Design Specification for Local Emergency Area Network (LEAN)

Prepared by:

Group: 4

Justin Scothorn	scothorn.2@wright.edu
Jorge Sosa Huapaya	sosahuapaya.2@wright.edu
Jeremy Van Eps	vaneps.2@wright.edu

For:

Project Sponsor: Jim Gruenberg

Course Faculty: Dr. John Gallagher
Dr. Fred Garber
Dr. Thomas Wischgoll
Dr. Subhashini Ganapathy
Ms. Brandy Foster

Document Tracking Information:

Document Version: 1
Date: May 6, 2016
Final Approval Date: May 6, 2016
Final Approval By: Justin Scothorn, Jorge Sosa Huapaya, Jeremy Van Eps

Contents

1 Executive Summary

This document outlines the proposed system design for LEAN(Local Area Emergency Network). Communication during emergency events is imperative to ICS personnel to ensure the safety and uniformity for all activity within the incident area. According to Jim Gruenberg, at times the best communication responders can use is text messaging from a smartphone [1]. This limits the capability of ICS responders to efficiently do their job. LEAN will establish stable data transmission through an ad-hoc network used for intranet connectability, providing the incident command personnel with the communication system that they need. This document is providing a detailed approach to the design and implementation for LEAN and will be viewed by ICS personnel and any relevant stakeholders.

1.1 Purpose of this document

The purpose of this document is to describe in complete detail how LEAN will be constructed and the software designed. This design document translates what was defined in the requirements document from which future teams can develop and build LEAN. This document focuses on design objectives, assumptions, requirements, constraints, standards, and functionality of key hardware and software components.

1.2 Design Scope

The overall goal of this project is to construct a Local Emergency Area Network that allows communication between Incident Command and ICS staff.

LEAN will provide an intranet for ICS responders through a wireless network managed by a centralized server and a hardened Wi-Fi repeaters cluster. LEAN will dynamically fit the range of the incident area by determining the best location for each node in the repeater cluster using an algorithm.

LEAN includes the following capabilities:

1. A portable ad-hoc network that is procedurally adaptive to any location.
2. LEAN will provide Local Area Network communication only for ICS and third party software applications.
3. LEAN will provide an intranet connection.
4. The location and amount of Wi-Fi repeaters will vary depending upon the size of the incident area.
   (a) An algorithm will be provided by the developers that upon initial setup will recommend the number of Wi-Fi repeaters needed in a particular incident area.
   (b) An algorithm will be provided by the developers that upon initial setup will recommend the best geographical location for the Wi-Fi repeater pods to be placed.
5. At minimum the product will handle 600 Mbps of bandwidth for data transfer.

6. Wi-Fi repeaters will run table driven routing protocols to automatically route information to desired nodes.

7. Wi-Fi repeaters/Pods will be hardened using a special casing/shell by the developers.

8. Pods will contain a sensor array that analyzes pod status.

LEANs design purpose is to provide a secure and reliable network infrastructure for ICS software applications. Although LEAN will be capable of allowing extra network appliances such as switches, routers, servers and technologies to connect or work over the network, the developers will not be accountable for later additions of network appliances or technologies.

Please refer to our requirements specification document for an in depth breakdown of the requirements that will be detailed in this design document.

1.3 Intended Audience and Document Overview

This section is aimed to suggest which sections of this document would be more useful for each of the following people:ICS commander, project stakeholders, technical support staff, and technical writers.

1. ICS commander will benefit from all sections of this document, they must know how the system works from start to end as well as the problem being faced, benefits and constraints of LEAN.

2. Project stakeholders will be interested in all sections of this document to better understand how their investment will be created, sections 1 and 2 will give them a better understanding of what LEAN is and what LEAN is solving, which directly correlates with what a stakeholders interests are.

3. Technical support staff will need to be familiar with sections 3 and 4 in this document so they can understand how to better maintain and troubleshoot LEAN.

4. Technical writers who will be writing user manuals for LEAN will utilize sections 3 and 4.

1.4 Definitions, Acronyms, and Abbreviations

Name	Definition
LEAN	Local Emergency Area Network
ICS	Incident Command System
Pod	Physical network device that is used in this instance as a Wi-Fi repeater and sensor data collector.
Wi-Fi	Wireless Fidelity technology.
Ad-hoc	A decentralized type of wireless network.In which each node participates in routing by forwarding data for other nodes.
Intranet	A private network accessible only to an organization's staff.
Network appliances	Hardware that can be connected to a network such as Routers, Switches, Servers.
WRP	Wireless routing protocol
HTTP	Hyper Text Transfer Protocol
WPA/WPA2	Wi-Fi Protected Access / Wi-Fi Protected Access 2
Delta Data	Data indicating a change in value
IEEE	Institute of Electrical and Electronic Engineers
DDR3 SDRAM	double data rate type three synchronous dynamic random-access memory
RAID 5	configurations that employ the techniques of striping, mirroring, or parity to create large reliable data stores from multiple computer hard disk drives.RAID 5 consists of block-level striping with distributed parity.
TCP	Transmission Control Protocol
JSON	JavaScript Object Notation
XML	Extensible Markup Language
IP	Internet Protocol
GPS	Global Positioning System
GPIO	General Purpose Input/Output
SQL	Structured Query Language is a special-purpose programming language designed for managing data held in a relational database management system.
SSL/TSL	cryptographic protocols designed to provide communications security over a computer network.

Name	Definition
EIGRP	Enhanced Interior Gateway Routing Protocol is an advanced distance-vector routing protocol that is used on a computer network to help automate routing decisions and configuration.
Distance-vector protocol	A simple routing protocol that uses distance or hop count as its primary metric for determining the best forwarding path
MAC	The media access control layer, the lower sublayer of the data link layer, provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium.
DSDV	Destination-Sequenced Distance-Vector Routing is a table-driven routing scheme for ad hoc mobile networks
AODV	Ad hoc On-Demand Distance Vector Routing is a routing protocol for mobile ad hoc networks and other wireless ad hoc networks.
TKIP	Temporary Key Integrity Protocol- a cipher that extends the basic RC4 cipher
WPS	Wireless Protected Setup button
WAP	Wireless Access Point
RC4	Rivest Cipher 4 is a stream cipher which is a symmetric key cipher where plaintext digits are combined with a pseudo-random cipher digit stream called a keystream
WEP	Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks.

1.5 References and Acknowledgments

References

[1] J. Gruenberg, "Command and coordination," In-class briefing, August 2015.

[2] B. Stone, "Why cell phone networks fail in emergencies," April 2013.

[3] Privateline. (2015, October) Pmc - the national center for biotechnology information. [Online]. Available: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1550843/

[4] CISCO. (2015, November) Mobile ad hoc networks for router-to-radio communications. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/ios/12_4t/ip_mobility/configuration/guide/ip_manet.html#wp1257934

[5] GeekStaff. (2012, June) How hot does the raspberry pi operate, a study of the operating temperatures [translated from spanish]. [Online]. Available: http://translate.google.com/translate?sl=es&tl=en&js=n&prev=_t&hl=en&ie=UTF-8&layout=2&eotf=1&u=http://www.geektopia.es/es/technology/2012/06/22/articulos/se-calienta-el-ordenador-raspberry-pi-estudio-de-sus-temperaturas-en-funcionamiento.html&act=url

[6] "Ieee standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements." *IEEE Std 802.11n-2009*, 2009.

[7] M. Stanford. (2015, October) How does 802.11n get to 600mbps? [Online]. Available: http://www.wirevolution.com/2007/09/07/how-does-80211n-get-to-600mbps/

[8] A. Wired and Cable. (2015, October) Insulation materials. [Online]. Available: http://www.awcwire.com/insulation-materials.aspx

[9] IEEE, "Ieee recommended practice for installation design and instavented lead-acid batteries for llation of stationary applications," *IEEE Std 484-2002*, 2013.

[10] MySQL. (2015, October) Using foreign keys. [Online]. Available: https://dev.mysql.com/doc/refman/5.0/en/example-foreign-keys.html

[11] w3resource. (2015, October) Structures of json. [Online]. Available: http://www.w3resource.com/JSON/structures.php

[12] w3. (2015, October) Status code definitions. [Online]. Available: http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html

[13] U. B. M. Company. (2015, October) Safe handling tips for servicing flooded lead acid batteries. [Online]. Available: http://usbattery.com/safe-handling-tips-for-servicing-flooded-lead-acid-batteries/

[14] T. B. Company. (2015, October) Frequently asked questions. [Online]. Available: http://www.trojanbattery.com/tech-support/faq/

[15] ISO/IEC. (2015, October) Information technology – security techniques – encryption algorithms. [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=37972

[16] J. Chroboczek. (2015, November) Babel a loop-avoiding distance-vector routing protocol. [Online]. Available: http://www.pps.univ-paris-diderot.fr/~jch/software/babel/

[17] C. D. of Conservation. (2015, November) California strong motion instrumentation program - frequently asked questions. [Online]. Available: http://www.conservation.ca.gov/cgs/smip/Pages/faq.aspx

[18] MIKEGRUSIN. (2015, November) Tsl2561 luminosity sensor hookup guide. [Online]. Available: https://learn.sparkfun.com/tutorials/tsl2561-luminosity-sensor-hookup-guide

[19] Intel. (2015, November) Intel xeon processor e5345. [Online]. Available: http://ark.intel.com/es/products/28032/Intel-Xeon-Processor-E5345-8M-Cache-2_33-GHz-1333-MHz-FSB

[20] Adafruit. (2015, November) Learn raspberry pi: Console cable. [Online]. Available: https://learn.adafruit.com/system/assets/assets/000/003/129/medium800/learn_raspberry_pi_console_cable.jpg?1396791828

[21] ——. (2015, November) Adafruit ultimate gps breakout. [Online]. Available: http://www.adafruit.com/products/746

[22] SparkFun. (2015, November) Sparkfun triple axis accelerometer breakout - adxl335. [Online]. Available: https://www.sparkfun.com/products/9269

[23] ——. (2015, November) Sparkfun weather shield. [Online]. Available: https://www.sparkfun.com/products/12081

[24] xtreamer.net. (2015, November) Usb antenna. [Online]. Available: http://www.xtreamer.net/ultra2/images/products/usb-antenna.png

[25] Solarstik.com. (2015, November) Flooded lead acid. [Online]. Available: http://www.solarstik.com/sites/default/files/content/flooded-lead-acid.jpg

[26] Amazon. (2015, November) Noco hm485 dual 8d commercial grade battery box for automotive, marine and rv batteries. [Online]. Available: http://www.amazon.com/NOCO-HM485-Commercial-Automotive-Batteries/dp/B00319MIWU

[27] RaspberryPi.org. (2015, November) Pi 2 model b. [Online]. Available: https://www.raspberrypi.org/wp-content/uploads/2015/02/Pi_2_Model_B.png

[28] R. Natarajan. (2010, August) Raid 0, raid 1, raid 5, raid 10 explained with diagrams. [Online]. Available: www.thegeekstuff.com/2010/08/raid-levels-tutorial/

[29] security.stackexchange.com/Begueradj. (2015, November) Significance of the difference between dsa and rsa in signature verifying speed. [Online]. Available: http://security.stackexchange.com/questions/97411/significance-of-the-difference-between-dsa-and-rsa-in-signature-verifying-speed

[30] Amazon. (2015, November) Hiro h50194 wireless 802.11n usb wifi wlan network adapter high gain 5dbi omnidirectional external antenna wps hotkey rohs windows 10 8.1 8 7 vista xp 32-bit 64-bit. [Online]. Available: http://www.amazon.com/H50194-Wireless-802-11n-Omnidirectional-External/dp/B003516BJU/ref=sr_1_1/190-5835275-5906436?ie=UTF8&qid=1447420063&sr=8-1&keywords=high+gain+usb+wifi+adapter

[31] blog.adafruit.com. (2015, November) Raspberry pi 2 model b v1.1. [Online]. Available: https://blog.adafruit.com/wp-content/uploads/2015/02/Pi_II_top_ORIG.jpg

[32] Amazon/NOCO. (2015, November) Noco hm485 dual 8d commercial grade battery box for automotive, marine and rv batteries. [Online]. Available: http://www.amazon.com/NOCO-HM485-Commercial-Automotive-Batteries/dp/B00319MIWU

[33] adafruit.com. (2015, November) Adafruit console cable. [Online]. Available: http://www.adafruit.com/product/954

[34] J. C.-P. W. M. Abolhasan, Brett Hagelstein. (2015, November) Real-world performance of current proactive multihop mesh protocols. [Online]. Available: http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1747&context=infopapers

[35] C. N. R. Institute. (2015, November) Detecting distributed denial of service (ddos) attacks in wireless mesh network. [Online]. Available: http://www.cnri.dit.ie/research.mesh.security.html

[36] J. Morrow. (2011, February) Optimal placement of radio repeater networks. [Online]. Available: http://www.math.washington.edu/~morrow/mcm/10754.pdf

[37] K. S. S. Laxmi Nissanka Rao. (2015, November) Temporal key integrity protocol(tkip). [Online]. Available: http://www.slideserve.com/niesha/temporal-key-integrity-protocol-tkip

2 Problem Statement

During an ICS event, communication between ICS personnel and command is imperative, to maintain structure and insure safety and efficiency of the event objectives. During an emergency incident, for example the Boston marathon bombings in 2013, cellular networks that are imperative for relaying information between ICS personnel became saturated with the local populous trying to contact their loved ones[2].

According to Jim Gruenberg, the need for stable communication during an ICS event is lacking in reliability and sometimes is obsolete all together[1]. The best means of communication when the communication infrastructure is becoming overloaded is text-messaging because messages can be queued and sent out when the tower has the resources.

ICS needs a closed, controllable, secure, stable network which within can send commands and update personnel without competing for bandwidth with the local populous. If ICS had this stable network, lives could be saved and further disastrous consequences due to a lack of communication between ICS command and personnel would have a higher probability of being avoided.

Some challenges in establishing a stable communication network include:

1. Stable connectivity over entire incident area, with little or no data loss.
2. Environmental challenges such as weather conditions and temperature with regard to equipment functionality.
3. A system that can scale as needed for any ICS event.

2.1 Historical Introduction

In the 1920s, the development of radio telephony, or voice communications using radio waves in safety and military communications started. By June 1942, the War Emergency Radio Service was created. In 1952, the Radio Amateur Civil Emergency Services were formed in conjunction with the federal Civil Defense effort when federal and local authorities realized the need for disaster and emergency communications that involved all aspects of civil life. After this, the world of technology had been evolving at a much higher rate than the level of sophistication of civil emergency planning; especially when transistors and integrated circuits came into existence [3].

The development of cellular phones, microwave relays, and fiber optic cables has allowed enormous advances in telecommunications, yet many of these techniques are still bound to the backbone of wire at some level. Therein lays the great potential for disruption in natural or man made disasters. Emergency services telecommunications, including public safety radio systems, have exhibited tremendous growth and improvement in capabilities, yet Trunking radio systems and other methods are still breakable as has been shown in recent natural disasters [3]. Hence the imperative necessity of coming with a better solution using the technologies available nowadays.

During the terrorist attacks on September 11th 2001, communication means were rendered useless.The system was brought down by damage or was overloaded by the massive amount of people trying to use the network. This communication failure would prove to be

a difficult task for ICS personnel to overcome, so they could communicate efficiently among themselves and better aid in the Incident response objectives.

LEAN is designed to provide a secure, stable communication network for ICS personnel. LEAN will be separate from public communication systems to eliminate the possibility of network overload. LEAN will be hardened to help prevent damage and thus preventing the system from not being available.

2.2 Market Analysis and Relevant Art

The idea of a large scale ad-hoc network like LEAN is currently on the cutting edge of technology. The LEAN development team has reviewed many papers covering techniques on this subject as it is a new highly researched technology. The closest product to the solution that LEAN proposes is the CISCO MANET[4]. LEAN separates itself from MANET by making it environmentally aware with the pod sensor arrays. This idea allows the network to be maintained and monitored to avoid communication loss.

2.3 Impact of Success

When completed, LEAN will provide reliable communication for ICS personnel. This will result in more efficient incident response communication that could mean the difference between life and death. LEAN will strengthen safety and effectiveness regarding ICS personnel by opening a new line of communication for 3rd party apps that can not exists without network connectivity.

3 Context of Design Solution

In order to ensure success, LEAN proposes to meet the following design solutions:

3.1 Design Objectives

1. LEAN will provide reliable data communication. LEAN will be a solution for ICS command that provides a stable intranet for use only by ICS personnel. LEAN will not provide connection outside of intranet like cellular data. LEAN will implement an ad-hoc wireless intranet network using WI-Fi repeater pods that are self-aware and scalable to every ICS incident.

2. LEAN will consist of stable WI-Fi repeater pods resistant to adverse conditions. LEAN will consist of a number of Wi-Fi repeater pods that will obtain environmental statistics and can be placed anywhere in the incident area as needed. The pods will be resistant to extreme temperatures, water, and seismic activity. The pods will not be able to resist temperatures above 138 degrees Fahrenheit [5]. The pods will be encased in a protective shell and will be self-aware. They will maintain a connection with the central server so ICS command can monitor their status.

3. An algorithm to determine number of pods needed and where the pods should be placed will be installed on the central server. During initial setup of incident command, LEAN will be given inputs for incident area location and number of ICS personnel to be on the LEAN network. LEAN will then provide the number of pods needed to cover the incident area as well as optimal locations for each pod to be placed.

4. LEAN will provide sufficient throughput for quick data communication.The bandwidth of the LEAN network will operate at 2.4 GHz, with a data rate of 600 Mbps. This is achieved by using the Raspberry Pi, and the proper Wi-Fi radio that can handle the required speed.

3.2 Design Assumptions

1. The LEAN development team will have enough background knowledge to design all software and algorithms to be installed on LEAN.

2. LEAN will use the Raspberry Pi as the main processing unit in the pods and will be powerful enough to compute routing tables, collect sensor data, and transmit data effectively.

3. The outer casing for the pods will be durable enough to protect the equipment from damage, weather, and atmospheric extremes while also not affecting the pods functionality.

4. Operating temperature will not exceed 138 degrees Fahrenheit as tested by Geekstaff, further testing will be done to verify [5].

5. LEAN will not provide storage space on it's centralized server, the applications using LEAN's network will provide their own means of data storage.

6. ICS logistics will be responsible for setup and maintenance of LEAN.

7. The battery with its protective casing will meet all official standards and safety requirements while also meeting the design requirements.

3.3 Design Requirements

3.3.1 User Interfaces

Requirement: The pods will assist in their placement by outputting network connectivity information through a console interface.

1. The console interface will be provided through a USB access port.

2. Administrators will connect through a laptop and open a bash shell to log in.

Requirement: The central server will provide a display that visualizes all pods placed in the emergency area on a map to be monitored for damage.

1. A monitor attached to the central server will display a map with green icons representing undamaged pods.
2. All pods will be located at their respective geolocation on the map.
3. Each pod can be selected to display their sensor array information and any anomaly detection.
4. Anomalies will be reported by flashing the pod icon red on the map.
5. Anomaly detection will begin an emergency mode that increases sensor interrogation for real time monitoring.

Requirement: Pod's system will be password protected to limit access to administrators only.

Requirement: The central server will be password protected to limit access to administrators only.

Requirement: The wireless network will be password protected to limit access to only ICS personnel.

1. LEAN will provide a WPA2 encrypted wireless connection that responders will connect to as if they were connecting to their business Wi-Fi.
   (a) LEAN will provide no user interaction through wireless connection. This will only be provided by third party applications.
2. ICS Unit specific passwords will be used to connect.

3.3.2 Hardware Interfaces

Requirement: The pods will have the ability to estimate their geolocation for visualization on a map.

1. Each pod will be equipped with a GPS sensor to estimate their geolocation.
   (a) Data will be interrogated at a maximum of once every thirty minutes to preserve pod battery life.

Requirement: The pods will have the ability to be environmentally aware to detect damage and alert administrators if they need repair or replacement.

1. Each pod will be equipped with an accelerometer to detect movement and seismic activity.
   (a) Data will be interrogated at a minimum of once every ten seconds.
2. Each pod will be equipped with a weather chip to detect the environment they're placed in.
   (a) Contains a minimum of one luminosity, temperature, and barometric sensor.
   (b) Luminosity sensor will be interrogated at a minimum of once every five minutes.
   (c) Temperature sensor will be interrogated at a minimum of once every five minutes.
   (d) Barometric sensor will be interrogated at a minimum of once every twenty minutes.
3. Each pod will be equipped with a power level sensor to detect if battery levels are low
   (a) The power level sensor will be interrogated once every five minutes.

Requirement: Each pod will act as a repeater to extend coverage over an emergency area.

1. Each pod will be equipped with a Wi-Fi radio
   (a) The radio will meet at a minimum IEEE standard 802.11n[6].
   (b) The radio configuration will have at a minimum a maximum data rate of 600 Mbps like what is provided by the IEEE standard 802.11n [7].

Requirement: Each pod will be battery powered

1. Each pod will be equipped with a flooded lead acid battery
   (a) Must have a minimum charge capacity of 30 Ahrs.
   (b) Terminal connections will be sealed and weather proofed.
   (c) The battery will be easily detachable from the rest of the hardware.
   (d) The battery will be insulated with an acid-resistant material. The following is a consideration for the insulating material:
      i. A layered design consisting of an inner layer of polyvinyl chloride (PVC) for acid and environmental protection, a middle layer of semi-rigid PVC (SR-PVC) to add abrasion resistance, and an outer layer of neoprene (polychloroprene) for excellent flame retardation[8].
   (e) The ventilation system will limit hydrogen accumulation to less than 2% of the total volume[9].

Requirement: The central server intranet connection will meet at a minimum IEEE standard 802.11n[6].

Requirement: The central server will be able to handle all ICS wireless traffic load.

1. Additional servers will be added when traffic load has exceeded 85% of the servers processing power.

3.3.3 Software Interface

Requirement: The pods will have the ability to display other pods that are within connectivity range to assist in placement.

1. The software will be executed through a bash shell.
2. The software will detect power levels of pods within range and output them through a bash shell via USB.
3. The software will refresh the power levels of the detected pods at a minimum of every 15 seconds.

Requirement: The central server will have the ability to store sensor information.

1. The server will store sensor data into databases according to the sensor type.
   (a) Joined tables through a foreign key defined as the pod ID [10].
   (b) No null data will be stored for time stamps that don't contain data for every sensor.
2. The server will only run MYSQL databases for uniformity.
3. Every data write will be done in one single query.

Requirement: Every pod will have the ability to interrogate a sensor array connected to the GPIO of the raspberry pi.

1. Sensor interrogation will be executed by python scripts started when the pods are placed.
   (a) There will be a separate python program for each of the sensor array endpoints to interrogate.
   (b) Each timer that tracks the sampling rate of a sensor endpoint will run on a separate thread.
   (c) When a sensor array endpoint has been sampled, the value will be immediately sent with JSON encoding described in section 3.1.3 p2.

Requirement: Every pod will have the ability to send sensor information to the central server.

1. The pods will use JSON to encode sensor data packets.
   (a) Each pod to server transmission will use one JSON hash with two keys; one for identification and one for sensor values[11].
      i. The identification key will have one value containing an unique ID describing the pod.
      ii. The sensor values key will contain one value for each endpoint in the sensor array.
   (b) Each server to pod transmission will use one JSON hash with the same keys received and flags.
      i. Flags pertaining to HTTP status codes[12].
      ii. Flags pertaining to pod normal/emergency mode.
2. The pods will compute routing tables.
   (a) The node cluster will run the table driven routing protocol, wireless routing protocol (WRP) [13].
   (b) The WRP provides extra information compared to other table driven protocols that will be useful for node integrity.

Requirement: The central server will have the ability to estimate the initial amount of pods needed for an emergency area.

Requirement: The central server will have the ability to estimate the location that every pod needs to be in to provide total coverage for an emergency area.

1. Pod placement will be estimated by software that examines the surrounding geographical location.
2. Pod placement will be dependent on streets and field of view so that unrealistic locations are not suggested.

3.3.4 Communications Interfaces

Requirement: LEAN must use a communication protocol that can work in a commonly used web browser.

1. LEAN will operate on the HTTP-Intranet to achieve the fastest speeds possible.

3.3.5 Functional Requirements

Requirement: Each pod will act as a wireless access point for ICS personnel.

1. Wireless intranet will provide basic connectivity to a user.
   (a) Share their information with a central server.
   (b) 3rd party applications that need a network.

Requirement: Every pod will be able to detect its environment and its location in it.

1. Every pod will be equipped with a sensor array.
2. A GPS sensor will be included in the sensor array.
   (a) Geographical location will be collected for placing the pods on an interactive map.
   (b) When geographical location can not be updated, it will be marked as an anomaly.
   (c) When delta data indicates a large change in geographical position it will be marked as an anomaly.
3. A Temperature sensor will be included in the sensor array.
   (a) Collect thermal data to determine operating conditions for the pods.
   (b) When maximum threshold temperature is passed, it will be marked as an anomaly.
   (c) When delta data indicates a fast change in temperature it will be marked as anomaly.
   (d) When temperature can not be collected, it will be marked as an anomaly.
4. A Luminosity sensor will be included in the sensor array.
   (a) Collect light intensity data.
   (b) When minimum light intensity threshold has been exceeded, it will be marked as an anomaly.
   (c) When maximum light intensity threshold has been passed, it will be indicated as an anomaly.
   (d) When delta data indicates a loss of light or a great increase in light intensity, it will be marked as an anomaly.
   (e) When light intensity can not be collected, it will be marked as an anomaly.
5. A Barometric sensor will be included in the sensor array.
   (a) Collect elevation data to add another element to location services.
   (b) When delta data indicates pressure change threshold has been exceeded, it will be marked as an anomaly.

6. A Power sensor will be included in the sensor array.
   (a) Detect battery charge capacity.
   (b) When battery charge capacity has reached a minimum threshold, it will be marked as an anomaly.
7. An Accelerometer sensor will be included in the sensor array.
   (a) Collect movement and seismic data.
   (b) When data indicates that the pod has moved beyond the maximum threshold, it will be marked as an anomaly.
   (c) When seismic activity has passed the maximum threshold, it will be marked as an anomaly.

Requirement: The central server will have the ability to detect anomalies in the pod network.

1. The central server will use sensor data to detect anomalies
   (a) Detect abnormal data that does not characterize with the normal operating data of the sensors.
   (b) Detect threshold data that exceeds conditions resulting in pod damage.
   (c) Detect a large change in data (delta data) that would indicate abnormality.
2. The central server will be able to put the pods into emergency or normal mode
   (a) When an anomaly has been detected, emergency mode will be entered.
   (b) Will increase sampling rate of all sensors to gather enough data to directly monitor the reason for an anomaly.

3.4 Design Constraints

1. Battery weight will need to be less than 100 pounds which will help determine portability by weighing the pods down but not being to heavy to be able to relocate.
2. Battery cannot be tilted more than 22 degrees from vertical as defined by Trojan Battery Company [14], this type of condition could occur during seismic events or adverse environmental conditions.
3. Processing speed - The default clock speed for a Raspberry Pi is 700 MHz.This will limit the processing speed of the Wi-Fi pods.
4. Bandwidth of LEAN network will operate at 2.4 GHz.This will limit the data transmission throughput capabilities.
5. LEAN will also contain a Wi-Fi radio that meets IEEE standard 802.11n with a data rate of 600 Mbps [7].

3.5 Design Standards

LEAN will meet the following design standards:

1. Network standard - IEEE 802.11n [7]. Used for wireless network access.
2. Battery standard - IEEE Std 484-2002 [9]. Used for maintaining battery safety.
3. Security standard - ISO/IEC 18033 [15]. Used to ensure data is stored securely.

3.6 Design Functionality

3.6.1 Central Server Communication

The central server will be where a majority of the network traffic will be directed too. LEAN will follow a HTTP client-server architecture that establishes a TCP connection where the pods will be the clients. The reason for choosing a client-server architecture over a peer-to-peer is to reserve processing power on the pods for transmitting and collecting data and computing routing tables. For storing and exchanging data, JSON will be used for its simplicity in comparison to XML.

JSON Object Schema: LEAN will use JSON to fully describe the data being transmitted and where the data is coming from. The object schema will consist of...

1. ID
2. Sensor Names
3. Sensor Values

The ID will be used to identify individual pods. The ID will be the IP address that the pod has on the network. The sensor name will identify what sensor value is being sent, and these sensor names will equal the sensor value. Every time data is collected it will be encoded using this JSON object schema.

Operating System: The most important considerations in choosing the operating system to support LEAN are reliability, security, flexibility, compatibility, and affordability. The Linux Operating System was chosen to run in both, the central server and the Wi-Fi repeater pods. Particularly, Ubuntu Linux 14.04 LTS distribution for the central server, and Raspbian Linux Jessie-kernel version 4.1 for the pods. Some of the advantages of the Linux Operating system are:

1. Stable and free/open source.
2. Less vulnerable to computer malware.
3. Requires less hardware specifications to run.
4. Many different distributions to choose from.

5. One of the most secure operating systems.

6. Compatible with most hardware vendors.

7. Large amounts of online documentation for troubleshooting and support.

Routing Protocol: The Routing Protocol chosen for LEAN is Babel due to its loop avoiding capabilities, fast convergence properties, and compatibility with the Linux distribution in the pods and central server.

Based on protocols such as DSDV, AODV and Cisco's EIGRP, Babel is a distance-vector protocol that will allow the developers to have the flexibility to choose metrics for smart routing in the wireless mesh network. Some of these metrics will include hop-count, packet loss, radio diversity and delay-based. Communication in LEAN will be greatly benefited by Babel's almost immediate convergence by using triggered updates and explicit requests for routing information after the link quality measure has completed. LEAN will also benefit from Babel's loop avoiding capabilities, which once Babel detects a wireless link, it disables split horizon and uses a metric, based on packet loss, that is designed for the 802.11 (Wi-Fi) MAC.

Among other advantages, Babel's routing information can be retrieved through a web interface; this, will allow the developers to visualize the routes for improvements and troubleshooting of the network. [16]

Server to Client: The server will have two reasons for communicating with the pods:

1. Updating the mode that the pod is in.

2. Confirming packet transmission.

There are two modes on each pod: emergency and normal. In normal mode, the pods collect data on the intervals described in the requirements. As the pod is normally gathering data it is being immediately sent to the central server for analysis and the data is kept on the pod no longer than the time it takes to confirm the data has been sent.

The data is analyzed for anomalies based on thresholds that the sensors will not measure above unless the pod has been or is in danger of being damaged. When these anomalies are detected a message is sent to the pod to put it into emergency mode for real time analysis of the data, allowing the admins to know pod status and determine if they need attention.

Client to Server: The pods only have one reason for communicating with the server (before any future 3rd party apps) which is sending the sensor data. As soon as a value is recorded from the sensor array, it is temporarily stored and sent to the central server. The reason for immediately sending this data is to avoid data loss. The sensor information needs to be stored on the server and analyzed as soon as possible so that any pod damage can be detected. If a pod goes down during an analysis of sensor data, it would not be detected as damaged.

3.6.2 Sensor Collection and Analysis

Each pod will be equipped with a sensor array to analyze its location and environment. The purpose of these sensor is to track pod status so that if any damage is received it can be detected and fixed. In this implementation of LEAN, the following sensors will be equipped:

1. GPS
2. Accelerometer
3. Weather Chip
   (a) Luminosity
   (b) Temperature
   (c) Barometric
4. Power Level

To conserve battery power and network bandwidth, the sensors will only be interrogated enough to track meaningful data.

GPS Sensor Data: The GPS sensors will be used to realize pod location. This data will be used to place the pods for initial placement algorithm calculations and to place the pods on a map for visualization at the central server.

The placement algorithm will estimate the optimal emergency area locations for the pods. While the logistic team will be placing the pods, they will be able to use GPS information to help them. Once the pods are placed, they will start collecting and transmitting GPS data.

GPS data is not critical enough to be continuously updated, therefor this data will be collected once every thirty minutes. The GPS will work in tandem with the accelerometer to determine if the pod has unexpectedly moved. As data is collected and sent to the central server, it will be analyzed and compared to previous geolocations. If data indicates that the pod has moved more than twenty meters, this means that the pod is in danger.

Once an anomaly like this is detected, the pod will receive a message to go into emergency mode and start collecting and transmitting it's data at one to ten hertz. After inspection of the data, if the anomaly is found to be true then the pod will be tracked down by the logistics team for replacement and inspection for damage.

Accelerometer Sensor Data: The accelerometer will be used to detect if the pod is being moved or if there is large seismic activity. Collection of this data requires a higher sampling rate since movement and seismic activity can happen for a short duration.

A balance needs to be found for the sampling rate of this data to conserve battery life, avoid unnecessary network traffic, and to avoid missing a movement. For this implementation of LEAN, the accelerometer will be interrogated at a minimum of seconds. At this rate, an equilibrium can be found.

The sensor will be a triple-axis accelerometer giving it the ability to detect gs in any direction. If the accelerometer detects strong motion, which is described by the California

department of conservation as being 1-2%g[17], then this is considered to be an anomaly. The pod will receive a message to enter emergency mode in which the sampling rate will increase to 1 Hertz for analysis at the central server. If the anomaly is found to be true then the logistics team will track down the pod for replacement and inspection of damage.

Weather Chip: The weather chip as explained in the requirements of section 3.3.2 will contain one luminosity, temperature, and barometric sensor. These sensors will be used to analyze the environment that the pod is in. This data is also not crucial to have a high sampling rate.

Luminosity Sensor:

The luminosity sensor will be used to detect if the pod has been unexpectedly buried by any number of environmental causes. The measurements will be in lux, which is equal to 1 lumen per square meter[18]. If damage is done to the pod, it is unlikely a large fluctuation of this data would be seen like it would in an accelerometer, therefor the sensor will be interrogated once every five minutes.

Lux analysis on the central server will associate the measurements with the time of day since these readings will change throughout the day. When lux falls below $\frac{1}{10{,}000}$ of the expected light at that time it will be marked as an anomaly. A message will be sent to the pod to put it into emergency mode; this will increase the sampling rate to 0.5 Hertz. If the anomaly is found to be true, the logistics team will replace and assess damage done to the pod.

Temperature Sensor:

The temperature sensor will be used to detect the temperature of the environment that the pod is in. Temperature measurements are not crucial enough to have a continuous sampling rate, therefor the sensor will be interrogated once every five minutes. All sensor measurements will be in degrees Fahrenheit.

In section 3.4 for the design assumptions, it is stated that the operating temperature will not exceed 138 degrees Fahrenheit; this is the currently known limit and if temperature increases beyond this threshold the pod will be at risk of damage. Upon analysis at the central server, if the measured data is within 10% of the threshold it will be marked as an anomaly. The central server will send a message to the pod changing its mode to emergency, which will increase the sampling rate of the temperature data to 1 Hertz. If the anomaly is found to be true, the logistics team will assess the environment that is causing the temperature spike increase and cautiously retrieve the pod before it becomes damaged.

Barometer Sensor:

The barometric sensor will be used to detect air pressure anomalies. This data is non crucial and is only sampled once every twenty minutes. All measurements will be converted to pascals for analysis. If the delta data shows a 4% difference between measurements it will be marked as an anomaly.

The central server will send a message to the pod changing it to emergency mode; this will increase the sampling rate to 1 Hertz. If the anomaly is found to be true, then the logistics team will examine the environment that is causing this change in pressure and asses the damage done to the pod.

Power Level Sensor: Each pod will be equipped with a power level sensor that indicates if the battery is getting low. Power consumption of the pods will not be very high, therefor the battery levels will not decrease at quick rates. This data will be sampled once every 5 minutes. If the measurement indicates battery levels have dropped close to 20% of full charge, then this will be marked as an anomaly.

The central server will send a message to the pod changing it to emergency mode; this will increase the sampling rate to 0.5 Hertz. Upon confirmation of the anomaly the logistics team will replace the battery on the pod immediately.

Storing the Data: Once this data is received by the central server, the packet will be queried and stored in a database using MySQL. Anytime this data needs to be analyzed, it will be done by accessing these databases.

3.6.3 Central Server

Disk Storage: The central server will use RAID 5 disk storage to ensure secure and reliable data storage for sensor data and algorithm implementation. LEAN will use 5 hard disks with one being a spare. This will allow for up to two disk drive failures and the the system will continue to run without data loss. Implementation details will be outlined in section 4.1.1

Central Server Pod Mapping: The central server will have the capability of mapping all the pod locations onto a monitor for visualization by the logistics team. This interface will also show the status of the pods based on their sensor data. On a map of the location, each pod will be a green light. Each of these lights are clickable, and when clicked they display the current sensor information.

When an anomaly has been detected the pod will light up red. The logistics unit then has a choice to view the sensor data already received to see if it is a true anomaly, or send a message to the pod to put it into emergency mode. The logistic team member will then be able to observe the measurements from the sensors in real time and confirm if there is an anomaly or not.

Security: MySql is the database that will used on the central server with LEAN. MySql can be vulnerable to attack, there are basic attacks like finding systems with no passwords, there are SQL injection attacks, and known MySql vulnerabilities. MySql will not be run as a root user on the central server and remote access will not be allowed. LEAN will use SSL/TLS to protect information as by default MySql uses unencrypted connections between the client and server, which is not secure.

3.6.4 Wi-Fi Repeater Pod:

Wi-Fi radio range: LEAN Wi-Fi repeater pods will be equipped with a Wi-Fi radio capable of handling up to 600 Mbps as described in section 2.5 of the requirements specification document. The Wi-Fi radio will meet IEEE standard 802.11n [7].

Raspberry Pi Processor: LEAN Wi-Fi repeater pods will be equipped with a Raspberry Pi Processor that will manage all sensor data and network trafficking. The Wi-Fi radio will be plugged into the Raspberry Pi through a USB port connection. There will also be a USB port connection that can be used by the ICS logistics team to assist with pod placement and updates or maintenance.

Sensors and Battery All sensors mentioned above in section 3.6.2 will be located within or connected to the Wi-Fi repeater pods. The battery will be located within the Wi-Fi repeater pods which will act as a weight to prevent the pods from being knocked over or stolen easily.

Pod Shell Enclosure: LEAN developers will use a pre-existing commercial grade battery box as the protective casing for it's Wi-Fi pods. Each pod will have a locked removable lid with two compartments one being used for the battery and one being used for the processor and sensor array. This would assist in keeping any harmful chemicals from the battery to come into contact with the electronic equipment.

USB User Interface: Each pod will have a USB accessible port that will provide an interface while setting up the pods. The interface will require an administrator password to run any programs. This interface will have no sudo permissions, even for the administrator running it. The purpose of this interface is to get feedback from the pod to see if it is in an optimal position and connecting to LEAN properly. The initial placement algorithm makes an estimation of where to place the pods, however upon inspection it may not be a good location for a pod. The USB interface will allow the administrator to place the pod and observe what pods are in range and what their signal strength is.

Security: LEAN Wi-Fi repeater pods will be used to connect ICS command with third party applications and might be used to transmit sensitive information. The pods will have a locked casing that encloses all hardware that could potentially be accessed as a security vulnerability. The key to the pods will be maintained by the logistics team responsible for pod deployment and maintenance as well. The USB port's used by ICS logistics will not be accessible from outside the casing. Wireless network security protocols are adhered to by following the networking standard IEEE 802.11n [7], to ensure data being transmitted is secure.

3.7 User Characteristics

The following users will be using LEAN ranked from most involved/interactivity with LEAN to least:

1. ICS command - this would be the most in depth users. ICS command will be responsible for overseeing logistics during setup and maintaining LEAN. ICS command will be the personnel that will implement the algorithm to determine pod placement. They will also be required to monitor all incoming sensor related data that may be required to monitor the ICS event.

2. ICS logistics - this group will be slightly less involved then ICS command, but will need a great understanding of LEAN and it's components and implementation. Logistics will be responsible for deployment and maintenance of LEAN. They should have access to training material provided as documentation and will work closely with ICS command to ensure LEAN remains in operating condition for the entire ICS event.

3. ICS personnel - this group will need limited knowledge of the technical aspects of LEAN. This group will use LEAN for their third party applications and will only be accessing LEAN and not performing any administration activities as the logistics or ICS command. This group will however need to have knowledge of connecting their applications to LEAN which will be provided in user documentation. This group is responsible for their own third party application knowledge including how to connect the application to LEAN.

3.8 Operating Environment

1. The server will consist of a Xeon E5345 2.33Ghz quad core processor (64-bit) [19], 16GB DDR3 SDRAM, and a terabyte hard drive set up in RAID 5 format.

2. The Operating System running on the server will be Linux Ubuntu 14.04 LTS.

3. The database management system running on the server will be MySQL 5.6.

4. The location algorithm for pod placement will run on the central server and be implemented by running a script already configured for LEAN.

5. The hardware over which the Wi-Fi repeaters will operate is the Raspberry Pi 2 Model B.

6. The Operating System running in the pods will be Raspbian Jessie-kernel version 4.1.

7. LEAN Wi-Fi pods will be encased in a protective casing to provide resistance to extreme environments. LEAN will operate under normal temperatures but can be expected to operate up to at least 138 degrees Fahrenheit [5].

3.9 User Documentation

In order to assist users of the system, the following deliverables will be provided:

1. Connecting to the network. A user tutorial on how to connect to the wireless network.

2. Disaster Recovery manual. A System Administrator manual on how to restore the entire operating system in the server and pods, how to replace the physical server, and pods, how to troubleshoot a variety of problems on the server and pods.

3. Network Administration. A System Administrator manual on how to log into the system, how to manage the pods in the network, how to gather statistics, how to maintain and query the database, how to run the algorithm to calculate the location of the pods, hardware specifications, software configurations, and licensing.

Each of these tutorial/manual will be delivered in printed format and will be available on-line for download as well.

4 Technical Approach

LEAN will be a local area emergency network that is procedurally adapted to any environment. This network will provide stable communication for ICS personnel. The system will have a set of Wi-Fi repeaters called pods that expand the area to give coverage to all authorized responders. Along with being a Wi-Fi repeater, each pod will be equipped with a sensor array to sense it's own status. This status determines if the pods are damaged, where they are located, and if they are lost from the network completely. Each pod reports its sensor data back to a central server for analyzing. The central server will analyze the data for anomalies that would indicate a change in pod status. After analyzing the data, the central server will update a GUI that displays all pods and their sensor information. LEAN will be able to monitor itself for damage and fit into any emergency area. A representation of a pod can be seen in figure 1.

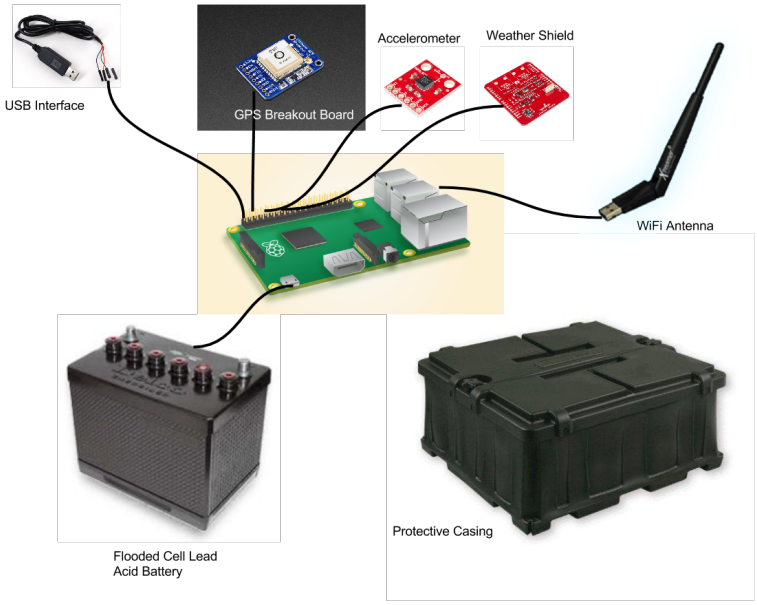

Figure 1: Representation of possible pod contents modified from ([20][21][22][23][24][25][26][27])

4.1 Hardware

For this implementation of LEAN, all hardware will be pre-built systems and breakout boards. This allows for quick development and proof of concept to determine if the design guides in this document are sufficient.

4.1.1 Central Server

Disk Storage: LEAN developers decided to implement RAID 5 disk storage rather than other disk storage options like RAID 10 because RAID 5 is less costly than RAID 10 and more efficient and secure than other RAID levels 0 - 4 and 6. RAID 5 implements block level striping and uses a distributed parity. Striping is the process of dividing a body of data into blocks and spreading the data blocks across multiple hard disks. Distributed parity is used to achieve redundancy. Parity information is written to a different disk in the array for each stripe. If a drive in the array fails, remaining data on the other drives can be combined with the parity data (using the Boolean XOR function) to reconstruct the missing data. Figure 2 shows a simple 3 disk RAID 5 distribution.

In the figure below:

1. A, B, C, D, E and F represents blocks
2. p1, p2, and p3 represents parity

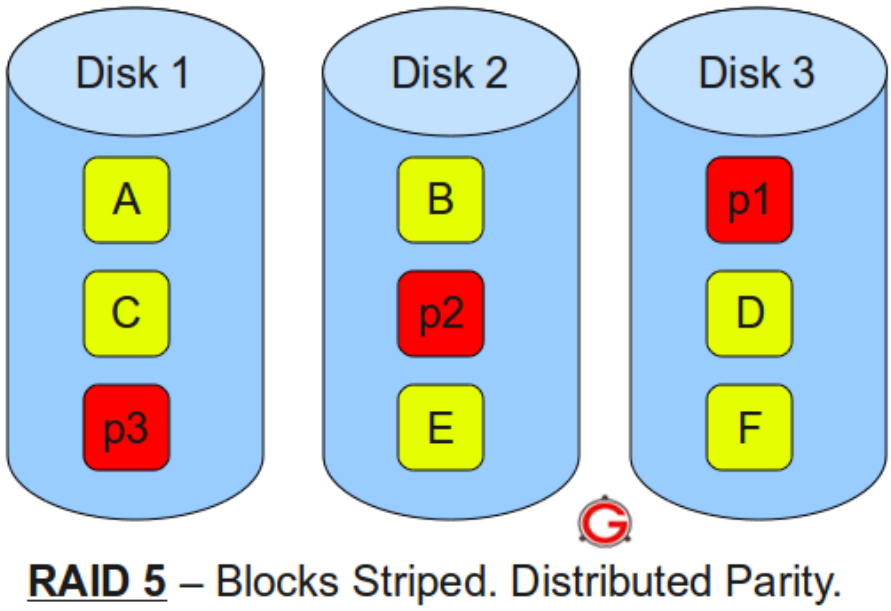

Figure 2: RAID 5 Block Striping. Distributed Parity [28]

Security: SSL/TLS is layered between Transport (TCP/IP) and Application layers and protects privacy, integrity and authentication. SSL/TLS use several algorithms to secure a large range of vulnerabilities, using hashing functions, block and stream ciphers, and public key options. LEAN developers will use the openSSL api for implementation on LEAN central server databases. LEAN developers decided on this security method because openSSL is a commercial-grade, full-featured, and Open Source toolkit implementing the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols as well as a full-strength general purpose cryptography library. Open source software is free and easily accessible thus making LEAN less costly. Figure 3 shows a handshake protocol which is a common process of steps that SSL/TLS follows to verify if a user can gain access.

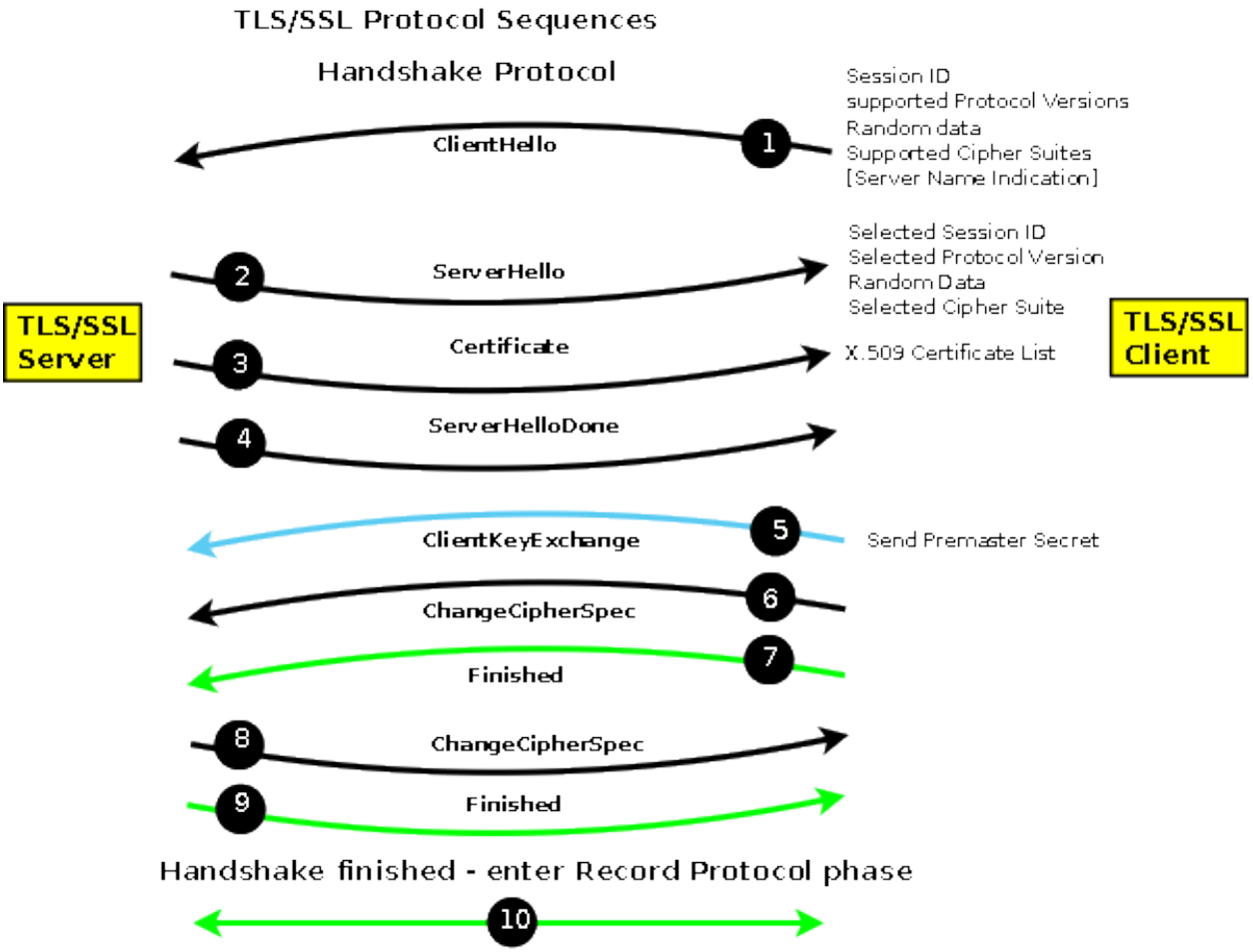

Figure 3: SSL/TLS [29]

4.1.2 Wi-Fi Repeater Pod

Wi-Fi radio: LEAN Wi-Fi repeater pods will contain a Wi-Fi radio capable of transmitting up to 600 Mbps. The radio will plug into the processor via USB port. The intended radio as of now before any actual testing has been done will be a HiRO H50194 Wireless 802.11n USB Wi-Fi WLAN Network Adapter High Gain 5dBi Omnidirectional External Antenna . This USB Wi-Fi radio has a Wireless Protected Setup button which adds an extra

layer of security to the network. This Wi-Fi radio was chosen as it meets the requirements of 600 Mbps and is low in cost and small in size. Figure 4 shows the Wi-Fi radio being used.

Figure 4: HiRO H50194 Wireless 802.11n USB Wi-Fi WLAN Network Adapter High Gain 5dBi Omnidirectional External Antenna [30]

Raspberry Pi Processor: LEAN Wi-Fi repeater pods will be equipped with a Raspberry Pi 2 Model B Processor that will manage all sensor data and network trafficking. There will be a USB port connection that can be used by the ICS logistics team. This processor will interface with the sensors described in section 4.1.3 of this document. The Raspberry Pi was chosen because it is flexible enough to operate the sensor array, and maintain network reliability at the same time, and it is very low cost. Figure 5 shows the Raspberry Pi 2 Model B Processor from a top down look to show all connections available.

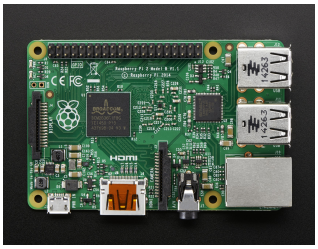

Figure 5: Raspberry Pi 2 Model B Processor [31]

Battery: The exact battery LEAN developers will use is still being researched. LEAN developers have determined the battery will be a flooded lead acid battery not weighing more than 100 pounds. The battery must have a minimum charge capacity of 30 Ahrs.

Pod Shell Enclosure: LEAN developers will use a pre-existing commercial grade battery box as the protective casing for it's Wi-Fi pods. Each pod will have a locked removable lid with two compartments one being used for the battery and one being used for the processor and sensor array. This would assist in keeping any harmful chemicals from the battery to come into contact with the electronic equipment. The battery box LEAN will use is called the NOCO HM485 Commercial Battery Box, this box is a rotationally molded enclosure for housing our battery on one side and electronic components on the other side. Made from high-impact polyethylene plastic, this battery box maintains its tough impact properties

down to -40F and is resistant to UV exposure, acid, gasoline, oil, salt or other contaminants [32]. This commercial battery box has a large electrolyte reservoir to effectively collect battery acid, allows proper ventilation and prevents accidental contact with battery terminals. This container was chosen as it is not costly. Figure 6 shows the container with the lid on and off so you can see the two compartments.

Figure 6: The NOCO HM485 Commercial Battery Box [32]

USB Interface: The USB interface will be equipped to the Raspberry Pi via the Adafruit console cable. This cable is a simple USB connection except with one end broken out to a squid cable for connecting it to the Raspberry Pi GPIO. This connection will allow the administrators to gain administrator access. The reason for having this access if for in field set-up. The placement algorithms are only an estimate, and this interface will allow for in field adjustments. When accessing the USB interface, the administrator will run a program already installed on the Pi. The program will then start outputting GPS data and what other pods are in range and what their signal strength is. Figure 7 shows the Adafruit Console Cable that will be used for administrator access.

Figure 7: Adafruit Console Cable [33]

4.1.3 Sensors

The sensor array that is equipped to the pod will have GPS, accelerometer, weather chip, and power level sensors.

GPS Sensor: The sensor chosen for this is the Adafruit Ultimate GPS Breakout. This board has 22 tracking and 66 searching satellite capability with a low form factor of only 1.0"X1.35"X0.25". This device also has an operating current of only 25mA and runs on a 3.0-5.5VDC supply. This device is chosen over the GPS Receiver - EM-506 (48 Channel) by SparkFun due to it's single form factor. The SparkFun receiver needs an additional breakout board to plug into. Another reason for choosing the Adafruit over the SparkFun option is the current draw; the Adafruit breakout board has a current draw of about half of the SparkFun board. The GPS sensor will be connected to the Raspberry Pi GPIO.

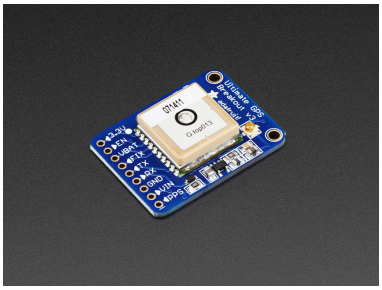

Figure 8: Adafruit GPS Breakout Board[21]

Accelerometer: The sensor chosen for this is the SparkFun Triple Axis Accelerometer Breakout equipped with the Analog Devices ADXL335. This board has the ability to measure acceleration up to 3 axis. This device has an operating current of only $350\mu A$. This device was chosen over its Adafruit equivalent ADXL335 - 5V ready triple-axis accelerometer due to familiarity of the LEAN developers. The accelerometer sensor will be connected to the Raspberry Pi GPIO.

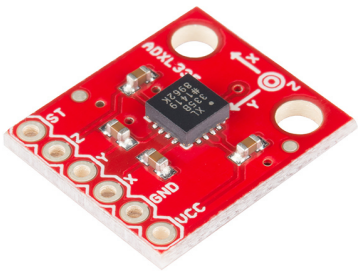

Figure 9: SparkFun Accelerometer Breakout Board[22]

Weather Chip: The board chosen for the weather chip is the SparkFun Weather Shield. This shield is equipped with a temperature, barometric, and luminosity sensor. The temperature sensor on the shield typically draws $450\mu A$, the barometric sensor typically draws $40\mu A$, and the luminosity sensor typically draws $0.1\mu A$ in the dark and in the light draws up to $150\mu A$. All sensors in the weather chip will be connected through the Raspberry Pi GPIO.

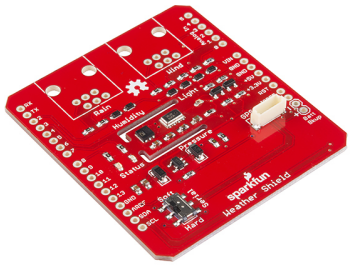

Figure 10: SparkFun Weather Shield[23]

Power Consumption: All together, the sensors will draw about 30 mA in addition to the 700 mA that the Raspberry Pi consumes leading to a total 730 mA current draw. The requirements state the the battery will have at a minimum a charge capacity of 30 Ahrs. This means that the pods will run for at least 41 hours (about 2 days). The calculations for this can be found in equations 1 and 2 below.

$$CurrentDraw = 25mA + 350\mu A + 450\mu A + 40\mu A + 150\mu A + 700mA \approx 730mA \quad (1)$$

$$Hours = 30Ahrs/0.730A \approx 41hrs \quad (2)$$

4.2 Software

4.2.1 Central Server

Operating Systems: The Operating System chosen to be installed in LEAN's central server was Linux Ubuntu 14.04 LTS because is flexible enough to interact with the sensor array through non-proprietary programming languages, supports a variety of ad-hoc routing protocols, runs over most hardware, has considerable amount of online for troubleshooting, and supports the MySQL Database Management system.

The Operating System chosen to be installed in all pods was Raspbian Jessie-kernel version 4.1 because its source code can be modified to work with the sensor array, and also because it supports a variety of ad hoc routing protocols. Both Operating Systems, Ubuntu and Raspbian, are computed by the device's processor where they are installed.

Routing Protocol: Due to its compatibility with Raspbian and easier implementation than other routing protocols, Babel was chosen to run in the pods. Manually maintaining

the routing tables would be a very challenging task, if not impossible, considering that the size of coverage area and amount of pods involved in an emergency scenario always varies. Therefore, the need to maintain the pod's routing tables automatically using a routing protocol. This way, regardless of the amount of pods to be used in a particular emergency scenario, or their location/arrangement, each pod will be able to announce themselves to neighbors, detect current and new neighbors, calculate and memorize most convenient routes, and update them in the event of any change. That being said, Babel, the chosen routing protocol, had to offer the flexibility to the developers to choose how to calculate shorter or more convenient routes choosing among a variety of metrics. Additionally, be able to avoid routing loops, have fast convergence, and be designed to support mesh wireless networks[16]. Ultimately, the strongest reason why the developers chose Babel was because it outperformed other mesh routing protocols such as OLSR and B.A.T.M.A.N.in all performance metrics examined, plus it offered the highest multi-hop bandwidth and the fastest route repair time [34].

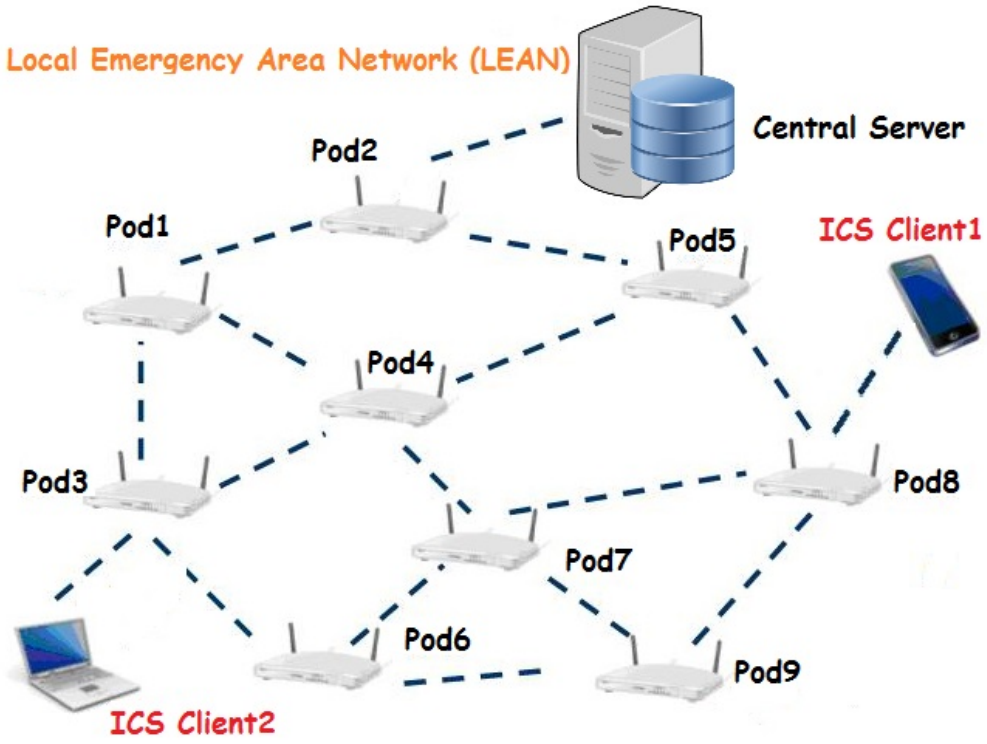

Figure 11: Representation of LEAN ad-hoc network. Modified from [35]

Pod Placement Algorithm: An algorithm is being developed by LEAN developers that will be used to determine optimum pod placement given an incident area and the number of expected ICS responders connecting or utilizing LEAN, the algorithm will likely be a hill climbing algorithm with some refinement. We will run the algorithm based on the area and number of expected users. This will determine a base coverage area and a fitness level for the LEAN network. Then we will run the algorithm again, only this time we will check each node placement location from the first run, and determine if a node within range of the

current network node being added or removed, will either increase or decrease the fitness level without loosing connectivity. Once a decision is made, all other nodes are checked. Once there are no longer nodes that can decrease the fitness level of the network, the remaining nodes will be the optimal pod locations for that particular incident [36].

Emergency Area Pod Mapping: The central servers will display the active pods covering the emergency area on a map. This will allow administrators to visualize pod location and monitor their status. A representation can be seen of this in Figure 12.

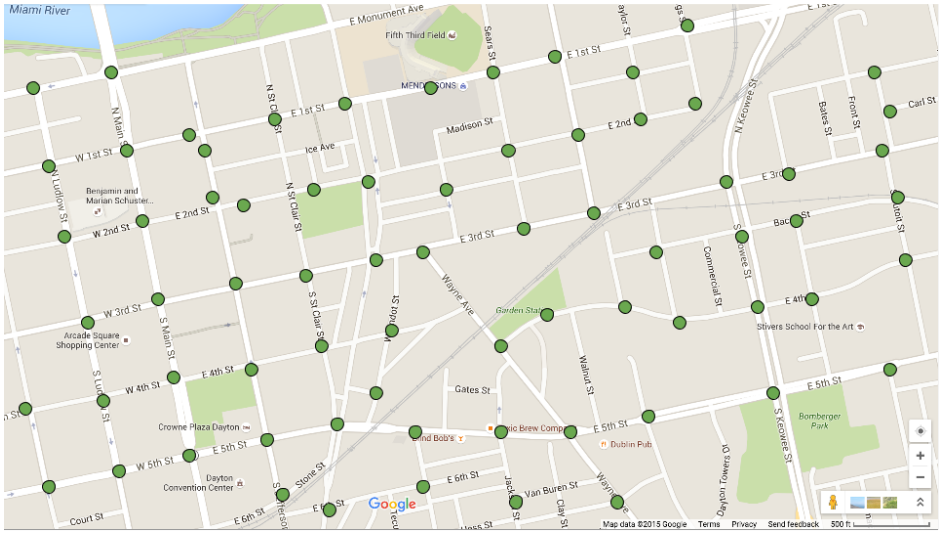

Figure 12: Pod Mapping Representation (Modified from Google Maps)

4.2.2 Wi-Fi Repeater Pods

Security: LEAN will implement WPA/WPA2 security protocols. All wireless hosts connect to LEAN via a WAP (Wireless Access Point). The WAP controls access and authentication to LEAN and provides access to the LEAN network. WPA(Wi-Fi Protected Access) uses one of several ciphers for data integrity. The only cipher required by WPA is the Temporary Key Integrity Protocol (TKIP). TKIP is a cipher that extends the basic RC4 cipher by adding integrity checking, tamper detection, and measures for responding to detected intrusions. Using WPA/WPA2 security protocols will ensure that LEAN will adhere to network security standards IEEE 802.11n [6]. Figure 13 and 14 show detailed flowcharts of the data being encrypted and decrypted using TKIP and WEP(security algorithm) protocol:

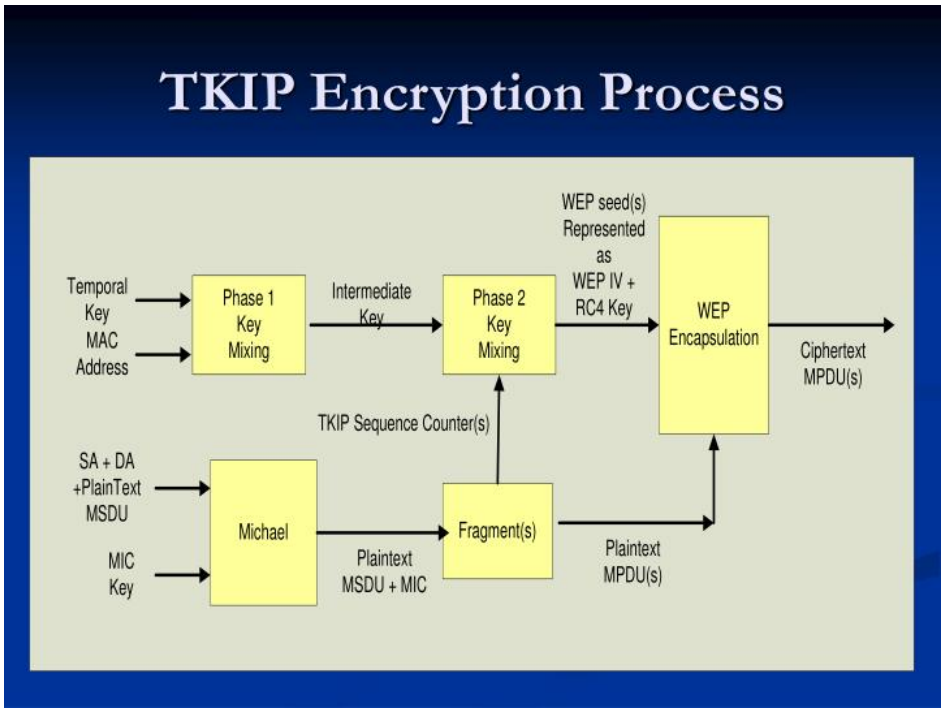

Figure 13: TKIP Encryption Flowchart [37]

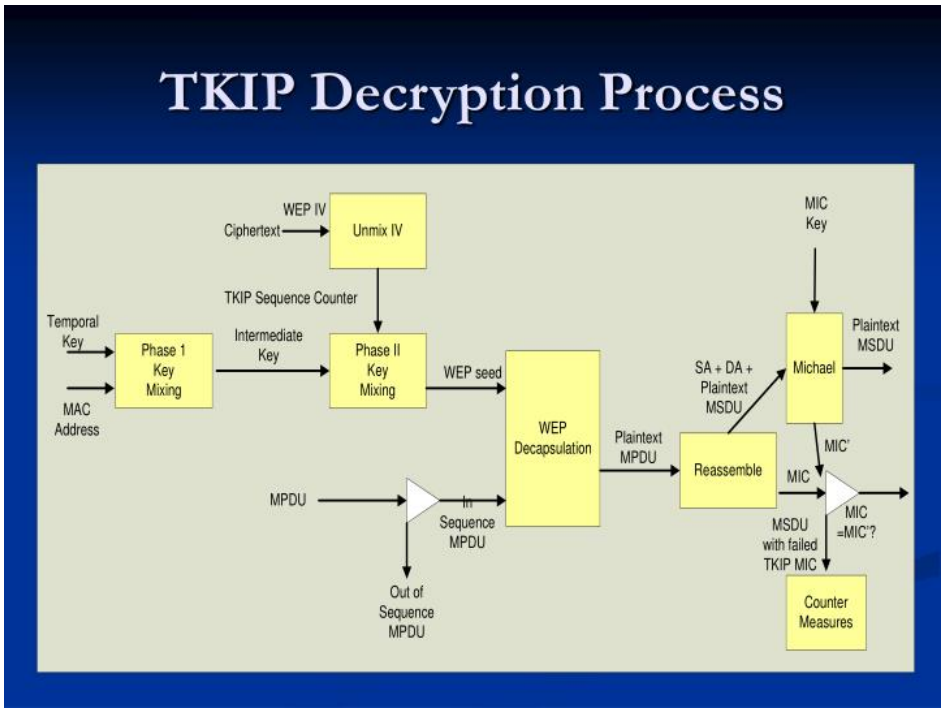

Figure 14: TKIP Decryption Flowchart [37]

Sensor Interrogation: Each pod will be equipped with a sensor array. This sensor array is connected to the GPIO of the Raspberry Pi giving the ability to interrogate them with a

python script. There will be a different python script for each sensor in the array. Interrogation will be performed on an interval to preserve battery power and network bandwidth. The interval will be different for each sensor since not all sensor data is crucial to sample at higher rates.

5 Appendix: Resumes of Team Members

JEREMY VAN EPS

www.linkedin.com/in/jeremyvaneps/en

5033 Worchester Dr. Dayton, OH 45431 | jeremyvaneps@gmail.com | (720)985-3299

SKILLS

- Applied **VHDL** to design, analyze, and synthesize digital integrated circuits and program **FPGAs** at Wright State University (**WSU**)
- Modeled signals and systems and created plots based on scattering parameters from a spectrum analyzer using **MATLAB**
- Low level **Linux** and **Windows** system and network manipulation using command line shells, regular expressions, **python**, and **bash scripting** at **WSU**
- Coded a variety of **Java** programs that implement file I/O, basic arithmetic, data structures, polymorphism, and JavaFX at **WSU**
- Derived complex algorithms in **C** to support the **embedded systems** platform at **Eccrine Systems**
- Developed an **Android** application to communicate over **Bluetooth** to an **Atmel micro controller**
- Designed multiple layer board layouts in **Kicad** and manufactured them through **OSHPark**

EXPERIENCE

ECCRINE SYSTEMS - Cincinnati, OH *05 / 2015 - Present*
Independent Contractor
Support development of **embedded systems** for the Eccrine Systems Sweatronics(TM) Platform, including hardware and **software coding**, electronics testing, and other services as necessary. Support the testing and integration of the Platform with Eccrine sensor technology.

INVOTEC ENGINEERING, INC. - Springboro, OH *01 / 2015 - 05 / 2015*
Co-Op
Assisted 5 engineers and independently designed electrical schematics using **AutoCAD**, performed software validations on Allen Bradley PLC driven machines, and **programmed PLCs** using Allen Bradley software.

WRIGHT STATE UNIVERSITY - Dayton, OH *01 / 2015 - 05 / 2015*
Lab Instructor Assistant
Apprenticeship for Graduate Teaching Assistant to learn how to instruct classes on basic circuit design, grade papers, and help students complete their lab.

AFRL DISCOVERY LAB - Dayton, OH *12 / 2012 - 12 / 2014*
Group Lead
Coded an autonomous system using **C#** in **Visual Studio** and a NAO humanoid robot, programmed an Emotive EEG headset to control robots and computers, performed video analysis using **MATLAB**, contributed to the development of an **IoT** project using **arduino** and **raspberry pi**, and **managed** and **mentored** other projects directly.

EDUCATION

WRIGHT STATE UNIVERSITY - Dayton, OH *2016*
Bachelor of Science (BS) , Electrical and Electronics Engineering, GPA: 3.578
IEEE, National Society for Colligate Scholars
Relevant Courses:
- Introduction to C Programming for Scientist and Engineers (CEG 2170)
- Digital Integrated Circuit Design with PLDs and FPGAs (EE 4620)
- Random Signals and Noise (EE 3260)
- Circuit Analysis (EE 2010)
- Operating Systems Concepts and Usage (CEG 2350)
- Computer Science I (CS 1180)

JORGE A. SOSA

Sosahuapaya.2@wright.edu UID: U00599202

WORK EXPERIENCE

Network administrator **Sept 2010-Aug 2013**

Alfred H. Knight

- First line helpdesk to on site user sand local branch users.
- Maintained desktop and servers applications
- Maintained the entire network infrastructure.

Campus Technology IT Assistant **Oct-Dec 2008**

TC3 – Tompkins Cortland Community College

- Developed Visual Basic and MS-DOS scripts to enhance and automate network maintenance tasks.
- Laptops and Desktops software support.

IT Services Assistant **Mar 2006 – Sept 2007**

KPMG

- Managed Network devices and servers.
- Implemented ISA Server 2004, WSUS Server applications.
- Coordinated tasks with KPMG ITS-Global staff.
- Remote and Onsite users' helpdesk.

Technical Support **Nov 2004– Jul 2005**

IPAE

- Maintained and supported the Information Technologies laboratories.
- Coordinated IT courses schedules and other administrative tasks.
- Supervised IT Student's exams.

EDUCATION

Wright State University **Sept 2013 - Present**
Dayton, Ohio
Sinclair Community College **Jan - Jun 2009**
Dayton, Ohio
AAS Computer Information Systems **Sept – Dec 2008**
Tompkins Cortland Community College (TC3) **Sept – Dec 2009**
Dryden, New York
Cisco Certified Network Associate (CCNA) **Feb 2007 – Mar 2008**
ISIL - San Ignacio de Loyola Institute
San Isidro, Lima, Peru
Computer Science Technician **2003 - 2006**
CIBERTEC Institute of technology
San Isidro, Lima, Peru

TRAINING AND CERTIFICATES

Cisco Certified Network Associate (CCNA) **2008**
CompTIA A+ Certified **2007**

JUSTIN R. SCOTHORN

Scothorn.2@wright.edu UID: U00580017

EDUCATION

Bachelor of Computer Science **August 2016**
Wright State University
Fairborn, Ohio, USA

WORK EXPERIENCE

Undergraduate Research Assistant **2015-present**
The Ohio Center Of Excellence in knowledge-enabled Computing

- Web Development
- Mobile Application Development
- Data Analysis
- Design and planning of projects

Undergraduate Research Assistant **2014-2015**
Southwestern Ohio Council for Higher Education,
Air Force Institute of Technology- Radar Instrumentation Laboratory

- Researched capabilities of processors for use in signal processing
- Benchmarked software algorithms for cross correlation of signals
- Implemented cross correlation algorithms using the raspberry pi processor

Teaching Assistant **2013-2014**
Wright State University

- Assist professor with student understanding of material
- Grade homework and project assignments
- Give lectures when professor not available

SKILLS

- HTML
- CSS
- JavaScript
- Java
- Python
- Linux
- C
- Leadership
- LaTeX

RELEVANT COURSEWORK

- Computer Science II
- Digital design
- Operating systems and concepts
- Operating systems and internals and design
- Discrete Structures and algorithms
- Data structures and algorithms
- Web design fundamentals
- Comparative Languages
- Tech Communications for EGR & CS
- Statistics for Engineers
- Physics I
- Host computer security
- Logic for computer Scientist
- Social implications of computing

HONORS AND AWARDS

Deans Leadership Institute **2014**
Wright State University
Deans Leadership Institute Award **2015**
Ohio State House of Representatives