2018-06

LEVERAGING COMMERCIAL-OFF-THE-SHELF TECHNOLOGIES TO CREATE WIRELESS SENSOR NETWORKS TO AUGMENT AIR BASE GROUND DEFENSE

Wu, Caleb Y.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

LEVERAGING COMMERCIAL-OFF-THE-SHELF TECHNOLOGIES TO CREATE WIRELESS SENSOR NETWORKS TO AUGMENT AIR BASE GROUND DEFENSE

by

Caleb Wu

June 2018

Thesis Advisor: John H. Gibson
Co-Advisor: Gurminder Singh

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE LEVERAGING COMMERCIAL-OFF-THE-SHELF TECHNOLOGIES TO CREATE WIRELESS SENSOR NETWORKS TO AUGMENT AIR BASE GROUND DEFENSE	**5. FUNDING NUMBERS**
6. AUTHOR(S) Caleb Wu	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Forward-deployed maneuver sustainment operations, such as Forward Arming and Refueling Points (FARPs), are a critical center of gravity that adversaries seek to disrupt or destroy in order to jeopardize friendly scheme of maneuver and operations. With adversaries' increased ability to attack such operating bases through indirect fire and infiltration, it becomes more difficult for perimeter defense assets to maintain situational awareness in order to respond to threats. A low-cost wireless sensor network composed of Raspberry Pi nodes equipped with short-range radars, cameras, and motion sensors was built to give force protection personnel early warning and to help them maintain situational awareness. While each layer alone had flaws, deployment of the wireless network of sensor nodes using the defense in depth principle proved capable of not only providing early warning to defenders, but also giving defenders detailed imagery and kinetic information on the intruder.

14. SUBJECT TERMS Air Base Ground Defense, short range radar, OpenCV, Raspberry Pi, wireless sensor network, facial recognition	**15. NUMBER OF PAGES 71**
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

LEVERAGING COMMERCIAL-OFF-THE-SHELF TECHNOLOGIES TO CREATE WIRELESS SENSOR NETWORKS TO AUGMENT AIR BASE GROUND DEFENSE

Caleb Y. Wu
Captain, United States Marine Corps
BA, University of Chicago, 2011

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 2018

Approved by: John H. Gibson
Advisor

Gurminder Singh
Co-Advisor

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Forward-deployed maneuver sustainment operations, such as Forward Arming and Refueling Points (FARPs), are a critical center of gravity that adversaries seek to disrupt or destroy in order to jeopardize friendly scheme of maneuver and operations. With adversaries' increased ability to attack such operating bases through indirect fire and infiltration, it becomes more difficult for perimeter defense assets to maintain situational awareness in order to respond to threats. A low-cost wireless sensor network composed of Raspberry Pi nodes equipped with short-range radars, cameras, and motion sensors was built to give force protection personnel early warning and to help them maintain situational awareness. While each layer alone had flaws, deployment of the wireless network of sensor nodes using the defense in depth principle proved capable of not only providing early warning to defenders, but also giving defenders detailed imagery and kinetic information on the intruder.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ABGD	Air Base Ground Defense
CACTF	Combined Arms Collective Training Facility
COTS	Commercial-off-the-Shelf
FARP	Forward Arming and Refueling Points
IOT	Internet of Things
NPS	Naval Postgraduate School
PIR	Passive Infrared
SCC	Sensor Control Center
SRR	Short-Range Radar
TTP	Tactics, Techniques and Procedures
WSN	Wireless Sensor Network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I give thanks to God for helping me through the entire thesis process. Many thanks to my advisors, Woodie, and my wife for their support and encouragement throughout. This project could not have been possible without their steadfast support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MOTIVATION

Forward-maneuver sustainment operations, such as Forward Arming and Refueling Points (FARPs), are critical centers of gravity that our adversaries seek to disrupt or destroy in order to jeopardize friendly scheme of maneuver and operations. The recent 2012 attack by Taliban fighters on Camp Bastion, resulting in the destruction of multiple aircrafts, highlights the devastation that even a small infiltration force can wreak on a heavily defended forward operating base [1]. Our adversaries understand that degrading our air capability decreases our overall fighting prowess; they will therefore continue to seek proven methods to overcome our current air base ground defenses. With our adversaries' increased ability to attack such operating locations from greater distances and to infiltrate base defenses, it becomes more difficult for perimeter defense personnel to maintain situational awareness and properly identify and respond to threats. Technological advantages should therefore be leveraged to aid perimeter defense personnel in the ground defense of air bases.

B. PROBLEM DESCRIPTION

Since the introduction of flight to military operations, air bases have suffered attacks of various intensity. Attackers' tactics have evolved over the century with the advent of new technology and defensive tactics, techniques, and procedures (TTPs), but both conventional and unconventional forces have continued to target air bases. These actors have repeatedly exploited gaps in the defense in order to damage aircraft and impair air operations.

In Operations Enduring Freedom and Iraqi Freedom, as well as in many past conflicts, the value of distributed operations to cover a wide geographic area in order to shape the battle space was widely recognized. Distributed operations concepts enabled U.S. and allied forces to efficiently allocate forces for a wide range of tasks from civil operations to combat, as well as successfully engage with local population and defeat insurgencies. Despite such successes, inherent in dispersing forces is an associated risk to these forces,

equipment, and infrastructures, and the consequent requirement to protect forward elements. Often times, the troop-to-task ratio is less than optimal and there is not a sufficient quantity of troops to execute proper force protection in a deployed environment. In order to address the deficiencies caused by increasingly distributed operations, leveraging technological efficiencies in surveillance and early detection can help alleviate the shortfall in manpower. By doing so, we can better provide force protection in a forward-deployed setting, from small platoon sized patrol bases to large forward operating bases.

Currently, sensor networks to aid in surveillance and early detection are employed in the operating forces. For the Marine Corps, the most recently fielded system is the Tactical Remote Sensor System (TRSS), a sensor suite capable of detecting human and vehicle movement in real time [2]. However, as Chapter II of this thesis discusses in more detail, this system is both extremely costly and difficult to deploy at lower units. In response to the lack of an effective and affordable surveillance and early detection system, we seek to leverage commercial off-the-shelf platforms to build a wireless sensor network (WSN) with certain proof of concept capabilities that can address this gap.

C. THESIS ORGANIZATION

The remainder of this thesis investigates the problem of leveraging the Raspberry Pi platform equipped with a set of sensors to create a WSN in order to augment air base ground defense (ABGD). Chapter II provides a detailed examination of air base ground defense, including current tactics, techniques, and procedures (TTPs), lessons learned from past conflicts, and challenges faced today. Additionally, Chapter II discusses the basic architecture of a wireless sensor network, the capabilities and limitations of the Raspberry Pi as a sensor node, the features of the OPS-241A short-range radar OPS-241A, and some routing protocols that are used for experimentation.

Chapter III presents the system architecture of our WSN and the functions that each component within the system will perform. It also discusses the communication protocols and mechanisms that the sensor nodes use to communicate with each other and to the command and control application server.

Chapter IV presents the experimental results, including a detailed discussion of the capabilities and limitations of our WSN during actual field testing. Chapter V concludes the research report, identifying areas where additional research is warranted.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LEVERAGING COMMERCIAL-OFF-THE-SHELF PLATFORMS TO AUGMENT AIR BASE GROUND DEFENSE

This chapter provides an in-depth analysis into the history of air base ground defense, the TTPs currently employed to defend air bases, and the future threats to air bases and FARPs. Following this analysis, this chapter presents background information on several components of a WSN and the networking protocols that are used to build our experimental WSN for augmenting ABGD.

A. AIR BASE GROUND DEFENSE

General Giulio Douhet, an Italian strategic air power theorist of the early 20th century, famously stated in 1921 that "it is easier and more effective to destroy the enemy's aerial power by destroying his nests and eggs on the ground than to hunt his flying birds in the air" [3]. Degrading an adversary's air power and projection capability by destroying or disabling its aircrafts, air bases, and support infrastructure on the ground instead of engaging aircrafts in flight presents an advantage that is readily evident. Simply put, aircraft are much harder to kill in the air than on the ground. In order to successfully project strategic power, enable distributed operations, and ensure tactical success, the U.S. military relies heavily on its air capabilities. As a result, an adversary, whether an insurgency or a peer competitor like China or Russia, possesses a keen interest in disrupting our military's air operations to aid battlefield success. Moreover, such tactics also undermine domestic political support and demonstrate allied vulnerability. Therefore, the physical security of forward air bases, regardless of their size, must be a priority to guarantee air superiority in any level of conflict.

Over the last century, the conduct of warfare has undergone significant changes as traditional front lines and massed attacks against largely distinct battle fronts gave way to more distributed battlefields. Operating in a distributed setting involves covering enormous physical areas with smaller forces in an attempt to outmaneuver the enemy by exploiting speed and tempo. For the United States, the value of distributed operations covering a wide geographic area in order to shape the battlespace was widely recognized during Operations

Enduring Freedom and Iraqi Freedom. Distributed operations concepts enabled U.S. and allied forces to efficiently allocate forces for a wide range of tasks from civil operations to sustained combat, as well as successfully engage with local population and defeat insurgencies. The U.S. military was only able to capitalize on the battlefield advantages of distributed operations because it had air dominance, which consequently enabled freedom of maneuver across the battlespace. However, if this decisive advantage in air superiority were to be degraded or no longer guaranteed, the effect would permeate to both ground and sea operations, with the potential for mission failure.

At present, the shift of strategic focus to the Pacific theater area of operations in order to balance a more aggressive China poses an ongoing problem regarding how the U.S. military may successfully adapt itself to meet future challenges. Distributed operations will continue to play a pivotal role as the Marine Air Ground Task Force (MAGTF) evolves to meet the demands of complex terrain requiring movement across large distances. Forward Arming and Refueling Points (FARP) in particular will be a critical logistical support structure for aircraft to rapidly refuel and continue missions. These small, makeshift air bases are far less costly to establish and maintain. More importantly, they can be deployed rapidly across the area of operations to support distributed operations. At the same time, FARPs are soft target opportunities that the enemy is likely to exploit. Aircraft require intensive supply and maintenance support, so damage or sabotage of such logistical bases might significantly hamper air operations.

The remainder of this section on air base ground defense discusses the following:

1. A brief history and evolution of threats to air bases over the past century;
2. An analysis of the current tactics, techniques, and procedures (TTP) for air base ground defense; and
3. A look into future threats to air bases.

1. History and Evolution of Threats to Air Bases

Since the first use of aircraft as weapons of war, adversaries have sought to exploit the critical vulnerability of inadequately protected air bases of various sizes. Major Michael Buonaugurio, in his study of air base defense in the 21st century, reports the following statistics on the frequency and objective of documented air base attacks:

> Since World War II, 645 attacks, damaging or destroying over 2000 aircraft have occurred. The preponderance of these attacks occurred during Vietnam (76%). Historical data on the 645 documented air base attacks compiled since World War II can be evaluated in terms of aggressor's objectives in the following categories: destroy the aircraft (60%), harass the defenders (27%), deny use of the airfield (7%), and capture the airfield (6%). The most likely occurring scenario that a defender would encounter is an attempt to destroy aircraft or harass the defenders. [3]

A separate RAND Corporation report by Alan J. Vick [1] classifies air base attacks by type of attacks, damage done, etc. Table 1 highlights that air base attacks are a common tactic, used by a diverse array of state and non-state actors in varying intensities of conflict throughout history.

Table 1. Historical Survey of Attacks on Airfields. Adapted from [1].

Conflict or Operation	Airfield Attacker	Airfield Defender	Type of Attack	Aircraft Lost
Battle of Britain	Germany	Great Britain	Air	56
Operation Barbarossa	Germany	Soviet Union	Air	800
Attack on Peral Harbor	Japan	U.S.	Air	347
North African Campaign	British Special Forces	Germany	Commando	367
Operation Bodenplatte	Germany	U.S., U.K., Canada	Air	388
World War II	USN,USMC, USAAF	Axis Countries	Air	18,222
India-Pakistan War	Pakistan and India	India and Pakistan	Air	IAF: 35, PAF: 9
Six-Day War	Israel	Egypt, Syria, Jordan, Iraq	Air	400
Vietnam War	NVA, VC	U.S.	Mortar/rocket	1,578
Vietnam War	USAF	North Vietnam	Air	163
ODS	Allied coalition	Iraq	Air	151
OAF	NATO	Serbia	Air	100

During World War II, both sides systematically and intentionally attacked air bases, with the main purpose being the destruction or capture of enemy aircraft and airfields [3]. However, over the next several decades, the tactics of attacking air bases changed as both

objectives and technology evolved. Attackers have used various weapons available, including “aircraft, missiles, naval guns, artillery, mortars, rockets, satchel charges, and small arms” in order to accomplish this purpose [1]. Buonaugurio [3] uses the North Vietnamese and Vietcong strategy to attack U.S. air bases to illustrate this change in tactics. Rather than incurring large costs to destroy, infiltrate, or capture airfields, the North Vietnamese and Vietcong found standoff weapons and other forms of command-detonated explosives more effective. By staying outside of the base perimeter, these forces had more freedom of movement and were still able to damage aircraft, facilities, runways, and ultimately impair sortie rates [3].

Tactics to degrade, interfere with, and damage air bases and aircraft through standoff attacks and infiltration are effective, and often much less costly than direct capture and destruction of enemy air bases. As a result, these approaches are still exploited to a great extent in present times. Two cases from the Vietnam War and Afghanistan War are presented to illustrate the destruction that both conventional and unconventional forces delivered to U.S. air bases through infiltration and short-range standoff attacks.

Case I: Vietcong Attack on Bien Hoa Air Base, November 1, 1964

> An example of the potential effectiveness of mortars when used against aircraft parked on a crowded ramp is found in the November 1, 1964, VC attack on Bien Hoa AB. During the night of October 31, elements of a VC company emplaced six 81-mm mortars approximately 1,400 m north of the B-57 parking ramp. Over the course of a 20-minute attack that began shortly after midnight, the attackers fired somewhere between 50 and 65 rounds at multiple targets on the air base. They first struck the B-57 ramp, then a U.S. Army cantonment area, where four U.S. personnel were killed and 74 wounded. As shown in Figure 4.2, 13 of the mortar rounds landed on the B-57 ramp, destroying five B-57s, causing heavy damage to eight aircraft and light damage to another seven. An entire B-57 squadron was taken out of action in a single attack. [1]

Case II: Taliban Attack on Camp Bastion, September 14, 2012

> Since 2003, insurgent forces have launched at least 1,800 ground-force attacks on U.S. airfields in Iraq and Afghanistan, primarily with mortars or rockets. Standoff attacks have typically been quite small, with the attackers fleeing after firing a couple of rounds. For example, USAF data for attacks

> on Joint Base Balad in Iraq between 2004 and 2010 document that roughly 66 percent of attacks fired only one round and that approximately 87 percent of attacks fired one or two rounds. The largest attack recorded fired only 11 rounds. Although attempts to directly assault or penetrate the perimeter of air bases were infrequent, the one spectacular success by insurgents was via commando assault. This was the September 14, 2012 commando attack on Camp Bastion, Afghanistan, that destroyed six USMC AV-8B Harrier jets and damaged another two. A dozen or so Taliban, dressed in U.S. Army uniforms, penetrated the perimeter and then used rocket-propelled grenades and hand grenades to destroy aircraft. [1]

As these two cases and many similar throughout history indicate, air bases have always been vulnerable targets and will continue to require appropriate force protection. While air base attacks on the scale of World War II have been less frequent, perimeter penetration and standoff attacks remain highly utilized tactics, especially by a technologically inferior adversary. In fact, air superiority often forces adversaries to use such tactics in order to overcome the asymmetry in capabilities.

2. Tactics, Techniques, Procedures and Principles for Air Base Ground Defense

Colonel Shannon Caudill [4], in his book *Defending Air Bases in an Age of Insurgency*, predicts air bases will continue to be attacked in armed conflicts because the benefits of committing small teams to destroy expensive aircraft greatly outweigh the risks. Therefore, protecting these personnel and assets must remain a top priority. What follows is a discussion of the TTPs and current best practices that have been adopted to protect air bases.

Emplacing physical security measures is the first logical step towards building a robust perimeter defense. During Vietnam, layered defenses composed of “fences, barriers, concertina wire, security lighting, and mine fields” undermined the effectiveness of base penetration attacks [3]. This defense concept is nothing new and has been widely adopted to protect infrastructures with a great deal of success. Furthermore, “the major components of air base defense first identified in World War I (active defense; camouflage, concealment, and deception (CCD); hardening; dispersal on and off base; and post-attack recovery) reflect enduring military principles and a sound framework for air base defense

planning today" [1]. Despite the plethora of physical security measures in place today to protect bases, it is evident from Operation Enduring Freedom and Iraqi Freedom that adversaries continue to discover weaknesses in these force protection measures and aggressively exploit them.

A robust layered perimeter defense is only the first step towards successful physical security, but the lack of personnel to guard across every sector of the perimeter makes perfect security impossible. It is even harder to protect against intruders who briefly enter the vicinity of a target, launch an attack using stand-off weapons such as mortars and rockets, and quickly extract themselves before friendly forces can respond. In order to counteract the standoff threat, Lieutenant Colonel Herbert T. Brown, in his analysis of current air base ground defense doctrine, argues that "active defense, patrols, counterintelligence are some of the key tactics" that help defenders maintain situational awareness and rapidly respond to threats [5]. As a proponent of active defense, Lieutenant Colonel Brown emphasizes the need to leave the wire and proactively establish the security environment around the base. Attackers often have the advantage because they not only control the time and place of their actions, but also operate from a position of stealth. As a result, it becomes particularly important for force protection forces to expand the defensive perimeter beyond just the local physical measures.

Furthermore, "information superiority… not firepower, may become the defender's critical capability…[and] as adversaries continue to be both innovative and adaptive, time may become the critical capability influencing Security Force engagement strategies" [3]. In other words, early warning systems that provide defenders actionable intelligence are just as essential as physical defense and fire superiority. By being able to detect threats before they are capable of causing harm, defenders can seize the initiative from the enemy and thwart enemy action.

In summary, expanding the local perimeter through early warning systems and active patrols feed the intelligence and situation awareness needed to augment a layered physical defense. Figure 1 illustrates this concept. Together, a robust defensive perimeter can be established.

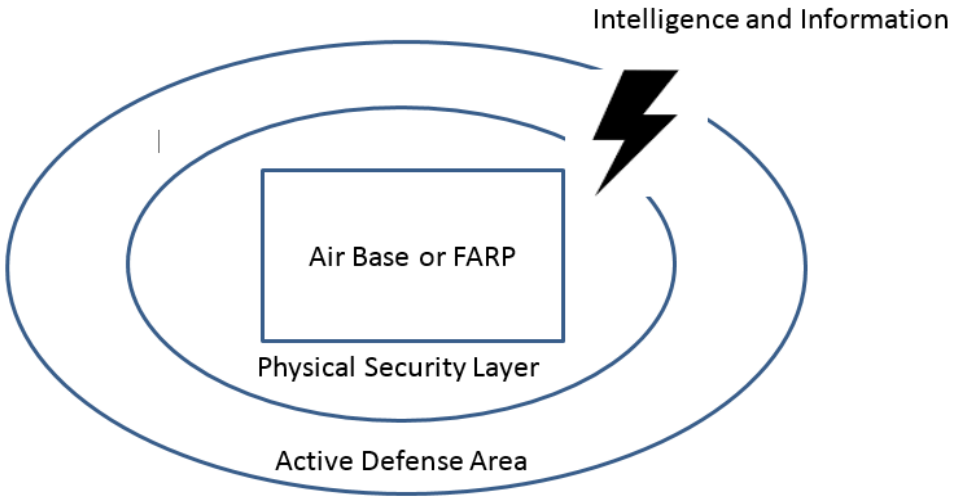

Figure 1. Proposed FARP Defense Model.

3. Future Threats to Air Bases and FARPs

As distributed operations continue to play a central role in how the U.S. military fights, remote air bases such as FARPs and other remote operating bases are critical centers of gravity which adversaries will seek to disrupt or destroy in order to jeopardize friendly commanders' scheme of maneuver and operations. With the increased ability of adversaries to attack such operating locations from increasing distances using more advanced technology, it becomes more difficult for perimeter defense assets to maintain situational awareness and to identify and respond to threats.

The tactics of infiltrating air bases surreptitiously or launching mortar attacks against air bases have demonstrated success in impairing air operations and damaging high valued assets. In his analysis of future ground threats to air bases, Vick identifies the following as high probability tactics: "(1) unguided mortar attacks executed by well-trained mortar crews (e.g., major-nation special operations forces [SOF]; (2) precision standoff attacks executed by adversary SOF, terrorists, or insurgents; and (3) penetrating attacks by well-trained commandos" [1].

The VietCong attack on Bien Hoa highlights the extensive damage that standoff attacks with mortars and rockets fired from outside the perimeter can cause. By stealthily entering advantageous terrain surrounding a FARP or other air base, enemy SOF or

insurgents can rapidly fire and exit before any base defense or rapid response teams can react. A small scale attack with a mere handful of mortars can launch downrange 75 rounds in just one minute [1]. As the precision of indirect fire and shoulder-launched surface-to-air missiles continue to spread, this threat is only exacerbated [4]. The enemy does not need to launch costly ground attacks against air bases or even penetrate perimeter defenses in order to have the desired effect of impairing sortie rates. They need merely get close enough without detection to launch mortar attacks or shoulder fired missiles at aircraft as they land or take off. In recent conflicts, night vision devices have granted U.S. forces a tremendous advantage in conducting operations at night. The availability of such technology to the enemy will only make our mission of defending against such attacks even more difficult.

Infiltration and sabotage attacks, as shown by the Camp Bastion case study, remain highly relevant despite the sometimes higher costs involved. Bases will continue to have to respond to such threats. Special operations forces are highly suited to carry out this type of operation against FARPs that are more lightly defended. Such tactics are effective and will continue to be exploited in order to overcome asymmetrical advantages. According to a separate RAND report by Roger Cliff and his coauthors, “Chinese sources indicate that covert operatives, such as SOF or saboteurs, would also play an important role in attacks on air bases […including] carrying out strikes on critical base facilities, destroying aircraft, and assassinating key personnel” [1]. Furthermore, militaries continue to explore incorporating unmanned or remotely piloted platforms for a versatile range of military applications, include infiltration and sabotage. Remotely piloted vehicles (RPVs) are an emerging threat to air bases, capable of not only conducting reconnaissance for targeting, but also carrying weapons and explosives [4]. In fact, these remote and unmanned technologies have already been exploited by groups within the last decade to deliver devastating effects. For example, the terrorist group Hezbollah utilized “explosive-laden RPVs and missile technology, even managing to cripple an Israeli warship” and launched “a remotely piloted surveillance plane, the Mirsad 1, that flew over Israeli towns and returned to Lebanon unharmed” [4]. The rapid increase in the usage of unmanned systems will continue to increase our vulnerability to enemy exploitation of such emerging technologies.

Standoff attacks using unguided or guided weaponry, penetration and sabotage, and remotely piloted vehicles are three proven methods adversaries will use against U.S. air bases, forward operating bases, and FARPs in a future conflict. It is imperative that our TTPs continue to adapt to meet these rising challenges.

B. WIRELESS SENSOR NETWORKS—A POWERFUL TOOL TO AUGMENT AIR BASE GROUND DEFENSE

As shown in the previous sections, both conventional and unconventional adversaries have aggressively exploited vulnerabilities in perimeter defense of air bases and are likely to continue to do so in future conflicts. In a distributed operational environment, FARPs and other small forward air bases are particularly vulnerable to infiltration and standoff attacks by enemy SOF and insurgents. First, because friendly forces are distributed over a wide geographic area to perform a myriad of different mission types, a shortage of trained forces to execute the force protection mission in the defense will often be the rule, rather than the exception. Second, because maneuvering at a tempo faster than the enemy is a central tenet of maneuver warfare, time is not always available to establish complex layered defenses to protect small but critical sustainment areas like FARPs. Therefore, if there is a dearth of personnel to adequately protect forward areas, alternate solutions such as technological advantages in surveillance and early detection systems should be considered.

The potential advantages of leveraging smart unmanned sensor networks to augment air base ground defense are many. First, the use of sensor networks to provide indication of perimeter breach reduces the number of personnel that need to be allocated towards force protection. In a remote FARP where only minimal personnel can be assigned for protection, an ad hoc network of sensors can cover gaps in personnel. Secondly, sensor networks have the capability to process raw data received, apply filters based on parameters determined by human operators, and automatically deliver timely and useful intelligence. Lastly, sensor networks placed around an air base or FARP can extend the detection range of threats, allowing defenders to gain precious time to analyze information from sensor networks and to devise the appropriate response.

Currently, sensor networks are employed in the operating forces. For the Marine Corps, the most recently fielded system is the Tactical Remote Sensor System (TRSS), a sensor suite capable of detecting human and vehicle movement in real time [2]. In their thesis on ground sensor networks, Palm and Richter [2] provide an overview of the TRSS and its associated issues. According to their research, the system costs $1,020,847.30 as recorded in Marine Corps Global Combat Support System (GCSS) [2]. Furthermore, the sensor monitoring system is HMMWV mounted, which increases the footprint and transport requirements of deploying such a system. In addition to being bulky and expensive, operators need approximately thirty-five days of training. The TRSS is considered a Marine Expeditionary Force (MEF) asset and only six are distributed for each MEF [2]. A system like TRSS that is currently employed by the Marine Corps is unwieldy and not available for distributed use at lower levels. Therefore, solutions that are less costly, more operator friendly, and require a smaller deployment footprint must be explored for the purpose of augmenting the perimeter defense of small air bases like FARPs.

A wireless sensor network composed of low-cost nodes can satisfy this requirement. Nodes equipped with sensors fit for a specific application can be deployed throughout an environment in order to capture relevant data. These nodes can then interconnect wirelessly, using various communication protocols and standards such as the IEEE 802.X standards, either to each other or to a gateway, which ultimately relays the data to the end user. Figure 2 depicts how a wireless sensor network can support communication in a disaster response scenario. As one can see from this example, the basic requirements of a wireless sensor network are not necessarily complex. Sensors need to detect events of interest, trigger a certain response, and ultimately communicate relevant data to the end user.

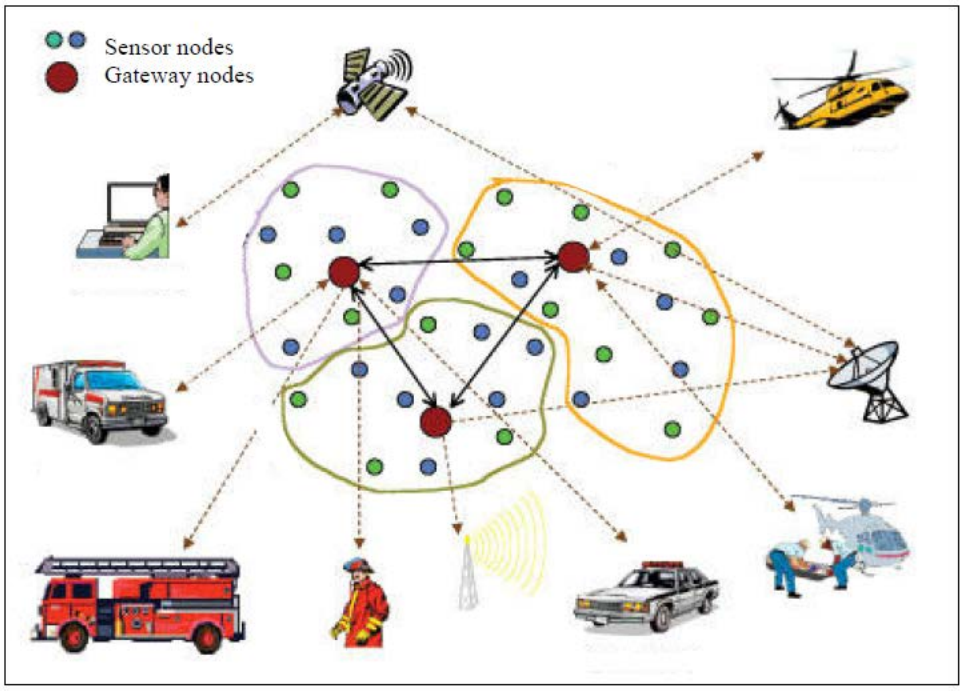

Figure 2. Wireless Sensor Network Example. Source: [6].

Applications of wireless sensor networks abound in numerous fields, but the basic architecture remains consistent: a set of dispersed sensors, a deployable communications network, and a command and control (C2) or coordination and control point. One can modify the network topology as desired to best fit the purpose of the sensor network. Our proposed architecture of a wireless sensor network for air base ground defense application also does not deviate from this basic structure. With an understanding of the basic structure of wireless sensor networks, we proceed to discuss the processor and sensors used for our experimental architecture.

C. RASPBERRY PI AS A GENERAL-PURPOSE PROCESSOR FOR SENSOR NODE

As discussed in the previous section, the end points of a WSN are the sensor nodes. This thesis seeks to build a WSN concept demonstrator composed of Raspberry Pi sensor nodes based on an architecture designed specifically for augmenting air base ground defense. Commercial-off-the-shelf (COTS) platforms that can be used to possibly satisfy this purpose range from microcontrollers, like the Arduino, to more powerful general

processors, like the Raspberry Pi running a full Linux operating system. As such low cost commercial processors and controllers continue to populate the market and rapid improvements in their capabilities are made, we believe that the military can benefit greatly by exploring how to leverage such devices for various military applications, such as air base ground defense.

Unlike a system such as TRSS, a sensor network composed of Raspberry Pi nodes can offer the same capabilities at a significant reduction in cost and with a much smaller footprint. A Raspberry Pi 3 model and associated suite of sensors can be purchased commercially for less than $100. Smaller than some smart phones, the Raspberry Pi adds almost no weight or space, allowing it to be easily transported. Employing a sensor network of these nodes can become a tremendous asset to force protection of small air bases like FARPs. The remainder of this section discusses the advantages of using the Raspberry Pi to build a WSN for perimeter defense application.

A WSN that can be both widely and effectively employed for perimeter defense applications should have at least the following characteristics:

1. Sensor nodes must be cost effective to allow for deployment at the lowest tactical level;
2. The WSN footprint needs to be relatively small in order to facilitate logistical and transportation requirements, and to avoid easy detection or targeting by an attacker;
3. The nodes must efficiently manage power consumption to ensure the usability of the WSN for the longest period possible without recharging;
4. The deployed sensors must also be durable and capable of being ruggedized to increase survivability in the field; and
5. While meeting the above requirements, the WSN must ultimately satisfy the mission requirement of communicating to defenders accurate and relevant information, as well as acting as an early warning system.

More specifically, the sensor nodes that comprise this network need to be low- cost, portable, yet still contain sufficient processing power and memory to process, store, and communicate useful data to the end user.

Given this set of specifications for an effective WSN in a tactical setting, the Raspberry Pi is a powerful and flexible COTS platform that can be utilized to satisfy these requirements. Extremely lightweight and low cost, sensor nodes built from the Raspberry Pi can also process, store, and communicate useful data to other nodes within the network and ultimately to the end user. Both physical size and cost are especially pertinent characteristics of a WSN deployed for perimeter defense applications. A sensor node that is inexpensive and small enables easy deployment and management of these nodes within a network. Other inexpensive microcontrollers, such as the Arduino, are available and can be explored as an alternative for base defense applications in future research. However, the Raspberry Pi is an overall affordable yet powerful processor with the memory and processing power required to satisfy our sensor network's purpose.

In order for a sensor node to be useful for the ABGD setting, it needs to be able to remain in the field without excessive external power requirements. The Raspberry Pi platform has the flexibility built-in to satisfy this lower power requirement. According to Vujovic and Maksimovic, "the processor of Raspberry Pi is a 32 bit, 700MHz System of a Chip (SoC), which is built on the ARM11 architecture" [7]. It can "operate on just the 5V 1A power supply provided by the onboard micro USB port" [7]. In other words, the "majority of the system components-its central and graphic processing units, audio and communications hardware, along with the 256–512 MB memory chip, are built onto a single component", with the Raspberry Pi only requiring up to 700 mA to operate [7]. Additionally, the Raspberry Pi is capable of being powered through a variety of sources, such as computer USB ports, alkaline battery, mobile phone backup battery, and solar cell system [7]. A number of different power modes are also available on the Raspberry Pi, from the fully operating mode to dormant and standby modes so that power can be conserved depending on field requirements [7]. Although this thesis does not focus on the issue of power in the establishment of the experimental WSN, power is a crucial issue when it comes to deployment of sensor nodes and should be thoroughly investigated. Nonetheless, as noted, the Raspberry Pi has several different power modes for operation and a versatile set of power sources, giving it great potential to be a highly flexible and viable platform to be used for our WSN setup. Given that the Raspberry Pi satisfies this

criteria of cost, power, footprint, and processing capability, we choose to use this processor for our sensor nodes.

D. WSN ARCHITECTURE OF PREVIOUS FIELD EXPERIMENT CONDUCTED USING RASPBERRY PI SENSOR NODES TO AUGMENT AIR BASE GROUND DEFENSE

In this section, we discuss the field experiment that our colleagues Kenneth Foo and Dingyao Hoon at the Naval Postgraduate School recently conducted using Raspberry Pi sensor nodes to augment perimeter defense, and the lessons learned from their study. We seek to improve upon their initial design from a networking perspective and introduce the usage of short-range radar sensors in our WSN design for this thesis. By doing so, we aim to make our ABGD-WSN more robust and capable.

Foo and Hoon's experimental WSN was designed to address the same problem as this thesis. Figure 3 shows the operating concept of their WSN. In their setup, sensor nodes are deployed in multiple layers around the FARP. The nodes communicate directly with the C2 application server located within the FARP. If an intrusion detection occurs, information on the intruder, including image analysis, is sent to the C2 server for processing [8].

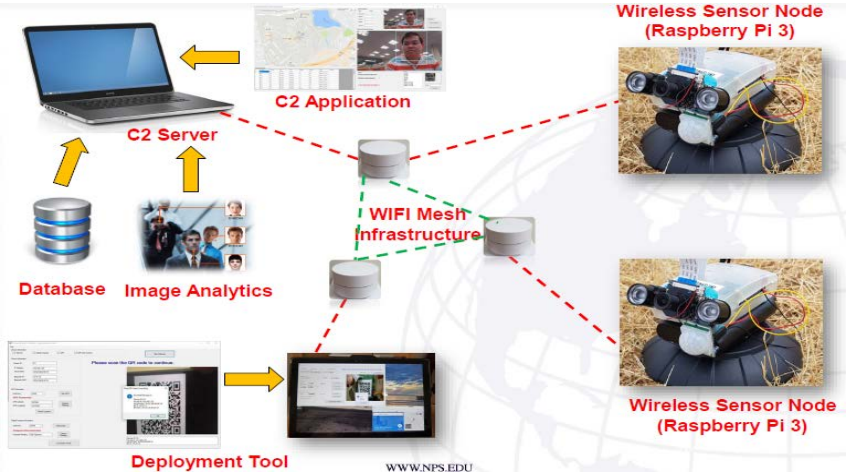

Figure 3. WSN Architecture Built by Foo and Hoon. Source: [8].

In their WSN setup, as depicted in Figure 3, the key technology used at the nodes is the Open Source Computer Vision Library (OpenCV), which contains open source libraries that offer a plethora of machine learning capabilities, including facial recognition. Once the WSN is established, sensors detect motion and turn on the cameras on the sensor nodes to capture pictures of the possible intruder, which are then processed by OpenCV facial recognition. The processed image is then sent to the C2 application server via 802.11b Wi-Fi onboard the Raspberry Pi. A Wi-Fi router enables the nodes to communicate in the mesh network. Once the processed image arrives at the C2 server, the user can use the designed GUI to perform management, monitoring, and analysis of possible threats [8].

While facial recognition nodes can be highly useful in an ABGD setting, an entire WSN of only these nodes is not adequate to provide the layered protection that is necessary. Relatively short detection range of cameras, false-positive rates of facial recognition, and dependence on optimal lighting environments were discovered to be issues during field experiments [8]. Additionally, the WSN architecture they built depended upon reliable network connections through a mesh router that routed data from nodes to the C2 server. In a deployed environment, fragile connections and low bandwidth can hinder the effectiveness of a WSN that depends on reliable network infrastructure. We aim to further their work by increasing the detection range of the WSN and using sensors not as easily affected by visibility conditions. Furthermore, we seek to implement our WSN in an ad hoc fashion so that nodes can still pass critical data in a network denied environment.

E. OPS-241A SHORT-RANGE RADAR SPECIFICATIONS

In order to add additional functionalities beyond the facial recognition nodes built by Foo and Hoon, this thesis experiments with the OPS-241A short-range radar (SRR) developed by Silicon Valley startup OmniPreSense. The OPS-241A was developed in 2017 for the hobbyist community that is capable of providing motion detection, speed, and direction reporting [9]. It is a powerful device of remarkably small footprint that can be connected to smart USB-hosts like the Raspberry Pi, Android devices, PC or Mac, and transformed into an Internet of Things (IOT) sensor [9]. Figure 4 is a picture of the OPS-241A and its antenna pattern.

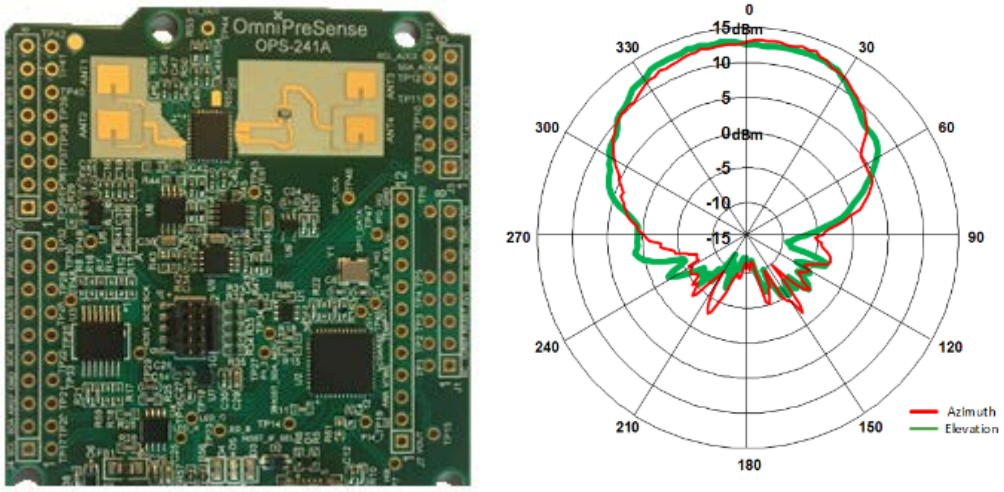

Figure 4. Picture of OPS-241A Short-Range Radar and its Antenna Pattern. Source: [9].

The following is the advertised capabilities and features of the OPS-241A [9]:

1. Detection up to 40 feet
2. Speed reporting up to 138mph with accuracy to within 0.5%
3. Reporting of direction (inbound or outbound)
4. 78^{o} beam width
5. USB interface with simple API control
6. 1.4W Active power, 0.6W idle power
7. Small form factor 53 x 59 x 12mm, 11 g

While the OPS-241A is a recently developed product, short-range radars have been utilized for various applications in the last decades. The automobile industry in particular has seen wide uses of such sensors in vehicles to provide functionalities such as collision avoidance, parking aid, and blind spot detection. In the same way, we believe that embedding sensor nodes armed with short-range radar technology into a WSN for perimeter defense can be highly effective.

F. MESSAGING AND NETWORK PROTOCOLS USED

This section provides an overview of the Better Approach to Mobile Ad hoc Networking (B.A.T.M.A.N) protocol and the Message Queue Telemetry Transport protocol (MQTT) used for our experimental WSN. Together, these two messaging and networking protocols enable a flexible WSN that can be deployed in an ad hoc environment where high bandwidth and reliable connectivity are not available.

1. MQTT Lightweight Messaging Protocol

MQTT is an open source machine-to-machine messaging protocol that rides over the TCP/IP protocol [10]. MQTT operates using a publish/subscribe mechanism in which a broker passes messages from publishers to clients that have subscribed to a specific or multiple topics [10]. Figure 5 presents a basic overview of how messages are passed using MQTT's publish/subscribe model. Based on the design principles of "minimizing network bandwidth and device resource requirements while also attempting to ensure reliability and some degree of assurance of delivery," the protocol was "designed for constrained devices and low-bandwidth, high-latency or unreliable networks" [10].

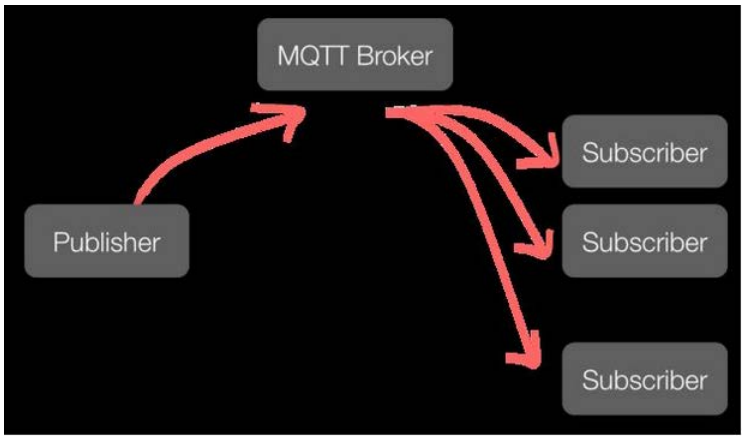

Figure 5. Depiction of MQTT's Publisher Subscriber Model. Source: [11].

MQTT has several highlights that make it an ideal messaging protocol for our WSN within an ABGD setting. First, it contains a "last will and testament" feature such that if a publisher node loses contact with the subscriber(s) for reasons such as battery depletion

and node destruction, a user specified message would be sent to inform the subscriber(s) [12]. Second, MQTT supports more than a one-to-one publish/subscribe connection, allowing publishers to send messages to multiple subscribers. Third, this messaging protocol carries "minimal headers, a small client footprint, and limited reliance on libraries" that make it useful in communication constrained environments [12]. Lastly, its use of a "push style message distribution keeps network use low" [12]. Together, these characteristics of MQTT provide a messaging mechanism that sensor nodes within our WSN can reliably use to deliver notifications and images back to the server with minimal overhead.

2. B.A.T.M.A.N. Advanced—Better Approach to Mobile Ad Hoc Networking Protocol Advanced

Developed by Open-Mesh, B.A.T.M.A.N. Advanced (batman-adv) is "an implementation of the B.A.T.M.A.N. routing protocol in [the] form of a Linux kernel module operating on layer 2" [13]. Most routing protocols, including those in conventional networks such as OSFP and RIP, work at Layer 3 (Internetwork) of the TCP/IP Internet model. In contrast, batman-adv works across layer 2, and transports both data traffic and routing information using Ethernet frames [13]. This implementation "encapsulates and forwards all traffic until it reaches the destination, hence emulating a virtual network switch of all nodes participating. Therefore, all nodes appear to be link local and are unaware of the network's topology as well as unaffected by any network changes" [13].

Operating over layer 2 enables batman-adv to be network agnostic, which means that IPv4, IPv6, or other internetwork layer protocol work on top of batman-adv [13]. Nodes connected in the mesh through batman-adv also do not need to be assigned IP addresses [13]. As for routing, each node "maintains a list of all single hop neighbors it detects [and] a list of all other nodes in the network and remembers in which direction to send the packet if data should be transmitted" [13]. batman-adv contains many other intricacies in its network formation and maintenance; Open-Mesh's website includes full documentation regarding the batman-adv networking protocol.

batman-adv provides our WSN the ability to automatically discover neighbors within range and determine routes to distant nodes. By using batman-adv, data passes from publisher of messages to subscribers without the need of fixed communication infrastructures. Because Raspberry Pi Model 3 supports WiFi, a Layer 2 protocol, Pi nodes can install batman-adv, join to a user designated ad hoc network, and communicate among themselves using this ad hoc routing protocol.

G. SUMMARY

This chapter provided an overview of the history of ABGD, the tactics and techniques currently employed to defend air bases, and the future threats that air bases and FARPs will face. From this analysis, it is clear that adversaries will continue to attempt to overcome the asymmetry in air capabilities by exploiting vulnerabilities in our air base defenses. From our research, we determined that it is feasible to build a cost effective WSN from commercial products such as the Raspberry Pi in order to augment the defense of FARPs. By equipping the Pi with various sensors and networking the nodes together in an ad hoc fashion through MQTT and batman-adv, we aim to build a low-cost yet robust WSN that can extend the early warning capabilities of air bases. Chapter III details the system architecture of this WSN and discuss the experimental design used in the field experiment.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SYSTEM ARCHITECTURE AND IMPLEMENTATION

This chapter presents the overall system design of the WSN we built in order to augment ABGD. Furthermore, it details the individual components that comprise the WSN and discusses how early warning information is communicated by the WSN nodes to the C2 application through the network.

A. SYSTEM ARCHITECTURE

The ultimate objective of our prototype WSN is to provide early warning so that FARP defense personnel have sufficient time to interdict the threat. Our system architecture applies the concept of layered defense in order to achieve this goal. By employing sensor nodes with different sensing and detection capabilities in multiple layers around the FARP, the WSN extends the distance at which a threat can be detected, identified, and interdicted. Figure 6 illustrates the proposed employment concept of our WSN.

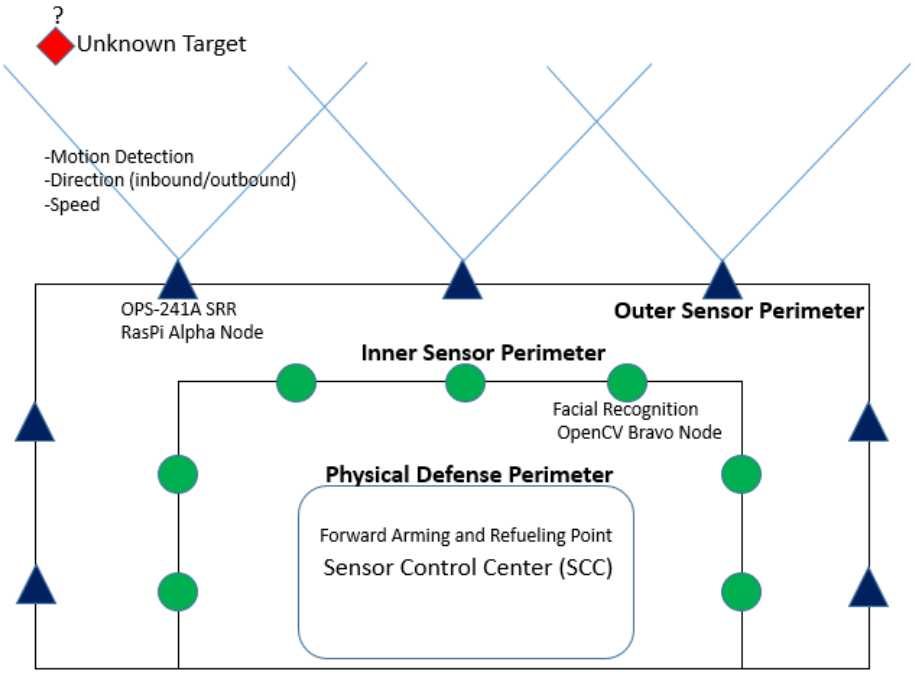

Figure 6. Sensor Network Deployed in a Layered Defense.

As Figure 6 shows, three layers separate the FARP from any potential threat. The outer sensor perimeter consists of nodes equipped with short-range radar (SRR) that provides the first layer of detection. The inner sensor perimeter consists of nodes with facial recognition capability that acts as the second layer of intelligence for the FARP. Lastly, the physical defense perimeter is made up of the combination of barriers and personnel that are ultimately required to respond to threats. Together, these layers provide the intelligence, early warning, and physical defense necessary for timely response to threats. The remainder of this section discusses in detail the nodes that comprise the outer and inner sensor perimeters, and their responses to different threat scenarios.

1. Alpha Node—OPS-241A Short-Range Radar Node

The outer sensor perimeter consists of the Alpha nodes, built on the Raspberry Pi 3 Model B platform connected to an OPS-241A SRR module via USB, and powered by an Anker PowerCore 10,000mAH single USB port battery pack. Figure 7 is a picture of the Alpha node.

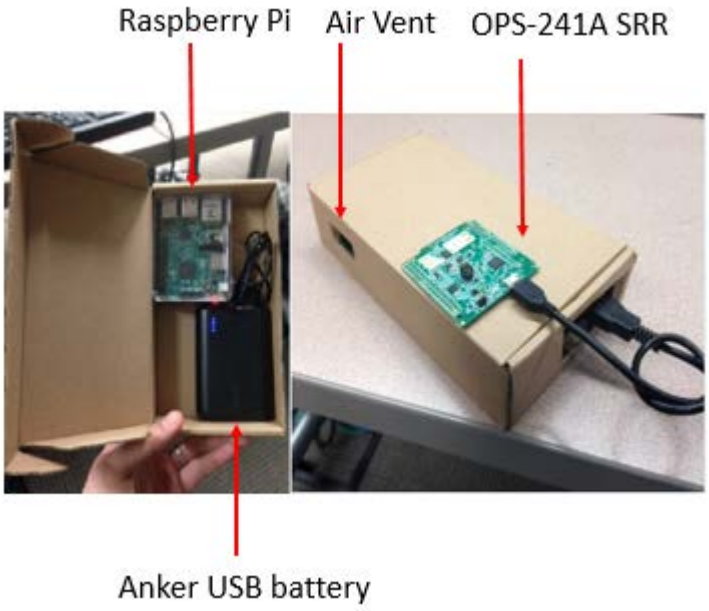

Figure 7. Short-Range Radar Node.

The Alpha node provides three essential capabilities: motion detection, speed classification, and direction reporting. The SRR sensor itself is programmed in Python. Commands, including the sampling frequency, transmit power, speed output units, and sensitivity settings, can be directly sent through the application programming interface (API) to control the OPS-241A module [14]. The SRR sensor, upon triggering, is programmed to detect motion, capture speed and direction (inbound or outbound) of the approaching object, and classify the inbound object as a high, medium, or low threat based on its speed. Outbound objects are ignored because they are most likely coming from within the perimeter. Additionally, the boundary for threat classification can be shifted based on the operating environment. For our experiment purposes, any object with speed below 0.5m/s is classified as low threat; 0.5m/s to 1.5m/s, the average speed of a human walking, classified as medium threat; and 1.5m/s or faster as high threat. A potential shortcoming of the Alpha node is that while it can effectively determine whether a target has entered the outer sensor perimeter, it cannot distinguish targets that enter the sensor field and then change direction in an attempt to feign from separate targets that enter the sensor field at different locations within a short time period. In other words, if a target first triggers an Alpha node, changes direction to another sector of the perimeter, and then triggers a different Alpha node, the second triggered node will treat the target as a separate threat.

Once the Alpha node has captured and processed the speed data, it has a variety of actions that it can take depending on the initial threat assessment. Figure 8 elucidates the actions taken at the Alpha node upon detection of the incoming object. This response model was developed with the goal of lowering the number of false positives while still giving responders enough early warning to process the intelligence and intercept the threat.

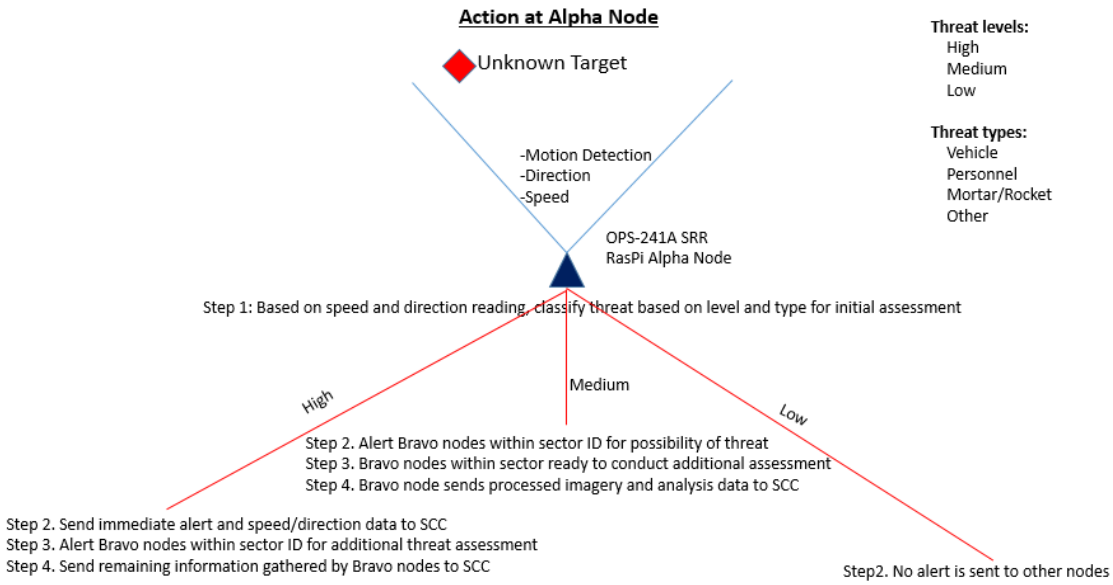

Figure 8. OPS-241 Alpha Node Decision Tree.

An object that approaches at a higher speed is likely to be a greater threat, thereby requiring the responders to be alerted immediately. After sending a high threat alert, the Alpha nodes also alert the nodes on the inner sensor perimeter within the designated sector such that, if the threat continues towards the FARP, the Bravo nodes can then capture imagery data and attempt to perform facial recognition on the intruder. If the intruder then encounters the Bravo nodes, the imagery analysis performed by Bravo nodes is sent to the C2 application so that responders can draw a more definitive conclusion regarding the intruder. In contrast, a medium threat classification doesn't immediately alert the SCC, but rather triggers the Bravo nodes to perform additional assessment before any information on the intruder is sent to the SCC. Lastly, a low threat is regarded as a false positive and no further action is taken. However, depending on the threat environment, the speed threshold to qualify as a higher threat can be adjusted so that even objects with very low speed trigger an alert.

2. Bravo Node—OpenCV Facial Recognition Node

The inner sensor perimeter consists of the Bravo nodes, which are constructed on the Raspberry Pi 3 Model B and uses OpenCV libraries for facial recognition. Additionally, Bravo nodes feature a USB webcam that supports facial recognition and a passive infrared sensor for short-range motion detection. Like the Alpha nodes, each is powered by an Anker battery. The Bravo nodes were built by Hoon and Foo as a part of their thesis and are adapted for our experiment. Figure 9 is a picture of the Bravo node as built by Hoon and Foo. For full details on these facial recognition nodes, refer to Hoon and Foo's thesis.

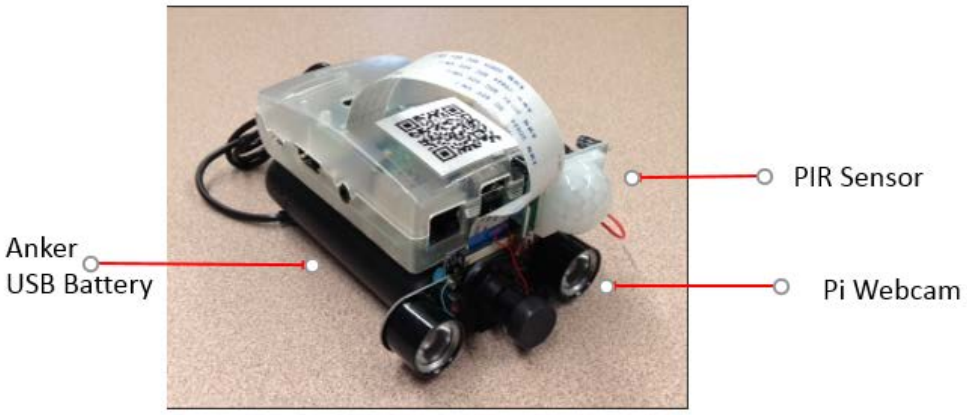

Figure 9. Bravo Node Prototype.

The facial recognition capability provided by the Bravo nodes remains unmodified, but the communication mechanism and protocol of these nodes is changed to allow for ad hoc wireless network formation with the other nodes while still being able to communicate with the C2 application over the 802.11b wireless protocol. Figure 10 depicts the actions that Bravo nodes take upon being alerted of possible intrusion by the outer sensor perimeter. Once Bravo nodes have been alerted of a potential breach, their passive infrared (PIR) sensors are activated to detect motion within their proximity. If motion is detected, the USB webcam turns on and "leverages the OpenCV computer vision algorithm to determine if the intruder within the camera field of view is a human, an animal or another object by means of frontal facial recognition" [8]. Using the OpenCV algorithm, the Bravo

node performs facial recognition and sends the imagery data to the C2 application. If no human faces are detected after the timeout counter expires, the node returns to idle mode.

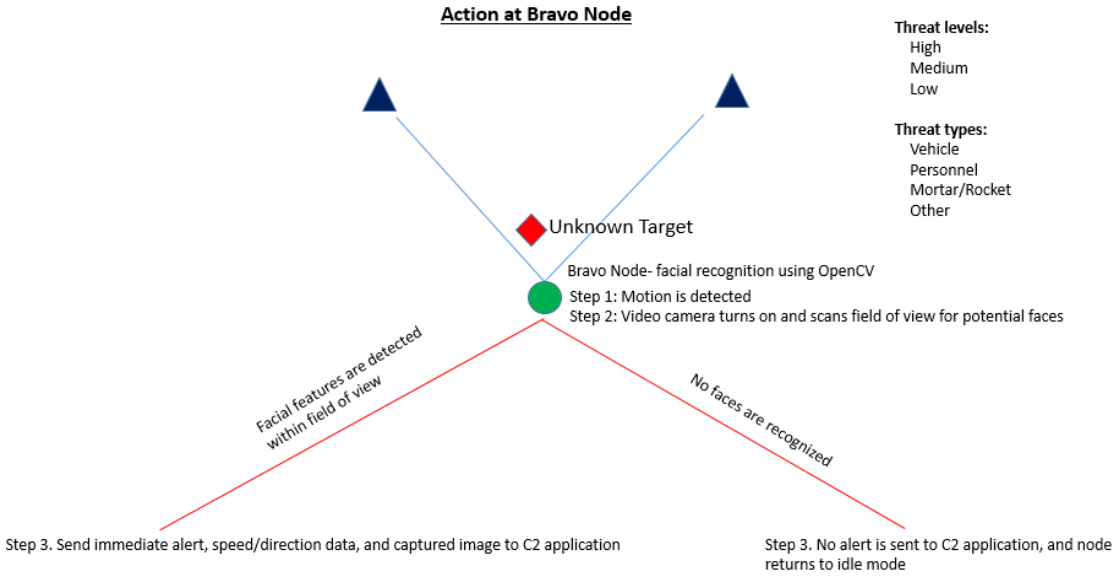

Figure 10. Facial Recognition Bravo Node Decision Tree.

3. C2 Application and Database

The C2 application built by Hoon and Foo is also utilized for our experimental WSN. Following instructions from their thesis, we rebuilt the SQL database using Microsoft SQL Server Management Studio 17 on a Dell laptop running Windows 8. The database table structures remain unchanged, except for the addition of a table to store the speed information captured by Alpha nodes. The C2 application is the user interface by which the user accesses all the imagery and speed data. Once Bravo nodes have transmitted intruder image and information to the C2 application, the C2 application can perform more in-depth facial analysis and attempt to match the captured image to learned facial images of known individuals already stored within the database [8]. Figure 11 is a screenshot of the C2 application's dashboard based on Hoon and Foo's original application. See Hoon and Foo's thesis for details and schematics of the C2 application.

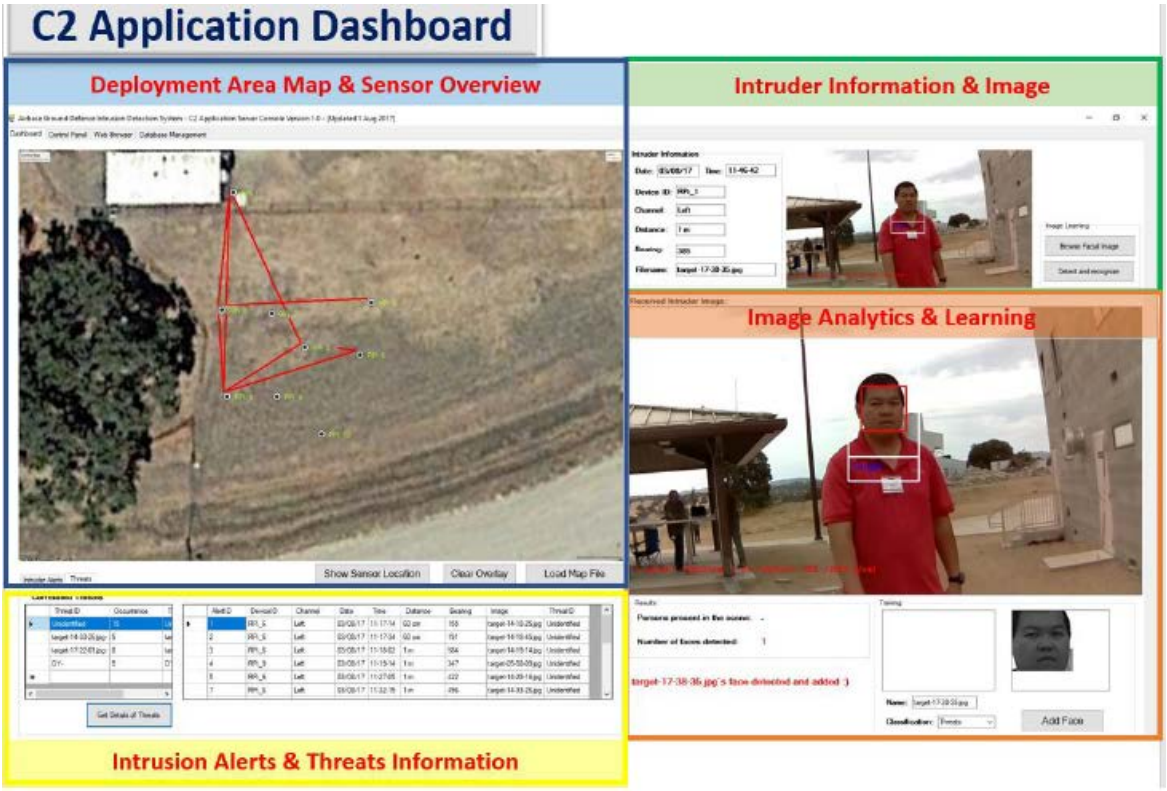

Figure 11. Screenshot of C2 Application Dashboard. Source: [8].

B. WIRELESS SENSOR NETWORK ARCHITECTURE

One of the main network goals of our WSN is to enable the nodes to communicate in an ad hoc manner and decrease the overall reliance on wireless or fixed communication infrastructure. By making at least a portion of our WSN ad hoc, the overall network is made more robust as it will now be more resilient to node failure. Since each node can communicate with every other node within range without depending on a single gateway or router, the overall network is easier to establish and is more resilient. The remainder of this section discusses in detail the network topology of our WSN, comprising eight nodes communicating with each other and transmitting information to the C2 server. Figure 12 presents the network topology of our experimental WSN.

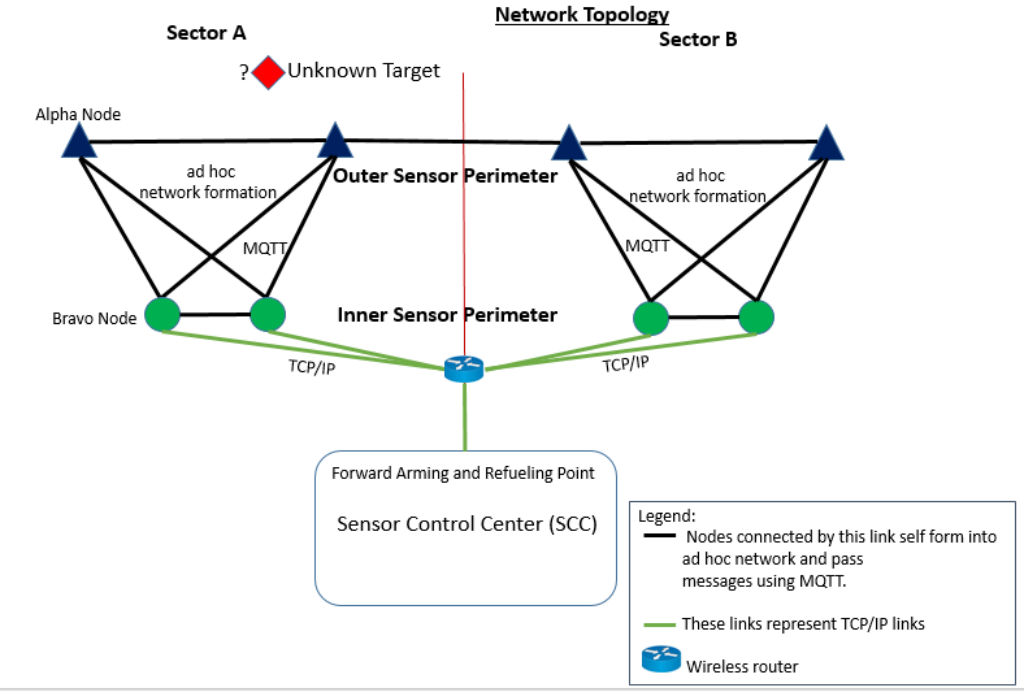

Figure 12. WSN Network Topology.

1. Communication between Outer Sensor Perimeter and Inner Sensor Perimeter

As shown in Figure 12, the Alpha and Bravo nodes self-organize into an ad hoc network and communicate using MQTT, a “publish-and-subscribe” communications methodology. The Raspberry Pi can be changed into wireless ad hoc mode by altering its network interfaces file, thereby enabling each node to automatically detect other nodes that are also in ad hoc mode. Figure 13 displays the Raspberry Pi’s interface configuration settings and shows that the Pi has been placed into wireless ad hoc mode.

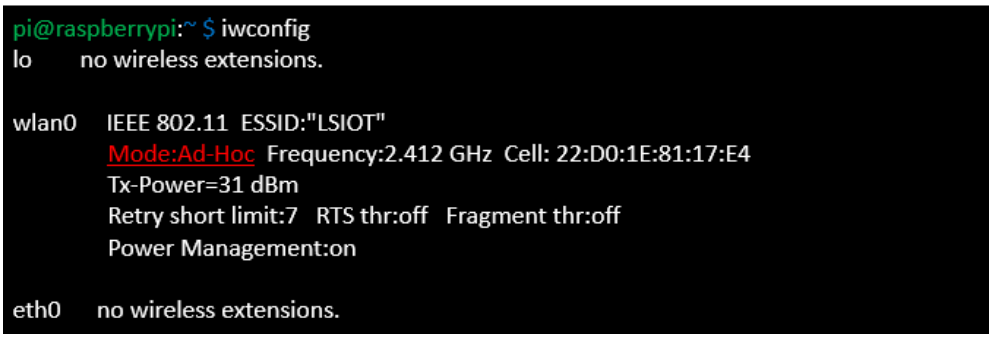

Figure 13. Raspberry Pi Wireless Interface in Ad Hoc Mode.

The Alpha nodes are each programmed to publish captured speed and direction data to the Bravo nodes. The Bravo nodes are programmed to subscribe to the same topic that the Alpha nodes publish. Additionally, the Bravo nodes act as the broker within the MQTT communication mechanism. Since the Alpha and Bravo nodes self-organize, they do not rely on external communication equipment or network connectivity. Consequently, the sensor nodes can be deployed rapidly and establish connectivity almost immediately.

2. Communication between the Inner Sensor Perimeter and C2 Application

The network communication between the Bravo nodes on the inner perimeter and the C2 application uses the same framework and software code that Hoon and Foo designed for their WSN. In that framework, the Bravo nodes establish TCP connections to the C2 application by using a random TCP port number, while the C2 application has several TCP listening threads on port 9001 so that it can simultaneously accept independent threads from various nodes [8]. The C2 application server also uses TCP/IP to send commands to the sensor nodes, which listen on port 9001 to incoming TCP traffic [8]. In essence, the Bravo nodes have been configured to act as both a MQTT subscriber as well as a TCP client. We configured the Bravo nodes in this manner in order to integrate Hoon and Foo's portion of the network with the outer sensor perimeter without eliminating the ad hoc network characteristic we wished to introduce for this thesis. Future work can be done to simplify the communication structure by using one protocol for the entire network. All TCP/IP traffic is transmitted via an intermediary wireless router between the Bravo nodes and the C2 application server. The use of this intermediary wireless router is a potential

single point of failure and can be mitigated if our entire WSN communicated in an ad hoc manner. We did not set up our network in an entirely ad hoc fashion for this thesis because we would have needed to make significant modifications to Hoon and Foo's software code in order to make the entire system ad hoc. However, it is important to note that a purely ad hoc WSN can greatly increase resiliency and robustness of the network, a worthy topic for future work. Figure 14 depicts the TCP communication occurring between the Bravo nodes and the C2 application server.

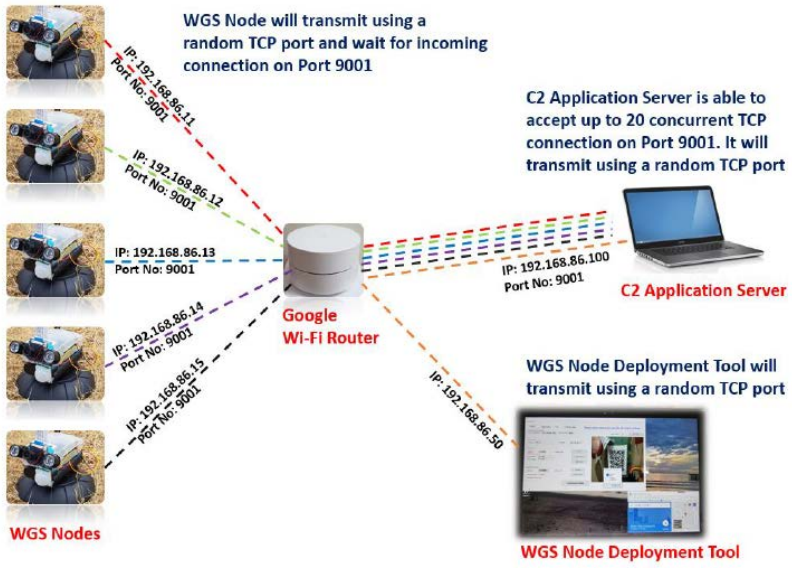

Figure 14. TCP Communication between Bravo Nodes and C2 Application Server. Source: [8].

The message formats and the control messages that the C2 application server sends and receives from the Bravo nodes are unchanged from Hoon and Foo's design. Detailed information on data format and types of control messages sent are presented in their thesis.

Since Bravo nodes communicate with the C2 application server through a wireless router using TCP/IP, but communicate with the Alpha nodes using MQTT in an ad hoc fashion, the use of an external USB wireless adapter on the Bravo nodes is necessary to make this dual communication work. This is because if a wireless adapter has been set to ad hoc mode, it cannot be used to establish a separate connection to the wireless router. Bravo nodes need to communicate with both the C2 application and the Alpha nodes,

therefore an additional USB wireless adapter is plugged into the Bravo nodes so that they can use one adapter to communicate in ad hoc mode to the Alpha nodes and the other adapter to communicate in traditional mode to the C2 application over a wireless router. In this thesis, we use the Dexter Industries 802.11N USB wireless adapter.

C. SUMMARY

This chapter presented the system architecture of our WSN and discussed the functions of each component within this network. Alpha nodes with short-range radar sensors form the outer perimeter layer, while the Bravo nodes with facial recognition capability form the inner perimeter. Together, the two layers complement each other in capabilities and form a defense in depth to provide early warning to defenders. This chapter also discussed the actions that each node takes depending on the nature of the threat. Higher threats demand a more immediate response and lower threats require further analysis to determine whether the threat is a true- or false-positive. Finally, this chapter detailed the communication mechanisms and protocols used by the nodes and C2 application server to exchange data. Chapter IV presents the results of our experiment and discusses the capabilities and limitations of our WSN observed during field experimentation.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TESTING AND IMPLEMENTATION

Based on the system architecture presented in Chapter III, this chapter presents the field experiments conducted to test the effectiveness of the proposed system design. We evaluate the effectiveness of individual components and the overall WSN to achieve the objective of providing early detection, and also identify their capabilities and limitations. Two separate experiments were conducted, one at the NPS campus and the other at Camp Robert's Combined Arms Collective Training Facility (CACTF). The experimental results are analyzed to determine the system's overall performance in providing early detection.

A. FIELD EXPERIMENT SETUP AND PROCEDURE

1. NPS Campus

We conducted our first field experiment at the NPS campus on February 9, 2018 at 0800 when pedestrian traffic in the experiment site was minimal. Weather conditions were sunny with clear skies, with a temperature of 55 degrees Fahrenheit. The humidity was measured at 54% with little to no wind at the experiment site. Figure 15 is a Google satellite image of the experiment site with the location of our nodes annotated. We selected the courtyard in front of Spanagel Hall as the deployment site for our WSN and chose the east corner of Bullard Hall to be the Sensor Control Center (SCC) where the C2 application server laptop was located. We deployed the Alpha nodes along the outer sensor perimeter at 6.75 meter intervals on the outdoor tables with their SRRs facing outward from the perimeter. Similarly, we deployed the Bravo nodes along the inner sensor perimeter at 6.40 meter intervals with cameras and motion sensors pointed towards the outer sensor perimeter.

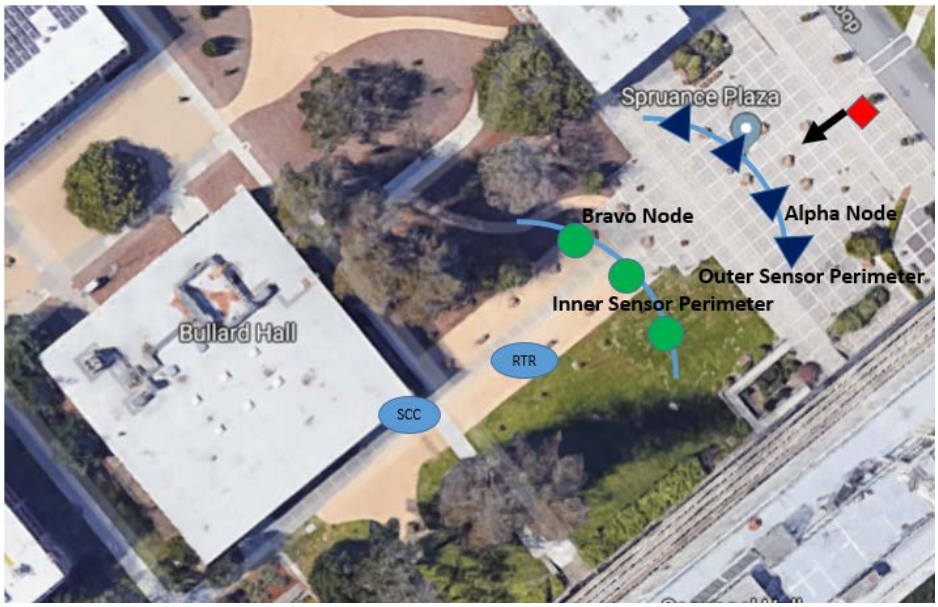

Figure 15. WSN Setup NPS Campus.

The distance between the outer and inner sensor perimeter was 35.05 meters, and the Zoom 3G Wireless-N Travel Router was placed 40.0 meters away from the SCC and 22.4 meters away from the inner sensor perimeter. These distances were established based on the tested effective WiFi range of each device. The method used to measure these distances is discussed later in this chapter. Once all nodes were turned on and placed in their respective locations, we pinged each node from the C2 application laptop via command line to verify connectivity. Using VNC Viewer, we sent commands to the Bravo nodes first to run their Python script and begin subscribing to incoming messages from Alpha nodes via MQTT. Once Bravo nodes were successfully subscribed to the predetermined topic, we sent commands to Alpha nodes via VNC Viewer to run their Python script and publish data in the event of intrusions. At this point, the WSN was deemed operational and ready to provide early detection and transmit intruder data. The time it took to set up the nodes, establish connectivity, and register them on the C2 application was approximately between 40 to 50 minutes. Most of this time was utilized to set up the physical equipment, place the nodes in their locations, and establish the SCC.

Once the WSN was deemed operational, we officially began the intrusion detection portion of the experiment. We instructed our experimental aide to walk towards the outer sensor perimeter at a casual walking pace from a starting position of about 10 meters away, as depicted in Figure 15. Without stopping, the experimental aide continued on a current straight-line trajectory towards the SCC at the same pace. After the walk portion of the experiment was conducted and the results recorded, we began the run portion and also conducted the runs. We instructed the experimental aide to run, without sprinting, into the outer sensor perimeter from a starting position of about 10 meters away. Again, the experimental aide continued on a straight-line trajectory towards the SCC at the running pace.

2. Camp Roberts CACTF

After initial field-testing was conducted at the NPS campus, we followed the same setup procedures and used the effective distances determined during the NPS field experiment to establish our WSN at the CACTF on February 27 at 0930. The CACTF is a mock build of a small village with several avenues of approach. Weather conditions were partly cloudy with an average temperature of 41 degrees Fahrenheit. The humidity was measured at 50%. Winds were approximately five miles per hour, which was significantly higher compared to the wind conditions during the NPS field experiment. Figure 16 shows the birds-eye view of our experiment setup of the outer and inner sensor perimeter along a key avenue of approach to the village. Figure 17 and 18 show the deployment of the outer and inner sensor perimeters, respectively.

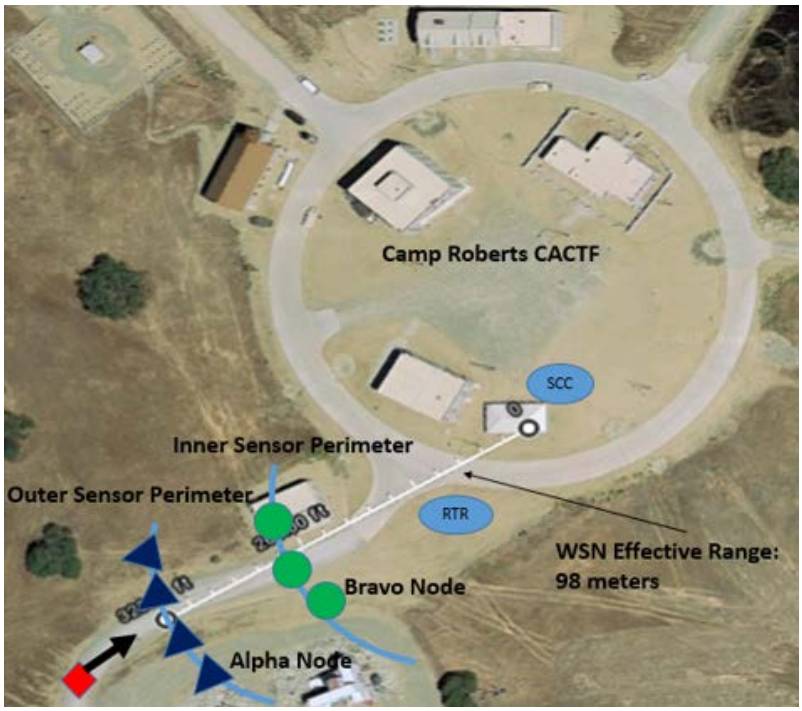

Figure 16. CACTF WSN Setup: Intrusion along Avenue of Approach.

Figure 17. Outer Sensor Perimeter Deployed at CACTF.

Figure 18. Inner Sensor Perimeter Deployed at CACTF.

B. SYSTEM PERFORMANCE

1. Intrusion Detection Performance of Alpha Nodes

After ensuring that the area was clear of any moving objects, we verbally instructed an aide to walk towards the SRR module from a distance of 5 meters. Meanwhile, we monitored the output from an Alpha node remotely using VNC Viewer. As soon as any speed output was detected from the node, the person was verbally instructed to stop. We repeated this process five times to determine the approximate effective distance of the SRR to be about a meter**.** Using the configuration settings shown in Table 2, the Alpha node picked up movement and recorded speed without fail during each of the five trials, but the SRR sensor did not register movement until the target was very close to it.

Table 2 shows the configuration settings applied to the OPS-241A through the API. We selected these settings based on OmniPreSense's guidelines to provide the most optimal performance at various power settings, sample frequency, and desired speed range. We set the transmit power to the highest setting at 9 dBm [14]. Additionally, we set the sampling frequency to 5,000 samples per second to keep the rate at which data is reported relatively low in order to avoid inundating the WSN with too much speed data [14]. A

higher sample frequency increases the “output data and the rate at which the data is reported”, but decreases the “accuracy of the reported speed” [14]. Lastly, we used the Squelch Control-50 command, which is the second highest sensitivity setting available [14]. We did not set the sensitivity to the highest level possible because we wanted to mitigate potential false positives. Using these settings, the SRR was able to detect the moving person and calculate the speed without any failures to detect movement. It proved highly effective in detecting movement and capturing speed data, but its detection range at these settings were not as high as the advertised capability. Changing the squelch control to a higher sensitivity setting could have increased the range, but likely would have increased the false positive rate.

Table 2. OPS-241A Short-Range Radar Configurations. Adapted from [14].

Type of Command	**Value**	**API Command**
Sample Frequency	5,000 per second	SV
Speed Output Units	Meters per second	UM
Module/Transmit Power	Max Transmit	PX
Squelch Control	Squelch Control-50	QV

The speed ranges used at the NPS field experiment and the CACTF to classify the intrusion event into low, medium, or high threats are depicted in Tables 3 and 4. We discovered that because of the higher wind conditions at the CACTF, the same speed ranges determined to be effective at the NPS field experiment were not as effective at the CACTF. The wind resulted in the SRR sensors triggering false positives. Noticing this effect, we adjusted the speed ranges accordingly to successfully reduce the number of false readings. The need to perform this adjustment showed us that the same sensor settings will not have the same effectiveness in every environment, but need to be adjusted accordingly to fit the environmental conditions.

Table 3. Speed Ranges Used to Classify Initial Threat Assessment (NPS).

Speed Range (meters per second)	**Threat Classification**
Less than 0.5m/s	Low
Between 0.5m/s and 1.5m/s	Medium
Above 1.5m/s	High

Table 4. Speed Ranges Used to Classify Initial Threat Assessment (CACTF).

Speed Range (meters per second)	**Threat Classification**
Less than 0.7m/s	Low
Between 0.7m/s and 2.0m/s	Medium
Above 2.0m/s	High

2. Intrusion Detection Performance of Bravo Nodes

The capabilities and limitations of the Bravo nodes with facial recognition capabilities were documented in Hoon and Foo's thesis. The same sensors and cameras from their thesis were used for the Bravo nodes in this experiment. Key findings regarding the facial recognition mode and its sensors from their field experiment were that "PIR sensor performance was greatly affected by ambient temperature and light intensity," and that "detection of the intruder facial image was affected by the position of the sun, the intensity of the backlight, and the level of contrast between the intruder face and the background" [8]. These characteristics were also found to be true for our experiment. The PIR sensors on the Bravo nodes were more susceptible to false readings as the temperature rose and light intensity increased. In addition to identifying facial features of an actual intruder, we found that the Bravo nodes occasionally classified clouds as intruders as well. The use of more accurate PIR sensors for the Bravo nodes can probably greatly reduce the

false detection rate of the PIR sensors. For more details on the performance of the facial recognition capability and sensors of the Bravo nodes, refer to Hoon and Foo's thesis.

3. Wireless Network and Coverage Assessment

The overall ability of our experimental WSN to provide early detection depends on both the effectiveness of the individual nodes, as well as the robustness of the network on which the data travels. This section presents findings captured from the initial establishment of the WSN and node failure tests that were conducted.

Because the Alpha and Bravo nodes were set to Wi-Fi ad hoc mode and configured to join a common network name, we expected connectivity to be almost instantly established upon the devices being powered on. This was verified to be the case by successful ping connectivity among the nodes immediately after start up. There was also no issue connecting the Bravo nodes to the Zoom router and the C2 application laptop.

a. MQTT Broker Failure Test

As discussed in Chapter II, MQTT operates on a publish-subscribe model with a broker acting as the intermediary the data publisher and the various subscribers. Therefore, the node that runs the MQTT broker can be a single point of failure for the entire WSN. To avoid this potentially disastrous outcome, all Alpha nodes were assigned both a primary and secondary gateway. When an Alpha node has a message to publish, it first attempts to connect to the primary broker. In the event that the primary broker cannot be reached, the Alpha node proceeds to connect to the secondary broker and publishes the message using the available broker.

During our experiment, Bravo Node 8 acted as the primary MQTT broker, and Bravo Node 5 acted as the secondary MQTT broker. In order to test that Bravo Node 8 successfully passed the published message to the MQTT subscriber, an Alpha node was intentionally triggered so that it could publish speed data to the Bravo nodes. Once this was verified, Bravo Node 8 was turned off in order to test if the next published message still reached the Bravo nodes despite the primary gateway being disabled. We triggered the Alpha node once again and showed that the published speed data could still reach the Bravo

nodes. This demonstrated that messages could travel to the subscribers using a secondary MQTT broker. This simple mechanism put in place guaranteed a basic form of redundancy in case of primary broker failure.

b. Node Failure Alert

Since the individual nodes act together to provide a defense in depth, it is important to ensure that the human operator behind the SCC is aware of individual node failures. As discussed in Chapter II, MQTT's "last will and testament" feature enables a publisher node to send a message to the subscribers in the event of lost connection. The operator then has the opportunity to identify the cause of the outage and troubleshoot accordingly. We verified this feature by turning off several publisher nodes and seeing that subscriber nodes did in fact receive last will and testament messages from the publishers that went offline.

4. System Integration Testing and Assessment

The previous two sections discussed the tested capability and limitations of individual nodes as well as the network's ability to route the data captured by the nodes. This section discusses the performance of the overall WSN in accomplishing its primary purpose of early intruder detection.

When an intruder first triggers the outer sensor perimeter, the speed of the intruder is classified into high, medium, or low threat categories. During our experiment, we wanted to ensure that a "high" threat classification would result in the immediate notification of the operator. This meant that the speed data had to be received by the C2 application moments after the intrusion event. During our run trials, the experimental aide was instructed to run towards the outer sensor perimeter in order to generate a speed fast enough to be classified as a high threat. We successfully verified that the C2 application immediately received the captured speed data and the high threat alert within seconds after the Alpha node was triggered. This meant that the human operator in the SCC would be granted the longest time possible to respond to a 'high' threat after it is first detected. During our experiment at CACTF, we also discovered that the Alpha nodes were more susceptible to false positives due to the higher wind conditions. This meant that the speed

ranges we used for classifying threat at the NPS experiment needed to be adjusted to reduce the false positives.

Once an intruder has triggered the outer sensor perimeter, the PIR sensors on the Bravo nodes are activated to sense for any motion. As detailed by Hoon and Foo's thesis, accuracy in detection became an issue at this stage. While the Alpha nodes never failed to capture motion and was intentionally programmed to ignore speeds below 0.5m/s in order to avoid false positives, the PIR sensors on the Bravo nodes were less reliable and sometimes resulted in false positives. Furthermore, Bravo nodes also varied in the amount of time it took for OpenCV to determine that a human intruder was passing by the cameras. This difference in the time it took to identify an intruder as human reached upwards of approximately 30 seconds. While sometimes it was possible for the Bravo node to detect human features immediately upon its PIR being triggered and then send the image to the C2 application, other times it took more than 30 seconds to achieve. Once a Bravo node did detect human features and classify the threat as an intruder, it had no issues sending the image to the C2 application within seconds. Despite this inconsistency, as facial recognition technology can be expected to advance over the coming years, we expect both the speed and accuracy of recognition to greatly improve.

Given that early detection is a priority objective of our WSN, maximizing the detection range of the WSN was a goal of our experiment. The placement of nodes depends on the operating environment. For example, nodes may need to be placed closer together in crowded urban environments and be placed further apart in wide-open spaces. For our experiment, we wanted to test the maximum range that we could extend the network in a relatively open space. To determine the maximum range, we started from the location of the C2 application and proceeded outward from there. We took the Zoom router as far away from the C2 application as possible without losing connectivity. Then we extended the Bravo node from the router until it could no longer ping the router. Lastly, we extended the Alpha node from the Bravo node until they could no longer connect to each other. The distances were then summed to calculate the maximum detection distance of the WSN. In our experiment, we determined the maximum detection distance of our WSN to be approximately 98.45 meters. More powerful wireless routers can certainly boost this range

even further. The SRR may also alter this range calculation depending on the configurations that were set via the API. Figure 19 demonstrates the method by which maximum detection range of the WSN was determined.

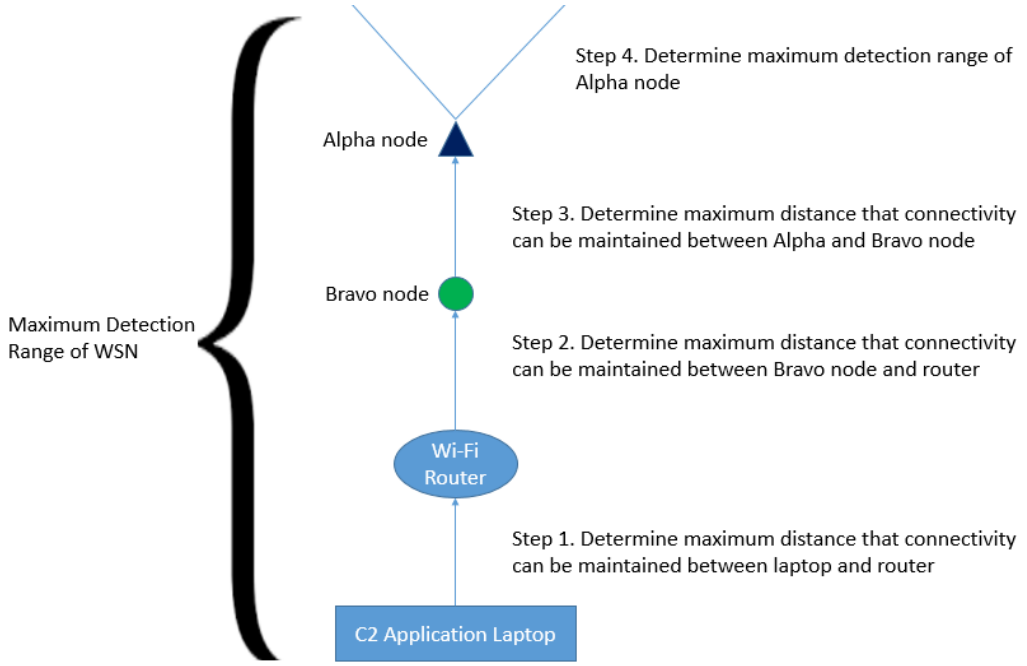

Figure 19. Method Used to Calculate Maximum Detection Range of WSN.

The detection range of the WSN directly affects the amount of time that responders have to respond to an intrusion event. For both the NPS and CACTF field experiments, we measured the amount of time it takes for the intruder to reach the SCC while running and walking. Starting from a distance of about 10 meters outside of the outer sensor perimeter, we measured that on average, it took about 1 minute and 23 seconds for an intruder walking to reach the SCC, and about 54 seconds for an intruder running to reach the SCC. While this is not a large amount of time that defenders have, these crucial seconds can enable the SCC to alert personnel along the physical defense perimeter to look towards a specific area of the perimeter and take action.

C. SUMMARY

This chapter detailed the field experiments that were conducted to test the effectiveness of our system architecture. The results from our field experiments demonstrate the advantages of the layered defense approach using a variety of sensors at each layer. The short-range radar nodes proved highly successful in detecting motion and capturing the speed data, but its detection range fell short of the its advertised capabilities based on the configuration settings we used. The less computing intensive nodes along the outer sensor perimeter were able to vet the threat so that the Bravo nodes, which were much more computing intensive as they run OpenCV, did not have to repeatedly activate in response to every possible intrusion. Furthermore, the Alpha nodes enabled a more flexible response to each threat based on its classification. In other words, operators could allow the inner sensor perimeter to perform additional analysis before taking action to interdict the threat. The network architecture successfully supported the communication requirement among the sensor nodes and proved resilient to several node failure scenarios. While false positives remained an issue with the facial recognition capability, the overall system worked well to provide early detection of intrusions. Although each layer alone had flaws, the application of the defense in depth principle enabled the outer and inner sensor perimeters to provide mutual support and better provide intrusion detection as an overall system.

V. CONCLUSION

A. SUMMARY

The security of air bases and FARPs will remain a top priority in 21st century operations. Our adversaries will continue to utilize proven tactics of infiltration and short-range attacks in order to degrade our air superiority. To address this problem, we conducted this research to investigate how to leverage low-cost COTS platforms in order to augment the defense of FARPs.

Our colleagues, Ding Yao Hoon and Kenneth Foo, developed a WSN of Raspberry Pi sensor nodes capable of performing facial recognition of intruders. We expanded upon their WSN by building an extra set of Raspberry Pi nodes equipped with short-range radar sensors in order to complement and enhance the existing capabilities of the facial recognition nodes. By introducing this heterogeneity into the WSN, the overall system became more robust and capable of detecting intrusions. Furthermore, the sensor nodes were programmed to establish the network autonomously in an ad hoc manner instead of connecting to a central wireless router. Building part of the WSN in an ad hoc manner further improved the ease of deployment and setup as well as improving the robustness and reliability of the network.

B. PERFORMANCE

Performing two separate field experiments, at the NPS campus and at Camp Robert's CACTF, we validated the effectiveness of our experimental WSN. The Alpha and Bravo nodes with different sensors were successfully integrated into a layered-defense construct to provide early warning in intrusion detection scenarios. While the facial recognition capability was not 100 percent reliable, this did not significantly degrade the feasibility of the system architecture and the ability of our WSN to detect intruders. The experiments conducted by no means exhaust the conditions under which the system or a similar one may be deployed. There is no doubt that environments where the 802.11 spectrum is saturated or degraded by urban sprawl can degrade the performance of the WSN. However, through these experiments, we showed that by applying the principle of

defense in depth, relatively cheap COTS platforms and sensors can indeed be leveraged to provide decent early detection of intrusion events.

C. RECOMMENDATION FOR FUTURE WORK

In this thesis, we built our WSN using Raspberry Pi nodes equipped with a variety of sensors, including the OPS-241A short-range radar, webcam, and PIR sensors. While this combination of sensors provides excellent imagery and kinetic data in our airbase defense application, a myriad of other sensors can be explored for the capabilities they bring. Additionally, the Raspberry Pi is only one of many low-cost computing platforms that can be used for a perimeter defense application. Other platforms, such as the Arduino, should be explored in order to identify if the same capabilities can be offered at even lower costs.

Scalability and manageability of a large number of sensor nodes also present a challenge that requires further research. In order for sensor nodes such as the ones we developed to be deployed at scale to cover a large area or perimeter, management of these nodes and the network that they form become critically important. A system is only as useful as the degree to which it is manageable. The efficient management of nodes within a wireless sensor network at scale is an important research area that must be addressed.

Security is also a concern when trying to leverage low-cost COTS platforms for military applications. Both the individual nodes and the network are vulnerable to cyberattacks. Research should be conducted into how to effectively and cheaply secure a WSN built from COTS platforms.

LIST OF REFERENCES

[1] A. J. Vick, “Air base attacks and defensive counters: Historical lessons and future challenges,” RAND Corp, Santa Monica, CA, USA, 2015. [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a620337.pdf

[2] B. C. Palm and R. P. Richter, “Mobile situational awareness tool: Unattended ground sensor-based remote surveillance system,” M.S. thesis, Dept. of Comp. Sci., NPS, Monterey, CA, USA, 2014. [Online]. Available: https://calhoun.nps.edu/handle/10945/43971

[3] M. P. Buonaugurio, “Air base defense in the 21st century: USAF security forces protecting the look of the joint vision,” M.S. thesis, USMC Command and Staff College, Quantico, VA, USA, 2002. [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a401262.pdf

[4] S. W. Caudill, *Defending Air Bases in an Age of Insurgency*. Maxwell Air Force Base, AL, USA: Air University Press, 2014.

[5] H. T. Brown, “Current air base ground defense doctrine: Are we postured to meet the expectations of the AEF,” Air Command and Staff College, Maxwell Air Force Base, AL, USA, 2001. [Online]. Available: http://www.vspa.com/pdf/current-air-base-ground-defense-doctrine.pdf

[6] J. Sundram and P. P. Sim, “Using wireless sensor networks in improvised explosive device detection,” M.S. thesis, Dept. of Comp. Sci., NPS, Monterey, CA, USA, 2007. [Online]. Available: https://calhoun.nps.edu/bitstream/handle/10945/3129/07Dec_Sundram.pdf?sequence=1

[7] V. Vujovic and M. Maksimovic, “Raspberry pi as a wireless sensor node: Performances and constraints,” in *2014 37th Intl. Con. on Info and Comm Tech, MIPRO*, 2014. [Online]. doi: 10.1109/MIPRO.2014.6859717

[8] K. Foo and D. Y. Hoon, “Low-cost ground sensor network for intrusion detection,” M.S. thesis, Dept. of Comp. Sci., NPS, Monterey, CA, USA, 2017. [Online]. Available: https://calhoun.nps.edu/handle/10945/56137

[9] OmniPreSense. Accessed October 20, 2017. [Online]. Available: http://www.omnipresense.com

[10] MQTT. Accessed October 20, 2017. [Online]. Available: http://mqtt.org

[11] Armtronix, “Installing mqtt broker (mosquitto) on raspberry pi,” Instructables, April 11, 2016. [Online]. Available: http://www.instructables.com/id/Installing-MQTT-BrokerMosquitto-on-Raspberry-Pi/

[12] W.J. Chen, R. Gupta, V. Lampkin, D. M. Robertson, and N. Subrahmanyam, *Responsive Mobile User Experience Using MQTT and IBM MessageSight*. Poughkeepsie, NY: International Business Machines Corporation, 2014. [Online]. Available: http://www.redbooks.ibm.com/redbooks/pdfs/sg248183.pdf

[13] Open-Mesh. Accessed October 20, 2017. [Online]. Available: http://www.open-mesh.org

[14] OmniPreSense, “AN - 010 api interface specification,” San Jose, CA, USA, 2017. [Online]. Available: https://www.omnipresense.com/wp-content/uploads/2017/08/AN-010-A_API-Interface.pdf

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California