NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SCALABILITY AND ROBUSTNESS TESTING OF IOT NETWORKS USING LEACH PROTOCOL SIMULATION

by

Christopher L. Henson

March 2018

Thesis Advisor: Gurminder Singh
Second Reader: Steven J. Iatrou

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE SCALABILITY AND ROBUSTNESS TESTING OF IOT NETWORKS USING LEACH PROTOCOL SIMULATION			**5. FUNDING NUMBERS**
6. AUTHOR(S) Christopher L. Henson			
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** A

13. ABSTRACT (maximum 200 words)

The Navy's new Distributed Lethality strategy will require an extensive sensor network to support increased information requirements. Wireless sensor networks (WSN) for Intelligence, surveillance and reconnaissance (ISR) support offer a means to gather this information, and commercial-off-the-shelf (COTS) solutions offer an economical option for the required WSN components. Through computer simulation using the LEACH protocol and Raspberry Pi 3 Model B (RPi) parameters as the sensor nodes, this research explored the technical feasibility of using COTS technologies to implement a low-cost WSN. Simulations were designed to measure the number of rounds for RPi node death to compare performance against the current WSN structure using micro-sensor (MS) nodes. Measurements were taken from the RPi in transmit and receive modes to represent the joule/bit rate for energy used by RPi nodes in the simulation. Modified parameters were the percentage of nodes serving as cluster-head (CH), initial power for each node, number of nodes, and packet size from CH-to-base station. The results showed that adjustments to the Clusterhead-to base station packet size and the initial node power provided results where the RPi's robustness and scalability capabilities equaled or exceeded the performance of the current micro-sensor networks.

14. SUBJECT TERMS wireless sensor networks; internet-of-things; intelligence, surveillance and reconnaissance, LEACH protocol			**15. NUMBER OF PAGES** 85
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

SCALABILITY AND ROBUSTNESS TESTING OF IOT NETWORKS USING LEACH PROTOCOL SIMULATION

Christopher L. Henson
Lieutenant, United States Navy
B.S., Trident University International, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN NETWORK OPERATIONS AND TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
March 2018

Approved by: Gurminder Singh, Ph.D.
Thesis Advisor

Steven J. Iatrou
Second Reader

Dan Boger, Ph.D.
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Navy's new Distributed Lethality strategy will require an extensive sensor network to support increased information requirements. Wireless sensor networks (WSN) for Intelligence, surveillance and reconnaissance (ISR) support offer a means to gather this information, and commercial-off-the-shelf (COTS) solutions offer an economical option for the required WSN components. Through computer simulation using the LEACH protocol and Raspberry Pi 3 Model B (RPi) parameters as the sensor nodes, this research explored the technical feasibility of using COTS technologies to implement a low-cost WSN. Simulations were designed to measure the number of rounds for RPi node death to compare performance against the current WSN structure using micro-sensor (MS) nodes. Measurements were taken from the RPi in transmit and receive modes to represent the joule/bit rate for energy used by RPi nodes in the simulation. Modified parameters were the percentage of nodes serving as cluster-head (CH), initial power for each node, number of nodes, and packet size from CH-to-base station. The results showed that adjustments to the Clusterhead-to base station packet size and the initial node power provided results where the RPi's robustness and scalability capabilities equaled or exceeded the performance of the current micro-sensor networks.

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

ADV	advertisement message
BATMAN	better approach to mobile ad-hoc networking
CH	cluster-head
COTS	commercial-off-the-shelf
CSMA	carrier-sense multiple access
BBB	BeagleBone Black
BLE	Bluetooth Low Energy
bit/s	bits per second
BS	base station
DTN	disruption or delay tolerant network
EW	electronic warfare
GUI	graphical user interface
IoT	Internet of things
ISR	intelligence, surveillance and reconnaissance
KPI	key performance indicators
LEACH	Low-Energy Adaptive Clustering Hierarchy
M2M	Machine to Machine
mAh	Milliampere-hour
MANET	mobile ad-hoc network
MQTT	message queue telemetry transport
MS	micro-sensor
OS	operating system
QoS	quality of service
RF	Radio frequency
RFID	Radio-Frequency Identification
RPi	Raspberry Pi 3 Model B
RPiZ	Raspberry Pi Zero W
WSN	wireless sensor network
SOA	Service Oriented Architecture
TDMA	time-division multiple-access

UGS	unattended ground sensors
UNO	Arduino UNO Wifi
V	voltage

ACKNOWLEDGMENTS

To my advisors, thank you for all of the assistance, and for the countless copious hours spent reviewing and critiquing this paper.

To my amazing wife, thank you for your patience and understanding. I never would have been able to finish this thesis without you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MOTIVATION

The U.S. Navy's employment of large-scale maritime Intelligence, Surveillance, and Reconnaissance (ISR) sensor networks in a littoral environment is severely limited by fiscal and logistical constraints that prevent the effective deployment of the sensors currently available for littoral operations. Current configurations for unattended maritime sensor networks include complexity of design; intensive resources for deployment and retrieval mechanisms; complicated data methods; limited availability; and costs. The limited node structure of existing maritime sensor networks composed of costly, complicated data collection equipment using complicated communication channels severely limits the ISR capabilities in littoral operations. Current options for sensor networks for the maritime environment are limited to the options of sonobuoy fields, with a cost of over $1300 dollars per unit from Erapsco alone. The need for maritime sensor networks has been the topic of recent studies, such as *In-Network Processing on Low-Cost IoT Nodes for Maritime Surveillance* (Belding, 2016), with an exploration for a variety of persistent deployment options, and the use of commercial-off-the-shelf (COTS) Internet of Things (IoT) devices presents a low-cost viable alternative for sensor development. Emerging small form-factor devices, such as Raspberry Pi 3 Model B (RPi), offer devices capable of forming large scale self-organizing networks. Low-cost sensors interfaced with small form-factor computing and communication devices provide flexibility in node design. However, the increase in node count causes concern for the amount of network traffic generated by node activity. This study will look at robustness and scalability performance in a wireless sensor network (WSN) within a littoral ISR network.

B. OBJECTIVE

This thesis researches the parameters for optimal simulated network performance in a large-scale maritime ISR sensor network comprised of COTS IoT sensor platforms. Network simulation will provide the scalability and flexibility necessary to determine the feasibility of the IoT platform for ISR sensor networks. With the flexibility provided by

simulations additional determinations may be possible for the optimal network architecture to manage large-scale ISR sensor networks, based on the IoT platform.

C. THESIS STRUCTURE

This thesis explores the application of large-scale IoT networks as a source for littoral sensor networks. Chapter II provides facts bearing on the problem so that the reader can understand the significance of the problem and expansion of previous research which includes the tactical uses of maritime ISR sensor networks; sensor capabilities currently in use; overview of COTS components; and capability gaps that can be filled by wireless sensor networks. Chapter III provides the design and implementation details of components selected, development of system architecture, protocol selection, and characteristics of nodes. Chapter IV focuses on the problem exploration and provides an overview of the testing environment and actual test results. Chapter V concludes the thesis and provides remarks about the problem solution recommended, with clear guidance on areas of the problem space not addressed by the thesis in sufficient detail to allow follow-on thesis exploration.

II. LITERATURE REVIEW AND BACKGROUND

> What we need to do is distribute the lethality of our Navy and make all of our Navy more lethal, not just surface ships but surface ships, submarines and aircraft across the broad spectrum that we operate.
>
> —Vice Admiral Thomas Rowden
> Commander, Naval Surface Forces, 2016

A. PROBLEM DOMAIN

The Navy is seeing a force shift that presents new challenges. CNO Admiral Richardson pointed out that "the scope and complexity of the challenges we face demand a different approach than that offered by a classic campaign" (Richardson, 2016). Potential challenges for force components will require new means of developing warfighting capabilities. The Surface Force strategy of Distributed Lethality outlines the concept for meeting the need for collaboration and integration across warfighting domains through innovation to employ naval combat power in any anti-access/area-denial (A2/AD) environment (Rowden, Gumataotao, & Fanta, 2015). As the Navy decentralizes activities the need to support the strategy of surface forces will require increased capabilities for a competitive edge.

1. Maritime Domain Awareness

The need for expanded capabilities of surface forces does not mean that focus should be placed squarely on developing defensive resources. The application of technology to meet new strategy requirements provides an opportunity for innovation in intelligence, surveillance and reconnaissance (ISR) to provide Maritime Domain Awareness (MDA). MDA focuses on the security, safety, economy, or environment of the maritime domain (White, 2014). The Secretary of the Navy's office responsible for MDA is the Executive Agent for Maritime Domain Awareness (EAMDA). The EAMDA has determined that effective MDA provides early identification of threats to enhance appropriate response; requires the capability to integrate different sources of intelligence; and is heavily dependent on information sharing (White, 2014). Although systems like

Automatic Identification System (AIS) are currently in place, the implementation of new ISR resources will provide increased capabilities for MDA.

2. Historical Precedent

The development of unmanned systems started as early as 1917 when Unmanned Aerial Systems (UAS) were tested in World War I, using balloons to provide adjustment for indirect fires (Blom, 2010). By the time of the Vietnam War, the United States was employing UAS such as the AQM-34 Firebee for combat purposes (Gertler, 2012). Gertler (2012) pointed out the main advantages of UAS, which are the elimination of the risk to life and removal of the endurance limitations of crewed aircraft. UAS could be used to perform the dull, dirty, and dangerous missions that do not require a human pilot.

DOD leadership understands that unmanned systems provide enhanced battlefield capabilities in the three operational domains of air, ground and maritime (DOD, 2012). Utilization of UAS has steadily grown, with uses branching out from the typical ISR mission to varied applications (Gertler, 2012). Drawdown in manned aircraft dropped from 95% of inventory to 59% in 2012. ScanEagle has been in use by the Marine Corp since 2004, and by the Navy since 2005.

There are some issues with UAS that present some concern. First is the slow advancement of interoperability with humans, which complicates mission effectiveness, since systems are operating without common interface components (Gertler, 2012). Duplication of platforms for different programs causes additional cost for operations. The GAO pointed out that even as systems achieve commonality in airframe structures, ineffective collaboration inhibit commonality in the subsystems and payloads used by different organizations (Gertler, 2012). Looking at the current domains of operation, the value of UAS offers insight into potential requirements of ISR solutions that can meet the Fleet's needs for distributed lethality.

3. Lessons from Commercial Industry

Gartner, Inc. identified 236 emerging technologies, such as IoT, between 2003 and 2015; the rate of adoption can have huge implications for the entities that engage emerging

technologies (Stratopoulos, 2016). Understanding trends of emerging technologies is important to avoid influence of bad hype that often accompanies developing technologies. The Hype Cycle developed by Gartner Inc. offers a representation of maturity, adoption, and application of technologies (Stratopoulos, 2016). Stratopoulos (2016) identified three conditions that equate to the commencement point for new technologies: a public signal indicates technology is available for adoption; the technology provides a source of competitive advantage; and its inherent capabilities provide a technological advantage. Technology capabilities are important when determining the level of risk that will be assumed to implement a new technology in order to benefit from relative competitive advantage provided.

As technology continues to expand and new areas of competitive edge are developed, it is important to remember that delays in implementation can create gaps. Becker (2016) pointed out that the Navy's advantage could erode as adversaries start to implement and exploit modern technologies at a faster rate than the DOD. Aside from the competitive advantage, it is equally important for the technology owner to understand technologies may not provide benefit independently and will need complementary systems for support. Meddeb (2016) gave an example of the big data, cloud computing, and sensor network paradigms, where the removal of one component makes the system useless. Meddeb (2016) pointed out that if you set up a sensor network, but do not process the big data, the sensed data are worthless. Understanding the relationship between technologies for effective implementation is important when looking to commercial technologies as potential solutions for technology gaps. One area of commercial technology growth has come in development of mobile devices for communication solutions.

The proliferation of mobile devices, such as smart phones, in everyday life has been staggering. The total number of mobile devices worldwide is expected to reach 4.93 billion in 2018 (Statista, n.d.). The explosion of mobile technology brings the concept of large-scale distributed computing into mainstream focus and demonstrates a potential for the military application of IoT technologies. Ray (2016) described IoT as connecting the digital and physical world and that Gartner expects 25 billion devices connected by 2020. With

the growth of mobile devices, the DOD will need to have acquisition procedures in place to support the requirements for IoT programs.

The military acquisition process could impede implementation of new technologies, as Arellano, Pringle, and Sowell (2015) stated the DOD is in desperate need of a rapid acquisition process that is responsive to critical needs of the warfighter in the approval of new technologies. The disparity between the growth of IoT technology and the trend of elongated DOD acquisition systems demonstrate the critical changes needed for advancing new technologies.

Combining the ISR data from multiple sources offers the Navy an increased battle space awareness; IoT presents an opportunity to fill potential science and technology gaps for advanced sensing requirements (Becker, 2014). The employment of sensor networks in the field bringing new sources of ISR information from littoral settings for tactical decision making. Employing IoT will require new practices for information management and utilization, but provide leaders information sources to support current and future operational environments.

B. CURRENT USES AND APPLICATIONS FOR SENSOR NETWORKS

The use of unattended sensors in the maritime domain can provide increased battle space awareness by improving sensing capabilities and expanding utility of wireless sensor networks (WSN). Sensor networks provide a means of collecting ISR information for static and dynamic applications that can exploit multiple types of captured signals that can be used to meet the tactical requirements of the environment. The following sections discuss current uses of sensor networks in various domains.

1. Intelligence, Surveillance, and Reconnaissance (ISR)

The use of unattended sensor networks for ISR is a concept that has existed in many different forms which can include environmental monitoring, communication relays, and sound detection. The expansion of battle space communication networks has expanded the capabilities for meeting ISR requirements to obtain mission objectives. The benefit of the

WSN is that networks can be used to target different sources of information to support battle space decisions.

Under ISR, diversity of intelligence sources can include communications intelligence (COMINT) which covers the collection of information from electromagnetic sources, and electronic intelligence (ELINT) which can include operational (OPELINT) or technical (TECHELINT), and intelligence collected from foreign sources, (Dempsey, 2013). Diversity of sources provides information to the commander in the field that aid in persistent surveillance of the environment for an accurate picture, which is necessary for timely decision making (Scott, 2017). For successful ISR the diverse intelligence collection resources are necessary to support the global battle space.

2. Cyber Effects

In planning for Cyberspace Operations (CO) sensor networks can provide a component that offers information for timely and informed decision making. As part of the common operational picture (COP), the use of global sensor networks can provide a reliable picture of the battle space to differentiate between friendly, neutral and adversarial forces and outline locations and activities (Scaparrotti, 2013). This time sensitive capability allows for the targeting and identification of suitable strike assets providing a rapid response and increased situational awareness (Scaparrotti, 2013). Cyber effects will provide monitoring that will greatly enhance decision making for defensive and offensive situations in multi-domain environments.

3. Electronic Warfare

In Electronic Warfare (EW) the Electromagnetic Spectrum (EMS) plays an important role in the modern military. Sensor networks integrate into the planning process under Electronic Warfare Support (ES) to reduce uncertainty in decision making for the battle space (Gortney, 2012). Within Electromagnetic Battle Management (EMBM) unattended sensor networks allow for dynamic monitoring to provide information valuable to the battle commander. When dealing with the electromagnetic (EM) emissions considerations need to be made for the following regarding sensor networks. First is detection by the enemy of EM emissions from networks which can display characteristics

valuable to the adversary if not managed correctly. Deception can be done directly through sensors and is important in attacking the enemy's decision loop (Gortney, 2012). Destruction becomes a key concern for sensor networks in the battle space, removing the ability to monitor the environment and make effective decisions. Protection from degradation by EW is also an important management aspect for sensor networks that requires preventive measures (Gortney, 2012). It is important that EW requirements are managed and observed to maximize the effective use of sensor networks.

4. Meteorological Study

Unattended sensor networks offer great value in the field of meteorological survey on a global scale. The National Oceanic and Atmospheric Administration (NOAA) (2011), identified weather systems and patterns, for example, air masses create patterns that include fronts, jet streams, and the Coriolis effect have global impact. Monitoring these systems as they move through various stages greatly benefit from the use of large-scale wireless sensor networks (WSN) in maritime and other domains.

C. CURRENT SYSTEM CHARACTERISTICS

Sensor nodes have had various modalities and networks application for years, ranging from the use of unattended ground sensors (UGS) in Vietnam for target acquisition (Kent, 2015) to coastal marine monitoring (Albaladejo, Fulgencio, Torres, Sanchez, & Lopez, 2012). Haider (1998) pointed out that real-time sensor networks can provide information at the granular level to provide detailed information for defensive and offensive operations. IoT can act as a bridge for WSN that provides a standard that can be used for the development of devices of reduced size and improve power-efficiency.

Wireless sensor network architecture consists of two categories; first is the components for creation and control of wireless network systems; this thesis will focus on this area looking at scalability and robustness for sensor networks. The second category is forms of sensor modality, which can range from presence/intrusion; Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE); imaging; and noise detection, and the variation in sensory data can offer a wide range of configurations for measurement systems

that are necessary to provide a picture of the battle space (Đurišić, Tafa, Dimić, & Milutinović, 2012).

The following subsections review current systems under development or in use as sensor platforms. This is not a comprehensive list, but a representative sample of tactical and maritime capabilities that demonstrate the potential for WSN application in a maritime environment.

1. Tactical Network Technologies

Components used in the tactical environment require seamless integration of equipment, without concern for product vendor. Additionally, centralization of network organization would be a hindrance in the tactical environment making selection of ad hoc connections such as mobile ad-hoc networks (MANET) the optimal solution for managing devices through Radio Frequency (RF) communications.

a. Persistent Systems

Under the Wave Relay line of products Persistent Systems offers solutions that provide self-forming and self-healing characteristics, which are important in operational situations where terrain and environmental changes are a constant factor. Persistent Systems offers products that include common handheld radios, embedded systems, and tether devices. These devices provide the ability to connect entities such as individual, vehicles, or operational sites, to create an ad hoc network capable of transmitting data and voice.

The product line for Man-Portable Unit (MPU) devices offers a scalable solution for real time data, video, and voice. The MPU4 allows individuals to connect to Android devices and provide computing in the field (Persistent Systems, n.d.). The MPU5 having surpassed this by bringing the Android OS onboard to provide computing in the field (Persistent Systems, n.d.). Moving up from handhelds the Quad Radio Router provides the same wave relay connectivity for platforms such as vehicles, mounted for large geographic sites, and air-to-ground connectivity (Persistent Systems, n.d.).

The Embedded Module from Persistent Systems, shown in Figure 1, is a form factor device that can be integrated into larger system and add connectivity via MANET (Persistent Systems, n.d.). With features such as video encoders and onboard Android computers, this device can remove redundancy from platforms such as unmanned systems (Persistent Systems, n.d.). With the Embedded Module devices can avoid obsolescence and find enhanced purpose in the battle space.

Figure 1. Embedded Module. Source: Persistent Systems (n.d.).

b. TrellisWare

TrellisWare radios and radio modules, shown in Figure 2, offer an alternative source for MANET equipment in a tactical environment. The TW line of radios offers infrastructure-less system for creating a self-forming/ self-healing wireless network. These radio systems are capable of handling 200+ node configurations in harsh field environments (TrellisWare, n.d.). TrellisWare also offers the TW-600 Ocelot which is also designed as an embedded device. Like the TrellisWare radios the TW-600 can be used in formation of a MANET. All TrellisWare products can act as network relays and provide easy integration into any environment and expand or optimize various platforms (TrellisWare, n.d.).

Figure 2. Tactical Radios and Ocelot Module. Source: TrellisWare (n.d.).

c. Silvus Technologies

Silvus Technologies has developed multiple input, multiple output (MIMO) tactical radios since 2011 (Silvus Technologies, n.d.). Presently known as the StreamCaster line, Silvus Technologies previously offered its 3000 model line which are being made obsolete, and presently offers the SC4200 or SC4400, shown in Figure 3, which can provide beamforming and spatial multiplexing for enhanced throughput with self-forming/ self-healing ad hoc networks. Additional features like Wi-Fi hotspot and GPS modules with a maximum throughput of up to 100+ Mbps and 128GB onboard storage provide a tactical system in a robust package for the battle space (Silvus Technologies, n.d.).

Figure 3. Streamcaster 4400 MIMO Series. Source: Silvus Technologies (n.d.).

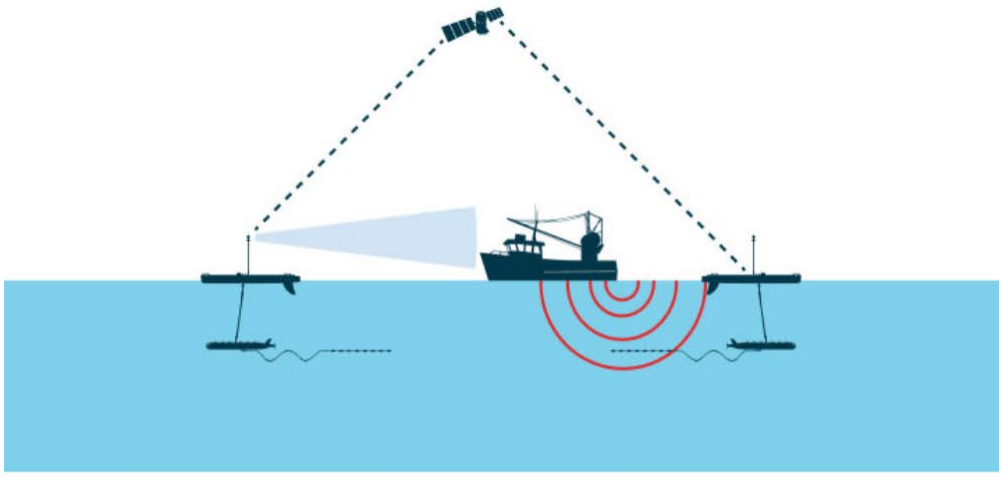
2. Integrated Sensor Platforms

Integrated sensor platforms include a wide range of systems. This subsection will discuss a sample of the platforms available for maritime use with features which are highly mobile and expandable.

a. Liquid Robotics

Liquid Robotics' Wave Glider, shown in Figure 4, is a versatile unmanned surface vehicle designed to monitor the ocean environments. The new Wave Glider platform is rated at providing mobile data collection 24 hours a day for up to 12 months functioning as a real time gateway offering real-time situational awareness. Sensors can be mounted in five locations and functionality varies from weather monitoring, wave height and motion, temperature, etc. Communication components can also be integrated into the Wave Glider to allow satellite transmission for data submission (Liquid Robotics, 2017). With the "Open Oceans Program" customized sensors can be developed to meet the specific requirements of the end-user (Liquid Robotics, 2017). The mixture of capabilities the Wave Glider offers present a great resource for sensor networks.

Figure 4. Wave Glider Example. Source: Liquid Robotics (2017).



b. SEAWEB

The SEAWEB platform is designed for the undersea battle space. The system is self-configuring, uses acoustic sensors that interface with a surface gateway node for radio communications, and can be rapidly deployed from a variety of platforms (Honegger, 2010). The benefit of SEAWEB as an undersea platform provides theater commanders the ability to match resources to the environment by expanding the picture of the battle space.

c. Sonobuoys

Sonobuoys are a common form of sensor employed by the Navy for underwater sound monitoring. Passive Sonobuoys are designed to use hydrophones for converting sound to electronic signals (Sonobuoy TechSystems, n.d.). These signals can then be amplified and transmitted for interpretation. Active sonobuoys work by sending out a signal to detect submarines moving within a target area to provide speed and positioning. Some downsides of sonobuoys are their limited deployment life of only eight hours, and that their drifting with currents can cause gaps in coverage areas (Sonobuoy TechSystems, n.d.). Despite their limitations they offer a maritime sensor platform for underwater monitoring.

3. Wireless Sensor Network and Internet of Things

Internet of Things covers a broad domain of applications in the areas of radio-frequency identification (RFID), service-oriented architecture (SOA), cloud services, healthcare, and WSN. The ideas of IoT and WSN were originally developed in parallel, (International Electrotechnical Commission [IEC], 2014). The IEC (2014) referred to IoT as the interconnection of embedded devices within the existing Internet infrastructure, and the WSN as self-organizing, multi-hop networks of wireless sensors nodes used to monitor or control their environment. IoT is growing everyday with applications and scenarios continually expanding (Gardasevic, Veletic, Maletic, Vasiljevic, Radusinovic, Tomovic, & Radonjic, 2016). The versatility of IoT provides a variety in the options for development of the “things” used within WSN platforms. The WSN architecture uses a base station (BS) for Internet connection; with two structure forms of flat, composed of heterogeneous nodes that share the same functionality; and hierarchical, where nodes are broken into sensing

nodes and cluster heads which aggregates data and reduce processing at the BS (Kahn, Pathan, & Alrajeh, 2012). Power is a major issue with WSNs and the effect of node failure on network operation. Scalability and robustness effects in a large-scale WSN sensor network environment must be addressed to increase network life for extended operation.

a. Scalability for Wireless Sensor Networks

The scalability is concerned with the network's ability to maintain performance integrity regardless of the number of nodes in the network. Scalability requires architecture and protocols to be designed for appropriate support changes in the network with consideration for the limitations of sensor nodes (Karl & Willig, 2007).

(1) Scalability Requirements for WSN

WSN scalability requires that the network be capable of meeting the demands of nodes as they increase, plus all associated tasks and functions (Kahn et al., 2012). When considering growth of nodes within a network it is important to understand that counts will not be by adding a handful of devices, but in multiples of 100, 1000, or more. Requirements for a WSN can vary dependent upon form and task; it is important to remember that WSN generally have a greater number of nodes than a standard network (Karl et al., 2007). This plays heavily on designating the roles of computing resources, for example, where will in-network processing occur; or what will the gateway's role be. Karl et al. (2007) pointed out that scalability is an indispensable trait, and cannot be stifled by addresses and routing tables that have to be maintained.

(2) Growth of Devices and Data

As the number of nodes increases, the data flow on the network increases as well. Cañedo, Skjellum and Ginn (2016) pointed out that architecture scalability must consider edge devices, and gateways for increasing performance in the entire system. Kafi, Challal, Djenouri, Doudou, Bouabdallah, and Badache (2013) pointed out that reliability is crucial part of scalability, for as a network grows unexpectedly undesired system behavior could occur if data packets are lost. Cañedo et al. (2016) recommend an architecture that uses parallel computing from edge devices to reduce the stress on gateways. As the WSN size

increases, architectural considerations must determine needs for the flow and reliability of data, and way to optimize the distribution of computing.

(3) WSN Architecture

As noted by Karl et al. (2007), the WSN does not use the standard of form of routing tables and centralized management as found in customary network protocols. Star, cluster, or mesh are the three design structures available for WSN network architecture and can be selected based on task requirements of network (Kahn et al., 2012). Protocols are a necessary part of the network architecture design and provide a means of managing network structure (IEC, 2014). WSN will need protocols and architecture structures that are designed to support growth as data and processing requirements increase with network size.

b. Robustness in a WSN

Robustness is the ability of the WSN to maintain network connectivity regardless of node failure. For an individual node the level of robustness is not singularly important, the WSN should be designed to perform tasks in the event of failure of some devices (Kahn et al., 2012). This requires that a WSN are able to self-form, self-heal, and self-configure, (Anitha & Mythili, 2016). The network should not fail if a limited number of nodes run out of energy, or environmental factors sever existing links between two nodes (Karl et al., 2007).

(1) Energy Conservation Considerations

Energy consumption is closely associated with the amount of data gathered, transmitted, and received in a WSN (Villas et al., 2013). The design of the network needs to focus on compensating for node and communication link failures (Karl et al., 2007). Protocol design needs to keep sensors alive for extended periods of time, because a sensor depleted of energy will no longer fulfill its role (Warrier & Kumar, 2016). Techniques such as data-centric routing and in-network processing provide strategies to conserve energy and optimize the task of routing by using intermediate sensor nodes along the routing paths, and conserve the limited resources within the WSN (Villas et al., 2013). There is a definite

need to use approaches that distribute processing throughout the network and provide a means of balancing the use of energy resources.

(2) Support for Multi-Hop Considerations

Multi-Hop communications add a powerful feature to the WSN design by moving away from the bottle-neck of centralized network structure. Instead of a central component that provides all information about neighboring devices, a distributed solution that uses multi-channel RF for communications (Zhao & Cao, 2014). Zhao and Cao (2014) pointed that it is necessary to control the channel assignments of nodes in a cognitive radio network to prevent interference and improve performance. Routing by location would provide a simple routing solutions but, as Kahn et al. (2012) explained, providing GPS to each node would deplete energy, increase size, and require satellite access. This minimizes the situation when a WSN would benefit from GPS devices, but in order to solve for localization needs, algorithm support is required for network robustness.

(3) Operational Considerations for Robustness

Kahn et al. (2012) identified four requirements to provide robustness within a WSN: self-organization, self-healing, self-configuration, and self-adaptation. Villas et al. (2013) recognized the need for development of protocols and algorithms that are designed to route in a fashion that conserves energy and transmit around obstacles. As Karl et al. (2007) pointed out when selecting a protocol, distributed organization is a trait that will conserve energy by managing communication between nodes within its local RF range, and compensate for node failure. In order for a WSN to perform its designated task, the operation of the network must incorporate fluid concepts that allow independent operation without outside assistance.

4. Features for the Simulation of a WSN

Simulation of a WSN will provide the performance characteristics that could potentially impact robustness and scalability. Nodes in the simulation will be modeled after the Raspberry PI 3 Model B (RPi) to represent energy consumption and communication performance of this IoT platform. Design will not represent specific modalities or operation

scenarios for a WSN, but the factors that impact scalability and robustness. Chapter III will provide the details on testing to determine operational configuration and power needs for the RPi that will be used for the simulation. These inputs will be taken and used in the simulation to determine the impact of varying node counts and power inputs will represent.

a. Capabilities Simulation Design

The simulation will be designed to represent the behavior of nodes within the WSN structure. Requirements for scalability and robustness will be incorporated to provide a representation of a COTS IoT platform for sensor nodes. The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol will be simulated to represent the communication between nodes. The simulation will use parameters specific to the Raspberry PI 3 Model B (RPi) to provide a comparison with standard sensor nodes. Documentation of the study and parameters will be observed, because as Kahn et al. (2012) pointed out that lack of information about simulations, parameter values, and code access contribute to lack of reproducible results.

(1) Node Specification

For nodes within the simulated environment the features and capabilities of the RPi will be used. This form-factor platform is a commercial-off-the-shelf (COTS) technology with the ability to create a diverse array of custom sensor nodes. The RPi contains features such as; 1.2 GHz Quad Core, 1GB RAM, 40 GPIO pins, USB ports, built-in Wi-Fi and BLE, and camera port (Raspberry Pi Foundation, n.d.). Specifications of interest to this research are the onboard BCM43438 wireless and Bluetooth Low Energy (BLE) components. Modality will not play a role in this simulation design; nodes will be simulated to sense events randomly and forward information to the cluster head for traffic flow.

(2) Network Structure

Network design for a WSN is usually not based on standard client server model that uses routing table and centralized processing structure. In a WSN simulation environment all nodes and gateway components will simulate wireless ad hoc connections for managing communications between devices. Since the purpose of the network is to cover a large area

with the need to conserve energy in nodes, a cluster head hierarchy offers a better option for a WSN in the battle space.

b. Design Constraints

Design constraints will not be able to represent all aspects of the littoral environment. The design of protocol will be used to understand scalability and robustness (Sharma, Saini, & Solan, 2015). Design constraints can limit the accuracy of simulation results, so careful protocol selection and implementation will be an important part of simulation.

5. Summary

In order to improve ISR systems for collecting information about the battle space WSN offer a means to support strategic objectives. This chapter presents how deployment of WSN in a littoral setting can meet the Navy's requirement for distributed lethality by incorporating resources to maximize tactical force capabilities. IoT is evolving into multiple areas and provides a platform for developing components for WSN. The use of COTS technology may offer a potential opportunity to develop rapidly-deployable IoT based wireless sensor networks to support maritime operations. In Chapter III, selection of protocols, simulation tool, and behavior traits for network and nodes will be discussed.

III. SYSTEM ARCHITECTURE AND PARAMETERS

This chapter addresses the specifications of the hardware components, simulation parameters, and network structure of the cluster-based Wireless Sensor Network (WSN). The purpose of the simulation is to determine the robustness and scalability required for COTS devices, like the Raspberry Pi 3 Model B (RPi), Raspberry Pi Zero W (RPiZ), BeagleBone Black (BBB), or the Arduino UNO Wifi (UNO), used as nodes for a WSN. The chapter begins by discussing the network structure of a WSN and concerns for managing communications and conserving battery power of nodes. Next it discusses the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol and the processes used for managing node communication behavior and conservation of power within the network. The chapter concludes with the selection of parameters and measurement of power requirements.

Component selection is based on the previous research conducted in the thesis *In-Network Processing on Low-Cost IoT Nodes for Maritime Surveillance* (Belding, 2016). Belding's objective was to use commercially available, low-cost components, for this research it is Raspberry Pi (RPi) that was selected, to create a sensor platform. This research expands on the use of RPi to serve as nodes within a large-scale WSN. Measurements of the RPi are taken to gain an understanding of the power consumption of the electronics and the WiFi transmission. This is measured against the transmitting speeds for the bit rate to provide the bits per second (bit/s) to determine the joules required to process one bit of information or joules/bit. The collected parameters are then used as inputs for the simulation.

COTS products, like the RPi, often do not meet military performance requirements, especially for a maritime environment. The focus of this research is not to provide a proven solution, but rather to understand the robustness and scalability needs of an available COTS platform to provide a potential solution for littoral Intelligence, Surveillance, Reconnaissance (ISR) wireless sensor networks.

A. SYSTEM ARCHITECTURE

The function of a WSN in this context is to create a group of common nodes that work together to collect and organize information about the battle space environment. Since network characteristics for each system can vary, in order to understand the value of a large-scale WSN it is important to discuss the different roles the nodes fulfill within the network.

This section discusses the features specific to managing a WSN based on the onboard capabilities of the RPi. Specific attention is focused on the following concepts of a WSN: cluster-head (CH) network structure, the LEACH protocol, and sensor node characteristics.

1. Cluster-Head Network Structure

WSN nodes do not have a steady source of energy available to them, therefore power is at a premium. In addition to this restricted power budget, the lack of individual Internet connectivity makes distribution of data processing an essential consideration in the network design. For this reason, cluster-based routing protocols have been developed as a way to maximize the limited power resources available to WSNs.

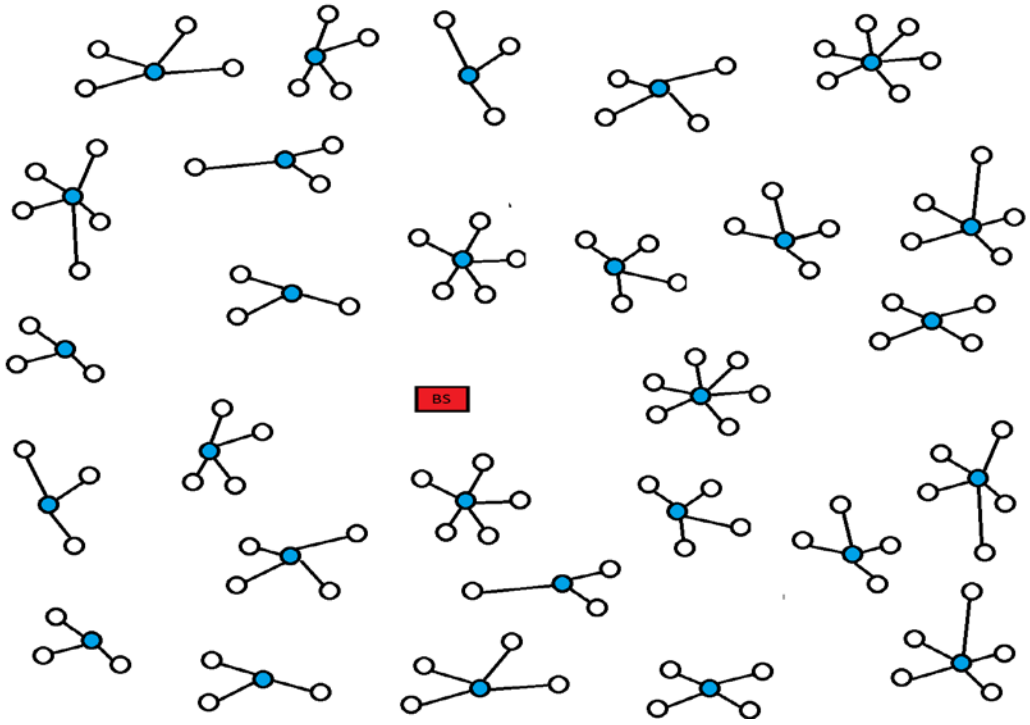
Most large-scale WSNs consist of a base station which manages the machine-to-machine (M2M) communications, processes sensor inputs, and forwards data to the Internet or some central system. Nodes for WSN can vary in configuration to serve network- or application-specific purposes. Heterogeneous networks contain some nodes that have advanced capabilities beyond the common sensor nodes. Homogeneous networks have nodes that are identical in configuration and initial power. In both arrangements, nodes may rotate the responsibility to perform as CH for a group of nodes to provide in-network processing to extend the life of the network.

2. Low-Energy Adaptive Clustering Hierarchy Protocol (LEACH)

The LEACH protocol and its many variants are popular in WSN simulation and analysis, shown in Figure 5 (Comeau & Aslam, 2011). The LEACH protocol is based on cluster forming algorithms that use ad-hoc connections to create self-organizing, large-

scale networks (Heinzelman, Chandraksan, & Balakrishnan, 2002). At the beginning of the WSN's lifetime, it is assumed that all nodes will have the same amount of power available. The LEACH protocol allows node configuration to be heterogeneous or homogeneous. All nodes are required to communicate with the Base Station, support different MAC protocols, and perform single processing functions (Heinzelman et al., 2002).

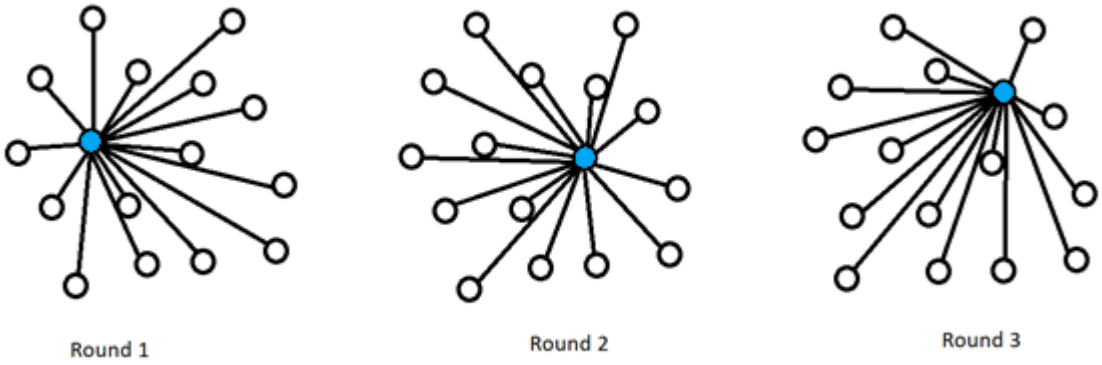
Figure 5. Example of LEACH WSN



a. Cluster-Head Selection

Clustering enables reuse of bandwidth to increase system capacity and provide better use of resources for improved power control (Heinzelman et al., 2002). LEACH falls into the category of energy conscious protocols or, simply put is considered "power aware" (Heinzelman et al., 2002). LEACH uses an algorithm for random rotation of CH selection, shown in Figure 6. All nodes are eligible for the status of CH, but no node will serve this role for two consecutive rounds.

Figure 6. LEACH Protocol Example (Cluster-Head in Red)



b. Cluster Set-Up Phase

Groups of nodes are organized into local clusters. The beginning of each round of the simulation starts with a set-up phase (Heinzelman et al., 2002). This process requires each eligible node to request election as CH for a new round. Once a CH has been elected, an advertisement message (ADV) is sent out using the Carrier-Sense Multiple Access (CSMA) protocol with the CH node ID. The CH will then set up a Time-Division Multiple-Access (TDMA) schedule and transmit it to each node in the cluster to conclude the set-up phase and place the cluster in the steady-state phase (Heinzelman et al., 2002).

c. Cluster Steady-State Phase

The steady-state phase permits the nodes to communicate with the CH during a designated transmission slot. The number of frames for data is dependent upon the number of nodes per cluster (Heinzelman et al., 2002). Time can be synchronized by having the Base Station transmit pulses to nodes to coordinate start-up phases and CH advertisements. During the steady-state phase, all CH(s) must be awake for collection of data and provide in-network processing through data-aggregation, if a CH is asleep during this phase it cannot receive schedule information for the next round of network operations and could cause unequal distribution of power. The TDMA schedule signals non-CH nodes to turn off radio communications and reduce power consumption.

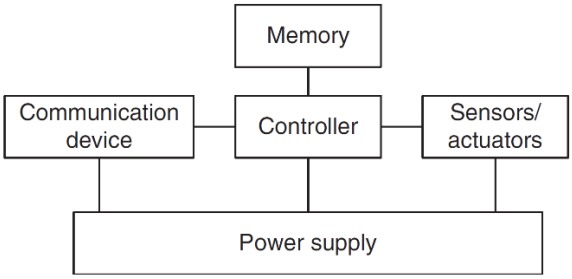
B. SENSOR NODE COMPONENT

Using COTS devices is becoming a common approach for finding solutions within the realm of technology. The focus of this study is the use of COTS devices as a sensor platform in littoral settings. RPi is the platform that will perform the role of the sensor node in a WSN.

1. Sensor Node Hardware

Sensor nodes perceive information about the surrounding environment. A sensor node consists of a controller, memory, sensors and actuators, communication, and power supply (Karl et al., 2007), shown in Figure 7. The ability to provide a sensor or actuator offers sensor nodes the ability to passively observe the environment or interact with it based on stimuli. Each of these components requires balance in the energy consumption of the device to fulfill its task (Karl et al., 2007).

Figure 7. Sensor Node Hardware. Source: Karl et al. (2007)



2. Raspberry Pi 3 Model B

This COTS device was chosen based on the fact that the RPi has the hardware capabilities to qualify as a common sensor node. It also can serve as a versatile resource that can support both sensing and actuating.

Features of the Raspberry Pi 3, shown in Figure 8:

- Quad Core 1.2GHz Broadcom BCM2837 64bit CPU
- 1GB RAM
- BCM43438 wireless LAN and Bluetooth Low Energy (BLE) on board
- 40-pin extended GPIO

- 4 USB 2 ports
- 4 Pole stereo output and composite video port
- Full size HDMI
- CSI camera port for connecting a Raspberry Pi camera
- DSI display port for connecting a Raspberry Pi touchscreen display
- Micro SD port for loading your operating system and storing data
- Upgraded switched Micro USB power source up to 2.5A

(Raspberry Pi Foundation, n.d.),

Figure 8. Raspberry Pi 3 Model B. Source: Raspberry Pi Foundation (n.d.)

The RPi is an acceptable prospect for use as a processor node in a WSN because it provides the necessary hardware requirements of a sensor node. The Quad Core CPU is more than capable as a system controller. The on-board RAM and Micro SD port serve as a sufficient memory configuration. With 40 GPIO pins on the main board, the system can take on multiple sensors, actuators, or combinations. Built-in wireless communications are a new feature that expands the system capabilities. Power can be applied using the Micro USB power input source or GPIO pins. The RPi can use a variety of operating systems (OS) for controlling the device. For this study the standard RPi Raspbian Lite OS was selected. This OS runs with reduced requirements, eliminates the desktop, and can run programs and protocols in multiple programming languages and communication protocols.

C. TARGET NODE PARAMETERS

Node traits for the simulation will model the capabilities of the RPi using measurements of communication power for data bit rates. Communication testing is conducted using ad-hoc wireless-mode, using 802.11 protocols. The collection of measurements assists in determining capabilities and limitations of the RPi as a sensor node platform within a WSN simulation. A Base Station is introduced into the simulation, and serves as the centralized communication gateway that connects the network to an external source, which could be the Internet or a specific cloud source. The simulation assumes that the Base Station has sufficient power for continuous operation throughout the life of the network which ceases when all nodes are dead.

1. Node Operation Characteristics

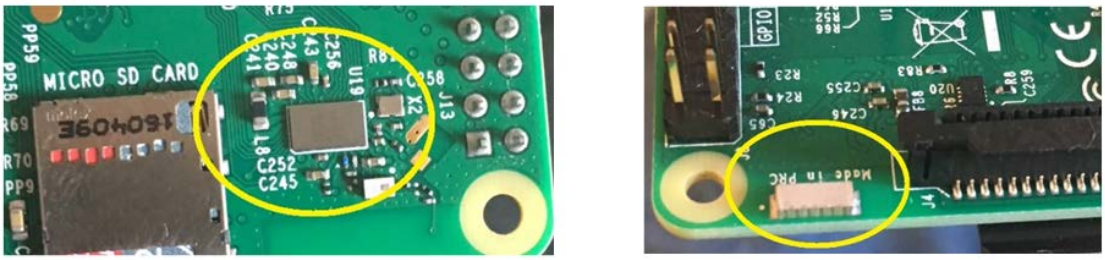
The power consumption for all sensor nodes within the network is represented in joules. Power measurements focus on the amount of energy consumed by the electronics for transmitting and receiving data, by bit rate, within a WSN. Modality power needs are not discussed in this study because of the potential amount of variations in forms of modality and sensor activity.

a. Communication Components

The latest release of the Raspberry Pi, 3 Model B, incorporated onboard wireless communications into the platform. The CYQ43438, formerly BCM43438, integrated single-chip provides communications for the RPi. This chip provides 2.4 GHz WLAN for IEEE 802.11 b/g/n MAC/baseband/radio, Bluetooth 4.1 support, and an FM receiver (Cypress Semiconductor Corporation, n.d.). An onboard chip antenna, soldered directly to the board, can support both Wi-Fi and Bluetooth communications at 2.4 GHz radio frequency (RF), shown in Figure 9. For the purpose of this research, operating parameters from Wi-Fi are used to represent node communication power use. Although it may have greater power requirements, the purpose for selecting Wi-Fi over Bluetooth is the ease of creating ad-hoc connections, and no additional programming is required. Standard Wi-Fi also offers the potential for greater communication ranges, without the need for additional antennas or range extender. This decision aligns with using a COTS solution, without

additional equipment or range extenders. Testing transmission between two RPi devices revealed a maximum range of 320 meters achieved using ad-hoc Wi-Fi connections.

Figure 9. Onboard Communication Chip and Antenna



Communication Chip **Antenna**

b. Ad-Hoc Network Connectivity

A WSN does not use a network that relies on a central management server which could introduce latency by managing connections between nodes. Devices communicate directly and manage connections independently. The Linux manual pages identify six modes in which wireless network interface can be configured. Ad-hoc mode is used for connections to emulate a WSN connection and gather bit rates for the study. This is achieved through the use of the Open-Mesh project, called a Better Approach to Mobile Ad-hoc networking (BATMAN). The purpose of Open-Mesh is to create a routing protocol for multi-hop ad-hoc mesh networks (Open-Mesh, n.d.). This makes it an ideal resource for emulating the desired network environment, and reduces additional network traffic overhead, typically found in a centralized network.

2. Data Bit Rate Determination

Data bit rates are an essential metric for the simulation of a WSN. Bit rates represent the speed at which nodes transmit and receive data streams. The transmission and receipt of data will have a correlating power consumption rate for nodes operating in the network. As mentioned above, nodes were configured to use ad-hoc connections to emulate actual

WSN communications. Message Queue Telemetry Transport (MQTT) (MQTT.org, n.d.) was used to support the message traffic between nodes. The number of bits transmitted and received for nodes will be determined through capturing files for each mode, and the resulting network packet capture files will be analyzed in the Wireshark (Solarwinds, n.d.) program to provide the bit rate.

a. Message Queue Telemetry Transport

MQTT is a protocol used in many sensor networks as a publish-subscribe system for sending messages. MQTT is designed to use a publisher that can be set to send messages for any number of topics. A broker serves to consolidate messages and push them out to all subscribers set for receipt on a specific topic. MQTT can set quality of service (QoS) to any of three levels that can restrict messages to transmit "at most once," "at least once," or "exactly once." MQTT.org (n.d.) identifies it as a M2M/IoT connectivity protocol useful for connecting remote locations that need a small footprint. The publisher and subscriber codes used for emulating network traffic bit rates were written using the python "paho-mqtt" libraries. The reasons for selecting this solution were that first, a separate broker was not necessary, as publishers and subscribers connect directly, thereby reducing additional devices or power requirements for the network. Second, the python libraries can be run from command line and do not require the power overhead of graphical user interface (GUI).

b. Packet Capture for Bit Rate

Determining the amount of power consumption for data transmission between nodes operating in a WSN requires collection and study of the bit rate of transmitted and received packets. It is necessary to capture the bit rate of data being sent between nodes. To reduce external power influence, the RPi has all other interfaces powered down or disabled. Since the Bluetooth and Wi-Fi use the same communication and antenna chips, it is important to make sure the Bluetooth feature is turned off. In order to collect the bit rate, a 1kB message is sent every millisecond, between nodes via MQTT. Packets are collected via the Linux command line tool "tcpdump." Tcpdump is a tool for collecting information about packet contents of a network interface. Tcpdump will have flags set to

save information to a .pcap, packet capture, or file, and for the targeted interface “bat0.” A sample command line looks like “tcpdump -w capture.pcap -i bat0.”

c. Bit Rate Data Measurements

The completed packet capture files are evaluated using ‘Ethereal’ a network protocol analyzer program. This allows packet information to be read so that determinations can be made in the number of bits transmitted or received between nodes. Data are collected between nodes for multiple five minute periods. The capture process alternates focus between the sending and receiving process. The information from multiple readings is averaged to determine the amount of bits per second that nodes can be expected to transmit in a WSN. This information is used with energy readings to determine the average joules per bit used in the network simulation.

3. Transmit and Receive Power Measurements

As stated previously, the life of a WSN and its components are energy dependent. LEACH is an energy aware protocol that focuses on conservation of energy. Equally important as the data bit rate measurement is the measurement of power consumption by nodes.

a. Electronics Power Measurement Devices

The amount of power used for processing wireless data transmission is accomplished using devices that capture the milliampere-hour (mAh) and voltage (V) consumed by the RPi. These two attributes are used to calculate the power consumed. Two devices are selected to provide measurement; the Drok USB Security Monitor, Model J7-b/c/d and the Drok USB Meter, Model USB 3.0 Meter (H). These devices are able to operate within the power requirements of the RPi and can provide validation between devices. Readings will be taken separately for transmit and receive operation testing.

b. Raspberry Pi 3 Model B Power Measurements

The power for the RPi requires a +5.1V micro USB supply with 2.5 Amps. This can be supplied from connection to a standard electrical source or battery. A direct

power source, using a standard wall adapter and USB battery bank, was selected for all power readings.

c. Communication Power Usage

The power used in the simulation is based on the combination of power and data bit rate readings during the testing using power measurement devices. A separate reading is collected for power consumption during transmitting and receiving modes. The following formula is used to determine the amount of joules:

*mAh * V * 3.6 = joules*. Source: RC Electronics (n.d.)

The output from this formula represents the total amount of joules used for the device during transmit and receive mode operations. This value is then divided by the total number of seconds to provide the rate of joules per second. Once this value is determined it is divided by the data rate, for both transmitted and received, bits per second:

joules per sec / bits per sec = joules / bit

The end result provides the energy required to transmit or receive a single bit of data. Free space path loss represents the attenuation of signal strength between two isotropic antennas. Multi-path propagation represents the energy used to transmit along multiple signal paths from transmitter to receiver. The power metrics for free space path loss and multi-path propagation transmission are supplied based on research source inputs.

D. SIMULATOR SETTINGS

The platform chosen for the simulator is MATLAB release R2017b version (9.3.0.713579) from MathWorks. This simulator was chosen over other platforms based on the amount of research of the LEACH protocol using MATLAB simulations to test and collect data. MATLAB allows for the use of scripts that can accept input parameters; conduct the multiple rounds required quickly, and deliver values at completion.

1. LEACH Simulation Script

For the simulation in this study the script “LEACH (Low Energy Adaptive Clustering Hierarchy protocol)” created by Homaei (2014) was selected. The advantages

of using this script is the flexibility of inputs that allow for the provision of quick modification of inputs and immediate testing. There are multiple script examples available for simulating WSNs using the LEACH protocol readily available on the MathWorks File Exchange site (Mathworks, n.d.).

2. Simulation Inputs

Selection of simulation input comes from two primary resources. First is the previous research values used for testing LEACH configurations. This provides a foundation for the decisions made in selection of parameters. Simulation inputs range from yard dimensions, base station location, number of clusters, to energy inputs. Second is the energy input pertinent for the RPi (determined in Chapter II) to transmit and receive data, used in comparison with the energy inputs for micro-sensors. The energy for transmitting each bit will be set to 309 nj/bit and the energy to receive each bit will be set for 199 nj/bit. Information for calculating the free space and multi-path propagation was requested from the raspberry pi foundation, but no information was received. For these input variables data supplied for Bluetooth, which also uses 2.4GHz RF wave length, is substituted. This provides a free space path loss set to 255 pj/bit/m2 and multi-path set to 0.0063 pj/bit/m4 (Comeau et al., 2011). Two other variables will be modified to determine potential effects; these are the number of nodes and number of clusters within the WSN. For all other values, standard protocol inputs will be applied. This decision provides a comparison model against traditional WSN(s), using micro-sensors, and determines the value of using RPi as a sensor node.

3. Items Not Represented in Simulation

With the MATLAB simulation certain traits of a WSN are not represented in this study. The process for electing CH is abridged in this framework. The use of advertisement messages via the CSMA protocol identifying new CH for each round is not performed. The TDMA schedule is also not used, but nodes operate as if a schedule were in place. Rounds in the simulation have input parameters for node behavior, but the focus is on energy usage not node behavior. As previously mentioned, modality of sensors is not explored because of the potential for wide variance in types of modality and collection settings.

E. SUMMARY

With the addition of built-in communications in the Raspberry Pi 3 Model B, the potential for using this platform to serve as nodes in a WSN has improved. With the added communication feature, the COTS RPi met the five criteria necessary to function as a sensor node:

- Sensor node controller
- Memory
- Connector for sensor/actuator
- Power supply
- Communication device

Determining the amount of energy that would be consumed by nodes for this simulation is necessary, so measurements are collected from devices sending and receiving messages using the MQTT protocol. These measurements are converted into the joules per bit for both transmitting and receiving modes to represent node energy behavior in the simulation. The LEACH protocol was selected for simulating the operations of the WSN. This is a common protocol used in large-scale networks for micro-sensors, supported by numerous research sources. A script developed for MATLAB, from Mathworks, is used as the platform for running the simulation. Input variables focus on the measurements of the RPi compared against standard micro-sensor values. Inputs were restricted to energy values for transmitting and receiving data for RPi against those of micro-sensors. This provided a comparison to determine the feasibility of using a RPi for service as nodes in a WSN.

THIS PAGE INTENTIONALLY LEFT BLANK.

IV. IMPLEMENTATION AND TESTING

This chapter discusses the implementation of the network simulation used for the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol. A description of the simulation code modules and the traits provide an outline for the operational design. The simulations focus on the traits of the wireless sensor network (WSN) to determine the robustness and scalability behavior of the Raspberry Pi 3 Model B (RPi). The testing begins with a baseline result model for the output of a WSN using the LEACH protocol that utilizes standard micro-sensor (MS) inputs. Multiple simulations are then run using power inputs that represent the RPi in various configurations. Three inputs are used to demonstrate possible configuration and determine the settings for a network using RPi to provide a comparative performance for MS. The first input is the proportion of nodes acting as cluster-heads (CH); second is the node count for each simulation; third is the amount of initial power provided for each node at the beginning of the simulation. Changing the combinations for these inputs show the effect of robustness and scalability on a WSN comprised of RPi that uses the LEACH protocol.

A. SIMULATION IMPLEMENTATION

The environment for conducting the simulation is MathWorks, MATLAB platform. MATLAB provides an interactive environment that allows custom program development to create a scalable environment to represent conditions for using the LEACH protocol. It also provides a built-in Statistics and Machine Learning Toolbox in MATLAB with the features of randomization, multidimensional data analysis, descriptive statistics, and plots that represent the data of a WSN using the LEACH protocol. This section reviews the functions of each module from LEACH protocol, script created by Homai (2014), for the simulation design.

1. Simulation Design

The simulation design is set to model certain inputs of a WSN using the LEACH protocol. The coverage area, referred to as the “yard,” is set to 100 meters in length and width. This places each node within 50m or less of the base station and is the range limit

used for micro-sensors (MS) and RPi nodes. The placement of the base station can be customized for different network layouts, but for this simulation the base station is placed in the center to maximize the number of nodes in the yard in each simulation.

At the start of the simulation all nodes are randomly distributed throughout the yard, and nodes retain their location for all successive rounds. An input is set for the number of cluster heads, which is a preselected percentage of nodes. At the outset each node has the same amount of initial power provided in joules. Each round begins with the random election of nodes for CH. Once chosen as a CH, the same node cannot serve this role again until all nodes have successfully served in the CH role.

The simulation does not use an actual Time-Division Multiple-Access (TDMA) schedule for managing communications. Simulated energy represents the amount of data sent depending on the role the node is fulfilling for that round. Node death is the indicator that represents the robustness and scalability of the network. Factors that are not considered are environmental effects, such as weather or terrain. Also component failure, which includes electronics and power source, are not attributed to node death. All attributes are managed by specific functions outlined in the next section.

2. Simulation Modules

The modules within the simulation are designed to represent specific functions of a WSN. Elements that the simulation program models are network and node structure, round and cluster management, and energy dissipation. The output is then collected within the MATLAB program for export and results analysis.

a. Network and Node Structure

The network structure is composed of two constructs, network and node structure. The “newNetwork” function controls the network structure settings of the coverage area, base station location, node energy settings, and node placement. Three network sizes were used in this research with node counts of 100, 200, and 500. The coverage area for the yard provides a distance that allows each node to communicate with the base station in order to fulfill the role of CH. The x and y coordinates of the base station place it in the center of

the yard for equal distance to each node. These setting are uniform for each simulation run. The energy settings are also managed in the function but vary for node source.

The energy requirements for the simulation use six inputs that include; initial energy for each node, transferring data bits, receiving data bits, free space energy, multi-path energy, and data aggregation energy. Table 1 contains the setting for each of the power requirement for the respective node type:

Table 1. Node Energy Requirements for Simulation

Node Type:	Micro-Sensor	Raspberry Pi 3 Model B
Initial energy for each node:	0.5 J *	Various Settings
Energy for transferring each bit:	50 nJ *	309 nJ **
Energy for receiving each bit:	50 nJ *	199 nJ **
Energy for free space:	10 pJ *	255 pJ *
Energy for multi-path:	0.0013 pJ *	0.0063 pJ *
Data aggregation energy:	5 nJ ***	5 nJ ***

* Comeau et al., (2011)

** Results from power consumption test on RPi (as described in Chapter 3)

*** Homaei (2014)

As Table 1 indicates, the initial energy for RPi nodes varies based on each simulation run, in order to compare node performance between the RPi with the MS. Network architecture also controls the placement of nodes within the yard.

The “newNodes” function requires inputs for the number of nodes in the network, network size, and base station location to determine the random distribution of nodes. This function also assigns the energy to each node initially and determines the portion of nodes assigned the status of cluster head (CH). This sets the initial round and updates as the simulation progresses through each additional round of the simulation.

b. Round and Cluster Management

The simulation has several interdependencies among the functions, this is more obvious in the management of the round behavior and cluster formation. The “newCluster” function incorporates outputs from the “newNetwork” and “newNodes” functions to set the inputs for cluster development, the percentage of CH and to establish the limitations for node and network requirements. This function specifies the protocol to be used with LEACH being the default and target protocol of this thesis.

In the LEACH protocol each round is managed by a TDMA schedule to control when nodes transmit data to the active CH. For the simulation the schedule is used but the simulation uses energy-to-bit ratios and energy dissipation to represent typical WSN behavior. The “newRound” function manages both the number of rounds for the duration of the simulation and the packet size for data transmitted from nodes to CH and from CH-to-base station. For the nodes to CH packet size was left at a constant size of 200 bits. For CH-to-base station the packet size for MS was set to 6400 bits, but the packet for RPi used various sizes to determine the optimal packet size for mirroring MS. The importance of packet size is to control the rate that energy is depleted during the simulation.

c. Energy Dissipation

Energy dissipation is managed by two separate functions “dissEnergyCH” for managing energy used by cluster heads and “dissEnergyNonCH” for all other nodes in each cluster. The function for CH energy dissipation determines the number of CHs based on the count of active nodes. The “dissEnergyCH” function calculates the amount of energy used for both aggregation and transfer of data to the base station. For common nodes the “dissEnergyNonCH” function calculates the energy consumption of nodes in a non CH status. This function determines which nodes are alive and finds the closest CH. The smallest distance between the node and CH is provided to calculate the minimum energy consumption. These functions work interdependently to emulate network architecture and cluster behavior for simulation of a WSN using the LEACH protocol.

B. NODE TESTING

Baseline standards were established from running simulations using MS operational settings for the original simulation. Multiple simulations using RPi settings provide comparison of performance traits. The focus of testing is to investigate the effects different simulation configurations have on robustness and scalability of a WSN. The unit of interest is the rate at which nodes expire based on different inputs for the amount of initial power, number of nodes in the field, and size of packets sent to base station.

1. Simulation Test Plan

The simulation test plan tracks the progression of rounds as nodes start to expire. The number of rounds is the measurement collected for the following points:

1. Death of the First Node
2. 10% Node Death
3. 25% Node Death
4. 50% Node Death
5. 75% Node Death
6. 90% Node Death
7. 5 or fewer Node Deaths

Item seven is based on initial testing which indicated that waiting for the last few nodes to fail could extend the length of the simulation. Since multiple nodes can fail during a single round a code modification was implemented which halts the simulation when five or fewer nodes were still operating.

2. Simulation Node Inputs

The testing plan requires four inputs that are configured in the simulation to determine the effects on WSN using the LEACH protocol. These inputs include the initial energy for each node, percentage of nodes that act as CH, packet size from CH-to-base station, and the number of nodes in the WSN field. Each variation in inputs were configured to run in the simulation to provide results.

a. Initial Node Energy

The initial node energy for the simulation is 0.5 joules as the setting for micro-sensor (MS). A simulation was run using the energy setting for MS which established a target baseline against which simulations that used RPi as nodes were compared. The selected energy settings in RPi simulations are 0.5, 1.0, 2.0, and 2.5 joules respectively. These energy settings were used in each simulation configuration to provide results that are compared to the baseline.

b. Percentage of Nodes as Cluster-Head

The number of CHs is the second input for the simulation. Three levels were used for percentage of CHs, ranging from 0.1 – 0.3. These values were chosen to see the effect the number of active CHs have on the robustness and scalability of a WSN. CHs transmit larger packets to base station than standard nodes and it was important to understand the impact.

c. Packet Size

Packet size represents bit length of the two packet types and is used as a multiple for energy consumption values of data for transmission and receipt. There are two packet sizes used in the LEACH simulation. The first one represents packets sent from the non-CH nodes to the CH. These packets were set at a multiple size of 200 for all simulations, to calculate the amount of energy consumed by normal nodes during a round. The other packets represent the merged data sent from CH-to-base station. This packet value is set at a multiple of 6400 for micro-sensor to determine the baseline value, and modified between 3200 and 6400 for different simulations using the RPi.

d. Number of Nodes in the Yard

The last relationship between robustness and scalability that was tested in the simulation is the number of nodes in the yard for a WSN field. The number of nodes selected for different runs of the simulation was 100, 200, and 500. The variation from 100 nodes to 200 and 500 nodes is to understand the effects that increased node capacity has on the network. Adjusting the inputs of initial energy for each node, percentage of cluster-

heads, and number of nodes are then used to demonstrate the results on robustness and scalability in a WSN used in a littoral environment.

C. TEST RESULTS

All testing configurations ran successfully using each input combination. The specific results for each set of inputs are outlined and discussed below. The results for each setting are presented in separate charts for the three node counts. Color-coded bars identify the number of rounds to attain specific node failure levels, for each percentage of cluster-heads within the network.

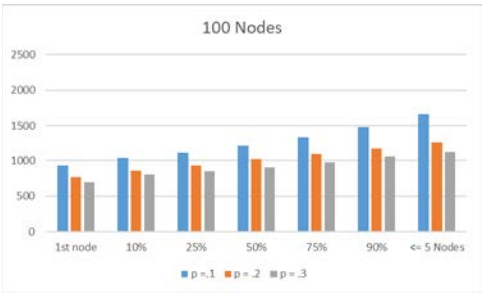
a. Micro-Sensors

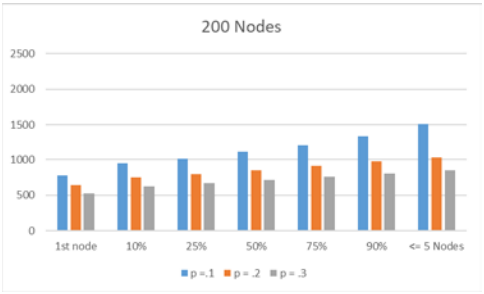
The results for the MS, shown in Table 2, provide the baseline for all test results to identify how RPi configurations compare for communication between cluster-head (CH) and base station (BS).

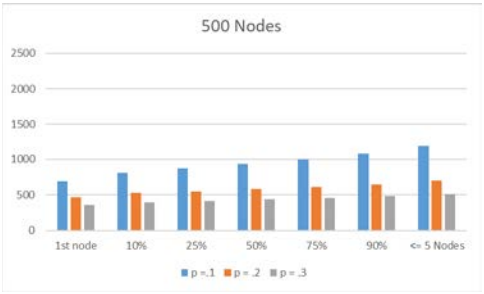
Simulations using MS as the node platform show that when the CH percentage is set to an amount greater than ten percent, CHs start to fail at a faster rate throughout the simulation. For the simulations with ten percent of the nodes as CH, the first node fails in fewer rounds, but the energy to sustain the life of the network lasts longer when managing fewer nodes.

Table 2. Micro-Sensor Results

Micro-Sensors
Initial Power = 0.5 Joule(s)
CH to BS Packet = 6400







b. Raspberry Pi 3 Model B - Initial Power

The results for the RPi with 0.5 and 1.0 joules and packets from CH-to-base station set at 6400, with 100 nodes, shown in Tables 3 and 4, report that network lifetime is diminished when compared to MS. Appendix A lists results for all node counts and displays a similar diminished capacity that is observed with the yards containing 200 and 500 nodes at these initial power settings for each node.

Table 3. Comparison for results with RPi using 0.5 Joules

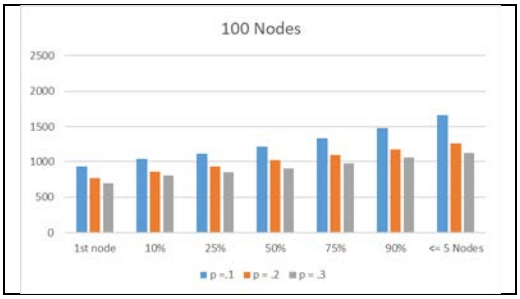
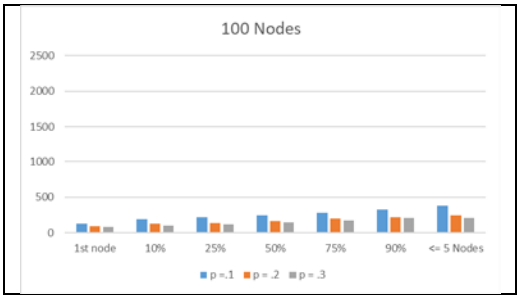
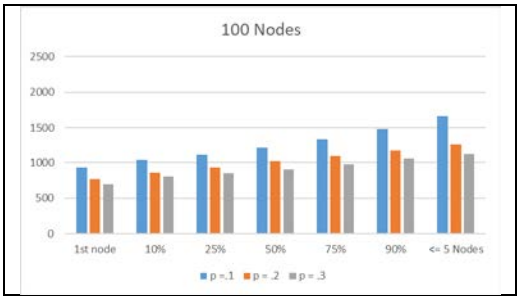
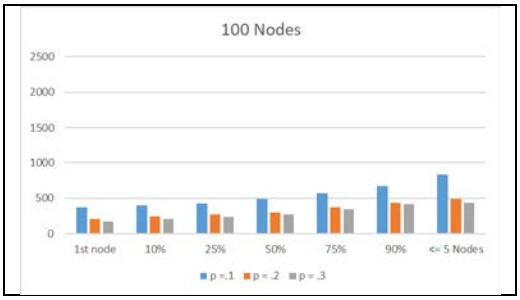
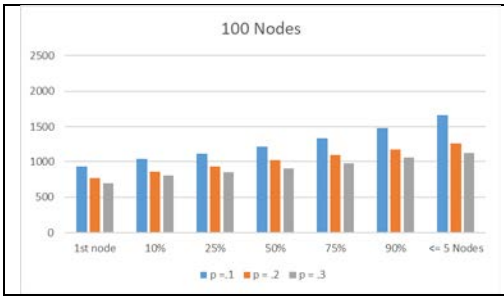
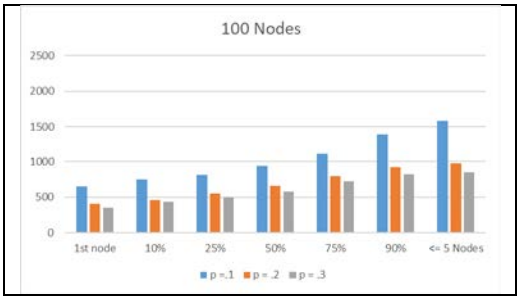
Micro-Sensors **Initial Power = 0.5 Joule(s)** **CH to BS Packet = 6400**	**Raspberry Pi** **Initial Power =0.5 Joule(s)** **CH to BS Packet = 6400**
	
For all node level comparisons see Appendix.	

Table 4. Comparison for results with RPi using 1.0 Joules

Micro-Sensors **Initial Power = 0.5 Joule(s)** **CH to BS Packet = 6400**	**Raspberry Pi** **Initial Power = 1.0 Joule(s)** **CH to BS Packet = 6400**
	

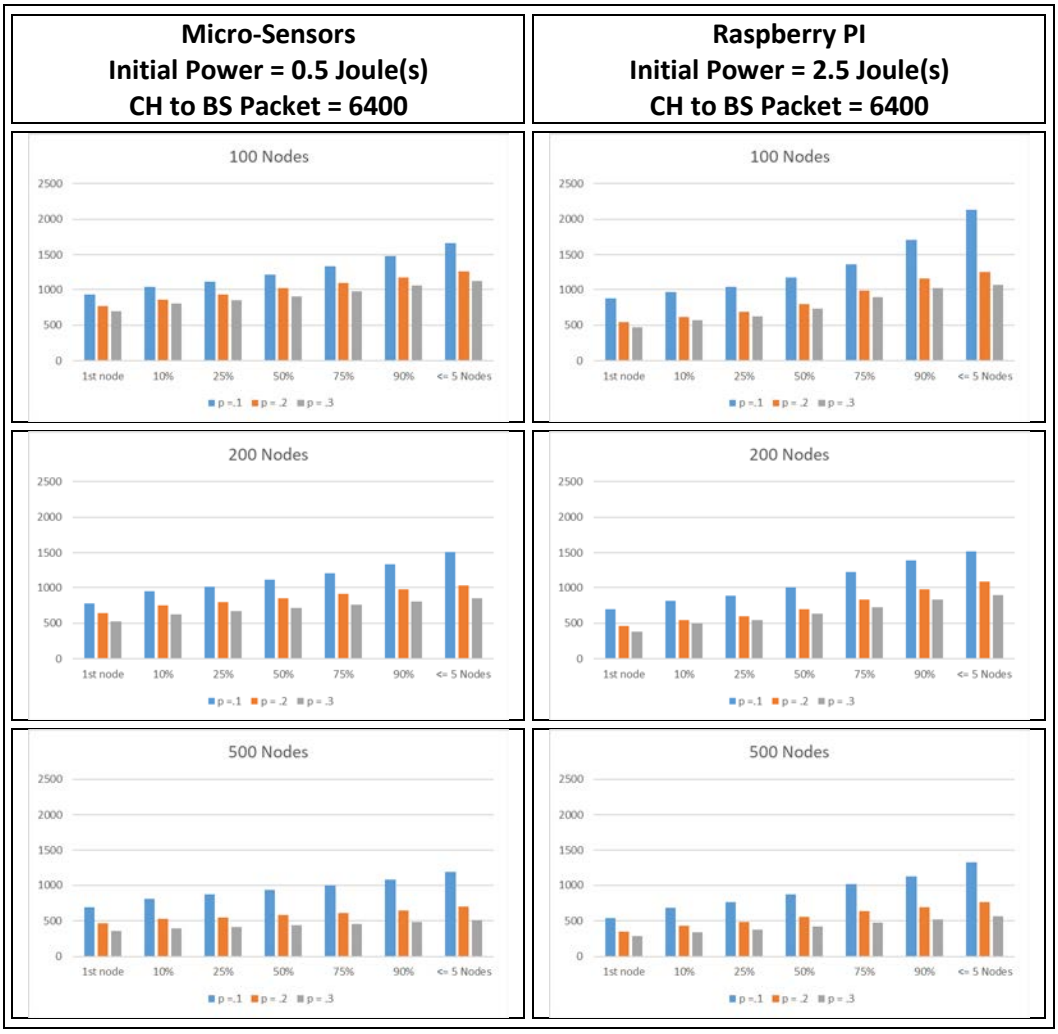
The initial power to 2.0 joules, as shown in Table 5, produced network lifetime results similar to MS when CH was set to 10%, but when the CH is set to 20% or 30% the life of the network was proportionally shorter in number of successful rounds than the network based on MS nodes.

Table 5. Comparison for results with RPi using 2.0 Joules

Micro-Sensors **Initial Power = 0.5 Joule(s)** **CH to BS Packet = 6400**	**Raspberry Pi** **Initial Power = 2.0 Joule(s)** **CH to BS Packet = 6400**
	
For all node level comparisons see Appendix.	

The last input of node energy setting of 2.5 joules, as initial node power for all nodes, shown in Table 6, provides a comparative performance to the lifetime of the network with node deaths providing similar values for each yard size and CH ratio. With the CH ratio of 10% the death of nodes actually exceeds MS with initial power of 0.5 joules, but with CH ratio greater than 10% performance of the network models MS network with no performance increase. Adjustment to packet size offers another option for improving robustness and scalability by lengthening the life of the network.

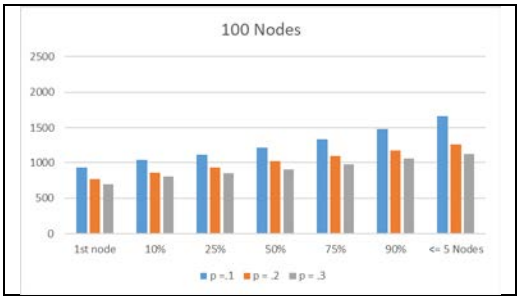
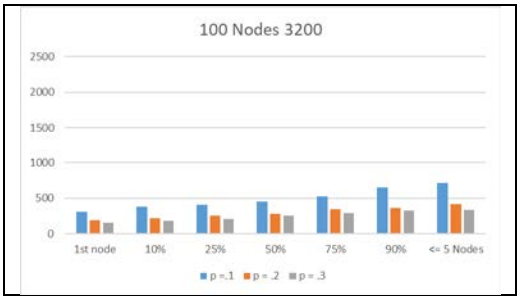
Table 6. Comparison for results with RPi using 2.5 Joules



c. Raspberry Pi 3 Model B – Packet Size

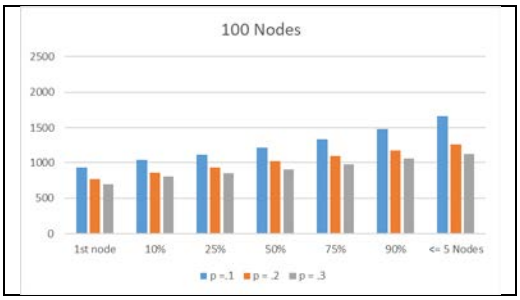
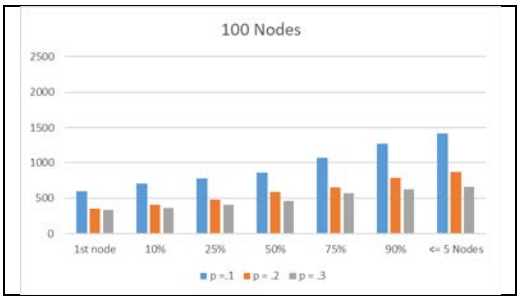
The size of packets sent from CH to the base station is another input modified to determine impact on performance of the WSN. The RPi provides additional processing capability that could increase processing directly at the node to reduce packet size for processing. A comparison of the RPi using 0.5 joules for initial node energy and CH-to-base station packet size of 3200, shown in Table 7, reports that decreasing the packet size does extend the life of the network when compared to the results in Table 3, but performance less than that of MS baseline established in Table 2 using 0.5 joules for initial energy and a packet size of 6400.

Table 7. Comparison for results with RPi using 0.5 Joules w/ 3200 packet

Micro-Sensors Initial Power = 0.5 Joule(s) CH to BS Packet = 6400	Raspberry Pi Initial Power = 0.5 Joule(s) CH to BS Packet = 3200
	
For all node level comparisons see Appendix.	

The power increment of 1.0 joules with a packet size of 3200 is presented in table 8. These simulation results provide comparable results to MS results when the CH ratio is set to 10%, but with CH ratio of 20% and 30% continue to show decreased network lifetime.

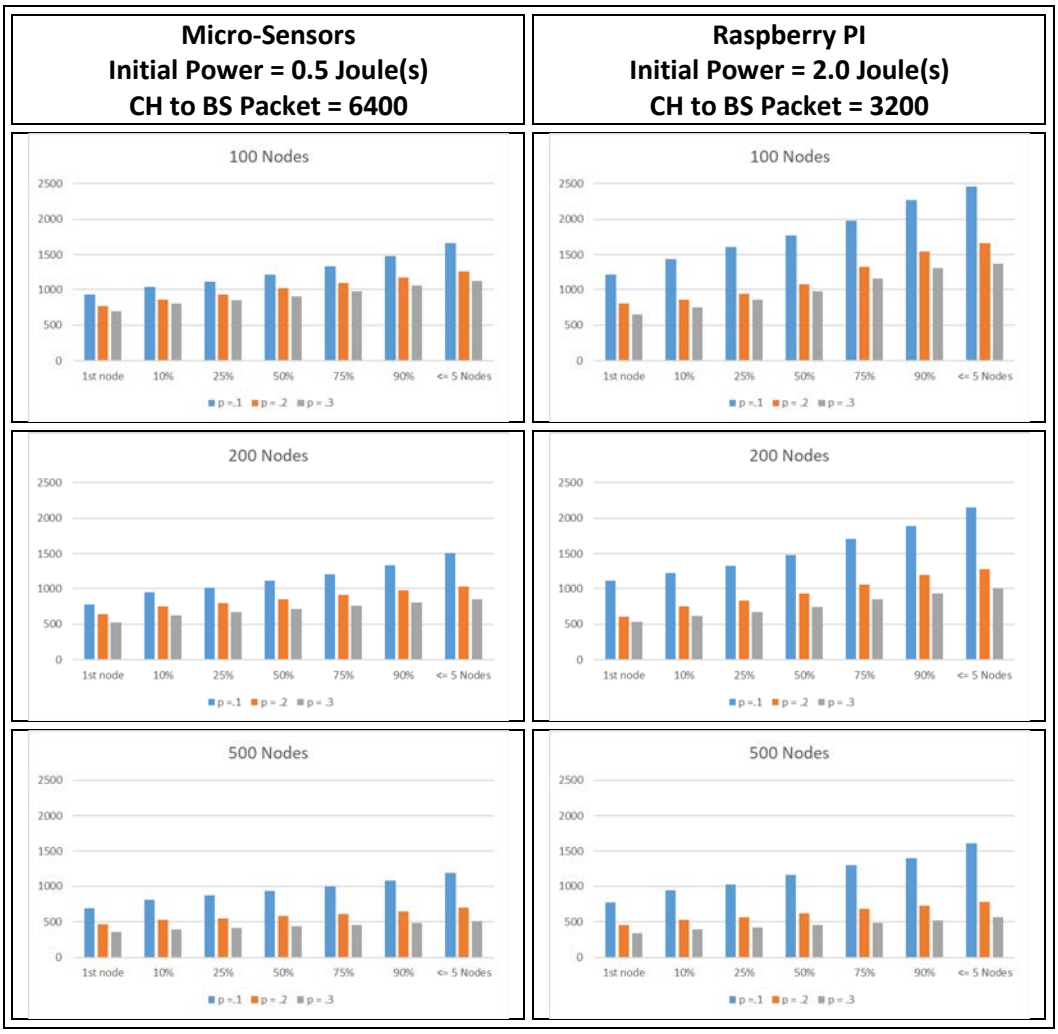
Table 8. Comparison for results with RPi using 1.0 Joules w/ 3200 packet

Micro-Sensors Initial Power = 0.5 Joule(s) CH to BS Packet = 6400	Raspberry Pi Initial Power = 1.0 Joule(s) CH to BS Packet = 3200
	
For all node level comparisons see Appendix.	

The results for RPi with 2.0 joules as initial node power and CH-to-base station packet size of 3200 has all CH ratios as meeting or exceeding the standard for MS with a packet size of 6400. Table 9 displays the results for the simulation run compared to the MS

standard for yards with 100, 200, and 500 nodes. The results for CH with a ratio of 10% exceeds the standard for MS, but for CH at ratios of 20% and 30% the network lifetime is comparable to MS.

Table 9. Comparison for results with RPi using 2.0 Joules



Appendix A contains charts for all configuration options based on yard sizes of 100, 200, and 500, with initial power ranges from 0.5 through 2.5, and CH-to-base station packets sizes of 3200 and 6400. For RPi using CH packet size of 3200 the data for initial power of 2.5 joules were not presented because nodes with initial power of 2.0 joules was greater than or equal to those of MS baseline. Adjustments to inputs allowed the RPi to

perform as a node in a WSN, but this performance could not meet or exceed the performance of a MS nodes using the LEACH protocol in a WSN

D. SUMMARY

Simulations for the LEACH protocol demonstrate the effects of various inputs on a WSN using Raspberry Pi 3 Model B as nodes. The power consumption performance of the RPi based simulation was greater than or equal to the simulation using MS nodes by adjusting initial power or CH-to-base station packet size. Two simulation configurations provided results where the RPi performed similarly to that of the MS used as a baseline.

With the packet size set to 3200 and initial power set to 2.0 joules for the RPi simulation the rate of node death was either greater than or equal to the MS baseline. With equal simulation performance falling into a range of less than 10 %. This means that the RPi simulation would not surpass the MS in all measurements points for node death, but was within a 10% variance for these points with no identifiable trends. This variance indicates that for some simulations the MS may have performed slightly better than the RPi, but by less than 10% and that randomization in the simulation could change the results in other simulation runs.

In the RPi simulations that used a CH-to-base station packet size of 6400 with initial power set to 2.5 joules the MS baseline performed better for the measurement points from 1st node death to 25% of nodes dead. After this point the RPi simulation performance started to improve over the MS baseline. When the CH was set to 10% of the nodes in the network the RPi simulation performed significantly better initially than when CH was set to greater than or equal to 20%. When the number of nodes was set to 100 with a CH ratio of 10% the performance of the RPi simulation was greater than are equal to MS simulation within a 10% variance for these points. As the number of nodes increased to 200 and 500 the performance declined for the CH ratio of 10% for the initial nodes measurement points with less than 25% of nodes remaining. As the network simulation pass the 50% of nodes dead mark all configurations start to improve. The network with 500 nodes actually performed significantly better than the networks with 100 and 200 nodes compared the MS baseline.

Adjustments for the CH-to-base station packet size and the initial node power provided results where the RPi's robustness and scalability capabilities closer to that of the standard MS acting as nodes in a WSN. While the reduction of the CH-to-base station packet size to 3200 versus 6400 produced better performance for the RPi simulation there was no proportionally correlation to the initial power for each node and packet size. The RPi was able to perform at the comparable level to the MS baseline, and adjustments to the initial power, packet size, and number of CHs were evident factors that influence this performance.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND FUTURE WORK

A. SUMMARY

The Navy is limited in its ability to deploy large-scale maritime Intelligence, Surveillance, and Reconnaissance (ISR) sensor networks is both fiscally and logistically constrained. The employment of commercial-off-the-shelf (COTS) technology offers an alternative source for developing new ISR solutions. The purpose of this research was to determine the viability of COTS devices to serve as internet of things (IoT) nodes in a wireless sensor network (WSN) in place of micro-sensors (MS). Robustness and scalability of the network were the metrics of interest for determining if COTS devices were an acceptable solution for WSN nodes. The COTS device selected for this study was the Raspberry Pi 3 Model B (RPi).

Our reason for selecting RPi was that it met the functional criteria for an IoT node, which include controller, memory, communication device, power supply, and connections for sensor/actuator it was COTS and was low cost. RPis were programmed to use WiFi communications to send and receive a 1kB MQTT message to determine energy usage. Power measurements were taken from the RPi using inline measuring devices during transmit and receive communication modes. Packets were captured in files for both modes and the results from power and bits captured were used to determine "joules/bit." These rates were used as inputs in the protocol to represent energy nodes use for transmitting and receiving data.

The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol was selected for simulating WSN with RPi nodes. This protocol was selected because it is designed to conserve energy by evenly distributing it throughout all nodes during operation of the network. The LEACH protocol uses Time-Division Multiple-Access (TDMA) schedules to rotate nodes through the role of cluster-head (CH), distributing the power consumption equally throughout the network. Another benefit of the LEACH protocol program is that it easily allows for a variety of inputs to test multiple network configurations.

The MathWorks MATLAB program was chosen as the platform for developing the simulation. The simulation program relied upon interdependent functions for controlling the WSN. The different functions were able to provide a representation of communication traits for nodes, random election of cluster-heads, and management of processes involved in round structure. The simulation program allowed simplified inputs for initial node power, node power usage, yard dimensions, and node count which provided for modifications between simulation runs. This flexibility in design allowed for tailoring of the WSN configurations to determine what setting might be altered for the RPi node to provide comparative results in robustness and scalability to a network based on MS nodes.

B. CONCLUSIONS

The number of rounds at which nodes expired was the measurement used to determine performance within the simulation. Within the simulation certain observations were made regarding the impact of specific inputs. When the percentage of nodes acting as CH was set to 10%, nodes in the network remained powered significantly longer than when the percentage was set to 20% or 30%. This pattern was noted for all initial node power levels and node counts. Power settings for initial node status were also influential on network performance.

For the micro-sensor the initial node power was set at 0.5 joules. The RPi was not able to provide network performance conforming to similar levels under this amount of initial power. Without altering any other inputs for the RPi network, 2.5 joules as initial node power provided the same number of rounds before network failure as the MS based network. Changes to the packet size sent from the base station to the CH also provided improvement in network performance.

There are two types of packets used in the simulation: those sent from local nodes to the closest CH, and those sent from CH-to-base station. These two packet types were set to different sizes for the purpose of the simulation. The packets for node communication with the CH were set to the value of 200 and were not modified. The packet for communication between the CH and the base station were set for the value of 6400 and 3200 under all simulation configurations. Setting the input for the CH-to-base station

packet size to 3200 provided improved network performance. With the reduced packet size, 2.0 joules for initial node power provided similar performance to a MS based network.

The simulation for RPi was not able to equal the performance of the simulation for MS network. The MS network, with the initial power of 0.5 joules, was able to keep nodes alive for a significant number of rounds compared to the RPi network. Adjusting inputs for the initial power and packet size for CH-to-base station communication were able to provide increased node performance for the RPi network. This indicates that the RPi's increased computing capacity would require configuration changes to match the performance of a MS based WSN.

C. FOLLOW-ON WORK

Proposals for follow-on work fall into four possible categories of research. Categories include other COTS node platforms, physical networks using RPi, sensor modalities, and multiple sensor yards.

a. COTS Devices

In this research, the Raspberry PI 3 Model B was the sole device tested for potential node traits. Presently there are a number of COTS devices available that could meet the requirements for a sensor node with a controller, memory, communication, power supply and means to connect sensors and actuators. Example devices are Raspberry Pi Zero W (RPiZ), BeagleBone Black (BBB), or the Arduino UNO Wifi (UNO). Research into COTS devices can determine performance capabilities for comparison to MS based networks.

b. Physical Network Testing

The simulation provides information on the potential performance of the RPi as nodes in a WSN. Physical testing of the RPi in a WSN using the LEACH protocol is necessary to determine performance characteristics. This can focus the effects, such as environmental factors, battery endurance, and communication, within varying terrain. Testing in the physical environment can identify limitations for nodes and potential operating barriers. Physical testing is an important step in determining the viability of COTS devices as sensor nodes in a littoral setting.

c. Sensor Modalities

The variety of modality for sensors was too extensive for this study. Research into different sensor types may provide potential utility of COTS nodes in a WSN. Areas of research can focus on modality selection, configuration, and power requirements. Research into different sensor modes will aid in determining the right options for node platforms and identify potential obstacles for specific sensor types.

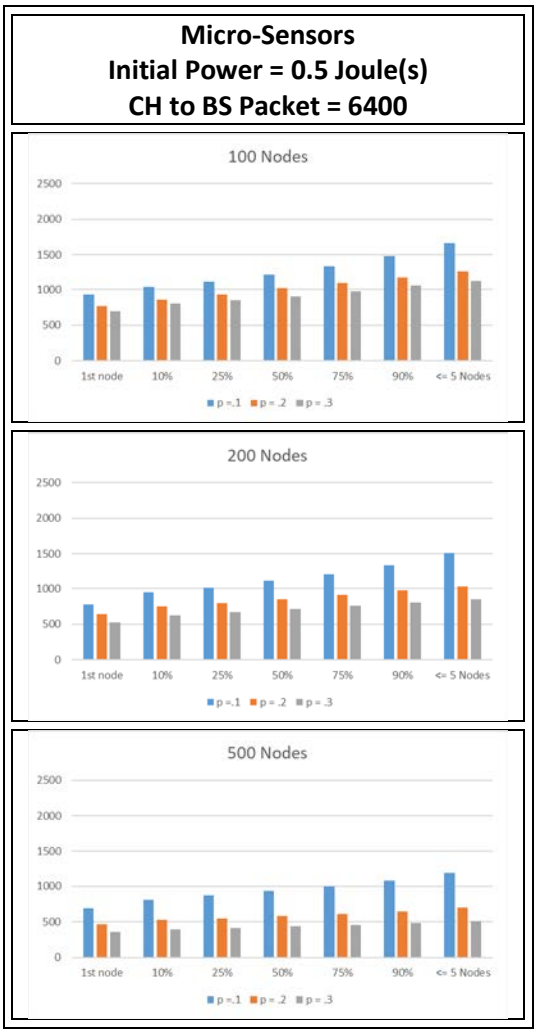
d. Multiple Sensor Yards

This research focused on a single WSN yard. Further research could focus on simulating the use of multiple yards for developing larger interrelated networks. Topics of interest can include the interaction between nodes from different groups, impact of base station failure within interconnected yards, and potential communication options for base station nodes. Research on WSN yards working interdependently could provide potential information on expanding the capabilities of COTS based networks.

APPENDIX. TEST RESULTS

A. MICRO-SENSOR BASELINE RESULTS

Table 10. Micro-Sensor Results



B. RASPBERRY PI 3 MODEL B COMPARISONS TO MICRO-SENSOR

Table 11. RPi with Initial Power of 0.5 j and Packet of 6400

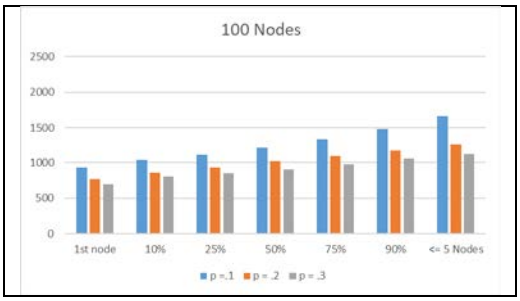
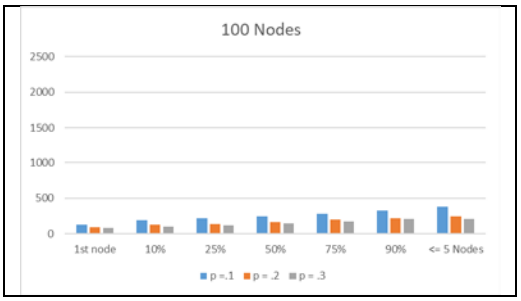
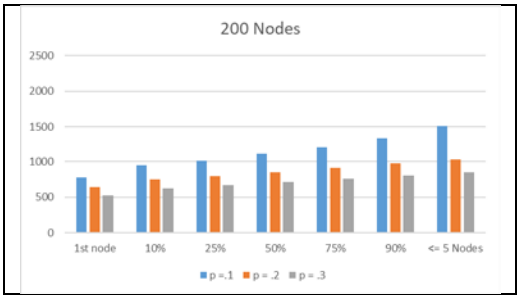
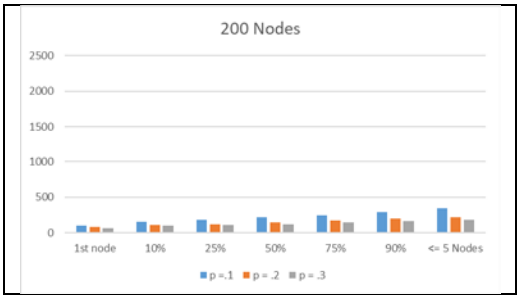
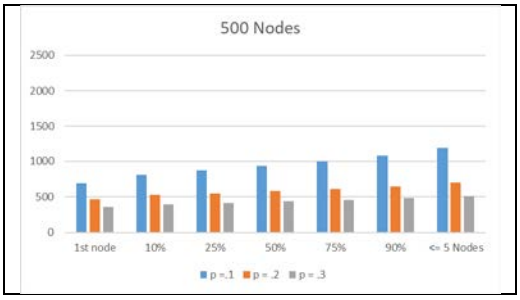
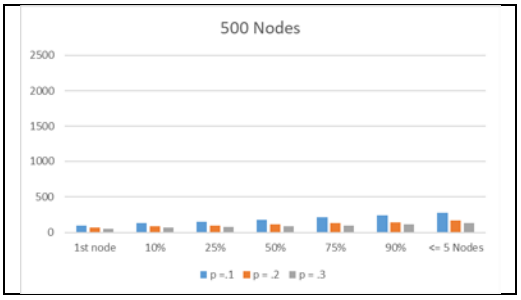
Micro-Sensors Initial Power = 0.5 Joule(s) CH to BS Packet = 6400	Raspberry PI Initial Power = 0.5 Joule(s) CH to BS Packet = 6400
	
	
	

Table 12. RPi with Initial Power of 1.0 j and Packet of 6400

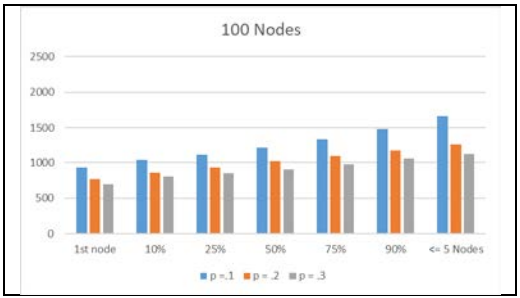
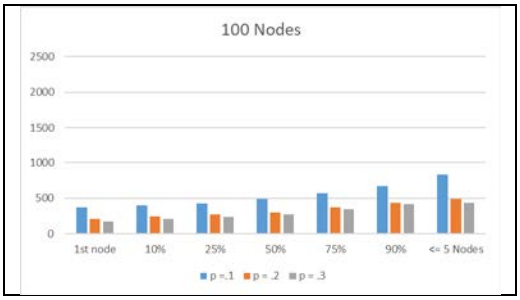
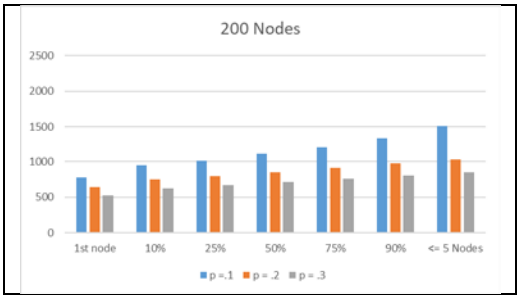
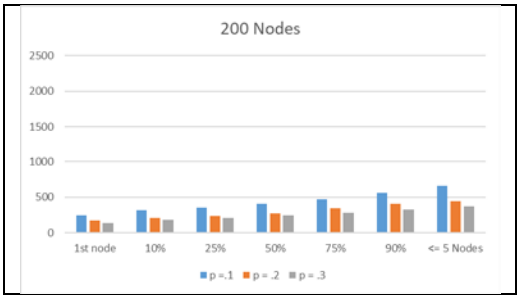
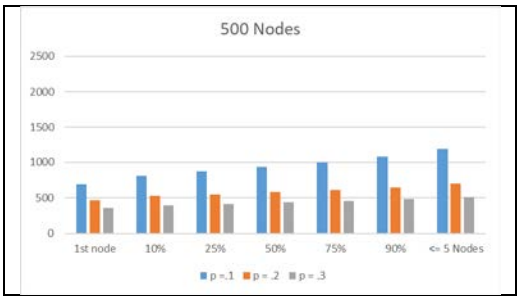
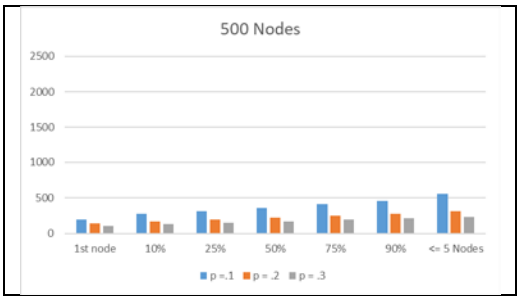
Micro-Sensors Initial Power = 0.5 Joule(s) CH to BS Packet = 6400	Raspberry PI Initial Power = 1.0 Joule(s) CH to BS Packet = 6400
	
	
	

Table 13. RPi with Initial Power of 2.0 j and Packet of 6400

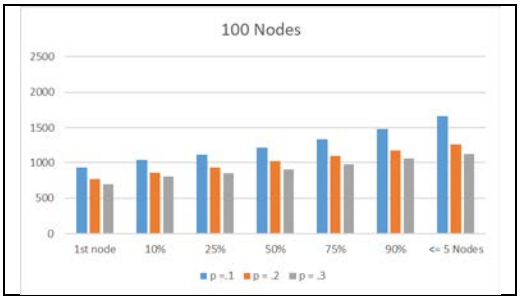
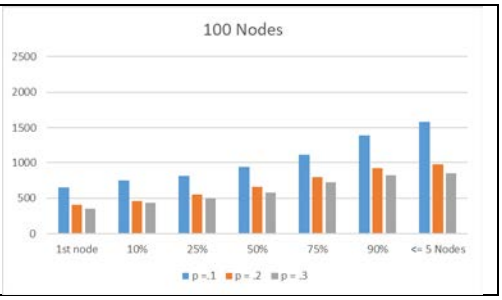
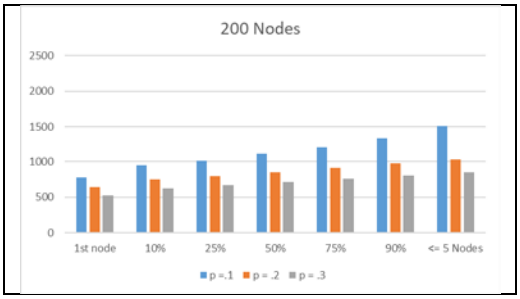
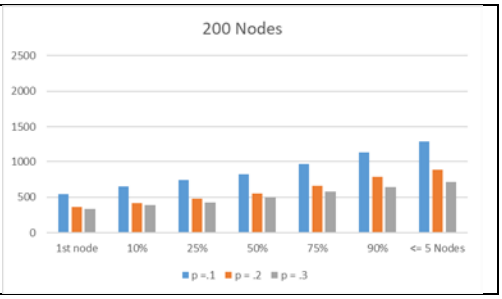
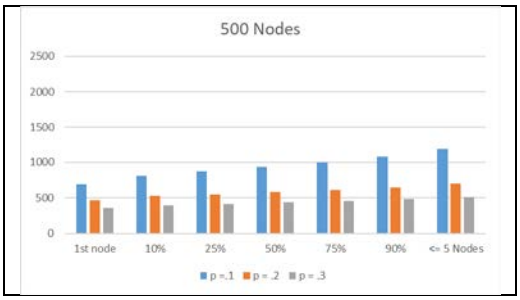
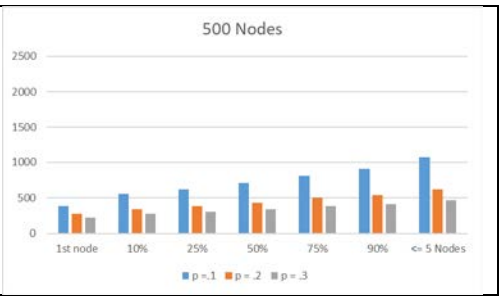
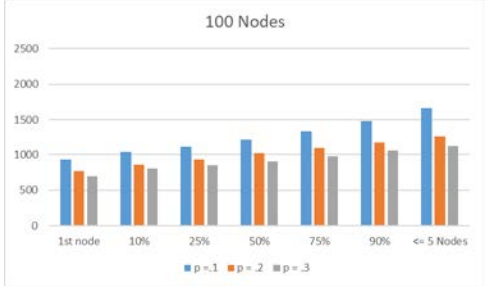
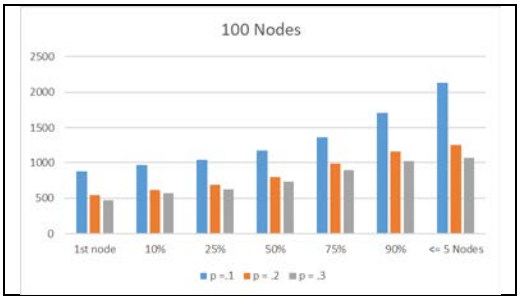
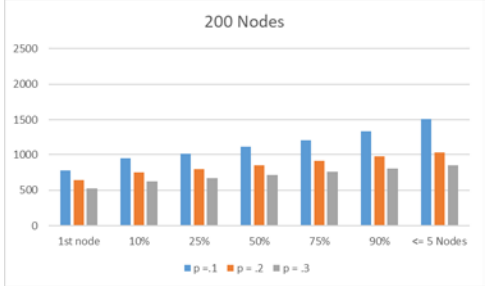
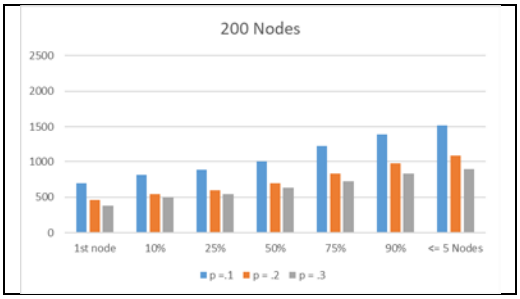
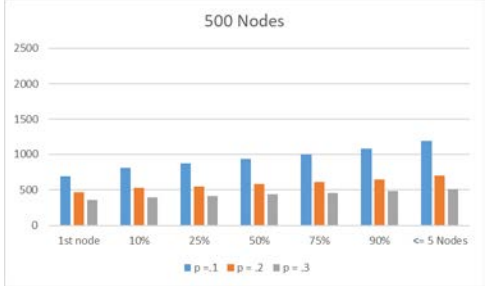
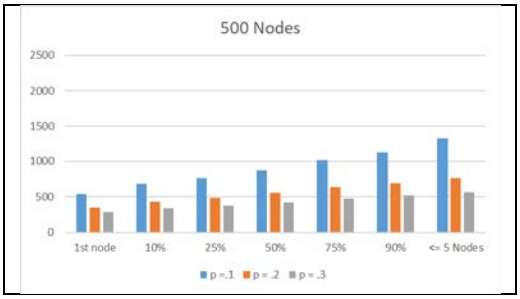
Micro-Sensors Initial Power = 0.5 Joule(s) CH to BS Packet = 6400	Raspberry PI Initial Power = 2.0 Joule(s) CH to BS Packet = 6400
	
	
	

Table 14. RPi with Initial Power of 2.5 j and Packet of 6400

Micro-Sensors Initial Power = 0.5 Joule(s) CH to BS Packet = 6400	Raspberry PI Initial Power = 2.5 Joule(s) CH to BS Packet = 6400
	
	
	

C. RASPBERRY PI 3 MODEL B COMPARISONS WITH 3200 CH PACKET

Table 15. RPi with Initial Power of 0.5 j and Packet of 3200

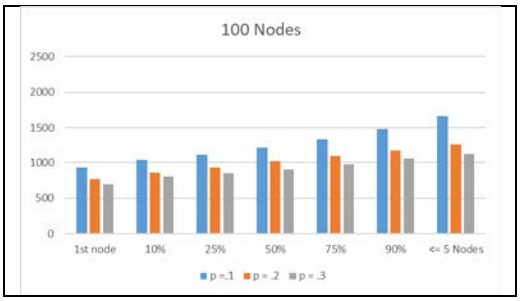
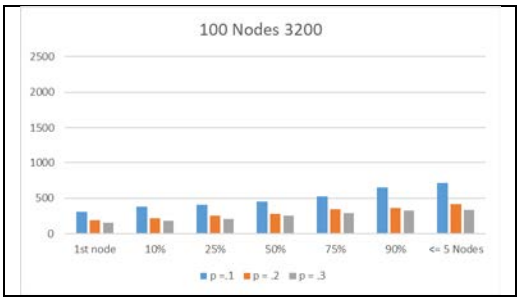
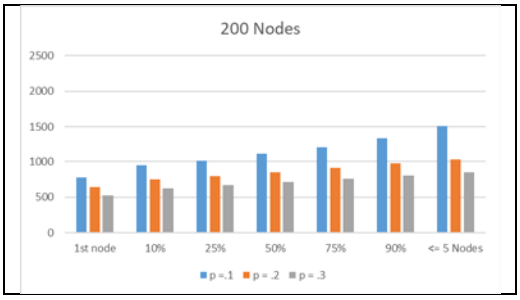
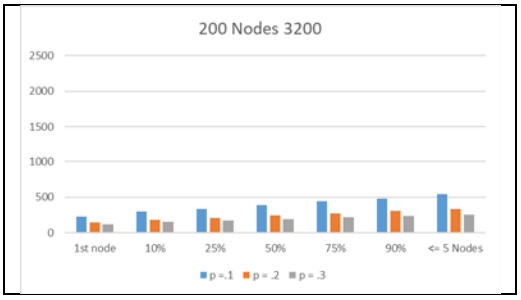
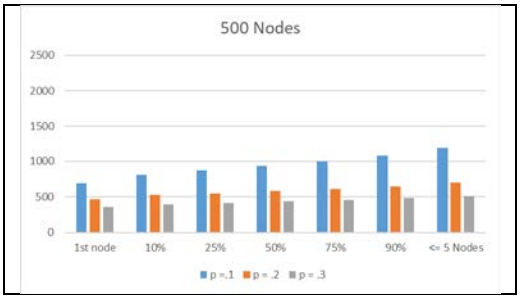
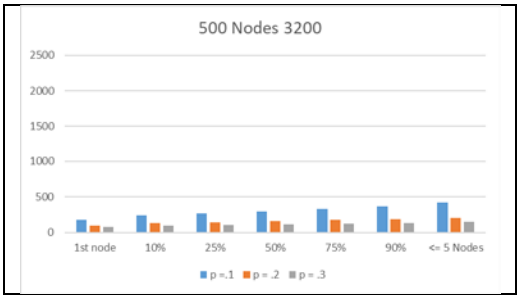
Micro-Sensors Initial Power = 0.5 Joule(s) CH to BS Packet = 6400	Raspberry PI Initial Power = 0.5 Joule(s) CH to BS Packet = 3200
	
	
	

Table 16. RPi with Initial Power of 1.0 j and Packet of 3200

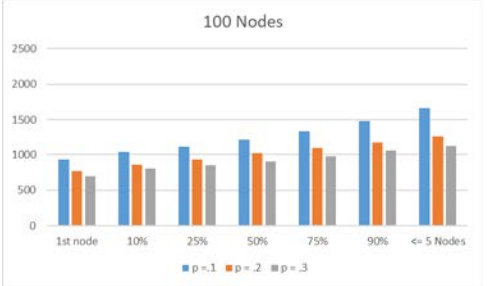
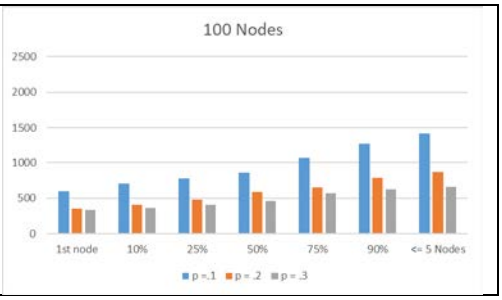
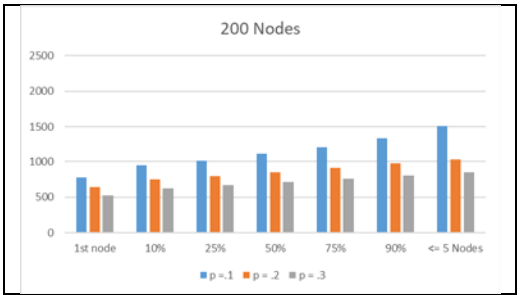
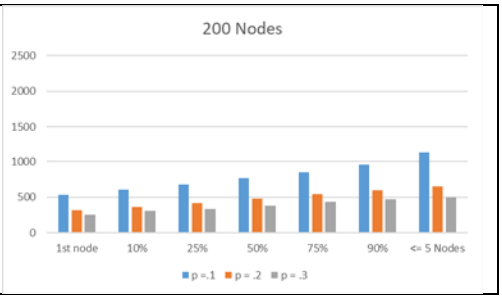
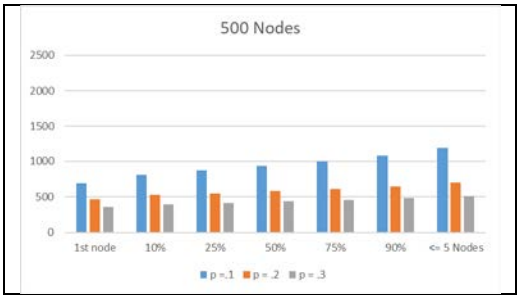
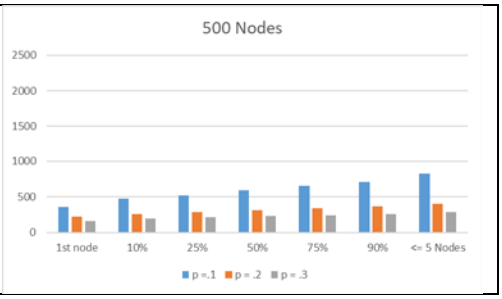
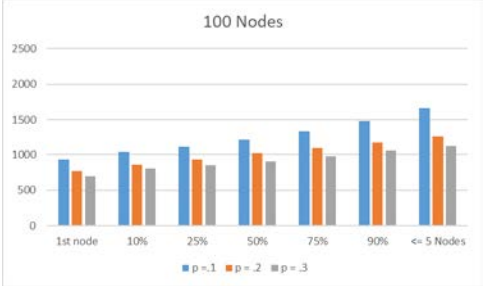
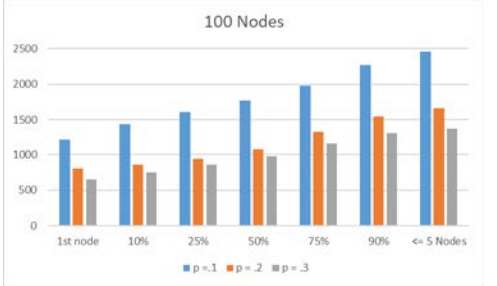
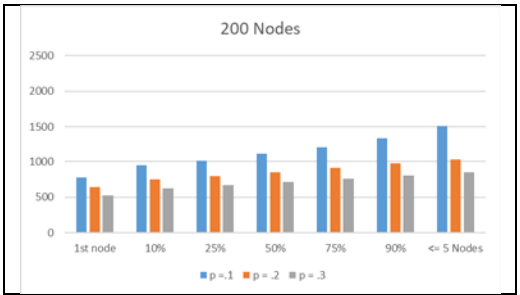
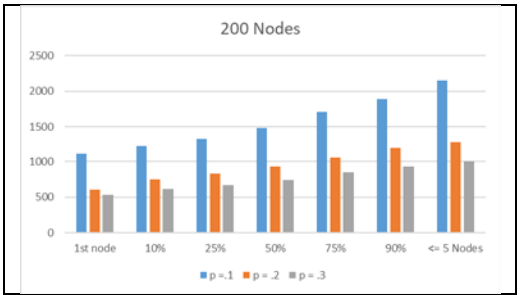
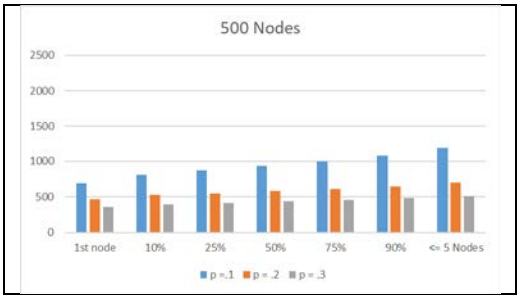
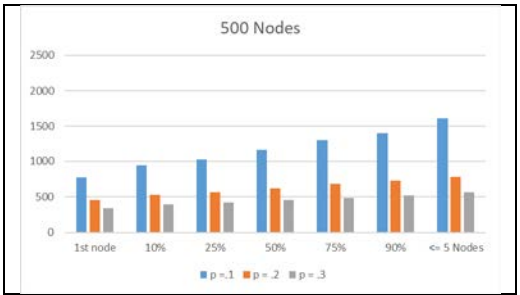
Micro-Sensors Initial Power = 0.5 Joule(s) CH to BS Packet = 6400	Raspberry PI Initial Power = 1.0 Joule(s) CH to BS Packet = 3200
	
	
	

Table 17. RPi with Initial Power of 2.0 j and Packet of 3200

Micro-Sensors Initial Power = 0.5 Joule(s) CH to BS Packet = 6400	Raspberry PI Initial Power = 2.0 Joule(s) CH to BS Packet = 3200
	
	
	

LIST OF REFERENCES

Albaladejo, C., Fulgencio, S., Torres, R., Sanchez, P., & Lopez, J. A. (2012, July 16). A low-cost sensor buoy system for monitoring shallow marine environments. *Sensors, 12*, 9613–9634. http://www.mdpi.com/1424-8220/12/7/9613

Anitha, A., & Mythili, S. (2016, September). A survey on secure routing in multi-hop wireless network. *International Journal of Advanced Research in Computer Science, 5*(5), 72–74.

Arellano, R. L., Pringle, R. G., & Sowell, K. L. (2015, December). *Analysis of rapid acquisition processes to fulfill future urgent needs* (Master's thesis). Retrieved from https://calhoun.nps.edu/handle/10945/47836

Arthur, C. (2012, January 24). The history of smartphones: Timeline. *The Guardian*. Retrieved from httpsr://www.theguardian.com/technology/2012/jan/24/smartphones-timeline

Belding, A. R. (2017, March). *In-network processing on low-cost IoT nodes for maritime surveillance* (Master's thesis). Retrieved from https://calhoun.nps.edu/handle/10945/53032

Becker, C. D. (2014, June 09). PEO C4I 2014 acquisition gaps for science & technology. Retrieved from http://www.public.navy.mil/spawar/PEOC4I/Documents/PEOC4I_ST_Acq_Gaps June2014S.pdf

Becker, C. D. (2016, December 08). FY17 PEO C4I science and technology capability gaps. Retrieved from http://www.public.navy.mil/spawar/PEOC4I/Documents/PEO%20C4I%20Acquisition%20Gaps%20for%20ST%20Jan%202017.pdf

Bi, Y., Shan, H., & Shen, X. S. (2016, March). A multi-hop broadcast protocol for emergency message dissemination in urban vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, *17*(3), 736–750. https://doi.org/ 10.1109/titsn.2015.2481486.

Blom, J. D. (September, 2010). *Unmanned aerial systems: A historical perspective.* Fort Leavenworth, KS: Combat Studies Institute Press. Retrieved from http://usacac.army.mil/cac2/cgsc/carl/download/csipubs/OP37.pdf

Cañedo, J., Skjellum, A., & Ginn, S. (2016, December 01). Adding scalability to Internet of Things gateways using parallel computation of edge device data. *High Performance Extreme Computing Conference (HPEC), 2016 IEEE*. Retrieved from http://ieeexplore.ieee.org.libproxy.nps.edu/document/7761601/

Cid-Fuentes, R. G., Naderi, M. Y., Chowdhury, K. R., Cabellos-Aparicio, A., & Alarcón E. (2016, December 12). On the scalability of energy in wireless RF powered Internet of Things. *IEEE Communications Letters*, *20*(12), 2554–2557. https://doi.org/10.1109/lcomm.2016.2612189

Comeau, F., & Aslam, N. (2011, January 01). Analysis of LEACH energy parameters. *Workshop on Emerging Topics in Sensor Networks (EmSeNs 2011)*. Retrieved from https://doi.org/10.1016/j.procs.2011.07.131

Cypress Semiconductor Corporation. (n.d.). *CYW4343*, Retrieved from http://www.cypress.com/file/298076/download

Dempsey, M. E. (2013, October 22). *Joint Publication 2–0; Joint Intelligence*. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf

Department of Defense, (2012, November). *Unmanned systems integrated roadmap – FY2103 – 2038 (2013).* Retrieved from https://www.defense.gov/Portals/1/Documents/pubs/DOD-USRM-2013.pdf

Đurišić, M. P., Tafa, Z., Dimić, G., & Milutinović, V. (2012, June). A survey of military applications of wireless sensor networks. *In Embedded Computing (MECO), 2012 Mediterranean Conference on* (196–199). IEEE.

Gardasevic, G., Veletic, M., Maletic, N., Vasiljevic, D., Radusinovic, I., Tomovic, S., & Radonjic, M. (2016, October 25). The IoT architectural framework, design issues and application domains. *Wireless Personal Communications*. *92*(127). Retrieved from https://doi.org/10.1007/s11277-016-3842-3

Gartner Study Finds a 31% Spike in IoT worldwide. (2017, May 01). *Information management*, *51*(3). Retrieved from http://search.proquest.com/docview/1923658603/

Gertler, J. (2012, January 3). U.S. unmanned aerial systems. Retrieved from https://fas.org/sgp/crs/natsec/R42136.pdf

Gortney, W. E. (2012, February 08). *Joint Publication 3–13.1; Electronic Warfare.* https://www.usna.edu/Training/_files/documents/References/3C%20MQS%20References/2015-2016%203C%20MQS%20References/Joint%20Publication%203-13.1_Electronic%20Warfare_FEB2012.pdf

Heinzleman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002, October 04). An application-specific protocol architecture for wireless microsensor networks, *IEEE Transactions on Wireless Communications*. *1*(4), 660–671.

Homaei, M. H. (2014, October 19). *LEACH (Low Energy Adaptive Clustering Hierarchy protocol) v. 1.1*. Retrieved from https://www.mathworks.com/matlabcentral/fileexchange/48162-leach--low-energy-adaptive-clustering-hierarchy-protocol-#feedbacks

Honegger, Barbara (2010, August 02). NPS Pioneers "Seaweb" underwater sensor networks. Retrieved from https://web.nps.edu/About/News/NPS-Pioneers-Seaweb-Underwater-Sensor-Networks.html

International Electrotechnical Commission (2014). *Internet of Things: Wireless sensor networks, white paper*. Geneva: Switzerland. Retrieved from http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf

Jones, K. D., & Dobrokhodov, V. N. (2016, October 04). *Multirotor mobile buoy for persistent surface and underwater exploration*. (Master's thesis). Retrieved from https://calhoun.nps.edu/handle/10945/50216

Kafi, M. A., Challal, Y., Djenouri, D., Doudou, M. Bouabdallah, A., & Badache, N. (2013). A study of wireless sensor networks for urban traffic monitoring: Applications and architectures. *ScienceDirect, 19*, 617–622. https://doi.org/10.1016/j.procs.2013.06.082

Kahn, S., Pathan, A. K., & Alrajeh N. A. (Eds.) (2012). *Wireless sensor networks: Current status and future trends*. Boca Rotan, FL: CRC Press.

Karl, H. & Willig, A. (2007). *Protocols and architectures for wireless sensor networks* Chichester, West Sussex, England: John Wiley & Sons Ltd. (pbk. ed.).

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

Kontogiannis, T. (2012, September). *Ad-hoc sensor networks for Maritime interdiction 0perations and regional security*. (Master's thesis). Retrieved from https://calhoun.nps.edu/handle/10945/17389

Liquid Robotics (2017, September 07). Liquid Robotics announces next generation of the Wave Glider, unmanned surface vehicle. Retrieved from https://www.liquid-robotics.com/press-releases/liquid-robotics-announces-next-generation-of-the-wave-glider-unmanned-surface-vehicle/.

MathWorks (n.d.), MathWorks File Exchange. Retrieved from https://www.mathworks.com/matlabcentral/fileexchange?term=leach

Maupin, M.S. (2016, March). *Fighting the network: MANET management in support of littoral operations*. (Master's thesis). Retrieved from https://calhoun.nps.edu/handle/10945/48561

Meddeb, A. (2016, July). Internet of Things standards: Who stands out from the Crowd? *IEEE Communications Magazine*. 0163–6804/16. Retrieved from http://ieeexplore.ieee.org.libproxy.nps.edu/document/7514162/

Meister, J. (2015, October 15). $178M Navy contract awarded for submarine-seeking sonobuoys. *Real time digital reporter*. Retrieved from https://www.pddnet.com/news/2015/10/178m-navy-contract-awarded-submarine-seeking-sonobuoys

MQTT.org (n.d.) MQTT.org. Retrieved from http://mqtt.org/

Mu, D., Ge, Y. & Sha, M. (2017, June). Adaptive radio and transmission power selection for Internet of Things. *2017 IEEE/ACM 25th International Symposium on Quality of Service (IWQoS)*. 1–10. Retrieved from http://ieeexplore.ieee.org.libproxy.nps.edu/document/7969111/

National Oceanic and Atmospheric Administration (NOAA). (2011, February 14). Weather systems & patterns. Retrieved from http://www.noaa.gov/resource-collections/weather-systems-patterns

NAVAIR (n.d.) Small tactical unmanned aircraft systems. Retrieved from http://www.navair.navy.mil/index.cfm?fuseaction=home.display&key=4043B5FA-7056-4A3A-B038-C60B21641288

Open-Mesh (n.d.). B.A.T.M.A.N. Retrieved from https://www.open-mesh.org/projects/open-mesh/wiki

Persistent Systems. (n.d.). Retrieved from http://www.persistentsystems.com/

Raspberry Pi Foundation, (n.d.). Power supply. Retrieved from https://www.raspberrypi.org/documentation/hardware/raspberrypi/power/README.md

Raspberry Pi Foundation, (n.d.). Raspberry Pi 3 is out now! Specs and, benchmarks, and more. Retrieved from https://www.raspberrypi.org/magpi/raspberry-pi-3-specs-benchmarks/

Raspberry Pi Foundation, (n.d.). *Raspberry Pi Model 3 B, specifications*. Retrieved from https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

Ray, P.P. (2016, October 08). A survey of Internet of Things architectures. *Journal of King Saud University—Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2016.10.003

RC Electronics. (n.d.) Retrieved from http://www.rc-electronics-usa.com/battery-electronics-101.html

Richadrson, J. M. (2016, January). *A design for maintaining maritime superiority, version 1.0*. Retrieved from http://www.navy.mil/cno/docs/cno_stg.pdf

Rowden, T. (2017, January 9). *The U.S. Navy's Surface Force strategy: Return to sea control*. Retrieved from http://navylive.dodlive.mil/2017/01/09/the-u-s-navys-surface-force-strategy-return-to-sea-control/

Rowden, T., Gumataotao, P., & Fanta, P. (2015, January). Distributed Lethality. *Proceedings Magazine*, *141*(1), 343. Retrieved August from https://www.usni.org/magazines/proceedings/2015-01/distributed-lethality

Scaparrotti, C. M. (2013, February 05). *Joint Publications 3–12 (R); Cyberspace operations*. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

Scott, K. D. (2017, July 05). *Joint Publication 2–01; Joint and National Intelligence support to military operations*. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp2_01_20170705.pdf

Sharma, V., Saini, D.S., & Solan, W. (2015, May). Performance investigation of advanced multi-hop and single-hop energy efficient LEACH protocol with heterogeneous nodes in wireless sensor networks. Paper presented at the *2015 Second International Conference on Advances in Computing and Communication Engineering*. 192–197. http://ieeexplore.ieee.org.libproxy.nps.edu/document/7306677/

Silvus Technologies (n.d.). Streamcaster radios. Retrieved from http://silvustechnologies.com/products

Sohraby, K., Minoli, D. & Znati, T. (2007, April 06). *Wireless sensor networks: Technology, protocols, and applications*. Hoboken, New Jersey: John Wiley & Sons Ltd.).

Solarwinds (n.d.). Response time viewer for Wireshark. Retrieved from https://www.solarwinds.com/free-tools/response-time-viewer-for-wireshark

Sonobuoy TechSystems. (n.d.). All products from Sonobuoy TechSystems. Retrieved from http://www.sonobuoytechsystems.com/products/

Statista. (n.d.). Number of mobile phone users worldwide 2013–2019. Retrieved from https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/

Stratopoulos, T. C. (2016, May 08). Emerging technology adoption and expected duration of competitive advantage. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2695858

Todolí-Ferrandis, D., Silvestre-Blanes, J., Santonja-Climent, S., Sempere-Paya, V., & Vera-Pérez, J. (2017). Deploy & forget wireless sensor networks for itinerant applications. https://doi.org/10.1016/j.csi.2017.09.002

TrellisWare (n.d.). *TrellisWare*. Retrieved from https://www.trellisware.com/

Warrier, M. M., & Kumar, A. (2016). An energy efficient approach for routing in wireless sensor networks. https://doi.org/10.1016/j.protcy.2016.08.140

White, J. W. (2014, January 16). Advanced maritime domain awareness (MDA) for the fleet and the nation. Retrieved from http://navylive.dodlive.mil/2014/01/16/advancing-maritime-domain-awareness-mda-for-the-fleet-and-the-nation/

White, K.A. (2013, December). *Tactical network load balancing in multi-gateway wireless sensor networks*. (Master's thesis). Retrieved from https://calhoun.nps.edu/handle/10945/39036

Villas L. A., Boukerche, A., Ramos, H. S., de Oliveira, H. A. B. F., de Araujo, R. B. & Loureiro, A. A. F. (April, 2013). DRINA: A lightweight and reliable routing approach for in-network aggregation in wireless sensor networks. *IEEE Transactions on Computers*, *62*(4), 676–689.

Zhao, J. & Cao, G. (2014, March 20). Robust topology control in multi-hop cognitive radio networks. *IEEE Transactions on Mobile Computing*. https://doi.org/ 10.1109/tmc.2014.2312715. *13*(11), 2634–2647.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California