AFRL-RI-RS-TR-2014-308

SURROGATE JOINT AERIAL LAYER NETWORK (JALN) EXPERIMENT: APPLICATIONS OF COMMERCIAL-OFF-THE-SHELF TECHNOLOGIES FOR RESEARCHING FUTURE JALN CHALLENGES

DECEMBER 2014

TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2014-308 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/ S /
MICHAEL MEDLEY
Acting Branch Chief
Information Transmission Branch

/ S /
MARK LINDERMAN
Technical Advisor, Computing
and Communications Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, 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 Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*
DECEMBER 2014

2. REPORT TYPE
TECHNICAL REPORT

3. DATES COVERED *(From - To)*
MAY 2012 – JAN 2013

4. TITLE AND SUBTITLE

SURROGATE JOINT AERIAL LAYER NETWORK (JALN) EXPERIMENT: APPLICATION OF COMMERCIAL-OFF-THE-SHELF TECHNOLOGIES FOR RESEARCHING FUTURE JALN CHALLENGES

5a. CONTRACT NUMBER
IN-HOUSE

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Derek Moore, Joshua Goliber, Dustin Isereau, and Michael Gudaitis

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site/RITE
525 Brooks Road
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site/RITE
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RI

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TR-2014-308

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. PA# 88ABW-2014-5865
Date Cleared: 11 DEC 2014

13. SUPPLEMENTARY NOTES
This technical report presents in-house work performed by AFRL scientists and engineers in their official work capacity. No official in-house JON was established for this effort.

14. ABSTRACT
This report documents the results of experiments performed to demonstrate use of commercial-off-the-shelf (COTS) wireless networking technology as a surrogate for military-grade networking equipment in the investigation of Joint Aerial Layer Network (JALN) concepts. Field measurements were performed at the Air Force Research Laboratory's (AFRL's) Newport Test Facility using a scaled-down JALN architecture. A number of static ground nodes were linked using a variety of COTS wireless bridges and access points which is provided communication channels at of different frequency and capacity. In addition, a Mini-Common Data Link (Mini-CDL) radio was utilized for making side-by-side performance comparisons of COTS and military wireless technology. Measurements were made to a assess link capacity by incrementally increasing channel utilization. Varying amounts of text, voice and video data were transferred between network nodes and the data rates were recorded. Results are presented and the implications for testing network operations are discussed.

15. SUBJECT TERMS
Aerial Layer Network, Surrogate Wireless Network, Commercial-off-the-shelf (COTS), Joint Aerial Layer Network (JALN)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					THOMAS SCATKO
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (*Include area code)*
U	U	U	SAR	43	**315-330-4413**

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 SUMMARY

This report documents the results of experiments performed to demonstrate use of commercial-off-the-shelf (COTS) wireless networking technology as a surrogate for military-grade networking equipment in the investigation of Joint Aerial Layer Network (JALN) concepts. Field measurements were performed at the Air Force Research Laboratory's (AFRL's) Newport Test Facility using a scaled-down JALN architecture.

A number of static ground nodes were linked using a variety of COTS wireless bridges and access points which provided communication channels at of different frequency and capacity. In addition, a Mini-Common Data Link (Mini-CDL) radio was utilized for making side-by-side performance comparisons of COTS and military wireless technology. Measurements were made to a assess link capacity by incrementally increasing channel utilization. Varying amounts of text, voice and video data were transferred between network nodes and the data rates were recorded. Results are presented and the implications for testing network operations are discussed.

This experiment has successfully demonstrated that COTS wireless technology can be used to examine design issues that will challenge JALN developers. The use of low-cost COTS wireless technology is found to be a suitable surrogate for military hardware for investigating networking problems expected to be encountered in an aerial Layered network (ALN). Additional field experiments are being planned that will involve a larger number of nodes and links. The work will also employ dynamic routing to further challenge network operations and better represent JALN operations.

2.0 INTRODUCTION

The objective of this in-house effort is to research, develop and evaluate a wireless topology for addressing the network connectivity, capacity, data sharing, and management issues associated with next-generation military communications networks, such as the Department of Defense's Joint Aerial Layer Network (JALN). A general lack of synergy between military operators, government labs, industry, and the academic community in resolving increasingly complex problems of integrating and operating wireless technologies presents obstacles to the adoption of new networking approaches. This effort proposes to make use commercial-off-the-shelf (COTS) wireless technologies as cost-effective data link surrogates for instantiating a JALN test bed concept.

Mobile nodes will be assembled using different combinations of these devices to create network conditions encountered in JALN-like scenarios. Link conditions will be measured and networking concepts will be evaluated to assess the effects on application services, such as streaming video and voice, chat, data file transfers and database queries executed over the network. Routing technologies and topology control mechanisms will be studied in an effort to quantify the impacts on throughput, latency, and scalability as network topologies change in an ad hoc environment. The cost-effective approach provides a convenient framework for identifying and investigating key design drivers that impact development of current and future JALN concepts.

The typical Operational View (OV) chart, such as that illustrated in Figure 1, usually illustrates battlefield connectivity using "lightning bolts" or "line segments"—implying that network connectivity is a trivial undertaking. The truth is, implementing reliable and secure

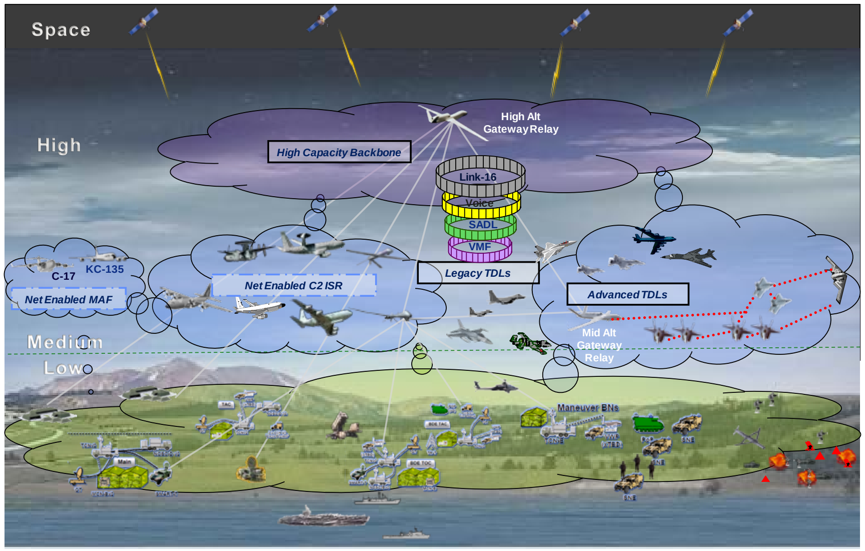


Figure 1 - Nominal Joint Aerial Layer Network Diagram.

tactical network communications is difficult; in that modern tactical operations can involve large numbers of operational personnel and equipment that are deployed in complex combat situations. As one system designer explains it: "Every customer we talk to recognizes that the network is hybrid…One technology doesn't solve all problems. Satellites can't solve 100 percent of the communication requirements; tactical radios can't; Wi-Fi can't. It is a combination of all these technologies in an architecture that ultimately makes sense to deliver the capability to the warfighter [2]." And given the rapid rate of change in wireless technologies, communication system designers need to be continually re-thinking and re-evaluating just what makes sense with regards to information delivery. An effective aerial layer network not only incorporates newly available technological advances as needed, but also is able to seamlessly integrate with existing systems and networks [3]. And many changes in the military operating environment are now being driven from the bottom-up, by younger users familiar with instant messaging, web services and multi-media in their non-military lives.

The USAF Airborne Network Special Interest Group [4] identifies the key defining architectural elements, components, and design objectives for future Aerial Networks (ANs) in terms of the connectivity that can be established, the services that can be supported over the network connections, and the operations that are required for the user to establish, maintain and access the network connections.

- *Connectivity includes: coverage, diversity of links, throughput, type of connection, and network interface (e.g., geographic span of links, total number and type of links, and nature of connections that can be established).*

- *Services include: real-time data; continuous interactive voice (e.g., voice over IP telephone and radio nets); continuous interactive video (e.g., video over IP, video teleconferencing); streaming multimedia and multicast (e.g., video imagery); block transfer and transactional data (e.g., Telnet, HTTP, client/server, chat); and batch transfer data (e.g., email, FTP).*

- *Operations include: managing the links and network; planning (e.g., frequency allocation, transmission, routing, and traffic); monitoring (e.g., performance and use, fault, and security); analyzing (e.g., performance optimization, diagnostics); controlling (e.g., add, remove, initialize, and configure links, networks, or network components); forming and adapting (e.g., provisioning and obtaining need link and network resources, and initialization and restoration of a link or network service); and protection (i.e., communications security as well as authentication, authorization, accounting detection, and reaction).*

It is expected that next generation ALNs will be capable of connecting all platforms, supporting all needed information services, and guaranteeing certain levels of performance to support bandwidth, latency or loss-sensitive applications. The demands placed on future tactical communications systems will only intensify as users' information needs and delivery options increase. As such, the development, adoption and deployment of new communications technologies is critical to the timely sharing of situational awareness data between sensors, decision-makers and weapon systems regardless of their location [5].

The Air Force's 2012 *Aerial Layer Networking Enabling Concept* document defines an ALN "as the integration and application of processes, procedures, and policies that provide the framework for sharing, exchanging, and using data that originates, traverses, or terminates on any AF platform in a joint operational area"[6]. The document goes on to state that:

- *Future ALN systems must be modular and use open standards to allow AF platforms to adapt quickly to new mission needs and technology improvements.*
- *Networks are required to provide connectivity across the multiple disparate physical waveforms which will be used throughout the aerial layer. Several different network domains will need to be operated within the aerial layer to meet the various information assurance requirements, policies and functional system requirements which exist throughout the warfighting environment.*
- *An information sharing infrastructure must be established and managed to achieve end-to-end interoperability. The information sharing infrastructure will leverage the rapid advancement of technology and economy of scale in the commercial sector to enable on-demand, real-time and secure exchange of voice, data, video, control and management information across the ALN and its external interfaces.*
- *Scalability is important as transformation from tactical data links to network architecture will take place incrementally over the years.*
- *The infrastructure will be designed to leverage user experience to ensure that effective capabilities are provided to the warfighter, especially over mobile, low bandwidth and unstable networks.*

Implementing next generation of ALNs, using legacy systems and existing networking architectures, have not yielded needed levels of effectiveness. Meeting the wide range of operational requirements deemed critical to future Air Force missions, will most likely require use of an equally wide range of networking approaches. New technologies and networking approaches being developed for commercial applications cannot be excluded from consideration.

3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

The objective of this effort was to implement a low-cost wireless network for the purpose of demonstrating that commercially available devices and applications can be employed, as low-cost surrogates for military-grade hardware, in the investigation and evaluation of various networking concepts to help further development of aerial layer networks.

Three core principles were preserved throughout development of the network used in the experiment to represent a surrogate JALN. The first was minimizing the cost of hardware. The price of each device was not to exceed $500.00. The second was to avoid proprietary device functionality. This included choosing protocols and applications that were standards across industry, rather than a function only specific to a certain manufacture. Finally, the third was to ensure repeatability.

The location chosen to implement this surrogate network was AFRL's Newport Test Facility. The facility offered a quiet RF environment and provided distances between links that could be scaled (100:1) appropriately to theater. An aerial view of the Test Facility's two hilltop sites (Tanner Hill and Irish Hill) is provided in Figure 2.

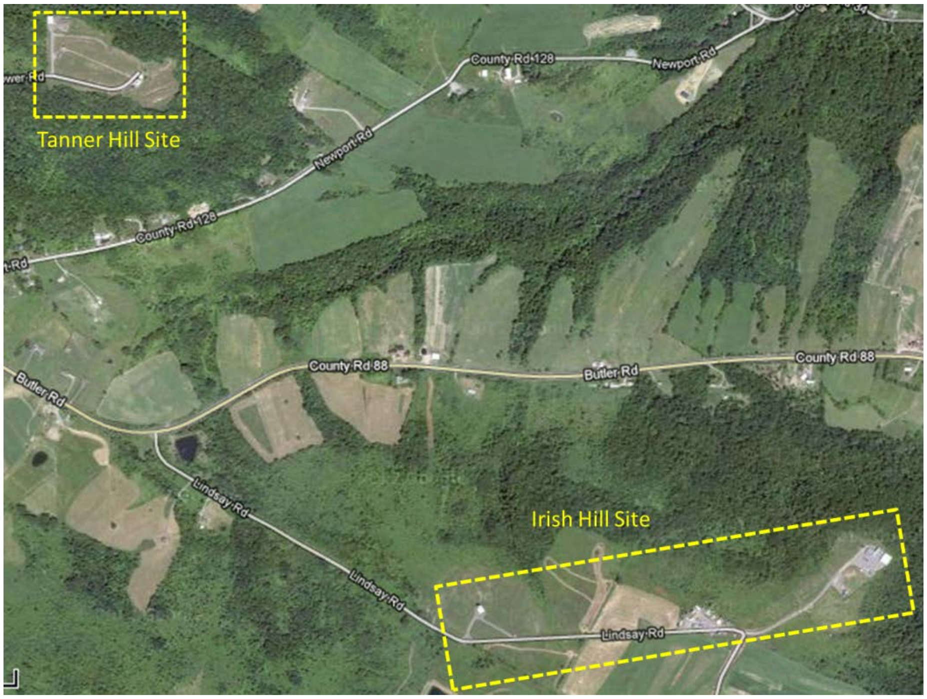


Figure 2 – Newport Test Facility Aerial View.

3.1 Network Design

The experiment's network topology is representative of the high capacity communication links (10 Mbps-274 Mbps) employed between high and medium altitude airborne nodes – such as those links highlighted in the JALN OV diagram shown in Figure 3. Here line segments signify communication link availability, while colors (yellow, red, blue, and black) indicate link of similar bandwidth. This topology was in turn scaled, in terms of range, in order to allow for its set-up at AFRL's Newport outdoor test ranges.

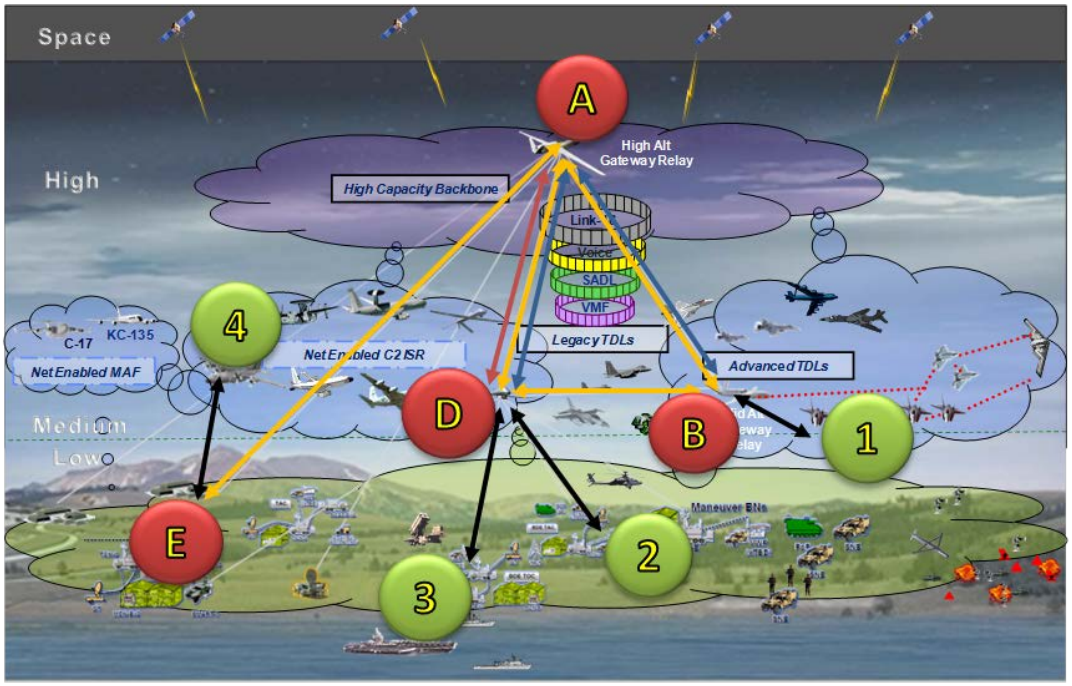


Figure 3 – Experiment Architecture Overlaid on JALN Concept Diagram.

The IEEE wireless (WiFi) standard 802.11g/n was used with COTS devices to provide a cost effective data-link surrogate. These devices provided representative high capacity links with a bi-directional rate ranging from 10-30 Mbps. Additional data-links were also established to emulate backup data-links. Different wireless frequencies were dedicated to these links. All primary links operated over the 5 GHz frequency range, while backup links operated over the 900 MHz and 2.4 GHz ranges. To offer a comparison between the COTS devices and a tactical high capacity tactical link, a mini-CDL operating over the KU band was also incorporated into the design. Figure 4 shows the JALN diagram transposed to different sites within the Newport facility. The figure also identifies the backup links and their associated frequency. The geographical location of the wireless links at the Newport facility can be seen in Figure 5.

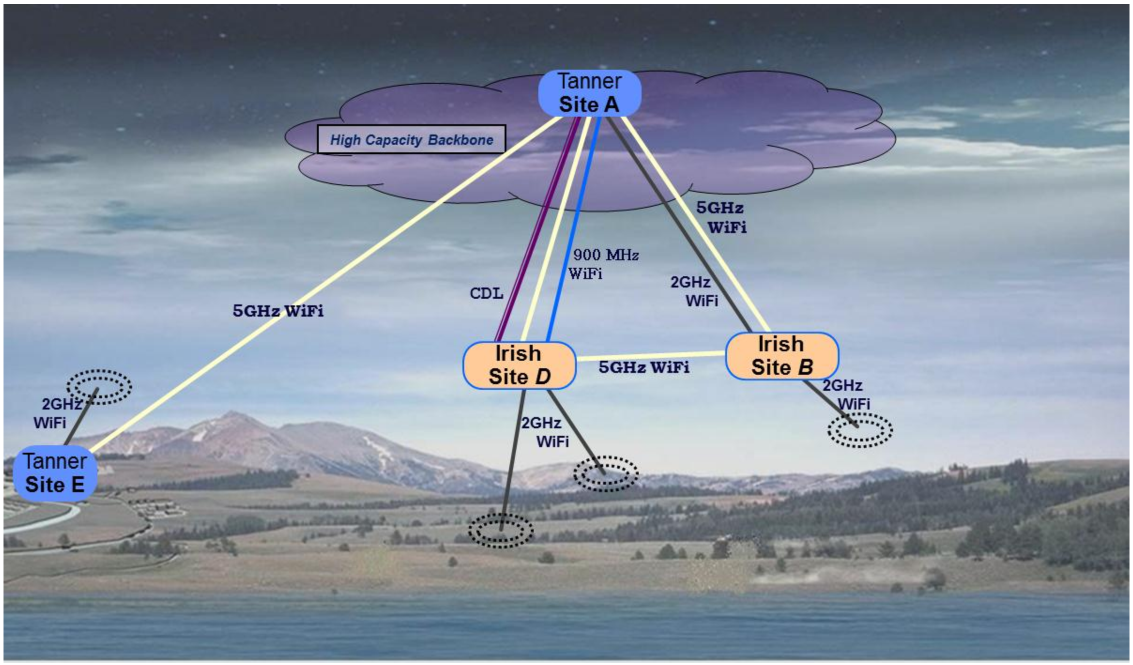


Figure 4 - Joint Aerial Layer Network Diagram (Newport Transposed).

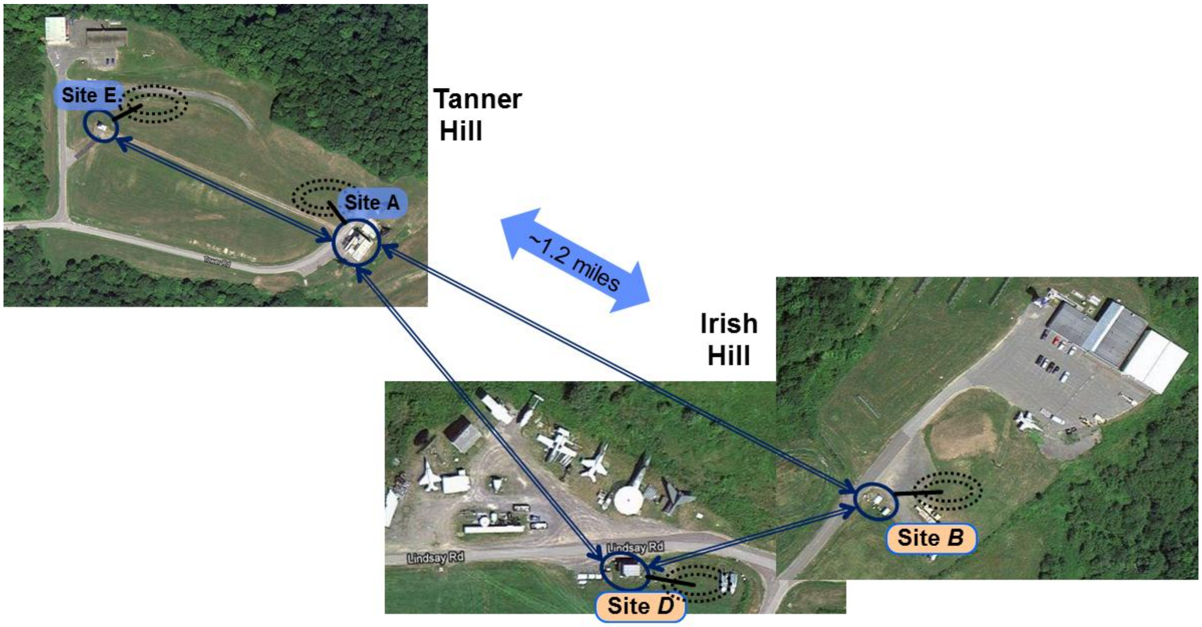


Figure 5 - Newport Facility Wireless Links.

The network was designed so that each site would have a router, switch, wireless access point, and a wired workstation along with various wireless devices such as laptops, tablets and cameras all contained within a local network. Connections between the routers were made using one or more wireless access points that operated in AP/Client mode (similar to bridge mode). The wireless access points were high power and contained directional antennas offering the necessary range across the hills.

Each of the local networks consisted of a class B IPv4 network address, with a 16-bit subnet mask, allowing up to 65,534 nodes. The wireless links between each site were also contained within a local subnet and used class C IPv4 network addresses with a 24-bit subnet mask. Class C addresses were chosen since the number of nodes would be limited to those needed to create a secure wireless connection, much less than the number of nodes at each site. Figure 6 shows the network topology and IP address structure of the JALN surrogate.

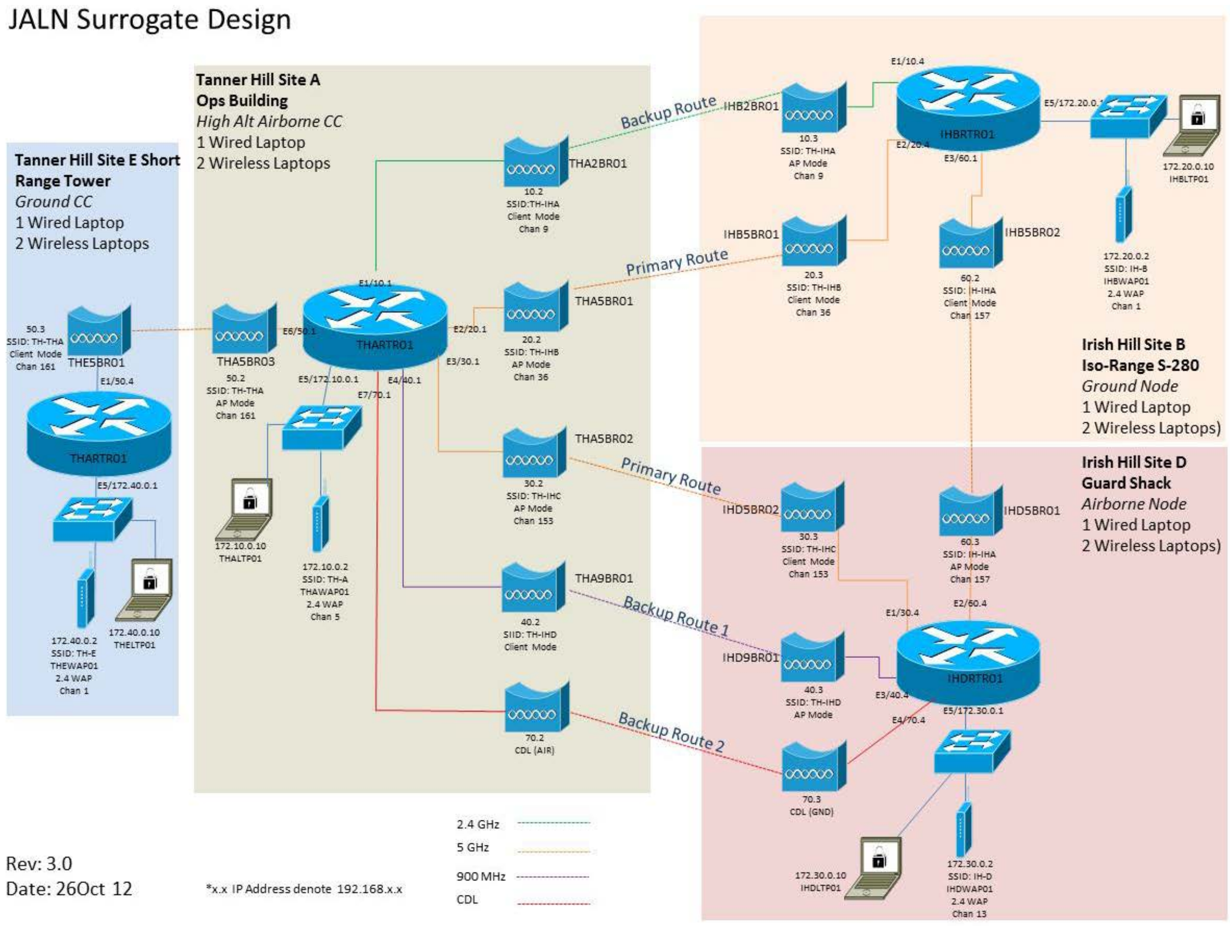


Figure 6 - JALN Surrogate Network Design.

Different routing methods i.e., dynamic versus static were researched and evaluated in the lab. And while a dynamic routing protocol would in all likelihood provide the versatility needed for testing purposes, static routing was instead used to ensure repeatability and control of network response. Static routes proved to be the most reliable and allowed for the focus to be placed on the wireless connectivity rather than on routing operations. The use of static routing also provided a means for establishing a baseline for how link failover should operate in a tactical environment. Static routes were set up manually. Whenever redundant links were used between sites metrics were employed to determine link priority. All primary routes were given the highest metrics while the backup routes were assigned lower ones.

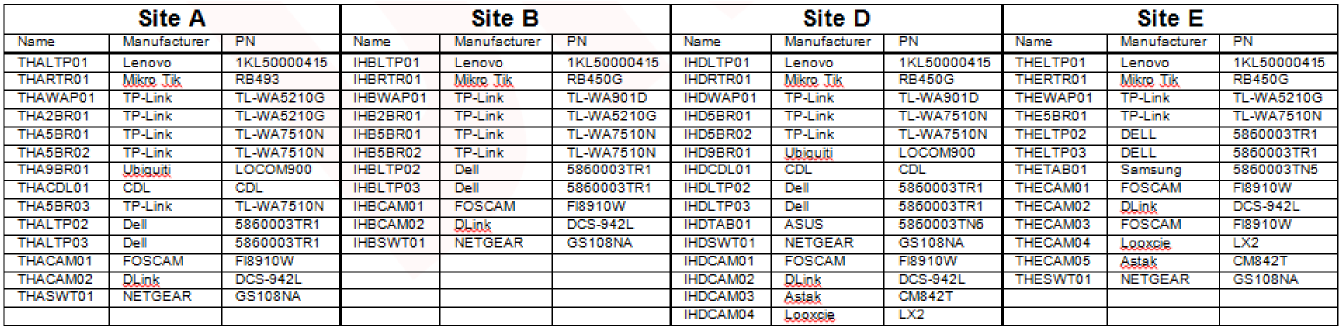
Frequency management was also of concern. In order to maximize link bandwidth, wireless access points, including each site's local access point and the site-to-site directional access points needed to have the correct channel separation and physical placement and alignment. This would ensure proper access point isolation and would maximize the channel bandwidth across the wireless link. Figure 6 above shows the channel configuration for each wireless access point.

3.2 Hardware Configuration

Prior to conducting the field experiment, each of the network devices were researched and their performance evaluated against available alternatives. The routers selected were *MikroTik 450g™* amd *MikroTik 493g™* models both running *MikroTik RouterOS™.* These units offered a number of features set by industry standards at minimal costs. Other small-business routers, such as a *Cisco RV016™* and a *Netgear SRX5308-100NAS™,* were evaluated but were found to have limited configuration options for static routing and their use was constrained by the number of proprietary functions. Site A used a 9-port *MikroTik 493g™* while Sites B, D, and E each used a 5-port *MikroTik 450g™.* Each site also contained a layer-2 *Netgear GS108NA™* switch. Each router was configured with a local LAN port and a number of WAN ports for wireless connections to adjacent routers. Ports on both the routers and the switches featured full-duplex and provided gigabyte speeds.

Each was configured with WPAv2-AES encryption and was given its own SSID. Wireless connections between sites were created using *TP-Link TL-WA5210G™, TP-Link TL-WA7510N™, Ubiquiti LOCOM900™* and Mini-CDL using the 2.4 GHz, 5 GHz, 900 MHz, and KU band frequencies respectfully. *The TP-Link™* and *Ubiquiti™* access points were configured in pairs with one in AP mode and the other in Client mode. This paired-mode is similar to Bridge mode, but allows for additional devices to connect directly to the access point in AP mode. More importantly, bridge-mode does not allow for WPAv2 encryption. So while no other additional devices were connected to the AP Mode access point, the units were able to employ encryption. For local site wireless access, Site A used a *TP-Link TL-WA5210G™* with a directional antenna while Sites B, D, E used a *TP-Link TL-WA901D™* with omni-directional antennas. These were configured in access point (AP) mode and used the 2.4 GHz spectrum. Each site also contained nodes, consisting of one wired laptop, two wireless laptops and various cameras and tablets. Table 1 lists the hardware installed at each site.

Table 1 - Site Hardware List.



Site A			Site B			Site D			Site E		
Name	Manufacturer	PN	Name	Manufacturer	PN	Name	Manufacturer	PN	Name	Manufacturer	PN
THALTP01	Lenovo	1KL50000415	IHBLTP01	Lenovo	1KL50000415	IHDLTP01	Lenovo	1KL50000415	THELTP01	Lenovo	1KL50000415
THARTR01	Mikro Tik	RB493	IHBRTR01	Mikro Tik	RB450G	IHDRTR01	Mikro Tik	RB450G	THERTR01	Mikro Tik	RB450G
THAWAP01	TP-Link	TL-WA5210G	IHBWAP01	TP-Link	TL-WA901D	IHDWAP01	TP-Link	TL-WA901D	THEWAP01	TP-Link	TL-WA5210G
THA2BR01	TP-Link	TL-WA5210G	IHB2BR01	TP-Link	TL-WA5210G	IHD5BR01	TP-Link	TL-WA7510N	THE5BR01	TP-Link	TL-WA7510N
THA5BR01	TP-Link	TL-WA7510N	IHB5BR01	TP-Link	TL-WA7510N	IHD5BR02	TP-Link	TL-WA7510N	THELTP02	DELL	5860003TR1
THA5BR02	TP-Link	TL-WA7510N	IHB5BR02	TP-Link	TL-WA7510N	IHD9BR01	Ubiguiti	LOCOM900	THELTP03	DELL	5860003TR1
THA9BR01	Ubiguiti	LOCOM900	IHBLTP02	Dell	5860003TR1	IHDCDL01	CDL	CDL	THETAB01	Samsung	5860003TN5
THACDL01	CDL	CDL	IHBLTP03	Dell	5860003TR1	IHDLTP02	Dell	5860003TR1	THECAM01	FOSCAM	FI8910W
THA5BR03	TP-Link	TL-WA7510N	IHBCAM01	FOSCAM	FI8910W	IHDLTP03	Dell	5860003TR1	THECAM02	DLink	DCS-942L
THALTP02	Dell	5860003TR1	IHBCAM02	DLink	DCS-942L	IHDTAB01	ASUS	5860003TN6	THECAM03	FOSCAM	FI8910W
THALTP03	Dell	5860003TR1	IHBSWT01	NETGEAR	GS108NA	IHDSWT01	NETGEAR	GS108NA	THECAM04	Looxcie	LX2
THACAM01	FOSCAM	FI8910W				IHDCAM01	FOSCAM	FI8910W	THECAM05	Astak	CM842T
THACAM02	DLink	DCS-942L				IHDCAM02	DLink	DCS-942L	THESWT01	NETGEAR	GS108NA
THASWT01	NETGEAR	GS108NA				IHDCAM03	Astak	CM842T			
						IHDCAM04	Looxcie	LX2			

The photographs provided in Figures 7 through 11 show the antenna installations at each of the four sites. Included in some of these images are photographs of some of the wire cameras used at the various locations.

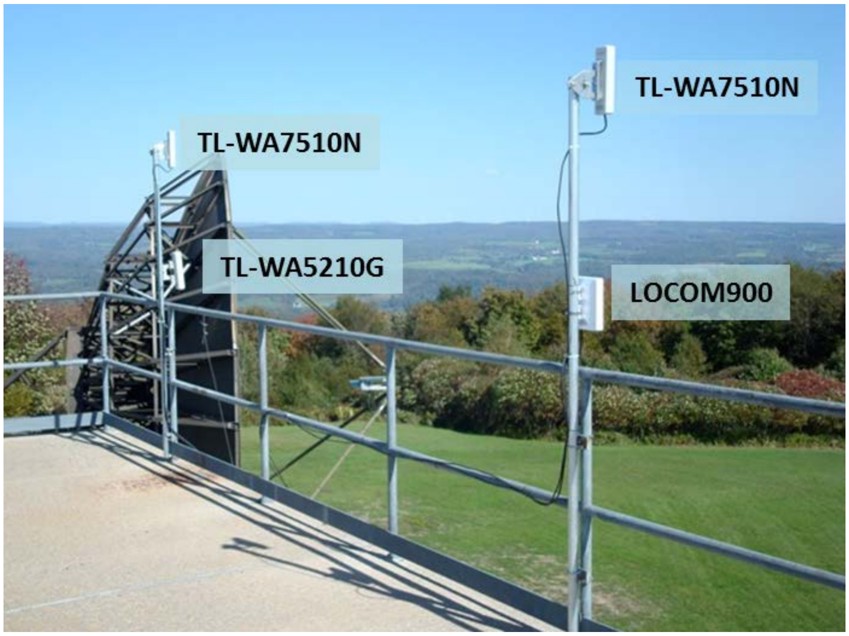


Figure 7 – Site A Antennas For Sites B and D.

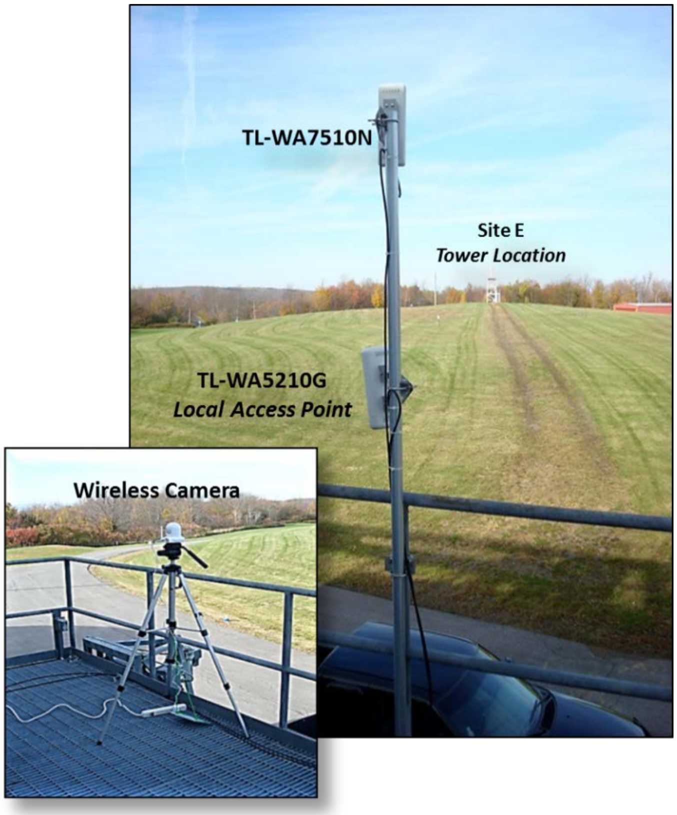


Figure 8 – Site A Antennas For Site E and Local Access.

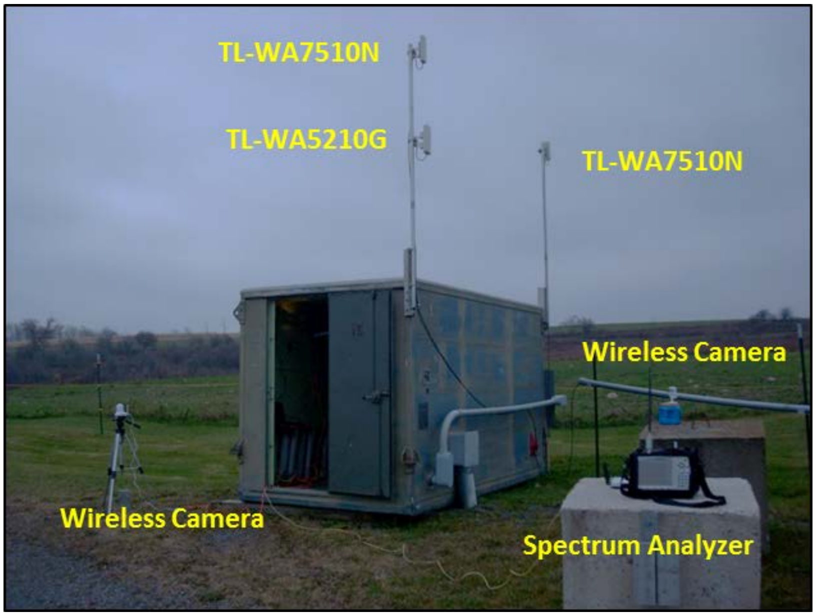


Figure 9 – Site B Antennas for Sites A and D.

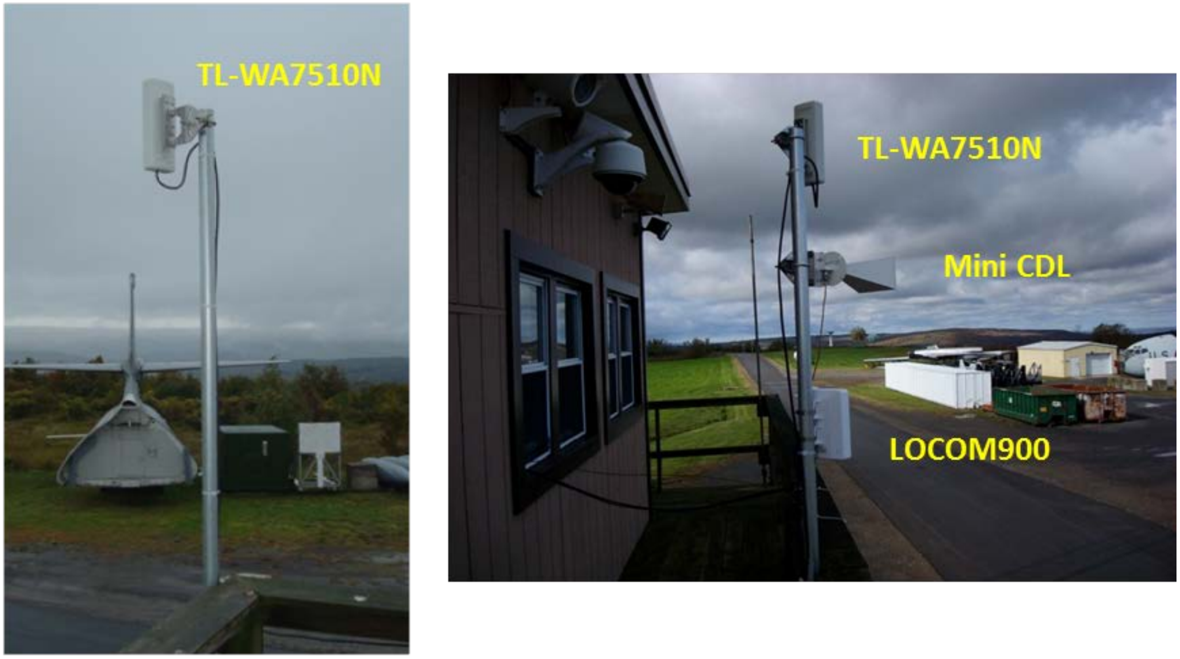


Figure 10 – Site D Antennas For Site A and B.

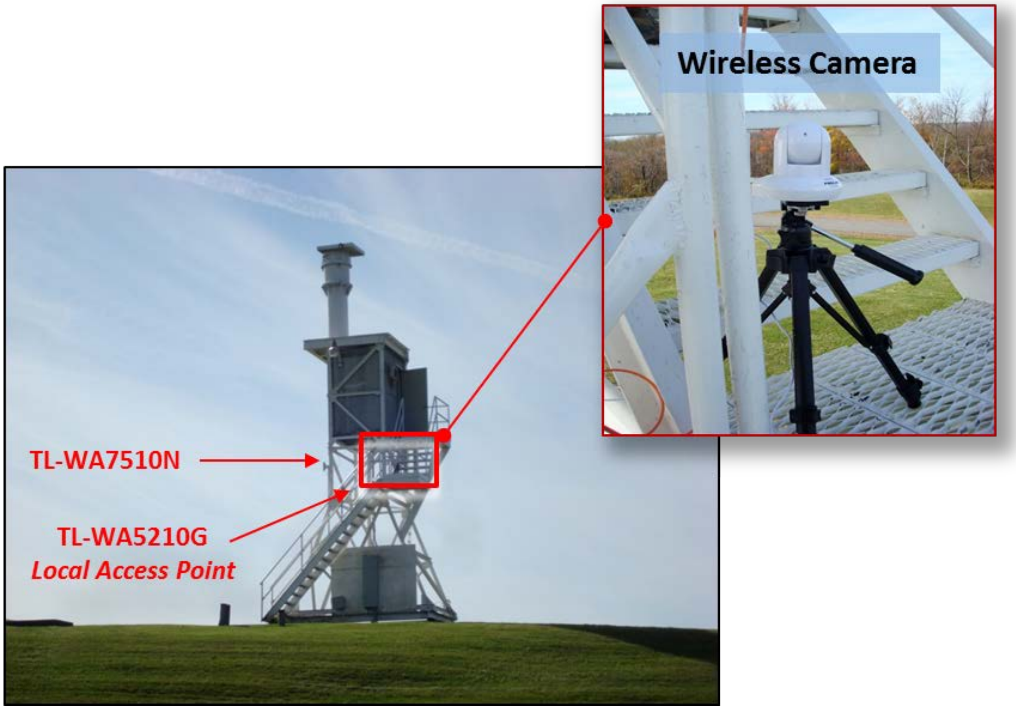


Figure 11 – Site E Antennas For Site A and Local Access.

3.3 Baseline Data Rates

The wireless data links used in this experiment utilized *Ubiquity LOCOM900*™ 900 MHz stations, *TP-Link TL-WA5210G™* 2.4 GHz stations, *TP-Link TL-WA7510N™* 5 GHz stations and the military grade mini CDL KU band transceiver. It is important to note wireless manufactures commonly advertise the max transmission rate (throughput) based on the IEEE industry standards, see Table 2. The advertised and measured throughputs for the devices are provided in Table 3.

Table 2 - 802.11 Standard Throughput.

Standard	Frequency	Channel Bandwidth	Max Advertised Throughput
802.11b	2.4 GHz	20 MHz	11 Mbps
802.11a	5 GHz	20 MHz	54 Mbps
802.11g	2.4 GHz	20 MHz	54 Mbps
802.11n	2.4/5 GHz	20/40 MHz	54-600 Mbps

Table 3 - Advertised and Measured Throughput.

Link	Freq	BW	ADV.*	RAW*	EFF.*
A-B	2.4 GHz	20 MHz	54	14.5	14.5
A-B	5 GHz	40 MHz	150	27.29	27.29
A-D	5 GHz	40 MHz	150	29.72	20.8
A-D	900 GHz	20 MHz	150	19.99	12.4
A-D	KU-Band	Proprietary	44.73	34.07	34.07
A-E	5 GHz	40 MHz	150	34.07	34.07
B-D	5 GHz	40 MHz	150	33	32.94

*Unlabeled rates in Mbps

When comparing the measured and advertised throughput data it becomes evident that the advertised values are significantly higher than those measured. Aspects such as channel bandwidth, TCP/IP overhead, antenna alignment, physical obstructions, and channel interference have major impacts on baseline data transmission measurements. Antenna alignment and line of sight have been adequately demonstrated in this experiment by manual alignment and verification through each devices utility. The increase in performance on the 5 GHz link is due to the increase in channel bandwidth from 20 MHz (in the 2.4 GHz link) to 40 MHz. Increasing the channel bandwidth from 20 MHz to 40 MHz theoretically doubles throughput. However, an increase in bandwidth causes data transmission to be more susceptible to noise. This noise/interference will inevitably lead to packet retransmissions thus decreasing effective throughput even further.

3.4 Spectrum Utilization

Each wireless access point operates on a designated channel. The 900 MHz device uses a 902-928 MHz band. The channels available for the 2.4 GHz Bridges, 20 MHz + 1 on each end makes a total of 14 22 MHz channels, are shown in Figure 12. The 2.4 GHz frequency band is however the most commonly used and it exhibits the most interference – primarily because of channel overlap. Due to the 2.4 GHz band channel availability, the band only allows for a maximum of three channels (1, 6, 11 – 14 is not to be used and 12 and 13 can only be used under low power conditions in North America) for fully independent, non-overlapping, frequencies at a single location. Channel selection in the 2.4 GHz band needs to be carefully considered to ensure channel availability. The 5 GHz frequency band is shown in 13.

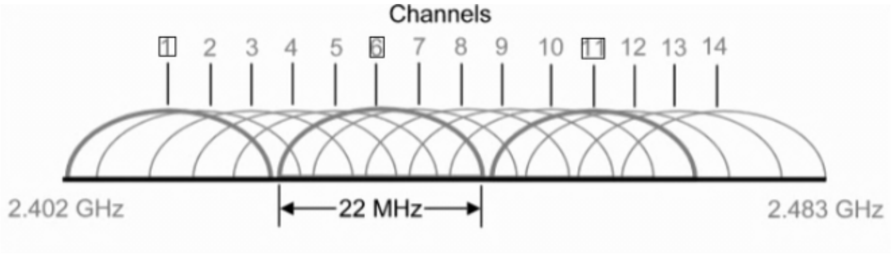


Figure 12 - 2.4 GHz Channels.

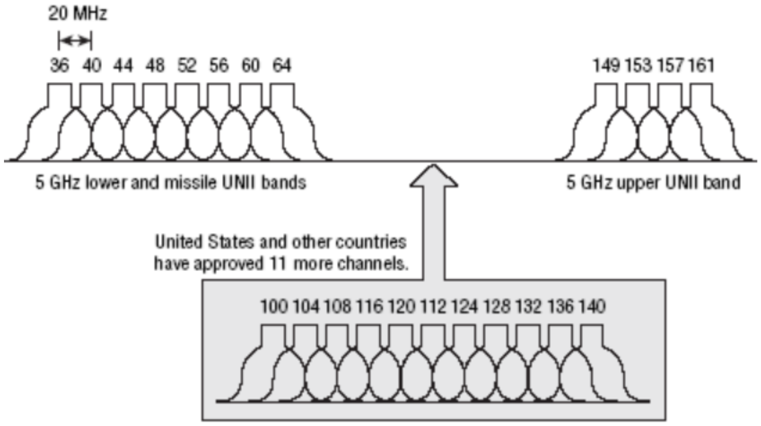


Figure 13 – 5 GHz Channels.

The flexibility of the 5 GHz and relatively low use, compared to 2.4 GHz, makes selecting channels less of a burden. However, it is possible to have channel overlap especially when 40 MHz channel bandwidth is chosen. The frequency for the Miniature CDL is KU-Band and is relatively free of interference due to its military frequency range. The theoretical frequency spectrum for 900 MHz, 2.4 GHz and 5 GHz at site A, B, D, and E in this experiment are shown in Figures 14, 15, 16 and 17 respectively:

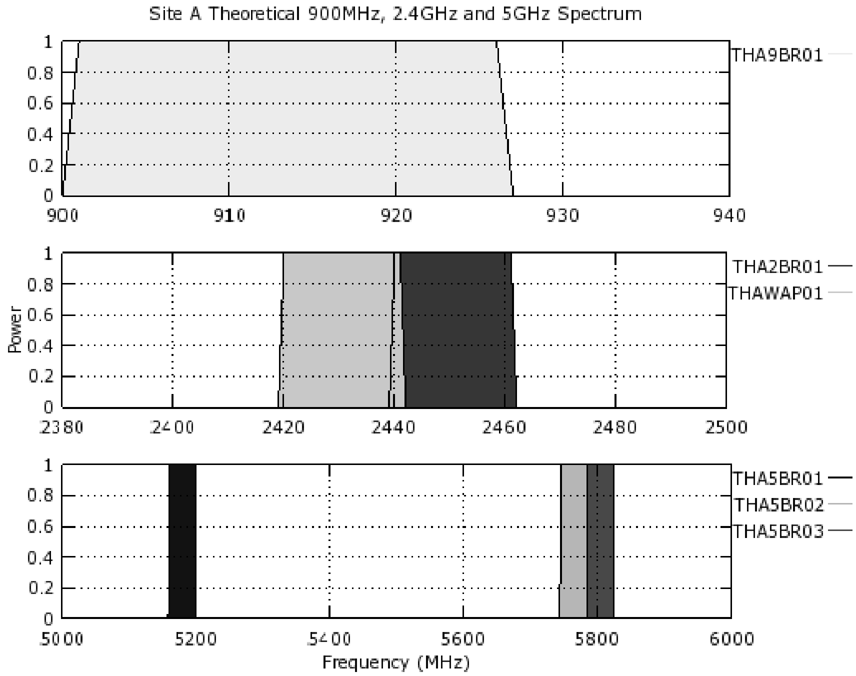


Figure 14 - Site A Theoretical Spectrum.

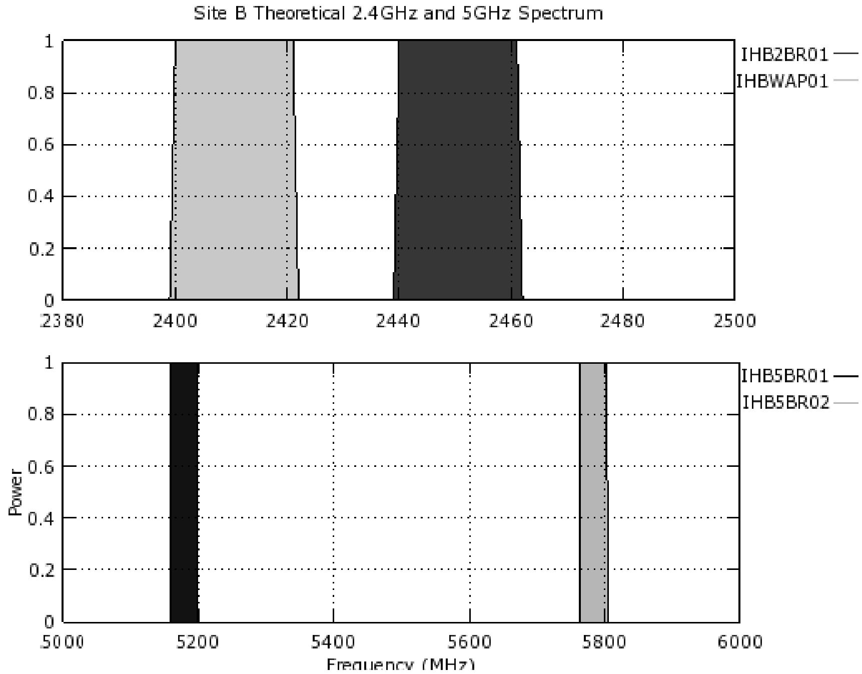


Figure 15 - Site B Theoretical Spectrum.

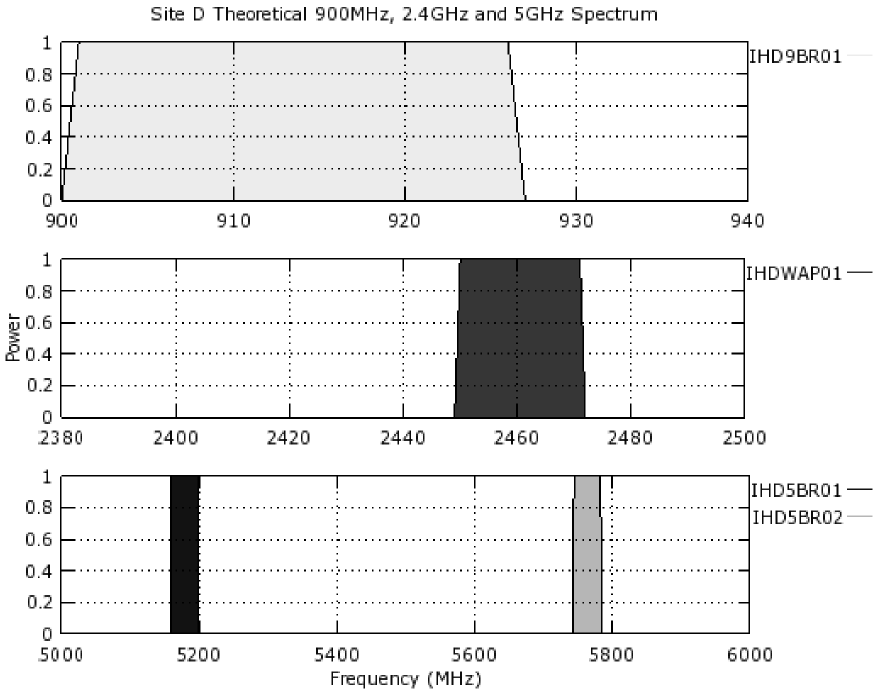


Figure 16 - Site D Theoretical Spectrum.

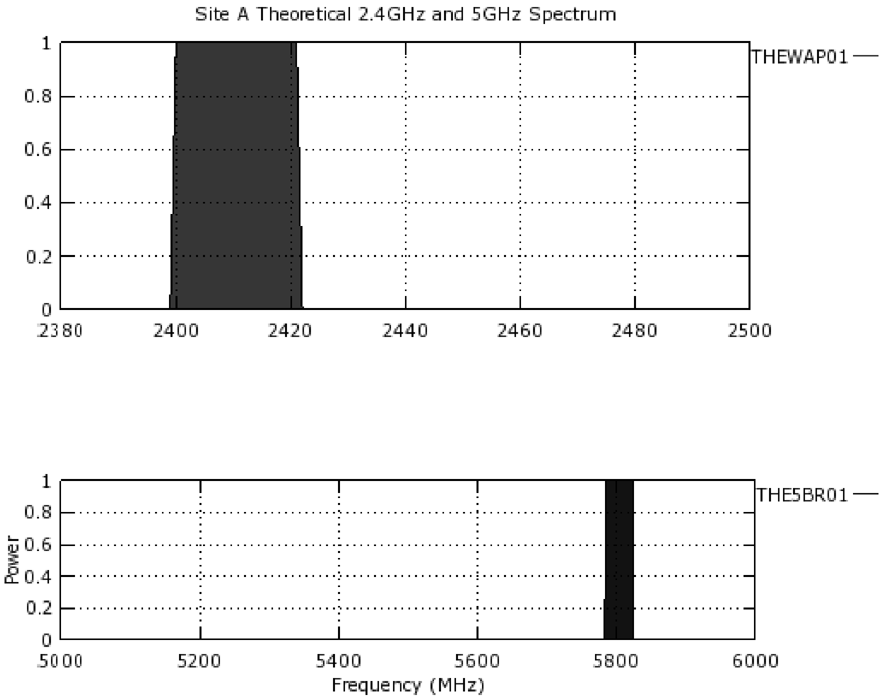
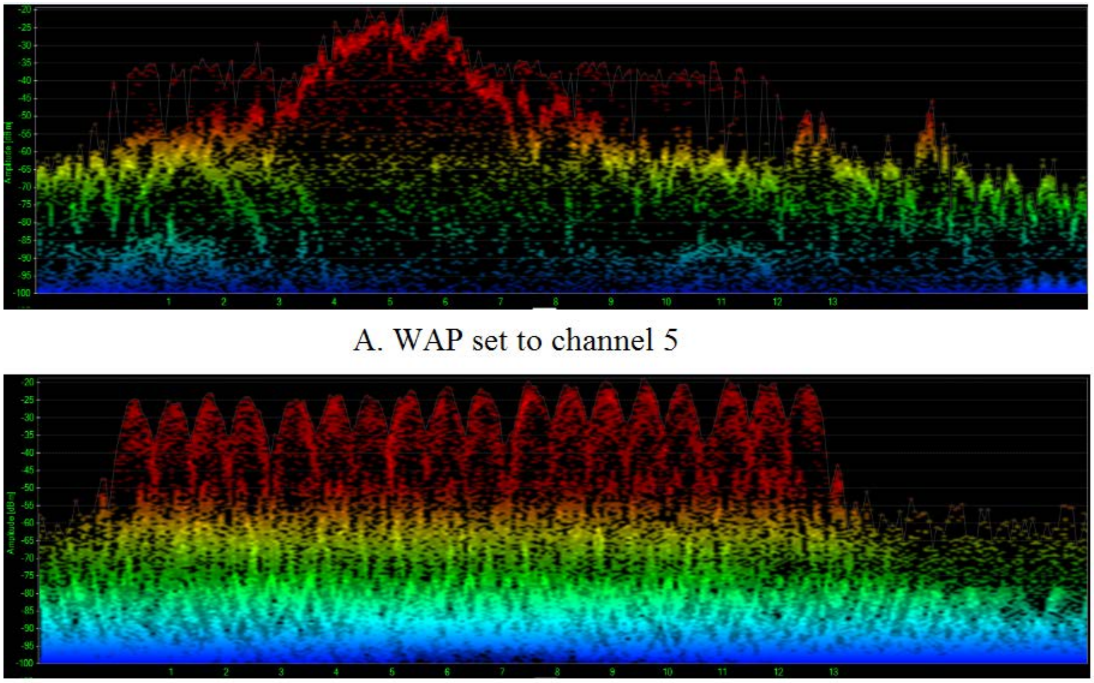


Figure 17 - Site E Theoretical Spectrum.

In Figure 14 it is apparent that there is overlap in the 2.4 GHz wireless connection to site site B and the wireless access point. It was determined that this overlap have minimal impact on performance due to directional antennas used. The antennas were pointed in opposing directions and were separated by a concrete building. Interference can come from multiple sources and have a major impact on the network. A device was tested which drastically reduced throughput on the WLAN at one of the sites. The root cause was interference with the 2.4 GHz wireless access point. The interfering device was a USB 2.4 GHz based wireless camera. This camera uses a proprietary frequency hopping method for the wireless capability. The spectrum impact when the camera in enabled is shown in Figure 18.

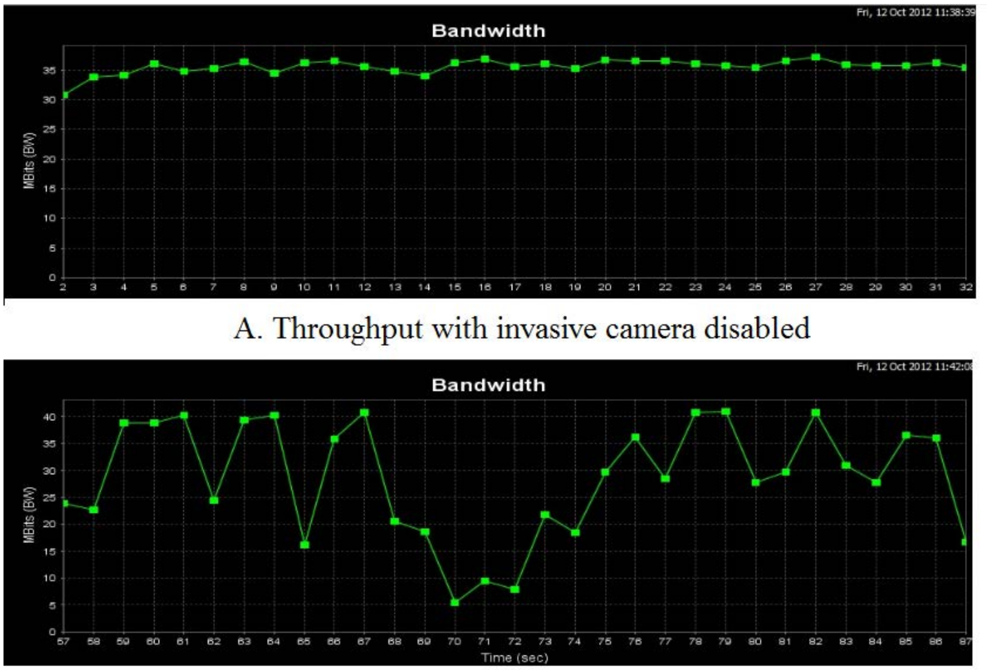


A. WAP set to channel 5

B. Spectrum with invasive camera enabled

Figure 18 - Spectrum Interference Caused by Frequency Hopping Camera.

Throughput on the wireless links is impacted severely when measured with the JPerf tool shown in Figure 19. After testing with different channels on the camera with the same results, it was determined that the camera was not sufficient for adequate operation of this network test setup and was eliminated. However, non-frequency hopping devices can be used in if setup in a manner to avoid interference with other wireless devices. The takeaway from this finding is that frequency management plays an important role in wireless network configuration.



A. Throughput with invasive camera disabled

B. Throughput with invasive camera enabled

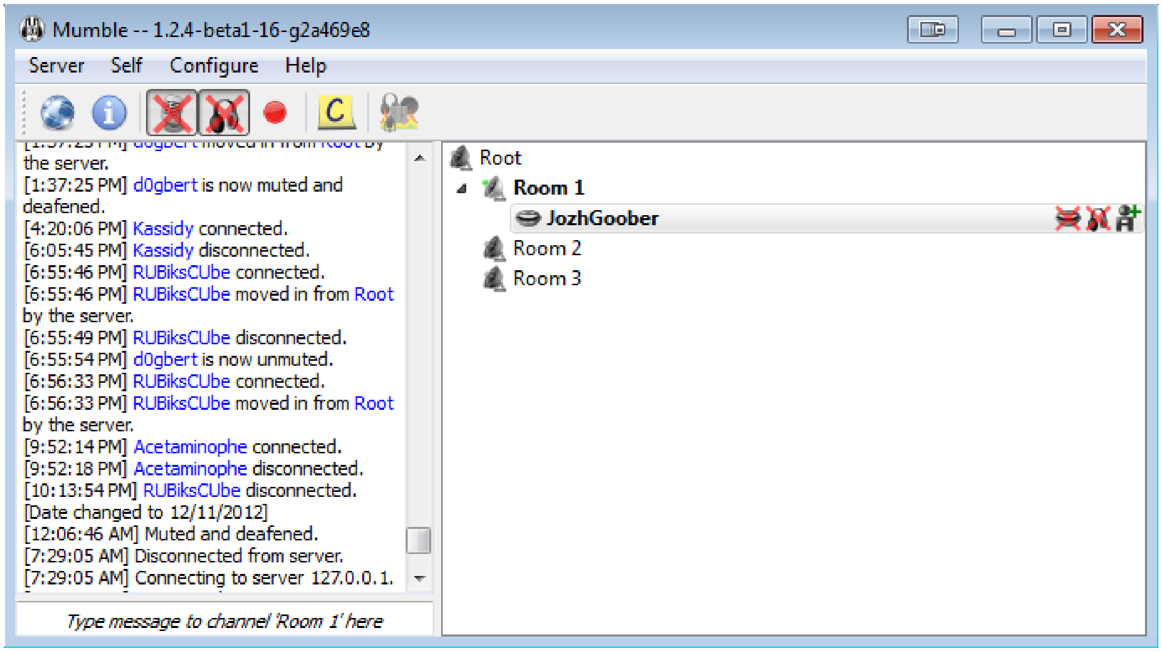
Figure 19 - Throughput Impact from Frequency Hopping Camera.

3.5 Applications

The following applications were used throughout experiment. They were selected due to their simplicity and functionality representative of tactical applications.

Mumble

Mumble is an open-source Voice over Internet Protocol (VoIP) client available from mumble.sourceforge.net. It was chosen as our VoIP client due to its ease of setup and use. Mumble uses a standard client/server model, with multiple Mumble clients connecting to a single server, known as Murmur. The Mumble interface is simple, with clients able to select a server, and once connected join different channels.


Mumble -- 1.2.4-beta1-16-g2a469e8
Server
Self
Configure
Help
Root
Room 1
JozhGoober
Room 2
Room 3
Type message to channel 'Room 1' here

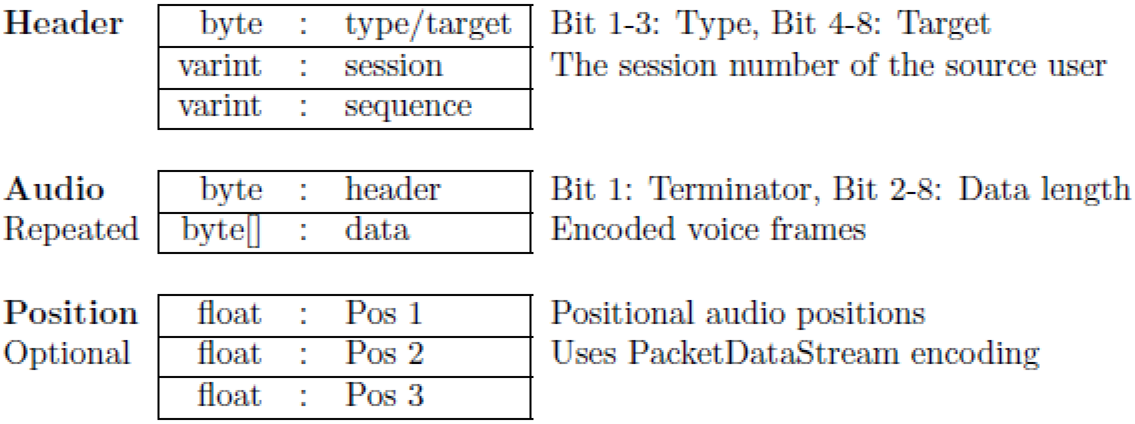
```
the server.
[1:37:25 PM] d0gbert is now muted and
deafened.
[4:20:06 PM] Kassidy connected.
[6:05:45 PM] Kassidy disconnected.
[6:55:46 PM] RUBiksCUbe connected.
[6:55:46 PM] RUBiksCUbe moved in from Root
by the server.
[6:55:49 PM] RUBiksCUbe disconnected.
[6:55:54 PM] d0gbert is now unmuted.
[6:56:33 PM] RUBiksCUbe connected.
[6:56:33 PM] RUBiksCUbe moved in from Root
by the server.
[9:52:14 PM] Acetaminophe connected.
[9:52:18 PM] Acetaminophe disconnected.
[10:13:54 PM] RUBiksCUbe disconnected.
[Date changed to 12/11/2012]
[12:06:46 AM] Muted and deafened.
[7:29:05 AM] Disconnected from server.
[7:29:05 AM] Connecting to server 127.0.0.1.
```

Figure 20- Mumble Interface.

Mumble/Murmur uses two channels of communication. First is a control channel using a TCP connection, used to reliably send control data between the client and the server. The second one is a UDP connection used to send voice data quickly, though unreliably. In situations where the UDP traffic is blocked, the voice traffic can be tunneled through the TCP connection. Both channels utilize strong encryption which is mandatory and cannot be disabled. The TCP control channel uses TLSv1 AES256-SHA, and the voice channel uses OCB-AES128.

The connection between Mumble and Murmur is first established over the TCP control channel using a basic handshake and version exchange, establishing cryptography, then the server provides the client with the current channel states, user states, and server sync information. After this has been established the client attempts to make a UDP connection through a simple ping. Once the ping is responded to, all voice communications will be sent over this UDP channel. If UDP communications are interrupted or this ping is not received, all traffic will be tunneled over TCP until the UDP connection can be reestablished.

Voice data is transmitted in variable length packets, which consist of a header followed by data segments. The encoded voice data is contained in a variable number of audio segments. An optional positional audio segment may be added, however this functionality was disable for this test. The UDP payload is limited to 1020 bytes, in order to use a 1024 byte UDP buffer after the 4 byte encryption header is added. The UDP packet structure is broken down in Figure 21.



Header	byte	:	type/target	Bit 1-3: Type, Bit 4-8: Target
	varint	:	session	The session number of the source user
	varint	:	sequence	
Audio	byte	:	header	Bit 1: Terminator, Bit 2-8: Data length
Repeated	byte[]	:	data	Encoded voice frames
Position	float	:	Pos 1	Positional audio positions
Optional	float	:	Pos 2	Uses PacketDataStream encoding
	float	:	Pos 3	

Figure 21 - UDP Packet Structure.

Mumble uses two different codecs for voice traffic. The first one is Speex (www.speex.org) , which is optimized for low bit rate audio. The second is CELT (www.celt-codec.org), which is used for higher quality audio. Newer versions of Mumble are replacing both of these codecs with a newer codec called Opus (opus-codec.org/), but the functionality remains the same. All of these codecs are optimized for low latency, variable bitrates, and variable frame sizes. Speex supports bitrates from 2.14-44 kbps, while CELT is optimized for 24-128 kbps. Opus is designed to work from 6-510 kbps. In practice, these values are varied continuously as voice data is encoded, and the available bandwidth changes. For additional details about the codecs, please consult their respective websites.

Linphone

Linphone was chosen as our point to point communications software. It offers voice and video communications using Session Initiation Protocol (SIP). SIP is used to establish and control communications channels, but does not require any specific protocol to be used. It is also transport layer independent, able to operate over TCP, UDP, or SCTP (Stream Control Transmission Protocol). It is also capable of using TLS for security. A chart of SIP requests is shown in Table 4.

Table 4 - SIP Messages.

Request	Description	Defined in
INVITE	Indicates a client is being invited to participate in a call session.	RFC 3261
ACK	Confirms that the client has received a final response to an INVITE request.	RFC 3261
BYE	Terminates a call and can be sent by either the caller or the callee.	RFC 3261
CANCEL	Cancels any pending request.	RFC 3261
OPTIONS	Queries the capabilities of servers.	RFC 3261
REGISTER	Registers the address listed in the To header field with a SIP server.	RFC 3261
PRACK	Provisional acknowledgement.	RFC 3262
SUBSCRIBE	Subscribes for an Event of Notification from the Notifier.	RFC 3265
NOTIFY	Notify the subscriber of a new Event.	RFC 3265
PUBLISH	Publishes an event to the Server.	RFC 3903
INFO	Sends mid-session information that does not modify the session state.	RFC 6086
REFER	Asks recipient to issue SIP request (call transfer.)	RFC 3515
MESSAGE	Transports instant messages using SIP.	RFC3428
UPDATE	Modifies the state of a session without changing the state of the dialog.	RFC3311

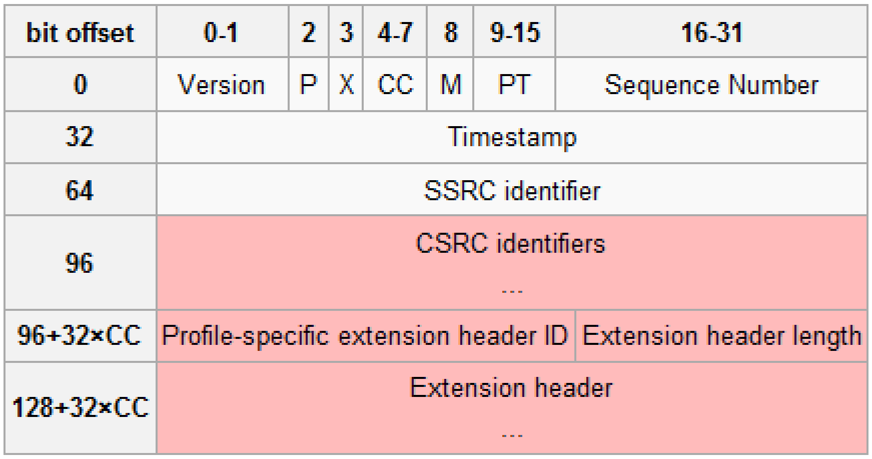
Linphone is capable of using a variety of codecs for both voice and video channels. Supported voice codecs include Speex (as was used with Mumble), G.711 (both µ-law and A-law), GSM (as used in cellular telephony), and iLBC through a plugin, which was not used in this test. Supported video codecs are VP8, H263, MPEG-4, Theora, and H.264, with varying resolutions dependent on network bandwidth and CPU power.

For the purposes of this experiment, Linphone was only used as a demonstration of point to point video communications using the laptops' built in cameras. The default settings of Speex and VP8 codecs where kept, with adaptive rate control enabled. One limitation of Linphone is the inability to conference multiple video links. However, voice conferencing is possible.

VLC

VLC Media Player was used as a client to receive the various video streams from the different cameras set up during the experiment. VLC was chosen because it supports a broad set of protocols and codecs.

Each camera operated with a different codec and streaming protocol, and a separate instance of VLC was opened for each stream. The FOSCAM FI8910W pan and tilt cameras used the MJPEG video codec over a standard HTTP link. The D-Link DCS-942L cameras used the MPEG-4 video codec, streamed using Real-Time Streaming Protocol (RTSP). RTSP is designed specifically for multimedia playback, with control sequences sent over an established TCP connection. In conjunction with RTSP is RTP (Real-Time Transport Protocol), which carries the actual video traffic. The RTP packet header format is shown in Figure 22.



bit offset	0-1	2	3	4-7	8	9-15	16-31
0	Version	P	X	CC	M	PT	Sequence Number
32	Timestamp						
64	SSRC identifier						
96	CSRC identifiers ...						
96+32×CC	Profile-specific extension header ID						Extension header length
128+32×CC	Extension header ...						

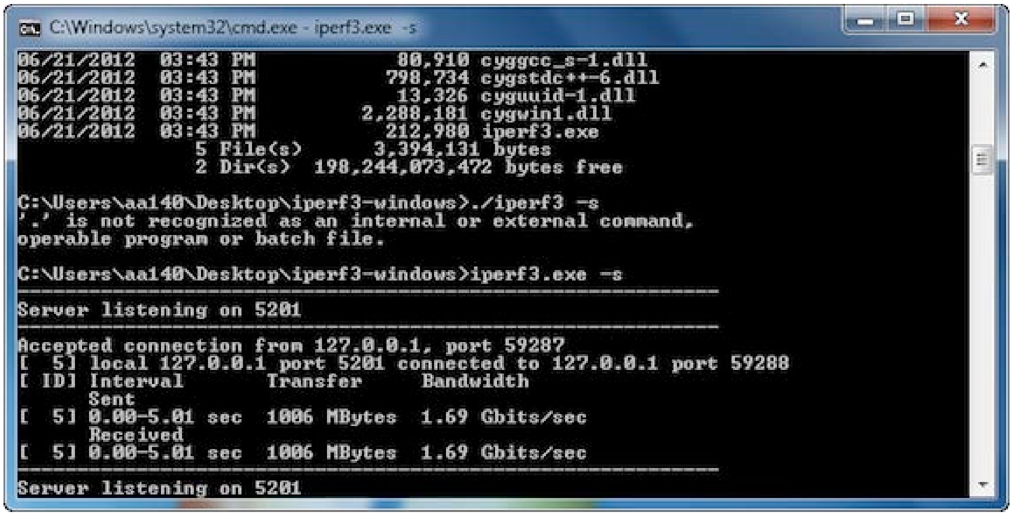
Figure 22 – RTP Packet Header.

The extension is where the video data is contained. The RTP payload is defined by the Payload Type (PT) segment, which are predefined in RTP profiles. For additional information about RTP, consult RFC 3550 and 3551.

An additional functionality of VLC that was tested in the lab is its ability to accept video input, transcode (if desired), and stream it through a selected protocol. Available protocols include standard HTTP traffic, RTSP and RTP streams, and UDP streams (which can be broadcast on a multicast address). This can be used to stream analog video through a computer, out into the network. The ASTAK CM842T cameras required this functionality in order to be streamed over the network, as they only provided analog video output.

Iperf/Jperf

Iperf is an open source command line network testing tool that is able to create TCP and UDP data streams and measure their throughput. It operates on a client-server model with one instance of iPerf sending data to another, though it is also able to operate in bidirectional modes. When operating in TCP mode, Iperf measures the maximum throughput of the link in real-time, with available bandwidth increasing or decreasing with the presence of other network traffic. In UDP mode, the user sets the bandwidth Iperf will attempt to use, and then Iperf will measure the actual throughput. This method can be used to stress test the network by generating more traffic than the network can support.



C:\Windows\system32\cmd.exe - iperf3.exe -s

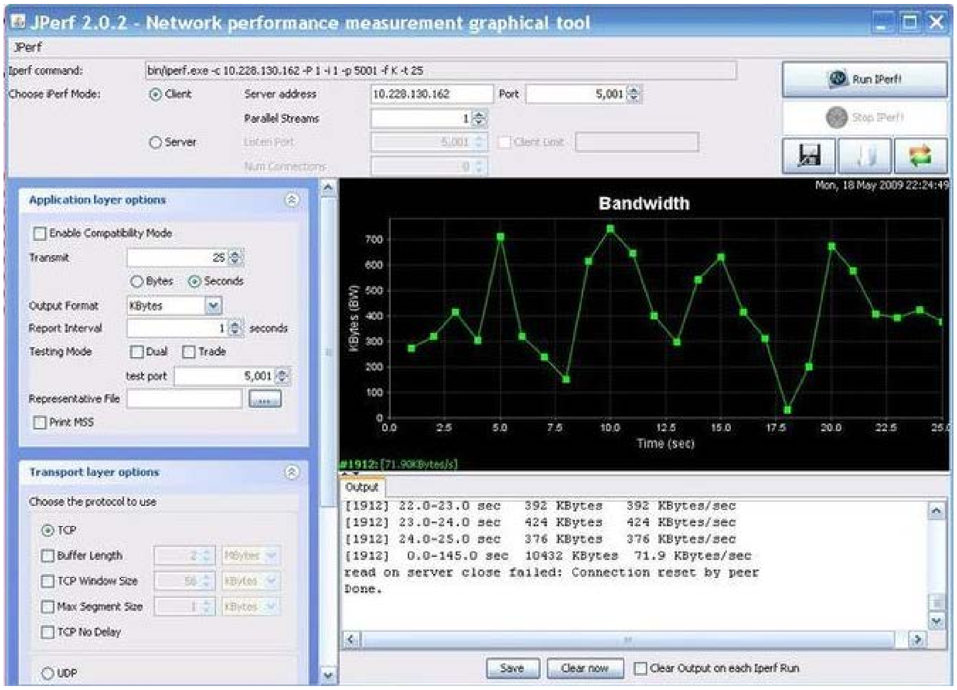
```
06/21/2012  03:43 PM            80,910 cyggcc_s-1.dll
06/21/2012  03:43 PM           798,734 cygstdc++-6.dll
06/21/2012  03:43 PM            13,326 cyguuid-1.dll
06/21/2012  03:43 PM         2,288,181 cygwin1.dll
06/21/2012  03:43 PM           212,980 iperf3.exe
               5 File(s)      3,394,131 bytes
               2 Dir(s)  198,244,073,472 bytes free

C:\Users\aa140\Desktop\iperf3-windows>./iperf3 -s
'.' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\aa140\Desktop\iperf3-windows>iperf3.exe -s
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from 127.0.0.1, port 59287
[  5] local 127.0.0.1 port 5201 connected to 127.0.0.1 port 59288
[ ID] Interval        Transfer     Bandwidth
      Sent
[  5] 0.00-5.01 sec  1006 MBytes  1.69 Gbits/sec
      Received
[  5] 0.00-5.01 sec  1006 MBytes  1.69 Gbits/sec
-----------------------------------------------------------
Server listening on 5201
```

Figure 23 - Iperf ScreenShot.

Jperf is a graphical frontend for Iperf, providing the user with an easy to use interface as well as charts of current bandwidth results. This allows for easy visualization of network traffic, and the effects of various disruptions to throughput, as seen in Figure 24. It is possible to run multiple instances of Iperf/Jperf on a single link, allowing measurement of bandwidth while traffic is generated.



JPerf 2.0.2 - Network performance measurement graphical tool

Iperf command: bin/iperf.exe -c 10.228.130.162 -P 1 -i 1 -p 5001 -f K -t 25

Choose iPerf Mode: ● Client ○ Server

Server address: 10.228.130.162 Port: 5,001

Parallel Streams: 1

Listen Port: 5,001 □ Client Limit

Num Connections: 0

Application layer options

□ Enable Compatibility Mode

Transmit: 25 ○ Bytes ● Seconds

Output Format: KBytes

Report Interval: 1 seconds

Testing Mode: □ Dual □ Trade

test port: 5,001

Representative File: ...

□ Print MSS

Transport layer options

Choose the protocol to use

● TCP

□ Buffer Length 2 MBytes

□ TCP Window Size 56 KBytes

□ Max Segment Size 1 KBytes

□ TCP No Delay

○ UDP

Output

```
[1912] 22.0-23.0 sec   392 KBytes   392 KBytes/sec
[1912] 23.0-24.0 sec   424 KBytes   424 KBytes/sec
[1912] 24.0-25.0 sec   376 KBytes   376 KBytes/sec
[1912]  0.0-145.0 sec  10432 KBytes  71.9 KBytes/sec
read on server close failed: Connection reset by peer
Done.
```

Figure 24 - JPerf Screenshot.

4.0 Results and Discussion

To capture the performance of the JALN surrogate and to expose the JALN Gaps an experiment under the pretenses to support a disaster response operation was developed. The experiment featured six scenarios that were performed on 26 October 2012.

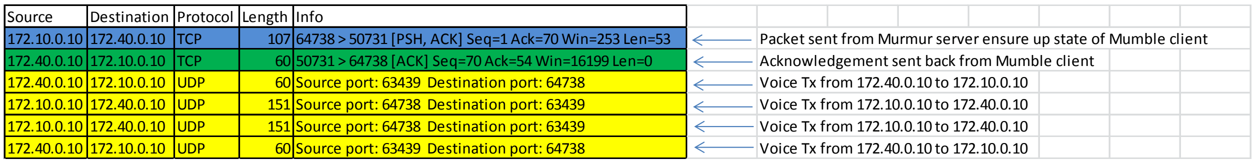
Four preliminary tasks were conducted prior to the start of these scenarios to ensure smooth test execution. The first Pre-Op was to provide communication between local site members via 900 MHz hand-held radios. The second was to ensure link connectivity between all network nodes. This was accomplished using a 32-bit Internet Control Message Protocol (ICMP) packet that was sent to every node from each workstation. The third was to run packet monitoring software to enable real time collection at each host. This was accomplished using *Wireshark* network protocol analyzer. The fourth was to run bandwidth monitoring software to allow remote host connections for bandwidth measurements. This was accomplished by opening a server on each node using JPERF GUI tool for IPerf.

Once these Pre-Ops were accomplished, the following Scenarios were conducted respectfully.

4.1 Scenario 1: Emergency Team Check-In

The first scenario's objective was to establish VoIP communications with all disaster response team members across all four sites. As previously mentioned, a server-client based application called Murmur (server) and Mumble (client) was used. Murmur and Mumble were installed and operated on THALTP01, while all other manned workstation ran the client application Mumble only. Through the Murmur server application a VoIP network called "Main Ops Net" was created and all clients were joined to this network. A roll call was then performed and the clarity of the voice transmissions was measured qualitatively. All members were able to effectively transmit and receive voice communication without degradation. Quantitative data was collected as well. Table 5 shows the typical traffic generated from Murmur and Mumble.

Table 5 - Murmur and Mumble Packet Capture.

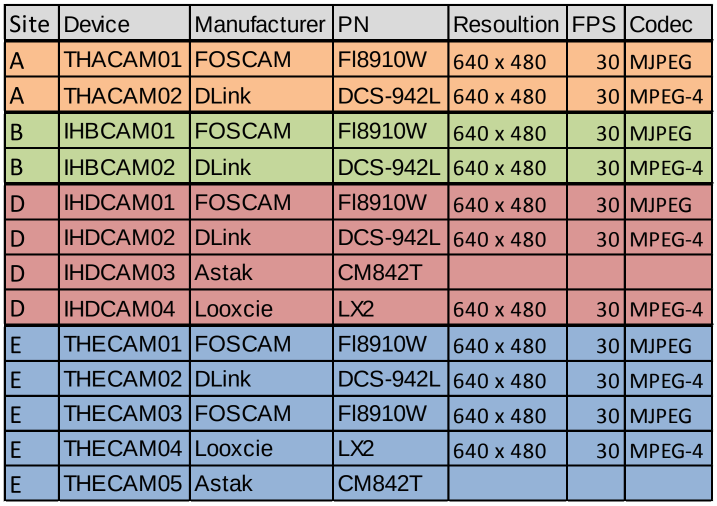


Source	Destination	Protocol	Length	Info		
172.10.0.10	172.40.0.10	TCP	107	64738 > 50731 [PSH, ACK] Seq=1 Ack=70 Win=253 Len=53	←	Packet sent from Murmur server ensure up state of Mumble client
172.40.0.10	172.10.0.10	TCP	60	50731 > 64738 [ACK] Seq=70 Ack=54 Win=16199 Len=0	←	Acknowledgement sent back from Mumble client
172.40.0.10	172.10.0.10	UDP	60	Source port: 63439 Destination port: 64738	←	Voice Tx from 172.40.0.10 to 172.10.0.10
172.10.0.10	172.40.0.10	UDP	151	Source port: 64738 Destination port: 63439	←	Voice Tx from 172.10.0.10 to 172.40.0.10
172.10.0.10	172.40.0.10	UDP	151	Source port: 64738 Destination port: 63439	←	Voice Tx from 172.10.0.10 to 172.40.0.10
172.40.0.10	172.10.0.10	UDP	60	Source port: 63439 Destination port: 64738	←	Voice Tx from 172.40.0.10 to 172.10.0.10

4.2 Scenario 2: Launch Local Video Feeds

The second scenario's objective was for each manned workstation to gain visual situational awareness of their local responsible disaster area. This involved launching video streams from IP video cameras only running within their local subnet. A list of each sites' video sources can be seen in Table 6.

Table 6 - Site Video Sources.



Site	Device	Manufacturer	PN	Resoultion	FPS	Codec
A	THACAM01	FOSCAM	FI8910W	640 x 480	30	MJPEG
A	THACAM02	DLink	DCS-942L	640 x 480	30	MPEG-4
B	IHBCAM01	FOSCAM	FI8910W	640 x 480	30	MJPEG
B	IHBCAM02	DLink	DCS-942L	640 x 480	30	MPEG-4
D	IHDCAM01	FOSCAM	FI8910W	640 x 480	30	MJPEG
D	IHDCAM02	DLink	DCS-942L	640 x 480	30	MPEG-4
D	IHDCAM03	Astak	CM842T			
D	IHDCAM04	Looxcie	LX2	640 x 480	30	MPEG-4
E	THECAM01	FOSCAM	FI8910W	640 x 480	30	MJPEG
E	THECAM02	DLink	DCS-942L	640 x 480	30	MPEG-4
E	THECAM03	FOSCAM	FI8910W	640 x 480	30	MJPEG
E	THECAM04	Looxcie	LX2	640 x 480	30	MPEG-4
E	THECAM05	Astak	CM842T			

All IP video cameras broadcasted their feeds over TCP Port 80. A custom program using VideoLAN (VLC) was written to simply launching all of IP video streams for each subnet. During this scenario each manned workstation was able to successfully launch all of their local video feeds. Qualitatively, all video streams delivered a crisp, smooth picture with very little latency and providing team members effective situational awareness of their responsible site. The available bandwidth across each site's local subnet was reduced due to the number of high resolution video streams traversing the network. For instance, Figure 25 shows the bandwidth between a wired and wireless workstation at site E before and after video streams are launched. As seen in the figure, the bandwidth is significantly reduced when the first workstation launches the five streams and further reduced when another workstation launches.

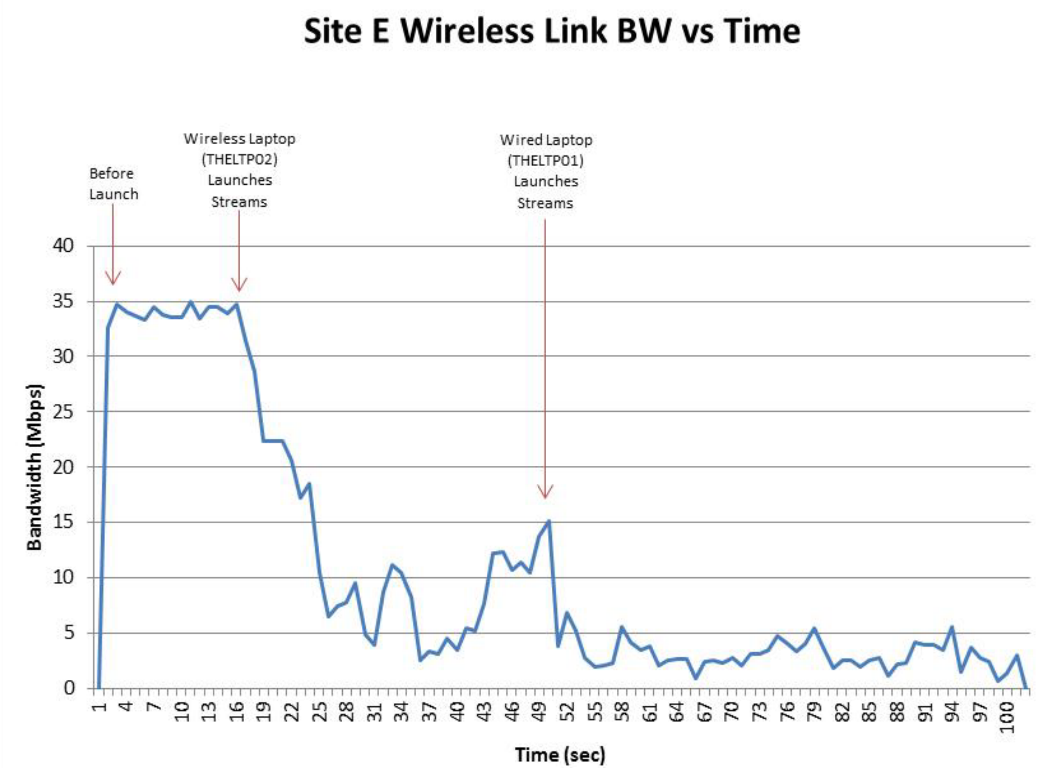


Figure 25 - Site E jPerf results between wired and wireless workstations.

4.3 Scenario 3: Launch Remote Video Feeds

The third scenario's objective was to enhance situational awareness across all sites. Specifically, this included launching video streams from all sites, on each manned workstation. The same custom program was used to launch these video streams. During this event, network performance was significantly degraded. Workstations were still able to launch local video streams; however, when pulling remote video streams they were either extremely slow to launch or failed to launch entirely. Streams that would launch had high latency and provided choppy video. Figure 26 shows the bandwidth of the site E's wireless link during this scenario. The figure also identifies bandwidth after each node pulls the video streams from site E.

In addition to these issues, other network resources were impacted, such as VoIP communication and desktop sharing. Due to the limited bandwidth available at Site A, the Murmur server was unable to keep alive VoIP sessions. Malformed Murmur packets and mumble checksum errors can be seen in Table 7. The packets also show that data was only lost from Site E's workstation to Site A's workstation.

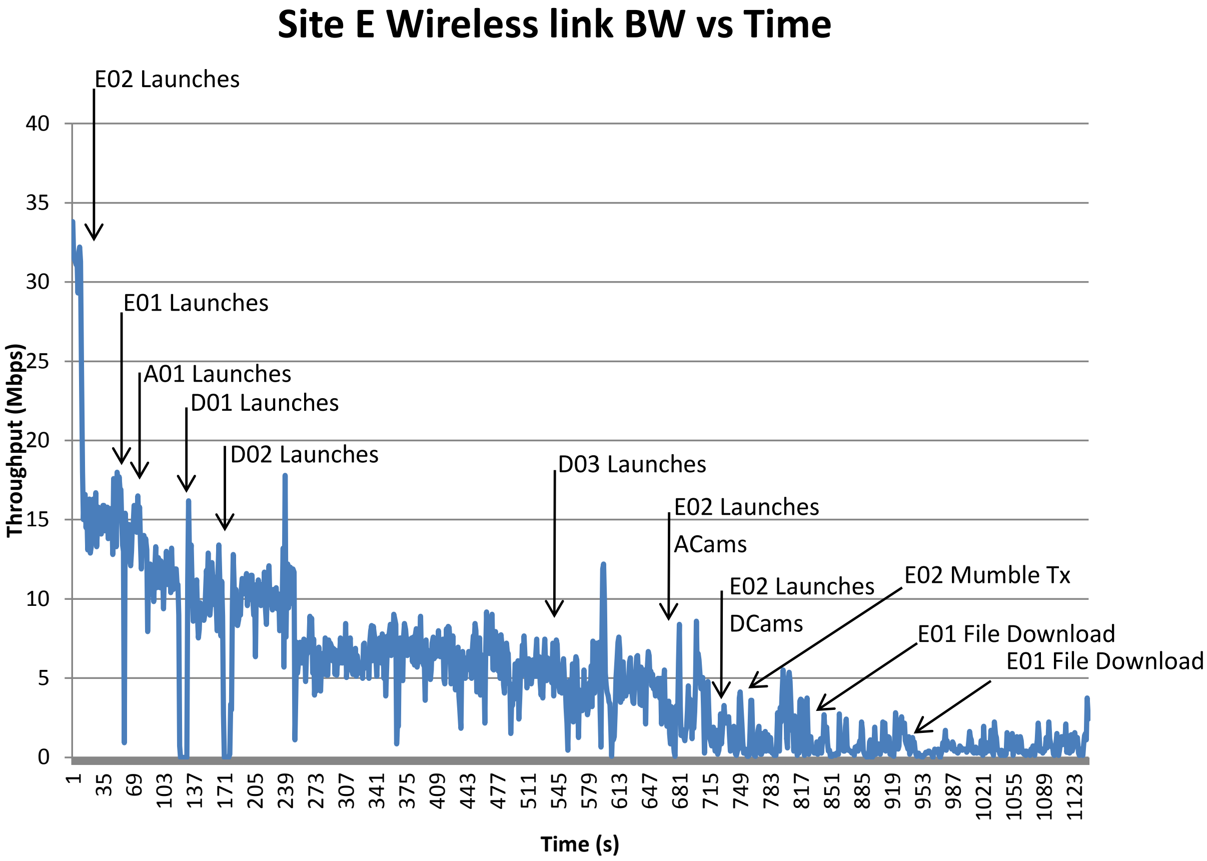
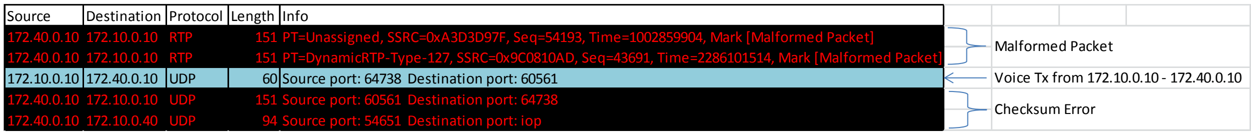


Figure 26 – Site E jPerf Link BW measurements made during remote video stream launches.

Table 7 – Murmur and Mumble Malformed Packets and Checksum Errors.



Source	Destination	Protocol	Length	Info	
172.40.0.10	172.10.0.10	RTP	151	PT=Unassigned, SSRC=0xA3D3D97F, Seq=54193, Time=1002859904, Mark [Malformed Packet]	Malformed Packet
172.40.0.10	172.10.0.10	RTP	151	PT=DynamicRTP-Type-127, SSRC=0x9C0810AD, Seq=43691, Time=2286101514, Mark [Malformed Packet]	
172.10.0.10	172.40.0.10	UDP	60	Source port: 64738 Destination port: 60561	Voice Tx from 172.10.0.10 - 172.40.0.10
172.40.0.10	172.10.0.10	UDP	151	Source port: 60561 Destination port: 64738	Checksum Error
172.40.0.10	172.10.0.40	UDP	94	Source port: 54651 Destination port: iop	

4.4 Scenario 4: File Transfer

The fourth scenario's objective was to send file data (180 MB) from each manned workstation at sites B, D and E to A. This was to determine the rate at which files could be transferred and to identify any associated impacts to other network resources. This event was effectively completed. In all cases, data was quickly transferred from each manned workstation to site A. Table 8 shows the data rate and time for each upload to Site A.

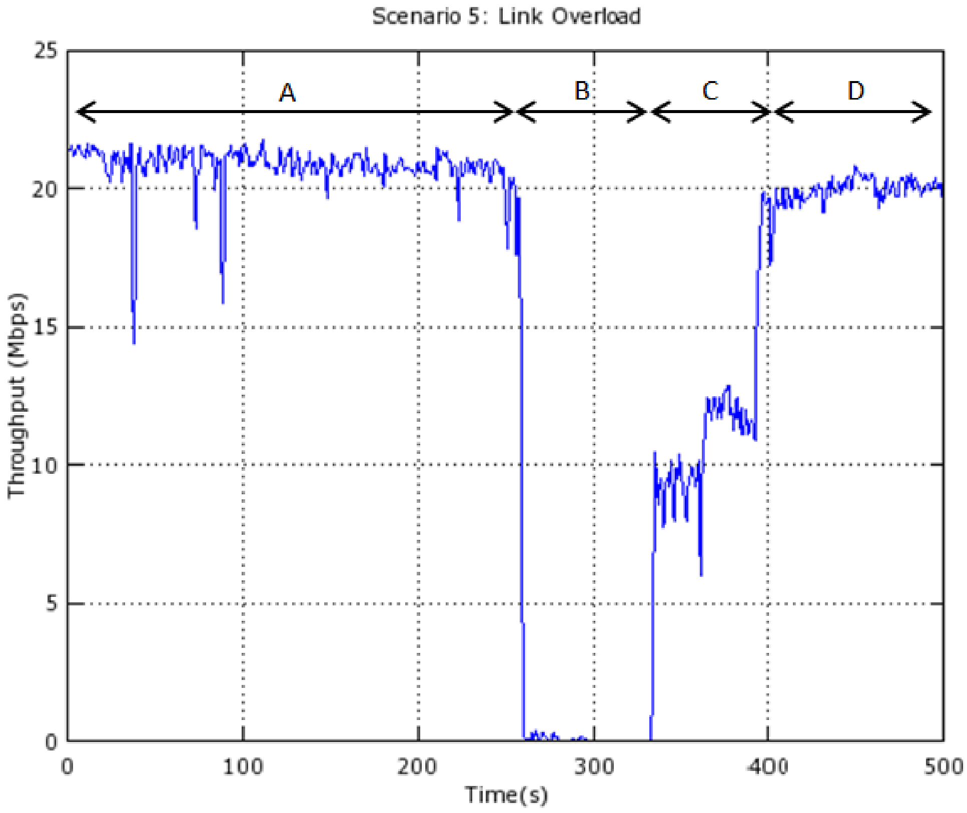
Table 8 – File Transfer Rates.

Device	Start Time	End Time	Rate (MBps)
THALTP02	11:04	11:11	1.24
THALTP03	11:03	11:11	1.2
IHBLTP01	11:03	11:05	4.45
IHBLTP02	11:03	11:06	2.2
IHDLTP01	11:05	11:09	4.5
IHDLTP02	11:04	11:06	4
THELTP01	11:07	11:10	8.6
THELTP02	11:06	11:09	2.5

4.5 Scenario 5: Link Overload

The fifth scenario's objective was to demonstrate a link failover for an overloaded primary link. Link overload occurs when there is enough traffic on a link such that the ping response times out on the corresponding link. Link overload was achieved by utilizing the *MikroTik* router's traffic generator to flood the primary link to site D. Performance monitoring was achieved by using jPerf. The expected result is to see throughput degradation once the traffic generator is enabled, throughput drop to nearly zero, switch to secondary 900 MHz link and throughput adjust accordingly.

Once the through put became noticeably higher (and the traffic generator still flooding the primary link with traffic), a path ping was used to verify the link failover. Once the pathping verified failover the traffic generator was disabled on the MikroTik and the link was restored to normal operation on the primary 5 GHz link. The results of this process are documented in Figure 27.



A: 5GHz Primary Link.
B: Traffic Generator enabled, link throughput degration.
C: Failover to 900MHz secondary link.
D: Traffic Generator disabled, link returns to primary 5GHz Link.

Figure 27 - Site A Scenario 5 - Link Overload.

4.6 Scenario 6: Link Loss

The sixth scenario's objective was to demonstrate link and routing failure/recovery. In a tactical scenario this would represent an airborne or ground node exceeding the backbone distance requirement or becoming completely compromised. The scenario in this setup will verify four link failovers and recoveries. Each link was assigned a metric (in the static routing table), therefore if a link goes down the traffic will be routed through the link with the next highest metric that is available. Link metrics can be seen in Table 9.

Table 9 - Link Metrics.

Link	Destination	Gateway	Priority	Metric
5 GHz A-D	172.30.0.0/16	192.168.30.4	Primary	2
900 MHz A-D	172.30.0.0/16	192.168.40.4	Secondary	4
CDL A-D	172.30.0.0/16	192.168.70.4	Tertiary	6
5 GHz A-B-D	172.30.0.0/16	192.168.20.4	Quaternary	8
2.4 GHz A-B-D	172.30.0.0/16	192.168.10.4	Quinary	10

The link failover occurs in the following order: Site A – Site D 5 GHz Link, Site A – Site D 900 MHz link, Site A – Site D CDL link, Site A – Site B 5 GHz link – Site D 5 GHz link and Site A – Site B 2.4 GHz link – Site D 5 GHz Link. The failure is accomplished by simply disconnecting each link from Site A's router – effectively creating an instantaneous downed link. The flow diagram shown in Figure 28 represents the process described above.

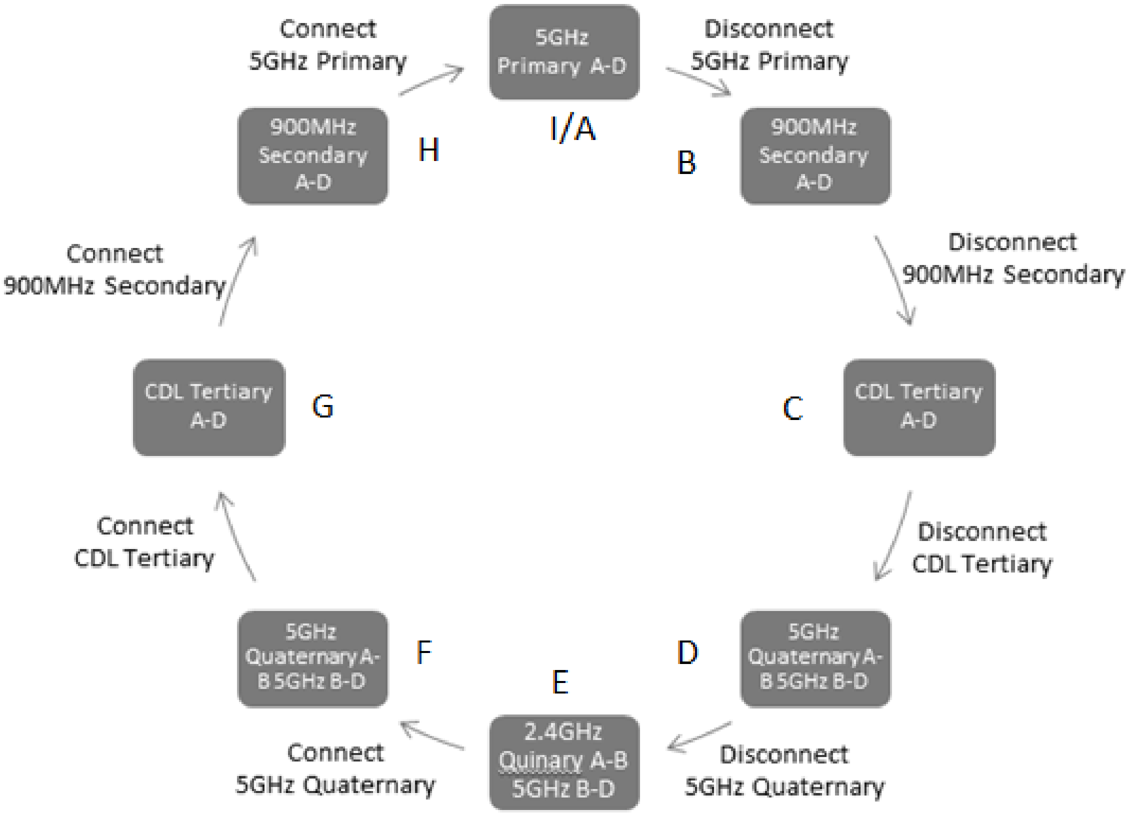


Figure 28 - Scenario 6 Link Loss State Diagram.

The throughput was monitored with JPerf during this scenario. From the data collected it is evident when each link fails over. The data is shown in A: 5 GHz Primary A-D.

B: 900 MHz Secondary A-D.

C: CDL Tertiary A-D.

D: 5 GHz Quaternary A-B-D.

E: 2.4 GHz Quinary A-B-D.

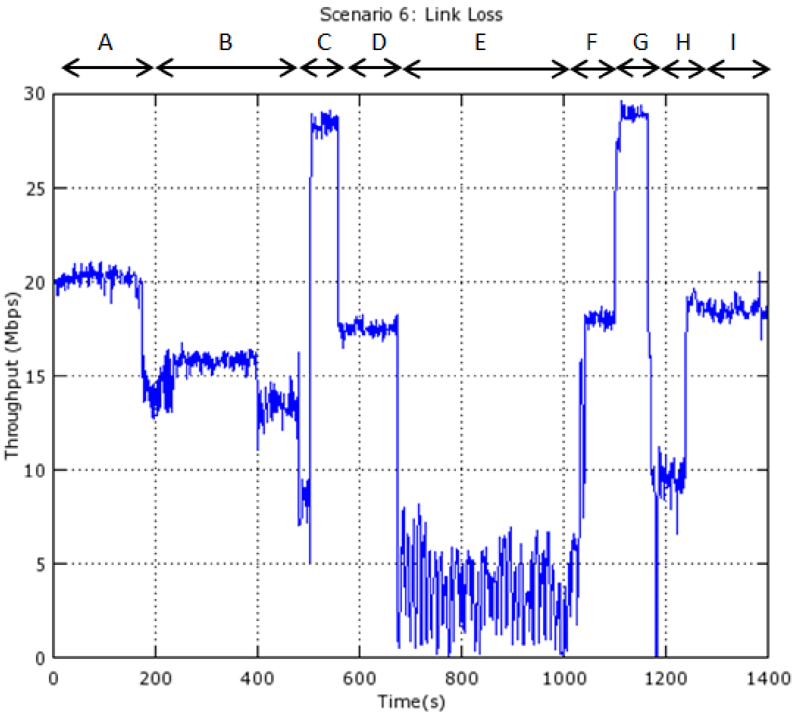
F: 5 GHz Quaternary A-B-D.

G: CDL Tertiary A-D.

H: 900 MHz Secondary A-D.

I: 5 GHz Primary A-D.

Figure 29 below (Corresponding states indicated by letters A-I correspond to the letters in Figure 29.



A: 5 GHz Primary A-D.

B: 900 MHz Secondary A-D.

C: CDL Tertiary A-D.

D: 5 GHz Quaternary A-B-D.

E: 2.4 GHz Quinary A-B-D.

F: 5 GHz Quaternary A-B-D.

G: CDL Tertiary A-D.

H: 900 MHz Secondary A-D.

I: 5 GHz Primary A-D.

Figure 29 - Scenario 6 – Link Loss.

It is important to note that having dedicated links and only failover backups will eventually result in link overload if the link is flooded with data, similar to scenario 5. In this situation the primary link will saturate and fail over to the secondary link and all traffic will be routed on that path. If the secondary link cannot handle the amount of traffic on the link it will also fail. This will happen inevitably so long as there is too much data for the links to handle. To mediate this risk load balancing can be performed. Load balancing distributes the workload across multiple available links to maximize throughput. In this experiment load balancing will improve throughput across bottlenecked wireless links.

5.0 CONCLUSIONS

Field measurements carried at AFRL's Newport Test Facility demonstrated that COTS wireless networking technology can be used for investigation of JALN related architecture and operations issues. The network topology used in the experiment the communication paths that were installed between AFRL's Rome and Stockbridge Test Sites. Follow-on experiments will be required to verify that the networking approach is sufficiently scalable so as to allow for the investigation of larger, more complex, network configurations like those expected to be realized in future ALNs.

6.0 RECOMMENDATIONS

Going forward, work should first focus on better understanding the current JALN capabilities and specific weaknesses. Objectives and goals should be well defined to ensure continued work meets the needs of the JALN effort. In particular, the types of tactical applications and scenarios should be defined and described to ensure proper surrogate design. To gain insight, direct interaction should be made with JALN working groups and the Joint Tactical Edge Network (JTEN). Industry research should also be conducted to lessen the risk for duplication of effort and to ensure that a plausible solution is neither already in work or exists. This should include LIT and Defense Technical Information Center (DTIC) report searches.

6.1 Simulations

Simulation of network functionality should be integrated into the JALN surrogate design. This would help characterize network performance for a scaled number of nodes. This type of simulation could be performed prior or after field experimentation as either a baseline or to confirm measured data. Simulation would also help identify parts of the network that may be or become bottlenecks under network loading. OPNET enables planning and design of networks with industry standard protocols and built-in device models.

6.2 Address Structure

The address structure should also be reinvestigated. IPv6 offers addresses to automatically configure through Stateless Autoconfiguration. Stateless Autoconfiguration allows for automated IP address configuration without the use of dynamic host configuration protocol (DHCP).   Autoconfiguration of an individual node derives tentative link-local addresses with a prefix of FE80::/64 and initiates Duplicate Address Detection (DAD) to verify uniqueness of the local link. Autoconfiguration also could prove to be very useful in the JALN due to its ease of address configuration. This will also assist with network entry/exit. With Autoconfiguration the new nodes will simply move into range to join the network.

6.3 Routing

Static routing, like that used in this experiment, is the simplest form of routing – however it is entirely manual. Static routing is beneficial when there are a relatively low number of devices in the network and the routes are not likely to change. In a realistic the JALN scenario, static routing is a constraining factor. That is to say, if a node is added to the network it will need to be manually configured and the operator must know the subnet that the device will be used on. Dynamic routing protocols reduce the amount of configuration by 'learning' the network which they are connected to. Dynamic routing protocols allow routers to dynamically learn network destinations, the route to them and how to advertise them to other routers. Directly connected routers also have the ability to learn routes from their next hop running a different routing protocol. A Router can then sort through their list of routes and select one or more best routes for each network destination the router knows or has learned. Utilizing dynamic routing in this scenario will benefit the wireless versatility of the JALN network.

7.0 References

[1] Air Force Chief of Staff, *Air Force Aerial Layer Networking Enabling Concept*, June 2012, (FOUO).

[2] J. C. Koziol, Lt. General, Director of Intelligence, Surveillance, and Reconnaissance Task Force, “ISR Leader: Ensuring Warfighters have the Intelligence Support They Require,” Geospatial Intelligence Forum, September 2010.

[3] AFCEA Intelligence, “Secretary of Defense Intelligence, Surveillance, and Reconnaissance Task Force”, http://www.afcea.org/mission/intel/ISR.asp.

[4] HQ ESC/NI1 for the USAF Airborne Network Special Interest Group, “Airborne Network Architecture: System Communications Description & Technical Architecture Profile”, v 1.1, pp. 5-6, October 7, 2004.

[5] Joint Vision 2020, Director for Strategic Plans and Policy, Strategy Division, U.S. Government Printing Office, Washington D.C., June 2000.

[6] *Air Force Aerial Layer Networking Enabling Concept*, et. al.

[7] Understanding IPv6, Second Edition by Joseph Davies.

8.0 LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

ALN	Aerial Layered Network
AP	Access Point
CDL	Common Data Link
COTS	Commercial-Of-The-Shelf
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DTIC	Defense Technical Information Center
GHz	Giga Hertz
GSM	Global System for Mobile
GUI	Graphical User Interface
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Message Control Protocol
IPv6	Internet Protocol version 6
JALN	Joint Aerial Layered Network
JTEN	Joint Tactical Edge Network
Mbps	Mega bits-per-second
MHz	Mega Hertz
PT	Payload Type
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SCTP	Stream Control Transmission Protocol
SIP	Session Initiation Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
OV	Operational View
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network