DISSERTATION

FULLY INTEGRATED NETWORK OF NETWORKS

Submitted by

Suzanna LaMar

Department of Systems Engineering

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Spring 2022

Doctoral Committee:

Advisor: Anura Jayasumana

Jim Cale
Yanlin Guo
Steve Simske

ABSTRACT

FULLY INTEGRATED NETWORK OF NETWORKS

There are many different facets to developing a fully integrated network of networks system that can facilitate seamless information exchange between nodes within a complex network topology. As an example, individual link resiliency, enhanced waveform capabilities, spectral and spatial diversity are all critical features in providing communications that can enable connectivity and interoperability for a fully networked system extending into multiple domains (ground, surface, air, and space). Steps taken toward achieving such an architecture are introduced with emerging millimeter wave (mmW) and high-band antenna technologies that can be integrated with future tactical multifunction software defined radios (SDRs) to enable information distribution between vital networked participants, including 5th generation aircraft. Small, lightweight mmW and high-band antenna designs that will enable small unit tactical operations to persist under electronic warfare conditions will be discussed. These small units are typically fielded with multiple communications radios but are limited in function and do not enable rapid communication on the move, or high-capacity data transfers at the halt.

Additionally, a revolutionary cognitive antenna (CA) is introduced where artificial intelligence (AI) techniques are proposed to aid in improving antenna functions, support self-healing attributes, and promote autonomous communication operations. A CA designed for future spacecraft (S/C) communications systems that is environmentally perceptive will be presented where it can sense and transmit radio frequency (RF) signals and cooperate with a cognitive radio

(CR) to modify waveform and beam pattern characteristics for enhanced resiliency and communications.

As an extrapolation to interoperability and information exchanges, data must be always secured. Common communications payload security architectures are presented as a basis for offering data protection to not only the system itself, but also to networks that are part of the larger enterprise solution. Similarly, machine learning methods are proposed to combat malicious cyber-attacks within an enterprise security space-based communications architecture to offer a more resilient, protective adaptive framework. Additionally, the machine learning algorithms seek to provide a viable solution for identifying, classifying, and detecting possible intrusions in a highly dynamic environment.

Machine learning is also applied to networking strategies to predict congestion before it happens; thereby, preventing bottlenecks within the network. This is especially important for critical, high-value information. A CONgestion Aware Intent-based Routing (CONAIR) architecture that facilitates faster and more reliable data exchanges between end users is proposed. The CONAIR architecture leverages platform and mission information to derive quality of service (QoS) metrics that can be used to support network route optimizations by using a network controller (NC) with machine learning to predict future network behaviors.

Finally, the CA, multifunction SDRs and NC subsystems are integrated into a robust architecture on unmanned aerial vehicles (UAVs) to form collaborative cognitive communications systems that are responsive to stressing operating conditions. Through collaborative behaviors and interactions, communications can be optimized. These discriminating technologies support the continued ambition for maturating military communications systems to benefit cooperative interactions and information exchanges between various users in multi-hop, complex networks.

ACKNOWLEDGEMENTS

I would like to thank Dr. Anura Jayasumana, from the Department of Electrical and Computer Engineering at Colorado State University (CSU), for his unwavering leadership and technical guidance in this research. Additionally, I wish to thank Dr. Sudhakar Rao, Dr. Melissa Young, Dr. Scott Seidel, and Dr. Jordan J. Gosselin as technical collaborators in providing support during the development of this research. As academic and industry cohorts, they were instrumental in providing technical interchanges and fundamental scientific discussions on technology focus areas.

DEDICATION

I would like to dedicate this dissertation to my loving family who supported and believed in me during my academic, professional, and research pursuits.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1. Introduction and Background

Different engineered network topologies exist today in military networks, such as star, mesh, tree, ring, point-to-point, circular, hybrid and bus topology networks, each with different configurations of nodes and communications links. Network of networks extend engineering network topologies such that they can all be connected to enable interoperability and facilitate faster and more reliable data exchanges. However, historically, directional communications were primarily found in high-end systems such as stealth fighters or fixed microwave backhaul, and systems tended to migrate away from omnidirectional systems to gain tactical advantage. This suggests that a revisit to directional communications to regain the spatial degrees of freedom is necessary, and with that, will come the provisioning for offering Low Probability of Interception (LPI) / Low Probability of Detection (LPD) capability at increased performance (e.g., realizable gain, range, or increased communications margin). Previous literature indicates that there are no one-sized fits all military communications systems; however, with the maturation in SDRs, innovative technology pairing to either use uniquely qualified antennas or support path diversity with opportunistic networking methods is possible with solid systems engineering frameworks and architectures at the communication system's core.

There is a divergence from omnidirectional systems that should occur to assure communication effectivity. For example, in currently fielded systems, communications and electronic warfare apertures are stove-piped in nature, meaning they hinder communications and cooperative operations with others who do not possess the same fielded system. Omnidirectional systems can degrade the air vehicle, ground vehicle, and surface vessel overall cross radar section, and therefore, do not reduce the low observability of the platforms from an adversarial standpoint. Stealth and speed of execution are of upmost importance to ensure soldier safety, but there is a

delicate balance as systems still need to be able to support various functions which include communications, interception, jamming, sensing, and most importantly the fusion of all information combined. While this thesis presents omnidirectional antenna systems as a hinderance because of the properties it introduces to the platform, it also recognizes that they should not be abandoned, but rather augmented for extending capabilities. Augmentation (or upgrades) should include evaluating cutting-edge antenna technology alternatives, and the application of AI for improved decision making as well.

A fully integrated network of networks system is important because new communications systems are emerging which need to be compatible and interoperable with legacy systems and yet still offer resiliency. This information exchange will provide reach back capability to decision makers (and executive leaders) to make real-time informative decisions about how to fight at the front of the battlefields. We know that the military will not divert from already funded, high technology readiness level systems due to both the need to have ready assets on hand and the excessive costs with any platform modification, testing and training. Therefore, this research will target a systematic approach for modifying, integrating, or increasing current communications systems capability to maximize the full use of available information (command, control, communication, and computer information). A fully integrated network of networks system will unite a directional communications triad to use an assortment of SDRs (and robust communications waveforms), distributed position, navigation and timing and advanced antenna technologies with AI or machine learning methods to improve system behaviors for increased situational awareness.

Several research questions and tasks are described in Chapter 2 that provide progress towards solving challenges that arise with compound diverse, stove-piped communications

systems and networks. Systems definitions, systems science concepts, simulated conceptual models, and physical system prototypes will provide an origin for this research. Not only do revolutionary antenna technologies or sophisticated aperture functions built on the premise of machine learning techniques need to be advanced, but security and networking frameworks also using machine learning methods need to be proposed to secure data and enable the optimal selection of available communications links to exchange information seamlessly across multi-hop networks. Table 1.1 provides a view of the research bottom-line up-front (BLUF) summary and discloses the key findings as an output of this research.

Table 1.1. Research Findings Summary

No.	Innovation Area	Technology	Contribution
1	Emerging Antenna Technology	Millimeter wave antenna designs (omnidirectional)	New small, lightweight millimeter wave antenna designs for the Pen-Cap Air antenna and Bunker. Completion of physical system prototype build and RF performance testing [1][2][3].
2		High-band antenna design (directional)	New quad-band petal reflector antenna design capable of supporting Ku Transmit (TX), Ku Receive (RX), K RX, and Ka TX for high capacity beyond line-of-sight (BLOS) communications. Completion of representative physical system prototype build and RF performance testing [4].
3	Multifunction Software Defined Radio Technology	Tactical manpack radio that can be integrated with the emerging antenna technologies to act as the communications radio	Novel systems definition and conceptual system design for tactical multifunction manpack radio. Readily integrated with key antenna technology for various military mission support while reducing soldier size, weight, and power (SWAP) from legacy communications equipment [5].

No.	Innovation Area	Technology	Contribution
4	Machine Learning Influenced Architectures	Cognitive aperture using ML for self-healing and environmental adaptation	A new method to decompose or slice aperture functions and use dedicated ML algorithms to improve aperture performance and sustainability is presented. A systems trade study was conducted to evaluate viable candidate algorithms to formulate recommendations for enabling self-healing and an environmentally aware aperture solution [6].
5		Cognitive aperture using ML for intrusion detection and combatting threats	Extending communications systems in space with known and vicious cyber threats is challenging. Security data architectures and ML at a system level can be applied to the cognitive aperture to combat threats [7]. A systems trade study was conducted to evaluate different flavors of algorithms, and analysis was performed on selected data set acquired for network intrusions. By extrapolation, neural networks proved to be the superior algorithm to identify, detect and classify different cyber threats [8].
6		Cognitive networking using ML for predicting congestion before it happens	An innovative architecture to increase network reliability and scalability is presented with the Congestion Aware Intent-based Routing (CONAIR) architecture. Simulated results demonstrate the ability to re-route high priority traffic to more capable communications paths to guarantee delivery of data at the destination [9].
7	System of Systems Integration	Integration of cognitive aperture, multifunction SDRs, and cognitive networking to present a cognitive communication system for small platforms	Novel system of systems architecture for low SWAP attributable platforms is presented. A mission use case is presented to which communications are disrupted. Results show with the fully integrated cognitive communications system, communications can persist [10].

1.1 Background

This section will provide a background into different technologies to understand what prior work has been done to address the problem statement posed in the introduction. Specifically, latest antenna designs for mmW (omnidirectional) and high-band (directional) antennas will be discussed, AI benefits and useful algorithms for applications to system architectures will be reviewed, and advanced networking routing techniques to distribute information seamlessly across the network will be described.

1.1.1 Millimeter-wave Antenna Technology Survey

Millimeter-wave communication has been identified as one of the most palatable techniques in the 5G mobile communications systems as it has the capability to significantly increase wireless data traffic [11]. Additionally, various external factors offer challenges (e.g., blockage, communication security, hardware development, etc.) for limiting the application in an outdoor environment. Different antenna element configurations such as cross, circle, or hexagon and the conventional rectangle were analyzed, where the circular antenna array showed to be more robust to angle variations that frequently occur due to antenna vibration in an outdoor environment. To guarantee effective coverage of such mmW communications systems, techniques such as cooperative multi-hop relaying in conjunction with these distributed antenna system configurations as a mechanism to extend range and provide increased gain were discussed. A case study of a novel, high gain, wideband and compact mmW 5G antenna, the clover antenna for cellular handsets, was presented by *Ozpinar et al.*, where the antenna achieved a measured peak gain of 7.8-9 decibels – isotropic (dBi) in the experimental frequency band of 24-28 Gigahertz (GHz) [12]. Since the capacity of the current 4G wireless cellular systems was not enough to sustain the continuing demand for wireless data traffic, which has been growing exponentially with emerging mobile applications requiring more bandwidth, the clover antenna in addition to other

antenna technologies should be designed and evaluated for use. Also, new mmW broadband monopole antenna designs and procedures for optimizing antenna parameters using a Computer Simulation Technology EM simulator for future 5G mobile network applications were described by *Abdalla et al.* [13].

Aqwil and Sxena highlighted that 5G wireless systems with improved data rates, capacity, latency, and QoS are expected to be the panacea of most of the current cellular networks' problems. An exhaustive review of wireless evolution toward 5G networks, new architectural changes associated with the radio access network design, underlying novel mmW physical (PHY) layer technologies (e.g., new channel model estimation, directional antenna design, and beamforming algorithms), and details of Medium Access Control (MAC) layer protocols and multiplexing schemes needed to efficiently support this new PHY layer were discussed [14]. In blending the different research initiatives by industries and academia, seven fundamental requirements of next generation 5G systems were defined: 1) 1 – 10 Gigabits per second (Gbps) data rates in real networks; this is almost ten times greater than traditional Long-Term Evolution (LTE) network's theoretical peak data rate of 150 Megabits per second (Mbps). 2) 1 millisecond (ms) round trip latency; this is almost 10 times less than 4G's 10 ms round trip time. 3) High bandwidth in unit area; this is needed to enable many connected devices with higher bandwidths for longer durations in specific areas. 4) Large quantity of connected devices; this is a mechanism for realizing the vision of internet of things (IoT), where emerging 5G networks need to provide connectivity to many devices. 5) Perceived availability of 99.999%; here, 5G envisions that the network should practically be always available. 6) Almost 100% coverage for anytime anywhere connectivity; this is to guarantee user coverage irrespective of the user's location. 7) Reduction in energy usage by almost 90%; this is targeted to promote the use of green technology [15]. The combined effect of

emerging mmW spectrum access, hyper-connected vision and new application-specific requirements has triggered the 5G evolution.

Finally, *Helander et al.* introduced the usage of high-gain steerable antenna arrays operating at mmW frequencies to support future cellular networks and a method for characterizing phased array antennas [16]. They suggested that for analyzing the performance, the total scan pattern of the array configuration together with its respective coverage efficiency be considered in order to compare different antenna designs and topology approaches to each other. These articles suggest that there are multiple mmW antenna technologies under development, with varying degrees of configurations and designs that have been analyzed to meet the key 5G requirements for different applications for future network of networks systems.

1.1.2 High-band Antenna Technology Survey

A review of high-band antenna technology is presented in this section where antenna designs, realizable gains, and approaches are considered as a mechanism to support multiple, high-band frequencies (e.g., Ku, K, and Ka-band) simultaneously. Specifically, the differences between common reflector antennas and phased arrays are described to understand their key performance requirements, capabilities, and overall offerings to apply for future communications at the halt (CATH) strategies. Reflector antennas are principally used in satellite communications. *Osaretin et al.* presented a quad-band antenna design that had an offset-fed parabolic reflector with dual feeds, using a polarization grid to diplex RF energy onto both compact corrugated feedhorns. Key antenna requirements for gain were cited as >35 dBi, beam efficiency > 95%, half-power beam widths (W-band at 3º, F-band at 2.4º, G-band at 1.5º, cross-polarization <-30 dB, return loss <-18 dB, and linear polarization [17]. *Deng et al.* described a shared aperture quad-band high gain reflectarray antenna (RA) which consisted of a Ka-band dual-band circular polarized RA, and a

tri-band double-screen frequency selective surface in between. The RA transmitted and received signals at both Ku-and Ka-bands with measured gains at 31 dBi at 12.5 GHz, 32 dBi at 14.25 GHz, 36.1 decibels –isotropic over circular polarization (dBiC) at 20.4 GHz and 39.4 dBiC at 30.2 GHz with corresponding aperture efficiencies of 45.6%, 44%, 56% and 54.8% respectively [18]. Commercial Ka and Ku-band reflectors antennas were needed for satellite reception to support the digital revolution applications which require data rates ranging from 100 Kilobits per second (kbps) to a few 100 Mbps [19]. The reflector and feed designs were presented in addition to the approach of low-cost production. Three dual-band concentric feeds were developed, one for Ka/Ku (30/12 GHz), Ka/K (30/20 GHz) and Ku / Ku (14/12 GHz) bands. The Ka/Ku feed had a corrugated horn that was integrated with COTS Orthomode Transducer (OMT) and a Low Noise Block (LNB) converter. Likewise, a single layer, dual linear polarized unit cell was introduced by *Harned et al.* for a quad-band RA antenna in the Ku-band region centered around 12, 13, 14, and 15.5 GHz. Prototypes were fabricated, analyzed, and measured for performance [20]. While, *Rao et al.* performed successful testing of shaped reflectors that allowed a single feed illuminating a reflector whose surface was shaped to fit the desired coverage shape on the ground [21]. In the past, single- and dual-reflector antenna configurations have been used for dual-linear or dual-circular polarization applications. For example, in the 1990s, direct broadcast satellites using high-powered downlink beam over the coverage region were developed; these satellites allowed users to receive high-definition TV channels using large circular dishes mounted on the rooftops of houses and buildings. Different types of satellite services that are widely being used for commercial and military communications are described as fixed satellite service (FSS), broadcast satellite service (BSS), personal communication service (PCS), mobile satellite service (MSS), and inter satellite service (ISS). FSS provides shaped or contoured beams for domestic or regional satellite services

at C-, Ku-, or Ka-band frequencies, where BSS provides downlink beams over a coverage region and provide weighted contoured beams to compensate for rain attenuation. PCS provides K/Ka band multiple beams to employ multiple reflector antennas. Each reflector uses many feeds for personal communications and data transfer from user-to-user via satellite, and it generally employs a forward link (ground-to-satellite-to-user) and a reverse link (user-to-satellite-to-ground). MSS provides communications to mobile users via satellite. These mobile satellites operate at low frequencies Ultra High Frequency (UHF), L- or S-bands and, therefore, need to use large deployable mesh reflector technology. The feed array employs many feeds with overlapping beams on the ground. Lastly, ISS provides data transfers from satellite to satellite and employs large gimbaled dual-reflector antennas with auto-track capability for global communications.

When compared with phased arrays, the reflector antennas are inexpensive and more efficient. However, the reflector antennas are typically heavy and operate in a single-band or dual-band supporting transmit or receive or both transmit and receive frequencies [22] - [27]. They are made of composite graphite material due to thermal stability required to operate in a space environment and are up to 3 meters (m) in size. Phased arrays play a crucial role in modern wireless communication systems due to their fantastic abilities to shape, switch, and/or steer the radiation beam of antennas [28]. Without using digital signal processing units, beam-switching, beam-steering, and even multi-beam arrays can be realized at microwave and mmW frequencies using RF circuit components. A phased array generally requires a complicated feeding network whose architecture is highly dependent on the application purpose. Due to the uniqueness of feeding topologies, in traditional thinking, it would be very challenging to integrate multiple phased arrays into a single network without dramatically increasing the overall size and fabrication cost. There are several innovative heterogenous integrated phased array systems, including the

beam-switching array, Van Atta array, reflection-type retrodirective array, and phase-conjugating array. Dual-mode retrodirective arrays can enable dual-band operation for increasing the data throughput and high quality of service, as an example. There is also a tri-mode heterogeneous integrated phased array that serves as a beam-switching array, a Van Atta array, and a phase-conjugating array respectively in the low, mid, and high bands. All of these identified phased array systems support high-band communications, but are a relatively expensive cost to fabricate making them undesirable for soldier protected CATH. One rationale, for desiring inexpensive and highly capable antenna technologies is because warfighters have a tendency to be emplaced in ruggedized terrains, and often in very extreme environmental conditions which would render the antennas unusable after only several deployments.

1.1.3 Artificial Intelligence / Machine Learning Algorithms

In this section, a review of AI algorithms is performed to understand the maturity and applications the algorithms have been applied to, and how they could be leveraged for advancing networking. Networking is the process of interacting with others to exchange information and is important to a communications system as a whole because while empowered by modems (to generate the waveforms to which the data resides on) and apertures (which point in the direction of transmission), networking uses protocols to route the data across multiple nodes within a network in order to extend beyond only point to point communications. An introduction of cognitive reasoning can solve a multitude of problems, for example, with mapping like pattern recognition, classification, and forecasting. Artificial Neural Networks (ANN) provide these types of models, and essentially are mathematical models that describe a function and are associated with a particular learning algorithm or rule to emulate human actions. ANN is characterized by three types of parameters; (a) based on its interconnection property (as feed forward network and recurrent network), (b) on its application function (as Classification model, Association model,

Optimization model and Self-organizing model), and c) based on the learning rule (supervised learning, unsupervised learning, reinforcement learning, etc.) In this case, ANN learning paradigms to which learning can refer to either acquiring or enhancing knowledge is emphasized. Supervised machine learning is the search for algorithms that reason from externally supplied instances to produce general hypotheses, which then make predictions about future instances. In other words, the goal of supervised learning is to build a concise model of the distribution of class labels in terms of predictor features. The resulting classifier is then used to assign class labels to the testing instances where the values of the predictor features are known, but the value of the class labels are unknown. There are various supervised machine learning classification techniques (e.g., decision trees and rule-based classifiers) [29]. As an example, decision trees are pathways that classify instances by sorting them based on feature values. Each node in a decision tree represents a feature in an instance to be classified, and each branch represents a value that the node can assume. Instances are classified starting at the root node and sorted based on their feature values [30]. In essence, supervised learning allows one to collect data or produce a data output and optimize criteria using previous experience. Alternatively, unsupervised learning techniques could be used to perform more complex processing tasks compared to supervised learning. Although it can be more unpredictable compared to other deep learning and reinforcement methods. Some prime reasons for using unsupervised learning methods are that it can find unknown patterns in data and features which can be useful in categorization [31]. Reinforcement learning (RL) discovers through trial-and-error interactions with its environment using a reward / penalty assignment [32]. RL is concerned with how intelligent agents take actions in an environment to maximize the notion of cumulative reward, and it differs from supervised learning in that it does

not need labelled input / output pairs, nor suboptimal actions to be corrected. Instead, the focus is on finding the balance between exploration and exploitation of current knowledge.

A deep neural network (DNN) is an ANN with multiple layers between the input and output layers, where learning can be supervised, semi-supervised or unsupervised. Graph neural networks (GNNs) were shown to achieve superior accuracy on a number of standard benchmark datasets for graph-based supervised learning, where learning tasks dealt with graph data which contained rich relation information among elements (e.g., in modeling physics system, learning molecular fingerprints, prediction protein interface, and classifying diseases) [33]. GNNs are deep learning-based methods that operate on graph domains. Although cited that GNNs are difficult to train for a fixed point, recent advances in network architectures, as explored in Chapter 8, optimization techniques, and parallel computations have enabled successful learning. From a systems engineering perspective both DNN and GNN have shown to be advanced machine learning approaches and can be utilized with existing and new multi-hop networks under investigation.

1.1.4 Advanced Networking Strategies

Advanced networking techniques and solutions are a powerful way to balance resources, handle traffic, and make effective decisions for providing information to the eventual destination. Deep learning was cited to improve heterogeneous network traffic control by characterizing the input and output patterns [34]. The results were reported as encouraging when using the deep learning system in comparison to a benchmark routing strategy, such as Open Shortest Path First (OSPF) in terms of significantly improving signaling overhead, throughput and delay. Also, software defined networking (SDN) is currently regarded as one of the most promising paradigms of the future Internet. A centralized controller in SDN can be replaced with multiple controllers to facilitate network scalability; however, there still lacks a flexible mechanism to balance traffic

load among controllers. *Yu et al.* identified a load balancing approach based on load informing strategy for multiple distributed controllers where a controller could make load-balancing decisions locally to reduce the time of load balancing in a complex network [35]. Additionally, besides the pedantic challenges with networking and load balancing, ensuring network service availability in link state routing networks through protection schemes is important [36]. There have been significant efforts applied to learn how to move packets between desired nodes effectively using routing tables [37]. Proposed solutions reduce the lookup complexity in forwarding tables by incorporating an improved computation and storage optimization strategy in edge routers. However, with the advent of real-time delay sensitive and mission critical application needs, stringent network availability requirements are levied on the internet service providers. And moreover, commonly deployed intra-domain link-state routing protocols react to link failures by globally exchanging link state advertisements and recalculating routing tables, which inevitably cause significant forwarding discontinuity after a failure. A hybrid link protection scheme can be applied to allow the network to achieve full failure coverage with loop-free criterion (e.g., uses large internet backbones for comping with single component failures). Lastly, it is noted, that modeling of cyber threats and vulnerabilities as part of the initial design and architectural stages of designing networks is highly recommended [38]. A way to improve networking is to ensure network availability against ever evolving cyber threats encouraging the need for enforcing data security architectures when formulating a robust system as described in Chapter 7.

1.2 Organizational Structure

This document is organized in a succinct manner to provide insight on enabling technology, where Chapter 1 provides general literature surveys of relevant technologies for achieving a fully integrated network of networks system. Chapter 2 provides a description of the research questions

sought to be answered and the corresponding tasks performed to progress towards some recommended solutions. Chapter 3 introduces novel mmW antenna technologies that enable communications on the move (COTM) for deployed operators to support communications under disadvantaged conditions, and on the move with a need to communicate rapidly. Standard antenna technologies for field operators are commonly deployed with commercial off the shelf Very High Frequency (VHF), UHF, L-band dipole antennas. Here, the operational context and rationale for the mmW antenna technology will be described, in addition to the designs, supporting modeling and simulation and analysis (M&S&A), and achieved validation measurements. Compact and lightweight antennas are required for future ground communication systems to provide wide angle 4π steradians coverage for manpack radio communications units carried by soldiers on the ground. Two innovative Bunker antenna designs at K-band will be described. The novelty includes antenna deployment from folded to unfolded configurations, compact size, low mass, near 4π steradians coverage, low-cost, wide bandwidth performance, and built-in radome for protection from severe environmental conditions. Design of these antennas, trades, RF simulations, mechanical design, antenna deployment, and material selection leading to product development will also be discussed. A prototype antenna has been fabricated and measured results are also presented. An excellent correlation between measured and simulated patterns has been achieved. The Bunker antenna has very wide frequency bandwidth of 86% covering Ku and Ka secondary frequency bands in addition to its primary K-band and thus could in the future replace three independent antennas on a dedicated manpack with a single tri-band antenna solution.

Future protected communications require soldiers on the ground to carry several antennas to integrate with their manpacks to provide secure and reliable communications at several frequency bands. Chapter 4 describes a novel petal-reflector that combines four antennas into one

using a quad-band antenna design. A dual-reflector antenna using axially displaced ellipsoid (ADE) sub-reflector fed with a wideband quad-ridged horn provided Ku-band TX, Ku-band RX, K-band RX, and Ka-band TX frequencies using a high performance quadruplexer. The main reflector is made of six identical petals that can be quickly assembled and disassembled in the battlefield. The antenna is assembled on a lightweight 2-axis gimbal to provide beam scanning over +/- 90^0 in elevation and 360^0 in azimuth. The antenna / gimbal combination is then mounted on a tripod structure for field operations and uses COTS components and 3-D manufactured parts to minimize cost and overall equipment weight. Details on the antenna design, analyses, hardware, integration, and test results are explained in Chapter 4.

Chapter 5 describes a future tactical manpack SDR that can be integrated with such sophisticated mmW and high-band antenna technologies for optimizing communications and increasing range. Here, emerging tactical manpack communications systems are being designed and developed to combat electronic warfare conditions in permissive environments. Ground operators are subjected to highly capable adversarial emitters or interference which degrade communications with their intended receivers, e.g., local squads, air platforms, or reach-back communications with headquarters. A future manpack SDR (and its accompanied antenna technologies) design will be outlined. Additionally, high-level descriptions of curated antenna technologies are re-capped. Key antennas such as the deployable and stowable Bunker ultra-wideband antenna and fixed, CATH rapidly assembled Quad-band Petal Reflector antenna are summarized in Chapter 5 as well but are detailed in 0 and Chapter 4. Future work will define the scope of the testing planned for 2022 to validate the manpack's radio performance.

CR technology has only recently been explored in the space domain via a National Aeronautics and Space Administration (NASA) Space Communications and Navigation (SCaN)

test bed onboard the International Space Station (ISS) in 2012 [39]. Chapter 6 presents the novel concept of a wideband CA functioning in concert with a CR that is able to learn from its experiences over time to determine action and parameter selections to avoid interferences and operate in anticipation of network challenges to support future space networks interoperability. By extending cognition to the system's front-end, beamforming, beam steering, nulling, and spectrum allocation at the antenna can be enhanced using learned experiences gained from interacting with the environment, and an introspective understanding of the antenna's health. The applied cognition will provide more robust interference mitigation, link optimization, and will improve cognitive networking (e.g., sharing the RF spectrum with other CRs while minimizing interference to primary users). The ability to adapt to current conditions and future challenges is a key performance parameter of the CA. For example, with the development of prospective mega-constellations totaling 15,000+ satellites [40] future challenges are to be expected with satellite communications interferences and interoperability. With the need to optimize channel capacity from an economics perspective, CRs built on SDR platforms have evolved to address the problem of spectrum congestion and maximization of frequency utilization. The emergence of CRs has introduced the notion of reconfiguration and adaptability within the space communications architecture. However, even the ideal SDR is limited by its physical hardware and component capability. Therefore, as CR technology becomes increasingly wideband, it is necessary to have a complementary wideband antenna technology developed.

Chapter 7 presents a comparison trade survey for two distinct data security architectures for space communications, which can be directly applied for consideration in the design of a more robust CA system. Space based communications networks require data to be handled and transferred at different sensitivity levels as well. The architecture evaluation focuses on a subset of

features, e.g., key space payload design constraints, and commonality of the encryption methods for various payloads to yield an architectural approach that can be applied to a resource constrained multiple levels of security (MLS) space communications network.

With the insurgency of Low Earth Orbit (LEO) S/C constellations, there is a need to safeguard and protect science, military, and commercial data against radical adversaries to maintain the Third Offset advantage. Adversaries are using Advanced Persistent Threats (APT) to target high priority communication systems, which continue to evolve with the advent of AI where machines inherently can identify system vulnerabilities expeditiously over naive human threat actors. Using a system engineering approach, Chapter 8 describes a disruptive abuse case (attack-plan) for an APT-attack on LEO Cognitive Systems (CS). Additionally, a trade-off analysis was performed that evaluated machine learning methods that could be used in the rapid detection and mitigation of an APT-attack. The trade results indicate that with the employment of neural networks, the CS's resiliency would increase in its operational state, and therefore, on-demand global communication services network reliability would increase.

Individual link resiliency, enhanced waveform capabilities, spectral and spatial diversity are all critical features in providing secure communications that can enable connectivity and interoperability for a fully integrated network of networks system. While different engineered network topologies exist, such as star, mesh, tree, ring, point-to-point, circular, hybrid and bus topology networks [41], each consisting of different configurations of nodes and links, we propose to use training and adaptive machine learning to smooth the transition between those engineered networks to enable interoperability in a network of networks system. Empowering network of networks communications with a robust, resilient architecture will facilitate faster and more reliable data exchanges between the end users. Chapter 9 describes the proposed CONAIR

architecture that will respond to platform and mission communications by leveraging available QoS information (e.g., link capacity, throughput, latency, and packet delivery ratio, etc.) to support network route optimizations using a NC. Furthermore, AI techniques can be applied to predict network behaviors under certain pre-trained conditions.

Chapter 9 provides a basis for using an NC to provide network resilience. Additionally, the novel CONAIR architecture and the AI technique designated to predict and mitigate link congestion is introduced. And lastly, the simulation approach which substantiates the network performance improvements using the CONAIR architecture for a complex network of networks system is presented.

Small attributable platforms, such as mini-drones, are promising vehicles to serve as communications relays to provide increased intelligence, surveillance and reconnaissance to decision makers at the forefront of the battlefield. Mini-drones can aid in distributed collaboration of information in highly competitive, dynamic, and stressing environments without endangering soldiers or high-value assets near immediate adversaries. Chapter 10 introduces a novel cognitive communications system that can be equipped on small attributable platforms; the system architecture amalgamates a highly capable environmentally perceptive aperture, a software defined radio, and sophisticated networking techniques. The proposed cognitive communications system uses the 5G new radio (NR) waveform and applies groundbreaking machine learning methods to facilitate systems orchestration amongst its subsystems to transfer information effectively between nodes, and across large-scale multi-hop networks, essential for rapid strike missions. With the challenges imposed by mature and readily available jammers, a cognitive communications system can be used to maintain and sustain continuous communication to provide near real-time surveillance and situational awareness updates. In addition to providing a comprehensive overview

of the cognitive communications system, a jamming analysis will be presented. Performance results will be compared to existing trite architectures consisting of siloed apertures and standard radio systems to demonstrate the auspicious technology offering of the cognitive communications system for low SWAP attributable platforms.

Chapter 11 will summarize the technical research contributions and findings presented and describe the important roles these capabilities play in developing a fully integrated network of networks system.

Chapter 2. Research Questions and Tasks

This chapter presents the research questions and tasks that provide progress towards resolving the problem statement and mitigating challenges that arise with complex heterogeneous, stove-piped systems and networks. In general, systems definitions and systems science concepts provide a basis for the research included in this thesis and include high-level systems engineering processes and analyses as shown in Figure 2.1. Conceptual systems designs are presented to set a plan and specifications defined for the physical systems before they are built. In all cases, the proposed physical system is simulated in the abstract by mathematical or other conceptual models which provide a mechanism to evaluate the performance or key role the physical system is intended to execute in the real world.

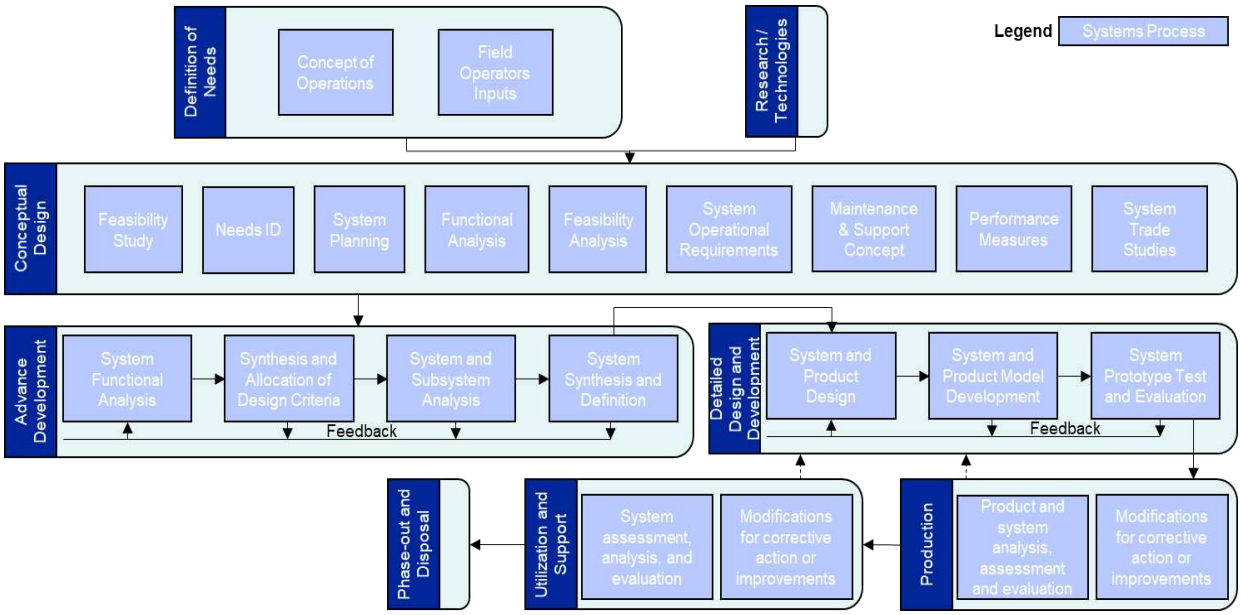


Figure 2.1. Systems Engineering Methodology

2.1 Research Questions

There are several specific research questions that are asked that will help determine the ideal technical approach for forming fully integrated network of networks systems. Systems are composed of components, subsystems, attributes, and relationships. The research questions

proposed shape the scope of the engineering tasks performed in support of this thesis, and they are further described in Section 2.2.

1. What improvements can be made to antenna technology that can enable soldier communications on the move and with future 5th generation aircraft?
2. What improvements can be made to antenna technology that can enable high-capacity data transfers for solider communications with future 5th generation aircraft or even long range backhaul communications with a strategic headquarters site?
3. How can SDRs or CRs be adapted to increase capability and offer multiple supporting functions, while minimizing SWAP, a key metric for communications equipment in any field operational situation?
4. How can multi-faceted, multi-domain phased arrays be improved to learn from environmental conditions and their surroundings, and available spacecraft information to improve sustainability, reliability, and RF performance by providing self-healing?
5. What architectures should be obligatory for communications systems to provide resiliency, and more so, what advanced methods can assure the protection of data across a network?
6. How can machine learning improve networking across heterogeneous networks when information is available to a network controller with multiple communication path options?
7. What systematic coordination can be made between technologies to optimize communications in general or for smaller, unmanned platforms?

2.2 Supporting Research Tasks

Through complex systems engineering methodologies, processes and activities, key tasks have been completed to further progress technologies and capability offerings through systemology and synthesis. The vital tasks performed are delineated below and describe the

primary scope of each effort achieved to evolve unique developments for fully integrated network of networks systems across multiple domains (ground, surface, air, and space).

Systems engineering and analysis reveal unexpected ways of using technology to bring new and improved systems and products to fruition. New and emerging technologies are expanding physically realizable design options and enhancing capabilities for developing more cost-effective systems. To address research question 1, Chapter 1 defines the system-level requirements for mmW antenna technologies for enabling COTM. The definition of needs at the system level (requirements) was the starting point for determining the antenna design criteria. The mmW antenna design was then modeled to analyze the predicted RF performance over the operational frequency range. Next, several physical antennas were manufactured, built, and assembled for two distinct configurations (Pen-Cap air antenna and the Bunker antenna). RF performance testing of the physical antenna prototypes was conducted at an antenna range to acquire performance measurements. Measured results were then compared to simulation to verify the model analysis and more importantly the prototype performance.

Likewise, for research question 2, Chapter 4 introduces the development of emerging high-band antenna technologies for enabling CATH. The system-level requirements as an entity are established by describing the functions that must be performed (those required to accomplish a specified mission scenario or series of missions, and those required to ensure the system is able to perform the needed functions when required) and are used for developing the high-band antenna design criteria. M&S&A was performed to verify the antenna model would meet the expected RF performance over the operational frequency range required. In design evaluation, an early model setup that fully meets design criteria was established as the baseline for the quad-band petal reflector antenna. Next the physical representative antenna (referred to as the solid reflector

antenna) was manufactured, built, and assembled. RF performance testing of the antenna prototype was conducted at an antenna range to acquire performance measurements. Measured results were compared to simulation to verify the model analysis and the solid reflector prototype performance.

System design is the prime agent of systems engineering, where it requires both integration and iteration, and invokes a process that coordinates synthesis, analysis, and evaluation. Research question 3 queries how one can adapt current radio technology with emerging SDRs or CRs to provide multi-function capabilities. To this notion, Chapter 5 applies principles from the engineering development phase, to derive system-level requirements obtained from mission operational scenarios and field operator surveys to generate the optimal SDR configuration to maximize capability and flexibility. A manpack SDR conceptual design was generated which afforded the opportunity to identify and prioritize design functions such that the technical performance measures and the related criteria for the design could be documented. Also, the plan to complete integration and evaluation to validate that the system was built correctly and was built as intended for operational use was defined. With the application of the iterative system design process which focused on minimizing SWAP, a viable enhanced SDR capable of supporting multiple missions (local, air, and BLOS conversations) with common communications equipment was abstracted. Another key benefit of the novel SDR technology was the reduction to equipment exchange time. This benefit allowed for soldier diversity based on the situation at hand.

There are many categories of systems, and there are several application domains where the concepts and principles of systems engineering can be effectively implemented. In that vein, a cognitive phased array system is investigated to address research question 4. First, every time there is a newly identified need to accomplish some function, a new system requirement is established. Chapter 6 performs a communication link analysis to derive the array's design criteria for space

domain operations. To further improve the phased array technology's performance in its operational state, complex methods of machine learning are applied to maximize subsystem and component interactions. Different machine learning algorithms were traded to determine the best suited algorithm to perform the function needed within the array based on pre-deployment training and other available resources. Important engineering domain manifestations of emerging technology and machine learning can be applied to optimize communications in general.

When addressing research question 5, the following tasks were performed and are described in both Chapter 7 and Chapter 8. General systems theory is concerned with developing a systematic framework for describing relationships amongst functions. One approach to an orderly framework is the structuring of a hierarchy of levels of complexity for subsystems studied in the fields of inquiry. A hierarchy of levels can lead to a systematic approach to systems that have broad application, where starting with the simplest level with defining the systems architecture and increasing to complex levels to incorporate more or improved capabilities by applying machine learning. Here, two space-based systems architectures were defined (distributed and centralized) to provide MLS and ensure data protection. A systems trade assessment was performed to approximate which security approach would be best selected in practice, given normal operations with no threats introduced, to protect the system data and data being transferred across the network. Next, an abuse case was developed to learn how a potential attacker could compromise the security infrastructure on a space-based communications system. Machine learning algorithms were researched and traded as a means to determine the best algorithm recommendation for identifying, classifying, and detecting advanced persistent threats. Using open-source test collection of data from Defense Advanced Research Project Agency (DARPA), training and learning curves for a subset of machine learning algorithms were generated from MATLAB to predict their expected

performance over a period in the presence of intrusions. These results were compared to the trade study to reaffirm the recommended algorithm selection.

Networking across heterogeneous networks is not an easy feat. To work towards addressing research question 6, a systematic approach was taken to develop a high-level systems architecture that could be used to influence communication path selection using a network controller to opportunistically route higher priority traffic to guarantee data delivery as described in Chapter 9. The systematic approach used translated operational needs and requirements into operational suitability blocks of the system. It consisted of a top-down, iterative process of requirements analysis, functional analysis and allocation, design synthesis, verification, and systems analysis and control. The top-down approach allowed for the view of the system as a whole and was necessary to ensure each subsystem effectively performs the role needed and its interfaces / flow of information is well understood. Given that, a network model was developed using EXata which consisted of multiple SDRs and highly capable network controllers. Machine learning was applied to the network controller to aid in the rapid decomposition of available link information to move traffic across the network effectively. Two test cases were constructed to validate the resiliency and scalability of the network when equipped with this architecture (and machine learning). The performance results proved that the total end-to-end latency was reduced when sending data across the network, and the total packet loss was minimized, and potential network bottlenecks were avoided with open, collaborative network system frameworks.

Lastly, when working to solve research question 7, we know that a system is a set of interrelated subsystems/components functioning together toward some common objective or purpose. The properties and behaviors of each subsystem have an effect on the properties and behavior of the set as a whole. Single relationships exist between subsystems, and they are

connected in some way to contribute positively to the overall system's function. In order to form a relationship of maximum effectiveness, the attributes of each subsystem must be engineered so that the collaborative functioning of the subsystems is optimized. To this end, explicit tasks performed commenced with the systems definition phase to express each enabling subsystem and their respective benefits to the collective system. Next, system-level requirements for a communications payload for small attributable platforms (e.g., mini-drones) were developed and are described in Chapter 10. Selected architectures were integrated, and machine learning methods were applied to provide a fully integrated cognitive communication system. To validate the effectivity of the cognitive communication system, a realistic mission use case was generated. Communications physical-level analyses were performed in accordance with a carefully crafted scientific methodology to evaluate the performance of a cognitive system over non-cognitive (stove-piped and federated) systems to justify the importance of systematic interactions built on relationships and behavior coordination in the presence of communications interference (purposely or non-purposely targeting receivers).

All of these support research tasks stemmed from broader systems engineering methodologies for engineering development and post engineering development stages and systems theory, to provide a path focusing on maturing technology offerings that would aid in fully integrated networks of networks systems, and that would exclusively benefit soldiers or troops typically in harms way by providing access to more data or information at their fingertips to make informed decisions thereby promoting increased situational awareness and military effectiveness.

Chapter 3. Compact Millimeter-Wave Antenna Designs

This chapter will describe new antenna designs that improve soldier communications while on the move. The antenna designs make communications possible with future 5th generation aircraft and enable small unit tactical operations to persist under electronic warfare conditions using robust small, lightweight antennas that operate at mmW frequencies. This work was published in elite peer-reviewed IEEE technical conferences as noted in [1] [2] and [3].

3.1 Millimeter-Wave Antenna Designs Background

An in-depth antenna trade study was conducted that evaluated several designs at mmW, and selections were made based on system metrics with antenna performance, human factor considerations and costs. With the selected designs, the performance was optimized for high gain and sidelobe suppression. Preliminary designs for a novel Pen-Cap antenna for air applications, and an innovative, functional deployable and stowable Bunker antenna for ground tactical operations will be described, both of which are critical for on the move operations in support of close air support (CAS) missions. Here, communications need to be dependable, interoperable, and secure both within the unit, and with the aircraft the operators are communicating with to exercise control. The antenna geometries, RF performance to include, return loss and radiation patterns, and prototype designs will be depicted. The Pen-Cap antenna design illustrates the suitability for use on small UAVs with certain profiles / contours and seeks to minimize airflow disturbances to the platform. In the case of the Bunker antenna, an impact assessment of the supporting mechanical rods on performance will be described. The flexible, but robust antenna deployment mechanism offers ease of use and increased maneuverability that are required for mission success. Measured results and correlation with simulations will be described for both antenna types.

3.2 Operational Context Review

For operational relevancy, it is useful to think about the end user requirements and applications of these antenna technologies. An integrated communications system (ICS) was developed to protect local, airborne, and reach-back communications from detection, interception, and exploitation. The ICS manpack (as described in Chapter 5) equipped with these advanced antenna technologies, such as the discriminating tri-band Bunker antenna, provides dependable, interoperable, and secure communications both within the unit, and with the aircraft the operators are communicating with to exercise a set of highly complex missions. A key mission that will be significantly enhanced with this technology is the CAS mission. CAS is a critical element of joint fire support that employs aircraft fires to destroy, suppress, or neutralize enemy forces to permit movement, maneuver, and control terrain. Soldiers on the ground require lightweight, enabling technologies, versus currently fielded legacy radios that have many limitations with survivability which will become a liability in the future. The ICS manpack and the innovative, functional, deployable and stowable Bunker antenna will enable fast, on the move and at the halt operations to future airborne platforms crucial to both air superiority and establishing air supremacy. Figure 3.1 shows a notional scenario using the ICS and the Bunker antenna as part of the soldier's manpack unit for communicating with future platforms, to identify, secure and disrupt the potential adversaries.

Wide-angle coverage antennas with compact size, low mass, and low-cost are required for soldiers' manpack radio units. In addition, the antennas need to be deployed in two unique configurations, (1) when the soldier is lying down on the ground "CATH" and (2) when the soldier is on the move (communications on the move "COTM"). A full coverage of 4π steradians is necessary for these antennas in order to communicate with both aircraft and the ground network

infrastructure. Part of this chapter will describe a novel Bunker antenna at K-band providing a small, non-invasive, deployable antenna solution in the field that could effectively support communications from ground operators and / or air vehicles in or near contested environments. The antenna is required for the ICS manpack applications with deployable configurations. An added capability of the Bunker antenna is that it is designed to support secondary Ku and Ka frequency bands in addition to the primary K-band frequencies where a single Bunker antenna replaces three separate antennas in the future.

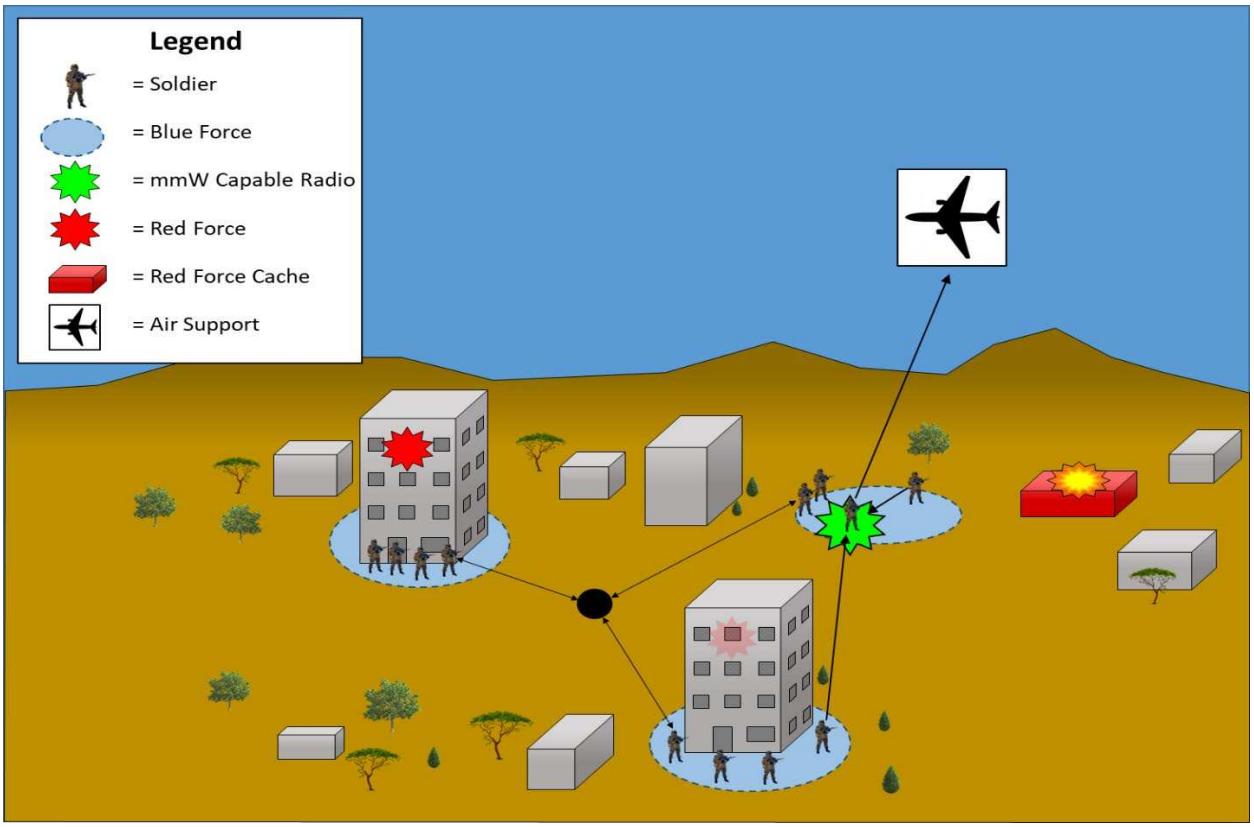


Figure 3.1. Millimeter-Wave Antenna with ICS Manpack Enabling Scenario

3.3 Antenna Designs

A preliminary trade evaluation was performed where different antenna configurations were investigated for 4π steradian coverage. The output of this trade resulted in two different antenna design options moving forward based on operational utility and need. The first antenna design

option is referred to as the Pen-Cap air antenna. It is narrowband by design providing 2π coverage (see Figure 3.2) and is capable of supporting K-band frequencies. Four prototype units were built, manufactured, and then tested in an anechoic chamber facility at Custom Microwave Incorporated (CMi) in Colorado.

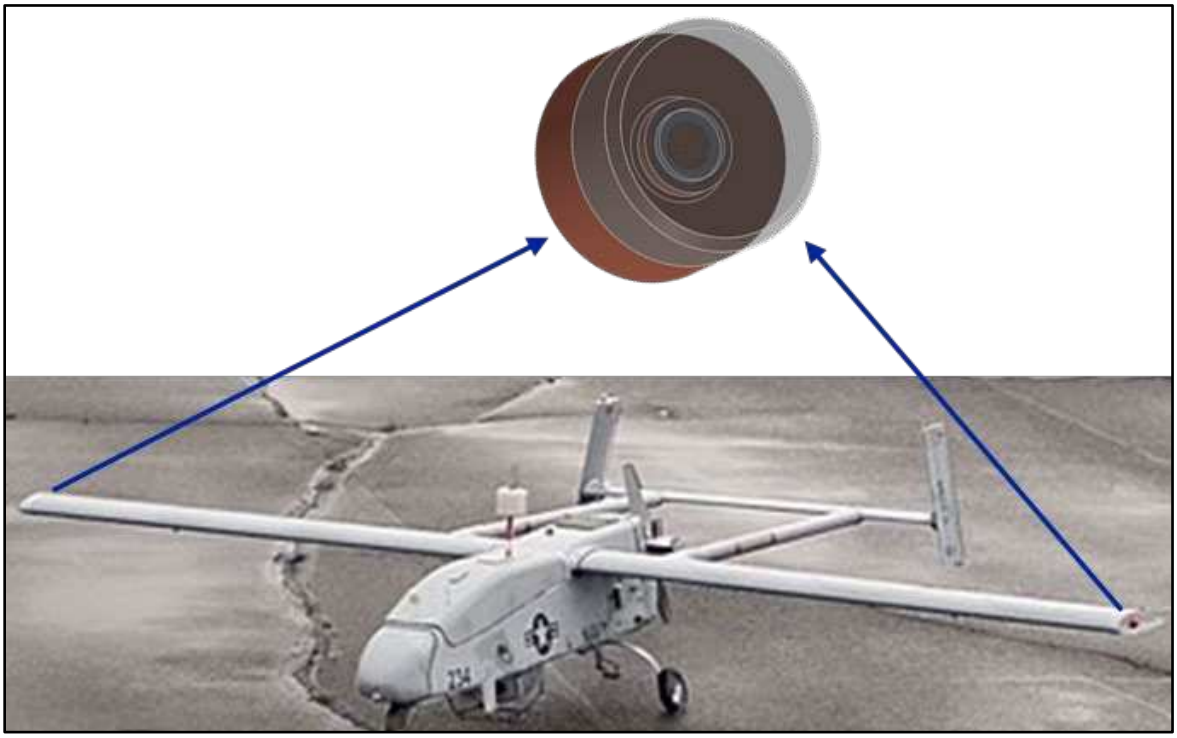


Figure 3.2. Example of Pen-Cap Air Antenna Placement for Total Coverage

The second antenna design option, that resulted from the output of the trade study, was the Bunker antenna. It is wideband by design providing 4π steradian coverage, capable of supporting frequencies extending from Ku-band to Ka-band (10 – 30 GHz). Six prototype units were built, fabricated, and tested in an anechoic chamber to characterize the performance. The antennas technical descriptions will be discussed in depth in the following sections.

3.3.1 Pen-Cap Air Antenna Geometry, Analysis and Measured Results

The Pen-Cap air antenna is designed to support small platforms for low data rate, air communications. The extremely small antenna, 0.8" x 0.58 ", and low weight of 10 grams makes this a very practical and feasible solution. Figure 3.3 shows the Pen-Cap air antenna with a radome,

it has a metal base to connect to an mmW capable radio back-end via a coaxial connector. It was designed specifically such that the ground plane behind the antenna was shaped to improve the front-to-back ratio whereby improving the signal strength transmitted in the forward direction to maximize expected range goals.

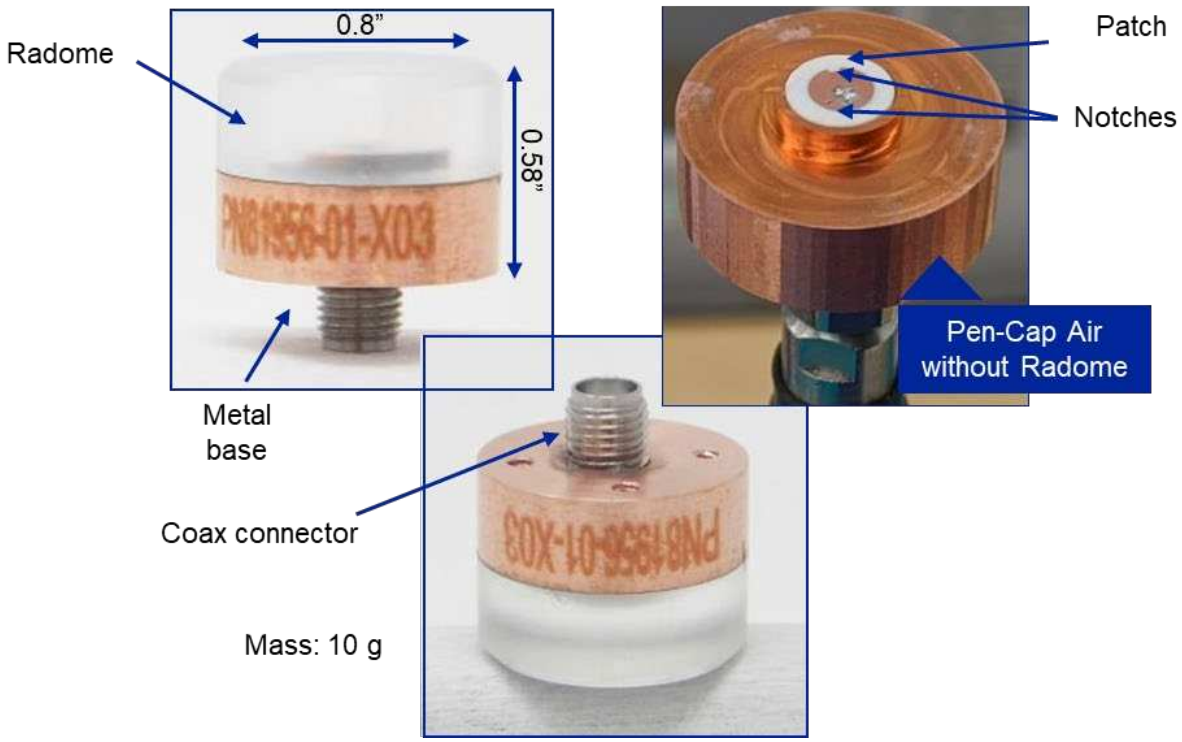


Figure 3.3. Pen-Cap Air Antenna Geometry

Modelling and simulation was performed to characterize the expected performance of the Pen-Cap air antenna configuration (shown in Figure 3.4) and design. Here, the minimal realized gain is shown across K-band frequencies to be approximately -4.0 dB; this accounts for mismatch, material and connector losses as presented in Figure 3.5. The broadside axial ratio is reasonably degraded away from the main beam at about 3 dB as depicted in Figure 3.6.

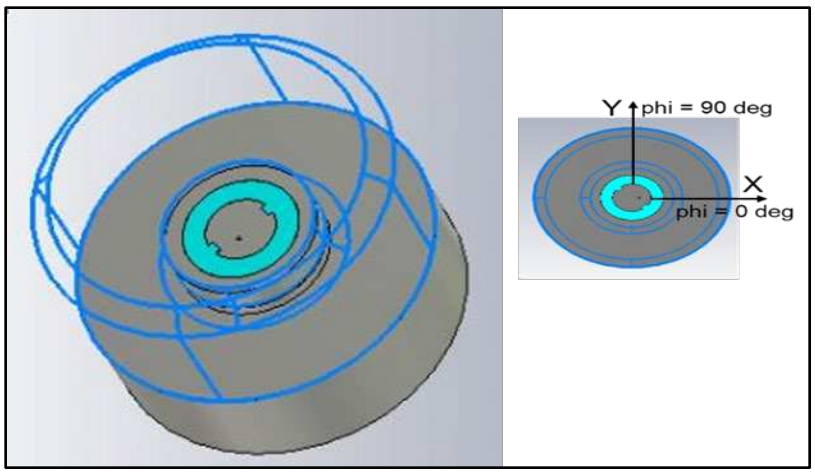


Figure 3.4. Pen-Cap Air Antenna Configuration

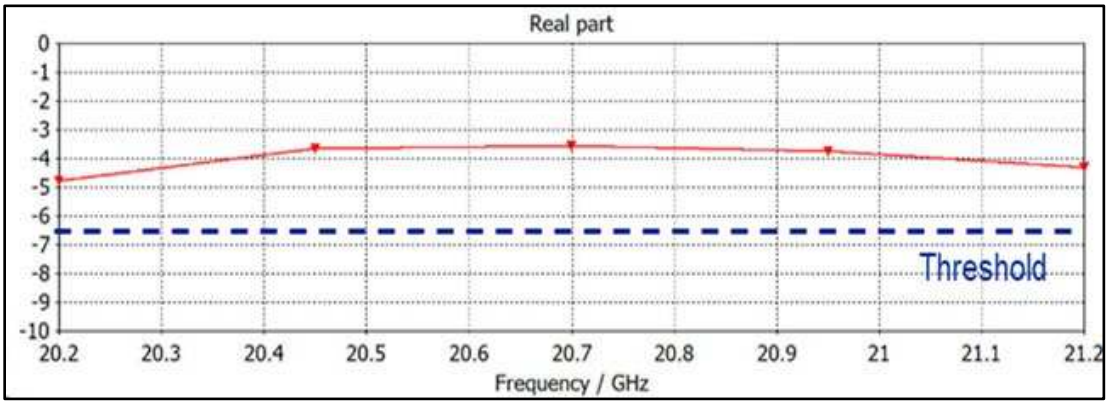


Figure 3.5. Pen-Cap Air Minimum Realized Gain (RHCP) in 2π dBic

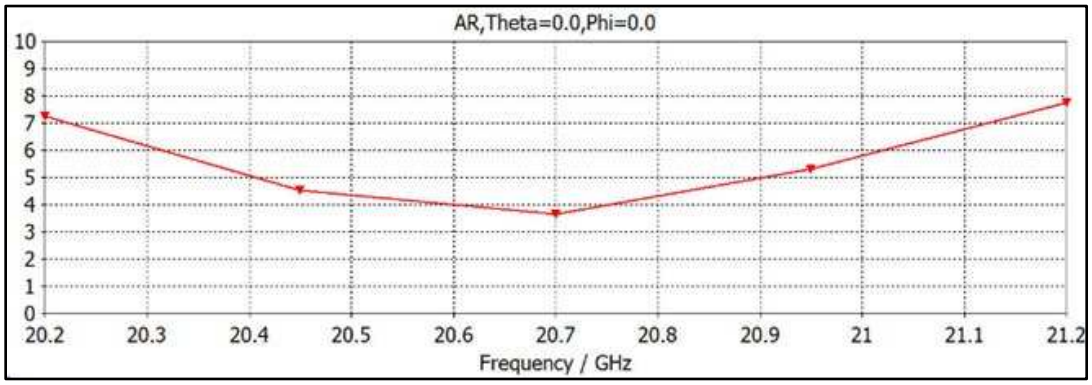


Figure 3.6. Pen-Cap Air Antenna Broadside Axial Ratio

Next, as with any good systems engineering practices, after fabrication and manufacturing of the Pen-Cap air antenna, we sought to verify its performance through rigorous anechoic chamber testing. Measured results for each prototype developed were obtained and compared to the numerical analysis for the measured gain and return loss. In all cases, the measured results were

highly correlated with the computed results showing that a detailed design process indeed works well, test methods and results were repeatable, and the performance goals were met initiated with experienced modelling and simulation.

Figure 3.7. Pen-Cap Air Antenna in Anechoic Chamber Setup

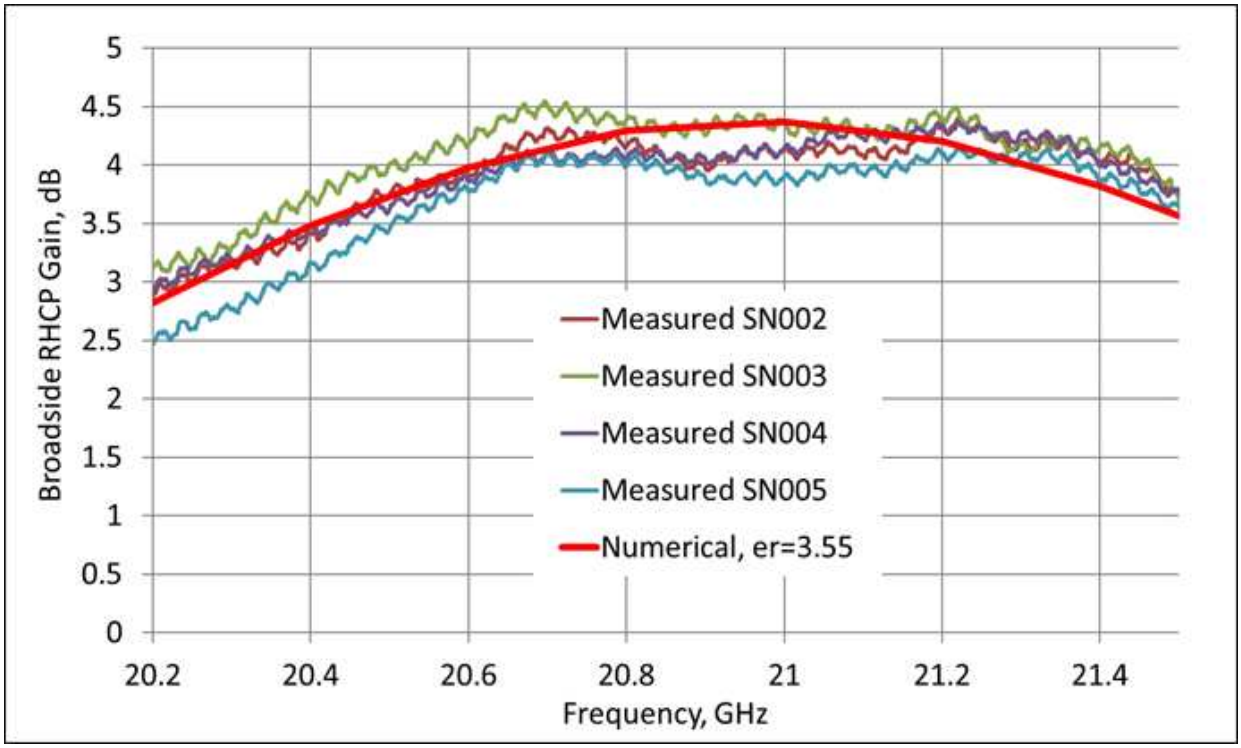


Figure 3.8. Pen-Cap Air Antenna Measured Gain vs. Numerical Data

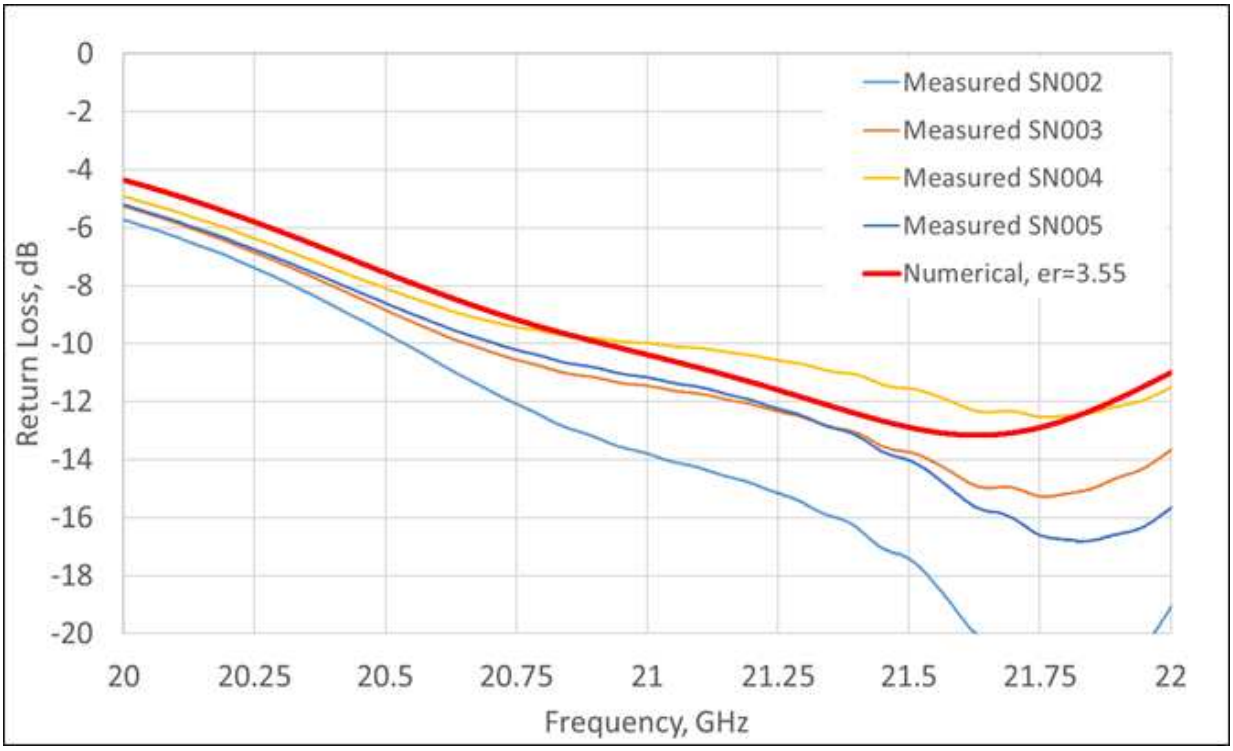


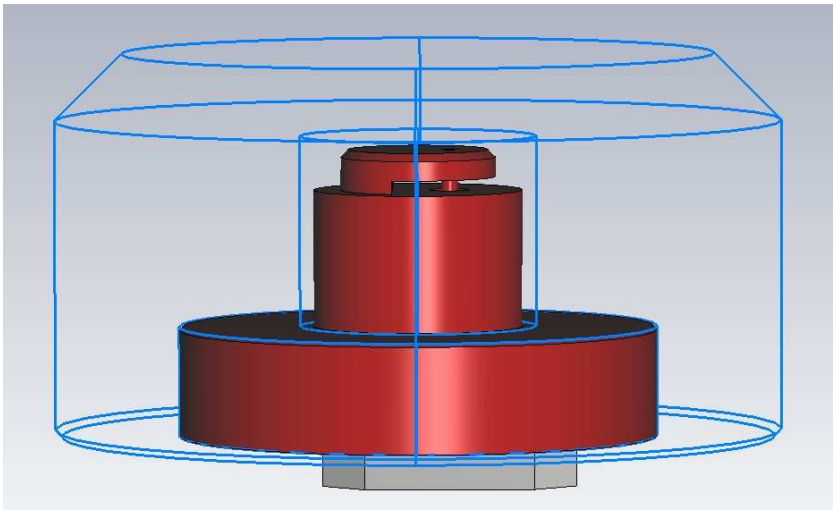
Figure 3.9. Pen-Cap Air Antenna Measured Return Loss vs. Numerical Data

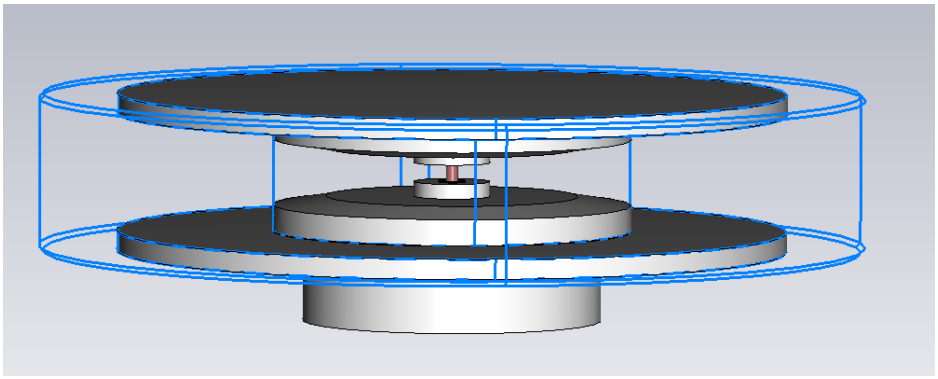
3.3.2 Bunker Antenna Geometry Options, Analysis and Measured Results

An isotropic antenna with no cross-polarization is used only as a theoretical reference to compare the directional gain of any antenna. In practice, an isotropic coverage over 4π steradians is not realizable as the antenna patterns are affected by the mounting structure, feeding assembly and scattering effects of the finite antenna structure. A number of low gain wide coverage antennas are described in [42][43] for satellite applications providing either earth coverage of +/- 9^0 when the satellite is in-orbit or providing a toroidal coverage with peak at 90^0 with +/- 20^0 coverage around the peak when the satellite is in the transfer orbit providing telemetry and tracking communications to the ground. The isotropic performance is severely impacted by the mounting structure such as S/C and scattering from other support structure and antennas [44]. One way to achieve nearly uniform coverage of a full sphere is to employ a number of switchable quasi-directional antennas pointing in different directions [45]. None of the existing antennas cover the

entire sphere but switching them on and off allows a full coverage pattern to be realized. This approach has drawbacks of increased losses due to switching network, and increased complexity, mass, and cost. Quasi-isotropic antennas provide uniform power coverage without the control of polarization [46]. Generally, these antennas are made of two orthogonal electric and/or magnetic dipoles. The nulls in the patterns of each dipole are filled by the second dipole with proper amplitude and phase excitation. Examples include two electric dipoles, where proper phasing is achieved by adjusting the length difference of the dipoles [47], four L-shaped monopoles with 90^0 phase progressions provided by a built-in feed network [48], equivalent electric and magnetic dipoles are excited in dielectric resonator antenna [49], U-shape patch [50], and circular sector cavity [51]. In a majority of the above cases, quasi-isotropic antennas are a quarter wavelength or smaller, and thus they become less than the size of a coaxial connector at frequencies higher than X-band leading to high sensitivity of radiation patterns to mounting platforms, handles, and connectors itself. In this case, having a null in the direction of the platform is beneficial. Unlike quasi-isotropic antennas, omni-directional antennas with toroidal patterns radiate perpendicularly to their axes with doughnut-shaped patterns having two nulls, where one of them can be directed in the direction of the platform. The nulls are typically wide and significantly affect the antenna coverage. A compact antenna using a cavity-backed annular slot operating at L-band is discussed in [52]. This antenna has a narrow bandwidth of 5% and provides less than 2π steradians coverage. A bi-conical antenna (BCA) with narrow elevation coverage is described in [53] A low-profile dual-polarized wideband omni-directional antenna was proposed [54] with artificial magnetic conductor (AMC) reflector supporting LTE band (1.7-2.7 GHz). The antenna structure consists of a horizontally polarized circular loop antenna, a vertically polarized monopole antenna and an AMC reflector. This antenna is too directive with limited coverage. Gronich [55] suggested a

[56]. Parasitic elements are used here to get the wide bandwidth, but the antenna has drawbacks of larger area, increased complexity, and limited coverage. The prior-art literature shows lack of full coverage omni-directional antennas that are needed for future protected communications used for soldiers' manpack units.





(b)

Figure 3.10. Bunker Design Options (a) Bunker IFA Design Option and (b) Bunker BCA Design Option

This section presents two types of antennas as shown in Figure 3.10, both capable of providing K-band primary coverage and Ku-band and Ka-band secondary coverages using a single antenna. The first one employs an inverted-F antenna (IFA) providing a cardioidal pattern with beam peak perpendicular to antenna aperture providing a quasi-isotropic coverage (Figure 3.10a). The second antenna uses an all-metal BCA with better omni-directionality and provides a toroidal pattern with beam peak perpendicular to the surface of the antenna (Figure 3.10b). The omni-directional pattern allows for better polarization control, whereas nulls in the patterns are minimized to improve the coverage. By comparing the quasi-isotropic with omni-directional designs, it is shown that the omni-directional approach has better coverage, and hence, is selected for fabrication and test.

Key features of the Bunker antenna include: (a) it provides 4π steradians of coverage, (b) the antenna has a novel support mechanism using two fiberglass rods, a conduit, an RF cable inside, clip release mechanism to fold and unfold the antenna from lying down to standing up positions of the soldier and a 2.92 mm coaxial connector that interfaces with the ICS manpack radio, (c) it has a protective radome and a small metallic ground-plane, and (d) it is compact and lightweight for soldiers to carry easily in the battlefield [57]. Measured results of the IFA and BCA prototype Bunker antennas are presented and compared with analytical simulations. Additionally, the mechanical deployment of the antenna between the two configurations is demonstrated where the impact of the mechanical support on antenna performance is included.

3.3.2.1 Antenna Requirements

The Bunker antenna carried by the soldier for radio communication with aircraft, headquarters, and other ground sites within a theater area shall meet the following key primary requirements:

- Frequency range: 20.2 GHz to 21.5 GHz

- Polarization: RHCP
- Coverage: 4π steradians
- Antenna gain: > -6.5 dBic (90% of coverage) and > -9.2 dBic (95% of coverage)
- Return loss: > 10 dB
- Stowage and deployment: 12” when soldier lying on the ground to 24” when soldier is standing
- Mass: < 300 grams without support structure and cable
- Size: 2.5” dia. x 2.0” long (without support rod)
- Protection: Radome cover for field operation

In addition to the above requirements, the Bunker antenna cost must be substantially low due to thousands of quantities needed for future manpack radio applications. The secondary requirements include capability to support Ku-band and Ka-band frequencies in the future where one antenna could replace three uniquely different antennas for manpack radio communications.

3.3.2.2 Bunker Antenna Design Approach

Design optimization and RF analysis of the Bunker antenna are performed using CST Microwave Studio, which is a 3D full wave tool capable of efficient modeling of complex electromagnetic (EM) antenna geometries. The frequency domain solver used is based on the Finite Element Method (FEM). It automatically refines the mesh in the required areas, thus significantly improving the accuracy with a moderate increase in memory and time requirements. The numerical approach is validated by means of measurements.

Antenna patterns were optimized by means of the CST's CMA (Covariance Matrix Adaptation) Evolution Strategy optimizer. Depending on settings, the optimizer can behave as local or global method. For the Bunker antenna design, the optimizer is set as global. The cost function consisted of an impedance goal and a coverage goal. The coverage goal compares the computed minimal directivity within field-of-view over a given frequency range with the threshold required directivity value. The reported percentage coverage is relative to full 4π steradians and is evaluated for a given gain value using the following equations:

$$\%\ Coverage = \frac{100}{4\pi}\int_0^{2\pi} d\varphi \int_0^{\pi} f(\theta,\ \varphi)\sin\theta\, d\theta \qquad (2.3.2.4.1)$$

where the function f (θ, φ) is given as

$$f(\theta,\ \varphi) = \begin{bmatrix} 1,\ G(\theta,\varphi) \geq G_{threshold} \\ 0,\ G(\theta,\varphi) < G_{threshold} \end{bmatrix} \qquad (2.3.2.4.2)$$

where, $G(\theta,\varphi)$ in eqn (2.3.2.4.2) is the antenna realized gain in the direction of (θ,φ) and $G_{threshold}$ is the gain threshold level.

The percentage coverage is evaluated for the required threshold gain values of -6.5 dBic and -9.2 dBic. Considering a 1.3 dB cable loss and 0.1 dB loss due to mismatch and material losses, the resulting directivity thresholds are -5.1 dBic for 90% coverage and -7.8 dBic for 95% coverage. To account for the polarization mismatch loss, far field is evaluated in terms of circularly polarized components, and thresholds are applied directly to RHCP component. Angular resolution of 1^0 is used in both azimuth and elevation to get sufficient samples for % coverage evaluation. This design methodology and analyses resulted in successfully developing Bunker antenna hardware that met all the requirements.

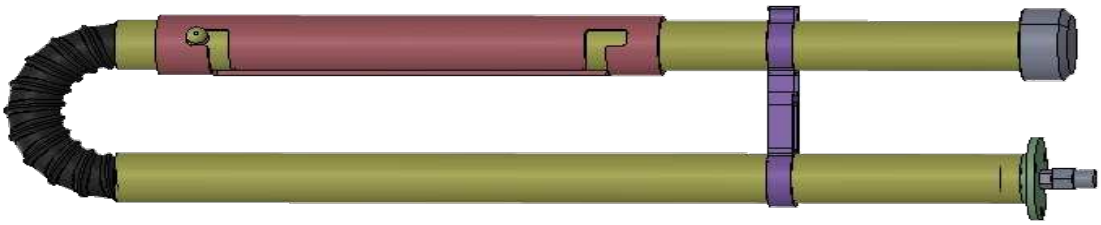
3.3.2.3 Fabrication and Reconfiguration Approach

The reconfigurable mechanical assembly (RMA) is the key component apart from the antenna that provides deployment and stowage functions when the soldier is standing and when

the soldier is lying on the ground in the battlefield respectively. The RMA is common to both types of antenna configurations and hence described upfront. The stowed and deployed configurations of the antenna with RMA are shown in Figure 3.11. In the stowed configuration the antenna is far from the soldier's head and is close to the waist to minimize the radiation intensity for the safety of the soldier while simultaneously maximizing the field of view of the antenna itself. The antenna is above the head by more than 6" to minimize the radiation intensity. Details of the RMA are shown in Figure 3.12.

In addition to meeting functional requirements, the design, choice of material, and manufacturing methods are carefully chosen to maximize use of commercial-off-the-shelf (COTS) items to minimize costs. The following components, as seen in Figure 3.12, are readily available as COTS from several suppliers: the 2.9 mm flexible coaxial cable; the 3/4" diameter fiberglass support rods A and B; the 3/8" diameter plastic flexible conduit; and the 1" diameter PTFE sleeve.

The stops and stowing clip are 3-D printed out of ABS plastic and are glued to their respective support rods. The base flange is machined from aluminum and is attached to support rod A using metal pins. The antenna aperture is machined from copper and is fed by a coaxial center conductor that is electrically connected to the copper section by soldering. A machined Rexolite radome is glued to the antenna aperture. The radome/antenna aperture assembly and flexible conduit are attached to support rod B using metal pins. Figure 3.13 shows the fabricated parts of the RMA. As can be seen, the Bunker antennas not only uses several COTS items, but are also easy to manufacture and assemble. They are lightweight and compact and require low to no maintenance by design.



(a)

(b)

(c)

(d)

Figure 3.11. Bunker Antenna Integrated with the RMA. (a) Stowed Configuration, (b) Soldier Carrying K-Band Antenna Lying Down, (c) Deployed Configuration, and (d) Soldier Carrying K-Band Antenna while Standing.

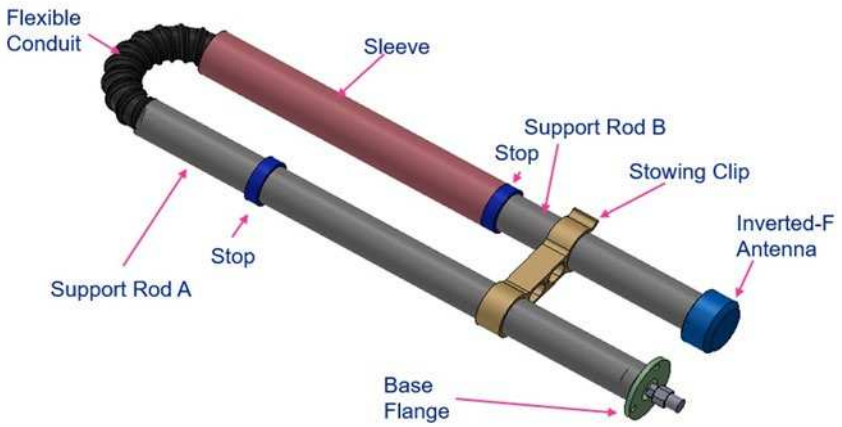


Figure 3.12. Details of the RMA and its Components

Figure 3.13. RMA Prototype showing Deployed (Top) and Stowed (Bottom) Configuration

3.3.2.4 Inverted-F Antenna

The IFA is optimized for maximizing the antenna coverage in terms of total field and then evaluated with RHCP component of the field. Total field is a combination of co-polarized and cross-polarized field components, and thus the antenna is not designed to distinguish different senses of polarization, but solely to minimize the directivity variation across full sphere. The antenna is expected to behave well in statistical sense in multipath environment when polarization and direction of an incident signal are unknown.

The IFA consists of two parts, a radiating antenna element and the RMA. The radiating segment comprises an IFA fed with a single feed point, a shaped ground plane, a rexolite radome, and a 2.92 mm coaxial connector. The RMA consists of a coaxial cable, support rods and a conduit for deployment and stowage of the antenna. Figure 3.14 shows the geometry of the IFA that includes a metallic base, a rexolite radome with relative permittivity of 2.53, an airgap between the top of IFA, and the radome for improving the impedance match, a shaped ground plane for widening the coverage, and a 2.92 mm coaxial connector interface. Details of the RMA are presented in the previous section. The simulated return loss of the IFA including the RMA support structure is plotted in Figure 3.15. Return loss is better than 19 dB over the desired band of 20.2 GHz to 21.5 GHz. The 10 dB return loss bandwidth is 35% and is over 16.6 GHz to 23.7 GHz.

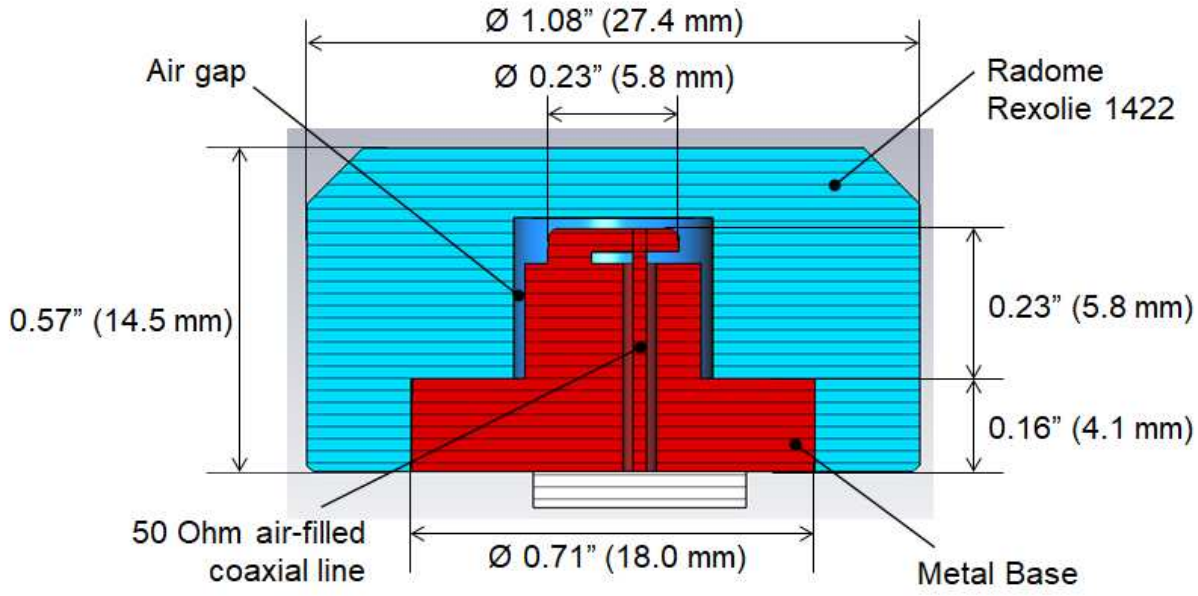


Figure 3.14. Inverted-F Antenna Geometry

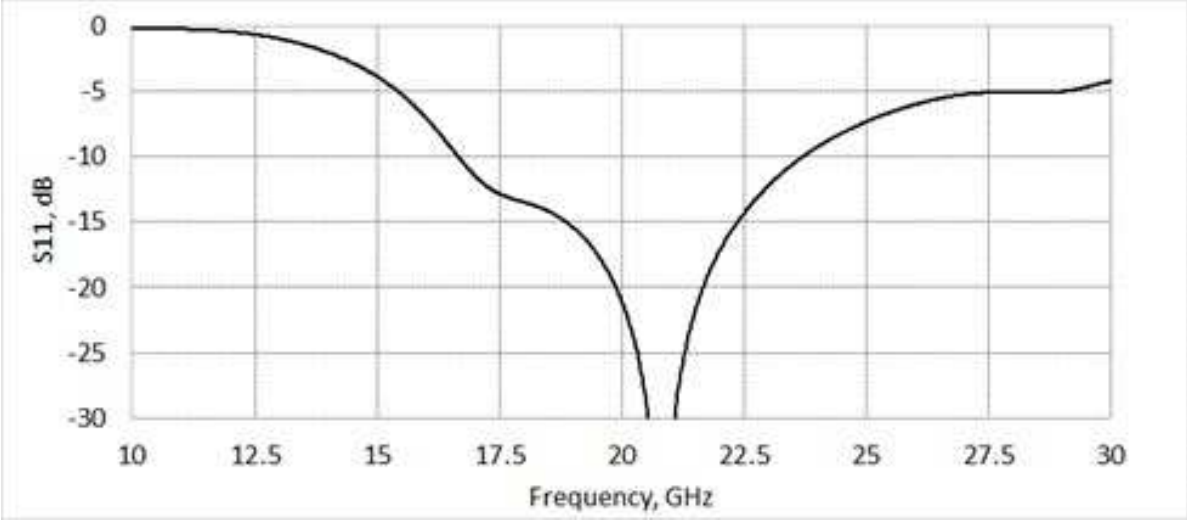


Figure 3.15. Computed Return Loss of the IFA over 10 – 30 GHz

Table 3.1. Calculated Minimal Percentage Coverage of IFA without Support Structure. Threshold is either applied to Total or RHCP Field.

	Total Field		RHCP	
Threshold / Frequency	-7.8 dBic	-5.1 dBic	-7.8 dBic	-5.1 dBic
20.2 GHz	100 %	100 %	86.0 %	72.5 %
20.4 GHz	100 %	100 %	86.2 %	72.6 %
20.6 GHz	100 %	100 %	86.2 %	72.5 %
20.8 GHz	100 %	100 %	86.1 %	72.1 %
21.0 GHz	100 %	100 %	86.1 %	71.4 %
21.2 GHz	100 %	100 %	85.9 %	70.9 %
21.4 GHz	100 %	100 %	85.7 %	70.2 %
21.5 GHz	100 %	100 %	85.6 %	70.0 %

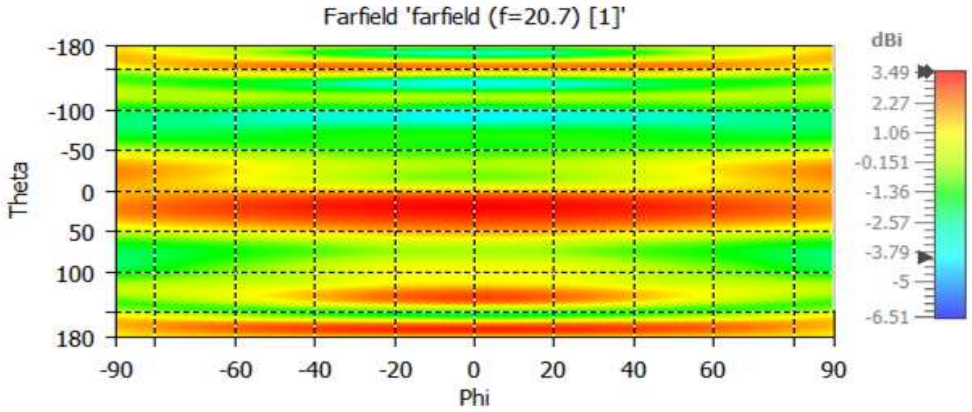
2D projection of the computed total field directivity along with elevation cuts of the IFA are shown in Figure 3.16. They are computed without the mechanical support structure RMA. The projection at mid-band shows close to quasi-isotropic radiation with directivity variation of 6.3 dBi (Figure 3.16a). Note that the antenna diameter is about 2 wavelengths, which is significantly

larger than majority of published quasi-isotropic antenna designs. Directivity variation can be seen clearer in elevation θ angle cuts in both XZ and YZ planes (Figure 3.16b & Figure 3.16c).

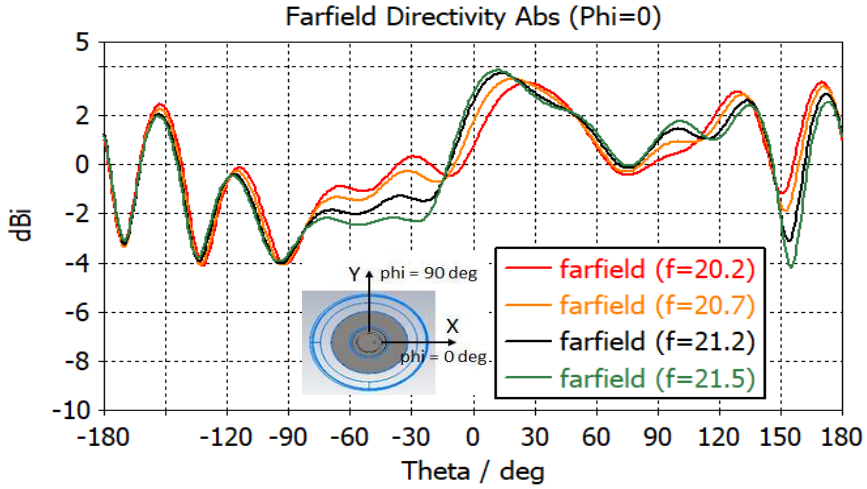
The percentage coverages for two gain threshold values of -7.8 dBic and -5.1 dBic are shown in Table 3.1. Support structure is not accounted in the estimations. As seen, when threshold is applied to total field, the coverage is 100 % by design. Coupling to RHCP has lower coverage mainly since IFA radiates both theta and phi far field components, resulting in high axial ratio at some angles.

The impact of the support structure RMA on the radiation patterns of the IFA is analyzed using a 10" PTFE rod with cable inside and is shown in Figure 3.17. The gain variation in the backlobe region is large as could be expected due to the quasi-isotropic shape of the radiation. However, the impact of the support structure on coverage is minimal (Table 3.2).

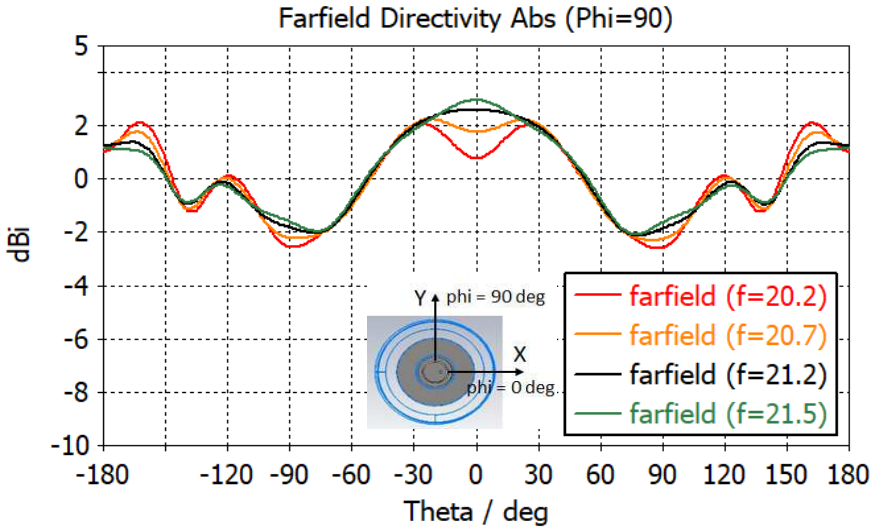
Even though this antenna has perfect coverage in terms of total field, coverage requirements for RHCP are not fulfilled. An omni-directional antenna is designed in the next section for better coverage.



(a)

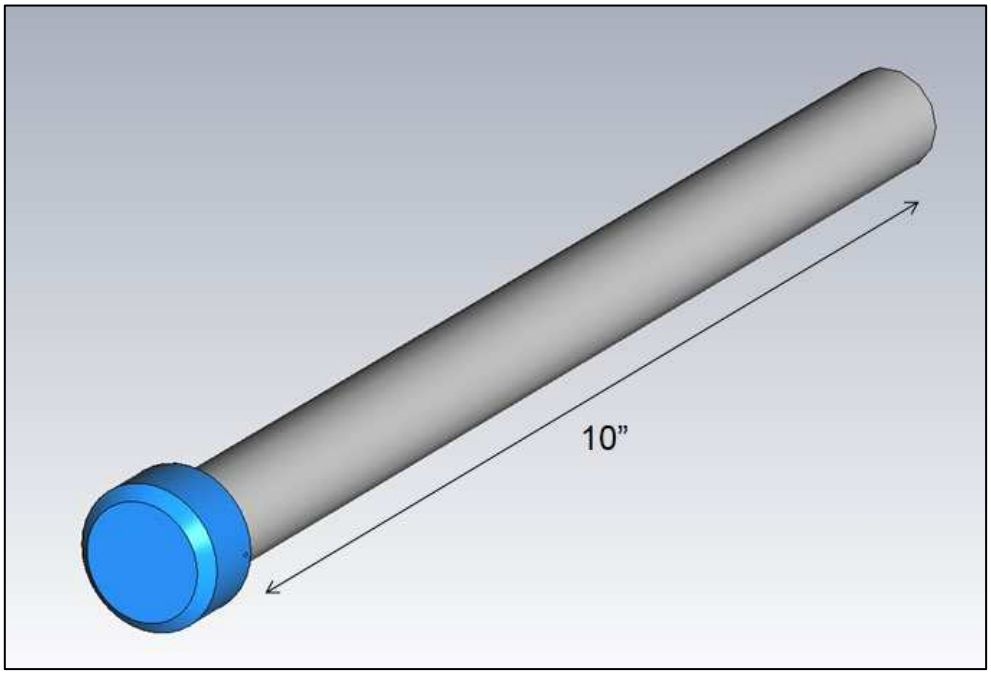


(b)

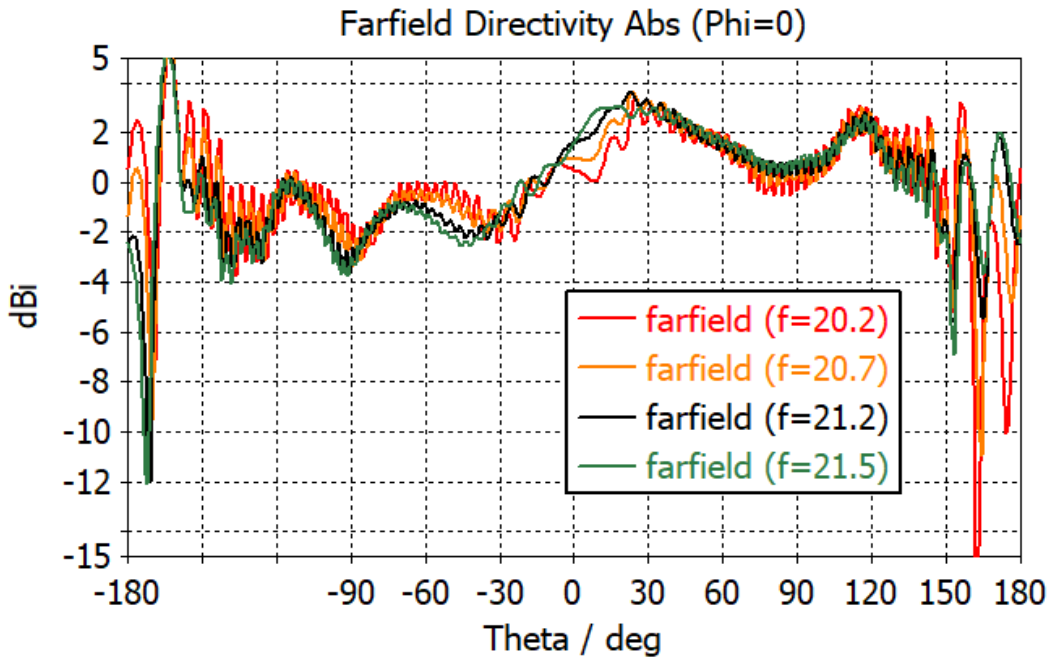


(c)

Figure 3.16. Computed Directivity of Total Field of Quasi-Isotropic IFA without Support Structure RMA. (a) Equirectanglular Projection at 20.7 GHz, (b) Computed Elevation Cuts in the Plane of the Pin Offset (phi=0 deg), and (c) Computed Elevation Cuts in the Plane Normal to the Pin Offset (phi=0 deg).



(a)



(b)

Figure 3.17. Computed Directivity of Total Field of Quasi-Isotropic IFA with 10” Support Structure RMA. (a) IFA with RMA Geometry and (b) Computed Elevation Cuts in the Plane of the Pin Offset (phi = 0 deg).

Table 3.2. Calculated Minimum Percentage Coverage of IFA with Support Structure Threshold is either applied to Total or RHCP Field.

	Total Field		RHCP	
Threshold / Frequency	-7.8 dBic	-5.1 dBic	-7.8 dBic	-5.1 dBic
20.2 GHz	99.8 %	99.5 %	89.0 %	72.1 %
20.4 GHz	99.7 %	99.5 %	89.2 %	71.3 %
20.6 GHz	99.7 %	99.4 %	88.1 %	71.0 %
20.8 GHz	99.7 %	99.4 %	89.0 %	71.1 %
21.0 GHz	99.8 %	99.5 %	88.3 %	70.3 %
21.2 GHz	99.8 %	99.4 %	87.8 %	70.4 %
21.4 GHz	99.8 %	99.4 %	88.2 %	70.1 %
21.5 GHz	99.8 %	99.5 %	87.8 %	69.8 %

3.3.2.5 Bi-Conical Antenna

BCAs are widely used in communication satellites to provide communication links when the satellite is in the transfer orbit with coverage of $+/-20^0$ around $\theta = 90^0$. For this application, the size and mass are reduced by using coaxial feeding (instead of conventional waveguide used for satellites). The design is modified to extend the coverage over 4π steradians mainly by making cone angle as 0^0 resulting in reduced radiating aperture size. The BCA provides a dip near the axis perpendicular to the bi-cone aperture over a small region but provides better backlobe performance. Besides, it is mainly theta-polarized, so that polarization loss is 3 dB at all angles. As a result, the percentage coverage will be better than that of IFA, and hence is the selected antenna configuration for the manpack radio. BCA consists of bi-conical antenna with copper conical structure, airgap, rexolite radome, fiberglass support structure, coaxial cable within the fiberglass rod support and a coaxial connector. The overall size of the antenna without the support structure RMA is 1.9” diameter and a length of 0.48” (Figure 3.18).

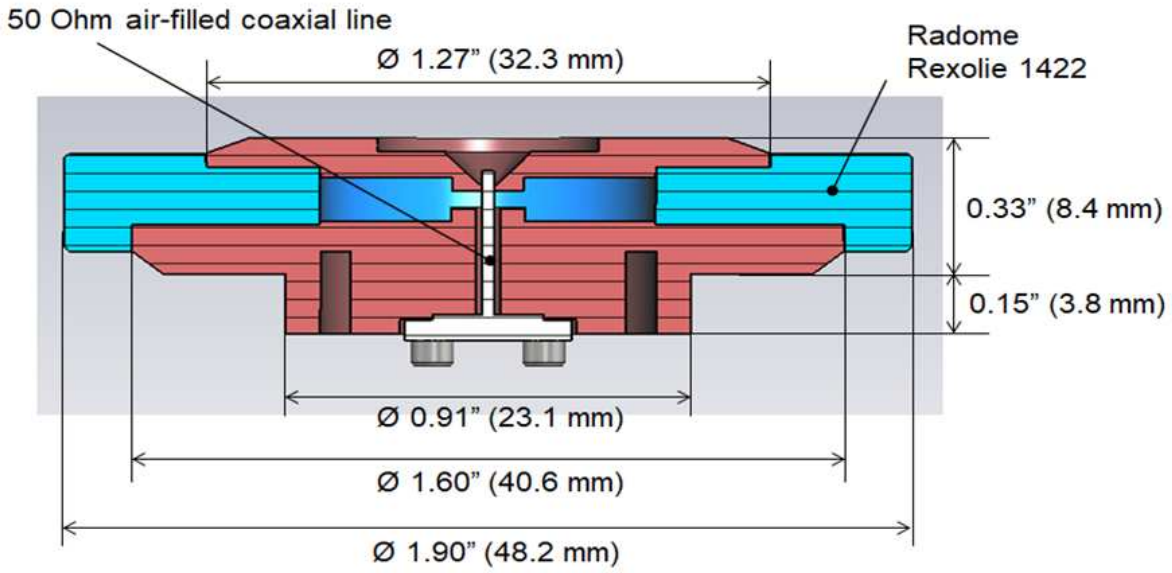


Figure 3.18. Geometry of Bi-Conical Antenna (BCA)

Table 3.3. Calculated Minimal Percentage Coverage of BCA without Support Structure Threshold is either applied to Total or RHCP Field.

	Total Field		RHCP	
Threshold / Frequency	-7.8 dBic	-5.1 dBic	-7.8 dBic	-5.1 dBic
20.2 GHz	99.9 %	99.8 %	99.8 %	92.4 %
20.4 GHz	99.9 %	99.8 %	99.8 %	92.5 %
20.6 GHz	99.9 %	99.8 %	99.8 %	92.6 %
20.8 GHz	99.9 %	99.8 %	99.8 %	92.2 %
21.0 GHz	99.8 %	99.8 %	99.8 %	92.4 %
21.2 GHz	99.9 %	99.8 %	99.8 %	92.5 %
21.4 GHz	99.9 %	99.8 %	99.7 %	92.5 %
21.5 GHz	99.9 %	99.8 %	99.7 %	92.3 %

Table 3.4. Calculated Minimal Percentage Coverage of BCA with Support Structure Threshold is either applied to Total or RHCP Field.

	Total Field		RHCP	
Threshold / Frequency	-7.8 dBic	-5.1 dBic	-7.8 dBic	-5.1 dBic
20.2 GHz	99.3 %	98.9 %	98.8 %	95.0 %
20.4 GHz	99.2 %	98.8 %	98.8 %	93.4 %
20.6 GHz	99.6 %	98.7 %	98.7 %	94.9 %
20.8 GHz	99.6 %	98.8 %	98.8 %	95.2 %
21.0 GHz	99.4 %	98.7 %	98.4 %	94.0 %
21.2 GHz	99.8 %	98.9 %	98.7 %	93.9 %
21.4 GHz	98.1 %	98.1 %	97.8 %	91.3 %
21.5 GHz	99.7 %	97.5 %	97.4 %	90.6 %

Calculated percentage coverage for BCA without and with supporting structure are shown in Table 3.3 and Table 3.4 respectively. Relative permittivity of the handle is 5. The antenna satisfies the coverage requirements for RHCP component in both cases.

Six prototype units of the BCA have been fabricated along with their RMAs. The fabricated BCA along with the protective radome and RMA is shown in Figure 3.19. The antenna without RMA is very compact and is 1.9” (48.33 mm) diameter and 0.48” (12.3 mm) long with low mass of 66 grams. Measured return loss of the 6 units along with computed results are shown in Figure 3.20. The return loss is better than 19 dB over the desired K-band frequencies. It shows wide bandwidth of 12.5 GHz to 29 GHz with return loss better than 10 dB over 80% bandwidth. The wideband capability of the BCA allows the unit to support multiple missions at Ku, K and Ka-bands thereby reducing the number of antennas carried by the soldier.

Figure 3.19. Prototype Unit of the BCA with a Protective Radome and the RMA

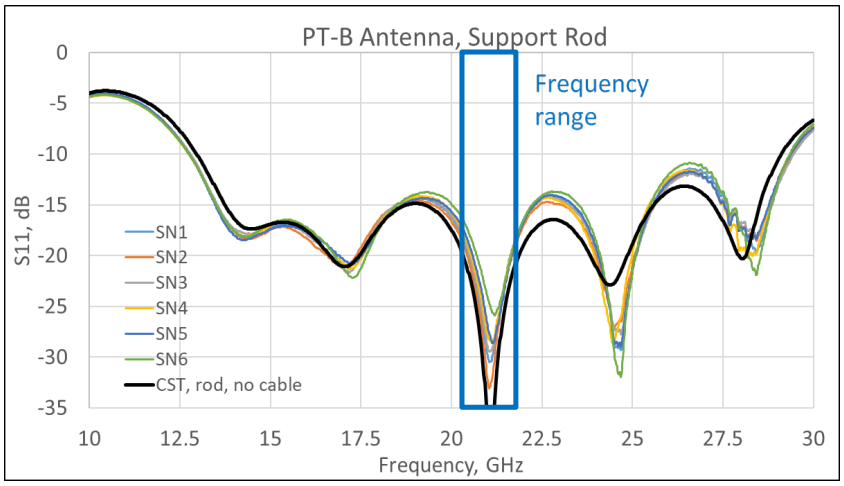


Figure 3.20. Measured Return Loss of 6 BCA Prototypes with RMA and Simulated Results

The radiation pattern measurement of the BCA is not an easy task. This is since the antenna has low gain, full 4π steradians coverage and the back lobe pattern measurements need special attention due to the support structure. They have been measured in an anechoic chamber and the set-ups for forward radiation and backward radiation are shown in Figure 3.21. It is to be noted that special care has been taken for the backward radiation set-up where non-metallic support structure (made of wood) is used to support the BCA causing reduced scattering effects and an absorber material covering the positioner. Measured forward radiation patterns in the forward direction (θ from -90^0 to $+90^0$) are shown in Figure 3.22 - Figure 3.24 for the six units along with computed patterns shown in dark red at three different frequencies covering the K-band. The radiation patterns of the six units track well and match closely with the simulated patterns.

Measured radiation patterns in the backward hemisphere have been measured with the test set-up shown in Figure 3.21 where care is taken to support the BCA with non-metallic wooden support structure so that the antenna remains stationary while the positioner is moving. Also, absorber material is placed behind the BCA to shield the scattering from the positioner. Radiation patterns measurements are shown in Figure 3.25 - Figure 3.27 show measured backward radiation patterns at 20.2 GHz, 20.8 GHz and 21.5 GHz respectively and are compared with simulated patterns. A good agreement is obtained between measurements and simulations. The disagreement is mostly in the areas of deep nulls that got filled due to measurement uncertainties caused by low gain and scattering from the set-up as can be expected.

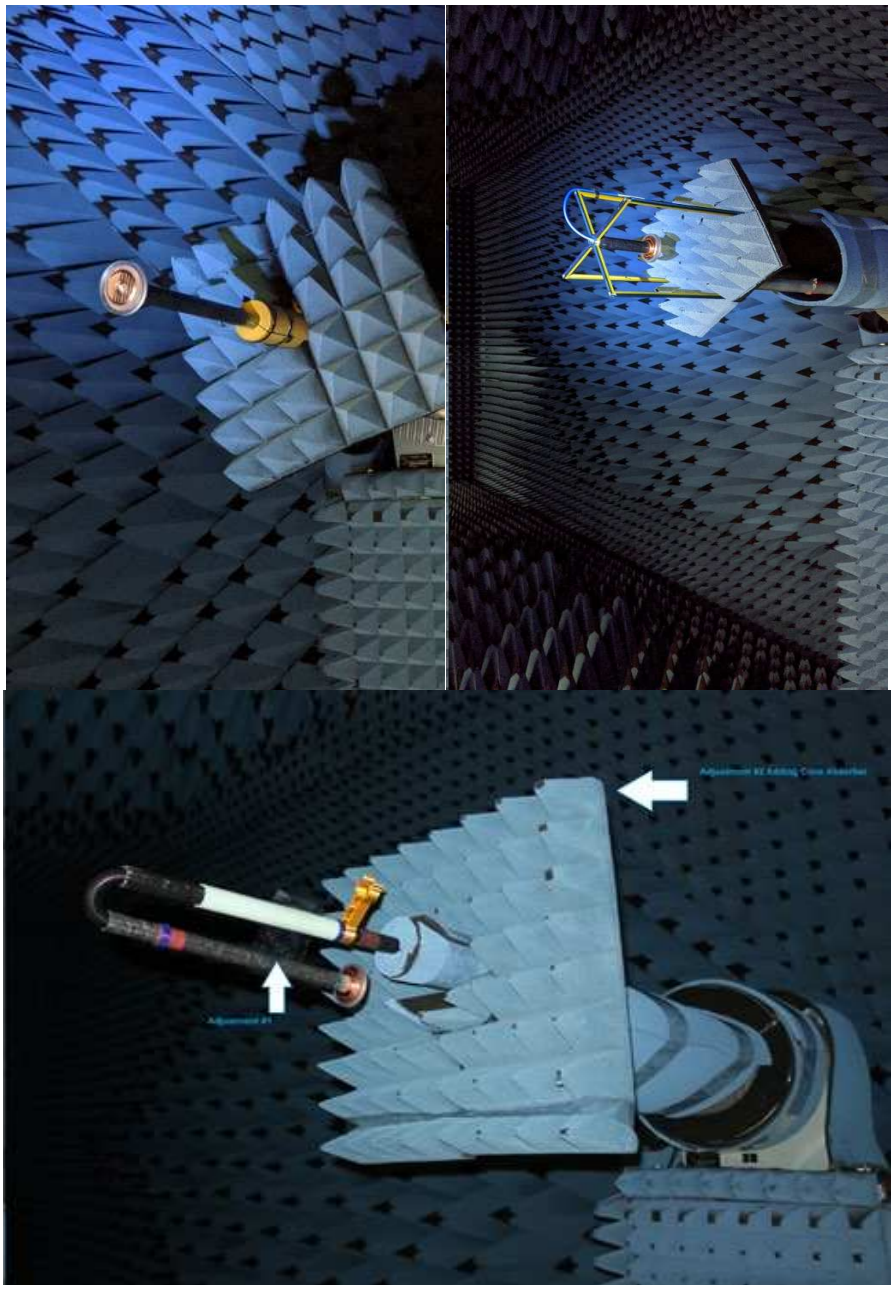


Figure 3.21. Anechoic Chamber Test Set-Up for Radiation Pattern Measurements of BCA in Deployed Configuration. (Top Left) Forward Radiation in Deployed State, (Top Right) Backward Radiation in Deployed State, and (Bottom) Stowed State.

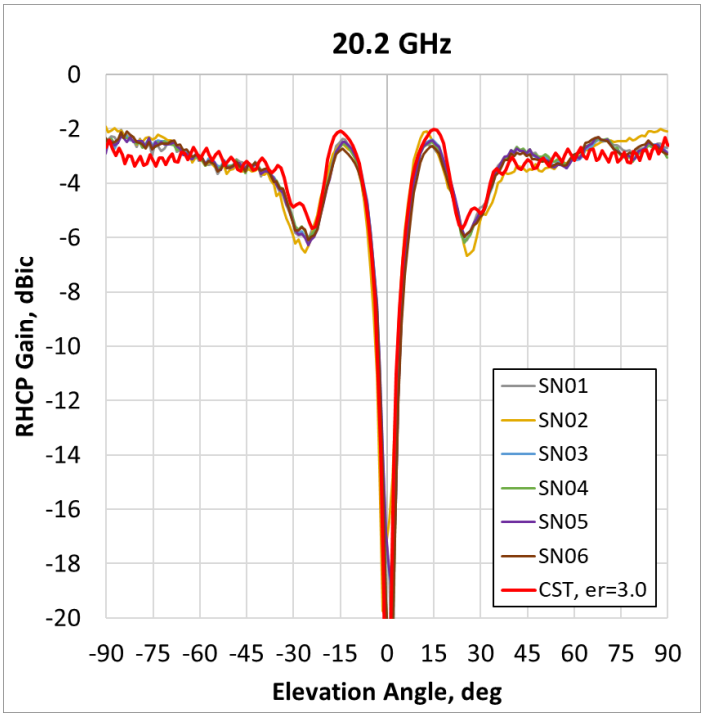


Figure 3.22. Measured Forward Radiation Patterns of 6 Prototype BCA Units at 20.2 GHz

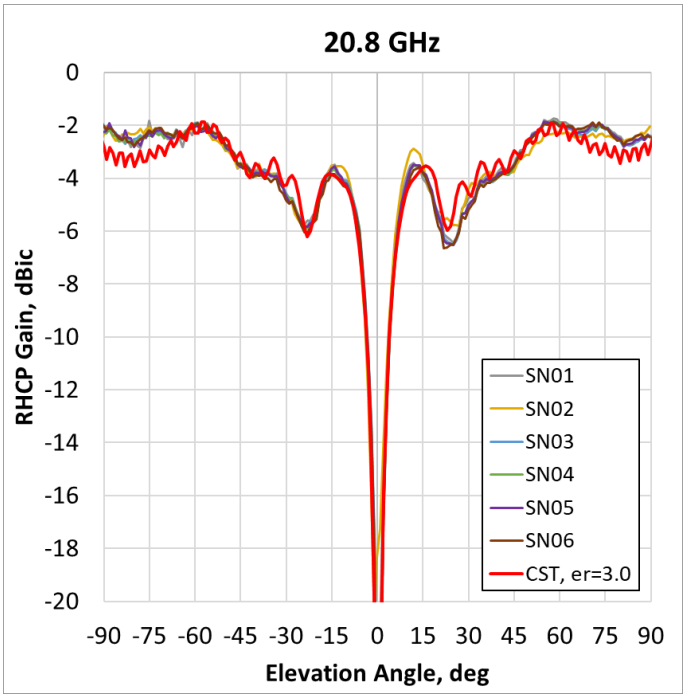


Figure 3.23. Measured Forward Radiation Patterns of 6 Prototype BCA Units at 20.8 GHz

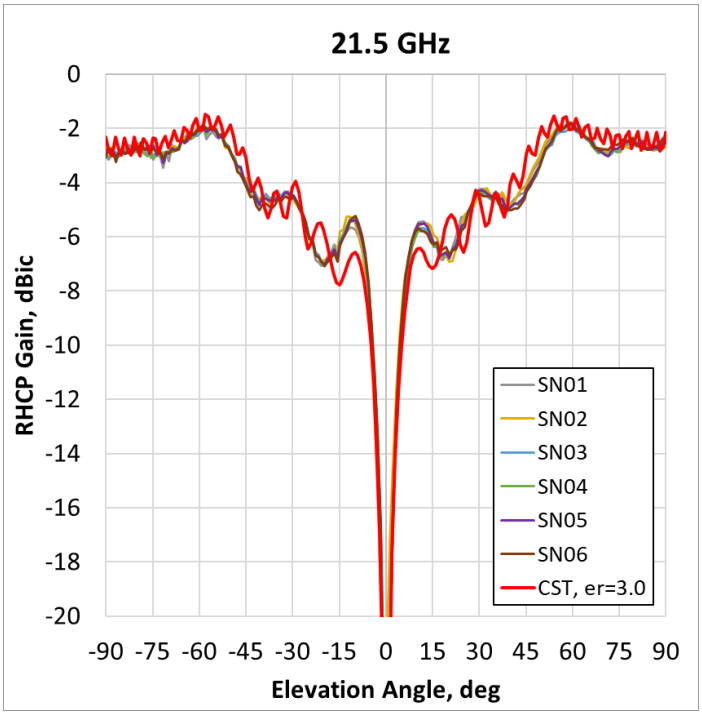


Figure 3.24. Measured Forward Radiation Patterns of 6 Prototype BCA Units at 21.5 GHz

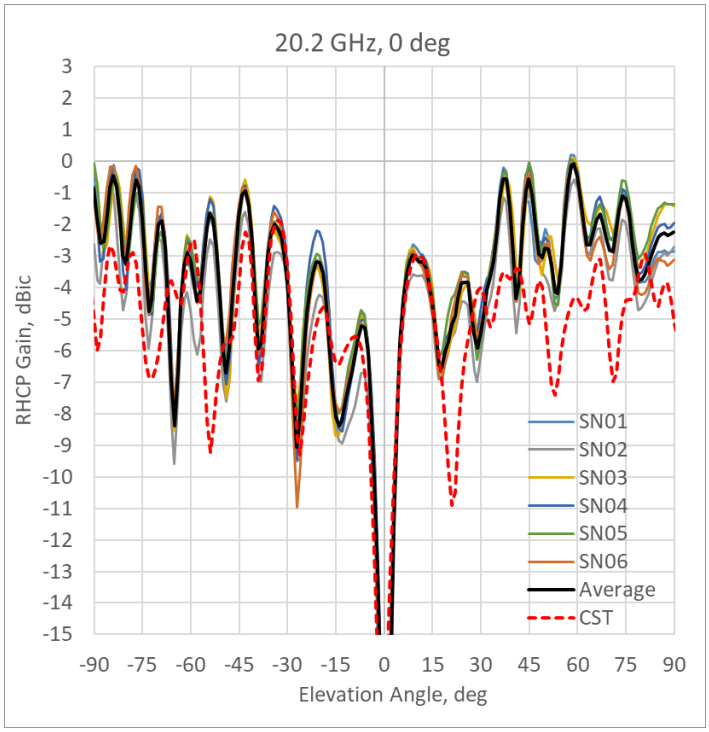


Figure 3.25. Measured Backward Radiation Patterns of 6 Prototype BCA Units at 20.2 GHz

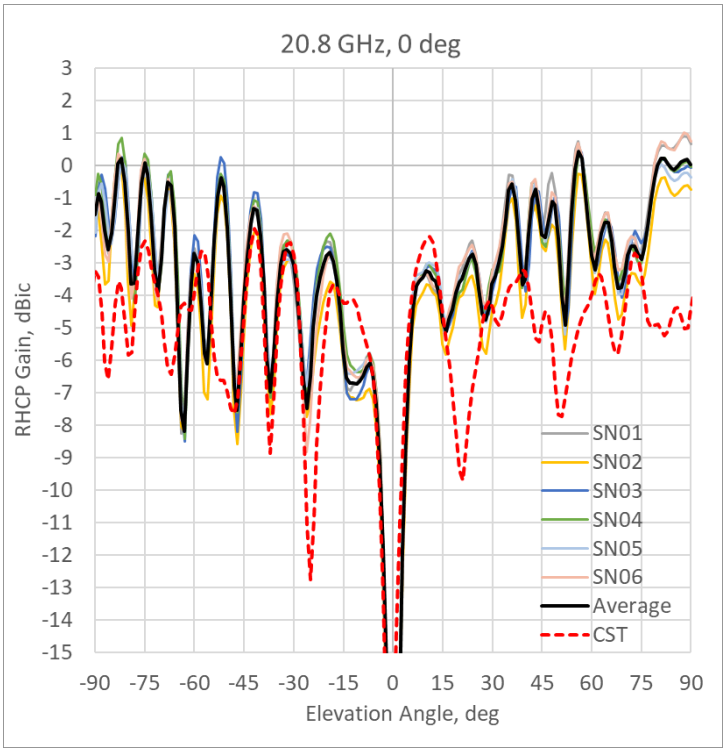


Figure 3.26. Measured Backward Radiation Patterns of 6 Prototype BCA Units at 20.8 GHz

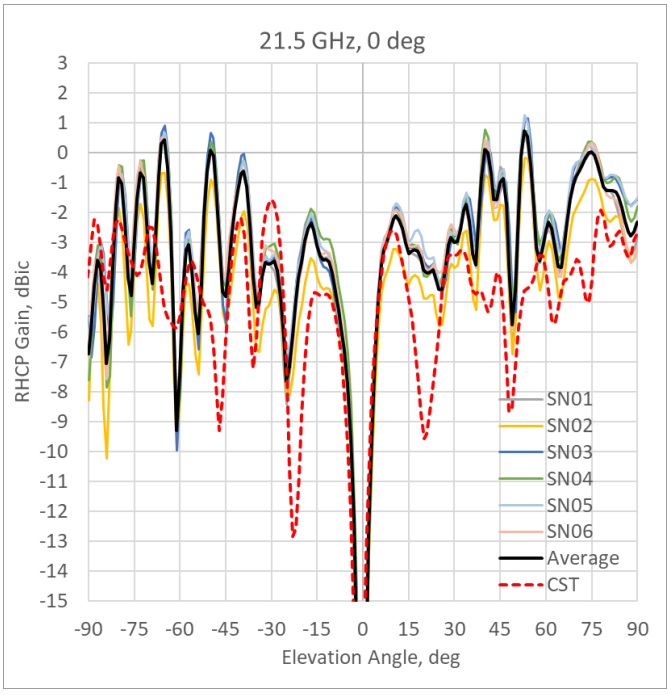


Figure 3.27. Measured Backward Radiation Patterns of 6 Prototype BCA Units at 21.5 GHz

Table 3.5. Compliance of BCA with the Requirements

Requirement	Required	Achieved
Impedance bandwidth, GHz	20.2~21.5	12.7~27.7
Performance bandwidth, GHz	20.2~21.5	20.2~21.5
Polarization	RHCP	Equivalent RHCP (*)
Coverage of 4π		
-6.5 dBic	90%	90.6%
-9.2 dBic	95%	97.4%
Weight (no handle, cable), g	300	66
Size, in	2.5” x 2.0”	1.9” x 0.5”
Protection	Radome	Radome

(*) Antenna is theta polarized; polarization mismatch is accounted in the coverage calculation.

The measured performance of the BCA is summarized in Table 3.5 and compared with the requirements of the K-band manpack antenna. The BCA meets all the requirements for each of the six antennas manufactured and the RF performance tracks well among the units in terms of measured return loss, gain and shape of the radiation patterns. The antennas have wide bandwidth covering K-band primarily as well as secondary Ku and Ka-bands. This allows a single tri-band BCA replacing three different antennas on the manpack radio thereby reducing mass, complexity, and cost for future protected communication systems. The development of a tri-band antenna is being considered currently. In addition to the manpack applications on the ground, the BCA and IFA are planned for use in current UAV and aircraft applications.

3.4 Millimeter-Wave Antenna Technologies Summary

In summary, we presented two antenna designs that would be of value and could support smaller platform communications and operational ground users in tactical situations.

Figure 3.28. Pen-Cap Air & Bunker Antenna Prototypes

The mmW antenna design options, where the preliminary antenna geometries, configurations, analyses, and measurements were described demonstrating that the designs would meet the system requirements. This chapter further detailed different antenna geometry options, IFA and BCA. In comparison, the BCA geometry has better gain performance over the coverage and can support K-band primary communications, but also supports secondary communications required at Ku and Ka-bands due to its wideband characteristics. These mmW antenna designs and prototypes will ultimately be used as enablers to support survivable communications in severely challenged environments for future operations and tactical missions.

Chapter 4. High-Band Antenna Designs for Communications at the Halt

This chapter will describe a novel antenna design that improves soldier communications while stationary to be used when soldiers are in remote, fixed locations and intend to transfer large amounts of data. The innovative and diverse reflector antenna design makes communications possible with future 5th generation aircraft and long range backhaul operational centers using a lightweight, highly capable reflector antenna that can operate across multiple frequency bands. This work was published in the peer-reviewed IEEE technical conference as noted in [4].

4.1 Portable, High-Band Antennas Background

An innovative, easy to deploy, ruggedized, lightweight Quad-Band Petal Reflector Antenna (QPRA) has been designed and developed to provide high-band, full duplex (FD) communications at Ku-band TX, Ku-band RX, K-band RX, and Ka-band TX operations. The QPRA design supports FD operation and RHCP for 14.4-14.83 GHz (Rx) and 15.15-15.35 GHz (TX) with 24.4 dBi directivity, and K/Ka-bands at 20.2- 21.2 GHz (RX) and 30-31 GHz (TX) with switchable RHCP and Left-Hand Circular Polarization (LHCP) with 35.8 dBi directivity at K-band and 37.2 dBi directivity at Ka-band. The QPRA can be integrated with a lightweight COTS gimbal and a small tripod to provide beam scanning of +/- 90^0 in elevation and 360^0 in azimuth. High-band communications options are essential for dexterity, diversity and tactfully gaining advantage in some geographic locations. Personnel on the ground require advanced antenna technologies, such as the novel QPRA, that can be integrated with emerging software defined radio communication devices to provide high capacity for CATH as shown in Figure 4.1. Currently, there are a great number of high bandwidth applications that the QPRA could be used with, to include distribution of data, video and commercial command and control (C2) or data

dissemination, or surrogate communications system should control towers be compromised, e.g., national disaster scenario.

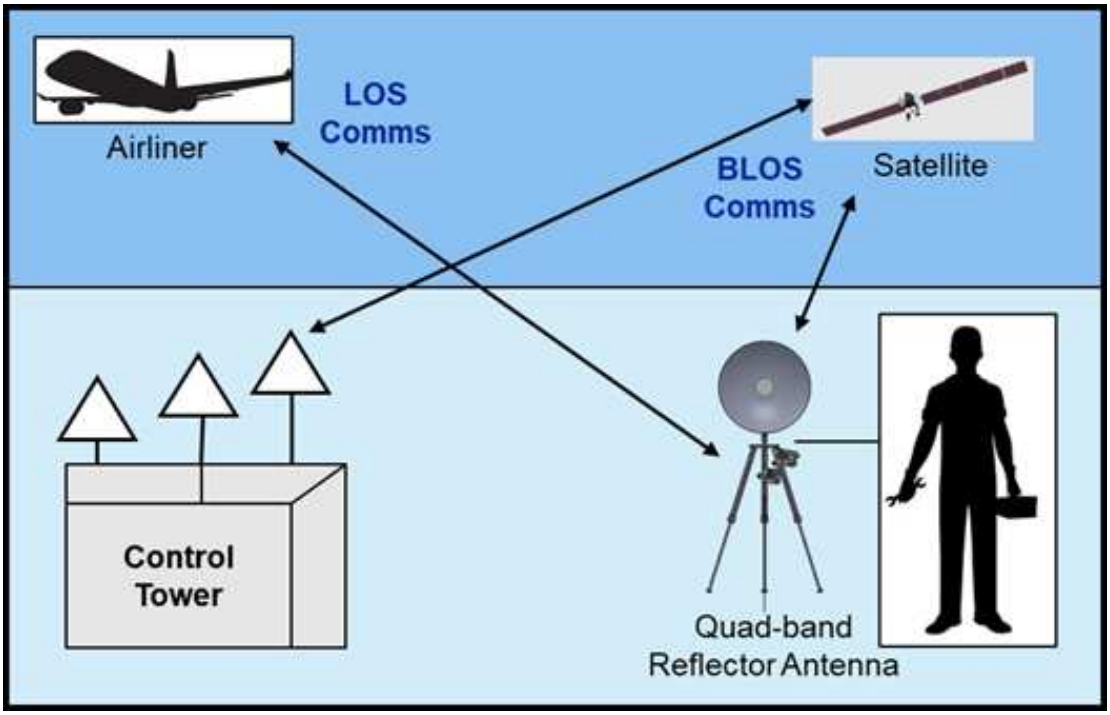


Figure 4.1. Diagram showing the Quad-Band Reflector Antenna Communications Capability

This chapter presents the technical description for a novel QPRA [58] that will function simultaneously at four discrete and independent frequency bands. This solution replaces commonly used phased array options with more than 5,000 combined elements and is an order of magnitude cheaper (approximately 30 times), and very lightweight. Fundamental key components that the QPRA is comprised of include its quad-band feed having more than an octave bandwidth, a sub-reflector supported by the feed cone, petal reflector where the main reflector consists of six petals that can be readily and easily assembled / dissembled for communications, a wide-band polarizer, two quadruplexes (one for each polarization) that separate the four frequency bands with sufficient isolation to avoid signal reduction, a COTS gimbal that can position the beam over a hemispherical coverage, and a tripod for mating the assembled antenna to for ground operations. A major benefit to the QPRA design is that most of the components are either 3-D manufactured

or COTS parts which reduce the overall size, weight, and cost per unit. Section 4.2 will describe the QPRA system design and Section 4.3 will present the feed assembly design, in addition to measured radiation patterns and return loss for the feed assembly obtained through anechoic chamber performance testing. Section 4.4 describes the quadruplexer design to include the topology and overall geometry of the unit. Return loss measurements are also presented for the two fabricated quadruplexer units and compared with simulations to gage performance. Section 4.5 provides the reflector antenna performance by presenting measured performance of the fully integrated QPRA system.

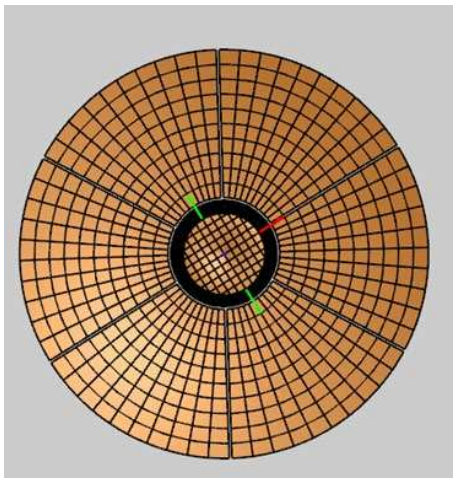
4.2 Petal-Reflector Antenna Design

The QPRA assembly is shown in Figure 4.2. The main components of QPRA are a 15" dia. main reflector, a sub-reflector supported by the feed using a conical radome, a feed assembly comprising a wideband ridged horn, a wideband polarizer, two quadruplexers, two-axis COTS gimbal and a tripod structure to mount the antenna assembly and the gimbal on for supporting ground operations. The reflector uses a small focal-length to diameter ratio (F/D) of 0.21 in order to keep the antenna overall size very compact. The reflector design, sub-reflector surface profile optimization and RF analysis were performed using TICRA's GRASP commercial software package. GRASP is a very efficient tool which uses physical optics to accurately predict QPRA radiation patterns. The main reflector is made of 6 identical petals comprised of plastic (rexolite) with metal coating on the top of the reflecting surface. The petal geometry is shown in Figure 4.3. The petals have an adjacent gap of 0.1" so that they can be easily inserted into a common circular mounting structure in the field when the soldier is stationary and easily and rapidly removed and stored in a carrying case when the soldier needs to roam. Analysis was performed to show that the gap between the petals would have minimal impact to performance over all frequency bands. The

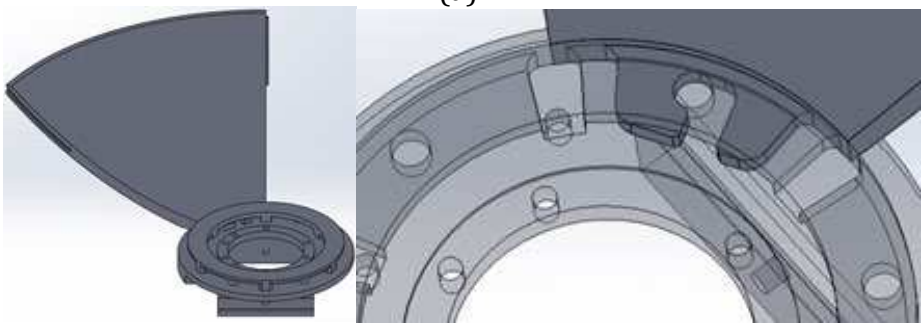
overall size of the QPRA in its assembled state is 15” dia. with height adjustable to 40” and the overall mass is approximately 16 lbs so that the soldier can carry it effortlessly in the battlefield. The antenna can scan over 90^0 in elevation plane and 360^0 in azimuth plane using the COTS 2-axis gimbal procured from FLIR (model PTU/5). It is mounted on a carbon fiber tripod structure which is a COTS part procured from K&F Concept. The main advantages and novel features of the QPRA when compared to conventional phased arrays are:

- Single quad-band petal reflector antenna instead of four separate phased array antennas
- 5 dB gain advantage due to avoidance of scan loss through the use of gimbal mechanisms
- One wideband horn element compared to 5,000 elements required for four phased arrays
- 3-D manufactured parts and COTS items to reduce cost and delivery schedule
- Lower DC and dissipated power by a factor of 4, and
- 6 times lighter than conventional phased arrays

Figure 4.2. Geometry of the QPRA (Left) and Gimbal Mechanism (Right)



(a)



(b) (c)

Figure 4.3. Petal Reflector Antenna Design Details . (a) Petal Reflector with 6 Petals, (b) One Petal in Circular Mounting Structure, and (c) View of Locking Feature of the Petal to Mounting Structure

4.3 Feed Assembly

The feed assembly includes a wideband quad-ridged horn with 73% bandwidth, a matching section and an OMT to generate two orthogonal linear polarization ports. The two linear polarization ports are connected to a COTS hybrid coupler to generate RHCP and LHCP signals. The two circular polarization (CP) ports are connected to two quadruplexers using two 2.92 mm coaxial RF cables. The quadruplexers separate the four frequency bands with sufficient isolation among them. Figure 4.4 shows the geometry of the horn assembly. The horn performance has been analyzed using the CST software. Measured return loss of the horn is shown in Figure 4.5 and compared with simulation results over the 14 GHz to 31 GHz frequency range. The agreement is reasonably good in spite of the increased dimensional tolerances due to 3-D manufacturing of the

horn using AlSiMg metal alloy. The return loss measured is better than 10 dB at both the orthogonal LP ports of the horn. The measured isolation performance between the two ports of the feed assembly is shown in Figure 4.6 and compared with simulations. The isolation is better than 30 dB mostly with the worst-case value of 28 dB at 30 GHz. Good agreement has been achieved between the two even with the increased tolerances associated with 3-D manufacturing of the feed assembly.

Figure 4.4. Quad-Ridge Horn Assembly with Transitions showing Orthogonal Ports

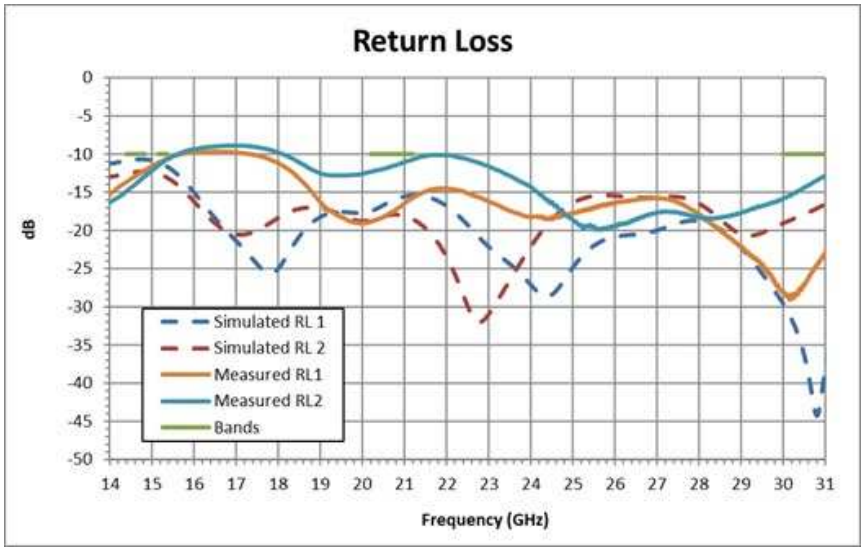


Figure 4.5. Return Loss of the Quad-Ridge Horn and Transition at Orthogonal Ports

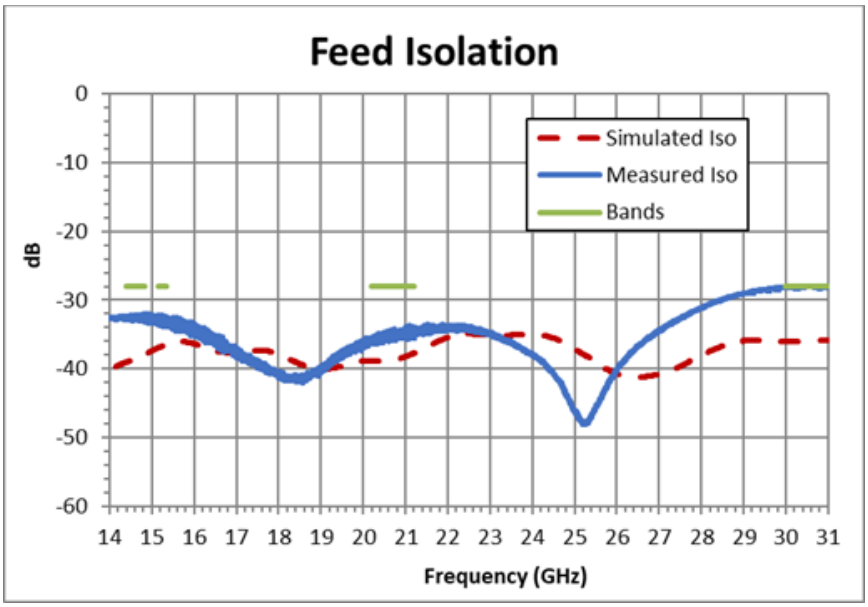


Figure 4.6. Isolation Performance between Orthogonal Ports of the Quad-Ridged Horn

The radiation patterns of the feed assembly have been measured in an anechoic chamber using a source horn and compared with simulated results in Figure 4.7 to Figure 4.10 at 14.4 GHz, 15.15 GHz, 20.2 GHz and 30.0 GHz, respectively. Co-polar and cross-polar radiation patterns are shown in $\varphi = 45^0$ plane in the plots. The horn patterns are well behaved over more than octave bandwidth and the agreement between measurements and simulations is excellent. The cross-polar patterns also agree well, and the differences are due to manufactured tolerances.

The sub-reflector is supported by a foam radome machined out of a solid piece of General Plastics Dielectric Foam, RF-2203, which is typically used for radome applications. The foam radome and quad ridge feed are analysed in CST, to include the performance impact of the foam radome support. The data from the CST simulations of the feed horn and foam radome is then used together with the sub-reflector and main reflector geometrical profiles in the GRASP simulation to predict final performance of the QPRA. The horn, radome support and sub-reflector assembly are depicted in Figure 4.11.

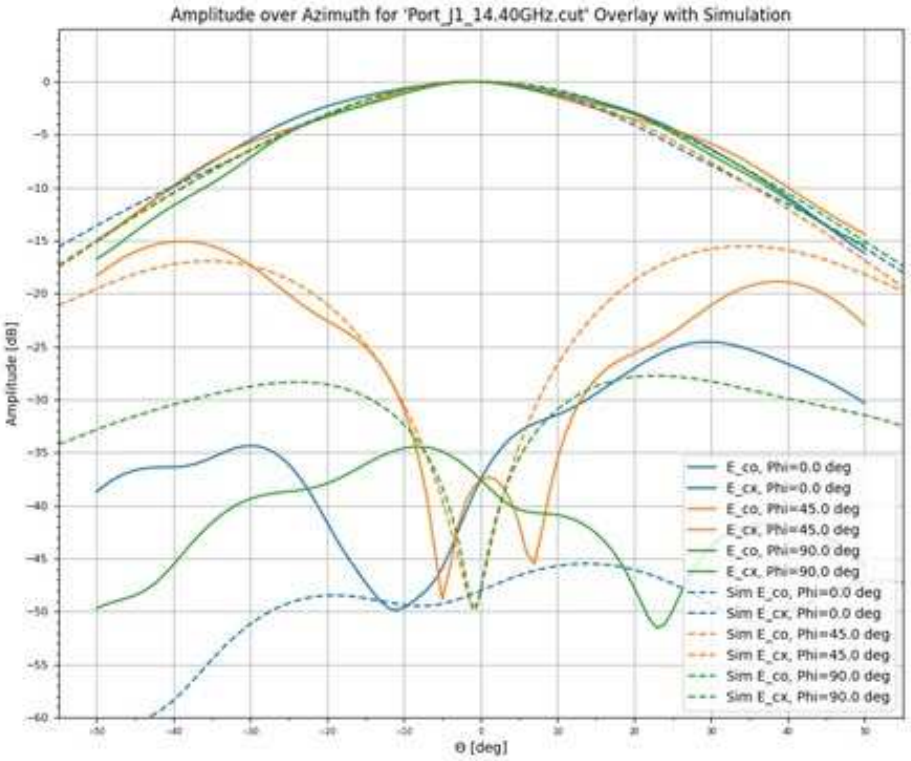


Figure 4.7. Radiation Patterns of the Quad-Ridged Horn at 14.4 GHz

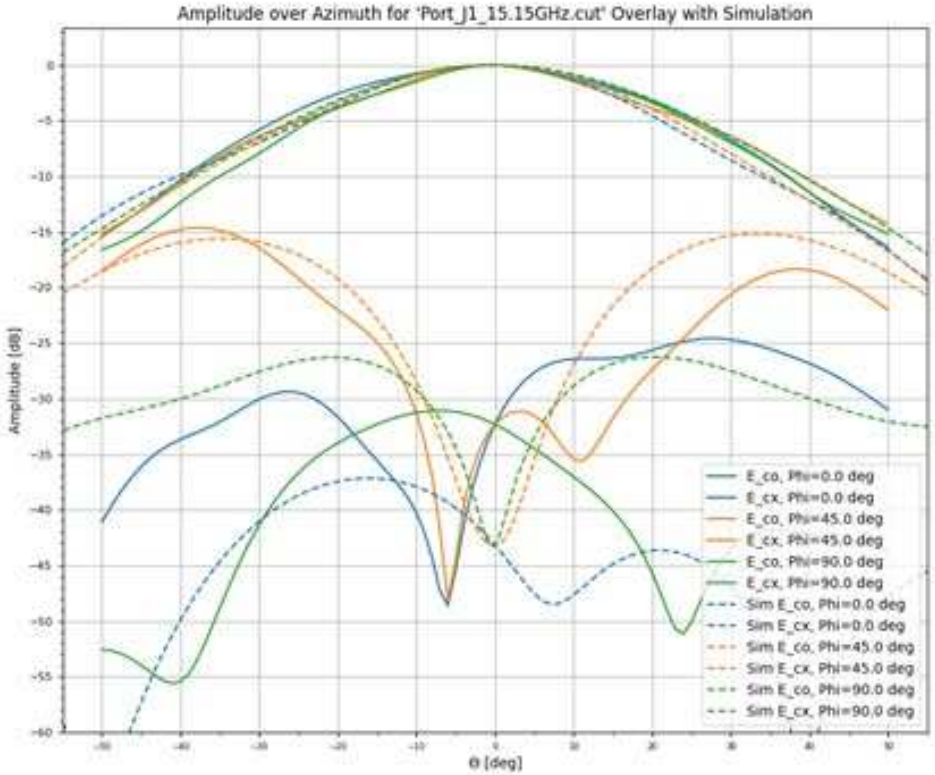


Figure 4.8. Radiation Patterns of the Quad-Ridged Horn at 15.15 GHz

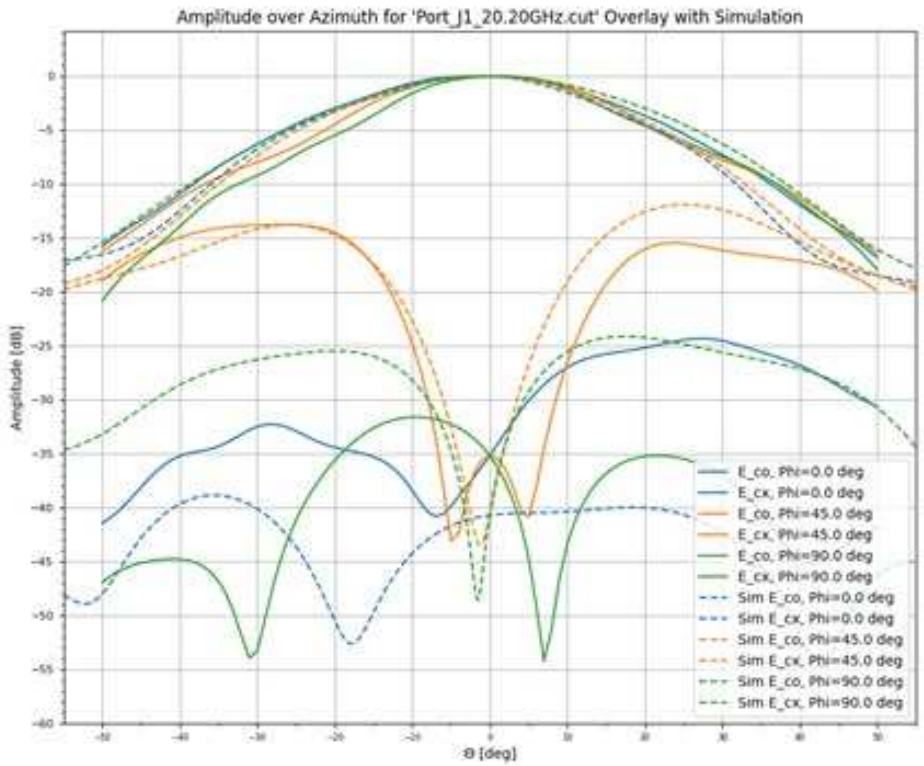


Figure 4.9. Radiation Patterns of the Quad-Ridged Horn at 20.2 GHz

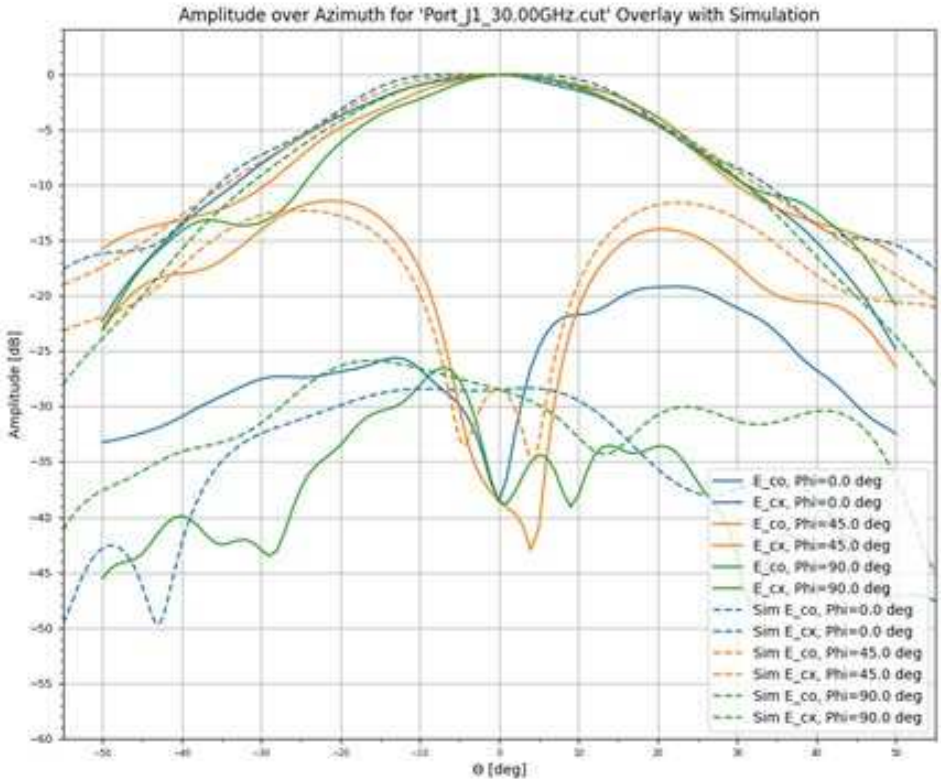


Figure 4.10. Radiation Patterns of the Quad-Ridged Horn at 30.0 GHz

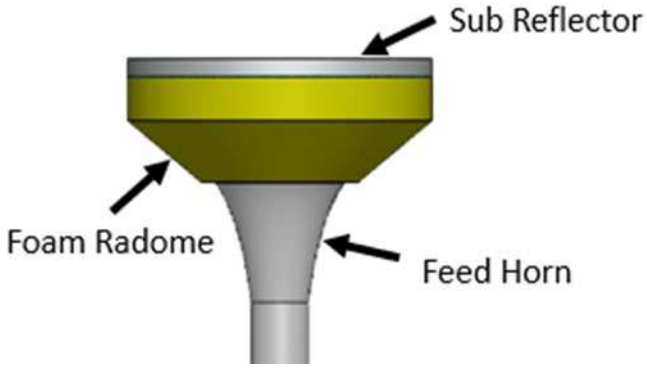


Figure 4.11. Sub-reflector and Feed Horn Assembled with Foam Radome Structure

4.4 Quadruplexer Design

A pair of quadruplexers are required to interface between each of the two orthogonal CP ports of the antenna feed and the four RF chains per polarization within the manpack. Primary design drivers are the very wide total bandwidth that must be supported within the communication system, and the high-power handling requirement, that makes the microstrip implementation undesirable. Low insertion loss and high isolation among the frequency bands, as well as low mass are other key design drivers. The design criticality is to achieve high isolation between the closely spaced Ku Rx and Ku Tx frequency bands with 2.15% band separation between the two.

The topology arrived at consists of a cascade of three diplexers as shown in Figure 4.12. A custom waveguide with reduced width and height custom has been selected as the internal transmission line media to minimize the occurrence of higher order mode propagation within the structure. This waveguide allows TE10 to propagate at the lowest frequency (14.4 GHz) and allows only the TE20 mode to propagate at the highest frequency band (31 GHz). Excitation of this mode can be avoided using a side-to-side symmetric structure throughout the device, which has the additional benefit of simplifying the electromagnetic model for computational analyses and optimization. Diplexer1 consists of a cut-off waveguide, with reduced waveguide dimensions, selected to pass the TE10 mode at 20.2-21.2 GHz, which extracts the K band at a tee junction while

a corrugated low pass structure passes the Ku-bands through to the next diplexer. Diplexer3 consists of a pair of traditional narrow bandpass inductive iris cavity filters with, 6 poles for low band and 7 poles for the high band, to achieve high adjacent band rejection.

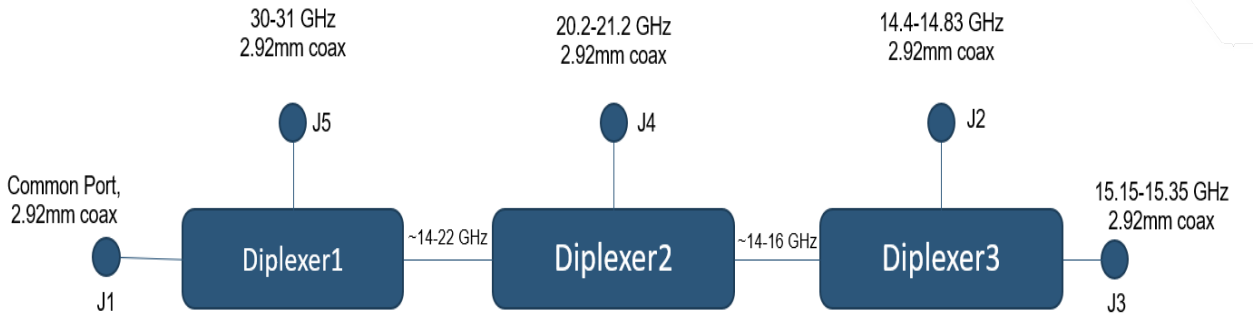


Figure 4.12. Layout of the Quadruplexer Topology

All three diplexers were designed using Microwave Wizard, a commercial software package developed for the design of complex waveguide components using mode matching, boundary contour mode matching, 2D Finite Element Method, 3D Finite Element Method, and the efficient cascading and intermixing of all of these electromagnetic techniques. This allows the user the most efficient method to simulate each element of a circuit, minimizing computation time. Additionally, Diplexer3 was optimized using an add-on filter optimization package, Equal Ripple Optimization, by DGS Associates, which is a highly efficient optimizer developed specifically for filters. The combination of Microwave Wizard and Equal Ripple Optimizer has proven very effective and efficient for the design of tuning-less filters, diplexer, and multiplexers.

The three diplexers were designed independently first, and then cascaded with only minor optimization of connection lengths to improve the return loss. One end launcher and four side launcher coaxial connector transitions were designed using Microwave Wizard and then integrated into the package. Southwest Microwave Inc 2.92 mm thread-in Hi-Rel connectors were selected for this prototype. The quadruplexer was precision CNC machined from 6061-T6 Aluminum in

two halves to create a split-block / clamshell construction, with no provision or need for tuning screws. The diplexers are laid out such that they can be parted at the waveguide zero current line to reduce RF leakage. The quadruplexer design layout and the fabricated hardware are shown in Figure 4.13 and Figure 4.14 respectively.

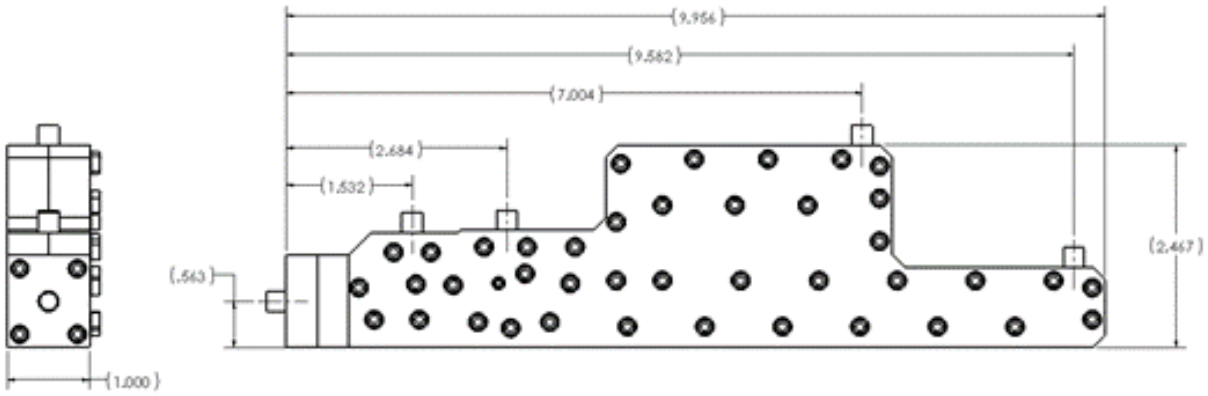


Figure 4.13. Quadruplexer Geometry Layout

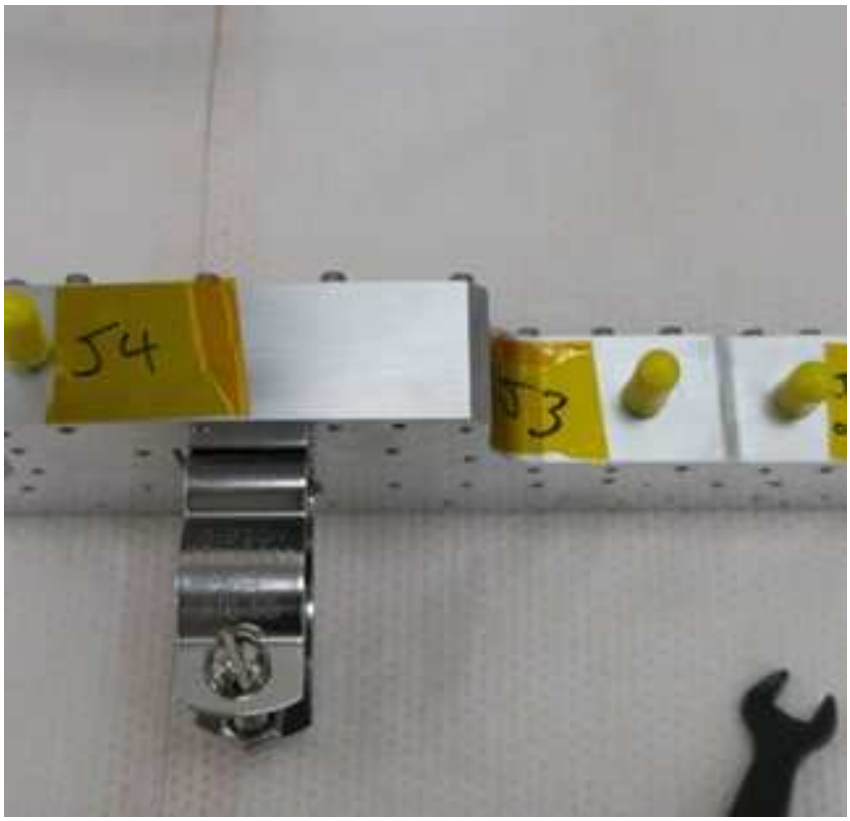


Figure 4.14. Quadruplexer Fabricated Unit

The return loss of the quadruplexer has been measured and compared with simulated results and is depicted in Figure 4.15. The measured results match well with simulations and return loss specification of 15 dB is met at all the four bands with margin. A high isolation of > 40 dB is achieved among the frequency bands. Figure 4.16 shows the measured passband characteristics at 30 GHz band and the isolation achieved at Ku Rx, Ku Tx and K Rx bands. Isolation of better than 65 dB at K-band and better than 80 dB has been accomplished for the quadruplexer with passband at Ka. Isolation performance for the Ku Tx passband at other three bands is shown in Figure 4.17. Insertion loss has been measured at all four bands and the results are plotted in Figure 4.18. Measured insertion loss is 0.8 dB, 0.9 dB, 0.5 dB and 0.5 dB at Ku-Rx, Ku-Tx, K Rx and Ka Tx frequency bands respectively. Insertion loss is higher at the two Ku-bands due to close proximity of the two Ku-band frequencies. Two units of quadruplexer have been fabricated and tested. All requirements have been met for the two prototype quadruplexers.

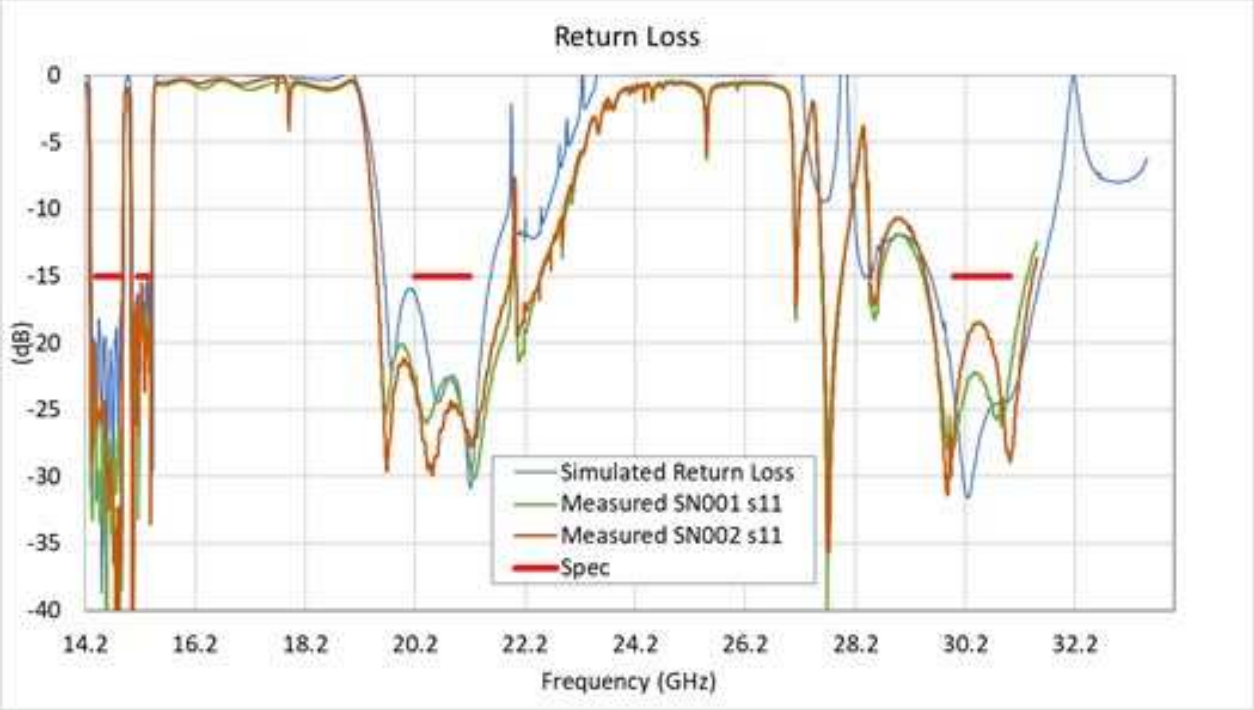


Figure 4.15. Measured Return Loss Performance of the Quadruplexer

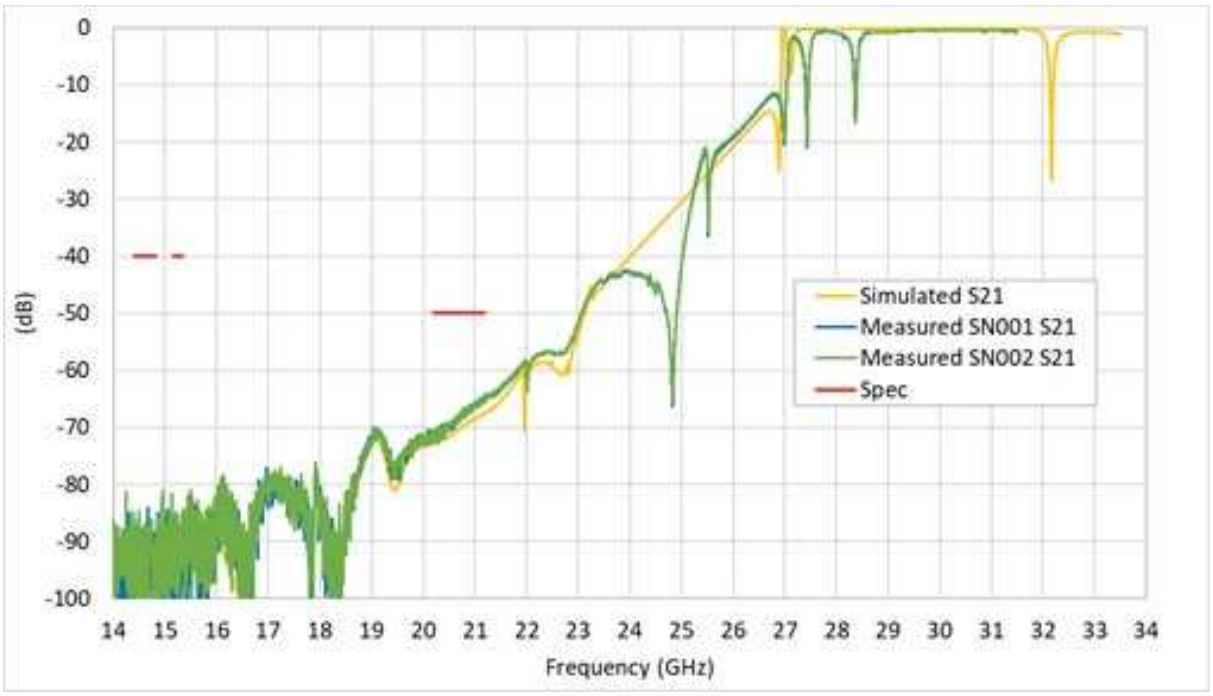


Figure 4.16. Measured Isolation of the 30 GHz Passband over Three Other Bands

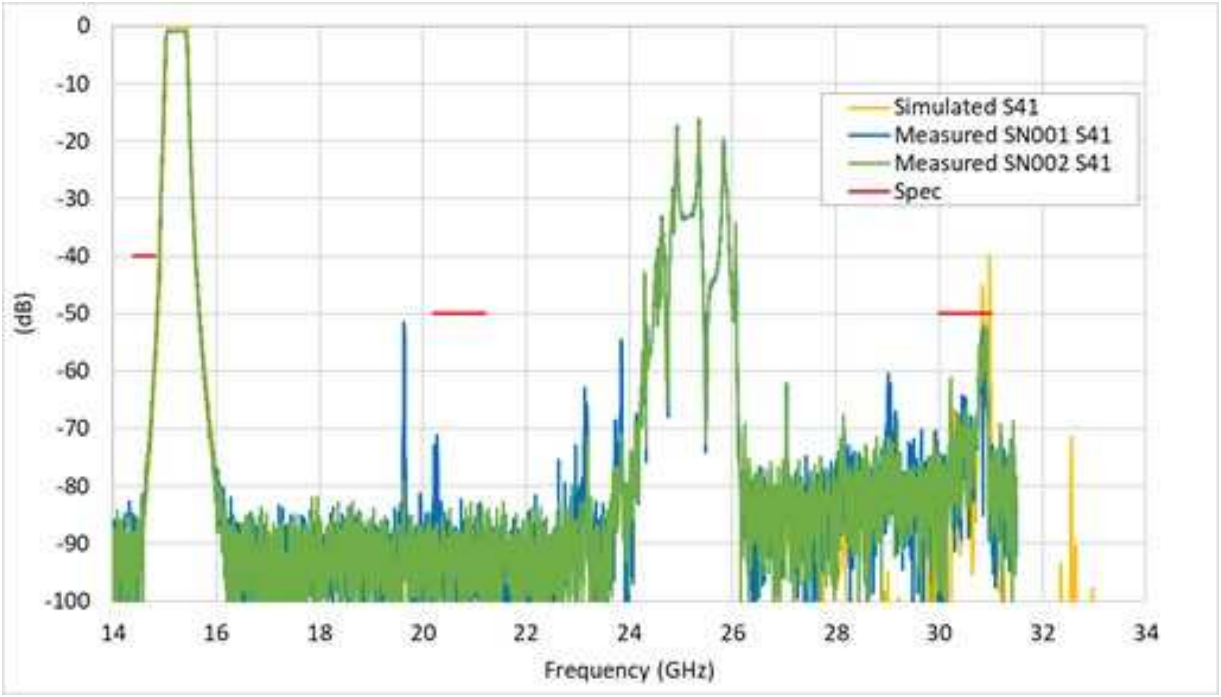
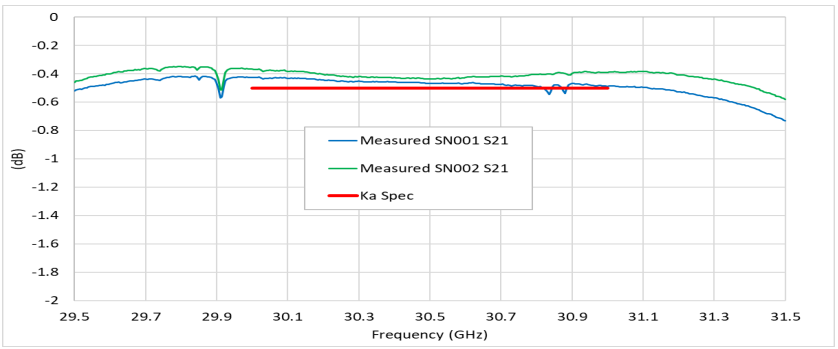
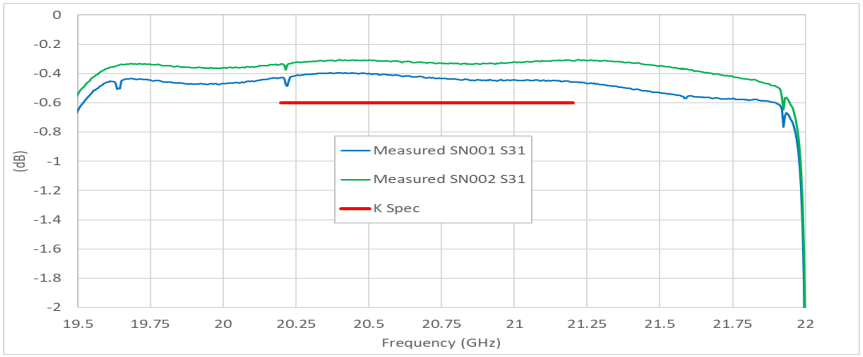


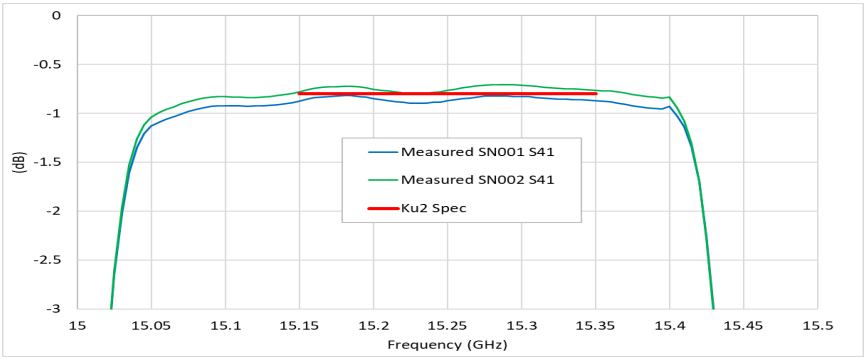
Figure 4.17. Measured Isolation of the 15 GHz Passband over Three Other Bands



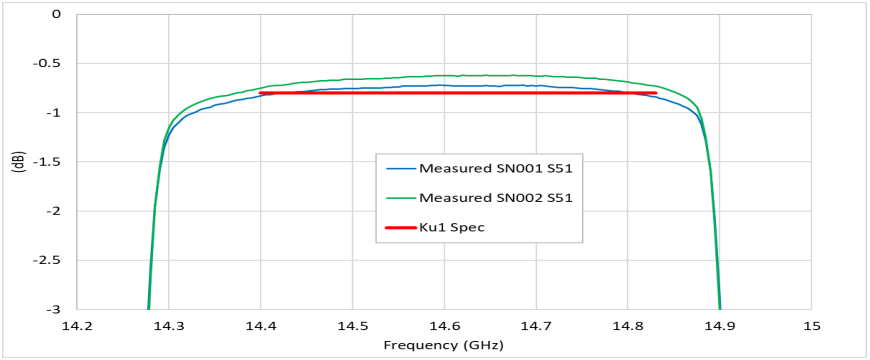
(a)



(b)



(c)



(d)

Figure 4.18. Measured Isolation Loss of the Quadruplexer at the Four Bands

4.5 Antenna Performance

Measured radiation patterns of the QPRA are shown in Figure 4.19 through Figure 4.22 at Ku Rx, Ku Tx, K Rx and Ka Tx bands respectively.

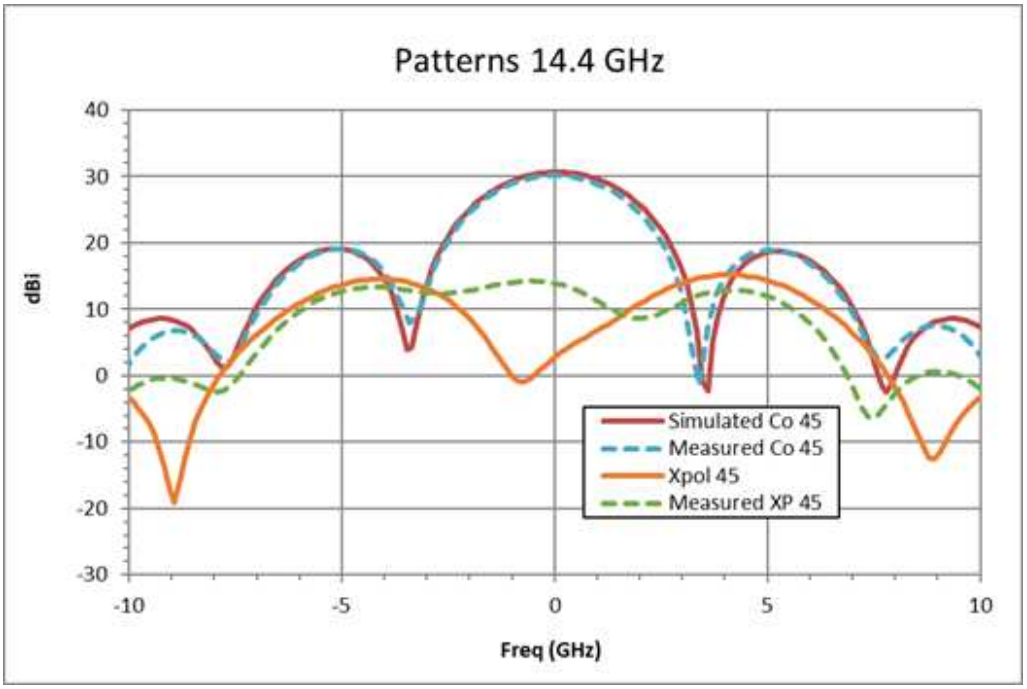


Figure 4.19. Radiation Patterns at 14.4 GHz

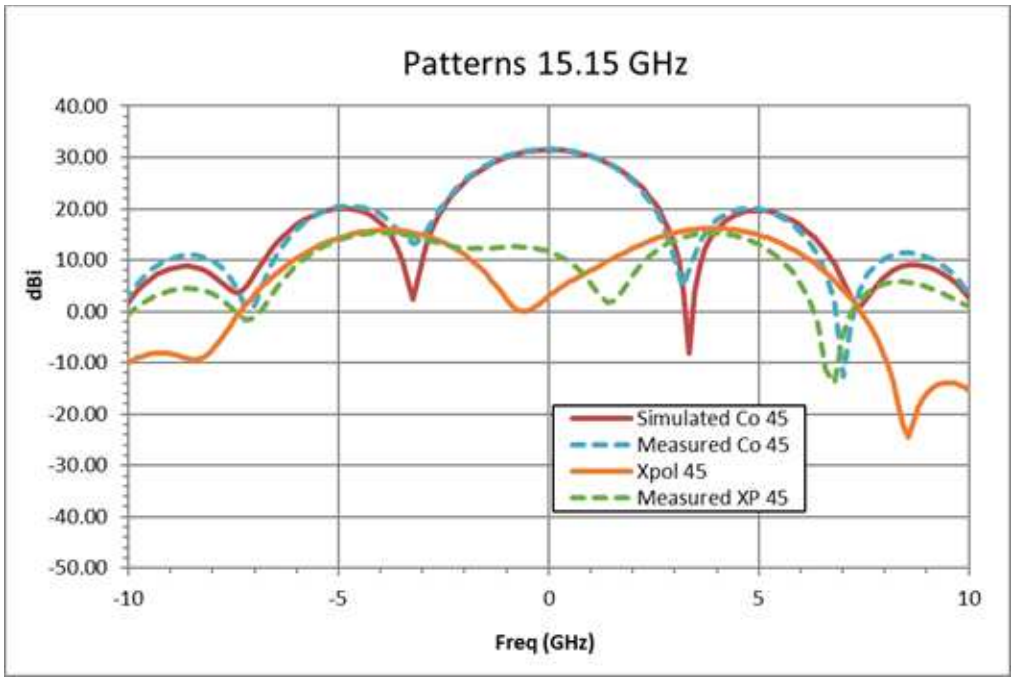


Figure 4.20. Radiation Patterns at 15.15 GHz

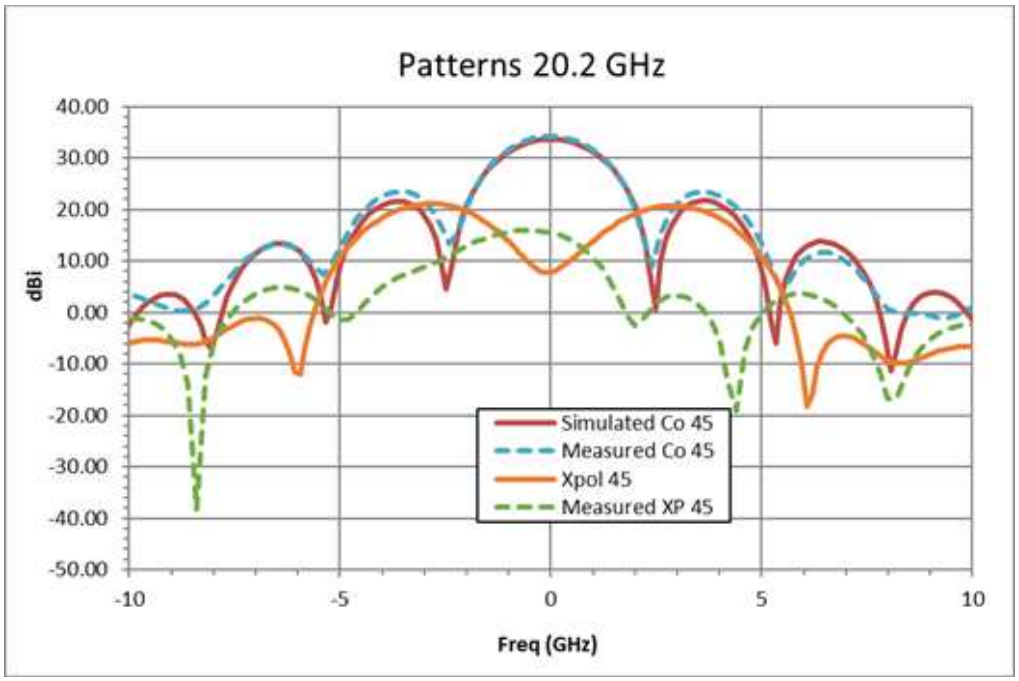


Figure 4.21. Radiation Patterns at 20.2 GHz

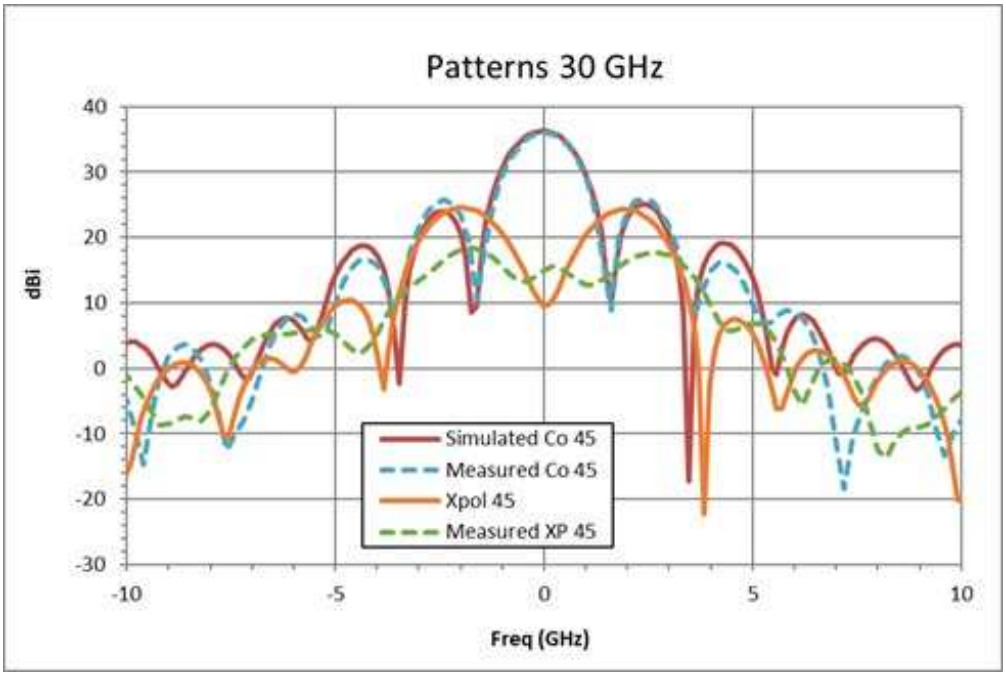


Figure 4.22. Radiation Patterns at 30.0 GHz

Detailed loss budget and antenna gain performance is summarized in Table 4.1. The loss budget includes feed assembly loss, quadruplexer loss, cable loss, surface RMS loss of the main reflector and sub-reflector, and thermal distortion loss. The total loss is subtracted from the measured antenna directivity to obtain the antenna gain. Measured antenna gain meets the requirements with margin at all four frequency bands.

Table 4.1. Measured Gain / Loss Budget of Quad-band Petal Reflector Antenna

Frequency, GHz	14.4	15.15	20.2	30.0
Peak Gain Measured	30.15	31.71	34.32	36.06
Antenna Losses				
Cable Loss 2 ft	-1.12	-1.12	-1.22	-1.44
QuadPlexer Loss	-0.79	-0.87	-0.43	-0.42
Feed System Losses	-1.91	-1.99	-1.65	-1.86
Antenna Assembly Loss at ambient	-1.91	-1.99	-1.65	-1.86
Feed Loss at 40ºC	-0.15	-0.15	-0.15	-0.15
Loss due to thermal distortion	-0.027	-0.027	-0.084	-0.117
Random Errors (RSS)	-0.15	-0.15	-0.17	-0.19
Total Antenna Loss, dB	-2.06	-2.15	-1.82	-2.05
Antenna Peak Gain, dB	28.08	29.56	32.50	34.00

4.6 High-Band Antennas for Comms at the Halt Summary

This chapter presented development results of a novel QPRA for soldiers on the ground communicating with other aircraft in hostile situations, satellites, and command headquarters, and is intended to support high-capacity CATH. The antenna has more than an octave bandwidth enabling it to operate simultaneously at four frequency bands; Ku RX, Ku TX, K RX and Ka TX. A single QPRA replaces conventional design using four phased arrays, one for each band, reducing the cost, mass, and production schedule significantly. The fabricated antenna has been tested, and

measured results agree well with simulations, and it meets all the system requirements with margin. The antenna beams are scanned over the hemispherical coverage region using COTS gimbals. One advantage is that there is no scan loss associated with beam scanning unlike phased arrays. Key aspects of the antenna design including low mass, low-cost, ease of deployment and stowage, combined with significantly higher gain, have been successfully demonstrated. This antenna will be field-tested in 2022 and later will be produced with thousands of units for ground applications with an emphasis on expeditious deployment in the battlefield.

Chapter 5. Future Manpack Multifunction Software Defined Radio

This chapter seeks to describe a future manpack SDR that was designed to support multiple missions (ground-to-squad conversations, ground-to-air conversations, and BLOS ground-to-satellite-to-headquarters conversations) while minimizing SWAP. This flexible, reconfigurable, scalable manpack SDR can be inherently paired with the mmW (refer to Chapter 3) and high-band (refer to Chapter 4) antenna technologies for supporting both COTM and CATH operations. This work is planned to be published in the peer-reviewed IEEE technical conference as noted in [5].

5.1 Manpack SDR Background

Communications are indispensable for warfighter dexterity, diversity and gaining advantage over adversarial detectors and interference. Military ground operators require proven tactical multifunction SDRs with integrated antennas to provide high capacity, protected at the halt communications with future Intelligence, Surveillance and Reconnaissance (ISR) platforms and Department of Defense (DoD) Geosynchronous Earth Orbit (GEO) satellites, and low capacity, on the move communications for survivability and immediate air support. Advanced ISR capabilities provide an inherent benefit to friendly forces through SA, knowledge of the adversary and environment, and condensing the duration between sensing enemy forces and responding to them through advanced weapon targeting systems. Figure 5.1 shows an operational view for how the emplaced environment that the future tactical manpack SDR will reside in supporting an emplaced near peer scenario with dispersed blue force teams to provide local, air, and BLOS communications. Here, high bandwidth applications that can be supported with the directional antenna to provide the distribution of biodata, video, time sensitive data discovered on high value targets, and special force target collection data.

In this chapter, we will provide a background into what spawned the design and development of the tactical manpack multifunction SDR and we will provide a technical description of the SDR to include its discriminating antenna technologies that are enablers for communications. Additionally, prototype designs of supporting original antenna technologies will be summarized to facilitate empowering communications between key operational assets. Finally, a testing roadmap will be outlined for future-design and manufacturing improvements.

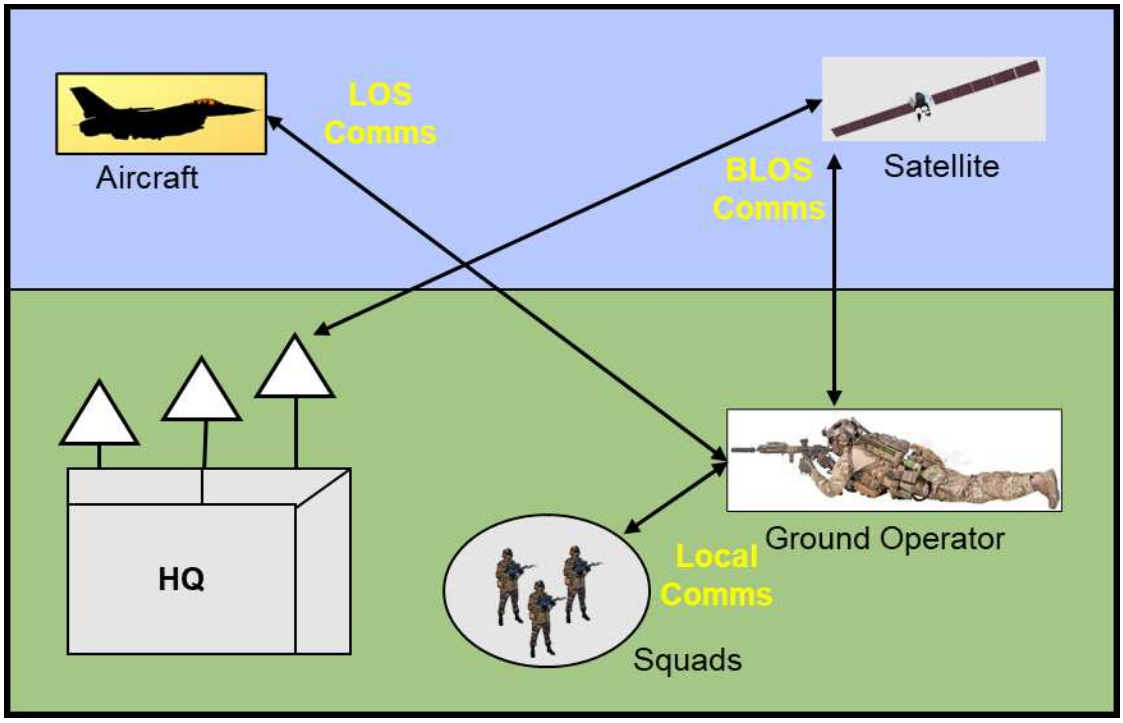


Figure 5.1. Future Tactical Manpack Radio Operational Boundary

The tactical manpack SDR will enable small unit tactical operations to persist under diverse electronic warfare conditions by developing an integrated communications systems protecting local, airborne, and reach-back communications from exploitation and denial. This is necessary, as United States (U.S.) forces have grown increasing effective at using small tactical unit operations to perform a multitude of missions ranging from communications, data collection, and strike operations. However, these forward units often find themselves operating in the proximity near adversarial forces which attempt to degrade or deny communications between operational

platforms or units. These information exchanges are vital to protect, and as such, a future tactical manpack SDR integrated with advanced antenna technologies has been developed.

5.2 Manpack Multifunction Radio Description

Physical and design specifications for the tactical manpack SDR are presented in Table 5.1. In addition to the physical requirements, the manpack radios and associated antenna technology must be low-cost such that they can be expendable if needed, and mass produced for small tactical unit operations. Figure 5.2 provides a depiction of the emerging tactical manpack radio prototype. Connectors are shown for attaching instrumental antenna technologies and an engineering graphic user interface (GUI) / display.

The manpack SDR also supports a full gamut of frequency bands including VHF, UHF, L, S, Ku, K, and Ka-bands which enable the selection of exclusive waveforms dependent on intended communicant, environment, and need. This technical manpack radio solution will allow, through configuration, the support of multiple waveforms simultaneously to facilitate communications for different operational missions.

Table 5.1. Physical Radio Specifications

No.	Requirements	Parameter
1	Size	• 7.9”(h)x8.4”(w)x2.8”(t) (w/o battery) • 12.0”(h)x8.4”(w)x2.8”(t) (w/ battery)
2	Weight	• 9.7 lbs (w/o battery) • 14.1 lbs (w/ battery)
3	Power	• 80 Watts at high duty cycle
4	Environment (Designed to)	• Operating Temperature: -20°C to 51°C • Vibration, Shock, Sand, Dust & Humidity IAW MIL-STD-810G • EMI / EMC IAW MIL-STD-461F
5	Accessories (Designed for compatibility)	• Battery harness to convert from MBITR to BA-5590 or vehicle power / wall power • ATAK • Dual voice interface headset

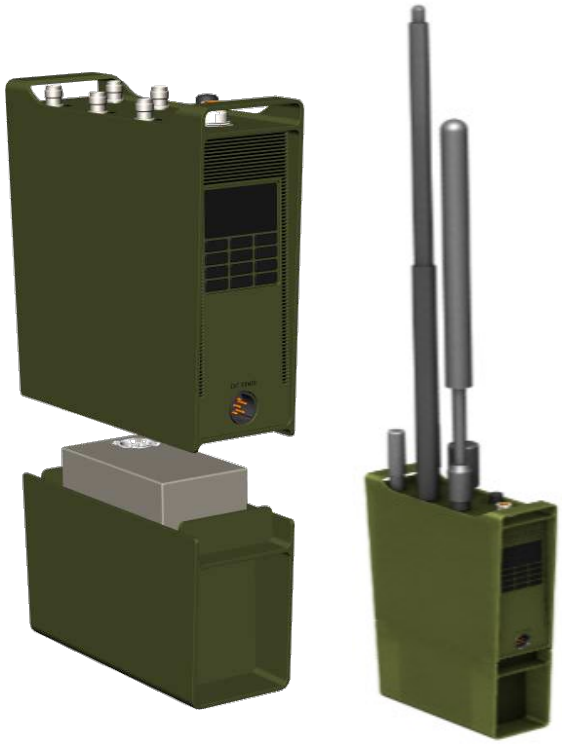


Figure 5.2. Future Tactical Manpack Radio . (Left) With Battery Housing (Right) Radio and COTM Antennas

5.3 Enabling Antenna Technologies

Advanced antenna technologies that can easily be integrated with the manpack SDR are critical to high-capacity communications both on the move and at the halt dependent on the operator situation. In Chapter 3, the Bunker antenna where wide-angle coverage is provided with this deployable antenna was described. Through continuous technical engagements with operator end-users, the final, lightweight design was conceived as shown in Figure 5.3. Measured radiation patterns across the supporting frequencies were also obtained for the six prototype antennas manufactured. Additionally, Figure 5.3 depicts an easy to deploy, ruggedized, lightweight Quad-Band Petal Reflector Antenna (QPRA). This antenna has been developed to provide high-band, full duplex communications at Ku-band TX, Ku-band RX, K-band RX, and Ka-band TX operations. Measured test results for antenna performance are documented in Chapter 4. Other

commercial antennas are available to integrate with the radio to support VHF, UHF, and L/S-band frequencies.

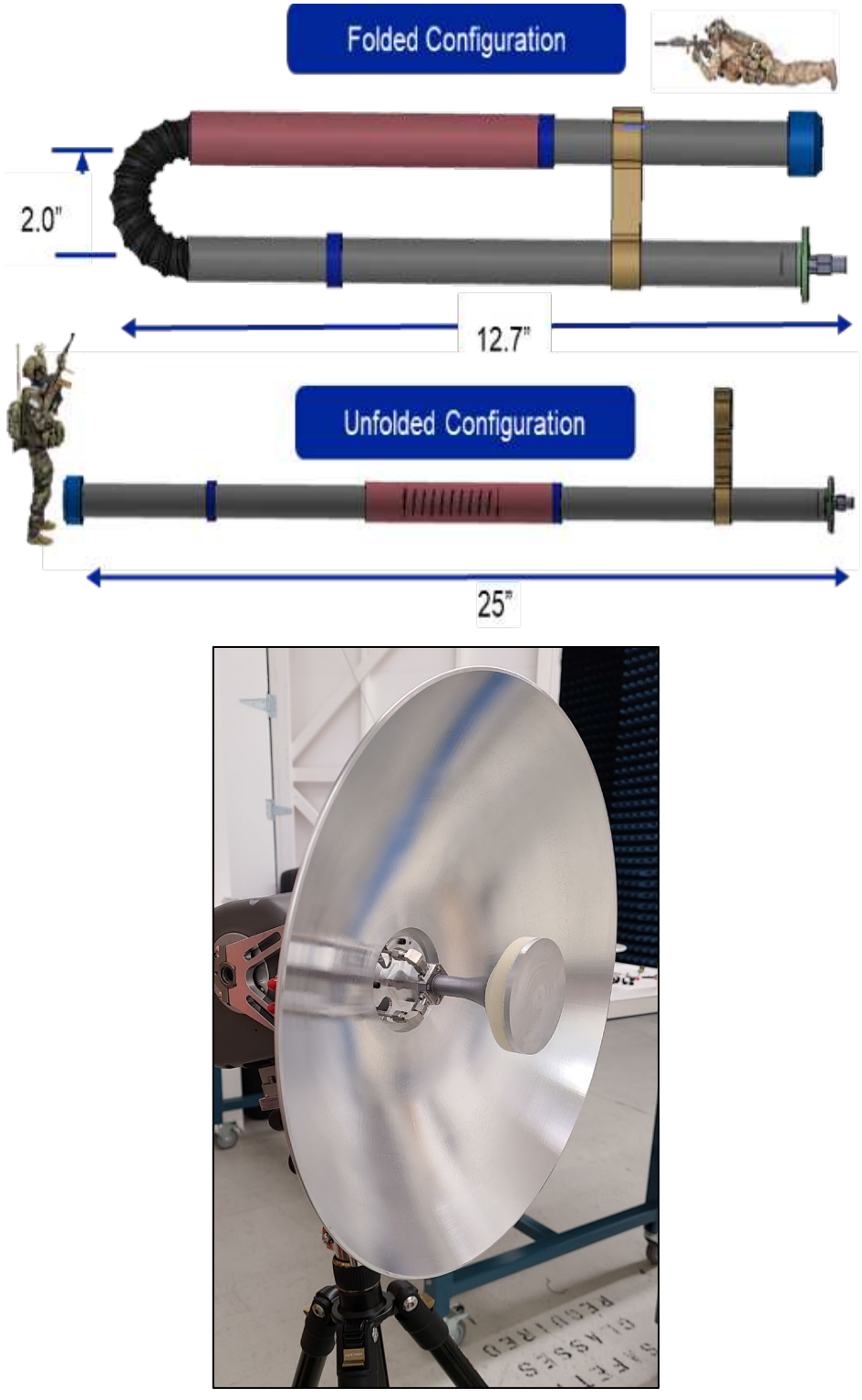


Figure 5.3. Bunker Antenna (Top) & Solid Reflector Antenna (Bottom)

5.4 Tactical Manpack SDR Summary

A novel tactical multifunction SDR coupled with innovative antenna technologies that can be used for multiple missions was presented. Vulnerability to sophisticated detectors and interference has facilitated the necessity for such a compact, manpack radio. Unique antennas, extending from high-band directional sub-reflector technologies and wideband omni-directional antennas integrated with the manpack enable multi-facet communications which strengthen our tactical relevancy.

Future work planned for the manpack SDR post development is to conduct over-the-air testing of the radio for selected military waveforms. The testing will involve the prototype systems, dynamic environments, and real-RF conditions to fully characterize the performance of the waveforms exercised in an operationally relevant environment in July 2022. Upon completion of the over-the-air manpack testing, a flight demonstration will be performed in the Georgetown Delaware local in December 2022, where a ground based manpack will communicate with an aircraft at high speeds to exchange critical information; this will showcase the multi-mission capability of the manpack multifunction SDR and overall benefits to the armed forces.

Chapter 6. Cognitive Antennas for Space Networks Interoperability

This chapter seeks to provide technical design parameters required for a multi-faceted, multi-domain phased array that can be used to support space-based communications to multiple destinations (other satellites and large ground-based networks). Additionally, it presents a way to improve phased array technology by adding cognition to optimize communications. This work was published in the peer-reviewed IEEE technical conference as noted in [6], and describes revolutionary CAs for not only space networks interoperability, but compatibility as well.

6.1 Cognitive Antenna Background

A CA is the empowering front-end of a cognitive communications system (CCS), and essential for future space networks compatibility. The differences between phased arrays, reconfigurable antennas, smart antennas, and CAs are provided in Table 6.1. In this description, phased arrays produce an electronically scanned beam based on constructive and destructive interference patterns generated by adjustable delay devices associated with each radiator in the array. Individual delays are programmed by a remote beam steering controller that derives attitude and pointing information from S/C available information. Reconfigurable (Reconf.) antennas are capable of dynamically adjusting frequency, radiation pattern, or polarization in a reversible manner, using some integrated mechanism to modify current distribution across the aperture. A smart antenna is an array that utilizes signal processing algorithms to identify spatial information such as the directional of arrival to autonomously calculate beamformer vectors to locate targets. A CA is an environmentally aware antenna that can dynamically allocate bandwidth and/or adjust beam direction and directivity, equivalent isotropic radiated power (EIRP), provide beam nulling, etc. to optimize spectral, spatial, and temporal resources to complement CR technology. The CA is continuously learning about the environment through experiences gained from collaborative interactions from users, resources, and

the environment, to emulate the Bloom's Taxonomy paradigm [59], inspired from human lower order thinking to remember, understand and apply changes based on awareness, category information, and pattern recognition.

Table 6.1. Cognitive Antenna vs. Legacy Antenna Technologies

Capability	Phased Array	Reconfig. Antenna	Smart Antenna	Cognitive Antenna
Adjust radiation pattern to increase gain or insert null				
Beam steer to track target while in relative motion				
Ability to change frequencies of operation				
Estimate direction of arrival (DOA) of received signal				
Learn and exploit spatial and spectral configurations				
Detect antenna faults and optimize antenna pattern(s)				
Incorporate spacecraft dynamics into optimization calculations				
Interact with cognitive radio to jointly optimize system performance				

6.2 Cognitive Antenna System Requirements

This section describes the scenario development, driving requirements and its operational view with information data flow exchange expected amongst users. It also provides a look into the M&S&A conducted to understand what expected EIRP the antenna needs to provide.

There are a number of high-level system requirements for future space CA systems. The system requirements are categorized as shown in Table 6.2 and are essential in designing a future CA relay system.

Table 6.2. Cognitive Antenna Requirements Summary

No.	Category	System Requirement
1	Frequency	The Cognitive Antenna shall operate anywhere from 18 GHz to 33 GHz.
2	Bandwidth	The Cognitive Antenna shall have an adjustable bandwidth from 10 MHz to 200 MHz.
3	Beamwidth	The Cognitive Antenna shall support an arbitrary beamwidth for variable data rates.

No.	Category	System Requirement
4	Coverage	The Cognitive Antenna shall provide Hemispherical coverage.
5	Beams	The Cognitive Antenna shall support at least four (4) independent beams.
6	EIRP	The Cognitive Antenna shall support variable EIRP dependent on use case applications.
7	Nulling	The Cognitive Antenna shall provide directional nulling to minimize interference.
8	Power	The Cognitive Antenna shall support low power per channel, e.g. <500 mW where feasible.
9	Interoperability	The Cognitive Antenna shall be interactive with a Cognitive Radio.

6.3 Operational View

With the addition of a CA, it provides an opportunity for enhanced network connectivity and performance through complementary interference mitigation and link optimization capabilities. Figure 6.1 below provides an expected operational use of the CA at LEO acting as a relay node between various resources, to include Commercial and DoD space networks.

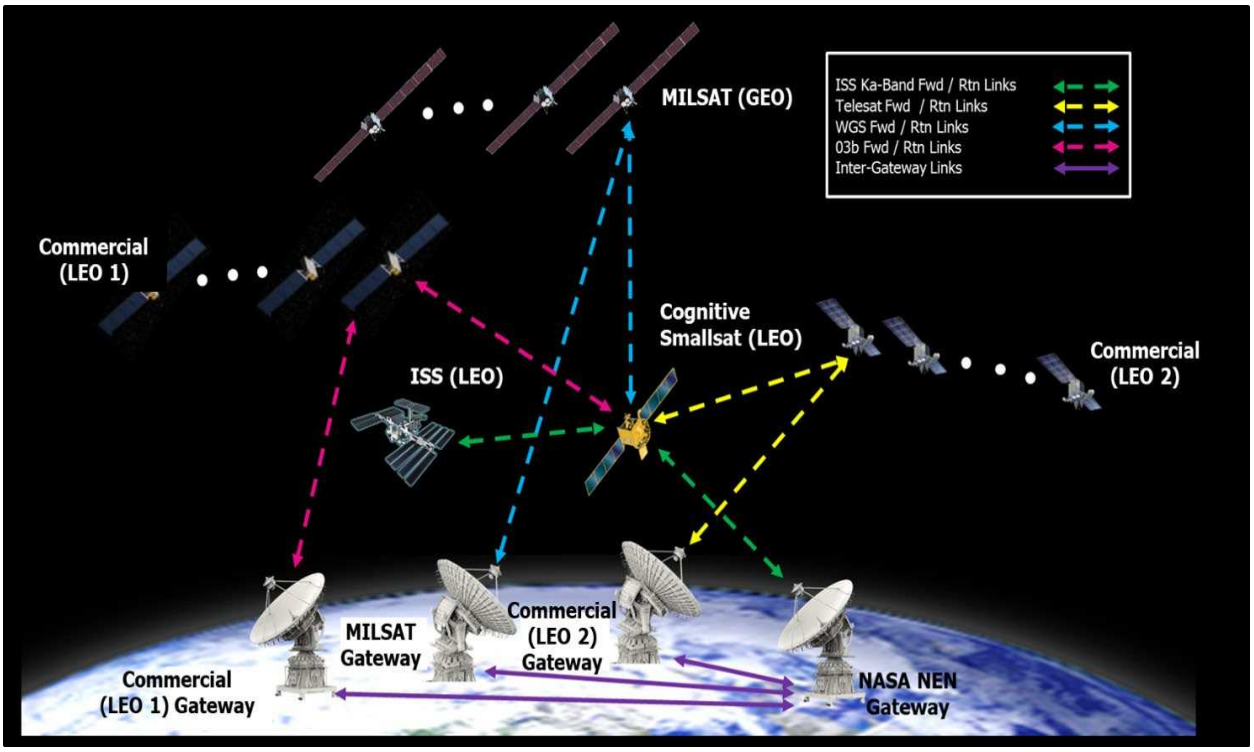


Figure 6.1. Cognitive Antenna Operational View for LEO Relay

An example use-case thread for *Interference Mitigation* using the CA is shown below to signify the importance of the use and its innovative offerings.

1. ISS transmits science data to CA Smallsat (LEO) for forwarding to NASA NEN Gateway.
2. CA receives ISS science data with sufficient link margin for healthy communications.
3. Interferer begins transmitting within CA Receive (Rx) channel / Rx beam disrupting ISS <-> CA communications and impairing NASA data collection efforts.
4. CA sense / characterizes interference and optimizes antenna parameters for ISS <-> CA link while providing beam nulling in direction of interferer. CA learns to implement optimal configuration for future flybys of interferer and other similar interferers.
5. NASA mission experiences improved science data collection rates.

6.4 Modeling & Simulation & Analysis

M&S&A was conducted to understand the array design constraints. Analysis performed evaluated (5) primary NASA services at varying data rates. A *What If* condition was applied to the Margin set to 2 dB to derive the required Terminal EIRP to close the communications link at the specified ranges between each node. Here, the LEO Satellite Relay to Ground, LEO Satellite Relay to Communication GEO Satellite, and LEO Satellite Relay to Communication LEO Satellite are use cases presented. The consensus of the analysis was that the results were analogous to those completed by NASA for Lunar missions.

LEO Satellite Relay to Ground Sample

			LEO Sat to Ground	LEO Sat to Ground
ITEM	LINK PARAMETER	UNITS	Value	Value
1	Terminal EIRP	dBW	20.1	33.1
2	Free Space Path Loss	dB	202.65	202.65
3	Frequency	Hz	2.70E+11	2.70E+11
4	Speed of Light	m/s	3.00E+08	3.00E+08
5	Range	nmi	647.9	647.9
6	Atmospheric Loss	dB	2.0	2.0
7	Weather Loss	dB	0.0	0.0
8	Scintillation Loss	dB	0.0	0.0
9	Propogation Loss	dB	204.65	204.65
10	System G/T	dB/K	46.0	46.0
11	Boltzmann's Constant	dBW/K-Hz	-228.6	-228.6
12	Single Link Received C/N_0	dB-Hz	90.0	103.0
13	Information Bit Rate	dB-bits/s	8.00E+01	9.30E+01
14	Implementation Loss	dB	0.0	0.0
15	Required E_b/N_0	dB	8.0	8.0
16	Required C/N_0	dB-Hz	88.0	101.0
17	Margin for Up / Downlink (Clear Sky)	dB	2.00	2.00

Figure 6.2. LEO Satellite Relay to Ground Link Budget Analysis

LEO Satellite Relay to Comm GEO Satellite Sample

			LEO Sat to Comm LEO	LEO Sat to Comm LEO	LEO Sat to Comm LEO	LEO Sat to Comm LEO
ITEM	LINK PARAMETER	UNITS	Value	Value	Value	Value
1	Terminal EIRP	dBW	12.2	22.2	29.2	39.2
2	Free Space Path Loss	dB	197.12	197.12	197.12	197.12
3	Frequency	Hz	1.85E+11	1.85E+11	1.85E+11	1.85E+11
4	Speed of Light	m/s	3.00E+08	3.00E+08	3.00E+08	3.00E+08
5	Range	nmi	500.0	500.0	500.0	500.0
6	Atmospheric Loss	dB	2.0	2.0	2.0	2.0
7	Weather Loss	dB	0.0	0.0	0.0	0.0
8	Scintillation Loss	dB	0.0	0.0	0.0	0.0
9	Propogation Loss	dB	199.12	199.12	199.12	199.12
10	System G/T	dB/K	14.9	14.9	14.9	14.9
11	Boltzmann's Constant	dBW/K-Hz	-228.6	-228.6	-228.6	-228.6
12	Single Link Received C/N_0	dB-Hz	56.6	66.6	73.6	83.6
13	Information Bit Rate	dB-bits/s	5.00E+01	6.00E+01	6.70E+01	7.70E+01
14	Implementation Loss	dB	0.0	0.0	0.0	0.0
15	Required E_b/N_0	dB	4.6	4.6	4.6	4.6
16	Required C/N_0	dB-Hz	54.6	64.6	71.6	81.6
17	Margin for Up / Downlink (Clear Sky)	dB	2.00	2.00	2.00	2.00

Figure 6.3. LEO Satellite Relay to Comm GEO Satellite Link Budget Analysis

LEO Satellite Relay to Comm LEO Satellite Sample

ITEM	LINK PARAMETER	UNITS	LEO Sat to Comm GEO Value	LEO Sat to Comm GEO Value	LEO Sat to Comm GEO Value	LEO Sat to Comm GEO Value
1	Terminal EIRP	dBW	13.2	24.9	28.4	38.7
2	Free Space Path Loss	dB	191.00	191.00	191.00	191.00
3	Frequency	Hz	3.05E+10	3.05E+10	3.05E+10	3.05E+10
4	Speed of Light	m/s	3.00E+08	3.00E+08	3.00E+08	3.00E+08
5	Range	nmi	1500.0	1500.0	1500.0	1500.0
6	Atmospheric Loss	dB	1.0	1.0	1.0	1.0
7	Weather Loss	dB	0.0	0.0	0.0	0.0
8	Scintillation Loss	dB	2.0	2.0	2.0	2.0
9	Propogation Loss	dB	194.00	194.00	194.00	194.00
10	System G/T	dB/K	8.4	8.4	8.4	8.4
11	Boltzmann's Constant	dBW/K-Hz	-228.6	-228.6	-228.6	-228.6
12	Single Link Received C/N_0	dB-Hz	56.2	67.9	71.4	81.7
13	Information Bit Rate	dB-bits/s	5.00E+01	6.00E+01	6.70E+01	7.70E+01
14	Implementation Loss	dB	0.0	0.0	0.0	0.0
15	Required E_b/N_0	dB	4.2	5.9	2.4	2.7
16	Required C/N_0	dB-Hz	54.2	65.9	69.4	79.7
17	Margin for Up / Downlink (Clear Sky)	dB	2.00	2.00	2.00	2.00

Figure 6.4. LEO Satellite Relay to Comm LEO Satellite Link Budget Analysis

The results of this analysis are summarized in Table 6.3.

Table 6.3. Analysis Results Drive Array Design

No.	Service	Min Data Rate	Max Data Rate	Min Analysis EIRP	Max Analysis EIRP	Data Type
1	LEO Relay Satellite Direct to Ground	100 Mbps	2 Gbps	20.1 dBW	33.1 dBW	Various Data
2	LEO Relay Satellite to Commercial LEO Satellite	100 kbps	1 Mbps	12.2 dBW	22.2 dBW	Telemetry Data
3	LEO Relay Satellite to Commercial LEO Satellite	5 Mbps	50 Mbps	29.2 dBW	39.2 dBW	Science Data
4	LEO Relay Satellite to TDRS or WGS GEO	100 kbps	1 Mbps	13.2 dBW	24.9 dBW	Telemetry Data
5	LEO Relay Satellite to TDRS or WGS GEO	5 Mbps	50 Mbps	28.4 dBW	38.7 dBW	Science Data

The antenna design using this analysis needs to be designed to support the **worst case** EIRP shown which is equivalent to 40 dBW. Using a straightforward calculation for scan loss from the minimum to maximum frequencies that the CA technology will need to support, the antenna element quantity can be computed. The assumptions for Table 6.4 used a known hardware architecture that has a design for power amplifier (PA) transmit power of 16.5 dBm and an average power added efficiency (PAE) of 40%.

Table 6.4. Element Count for Design

No.	Element Count	64	128	256	512
1	18 GHz EIRP @ boresight (dBW)	-5.0	1.0	7.0	13.0
2	33 GHz EIRP @ boresight (dBW)	24.5	30.5	36.5	43.0
3	18 GHz EIRP @ 35 deg scan (dBW)	-6.2	-0.2	5.8	11.8
4	33 GHz EIRP @ 35 deg scan (dBW)	23.3	29.3	35.3	41.3
5	18 GHz EIRP @ 70 deg scan (dBW)	-11.5	-5.5	0.5	6.5
6	33 GHz EIRP @ 70 deg scan (dBW)	18.0	24.0	30.0	36.0
7	Power Consumption (W)	25.5	51.0	102.0	204.0

In reviewing this assessment, the total number of antenna elements required to obtain the level of required terminal EIRP to support the NASA missions is **512**. This is an important analysis, as it will allow us to conduct a comparison for the total number of elements for each selected hardware option as part of the CA hardware architecture trade evaluation in the future.

6.5 Cognitive System Controller Architecture

The cognitive system controller (CSC) architecture is defined to leverage the architecture of a distributed Dynamic Spectrum Access (DSA) system. A distributed DSA system uses RF sensing in the radio to gather and use spectrum SA to dynamically select operating frequency. This capability runs locally in each radio to rapidly recognize and resolve interferences and connect to

previously undiscovered networks with different frequencies. Adaptation is constrained by knowledge of spectrum regulations that are loaded into the radio to ensure compliant operations. DSA was developed as a CR function for use with simple antennas and the architecture can be extended for use in a CA by expanding the sensing capabilities to scan the frequency spectrum over time, frequency, and direction.

The DSA sensor approach is enhanced to account for directionality by creating multiple scanning functions across time, frequency, and both beamwidth and antenna pointing direction. Example scan patterns include the following:

- **Continuous fixed beam(s), wideband scan –** point the antenna in a fixed direction and scan across a defined wideband frequency range.
- **Fixed bandwidth, wide angle scan –** configure the sensor for a defined frequency range (up to the sensor single snapshot bandwidth) and sweep the antenna through a broad range of pointing angles.
- **Full bandwidth / angle scan –** sense over both wide bandwidth and wide angles.
- **Custom prioritized scan pattern(s) –** cycle through a list of bandwidth / pointing directions.
- **Dedicated beam / time-shared beam –** implement the scan as a dedicated function for an individual antenna beam or time-share the beam with other functions, such as demodulation
- **Interferometer-based sensing –** use the sensor to determine the angle of arrival of a detected signal.

A CA will implement scan pattern selection for efficient scanning, and over time will develop new scan patterns by modifying existing patterns and building new ones as it operates and learns about its operating environment. While sensing can be implemented as a time-shared

function with other functions such as demodulation, highly functional CAs will support multi-beam operation where one or more logical antenna beams can be used for full-time dedicated sensing. Depending on mission requirements, the number of beams used for sensing and scanning can be adaptively adjusted and placed under cognitive antenna control. For efficient operation and ease of control, the multiple antenna beams should be fully independent from one another in terms of supporting simultaneous transmit and receive functionality and tune frequency in addition to the assumed independence of beam pattern and pointing direction.

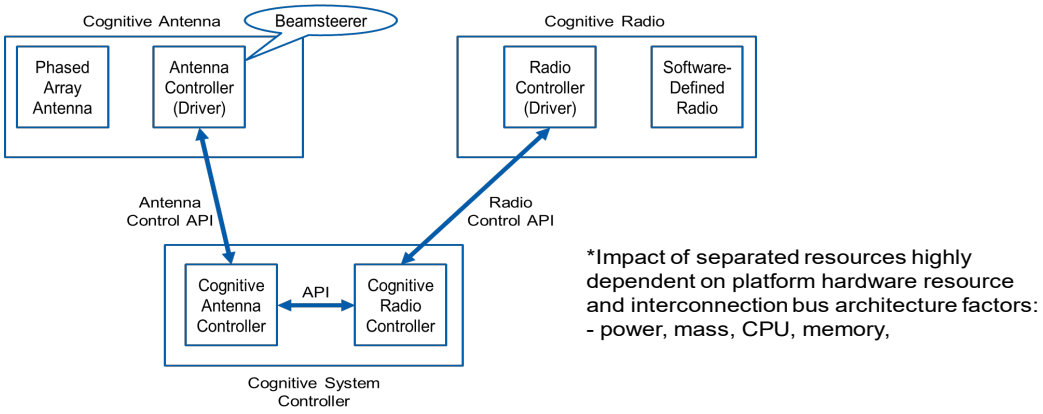
DSA uses a sensor-aided frequency rendezvous capability for joining candidate communications networks within range. For the CA, the rendezvous capability is extended to provide a function that identifies candidate Commercial and Government (e.g., WGS) satellites that the CR can join.

For maximum compatibility to support different system components, the Cognitive System assumes the CA and its controller, and the CR and its controller can be all physically separated from one another. For a physically separated antenna and radio, each with their own controller, there are four architecture combinations for where to place the distinct CA controller and CR controller as follows:

- Both controllers contained as part of the CA.
- Both controllers contained as part of the CR.
- Split between antenna and radio with each controller near its controlled element.
- External to both the antenna and the radio.

Figure 6.5 depicts the last option in the list where both the CA and CR controllers are separate from the CA and CR. The CA and the CR can each be partitioned into low-level and high-level tasks. The low-level tasks are items that are rapidly adaptive such as applying antenna

element weights for beam steering, and beam nulling for the CA, adaptive modulation and coding and signal path routing in the CR, as well as driver-like activities. High-level tasks operate over broader sets of tasks which typically require greater amounts of external data. The low-level tasks are always placed close to the item they are controlling. This architecture creates a series of Application Programming Interfaces (APIs) in the system defining communications between system elements.



*Cognitive System Controller (CSC)
Option 1: Part of Cognitive Antenna
Option 2: Part of Cognitive Radio
Option 3: Split between Antenna and Radio
Option 4: External to Antenna and Radio (depicted in diagram)

Figure 6.5. Cognitive System Controller Architecture Options

Candidate functions for inclusion in the CA Controller include the following:

- Evaluate suitability of requests/commands from radio (e.g., consider impact on S/C power consumption).
- Decide on something to learn / optimize.
- Execute learning algorithm(s).
- Coordinate with CR Controller.
- Assess antenna health.
- Compensate for poor antenna health.
- Manage use of available resources (e.g., maximum number of beams).

- Scan (direction and frequency space).
    - Identify signals (to connect to or avoid).
- Assess atmospheric environment (e.g., estimate whether there is rain fade).
- Memory.
- When to turn on interference mitigation techniques – technique selection, starting solution hypothesis, etc.
- Beam steering to maximize SINR for near angle interference.

Candidate functions for inclusion in the CR Controller include the following:

- Cross-system routing.
- Decide on something to learn / optimize.
- Execute learning algorithm(s).
- Coordinate with CA Controller.
- Assess radio health.
- Compensate for poor radio health.
- Manage assignment of available resources (e.g., map transceivers to beams).

The advantages and challenges of each CSC architecture option are summarized below in Table 6.5. The recommended architecture (marked by a * is to split the CA Controller and the CR Controller to keep each controller with its corresponding device. This recommendation is driven primarily by a desire to be as radio agnostic as possible for maximum compatibility for ease of operation with a wide range of cognitive radio instantiations. Additionally, this is the most intuitive option that avoids major separations between a controller and its device. Cognitive algorithms that utilize elements of both the CA and CR controller will need to account for any additional

challenges that arise by having to work through an external interface between the CA and CR controllers.

Table 6.5. Advantages/Challenges of Cognitive System Controller Architecture Options

Architecture	Advantages	Challenges
CSC Contained in CA	-Antenna functions located with antenna. -CA could be standalone terminal and save system SWAP assuming backend could provide modem and AWG capability. -Algorithms jointly optimizing radio and antenna parameters would have less overhead during runtime (both controllers on same processor).	-Radio functions separated from radio -Additional latency / overhead for radio commands to reach radio
CSC Contained in CR	-Radio functions located with radio. -Attractive when limited processing resources available at antenna. -Algorithms jointly optimizing radio and antenna parameters would have less overhead during runtime (both controllers on same processor).	-Antenna functions separated from antenna -Additional latency / overhead for antenna commands to reach antenna
*CSC Split Between CA and CR	-Antenna functions located with antenna -Radio functions located with radio. -Most intuitive option. -Allows ease of interoperability / modularity with replaceable CRs and their CR Controllers -CA Controller would be expected to provide introspection data to external CR hardware	-CA Controller and CR Controller are separated -Algorithms jointly optimizing antenna and radio parameters would have additional interconnection latency / overhead potentially increasing runtime -Leads to increased CA processing requirements
CSC External to Both CA and CR	-Allows flexibility for additional processing resource(s) for likely computationally intensive tasks. -Allows support for purpose-built processing resources (e.g., neuromorphic). -Algorithms jointly optimizing radio and antenna parameters would have less overhead during runtime (both controllers on same processor).	-Antenna functions separated from antenna -Radio functions separated from radio -Requires additional processing resource and hardware -Additional latency / overhead for both antenna and radio commands

A discriminating advantage for using this architectural approach is that it minimizes interconnection latency and overhead, which may potentially increase runtime, and enables the antenna and radio controllers to adjust and tune their own parameters exclusively. The CA controller would be expected to provide introspection data to external CR hardware and would allow for ease of interoperability and modularity with replaceable CRs and their respective CR controllers.

While a CA can have multiple independent beams, a CR can have multiple independent transceivers. Additionally, the sense/scan function will need its own receiver capability. Though not as complex as a full receiver, the sense receiver does require additional processing of the digital samples it receives from the antenna. Since sense/scan is an antenna function, this receiver is shown as being included as part of the CA. Nominally the Nth beam can be used for sense/scan. This capability is depicted in Figure 6.6. If the number of desire sense/scan beams exceeds the local resources on the CA, an available communications receiver can be re-programmed to provide this function.

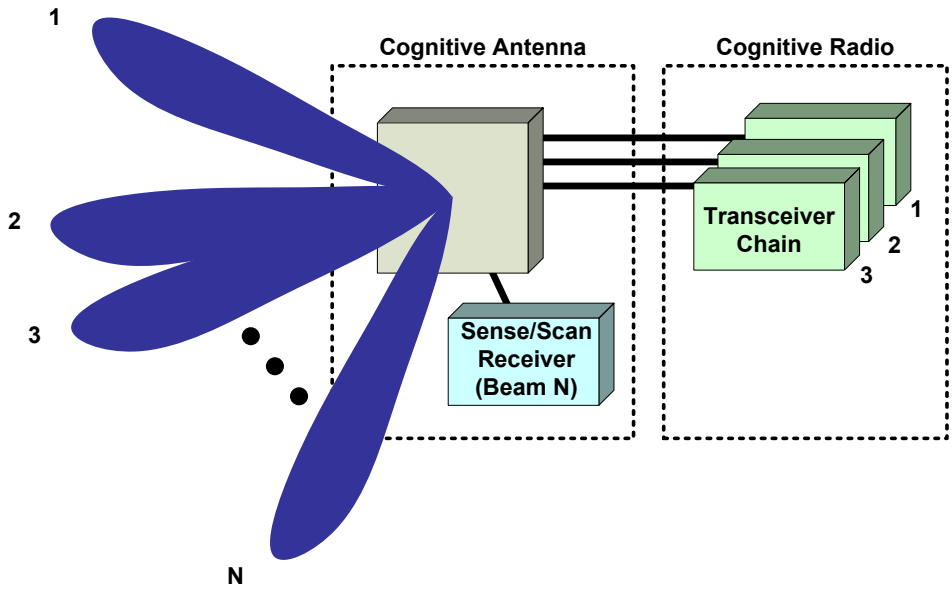


Figure 6.6. Cognitive Antenna with Multiple Beams Map to Multiple Transceiver Chains for Communications with One or More Beams Dedicated for Sensing and Scanning Functions

6.6 Antenna Functional Decomposition & Results

In this section, we will present the proposed antenna functional sequencing and the rationale for applying machine learning techniques to specific antenna functions for seamless space networks interoperability and compatibility. Figure 6.7 shows the system defined antenna functions as planning and design, operations and management, monitoring, security, and fault detection. Notably, the planning and design function will occur primarily prior to deployment of the CA system, as well as in subsequent cognitive model updates.

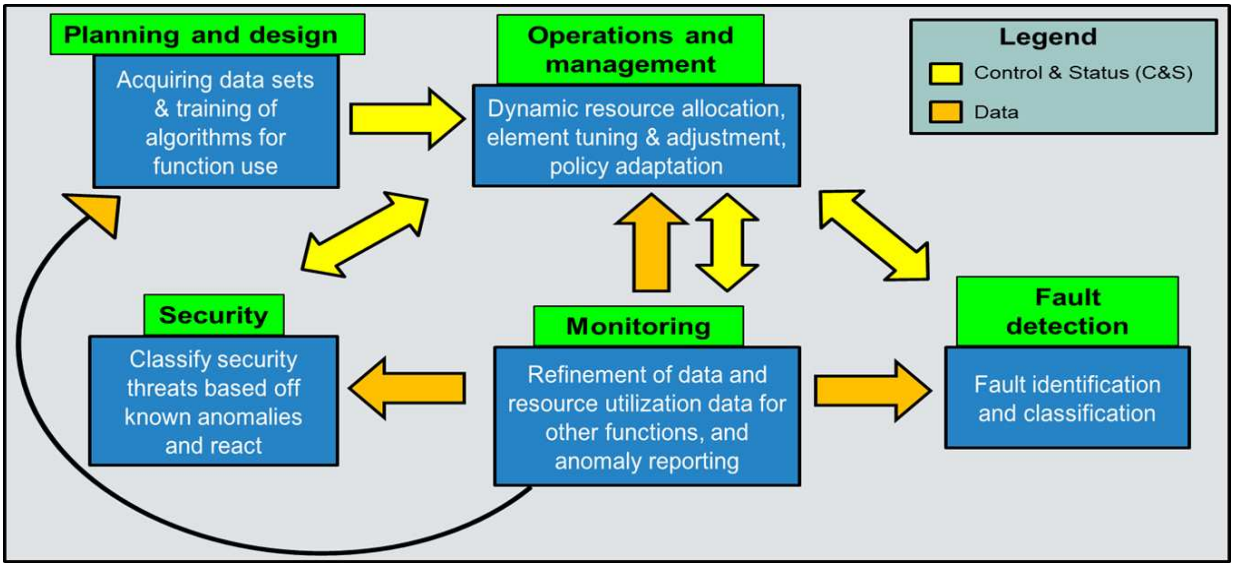


Figure 6.7. Antenna Function Sequence for Cognition

Using systems engineering best practices [60], a trade-off analysis was conducted to evaluate which machine learning techniques would be best suited for each antenna function given the problem each function needed to solve. As a mechanism for differentiating between alternative solutions, a set of quantifiable selection criteria was chosen that includes Data Set (size, nature, and quality), Accuracy, Available Computation Time, and Urgency of Task to be performed. For a given set of criteria, not all of them are equally important in determining the overall value of an alternative for each function. Such differences in importance are considered by assigning each criterion a weighting factor that magnifies the contribution of the most critical criteria. For the

purposes of this trade-off analysis, the subjective value method was implemented to apply a judgement of the relative utility of each criterion on a scale one through ten. This was derived specifically for the CA space application and may vary dependent on intended applications. The score assigned was then normalized using the linear maximization method for simple additive weight trade methodology in accordance with [61] using a benefit and cost criteria as shown in equations (6.6.1) and (6.6.2) respectively.

$$\text{Benefit Criteria: } n_{ij} = \frac{r_{ij}}{\text{rmax}} \qquad (6.6.1)$$

$$\text{Cost Criteria: } n_{ij} = 1 - \frac{r_{ij}}{\text{rmax}} \qquad (6.6.2)$$

By applying a normalization scheme, the total weighted score can be used to select the optimal candidate algorithm to implement for each antenna function within the CA system.

6.6.1 Planning & Design

The Planning and Design phase will be used to acquire data sets essential for training the algorithms for functional use. Additionally, unknown faults or anomalies that are reported from the Monitoring function during operations will be provided for manual assessment and can be folded back into this phase for future cognitive model updates. The anomaly analysis may also serve an automated data curation capability for continuous training in-situ, provided sufficient computational resources given the substantially greater computational cost of model training. Here, Operations and Management resource allocation (a future target for cognitive techniques) function determines when to train and how much data to train on given the Monitoring function's provisioning and labelling of data.

6.6.2 Operations & Management

The Operations and Management function requires some flavor of reinforcement learning (RL) for action selection and parameter turning where there is no known correct output [62]. As

an example use case, the CA must be capable of self-healing. To do this, it must support real-time operations by reconfiguring its beam pattern to optimize communications links, where algorithmic training is completed during the Planning and Design phase by using simulated element malfunctions. Additional live training may be enabled by the Monitoring function which can filter data for underrepresented scenarios and opportunities for improved operational function.

RL, despite its simplicity, is an effective algorithm in enhancing deep neural network policies, and RL with large, not clearly defined state space can utilize Deep Q Network or Deep Deterministic Policy Gradient (DDPG) algorithms and has been shown to attain human level performance using deep neural network function approximations to estimate the action-value function [63]. Another advanced algorithm is Neural Architecture Search (NAS) with RL which is a gradient-based method for optimizing architectures (e.g., neural network meta-parameters such as depth and layer size) and implements a reward signal computed from the policy gradient to update the recurrent network [64]. NAS with RL can determine the best model architecture to use, to make more accurate and timely decisions.

Some of the trade-off analysis considerations are the method for parameter selection for fine-grained beamforming, steering nulling, and self-healing, where the data available is assumed to be inputs from antenna elements and processed signals. Training is expected to occur in simulation, training, and during live operations. Also, the Available Computation Time refers to computational cost when running real-time using system resources, and Urgency of Task refers to the speed to select an action or set of parameters when running real-time. The weighting factor applied to the selection criteria was defined as 30% for Data Set, 30% for Accuracy, 20% for Available Computation Time, and 20% for Urgency of Task.

The results indicate a combination of DDPG with NAS should be the selected machine learning technique for the Operations and Management function. However, given that NAS produces a sufficiently optimized model architecture in pre-deployment training and is of higher computational cost, additional training in-situ should only use DDPG.

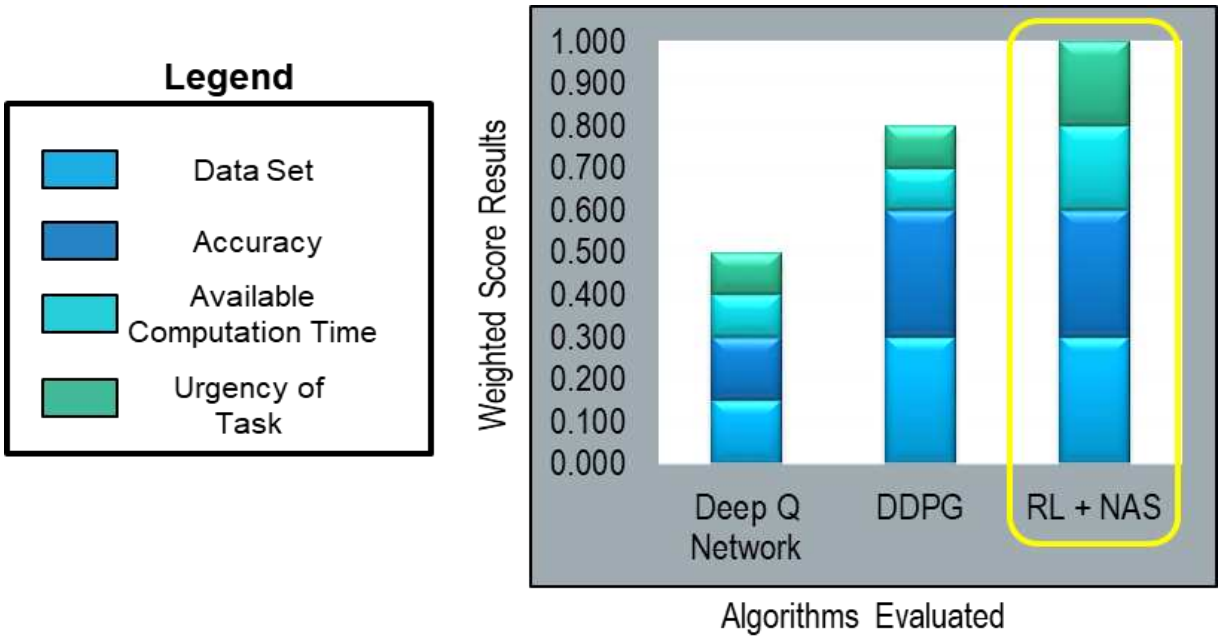


Figure 6.8. Operations & Management Results

6.6.3 Monitoring

The Monitoring function encapsulates the use of dimensionality reduction techniques to extract features to serve other functions and detects anomalies that may be used in future training and analysis. Dimensionality reduction transforms features based on relationships within the data set. For the CA, this transformation will be applied on data across spatially distributed elements and at multiple time scales. A key benefit is the removal of additive noise components from independently derived data measures. The Monitoring function data will contribute to Operations and Management, Security, Fault Detection, and unknown anomaly detection. Anomalies are identified as abnormalities, deviants, or outliers in the data observations. Algorithms considered for supporting this function are Principle Component Analysis (PCA), Independent Component

Analysis (ICA), and Multi-Scale Convolutional Recurrent Encoder-Decoder (MSCRED). The MSCRED performs anomaly detection and diagnosis in multivariate time series data, where it first constructs multi-scale (resolution) signature matrices to characterize multiple levels of the system statuses in different time steps. Subsequently, given the signature matrices, a convolutional encoder is employed to encode the inter-sensor (time series) correlations and an attention based Convolutional Long-Short Term Memory (ConvLSTM) network can be developed to capture the temporal patterns and serve as an input to the other functions. Based on the feature maps which encode the inter-sensor correlations and temporal information, a convolutional decoder is applied to reconstruct the input signature matrices and the residual signature matrices are further utilized to detect and diagnose anomalies [65].

The data available is assumed to be any signal data, environmental data, and resource data, where training is expected to use an initial data set required for defining the transformation of features. Some trade-off analysis considerations are that neural network approaches with large, but not at the scale of Big Data, training sets benefit from autoencoder feature extraction. Autoencoders, and related sequential encoder-decoders, represent data within multiple hidden layers, learning features by attempting to reconstruct the input data, effectively learning an identity function. Anomalies are rarely seen, and as such autoencoders fail to reconstruct them, producing a large reconstruction error. Thus, the data samples which produce high residual errors are considered outliers [66].

Available Computation Time & Urgency of Task for operations do not differ considerably within this trade space but may be dependent on the training data available. Non-linear relationships are highly likely given the environment, thus PCA would not provide a reliable feature set. The weighting factor applied to the selection criteria was defined as 30% for Data Set,

30% for Accuracy, 25% for Available Computation Time, and 15% for Urgency of Task totaling 100%.

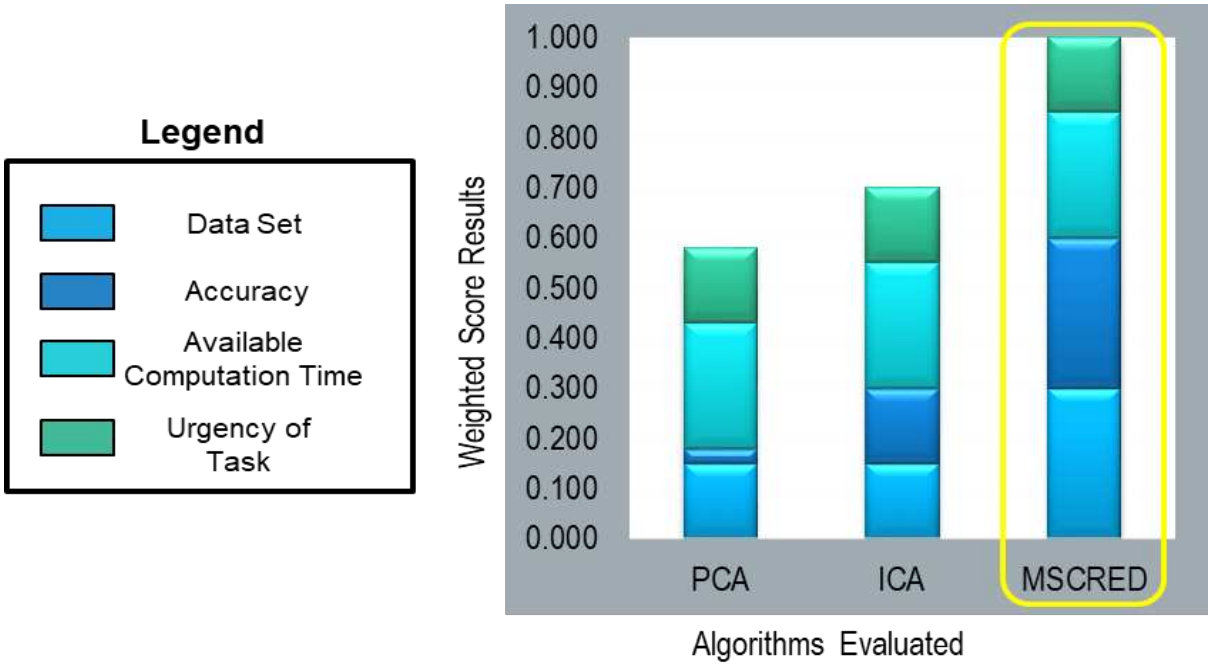


Figure 6.9. Monitoring Results

6.6.4 Security & Fault Detection

The Security function provides classification for known security threats to include an example use case of electronic warfare. Jamming attacks consist of radio signals maliciously emitted to disrupt legitimate communications. In this example, the machine learning algorithm can recognize adversary threats, enabling the CA to combat them by migrating the communications to a different frequency band that is interference free using dynamic spectrum access techniques and/or nulling the interferer. Interferers classified as intentional threats can be geolocated and reported to mission control. In order to train this algorithm, simulated adversarial narrowband and wideband interference sources could be used [67].

In addition to supporting electronic resiliency, this function classifies known threat behaviors for the system to support cyber resiliency, specifically continuous trust recognition of

the data and control interfaces. Security detections can be performed by relying on previously acquired knowledge of the communication behavior under normal and intrusion conditions and requires the tracking of potential indicators (or metrics) of intrusion activity. This emphasizes the importance of the Cognitive system architecture where information exchange between the CA and CR is critical to lessen intrusions. Here, the CA can receive data from the different layers e.g., packet delivery rate of the application layer or channel busy time at the MAC layer) to react to security impediments. Intrusion conditions can be developed specific to threats from an integrity team using simulations. Training would be handled with known intrusions at time of development of the CA system. Unknown intrusions may be caught by the Monitoring function's anomaly detection and used by the Security function as defined by security policy, and its associated data can further be leveraged for future training and improvement of security classifications.

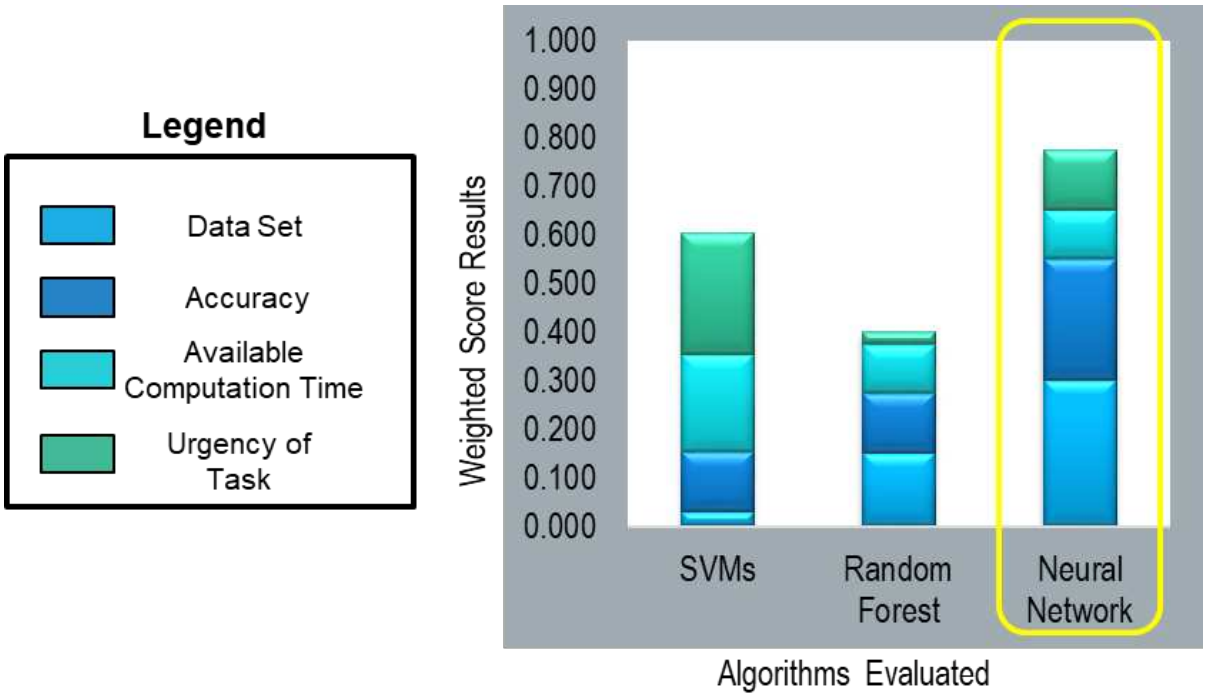


Figure 6.10. Security & Fault Detection Results

Some leading assumptions in this functional trade-off analysis is that we assume we have access to a general purpose unit (GPU) or Field Programmable Gate Arrays (FPGA) for methods

using matrix-heavy operations, and that we have a sufficiently large training data set to enable the classification of security intrusions. The weighting factor applied to the selection criteria was defined as 20% for Data Set, 25% for Accuracy, 25% for Available Computation Time, and 30% for Urgency of Task totaling 100%.

Like the Security function, the Fault Detection uses classification techniques for detecting and classifying faults [68]. Random Forest / Decision Trees provide the benefit of greater ease of interpretability of the basis of classification. However, provided sufficient training data and hardware, neural networks are likely to provide better performance in accuracy and speed, classifying faults for feedback into the Operations and Management function.

6.7 Cognitive Antenna Summary

In the mission and requirements definition phase, we described the Cognitive System requirements, and delineated the difference between a CR and a CA system. We also described a high-level problem space for the application of CA capabilities and described how these new capabilities differentiate a CA from currently existing antenna technologies. We also provided a justification for the use of a CA as enabling technology for improved resiliency and performance and determine what the system needs would be with respect to NASA's future missions as observed in the depicted Operational View. M&S&A was conducted to define fundamental required hardware architecture constraints to support the NASA mission use case. The needs analysis results indicate that there is a strong need for a CA to reliably support future space networks interoperability and compatibility.

An innovative concept of a wideband CA working in conjunction with emerging CR technology to learn from its experiences to overcome future space network challenges was presented. Varying levels of cognition using machine learning techniques were evaluated to enable

improved link performance, interference mitigation, and electronic/cyber resiliency, essential for the rapid expansion of S/C constellations and communications. Planning and Design would acquire data and train the functions for intended operations. Operations and Management would implement DDPG with NAS for robust, agile operations. Monitoring would use MSCRED to tailor the data for other functional use and to detect anomalies. Finally, both Security and Fault Detection functions would apply neural networks to classify known threats or systematic faults. With the growing complexity of current and future heterogeneous networks, more sophisticated learning algorithms like the recommendations presented should be applied to optimize system performance.

Chapter 7. Data Security for Space Communication Architectures

With an increase in demand for resilient space communication networks capable of supporting military and commercial users, securing the data in the network is vital, as well as minimizing the footprint on a said S/C. This chapter presents a survey of different S/C architecture designs that will provide protection at the core and consider the need for adaptability for aggregated users, flexibility, and interoperability for future space networks. The assessment will identify which security approach would be best selected in practice, given normal operations with no threats introduced, to protect the system data and data being transferred across the network. This work was published in the peer-reviewed ICSSC technical conference as noted [7].

7.1 Space Communications Architecture

Enforcing security policies in resilient space communication networks can be challenging in a SWAP power constrained environment. Users need to be permitted to access data at the proper sensitivity level only if authorized. An MLS architecture maintains security classification and compartment levels throughout the coordinated transfer and access of data. If all data is over classified (e.g., all data is at the highest classification within the system), the processing of data needs to be done only at the highest classification level which becomes inefficient as the number of security domains increase. In general, while there are data encryption and access control techniques that can be imposed to secure the network, these solutions grow in proportion to the number of sensitivity levels and supporting multiple sensitivity levels with minimal resources becomes untenable. The increasing demand for future space networks to be capable of supporting both military and commercial users solicit the implementation of security services and protections against conceivable attacks or vulnerabilities that also supports many simultaneous sensitivity levels.

Tremendous flexibility and economic benefits can be provided from distributed space systems since smaller and lighter satellites are cheaper to build, launch, and maintain. It can also result in a system, which hosts distinct applications that interact with each other using succinct paradigms for networking. S/C communications architectures have evolved over the years. Resilient networking amongst space constellations requires a strong emphasis on security, and therefore cannot afford security compromises with long-term effects on the system, and shared space systems are used by components that are extremely sensitive about their data and therefore require a strict security model.

S/C communications architecture consists of an on-board processor, a variety of subsystems, and one or more hosted payloads as illustrated in Figure 7.1.

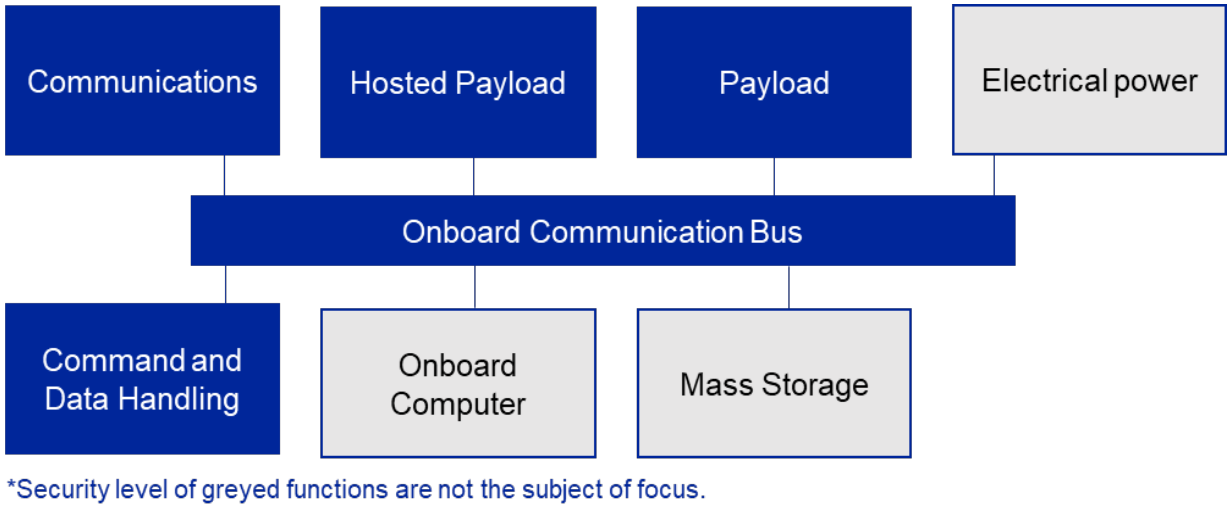


Figure 7.1. Notional Space Communications Architecture

The processor controls the operation of the satellite, including commands execution, attitude and orbit control, time synchronization, failure detection and recovery, and maintenance. The communications subsystem manages the bidirectional communication channel between the satellite and ground station, and the electric power subsystem controls the main power bus of the satellite. The data handling subsystem handles the data sent and received by the S/C via the

communications subsystem. The data handling subsystem receives incoming data for both the S/C platform and the payloads on the uplink where it decodes the commands and executes them if they are for the S/C platform. If they are not for the platform, then the subsystem will forward the data to the targeted payload for processing. The data handling subsystem also assembles both S/C data and payload data and transmits it to the ground segment on the downlink.

The typical threat identified for space networks is represented as two adversaries that communicate covertly, in violation of the system security policy, to leak information that is otherwise not available to unprivileged and/or unauthorized users. For Government hosted payload missions, the critical payload data are encrypted. However, protocol metadata, e.g., information in packet headers, are transmitted in the clear on the shared communications channels. Most attacks are performed on this type of data. Additionally, with the use of SpaceWire, which is a switched network with nodes connected via point-to-point links, each node may have one or more interfaces. In the context of the commercially hosted payload, the interfaces in a multi-interface node can operate at different sensitivity levels, and because of the direct connection between nodes, malicious disclosure between two adversaries attached to the same multi-interface node can be accomplished through shared resources in the shared node. With sophisticated encryption techniques, MLS architectures, and advancements in secure protocols, these cyber-attacks can be mitigated.

7.2 Security Policies

The overall organizational policy and objectives are not only individual employees or departments that are responsible for the security of confidential information, but also the institution itself that develops and uses the space communications system. It is, therefore, incumbent for top administrators who protect the institution's best interest to ensure that an appropriate and effective

security policy is developed and put into practice through the organization by using the Defense-In-Depth Methodology.

Security policy refers to clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an organization's system and the information included in it. Good policy protects not only information and systems, but also individual employees and the organization as a whole. It also serves as a prominent statement to the attackers about the commitment of the organization to security. Three specific items for a security policy that is used to implement the organizational policy and objectives are as follows:

1) Identify sensitive information and critical systems.
2) Define institutional security goals and objectives.
3) Ensure that necessary mechanisms for accomplishing the goals and objectives are in place.

Broadly, speaking, defense-in-depth use cases can be broken down into user protection scenarios and network security scenarios. For example, one use case is website protection. Defense-in-depth involves a combination of security offerings (e.g., antivirus, antispam software, etc.) and training to block threats and protect critical data. A vendor providing software to protect end-user from cyberattacks can bundle multiple security offerings in the same product. For example, packing together antivirus, firewall, anti-spam and privacy controls. Because of this security protection, the user or developer's network is secured against malware, web application attacks, and more. Another use case is network security, where the developer's organization sets up a firewall, and in addition, encrypts data flowing through the network, and encrypts data at rest. Even if attackers get past the firewall and steal data, the data is encrypted. In this case, an organization sets up a firewall, runs an Intrusion Protection System (IPS) with trained security operators, and deploys an antivirus program. This provides three layers of security, even if attackers can get beyond the

firewall, they can be detected and stopped by the IPS. In addition, the last use case is using the space communications system to transfer data between source and destination nodes. Here, data security needs to be applied. Data security includes database monitoring, data masking and vulnerability detection. Data security architectures are further described in Section 6.5.

7.3 Governance

The space domain is largely ungoverned, as one cannot visualize it directly; however, there are key areas of space governance that should be explored to understand international perspectives on ongoing debates in the field, such as space debris mitigation and sustainability efforts, rendezvous and proximity operations, and insurance for space launch and satellites on orbit. As an immediate example, the best developed governance in these areas is space sustainability and debris mitigation efforts. An indiscriminate issue for the space domain, space debris is a growing problem with almost every launch. Many space experts acknowledge that without norms of behaviour or debris removal missions, the space environment may be permanently damaged and become cluttered. There are several international mechanisms, national policies, multinational activities and industry efforts to curb the creation and proliferation of space debris. Several guidelines have been published that suggest best practices for operating in the space domain in a sustainable manner, as such there is a commonly practiced 25-year deorbit norm for out-of-date technology or commercial satellites. Understanding where objects are in space and projecting their orbital path is a cornerstone of developing a robust secure space environment that encourages economic activity, global space debris mitigation regulations and sustainability requirements.

Figure 7.2 shows the interactions between satellite operators, international organizations and analysis communities, international standards development organizations, satellite operator associations, and national regulatory bodies that are organizationally needed to implement strategy

in general. The organizational roles and contributions each makes towards the long-term sustainability of the space environment is very important.

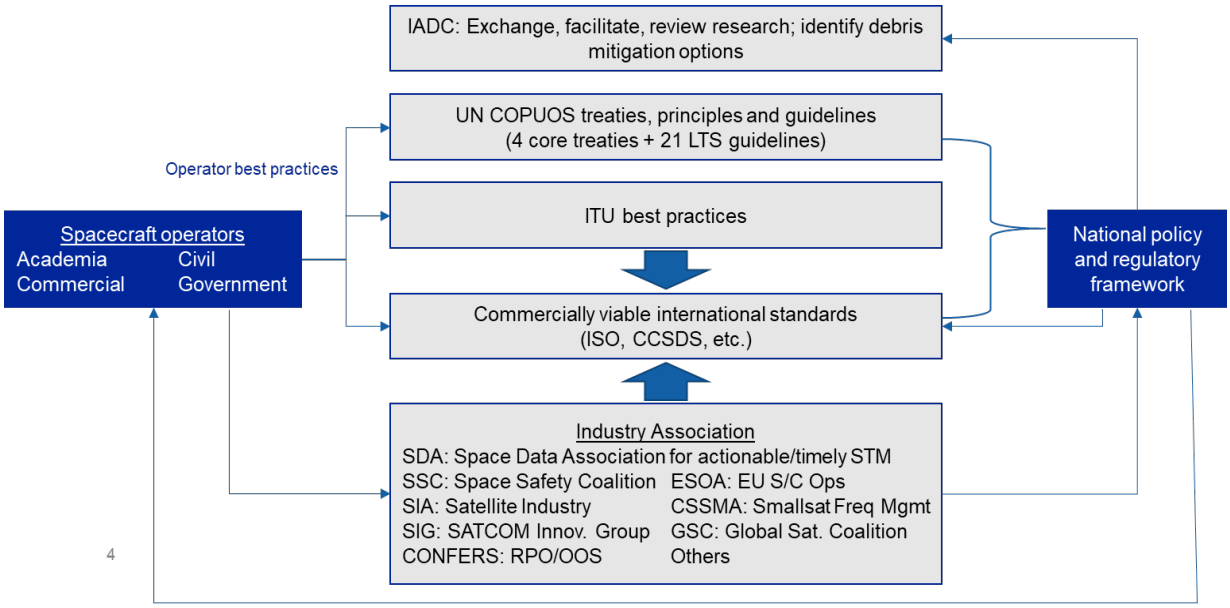


Figure 7.2. Organizational Interaction of Global Space Debris Mitigation Activities

Here, IADC refers to Inter-agency debris coordination committee, UN COPUOS is the United Nations Committee for the Peaceful Use of Outer Space, ITU is the International Telecommunications Union, ISO is the International Standards Organization, and CCSDS is the Consultative Committee for Space Data Standards. Metrics should be captured to assess governance effectiveness of space systems; examples are the number of application vulnerabilities over the year, percentage of spacecraft communication link downtime during active hours deployed, cost to mitigate or apply countermeasure for security vulnerability.

7.4 Cybersecurity Requirements

Cybersecurity requirements are often country, and even mission specific. In the U.S. DoD space-based National Security Systems (NSS) that include systems using commercial space platforms to host NSS-payloads have cybersecurity requirements defined in CNSS Instruction No. 1200 (National Information Assurance Instruction for Space Systems Used to Support National

Security Missions) [69]. The requirement categories are segregated into several focus areas, cross domain solutions (CDS), separation of payload mission data from the host platform, payload command and control (C2) data processing, and information exchange between host platform and the payloads space and ground segments.

A S/C with payloads operating at different sensitivity levels must meet the information assurance security controls specified in the Space Platform Overlay [70] and Cross Domain Solution Overlay [71]. The Space Platform Overlay mitigates the risk related to unmanned space platforms in the space segment of national security space systems, and the CDS Overlay implements measures to protect systems that provide access to and/or transfer of data between different security domains. These requirements are essential when multiple payloads with various sensitivity levels are commercially hosted payloads, and the MLS architectures provide resource savings.

7.5 Security Architecture Approaches

In this section, we compare two different security architecture approaches outside of what is presented in [72] and [73]. For the purposes of the comparison, it is assumed that each payload hosts an application and/or produces data of a unique security levels or caveats. Each payload is a distinct security domain. One architectural approach is shown in Figure 7.3 where the security enforcing components are contained within a centrally located security perimeter. We term this the centralized approach. In the second approach, as shown in Figure 7.4, each payload individual contains the security features necessary for that payload. For example, if there is a payload that requires data encryption, the encryption algorithm and management of keys for the algorithm are contained within the payload boundary and only protected data is transmitted onto the shared on-

board communications bus. There is common approach to the separation of system payload control, or configuration information, and the traffic data within the on-board communication bus.

In the centralized approach, security functions and a CDS are centralized. The CDS enforces the Bell-LaPadula security model [74] for information exchange between security domains, so if it is necessary to share data between security domains, a cross-domain guard function is invoked to ensure data with allowable sensitivity levels is shared. The encryption and decryption algorithms, key management are contained within centralized boundary. The advantage to this approach is that security certification activities focus on this portion of the architecture. The key management functions including filling, loading, protections and zeroization are consistent. Various key types, keys lengths, the over air re-keying are handed in a uniform manner. The centralized system needs may need to implement different algorithms as required by the payload, must provide adequate encryption/decryption data rates and key agility for each algorithm. A disadvantage of this approach is when an algorithm specific to one of the payloads needs to change; the centralized cryptographic subsystem may also need to be updated. To avoid this type of coupling, a distributed security architecture is an alternative architecture.

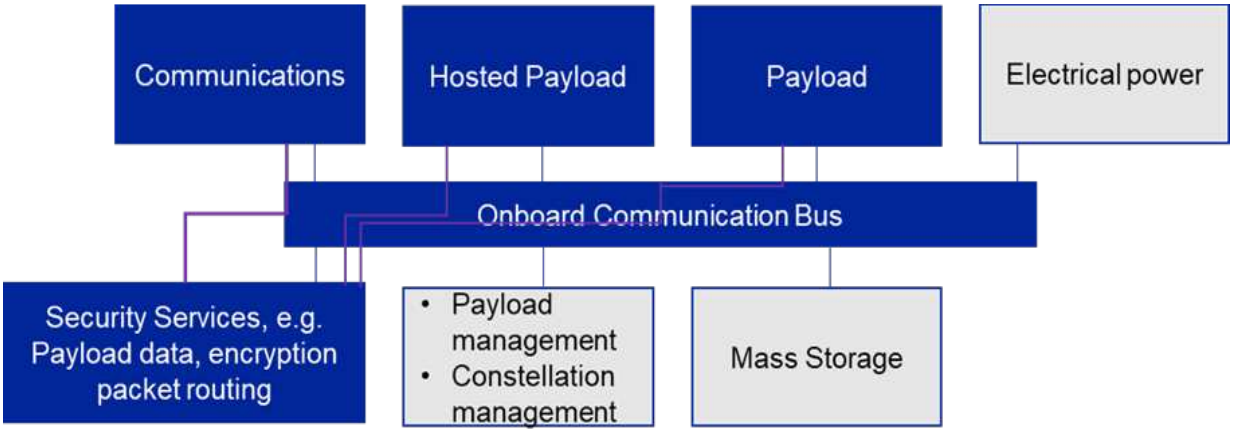


Figure 7.3. Space Communications Architecture with Centralized Security Services

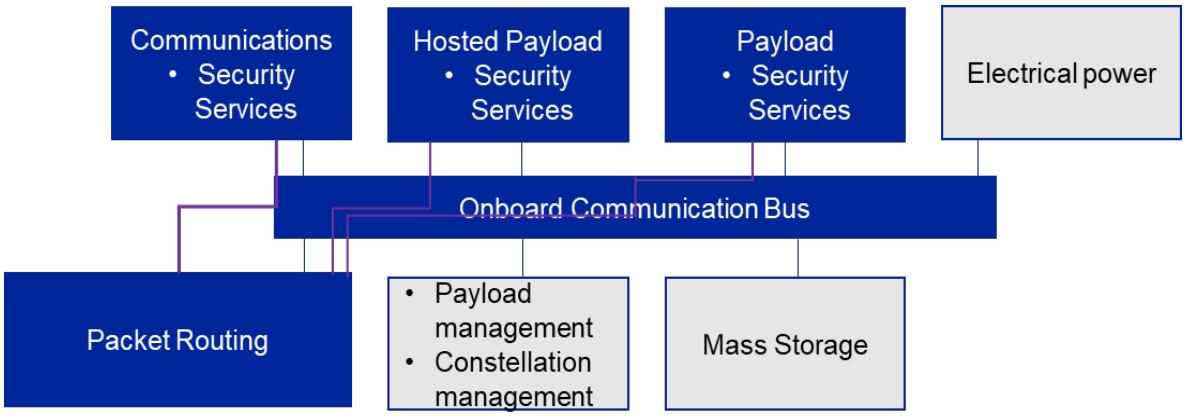


Figure 7.4. Space Communications Architecture with Distributed Security Services

A high-level assessment was conducted to determine the optimal MLS architecture solution for an example space communications system. As with any trade assessment, the weighting of each evaluation criteria is subjective, and may change the outcome of the trade if different weighting were selected. Here we evaluated both the centralized and distributed MLS architectures against the ease at which on-board sharing of data could occur, the independence of the payloads from the security services, and the certification commonality for this future space architecture with diverse commercially hosted payloads. The results for this trade indicate that the centralized approach was the optimum choice for the overall data security strategy; however, other factors such as on the selected mission of operation and timeline for implementation make either approach an acceptable option.

Table 7.1. Example MLS Architecture Comparison Results

Item	Evaluation Criteria	Scoring Function	Weight	Centralized MLS Approach		Distributed MLS Approach	
				Score	Weighted Score	Score	Weighted Score
1	On-board Sharing of Data	10 = Good 5 = Medium 1 = Poor	30%	10	3.0	5	1.5
2	Independence of Payloads		20%	10	2.0	10	2.0
3	Certification Commonality		50%	10	5.0	1	0.5
Total			100%		10		4

7.6 MLS for Space Communications Architectures Summary

The ability to develop space systems to accommodate MLS with state-of-the art technology is available, the drawback being the amount of time it may take to certify and accredit such a system. This chapter presented two divergent approaches for an MLS architecture for space networks, centralized and distributed MLS frameworks. Technically, both approaches are an acceptable method for securing the data in the network for military and commercial end users; however, dependent on S/C constraints, subject communication relays, and the operational mission to be performed, one may be more advantageous over the other. Further, the mission architect for space network solutions needs weigh the cybersecurity and architectural approaches to implement a holistic approach ensuring classification requirements for data security across all levels are handled appropriately and effectively.

Chapter 8. Cybersecurity Controls for Space Cognitive Systems

As discussed in the preceding chapter, distributed and centralized architectures can be used to protect data in general under benign conditions. When systems encounter cybersecurity threats, particularly, advanced ones, AI strategies should be employed within the communications system. This section will describe machine learning algorithms that can be applied to combat advanced persistent threats for future space cognitive systems. This work was published in the prestigious IEEE peer-reviewed technical conference as noted in [8].

8.1 Background

Cybersecurity controls play a crucial role in protecting prospective NASA Cognitive Systems (CS) operating at LEO intended to provide enhanced network connectivity and increased performance through complementary interference mitigation and link optimization capabilities. The CS will reside at LEO acting as a relay node between various resources, to include Commercial and DoD space networks, and will distribute both science and telemetry data from the ISS to NASA NEN ground nodes, other satellite nodes, and TDRS. The CS consists of both a CA and CR technology, where a CA is an environmentally aware antenna that can dynamically allocate bandwidth and/or adapt its beam direction and directivity, EIRP, provide beam nulling to optimize spectral, spatial, and temporal resources to complement the CR technology (as described in Chapter 6). For context, an example mission thread for interference mitigation using the CS is represented in Figure 6.1 to signify the importance of its use and innovation offerings where the ISS transmits science data to the CS system residing on a LEO for forwarding data to the NASA NEN Gateway. Here, the CS receives ISS science data with sufficient link margin for healthy communications. An interferer then begins transmitting on the same Rx channel / Rx beam, thereby disrupting the communications and impairing NASA data collection efforts. The CS system by design can sense

and characterize the interference and optimize the antenna parameters for the communications link while providing beam nulling in the direction of the interferer. In doing this, the CS system can learn to implement the desired configuration for future flybys of interferers. The result of this automated machine learning process enables NASA to experience improved science data collection rates during its mission of execution. The CS primary system users are noted as NASA scientists and astronauts. In addition, it is envisioned that the CS will be able to serve as a surrogate satellite relay node for Government information transfer because it will be able to adapt to potential adversarial jammers and interferers.

Enforcing security policies in resilient space communication networks can be challenging where users need to be permitted to access data at the proper sensitivity level only if authorized. In general, while there are data encryption and access control techniques that can be imposed to secure the network, these solutions grow in proportion to the number of sensitivity levels and supporting multiple sensitivity levels with minimal resources becomes indefensible. The surging call for future space networks to be capable of supporting both military and commercial users solicit the implementation of sophisticated security services and protections against credible attacks or vulnerabilities that also supports many simultaneous sensitivity levels. This section will provide a background on the vital need for cybersecurity controls and protective measures for LEO CS systems based on known cyber-attacks, threat plan and mitigations against APT-attacks, and recommended machine learning techniques to be used to mitigate any vulnerabilities or possible attacks.

Recently, space vehicles and systems have become targets of cyber-attacks. This issue has worsened with the emergent thrust for military system payloads to be able access space networks at reduced costs by hosting Government-supplied payloads on commercial space platforms. The

commercially hosted payloads will require arduous security protections and MLS encryption to protect against information leakage on a S/C with MLS capabilities. A 2011 report to the United States Congress discusses several suspicious cyber events that interfered with (2) two Government earth observation satellites in 2007 and 2008, where the U.S. Geological Survey and National Aeronautics and Space Administration offices confirmed the attacks on the Landsat-7 and Terra EOS AM-1 satellites in [75] respectively. In [76], an American cybersecurity firm reported several key findings of APT attacks performed by one of the largest APT organizations on a broad range of victims for lengthy durations, starting from 2006, by maintaining an extensive infrastructure of computers across the world. While there have been various known attacks, hosting Government payloads on commercial LEO S/C can provide flexibility and costs savings. However, the security ramifications associated with the management of the satellite's shared resources with the satellite bus and payload owners requires additional scrutiny and certification of which can be provisioned by a mission systems satellite security architecture and its underlining enterprise security architecture.

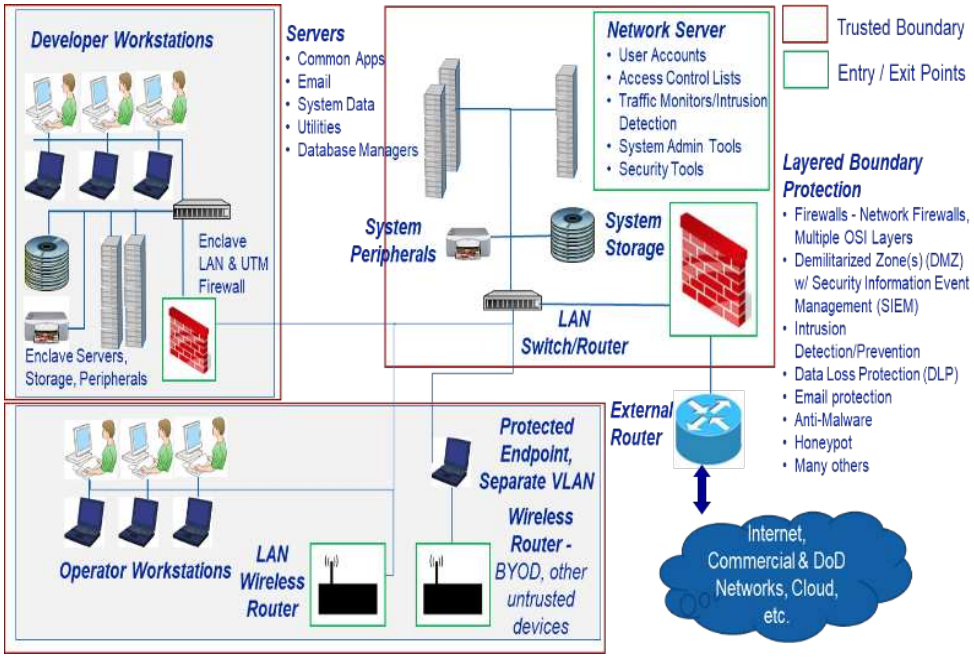


Figure 8.1. Cognitive System Enterprise Architecture

Figure 8.1 shows a notional LEO CS enterprise architecture. This architecture representation is an example of how complex the systems, interactions, and device selections can be. The corresponding infrastructure plays a significant role in safeguarding the development, deployment, and operational use of the space-based system. Possible entry and exit points for an intruder / attacker are noted in "green" at the Developer Workstations, Operator Workstations, and Network Workstations through the established routers and firewalls, and one or more trusted boundaries are indicated in "red" as clearly partitioned enclaves based on functional need. Within the deployed system that resides in the cloud-based network, consists of an on-board processor supporting cognition functions (e.g., CA or CR) of the CS, a variety of subsystems, and one or more hosted payloads.

The on-board processor controls the operation of the satellite, including commands execution, attitude and orbit control, time synchronization, failure detection and recovery, and maintenance, in addition to utilities such as self-healing and antenna control. The communications subsystem manages the bidirectional communication channel between the satellite and ground station, and the electric power subsystem controls the main power bus of the satellite. The data handling subsystem has a large role, as it receives incoming data for both the S/C platform and the payloads on the uplink where it decodes the commands. If the commands are not for the platform, then the subsystem will forward the data to the targeted payload for processing. The data handling subsystem also accumulates both S/C data and payload data and transmits it to the ground segment on the downlink.

8.2 Abuse Case Description

Threat actors can execute a well-planned cyber-attack. The lifecycle stages of such an attack are described below, and most notably, upon completion of *stage 3*, the LEO CS system would be considered compromised.

1) Intelligence gathering – Refers to information collection on the intended target, network, data, teams and departments to determine security weaknesses.
2) Points of Entry – Refers to intruder entry points into the system that enable access; this is commonly performed with spear phishing that inserts malware or infected files.
3) Command and Control (C2) – Namely refers to a point in the threat execution plan where a hacker gains control of the machines, networks, and system under attack.
4) Lateral Movement – Accomplished once the hacker has gained control and can freely move within the network and hide his or her malevolent activities.
5) Maintenance – The process where a hacker creates a new backdoor, servers, malicious "patches" to create or exploit vulnerabilities of the system.
6) Data Exfiltration – Refers to the process in which sensitive information is retrieved.

A calculated attack can be performed from threat actors that seek the underlining information or processes that the LEO CS utilizes. Three specific threat actors are identified and include the insider threat, hackers, and APT. An insider threat with access to the developer system can be install malicious software (e.g., malware) locally on the system prior to the deployment of the CS system. This, by far, is the most dangerous threat category as the individuals are trusted and have access to sensitive system content. Hackers or individual criminals also are a natural threat, where their motivations may range from thrill seekers to financial gain for information mined from DoD secure network systems. For example, a hacker could be considered when two

adversaries communicate covertly, in violation of the system security policy, to leak information that is else not available to unauthorized users. For Government-hosted payload missions, the critical payload data are encrypted. However, protocol metadata, e.g., information in packet headers, are transmitted in the clear on the shared communications channels. Most cyber-attacks are performed on this type of data, but with encryption algorithms and/or cross domain solutions implemented within the S/C communications architectures, and advancements in security countermeasures, these cyber-attacks can be alleviated.

Lastly, APT are more modern threats that use continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period, with potentially destructive consequences. This is typically a threat for high value targets, such as large corporations or national state sensitive information, with the goal of stealing information over a long period, rather than simply executing a fast attack and leaving with small amounts of information [77]. APT-attacks involve gathering information usually through social engineering methods, reconnaissance performed at site facilities, port scanning, and service scanning, which refers to psychological influence of people into realizing goals that may or may not be in the targets best interest [78]. Accurate detection and prediction of APT has been an ongoing challenge, where with the introduction of the CS system, innovative machine learning algorithms can be used in the ***security*** function, mainly continuous trust recognition of the data and control interfaces leveraging optimized machine learning algorithms, to combat these [79].

Here forward, we will focus on the APT-attack and what methods can be used for detecting, identifying, and classifying an attack in LEO CS systems such that it can be effectively combated and therefore safeguard all critical information. Critical information refers to sensitive information, processes, and other content that would require protection. This includes commercial company or

DoD data, geographic locations of strategic military personnel or troops, and advanced methods or machine learning processes, such as those used to detect, identify and adapt the CS system to offer self-healing capability to keep the serviced system available for operational use should be protected against threats.

8.3 Machine Learning Survey

Traditional Intrusion Detection Systems (IDS) have known limitations, where they require processing large quantities of audit data, making it both computationally expensive and error-proned. This supports the initiative for finding alternative automated approaches to suspicious or irregular pattern recognition for better analysis and predictions of an APT-attack. As described in [80], an APT-attack can be detected through the identification of anomalous network traffic by using machine-learning methods of C5.0 decision tree, Bayesian network, and deep learning for detecting and classifying the APT-attack on the NSL-KDD data set (includes 148,517 samples where 90% of samples were used for training and 10% for testing). Experiments were run using criterion of false positive rate, sensitivity, specificity, accuracy, false-negative rate, and F-measure where preliminary results using the confusion matrix evaluation method showed that deep learning methods with automatic multi-layer extraction of features has the best performance for timely detection of an APT-attack in comparison to other classification methods. Additionally, in [81], APT-attacks and countermeasures for future networks and communications are described, where modelling phases of typical steps in APT attacks to collect the desired information by attackers is proposed. [82] indicates that with the rate at which attack tools are evolving, existing security measures are inadequate and require solutions that include fine-grained behavior analysis of users and systems within and across networks that allow the detection of intrusions at different stages of APT attacks; this can be accomplished with monitoring tools and mitigation methods. In [83], a

machine learning based system, referred to as MLAPT, is suggested to rapidly detect and predict APT attacks systematically. In this work, the MLAPT executes three main phases, (1) threat detection, (2) alert correlation, and (3) attack prediction based on the correlation framework output. The MLAPT when applied to experiments was able to predict an APT-attack with an accuracy of approximately 85% in its early phases. Furthermore, in [84], APT-attacks are cited to use encrypted connections that mimic normal behaviors in order to evade detections, but an approach to analyze high volumes of network traffic to distinguish weak signals related to data exfiltration is advocated. To that end, it is not sufficient to search for a malicious traffic, but rather an understanding of the state of the system is required. For example, it may be possible to classify attacks or types of system state changes that may occur because of the influence of an attacker; however, this is hindered by the dimensionality of the data when the state is considered. As evidenced in these investigative works, APT-attacks are real and challenging to mitigate; however, some machine learning algorithms have been shown to aid in the early detection, identification and classification of an APT-attack for abuse cases for heterogeneous networks.

8.4 Trade-Off Analysis & Results

A disciplined trade-off analysis was performed to evaluate which machine learning techniques would be best suited for a LEO CS to use for early detection and classification of an APT-attack. There are three main categories of machine learning which include supervised learning, unsupervised learning and reinforcement learning. In the supervised learning, each data point is associated with a label, which assists in supporting predictions about future data points. In unsupervised learning, the data points have no labels, but instead the algorithm attempts to organize the data in some structured manner to enable interpretation of complex data in a simpler way. Lastly, in reinforcement learning, the algorithm is able to choose an action in response to

each data point, and a reward is assigned for indicating how good the decision was. This allows the algorithm to modify its strategy to achieve the highest reward [85].

In the trade-off analysis completed, the selection criteria used to determine the best algorithm were Accuracy, Training time, Linearity, Number of parameters, and Number of features. For a given set of criteria, not all of them are equally important in determining the overall value of an alternative algorithm, and differences in importance were considered by assigning a weighting factor for each criterion that magnified the contribution of the most critical criteria. In machine learning, *Accuracy* is the measurement of how effective the trained model is for all cases. For example, acquiring the most accurate answer may not always be necessary, where obtaining an approximation may be more than adequate dependent on the use case, and it would allow one to reduce the total processing time. *Training time* refers to the length of time required to train a model; this could vary significantly between algorithms and often goes hand in hand with accuracy. In supervised learning for example, training means using historical data to build a high-fidelity model that minimized errors. Once the model has been trained, it can be used to make predictions on new data. *Linearity* is also used as a criterion in the trade-off analysis, where if a linear relationship exists between a variable and a constant in the data set exists the data trends follow a straight line. Linear algorithms are known to reduce accuracy because large errors can occur between the actual and linear trend lines drawn from the data used, but they are straightforward and fast to train which enables rapid decision-making. The *Number of Parameters* denotes the available dials that can be turned when setting up the algorithm. There may be a number of parameters that affect the behaviour of the algorithm, such as error tolerance or number of interactions. While it is, a good method to ensure your algorithm spans the full parameter space due to increased flexibility, the time required to train a model increases exponentially with the

number of parameters. The *Number of Features* can be very large compared to the number of samples of the data set and may significantly slow down learning algorithms making the training time intolerably long.

Table 8.1 provides a comparison of the raw data score for different machine learning algorithm options against the selection criteria used in this trade-off analysis. Here, the subjective value method was implemented to apply a judgement of the relative utility of each criterion on a scale one through ten, where one is the lowest score, five is an acceptable average score, and ten is the highest, best score that could be received.

Table 8.1. Selection Criteria vs. Machine Learning Algorithms Raw Data

Selection Criteria	SVM	GA	FL	GNB	DT	NN
Accuracy	5.0	10.0	5.0	5.0	5.0	10.0
Training Time	5.0	1.0	5.0	10.0	5.0	1.0
Linearity	1.0	5.0	1.0	1.0	10.0	10.0
Number of Parameters	5.0	10.0	10.0	10.0	1.0	10.0
Number of Features	10.0	10.0	10.0	10.0	5.0	10.0

The total weighted score can be used to select the optimal candidate algorithm to implement for early detection and classification of an APT-attack as shown in Figure 8.2. Algorithms such as Support Vector Machine (SVM), Genetic Algorithms (GA), Fuzzy Logics (FL), Gaussian Naïve Bayes (GNB), Decision Trees (DT), and Neural Networks (NN) were evaluated as a potential solution focusing primarily on network intrusion detection. The weighting factor applied to the selection criteria was defined as 25% for Accuracy, 15% for Training Time, 20% for Linearity, 20% for Number of Parameters, and 20% for Number of Features. With next generation sensors and communications systems, collecting and distributing greater amounts of

data is required to support the urgent transfer of information at increased data rates, and at longer ranges for varying missions. To that end, the unmanned space-based CS needs to balance intelligence and processing capability with available platform SWAP. This very fact makes the selection criterion of *Accuracy* a higher weighted factor in this trade.

Figure 8.2. Machine Learning Algorithms Best Suited for Mitigating APT-Attacks

The trade-off analysis results yield that the selection of neural networks would be the favoured algorithm for use to detect, identify and classify APT-attacks. The traditional neural network definition suggests that it is an interconnected assembly of simple processing elements, units or nodes, whose functionality is based on the instinctive neuron, where the processing ability of the network (actions and reactions) is stored in the weights obtained from adapting or learning from a set of training patterns. As indicated in [86], neural networks are used for statistical analysis and data modelling, in which they play a large role in cluster analysis techniques, which are used to solve problems in the domains of classification or forecasting. [87] also implies that neural

networks are an effective method to use in the detection of network intrusions due to their ability to learn and adapt to new data quickly. Applying neural networks to remotely operated, space-based CS to uniquely categorize pattern variances and irregularities from normal traffic when meritoriously trained on known attacks and entity features, could be beneficial to not only maintain continuous communication coverage for network survivability, but could enable system learning for predicting unknown, more advanced machine-based malicious attacks.

Modelling and simulation was performed using the Knowledge Discovery and Data Mining (KDD) Cup 1999 Classification Model and associated data set [88] on several of the machine learning algorithms, e.g., NN, DT, and GNB, as a mechanism to evaluate the validity of the scoring for both *Training Time* and *Number of Parameters* as a subset of the trade space. For a point of comparison, training and cross-validation learning curves were computed to model the learning performance over experience or time. Learning curves are investigative tools typically used to assess how one algorithm learns from a selected training data set incrementally and plays a significant role in larger network topologies to understand the potential performance impacts of learning given the vast number of parameter options and nodes within the network. Figure 8.3 through Figure 8.5 provide training and cross-validation score curves. This allows one to determine if applying more training data would improve the algorithmic performance long term, or if the model itself is too simplistic. Here, multilayer perceptron (MLP) NN with a sigmoid classier and Rectified Linear Unit (ReLU) activation function were used for the NN model, the DT model used the Gini impurity to measure the quality of the split (over entropy and classification error), and the GNB model measured the likelihood of features that were assumed to be Gaussian. The results presented are consistent with the subjective scores identified in Table 8.1 for the *Training Time*

and *Number of Parameters*, which provide a high-level of confidence in the overall trade-off analysis results documented in Figure 8.2.

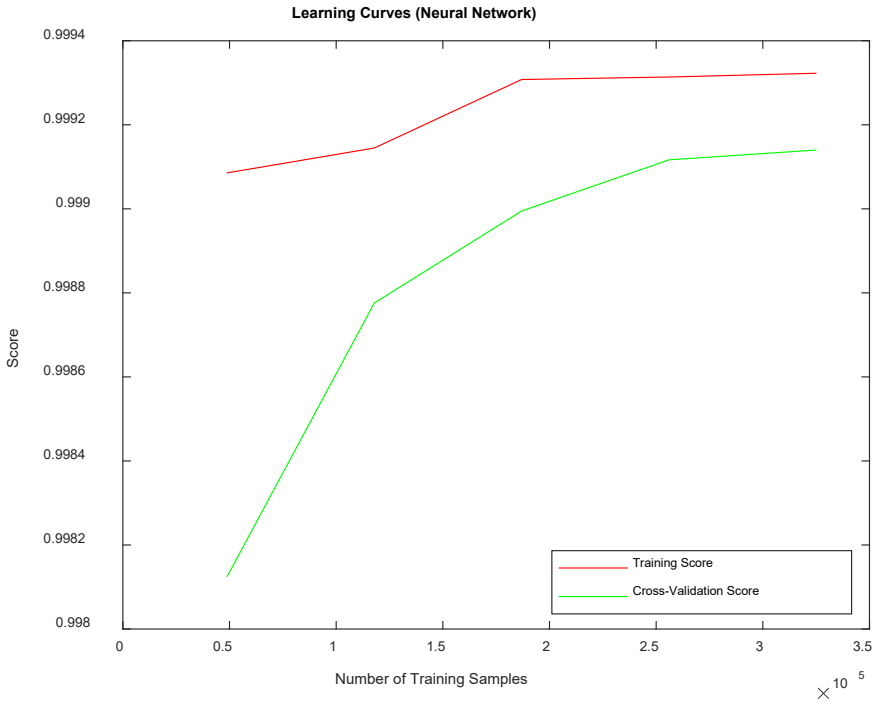


Figure 8.3. Learning Curves of NN with KDD Cup 1999 Data

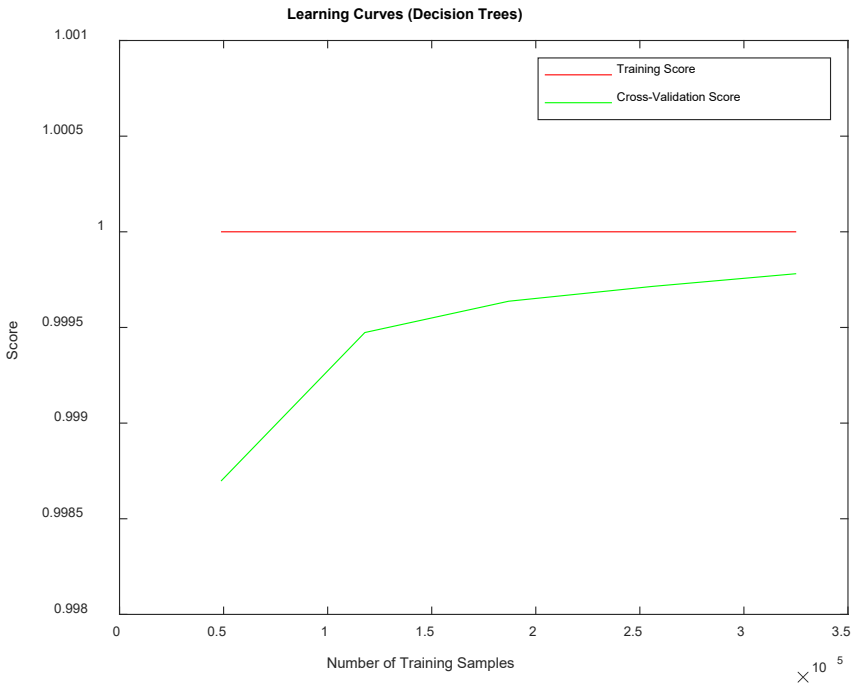


Figure 8.4. Learning Curves of DT with KDD Cup 1999 Data

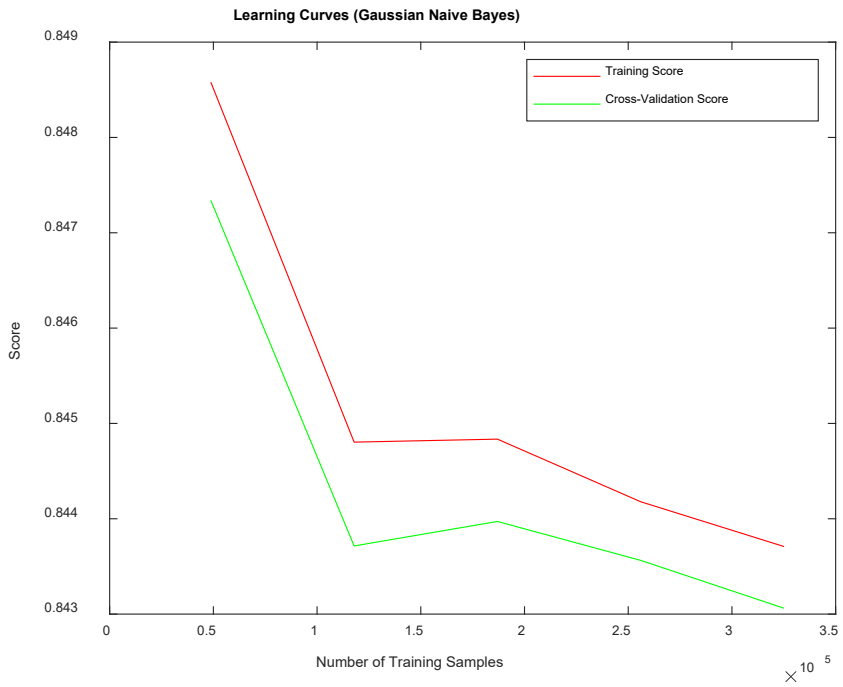


Figure 8.5. Learning Curves of GNB with KDD Cup 1999 Data

In addition, a validation curve is a great diagnostic tool for discovering worthy hyper parameter settings to be used for effective machine learning algorithm performance improvements. For example, some hyper parameters such as the number of neurons in a NN, maximum tree depth in a DT, amount of regularization, etc., control the complexity of the model. We would like the model to be multifaceted to capture anomalies, e.g., APT-attacks or detection intrusions, using the training data, but not too complex to avoid overfitting. The KDD Cup 1999 Classification model and data set was used primarily for this analysis since the database contains a wide variety of intrusions simulated in a military network environment. It consists of approximately 4,900,000 single connection vectors each of which contain 41 features and is labeled as either normal or an attack with exactly one specific attack type and is helpful in understanding if a machine learning algorithm applied to this data set could overcome the weakness of signature-based intrusion detection systems in detecting attacks. There are some inherent problems in the KDD Cup 1999 data set but is widely used because it is one of the few publicly available data sets for network-

based anomaly detection systems. The first important deficiency in the KDD data set is the huge number of redundant records. Analyzing KDD training and test sets, it was found that about 78% and 75% of the records are duplicated in the training and test sets respectively. This large amount of redundant records in the training set will cause learning algorithms to be biased towards the more frequent records, and will prevent the machine learning algorithm from learning un-frequent records which are usually more harmful to networks such as zero-day (0-day) attacks. There are new data sets publicly available that may be better to use in this evaluation which include NSL-KDD [89], ADFA-WD [90], ADFA-LD, CICIDS2017, or Bot-IoT data sets; however, application to military network environment is unclear. Future work will develop several validation curves for NN and will investigate a combination of machine learning algorithms using one of the data sets that is more applicable to 0-day attacks and will validate the classification and performance predictions for anomalous data outliers possibly experienced in LEO CS systems.

8.5 Cybersecurity Controls for Cognitive Systems Summary

Like any other increasingly digitized critical infrastructure, satellites and other space-based assets are vulnerable to cyber-attacks. These cyber vulnerabilities pose serious risks not just for space-based assets themselves but also for ground-based critical infrastructure. If not contained, these threats could interfere with national security. The attack surface is becoming exponentially larger as more S/C connect with ground-based assets and users. Through resilient security design architectures, encryption techniques, and machine learning methods such as neural networks, APT-attacks and security vulnerabilities can be prevented and / or future instances mitigated, thereby increasing networking connectivity safely for commercial, NASA, and extended military users.

Chapter 9. Congestion Aware Intent-based Routing Architecture

This chapter will describe the CONAIR architecture which promotes the exchange of information across heterogeneous networks by using traditional routing methods complimented with Deep GNN AI to predict and mitigate traffic congestion or typically experienced bottle necks. Additionally, with the CONAIR architecture, information will be readily passed to the network controller to where an intelligent communication path selection can be made. This work was published in an IEEE technical peer-reviewed conference as noted in [9].

9.1 Background

Network resiliency is defined in [91], and further extended in [92] as the ability of a network to defend against and maintain an acceptable level of service in the presence of challenges (e.g., vulnerable to malicious attacks, software and hardware faults, human mistakes which include both software and hardware misconfigurations, and unprecedented natural disasters). Here, we can use resilience targeted metrics which reflects the requirements of end users, network operators, and service provider [93], to evaluate the value of the CONAIR architecture for varying network of networks using M&S. One key contributor of the CONAIR architecture is the NC which is responsible for controlling resilience mechanisms embedded in the network and service infrastructure, which allows the operation of the target service and ensures the graceful degradation of certain QoS attributes should challenges arise.

Current platforms contain NCs that seek to provide significant insight into the coordination of the network and PHY layers and open standards / data models for this coordination, e.g., connecting. By optimizing the use of available bandwidth and other resources, a NC and its overlay can be applied to the network that affords adaptability to various services to accommodate requirements of multi-mission platforms as well as multifunction devices. The typical problems of

non-interoperable stove-piped systems are eliminated using a network-of-networks approach, similar to SDN, but designed for the highly complex and dynamic topologies formed using line-of-sight (LOS) and BLOS radio links, ensuring survivability in a contested environment towards a secure tactical network.

An overlay can function as an application and content server residing in any node in the network, allowing for full remote operator control of all radios and other networked devices within any payload using a common web browser operating over any of the payload-hosted radio links. As such, an autonomous Decision Engine (DE) can optimize network operation and manage all payload applications (software) and devices (hardware) including but not limited to sensors, data links (IP and non-IP), satellite communications, and multi-function devices using an advanced architecture.

The overlay provides message and frequency translation and creates interoperability between disparate radios. Additionally, it is able to dynamically adjust to network performance constraints (e.g., bandwidth, delay) in support of multi-mission deployments. In conjunction with the overlay capability, cognitive capabilities can be used to serve as the DE to enable autonomous operations and to support automatic transfer of devices on a specific network to another network ensuring seamless and continuous communications are maintained. The NC selected for inclusion in the CONAIR architecture embraces critical cognitive techniques coupled with open standard / data model methods to provide alternate network path options in response to physical and network layer challenges (e.g., connectivity outages, bandwidth deterioration, application needs/priorities, or excessive delays), to sustain communications between networked participants agnostic to the radio, ensuring survivability for a robust, resilient network.

9.2 Network of Networks Architecture

Communications is critical to the operator gaining and retaining advantage over a potential adversary, but there are network challenges with capacity, bandwidth demands, latency, node priority, and station time. Additionally, bridging communications across domains has been challenging due to legacy stove-pipe / federated radio systems. The CONAIR architecture is a cognitive communications system, meaning it applies perception, learning, reasoning, memory and adaptive approaches in the design of the communication systems [94]. Service latency is a grave constraint in many of the mission applications for end users, therefore when designing a cognitive communications system, it is of utmost importance that routing optimization techniques of heterogeneous networks be an integral part of the solution. As described in [95], scheduling schemes, spectrum-aware routing and QoS control requires collaboration between the radios and engineered networks to truly be a cognitive network of networks system. The CONAIR architecture objective is to mitigate system overloading, dynamically adjusts resources allocated to low priority through continued collaboration methods, thereby increasing the probability of higher priority messages to be delivered within a useful time duration.

Figure 9.1 provides a high-level view of the CONAIR architecture. Here, the NC node can proactively mitigate congestion using the Inference Engine. The Inference Engine contains both the Oracle and the Route Filter functionality. The Inference Engine acts as an expert model of network traffic in a network, looking at time histories of traffic across the network links in order to predict the onset of congestion. Low priority traffic can be re-routed onto rarely utilized links in order to mitigate congestion before it happens. The CONAIR architecture seeks to provide resilient, multi-domain communications by offering a flexible, self-healing network of networks capability with an AI-enabled NC.

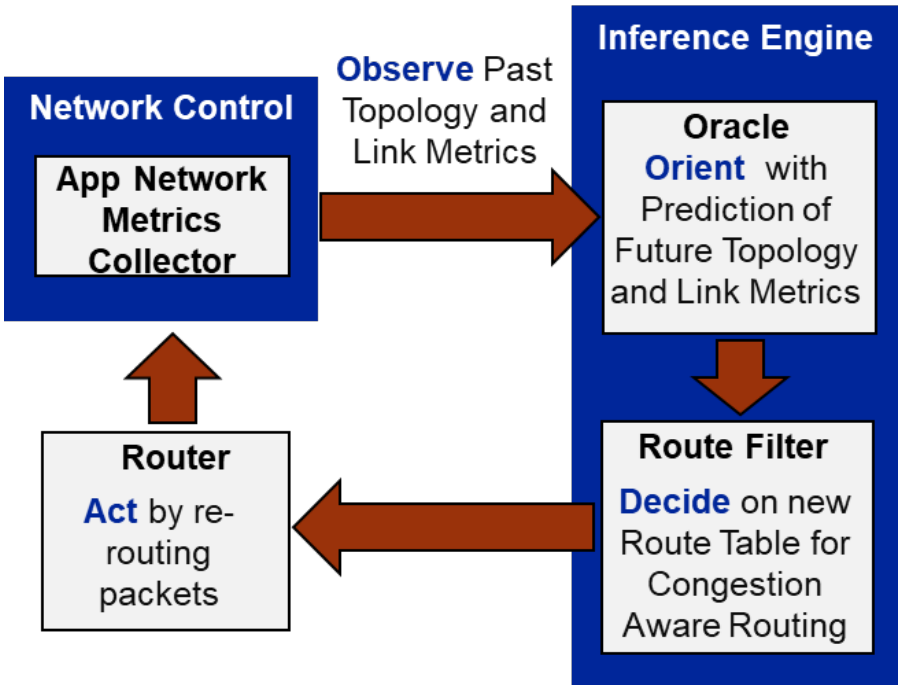


Figure 9.1. CONgestion Aware Intent-based Routing (CONAIR) Architecture

The CONAIR architecture can be most easily described using the Observe, Orient, Decide, Act (OODA) loop framework for command and control described by John Boyd in [96]. The Observe component of the loop is performed by the NC ingesting OSI layer 2 and 3 data describing the current state of IP traffic flow and network topology. These observations are provided to the Oracle, a predictive machine learning model within the Inference Engine. This model has been pre-trained under a wide variety of network conditions to become an expert model of network behavior. The Orient step is completed using Graph Neural Network (GNN) to generate predictions of latency and load of each communication link in the network [97]. These predictions are provided to the Route Filter within the Interference engine. The Route Filter performs the Decide step, populating a congestion-aware route table which prioritizes low-utilization routes. Once the new routes have been dynamically adjusted, the router completes the OODA loop, acting to push low priority packets to seldom utilized routes in the network, leaving the quickest routes open for the highest priority traffic.

A cognitive communications system is needed to support a fully integrated network of networks system to apply perception, learning and adaptive processes that facilitate message delivery assurance. With the design and implementation of the CONAIR architecture, the end user's QoE is enriched, and network resources are more readily available for higher priority traffic, thereby enabling the faster, timelier receipt of information. QoE, as defined in [98], is purely a subjective measure from the user's perspective of the overall quality of the service provided, by capturing people's aesthetic and hedonic needs, and are often influenced by human, system, contextual factors [99].

9.3 Graph Neural Networks

First introduced in 2009 [100], GNNs were developed to capture relationships represented as graphs. Unlike standard neural networks, GNNs retain a state that can represent information from its neighborhood with arbitrary depth. The target of GNN is to learn a state embedding within the m-dimensional Euclidean space, which contains the information for each node's nearest neighbors. In [101] interaction networks were proposed to make predictions and inferences about different physical systems. The model takes objects and relations as input, reasons about the interactions, and applies the effects and physical dynamics to predict new states. A key insight from this work comes from an analogy to a physics-based simulation engine. The interactions between objects depend on their relationships, and in turn the objects have states governed by these interactions. In the graph representation the interactions and objects are represented by edges and nodes, respectively.

Graphs have tremendous expressive controls and are therefore gaining a lot of attention in the field of machine learning. GNNs use neural networks to learn how relationships affect interactions, and in turn how those interactions affect the state of the nodes in the graph as shown

in Figure 9.2. While the machine learning researchers at DeepMind used these networks to solve n-body collision problems, the same logic can be applied to surmise the algorithms usefulness for networking problems, which is precisely what other authors have done to learn routing protocols [102], predict jitter and delay [103], optimize resource allocation in wireless networks [104], and distributed transmission scheduling.

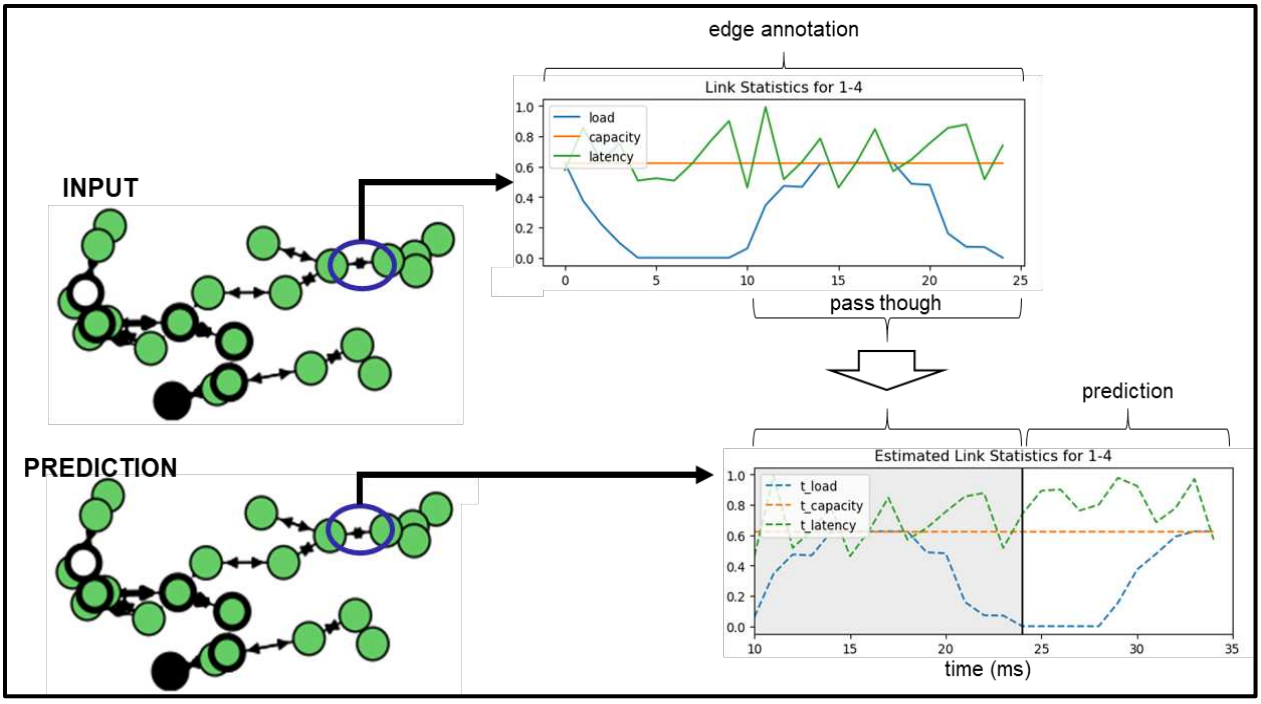


Figure 9.2. Example Input Data and Output Predictions from GNNs

Additionally, in [105], GNNs were proven to be highly valuable and used in social network prediction. To this notion, in the CONAIR architecture, GNNs predictions can be made to estimate the future state of the network based on QoS metrics at each input node within the network; this technique can be applied to dynamic networking topologies once trained on several physical network constructs.

Training is performed not with a fixed sampling method, but with a parameterized and trainable sampler to perform layer-wise sampling conditioned on the former layer which provides a level of adaptability for dynamic networks. We successfully ran over one-hundred experiments

on artificial data sets to assess the GNN prediction capability, varied model training and hyper parameters, and used the best performing model parameters for the baseline synthetic data. The training and tuning model used this baseline data, obtained from a simulation tool, to assess prediction accuracy and the overall network performance. As an example, in Figure 9.3, a GNN architecture was used to calculate the shortest route between two nodes in a network. Here, the GNN was trained on networks with approximately fifty nodes, and the algorithm was able to successfully calculate the shorted path on a three-hundred- node network.

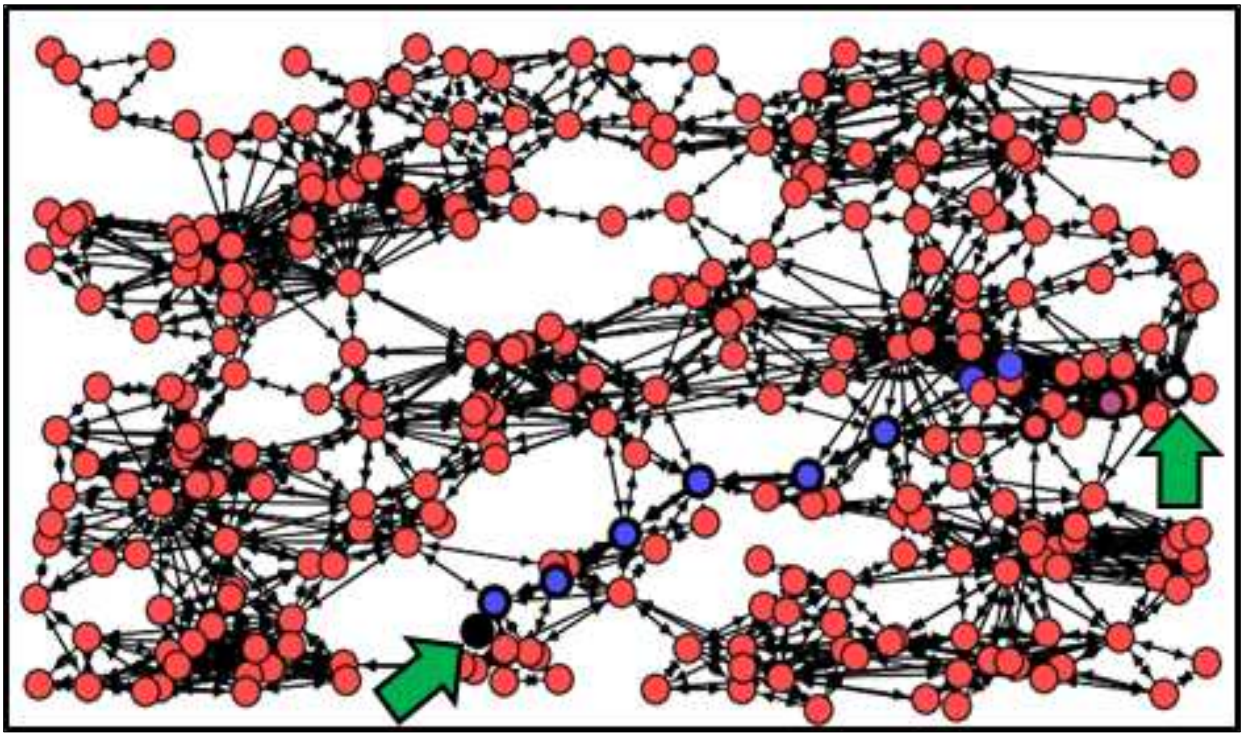


Figure 9.3. GNNs using Edge Node Information for Prediction

9.4 Modeling & Simulation & Analysis

Operational M&S examines the architecture from the perspective of a system operator and other users who are concerned with accomplishing the tasks for which the system is intended. It deals with the environment in which the system operates, operational scenarios and interactions of the participants, the outcomes of employing the system in various ways, and measures operational

performance and effectiveness [106]. Accordingly, M&S can be used to create an overall context for architectural analysis and to visualize the behavior of the network of networks system as a whole. For this work, we have implemented physical models which represent the hardware and software of the CONAIR architecture with high fidelity to reproduce detailed behaviors and to compute processor throughput and loading, latencies, and packet delivery ratios based on dynamic network topologies and differing operating scenarios using Scalable Network Technologies network emulation software, EXata [107].

EXata is used to evaluate on-the-move communication networks faster and with more realism using a software virtual network to digitally represent the entire network, and the various protocol layers. The system can interoperate, at one or more protocol layers, with real radios and devices to provide hardware-in-the-loop capabilities, and in the long run, allows for the successful design, analysis, and verification of a new communications system design and networking technologies. As described in [108], EXata was used to quantify traffic management schemes (e.g., segment routing) for airborne backbone networks, which provided continued coverage and reach-back capability when terrestrial networks are not available or cannot be flexibly deployed. And in [109], a Mobile Ad hoc Network (MANET) testbed was designed and integrated with EXata-Cyber network emulator to evaluate the performance of real-time video streaming applications. The performance of both proactive and reactive routing protocols were evaluated, in addition to measures for perceived video quality at the end users in the form of influencing QoE were evaluated to include mean opinion score, signal-to-interference and noise ratio (SINR) and packet delivery ratio at various layers of the TCP/IP protocol stack. To that end, while EXata will be used for the characterizing the network improvements of the CONAIR architecture, there are several candidate factors that impact the overall results. These factors include, but are not limited to, the

total number of nodes within the network, percent NC nodes (of total number of nodes), number of neighbors per node, number of links between a pair of neighbors, link capacity (e.g., bandwidth) available, time scale of total traffic change, and percentage of network capacity used. Through robust M&S of the CONAIR architecture with varying degrees of these adjustable factors, a reasonable performance assessment can be derived [110].

An example verification exercise can cover a large domain of operational parameters (e.g., throughput, latency, cumulative data rate, etc.). For the purposes of verifying predictive capability of the NC, a simple experiment was performed in accordance with Figure 9.4.

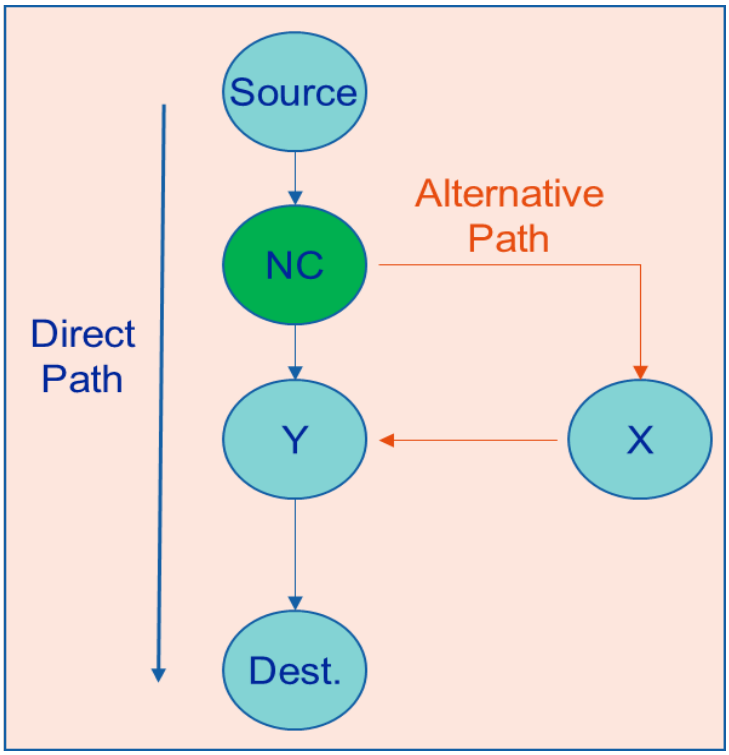


Figure 9.4. M&S Test Block Diagram for Predictive NC Setup

Here, a router operating the OSPF routing protocol [111] will always distribute data through the direct path leading to congestion when the data rate exceeds the link capacity. The NC node hosts the predictive routing system, when congestion is predicted low priority traffic should be redistributed to the alternative path, thereby freeing up the direct path for high priority traffic. This

experiment demonstrated enhanced QoS for high priority traffic by re-routing the low priority traffic through the longer paths; this was achievable using the CONAIR architecture solution.

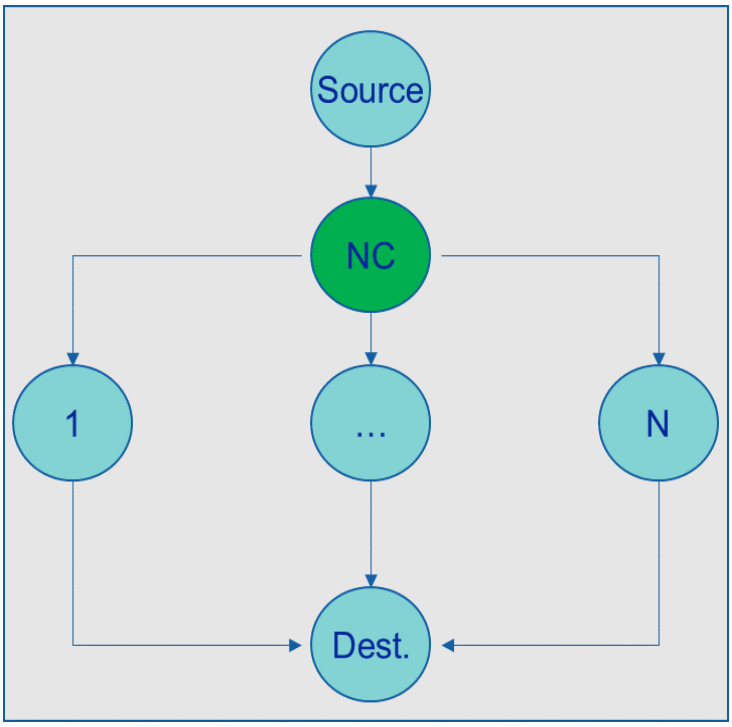


Figure 9.5. M&S Test Block Diagram for Resiliency & Scalability Setup

To extend the testing of the CONAIR architecture, two additional verification experiments were performed to evaluate the resiliency and scalability of the architecture in accordance with Figure 9.5. For the resiliency experiment, the network utilized fixed source and destination nodes, one NC node, and N = 48 parallel links with equal bandwidth. Two target architectures were evaluated, 1) OSPF routing protocol and 2) CONAIR architecture with Oracle predictions. Every 4 seconds, a static fault was injected on k= 2, 4, and 8 links to represent a compromised network (e.g., possible malicious attacks or software/hardware faults). The static fault renders the link broken, and at the conclusion of the simulation, only 34 operational links are remaining.

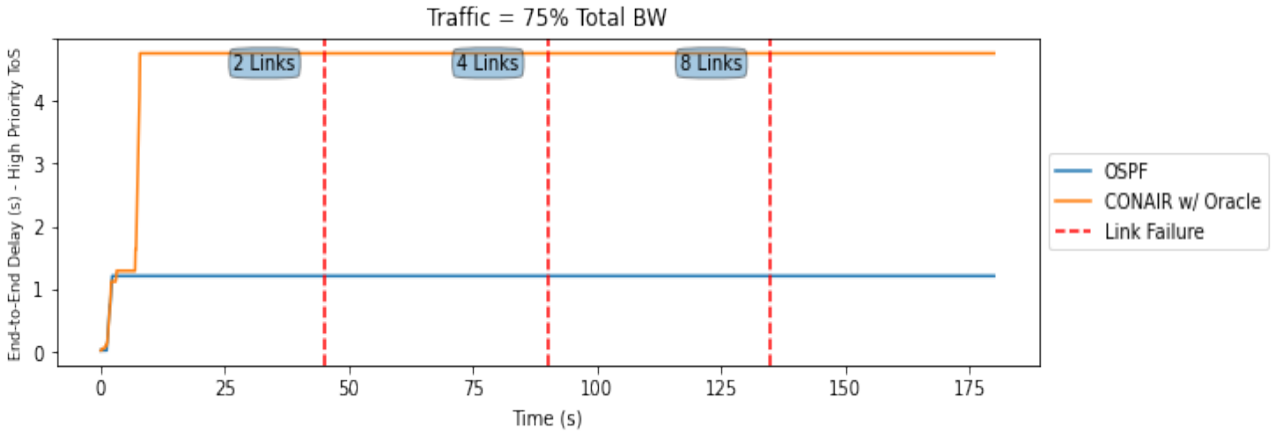


Figure 9.6. Resiliency High Priority Traffic Experiment Results

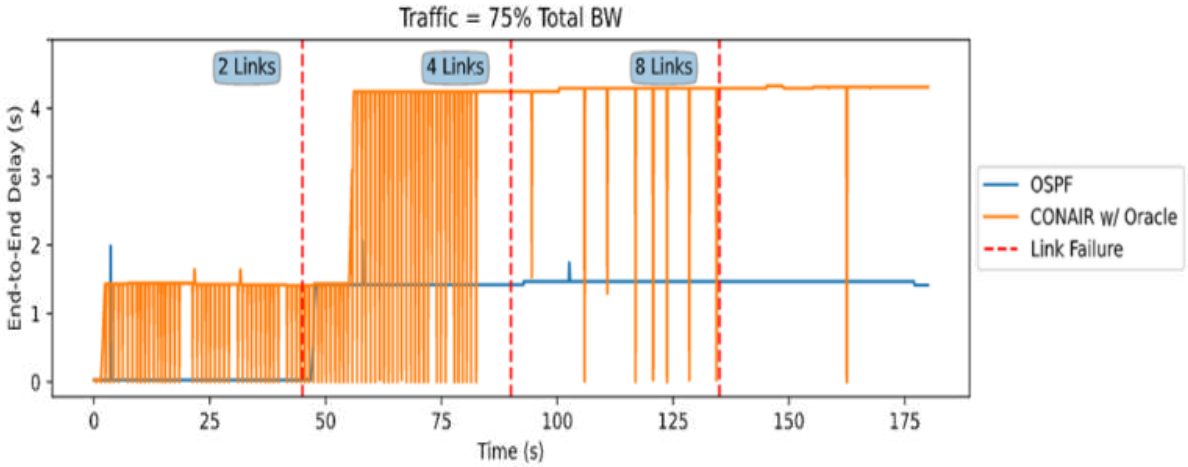


Figure 9.7. Resiliency Low Priority Traffic Experiment Results

The resiliency experiment results, both high priority and low priority traffic are shown in Figure 9.6 and Figure 9.7. Here, the OSPF protocol does not instantly recognize a faulty or degraded link, resulting in dropped packets on the segmented links, where the CONAIR architecture with Oracle predictions re-routes traffic resulting in increased end-to-end latency but no loss of packets.

For the scalability experiment, the network setup is based on Figure 9.5. The minimum message size was set to the link bandwidth and the maximum message size was set to the link bandwidth multiplied by 48 (equivalent to the total number of parallel links within the network). The message size was varied based on the ratios of the total network capacity (e.g. 50%, 75%,

100%, 125%, 150%, 175%, and 200% of the total bandwidth). Results presented in Figure 9.8 and Figure 9.9 show that the CONAIR architecture outperforms OSPF in terms of message delivery ratio for high and low priority traffic, respectively, when presented with multiple nodes within the network.

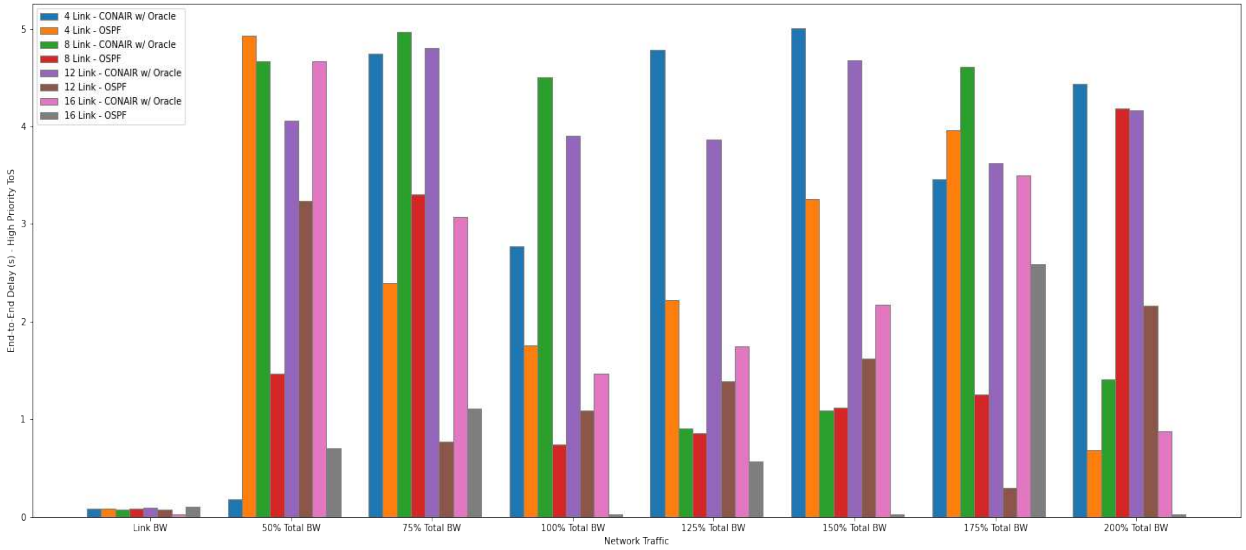


Figure 9.8. Scalability High Priority Traffic Experiment Results

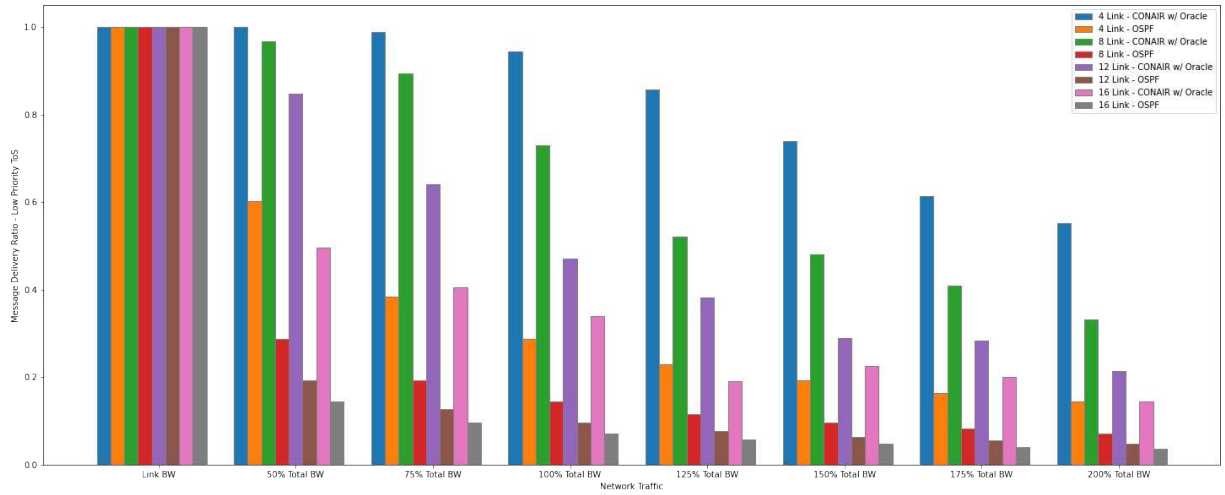


Figure 9.9. Scalability Low Priority Traffic Experiment Results

In these experiments, the prototyping strategies employed virtual machines hosting the NC within the EXata emulation environment to obtain diagnostic and performance measurements for a multi-hop network. In principle, prototyping experiments provide a mechanism to develop a

technical architecture that is capable of meetings its performance objectives while analyzing the results incrementally to verify the technology is functioning acceptably. Each of the experiments conducted revealed favorable results with the application of the CONAIR architecture. The results signify that future states of the network can be predicted when the model parameters are adequately trained using synthetic data for certain conditions, and that with heterogeneous networks GNNs will improve not only end user QoE, but ultimately warfighter productivity due to increased receipt of information more timely.

9.5 Cognitive Network Management Summary

In summary, we presented a novel method for predicting and mitigating link congestion with the implementation of the CONAIR architecture. Here, a predictive routing application has been developed leveraging cutting edge-AI techniques that can help in the navigation of complicated, multi-hop network of networks. Results show that with intricate, dynamic network topologies, both packet delivery and end-to-end latency can be improved for varying traffic profiles, and more so, higher priority traffic can be favored to ensure routes are available to distribute information quickly to the end user. Ultimately, operator QoE can be significantly improved with this implementation, allowing information to be received more rapidly and increasing overall mission effectiveness. Inevitably, a combination of individual link resiliency, enhanced waveform capabilities, spectral and spatial diversity, are all primary features in providing communications; however, the CONAIR architecture is the underlining framework that enables the flexibility and empowers these features to be employed for supporting a fully integrated network.

Chapter 10. Cognitive Communications System for Attributable Platforms

This chapter combines philosophies and novel strategies from Chapter 6 and Chapter 9 to formulate a cognitive communications system built on the foundations of systems level decision making and next generation wireless communications waveforms. The research question of what systematic coordination can be devised between emerging technologies (e.g., cognitive antennas and cognitive networking architectures) to optimize communications under stressing conditions is addressed. Here, machine learning algorithms can be applied to improve system reactions that are influenced by environmental and/or network related disturbances. This work is planned to be published in the IEEE peer-reviewed technical journal as noted in [10].

10.1 Background

Communications resiliency can be achieved by exploiting spectral and spatial diversity with cultivated aperture technology, emerging DSA capable radios, and advanced networking solutions that enable connectivity and interoperability for large-scale, multi-hop networks. Key to communications resiliency is the assurance of data delivery by providing reach-back and data distribution to commanders outside of enemy lines. More recently, small attributable platforms are replacing locally distributed soldiers near adversaries due to increased communications and weapons capabilities, thereby reducing probability of blue force peril [112] and [113]. In [114] maintaining small attributables cooperation and control is presented where the lack of efficient networking schemas that can manage communications in rapidly changing environments are identified as key challenges. While different engineered network topologies may exist for small attributables in the future, for example, as expected with microcosm swarm topologies, we propose to use a cognitive communications system (CCS) architecture that conducts cutting-edge systems

orchestration between its three segregated subsystems to optimize data distribution and delivery amongst network participants while operating the 5G new radio (NR) waveform.

In this chapter, small attributable platform requirements for hosting communications payloads are described. Also, the innovative CCS architecture which utilizes high-level systems operations to improve communications between nodes is outlined. Machine learning techniques are employed within each subsystem to predict aperture and networking behaviors that influence the way decisions are made to optimize information exchanges. Finally, a jamming analysis is presented to demonstrate the effectiveness of the CCS architecture when exercising the 5G NR waveform in its operationally deployed state. The analysis will be compared to legacy radio systems which use commercially available technology to highlight the benefits of such a CCS framework.

10.1.1 5G New Radio Waveform Description

5G is the 5th generation wireless telecommunications standard, which builds on previous generations of wireless technologies, but expands the use cases to critical functions for calling, messaging, and web browsing. The major benefits identified as part of the 5G innovation area include better mobility, lower latency, faster access to data, and enhanced throughput, enabling capabilities like livestream video. The 5G technology requires the use of three radio frequencies: below 1 GHz, 1-6 GHz, and above 24 GHz (commonly referred to as mmW). The lower bands allow for broad coverage, while the higher frequency bands deliver faster speeds and better quality. The 5G NR development is key to enabling the 5G mobile communications system to work and it provides a number of significant advantages when compared to 4G. The 5G NR initiative uses modulation, waveforms, and access technologies that enable the communications system to meet the demands of high data rate services at low latencies. The waveform format of 5G NR is based on Orthogonal Frequency Division Multiplexing (OFDM) and Discrete Fourier Transform spread

OFDM (DFT-s-OFDM) with adaptive modulation including Quadrature Phase Shift Keying (QPSK), 16 Quadrature Amplitude Modulation (QAM), 64QAM, and 256QAM. OFDM gives a respectable spectral efficiency whilst providing resilience to selective fading and enabling multiple access capability to be implemented using OFDM access (OFDMA) [115].

The specific version of OFDM used in 5G NR downlink is Cyclic Prefix (CP) OFDM (CP-OFDM) and is the same waveform LTE has adopted for the downlink signal. Within CP-OFDM, the last part of the OFDM data frame is appended at the beginning of the OFDM frame and the length of cyclic prefix is chosen to be greater than the channel delay spread. This overcomes the inter-symbol interference that can result from delays and reflections. In addition to this, the channel delay spread is frequency dependent with the cyclic prefix length chosen to be long enough to account for both interferences. For this reason, the CP length is adaptive according to the link conditions. The 5G NR uplink has used a different format to 5G LTE. CP-OFDM- and DFT-s-OFDM-based waveforms are used in the uplink. Additionally, 5G NR provides for the use of flexible subcarrier spacing. LTE subcarriers normally had a 15 Kilohertz (kHz) spacing, but the 5G NR allows the subcarriers to be spaced at 15 kHz x 2s with a maximum spacing of 240 kHz. The integral carrier spacing, rather than fractional carrier spacing, is required to preserve the orthogonality of the carriers. The flexible carrier spacing is used to properly support the diverse spectrum bands/types and deployment models that 5G NR will need to accommodate. For example, 5G NR must be able to operate in mmW bands that have wider channel widths of up to 400 MHz. 3GPP 5G NR Release-15 specification details the scalable OFDM numerology with 2s scaling of subcarrier spacing that can scale with the channel width, so the Fast Fourier Transform (FFT) size scales so that processing complexity does not increase unnecessarily for wider bandwidths. The flexible carrier spacing also gives additional resilience to the effects of phase

noise within the system. The use of OFDM waveforms offers a lower implementation complexity compared to that which would be needed if some of the other waveforms considered for 5G had been implemented. In addition to this, OFDM is well understood as it has been used for 4G and many other wireless systems.

DFT-s-OFDM is a Single Carrier (SC)-like transmission scheme that can be combined with OFDM that gives significant flexibility for a mobile communications system like 5G. It is more commonly known as Single Carrier Frequency Division Multiple Access (SC-FDMA). The transmission processing of SC-FDMA is very similar to that of OFDMA. For each user, the sequence of bits transmitted is mapped to a complex constellation of symbols (Binary Phase Shift Keying (BPSK), QPSK, or Multilevel Quadrature Amplitude Modulation (M-QAM)). Then different transmitters (users) are assigned different Fourier coefficients. This assignment is carried out in the mapping and de-mapping blocks. The receiver side includes one de-mapping block, one Inverse Discrete Fourier Transform (IDFT) block, and one detection block for each user signal to be received. Just like in OFDM, guard intervals (called cyclic prefixes) with cyclic repetition are introduced between blocks of symbols in view to efficiently eliminate inter-symbol interference from time spreading (caused by multi-path propagation) among the blocks.

Within the overall waveform format, different types of carrier modulation can be used. Within the 5G communications system, these are variants of phase shift keying and QAM. Here, QPSK is implemented in 5G technology. QPSK is the lowest order modulation format. Although this will provide the slowest data throughput, it will also provide the most robust link and as such, it can be used when signal levels are low or when interference is high. QAM enables the data throughput to be increased. Formats used within 5G mobile communications system include 16QAM, 64QAM, and 256QAM. The higher the order of modulation, the greater the throughput,

although the penalty is noise resilience. Therefore, 256QAM is only used when link quality is good, and it reduces to 64QAM, and then 16QAM, etc., as the link deteriorates.

10.2 Platform & Payload Requirements

Small attributable platforms are emerging as new vehicles that can enable a multitude of tasks (e.g., support of commercial disaster recovery operations including wild-fire communications relays with command centers, etc.). The design and constraint requirements for a medium size unmanned aerial vehicle (UAV) are presented in Table 10.1 as defined in [116]. The payload SWAP requirements are crucial metrics that need to be considered when designing the CCS architecture such that it can fit adequately within the bay of the platform, take advantage of platform power, and not exceed the maximum weight capacity, which would undoubtedly limit operations.

Table 10.1. Communications Relay Platform & Payload Requirements

Category	Requirement	Metric
Platform	Fuselage Length	73”
	Fuselage Width	8”
	Height	9”
	Weight	<100 lbs
Payload	Available Power	300 Watts
	Volume (Max)	975 in^3
	Weight (Max)	30 lbs

In addition to the defined requirements above, the payload cost must be substantially low due to thousands of quantities needed for future unmanned military operations, such as surveillance activities. Also, these platforms would serve useful to be armed with advanced weaponry to support parallel strike missions if they successfully penetrated anti-access enemy territory.

10.3 Cognitive Communication System Description

The CCS architecture is depicted in Figure 10.1; it consists of an environmentally perceptive aperture (EPA) subsystem [6], DSA capable software defined radio (SDR) subsystem, and a network controller (NC) subsystem [9]. Here, the wideband EPA functions in concert with an advanced SDR that can learn from its experiences over time to determine action and parameter selections to avoid interferences and operate in anticipation of connectivity challenges. The EPA subsystem can perform textbook beamforming, beam steering, and nulling by using learned experiences gained from interacting with the environment, and by having an introspective understanding of its own health and element status. The SDR is a powerful radio which comprises of a general-purpose processor used to perform signal processing, modulation and demodulation of the radio signals and can support different waveforms. The SDR is DSA aware, where the radio can effectively address spectrum scarcity challenges by sharing licensed frequency bands amongst users without any modifications to the radios or services in use. The NC will use available quality of service (QoS) information, such as link capacity, throughput, latency, and packet delivery ratio provided from the SDR via proxy services, to support network route recommendations.

Furthermore, the CCS architecture applies machine learning to predict aperture and network behaviors under certain pre-trained conditions. The applied cognition improves link performance, interference mitigation, traffic routing, and therefore improves QoE from an end user's perspective. Empowering communications with a robust, resilient CCS architecture will facilitate faster and more reliable data exchanges between the UAV platforms and executive leaders.

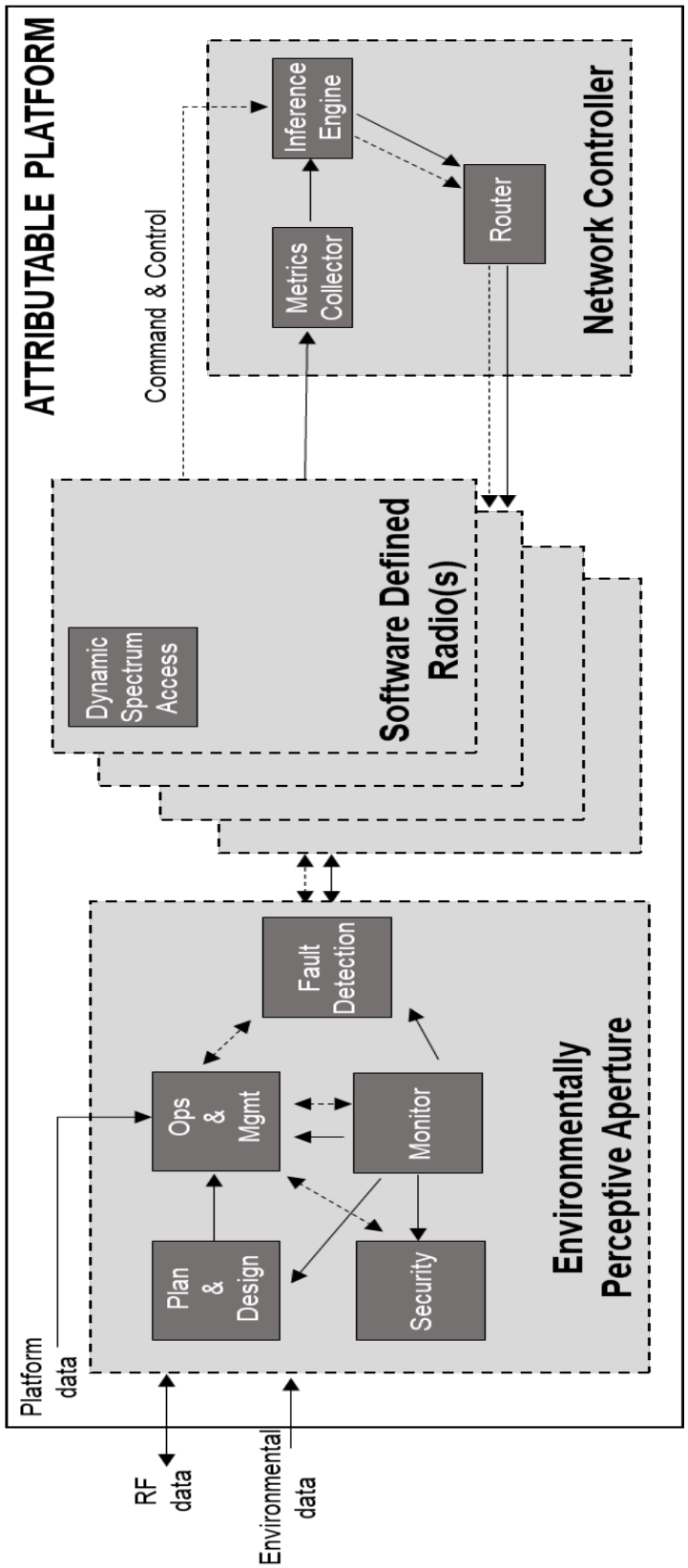


Figure 10.1. Cognitive Communications System within an Attributable Platform

10.3.1 Environmentally Perceptive Aperture Subsystem

The EPA subsystem is composed of functional sequencing components built upon erudite machine learning techniques that perform designated functions or key roles as shown in Figure 10.2. These roles are defined as planning and design, operations and management, monitoring, security, and fault detection. Here, planning and design will acquire data and train the functions for their intended operations prior to deployment. Operations and management function will implement a combination of DDPG with NAS for vigorous, agile operations. Where the monitoring block will use MSCRED to tailor the data for other functional use (dimensionality reduction) and to detect anomalies. Finally, both security and fault detection functional blocks will apply neural networks to classify known threats or systematic faults. With the growing complexity of current and future heterogeneous networks, advanced learning algorithms like the recommendations presented within this subsystem should be applied to optimize system performance. The EPA subsystem integrates with emerging SDR technology to learn from its experiences to overcome link performance challenges and interference mitigation, essential for the rapid expansion of small attributable platform communications.

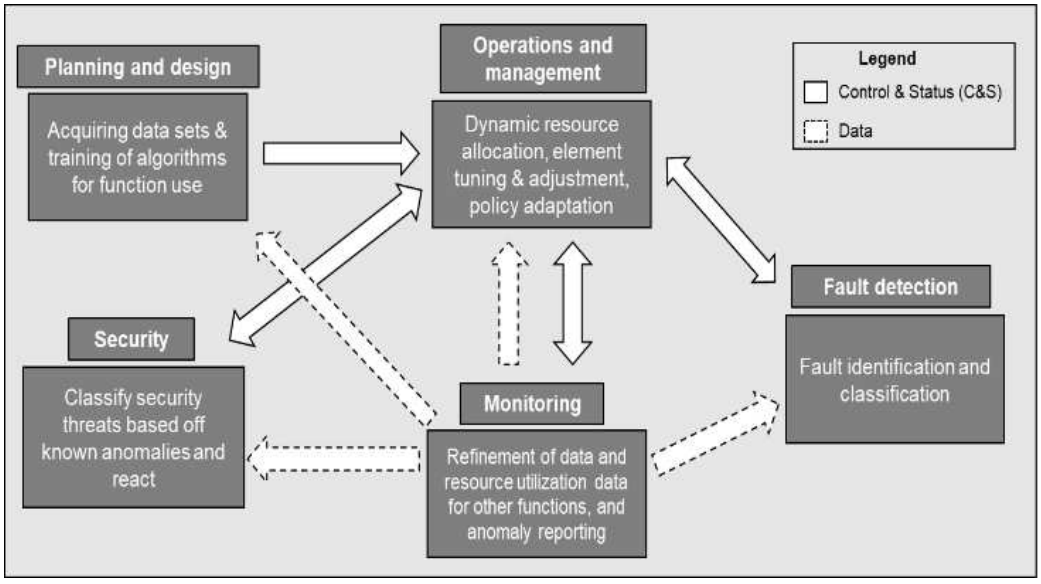


Figure 10.2. Functional Sequencing for Environmentally Perceptive Aperture

Using systems engineering best practices, a trade-off analysis was conducted to evaluate which machine learning techniques would be best suited for each antenna function given the problem each function needed to solve. As a mechanism for differentiating between alternative solutions, a set of quantifiable selection criteria was chosen that includes data set (size, nature, and quality), accuracy, available computation time, and urgency of task to be performed. For a given set of criteria, not all of them are equally important in determining the overall value of an alternative for each function. Such differences in importance are considered by assigning each criterion a weighting factor that magnifies the contribution of the most critical criteria. For the purposes of this trade-off analysis, the subjective value method was implemented to apply a judgement of the relative utility of each criterion on a scale one through ten. This was derived specifically for contested communications application and may vary dependent on intended applications. The score assigned was then normalized using the linear maximization method for simple additive weight trade methodology using a benefit and cost criteria respectively. Results of the selected machine learning techniques for their quantifiable selection criteria for each function are summarized in Figure 10.3.

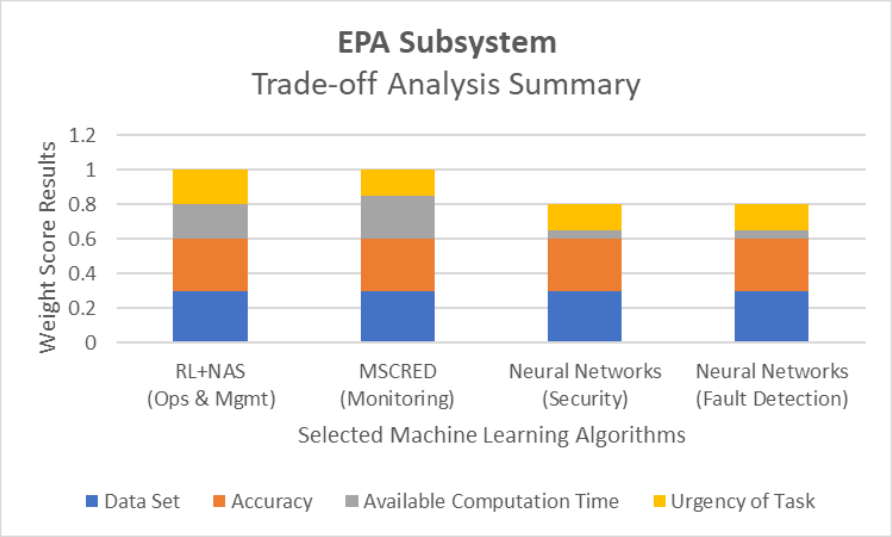


Figure 10.3. Trade-off Analysis Summary for Machine Learning Methods for Environmentally Perceptive Aperture

10.3.2 Software Defined Radio Subsystem

The SDR subsystem will be DSA aware which will allow the radio to take advantage of RF sensing to gather and use spectrum SA to dynamically select operational frequencies to transmit and receive communications on. This capability will run locally within each radio to swiftly recognize and resolve spectrum congestion and connect to previously undiscovered networks different available frequencies. Adaptation is constrained by knowledge of spectrum regulations that are loaded into the radio to ensure compliant operations.

10.3.3 Network Controller Subsystem

The NC subsystem applies perception, learning, reasoning, memory, and adaptive approaches, and can proactively mitigate congestion using an inference engine as described in Chapter 9. The inference engine contains both an oracle and a route filter capability. The inference engine acts as an expert model of the network traffic in a network, looking at time histories of traffic across the network links to predict the onset of congestion. Low priority traffic can be opportunistically re-routed onto underutilized links to mitigate congestion before it happens.

The NC subsystem can be most easily described using the observe, orient, decide, act (OODA) loop framework (as shown in Figure 9.1) for command and control described by John Boyd. The *observe* element of the loop is performed by the NC ingesting Open Systems Interconnection (OSI) layer 2 and 3 data describing the current state of Internet Protocol (IP) traffic flow and network topology. These observations are provided to the oracle, a predictive machine learning model within the inference engine. This model has been pre-trained under a wide variety of network conditions to become an expert model of network behavior. The *orient* step is completed using GNN to generate predictions of latency and the load of each communication link in the network. These predictions are provided to the route filter within the interference

engine. The route filter performs the *decide* step, populating a congestion-aware route table which prioritizes low-utilization routes. Once the new routes have been dynamically adjusted, the router completes the OODA loop, *acting* to push low priority packets to seldom utilized routes in the network, leaving the quickest routes open for the highest priority traffic.

GNNs use neural networks to learn how relationships affect interactions, and in turn how those interactions affect the state of the nodes in the graph as shown in Figure 9.2. Researchers have used these networks to solve n-body collision problems, networking problems to learn routing protocols, predict jitter and delay, optimize resource allocations, and perform distributed transmission scheduling.

10.4 Modeling Overview

Operational modeling examines the architecture from the perspective of a system operator and other users who are concerned with accomplishing the tasks for which the system is intended. It deals with the environment in which the system operates, operational scenarios and interactions of the participants, the outcomes of employing the system in various ways, and measures operational performance and effectiveness. Accordingly, operational modeling can be used to demonstrate the benefits of deploying such a CCS architecture within attributable platforms.

For context, an example use case for using the CCS architecture for interference mitigation is presented in Figure 10.4 to show the importance of its utility and cognition. Here, Drone-1 infiltrates enemy territory, and transmits surveillance data to Drone-2 and Drone-3. Drone-2 or Drone-3 acts as a communications relay and forwards data to the Operations Center (OC) for processing. Drone-2 and Drone-3 can communicate freely using 5G NR waveform when no interference is present. Red forces quickly detect the drones in the area of interest, and deploy an omni-directional, in-band, mature jammer to obfuscate communications between Drone-1 and its

two intended receivers. The jammer then transmits on the same Receive (Rx) channel / Rx beam, thereby disrupting the communications and impairing the OC data collection efforts. The drones equipped with the CCS architecture by design can sense and characterize the interference and optimize the aperture parameters for the communications link while providing beam nulling in the direction of the jammer. In doing this, the drones can learn to implement the desired configuration for future deployed jammers as well. Additionally, with DSA aware technology, the SDRs can modify the given transmit and/or receive frequencies to avoid the spectrum congestion. Also, if other radios are available that operate at frequencies outside of those being jammed, the NC can select to route the data using those. The effect of these coordinated operations between subsystems within the CCS architecture enabled by machine learning is the successful receipt of data at the OC at increased rates during mission execution, even in the presence of jammers.

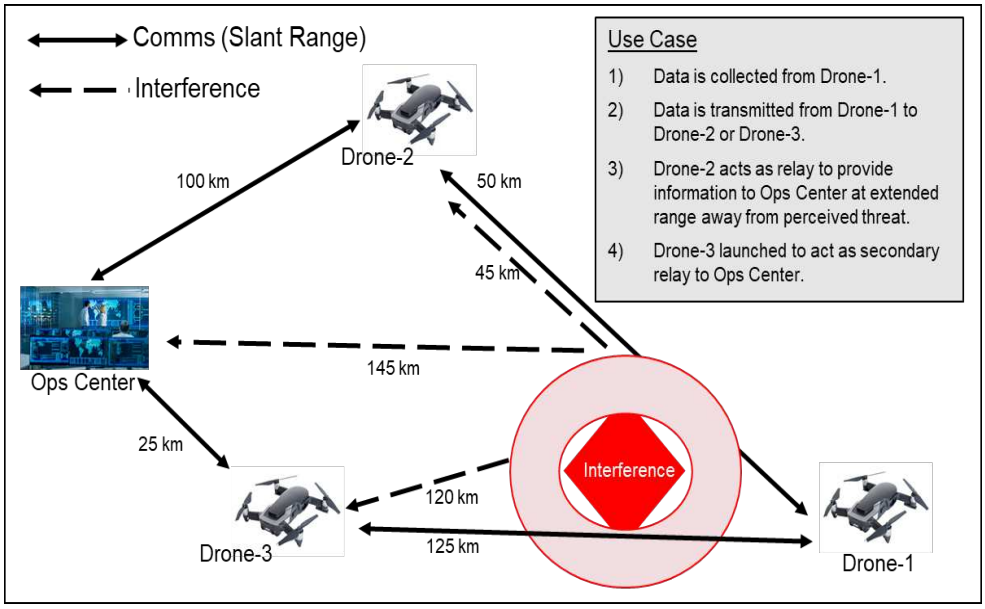


Figure 10.4. Operational Scenario for Mini-Drone Usage . Extraction of Data from Behind Enemy Lines

10.4.1 Performance Analysis Methodology

The following methodology was used to assess the jam resistance capabilities of the CCS architecture outfitted on the drones and its overall performance benefits.

1. 5G NR waveform fundamental link budgets for all communication paths available were performed. The analysis assumed a maximum operating frequency of 29.5 GHz, maximum available bandwidth of 850 MHz, and maximum channel bandwidth of 400 MHz as defined in the 5G NR specification [117].
2. Using the Friis equation for free space transmission, the jammer to signal (J/S) ratio was computed with the simplified equation derived below [118].

$$\frac{J}{S} = \left(\frac{PjGj}{PtGt}\right)\left(\frac{ds^2}{dj^2}\right) \qquad (9.4.1.1)$$

Here, J is the jammer signal power at the intended receiver (dB), S is the transmitter signal power at the intended receiver (dB), P_j is the jammer output power (dBW), P_t is the transmitter output power (dBW), G_j is the jammer antenna gain (dBi), G_t is the transmitter antenna gain (dBi), d_j is the distance from the jammer to the receiver (m), and d_s is the distance from the transmitter to the receiver (m).

3. Using the jammer bandwidth, calculate the updated received C/N_0 due to the jammer which is a function of the received C/N_0, jammer bandwidth, and the J/S ratio. This equation computes the effect of the received jammer to signal power (J/C in equation below) on the received signal to noise ratio.

$$\frac{C}{N_0} = \frac{C}{N_{RF}+N_J} = \frac{\mathrm{C}}{\mathrm{N_{RF}}+\left(\frac{\mathrm{J}}{\mathrm{C}}\right)\left(\frac{\mathrm{C}}{\mathrm{B}}\right)} = \frac{\frac{\mathrm{C}}{\mathrm{NRF}}}{\left(1+\left(\frac{1}{B}\right)\left(\frac{J}{C}\right)\left(\frac{C}{NRF}\right)\right)}\frac{\mathrm{C}}{\mathrm{N_0}} = \frac{\mathrm{C}}{\mathrm{NRF+NJ}} = \frac{\mathrm{c}}{\mathrm{NRF}+\left(\frac{\mathrm{J}}{\mathrm{C}}\right)\left(\frac{\mathrm{C}}{\mathrm{B}}\right)} = \frac{\frac{\mathrm{C}}{\mathrm{NRF}}}{\left(1+\left(\frac{1}{\mathrm{B}}\right)\left(\frac{\mathrm{J}}{\mathrm{C}}\right)\left(\frac{\mathrm{C}}{\mathrm{NRF}}\right)\right)}$$

(9.4.1.2)

where C is the total average received signal power, N_0 is the total noise power spectral density at the receiver, N_{RF} is the noise power spectral density due to the RF front end thermal noise, N_J is noise power spectral density due to jammer, and B is the jammer bandwidth.

4. The margin with the jammer can be computed, by taking the result in step 3 subtracted from the required C/N_0 obtained for the 5G NR waveform in use.

The methodology above was used to evaluate the physical layer communications analysis, the available margin with and without interference present, and repeated to understand the possible responses from the CCS architecture when exercising certain machine learning influenced decisions.

10.4.2 Performance Analysis Results

Considering the 29.5 GHz frequency band with 400 MHz carrier bandwidth for exercising the 5G NR waveform, and an EPA EIRP of 20 dBW (RF power of 1 mW and 50 dBi antenna gain), we can derive the physical layer analysis as computed in Table 10.2. Here, atmospheric loss was set at an arbitrary value of 5 dB to account for the loss affect expected at higher frequency bands. The results indicate that there is sufficient margin to close each link without interference present.

Next, consistent with steps 2 – 4, the communications link margin results can be used as inputs into the jamming analysis. An omni-directional, in-band jammer with an EIRP of 30 dBW and instantaneous bandwidth of 150 MHz is introduced to interrupt the communication exchange between Drone-1 and Drone-2 and/or Drone-1 and Drone-3. The results are presented in Table 10.3; results demonstrate how mini-drones without an integrated CCS architecture would be vulnerable to deployed and fielded jammers. The jammer can disrupt the communication platform receivers which are using siloed apertures/antennas or standard radios such that the exchange of communications is halted between the drones that are close-in range which significantly impact the OC's data collection process.

Table 10.2. Communications Link Budget Analysis

No.	Analysis Parameter (Unit)	Drone-1 to Drone-2	Drone-1 to Drone-3	Drone-2 to OC	Drone-3 to OC
1	EIRP (dBW)	20.0	20.0	20.0	20.0
2	Tx Frequency (GHz)	29.5	29.5	29.5	29.5
3	Range (km)	50.0	125.0	100.0	25.0
4	Free Space Path Loss (dB)	155.8	163.8	161.8	149.8
5	Atmospheric Loss (dB)	5.0	5.0	5.0	5.0
6	Pointing Loss (dB)	2.0	2.0	2.0	2.0
7	Total Propagation Loss (dB)	162.8	170.8	168.8	156.8
8	System G/T (dB/K)	15.0	15.0	15.0	15.0
9	Received C/N_0 (dB-Hz)	100.8	92.8	94.8	106.8
10	Information Bit Rate (dB-bits)	83.0	83.0	83.0	83.0
11	Required C/N_0 (dB-Hz)	89.0	89.0	89.0	89.0
12	Margin (dB)	11.8	3.8	5.8	17.8

Table 10.3. Jamming Analysis without CCS Architecture

No.	Analysis Parameter (Unit)	Drone-1 to Drone-2	Drone-1 to Drone-3	Drone-2 to OC	Drone-3 to OC
1	Resulting Comms Margin (dB)	11.8	3.8	5.8	17.8
2	Distance between Tx and Rx Comms Nodes (km)	50.0	125.0	100.0	25.0
3	Distance between Jammer and Rx Nodes (km)	45.0	120.0	145.0	145.0
4	Jammer EIRP (dBW)	30.0	30.0	30.0	30.0
5	Jammer Propagation Loss (dB)	154.9	163.4	165.1	165.1
6	Jammer RIP (dBW)	-124.9	-133.4	-135.1	-135.1
7	Victim Receiver Gain in Direction of Jammer (dBi)	30.0	30.0	30.0	30.0
8	J_0 (dBW/Hz)	-176.7	-185.2	-186.8	-186.8
9	Victim Receiver Gain in Direction of Tx node (dBi)	50.0	50.0	50.0	50.0
10	Derived $N_0 = kTs$ (dBW/Hz)	-193.6	-193.6	-193.6	-193.6
11	$N_0 + J_0$ (dBW/Hz)	-176.6	-184.6	-186.0	-186.0
12	$C/(N_0 + J_0)$ (dB-Hz)	83.8	83.8	87.2	99.2
13	Comms Margin with Jam (dB)	-5.3	-5.2	-1.9	10.2

The CCS architecture can apply cognition by using coordinated systems interactions among its subsystems to optimize the communication link. Figure 10.5 depicts a decision flow chart for a CCS-enabled drone transmitting to another CCS-enabled drone. Some techniques the CCS implements are the nulling out of interference using adaptive beamforming methods, and if multiple interference sources exist, the segmenting of the EPA's EIRP based on the number of the gain required to close the link can be considered, or exercising DSA by changing frequencies or transmit / receive channels to avoid spectrum congestion for in-band jammers, and if there are multiple SDRs available on the platform, the NC subsystem can seek an available communications link based on radio link resources and knowledge of the interference. Other techniques such as adjusting the data rate of the selected waveform to maximize range may be handy as well, or switching waveforms if alternatives are available for communications.

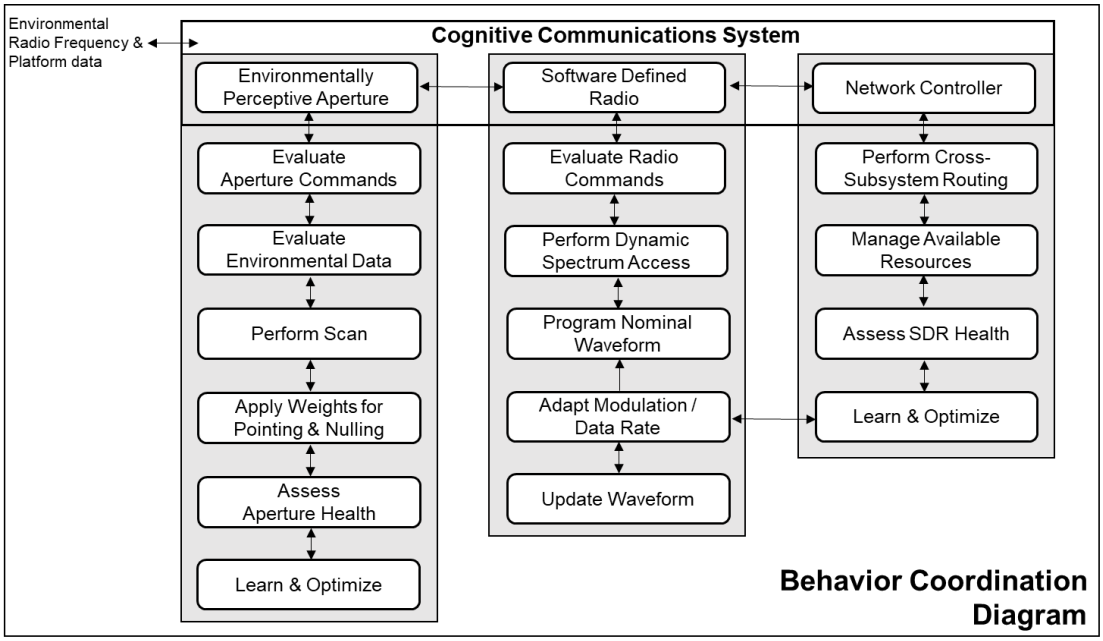


Figure 10.5. High-Level Behavior Coordination Diagram

To validate the significant offering of the CCS architecture, the jamming analysis was repeated where we assumed the drones were equipped with a CCS architecture. In this example, as the jammer is coming into position, the drones detect some of the degradation to

communications and can recognize it as an enemy jammer. Using the knowledge gained on the jammer's position, a null can be applied in the direction of the jammer by using the EPA subsystem, thereby suppressing the victim receiver gain in the direction of the jammer. Table 10.4 provides updated results which yield positive communications margin for all communication path options.

Table 10.4. Jamming Analysis with CCS Architecture

No.	Analysis Parameter (Unit)	Drone-1 to Drone-2	Drone-1 to Drone-3	Drone-2 to OC	Drone-3 to OC
1	Resulting Comms Margin (dB)	11.8	3.8	5.8	17.8
2	Distance between Tx and Rx Comms Nodes (km)	50.0	125.0	100.0	25.0
3	Distance between Jammer and Rx Nodes (km)	45.0	120.0	145.0	145.0
4	Jammer EIRP (dBW)	30.0	30.0	30.0	30.0
5	Jammer Propagation Loss (dB)	154.9	163.4	165.1	165.1
6	Jammer RIP (dBW)	-124.9	-133.4	-135.1	-135.1
7	Victim Receiver Gain in Direction of Jammer (dBi)	0.0	0.0	0.0	0.0
8	J_0 (dBW/Hz)	-206.7	-215.2	-216.8	-216.8
9	Victim Receiver Gain in Direction of Tx node (dBi)	50.0	50.0	50.0	50.0
10	Derived $N_0 = kTs$ (dBW/Hz)	-193.6	-193.6	-193.6	-193.6
11	$N_0 + J_0$ (dBW/Hz)	-193.4	-193.6	-193.6	-193.6
12	$C/ (N_0 + J_0)$ (dB-Hz)	100.6	92.8	94.7	106.8
13	Comms Margin with Jam (dB)	11.6	3.8	5.7	17.8

Coupled with the fact that the CCA architecture meets or exceeds the platform and communication payload requirements, and the promising empirical results, the CCS architecture is an optimal selection for small attributable platforms deployed in highly contested environments.

10.5 Cognitive Communications System Summary

A novel CCS architecture influenced by machine learning for attributable platforms which uses the 5G NR waveform to relay intelligence, surveillance, and reconnaissance to decision

makers at the forefront of the battlefield was described. The architecture combines a highly capable EPA, a SDR, and resilient networking techniques. The CCS architecture and its hardware assets meet the SWAP requirements given for a medium size UAV and the communications payload. This paper described the system architecture and the machine learning application to designated functions within each subsystem, and the importance of systems orchestration to transfer information effectively between nodes, and across large-scale multi-hop networks. Operational modeling was performed to demonstrate the performance benefits of the CCS when presented with the challenges imposed by mature and readily available jammers. Performance results compared to existing commonplace architectures showed favorable results where the flow of information distribution was not disrupted.

Future work will develop the selected machine learning algorithms as enablers for the CCS architecture. The CCS architecture will be integrated onto drones and staged in a testbed that applies a realistic operating environment to assess the immediate performance benefits for given use cases and will validate the interactions for collaborative systematic operations and decision making between the cognitive subsystems.

Chapter 11. Research Contributions & Conclusion

Fully integrated network of networks military communications systems have many challenges in ensuring seamless information exchange, fusion, and dissemination between nodes within a complex network structure. In this research, multiple steps towards achieving a fully integrated network of networks architecture were proposed and evaluated. Here, robust offerings for mmW and high-capacity capable antenna technologies, a future tactical multifunction capable SDR that can be readily paired with the antennas to facilitate communications were presented. Additionally, S/C security data architectures, revolutionary models for an AI enabled space-based antenna system, and AI techniques that could be applied to identify, detect, and classify APT-attacks on a LEO space-based cognitive system were offered. Finally, an advanced networking architecture influenced by AI to improve traffic flow control and prioritizations, and the integration of this with a CA system for small, mini-drones was presented to demonstrate the benefits of sophisticated AI technology and state-of-the-art subsystems in a common disruptive use case environment.

In Chapter 3, two antenna designs referred to as the Pen-Cap air antenna and the Bunker antenna were proposed. Antenna geometries, configurations, analyses, and engineering RF measurements were highlighted to demonstrate that the designs would meet the antenna system requirements and would ultimately provide an increased value to military operations. For the Bunker antenna, two unique geometries were explored, the IFA and BCA geometries, where the BCA geometry proved to have better gain performance over the coverage required and can support K-band primary communications, but also supports secondary communications required at Ku and Ka-bands due to its wideband characteristics. Both antenna options, the Pen-Cap air antenna and Bunker antenna, have discriminating, novel features, that could support smaller platform and

ground communications for soldiers on the move, critical for increased mobility and tactical advantage in highly contested environments.

Chapter 4 proposes the exhaustive design, manufacturing, and RF performance testing for the novel QPRA; this antenna is capable of supporting high-bandwidth communications at four frequency bands; Ku TX, Ku RX, K RX and Ka TX. Benefits of the antenna were noted as low mass, low-cost, ease of deployment and stowage, combined with significantly higher gain. Additionally, the QPRA has potential future space applications for LEO, MEO and GEO satellites. Moreover, it has direct applications to future communications for 5^{th} generation aircraft and UAVs where it could be placed either in the nosecone or included in a pod that is attached to the UAV body.

Future work to continue the progression of these antenna technologies optimizations is planned, and highly encouraged, as technologies are continuously evolving. We will evaluate a low cost, compact phased array that can provide advanced beamforming techniques that will effectively be able to null out potential interferers. A prototype system will be designed, fabricated to which it will undergo anechoic chamber testing to verify the aperture performance in an RF induced environment.

A short summary of a highly sought after tactical manpack SDR was described in Chapter 5. This manpack, integrated with the COTM and CATH antenna technologies, could be used as a multifunction communications radio for soldiers in the battlefield. The SDR quick-fact specifications were provided, where key metrics such as SWAP proved to be significantly lower than what soldiers in the military today are currently outfitted with for communications equipment, and further, have less capability. The design was developed through several iterative design spirals, using key technical interchange meetings with real field operators to provide insight into

day-to-day operations, equipment uses and design improvements that could be made for increasing reliability and functionality of the manpack system that would be highly desirable to the fleet.

Several space-based related applications were proposed, to include cognitive antennas, security data architectures, and AI based solutions for protecting the systems in general. A discriminating CA system for supporting future space networks interoperability and compatibility was presented in Chapter 6, where the mission-level performance requirements were identified for the communications system which through physical layer analysis led to the derivation of the CA supported hardware specific requirements (number of antenna elements, gain, etc.). An innovative concept of a wideband CA working in conjunction with emerging CR technology to overcome future space network challenges was presented. Varying levels of cognition using machine learning techniques were evaluated to enable improved link performance, interference mitigation, and electronic/cyber resiliency, essential for the rapid expansion of S/C constellations and communications. Future work for the revolutionary CA system may explore the development of the selected machine learning algorithms as enablers for the system, integrate the CA system with CR technology in a communications systems testbed that applies a realistic space-based operating environment to assess the immediate performance benefits for given use cases and can validate the interactions for collaborative decision making and conflict resolution between the cognitive decision engines.

Robust security data architectures for space-based systems that could accommodate MLS are introduced in Chapter 7. It is important to consider resilient, protective, architectures and frameworks that allow the underlining C2 and data to be secured to the maximum extent possible. In some instances, C2 and data is far more important to winning a war or even a conflict, and protecting underlining data, such as geographic coordinate locations of troops or communications

systems, is a must. Cyber-security requirements, policy and governance for space-based systems were briefly reviewed. Finally, a short investigative trade study was presented for two differing approaches for an MLS architecture for space networks, centralized and distributed MLS frameworks. Both approaches were outlined and determined to be an acceptable method for securing the data in the network for military and commercial end users with the trade results indicating that the centralized approach was slightly more favorable for the evaluation criteria considered; however, dependent on S/C constraints, subject communication relays, and the operational mission to be performed, any one of the architectures may be more advantageous over the other. It was noted that when designing an architectural approach for space network solutions that the architect should implement whichever architecture is most beneficial to performing the operational mission effectively while assuring data protection.

Major challenges for future space-based enterprise solutions include vulnerabilities due to cyber threats as addressed in Chapter 8. An abuse case was introduced to highlight the possibilities of how an attacker might compromise the system, featured data, and in general pose a threat to other critical infrastructure. This research investigated the use of AI algorithms to identify, detect and classify intrusions on the CA space-based system. The evaluation process extended from a simple trade study to a complex evaluation of learning and training curves of said algorithms using realistic open-source data for various intrusion collection data. Results yielded that with the inclusion of neural networks algorithms, APT-attacks and security vulnerabilities can be prevented and / or future instances mitigated, thereby increasing networking connectivity safely for commercial, NASA, and extended military users.

Approaches for improving communications QoE by using AI enabled techniques to optimize the network at a MAC layer are presented in Chapter 9. A sophisticated method for

predicting and mitigating link congestion with the implementation of the CONAIR architecture was described. Results show that with intricate, dynamic network topologies, both packet delivery and end-to-end latency can be improved for varying traffic profiles, and more so, higher priority traffic can be preferred to ensure routes are available to distribute information quickly to the end user. Future work for the CONAIR architecture may investigate a system of systems approach for resiliency by extending the architecture to learn what layers of resiliency should be applied for given operations, environmental conditions, and dynamic network topologies, in essence applying an outward OODA loop to the inner one described. In parallel, continued development of the CONAIR architecture as a micro-service to be compatible and interoperable with COTS NCs to assure network of networks collaboration and information data exchange effectiveness is recommended. Lastly, the CONAIR architecture may be integrated with operational nodes within a realistic operational network, where the performance improvements for given mission use cases can be fully characterized and compared to the M&S results to validate the physical models used in the EXata based network emulation environment.

Finally, Chapter 10 merges the concepts presented throughout the document by integrating the CA technology and tactical multifunction SDR with the CONAIR architecture on attributable platforms to create an innovated CCS architecture influenced by machine learning. Here, the mini-drones are intended to relay intelligence, surveillance, and reconnaissance to decision makers using the 5G NR waveform. The CCS architecture is an integrated system architecture that uses machine learning for designated functions within each subsystem, and additionally, introduces the notion of systems orchestration of information between each to transfer information effectively between nodes, and across large-scale multi-hop networks. Operational modeling was presented to illustrate the performance benefits of the CCS when inserted in a challenging, heavy

interference-based environment. Results in comparison to legacy stove-pipe communications systems were presented, to which the CCS demonstrated its effectiveness in coordinating communications across the network.

Future work of the CCS architecture embedded on a communications payload for mini-drones may be explored, to which the hardware architecture may be designed, developed and tested in a systems integrated laboratory facility. Communications payloads may be developed for the purposes of testing communications capability, and overall operational benefits to the fleet. In parallel with the hardware development process, the machine learning techniques may be explored further, developed and applied to each subsystem, to where it may undergo robust subsystem unit testing. Following success, the subsystems may be fully integrated into a communications payload, and the coordination between subsystems may be subjected to various operational test cases to validate the CCS system responses. Finally, with the completion and validation of testing in a laboratory environment, the communications payloads may be integrated into a small attributable platform and flight tested in 2024-time frame.

This research investigated a multitude of advanced communication technologies and their integration to optimize communications through a fully integrated network of networks system. With mmW and high-capacity capable antenna technologies which offer spectral and spatial diversity, and a tactically relevant multifunction SDR pairing, both COTM and CATH can be supported in a way that ensures soldier safety. Individual link resilience can be applied not only with data security architectures and advanced networking architectures, such as the CONAIR, but architectures enabled by AI to facilitate a faster identification of problems, recognition of how to deal with those challenges, and an improved response over traditional architectures. Enhancing waveform capabilities can be performed with the selection of newer 5^{th} generation waveforms,

e.g., 5G NR waveform, to improve realizable gain, introduce nulls in the direction of potential interferers, and facilitate short effective communications at higher capacities, that can be implemented in the SDR, along with other advanced resilient waveform options. Improving networking and communications by emerging engineering technology is a must moving forward to support fully integrated network of networks systems to provide individual link resiliency, spectrum and spatial diversity, and communication enhancements in general.

BIBLIOGRAPHY

[1] Rao, S., LaMar, S., Ignatenko, M., Lee-Yow, C., Jayasumana, A., "Compact Millimeter-Wave Antenna Designs for Line-of-Sight Communications in Permissive Operating Environments," Proc. 2021 National Radio Science Meeting, Boulder, Colorado, 2021.

[2] Rao, S., Ignatenko, M., LaMar, S., Lee-Yow, C., Venezia, P., "Deployable Bunker Antenna with 4π Steradians Coverage for Ground Communications," Proc. IEEE Wireless, Antenna and Microwave (WAM) Symposium 5-8 June 2022.

[3] Rao, S., Ignatenko, M., LaMar, S., Lee-Yow, C., and Venezia, P., "Wide-Angle Coverage Deployable Bunker Antenna for Ground Applications," Proc. IEEE Transactions on Antennas and Propagation, 2022.

[4] Rao, S., Venezia, P., Scupin, J., Lee-Yow, C., and LaMar, S., "Quad-band Petal Reflector Antenna for Ground Applications," Proc. IEEE Wireless, Antenna and Microwave (WAM) Symposium 5-8 June 2022.

[5] LaMar, S. and Rao, S., "Future Tactical Manpack Multifunction Software Defined Radio and Antennas for Ground Operations," Proc. 2022 National Radio Science Meeting, Boulder, Colorado, 2022.

[6] LaMar, S., Gillette, T., Vineyard, S., Seidel, S., Jayasumana, A., "Revolutionary Cognitive Antennas for Space Networks Interoperability," Proc. 2020 IEEE Systems Conference, 14th Annual IEEE International Systems Conference, Montreal, Canada, 2020.

[7] Happel, L., LaMar, S., "Multi-Level Data Security for Resilient Space Communication Architectures," Proc. 24th Ka and Broadband Communications Conference, Niagara Falls, Canada, October 14-18, 2018.

[8] LaMar, S., Gosselin, J., Happel, L., and Jayasumana, A., "Combating Adanced Persistent Threats (APT) for Imminent Low Earth Orbit (LEO) Cognitive Systems," Proc. IEEE SYSCON 2022 Conference, Montreal, Canada, 25-28 April 2022.

[9] LaMar, S., Gosselin, J., Caceres, I., Kapple, S., and Jayasumana, A., "Congestion Aware Intent-Based Routing Using Graph Neural Networks for Improved Quality of Experience in Heterogeneous Networks," Proc. IEEE Military Communications (MILCOM) 2021 Conference, San Diego, Ca, USA, Track 4 – Architectures, Applications, and System of Systems Perspectives, pp. 446- 450.

[10] LaMar, S., Fitting, R., and Jayasumana, A., "Cognitive Communications System for Ultra-Low Size, Weight and Power (SWAP) Attributable Platforms," IEEE Access Journal, 2022.

[11] J. Zhang, X. Ge, Q. Li, M. Guizani and Y. Zhang, "5G Millimeter-Wave Antenna Array: Design and Challenges," in IEEE Wireless Communications, vol. 24, no. 2, pp. 106-112, April 2017, doi: 10.1109/MCW.2016.1400374RP.

[12] H. Ozpinar, S. Aksimsek and N. T. Tokan, "A Novel Compact, Broadband, High Gain Millimter-Wave Antenna for 5G Beam Steering Applications," in IEEE Transactions on Vehicular Technology, vol. 69, no. 3, pp. 2389-2397, March 2020, doi: 10.1109TVT.2020.2966009.

[13] Abdelgader M. Abdalla; Jonathan Rodriguez; Issa Elfergani; Antonio Teixeira, "Millimeter Wave Antenna Design for 5G Applications," in Optical and Wireless Convergence for 5G Networks, IEEE, 2019, pp. 139-156, doi: 10.1002/9781119491590.ch7.

[14] M. Agwial, A. Roy and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1617-1655, thirdquarter 2016, doi: 10.1109/COMST.2016.2532458.

[15] S. Chen and J. Zhao, “The requirements challenges and technologies for 5G of terrestrial mobile telecommunication”, IEEE Comm Magazine, vol. 52, no. 5, pp. 36-43, May 2014.

[16] J. Helander, K. Zhao, Z. Ying and D. Sjoberg, “Performance Analysis of Millimeter-Wave Phased Array Antennas in Cellular Handsets,” in IEEE Antennas and Wireless Propagation Letters, vol. 15, pp. 504-507, 2016, doi: 10.1109/LAWP.2015.2455040.

[17] I. Osaretin, W. Blackwell, R. Wylde, S. M. Tun and G. Smith, "High-Performance Reflector Antenna Design for the TROPICS Mission," *2018 IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting*, 2018, pp. 1719-1720, doi: 10.1109/APUSNCURSINRSM.2018.8608857.

[18] R. Deng, S. Xu, F. Yang and M. Li, "An FSS-Backed Ku/Ka Quad-Band Reflectarray Antenna for Satellite Communications," in *IEEE Transactions on Antennas and Propagation*, vol. 66, no. 8, pp. 4353-4358, Aug. 2018, doi: 10.1109/TAP.2018.2835725.

[19] Yueh-Chi Chang and John Hanlin, "Commercial Ka and Ku bands reflector antennas," *2007 IEEE Antennas and Propagation Society International Symposium*, 2007, pp. 5175-5178, doi: 10.1109/APS.2007.4396712.

[20] Hasani, Hamed, et al. "Single-layer quad-band printed reflectarray antenna with dual linear polarization." *IEEE Transactions on Antennas and Propagation* 63.12 (2015): 5522-5528.

[21] S. K. Rao, "Advanced Antenna Technologies for Satellite Communications Payloads," in IEEE Transactions on Antennas and Propagation, vol. 63, no. 4, pp. 1205-1217, April 2015, doi: 10.1109/TAP.2015.2391283.

[22] N. Chahat et al, “CubeSat deployable Ka-band mesh reflector antenna development for earth science missions”, IEEE Trans. Antennas & Propagat., vol. 64, # 6, pp. 2083-2093, June 2016

[23] S. Rao and M. Tang, “Stepped-Reflector antenna for dual-band multiple beam satellite communications payloads”, IEEE Trans. Antennas & Propagation, Vol. 54, pp. 801-811, March 2006

[24] R.C. Gupta, S.K. Sagi & M. Mahajan, “Parallel-shaping technique for a ring-focus reflector antenna”, IEEE Antennas & Propagation Magazine, vol. 61, no. 5, pp. 87-96, October 2019

[25] C. Granet, “Designing axially symmetric Cassegrain and Gregorian dual-reflector antennas from combination of prescribed geometric parameters”, IEEE Antennas & Propagation Magazine, vol. 40, no.2, pp. 76-82, April 1998

[26] S. Rao, P. Venezia & C. Lee-Yow, “A reconfigurable reflector antenna system with hybrid scanning method”, IEEE Antennas & Propagation Magazine, vol. 61, no. 5, pp. 29-36, October 2019

[27] C. Hsu and S. Rao, “Horn antenna and system for transmitting and/or receiving radio frequency signals in multiple frequency bands”, U.S. Patent # 8,164,533, April 2021

[28] Tzyh-Ghuang Ma; Chao-Wei Wang; Chi-Hui Lai; Ying-Cheng Tseng, "Applications to Heterogeneous Integrated Phased Arrays," in Synthesized Transmission Lines: Design, Circuit Implementation, and Phased Array Applications, IEEE, 2017, pp. 95-125, doi: 10.1002/9781118975732.ch4.

[29] S. B. Kotsiantis, “Supervised Machine Learning: A Review of Classification Techniques,” in Informatica, vol. 31, pp. 249-268, 2007.

[30] Murthy, (1998), Automatic Construction of Decision Trees from Data: A Multi-Disciplinary Survey, Data Mining and knolwedge Discovery 2: 345-389.

[31] P. Chaovalit and L. Zhou, “Movie Review Mining: A comparison between Supervised and Unsupervised Classification Approaches,” Proceedings of the 38th Annual Hawaii

International Conference on System Sciences, Big Island, HI, USA, 2005, pp. 112c-112c, doi: 10.1109/HICSS.2005.445.

[32] R. Sathya, "Comparison of Supervised and Unsupervised Learning Algorithms for Pattern Classification," International Journal of Advanced Research in Artificial Intelligence, vol. 2, no. 2, 2013.

[33] J. Zhou, G. Cui, Z. Zhang, C. Yang, Z. Liu, L. Wang, C. Li, M. Sun, "Graph Neural Networks: A Review of Methods and Applications," arXiv:1812.08434v4[cs.LG], 10Jul19.

[34] N. Kato et al., "The Deep Learning Vision for Heterogenous Network Traffic Control: Proposal, Challenges, and Future Perspective," in IEEE Wireless Communicaitions, vol. 24, no. 3, pp. 146-153, June 2017, doi: 10.1109/MCW.2016.1600317WC.

[35] J. Yu, Y. Wang, K. Pei, S. Zhang and J. Li, "A load balancing mechanism for multiple SDN controllers based on load informing strategy," 2016 18th Asia-Pacific Network Operations and Management Symposium (APNOMS), Kanazawa, 2016, pp. 1-4, doi: 10.1109/APNOMS.2016.7737283.

[36] H. Geng et al., "A hybrid link protection scheme for ensuring network service availability in link-state routing networks," in Journal of Communications and Networks, vol. 22, no. 1, pp. 46-60, Feb. 2020, doi: 10.1109/JCN.2019.000056.

[37] S. Annd, P. M. Mathikshara and T. Jayavignesh, "An Efficient Mask Reduction Strategy to Optimize Storage and Computational Complexity in Routing Table Lookups," 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2019, pp. 1-5, doi: 10.1109/ICECCT.2019.8868972.

[38] S. Hassell et al., "Evaluating network cyber resiliency methods using cyber threat, Vulnerability and Defense Modeling and Simulation," MILCOM 2012-2012 IEEE Military

Communications Conference, Orlando, FL, 2012, pp. 1-6, doi: 10.1109/MILCOM.2012.6415565.

[39] Reinhard, R. (2015). Using International Space Station for Cognitive System Research and Technology with Spacebased Reconfigurable Software-Defined Radios. *66th International Astronautical Congress*.

[40] Tonkin, S. and Pierre de Vries, J. "New Space Spectrum Sharing: Assessing Interference Risk and Mitigations for New Satellite Constellations," TPRC46: Research Conference on Communications, Information and Internet Policy, 2018.

[41] H. Mamat, B. H. Ibrahim and M.P. Sulong, "Network Topology Comparison for Internet Communications and IoT Connectivity," 2019 IEEE Conference on Open Systems (ICOS), Pulau Pinang, Malaysia, 2019, pp. 1-5, doi: 10.1109/ICOS47562.2019.8975702.

[42] Rao, S., F. Mayol, M. Padilla, R. Sudarsanam & S. Chun, "Array antennas and low-gain TT&C Antennas", Chapter 9, Handbook of Reflector Antennas, Volume 2, pp. 299-349, Artech House Publishers, 2013.

[43] F. Mayol, M. Padilla and J.M. Montero, "Turnstile-junction-based omni directional antennas for space applications', IEEE Antennas and Propagation Magazine, vol. 53, # 3, pp. 255-262, June 2011.

[44] S. Rao, C. Hsu & R. Sudarsanam, "Low gain antenna performance impact due to spacecraft scattering", Proc. IEEE APS/URSI International Symposium, July 2010.

[45] Z. Zhang, X. Gao, W. Chen, Z. Feng, and M. F. Iskander, "Study of conformal switchable antenna system on cylindrical surface for isotropic coverage," IEEE Trans. Antennas Propag., vol. 59, no. 3, pp. 776–783, Mar. 2011.

[46] W. Scott and K. Hoo, ``A theorem on the polarization of null-free antennas," IEEE Trans. Antennas Propag., vol. AP-14, no. 5, pp. 587_590, Sep. 1966.

[47] G. Pan, Y. Li, Z. Zhang, and Z. Feng, “Isotropic radiation from a compact planar antenna using two crossed dipoles,” IEEE Antennas Wireless Propag. Lett., vol. 11, pp. 1338–1341, 2012.

[48] C. Deng, Y. Li, Z. Zhang, and Z. Feng, “A wideband isotropic radiated planar antenna using sequential rotated L-shaped monopoles,” IEEE Trans. Antennas Propag., vol. 62, no. 3, pp. 1461–1464, Mar. 2014.

[49] Y.-M. Pan, K. W. Leung, and K. Lu, “Compact quasi-isotropic dielectric resonator antenna with small ground plane,” IEEE Trans. Antennas & Propagat., vol. 62, no. 2, pp. 577–585, Feb. 2014.

[50] Y. M. Pan and S. Y. Zheng, ‘‘A compact quasi-isotropic shorted patch antenna,’’ IEEE Access, vol. 5, pp. 2771–2778, 2017.

[51] Q. Li, W.-J. Lu, S.-G. Wang and L. Zhu, "Planar quasi-isotropic magnetic dipole antenna using fractional-order circular sector cavity resonant mode", *IEEE Access*, vol. 5, pp. 8515-8525, June 2017.

[52] H.P. Coleman and B.D. Wright, “A compact flush-mounted antenna with direction finding and steerable cardiod pattern capability”, IEEE Transactions on Antennas and Propagation, vol. 32, no. 4, pp. 412-414, April 1984.

[53] C.A. Balanis. “Antenna Theory: Analysis and Design”, 3rd edition, John Wiley, 2005.

[54] J. Wu, S. Yang, Y. Chen, S. Qu and Z. Nie, “A Low Profile Dual-Polarized Wideband Omnidirectional Antenna Based on AMC Reflector,” in IEEE Transactions on Antennas and Propagation, vol. 65, no. 1, pp. 368-374, Jan. 2017.

[55] I. Gronich, “Omni directional ultra wideband asymmetric biconical antenna,” 2009 IEEE International Conference on Microwaves, Communications, Antennas and Electronic Systems, pp. 1-4, 2009.

[56] L. Li, W. Yan, B. Feng and L. Deng, “A Wideband Omni-directional Antenna Based on Printed Log-Periodic Element,” 2020 IEEE 3rd International Conference on Electronic Information and Communication Technology (ICEICT), pp. 719-720, 2020.

[57] Ignatenko, M., Rao, S., Lee-Yow, C., Venezia, P., and LaMar, S., “Compact wide angle coverage antenna for air and ground applications”, U.S. Patent Pending, August 2021.

[58] Lee-Yow, C., Rao, S., LaMar, S., and Venezia, P., “Quad-band petal reflector antenna”, U.S. Patent # 11,088,461, August 10, 2021.

[59] Bloom, B.S, Engelhart, M.D., Furst, E.J., Hill, W.H., and Krathwohl, D.R. (1956). Taxonomy of Educational Objectives, Handbook I: The Cognitive Domain. New York: David McKay Co Inc.

[60] Kossiakoff, A., Sweet, W.N., Seymour, S.J., and Biemer, S.M. 2011. Systems engineering: Principles and Practice (2nd ed.). Hoboken, NJ: John Wiley & Sons.

[61] Vafaei, N., Ribeiro, R., and Camarinha-Matos, L. Normalization Techniques for Multi-Criteria Decision Making: Analytical Hierarchy Process Case Study. 7th Doctoral Conference on Computing, Electrical and Industrial Systems (DoCEIS), Apr 2016, Costa de Caparica, Portugal. pp.261-269, 10.1007/978-3-319-31165-4_26. hal-01438251

[62] Duan, Y., Chen, X., Houthooft, R., Schulman, J., and Abbeel, P. Benchmarking Deep Reinforcement Learning for Continuous Control. Proceedings of the 33rd International Conference on Machine Learning, New York, NY, USA, 27 May 2016. JMLR: W&CP Volume 48.

[63] Lillicrap, T., Hunt, J., Pritzel, A., Heess, N., Erez, T., Tassa, Y., Silver, and D., Wierstra, D. Continuous Control with Deep Reinforcement Learning. Proceedings of the 4th International Conference of Learning Representations, ICLR 2016, San Juan, Puerto Rico, 2-4 May 2016.

[64] Zoph, B. and Le, Q. Neural Architecture Search with Reinforcement Learning. Proceedings of the 5th International Conference of Learning Representations, ICLR 2017, Toulon, France 24-26 April 2017.

[65] Zhang, C., Song, D., Chen, Y., and Feng, X. A Deep Neural Network for Unsupervised Anomaly Detection and Diagnosis in Multivariate Time Series Data. arXiv:1811. 08055v1 [cs.LG]

[66] Chalapathy, R. and Chawla, S. Deep Learning for Anomaly Detection: A Survey. arXiv:1901.03407 [cs.LG], 23 Jan 2019.

[67] Puñal, O., Schmelke, C., Abidin, G., and Wehrle, K. Machine learning-based Jamming Detection for IEEE 802.11: Design and Experimental Evaluation. Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014.

[68] Wang, L., Zhang, Z., Long, H., Xu, J., and Liu, R. Wind Turbine Gearbox Failure Identification With Deep Neural Networks. IEEE Transactions on Industrial Informatics, Volume 13, Issue 3 2017.

[69] United States Committee on National Security Systems, "CNSSI No. 1200 National Information Assurance Instruction for Space Systems Used to Support National Security Missions," Government Standard, May 2014.

[70] United States Committee on National Security Systems, "CNSSI No. 1253 Security Categorization and Control Selection for National Security Systems, Appendix F Attachment 2 Space Platform Overlay," Government Standard, June 2013.

[71] United States Committee on National Security Systems, "CNSSI No. 1253 Security Categorization and Control Selection for National Security Systems, Appendix F Attachment 3 Cross Domain Solution (CDS) Overlay," Government Standard, September 2013.

[72] Uchenick, G. and Vanfleet, W. "Multiple Independent Levels of Safety and Security: High Assurance Architecture for MSLS/MLS", in the proceedings of MILCOM, 2005.

[73] Levin, T.; Irvine, C.; Weissman, C.; and Nguyen T. "Analysis of Three Multilevel Security Architectures," in the proceedings of Cyber Security Awareness Week (CSAW), 2007.

[74] D. Bell and L. La Padula. "Secure Computer Systems: Unified Exposition and Multics Interpretation," Electronic Systems Division, USAF. ESD-TR-75-306, MTR-2997 Rev. 1. Hanscom AFB, MA. 1976.

[75] Nguyen, T. "A Study of covert communications in space platforms hosting government payloads," Naval Postgraduate School (NPS), 2015.

[76] U.S. – China Economic and Security Review Commission, "2011 Report to Congress of the U.S. – China Economic and Security Review Commission," November 2011.

[77] McWhorter, D., APT1: Exposing One of China's Cyber Espionage Units, Mandiant, Alexandria, VA, USA, vol. 18, 2013.

[78] Chen, J., Su, C., Yeh, K., and Yung, M. "Special Issue on Advanced Persistent Threat," Future Generation Computer Systems, 2019, vol. 79, pp. 243-246, doi:10.1016/j.future.2017.11.005.

[79] Chen, P., Desmet, L., and Huygens, C., "A study of advanced persistent threats", Proc. IFIP Int. Conf. Commun. Multimedia Security, pp. 63-72, 2014.

[80] Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K, Aparicio-Navarro, F., "Detection of advanced persistent threat using machine-learning correlation

analysis," Future Generation Computer Systems, 2018, vol. 89, pp. 349-359, doi:10.1016/j.future.2018.06.055.

[81] Hassannataj, J.. Haderadi, M., Mashmool, A., Ghasemigol, M., Band, S, and Mosavi, A. "Early Detection of the Advanced Persistent Threat Attack Using Performance Analysis of Deep Learning," in IEEE Access, vol. 8, pp. 186125-186137, 2020, doi: 10.1109/ACCESS.2020.3029202.

[82] Singh, S., Sharma, P., Moon, S., Moon, D.,and Park, J. "A comprehensive study on APT attacks and countermeasures for future networks and communications: Challenges and solutions", J. Supercomput. Vol. 75, no. 8, pp. 4543-4574, Aug. 2019.

[83] Alshamarani, A., Myneni, S., Chowdhary, A., and Huang, D., "A survey on advanced persistent threats: Techniques solutions challenges and research opportunities", IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1851-1877, 2nd Quart. 2019.

[84] Ghafir, I. Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., et al., "Detection of advanced persistent threat using machine-learning correlation analysis", Future Gener. Comput. Syst., vol. 89, pp. 349-359, Dec. 2018.

[85] Marchetti, M., Pierazzi, F., Colajamni, M., and Guido, A., " Analysis of high volumes of network traffic for Advanced Persistent Threat detection", Computer Networks, vol. 109, part 2, pp. 127-141, 2016.

[86] Chemouil, P. et al., "Special Issue on Artificial Intelligence and Machine Learning for Networking in Communications," in IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1185-1191, June 2019, doi: 10/1109/JSAC.2019.2909076.

[87] Cheng, B and Titterington, D., "Neural Networks: A Review from a Statistical Perspective," in Statstical Science, vol. 9, no. 1, pp. 2-30, 1994.

[88] Shun, J. and Malki, H., "Network Intrusion Detection System Using Neural Networks," 2008 Fourth International Conference on Natural Computation, 2008, pp. 242-246, doi: 10.1109/CNC.2008.900.

[89] KDD Cup 1999 Classification Model, accessed 26 July 2021, <GitHub - concision/kdd-cup-1999-model: A Tensorflow model to detect network intrusions in the KDD Cup 1999 data-set.>

[90] Xin, Y. et al., "Machine Learning and Deep Learning Methods for Cybersecurity," in IEEE Access, vol. 6, pp. 35365-35381, 2018, doi: 10.1109/ACCESS.2018.2836950.

[91] J.P.G. Sterbenz et al., "Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines," Elsevier Computer Networks, Special Issue on Resilient and Survivable Networks, vol. 54, no. 8, June 2010, pp. 1245-1265.

[92] P. Cholda et al., "A Survey of Resilience Differentiation Frameworks in Communication Networks," IEEE Communication Surveys & Tutorials, vol. 9, no. 4, 2007, pp. 32-55

[93] P. Smith et al., "Network resilience: a systematic approach," in IEEE Communications Magazine, vol. 49, no. 7, pp. 88-97, July 2011, doi: 10.1109/MCOM.2011.5936160.

[94] M. Serhman, A. N. Mody, R. Martinez, C. Rodriguez and R. Reddy, "IEEE Standards Supporting Cognitive Radio and Networks, Dynamic Spectrum Access, and Coexistence," in IEEE Communications Magazine, vol. 46, no. 7, pp. 72-79, July 2008, doi: 10.1109/MCOM.2008.4557045.

[95] Y. Liang, K. Chen, G.Y.Li ad P. Mahonen, "Cognitive radio networking and communications: an overview," in IEEE Transactions on Vehicular Technology, vol. 60, no. 7, pp. 3386-3407, Sept. 2011, doi: 10.1109/TVT.2011.2158673.

[96] J. R. Boyd. (3September 1976). Destruction and Creation. U.S. Army Command and General Staff College.

[97] J. Zhou, G. Cui, Z. Zhang, C. Yang, Z. Liu, L. Wang, C. Li & M. Sun.. Graph Neural Networks: A review of Methods and Applications. arxiv 2018.

[98] ITU-T Recommendation P.10: Vocabulary for performance and quality of service, Amendment 5 (07/16). https://www.itu.int/rec/T-REC-P.10

[99] Reiter, Ulrich; Brunnström, Kjell; Moor, Katrien De; Larabi, Mohamed-Chaker; Pereira, Manuela; Pinheiro, Antonio; You, Junyong; Zgank, Andrej (2014-01-01). Möller, Sebastian; Raake, Alexander (eds.). Factors Influencing Quality of Experience. T-Labs Series in Telecommunication Services. Springer International Publishing. pp. 55–72. doi:10.1007/978-3-319-02681-7_4. ISBN 978-3-319-02680-0.

[100] F. Scarselli, M. Gori, A. C. Tsoi, M. Hagenbuchner, and G. Monfardini, “The graph neural network model,” IEEE TNN 2009, vol 20, no. 1, pp. 61-80, 2009.

[101] Rusek, Krzysztof, et al. "Unveiling the potential of Graph Neural Networks for network modeling and optimization in SDN." Proceedings of the 2019 ACM Symposium on SDN Research. 2019.

[102] Zhao, Zhongyuan, et al. "Distributed Scheduling using Graph Neural Networks." *arXiv preprint arXiv:2011.09430* (2020).

[103] Eisen, Mark, and Alejandro R. Ribeiro. "Optimal wireless resource allocation with random edge graph neural networks." *IEEE Transactions on Signal Processing* (2020).

[104] T. N. Kipf and M. Welling, “Semi-supervised classification with graph convolutional networks,” ICLR 2017, 2017.

[105] Fabien Geyer and Georg Carle. 2018. Learning and Generating Distributed Routing Protocols Using Graph-Based Deep Learning. In Proceedings of the 2018 Workshop on Big Data Analytics and Machine Learning for Data Communication Networks (Big-DAMA '18). Association for Computing Machinery, New York, NY, USA, 40–45. DOI:https://doi.org/10.1145/3229607.3229610.

[106] J. M. Borky & T. H. Bradley. Effective Model-Based Systems Engineering, Spring International Publishing AG, 2019.

[107] EXata Network Emulator Software, https://www.scalable-networks.com/products/exata-network-emulator-software/

[108] K. Chen, S. Zhao, N. Lv, W. Gao, X. Wang and X. Zou, "Segment Routing Based Traffic Scheduling for the Software-Defined Airborne Backbone Network," in IEEE Access, vol. 7, pp. 106162-106178, 2019, doi: 10.1109/ACCESS.2019.2930229.

[109] C. Lal, V. Laxmi and M.S.Gaur, "Video streaming over MANETs: Testing and analysis using real-time emulation," 2013 19th Asia-Pacific Conference on Communications (APCC), Denpasar, 2013, pp. 190-195, doi: 10.1109/APCC.2013.6765940.

[110] O. Balci, "Quality assessment, verification, and validation of modeling and simulation applications," Proceedings of the 2004 Winter Simulation Conference, 2004, Washington, DC, USA, 2004, pp.129, doi:10.1109/WSC.2004.1371309.

[111] J. Moy, "Request for Comments: 2328 STD: 54, OSPF Version 2," April 1998.

[112] G. Udeanu, A. Dobrescu and M. Oltean, 2016, May. Unmanned aerial vehicle in military operations. In The 18th International Conference "Scientific Research and Education in the Air Force – AFASES", Brasov, Romania (pp. 199-205).

[113] M. A. Ma'sum et al., "Simulation of intelligent Unmanned Aerial Vehicle (UAV) for military surveillance," 2013 International Conference on Advanced Computer Science and Information Systems (ICACSIS), 2013, pp. 161-166, doi: 10.1109/ICACSIS.2013.6761569.

[114] J. Li, Y. Zhou, and L. Lamont, "Communication architectures and protocols for networking unmanned aerial vehicles," 2013 IEEE Globecom Workshops (GC Wkshps), 2013, pp. 1415-1420, doi:10.1109/GLOCOMW.2013.6825193.

[115] D. Hui, S. Sandberg, Y. Blankenship, M. Andersson and L. Grosjean, "Channel Coding in 5G New Radio: A Tutorial Overview and Performance Comparison with 4G LTE," in IEEE Vehicular Technology Magazine, vol. 13, no. 4, pp. 60-69, Dec. 2018, doi: 10.1109/MVT.2018.2867640.

[116] J. A. Benito, G. Glez-de-Rivera, J. Garrido and R. Ponticelli, "Design considerations of a small UAV platform carrying medium payloads," Design of Circuits and Integrated Systems, 2014, pp. 1-6, doi:10.1109/DCIS.2014.7035583.

[117] 5G New Radio (NR) Technical Specification, Release 15. https://www.3gpp.org/release-15.

[118] Friis, H.T. (May 1946). "A Note on a Simple Transmission Formula". IRE Proc. 34 (5):254–256. doi:10.1109/JRPROC.1946.234568.S2CID51630329.

Appendix A. Reference Table for Acronyms

Acronym	Description
ADE	Axially Displaced Ellipsoid
AI	Artificial Intelligence
AMC	Artificial Magnetic Conductor
ANN	Artificial Neural Networks
API	Application Programming Interface
APT	Advanced Persistent Threat
BCA	Biconical Antenna
BLUF	Bottom Line Up Front
BLOS	Beyond Line of Sight
BSS	Broadcast Satellite Service
C2	Command and Control
CA	Cognitive Antenna
CAS	Close Air Support
CATH	Communications at the Halt
CCS	Cognitive Communications System
CDS	Cross Domain Solution
CSC	Cognitive System Controller
CMA	Covariance Matrix Adaptation
CMi	Custom Microwave Incorporated
CONAIR	CONgestion Aware Intent-based Routing
COTM	Communications on the Move
COTS	Commercial Off the Shelf
CP	Circular Polarization
CR	Cognitive Radio
CS	Cognitive System
CSU	Colorado State University
DARPA	Defense Advanced Research Project Agency
dBi	decibels - isotropic
dBW	Decibels - Watts
DDPG	Deep Deterministic Policy Gradient
DE	Decision Engine
DNN	Deep neural Networks
DoD	Department of Defense
DSA	Dynamic Spectrum Access
DT	Decision Trees
EIRP	Equivalent Isotropic Radiated Power
EM	Electromagnetic
EPA	Environmentally Perceptive Aperture
FD	Full Duplex
FEM	Finite Element Method
FL	Fuzzy Logics

FPGA	Field Programmable Gate Arrays
FSS	Fixed Satellite Service
GA	Genetic Algorithms
GEO	Geosynchronous Earth Orbit
GHz	Gigahertz
GNB	Gaussian Naïve Bayes
GNN	Graph Neural Networks
GPU	General Purpose Unit
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
ICA	Independent Component Analysis
ICS	Integrated Communications System
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IFA	Inverted F-Antenna
IPS	Intrusion Protection System
ISS	International Space Station
ISS	Inter Satellite Service
KDD	Knowledge Discovery and Data Mining
OODA	Observe, Orient, Decide, Act
PAE	Power Added Efficiency
PCA	Principle Component Analysis
QPRA	Quad-band Petal Reflector Antenna
QoE	Quality of Experience
QoS	Quality of Service
LEO	Low Earth Orbit
LHCP	Left Hand Circular Polarization
LPD	Low Probability of Detection
LPI	Low Probability of Interception
LNB	Low Noise Block
M&S	Modeling and Simulation
M&S&A	Modeling and Simulation and Analysis
MAC	Medium Access Control
Mbps	Megabits per second
ML	Machine Learning
MLS	Multiple Levels of Security
mmW	Millimeter Wave
MSCRED	Multi-Scale Convolutional Recurrent Encoder-Decoder
MSS	Mobile Satellite Service
NAS	Neural Architecture Search
NASA	National Aeronautics and Space Administration
NC	Network Controller
NN	Neural Networks
NR	New Radio
OMT	Orthomode Transducer

OSFP	Open Shortest Path First
PCS	Personal Communication Service
PHY	Physical
RA	Reflectarray Antenna
RF	Radio Frequency
RHCP	Right Hand Circular Polarization
RL	Reinforcement Learning
RMA	Reconfigurable Mechanical Assembly
RX	Receive
S/C	Spacecraft
SCaN	Space Communications and Navigation
SDN	Software Defined Networking
SDR	Software Defined Radio
SVM	Support Vector Machine
SWAP	Size, Weight and Power
TX	Transmit
UAV	Unmanned Aerial Vehicle
UHF	Ultra High Frequency
U.S.	United States
VHF	Very High Frequency