of a multi-radio protocol, additional models are necessary to capture human mobility, channel losses and power attenuation in wireless

links, and AP placement. These models achieve a certain degree of life-like simulations that are desired.

### 3.1.1 Human Walk Mobility Model

Human mobility has a significant impact on the performance evaluation of mobile networks and wireless devices. Most people carry their smartphones or PDA devices on person and this is no exception to BANs. BANs are designed with sensors that are mounted on or implanted in the human body. As a result of this, the BAN mobility model is completely dependent on the human walk pattern. In order to get an accurate or realistic mobile behavior of a BAN aggregator in the simulation environment, we evaluate a few different human mobility models for their statistical description of human movement and ability to be implemented and simulated.

Some common terminology used for mobility models are listed here for clarification:

- *Flight or Path [Length]:* A flight or path is the trip from one point to another or from source to destination. It is a single straight line with no change in direction.
- *Flight time*: This is the duration of time required for the user to complete a single flight.
- *Direction*: The direction of a flight is the angle clock-wise away from 'North' that the user is traveling in.
- *Pause*: After each flight, the user decides whether there is a pause (of some time duration) at the destination. This reflects a user at rest at the end of travel.

The most common mobility model used for human motion, for a wide range of applications such as urban planning or disease management, is the Random Walk Model [47]. Each successive step is selected independently and consists of a flight length, time, direction and pause time. These steps can follow a distribution function such as the

Uniform or Gaussian distributions. In an effort to set bounds on a 2 dimensional random walk model for the proposed multi-radio system, we set three equally likely actions that dictate the next random waypoint: (1) Walking, (2) Running, or (3) Driving. As an alternate to dictating a waypoint by a length and time, one can also do so with a speed and time. The following pseudo-code explains the random walk model specific to the proposed works:

```
To define the next waypoint:

randNumber ← Uniform(1,3)
if randNumber = 1, Perform Walking
        Direction ← Uniform (0,359)
        Speed ← Normal(4km/h, 1.5km/h)
        Time ← Normal(3s, 2s)
if randNumber = 2, Perform Running
        Direction ← Uniform (0,359)
        Speed ← Normal(10km/h, 8km/h)
        Time ← Normal(7s, 3s)
if randNumber = 3, Perform Driving
        Direction ← Uniform (0,359)
        Speed ← Normal(30km/h, 90km/h)
        Time ← Normal(20s, 15s)

if Speed or Direction or Time < 0, regenerate Waypoint

if Waypoint reached
randNumber2 ← Uniform (1,2)
if randNumber2 = 1, Perform Pause
        PauseTime ← Normal(15 sec, 5 sec)
if randNumber2 = 1, define next Waypoint
```

The Normal/Gaussian (mean, standard deviation) and Uniform (with lower and upper threshold) distributions are used to generate the next random step or waypoint. For all generated variables, they must be greater than zero to have significance.

Random walks, while simple, have had very little validation with real human walk patterns. They are characterized by a large number of long flights. Brownian motion, which is governed by particle theory, is another random model that dictates movement or

diffusion for physical processes [47]. Brownian motion, unlike the random walk model, is characterized by a large number of shorter flights. Both random walks and Brownian motion are convenient to implement but are far from accurate within the context of human movement.

As an alternate to simulating with the random walk model, we introduce a second and more statistically complex model called the Levy walk [47]. Researchers have used Levy patterns to describe animal behavior. More recently, human walk patterns have been found to share statistical resemblances with the Levy walk in research collecting real walk trace information.

A Levy flight or 'tuple' is characterized by four components, two of which follow the Levy distribution [47]: flight length ($l$), flight time ($\Delta t_f$), direction ($\theta$) and pause time ($\Delta t_p$). Equations (1)-(4) highlight the distributions for each:

$$l \sim Levy(0.5,1,10,0) \tag{1}$$

$$\Delta t_f = k l^{1-\rho} \begin{cases} l < 500m, k = 18.72, \rho = 0.79 \\ l \geq 500m, k = 1.37, \rho = 0.36 \end{cases} \tag{2}$$

$$\theta \sim U(0^o, 359^o) \tag{3}$$

$$\Delta t_p \sim Levy(1,0,\sigma^2,m) \tag{4}$$

Where a variable X is distributed by the Levy Distribution according to:

$$X \sim Levy(Stability, Skewness, Std.Dev., Mean)$$

The flight time was found to have the relationship to the flight length as indicated in equation (2) based on the walk measurements conducted in [47]. When the value of $\rho$ trends towards 0, $\Delta t_f$ and $l$ are proportional to one another indicating a constant velocity.

On the other hand, when $\rho$ trends towards 1, $\Delta t_f$ becomes a constant value and the length of a flight then determines the velocity. The authors also utilize truncation factors for flight length to set upper thresholds for distances traveled. Similarly, within the context of our simulation, the user can move throughout the entire simulation area. If a boundary is reached before completing a flight, a new flight is generated.

While the Levy Walk may not be the perfect model for human walks, human walks are in no way random. Our walk patterns follow a number of spatial and temporal patterns. Places such as our homes or offices are frequently visited. We may have scheduled meetings or clubs that also dictate our schedule and location. Lee et al. propose a highly complex human walk model that incorporates some of these spatial and temporal patterns [48]. These include fractal waypoints (or 'popular' locations), confined or bounded areas, and inter-contact times (successive meetings between people).

Furthermore, in reality, our environments are full of obstacles that also affect human mobility. While this complicates the human walk model, it also represents a more accurate environment. In [49], Papageorgiou et al. propose an obstacle-aware mobility model designed to work around obstacles. When a user encounters one, a recursive procedure helps the user get around the obstacles by leading them to the obstacles vertex closest to the destination of the flight.

However, for our simulations, we select the Levy and Random walk models for simplicity and for comparison. We will also only be simulating a single user moving through a simulation area, therefore inter-contact times and user meetings do not need to be modeled as in [48][49].

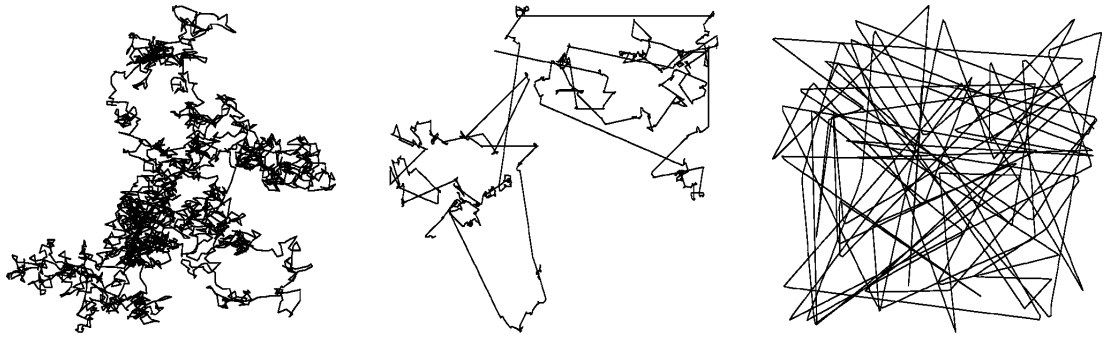


***Figure 3.3: Sample Human Walk Patterns or Trajectories for Brownian Motion (a), Levy Walk (b) and a Random Walk (c) Model [47]***

### 3.1.2 Access Point Placement or Network Architecture

In order to model varying channel quality and multi-radio handovers, not only will the user have to be mobile through the simulation area, but APs will be scattered throughout this area. Normally, network planners place these APs in strategic locations to maximize coverage. In an ideal situation, APs would be placed in an offset grid fashion (similar to the circle packing problem) with their circular cells. If there are more APs available than the network area, then their ranges can even overlap with one another. However, obstacles such as buildings, walls and terrain can be an issue for network planners. Certain locations may not be suitable for an AP placement, or an AP may not cover its full range if surrounding obstacles attenuate any signals. Therefore, we select the two extremes for simulation: a random placement of APs and an ordered placement of APs to account for worst and best case situations (respectively).

The ordered placement of APs distributes the APs in a grid fashion. Because we are simulating a multi-radio system, to further increase coverage, the primary and secondary APs are also offset from each other. By doing this, those regions that may not

be covered by Wi-Fi even with the ordered placement can be covered by Bluetooth and vice versa. Figure 3.4 illustrates this point. The random placement of APs (Figure 3.5) generates random coordinates in the simulation area for placement of all the APs. However, to prevent clusters of APs from congregating in one area, a 'not-so-strict' 5% coverage increase threshold is put in place. Each time a new AP is added, the threshold limits the overlap in their coverage area to 95%, meaning an additional approximately 5% coverage is added. However, this threshold is not strict, but rather a guideline, as complexity of this problem increases with the number of APs.

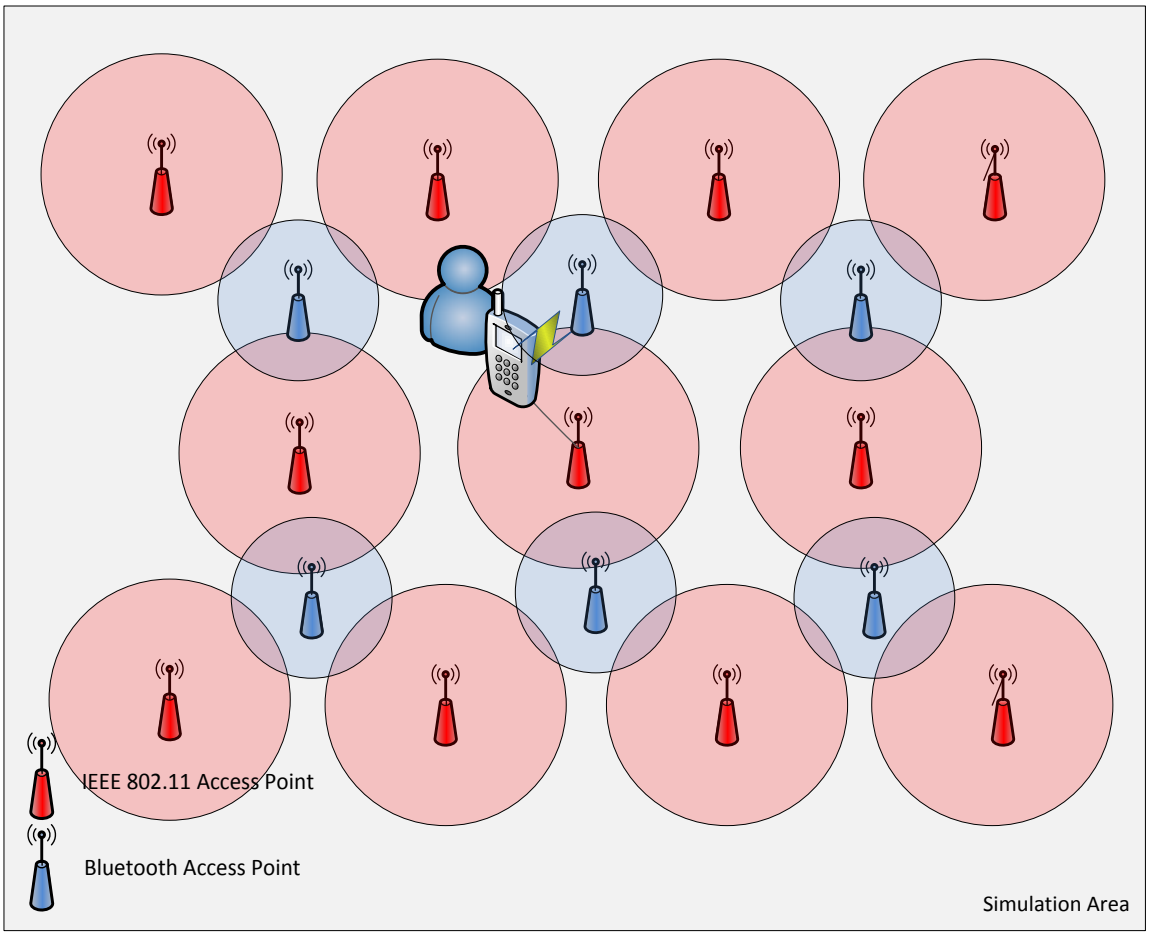


***Figure 3.4: Ordered AP Placement***

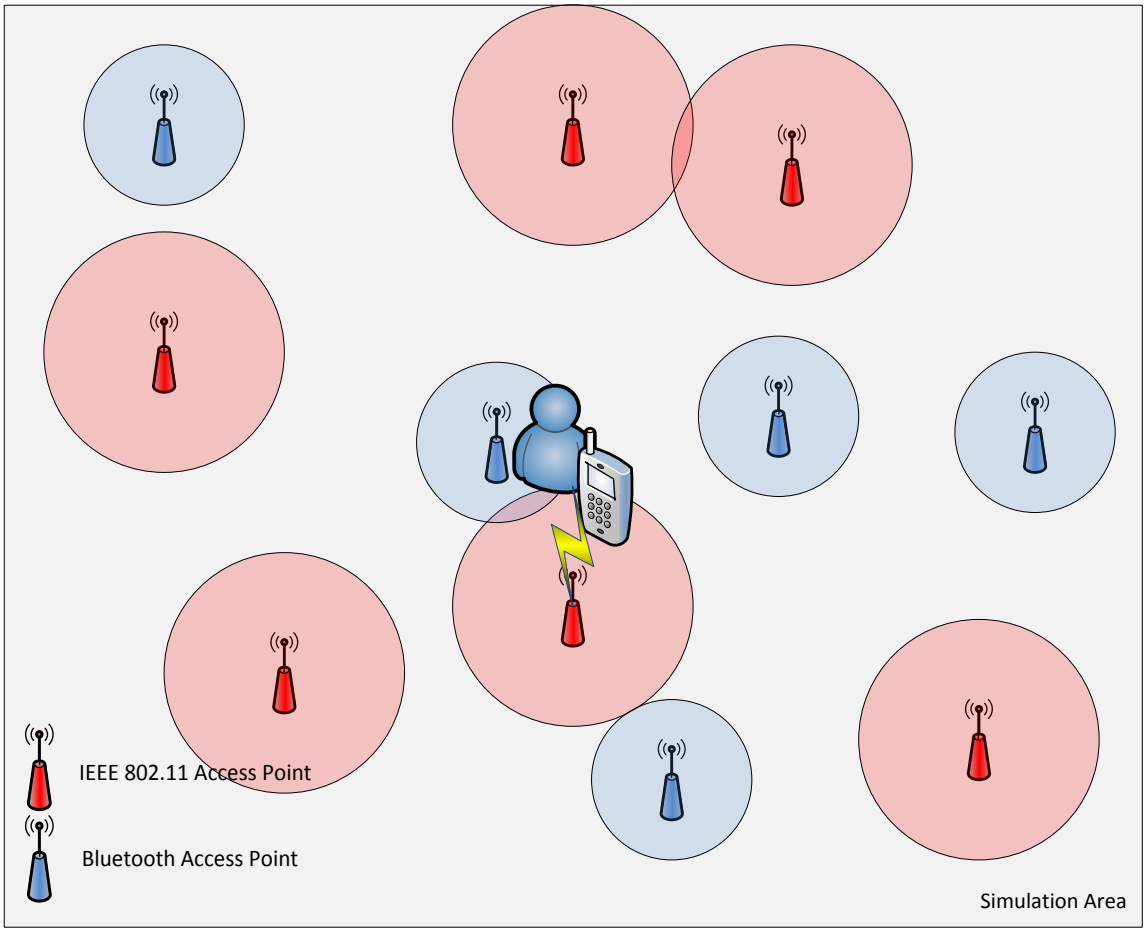


***Figure 3.5: Random AP Placement***

### 3.1.3 Wireless Link Model

Wireless communication channels of links always play a vital role in analyzing the performance of wireless protocols [50]. Because wireless technologies are quickly becoming a norm in day-to-day life, numerous researchers have stepped up to develop channel models that accurately reflect lossy links in WSNs, WLANs, WPANs, and more. Losses in wireless links can occur for the following different reasons [51]:

- Power Attenuation, Noise and Interference:

  The received signal strength through a wireless channel is dependent on distance, shadowing, diffraction, scattering and multipath fading. The mobile devices do not have a

high degree of control over these factors, as most are environmental or based on mobility. However, power control and transceiver gains can be adjusted (within reason) by these mobile devices. Most mobile devices are equipped to conserve energy by dynamic power control mechanisms and user intervention.

- Errors and Corruption:

  Packet losses or corruption are usually handled by simple link-layer retransmissions. However, poor radio conditions and complex handovers do aggravate this source of loss in wireless links.

- Delays and Out of Order Delivery:

  Network congestion and packet errors can cause delays that can further trigger out of order delivery.

- Link Asymmetry:

  Mobile devices and APs are significantly different in terms of resources available. As such, one can expect that the uplink and downlink connections would differ in latency and bandwidth. This is especially common in cellular networks.

Modeling wireless links requires consideration of some if not all of these sources of loss in wireless channels. Across literature, three main wireless models emerge: (1) Probabilistic Link Model [50] [52] [53], (2) Markov-Based Link Model [54] [55] [56], and Log-Distance or Deterministic Model [57].

With the probabilistic link model, outages are determined by a probability distribution centered on communication variables such as noise, attenuation, etc [53]. For example, the probability of a successful wireless packet transmission can be modeled as [52]:

$$P_{SUCCESS}(d, SNR) = e^{-d^k / SNR} \qquad (5)$$

where SNR is the signal to noise ratio, *d* is the distance between communicating devices, and k is the path-loss exponent.

Alternatively, one could perform a measurement-based study the behavior of communication channels after which a formalized Markov-based model can be formed [54] [55] [56]. In all of these works, the authors first conduct data collection phase to analyze failing behavior. This data can then be translated into a series of states that make up the Markov-model. Transitions between these states are dictated by probabilities extracted from behavioral analysis of the network.

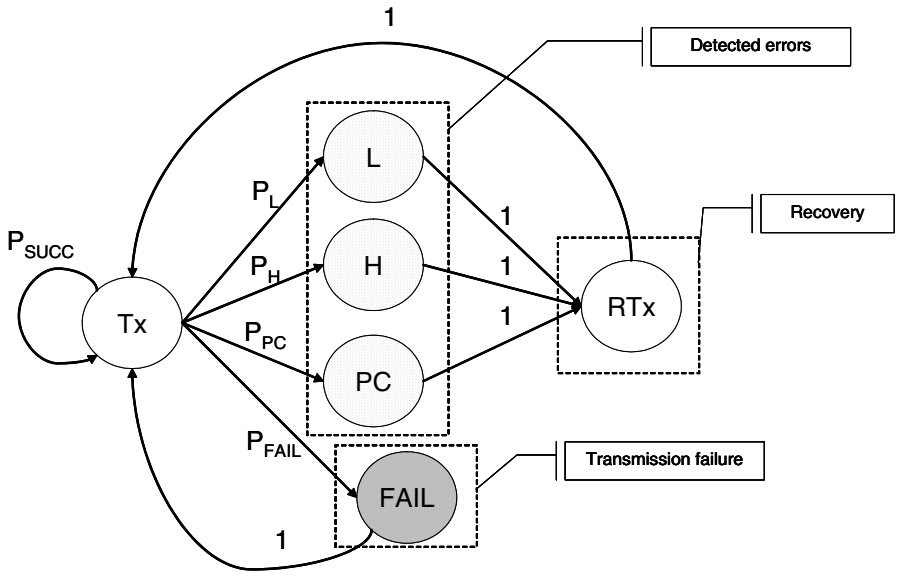


***Figure 3.6: Bluetooth Markov-based Channel Model with Length Mismatch (L), Header Corruption (H), and Payload Corruption (PC) Error Modes [54]***

For our simulations, it is important to model channel behavior based on distance between the two communicating devices as a BAN user is highly mobile. Additionally, it is important to stress the differences in capabilities between the aggregator and AP devices. And finally, it is important for us to select a channel model that would be

applicable to any wireless protocol. This is especially crucial for maintaining consistency when simulating a multi-radio network. For these reasons, the log-distance (or deterministic) channel link model is appropriate. A failure occurs when the received power is less than the sensitivity of the receiving device. The following model is used for our simulations [57]:

$$SNR = \frac{P_r}{P_{N_0} + P_{I_0} + \sum_{k=1}^{i} P_k} \qquad (6)$$

$P_r$ = Received Power
$P_{N_0}$ = Thermal Noise
$P_{I_0}$ = Background Interference
$P_k$ = Co - channel Transmitters Interference

$$\boxed{\begin{array}{l} Failure\ Occurs\ When: \\ SNR < Sensitivity_{receiver} \end{array}}$$

Furthermore, to define received power ($P_r$) and Co-channel Transmit Power ($P_k$), we use the following:

$$P_{dBm} = P_{t,dBm} + G_{t,dBi} - L_{c,dB} + G_{r,dBi} - L_{s,dB} \qquad (7)$$

$P_{dBm}$ = Received Power
$P_{t,dBm}$ = Transmitted Power
$G_{t,dBi}$ = Transmitter Antenna Gain
$G_{r,dBi}$ = Receiver Antenna Gain
$L_{c,dB}$ = Channel Propagation Losses
$L_{s,dB}$ = System Losses

$$L_{c,dB} = L_{0,dB} + X_{s,dB} + X_{f,dB} + \begin{cases} 10n_0 \log(d) & ; d \le d_1 \\ 10n_0 \log(d) + 10n_1 \log\left(\frac{d}{d_1}\right) & ; d > d_1 \end{cases} \quad (8)$$

$L_{c,dB}$ = Channel Propagation Loss
$L_{0,dB}$ = Reference Path Loss (1m)
$X_{s,dB}$ = Shadowing Loss
$X_{f,dB}$ = Fading Loss
$d$ = Current Distance
$d_1$ = Breakpoint Distance
$n_0$ = Path Loss Exponent before $d_1$
$n_1$ = Path Loss Exponent after $d_1$

The breakpoint distance is defined here as the distance at which we transition from a low path loss exponent to a higher path loss from a transmitter to receiver. More specific to our case, this is the transition from free space losses to a higher exponent indicating a rather lossy environment. This can be calculated as follows for wireless transmissions [58]:

$$d_1 = k_b \frac{h_t h_r}{\lambda} \quad (9)$$

$d_1$ = Breakpoint Distance
$k_b$ = Breakpoint Coefficient
$h_t$ = Height of Transmitter Antenna
$h_r$ = Height of Receiver Antenna
$\lambda$ = Radio Wavelength

Shadowing and fading losses follow the Gaussian and Gamma distributions respectively. Also it is assumed that they are independent.

$$X_{s,dB} \sim \mathrm{N}(m_s, \sigma_s) \quad (10)$$
$$X_{f,dB} = \Gamma(\theta, k) \quad (11)$$

$$\theta = scale$$
$$k = shape$$
$$mean = k\theta$$
$$\sigma^2 = k\theta^2$$

All the details and quantitative parameters used will be summarized in Section 3.3 for an overall picture of the simulation environment. This model does account for power attenuation losses from shadowing, fading, and interference. Additionally, it accounts for system losses such as transceiver cabling and losses due to distance. While is may not account for all the losses in wireless systems presented in [51], it provides us with a solid deterministic channel model that we can apply to our simulated Wi-Fi and Bluetooth transceivers.

## 3.2 Protocol Overview

In this section, the suggested multi-radio protocol for increasing dependability in BANs is outlined. As mentioned earlier, it will involve an aggregator with Wi-Fi and Bluetooth wireless capabilities. Wi-Fi will serve as the primary link and Bluetooth will therefore serve as the secondary or backup link.

The multi-radio BAN Aggregator will begin to transmit information via its primary link chosen under the impression that it will be the most widely available link. However, if it does fail, the aggregator will then initiate a handover in which it will place it's primary radio on standby, wake it's secondary radio, and begin to discover secondary APs. Should the secondary link fail as well, the BAN will then set both radios on standby and buffer sensor data until a link becomes once again available. In order to find this link,

the aggregator will have to proceed to alternately wake its primary and secondary (if necessary) radios to initiate a discovery process.

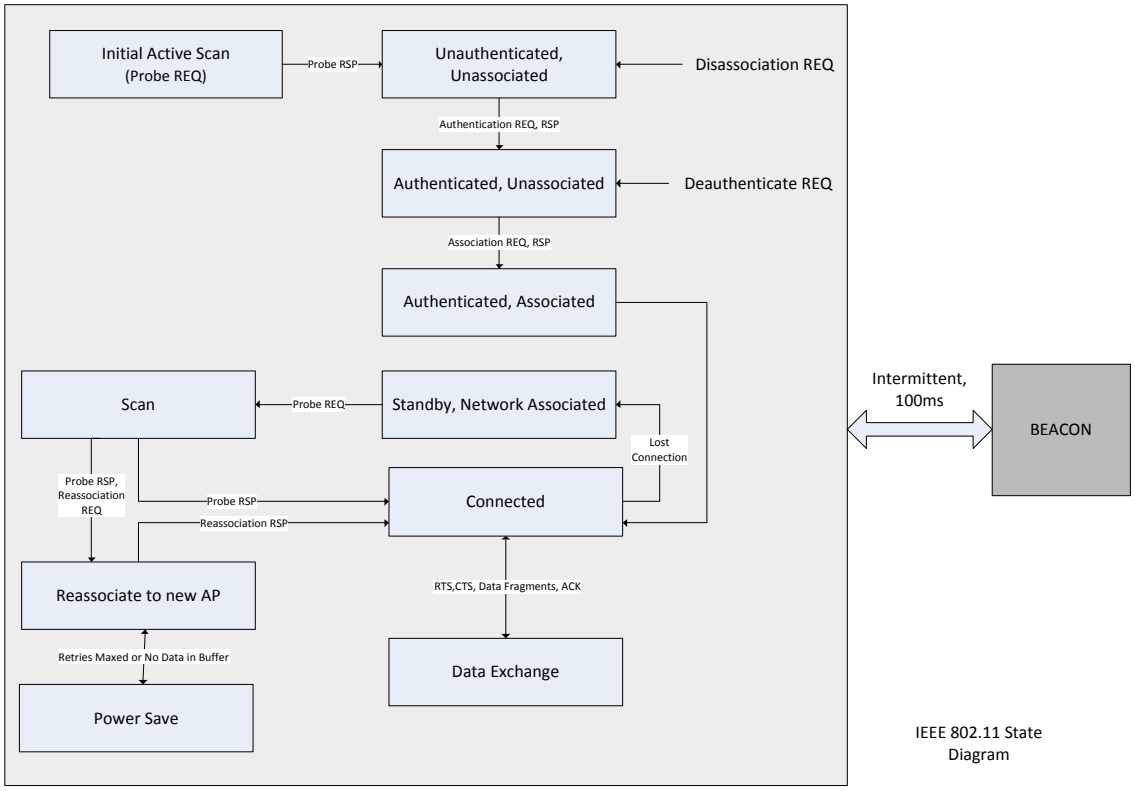


***Figure 3.7: IEEE 802.11 State Diagram and Transitions***

While the aggregator is active and connected on either the primary or secondary radios, the other radio will remain in a power saving mode. Hence the aggregator will essentially be behaving as single radio device with marginal additional power consumption due to the standby transceiver. It will follow the active wireless protocol as mentioned in Chapter 2 until a connection is lost at which point the device will switch. In order to prevent each of the wireless protocols from reattempting connections numerous times, we set a threshold for association reattempts before switching to the other radio.

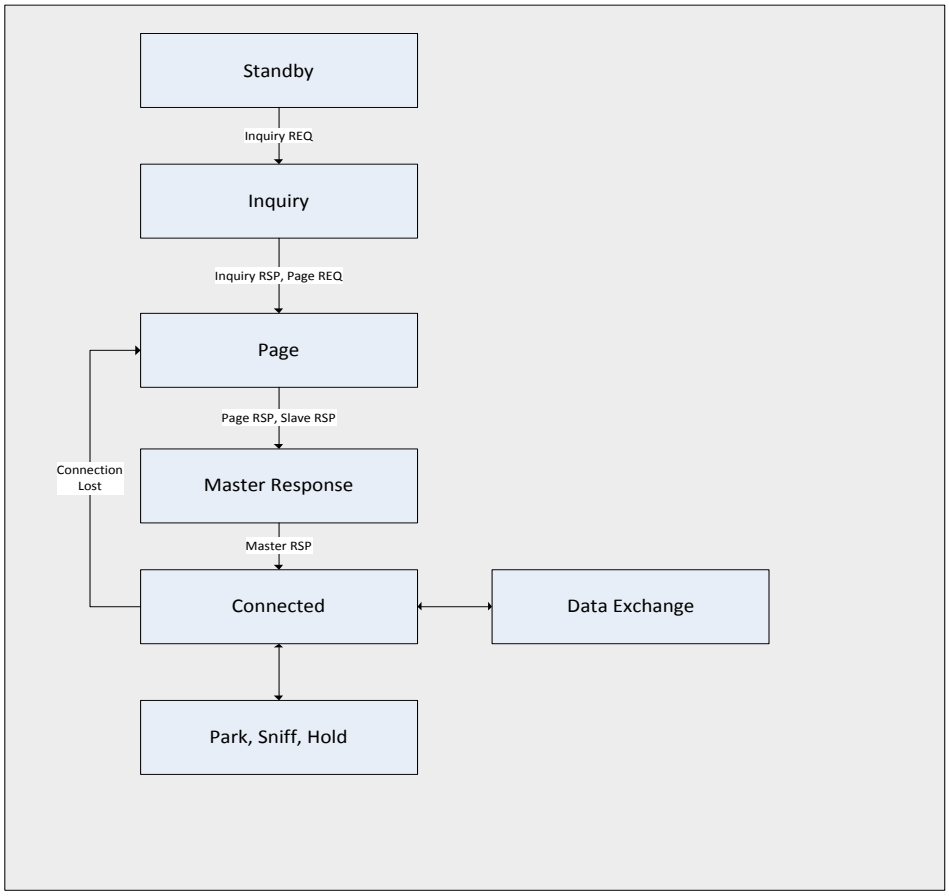


***Figure 3.8: Bluetooth State Diagram***

There are essentially four cases to be considered in the protocol:

1. Case 1: Wi-Fi is available and will be utilized for any data transmissions from the BAN aggregator.
2. Case 2: Either the Wi-Fi UL or DL channel is available, but not both. At this point, the aggregator would utilize the Bluetooth interface if available.
3. Case 3: Wi-Fi is completely unavailable (aggregators probe and reassociation requests are not finding any APs, and likewise for the DL connection). The aggregator would then use the secondary Bluetooth interface.

4. Case 4: In this case, neither the primary Wi-Fi nor secondary Bluetooth links are available at all. The aggregator would have to store all sensor data until a viable connection is found again.

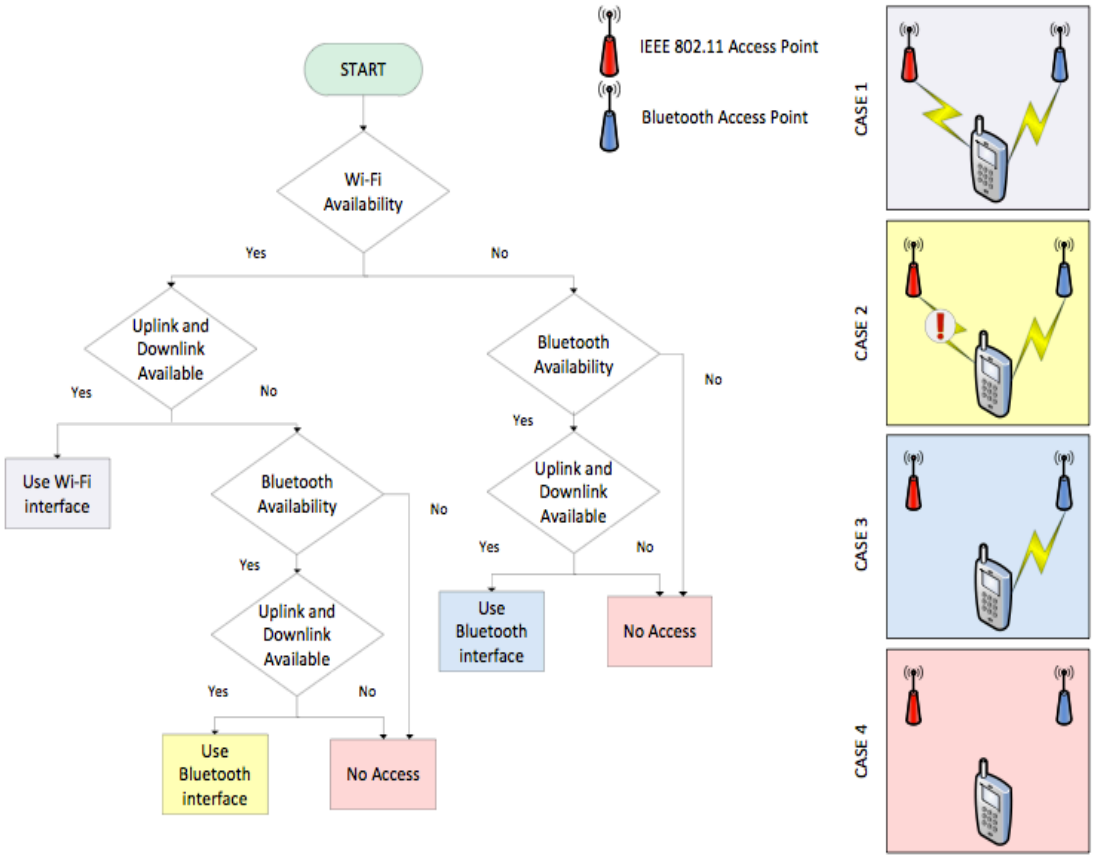


***Figure 3.9: Four Possible Link Cases or Scenarios for Proposed Protocol***

The following pseudo-code outlines the multi-radio protocol in more detail:

```
SimulationTime ← 1000s
currentProtocol ← Wi-Fi
NetworkAssociatedAuthenticated ← False
connected ← false
For time = 0 to SimulationTime

If currentProtocol = Wi-Fi Then

        If NetworkAssociatedAuthenticated = False Then
                Initiate Probe REQ, wait for RSP
        Else
                If connected = false Then
                        Initiate Reassociate REQ, wait for RSP or time-out
                        Re-tryAttempts ← Re-tryAttempts + 1
```

```
                    Else
                            If TransmitBuffer is Empty Then
                                    Initiate Power Save
                            Else
                                    Initiate Data Exchange


            If Probe RSP received Then
                    connected ← true

            If Reassociate RSP received Then
                    connected ← true

            If Re-tryAttempts > Threshold Then
                    Initiate Wi-Fi Power Save
                    Wake Bluetooth Transceiver
                    currentProtocol ← Bluetooth
                    Restore TransmitBuffer
                    connected ← false

If currentProtocol = Bluetooth Then

            If connected Then
                    If TransmitBuffer is Empty Then
                                    Initiate Park
                            Else
                                    Initiate Data Exchange

            Else
                    Initiate device discovery, wait for RSP
                    PagingAttempts ← PagingAttempts + 1

            If Inquiry and Paging RSP received Then
                    connected ← true

            If PagingAttempts > 3 Then
                    Initiate Park
                    Wake Wi-Fi Transceiver
                    currentProtocol ← Wi-Fi
                    Restore TransmitBuffer
                    connected ← false

End For
```

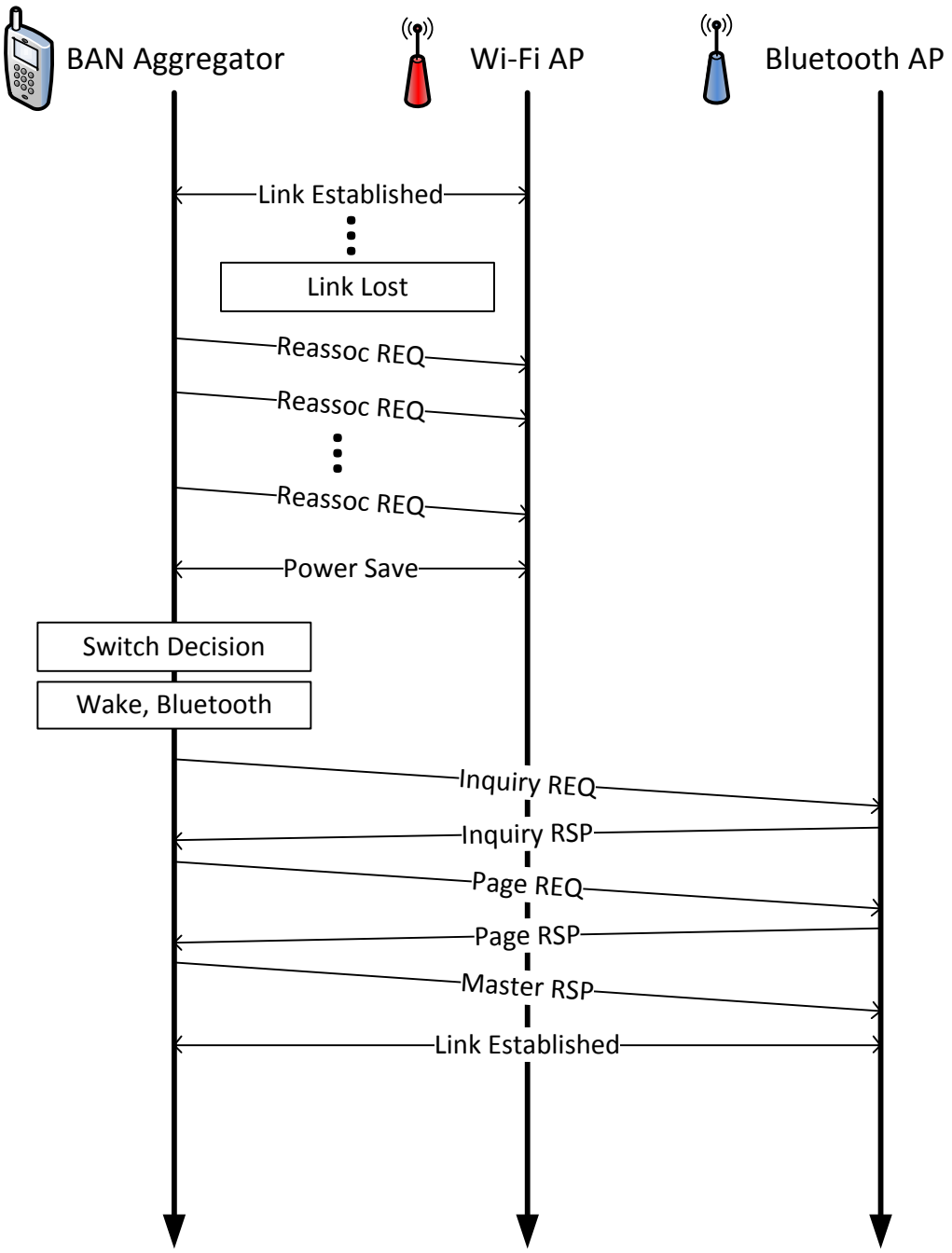


***Figure 3.10: Sequence of events for Wi-Fi to Bluetooth Inter-protocol Handover***

One important aspect to note is the number of times both the Wi-Fi and Bluetooth radios attempt to reassociate to their respective networks before initiating a protocol switch. For Wi-Fi, this number is varied in simulations and will be discussed in detail in

Chapter 4 along with other simulation results. But for Bluetooth, the number of times to retry device discovery is limited to a maximum of three. This is due to the fact that device discovery can last up to 10.24 seconds in the worst case scenario [41] [59]. This is attributed primarily to the inquiry hopping sequence that devices generate prior to either sending an Inquiry REQ or waiting to respond to an inquiry.

Another point to note is the restoration of the transmit buffer. The BAN aggregator collects and fuses the intra-BAN sensor data. However, suppose the system is using the Wi-Fi radio when the connection is lost mid-way through a fragmented data exchange. Wi-Fi and Bluetooth protocols assemble packets differently through their respective protocol stacks. Thus we need a shared transmission buffer transparent to each protocol stack to be able to restore data that has not been successfully transmitted. Packet assembly begins as high as the Transport Layer for Wi-Fi and the L2CAP Layer for Bluetooth. However, we also need their respective Link Layers to communicate with one another to ensure proper link set up and power save initializations. Therefore, a separate entity called the BAN controller communicates between all of these layers to achieve these goals:

- Restore data packets to the transmission buffer after an unsuccessful transmission attempt on either radio
- Manage Power Save and Wake control for each radio
- Manage radio status (ie: Wi-Fi or Bluetooth ON/OFF) and significant indicators (ie: Wi-Fi or Bluetooth retry attempts)
- Monitor errors and packet flow

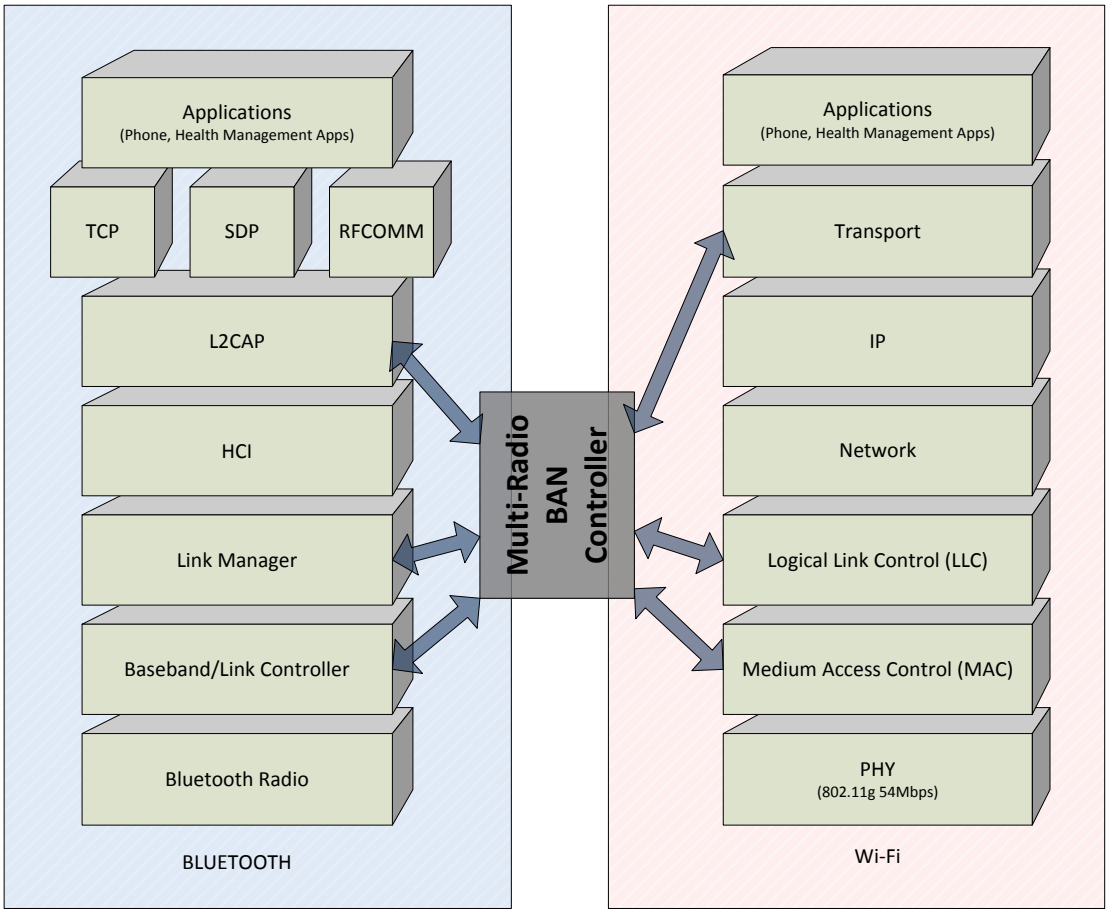


***Figure 3.11: Multi-Radio BAN Controller and its Relation to the Utilized Wireless Protocols***

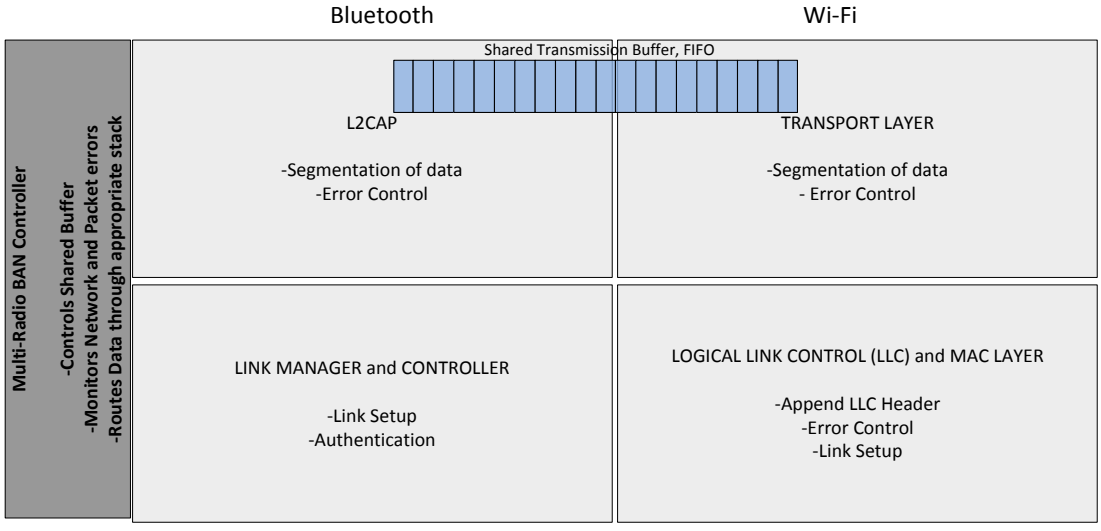


***Figure 3.12: Description of Multi-Radio BAN Controllers' functions***

## 3.3 Simulation Parameters & Assumptions

This section will break down all the simulation parameters into those used for the intra-BAN network, channel link model, protocols, simulation environment, and AP and aggregator transceivers into Tables 3.1-3.6. Additionally, all the assumptions made and their justifications are summarized.

A large number of simulations will be conducted with a single BAN user moving through a simulation area according to either the Random Walk or Levy Walk mobility models. There will be no other users in the environment and thus no interference from co-channel users ($P_k = 0$). Furthermore, the user will be equipped with an intra-BAN network consisting of seven sensors (Table 3.6). The data from these sensors will be sent to the aggregator where data fusion techniques will be utilized to create 30KB packets every second for transmission. Data will be sent from aggregator to the AP in simulations according to protocol specifications. Because we are concerned about real-time monitoring, this data will be transmitted as it becomes available if a viable connection via Wi-Fi or Bluetooth is available.

Within the environment, we assume that there are no repeaters available to extend the range of any AP. Additionally, we assume there is no power control at the AP or aggregator; therefore, both stations transmit at maximum power. Additionally, we also assume that the channel, shadowing and fading values remain constant for the duration of one time step in the simulation. Because human movement in such a small time frame is not very significant, we can assume that the BAN user will experience the same channel behavior and attenuation effects for that small period of time.

Finally, when the user authenticates and associates to the Wi-Fi network, if the connection is lost, all that is required is a reassociation request. The user does not have to reauthenticate.

***Table 3.1: Simulation Environment Parameters***

| Parameter | Value |
|---|---|
| Simulation Area | 500m x 500m |
| Simulation Time | 1000 sec |
| Time Step | 1 sec, 1ms |
| Repetitions * | 5 |
| Number of Wi-Fi APs | 10, 50, 100, 150, 200 |
| Number of Bluetooth APs | 0, 25, 50, 75, 100 |
| AP Placement | Random, Ordered |
| Human Walk Models | Random, Levy |
| Pause Time mean ($m$) | 0, 5, 10, 15, 20, 25, 30 sec. |
| Pause Time Std. Dev. ($\sigma^2$) | 5 sec. |
| Aggregator Transmission Buffer | 1MB |

**Each simulation is conducted 5 times at each combination of parameters*

***Table 3.2: Protocols and Corresponding Simulation Parameters [18] [19] [57] [59]***

| Parameter | Wi-Fi | Bluetooth |
|---|---|---|
| Standard | IEEE 802.11n | v2.1 + EDR |
| Multi-Radio Primary/Secondary | Primary | Secondary |
| Nominal Range | 100m | 10m (Class 2) |
| Frequency Band | 2.4/5GHz | 2.4GHz |
| Link | Symmetric | Symmetric ACL |
| Data Rate | 1 Mbps (Control), 24 Mbps (Management, Data) | 400 Kbps |
| Reassociation Attempts | 1, 5, 10 sec | 3 retries |
| Beacon Interval | 100ms | N/A |
| Discovery Time (Worst-Case) | N/A | 10.24 sec |

***Table 3.3: Transceiver Properties and Parameters***
***(From Survey of Commercially Available Chipsets – See Appendix A)***

| Parameter | Wi-Fi | | Bluetooth | |
|---|---|---|---|---|
| | AP | Aggregator | AP | Aggregator |
| Transmit Power (dBm) | 17 | 13 | 5 | 3 |
| Transmitter Gain (dBi) | 2.5 | 0 | 0 | 0 |
| Receiver Sensitivity (dBm) | -72 | -73 | -86 | -82 |
| Receiver Gain (dBi) | 0 | 0 | 0 | 0 |

*Table 3.4: Channel Link Model Parameters [57] [58]*

| Parameter | Wi-Fi | Bluetooth |
|---|---|---|
| $L_{0,dB}$ | 20 | 40 |
| $d_1$ | 10 | 1.5 |
| $n_0$ | 2 | 2 |
| $n_1$ | 4 | 4 |
| $L_{s,dB}$ | 0 | 0 |
| $m_s$ | 0 | 0 |
| $\sigma_s$ | 1 | 1 |
| $\theta$ | 0.2 | 0.2 |
| $k$ | 5 | 5 |

*Table 3.5: Transceiver Power Consumption Parameters [41]*

| | Wi-Fi | Bluetooth |
|---|---|---|
| Transfer (J/MB) | 5.0 | 0.1 |
| Idle (W) | 0.77 | 0.01 |
| Scan (W) | 1.29 | 0.12 |

*Table 3.6: Intra-BAN Sensor Properties [60]*

| Physiological Signal | Parameter Range | Data Arrival Time (Sec.) | Sample Size (bits) | Data Rate (kbps) |
|---|---|---|---|---|
| Blood Flow | 1-300mL/sec | 0.025 | 12 | 0.48 |
| ECG Signal | 0.5-4mV | 0.002 | 12 | 6.0 |
| Respiratory Rate | 2-50 breaths/min | 0.05 | 12 | 0.24 |
| Blood Pressure | 10-400mmHg | 0.01 | 12 | 1.2 |
| Blood pH | 6.8-7.8 | 0.25 | 12 | 0.48 |
| Nerve Potentials | 0.01-3mV | 0.00005 | 12 | 240 |
| Body Temperature | 32-40$^{o}$C | 5 | 12 | 0.0024 |
| TOTAL: | Assuming an intra-BAN network consisting of one of each type of sensor, then **30KB** packet generated every 1 second | | | |

# Chapter 4
# Simulations & Results

## 4.1 Simulation Setup

The simulations were all designed in MatLab for more flexible control over simulation parameters. The initial simulations were run in 1 second time steps with varying AP placement and numbers, pause times, and walk patterns to analyze the increase in link availability by incorporating the secondary backup radio. Secondary simulations were run at a 1 ms time step in order to incorporate both Wi-Fi and Bluetooth protocol details including the exchange of control frames and data frames. One millisecond was chosen as the time step as it was still short enough to maintain the integrity of the protocols but long enough to keep the simulations within a reasonable amount of time.

Next, each combination of parameters was simulated five times with the average, maximum and minimum values recorded. The values that appear in all the simulation

results and plots are these average values from five repetitions of the same simulation environment.

Last, because most people spend most of their time at home, we simulate a user moving through a home environment consisting of one Wi-Fi AP and one Bluetooth AP. The simulation area is also reduced from 500m x 500m to 50m x 50m to reflect the size of a household plot.

## 4.2 Performance Metrics

*Link availability* is measured as the ratio or percentage of total simulation time that a Wi-Fi or Bluetooth connection is available. A link is deemed 'available' if both the UL and DL channels are available and the respective receivers are able to distinguish a signal.

The secondary simulations incorporate more protocol details and thus we test the switching threshold to see potential effects. Some additional performance metrics used for the secondary simulations are *time overhead, power overhead* and *data lost*. The time and power overhead will be measured for the extraneous device discovery and reassociations needed to switch between the two radios. In reality, device storage is limited and to reflect that, we assume a 1MB FIFO transmission buffer at the aggregator. This buffer is used to store data when no connection is available. However, due to its limited size, data loss is still a reality if the user should undergo long periods of time outside the range of any AP (whether it is Wi-Fi and Bluetooth). Hence we measure data loss as 'un-transmitted' data that is accumulated then removed from the transmission buffer to make space for newer information.

## 4.3 Simulation Results

### *4.3.1 Initial Results*

The initial simulation results illustrate the effects of varying network density, AP placement, human mobility model, or pause times on the link availability for the multi-radio interface at the aggregator. In all the preliminary figures, the red line indicates the performance of Wi-Fi alone. The blue line indicates the performance of Wi-Fi and Bluetooth capitalizing on failed Wi-Fi Links (to be considered a failed link, either the UL or DL channel fails). The green link indicates the performance of Wi-Fi and Bluetooth capitalizing on both failed and unavailable Wi-Fi links. Therefore the differences between this lines will then indicate the added performance of incorporating the multi-radio interface for Cases 2 and 3 (failed and unavailable link failure respectively) in Figure 3.9.

Initially, we look at the effect on the link availability through the Random and Levy walk patterns. Simulation was conducted in a network environment with 100 Wi-Fi APs and between 0 and 100 Bluetooth APs all in an ordered placement fashion. The Levy walk pattern is characterized by a number of long flights balanced by short flights whereas the random walk pattern is characterized by a large number of short and long flights. It is therefore highly variable in comparison to the Levy walk pattern. Simulations have also illustrated this higher degree of variability in random walks. The random walk plot has a larger difference between the minimum and maximum results creating this comparatively erratic plot. The levy walk, on the other hand, is much more stable and with a smaller min-max interval range. However, we see a slight decrease in availability at the simulations with 100 Wi-Fi APs and 75 Bluetooth APs. One thing to note here is

the wider range of the min-max interval. This simulation was repeated 5 times and there were simulations that did pull this level down. With a higher simulation repetition we would expect to see a consistently increasing availability time with the addition of more APs due to more coverage area.

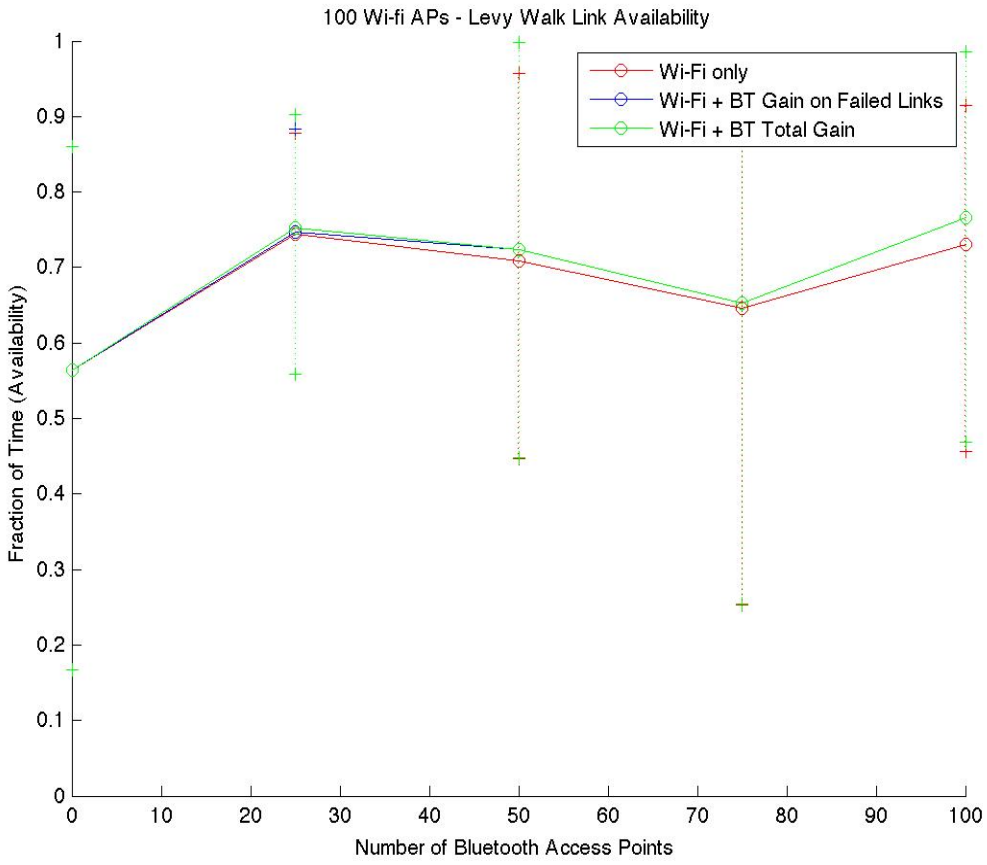


***Figure 4.1: Simulation Results with Levy Walk Mobility model***

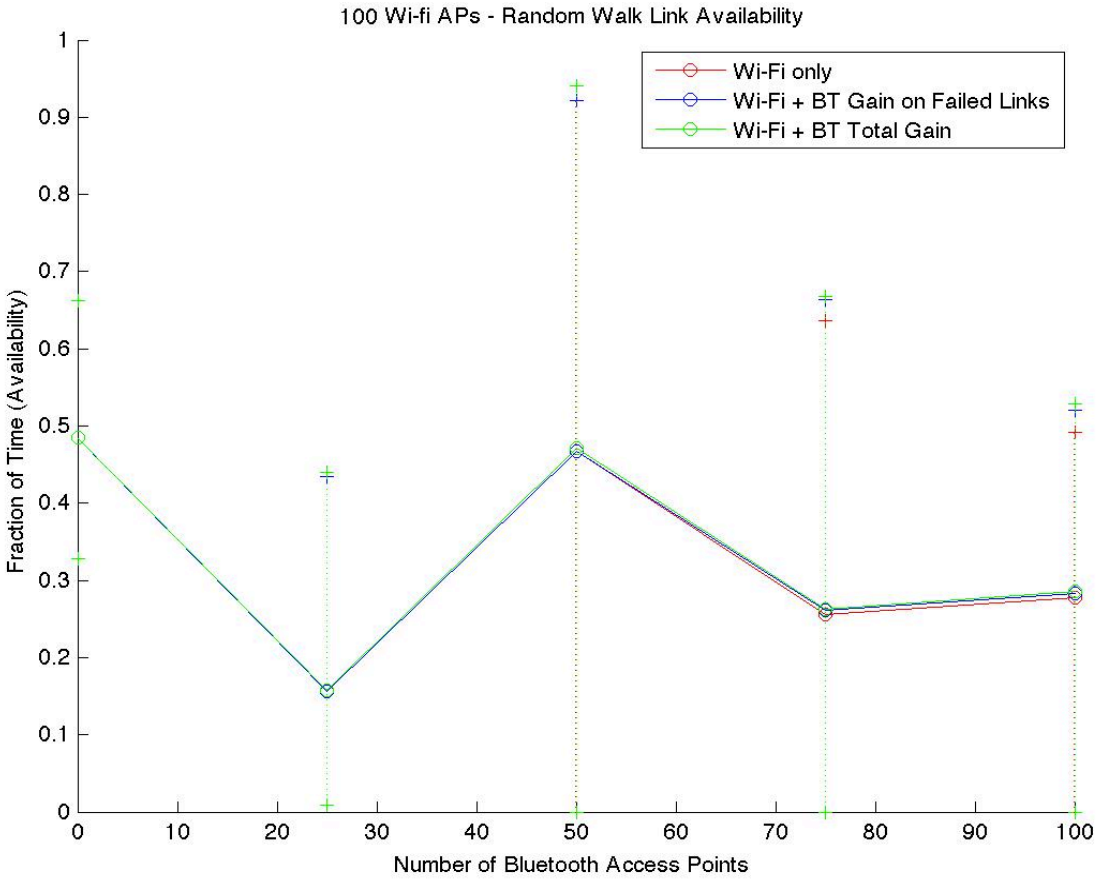


***Figure 4.2: Simulation Results with Random Walk Mobility model***

Next we look at the effect that AP Placement plays into link availability. We analyze both a random placement and ordered placement of Wi-Fi and Bluetooth APs. The main difference to note is that the ordered placement of APs already tries to optimize AP coverage and thus there is less to gain from the addition of a secondary network. With the random arrangement of APs, we have link availability gains ranging from approximately 10%-20% compared to 5%-10% for the ordered arrangement. This is not to say that there is nothing to gain from additional APs in the ordered arrangement, it is limited due to the coverage area optimization.

Another point to note is there is a difference in how one gains additional link availability in each network. The difference between the red and blue is the gain on Wi-Fi failed links by utilizing the Bluetooth radio. The difference between the blue and green is the gain on unavailable Wi-Fi links. In the ordered arrangement of APs, the Wi-Fi APs are already arranged in such a way to optimize coverage, thus, there are few areas in the simulation region outside the range of a Wi-Fi AP. This limits the gain on unavailable links (or blue-green difference). This also implies that most of our failures then arise from poor channel quality and failed Wi-Fi links (red-blue difference). With the random arrangement of APs, we observe the opposite effect. Because there is no network planning strategy to dictate Wi-Fi AP locations, we have larger areas in the simulation region without AP coverage. Therefore we see a larger gain on unavailable links versus failed links.

Last, similar to the walk pattern results described previously, we also see a high degree of variability in the range of the min-max interval for the random placement of APs in comparison to the ordered arrangement. Again, this is once again due to the random nature of the network compared to the coverage-optimized nature of the ordered arrangement.

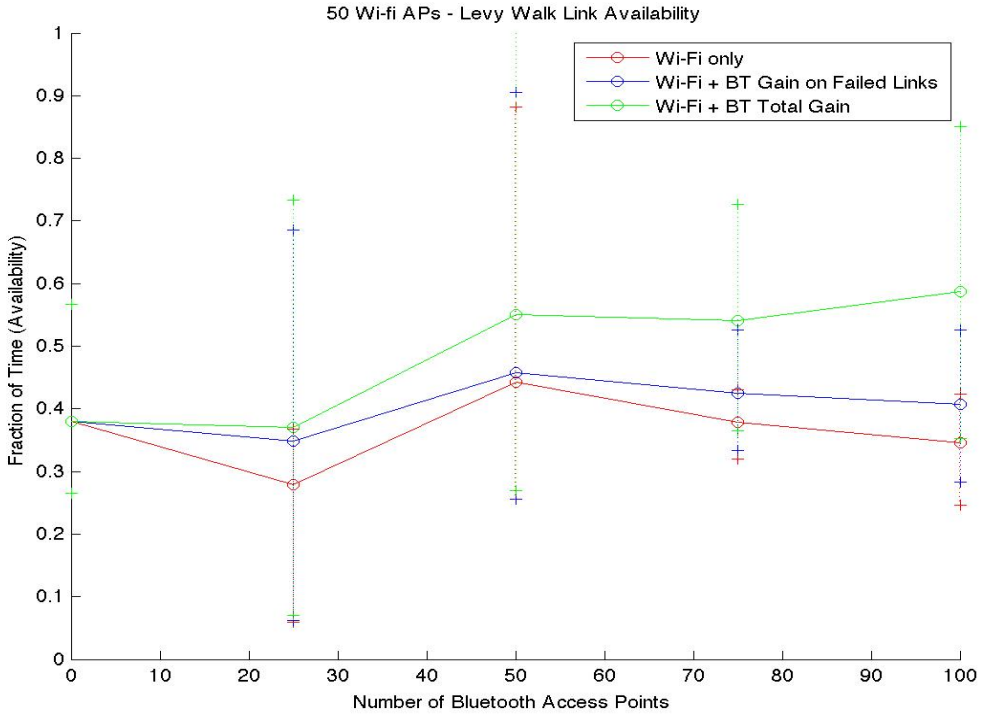


***Figure 4.3: Simulation Results with Random AP Placement***

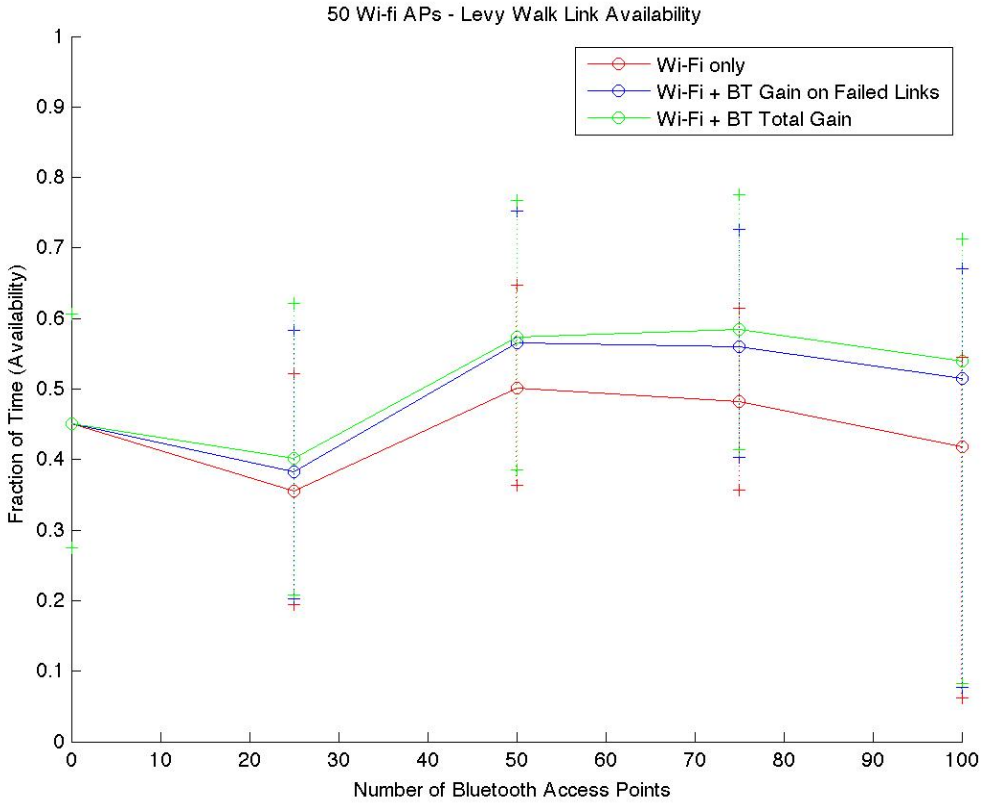


***Figure 4.4: Simulation Results with Ordered AP Placement***

Variations in network density are also simulated. We expect that with a very dense network (or one that is saturated with APs), that a primary link will almost always be available. A sparse network, on the other hand, will have more to gain by having an additional secondary radio interface. Upon simulation, we see that there is an approximately 5% - 35% gain in link availability for a sparse network compared to the negligible gain for a dense network. A moderately dense network simulated with the same parameters can be seen in Figure 4.3. As expected, as more primary APs are available, the less likely the secondary radio interface will be used. As we increase network density, we also see less relative gain on unavailable links and more relative gain on failed links. This is due to the increase in primary network coverage (more Wi-Fi APs).

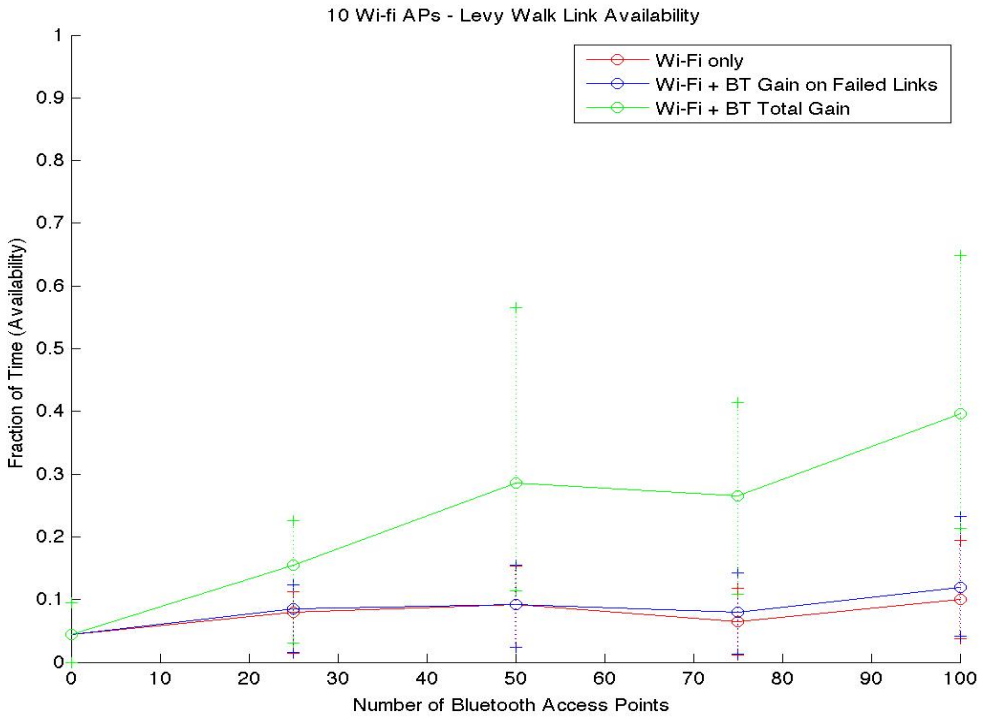


***Figure 4.5: Simulation Results in a Sparse Network***

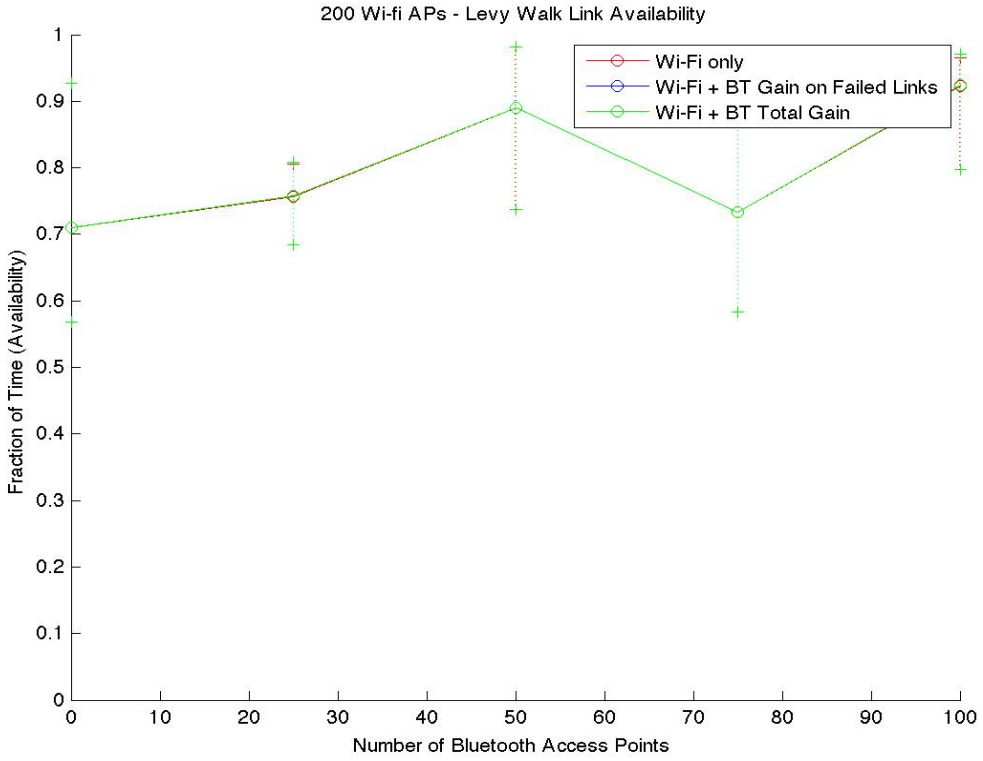


***Figure 4.6: Simulation Results in a Dense Network***

Last, we simulate the effects of static or dynamic human mobility by varying the pause times in a moderate network of 50 Wi-Fi APs and 50 Bluetooth APs. A larger and smaller pause time represents a static and dynamic user respectively. While not very obvious, we do see an upward trend in availability as a user becomes more static. This is due to a lesser need to reassociate and a more consistent connectivity due to less movement. We would expect if we were to further increase pause times, that this trend would become more visible.

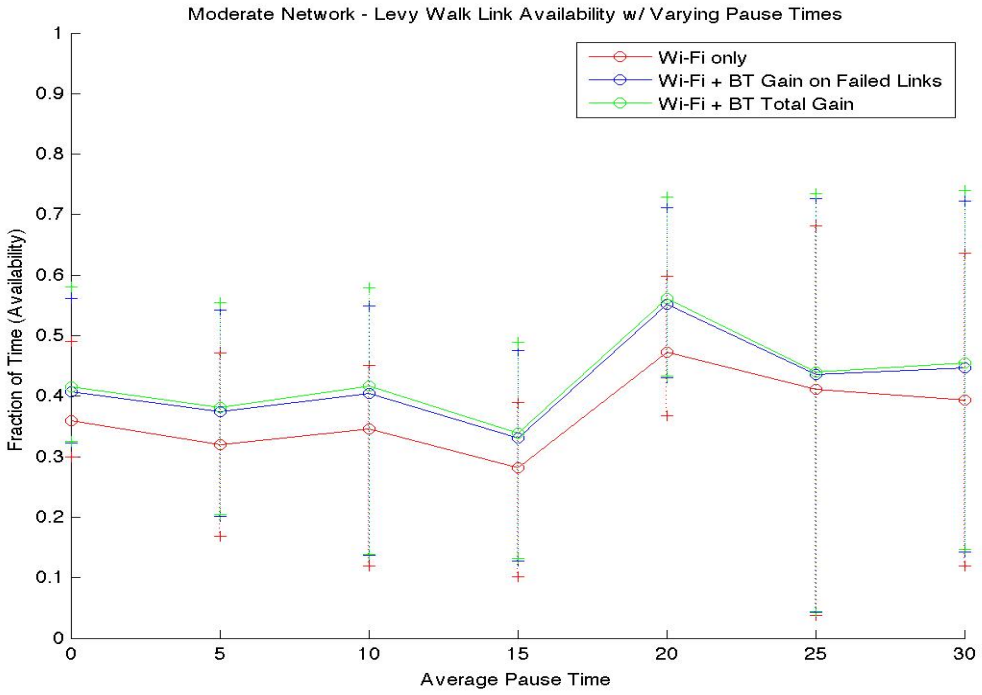


***Figure 4.7: Simulation Results with Various Pause Times (Levy Walk)***

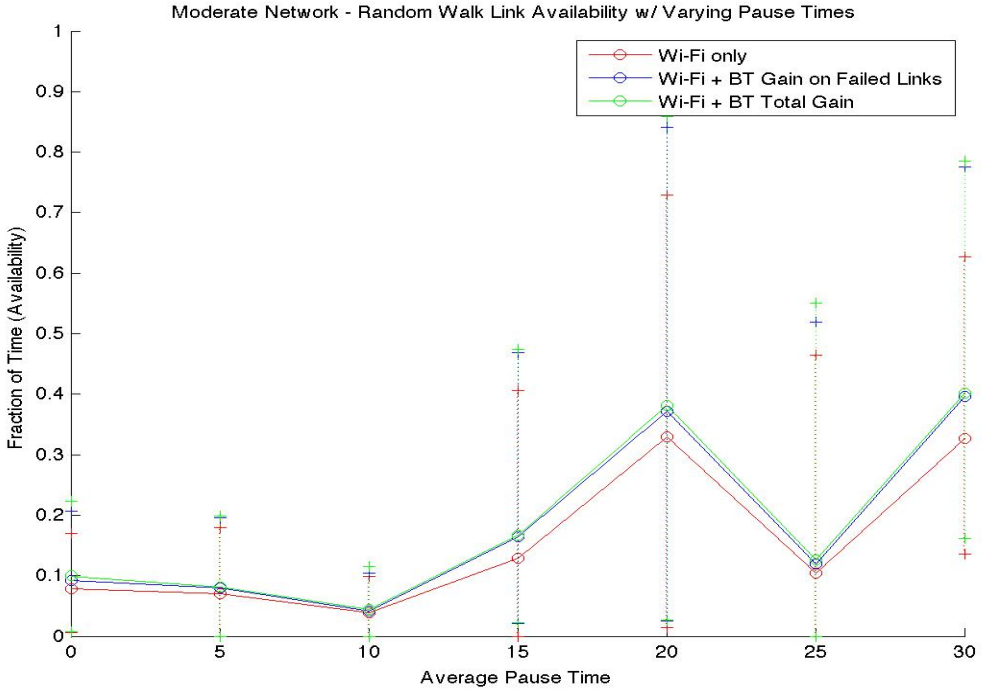


***Figure 4.8: Simulation Results with Various Pause Times (Random Walk)***

### 4.3.2 Secondary Results

The secondary simulations bring the simulation time step down to 1ms from the previous 1 second. The multi-radio protocol and corresponding inter-radio handover or switch is analyzed in more detail as well.

First, the link availability gain is analyzed for a sparse, moderate and dense network with a varying number of Bluetooth APs and 10, 100 and 200 Wi-Fi APs respectively. Similar to what was observed in the preliminary simulations, we find that a sparse network has a larger secondary radio gain compared to it's dense network counterpart with a negligible gain. With the high number of Wi-Fi APs in the dense network, there are fewer 'dead-zones' or areas not within the range of an AP. During the user walk, they would most likely be within range of a primary radio AP, reducing the need for a secondary radio. However, link availability gains ranging from approximately 10%-35% are apparent in a sparse network as more Bluetooth APs are available.

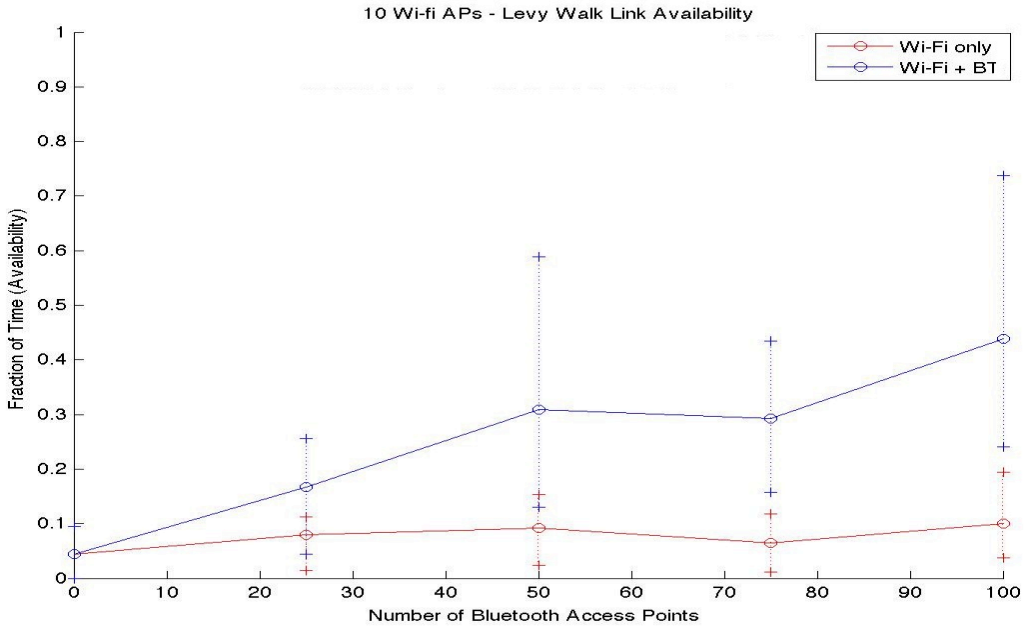


***Figure 4.9: Secondary Simulations in Sparse Network***

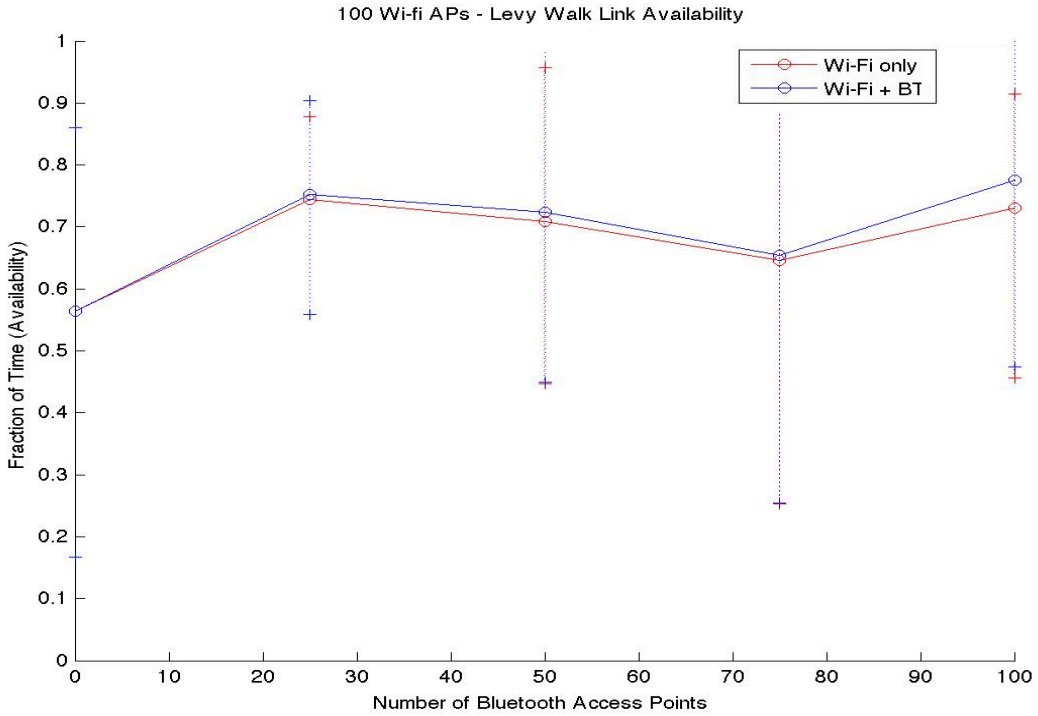


***Figure 4.10: Secondary Simulations in Moderate Network***

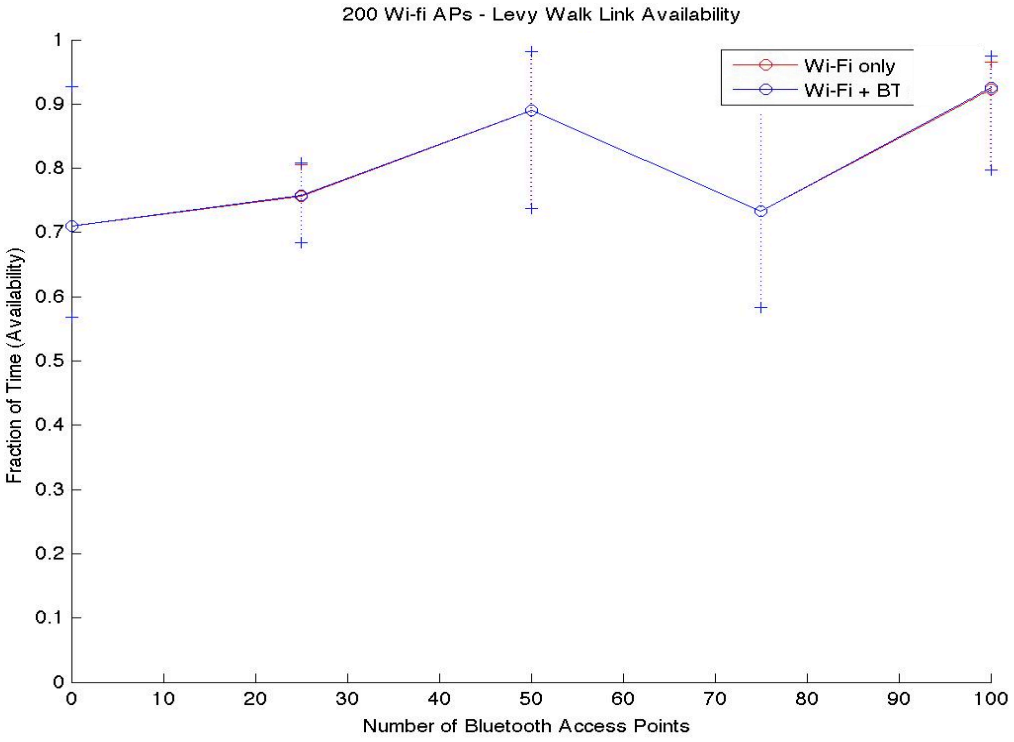


***Figure 4.11: Secondary Simulations in Dense Network***

Previously, all secondary simulations were conducted with a 5 second Wi-Fi reassociation retry attempt duration. Simulations were then conducted with a lower and

higher retry duration to see the effects of delaying or advancing the inter-radio handover or switch. All were simulated in a moderate network of 50 Wi-Fi APs and varying Bluetooth APs all in the ordered arrangement. Additionally, the user follows the Levy walk mobility model.

By advancing the inter-radio handover (or reducing the retry duration to 1 second), the link availability is increased by approximately 3-6%. The opposite happens as a result of delaying the handover. By initiating a handover quicker, the user is able to utilize the secondary Bluetooth radio quicker as well resulting in the higher link availability. However, this comes at a significant time and power overhead cost. Because of this advanced handover, the Bluetooth radio is initiated quicker after a Wi-Fi failure leaving less time for the Wi-Fi link to recover. Bluetooth has a high discovery period, which the user has to sustain after an inter-radio handover. This is what causes the higher time overhead. Furthermore, during this Bluetooth device discovery phase, we also have to account for the power overhead incurred during this time. Because of this relation between time and power overhead, a similar trend is observable in figures 4.13 and 4.14. Furthermore, while the advancement of the handover may have time and power costs, it comes with the added benefit of a higher throughput or fewer lost packets. By delaying the handover, the multi-radio BAN controller is taking the risk that the transmission buffer may overflow due to no viable connection. By initiating a switch earlier, it is taking a proactive approach to maintaining a constant connection and thus minimizing the packets in the buffer.

Depending on the user, the multi-radio protocol can then be fine tuned for a power-savings approach or a higher throughput approach by delaying or advancing the handover respectively.

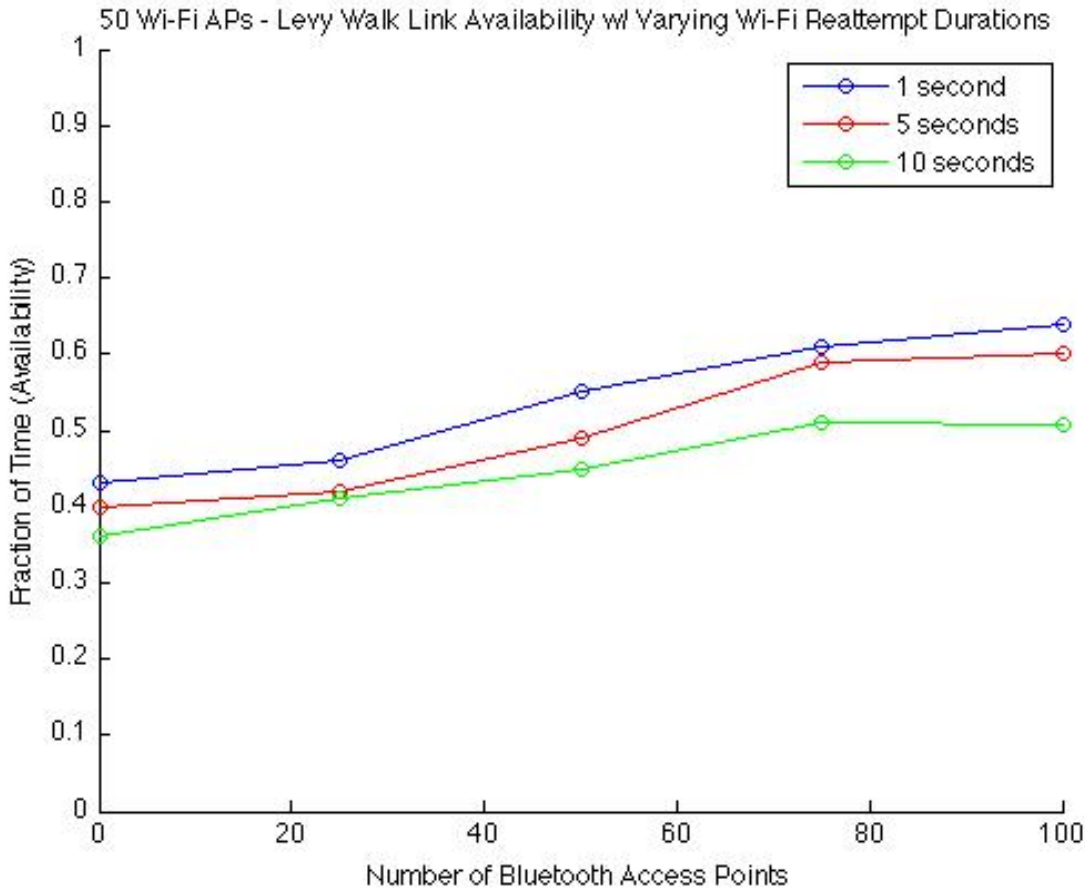


***Figure 4.12: Secondary Simulations with Varying Wi-Fi Reattempt durations***

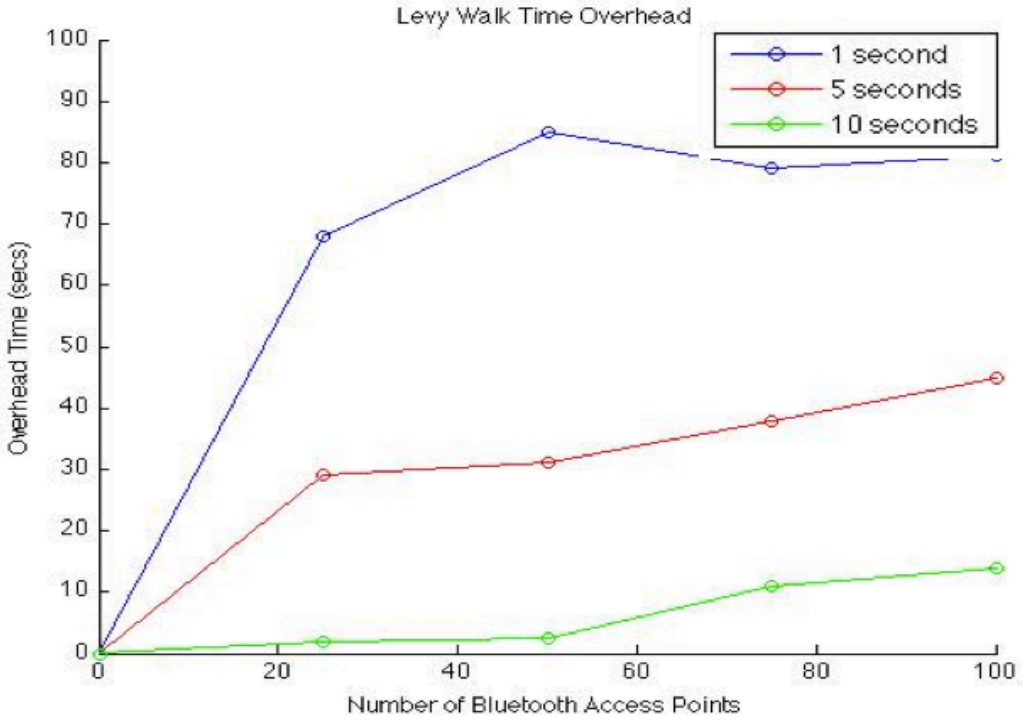


***Figure 4.13: Secondary Simulations Time Overhead Costs with Varying Wi-Fi Reattempt Durations***

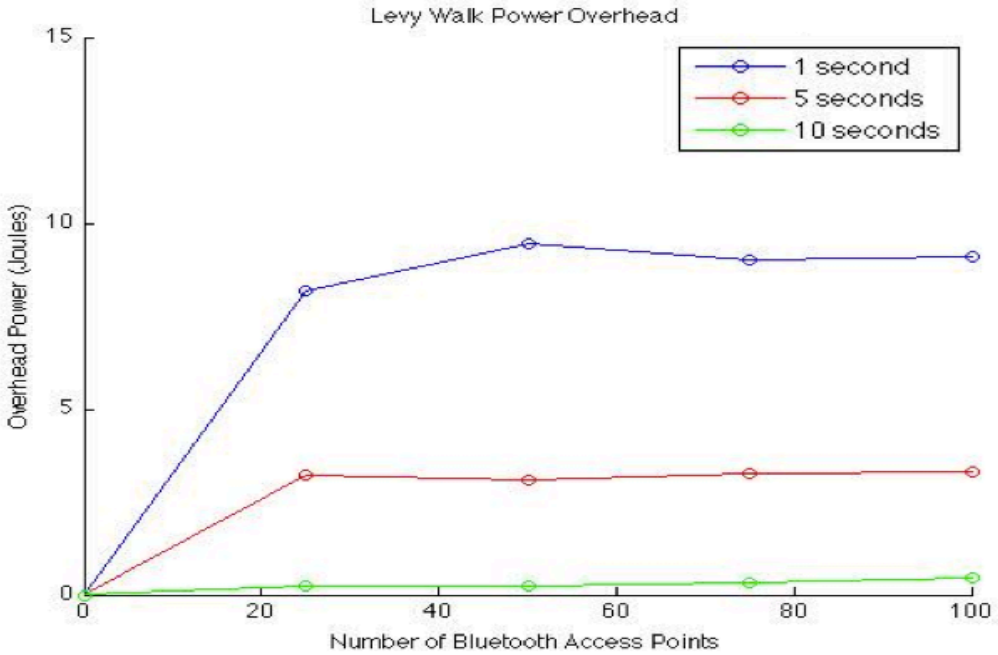


***Figure 4.14: Secondary Simulations Power Overhead Costs with Varying Wi-Fi Reattempt Durations***

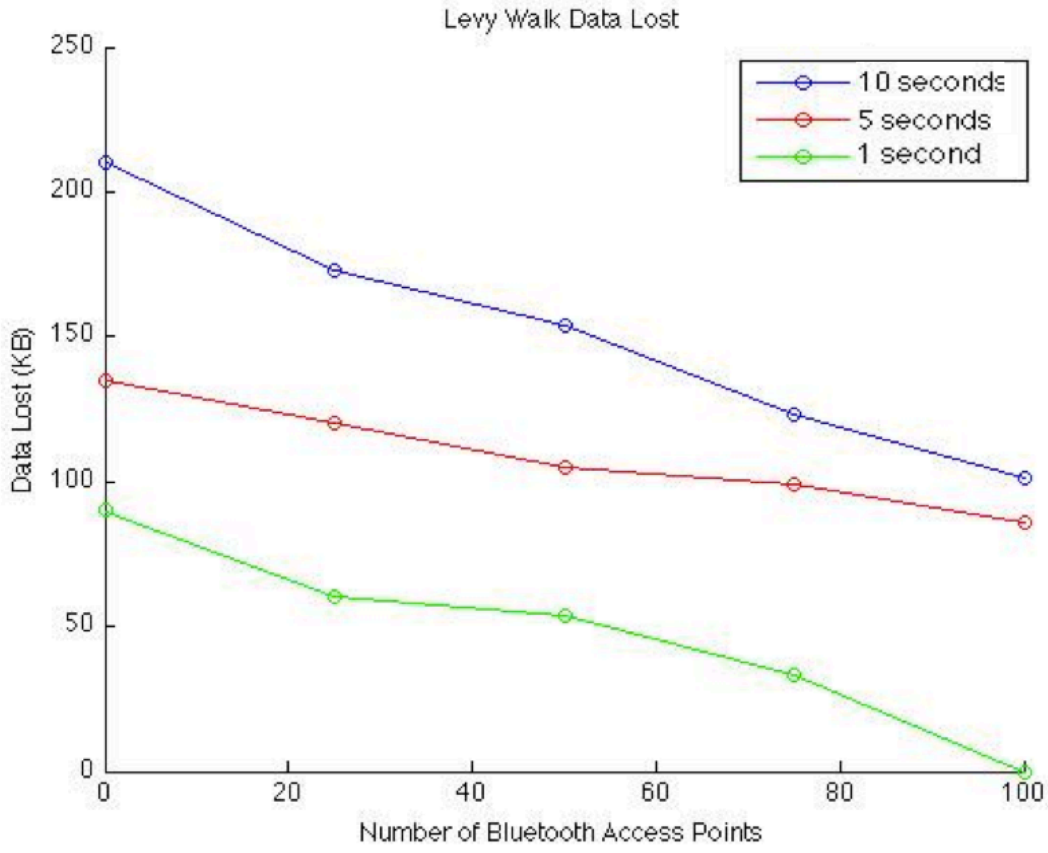


***Figure 4.15: Secondary Simulations Data Loss with Varying Wi-Fi Reattempt Durations***

### 4.3.3 Home Network Results

Last, a home network is simulated with a single Wi-Fi and Bluetooth AP in a 50m x 50m simulation area representing a house. Although the link availability is already very high with just Wi-Fi (averaging 90% of the time), the secondary Bluetooth radio offers an additional 3% of link availability. This shows that even for highly reliable networks such as Wi-Fi networks in our homes, the addition of a second radio interface does in fact bring us closer to having a continuous end-to-end communication link.

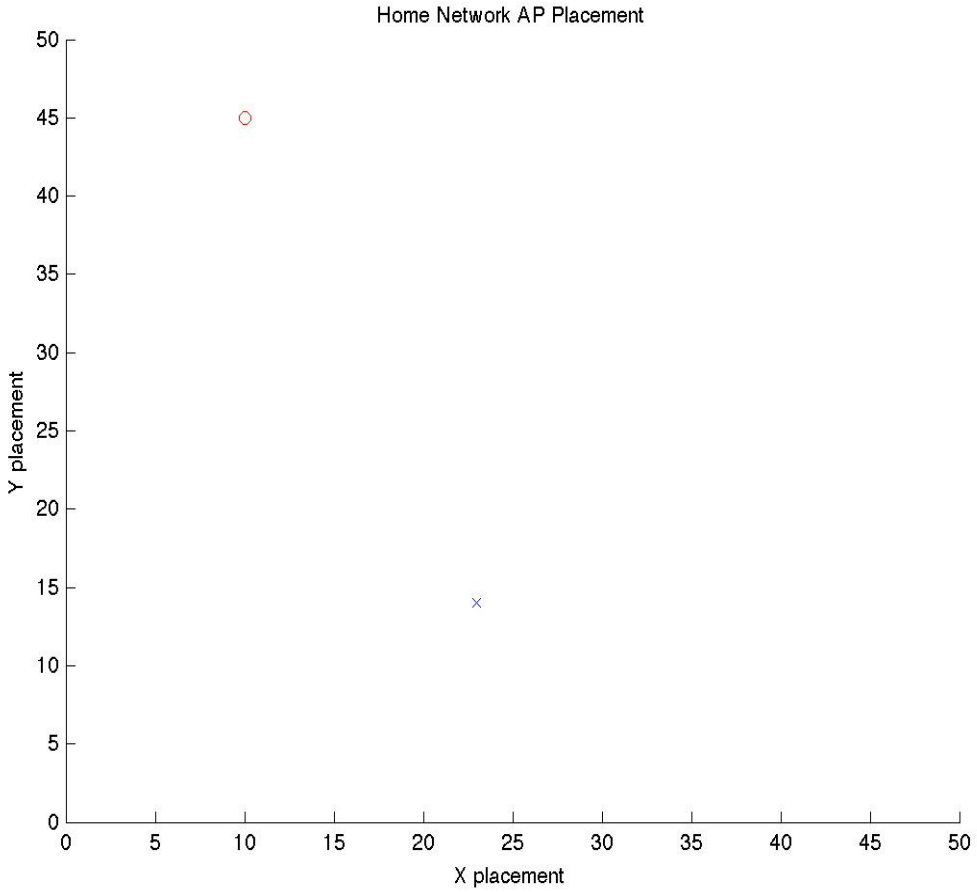


***Figure 4.16: Home Network Simulation Access Point Placement (Blue – Bluetooth, Red - Wi-Fi)***

***Table 4.1: Home Network Simulation Results***

| Mode | Fraction of Time Available | | |
|---|---|---|---|
| | Min | Mean | Max |
| Wi-Fi Only | 0.86 | 0.90 | 0.95 |
| Wi-Fi and Bluetooth Gains on Failed Links | 0.87 | 0.92 | 0.98 |
| Wi-Fi and Bluetooth Total Gain | 0.89 | 0.93 | 0.99 |

# Chapter 5
# Conclusion & Contribution

## 5.1 Summary & Concluding Remarks

Body Area Networks are showing great promise in the field of home healthcare and patient monitoring. However there still exist a few obstacles preventing wide scale BAN adoption ranging from biocompatible sensors, network congestions and failures, security, limited power sources and many more. One of those includes reliable end-to-end communications for real-time patient monitoring.

This thesis' contribution is a multi-radio protocol utilizing a Wi-Fi and Bluetooth radio to improve link availability. With real-time data transmission, it is critical to have a continuous link; however, if that is not an option, an active multi-radio approach to finding a viable link is presented. The protocol uses a multi-radio BAN controller linked to the Wi-Fi and Bluetooth MAC, Link, and Transport Layers to control a shared

transmission buffer, route data through the appropriate protocol stack and activate the desired radio after a handover decision. Handover decisions are made when the active protocol loses a viable connection and exceeds a retry threshold.

The proposed multi-radio protocol has shown significant improvements of up to 35% in link availability for sparse networks with large gaps in primary network coverage. A secondary radio opens up the possibility for the aggregator to actively search for an alternative if it happens to be in a primary network 'dead-zone' or experiencing poor channel quality on its primary link. As the network density increases, the coverage area of the primary network also increases, thus reducing the need for a handover to the secondary link. However, as the density increases, the Bluetooth gains also shift from capitalizing on unavailable links to failing links. Essentially, a higher network density means that the BAN aggregator will more likely be in the range of a Wi-Fi AP, however, there is still the possibility of a poor channel.

Simulations were conducted to test the effects of adjusting the switching or handover threshold. Advancing the handover from the primary to secondary link has the advantage of preventing transmission buffer overflows, fewer lost data packets and maintaining the real-time patient monitoring notion. The cost of doing so is a higher time and power overhead attributed to the high worst-case device discovery time for the Bluetooth protocol. On the other hand, if power conservation is crucial, one can delay the handover at the risk of higher packet loss and a lower throughput.

## 5.2 Future Work

The work done for this thesis has highlighted the capability of multi-radio wireless systems on improving end-to-end communications for real-time patient monitoring. However co-channel users and noise were two factors left out. Further simulations to incorporate these two issues can be conducted to further illustrate a more realistic network environment.

Furthermore, strict inter-radio handover thresholds were used in the proposed protocol. However, if we incorporate a learning algorithm with the option of radio power control, there may be an additional improvement on link availability. This learning algorithm could be trained on the spatial and temporal walk patterns of the BAN user and build a small database of network topology and congestion patterns. Additionally, Bluetooth to Wi-Fi switching thresholds were held at a constant 3 retry attempts. Simulations could be conducted to experiment with this value to discover the effects of delaying and advancing this type of inter-radio handover.

Lastly, different protocols could be tested in various environments in order to find optimum combinations of radios for various regions. For example, one could simulate using various combinations of Bluetooth, Wi-Fi and HSPA in a larger region to analyze which would result in a higher performing multi-radio system. The results of this thesis have provided a good starting point for further evaluations of wireless multi-radio interfaces.

# *References*


[1] D. Blumenthal, B. Chaiken, S. Shah, (Jan. 14, 2010) *10 Healthcare IT Trends to Watch in 2010*. [Online] Available: http://www.healthcaretechnologyonline.com/article.mvc/10-Healthcare-IT-Trends-To-Watch-In-2010-0001

[2] WHO Statistical Information System, *World Health Statistics 2005-2011*, [Online], Available: http://www.who.int/whosis/whostat/en/

[3] G.Z. Yang, "Chapter 1: Introduction," in *Body Sensor Networks*, 1st ed. London, UK: Springer – Verlag London Limited, 2006, pp. 1-40.

[4] X. Shen, N. Kato, X. Lin, "Wireless Technologies for e-Healthcare [Guest Editorial]," in *IEEE Wireless Communications*, Vol. 17 (1), Feb. 2010, pp. 10-11.

[5] YM. Fang, "Wireless Healthcare: Technologies for Bettering our Life [Message from the Editor-in-Chief]," in *IEEE Wireless Communications,* Vol. 17 (1), Feb. 2010, pp. 2-3.

[6] B. Latre, B. Braem, I. Moerman, C. Blondia, P. Demeester, "A survey on Wireless Body Area Networks," in *Journal of Wireless Networks,* Vol. 17 (1), Jan. 2011.

[7] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, V.C.M. Leung, "Body Area Networks: A Survey," *Mobile Network Applications*, 2010 ©Springer Science + Business Media, LLC. DOI: 10.1007/s11036-010-0260-8.

[8] G.Z. Yang, "Chapter 2: Biosensor Design and Interfacing," in *Body Sensor Networks*, 1st ed. London, UK: Springer – Verlag London Limited, 2006, pp. 41-88.

[9] M.A. Hanson, H.C. Powell Jr., A.T. Barth, K. Ringgenberg, B.H. Calhoun, J.H. Aylor, J.Lach, "Body Area Sensor Networks: Challenges and Opportunities," in *Computer*, Vol. 42 (1), Jan. 2009, pp. 58-65. DOI: 10.1109/MC.2009.5.

[10] P. Khan, MA. Hussain, K. Kwak, "Medical Applications of Wireless Body Area Networks," in *International Journal of Digital Content Technology and its Applications*, Vol. 3 (3), Sept., 2009.

[11] M. Hollick, I. Martinovic, T. Krop, I, Rimac, "A Survey on Dependable Routing in Sensor Networks, Ad Hoc Networks, and Cellular Networks," in *Proceedings of the 30th EUROMICRO Conference*, France, Aug 31- Sept 4, 2004, pp. 495 – 502.

[12] D. Siewiorek, R. Chillarege, Z.T. Kalbarczyk, "Reflections on Industry Trends and Experimental Research in Dependability," in *IEEE Trans. on Dependable and Secure Comm.,* Vol. 1(2), 2004, pp 109-127.

[13] A. Taherkordi, M.A. Taleghan, M. Sharifi, "Dependability Considerations in Wireless Sensor Network Applications," in *Journal of Networks,* Vol. 1 (6), 2006 .

[14] M.A. Hanson, H.C. Powell Jr., A.T. Barth, K. Ringgenberg, B.H. Calhoun, J.H. Aylor, J.Lach, "Body Area Sensor Networks: Challenges and Opportunities," in *Computer*, Vol. 42(1), Jan. 2009, pp. 58-65.

[15] A. Miu, H. Balakrishnan, C.E. Koksal, "Multi-radio Diversity in Wireless Networks," *Wireless Networks*, Vol. 13(6), 2007, pp.779-798.

[16] J. Lee, Y. Su, C. Shen, "Comparative Study of Wireless Protocols: Bluetooth, UWB, Zigbee, and Wi-Fi," in *Proceedings of the 33rd Annual Conference of the Industrial Electronics Society,* Taipei, Taiwan, Nov. 5-8, 2007, pp. 46-51.

[17] E. Ferro, F. Potorti, "Bluetooth and Wi-Fi Wireless Protocols: A Survey and a Comparison," in *IEEE Wireless Communications*, Vol. 12 (1), 2005, pp. 12-26.

[18] IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN MAC and PHY Specifications, IEEE 802.11 Standard, 2007. Including Amendment 5: Enhancements for Higher Throughput, IEEE 802.11n Standard, 2009.

[19] Specification of the Bluetooth System, Bluetooth Specification Version 4.0 (Vol. 0 – Vol. 6) Current Master TOC, June 30, 2010.

[20] S. Rathi, "Bluetooth Protocol Architecture," in *Dedicated Systems Magazine,* Q4 – 2000, pp. 28-33.

[21] Zigbee Specification, Zigbee Standards Organization, Document 053474r17, Jan. 17, 2008.

[22] J. Schiller, *Mobile Communications, 2nd Edition*. Essex, England: Pearson Education Limited, 2003.

[23] E. Dahlman, S. Parkvall, J. Skold, P. Berming, *3G Evolution: HSPA and LTE for Mobile Broadband, 2nd Edition.* Burlington, MA, USA: Elsevier Ltd., 2008.

[24] Y. Hovakeemian, K. Naik, A. Nayak, "A Survey on Dependability in Body Area Networks," in *Proceedings of 5th International Symposium on Medical Information & Communication Technology,* Montreux, Switzerland, March 27-30, 2011, pp. 10-14.

[25] A. Masoum, AH. Jahangir, Z. Taghikhaki, "Survivability Modeling of Wireless Sensor Networks," in *Proceedings of IEEE International Symposium on Wireless Communication Systems,* Reykjavik, Iceland, Oct. 21-24, 2008, pp. 593-597.

[26] GW. Skelton, A. Holton, "Survivability in Wireless Sensor Networks," in *Proceedings of IEEE SouthEast Con.*, Memphis, TN, USA, March 31 – April 2, 2006, pp. 341.

[27] C. Basile, M. Killijian, D. Powell, "A Survey of Dependability Issues in Mobile Wireless Networks," Technical Report, LAAS CNRS Toulouse, France, 2003.

[28] KS. Kwak, S. Ullah, N. Ullah, "An Overview of the IEEE 802.15.6 Standard," in *Proceedings of the 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies,* Rome, Italy, Nov. 7-10, 2010, pp. 1-6.

[29] D. Curiac, C.Volosencu, D. Pescaru, L. Jurca, A. Doboli, "A View Upon Redundancy In Wireless Sensor Networks," *in Proceedings of 8th WSEAS International Conference on Signal Processing, Robotics and Auto.*, 2009, pp. 341-346.

[30] N.D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, A.T. Campbell, "A Survey of Mobile Phone Sensing," in *IEEE Communications Magazine*, Vol. 48(9), Sept. 2010, pp. 140-150.

[31] S. Baskiyar, "A Real-Time Fault Tolerant Intra-Body Network," in *Proceedings of the 27th Annual IEEE Conference on Local Computer Networks*, Tampa, FL, Nov. 6-8, 2002, pp. 235-240.

[32] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications*, Vol. 17(1), pp. 51-58, February 2010.

[33] S. Saleem, S. Ullah, H.S. Yoo, "On the Security Issues in Wireless Body Area Networks," *in JDCTA: International Journal of Digital Content Technology and its Applications*, Vol. 3(3), 2009, pp. 178-184.

[34] A.D. Malloy, U. Varshney, A.P. Snow, "Supporting Mobile Commerce Applications Using Dependable Wireless Networks," in *Mobile Networks and Applications*, Vol. 7(3), 2002, pp. 225 – 234

[35] R. Gandhi, "Tolerance to Access-Point Failures in Dependable Wireless Local-Area Networks," in *Proceedings of 9th International Workshop on OO Real-Time Dependable Systems,* Capri, Italy, 2003, pp. 136-143.

[36] S. Hanna, "Regulations and Standards for Wireless Medical Applications," in *Proceedings of the 3rd International Symposium on Medical Information & Communication Technology*, Montreal, Canada, Feb. 24-27, 2009.

[37] E. Spadotto, J. Hawkins, K. Monrose, "ICT Convergence, Confluence & Creativity: The Application of Emerging Technologies for Healthcare Transformation," in *Proceedings of the 3rd International Symposium on Medical Information & Comm. Technology*, Montreal, Feb. 24-27, 2009.

[38] R. Gandhi, "Tolerance to Access-Point Failures in Dependable Wireless Local-Area Networks," in *Proceedings of 9th International Workshop on OO Real-Time Dependable Systems,* Capri, Italy, 2003, pp. 136-143.

[39] P. Bahl, A. Adya, J. Padhye, A. Walman, "Reconsidering Wireless Systems with Multiple Radios," in *ACM SIGCOMM Computer Communication Review*, Vol. 35(5), Oct. 2004, pp. 39-46.

[40] K. Chebrolu, R. Rao, "Communication Using Multiple Wireless Interfaces," in *Proceedings of IEEE Wireless Communications and Networking Conference,* Orlando, FL, March 17-21, 2002, pp. 327-331.

[41] G. Ananthanarayanan, I. Stoica, "Blue-Fi: Enhancing Wi-Fi Performance Using Bluetooth Signals," in *Proceedings of Mobisys '09,* Krakow, Poland, June 22-25, 2009, pp. 249-262.

[42] B. Raman, K. Chebrolu, R. Rao, "Network Layer approach to Enable TCP Over Multiple interfaces," in *Journal of Wireless Networks*, Vol. 11 (5), Sept. 2005, pp. 637-650.

[43] T. Pering, Y. Agarwal, R. Gupta, R. Want, "CoolSpots: Reducing the Power Consumption of Wireless Mobile Devices with Multiple Radio Interfaces," in *Proceedings of Mobisys '06*, Uppsala, Sweden, June 19-22, 2006, pp. 220-232.

[44] M. Caporuscio, D. Charlet, V. Issarny, A. Navarra, "Energetic Performance of Service-Oriented Multi-radio Networks: Issues and Perspectives," in *Proceedings of the 6th International Workshop on Software and Performance*, Buenos Aires, Argentina, Feb. 5-8, 2007.

[45] J. Gummeson, D. Ganesan, M. Corner, P. Shenoy, "An Adaptive Link Layer for Heterogeneous Multi-Radio Mobile Sensor Networks," in *IEEE Journal on Select Areas in Communications,* Vol. 28 (7), Sept. 2010, pp. 1094 – 1104.

[46] A. Farago, S. Basagni, "The Effect of Multi-Radio Nodes on Network Connectivity – A Graph Theoretic Analysis," in *Proceedings of 19th International Symposium on Personal, Indoor, and Mobile Radio Communications*, Cannes, France, Sept. 15-18, 2008, pp. 1-5.

[47] I. Rhee, M. Shin, S. Hong, K. Lee, S. Chong, "On the Levy walk Nature of Human Mobility," in *Proceedings of the 27th Conference on Computer Communications,* Phoenix, AZ, April 13-18, 2008, pp. 924- 932.

[48] K. Lee, S. Hong, S. Kim, I. Rhee, S. Chong, "SLAW: A New Mobility Model for Human Walks," in *Proceedings of INFOCOM 2009*, Rio de Janeiro, Brazil, April 19-25, 2009, pp. 855-863.

[49] C. Papageorgiou, K. Birkos, T. Dagiuklas, S. Kotsopoulos, "An Obstacle-Aware Human Mobility Model for Ad Hoc Networks," in *Proceedings of IEEE International Symposium on Modeling, Analysis & Simulation of Computer and Telecommunication Systems*, London, UK, Sept. 21-23, 2009, pp. 1-9.

[50] A. Cerpa, JL. Wong, L. Kuang, M. Potkonjak, D. Estrin, "Statistical Model of Lossy Link in Wireless Sensor Networks," in *Proceedings of the Fourth International*

*Symposium on Information Processing in Sensor Networks*, Los Angeles, CA, April 25-27, 2005, pp. 81-88.

[51] A. Gurtov, S. Floyd, "Modeling Wireless Links for Transport Protocols," in *ACM SIGCOMM Computer Communication Review,* Vol. 34 (2), April, 2004, pp. 85-96.

[52] AE. Khandani, J. Abounadi, E. Modiano, L. Zheng, "Reliability and route diversity in Wireless Networks," in *IEEE Transactions on Wireless Communications*, Vol. 7 (12), Dec., 2008, pp. 4772-4776.

[53] M. Ekpenyong, J. Isabona, "Probabilistic Link Reliability Model for Wireless Communication Networks," in *International Journal of Signal System Control and Engineering Application*, Vol. 2 (1), 2009, pp. 22-29.

[54] G. Carrozza, M. Cinque, D. Cotroneo, S. Russo, "Dependability Evaluation and Modeling of the Bluetooth Data Communication Channel," in *Proceedings of 16th Euromicro Conference on Parallel, Distributed, and Network-Based Processing*, Toulouse, France, Feb. 13-15, 2008, pp. 245-252.

[55] A. Konrad, B. Zhao, A. Joseph, R. Ludwig, "A Markov-Based Channel Model Algorithm for Wireless Networks," in *Journal of Wireless Networks*, Vol. 9 (3), May 2003, pp. 189-199.

[56] A. Kamthe, M. Carreira-Perpinan, A. Cerpa, "M&M: Multi-Level Markov Model for Wireless Link Simulations," in *Proceedings of the 7th ACM Conference on Embeded Networked Sensor Systems,* Berkeley, CA, Nov. 4-6, 2009.

[57] D. Griffith, M. Souryal, C. Gentile, N. Golmie, "An Integrated PHY and MAC Layer Model for Half-Duplex IEEE 802.11 Networks," in P*roceedings of Military Communications Conference,* San Jose, CA, Oct. 31- Nov. 3, 2010, pp. 1478-1483.

[58] Y. Ito, T. Taga, J. Muramatsu, N. Suzuki, "Prediction of Line-of-Sight Propagation Loss in Inter-vehicle Communication Environments," in *Proceedings of 18th International Symposium on Personal, Indoor, and Mobile Radio Communications,* Athens, Greece, Sept. 3-7, 2007, pp. 1-5.

[59] RW. Woodings, DD. Joos, T. Clifton, CD. Knutson, "Rapid Heterogeneous Ad Hoc Connection Establishment: Accelerating Bluetooth Inquiry Using IrDA," in *Proceedings of Wireless Communications and Networking Conference,* Orlando, FL, March 17-21, 2002, pp. 342-349 Vol. 1.

[60] J. Khan, M. Yuce, F. Karam, "Performance Evaluation of a Wireless Body Area Sensor Network for Remote Patient Monitoring," in *Proceedings of 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Vancouver, BS, Aug. 20-25, 2008, pp. 1266-1269.

[61] C. Yin, G. Wen, Z. Feng, "Simulation Research of 802.11n Channel Model D in NS2," in *Proceedings of 3rd IEEE International Conference on Computer Science and Information Technology,* Chengdu, China, July 9-11, 2010, pp. 530-533.

# *Appendix*

The following is a selection of a survey performed on commercially available chipset in order to derive transceiver parameters for simulation purposes (see Table 3.3). They are organized by Wi-Fi, Bluetooth, and Hybrid Mobile Chipsets and Wi-Fi and Bluetooth APs.

Wi-Fi Only Chipset:

| **Model Number** | **AirMagnet C1060** | | **Sagrad SG901-1071** | | **Cisco DPW632** | |
|---|---|---|---|---|---|---|
| Type | IEEE 802.11 a/b/g/n (2.4, 5GHz) | | IEEE 802.11 b/g/n (2.4GHz) | | IEEE 802.11b/g/n (2.4GHz) | |
| Transmitter Power (typical, unless otherwise stated) | 802.11a (5 GHz) | 14-15dBm | 802.11b, 1Mbps | 16.5 dBm | 802.11b | 17 dBm |
| | 802.11b (2.4GHz) | 16dBm | 802.11b, 11 Mbps | 16.2 dBm | | |
| | 802.11g (2.4GHz) | 16-17dBm | 802.11g, 9 Mbps | 18.2 dBm | 802.11g | 14 dBm |
| | 802.11n (2.4 GHz) | 12-13dBm | 802.11g, 54Mbps | 13.4 dBm | | |
| | 802.11n (5GHz) | 11-12dBm | 802.11n, MCS1 | 17 dBm | 802.11n | 14 dBm |
| | | | 802.11n, MCS7 | 13 dBm | | |
| Receiver Sensitivity (typical, unless otherwise stated) | 802.11a | -81dBm | 802.11b, 1Mbps | -96.3 dBm | 802.11b, 11Mbps | -91 dBm |
| | | | 802.11b, 2Mbps | -93.5 dBm | | |
| | 802.11b | -90dBm | 802.11b, 5.5Mbps | -91 dBm | | |
| | | | 802.11b, 11Mbps | -86.7 dBm | 802.11g, 54 Mbps | -77 dBm |
| | 802.11g | -82dBm | 802.11g, 9 Mbps | -89.6 dBm | | |
| | | | 802.11g, 18 Mbps | -85.9 dBm | | |
| | 802.11n (2.4GHz) | -77/-74 dBm | 802.11g, 36 Mbps | -78.6 dBm | 802.11n (20MHz), MCS7 | -73 dBm |
| | | | 802.11g, | -72.4 dBm | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 20MHz/ 40MHz | | 54 Mbps | | | |
| | 802.11n (5GHz) 20MHz/ 40MHz | -76/-74 dBm | 802.11n, MCS1 | -86 dBm | | |
| | | | 802.11n, MCS3 | -80 dBm | 802.11n (40MHz), MSC7 | -72 dBm |
| | | | 802.11n, MCS5 | -72 dBm | | |
| | | | 802.11n, MCS7 | -69 dBm | | |
| Data Rate | 300Mbps (max) w/ 40MHz Bandwidth (MCS15) | | 1Mbps ~150Mbps | | 300Mbps (max) w/ 40MHz Bandwidth (MCS15) | |
| Power Consumption | TX | 632mA (802.11n, 5GHz) | TX | 270mA | - | |
| | RX | 474mA (802.11n, 5GHz) | RX | 135mA | | |
| | Standby | 393mA (802.11n, 5GHz) | Standby | 2.5mA | | |
| | Sleep | 101mA (802.11n, 5GHz) | Sleep | 0.27mA | | |
| Operating Voltage | 3.3V (typical) | | 3.3V (typical) | | 3.3V (typical) | |

Bluetooth Only Chipset:

| Model Number | **National LMX9838** | | **Texas Instruments CC2540** | | **Blue Radios BR-C46AS** | |
|---|---|---|---|---|---|---|
| Type | Bluetooth Class 2 | | Bluetooth Low Energy Class 2 | | Bluetooth Class 2 | |
| Transmitter Power | Typical | 0 dBm | 4 dBm (max) | | 4dBm (max) | |
| | Max | 3 dBm | | | | |
| Transmitter Gain | -30dBm (max) | | -41 dBm (max) | | - | |
| Receiver Sensitivity | Typical | -80 dBm | Typical | -87 dBm | -82dBm (typical) | |
| | Max | -76 dBm | High Gain | -93 dBm | | |
| Receiver Gain | - | | 6 dBm (max) | | 5dBm (max) | |
| Max Data Rate | 900 kbps | | 1 Mbps | | 721 kbps (typical) | |
| Power Consumption | TX | 65mA | TX | 31.6mA | TX | 50mA |
| | RX | 65mA | RX | 22.1mA | RX | 40mA |
| | Standby | 1.1mA | Standby | 0.235mA | Standby | 1.4mA |
| | | | | | Sleep | 0.03mA |
| Operating Voltage | 3.3 V (typical) | | 3.6 V (max) | | 3.1 V (typical) | |

Combination Wi-Fi Bluetooth Chipsets:

| Model Number | **Delta Mobile MWL-41G2** | |
|---|---|---|
| Type | IEEE 802.11 b/g, Bluetooth V1.1 (Class 2) | |
| Transmitter Power (Wi-fi) | 16 dBm (typical | |
| Transmitter Power (Bluetooth) | 0dBm (typical) = 1mW | |
| Receiver Sensitivity (Wi-Fi) | 54 Mbps | -68 dBm |
| | 48 Mbps | -68 dBm |
| | 36 Mbps | -75 dBm |
| | 24 Mbps | -79 dBm |
| | 18 Mbps | -82 dBm |
| | 12 Mbps | -84 dBm |
| | 11 Mbps | -82 dBm |
| | 9 Mbps | -87 dBm |
| | 6 Mbps | -88 dBm |
| | 5.5 Mbps | -85 dBm |
| | 2 Mbps | -86 dBm |
| | 1 Mbps | -89 dBm |
| Receiver Sensitivity (Bluetooth) | -80dBm (typical) | |
| Max Data Rate | Wi-fi: 54Mbps Bluetooth: | |
| Power Consumption (Bluetooth) | 60mA (average when active) | |
| Power Consumption (Wi-fi) | TX | 250mA |
| | RX | 200mA |
| | Standby | 30mA |
| | Sleep | 5mA |
| Operating Voltage | 3.3 V | |

Wi-Fi AP:

| Model Number | **Cisco Aironet 1250 Series** | | **Aruba AP-105** | | **Meru AP 300** | |
|---|---|---|---|---|---|---|
| Type | IEEE 802.11 a/b/g/n (w/ 2 antennas) | | IEEE 802.11 n (high-density deployment) | | IEEE 802.11 a/b/g/n | |
| Transmitter Power (max) | 802.11 a | 17dBm | Limited to 23dBm (0.5dBm incremental configuration possible) | | 802.11 a | 13dBm |
| | 802.11 b | 23dBm | | | 802.11 b | 17dBm |
| | 802.11 g | 20dBm | | | 802.11 g | 17dBm |
| | 802.11 n (1 antenna) | 17dBm | | | 802.11n (2.4GHz) | 17dBm |
| | 802.11 n (2 antennas) | 20dBm | | | 802.11 n (5GHz) | 13dBm |
| Transmitter Gain | - | | 2.4GHz | 2.5dBi | 2.4GHz | 2.2dBi |
| | | | 5GHz | 4.0dBi | 5GHz | 3dBi |
| Receiver Sensitivity (@ Max Data Rates) | 802.11 a | -73dBm | 802.11 a | -83dBm | 802.11 a | -81dBm |
| | 802.11 b | -85dBm | 802.11 b | -93dBm | 802.11 b | -94dBm |
| | 802.11 g | -74dBm | 802.11 g | -83dBm | 802.11 g | -83dBm |
| | 802.11 n (2.4GHz) | -73dBm | 802.11 n (2.4/5 GHz, 20MHz) | -77dBm | 802.11 n (2.4GHz) | -74dBm |
| | 802.11 n (5GHz, 20MHz) | -72dBm | | | 802.11n (5GHz) | -72dBm |
| | 802.11 n (5GHz, 40 MHz) | -69dBm | | | | |
| Max Data Rate | 300Mbps | | 300Mbps | | 300Mbps | |

Bluetooth AP:

| Model Number | **Parani MSP1000** | **Bluecore4-PC-ROM WLCSP** | **Philips PH10491** |
|---|---|---|---|
| Type | Class 1 Bluetooth V2.0 Access Point | Class 2/3 Bluetooth V2.1 Chipset | Class 2 Bluetooth Chipset |
| External/ Internal | External | Internal | Internal |
| Transmitter Power | 17dBm | 6dBm (w/amplifier 35dBm) | 4dBm |
| Receiver Sensitivity | -88dBm | -86dBm | -85dBm |
| Max Data Rate | 3Mbps | 3Mbps | 3Mbps |