NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

LOW-COST GROUND SENSOR NETWORK FOR INTRUSION DETECTION

by

Dingyao Hoon
Yueng Hao Kenneth Foo

September 2017

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

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

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

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE LOW-COST GROUND SENSOR NETWORK FOR INTRUSION DETECTION	**5. FUNDING NUMBERS**
6. AUTHOR(S) Dingyao Hoon and Yueng Hao Kenneth Foo	
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. IRB number ____N/A____.	
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Perimeter surveillance of forward operating locations, such as Forward Arming and Refueling Points (FARPs), is crucial to ensure the survivability of personnel and materiel. FARPs are frequently located well outside the protective cover of the main forward operating bases. Therefore, they must provide their own organic perimeter defenses. Such defenses are manpower intensive. Our research investigates how cheap, remote, unattended sensors using commercial off-the-shelf (COTS) components can help reduce the manpower requirement for this task and yet not compromise the security of the operating location. We found Internet of Things (IoT) platforms such as Raspberry Pi, paired with passive infra-red sensors and cameras, to be useful in this application. We built a prototype sensor system, tested it in a simulated field environment, and evaluated its performance. We conclude that COTS IoT platforms have much potential to support surveillance of FARPs and other forward operating locations.

14. SUBJECT TERMS wireless, low-cost, network, IoT, PIR, image recognition, air base ground defense system, OpenCV, sensor, Raspberry Pi	**15. NUMBER OF PAGES** 147
	16. PRICE CODE

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

LOW-COST GROUND SENSOR NETWORK FOR INTRUSION DETECTION

Dingyao Hoon
Major, Army, Singapore Armed Forces
B.I.T., University of Queensland, 2012

Yueng Hao Kenneth Foo
Project Manager, Defence Science and Technology Agency, Singapore
M.C., National University of Singapore, 2012

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2017

Approved by: John H. Gibson
Thesis Advisor

Gurminder Singh, Ph.D.
Co-Advisor

Peter J. Denning, Ph.D.
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Perimeter surveillance of forward operating locations, such as Forward Arming and Refueling Points (FARPs), is crucial to ensure the survivability of personnel and materiel. FARPs are frequently located well outside the protective cover of the main forward operating bases. Therefore, they must provide their own organic perimeter defenses. Such defenses are manpower intensive. Our research investigates how cheap, remote, unattended sensors using commercial off-the-shelf (COTS) components can help reduce the manpower requirement for this task and yet not compromise the security of the operating location. We found Internet of Things (IoT) platforms such as Raspberry Pi, paired with passive infra-red sensors and cameras, to be useful in this application. We built a prototype sensor system, tested it in a simulated field environment, and evaluated its performance. We conclude that COTS IoT platforms have much potential to support surveillance of FARPs and other forward operating locations.

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 System
ADAPT	Adaptable sensor system
API	Application programming interface
C2	Command and Control
COM	Communication
COTS	Commercial off-the-shelf
DARPA	Defense Advanced Research Projects Agency
DC	Direct current
DOD	Department of Defense
FARP	Forward arming and refueling point
Gbps	Gigabits per second
GPS	Global positioning system
GUI	Graphical user interface
HF	High frequencies
IoT	Internet of Things
IP	Internet Protocol
LiDAR	Light Detection and Ranging
LTE	Long term evolution
MANET	Mobile ad-hoc network
MSAT	Mobile Situational Awareness Tool
OpenCV	Open-source Computer Vision
PIR	Passive infra-red
QR	Quick Response
RF	Radio frequencies
SQL	Structured Query Language
SSD	Solid state drive
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
UAV	Unmanned Aerial Vehicle

UGS	Unattended ground sensor
UGV	Unmanned ground vehicle
UHF	Ultra-high frequencies
VHF	Very-high frequencies
WGS	Wireless ground sensor
WGSN	Wireless ground sensor network
WWII	World War II

ACKNOWLEDGMENTS

First and foremost, we would like to thank our families for their continuous understanding and support while we pursued our master's degrees. It was not easy for our families while we focused on our studies and research.

Heartfelt gratitude to our advisors, Mr. John H. Gibson and Dr. Gurminder Singh, for lending their guidance and support to make our research meaningful and insightful. It was a very fulfilling journey for the both of us as; we were presented with an opportunity to build a technology demonstrator during the period our research, and tested it during a field experiment at Camp Roberts.

We would like to express thanks and gratitude to Mr. Brian Wood for supporting our field experiment and getting us ready for it prior to the actual field experiment. We would also like to thank Mr. Charles Prince for lending us the equipment so that we could build the sensors. Our field experiment would not have been possible without the help rendered to us.

We would also like to extend our thanks to our thesis processor, Aileen Houston, from the Thesis Processing Office, for advising and ensuring that our work is properly cited and formatted to publishable standards.

Finally, we would like to thank our organizations for sponsoring and giving us this opportunity to study at the Naval Postgraduate School (NPS). The program has enabled us to better understand each other's culture, and build networks with one another.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Perimeter surveillance of forward operating locations, such as Forward Arming and Refueling Point (FARP), is crucial to ensure the survivability of personnel and materiel within the operating locations. Perimeter defenses are intended to prevent any unauthorized access or intrusion of the facility, especially when operating outside the main defense zones. Such operations require significant manpower and, depending on the scale of the facility, additional manpower may be required to ensure continuous surveillance. We investigate how technology can help reduce the manpower requirement for this task and yet not compromise the security of the operating location.

With the rise and maturity of the Internet of Things (IoT) devices, we have the possibility of building a network of sensors with these devices. Similar technology can be adopted for a FARP's perimeter surveillance. Since the sensor data is perishable, we investigate how to develop an unmanned wireless sensor network using low-cost commercial off-the-shelf (COTS) components that can help to supplement or enhance the survivability of a FARP deployed overseas.

A. OBJECTIVES

The objective of this thesis is to design, develop and validate a low-cost unmanned wireless ground sensor network using COTS equipment (with an aggregated unit cost of approximately $100 USD per node) for surveillance in tactical FARPs. Together with these wireless sensor nodes, we leveraged existing technology to create a reliable and resilient ad-hoc mesh network across the operating base to allow any unmanned ground sensor nodes within the operating base to connect to the network automatically. The performance of the sensor network is validated in a field environment. The network architecture, network communication interfaces and resulting performance analysis and data are beneficial for the future employment and support of new suites of COTS sensors and devices.

B. RELEVANCE TO THE DEPARTMENT OF DEFENSE

There are many opportunities for the Department of Defense (DOD) to exploit the use of IoT platforms within its operating environment. The benefits include (1) better management of DOD assets, (2) identification of items or persons of interest, (3) improved readiness, and (4) ability to do more with less (Department of Defense Chief Information Officer, 2016). Specifically, the policy on IoT provided a case study regarding battlefield situational awareness. Our research is aligned with the intent described in the policy, which is to "provide warfighters with enhanced situational awareness" (p. C-4). This research investigates the challenges that the U.S. Marine Corps Aviation is facing with respect to intrusion detection and early warning for remote, small operating bases. Our research presents a proposed solution and implementation to provide such capability to augment the manpower available with remote, unattended sensors such that the available manpower can be most effectively utilized.

C. THESIS ORGANIZATION

The thesis consists of five chapters, namely, Introduction (Chapter I), Background (Chapter II), System Design (Chapter III), Field Experimentation (Chapter IV), and Conclusion (Chapter V).

Chapter I defines the problem statement and states the objectives of the research. It provides an overview on the motivation, objectives and benefits to DOD of the research. Finally, it provides the overall flow of the thesis and its organization.

Chapter II briefly covers the history of air base ground defense (ABGD) systems and their concepts of operation to provide security defense within an air base environment. It also provides a literature review of past sensor projects that study previous implementations. With the evolution of technology that has enabled fast capability growth and cheap components, it becomes prudent and sensible that we review these technologies to identify the right components for implementation by this research.

Chapter III discusses the system design of our prototype implementation and its design considerations. After assessing the available hardware and technologies, we discussed how we settled upon the various components and parts to build the prototype.

Chapter IV presents the field experimentation design and its results. This chapter covers the test plan that we designed and how we went about validating the sensor network implementation. From the field experimentation, we also identified possible future work that could help to further improve the current concept and make it more robust.

In Chapter V, we conclude and summarize the entire research journey. We also present and justify how our work answers the research question. Finally, we propose possible future works to help improve the current implementation.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. AIR BASE GROUND DEFENSE (ABGD)

The following section describes the characteristics of an ABGD system and why is it important in warfare. We discuss some of the pertinent points and rouse interest on how we can design an air base perimeter monitoring system for a forward arming and refueling points (FARP).

(1) History of Air Base Ground Defense

The concept of ABGD was first conceived during the World War II (WWII) after painful and costly lessons were learned during WWI (Purser, 1989). This capability has since been growing through the years. We now see infantry-trained soldiers providing perimeter defense to ensure the survivability of the air base and to ensure and support the undisrupted operations of an air base. Today, the air bases are prepared to face and counter both ground and air attacks.

(2) Characteristics of ABGD

A FARP is a site setup so that projection and support assets like aircrafts can land, rearm, refuel, and return to action soonest possible during operation. “The rapid movement and employment of fighter aircraft by means of mobile forward arming and refueling points (FARP) support this priority” (Davis, 2014, p. 6). A FARP, specifically one with air base to support fighter jets, remains to be the most effective, power projection of rapid air response forces.

> The most significant strategic benefit of the fighter FARP concept is its potential deterrent value. Possession of a credible capability to conduct fighter operations despite an adversary’s attempt to deny forward basing would likely have a deterrent effect and might prevent the need for lethal military force. (Davis, 2014, p. 18)

A FARP’s defense is therefore of paramount importance to the military mission. The main objective of the ABGD system is to ensure the survivability of the FARP, that is, to defend against air, ground attacks, and recovery after an attack. A sustainable

ABGD system requires the necessary manpower to respond to these external threats to the installation so as to protect critical weapon systems, equipment, and other key assets through strict access control (Purser, 1989).

B. EMERGENCE OF IoT AND WIRELESS SENSOR NETWORK

The IoT is fast becoming a popular and easily available technology to researchers and consumers. The interconnectedness of everyday devices, equipped with ubiquitous intelligence, allows us to integrate these devices and turn them into useful applications (Xia, Yang, Wang, & Vinel, 2012). These smart devices can act as sensors that allow us to keep track of our appliances' statuses and vital parameters, both locally and remotely. Examples of such appliances include smart TVs, refrigerators and air conditioners. From the Gartner's chart in Figure 1, it was observed that IoT platforms peak the inflated expectations (Gartner, 2016). Technology such as this has the potential to improve our daily lives and has many applications within the defense ecosystem. These wireless devices, when paired with wireless meshed networks, become a powerful tool for us to build a networked of sensors for surveillance monitoring in the military domain.

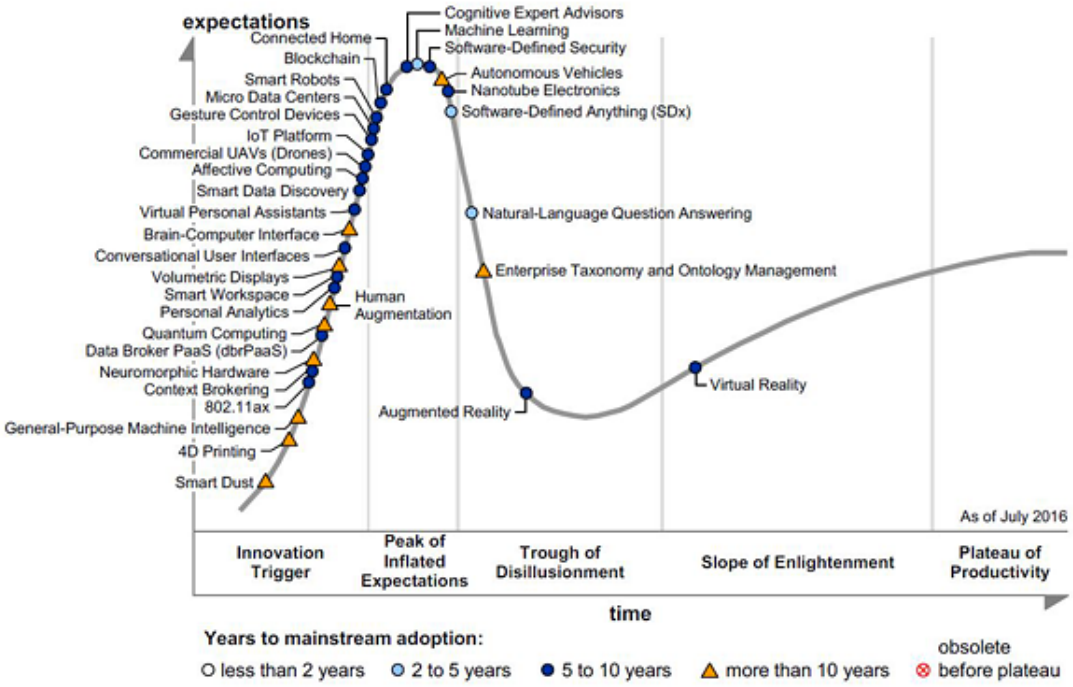


Figure 1. Hype Cycle for Emerging Technologies. Source: Gartner (2016).

Our research explores the possibility of leveraging IoT platforms to build a wireless sensor network to provide enhanced surveillance for perimeter defense to support an ABGD system within a FARP.

C. PREVIOUS IMPLEMENTATIONS TO SOLVE THE PROBLEM

This section reviews other projects that aim to provide some form of situational awareness, which is similar to our topic of interest. Finally, we review research that used the DRAPA's ADAPT sensors as a comparison. The aim is to study the similarities and differences between these efforts.

1. Low-Cost Alert System for Monitoring the Wildlife

This research reviews the development of a low-cost alert system for monitoring wildlife using IoT devices. It presents how Raspberry Pi when combined with a PIR sensor, can be used to track the movement of wildlife and illegal wildlife smuggling (Sheela et al., 2016). The central idea is to connect different sensors and establish a communication link to create an alert system within the nature reserve. The device is programmed using the Python language, and uses Open-source Computer Vision (OpenCV) for image processing and detection. The device is equipped with a GPRS/3G module to send images back to the control center for monitoring. Each sensor device is also equipped with a solar panel to charge the battery to power the device. This research presents a low-cost, reliable, and simple solution to solve its problem.

2. A Cost-Effective Unattended Ground Sensor Using COTS Products

Hempenius et al. (2012) investigated the use of Android smartphones and Arduino microcontrollers to create a low-cost plug and play sensor interface to be incorporated into existing tactical networks. The information that these sensors collect provides situational awareness to leaders, to aid them in making better decisions during operations. The authors chose an Android smartphone as the main processing core as it has all the essential sensors and communication capability on a small footprint device (in terms of size, weight and power density). An Android smartphone also makes the information assurance requirements for the sensor network easier as there are readily

available security hardening templates and guidelines available for an Android smartphone. The authors leveraged on an open-source Android application to create ad-hoc networks between multiple Android smartphones and Arduino microcontrollers. To demonstrate the capability of the cost-effective plug and play sensor interface, these smartphones and microcontrollers are installed on a number of Unmanned Ground Vehicles (UGV) and several tests were conducted to evaluate their performance. This easily customized, non-proprietary platform for unattended ground sensor networks was able to support simple data collection capabilities and is scalable to support surveillance using images and videos. This new cost-effective capability allows COTS sensors to be integrated into existing tactical networks easily and quickly, without having to leverage proprietary standards and products that are expensive to purchase and maintain, difficult to upgrade, and complex to integrate.

3. Border Patrol—Mobile Situation Awareness Tool (MSAT)

The Mobile Situational Awareness Tool (MSAT) is a user interface for handheld devices for the DARPA ADAPT prototype, providing access to the data from the passive infra-red (PIR) sensors and cameras aboard wireless network sensors. Its main purpose is to detect and classify intruders in the sensor field so as to reduce manpower requirements and the increased risk to friendly personnel, specifically in support of a rifle squad in a defensive battle position.

Previous research by Palm (2014) discussed how the sensor nodes can communicate with each other and handheld monitoring stations monitor the ground situation. The nodes were networked using 802.11 g/n, with a MiFi (mobile wireless router that supports ad-hoc networking) access point that provided 4G/LTE for outside Internet connectivity. Remote Command and Control (C2) monitoring was enabled and used a proxy server to provide additional network security. The study also revealed that multiple sensors may be used to enhance the robust threat classification algorithms to achieve better automation and autonomy.

4. Wireless Sensor Buoys for Perimeter Security of Military Vessels and Seabases

Previous work also explored the concept of using wireless sensors mounted on floating buoys that can be deployed around vessels or sea bases to support perimeter security and defense. The wireless sensor nodes used in the prototype leveraged the DARPA ADAPT wireless sensors, which are equipped with rechargeable battery packs, Global Positioning System (GPS), PIR sensors, WiFi (based on 802.11n wireless protocol for communication with a ground station) and 900 MHz ground radio (for inter-sensor node communication) all controlled by an Android-based processing core (Kent, 2015). Besides adapting the DARPA ADAPT wireless sensors to floating buoys, the author also researched the implementation of a mobile ad-hoc network (MANET), using both WiFi and 900MHz radio in an open ocean environment.

In order to evaluate the technology demonstrator and the performance of the MANET network in an open ocean environment, numerous tests were conducted and several limitations were identified and discussed. First, the author discovered that PIR sensors were not a suitable for intrusion detection in an open ocean environment as the frequent movement of the waves on the sea surface would result in a high frequency of detection, with most of the detection being false positives. Second, based on the tests conducted by the author, it was discovered that the communication range of standard WiFi, though around 250 meters in radius will pose a challenge to the overall system when deployed around a wide area as some of the wireless sensor node deployed further away from the base station will be near the 250-meters threshold and encounter weak or intermittent WiFi signal.

The author concluded the paper by proposing using alternate wireless sensors, other than PIR sensors, for detection and using longer-range networks, like Long Term Evolution (LTE) cellular network for long-range communication between the wireless sensor node and the base station. We plan to leverage a similar system design concept and attempt to build a wireless sensor node using low-cost components including a Raspberry Pi, COTS PIR sensors, cameras, WiFi, Bluetooth and possibly LTE for land-based perimeter defense applications.

D. RELATED TECHNOLOGY COMPONENTS

Previous work (Kent, 2015; Palm, 2014; Tingle, 2005; Williford, 2012) report several different hardware platforms used to build the wireless sensor networks by NPS researchers. These platforms include Raspberry Pi, Android mobile phones, DARPA's ADAPT sensor and low-powered processing board (Arduino). This section explores the different hardware availability and their suitability to our research.

1. Wireless Sensor Networks

The backend network infrastructure forms the communication links for the network devices to communicate with one another. This section discusses the importance and possible choices for the network that this research leveraged. Previous research investigated how experimental, wireless, unattended ground sensor (UGS) networks using COTS devices can effectively self-organize to support dynamic changes in the network such as during a node failure, signal degradation and mobility of the UGS nodes (Tingle, 2005). Each UGS node is equipped with an acoustic sensor, magnetic sensor, and acceleration sensor to provide various detection and sensing capabilities. Some of the UGS nodes are also equipped with GPS receivers that act as beacon nodes that transmit GPS location information to nearby UGS nodes that are not equipped with GPS. Tingle (2005) also explored using WiFi signal strength triangulation with nearby beacon nodes to determine the approximate location of the non-beacon UGS nodes. Through various indoor and outdoor test scenarios, the author could characterize the detection range and performance for the various sensors onboard the UGS node, as well as the effective communication range between UGS nodes. The author demonstrated that the wireless UGS networks could dynamically perform node discovery and autonomous reconfiguration when there are node failures and communication link degradation. This substantiated the feasibility of deploying such wireless UGS networks for military surveillance applications (Tingle, 2005). The author recommends researching different types of antenna and transmission power to improve the communication range and system performance, as well as exploring various software packages and algorithms that can help to better correlate and fuse different sensor data to improve the accuracy. We

considered one of the possible radio frequencies (RF) based communication links, which is WiFi, a non-license band radio frequency.

a. IEEE 802.11 WiFi

WiFi may be used to form the communication link between the wireless ground sensors (WGS) and the backend server. It is important that the link is highly resilient and inter-connected to ensure that data can be sent and receive from the server. The link must be self-healing and meshed networking is desired to ensure bandwidth availability. WiFi communicating on 2.4GHz is one of the available standard WiFi services that supports unlicensed usage, meaning that the band of the WiFi is available for anyone to use, without having to pay for operating within its frequency band.

b. Radio Frequencies

Other unlicensed radio frequencies offer another possible means to provide communication between the sensor nodes and the C2 server. The DARPA ADAPT sensor utilizes the 900 MHz ground radio.

There are many other radio frequency bands that are available; examples of these are High Frequency (HF), Very High Frequency (VHF), Ultra High Frequency (UHF). The cost to use the frequencies varies based on the band used for radio communications due to licensing considerations. The decision to implement WiFi or licensed/unlicensed radio frequencies need to be thoroughly considered and weighed based on budget, operational needs or even interoperability with other systmes.

2. Unattended Ground Sensor

In order to fulfill the operational requirements to provide surveillance on perimeter defense, we envisaged the sensor node to be non-mobile, and be able to provide autonomous reporting through the communication link when it detects a person passing through its perimeter. The ground sensor node should be small and able to operate on its own power for a considerable length of time. It should also be able to communicate with the backend server via the communication link. With these requirements in mind, further research was performed to understand components which are critical to making this

system work. Primarily, these components involve the potential sensors that may be adopted since the choice of sensors helps determine the signals on which detections are based, as well as the power supply needed for each node, which is a critical component of the system.

a. Raspberry Pi

Raspberry Pi (Raspbery Pi, n.d.) has become a very popular platform among IoT enthusiasts. It is compact, affordable and allows low-powered processing. It is a good choice for our IoT platform as we need a platform that can be easily deployed given the large quantities of sensors required for ABGD system. The Raspberry Pi comes in a few variants and currently the most capable model is the Raspberry Pi 3 model B. This particular model supports HDMI, USB, wireless, and Bluetooth connections.

b. Other IoT Devices

Williford (2012) examined the use of unattended ground sensors nodes, combined with wireless network and smartphones, to reduce manpower impacts on perimeter surveillance. The field experiment included the usage of Android smartphones and sensor control boards from Phidgets, Inc, to develop a real-time surveillance system. The sensors relied on external power and were not weather-resistant. Sensors deployed included IR, sound, accelerometer and vibration sensors (Williford, 2012). The experiment successfully captured and transmitted the sensor data over the local area network to the smartphone for monitoring. The use of sensors like accelerometer and vibration sensors may be of relevance to ours and the viability of implementation of such sensors on the Raspberry Pi is required.

c. Sensors

There are many different sensors available on the market that are relevant and may be used for detecting motion. With a mounted camera, the WGS could be able to capture images and perform correlation for threat analysis. A sensor, such as passive infra-red (PIR), is also useful for detecting movement, which is a critical component to a WGS to provide perimeter surveillance.

(1) Camera

The camera provides image capture to support facial recognition capability for the overall system. It is therefore important to look into the feasibility of implementing cameras that are suitable for the WGS. In particular, two types of cameras considered are USB web cameras and Raspberry Pi camera module. The USB web cameras allow the system to support additional cameras as long as there are sufficient USB ports, potentially increasing the WGS's field of view to as much as 360-degrees. As there is only a single Raspberry Pi camera module, only a single camera may be supported. However, the Raspberry Pi camera module does come with infra-red capability to allow images to be captured in a dark environment for night surveillance operation.

(2) Infra-red (IR) Sensor

The IR sensor allows the WGS to save its power by triggering the camera only when the movement is detected. This is the ideal mode of operation to cut down on the power required to power the WGS nodes. There are many commercially available IR sensors; an example is the Passive Infra-red (PIR) sensor, which is able to detect movement and consequently, activate the camera module on the WGS node.

(3) Location Mapping of Sensor Node

Todd E. Sims (2012) looked into mapping the location of the wireless sensor node without the use of GPS or acquiring prior knowledge of the locations of all the wireless sensor nodes. Inexpensive wireless routers/access points were deployed to gather data and location information of the wireless sensor nodes. ICMP echo message packets were used to calculate the distance from time-of-arrival (TOA) measurements. However, this method was deemed to be inaccurate due to lack of precise time stamps in the IEEE 802.11g protocol implementation.

COTS access points were found to be more reliable when used with a specifically calibrated range table. The author retrofitted the wireless access point with a GPS sensor and deployed it within the vicinity of the wireless sensor nodes. The signal-to-noise ratio of these nodes was measured to acquire location information (Sims, 2012). Our research

will explore ways to determine WGS locations and yet not create too much overhead on the node itself in terms of power consumption and cost to implement it.

d. Battery

The power supply for the WGS node is another critical component. Ideally, the system should be self-reliant and generate or harvest power. For this research, we considered a pocket battery pack, solar cell, and a portable generator. However, due to the nature of deployment of the envisaged sensor operations, it is ideal to adopt pocket battery packs, supplemented by solar cells so that users avoid having to replace the batteries as much as possible once the network has been established. However, the other consideration is that solar cells may be costly, which in return raises the overall cost of the WGS node.

3. Image Analytics (OpenCV)

The utility of the system and data analytics lie in the image analytics used. The analytics allow the system to not just simply take a photo or stream the video back to the command and control center, but also perform some level of facial recognition to detect if the facial features match those of a friend or a known foe.

OpenCV (OpenCV, n.d.) is an open-source framework that is used by many people for image processing and recognition capability. Its adoption rate is high and has been used by many for its flexibility and ease of use. A previous bachelor's project demonstrated the use of OpenCV libraries on Raspberry Pi to detect and keep track of objects captured by the Raspberry Pi camera module (Ivask, 2015). A GNU/Linux-based C/C++ application was created to achieve this. According to Ivask (2015), the system is able to (1) detect color blobs from the camera feed; (2) classify blobs as objects after meeting certain criteria and store them in memory to track their locations; (3) attempt to ensure realistic and linear movement of the objects; and (4) send useful information about these objects using UDP datagrams (p. 8). We explore different OpenCV image processing libraries, recognition techniques, and assess which is best suited for our usage.

E. SUMMARY

This chapter provided an overview of ABGD, a brief introduction to its concept of operations and why it is important to ensure that it is not compromised during operations. After a detailed study of previous research work and the types of sensors to be used, we narrowed our focus in order to construct a low-cost wireless ground sensor network for intrusion detection. It is also apparent that IoT technology has reached a level of maturity necessary for implementation and holds potential relevance to our research topic. The envisioned system will focus on leveraging available technology and resources to build a usable application of benefit to the U.S. Marine Corps Aviation in FARP operations. The research includes exploration of image capturing capability to perform facial recognition, as to its application to low-cost COTS components in support of military operations. The end-state of the research is to validate the capability through a technology demonstration during field experimentation and present the findings and recommendations for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SYSTEM DESIGN AND IMPLEMENTATION

This chapter discusses how the low-cost Wireless Ground Sensor Network (WGSN), consisting of nodes built using low-cost COTS components, can transmit early warning intrusion detection information to the C2 Application Server located within the FARPs tactical command post. Design concepts of our low-cost WGS node prototype for deployment within the FARPs tactical environment are presented. The chapter then provides details of the WGS Node Deployment Tool, WiFi mesh network infrastructure, C2 Application Server, Structured Query Language (SQL) database and the various applications that form the overall WGSN. Chapter III also explains the network connectivity and messaging protocol implemented between WGS node, WGS Node Deployment Tool, and C2 Application Server.

A. SYSTEM DESIGN CONCEPT

Our objective for early warning intrusion detection is to design and build a low-cost COTS components-based WGSN to provide US Marine Corps Aviation with an early intrusion detection capability for remote, small operating bases. This WGSN deployed around the perimeter of the remote, small operating bases will relay information to the centralized C2 Application Server through a WiFi network. The meshed WiFi network can be achieved by leveraging COTS meshed routers. Each router is connected to a few WGS nodes that will be responsible for providing intrusion detection data back to the C2 Application Server. The overall WGSN is designed to report any intrusion around the operating base's perimeter and attempt to recognize and track the intruder movement through the operating base using Passive Infra-red (PIR) and facial image recognition technology. The intrusion related information and images would be transmitted from the respective WGS nodes to the C2 Application Server and SQL database for processing, storage, and image analytics before presenting the consolidated situational picture and intrusion alert information as a dashboard on the C2 Application. Based on the presented information, the relevant base protection force can be activated to neutralize the intruder threats. Figure 2 provides the overall system design concept.

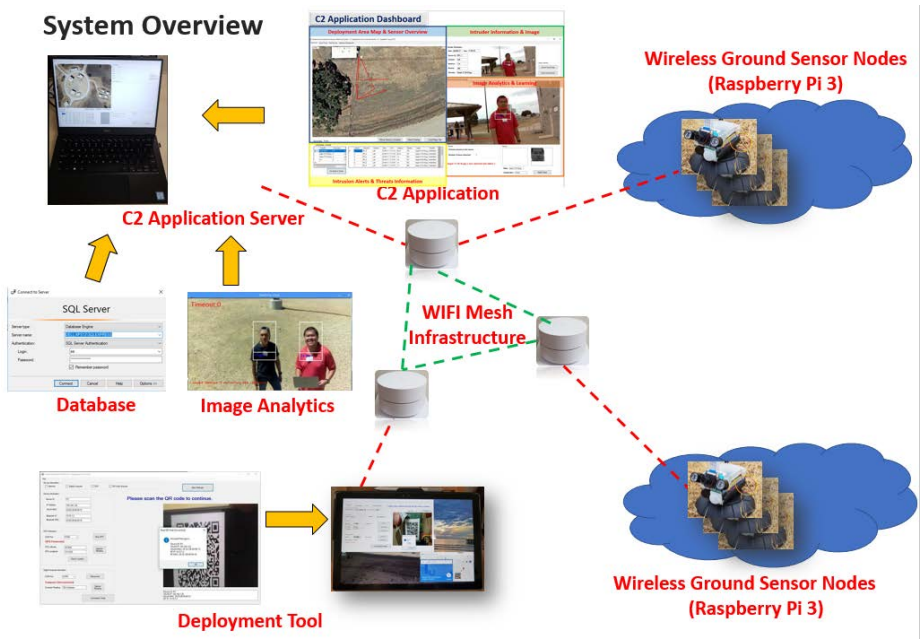


Figure 2. Overall System Design

The scenario presented in Figure 3 illustrates how the low-cost WGSN can be used to provide early intrusion detection and recognition within the operating base perimeter.

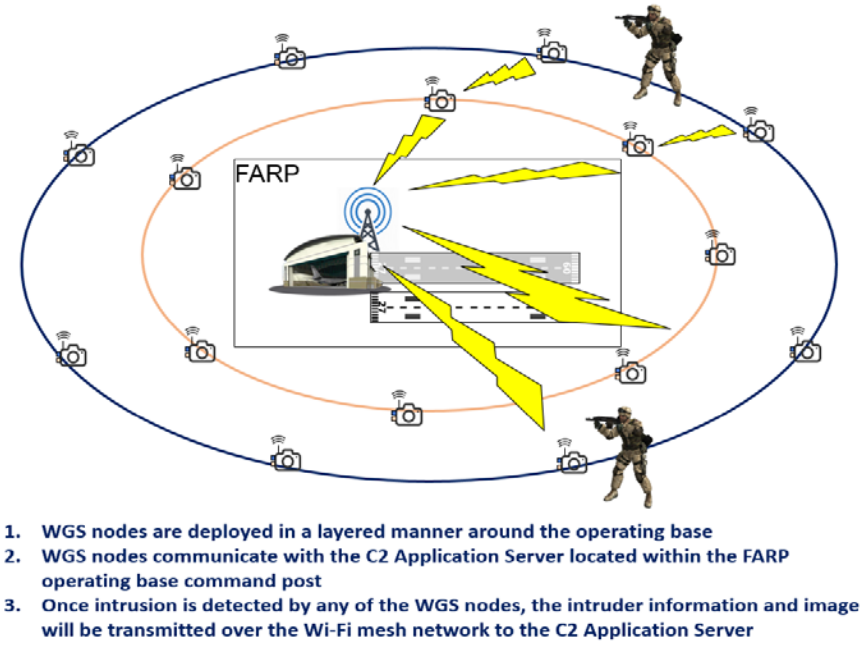


Figure 3. Overall System Operating Scenario

1. Wireless Ground Sensor Nodes

To provide round-the-clock unmanned perimeter surveillance and early intrusion detection, the WGS nodes deployed at different detection layers around the operating base perimeter must be able to actively detect an intrusion, determine the type of the intruder and send alerts to the C2 Application Server to alert the operator. To achieve this objective, the WGS node is equipped with PIR sensors to provide the initial intrusion motion detection, which in turn triggers the camera onboard the WGS node to turn on for a limited period to determine if the intruder is a human or an animal by means of facial recognition. Upon confirming that it is a human being detected, the camera captures the facial images of the human intruder(s) and transmits them to the C2 Application Server for image analysis and identification.

a. Housing

Two versions of housing design, as illustrated in Figure 4, were proposed for the two main variants of the WGS node. Both housing designs are based on a garden solar light design which is inspired by UGS developed by various companies, including DARPA (DARPA, 2013), PDP Projects Ltd (PDP Projects, 2015) and Exensor Technology AB (Exensor, n.d.). For our housing design, the camera, PIR sensor, core processing hardware (i.e., Raspberry Pi 3 Model B) and battery pack are all mounted on a normal garden solar light stand. Both housing designs can be extended to about 1.7 meters in height using a garden pole or an extendable pole, as illustrated in Figure 5, making it suitable for the WGS node to capture any human facial images at the average human-height eye level.

Housing design 1 is designed for the Variant A of WGS node that utilizes two or more USB web cameras (webcams) and PIR sensors to support a wider detection angle. For this design, the USB webcams are mounted on the top of the garden solar light while the PIR sensors, battery pack and the Raspberry Pi 3 hardware are mounted on the pole of the garden solar light.

Housing design 2 is designed for the Variant B of WGS node that utilizes a single IR-Cut Pi Camera and PIR sensor for intrusion detection. For this design, the battery pack and the Raspberry Pi 3 hardware are mounted on the top of the garden solar light. The IR-Cut Pi Camera and the PIR sensor are mounted on the back of the battery bank and Raspberry Pi 3 enclosure, respectively.

Figure 4. Variant A of WGS Node (left) and Variant B of WGS Node (right)

Housing design 2 offers greater flexibility in the deployment of Variant B WGS nodes within the operating base perimeter. These nodes, built in accordance with Housing design 2, can be deployed in three different modes, as shown in Table 1.

Table 1. Variant B WGS Node Deployment Mode

Deployment Mode:	**Deployment Location:**
On the Ground • Just the top of the Solar Garden light is deployed (see left of Figure 5)	Deployed at the ***innermost protection layer*** as intruder tends to approach in squat, prone or crawl position at that close standoff distance.
On the Solar Garden Light • The whole Solar Garden Light is deployed (see right of Figure 4)	Deployed at the ***middle protection layer*** as intruder tends to approach in tactical high alert movement position as they get closer to the operating base area.
On the Garden/Extendable Pole • The whole Solar Garden Light is deployed on a garden/extendable pole (see right of Figure 5)	Deployed at the ***outermost protection layer*** as intruder tends to approach in normal walking posture at that standoff distance.

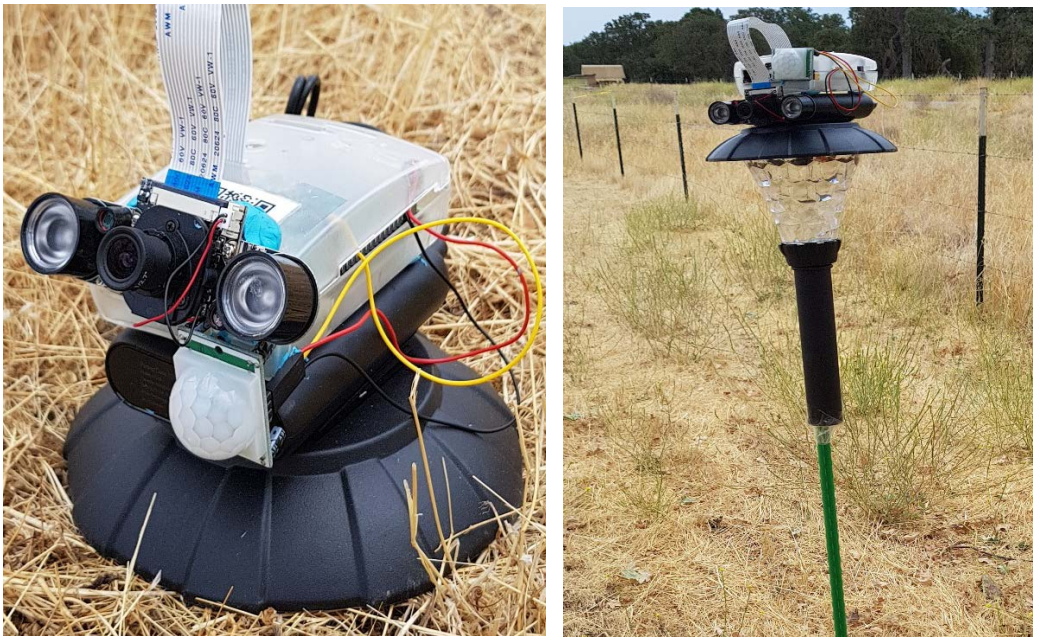


Figure 5. WGS Node Deployed on the Ground (left) and WGS Node Deployed on Garden/Extendable Pole (right)

b. Core Hardware and Operating System

The core processing hardware of the WGS node is a Raspberry Pi 3 Model B (see Figure 6), which consists of Quad Core 1.2GHz processor, 1GB RAM, on-board wireless

LAN (802.11n) and Low Energy Bluetooth, 4 x USB 2.0 ports, 40-pin extended General Purpose Input Output (GPIO) pins and Micro SD port for storing the operating system, application and data (Raspberry Pi, n.d.)

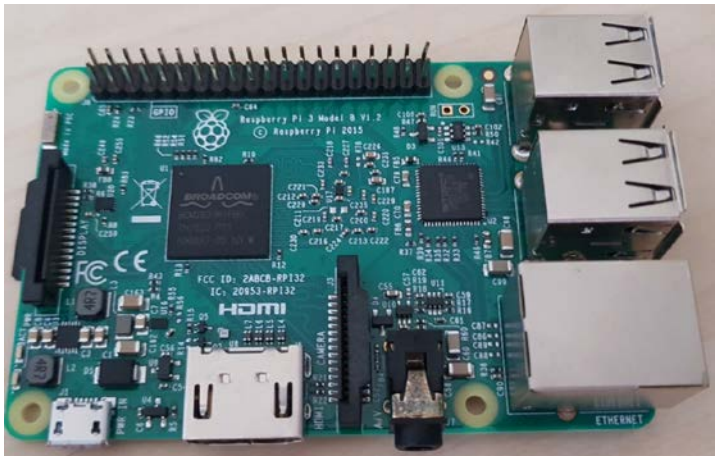


Figure 6. Raspberry Pi 3 Model B Board

The operating system installed on the 16GB MicroSD card within the Raspberry Pi 3 Model B is Raspberry Pi's official operating system, Raspbian Jessie (Version November 2016). The Raspberry Pi 3 core hardware together, with Raspbian Jessie operating system, supports a wide range of USB devices, such as USB webcams, and Raspberry Pi specific peripherals such as PIR sensors and Pi Camera, that can be connected to its USB ports, GPIO pins and Pi Camera interface, respectively.

c. Wireless Communication Protocol

The wireless communication protocol between the WGS node and the WiFi router is based on the IEEE 802.11n WiFi standard operating over the 2.4GHz frequency band. This WiFi standard and frequency band were chosen as it is the only WiFi standard and band supported by the onboard WiFi chip on the Raspberry Pi 3 Model B.

d. Sensors and Cameras

Variant A of the WGS node consists of two USB webcams and two PIR sensors, being designated as the left channel and right channel of the WGS node. The PIR sensors

and USB webcams have been carefully placed on the WGS node to provide a combined motion detection cone angle of up to 220 degrees using both PIR sensors; and intruder image detection and capturing of up to 120 degrees using both webcams. Figure 7 shows the motion detection and image capturing angle and range for Variant A of the WGS node.

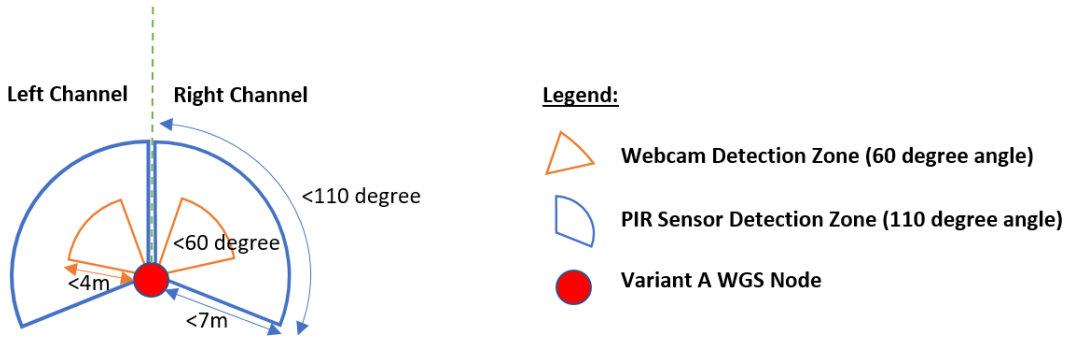


Figure 7. Motion Detection and Image Capturing Angle and Range for Variant A of the WGS Node

Variant B WGS node consists of an IR-Cut Infra-red Pi Camera and a PIR sensor which is designated as the main channel of the WGS node. The PIR sensor and IR-Cut Pi Camera are carefully placed on the front of WGS node to provide a motion detection cone angle of up to 110 degrees and intruder image detection and capturing of up to 70 degrees, respectively as illustrated in Figure 8.

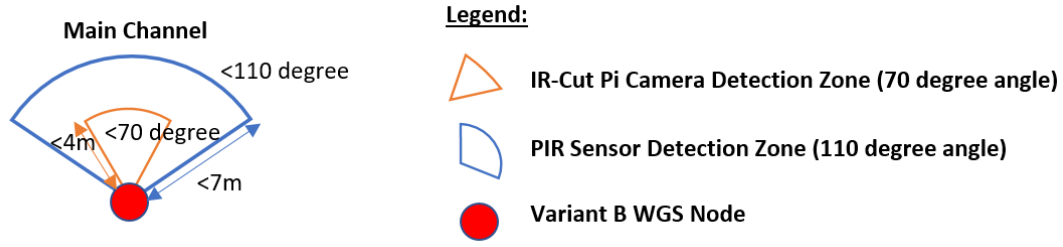


Figure 8. Motion Detection and Image Capturing Angle and Range for Variant B of the WGS Node

The PIR sensor is responsible for providing early intrusion alerts, as it has a wider and longer detection range as compared to an ultrasonic sensor or an active IR sensor, which typically have a detection range of less than tens of centimeters. Once the PIR sensor detects any motion, the webcam or IR-Cut Pi Camera will be turned on to visually detect and identify the warm body object as a human subject before attempting to capture the facial image of the human intruder.

The low-cost PIR sensor chosen for the wireless ground sensor node is HC-SR501 (Marlin P. Jones & Assoc. Inc., n.d.), as shown in Figure 9. It has a detection cone angle of up to 110 degrees and range of up to 7 meters. The PIR sensor detection capability is affected by the sensitivity adjustment knob settings, the size and thermal radiating property of the warm body object and environmental conditions like ambient temperature and brightness. While there are other long-range sensors like Garmin LIDAR-Lite 3, which has a detection range of up to 40 meters (RobotShop, n.d.); however, the cost of such sensors is higher than that of the PIR sensor used for this implementation.

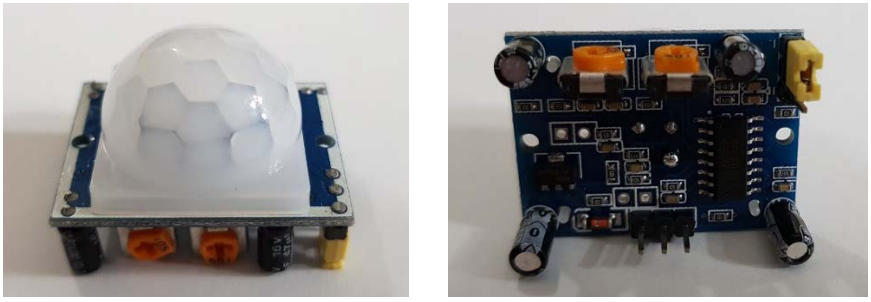


Figure 9. HC-SR501 PIR Sensor Top and Bottom View

The USB webcam chosen for Variant A of the WGS node is the Logitech C270 webcam (Logitech, n.d.), which supports video capture resolutions at standard definition (4:3) of 320 x 240, 640 x 480, 800 x 600 and wide-screen definition (16:9) of 360p (640x360), 480p (854x480) and 720p (1280x720), with a field of view of about 60 degrees. Figure 10 shows the Logitech C270 USB webcam.

Figure 10. Logitech C270 USB Webcam

The IR-Cut Pi Camera chosen for Variant B of the WGS node is the Waveshare RPi IR-Cut camera (Waveshare, n.d.), which supports adjustable focus lens and Infra-red night vision capability using a pair of IR transmitters. The camera is capable of capturing video at up to 1080p (1920x1080) resolution with a field of view of 75.7 degrees. Figure 11 shows the Waveshare RPi IR-Cut camera that is adapted for Variant B of the WGS node.

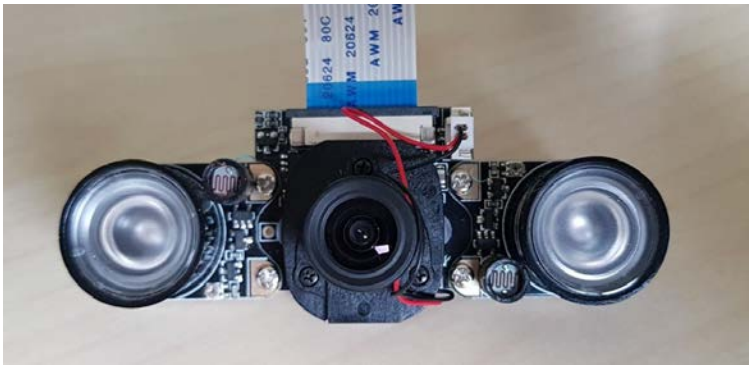


Figure 11. Waveshare RPi IR-Cut Pi Camera

Both the USB webcam and IR-Cut Pi Camera are configured to perform video surveillance upon detection of any motion by the PIR sensor. The camera works with the OpenCV library to perform real time image analysis and human facial detection. The Python-based OpenCV library (OpenCV, n.d.) was installed on the WGS node and the library is used to detect and capture any human facial image at the default video

resolution of 858 x 480 (480p). The default video resolution can be easily changed remotely by the operator of the WGSN at any time. Figure 12 illustrates the human facial image detection and capturing capability of the low-cost WGS node using either the Logitech C270 webcam or the IR-Cut Pi Camera with the OpenCV human front-facial detection Haar feature-based Cascade classifier.

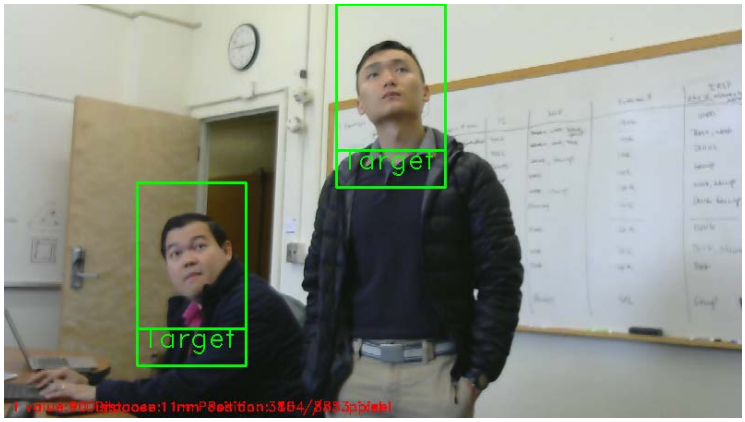


Figure 12. Real-Time Human Facial Image Detection on WGS Node

Once the facial image of the intruder has been detected and captured by the WGS node, the image and information of the intrusion, including identity of the WGS node that detected the intrusion, the date and time of the detected intrusion and the estimated distance of the intruder from the WGS node will be transmitted wirelessly to the C2 Application Server for further processing. A crop-out facial image of each of the intruders detected within the image and a high-resolution image of the intruders will also be captured and stored locally on the WGS node.

e. Power Consumption

The WGS nodes are powered by an Anker PowerCore 10000, as shown in Figure 13, which is a single USB port 10,000mAH standard battery pack that is capable of supplying 5V Direct Current (DC) and up to 2A current to the Raspberry Pi 3 Model B board. All PIR sensors, USB webcams, and IR-Cut Pi Camera are powered directly through the Raspberry Pi 3 Model B board's GPIO, USB and Pi camera interfaces, respectively.

Figure 13. Anker PowerCore 10,000mAH Single USB Port Battery Pack

Depending on the WGS node's state of operation, the power consumption will differ. The average power consumption for Variant A and Variant B of WGS node at the different stages of operations are as depicted in Table 2 and Table 3, respectively.

Table 2. Power Consumption for Variant A of WGS Node

Operating State	**Description**	**Power Consumption (Watt)**
A1	Only the Raspberry Pi 3 board is powered up.	1.4
A2	Left and right channel PIR sensor continuously performing intrusion detection.	1.6
A3	One of the channel webcam is turned on and is performing facial image detection and capturing.	3
	Both left and right channel webcam are turned on and are performing facial image detection and capture.	4.5
A4	One of the channel webcams has captured the intruder facial image and is transmitting the image file to the C2 Application Server and database.	3.25
	Both left and right channel webcam have captured the intruder facial image and are transmitting the image file to the C2 Application Server and database.	5
Estimated Runtime based on 10,000 mAH Battery Pack		**Minimum: 10 hours Maximum: 31 hours**

Table 3. Power Consumption for Variant B of WGS Node

Operating State	**Description**	**Power Consumption (Watt)**
B1	Raspberry Pi 3 board is powered up and in idle state	1.4
B2	PIR sensor is powered up and performing continuous intrusion detection	1.5
B3	IR-Cut Pi Camera is turned on and is performing facial image detection and capturing.	2.5
B4	The WGS node has captured the intruder facial image and is transmitting the image file and intrusion information to the C2 Application Server	2.75
Estimated Runtime based on 10,000 mAH Battery Pack		**Minimum: 18 hours Maximum: 33 hours**

After the WGS node has been deployed along the operating base perimeter, the WGS node will be in "*Operating State A1 or B1*." Once the intrusion detection algorithm has been initialized and is running on the Raspberry Pi 3 core processing hardware, the WGS node will transit to "*Operating State A2 or B2*" where all channel PIR sensors will be turned on continuously to detect any motion within the detection range of the WGS node.

When motion is detected by any channel of the PIR sensors, the corresponding channel's webcam or IR-Cut Pi Camera will be turned on to perform facial image detection and capturing, which can happen as fast as within 2 seconds. Now, the WGS node will transit to "*Operating State A3 or B3*." Once the intruder facial image has been successfully detected and captured by the WGS node, the image and intruder information will be transmitted over the wireless network to the C2 Application Server. At this point, the WGS node would have transited to "*Operating State A4 or B4*." Figure 14 illustrates the operating flow chart for the WGS node.

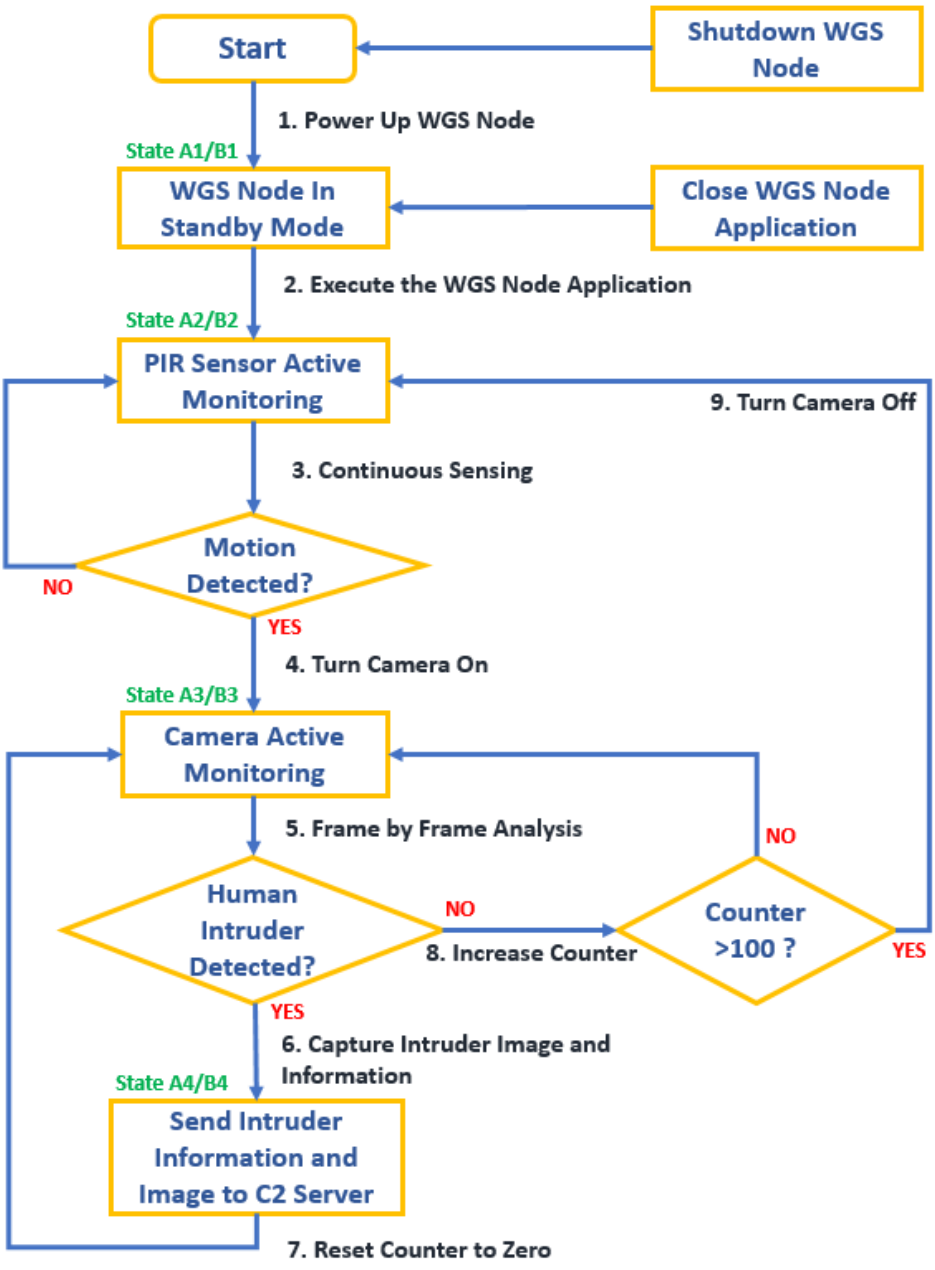


Figure 14. Operating Flow Chart for WGS Node

To reduce power consumption of the WGS node, the respective channel's webcam or IR-Cut Pi Camera is designed to only be turned on after motion has been detected by the respective channel's PIR sensor. After about two minutes where no human subject is being detected by the camera, the webcam or IR-Cut Pi Camera will be automatically turned off. The WGS node is also designed to minimise data transmission

on the wireless connection to reduce power consumption. The node will only transmit information through the wireless connection when it needs to transmit the intruder image and information that has been captured to the C2 Application Server.

f. Intrusion Detection Software

The intrusion detection software, which is running on the Raspberry Pi 3's Raspbian operating system, was developed using Python programming language. The intrusion detection software includes OpenCV image detection and facial image recognition library, the network socket programming library, the Raspberry GPIO library and MySQL database programming library. Once the intrusion detection software has been launched by the startup script on the WGS node, all the PIR sensors will be turned on.

After a motion has been detected by the respective channel's PIR sensor, the respective channel's webcam or IR-Cut Pi Camera will be turned on and the video stream will be shown within the Intrusion Detection Software. Figure 15 illustrates the real-time video streams within the Intrusion detection software.

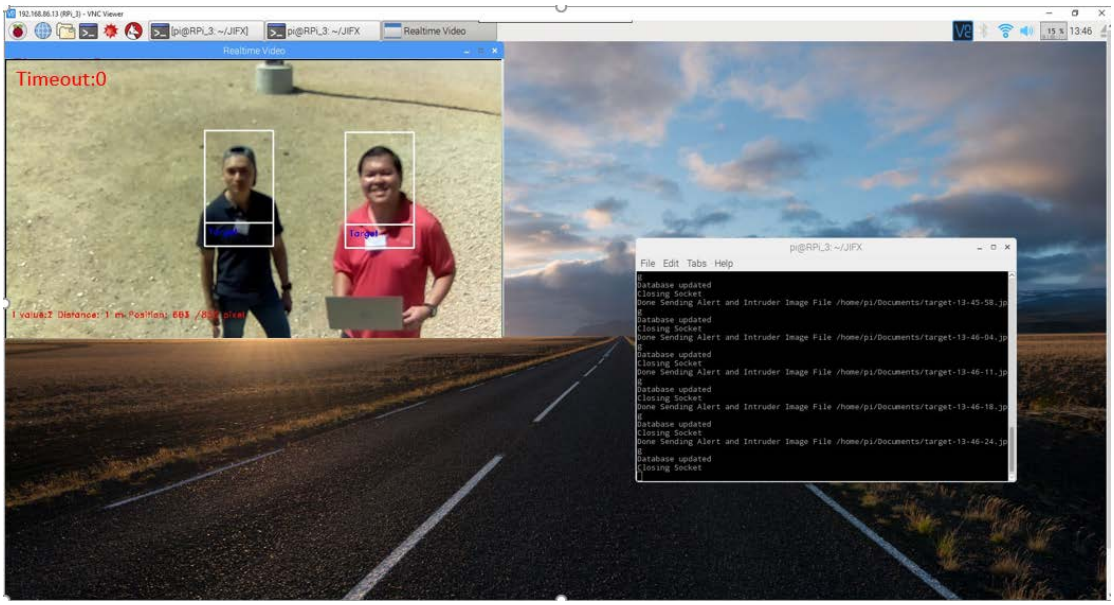


Figure 15. Real-Time Video Stream within the Intrusion Detection Software

The intrusion detection software has been designed to turn off the respective channel's camera when no human subject has been detected continuously for a period of about two minutes. The counter found on the top left-hand corner of the video streams will count to a value of 100 if no human subject is detected and the camera will be turned off after that. Every time a human subject is detected, the counter value will be reset to zero.

Upon detection of any facial image within the video stream, the software will draw a frame around each of the detected facial images, as shown in Figure 15. The software will provide an approximate distance to the intruder from the WGS node. In the background, the software will start sending the captured image of the intruders, including information with regards to the intrusion, to the C2 Application Server.

The intrusion detection software also supports several remotely-activated capabilities, like device wipe, video resolution change, shutting down of WGS nodes, requesting higher resolution image and creation of target watchlist.

g. MySQL Database

To implement the different advanced functionalities, such as target watch-list, target correlation, history of intruder movement through the operating base perimeter and capabilities, such as remote video resolution change and remote-request for higher resolution image of specific intruder images, MySQL database was installed on each of the WGS nodes. The Intrusion Detection Software, which utilizes the MySQL database software library, can perform a database query, insertion, deletion and modification using SQL statement directly. Figure 16 shows the version of MySQL database installed on the WGS node and the various database tables used to track the video resolution and intrusion history on the respective WGS node.

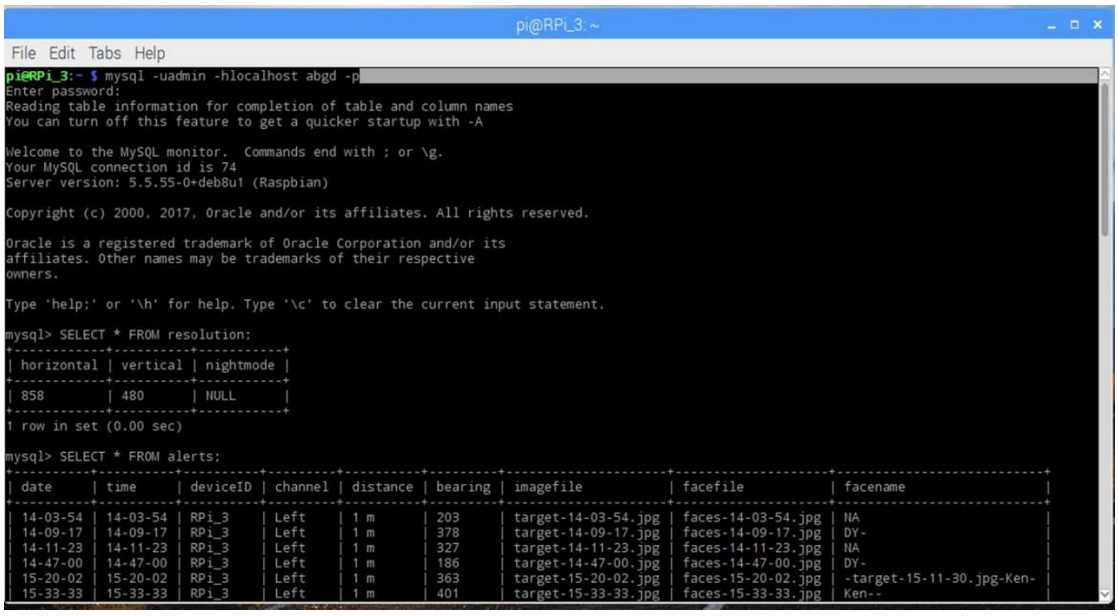


Figure 16. MySQL Database on WGS Node

2. WGS Node Deployment Tool

To obtain the accurate GPS location of the respective WGS node and to reduce the cost of each WGS node, the concept of using a WGS Node Deployment Tool, based on a Microsoft Windows 10 tablet computer, to deploy and commission the WGS nodes has been developed. This concept leverages the fact that WGS nodes will remain static at the same deployed location throughout the whole operating duration. This important fact eliminates the need to have a separate GPS module for each WGS node which lowers the cost of each WGS node. Further, it reduces energy consumption by the node.

As a part of the initial WGS node deployment around the tactical operating base perimeter, the deployment team plans and deploys each WGS node at a strategic location in accordance with the operating base environment. For WGS node deployment and commissioning process, the team powers up the WGS node and utilizes the WGS Node Deployment Tool to capture the WGS node's identity, Internet Protocol (IP) address, GPS location and approximate orientation of each WGS node using externally connected USB GPS receiver and USB 9-axis Accelerometer and Gyroscope. To facilitate fast deployment of many WGS Nodes with minimal data entry for the deployment team, the identity and IP address information for each WGS node has been encoded into a QR code

that is affixed on top of every WGS node. The QR code can be easily read by the WGS Node Deployment Tool's on-board rear camera. Figure 17 shows the QR code that is affixed on the top of a WGS node.

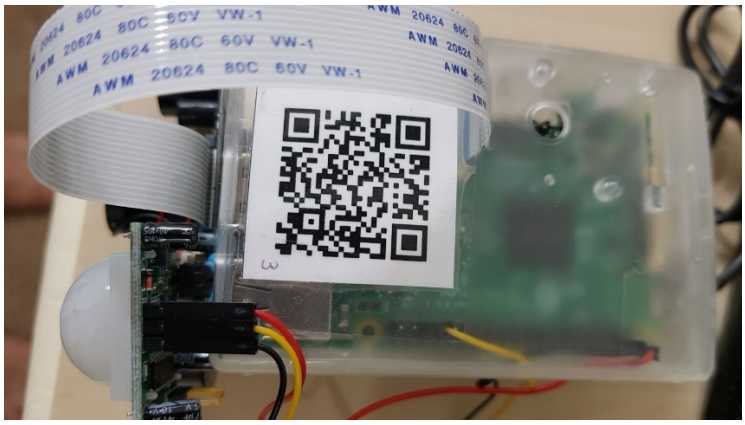


Figure 17. QR Code Affixed on the Top of Each WGS Node

a. Core Hardware and Operating System

The WGS Node Deployment Tool was developed on a Microsoft Surface Pro 4 touchscreen tablet with Intel Core m3 processor, 4GB RAM, 128GB hard disk and the Microsoft Windows 10 (64-bit) operating system. A touchscreen tablet was selected to facilitate easy data entry and usage on the move. Figure 18 shows the WGS Node Deployment Tool that was developed for the Microsoft Surface Pro 4.

Figure 18. WGS Node Deployment Tool Application

b. Sensors and Cameras

The WGS Node Deployment Tool is equipped with an external USB GPS receiver to acquire the accurate GPS location of each WGS node. The GlobalSat BU-353S4 USB GPS receiver (GlobalSat, n.d.) is based on SiRF STAR IV GSD4e chipset, which has a position accuracy of about 2.5 meters and can acquire a GPS satellite fix in 35 seconds on a cold start and eight seconds on a hot start. Figure 19 shows the GlobalSat BU-353S4 USB GPS receiver that has been adopted for the WGS Node Deployment Tool.

Figure 19. GlobalSat BU-353S4 USB GPS Receiver

To acquire the orientation of the WGS node, the WGS Node Deployment Tool leverages an externally-connected USB 9-Axis Accelerometer and Gyroscope. The WIT-motion JY901 9-Axis Accelerometer and Gyroscope (Amazon, n.d.) can provide a real-time measurement of 3-axis acceleration, 3-axis angular velocity and 3-axis magnetometer, which are processed through an onboard Kalman Filter. The WGS Node Deployment Tool captures the real-time Yaw reading of the 9-axis Accelerometer and Gyroscope to determine the approximate orientation of the WGS node. Figure 20 shows the WIT-Motion JY901 9-Axis Accelerometer and Gyroscope.

Figure 20. WIT-Motion JY901 9-Axis Accelerometer and Gyroscope

To facilitate fast and easy deployment of WGS node, the 8-megapixel rear facing camera, with autofocus function, onboard the WGS Node Deployment Tool is used to scan the quick response (QR) code affixed on top of each WGS node to retrieve essential information like the WGS node's identity and its IP address. The QR code enables the WGS Node Deployment Tool to capture the node's information in less than a second by just scanning the QR code.

c. Mobile Deployment Tool Application

The WGS Node Deployment Tool application is a Graphical User Interface (GUI) Microsoft Windows based application developed using the Microsoft C# .Net programming language. The application is designed for the Microsoft Windows 10 operating system and can be deployed on any Microsoft Windows 10 based laptop, desktop, and tablet. An overview of the WGS Node Deployment Tool Application can be found in Figure 18.

The application interfaces with the GlobalSat BU-353S4 USB GPS receiver and WIT-motion JY901 9-Axis Accelerometer and Gyroscope through the serial communication (COM) port. The COM port settings for both GlobalSat BU-353S4 USB GPS receiver and WIT-motion JY901 9-Axis Accelerometer and Gyroscope are as shown in Table 4.

Table 4. COM Port Settings for Externally Connected Sensors on WGS Node Deployment Tool

COM Port Parameters	**GlobalSat BU-353S4 USB GPS Receiver**	**WIT-motion JY901 9-Axis Accelerometer and Gyroscope**
Baud Rate (bps)	4800	115200
Data Bits	8	8
Stop Bit	1	1
Parity Bit	None	None
Flow Control	None	None

The WGS Node Deployment Tool application also incorporates the QR code scanning library function to decipher the QR code and Transmission Control Protocol (TCP) socket programming library function to send all the gathered WGS node deployment information to the C2 Application Server wirelessly using its onboard IEEE 802.11a/b/g/n/ac capable WiFi adapter, which can operate on both 2.4GHz and 5GHz band.

3. C2 Application Server and Database

The following section describes the C2 Application Server as well as the database design for the system. The C2 Application Server and database form the centralized infrastructure to which all WGS nodes send intrusion related information. All intrusion related information and images are processed, stored and analyzed on the C2 Application Server and database.

a. C2 Application Server

The C2 Application Server for the WGSN is hosted on a Dell XPS-13 laptop with 6th generation Intel Core i5 processor clocked at 2.3GHz, 8GB RAM, 500GB Solid State Disk (SSD) and Microsoft Windows 10 (64-bit). It has an onboard WiFi adapter supporting IEEE 802.11a/b/g/n/ac standards on both 2.4GHz and 5GHz band. Figure 21 shows the Dell XPS-13 laptop-based C2 Application Server. For a large-scale deployment, supporting many more nodes, this server should be run on a more substantial platform or in a cloud where computing and network resources can be scaled on demand.

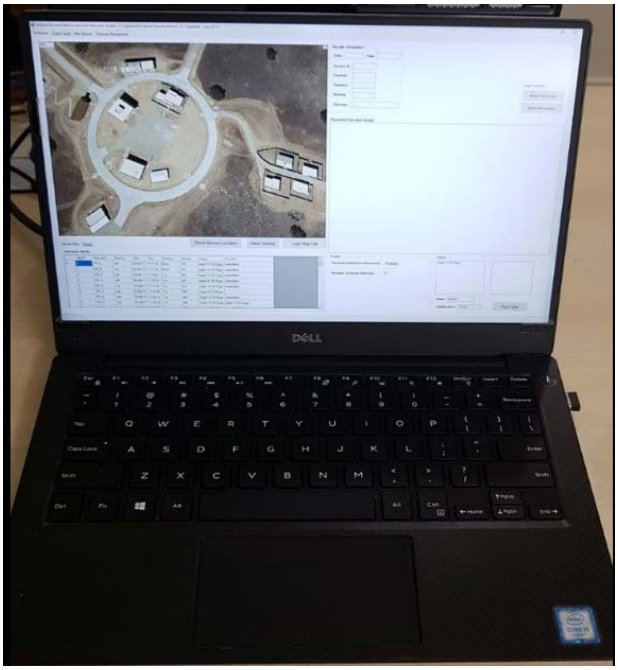


Figure 21. C2 Application Server Running on a Dell XPS-13 Laptop

b. SQL Database

The SQL database running on the C2 Application Server is an installation of Microsoft SQL Server Express 2016, which is a publicly available free entry-level version of SQL Server database for creating small and simple databases to support simple web applications. Figure 22 shows the Microsoft SQL Server Management Studio software that is used to manage the Microsoft SQL Server Express 2016 database on the C2 Application Server.

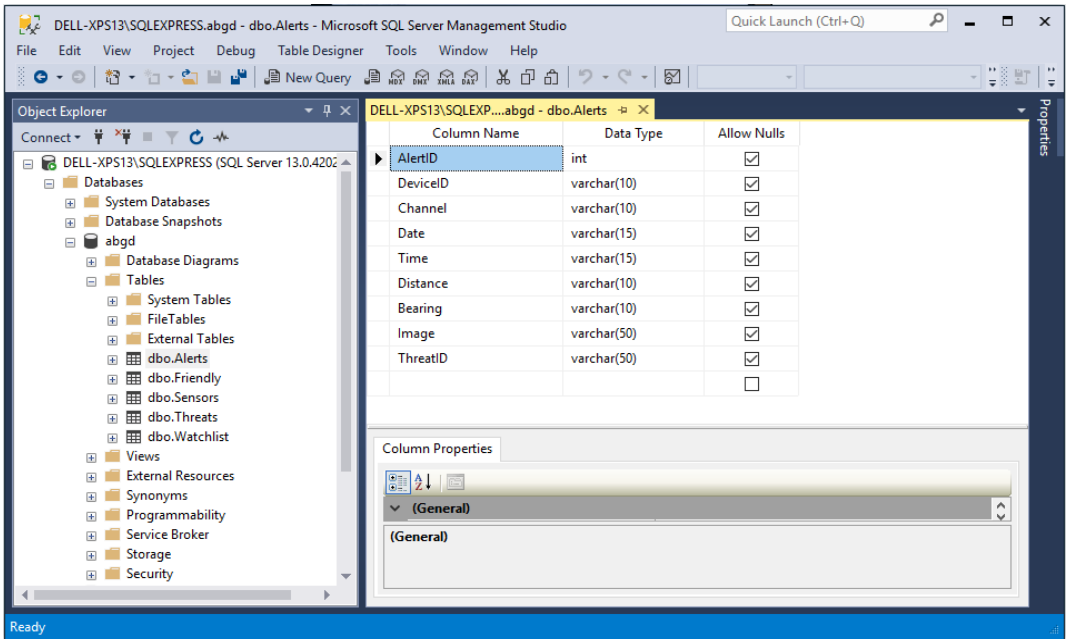


Figure 22. Microsoft SQL Server Express 2016 Database on C2 Application Server

A total of 5 different database tables, named “Sensors,” “Alerts,” “Threats,” “Watchlist” and “Friendly,” were created to store the WGS node information, intruder alert information, correlated threats information, intruder watch-list information and friendly forces information, respectively. Figure 23 shows the schema of the five database tables used by the C2 Application Server to store all essential information in a structured manner to facilitate search, data correlation, and analytics.

"Alerts" Table Schema

Name	Data Type
AlertID	int
DeviceID	varchar(10)
Channel	varchar(10)
Date	varchar(15)
Time	varchar(15)
Distance	varchar(10)
Bearing	varchar(10)
Image	varchar(50)
ThreatID	varchar(50)

"Threats" Table Schema

Name	Data Type
ThreatID	varchar(50)
ThreatName	varchar(50)
Occurrance	int

"Watchlist" Table Schema

Name	Data Type
WatchlistID	varchar(50)
IntruderName	varchar(50)

"Sensors" Table Schema

Name	Data Type
DeviceID	varchar(10)
IP	varchar(15)
Longitude	varchar(15)
Latitude	varchar(15)
Bearing	varchar(10)
Status	varchar(10)

"Friendly" Table Schema

Name	Data Type
Identity	varchar(50)

Figure 23. Schema of Database Tables Used to Store Essential Information on the C2 Application Server

c. WGSN Command and Control Application

The WGSN Command and Control Application running on the C2 Application Server was also developed in-house using the Microsoft C# .Net programming language. The WGSN Command and Control Application provides C2 and intelligence of the whole WGSN, which performs threat-correlation as well as image analytics and facial recognition. The application incorporates a dashboard that provides the operator with all the essential information pertaining to any detected intrusion events. Figure 24 shows the Dashboard view of the WGSN C2 application.

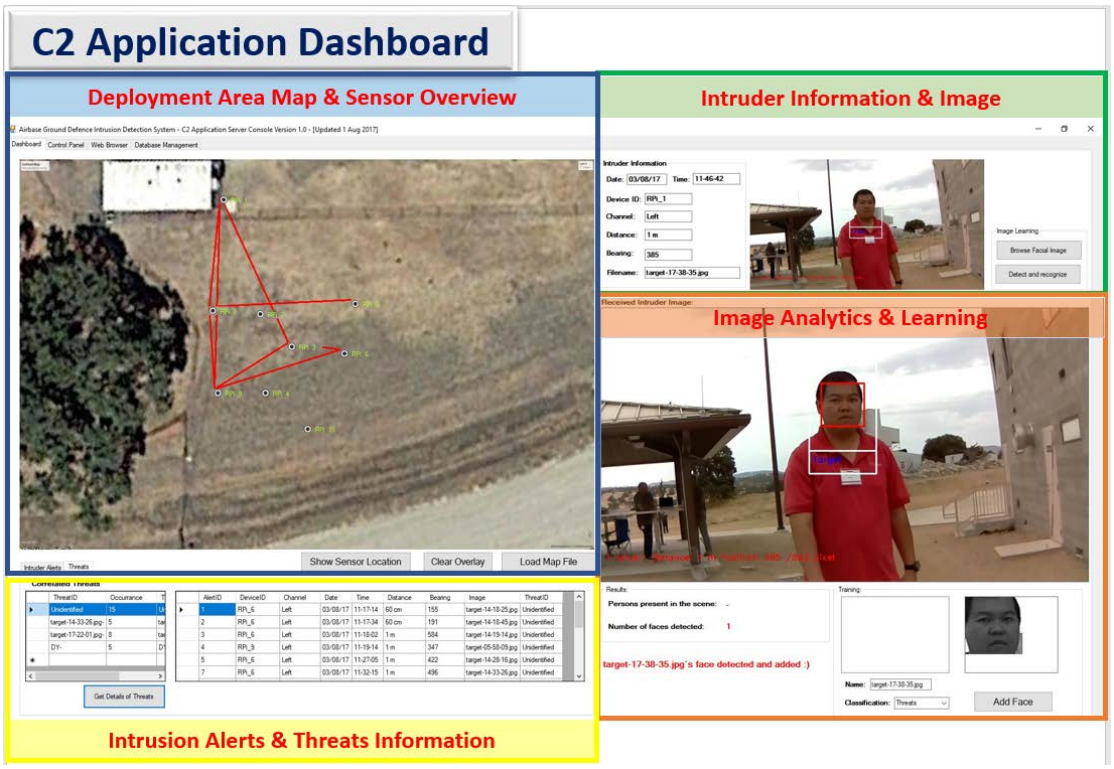


Figure 24. Dashboard View of WGSN C2 Application

The top left of the Dashboard view provides the operator with a satellite view or map view of the operating base perimeter, the location of the various WGS nodes (as marked with a black dot with green colour wording) and the intruder movement path (as marked with red colour lines) within the operating base perimeter. The bottom left of the Dashboard view provides the operator with real-time intrusion alerts and correlated threat information. The top right of the Dashboard view presents the captured image of the intruder, as well as essential information pertaining to that intrusion, for the most recently detected intrusion. The bottom right of the Dashboard presents the operator with an overview of the automatic image analysis, intruder identification, and facial image learning that is triggered every time a new image of the intruder is received by the C2 Application Server. The image analysis engine puts the image of the intruder through 3 different Haar feature-based Cascade classifier. The aim is to detect any other human intruder not picked up by the WGS node and to further improve the detection by looking for facial features like the eyes and side profile of the face. Figure 25 illustrates how the

image analysis engine on the WGSN C2 Application can identify another human intruder within that image who may be in the background of the image and not picked up by the WGS node, as well as identify additional features like eyes to improve the detection.

Figure 25. Image Analysis Engine with 3 Haar Feature-Based Cascade Classifier on WGSN C2 Application

After the image analysis has been completed, the intruder image is processed by a facial recognition algorithm to determine if the facial image of the human intruders matches any of the previous facial images stored in the database. If a match is found, the threats identifier (i.e., Threat ID) of the intruder is updated to be the same Threat ID of the previous intruder. If no match is found, a new intruder ID is created and the system learns the facial image of the intruder and adds the information to the facial image database. Once the same Threat ID appears more than three times, that is, the same intruder appears more than three times on different intrusion events, the intruder is automatically classified as a threat by the system and a record is created in the Threats database table. With that record, all intrusion events related to the intruder are presented and the movement path within the operating base perimeter is plotted when that threat is

selected from the list of all threats, which is found at the bottom right corner of the Dashboard view.

The WGSN currently supports several useful features that the operator can activate through the WGS Node Control Panel on the WGSN C2 Application. A list of currently supported features is shown in Table 5.

Table 5. Features Activated through the WGS Node Control

S/N	Features	Description
1	Enable Night Mode	Enable infra-red night photography mode for the IR-Cut Pi Camera on Variant B of the WGS node.
2	Wipe Nodes	Activate commands to remotely wipe off all the intruder images, program files and database on the WGS node during an emergency evacuation or when there is a need to restore the WGS node to pre-mission state.
3	Shutdown Nodes	Activate commands to remotely shut down the WGS node.
4	Change Resolution	Activate commands to change the video capturing resolution on the WGS node.
5	Send Watchlist	Send intruder watch-list information to the WGS node.
6	Request Higher Resolution Image	Send a request to retrieve the high-resolution image of the intruder from the WGS node should a higher-resolution image be required.

Figure 26 shows the WGS Node Control Panel of the WGSN C2 Application where the operator can send various control messages and commands to a selected list of WGS nodes. The operator can select the list of affected WGS nodes by first selecting the node from the list of all WGS nodes which is on the left and then adding it to the list of selected WGS nodes on the right. Once all the affected WGS nodes have been selected, the operator can then send the selected commands to the list of selected WGS nodes all at once.

The operator can retrieve the high-resolution image of an intruder from one of the WGS node by scrolling through the list of the file names for the intruder images stored on the C2 Application Server using the Intruder Image Control Panel of the WGSN C2 Application. As the operator scrolls through the list of the filenames for the intruder images, the corresponding image of the intruder is shown, together with the list of intrusion events where the intruder was detected previously. Figure 27 shows the Intruder Image Control Panel of the WGSN C2 application.

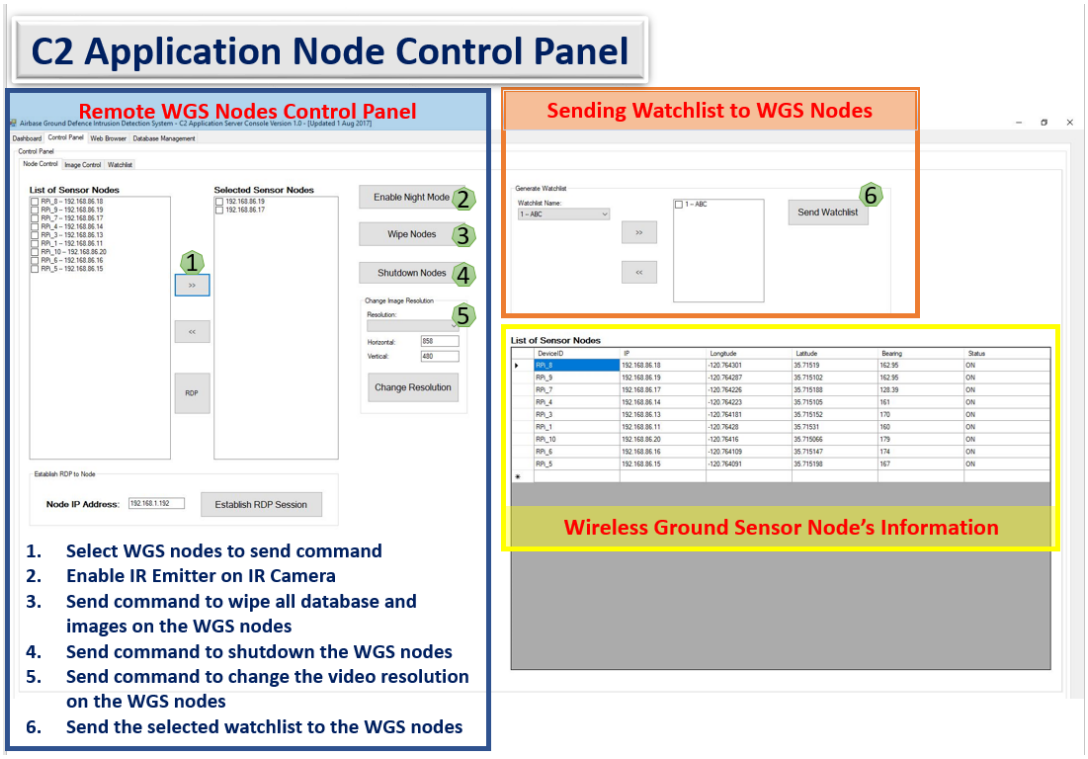


Figure 26. WGS Node Control Panel

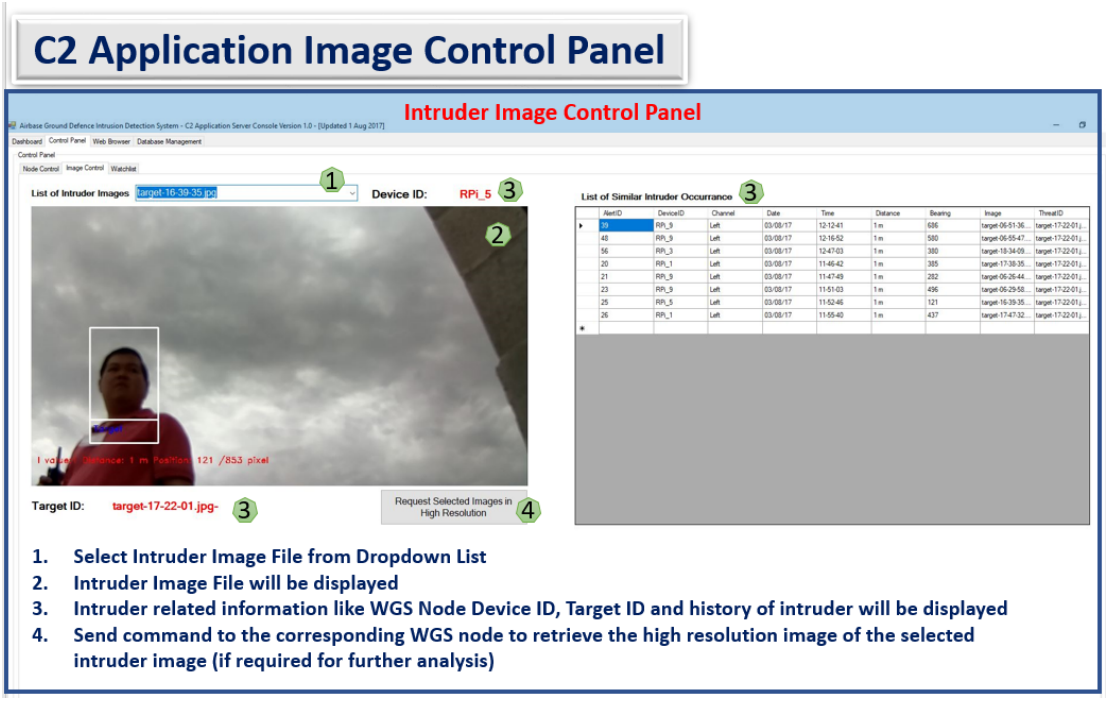


Figure 27. Intruder Image Control Panel

If a specific intruder is subsequently identified as the target of interest and the operator would like the WGSN C2 Application to generate an alarm when the target of interest is detected by any of the WGS nodes, the operator can set the specific intruder as a target of interest by creating a watchlist through the Intruder Watchlist Control Panel of the WGSN C2 Application. Figure 28 shows the Intruder Watchlist Control Panel of the WGSN C2 Application.

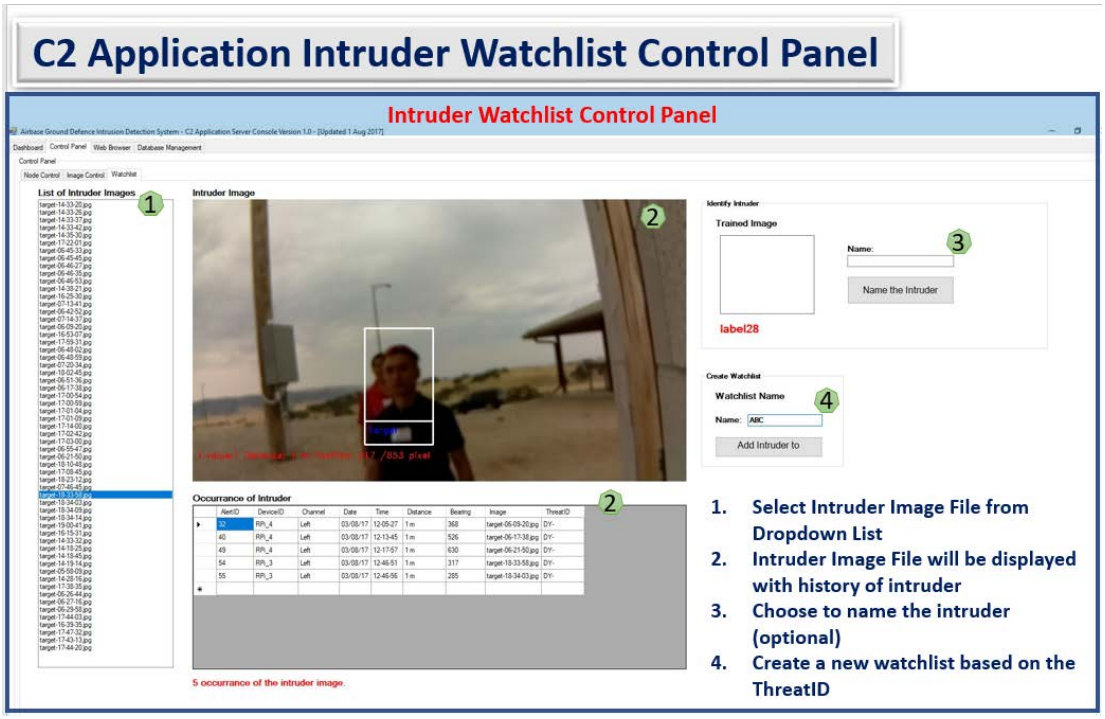


Figure 28. Intruder Watchlist Control Panel

To create a watchlist, the operator can identify the targets of interest by scrolling through the list of intruder images stored on the C2 Application Server and selecting desired images. This watchlist can be assigned a name for ease of identification. Once the watch-list has been created, the operator can now choose to send it to the WGS nodes through the WGS Node Control Panel using the same process as sending a remote wipe command to a list of selected WGS nodes.

B. WIRELESS NETWORK

The wireless network is a critical part of the WGSN. It is responsible for connecting all the WGS nodes, the WGS Node Deployment Tool and C2 Application Server together so that the various sub-systems can inter-communicate to provide the required early intruder detection capability in the tactical operating environment. The overall WGSN requires reliable data transmission to ensure that all threat information, alerts, commands and images are delivered without any errors to the desired recipient.

1. Communication Protocol

This section describes the various backend communication requirements to support the wireless sensor network. The design principles for the communication requirements are guided by the Transmission Control Protocol / Internet Protocol (TCP/IP) stack ranging from hardware to network, transport, layers and the application itself.

a. IEEE 802.11 Wireless Network

The WGSN is built on a Google WiFi router platform (Google, n.d.) that supports seamless formation and optimisation of a WiFi mesh network over a wide area using multiple Google WiFi routers. The Google WiFi, as shown in Figure 29, is a dual-band WiFi mesh router that supports transmission on both 2.4GHz and 5GHz bands concurrently. The AC-1200 router is capable of handling combined data throughput of up to 1.2 Gigabits per second (Gbps) over IEEE 802.11a/b/g/n/ac WiFi standard. The Google WiFi mesh router can be powered using a normal power pack such as used for the sensor nodes, which makes it suitable for deployment within the operating base perimeter.

Figure 29. Google WiFi Mesh Router Powered Using Battery Bank

The WGS nodes follow the IEEE 802.11n standard, operating on the 2.4GHz frequency band, to communicate with the Google WiFi mesh routers. This WiFi standard and frequency band were selected as the WGS node, which was built on the Raspberry Pi 3 Model B core hardware, can only support 802.11n on the 2.4GHz band, using Raspberry Pi 3 Model B's onboard WiFi chipset. For better WiFi range, performance and throughput on the WGS nodes, external USB WiFi adapter with a high-gain antenna can be added to each of the WGS nodes.

The WGS Node Deployment Tool and C2 Application Server support WiFi chipsets that can automatically select and switch among 802.11a/b/g/n/ac WiFi standards to achieve the most optimal WiFi performance.

b. Mesh Networking

To extend the WiFi coverage to the whole area of deployment without electrical power infrastructure, battery-powered COTS WiFi routers capable of mesh networking can be used. Currently, there are more than ten different vendors (such as Linksys, Netgear, TP-Link and Google) offering WiFi mesh network products. Figure 30 shows some of the more popular WiFi mesh network products.

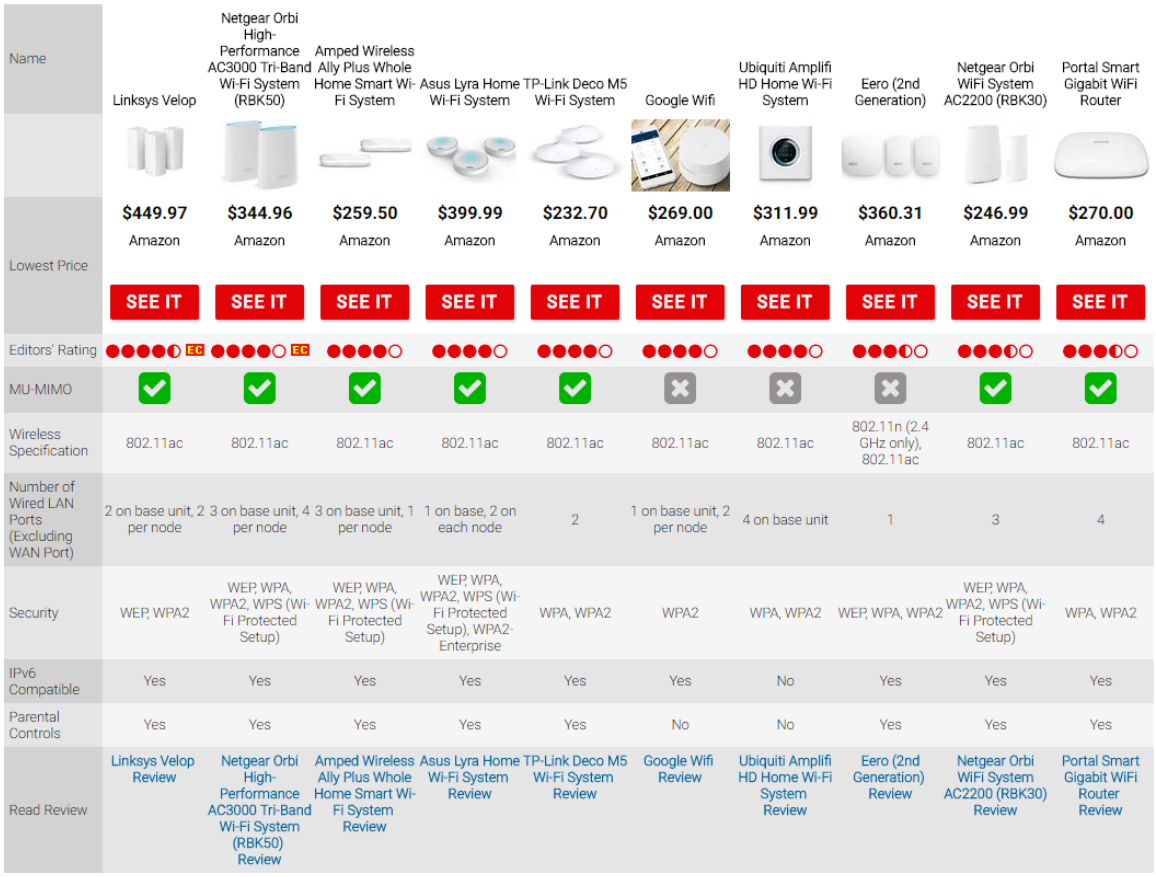


Figure 30. Comparison among Some of the Popular WiFi Mesh Network Products. Source: Delaney (2017a).

Among the 10 WiFi mesh network products featured in Figure 30, only a few can be battery powered using a USB Type-C interface. This includes Google WiFi, TP-Link Deco M5 WiFi System, Ubiquiti Amplifi HD Home WiFi System and second generation of Eero home WiFi system (Delaney, 2016a, 2016b, 2017b, 2017c). Google WiFi was selected as the WiFi mesh router for the WGSN as it is cost effective and can be USB powered. None of the remaining WiFi mesh router can be battery powered, so they are not be suitable for use within our operating base environment where there is no electrical power infrastructure.

c. TCP Transport Protocol

After establishing the IP layer network connectivity between all WGS nodes, WGS Node Deployment Tool and C2 Application Server, the next essential step is to define the transport protocol to be adopted. As the underlying network connectivity is based on a WiFi network, the reliability and performance of the data link can fluctuate with weather or environmental effects. To ensure all intruder alerts, intruder information, images, control messages, and commands are delivered without any errors, TCP was adopted as the transport layer protocol between WGS nodes, WGS Node Deployment Tool and the C2 Application Server. The TCP socket programming application programming interface (API) library in Python programming language and Microsoft C# .Net programming language were used to develop the application-level communications capability. A WGS Node establishes a TCP connection using a random TCP port number to the C2 Application Server that has multiple TCP listening threads waiting on TCP Port 9001 to accept multiple concurrent TCP connections from WGS nodes and the WGS Node Deployment Tool. The C2 Application Server is currently configured to accept up to 20 concurrent TCP connections and can be easily re-configured within the software to support a larger number of node connections when required. Figure 31 illustrates the TCP communication protocol adopted for the WGSN.

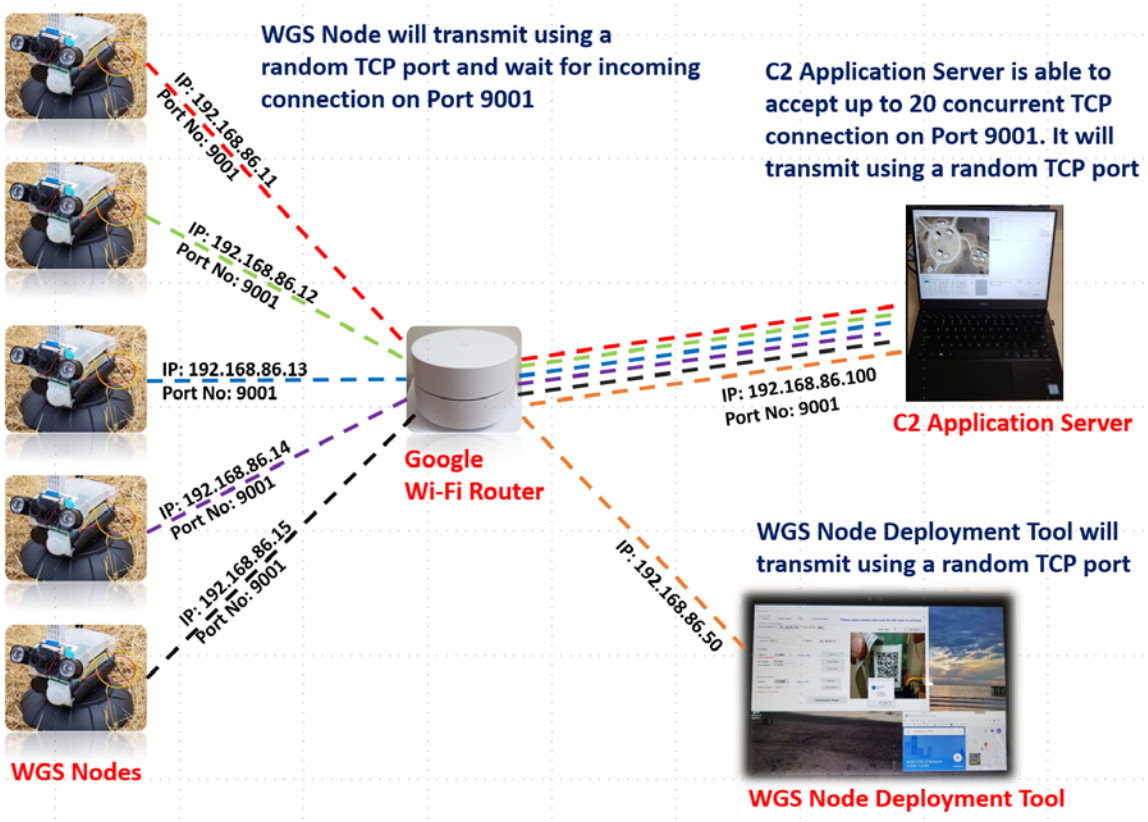


Figure 31. TCP Communication Protocol between WGS Nodes, WGS Node Deployment Tool, and C2 Application Server

The C2 Application Server sends control messages and commands to the various WGS nodes, each of which has a single listening thread on TCP port 9001 to receive the TCP message. The WGS Node Deployment Tool sends the WGS node information over to the C2 Application Server using a randomly selected TCP source port. The WGS Node Deployment Tool does not have a specific TCP listening port configured as it was designed to only send WGS node information to the C2 Application Server and will not be accepting any incoming TCP connection establishment request.

2. Message Protocol

The message protocol section details the message format between the WGS nodes and the C2 Application Server, as well as the WGS Node Deployment Tool. Message exchanges between the different devices are also illustrated in this section to provide a more in-depth understanding of the interactions between them.

a. WGS Node to C2 Application Server

The WGS node adopts the message protocol shown in Table 6 when sending intruder alerts and a high-resolution image of the intruder to the C2 Application Server using the TCP transport protocol.

Table 6. Message Protocol for Sending Information from WGS Node to C2 Application Server

S/N	Message Type (Command)	Message Parameters and Content	Functionality
1	Intruder Alerts (**Alerts**)	a) **Device ID** – ID of the WGS node b) **Channel** – Denote left or right camera channel of the WGS node. For WGS node with single camera channel, it will denote as the main channel. c) **Date and Time** of the intrusion event d) Approximate **distance and direction** of the intruder e) **Filename** of the intruder image file f) **Normal resolution JPEG image** file of the intruder	To send intruder information and intruder image captured by the WGS node to the C2 Application Server.
2	Higher Resolution Image File (**Image**)	a) **Filename** of the high-resolution intruder image file b) **High-resolution JPEG image** file of Intruder	To send the requested high-resolution JPEG image of the intruder image stored locally on the WGS node to the C2 Application Server.

b. C2 Application Server to WGS Node

The C2 Application Server adopts the message protocol shown in Table 7 when sending the various control messages and commands to the respective WGS nodes using the TCP transport protocol. The control messages and commands activate the functionalities on the WGS node.

Table 7. Message Protocol for Sending Information from C2 Application Server to WGS Node

S/N	Message Type (Command)	Message Parameters and Content	Functionality
1	Enable Night Mode on IR-Cut Pi Camera (**Night**)	a) **IP Address** of WGS Node	Enable infra-red night photography mode for the IR-Cut Pi Camera on Variant B of the WGS node.
2	Wipe Data and Image on WGS Node (**Wipe**)	a) **IP Address** of WGS Node	Activate commands to remotely wipe off all the intruder images, program files and database on the WGS node during an emergency evacuation or when there is a need to restore the WGS node to pre-mission state.
3	Shutdown WGS Node (**Shutdown**)	a) **IP Address** of WGS Node	Activate commands to remotely shut down the WGS node.
4	Change Video Resolution on WGS Node (**Resolution**)	a) **IP Address** of WGS Node b) **Horizontal resolution** in pixels c) **Vertical resolution** in pixels	Activate commands to change the video capturing resolution on the WGS node.
5	Send Watchlist to WGS Node (**Watchlist**)	a) **Watchlist name** b) **Intruder ID**	Send intruder watch-list information to the WGS node.
6	Request High-Resolution Image of Intruder (**Request**)	a) **Requested intruder image file name**	Send a request to retrieve the high-resolution image of the intruder from the WGS node should a higher-resolution image be required.
7	Send the identity of the intruder after it has been recognize by the C2 Application Server (**Response**)	a) **Alert ID** – The intruder alert ID created by the WGS node b) **Threat ID** – The identity of the intruder	Send the identity of the intruder after the C2 Application Server has detected and recognize the intruder based on the initial image of the intruder sent by the WGS node.

c. WGS Node Deployment Tool to C2 Application Server

The WGS Node Deployment Tool adopts the message protocol in Table 8 when sending the WGS node information to the C2 Application Server using the TCP transport protocol.

Table 8. Message Protocol for Sending Information from WGS Node Deployment Tool to C2 Application Server

S/N	Message Type (Command)	Message Parameters and Content	Functionality
1	WGS Node Information (**Nodes**)	a) **Device ID** – ID of the WGS node b) **IP Address** – IP address of the WGS node. c) **GPS Location** – GPS longitude and latitude information of the WGS node d) **Compass Bearing** – Orientation of the WGS node	To send WGS node information to the C2 Application Server.

3. Network Establishment

Deploying the WiFi network infrastructure and establishing network connectivity to all WGS nodes, the WGS Node Deployment Tool, and the C2 Application Server is essential for the proper operation of the WGSN within the operating base environment.

a. Configuring Mesh Network

The Google WiFi mesh router allows multiple Google WiFi mesh routers that are deployed at different location around the operating base perimeter to be meshed into a single wide area WiFi network to provide seamless connectivity to all the WGS nodes, the WGS Node Deployment Tool and the C2 Application Server. Before the start of the mission deployment, the operator needs to decide the number of Google WiFi mesh routers that will be needed to provide the required WiFi coverage across the whole operating base area. The operator also needs to decide the most optimal position at which to place each of the Google WiFi mesh routers to ensure that there is no WiFi dead zone

in places where there are WGS nodes deployed. Once the planning has been completed, the next step is to perform the one-time configuration on all Google WiFi mesh routers so that they are meshed together to form a wide area WiFi mesh network. Figure 32 illustrates the key steps to configure each of the Google WiFi mesh routers to be part of a mesh network using the Google WiFi application that is available on the Android Play store (for Android smartphones) or Apple Appstore (for iPhones):

1. Within the application, click on the ***Setting*** tab that is found on the top right-hand corner of the application to bring up the Setting page.
2. Under the Setting page, click on the ***Network & general*** button that is found under the Settings section of the page to bring up the Network & general page.
3. Under the Network & general page, click on the ***Wifi point*** button that is found under the Network section of the page to bring up the Wifi point configuration page.
4. Under the Wifi point configuration page, click on the ***ADD WIFI POINT*** button found at the bottom of the page.
5. Power up the next Google Wifi point and place it near the first Google Wifi point.
6. Upon detection by the new Google Wifi point by the first Google Wifi point, the new Google Wifi point will be automatically configured to join the mesh network.
7. Repeat step 5 and 6 to add more Google Wifi point to the same mesh network.

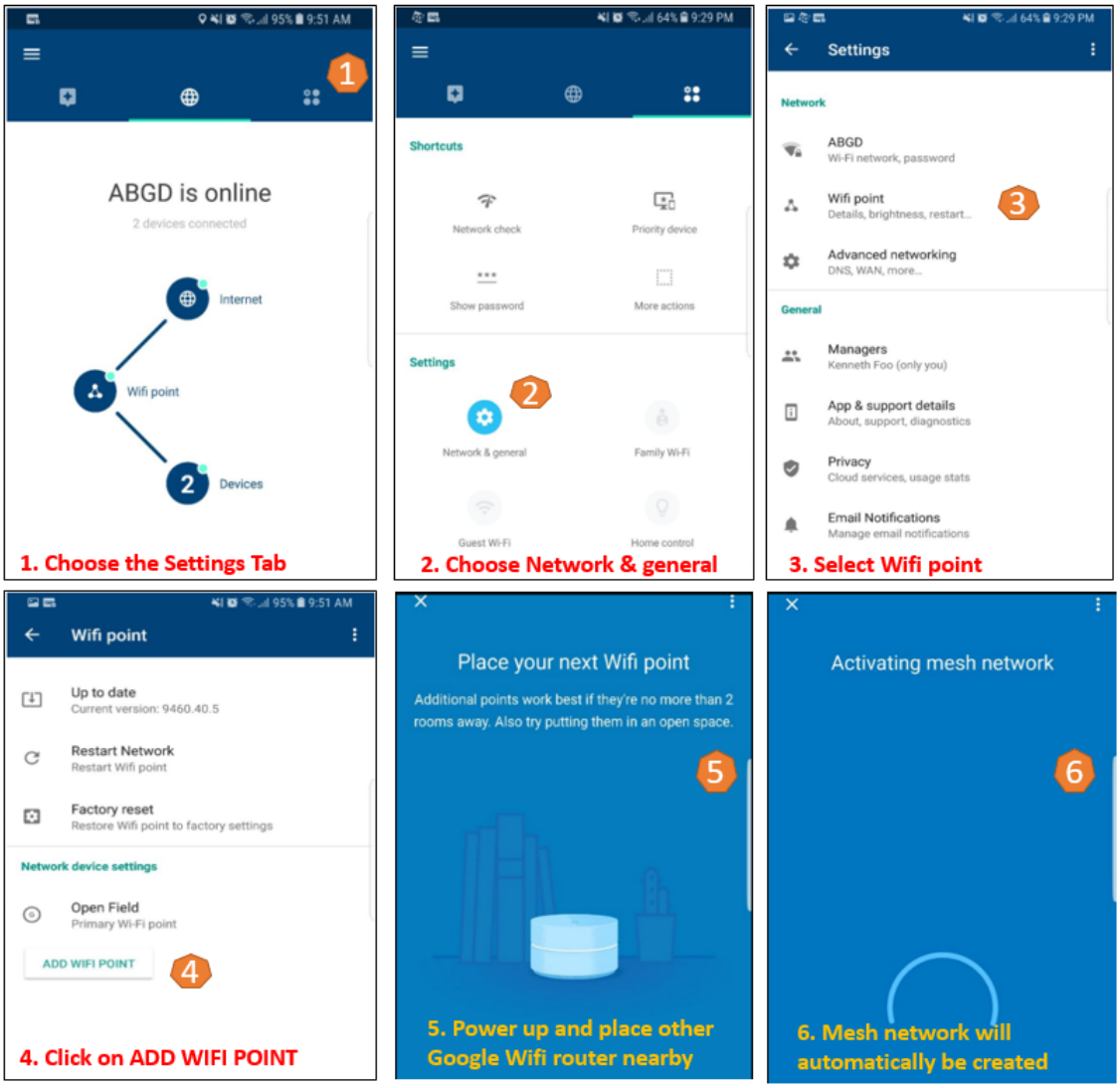


Figure 32. Key Steps to Configure Additional Google WiFi Mesh Routers to be Part of a Mesh Network Using Google WiFi Smartphone App

b. Security Settings on WiFi Network

Based on industrial security best practices for WiFi networks, there are a few security settings that can be configured on the WiFi router to minimise the risk of security compromise, information leakage and disruption of the WiFi network due to an unauthorized user or devices connecting to the WiFi network. The WGSN WiFi network has incorporated these security best practices to protect the WGSN from unauthorized access.

(1) Service Set Identifier (SSID)

The SSID of the WiFi network is not set to broadcast mode. This is to prevent non-malicious normal user with unauthorized devices from trying to connect to the network and at the same time conceal the existence of a WGSN WiFi network. All WGS nodes, WGS Node Deployment Tool and C2 Application Server are preconfigured with the corresponding SSID for a specific mission and these authorized devices are able to connect to the WGSN WiFi network even though the SSID is hidden.

(2) WPA2 Encryption

To protect all information that is transmitted wirelessly over the air from eavesdropping, the WPA2 encryption scheme is adopted to encrypt the WiFi channel between the end devices and the WiFi routers. The WPA2 encryption key can be changed for every mission and deployment based on security considerations. The network configuration team will have to ensure that all the corresponding WGS nodes, the WGS Node Deployment Tool and the C2 Application Server are properly configured with the right WPA2 encryption password before deployment.

(3) MAC Filtering or DHCP IP Reservation for Wireless Sensor Node

To prevent unauthorized devices from connecting to the WGSN WiFi network, it is recommended to adopt MAC filtering on the WiFi router if the feature is supported. In this way, only the authorized devices that have their MAC address configured as part of the MAC filtering whitelist are allowed to connect to the network. Unfortunately, the current version of Google WiFi mesh routers does not support MAC address filtering.

The DHCP IP reservation feature on the Google WiFi mesh router was used as an alternative to the lack of MAC filtering. As part of the pre-deployment preparation phase, each WGS node, the WGS Node Deployment Tool, and the C2 Application Server can connect to the WGSN WiFi network and have their MAC address captured and bound to a static IP address. By limiting the IP address range to exactly the total number of authorized devices that will be connecting to the WGSN WiFi network, unauthorized devices that attempt to the WGSN WiFi network will not be able to obtain a valid IP address and thus will not be able to connect to the WiFi network. Figure 33 illustrates the key steps to perform IP address reservation for WGSN devices using the Google WiFi Smartphone App:

1. Within the application, click on the ***Setting*** tab that is found on the top right-hand corner of the application to bring up the Setting page.
2. Under the Setting page, click on the ***Network & general*** button that is found under the Settings section of the page to bring up the Network & general page.
3. Under the Network & general page, click on the ***Advanced networking*** button that is found under the Network section of the page to bring up the Wifi point configuration page.
4. Under the Advanced networking configuration page, click on the ***DHCP IP reservations*** button to bring up the list of devices under the DHCP IP reservations list.
5. Click on the ***green +*** button found at the bottom right of the DHCP IP reservations page to assign a static IP address to a new WGS node.
6. Edit the device name and IP address as required. Once the device has been configured and connected to the mesh network, the page will show which Google Wifi point is the WGS node connected to and the Wifi band that is currently being selected.
7. Repeat step 5 and 6 to assign static IP address for each additional WGS nodes.

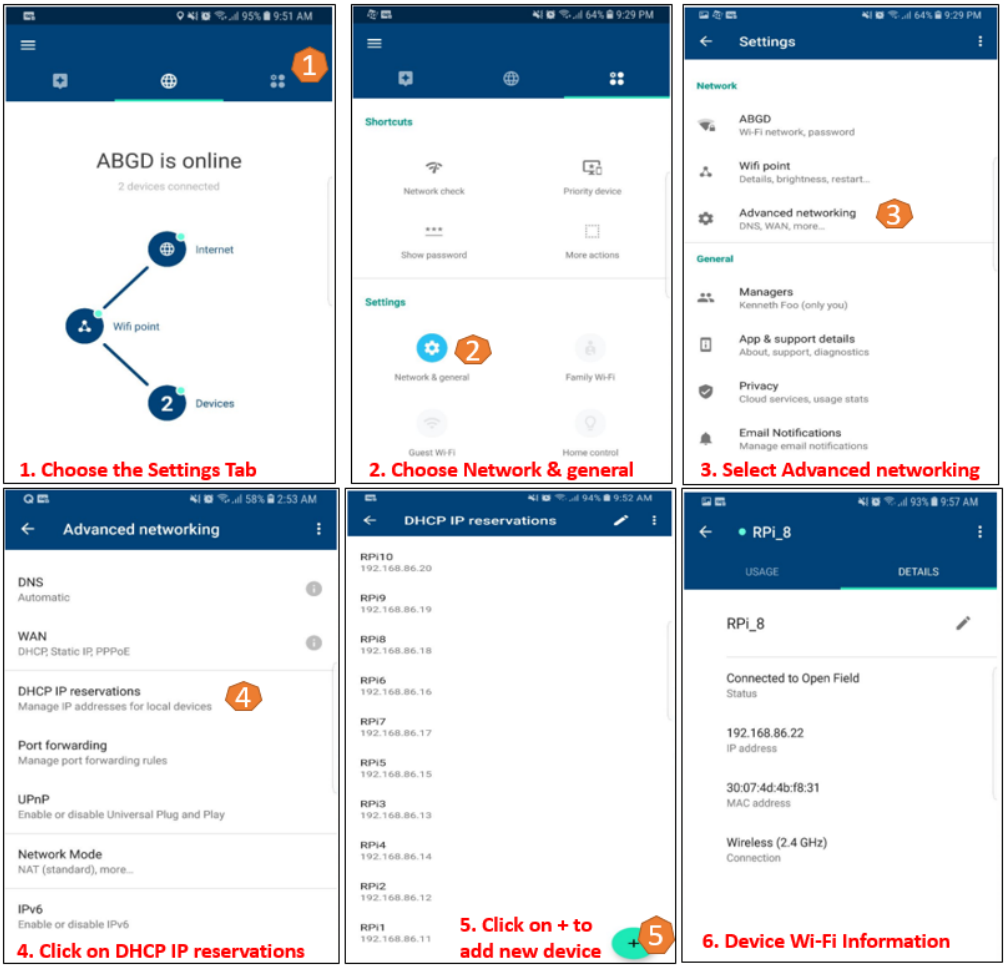


Figure 33. Key Steps to Perform IP Reservations Using Google WiFi Smartphone App

4. Threat Detection

To provide round the clock unmanned perimeter surveillance and early intrusion detection, the WGS nodes deployed at different detection layers around the operating base perimeter as illustrated in Figure 3, must be able to actively detect an intrusion, determine the nature of the intruder and send alerts to the C2 Application Server to alert the operator. To achieve this objective, the WGS node is equipped with PIR sensors to provide the initial intrusion motion detection capability. The PIR sensors, which are passive in nature, do not emit any infra-red but instead depends on the infra-red being emitted by objects within the sensor's field of view, which in this case is about 110 degrees.

The warm body intruder can be a human intruder, an animal or even a motorized vehicle, which typically have a higher heat signature as compared to the surrounding ambient temperature. Based on the difference between the temperature of the warm body intruder and the ambient temperature, any warm body intruder entering the PIR sensor's field of view can be effectively picked up by the PIR sensor. Since the PIR sensor works on the principle of measuring the difference in temperature of the warm body intruder and ambient temperature, the detection range, sensitivity and accuracy of the PIR are greatly affected by the ambient temperature and may not work well in an outdoor environment on a really a hot day. Thus, future research may be required to identify an alternate triggering sensor, such as an acoustic, seismic, or optical detector.

Since the PIR sensor is only able to provide preliminary information about a possible human intruder, the WGS node will need to turn on the camera after motion has been detected by the PIR sensor and leverage 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. Upon confirming a human, the camera captures the facial image of the human intruder and transmits it to the C2 Application Server for further image analysis and identification.

Upon receiving the intruder information and image from the various WGS nodes, the C2 Application Server first perform image analysis using the OpenCV computer vision to detect other human intruders that may be in the image but not picked up effectively by the WGS node's OpenCV facial detection algorithm, which is based on just the frontal facial recognition. The OpenCV algorithm on C2 Application Server can detect human subjects based on the eye profile, face-side profile and upper body profile instead of just the frontal face profile. This complements the limited detection capability of the WGS nodes constrained by the performance of OpenCV on Raspberry Pi 3 core hardware.

After WGS nodes send the preliminarily analysed images to the C2 Application server, the next step is to determine human subjects' identity based on OpenCV's facial recognition algorithm. The facial image of the human intruder will then be matched against the database, which consists of learned facial images of known individuals and

facial images of human intruders from various intrusion events in the past. Subsequently, if a human subject move through the base and his/her facial image is captured by multiple WGS nodes, the C2 Application Server is to be able to correlate and pinpoint the various intrusion events for the same intruder based on the facial image detection and recognition capability. With the correlated set of information, the path taken by that specific human intruder arranged in order of time, and the rate at which the intruder moves through the operating base can be determined. Using this information, the C2 Application Server then plots the route of advancement made by the intruder on the map, as shown in Figure 34.

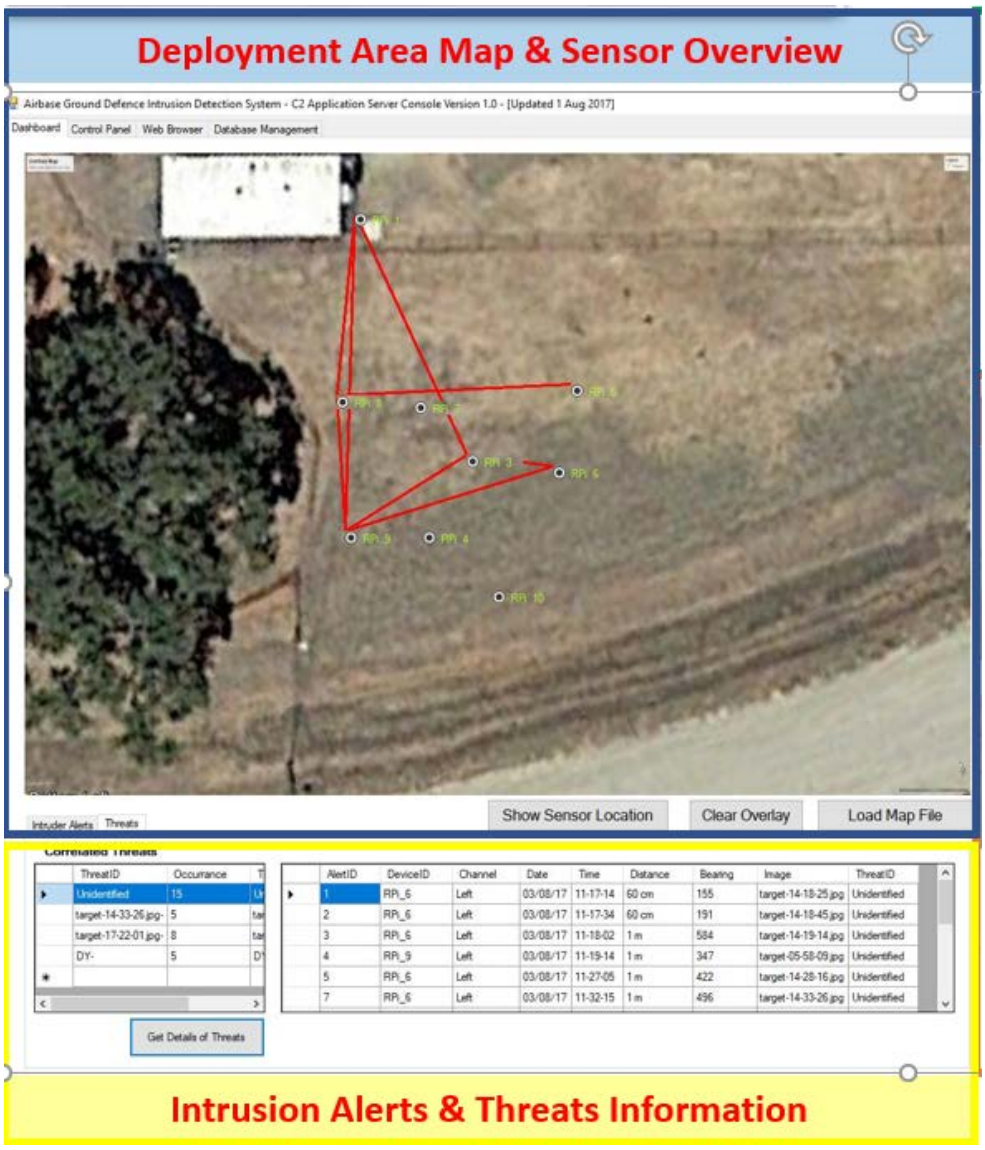


Figure 34. Path Taken by a Human Intruder Based on Correlated Intruder Information

5. Intrusion Information Sharing

The intrusion information and intruder image (both normal resolution and high-resolution image) are stored locally in the WGS node using a MySQL database. The intruder information and image in the normal resolution are also transmitted to the C2 Application Server for further processing and analysis before storing all the structured data and information on the Microsoft SQL Server database for support of correlation and search. After the identity of the intruder has been determined by the C2 Application Server using the OpenCV facial recognition algorithm, the identity information is sent back to the corresponding WGS node so that the identified information can be updated in the corresponding node's MySQL database table that stores all the intrusion event information.

6. Network Coverage Issue

Depending on the nature of the operating base environment (i.e., hostile or friendly environment, urban or open terrain environment) and the area of the overall deployment site, the WiFi network coverage and performance may be an issue. In a large area of deployment, the total number of WGS nodes and similarly the number of WiFi mesh router required to provide the required multi-layer early intrusion detection will increase rapidly. The placement of the various WiFi mesh routers with respect to the operating environment and location of the various WGS nodes affects the performance of the WGSN. If there are many WGS nodes deployed within a specific WiFi mesh router coverage area, the performance of those WGS nodes might also be affected as available bandwidth will be shared across all WGS nodes connected to that specific WiFi mesh router.

C. SUMMARY

In this chapter, the concept and system design of the WGSN, including the need for a WGS Node Deployment Tool, was discussed. The selection criteria for various components of the WGS nodes, WGS Node Deployment Tool and C2 Application Server, including the key technical specifications of those components, were presented.

The idea of mounting all components of the WGS nodes onto a normal solar garden light for ease of deployment of the WGS nodes in the deployment area was conceptualized.

Technology/concept demonstrators for each of the components were built and evaluated over the course of a few experiments.

Based on findings from the first few experiments, the design, performance, and functionality of the WGS node, WGS Node Deployment Tool and C2 Application Server were enhanced and refined. The WGS node was refined to include two variants to support deployment configuration requirements.

The requirement for a USB powered 802.11-based WiFi mesh network capable of providing wide area WiFi network coverage in the deployment area was presented together with the proposed WiFi security features. The key steps for configuring the Google WiFi mesh router, establishing network connectivity to the WiFi mesh network infrastructure including details on the WiFi standard, frequency band, transport layer protocol and message protocol being implemented for WGS node, WGS Node Deployment Tool, and C2 Application Server were discussed.

Finally, concerns with regards to the PIR sensor's detection capability under hot environment conditions and intruder facial detection performance of the WGS node were stated. In the following chapter, the various tests and experiments set up to evaluate the performance of individual components and WGSN sub-systems are discussed. The operating and design concept of the WGSN is also validated.

IV. WGSN TESTING AND EXPERIMENTATION

To validate the WGSN concept and performance of the WGS node, a system demonstration was conducted at the Naval Postgraduate School (NPS) and two field experiments were conducted during the 17-4 NPS Joint Interagency Field Experiment (JIFX) held at Camp Roberts from 31 July 2017 to 4 August 2017. The NPS JIFX is a valuable platform to validate the early intrusion and detection performance and capability of the WGSN in an actual field environment.

A. CONSTRUCTING THE WGS NODE

To evaluate the design and performance of the WGS node, two variants of WGS nodes were developed. Variant A of WGS node was based on the concept of using dual USB webcams and PIR sensors to provide a wider detection field of view. Variant B of WGS node was based on the concept of using IR-Cut Pi Camera to provide the WGS node with night photography capability using a pair of IR transmitters at the expense of having a narrower detection field of view by using a single IR-Cut Pi Camera and PIR sensor. This section illustrates the physical construction of both variants of the WGS node.

1. Battery Pack

For both variants of the WGS node, the battery pack is mounted onto the solar garden light using Velcro tape for ease of removal and attachment. This design facilitates replacing the battery pack in the field easily when the original battery pack capacity runs out. The Anker 10,000 mAH battery pack has LED indicators on the top of the battery pack to indicate its remaining charge capacity. The battery pack is mounted in a way that its LED indicators are visible externally to facilitate the deployment team in checking the remaining battery charge capacity of the WGS node.

For Variant A of the WGS node, the battery pack is mounted onto the pole of the solar garden light. For Variant B, the battery pack is mounted on the top of the solar garden light. Figure 35 and Figure 36 depicts the mounting of battery packs onto the solar

garden light using Velcro tape for Variant A and Variant B of the WGS node, respectively.

Figure 35. Mounting of Battery Pack onto the Solar Garden Light for Variant A of WGS Node

Figure 36. Mounting of Battery Pack onto the Top of Solar Garden Light for Variant B of WGS Node

2. Raspberry Pi 3 Model B Board

For both variants of the WGS node, the Raspberry Pi 3 Model B board is secured onto the solar garden light using Velcro tape for ease of removal and attachment. This design facilitates ease of replacement when the Raspberry Pi 3 Model B board fails. The Raspberry Pi 3 Model B board shall be placed with the USB ports facing down to prevent the accumulation of dust and water in the USB and Ethernet ports when deployed in outdoor environment. Figure 37 and Figure 38 depict the mounting and placement of the Raspberry Pi 3 Model B board onto the solar garden light using Velcro tape for Variant A and Variant B of the WGS node, respectively.

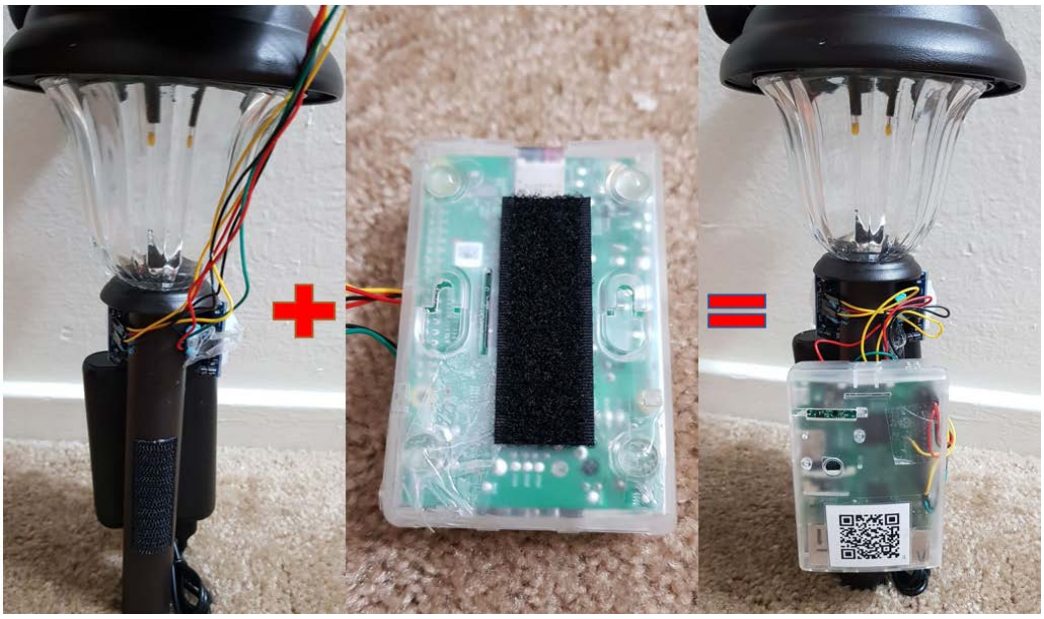


Figure 37. Mounting of Raspberry Pi 3 Model B Board onto the Solar Garden Light for Variant A of WGS Node

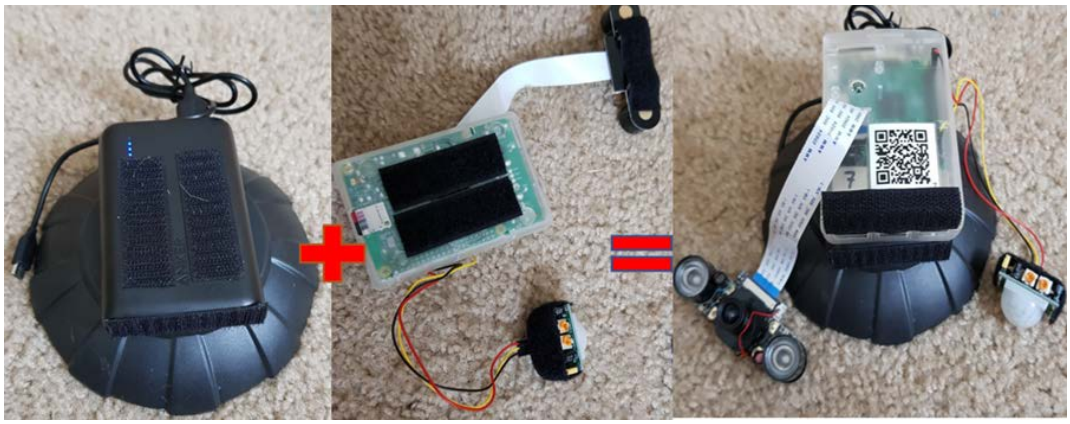


Figure 38. Mounting of Raspberry Pi 3 Model B Board onto the Solar Garden Light for Variant B of WGS Node

3. PIR Sensor

Variant A of the WGS node supports dual-channel PIR sensors to provide a combined detection field of angle of up to 220 degrees. The dual-channel PIR sensors are carefully mounted above the battery pack and Raspberry Pi 3 Model B board on the solar garden light using Velcro tape for ease of replacement when any of the PIR sensors fails. The PIR sensors are mounted on the pole of the solar garden light at 90-degree placement angle. For Variant B of the WGS node, the single-channel PIR sensor can be mounted at different location depending on the placement of the IR-Cut Pi Camera. Figure 39 depicts the mounting and placement of the PIR sensor onto the solar garden light using Velcro tape for Variant A (left of Figure 39) and Variant B (right of Figure 39) of the WGS node.

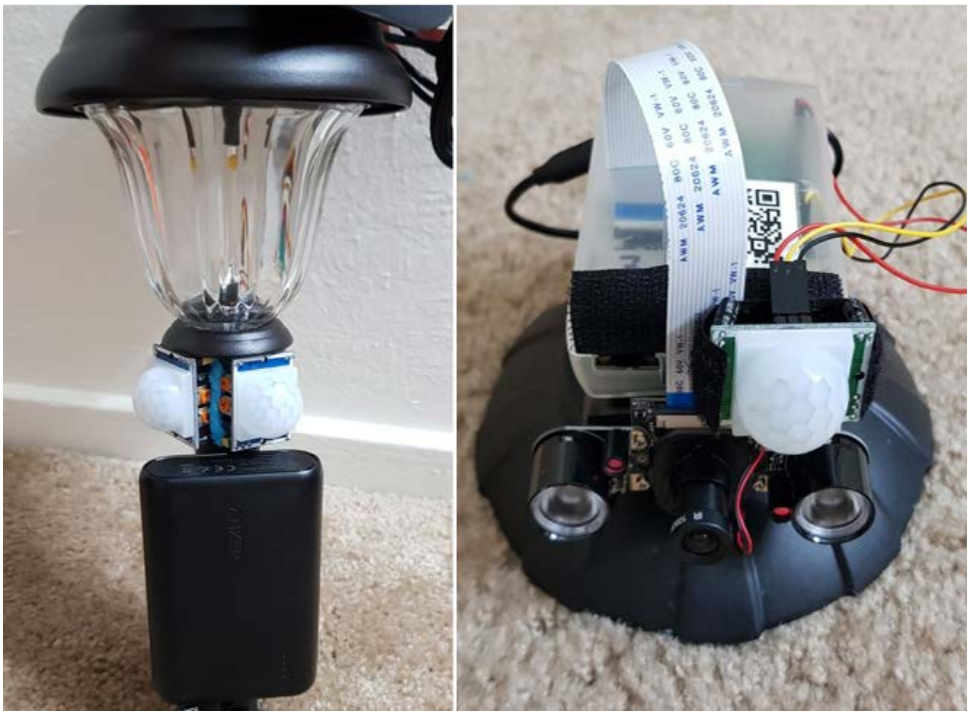


Figure 39. Mounting of PIR Sensor onto the Solar Garden Light for Variant A (left) and Variant B (right) of WGS Node

4. Camera

Variant A of the WGS node supports dual-channel USB web cameras to provide a combined image field of angle of about 120 degrees. The dual-channel USB webcams are carefully mounted on the top of the solar garden light using Velcro tape for ease of replacement when any of the USB webcam fails. The dual-channel USB webcams are mounted at 90-degree placement angle on the top of the solar garden light. For Variant B of the WGS node, the IR-Cut Pi Camera can be mounted in different configuration (i.e., 15, 30 or 45 degrees upward facing or front facing) depending on the nature of the deployment. Figure 40 and Figure 41 show the mounting and placement of the USB webcams and IR-Cut Pi Camera onto the solar garden light using Velcro tape for Variant A and Variant B of the WGS node, respectively.

Figure 40. Mounting of USB Webcam onto the Solar Garden Light for Variant A of WGS Node

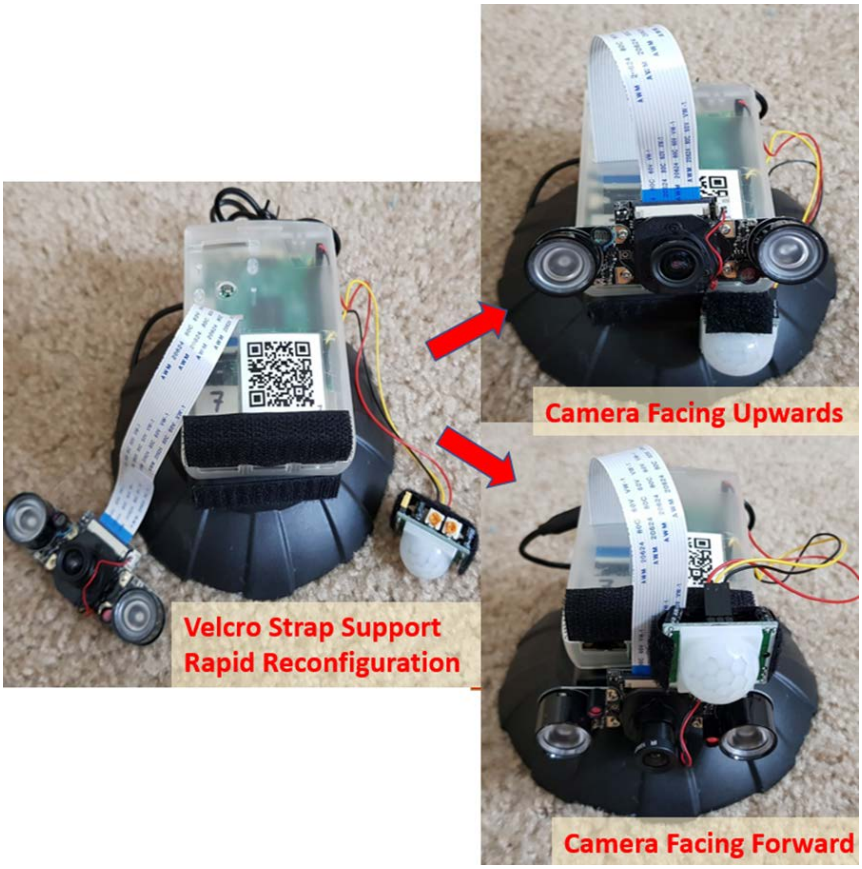


Figure 41. Mounting of IR-Cut Pi Camera onto the Solar Garden Light for Variant B of WGS Node

B. TESTING AND EXPERIMENTATION

Thorough testing of various components and sub-systems of the WGSN is essential for evaluating the performance and discovering the limitation of individual components and sub-systems. Following the successful testing and evaluation of various components and sub-systems, it is important to assess the overall WGSN performance in the actual field environment through a series of field experiments to understand the effect of the environment, terrain and weather on the performance of the WGS nodes, WiFi network and WGSN.

The test results gathered from the various field experiments provides a means to validate the design of the WGS node and operational concept of WGSN. It provides valuable insight into the possible areas of enhancement and improvement to make the overall system more robust, adaptable and intelligent. It serves as a baseline for what has been achieved and what are some of the future work areas and experiments that could be performed.

1. Summary of Action

To validate the design and operational concept of the WGSN for providing early intrusion detection around the FARPs deployment area and to test and evaluate the performance of each component and sub-system of the WGSN, a series of system tests were conducted.

The first system test was conducted around the Academic Quad open area within the NPS campus. The primary objective of conducting the system test was to evaluate the detection range and performance of the PIR sensor, USB webcam, IR-Cut Pi Camera and Google WiFi mesh router. The secondary objective was to test the integration of various components on the respective sub-systems. Finally, the interoperability of various WGSN sub-systems was tested.

After system testing was completed, two field experiments were scheduled and conducted at Camp Roberts. The first field experiment was conducted in an urban built-up environment within Camp Roberts to evaluate the WGSN overall system performance in such an urban environment. The design, layout and physical construct of various

buildings within the built-up environment may pose different challenges to the WiFi coverage and WGS node's detection capability. Two different phase of field experiments were conducted on two different types of buildings with two different WGS node configurations to assess how different WGS node deployment scenarios and node configurations may affect the performance of the WGSN.

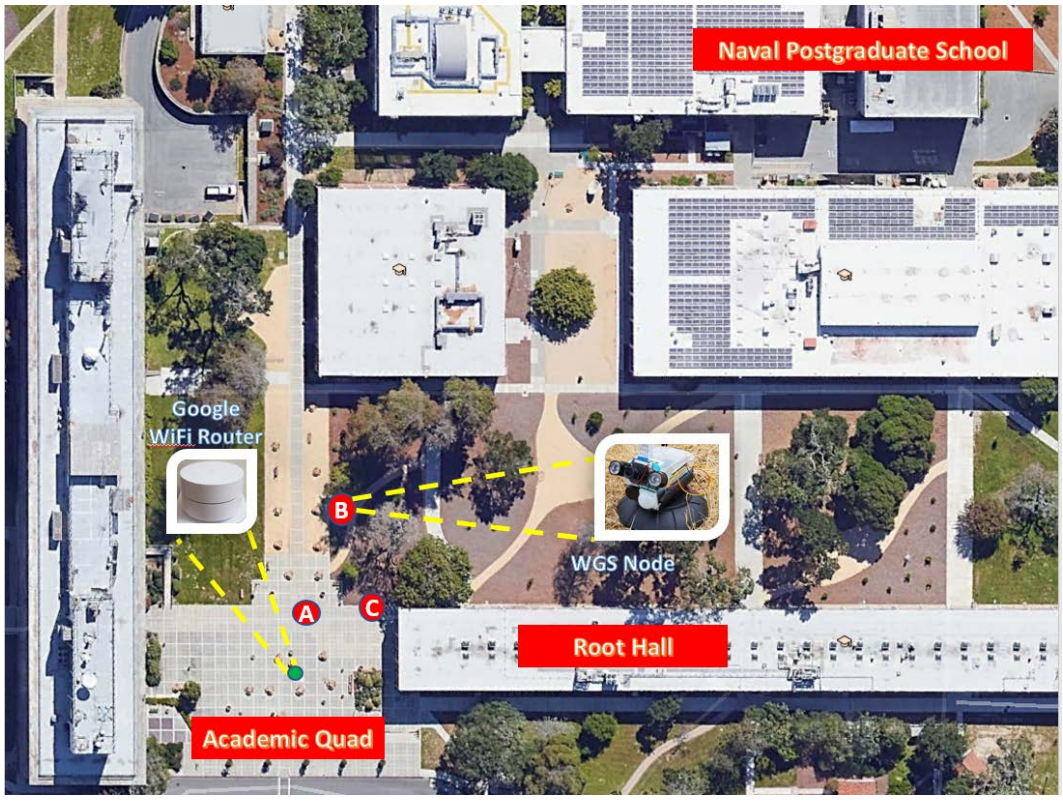
The second field experiment was conducted at an open airfield area within Camp Roberts that was similar to actual FARPs. The objective of the second field experiment was to validate the concept of using the WGSN for providing early intrusion detection capability for a FARP. Two different phases of field experiments were conducted with two different WGS node configurations to evaluate the performance of the WGSN under different WGS node deployment configurations.

For each phase of field experimentation, key findings were documented and summarized. Any gaps that could be addressed by means of minor configuration changes or software changes were implemented and tested immediately on site. Constraints and limitations of current WGSNs identified during system testing and field experiments that could not be immediately addressed on site were documented for further review. Enhancements that require minor component changes or minor system re-designing are implemented as part of this thesis. Other technical constraints and limitations that require a much longer lead time to develop, enhance, test and implement are highlighted as areas for further research.

2. System Testing—Component and Sub-system Testing (NPS Campus)

System testing was conducted around the Academic Quad and Root Hall area within NPS, Monterey, California on 2 June 2017 (Friday). The weather at the time (between 1pm to 4pm) of testing was sunny with an ambient temperature of about 24 degrees Celsius (75 degree Fahrenheit) and a light intensity of about 12,000 lux. The purpose of this system test was to evaluate the performance characteristics of individual components in an outdoor environment, test the integration of various components of the respective sub-system and finally test the interoperability of various WGSN sub-systems.

Figure 42 shows the satellite view of the Academic Quad and Root Hall area within NPS where the system test was conducted.



Naval Postgraduate School, Lat 36.594296 and Lon -121.876114. Image retrieved from Google Earth, April 15, 2016.

Figure 42. Satellite View of Academic Quad and Root Hall Area within Naval Postgraduate School, Monterey, California, where System Test Was Conducted

a. WGS Node

To test and evaluate the performance of the PIR sensor and camera on the WGS node, different variants of the WGS nodes were deployed at different location around the Academic Quad area as shown in Figure 43.

Figure 43. WGS Node Deployed at Location A and B near NPS Academic Quad

(1) PIR Sensor

The detection sensitivity of the PIR sensor was first evaluated by getting one of the team members to slowly approach the PIR sensor at various angles and determine distances at which the PIR sensor triggered a detection using a laser distance measurement meter. Figure 44 illustrates the testing methodology and test setup. Table 9 shows the detection ranges of the PIR Sensor at the different field of view angle.

Figure 44. PIR Sensor and Camera Test Setup with Laser Distance Measurement Tool

Table 9. PIR Sensor Detection Range

Field of View Angle (Degrees)	Detection Distance (Meters)
0	~ 3.5
30	~ 3.0
60	~ 2.5
90	~ 2.2
110	~ 1.5

During the PIR sensor performance evaluation, it was discovered that the PIR sensor performance was greatly affected by ambient temperature and sunlight intensity. During our test that was conducted on a sunny afternoon, there were several instances of false positive triggering of the PIR sensor, particularly at test locations A and B, likely due to the radiated heat reflected from nearby structures like bench, lamp post and even the concrete pavement and walkway.

(2) Camera

The performance of the camera onboard the WGS node was evaluated with the OpenCV facial detection algorithm running on the WGS node. Both Logitech C270 USB Webcam and WaveShare IR-Cut Pi Camera support a field of view of between 60 to 70 degrees. The key differences between the two types of cameras are summarized in Table 10.

Table 10. Key Differences between Logitech C270 USB Webcam and WaveShare IR-Cut Pi Camera

	Logitech C270 USB Webcam	**WaveShare IR-Cut Pi Camera**
Interface	USB 2.0	Raspberry Pi Camera Interface
Max. number of Camera Supported per WGS node	Up to 4	1
Maximum Supported Video Resolution	Up to 720p	Up to 1080p
Image Focus	Auto-Focus	Manual-Focus
Infra-red (IR) Night Photography	Not supported	Supported with onboard IR transmitter and IR camera

There are several parameters within the OpenCV facial detection algorithm that will affect the detection sensitivity and performance of facial detection. Table 11 summarizes the significance of each of the parameters, the recommended settings for each of the parameters and the settings adopted for the WGS node.

Table 11. Key Parameters in OpenCV Facial Image Detection Algorithm that Affect Facial Detection

Key Parameters	Settings on WGS Node	Significant of Setting Parameter
resolution	858, 480 pixels (16:9)	• Define the video resolution of the camera • 16:9 video resolution has wider field of view as compared to 4:3 video resolution • Lower resolution has faster performance but less image details on the intruder • Higher resolution has slower performance but more image details on the intruder
scaleFactor	1.8	• The scaling factor determines the scale at which each video frame will be resized downwards before the facial detection takes place. It is based on the image scale pyramid principle. • 1.05 is the recommended settings for more accurate facial detection but the detection time will be longer. • 1.4 is the recommended settings for faster detection but the accuracy of detection will be lower.
minNeighbors	5	• This value defines the minimum number of points of detection required • A higher number of minNeighbors results in less number of detections but each detection will be more accurate. • Typically used values for facial detection are from 3 to 6.
minSize	15, 15	• This value defines the minimum size of the facial image in pixel before the algorithm would classify it as a face. • 30 by 30 pixel is the recommended setting for face detection.

The facial image detection capability of the camera was first evaluated by getting one of the team members to slowly approach the camera at various angles and determine the distance at which the camera and OpenCV facial image detection algorithm can detect and lock on the facial image of the intruder. Figure 45 illustrates some of the

images that were taken by the WGS node during the camera's intruder facial image detection sensitivity test.

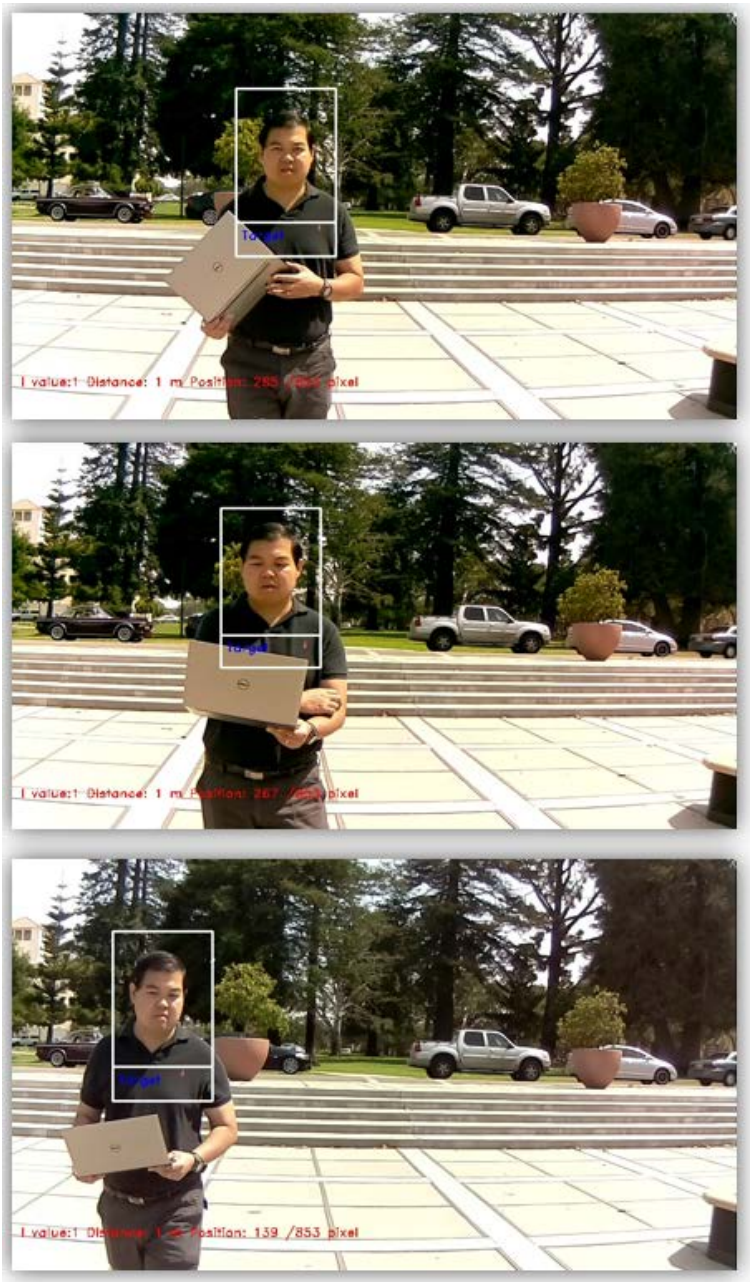


Figure 45. Camera Detection Range and Field of View Test

Table 12 shows the detection ranges of the camera and OpenCV facial image algorithm at the different field of view angles.

Table 12. Facial Image Detection Range of WGS Node

Field of View Angle (Degrees)	Detection Distance (Meters)
0	~ 3.5
30	~ 3.5
60	~ 3.5

During the camera performance evaluation, it was discovered that the detection of the intruder facial image is affected by the position of the sun, the intensity of the backlight and the level of color contrast between the intruder face and the background since the image is first converted to grayscale before facial image detection takes place. If the position of the sun is behind the intruder, the facial image detection sensitivity is lower and the time taken to detect the intruder facial image is a few seconds longer. If the intruder facial image has a high level of contract with the background, the detection sensitivity is increased and the time taken to detect the intruder facial image is greatly reduced. It was also discovered that the speed of detection by the OpenCV facial image detection algorithm is affected by the video capture resolution. A lower video resolution allows the OpenCV facial image detection algorithm to scan and analyze each frame of the video faster thereby reducing the detection time.

(3) WGS Node Integration Test

After testing the detection performance and sensitivity of the PIR sensor and camera at various locations around the Academic Quad area, the WGS node integration test was conducted. The objective of the integration test was to validate all aspects of the functional design of the WGS node which includes connectivity to the WiFi mesh network and the C2 Application Server, the automatic triggering of a camera to turn on after an intruder has been detected by the PIR sensor, the facial detection using the

camera and the OpenCV facial detection algorithm and, finally, capturing, storing, processing and sending of the intrusion related information and image to the C2 Application Server and the respective databases. Figure 46 illustrates the intruder detection capability under full functional testing of WGS node.

Figure 46. Intruder Detection Capability Tested under Full Functional Testing of WGS Node at Location C of NPS Academic Quad

b. WGS Node Deployment Tool

For the WGS Node Deployment Tool, the objective of the system test was to evaluate the user-friendliness of the tool in an outdoor environment under strong sunlight, to assess the QR code scanning speed and evaluate the performance, sensitivity and accuracy of the USB GPS receiver.

(1) WGS Node Deployment Tool Processing Hardware

The WGS Node Deployment Tool was developed using the Microsoft Surface Pro 4 tablet equipped with the Surface pen and a bright 12.2-inch display. The large and bright screen coupled with touchscreen and Surface pen makes the use of the WGS Node Deployment Tool in an outdoor environment effective. The WGS Node Deployment Application worked well and could capture each WGS node's network and GPS position

information quickly and easily. The information was verified to be transmitted to the C2 Application Server correctly in real-time through the WiFi mesh router. Based on the system test conducted, the deployment team was able to accurately tag the position of each WGS node and commission a WGS node in less than a minute.

(2) QR Code Scanning

The QR code scanning capability using the WGS Node Deployment Tool's onboard rear-facing camera was fast and accurate. Based on the numerous tests, the encoded QR code information could be retrieved from the QR code affixed on the top of various WGS nodes within a second and the tool achieved 100% accuracy. This form of data entry eliminates the need for the deployment team member to perform any manual data entry using the on-screen keyboard or the Surface pen and most importantly, to eliminate any possible human error during data entry.

(3) USB GPS Receiver

The USB GPS receiver connected to the WGS Node Deployment Tool is sensitive and can acquire a GPS fix in less than ten seconds on cold start in an outdoor environment. For subsequent warm start, the GPS receiver can acquire GPS fix in less than two seconds in an outdoor environment. In terms of GPS location accuracy, the GPS receiver has a random positional accuracy of about two meters. It was discovered that since the WGS nodes are typically placed less than 10 meters apart from each other, the acquired GPS position of WGS nodes when plotted onto the map of the deployment area may be slightly off due to the random positional error of about two meters. This may be a concern in a small deployment area but for a large deployment area like a FARP, it may be less of a concern.

c. WiFi Mesh Network Coverage and Throughput

To evaluate the WiFi performance of the Google WiFi mesh router particularly with Raspberry Pi 3 Model B based WGS node, the Google WiFi mesh router was placed in the center of the Academic Quad area as shown in Figure 47 below. A Raspberry Pi 3 Model B board equipped with Raspberry Pi Touchscreen Display was then configured as

a mobile WiFi coverage testing tool used to assess the WiFi coverage and throughput around the test location.

Figure 47. Google WiFi Mesh Router Deployed in the Center of the NPS Academic Quad

Figure 48 shows the Raspberry Pi 3 Model B board equipped with the Raspberry Pi 7-inch Touchscreen Display that was used to evaluate the performance of the Google WiFi mesh router.

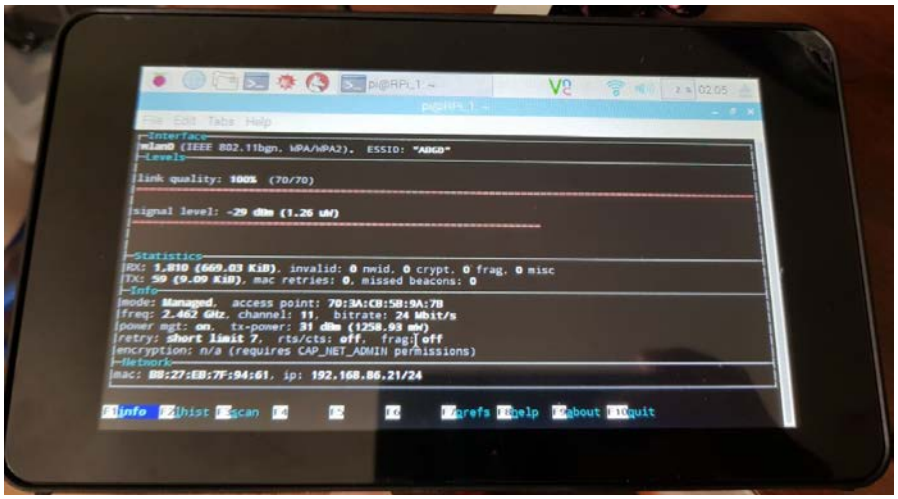


Figure 48. Raspberry Pi 3 Model B Board Equipped with Raspberry Pi 7-Inch Touchscreen Display Used for WiFi Performance Evaluation

Figure 49 shows the Wavemon WiFi monitoring tool running on Raspberry Pi 3 that shows key information like WiFi link quality, signal strength in terms of dBm or micro-watt and the channel bit rate (Matt, 2014). Additional functions are available on the Wavemon application and can be selected using the various function keys (e.g. F1 to F10) on the keyboard. Besides using Wavemon application to measure the WiFi signal strength and throughput, a continuous ping was also enabled to ensure that the data packets can indeed be transmitted between the Raspberry Pi 3 and the Google WiFi mesh router without any errors.

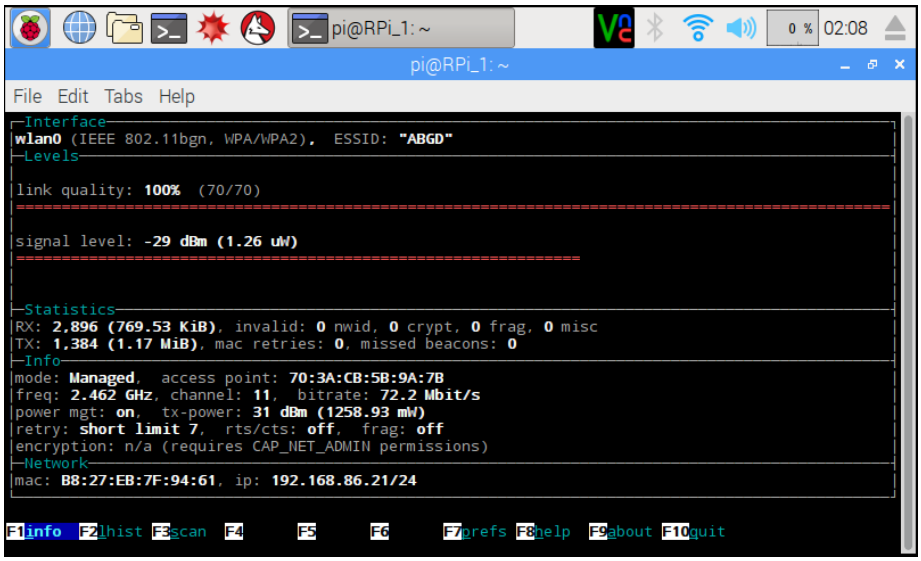


Figure 49. Wavemon Application Running on Raspberry Pi 3 Used to Monitor and Evaluate the WiFi Performance

Based on the Google WiFi coverage and throughput tests, it was discovered that a single Google WiFi mesh router powered by normal battery pack could provide useable WiFi coverage of about 120 meters in radius at our test location in NPS as shown in Figure 50.

Naval Postgraduate School, Lat 36.595201 and Lon -121.875254. Image retrieved from Google Earth, April 15, 2016.

Figure 50. Google WiFi Mesh Router Coverage around NPS Academic Quad

d. C2 Application Server

For the C2 Application Server, the objective of the system testing was to evaluate the user friendliness of the C2 Application Dashboard interface in providing essential real-time situation awareness information for the operator, to test all the key functionality available through the C2 Application Control Panel, to assess the performance of the OpenCV facial detection algorithm and facial recognition algorithm on the C2 Application Server and to ensure that all information, images and control messages can be received and sent correctly through the TCP based WiFi network connection.

(1) Receiving Intruder Alerts

During the interoperability testing of the system with a WGS node and the Google WiFi mesh router, it was determined that the C2 Application Server could receive all the intruder alerts and images correctly. The intruder information and image were also displayed correctly.

(2) User Friendliness of C2 Application Dashboard

The C2 Application Dashboard interface was evaluated to be effective in providing the operator with essential real-time information of any intrusion event without overwhelming the operator.

(3) Functional Testing of Various Remote WGS Node Configuration and Control Features

All remote WGS node configuration and control features were tested to be functional with the WGS node. All control messages were sent correctly to all of the selected WGS nodes and all requested actions were executed correctly by the WGS nodes.

(4) Image Analytics

The image analytics engine based on the OpenCV facial detection algorithm using three different Haar Cascade feature-based classifiers was tested to be effective in detecting the side facial profile of an intruder, the eyes of the intruder and additional intruders that may be in the background not picked up by the WGS node.

(5) Facial Image Recognition

The facial image recognition engine was also tested to be effective in correlating an intruder that previously had its facial image captured and learnt by the system. It was discovered that the effectiveness and accuracy of recognition and correlation depends on the number of different learnt facial features of the intruder as well as the quality and clarity of the intruder image captured.

3. Field Experiment 1—System Testing in Urban Environment (JFIX CACTF)

Field experiment 1 was conducted at the Combined Arms Collective Training Facility (CACTF) during the 17-4 NPS JIFX event that took place from 31 July 2017 to 4 August 2017. CACTF is situated within Camp Roberts, San Miguel, California. CACTF is an integrated urban built-up facility that allows a wide range of training and field

experiment to be conducted in an urban setting consisting of a variety of different types predominately cinder-block construction buildings (Cox Construction, n.d.).

For this field experiment, two different phases were conducted over two different days in two different buildings with two different WGS node camera configurations. Table 13 shows the detail of the two different phases of field experiment.

Table 13. Details of Two Different Phases of Field Experiment 1

	Phase 1 Field Experiment at CACTF	**Phase 2 Field Experiment at CACTF**
Date and Time of Field Experiment	• 1 August 2017 • 1000 to 1600 hours	• 3 August 2017 • 1000 to 1600 hours
Experiment Location	• Building with Boundary Wall	• 2-level Building without any Boundary Wall
WGS Node Deployment Location	• On boundary wall • Around boundary wall • At the gate • At building entrance	• Around building • In openings around building • At door entrance • At stairway
WGS Node' Camera Configuration	• Forward facing	• 30 degrees upward facing
Weather Condition	• Sunny	• Cloudy

Figure 51 shows the satellite view of the CACTF facility with the two buildings where two different phases of field experiments were conducted.

CACTF Facility, Camp Roberts, Lat 35.765090 and Lon -120.769728. Image retrieved from Google Earth, June 14, 2017.

Figure 51. Satellite View of CACTF Facility

This field experimentation conducted at the CACTF aimed to validate and evaluate the performance and capability of the WGSN and WGS nodes within an urban built-up environment.

a. Phase 1 Experiment—Building with Boundary Wall

In this portion of the experiment, the WGS nodes are deployed around a building with a boundary wall.

(1) Experiment Setup

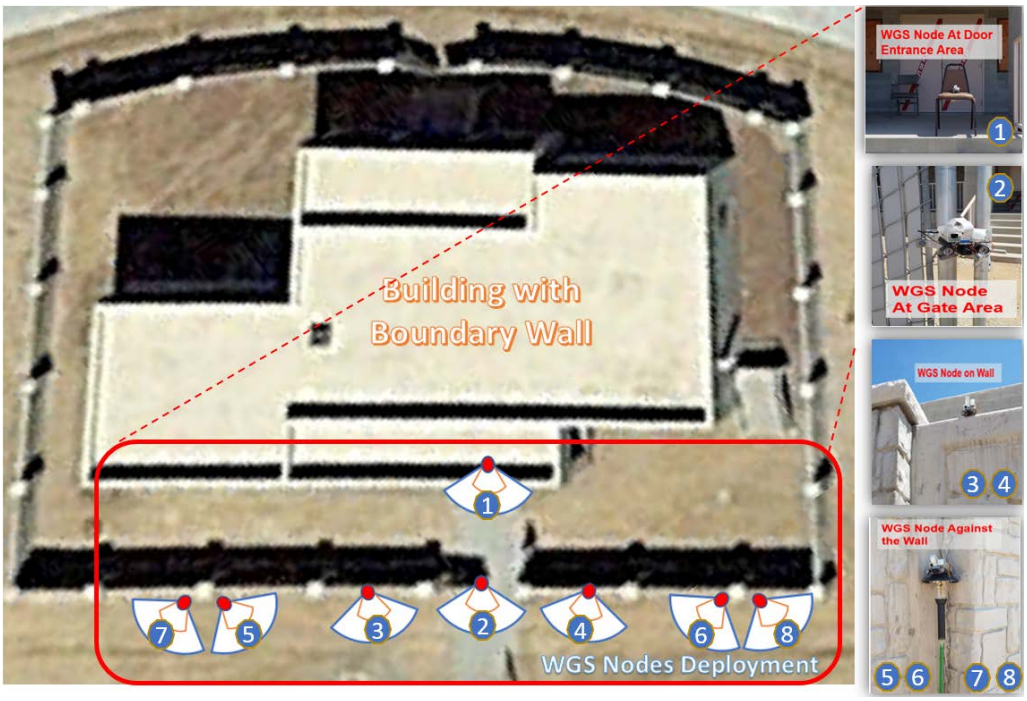
On 1st August 2017 (Day 2 of JFIX event), WGS nodes were deployed around the perimeter of the building, with a high boundary wall, to evaluate the performance of WGSN in providing perimeter defense and early intrusion detection for the protected building. The WGSN C2 Application Server was deployed in the sheltered training shed at the other end of the CACTF facility. To provide the required WiFi coverage around the

facility, the Google WiFi mesh router was deployed in the middle of the CACTF facility. Figure 52 shows the experiment setup for Phase 1 of field experiment at the CACTF facility.

CACTF Facility, Camp Roberts, Lat 35.765090 and Lon -120.769728. Image retrieved from Google Earth, June 14, 2017.

Figure 52. Experimental Setup for Phase 1 of Field Experiment at CACTF

The WGS nodes deployed around the perimeter of the building were either mounted onto the extendable pole or placed on top of the wall, gate or entrance. Figure 53 shows the different WGS node configurations placed at various locations around the perimeter of the building.



CACTF Facility, Camp Roberts, Lat 35.765432 and Lon -120.769721. Image retrieved from Google Earth, June 14, 2017.

Figure 53. Placement of WGS Nodes around the Perimeter of the Building

Figure 54 to Figure 56 shows the actual placement of WGS nodes around the perimeter of the building. The WGS nodes were either mounted onto the extendable pole or placed on top of the wall, gate and entrance.

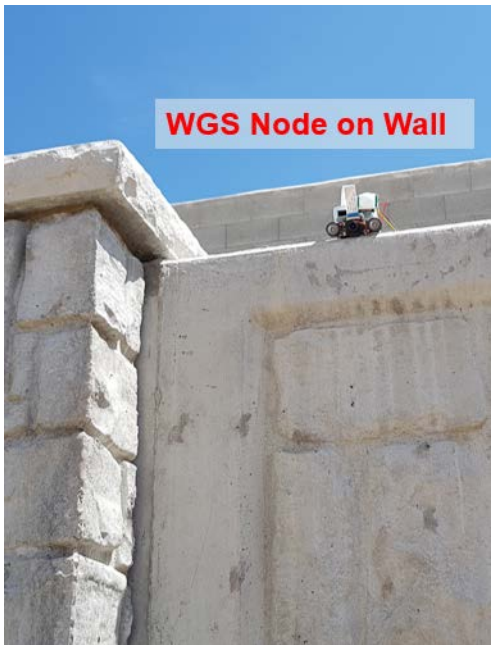


Figure 54. WGS Node Deployed on Top of Building Boundary Wall

Figure 55. WGS Node Deployed against the Building Boundary Wall

Figure 56. WGS Node Deployed at the Gate and Door Entrance Area

Figure 57 shows the C2 Application Server and the video monitoring station displaying real-time intruder information and video streaming from the various WGS nodes deployed in the sheltered training shed.

Figure 57. C2 Application Server (right) and Real-Time WGS Node Video Monitoring Station (left) Deployed in the Sheltered Training Shed at CACTF

(2) Intrusion Detection Capability of WGS Nodes

During this phase of field experiment, it was discovered that the PIR sensor on all WGS nodes were continuously triggered due to the high ambient temperature, around 38 degrees Celsius (100 degrees Fahrenheit), which in turn caused the cameras on-board all the WGS nodes to be continuously turned on. The strong sunlight that shined from behind the camera, also facilitated the WGS node's camera in detecting the intruder facial image quickly as the facial feature of the human intruder could be clearly seen, even when the intruder was wearing sunglasses and a cap (see Figure 58 and Figure 59).

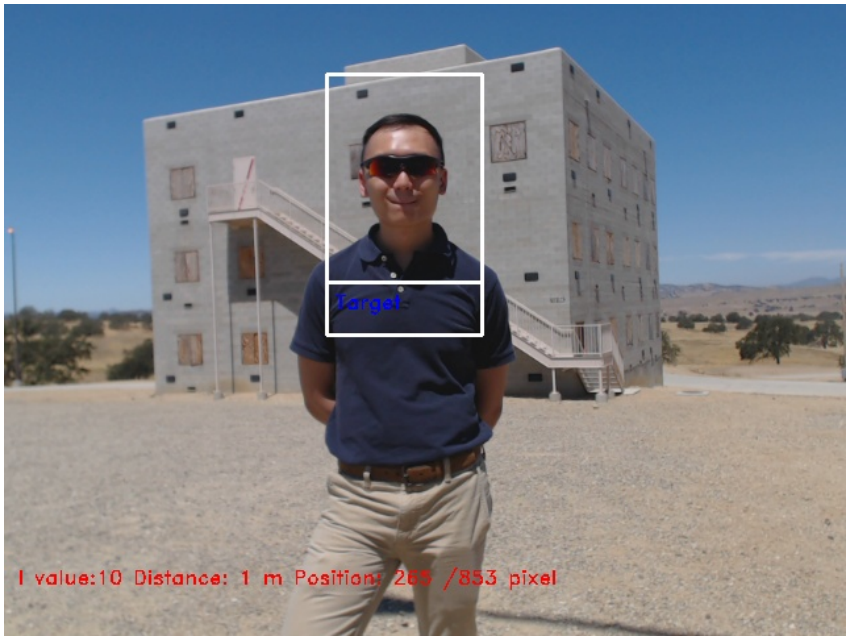


Figure 58. Intruder Wearing Sunglasses Being Detected by the WGS Node

Figure 59. Intruder Wearing Sunglasses and Hat Being Detected by the WGS Node

The WGS node was also able to detect multiple human intruder facial images within the camera field of view. Figure 60 shows the two-human intruders' facial images detected by the WGS node mounted at the top of the boundary wall.

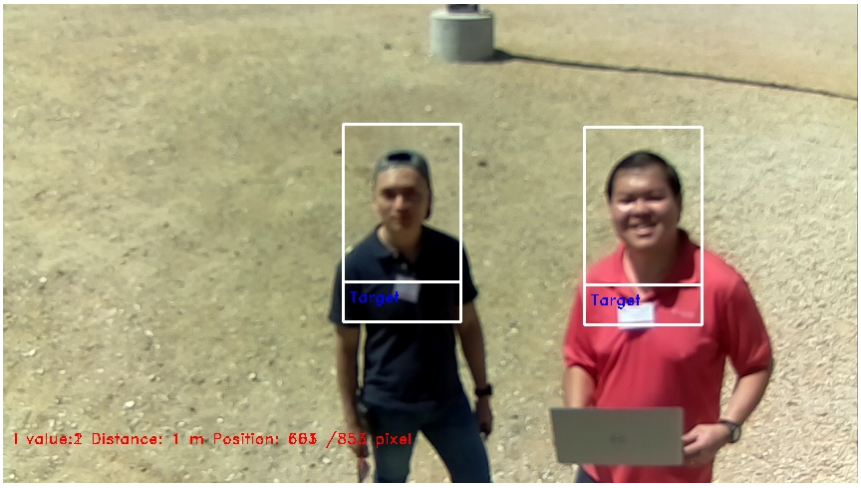


Figure 60. Multi-facial Image Detection Capability of the WGS Node

(3) Performance of WGSN

WiFi Coverage. Before deploying all WGS nodes, a WiFi coverage test was conducted on-site using the Mobile WiFi Scanning Tool, a Raspberry Pi 3 Model B

mounted with 7-inch Raspberry Pi Touchscreen display, running the Wavemon WiFi monitoring application. Based on the pre-deployment WiFi coverage test, it was validated that the Google WiFi mesh router deployed in the center of the CACTF facility could provide the required WiFi coverage around the CACTF facility. All WGS nodes deployed around the perimeter of the building could establish a WiFi communication link with the C2 Application Server that was in the training shed located at the other end of the CACTF facility. Figure 61 illustrates the Google WiFi mesh router coverage when deployed in the center of the CACTF facility. Due to the urban built-up nature of the environment with concrete buildings around the CACTF facility, the Google WiFi mesh router range has been greatly reduced from about 120 meters to about 45 meters in radius. There are also some WiFi dead spots around the CACTF facility, particularly behind the various buildings.

CACTF Facility, Camp Roberts, Lat 35.765090 and Lon -120.769728. Image retrieved from Google Earth, June 14, 2017.

Figure 61. Google WiFi Mesh Router Effective WiFi Range within CACTF Facility

WGS Node Deployment Tool. The WGS Node Deployment Tool worked as expected under this phase of experiment. The only limitation identified was the accuracy of WGS node's GPS location. Due to the urban nature of the environment and with the high boundary wall around the building, the time to obtain accurate GPS location was determined to take additional five to eight seconds. The accuracy of WGS node's GPS location was also affected due to the proximity of the WGS node deployed around the boundary of the building.

WGS Node. The WGS node worked and performed as designed under this phase of testing. One of the constraints identified was the sensitivity of the PIR sensor. Due to the high ambient temperature, the PIR sensor was always triggering, causing the camera on the WGS node to be always on. Another constraint that we discovered was the throughput and range of the onboard WiFi chipset. We also found that under an urban environment, it was challenging to plant the extendable pole and solar garden light into the dry solid ground.

C2 Application Server. The C2 Application Server worked and performed as designed under this phase of testing. All intrusion related information and images from multiple WGS nodes were received, processed and stored correctly. All control messages were also sent correctly to all selected WGS nodes. The only weakness identified during this phase was the processing delay of incoming intruder alerts when many intrusion alerts and images were received at the same time from multiple WGS node. Fortunately, with the use of Microsoft SQL Server database on the C2 Application Server as a virtual message queue, no incoming intrusion alerts and images were dropped or lost. Every intruder alert and image was processed by the C2 Application Server in a sequential manner.

b. Phase 2 Field Experiment—Two-Level Building without Boundary Wall

The following describes how the experiment was set-up, how the intrusion detection capability of the WGS nodes was executed, and the measurement of the performance of the WGSN.

(1) Experiment Setup

On 3 August 2017 (Day 4 of JIFX event), WGS nodes were deployed around the perimeter of a two-level building without a boundary wall. The WGS nodes deployed around the building perimeter were either placed on the ground or hidden in openings around the building to evaluate the performance of WGSN in providing perimeter defense capability and early intrusion detection for the 2-level building. The WGSN C2 Application Server was deployed in the same sheltered training shed, which was right beside the 2-level building. To provide the required WiFi coverage around the 2-level building and the sheltered training shed area, the Google WiFi mesh router was re-deployed above an electrical distribution-board mounted on the lamp pole in between the 2-level building and the sheltered training shed. Figure 62 shows the experiment setup for Phase 2 of Field Experimentation 1 at the CACTF facility.

CACTF Facility, Camp Roberts, Lat 35.765090 and Lon -120.769728. Image retrieved from Google Earth, June 14, 2017.

Figure 62. Experimental Setup for Phase 2 of Field Experimentation 1 at CACTF

The WGS nodes deployed around the perimeter of the 2-level building were either placed on the ground, hidden in openings around the building or near a door entrance. Figure 63 shows the different WGS node placements at various locations around the boundary of the 2-level building. Figure 64 to Figure 66 shows the actual placement of WGS nodes.

CACTF Facility, Camp Roberts, Lat 35.764907 and Lon -120.770062. Image retrieved from Google Earth, June 14, 2017.

Figure 63. Placement of WGS Nodes around the Boundary of the Two-Level Building

Figure 64. Placement of WGS Nodes on Ground and in Openings around the Two-Level Building

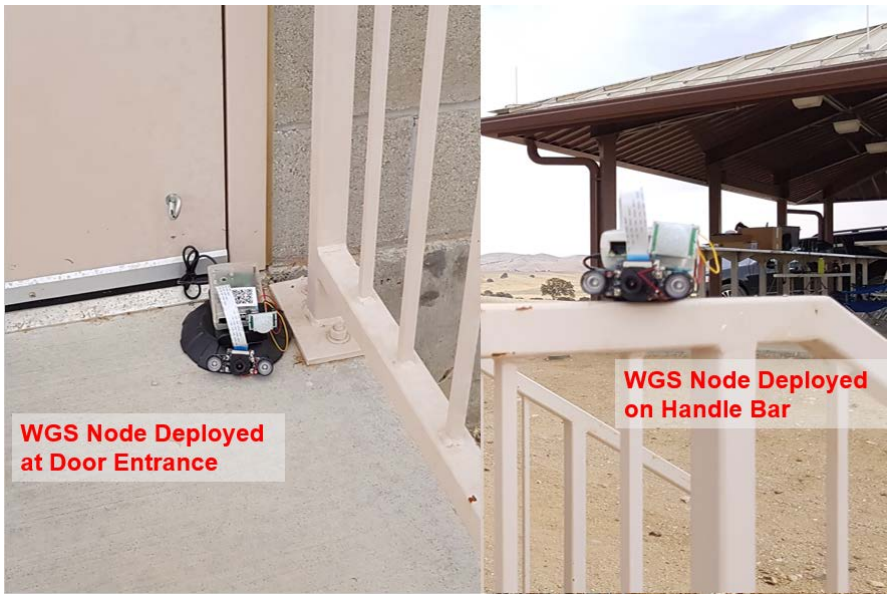


Figure 65. Placement of WGS Nodes at Door Entrance and Stairs Railing around the Two-Level Building

Figure 66. Placement of Google WiFi Mesh Router above the Electrical Distribution Board Mounted on the Lamp Post between the Two-Level Building and the Training Shed

(2) Intrusion Detection Capability of WGS Nodes

In this phase of the field experiment, though the weather was cloudy, the ambient temperature was still about 35 degrees Celsius (95 degrees Fahrenheit). This resulted in PIR sensor being triggered continuously and so the cameras onboard all WGS nodes were always on. All WGS nodes that were deployed on the ground, in openings around the building and at door entrance had been configured with the camera pointing around 30 degrees upwards. Only WGS nodes deployed on stair handrails had their cameras configured as forward facing.

It was discovered that with the camera being configured to be facing upwards, the intruder facial image would usually appear to be dark due to backlight from the sky which affected the facial detection sensitivity of the WGS node and facial recognition capability of the C2 Application Server. Figure 67 and Figure 68 shows the facial image detection capability of the WGS node with camera facing 30 degrees upwards and forward facing respectively.

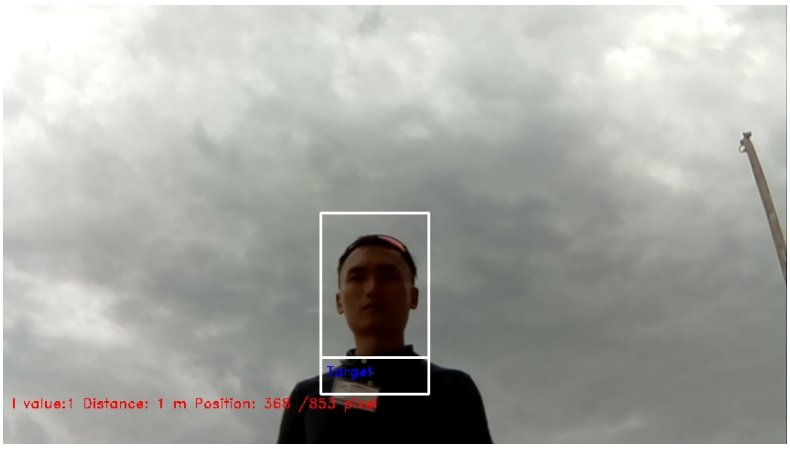


Figure 67. Facial Image Detection Capability of the WGS Node with Camera Facing Upward

Figure 68. Facial Image Detection Capability of the WGS Node with Camera Facing Forward

In cases in which the camera was out-of-focus, under low lighting or strong backlight condition, the WGS node was still able to detect the facial image of the intruder although it may take up to five seconds for the camera to adjust to the lighting condition and detect the facial image as compared to an average of 2 seconds otherwise. Figure 69 shows the facial detection capability of the WGS node under low lighting and an out-of-focus condition. Figure 70 shows facial detection capability of the WGS node under strong backlight condition.

Figure 69. Facial Image Detection Capability of the WGS Node under Low Lighting and Out-of-Focus Condition

Figure 70. Facial Image Detection Capability of the WGS Node under Highly Exposed Lighting Condition

On the day of the experiment, the clouds in the sky also resulted in several false positive triggers of intruder facial detection. Figure 71 shows the false positive of intruder detection being triggered by overhead clouds at the CACTF facility.

Figure 71. A Cloudy Condition Caused False Positive when Camera Was Pointing Upward

(3) Performance of WGSN

WiFi Coverage. Before deploying all WGS nodes, a WiFi coverage test was conducted on-site. Based on the pre-deployment WiFi coverage test, it was validated that the Google WiFi mesh router deployed in the center of the CACTF facility could provide the required WiFi coverage around the 2-Level building and the training shed. However, the WiFi link for WGS nodes deployed at the far corner of the 2-level building, away from the WiFi router, was discovered to be weak and intermittent. Some incoming intruder alerts to the C2 Application Server were also discovered to be delayed by up to ten seconds, especially for those WGS nodes that were deployed further away from the WiFi mesh router. It was assessed to be due to the longer transmission time required to send the same amount of intruder alert information and image over the lower throughput link.

WGS Node Deployment Tool. The WGS Node Deployment Tool worked as expected during this phase of testing. The only limitation identified was the accuracy of WGS node's GPS location as highlighted previously.

WGS Node. The WGS node worked and performed as designed under this phase of testing with several limitations due to WGS node placement on the ground and the camera placement on the WGS node. With camera configured to point upwards at 30

degrees angle, the speed and accuracy of intruder facial image detection capabilities were affected due to dark facial images against strong backlight and false positives from clouds in the sky. The same limitations on PIR sensors and onboard WiFi chipset as observed before also apply here.

C2 Application Server. The C2 Application Server worked and performed as designed during this phase of the field experiment. All intrusion related information and images from multiple WGS nodes were received, processed and stored correctly. All control messages were also sent correctly to all selected WGS nodes. The only weaknesses identified during this phase was the processing delay of incoming intruder alerts when many intrusion alerts were received at the same time from multiple WGS node. Figure 72 illustrates the C2 Application Server showing intruder information and image at CACTF.

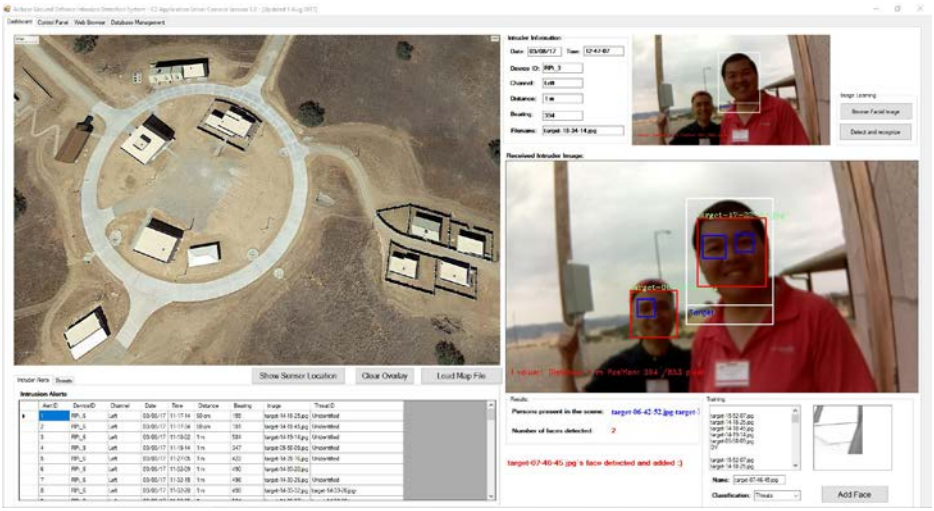


Figure 72. C2 Application Server Showing Intruder Information and Image at CACTF

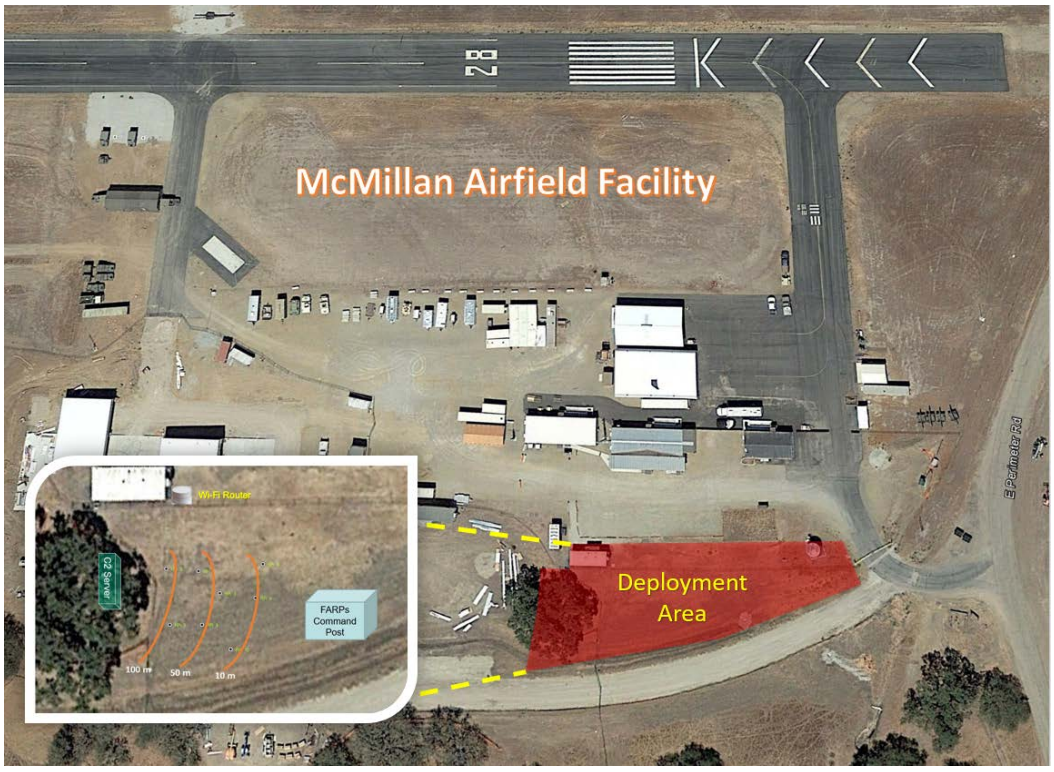
4. Field Experiment 2—System Testing in Open Environment (JIFX McMillan Airfield)

Field Experiment 2 was also conducted at the McMillan airfield during the 17-4 NPS JIFX. The airfield is used by NPS for field testing of any flight-related technologies and systems such as the drones and quadcopters.

In this field experiment, two phases were conducted over two different days with two different WGS node camera deployment configurations. Table 14 shows the details of two phases. Figure 73 shows the satellite view of the McMillan airfield with open field where the two field experiment phases were conducted.

Table 14. Details of Two-Phase System Testing 1

	Phase 1 Field Experiment at McMillan Airfield	**Phase 2 Field Experiment at McMillan Airfield**
Date and Time of Field Experiment	• 31 July 2017 • 1000 to 1600 hours	• 2 August 2017 • 1000 to 1600 hours
Experiment Location	• Open area near the McMillan Airfield	• Open area near the McMillan Airfield
WGS Node Deployment Configuration	• Three layers (simulating defense in-depth) • WGS Node deployed on extendable pole	• Three layers (simulating defense in-depth) • WGS Node deployed in different configuration
WGS Node' Camera Configuration	• Forward facing	• 30 degrees upward facing
Weather Condition	• Sunny	• Cloudy



McMillan Airfield Facility, Camp Roberts, Lat 35.715844 and Lon -120.764225. Image retrieved from Google Earth, June 14, 2017.

Figure 73. Satellite View of McMillian Airfield

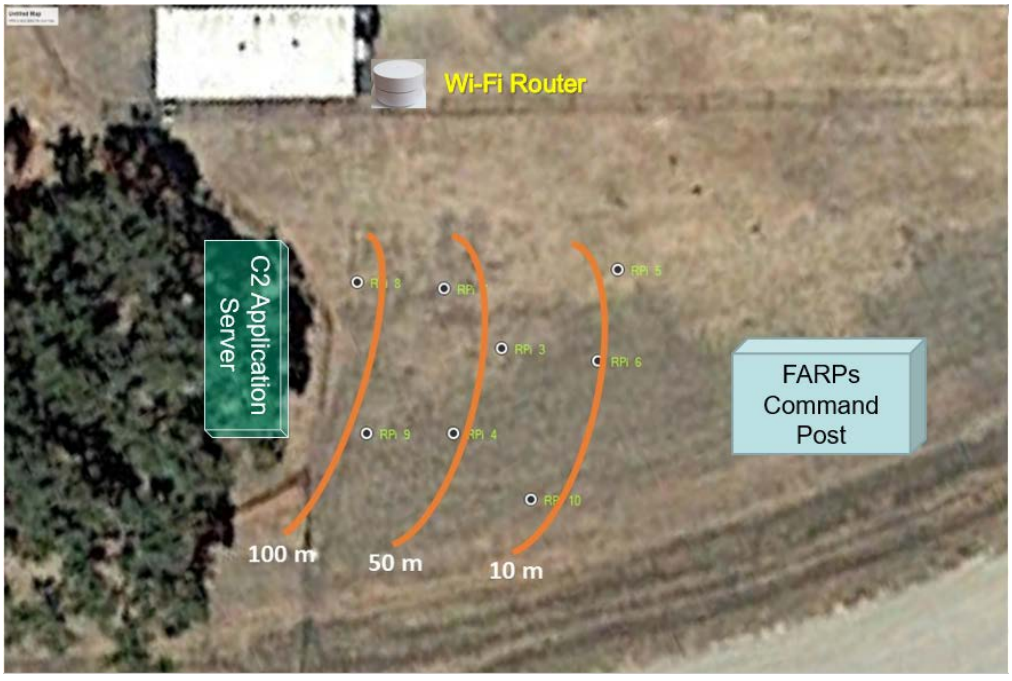
The field experiment conducted in McMillan airfield aimed to validate and evaluate the performance and capability of the WGSN and WGS nodes within an open air base environment.

a. Phase 1 Experiment—WGS Sensor on Extendable Pole

This section documents the first phase of the field experiment at McMillan airfield. It describes the experiment setup within the vicinity, followed by the results on the WGSN and WGS node intrusion detection performance. WGS nodes were deployed on extendable poles and the camera on each of the WGS nodes were configured to be forward facing at around eye-level height.

(1) Experiment Setup

On 31 July 2017 (Day 1 of JIFX event), the WGS nodes were deployed in the open field at the McMillan airfield. The main objective of this test was to evaluate the performance of each WGS node and to determine an intruder's route of advancement based on the detection by the respective WGS nodes. For the intruder's path tracking, the WGS nodes were deployed as three trip-lines as illustrated in Figure 74.



McMillan Airfield Facility, Camp Roberts, Lat 35.715290 and Lon -120.764321. Image retrieved from Google Earth, June 14, 2017.

Figure 74. Field Experiment Setup at McMillan Airfield

Figure 75 shows the C2 Application Server and Video Monitoring Station, displaying real-time intruder information and video streaming from the various WGS nodes deployed within the deployment area as seen previously in Figure 74.

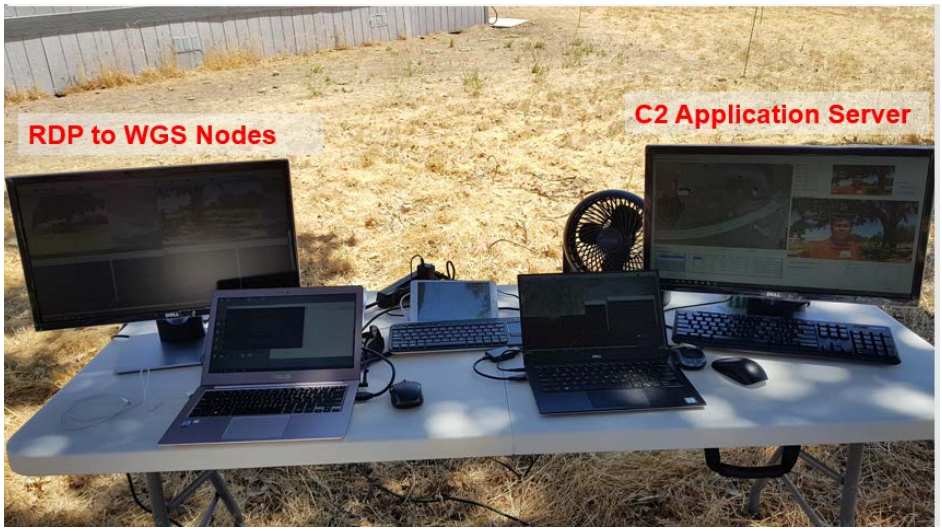


Figure 75. C2 Application Server and Real-Time WGS Node Video Monitoring Station Deployed at McMillan Airfield

The WGS nodes were deployed three to five meters apart from each other in a three trip-line manner to simulate a defense in-depth posture as shown in Figure 76. In this experiment, the cameras are deployed such that detection is done at eye-level height, set up on the extendable poles.

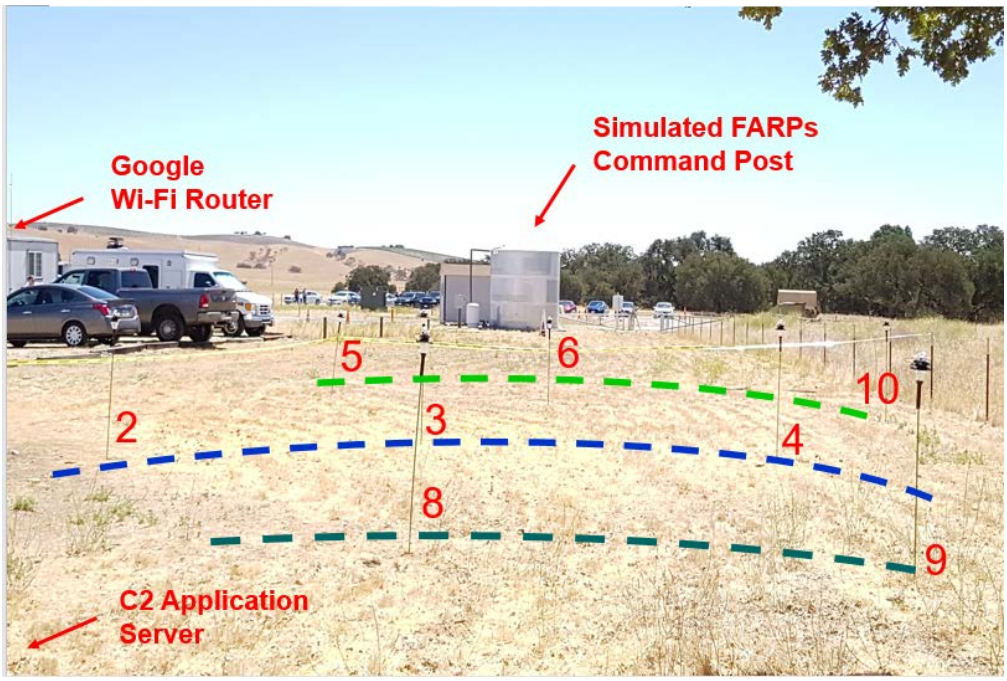


Figure 76. Deployment of WGS Nodes in a Defense-in-Depth Posture

(2) Intrusion Detection Capability of WGS Nodes

In this phase of the field experiment, it was observed that the PIR sensors continuously triggered due to the high ambient temperature of approximately 38 degrees Celsius (100 degrees Fahrenheit). As observed earlier, this caused the on-board camera to be continuously turned on. The position of the sun affected the detection sensitivity and detection time. When the sun illuminated the target from the front, the camera could detect the target's face easily and speedily. Figure 77 shows the OpenCV facial detection algorithm running on RPi_9 WGS node; it could detect the target from approximately two meters away. It was also observed that the WGS node was only able to detect a single target's face while the other intruder, which was approximately 1m behind the front target nearest to RPi_9 WGS node, were not detected by the WGS node. However, once the image was transmitted to the C2 Application Server for the second stage of facial image analysis, detection and recognition, the system was able to detect and recognize both intruders' faces.

Figure 77. Facial Detection Capability on WGS Node

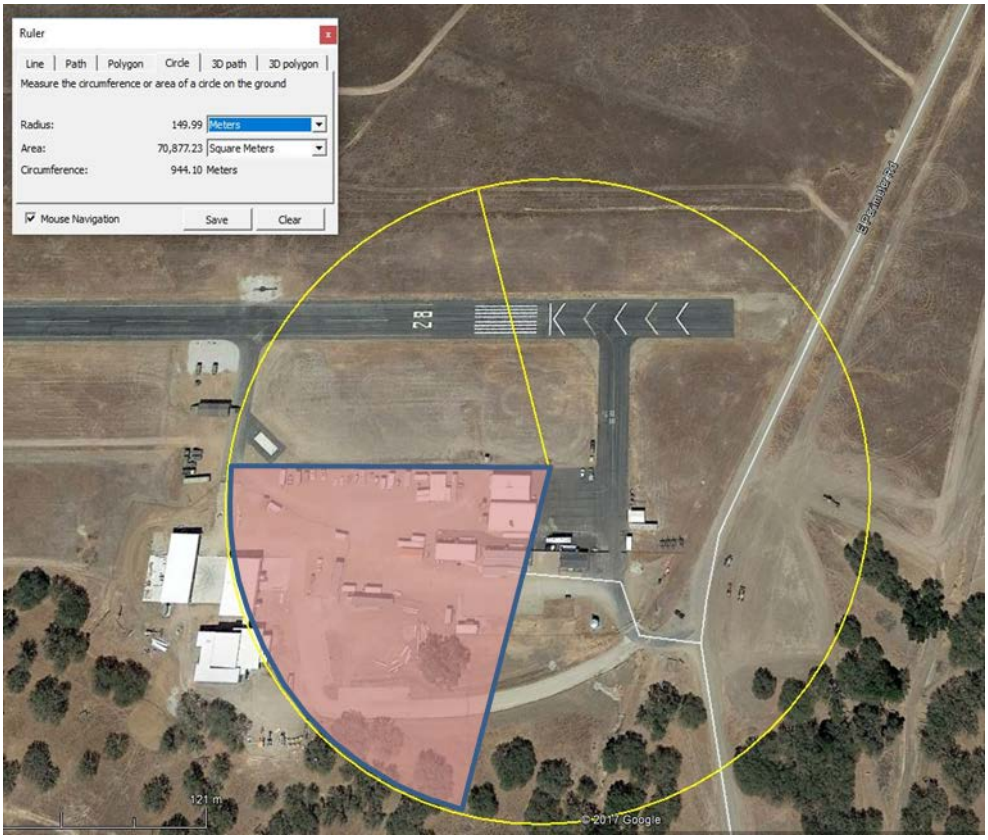
Adjustments were made on the ground to increase the detection range of the WGS. It was observed that by reducing the number of detection pixels from the facial recognition algorithm, we could successfully increase the range of detection by another two meters, raising it to a total of four meters as shown in Figure 78.

Figure 78. Facial Recognition from RPi_8 (left) and RPi_9 (right) WGS Node at 4m Range

(3) Performance of WGSN

Prior to the experiment setup, the coverage of the Google WiFi signal footprint was evaluated. It was observed that the WiFi coverage range can go up to approximately 150m, as shown in Figure 78, with the exception for areas with metal structures, such as

the hangar and containerized offices that caused screening effects and resulted in deteriorated WiFi signals. During the actual testing of the first phase of the experiment, the Google WiFi mesh router was deployed near the WGS nodes as seen previously in Figure 74, as such there were no problem with the WiFi signal reception.



McMillan Airfield Facility, Camp Roberts, Lat 35.715839 and Lon -120.764569. Image retrieved from Google Earth, June 14, 2017.

Figure 79. WiFi Signals Footprint of Google WiFi Router at McMillan Airfield

b. Phase 2 Experiment—WGS Node with Different Configuration

This section documents the second phase of the field experiment at McMillan airfield. It describes the experiment setup within the vicinity, followed by the results of the performance of the WGSN and WGS node detection capability. The various WGS nodes were deployed at various heights to assess and evaluate the performance of the

WGS node based on placement of the WGS node and the placement of camera on the WGS node.

(1) Experiment Setup

On 2 August 2017 (Day 3 of JIFX event), the WGS nodes were deployed at the open field area at the McMillan airfield. The objective of this experiment was to evaluate the WGS nodes performance based on the different heights of the camera placement. Figure 79 shows the WGS nodes deployed at different heights. Like Phase 1 of the field experiment, the WGS nodes are deployed in a three trip-line posture. The first trip-line (closest) is to simulate an intruder walking as he approaches the air base, the second and third trip-lines are to simulate that intruder creeping and leopard-crawling respectively, as he gets closer to the air base. The close-up deployments of the various configurations of cameras on the WGS nodes are shown in Figure 80.

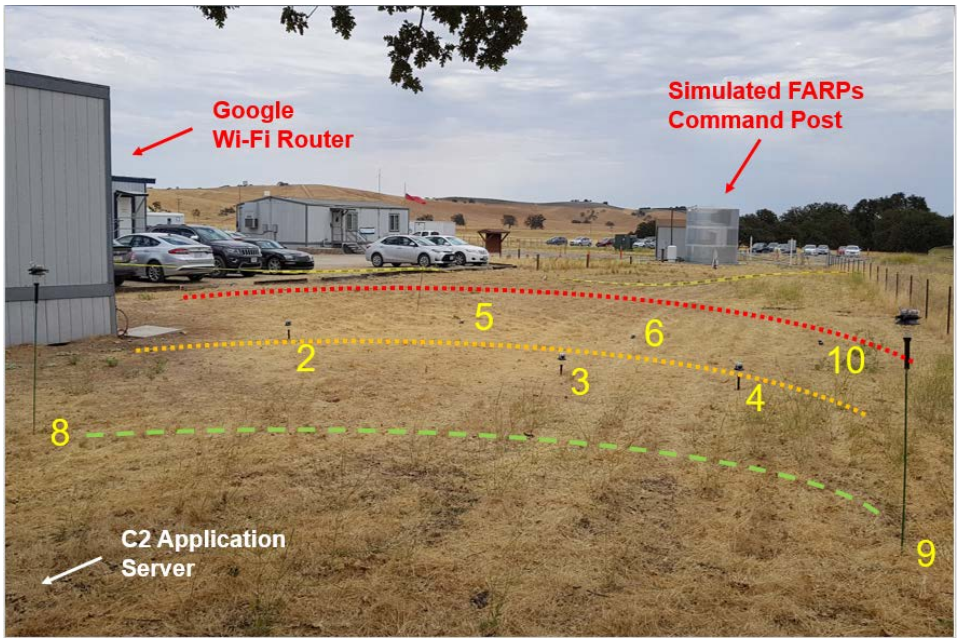


Figure 80. Deployment of WGS Nodes at Various Heights

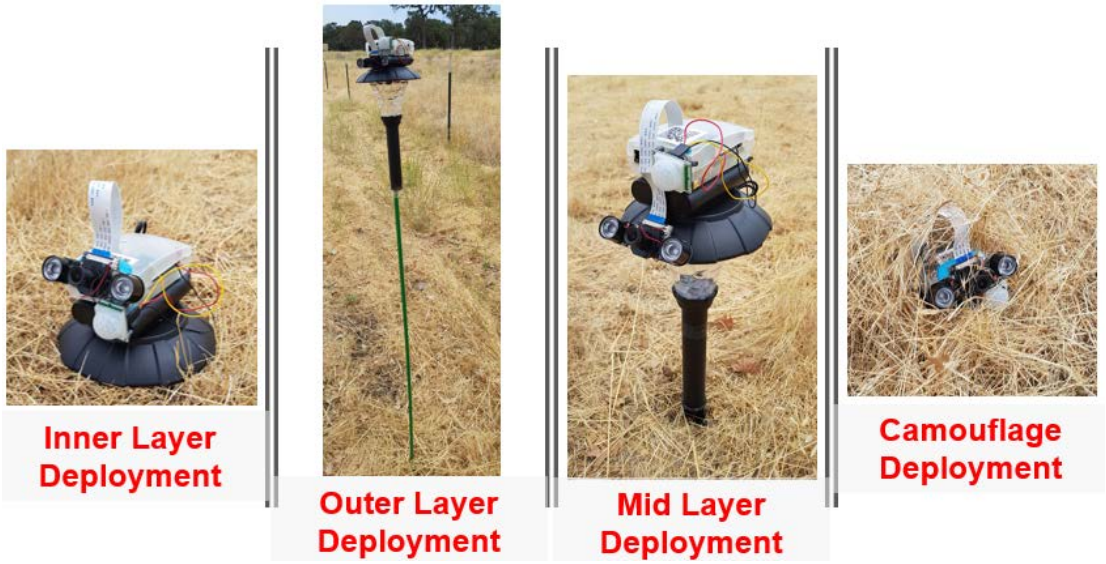


Figure 81. Variance of Camera Configurations

(2) Intrusion Detection Capability of WGS Nodes

In this phase of the field experiment, the PIR sensors continuously triggered due to the high ambient temperature of approximately 38 degrees Celsius (100 degrees Fahrenheit). This too, caused the on-board camera to be continuously turned on. We also observed that the position of the sun affected the performance of the intruder facial image detection time. One key observation was when the WGS nodes are placed on the ground with its camera pointing towards the sky at a 30-degree angle. Due to the strong backlight from the sky, it took between two to four seconds, depending on the intensity of the backlight, to detect a target's face as compared to camera deployed at eye-level. This was caused by the sunlight casting over the target, causing the silhouette effect and making the target harder or impossible to be detected, as shown in Figure 81. This also caused the WGS node to detect many false positives, which must be manually filtered by the operator at the C2 Application Server. From this experiment, it was discovered that the placement of cameras during the deployment is important as it determines the sensor effectiveness and the WGS node's ability to detect a human intruder.

Figure 82. Overcast of Strong Backlight Causing Silhouette Effect and False Positives

(3) Performance of WGSN

Like the first phase of the field experiment, there was no observed problem about the reception of the router's signals strength. The C2 Application Server could plot the path taken by a particular intruder based on correlation of a series of intruder alerts and images picked up by the respective WGS nodes. The C2 Application could present the intruder information and an image of the intruder correctly and timely. With the correlated list of intruder events, a graphical representation of the intruder's path is automatically determined and displayed in the C2 Application as shown in Figure 82.

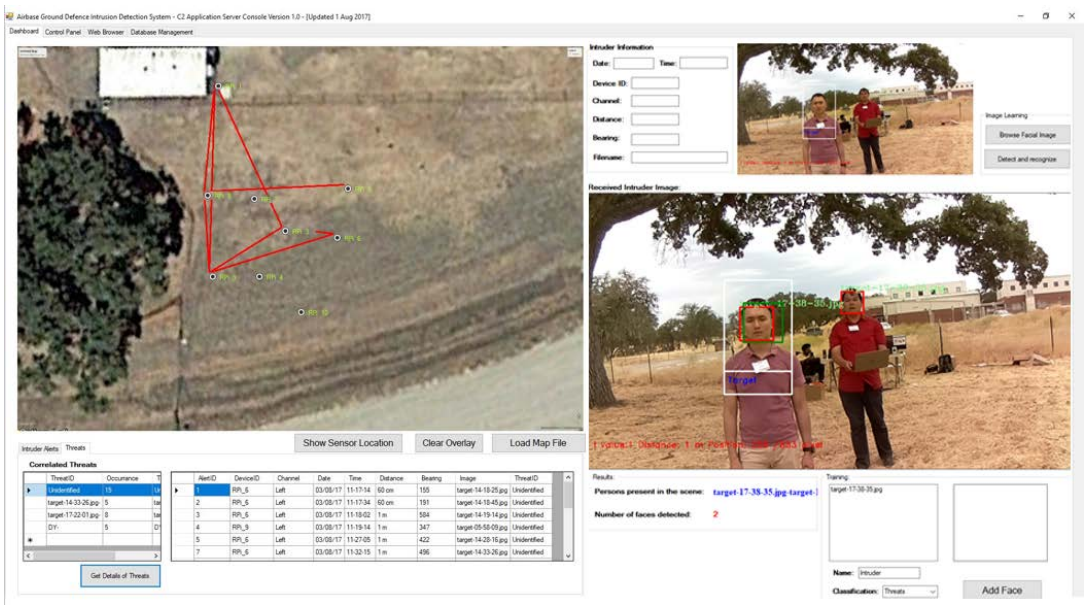


Figure 83. Intruder's Route of Advancement as Displayed on the C2 Application

C. CHAPTER SUMMARY

This chapter describes the physical construction of both variants of WGS node. The different system testing and field experiments, conducted at different locations with different environments and with different sensor configurations and placements, revealed that each sub-system under the WGSN worked as expected and could interoperate seamlessly to achieve the objective of providing early intrusion detection for operators situated at the command post where the C2 Application Server was located. The system offered more than just early intrusion detection by providing features like human intruder facial detection and human facial recognition using low-cost COTS-based components that contribute to a unit cost of less than USD $100 per WGS node. Simple data analytics coupled with a distributed database implemented across the whole WGSN system, including the WGS nodes, allows intelligent features like showing intruder movement waypoints, generating intruder watchlist alerts and post-event retrieval of high resolution intruder images.

Through the various field experiments conducted under different weather conditions and WGS node configurations, several performance limitations with regard to the PIR sensor and cameras installed on the WGS nodes were also discovered. These findings suggest additional sensors, like laser obstacle detection sensors that are less affected by ambient temperature, should be used as secondary sensors on the WGS nodes and that the placement of the camera on the WGS node should be either forward or downward facing. The camera could also be mounted on a small servo-motor that can allow the WGS node to dynamically adjust the camera facing in accordance to the sun position and possible intruder approach direction.

In conclusion, it was assessed through the different field experiments conducted during 17-4 NPS JIFX event at Camp Roberts that the WGSN and WGS nodes work under different field environments and conditions with some limitations on the detection sensitivity of the existing sensors. It was demonstrated that the concept of using low-cost COTS components to build an alternative low-cost wireless ground sensor node that is under USD $100 was achievable and could even deliver enhanced capability, like intruder facial detection and recognition, at that price point.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS

A. SUMMARY

This research investigated the use of a network of low-cost IoT devices to provide early warning capability to enhance perimeter defense of a FARP. The concept of building a WGSN and sending information back to the C2 server to perform image analytics for identifying intruders was investigated. By providing an automated means of surveillance, it demonstrated the potential for reducing manpower required for patrolling secluded areas around the perimeter of a FARP. We demonstrated that IoT devices provide much potential in military applications. The Raspberry Pi-based system is able to easily support many other sensors. It was identified that in high ambient temperature environments, the PIR sensors were not ideal as they were perpetually turned on.

Our research considered the backend communication infrastructure and its power requirements when deployed in an outdoor environment. The 802.11g/n WiFi was selected to provide communications between the WGS and the C2 server after considering a few other possible means of communications. The Google WiFi was specifically chosen as it not only provides WiFi communication, it is also able to be configured to operate in a meshed network. Additionally, it can be powered by an external power bank through the USB type C connection.

The system technology demonstrator was validated through a series of tests. The first was component and subsystem testing, which was carried out at NPS. The objective of this test was to measure the performance of each sensor component and observe how they measured against the technical specifications. The second test was to evaluate the sensors in a simulated field environment and examine how these sensors perform in the envisaged operational environment. We tested the sensors in two different environments, namely McMillan airfield and CACTF, Camp Roberts at San Miguel, California.

B. PERFORMANCE

Throughout the research, we experimented and found different ways to optimize the sensor system that we built. We tried and trialed different sensors such as employing the use of web cameras and the Raspberry Pi's camera modules. We found that by adjusting the different parameters of the facial recognition software, we could achieve improved recognition and correlation results. Our research also documented methods that work and others that did not work throughout the experimentation phases.

Testing our implementation in an operational environment helped us to further understand environmental impacts and pay attention to details that we did not observe during the localized test. One such example was the performance of the PIR sensors in high ambient temperatures. When we initially tested the node implementation at NPS and under Monterey's consistently lower temperature conditions, we did not encounter the high heat problem until we deployed the system at Camp Roberts, where the temperature may be much higher during the summer day.

C. RECOMMENDATIONS FOR FUTURE WORK

The recommendations for possible future work are describe in this section. The two recommendations are exploration of alternate sensor node configurations based on the operating environment, and use of other IoT devices or processors. In this field experiment, we examined the use of Raspberry Pi; other processors, like Odroid, may also be explored as an alternative.

1. Alternate Sensor Node Configurations

Our research found that the PIR sensors used during JIFX were not ideal for use in the high ambient temperature of outdoor environment. We propose future work to consider use of higher quality sensors meant for outdoor deployment, or explore use of other sensors to detect motion before turning on the camera to save on the power consumption of each WGS. Other sensors that may be considered include acoustic sensors to trigger the camera. Sensor combinations, such as Light Detection and Ranging (LiDAR) used in conjunction with PIR sensors, where each sensor complements the

others may help reduce false positive detections. Higher resolution wireless cameras may also be employed to capture greater details of detected intruders so that these can be sent to the C2 server for further analysis.

2. Use of Other Processors

Apart from Raspberry Pi, future research may also look into other low-cost, low-powered processors such as the Odroid, which is very popular among the UAV community as this processor comes with a dedicated graphics processor which may be useful for intensive image processing. Inter-node mesh communications may also be built over the Bluetooth connection to establish a Bluetooth Personal Area Network (PAN) or over another WiFi network using an additional external WiFi adapter to facilitate passing of intruder information to neighboring nodes so that those neighboring nodes will be able to transit into an alert state whereby their cameras can be triggered to look for the intruder even before any of its onboard sensors like PIR sensors detect any motion or intrusion, thus reducing the observed delay between detection and image capture.

With careful planning, implementation, and testing, the WGSN may change the concept of operations for perimeter protection of a FARP, where we leverage technology to help us become more efficient and effective in the effort required.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Amazon. (n.d.). WT901C JY901 inclinometer 232 version MPU9250 module angle output 9-axis accelerometer gyroscope. Retrieved July 2, 2017, from https://www.amazon.com/inclinometer-version-MPU9250-Accelerometer-Gyroscope/dp/B01MRIWZL1/ref=sr_1_1?ie=UTF8&qid=1502061076&sr=8-1&keywords=jy901

Cox Construction. (n.d.). Cox Construction Co. Project Combined Arms Collective Training Facility Camp Roberts. Retrieved August 25, 2017, from http://www.coxconstructionco.com/project-camp-roberts.htm

Davis, R. D. (2014). Forward arming and refueling points for fighter aircraft: Power projection in an antiaccess environment. *Air and Space Power Journal*, *28*(5), 5–18.

Delaney, J. R. (2016a). Google Wifi. Retrieved August 10, 2017, from https://www.pcmag.com/review/350076/google-wifi

Delaney, J. R. (2016b, September). Ubiquiti Amplifi HD Home Wi-Fi System. Retrieved August 10, 2017, from https://www.pcmag.com/review/347914/ubiquiti-amplifi-hd-home-wi-fi-system

Delaney, J. R.. (2017a, September 8). The best Wi-Fi mesh network systems of 2017. Retrieved from https://www.pcmag.com/roundup/350795/the-best-wi-fi-mesh-network-systems#

Delaney, J. R. (2017b, July). Eero (2nd generation). Retrieved August 10, 2017, from https://www.pcmag.com/review/355034/eero-2nd-generation

Delaney, J. R. (2017c, May). TP-Link Deco M5 Wi-Fi System. Retrieved August 10, 2017, from https://www.pcmag.com/review/353876/tp-link-deco-m5-wi-fi-system

Department of Defense Chief Information Officer. (2016). *DOD policy recommendations for the Internet of Things (IoT)*. Washington, DC: Department of Defense.

Exensor. (n.d.). Exensor UMRA Mini Sensor. Retrieved August 10, 2017, from http://www.exensor.com/product-category/

Gartner. (2016). Gartner's 2016 hype identifies three key trends that organizations must track to gain competitive advantage. Retrieved July 27, 2017, from http://www.gartner.com/newsroom/id/3412017

GlobalSat. (n.d.). GPS receiver. Retrieved August 10, 2017, from http://www.globalsat.com.tw/style/Frame/m5/product_detail.asp?customer_id=909&lang=2&content_set=color_2&name_id=51263&Directory_ID=30784&id=199952

Google. (n.d.). Google WiFi. Retrieved August 10, 2017, from https://madeby.google.com/wifi/specs/

Hempenius, K. A., Wilson, R. A., Kumar, M. J., Hosseini, N., Cordovez, M. E., & Sherriff, M. S. (2012). A more cost-effective unattended ground sensor using commercial off-the-shelf products. In *2012 IEEE Systems and Information Engineering Design Symposium*, 62–67. https://doi.org/10.1109/SIEDS.2012.6215148

Ivask, C.-M. (2015, June). *Raspberry Pi based system for visual object detection and tracking* (Bachelor's thesis). Retrieved from http://a-lab.ee/edu/theses/defended/984

Kent, S. D. (2015). *Wireless sensor buoys for perimeter security of military vessels and seabases* (Master's thesis). Retrieved from https://calhoun.nps.edu/handle/10945/47982

Logitech. (n.d.). HD Webcam C270 specifications. Retrieved August 10, 2017, from http://support.logitech.com/en_us/product/hd-webcam-c270/specs

Marlin P. Jones & Assoc. Inc. (n.d.). HC-SR501 PIR motion detector. Retrieved August 10, 2017, from https://www.mpja.com/download/31227sc.pdf

Matt. (2014, October). How to use wavemon to monitor your WiFi connection. Retrieved August 25, 2017, from http://www.raspberrypi-spy.co.uk/2014/10/how-to-use-wavemon-to-monitor-your-wifi-connection/

OpenCV. (n.d.). OpenCV library. Retrieved August 10, 2017, from http://opencv.org/

Palm, B. C. (2014, September). *Mobile Situational Awareness Tool: Unattended ground sensor-based remote surveillance system* (Master's thesis). Retrieved from https://calhoun.nps.edu/handle/10945/43971

PDP Projects. (2015, September). Rapid deployment perimeter security. Retrieved August 10, 2017, from http://www.pdpprojects.co.uk/services/physical-security/force-protection/

Purser, W. (1989). *Air base ground defense: An historical perspective and vision for the 1990s*. Retrieved from http://www.dtic.mil/docs/citations/ADA217294

Raspbery Pi. (n.d.). Raspberry Pi 3 Model B. Retrieved August 10, 2017, from https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

RobotShop. (n.d.). LIDAR-Lite 3 Laser Rangefinder. Retrieved August 10, 2017, from http://www.robotshop.com/en/lidar-lite-3-laser-rangefinder.html

Sheela, S., Shivaram, K. R., Chaitra, U., Kshama, P., Sneha, K. G., & Supriya, K. S. (2016). Low cost alert system for monitoring the wildlife from entering the human populated areas using IOT devices. *International Journal of Innovative Research in Science, Engineering and Technology*, *5*(10), 128–132.

Sims, T. E. (2012). *Wireless sensor node data gathering and location mapping*. Retrieved from https://calhoun.nps.edu/handle/10945/6869

Tingle, M. E. (2005, March). *Performance evaluation of a prototyped wireless ground sensor networks* (Master's thesis). Retrieved from http://calhoun.nps.edu/handle/10945/2263

Waveshare. (n.d.). RPi IR-CUT Camera, Raspberry Pi Camera Module, embedded IR-CUT, supports night vision. Retrieved August 10, 2017, from http://www.waveshare.com/rpi-ir-cut-camera.htm

Williford, B. J. (2012, March). *Mobile phones coupled with remote sensors for surveillance* (Master's thesis). Retrieved from https://calhoun.nps.edu/handle/10945/6887

Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. *International Journal of Communication Systems*, *25*(9), 1101–1102.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California