2022-12

A COMPREHENSIVE REVIEW OF INTERNET OF THINGS WAVEFORMS FOR A DOD LOW EARTH ORBIT CUBESAT MESH NETWORK

Laird, Brittany L.

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/71494

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A COMPREHENSIVE REVIEW OF INTERNET OF THINGS WAVEFORMS FOR A DOD LOW EARTH ORBIT CUBESAT MESH NETWORK

by

Brittany L. Laird

December 2022

Thesis Advisor:	Alex Bordetsky
Second Reader:	Eugene Bourakov

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE				*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.				
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis		
4. TITLE AND SUBTITLE A COMPREHENSIVE REVIEW OF INTERNET OF THINGS WAVEFORMS FOR A DOD LOW EARTH ORBIT CUBESAT MESH NETWORK				**5. FUNDING NUMBERS**
6. AUTHOR(S) Brittany L. Laird				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000				**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A				**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.				**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The Department of Defense (DOD) requires the military to provide command and control during missions in locations where terrestrial communications infrastructure is unreliable or unavailable, which results in a high reliance on satellite communications (SATCOM). This is problematic because they use and consume more digital data in the operational environment. The DOD has several forms of data capable of meeting Internet of Things (IoT) transmission parameters that could be diversified onto an IoT network. This research assesses the potential for an IoT satellite constellation in Low Earth Orbit to provide an alternative, space-based communication platform to military units while offering increased overall SATCOM capacity and resiliency. This research explores alternative IoT waveforms and compatible transceivers in place of LoRaWAN for the NPS CENETIX Ortbial-1 CubeSat. The study uses a descriptive comparative research approach to simultaneously assess several variables. Five alternative waveforms—Sigfox, NB-IoT, LTE-M, Wi-sun, and Ingenu—are evaluated. NB-IoT, LTE-M, and Ingenu meet the threshold to be feasible alternatives to replace the LoRaWAN waveform in the Orbital-1 CubeSat. Six potential IoT transceivers are assessed as replacements. Two transceivers for the NB-IoT and LTE-M IoT waveforms and one transceiver from U-blox for the Ingenu waveform are assessed as compliant.

14. SUBJECT TERMS CubeSat, satellite communications, SATCOM, military satellite communications, MILSATCOM, Internet of things, IoT, low earth orbit, LEO, low power wide area network, LPWAN, narrow band Internet of things, NB-IoT, LTE-M, FY19 NDAA, Executive Order 13873, chirp spread spectrum, CSS, LoRaWAN, Orbital-1, Ingenu			**15. NUMBER OF PAGES** 103
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

A COMPREHENSIVE REVIEW OF INTERNET OF THINGS WAVEFORMS FOR A DOD LOW EARTH ORBIT CUBESAT MESH NETWORK

Brittany L. Laird
Lieutenant, United States Navy
BS, University of La Verne, 2013

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN NETWORK OPERATIONS AND TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
December 2022

Approved by: Alex Bordetsky
Advisor

Eugene Bourakov
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Department of Defense (DOD) requires the military to provide command and control during missions in locations where terrestrial communications infrastructure is unreliable or unavailable, which results in a high reliance on satellite communications (SATCOM). This is problematic because they use and consume more digital data in the operational environment. The DOD has several forms of data capable of meeting Internet of Things (IoT) transmission parameters that could be diversified onto an IoT network. This research assesses the potential for an IoT satellite constellation in Low Earth Orbit to provide an alternative, space-based communication platform to military units while offering increased overall SATCOM capacity and resiliency. This research explores alternative IoT waveforms and compatible transceivers in place of LoRaWAN for the NPS CENETIX Ortbial-1 CubeSat. The study uses a descriptive comparative research approach to simultaneously assess several variables. Five alternative waveforms—Sigfox, NB-IoT, LTE-M, Wi-sun, and Ingenu—are evaluated. NB-IoT, LTE-M, and Ingenu meet the threshold to be feasible alternatives to replace the LoRaWAN waveform in the Orbital-1 CubeSat. Six potential IoT transceivers are assessed as replacements. Two transceivers for the NB-IoT and LTE-M IoT waveforms and one transceiver from U-blox for the Ingenu waveform are assessed as compliant.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
AFRL	Airforce Research Laboratory
AI	Artificial Intelligence
BER	Bit Error Rate
BGAN	Broadband Global Area Network
BLE	Bluetooth Low Energy
C2	Command and Control
CENETIX	Center for Network Innovation and Experimentation
COTS	Commercial Off The Shelf
CPS	Cyber Physical System
CSS	Chirp Spread Spectrum
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODIN	DOD Information Network
DSSS	Direct Sequence Spread Spectrum
DtS-IoT	Direct-to-Satellite Internet of Things
EHF	Extremely High Frequency
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
GEO	Geostationary Orbit
IDU	Indoor Unit
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPSec	Internet Protocol Security
ISL	Intersatellite Link
ISM	Industrial, Scientific, and Medical equipment
ITU	International Telecommunications Union
JADC2	Joint All Domain Command and Control
JCS	Joint Chiefs of Staff

LEO	Low Earth Orbit
LoRa	Long Range
LPWAN	Low Power Wide Area Network
LTE-M	Long-Term Evolution for Machine-Type Communications
LTE URLLC	LTE Ultra-Reliable and Low Latency Communication
M2M	Machine-to-Machine
ML	Machine Learning
MILSATCOM	Military Satellite Communications
mMTC	Massive Machine-Type Communication
MSS	Mobile Satellite Service
NB-IoT	Narrowband Internet of Things
NDAA	National Defense Authorization Act
NFV	Network Function Virtualization
NIST	National Institute of Standards and Technology
NR URLLC	New Radio Ultra-Reliable and Low Latency Communication
NRO	National Reconnaissance Office
ODU	Outdoor Unit
OG2	Orbcomm Generation 2
QoS	Quality of Service
PCB	Printer Circuit Board
POR	Program of Record
RAM	Random Access Memory
RF	Radio Frequency
RPMA	Ingenu Random Phase Multiple Access
RSSC	Regional SATCOM Support Center
RTT	Round Trip Time
SATCOM	Satellite Communications
SBD	Short Burst Data
SDR	Software Defined Radio
SHF	Super High Frequency
SNR	Signal to Noise
TLS	Transport Layer Security

UHF	Ultra High Frequency
USASMCD	US Army Space and Missile Defense Command
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to start by expressing my deepest gratitude to my advisors, Dr. Alex Bordetsky and Mr. Eugene Bourakov, for their time, mentorship, and encouragement throughout this thesis process and two years of postgraduate education. I am also grateful to my professors who gave me the foundational knowledge and support I needed to write my thesis: Mr. Glenn Cook, Dr. Anthony Pollman, Dr. Mustafa (Anthony) Canan, Mr. Matthew Crook, and the Information Sciences Department. Additionally, I could not have completed this journey without the help of my fantastic writing coaches. Thank you so much, Mr. Matt Norton and Ms. Lauren Callihan.

Words cannot begin to describe the appreciation I would like to express to my husband, Chris, and our children. Thank you for supporting me through the endless nights, long weekends, and numerous holidays I spent away from our family, up in my office, working on schoolwork. Finally, thank you to my friends and classmates near and far who helped me through this challenging endeavor: Carol, Jennifer, Nicole, Brian, and the 386 cohort.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In many ways, the Department of Defense (DOD) has been the founding organization of the Internet of things (IoT), especially the Internet of Remote Things (IoRT). For over eight decades, the United States (US) military has relied on wireless communications to conduct operations in remote environments (Britannica, n.d.). The DOD has operated in theaters spanning the globe while at the same time having the necessity to maintain communications with headquarters back in America. Technology advanced these communications from the use of letters, to the telegraph, to the radio, and then eventually along with the invention of the internet, to Satellite Communications (SATCOM) (Council on Foreign Relations [CFR], n.d.). The advancement of communications technology led to a data boom in the military and initiated the use of concepts like wireless sensor networks (WSN) and radio frequency identification (RFID). WSNs have been used by the military to improve situational awareness in many remote environments, including underwater, on the ocean's surface, and in the airspace above the seas or in foreign lands, while RFID has been implemented to track logistics accurately worldwide (CASCOM, 2020). These technologies yielded some of the first IoT-like data in the DOD, with more IoT-friendly data being generated daily.

Since the DOD is often required to operate in remote locations where terrestrial communications infrastructure is unreliable or unavailable, SATCOM has been the primary means to fill this critical communication gap. However, existing military satellite communication (MILSATCOM) constellations have limited capacity for IoT and other data, which is problematic due to the military forces' increased use of digital data in the operational environment, as they consume more capacity than ever before. Consequently, Regional SATCOM Support Centers (RSSCs) are forced to prioritize missions across the DOD, resulting in a reduction in allocated bandwidth compared to user-requested levels.

One possible solution to address this capacity shortage is the use of an IoT architecture based on a new MILSATCOM constellation. DOD SATCOM has historically been concentrated in the Geostationary orbit (GEO). GEO has the advantage of providing continuous coverage from 35,786 km above the earth's surface (Gordon &

Morgan, 1993). Constellations in GEO require fewer satellites for worldwide coverage but incur a more significant launch cost and longer roundtrip time (RTT) for data transmissions (De Sanctis et al., 2016; U.S. Army, 2013). The DOD also has communications spacecraft in Polar Orbit. These assets follow a highly elliptical path, passing over the poles on each orbit to enable polar communications in the northern hemisphere (U.S. Army, 2013). However, low earth orbit (LEO), which ranges from 160 km to 1000 km above the earth's surface, is a promising, previously underutilized orbit to explore IoT spaced-based communications in (ESA, 2020).

LEO is a growing constellation for communications and other missions. It is rapidly gaining popularity with the private sector due to its lower launch costs, lower transmission power requirements, and reduced transmission latency compared to GEO and polar orbits (U.S. Army, 2013). Companies like Lacuna Space, Eutelsat, Fleet Space Technologies, and Sateliot are racing to develop small, cube-shaped, and cost effective commercial-off-the-shelf (COTS) satellites known as CubeSats for operation in LEO (Arifin, 2021). Due to CubeSat performance parameters, these assets are predominantly being explored by the private sector for IoT applications in space.

Within the DOD, very little MILSATCOM has been conducted from LEO. The military and defense services presently use this orbit for remote sensing, reconnaissance, and weather observation missions (Crook, 2015; U.S. Navy, 2020). Consequently, LEO yields the DOD an opportunity to offload its IoT-friendly data from its GEO and polar satellites while increasing its communication resources and its space-based data capacity in remote and contested regions.

The challenge with this concept lies in the currently available IoT waveforms compatible with space-based communications. IoT architectures were originally designed with terrestrial communications in mind, so many IoT waveforms lack the range to reach space. Others that may have the necessary range have inherent security risks to the DOD. These security risks stem from the proprietary nature of the waveforms and the countries associated with the company that owns the rights to that waveform (Executive Order No. 13873, 2019). Careful examination of an IoT waveform's compatibility and background is necessary to determine if one that currently exists could be used by the DOD to transmit IoT data via a LEO constellation.

Overcoming these challenges would be highly beneficial to the DOD because current military-owned, space-based communications lack resiliency. Resiliency facilitates maneuverability within the electromagnetic spectrum and adds depth to DOD communication plans. In order to enable resilience, multiple communication paths through a variety of frequencies are required. Presently, the DOD relies heavily on SATCOM to provide command and control (C2) in remote and isolated environments. However, numerous signals that the DOD transmits may be suitable for IoT protocols and therefore for offloading to a LEO IoT constellation.

A. PURPOSE STATEMENT

This research seeks to support the Naval Postgraduate School (NPS) Center for Network Innovation and Experimentation (CENETIX) team's exploration of LEO IoT mesh networking node expected to be launched by the Firefly rocket and designated as the Firefly CENETIX Orbital-1 CubeSat. The CubeSat is a 2U (approximately 1 kg) Commercial Off the Shelf (COTS) satellite designed to demonstrate "Bursty Orbital Mesh Networking" (Bordetsky, n.d.). After the discovery of security threats in the Orbital-1's original waveform, an alternative was deemed necessary. The aim of this study is to directly contribute to the Orbital-1 CubeSat's resilient networking, system engineering process by identifying possible sources for alternative communication uplinks. Should a viable substitute be found, the authorized launch of the Orbital-1 will contribute valuable information on space-based IoT communications.

In addition to identifying IoT waveforms compatible in range and security, this study will also consider several key parameters necessary to support an IoT LEO CubeSat mesh concept for the DOD as a means to ensure any waveforms selected fit DOD communication requirements. The creation of a LEO CubeSat mesh with low-power, long-distance waveforms can enable bursty transmissions capable of carrying many kinds of small data packets. These data types include Bit Error Rate (BER), Signal-to-Noise (SNR) ratio readings, and data from small devices in IoT networks. This capability can expand the use of enterprise management systems for the monitoring and managing of self-forming mesh networks while also providing diversification to DOD SATCOM.

B. POTENTIAL BENEFITS AND LIMITATIONS

This research is beneficial in providing one of the first comprehensive, comparative analysis of current and near-future IoT waveforms in search of a viable alternative for the Orbital-1 transmission uplink. Both licensed and unlicensed frequency spectrum technologies are assessed for their capability to carry DOD signals and potentially integrate into the Joint All Domain Command and Control (JADC2) architecture. This research aims to support the integration of IoT into the DOD and highlight opportunities to improve DOD SATCOM diversity.

This study is limited by the fact that a feasible alternative IoT waveform for the Orbital-1 may not yet exist. If an option does exist, it may lack integration compatibility with current SATCOM systems and may be too expensive to implement. Recommendations will be based on analytic outcomes and the potential for future research.

C. RESEARCH QUESTIONS

The underlying idea of this research is the potential for an IoT constellation in LEO to provide an alternative, space-based communication platform to military units in remote and isolated environments while also offering increased overall SATCOM capacity and resiliency. Therefore, this thesis seeks to answer the following research questions.

1. Is there an alternative chirp spread spectrum (CSS) transceiver with the same form, fit, and function as the Semtech-based LoRaWAN transceiver that can meet the DOD requirements for use on the Orbital-1 CubeSat?

2. Is there an alternative to the LoRaWAN waveform that will meet the requirements for long-distance, low-power communications required for the Orbtial-1 CubeSat?

D. THESIS OUTLINE

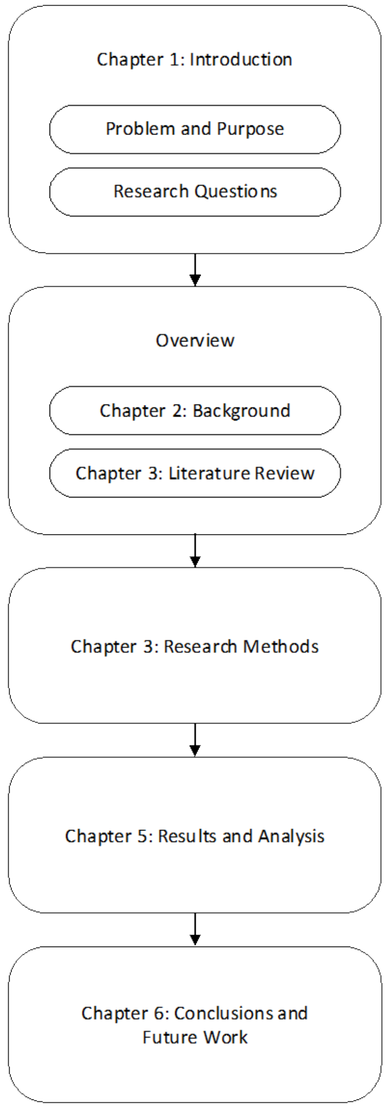

Figure 1. Thesis Outline. The First Three Chapters Provide Background Information. The Last Three Chapters Present the Results and Their Implications.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

This chapter is designed to provide a foundational understanding of key IoT terms and concepts. The chapter starts by defining IoT and correlating the seven-layer IoT architecture to the well-known Open System Infrastructure (OSI) Model. Then the four different categories of IoT protocols are briefly discussed. The section is followed by terms often confused with and within IoT. Finally, the chapter ends by discussing the concept of transmitting IoT data over satellite resources.

A. DEFINING IOT

As technology advances, more and more devices, or *things*, are becoming connected to the internet, to local networks, and to one another in a mesh architecture. According to the Internet Engineering Task Force (IETF) (2015), things can be classified into three categories: people, machines, and information. These things must be connected in such a way that they can intelligently interact with one another to make an effective IoT system (Iqbal et al., 2021, p. 5). The IETF provides nine identifying features of an IoT system:

1. Part of an interconnection of things
2. Connection of things to the internet
3. Uniquely identifiable things
4. Ubiquity
5. Sensor-actuator capability
6. Embedded intelligence
7. Self-configurability
8. Interoperable communication capability
9. Programmability. (IETF, 2015, pp. 72–73)

Based on these features, the IoT is a "self-configuring, adaptive, complex network that interconnects 'things' to the internet through the use of standard communication protocols" (IETF, 2015, p. 74).

Instrumental to a foundational understanding of IoT is the Seven-layer IoT Architecture with respect to the OSI Model, illustrated in Figure 2. The OSI Model is a well-established reference in the information sciences field and therefore a useful tool to understand IoT system concepts against. The layers of the IoT Architecture include Things; Edge Computing; Data Accumulation; Data Abstraction; Application; and People Collaboration and Processes (Iqbal et al., 2021, pp. 21–23). While the layers of the OSI Model consist of Physical, Data-Link, Network, Transport, Session, Presentation, Application, and the Human-Computer Interaction (HCI) (Bauer & Patrick, 2002). HCI was added to the traditional OSI stack by Benjamin Bauer and A. Patrick (2002) to facilitate a common language between practitioners and developers while also capturing the human requirements and interactions of networks. This added layer is highly valuable when examining the Seven-layer IoT architecture because it takes into consideration the end user of the data and how best to present it to maximize its usefulness for a specific consumer.

Iqbal et al. (2021) determined the Things layer includes the endpoint devices that will send and receive information. The Things layer closely aligns with the physical layer of the OSI model, which can be defined as the media used for communication (Zito, 2013). At the connectivity layer, the things transmit their data over their local mesh to other intelligent devices and across various networks through assorted gateways. This IoT Architecture layer combines the aspects of four layers in the OSI Model. The layers include: the Data-Link, the Network, the Transport, and the Session layers. The Data-Link layer enables local network, node-to-node, connection, while the Network layer connects the local network to other networks (the internet) (Zito, 2013). Then the Transport layer offers reliable or unreliable data transfer on that network, and the Session layer establishes the connection between two nodes (*1-3 OSI reference model*, 2013). Next, the Edge layer, Data Accumulation layer, and Data Abstraction layer from the IoT Architecture align with the OSI Presentation layer and, generally speaking, prepare the data for the Application layer. According to Iqbal et al. (2021), the Edge layer for IoT transforms heterogeneous network data by "data formatting, reduction, decoding, and evaluation" to prepare it for standardized storage at the Data Accumulation layer. In addition to storing the data, the Accumulation layer also performs some filtering of the IoT data (Iqbal et al., 2021). The data is then gathered and standardized further at the Data Abstraction layer to prepare it for application ingestion (Iqbal et al.; 2021). Then the Application layer in both the IoT Seven-Layer Architecture and the OSI Model enables the interpretation of the processed data. Lastly, the Collaboration layer from the IoT Architecture consists of human data interpretation and collaboration with other IoT applications and users, which is near-identical in purpose to Bauer and Patrick's (2002) HCI layer of the OSI Model.

Figure 2. An Evaluation of Iqbal et al.'s (2021) Seven-layer IoT Architecture in Reference to the OSI Model. Adapted from *1-3 OSI Reference Model* (2013); Bauer and Patrick (2002); GeeksforGeeks (2022); Iqbal et al. (2021); and Zito (2013).

B. IOT WIRELESS INFRASTRUCTURE PROTOCOLS

In general, numerous wireless IoT infrastructure protocols reside within the first three layers of the OSI Model and are capable of transmitting IoT data. These wireless protocols can be cataloged into four different categories: Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), cellular, and Low power wide area network (LPWAN) (Putland, 2020). The protocols can then be further categorized based on their transmission frequencies belonging to the licensed or unlicensed frequency spectrum.

WPAN is the first of four IoT protocol categories that can be considered when searching for an alternative IoT waveform for the Orbital-1 CubeSat. The (Wireless) Personal Area Network (PAN) is designed to connect a collection of devices that reside within close proximity to one another (Gratton, 2013). The network is described as personal based on the concept of linking several peripheral devices to a single-user computer. For example, one PAN could hypothetically consist of a personal computer, a cordless keyboard, a cordless mouse, and a printer (Gratton, 2013). When these devices are connected wirelessly, they use a radio frequency (RF), WPAN protocol (Gratton, 2013). Some WPAN protocols include Bluetooth, Bluetooth Low Energy (BLE), Zigbee, and IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) (Coleman & Westcott, 2021; Gratton, 2013). All of these standards operate in some or all of the unlicensed frequency bands of 868 MHZ, 915 MHz, and 2.4 GHz, and all are suitable for transmitting IoT data (Hackmann, 2006; IEEE, n.d.). While WPAN has many benefits like the ability to connect several unrelated assets, its primary limitation from the perspective of this study is that its limited range makes it incompatible for use to connect to a satellite 150+ km above the surface of the earth.

In contrast to the single-user nature of WPAN, WLAN's WiFi protocol offers wireless access to hundreds of users within a building or campus, while also providing these assets a gateway to other networks via the internet (Coleman & Westcott, 2021). However, like WPAN, WLAN also operates in the 2.4 GHz unlicensed frequency spectrum (Coleman & Westcott, 2021). Though, WLAN technologies can also transmit in the 5GHz and the recently released 6 GHz unlicensed frequency bands (Coleman &

Westcott, 2021; FCC, 2020). WLAN offers an increased transmission range and higher data rates compared to WPAN (Putland, 2020). Although WLAN has an improved transmission range compared to WPAN, the range is still insufficient to reach LEO.

Cellular networks are the first of the four categories that may have sufficient range to reach LEO. They provide an alternative mid- to long- range transmission path for assets that lack access to the internet (Milenkovic, 2020; Putland, 2020). Mobile cellular networks were initially designed to enable voice communications, then as technology advanced, data transmission was added to the network (Putland, 2020). Specific to IoT, five promising cellular protocols from the licensed spectrum include Extended Coverage Global System for Mobile Communications IoT (EC-GSM-IoT), Long-Term Evolution for Machine-Type Communications (LTE-M), Narrowband IoT (NB-IoT), LTE Ultra-Reliable and Low Latency Communication (LTE URLLC), and New Radio URLLC (NR URLLC) (Liberg et al., 2020). As Table 1 shows, these standards are compatible with the existing cellular 2G, 3G, 4G, and 5G networks (Coleman & Westcott, 2021).

Table 1. Cellular IoT Protocol to Cellular Network Generation Compatibility

	2G (GSM)	3G	4G (LTE)	5G
EC-GSM-IoT	X[b]	X[b]	X[b]	
LTE-M			X[a,c]	X[a,c]
NB-IoT	X[a,c]		X[a,c]	X[a,c]
LTE URLLC				X[a]
NR URLLC				X[a]

Note: Adapted from Coleman & Westcott, 2021[a]; Hwang, 2022[b]; Onomondo, 2021[c].

LPWAN is the last of the four IoT protocol categories, and it presently provides the longest transmission path of the four options, and therefore is also a candidate for transmission to space (Putland, 2020). However, Paul Putland (2020) notes that in return for distance, the protocol does sacrifice its data rate. The technology was designed to support devices that require long-range communications for transmission of intermittent, small amounts of data with a lower receive priority (Putland, 2020). The protocols operate in the unlicensed frequency spectrum, typically in frequencies below 1 GHz (Putland, 2020). LPWAN devices are designed to have low power requirements and a long battery life, while also competing in the unlicensed spectrum for transmission time (Putland, 2020). Four LPWAN protocols include Long Range (LoRa), SigFox, Weightless, and Ingenu (Putland, 2020). LoRa, which is based on chirp spread spectrum (CSS) modulation, is the most established of the four protocols. CSS is a combination of the two concepts: a chirp, sinusoidal signal and the use of frequency spread spectrum (Bocker, Arendt, Jorke, & Wietfeld, 2019). In CSS modulation, the signal frequency changes at a constant rate across the entire bandwidth to encode information (Bocker, Arendt, Jorke, & Wietfeld, 2019).

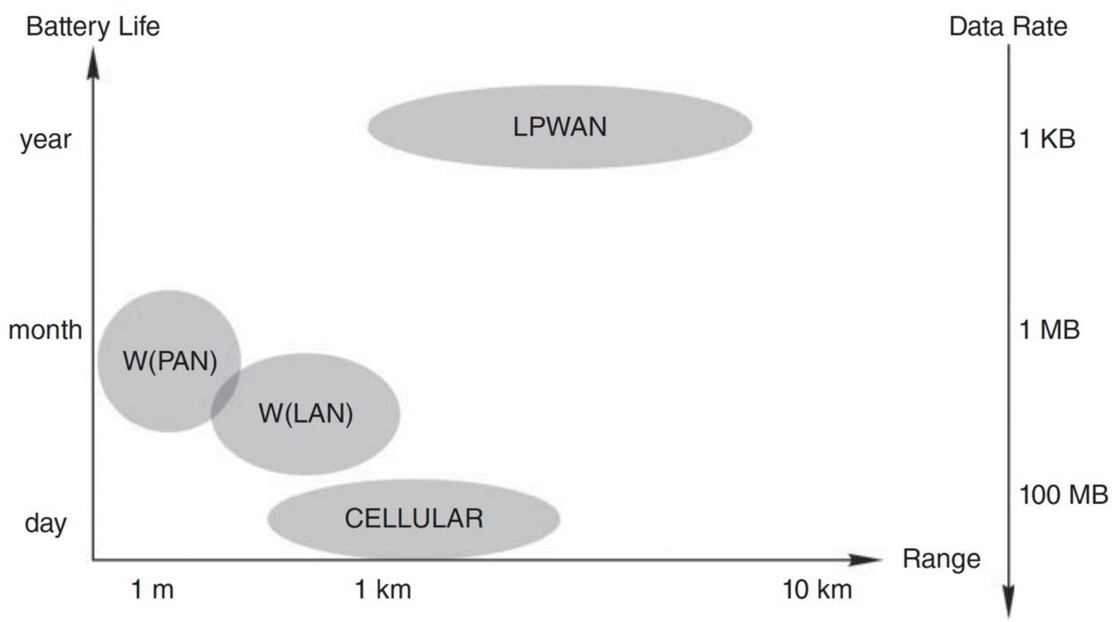

Figure 3. Comparison of IoT Protocols Battery Life, Range, and Data Rate. Source: Putland (2020).

C. SUBSETS OF IOT: M2M, WSN, AND CPS

The information sciences practitioners and scholars have explored the relation between IoT and several related wireless technology concepts due to the variations in IoT terminology and several concepts that fall into subcategories of IoT. Most correlated with this research are cyber-physical systems (CPS), machine-to-machine (M2M), and WSNs. Understanding the relationship between IoT and these associated concepts is extremely valuable when searching for an alternative IoT waveform for the Orbital-1 and subsequently designing an IoT operational concept because academia and the private sector sometimes refer to technology by these terms without a clear linkage to IoT. However, their work could be more narrowly focused but highly related to this thesis.

CPS is a term sometimes used interchangeably with IoT. However, Iqbal et al. (2021) highlight that CPS is more frequently used in the engineering field to define embedded devices that can "transmit physically sensed data over the network," whereas IoT is used in the information sciences to describe the same systems but with a focus on the next-generation network's quality of service (QoS) and handling of big data. Nonetheless, according to the National Institute of Standards and Technology (NIST) (2019), the terms CPS and IoT are converging through a common emphasis on hybrid systems engineered to operate rotted in integrated logic. The union of these notions will bring standardization in classification and research related to IoT (NIST, 2019).

Information science scholars like Iqbal et al. (2021), Wang and Fapojuwo (2017), and Park and Kim (2015) generally accept that M2M is a subset technology of IoT. In an M2M network, communication occurs among machines (devices) with computing and communicating capabilities, outside of human intervention (Wang & Fapojuwo, 2017). Based on the IETF definition of things encompassing people, machines, and information, M2M communication is therefore only a portion of the larger IoT ecosystem (IETF, 2015). Machines in M2M networks are typically designed to require marginal on-device computing, consume minimal amounts of energy, and have a low transmission power requirement in order to be battery powered (Minoli, 2015; Wang & Fapojuwo, 2017). Further, M2M networks are compatible with all four IoT protocol categories: WPAN, WLAN, cellular, and LPWAN (Adame et al., 2014; Liberg et al., 2020, p. 45; Park & Kim, 2015; Wang & Fapojuwo, 2017).

Iqbal et al. (2021) describe WSN as another subset technology under the IoT umbrella. They state a WSN consists of a set of ad hoc RF sensors used to "monitor, record, and transmit [the] physical parameters of an entity to a central location" (Iqbal et al., 2021). Their ad hoc nature supports IETF's broader parameter of IoT system self-configurability (IETF, 2015). WSNs are capable of transmitting smaller datasets like temperature, atmospheric, and environmental chemical content, as well as larger data like low- and high-resolution video (Minoli, 2015). Tetcos (n.d.) delineates that IoT enables each WSN to connect to a gateway and therefore to other networks, while without IoT, the WSN would only be a local network of sensors. Due to the remote nature of WSNs, they are often based on LPWAN and cellular IoT protocols (Minoli, 2015; Wu et al., 2020).

D. IOT OVER SATCOM

Satellites have been used to transmit IoT data for over a decade already, but as the number of connectable things increases, so has the research into the potential use cases for transmitting various forms of IoT data via satellite (Inmarsat, 2022). The first satellites to dedicate bandwidth to IoT were from Mobile Satellite Service (MSS) providers like Iridium, Orbcomm, and Inmarsat (Minoli, 2015, p. 232). MSS is a classification of satellites designed to provide communications to users with moving or transportable terminals, contrasting with fixed satellite service (FSS) systems which were traditionally used to communicate with stationary ground terminals (Minoli, 2015, p. 3,165). Daniel Minoli (2015, p. 3) states that most MSS providers place their satellites in LEO or MEO orbit, while FSS systems typically use GEO for broadband services.

Iridium and Orbcomm were some of the early implementors of IoT into LEO (Fierce Electronics, 2013; Iridium, 2020). Iridium introduced its trademarked Short Burst Data (SBD) in 2003 as a satellite transport network to bring IoT field data to a centralized computing site (Iridum, 2020). Their constellation currently consists of 66 LEO satellites facilitating global network coverage (Iridium, 2021). Orbcomm's Generation 2 (OG2) satellites were designed with M2M in mind (Krebs, 2008). Since 2014, 17 OG2 satellites have been successfully launched into LEO orbit (Orbcomm Satellites, n.d.). These MSS providers likely chose to build a LEO constellation to minimize the transmission range and therefore offer their customers smaller, more mobile terminals such as the two examples shown in Figure 4 (Orbcomm, 2021b).

Figure 4. Examples of Iridium and Orbcomm Mobile Satellite Terminals for IoT. Iridium source: *Iridium Edge Datasheet* (2020). Orbcomm source: *Orbcomm ST6100 Datasheet* (2021a).

In contrast with Minoli, Iridium, and Orbcomm, Inmarsat chose to establish its global IoT-capable constellation, ELERA, in GEO (Inmarsat, 2022). The constellation is made up of four satellites, and IoT support is only one of its four missions (Inmarsat, 2022). In addition to IoT, the constellation also supports broadband services for mobile land, air, and sea platforms (Inmarsat, 2022). Since the ELERA constellation is primarily for broadband services, its location in GEO conforms to the conventional use of that orbit (Minoli, 2015, p. 3). However, due to the increased distance to GEO, Inmarsat's satellite terminals require more power and a larger antenna. These requirements result in the larger form factor shown in Figure 5.

Figure 5. Hughes-branded Inmarsat Broadband Global Area Network (BGAN) M2M Satellite Terminal. Sources: Hughes *9502 BGAN Terminal Brochure* (2013) and *Asia Satellite* (n.d.). Note: The image only shows the outdoor unit (ODU), which is 38.5 cm x 38.5 cm x 3.3 cm. The indoor unit (IDU) containing the modem is an additional 15 cm x 20 cm x 45 cm.

These early SATCOM IoT implementors focused on providing service compatible with M2M data. However, the development of emerging technologies, like 5G, is opening the door for additional IoT data types over SATCOM. Concepts like wide area IoT services for critical infrastructure, autonomous driving, and remote surgery require higher reliability and a near-real-time communication link (less than one millisecond) (Onireti & Imran, 2018). By contrast, massive machine-type communication (mMTC) models are concerned with providing communications availability to a huge number of assets competing for resources (Soret et al., 2021). As connected as the world is today, the ability to connect even the smallest and most remote IoT devices to the internet via SATCOM will expand the global network by orders of magnitude.

E. SUMMARY

This research defined IoT based on the IETF features and definition and then examined how the seven-layer IoT architecture relates to the OSI model. The architecture-model comparison is meant to be a valuable reference for later analysis of components in an IoT system and the types of standard network communication necessary to support them. Further, a foundational understanding of the four wireless IoT protocol categories was discussed along with some terms closely associated with IoT. Finally, the background on IoT over SATCOM highlighted how it is not an entirely new concept. In fact, companies have been doing so for over a decade. However, IoT is growing, and so are the mission sets that IoT over SATCOM could support.

III. LITERATURE REVIEW FOR IOT IN SPACE

Based on the five research questions noted in Chapter I, this literature review is broken into three broad themes. The first section covers the views of academia, the private sectors, and the DOD on which orbits in space are ideal for IoT communications. The next section examines the communities' perspectives on the use of CubeSats in a LEO IoT constellation. Then the third section discusses the discourse on which IoT protocol is best for space-based communications. Within the section on IoT protocols, key government regulations that delineate the ability of the DOD to use a technology compared to academia and the private sector are highlighted.

A. SPACE ORBITS FOR IOT

When it comes to the ideal orbit to support an IoT architecture, the information sciences agree near-unanimously that LEO is their first choice. Giuseppe Cocco and Christian Ibars conclude in their study *On the Feasibility of Satellite M2M Systems* (2012) that LEO provides a more favorable link budget, while a comparable GEO configuration generates too low of an SNR to remain reliable for IoT devices. Likewise, Kenneth Peterson (2003) emphasizes LEO's shorter transmission path and consequently more favorable link budget, which means a more reliable link can be established with less power and a smaller antenna, hence at less cost than GEO. Further, Minoli (2015, p. 272) highlights LEO's benefits of low-latency communication links and superior performance in inclement weather. All of these conditions make LEO the ideal orbit choice when designing a distributed IoT network full of small, limited capacity devices.

The private sector agrees with academia that LEO is the ideal orbit for IoT. Established companies like Telesat and OneWeb and start-up companies like Sateliot are all investing heavily in creating a LEO satellite constellation capable of transmitting IoT data (OneWeb, 2022; Sateliot, n.d.; Telesat, 2022). For Telesat and Oneweb, IoT is a secondary mission, while for Sateliot, it is currently their only mission (OneWeb, 2022; Sateliot, n.d.; Telesat, 2022).

Where scholars diverge, however, is on the key technological advancements necessary to establish a LEO IoT architecture. A 2021 study titled *A Survey on Technologies, Standards, and Open Challenges in Satellite IoT* highlighted numerous satellite IoT enablers, including network function virtualization (NFV) in support of network slicing, offloading solutions such as edge computing, and flexibility at the physical layer of the OSI model through software defined radio (SDR) technology (Centenaro et al., 2021). Kua et al. (2021) agree on some of these IoT enablers, like the importance of NFV and edge computing, but they also believe terrestrial-space network integration and intersatellite links (ISL) are vital to a successful IoT space-based architecture. Yoon, Frese, and Briess' (2019) research supports Kua et al.'s (2021) emphasis on ISLs. Their research focuses on an IoT satellite network design where the use of ISLs is key to balancing capacity and reducing latency in mesh satellite networks.

The DOD sees great potential in all of these IoT-enabling technologies, but it is not currently pursuing them with IoT or LEO specifically in mind. For example, Defense Information Systems Agency (DISA), the DOD Information Network (DODIN) provider, implemented NFV on their networks in the Pentagon in 2022 to enable control of network functions and policies through software instead of hardware, thereby reducing the time it takes to make changes on a network and thus enhancing the network's cybersecurity (GDIT, 2022; Goldstein, 2021). The DOD was also an early implementer of ISLs. Its Milstar extremely high frequency (EHF) satellite constellation, whose first satellite launched in 1994, relies on ISLs to provide part of the constellation's secure communications and global coverage (USAF, 2015; USSF, 2021).

Unlike the previous examples, edge computing in the DOD closely aligns with the IoT enablers promoted by academia. The JADC2 hypothetical architecture is heavily reliant on sensors and devices operating at the edge (DOD, 2022). This concept seeks to standardize and integrate data regardless of the platform or environment it originated in (DOD, 2022). Further, the *Summary of the JADC2 Strategy* specifically calls out the significant need to "maintain an information advantage … in cyberspace, space, and the electromagnetic spectrum," a task ideal for IoT devices (DOD, 2022).

Still, there is a theoretical gap for the use of a LEO orbit for IoT within the DOD. Although academia and the private sector are exploring these emerging technologies, the requirements for systems within the DOD are more rigorous and lengthier. The DOD implementing some of these emerging technologies in non-IoT applications is a good first step, but further exploration into the use of LEO to support IoT friendly data is valuable given the DOD's constrained SATCOM capacity and need for resilient communications.

B. CUBESATS

Although researchers advocate for LEO as an IoT orbit, the use of CubeSats in LEO for the creation of an IoT network is less agreed upon by scholars. On one side, researchers like Jamal Arifin (2021); Tomás Ferrer, Sandra Céspedes, and Alex Becerra (2019); and Nasir Saeed et al. (2020) point to the COTS, low-cost nature of the CubeSat as an argument for its use in a LEO IoT architecture. Others like Mauro De Sanctis et al. (2016) agree with them but add the possibility to launch CubeSats as a secondary payload, which greatly reduces launch costs, sometimes to zero. Historically, CubeSats have been used by academia to conduct research based on these features. Conversely, scholars like Mohammad Afhamisis and Maria Rita Palattella (2022) and Kua et al. (2021) caution that CubeSats may not be suitable for every IoT use case due to their lower data rates and lack of continuous coverage. This fact is especially true for future 5G IoT protocols like NR URLLC, which are being designed to support things like remote surgery, emergency response, smart grid load control, and self-driving vehicles that can tolerate one millisecond of latency (Barros, 2019; Soret, Leyva-Mayorga, Cioni, & Popovski, 2021).

Researchers also hold differing views on the best deployment concept for CubeSats in LEO. Some, like Soret et al. (2021), Centenaro et al. (2021), and Saeed et al. (2020), believe a swarm of CubeSats with ISLs is necessary to provide continuous coverage to ground stations. Others like Juan Fraire and his two teams of researchers (2019, 2020) are exploring IoT direct-to-satellite (DtS-IoT) options, which can support sparse satellite constellations. In Fraire et al.'s 2020 study, they concluded that nine satellites are sufficient for a sparse IoT constellation compared to the 88 necessary for a dense constellation. The biggest difference in concepts again depends on the type of IoT data transiting the network. If the data requires minimal latency communications, then a swarm IoT network is a better match. On the other hand, if the data is designed to be transmitted intermittently, the use of DtS-IoT may reduce costs while still providing the necessary resources.

The relatively low-cost, low-risk nature of CubeSats has drawn the attention of academia and private sector communities alike (Fraire et al., 2020). The low barrier to entry and uniqueness of IoT data has attracted many start-up companies solely focused on developing CubeSat constellations for IoT. Lacuna Space and Eutelsat are two newer companies implementing LPWAN IoT protocols in LEO CubeSat networks to bridge terrestrial and space communications as well as provide access to remote areas (Eutelsat, n.d.; Launa Space, n.d.). Sateliot is another start-up company building a LEO IoT constellation. However, they are exploring the use of cellular protocols for their network (Sateliot, n.d.).

Unlike academia and the private sector, the DOD has been tentative with its investments in CubeSats so far. Organizations within the DOD such as the National Reconnaissance Office (NRO), U.S. Army Space and Missile Defense Command (USASMDC), and Airforce Research Laboratory (AFRL) have launched CubeSats primarily as technology demonstrations (Dailey, 2022; NRO, 2019; Strout, 2022). Their tests have spanned a vast array of missions. However, Perez (2022) noted that the AFRL did recently launch their Recurve CubeSat, which is designed specifically for testing "adaptive RF" communications. He stated, the AFRL Recurve interacts through mesh network behavior. This interaction improves the network's resilience and ability to move data across it (Perez, 2022). Nevertheless, the DOD is minimally invested in CubeSats, especially for communication missions. Moreover, the current CubeSat capabilities of the DOD are not fully operational and ready to handle military missions. Instead, they are in the beginning stage of testing.

The use of CubeSats in LEO for IoT protocols is a relatively new field with several knowledge gaps remaining. Some previously mentioned examples include, the fact that there is no current consensus in academia or the private sector about what IoT protocols a CubeSat can handle or which CubeSat deployment architecture is best for a given IoT protocol. The DOD has shown reserve in its use of CubeSats. Although DOD research with CubeSats is expanding, there is little focused on SATCOM or IoT protocols, a potentially valuable tool for diversifying current DOD data.

C. IOT PROTOCOLS FOR LEO

Which IoT protocol is best for transmitting IoT data over a satellite is perhaps the least agreed upon research question related to this study. Most researchers often fall into one of two camps: LPWAN protocols for space-based IoT or cellular protocols for space-based IoT. More specifically, academia has primarily focused on LoRaWAN under the LPWAN umbrella and NB-IoT in the cellular protocols category. Information scientists like Muhammad Ullah, Konstantin Mikhaylov, and Hirley Alves (2022) and Qu et al. (2019) dedicated their research to the feasibility of using LoRaWAN for theoretical LEO IoT satellite constellations. Ullah, Mikhaylov, and Alves (2022) examined direct and indirect communication approaches with LEO satellites and conclude a LoRaWAN-based LEO architecture is feasible. Qu et al.’s (2019) data supports Ullah, Mikhaylov, and Alves (2022) conclusion and also determines, based on simulations, that a LoRaWAN LEO constellation is achievable. Others like G. Sciddurlo et al. (2022); Rene Sorensen, Henrik Moller, and Per Koch (2021); and Timo Kellermann et al. (2022) examined potential NB-IoT satellite architectures and noted great potential in their use in remote locations supporting delay-tolerant IoT devices. Still others including Stephen Ugwuanyi, Greg Paul, and James Irvine (2021); Ala Khalifeh et al. (2021); and Centenaro et al. (2021) conducted surveys comparing IoT protocols and their utility in space. Ugwuanyi et al. and Khalifeh et al. (2019) both found NB-IoT is ideal for IoT data with high throughput and low latency requirements, while LoRaWAN is best for IoT networks with power efficiency as their main priority.

Outside of the two main IoT protocol camps, some researchers are looking for additional IoT SATCOM solutions. Sigfox is a LPWAN technology that is one alternative which Khalifeh et al. (2019) and Centenaro et al. (2021) examined. Both research teams noted Sigfox’s compatibility for IoT systems that require very low data rates (a total of 140 12-byte uplink messages a day and 4 8-byte downlink messages per day [Centenaro et al., 2021]). J. Queralta et al. (2019) and Wang and Fapojuwo (2017) also examined Sigfox and further demonstrated its limited data rates by noting its compatibility for very time-sparse meter sampling. Ingenu Random Phase Multiple Access (RPMA) was also assessed in Queralta et al. (2019) and Wang and Fapojuwo (2017)'s studies. Ingenu RPMA is another LPWAN technology. However, it is specifically designed for two-way M2M communications. The researchers found Ingenu RMPA can be an ideal match for systems involving high data rates and very minimal latency (10s of seconds). These less conventional IoT protocols are compared against the more typical LPWAN and cellular protocols in Figure 6.

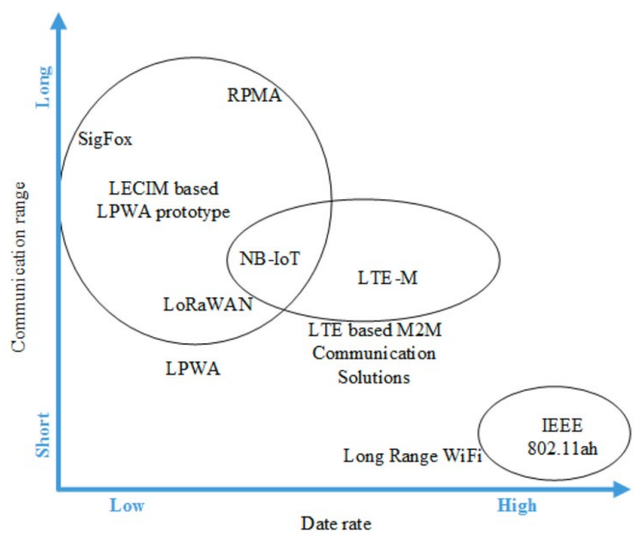

Figure 6. Comparison of IoT Protocols in Relation to Data Rate and Range. Source: Wang and Fapojuwo (2017).

The private sector is also at odds over the best IoT protocol for a LEO IoT satellite constellation. The previously mentioned Lacuna Space and Eutelsat along with Ingenu-Phantom Space are all creating LPWAN SATCOM architectures. Lacuna Space is exclusively deploying a LoRaWAN constellation, while Eutelsat's schema will be compatible with both LoRaWAN and Sigfox (Eutelsat, n.d.; Lacuna Space, n.d.). Ingenu-Phantom Space, however, has plans for a LEO constellation with 72 satellites based on the Ingenu RPMA M2M protocol (Weissberger, 2021). In the other camp, Sateliot is the only private company currently developing a NB-IoT LEO constellation (Sateliot, n.d). There is one other company demonstrating NB-IoT through space communications, Skylo, however, their services currently ride Inmarsat's GEO satellites (Swinhoe, 2021).

Whether for terrestrial or space-based networks, the DOD has done very little publicly released testing of these IoT protocols. Moreover, none of the protocols is currently part of any program of record (POR) system in the military. These facts leave a very large knowledge gap regarding how the implementation of IoT protocols could benefit DOD communications. This is especially important due to the overtasked DOD SATCOM infrastructure, the massive digital data requirement in the field, and the amount of DOD data that could be offloaded to IoT protocol-based systems.

Unfortunately, the DOD cannot just take research and concepts developed by academia and the private sector and put them to use in the DOD. Due to security threats and the risk of electromagnetic spectrum interference, the DOD must comply with U.S. government regulations. Several of the private sector companies previously mentioned are based in Europe and do not have the same frequency allocations that the Federal Communications Commission (FCC) mandates in the U.S. For example, the unlicensed frequency bands used for LoRaWAN and Sigfox are designated by the FCC for services like RF devices; private land mobile; amateur radio; and industrial, scientific, and medical equipment (ISM), but not space-based communications (FCC, 2022a). Moreover, the FCC has further regulations on those frequencies that fall into ISM bands, such as limitations to device generated RF power and transmission range (FCC, 2022b).

Finally, the most significant limitation on the DOD is security. *Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019* forbids government agencies from purchasing telecommunications and video surveillance equipment from unauthorized companies that have ties to collecting intelligence on the U.S. through their technology:

> The head of an executive agency may not— (A) procure or obtain or extend or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a

> substantial or essential component of any system, or as critical technology as part of any system; or (B) enter into a contract (or extend or renew a contract) with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. (NDAA, 2018, p. 132 STAT 1917)

The Fiscal Year (FY) 2019 NDAA also explains the definition of covered telecommunications and provides which companies meet the definition at the time of its writing:

> The term ''covered telecommunications equipment or services'' means any of the following: (A) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities). (B) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities). (C) Telecommunications or video surveillance services provided by such entities or using such equipment. (D) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country. (NDAA, 2018, p. 132 STAT 1918)

As shown above in the noted passages, the covered telecommunications equipment and services list began with just four companies who were deemed a threat to U.S. security interests.

However, following the release of the FY2019 NDAA, Executive Order 13873 (2019, p. 22689) expanded telecommunication equipment purchase limitations and stated transactions are prohibited if the technology was “designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.” Use of equipment is also prohibited if the technology “poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services" or "poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States" or "otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons" (Executive Order No. 13873, 2019, p. 22690). In addition to the broad threat expansion to telecommunications under Executive Order 13873, the FCC now maintains an active list of covered communications equipment and services that have been determined by the Public Safety and Homeland Security Bureau to be a threat to the U.S. (FCC, 2022c). The covered list currently contains eight companies from People's Republic of China (FCC, 2022c). The latest additions to the list in March of 2022 were linked with an order that banned PacificNetworks Corp. and ComNet (USA) LLC from providing services in the U.S. due to their approximate "58% indirectly owned and controlled by" the CITIC Group Corporation, which is a Chinese state-owned company (FCC, 2022d).

Due to these security risks and the regulations in the electromagnetic spectrum, the DOD must be cautious and strategic in the kinds of communication systems it designs and in the components it selects to build these systems. These challenges must be balanced with the need of the DOD to expand and harden its communication resources. The lack of studies within the DOD on IoT protocol use either in space or for terrestrial networks is therefore a significant gap worth exploring.

D. SUMMARY

This research draws upon three major concepts: which orbit is best for IoT in space, CubeSats as a satellite of choice in LEO, and which IoT protocol is best for space-based communications. Based on this research, it is clear that the use of LEO for an IoT network in space is highly preferred by both academia and the private sector due to its positive attributes, such as low overall cost and minimal transmission latency. However, there is less agreement on the architectural design of a LEO IoT orbit. This statement is true regarding the key technologies to include in a system design, as well as which deployment concept is best for an IoT CubeSat constellation in LEO. These disagreements are likely due to the novelty of IoT in space and most concepts still being theoretical. Further, there are two main camps of thought on which IoT protocol is best for use in space: LoRaWAN and NB-IoT. Some private sector companies are beginning to launch CubeSats with these two IoT protocols as their waveform.

However, the DOD is minimally invested in all three of these major areas, especially the use of IoT protocols to diversify and expand its communication base. Several important gaps identified in this literature review will benefit from further study and inquiry. This research aims to help fill these gaps.

IV. METHODS

This chapter details the research methods used to address the primary research questions: "1. Is there an alternative chirp spread spectrum (CSS) transceiver with the same form, fit, and function as the Semtech-based LoRaWAN transceiver that can meet the DOD requirements for use on the Orbital-1 CubeSat?" and "2. Is there an alternative to the LoRaWAN waveform that will meet the requirements for long-distance, low-power communications required for the Orbital-1 CubeSat?" The chapter begins with an examination of the philosophical assumptions and the design concepts underpinning this study, followed by a discussion of the methods used for data collection and analysis. Next, the limitations to the study's methods are highlighted. Finally, the variables for identifying alternative IoT waveforms and replacement transceivers are defined.

A. RESEARCH DESIGN

This research is founded on a pragmatic worldview. As John Creswell and David Creswell (2018) note this perspective emphasizes "the research problem and question and use [s] all approaches available to understand the problem" (p. 10). Further, pragmatists are concerned with what works and finding solutions to identified problems (Creswell & Creswell, 2018). This worldview also accepts that research occurs in multiple contexts including technical, social, and political (Creswell & Creswell, 2018). Pragmatists traditionally take a mixed methods approach to research which includes both quantitative and qualitative methods. However, based on the research questions selected in this study, only quantitative analysis is necessary. The quantitative method is chosen because it enables the collection and assessment of the numerical properties of the CubeSat transceiver components as well as various IoT waveforms. These data are necessary to compare the alternatives, analyze their compatibility with the Ortibal-1 CubeSat, and then generalize the results to space-based IoT for the DOD. Further, this application is able to consider the social-political limitations of government and international regulations in a binary fashion; either the solution meets the current regulations, or it does not.

In particular, the research design for this study is a descriptive comparative research approach based on quantitative methods. Sandra Siedlecki (2020) explains that the purpose of descriptive research is the depiction of conditions or events by studying them as they are in the world, as opposed to models or simulations. She further states, "the researcher does not manipulate any of the variables but rather only describes the sample and/or the variables" (Siedlecki, 2020). Therefore, through the use of this observational research method, none of the variables included in the study are influenced during the research process (Voxco, 2022). Further, this type of research does not necessitate the isolation of an independent variable. Instead, all the variables are studied in relation to the other variables within the scope of the research project (ORI, n.d.).

Descriptive comparative research is the best match for this study due to the freedom from identifying one independent variable. Several equally valuable variables must be assessed to identify an alternative IoT waveform capable of space communications and when searching for an alternative transceiver for the Orbital-1 CubeSat. Further, this area of research is emerging, and there is value in the establishment of associations between the identified variables.

B. RESEARCH METHODS

The following subsections discuss the detailed approach taken to perform data collection and analysis in order to generate reliable and repeatable results.

1. Method Foundation

The research in this study focused on the collection of the key statistics necessary to evaluate replacement transceivers and alternative IoT waveforms for the Orbital-1 CubeSat. The study's analysis is based on existing datasets and therefore was conducted as secondary research. The time horizon for this study was cross-sectional and involved scholarly and commercial references from 2017 to 2022.

Although the identification of a replacement CSS transceiver was the first-choice solution for the CENETIX research team, a preliminary search determined that such components do not currently exist. LoRa is presently the only CSS-based transceiver on the market, and it is trademarked by Semtech (Pegulu, 2022). However, Semtech was found to have ties to the covered company, Huawei Technologies, and therefore their technology has been unauthorized for DOD telecommunications use (NDAA, 2018; Semtech, n.d.). The trademark indicates Semtech owns the technology, and other companies may only request to license LoRa's intellectual property (Bloechl, n.d.). Since Semtech owns the intellectual property, the schematics for the LoRa transceiver will be the same regardless of who builds them, and therefore they possess the same security risks as those produced by Semtech. Based on this knowledge, the study shifted to focus first on finding an alternative IoT waveform and then searching for an existing COTS transceiver to support the identified waveform.

2. Data Collection and Analysis Methods

The first step in the data collection process was to define the key variables for alternative IoT waveforms as discussed in Section C. After the variables necessary to address research question and 2 were established, an examination of existing research and scholarly literature on alternative waveforms was conducted. Several academic references were consulted per waveform for a handful of reasons. First, this area of research is emerging, and many of the waveforms in this research are not well studied for IoT. Next, since the present research is based on existing datasets, several sources were necessary to find the data points related to this study's variables. Lastly, multiple sources were used to increase the reliability of this study's results.

Data points were collected in a Microsoft Excel spreadsheet to sort and compare the different sources. For variables with a scholarly consensus, that value is referenced in this study. When the sources lacked consensus, the mode of the dataset was used as the variable's value. Finally, normalization was utilized on data points that were presented in different formats.

Following data collection and fusing of the IoT waveform data in Excel, the final data points were prepared in a table for an examination. First, descriptive statistics were used as a means to define the datasets quantitively (Lee, 2020). Waveforms with missing variables were noted in the table. Then the alternative waveform results were compared against the LoRaWAN parameters and LEO IoT constraints. Waveforms that were comparable to LoRaWAN or showed promise as a space-based waveform based on their primary variable results, were marked for further research into their COTS transceiver viability.

The second round of inquiry, for a COTS transceiver, was based on the variables identified in Section C, Table 4. Online electronic component databases like DigiKey and Octopart were the primary search engines used in this phase. Manufacturer datasheets were pulled from these sites to identify the necessary data points for alternative transceivers. Then the potential COTS transceiver data were placed in a table for assessment against the L04 LoRa transceiver. Next, data normalization was used to standardize the datasets. Finally, a descriptive comparative analysis was used to determine if the potential transceivers could replace the L04 in form, fit, and function.

3. Method Limitations

The primary limitations of this research were due to the data collection process and the time constraints of the study. Since the research relied on previous datasets, there were noted variations in data points as well as unattainable gaps in information. The gaps resulted in a less robust analysis. Further, the technology discussed in this study is emerging, so there is a lack of data on the IoT waveforms and a limited number of companies manufacturing IoT transceivers. Lastly, the study's constrained time prevented the application of other means to seek results for the absent data.

C. KEY VARIABLES

1. IoT Waveform Variables

The first step in identifying key variables was based on research question 2, which focuses on identifying an alternative waveform to LoRaWAN that will meet the low-power long-distance requirements of the Orbital-1 CubeSat. Due to the complexity of waveform parameters, nine variables were selected. Five were deemed primary variables due to their significance in determining if a waveform could be authorized, able to reach space, and support various types of IoT data. Four were classified as supporting variables for two distinct reasons: first, most of the supporting variables influence the outputs of the primary variables, and second, some of the supporting variables were regarded as “nice-to-haves” versus the primary variables’ “must-have” status. The five primary variables for an alternative IoT waveform are as follows:

a. Radio Frequency Spectrum

Saad Asif (2018) defines the RF spectrum as the “frequency range from 3 kHz to 300 GHz corresponding to wavelengths ranging from 100 km to 1 mm” (p. 15). The International Telecommunications Union Radiocommunications Sector (ITU-R) (1984) divides the RF spectrum into numerous frequency bands within that frequency range. The Institute of Electrical and Electronics Engineers (IEEE) further refines the RF spectrum and divides the ITU-R frequency bands into smaller frequency ranges with single-letter designations (IEEE, 1998).

The bands that relate to this study are shown in Table 2 and include ultra high frequency (UHF) and super high frequency (SHF) as well as their IEEE sub-designations of L, S, C for UHF and X, Ku, K, and Ka for SHF (Gordon & Morgan, 1993; IEEE, 1984). These bands are relevant to this study because they encompass the frequencies most IoT protocols are currently transmitting on. However, there are use limitations by the FCC that prevent some of these frequencies from transmitting to space. Currently, as mentioned in Chapter II Section C, the common IoT, UHF frequencies of 868 MHz and 915 MHz are authorized for use in RF devices, ISM equipment, private land mobile, and amateur radio, but they are not authorized for SATCOM (FCC, 2022a). Conversely, 2.4 GHz is authorized for both ISM equipment and SATCOM (FCC, 2022a). Moreover, frequencies in the C-band are being purchased by companies like Verizon to implement 5G in space, which will support IoT protocols like NB-IoT and LTE-M (Verizon, 2021).

Table 2. Radio Frequency Bands

<table>
<tr><th>Frequency Band</th><th>Sub-frequency Range</th><th>IEEE Letter Designation</th><th>Band Number</th><th>Acronym</th><th>Band Name</th><th>Wavelength</th></tr>
<tr><td rowspan="3">0.3-3 GHz</td><td>1-2 GHz</td><td>L</td><td rowspan="3">9</td><td rowspan="3">UHF</td><td rowspan="3">Ultra High Frequency</td><td rowspan="3">10-100 cm</td></tr>
<tr><td>2-4 GHz</td><td>S</td></tr>
<tr><td>4-8 GHz</td><td>C</td></tr>
<tr><td rowspan="4">3-30 GHz</td><td>8-12 GHz</td><td>X</td><td rowspan="4">10</td><td rowspan="4">SHF</td><td rowspan="4">Super High Frequency</td><td rowspan="4">1-10 cm</td></tr>
<tr><td>12-18 GHz</td><td>Ku</td></tr>
<tr><td>18-27 GHz</td><td>K</td></tr>
<tr><td>27- 40 GHz</td><td>Ka</td></tr>
</table>

Note: Adapted from Australian Space Academy, n.d.; Gordon and Morgan, 1993.; IEEE, 1984.

In addition to dividing the RF spectrum by frequency, the spectrum is also apportioned by use case. Broadly, a frequency band can either be licensed or unlicensed. Licensed frequency bands are protected from interference by a regulator, have a limited number of users, and guaranteed quality of service (QoS) management (Chaudhari & Borkar, 2020; Höyhtyä & Mustonen, 2018). However, licensed bands are expensive and time-consuming to acquire and often result in technology delays to market (Chaudhari & Borkar, 2020; Höyhtyä & Mustonen, 2018). Alternatively, unlicensed frequency bands encourage innovation through easy access to the spectrum, but the access comes at the risk of interference and operation in a crowded spectrum (Chaudhari & Borkar, 2020; Höyhtyä & Mustonen, 2018).

b. Transmission Range

Generically, transmission range can be described as the maximum distance between two wireless antennas, a transmitter and a receiver, at which communication can occur (Faludi, 2021). More specifically, Natarajan Meghanathan (2014, p. 274) defines the transmission range as "the maximum distance between any two nodes such that the signal emanating from one node could directly reach the other node with strength appreciable enough to correctly extract the encoded information." This variable is crucial to this study because the signal must be able to travel from a sensor on the ground to a satellite in LEO. The distance from the Earth's surface to LEO can be anywhere from 160 km to 1000 km (ESA, 2020).

c. Maximum Data Rate

Coleman and Westcott (2021) describe data rate as the number of bits per second carried on a transmission. A bit is the smallest unit of measurement in digital data and is represented as a single value, either a one or a zero (Stanford University, n.d.). The rate of bit transmission across the network is an important consideration for this study. Whether the IoT application is delay-tolerant or requires near-real time data will determine the threshold data rate for the application.

d. Maximum Payload

A data payload is the collection of bits transmitted between applications, programs, or networks (West, Dean, & Andrews, 2019). It can also be described as the carrying capacity of a network packet (Froehlich & Loshin, 2021). The size of a data payload determines how much data can be sent in a single transmission, which is especially important for IoT applications that transmit intermittently. The larger the payload, the more information an IoT end device will be able to send in one burst.

e. Latency

West, Dean, and Andrews (2019) define latency as the delay between when data leaves a source and arrives at its destination. This variable is also known as *RTT*. Latency, like data rate, is a key factor in a LEO IoT network because different applications have varying tolerances for delay in data receipt. IoT sensor networks monitoring critical infrastructure require near-real time updates, while data from relatively stable environments like smart building sensors may support lengthy RTT configurations, even hours between transmissions (Mekki, Bajic, Chaxel, & Meyer, 2019).

The four supporting variables for evaluating IoT waveforms are as follows:

f. Bandwidth

Bandwidth is the difference between the highest and lowest frequencies constituting a carrier channel (Salih, n.d.; Weik, 2000). To assess bandwidth relative to the central carrier frequency, the following equation is used: $B = \frac{f_H - f_L}{f_C}$, where f_H is the highest frequency, f_L is the lowest frequency, and f_C is the central frequency (Waghmare, 2022). Bandwidth is valuable to an IoT waveform assessment because it is directly related to the data capacity available in a given transmission, and capacity is synonymous with maximum data rate. Furthermore, the wider the bandwidth, the smaller the SNR can be for the same capacity. The Shannon-Hartley theorem portrays this relation: $C = B\, log_2\left(1 + \frac{S}{N}\right)$, where C is capacity, B is bandwidth, S is signal, and N is noise (CSUSB, n.d.).

g. Spread Spectrum Modulation Scheme

The NIST Computer Security Resource Center (NIST CSRC) (n.d.) defines spread spectrum as "a communications technique in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information." Chapman et al. (2015) note that the wider the bandwidth, the more resilient the signal is to narrowband interference. There are many forms of spectrum modulation. Three of the most common are frequency hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), and chirp spread spectrum (CSS) (Chapman et al., 2015; Reynders & Pollin, 2016). FHSS divides a defined bandwidth into channels that a transmitted signal will "hop" between (Fund, 2019). The hopping pattern is determined by a spreading code based on a pseudo-noise sequence (Fund, 2019). In DSSS modulation, the digital signal uses a chipping code to spread the waveform over a wider bandwidth than necessary, transmitting the data simultaneously on numerous frequencies within a particular bandwidth (Dubrawsky, 2010; Large & Ciciora, 2004). The simultaneous transmissions spread across the wider bandwidth provide communication redundancy and significant protection from electromagnetic interference (Dubrawsky, 2010). Like FHSS and DSSS, CSS uses a much larger bandwidth than required to spread the signal over a wider frequency range (Bizon Franco de Almeida, Chafii, Nimr, & Fettweis, 2021). CSS uses chirps as the carrier of the data (The Things Network, 2021). The spreading factor determines the chirp rate, which in turn controls the speed of data transmissions (The Things Network, 2021). CSS is similar enough to DSSS that it is backward compatible with it (IEEE P802.15 WG, 2003). The spectrum modulation scheme was a factor in this study because it was foundational information in locating a transmission alternative for the Orbital-1. The first choice was to identify an option based on CSS modulation, then to search for IoT solutions based on other modulation techniques.

h. Cybersecurity and Encryption

Cybersecurity and encryption are the first secondary variable for an alternative Orbital-1 IoT waveform. In Joint Publication 3-12 *Cyberspace Operations* (2018), the Joint Chiefs of Staff (JCS) define cyberspace security as "actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" (p. II-2). Encryption supports cybersecurity by transforming the data into an unreadable form that can only be understood once the proper decryption key is applied to the encoded data (Cisco, 2022). Although an extensive dive into cybersecurity is outside the scope of this study, careful consideration of the transmission waveform and carried data's security is critical when selecting an alternative waveform for a DOD CubeSat. Accordingly, cybersecurity and encryption are not a supporting variable because security is unimportant. Instead, it is because if an alternative waveform were identified, then it is likely possible to implement additional security elsewhere within the Orbital-1 payload Printer Circuit Board (PCB).

i. Power Consumption and Battery Life

Sarah L. Harris and David Harris (2022) define power consumption as the amount of energy used per unit of time. The power consumption of a waveform is an important consideration because a CubeSat has a finite amount of power onboard, and due to its small size, it does not have space to add more energy support. Further, the power requirement directly impacts the size and life of a battery supporting a satellite payload. The higher the power consumption, the larger the battery must be to support the same transceiver lifespan (Zorzi & Chockalingam, 2003). The larger the battery is, the less space the CubeSat has for other required components and the more expensive the asset will be overall. Although scientists are expending great efforts to improve battery technology, for now, it is still a significant consideration for an IoT waveform (University of Cambridge, 2022).

2. Operationalization of IoT Waveform Variables

In order to use the IoT waveform variables in a quantifiable way, congruent operational definitions for each variable were defined based on Siedlecki's (2020) research guidance. Table 3 shows corresponding operational definitions for each variable's conceptual description. The operational definitions provide standardized units to measure comparative datapoints against.

Table 3. Conceptual and Operational Definitions for Alternative IoT Waveform Variables

Variable	Conceptual Definition	Operational Definition
RF spectrum	The frequency range from 3 kHz to 300 GHz corresponding to wavelengths ranging from 100 km to 1 mm. (Asif; 2018, p. 15)	Radio wave oscillations in Hertz (Hz) Million Hertz: Mega (MHz) Billion Hertz: Giga (GHz)
Transmission Range	The maximum distance between any two nodes such that the signal emanating from one node could directly reach the other node with strength appreciable enough to correctly extract the encoded information. (Meghanathan, 2014, p. 274)	Theoretical maximum range in kilometers (km)
Data Rate	The number of bits per second carried on a transmission (Coleman & Westcott, 2021).	Data transmission rate in bits per second (bps)
Payload	The carrying capacity of a network packet (Froehlich & Loshin, 2021).	Size of network packet in Bytes

Variable	Conceptual Definition	Operational Definition
		Thousand Bytes: Kilo (KB) Million Bytes: Mega (MB)
Latency	The delay between when data leaves a source and arrives at its destination (West et al., 2019).	Delay in data receipt in seconds (s) 1/1000 seconds: Mili (ms)
Bandwidth	The difference between the highest and lowest frequencies surrounding a carrier channel (Salih, n.d.; Weik, 2000).	Width of the frequency band in Hertz (Hz) Kilohertz: kHz
Spread Spectrum Modulation Scheme	A communications technique in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information (NIST CSRC, n.d.).	Application of a modulation technique such as DSSS, FHSS, or CSS, or the lack of (use of narrowband)
Cybersecurity	Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (JCS, 2018, p. II-2)	Application of security protocols such as SSL, TLS, HTTPS, and IPSec. Application of encryption algorithms such as SHA, AES, and RSA.
Power Consumption & Battery Life	The amount of energy used per unit of time (Harris & Harris, 2022).	Power: Energy in Watt hours (Wh) Battery Life: length of time until inoperable in months

3. Transceiver Variables

To address research question 1 and determine if a feasible alternative to the current Orbital-1 CubeSat transceiver exists, the key variables for that component were determined and defined. The study identified five primary variables and two secondary variables. Like the waveform variables, the five primary variables are the “must-haves” in order for a transceiver to be able to replace the L04. The secondary variables are the “nice-to-haves.” Should two solutions prevail, the secondary variables can help determine the best match for the Orbital-1 CubeSat. The five primary variables for a replacement transceiver are the following:

a. Power Consumption

The consideration of power consumption noted in Section C.1 also applies to the transceiver. However, for a transceiver, power consumption should be considered in three different scenarios: during transmission, during reception, and while in sleep mode. Although there are several other modes for the transceiver to operate in, these modes represent the two most significant features of the transceiver for this study: transmission and reception of IoT data, and the state when the component requires the least amount of power: sleep mode.

b. Maximum Transmission Range

Transmission range was defined in Section C.1. This variable is important to selecting a transceiver for the same reasons as it is important in identifying an alternative waveform: it is a significant variable because the signal must be able to travel from a sensor on the ground to a satellite in LEO.

c. Transmission Frequency

The University of California (n.d.) defines *frequency* as "the number of cycles…per unit of time for a wave or oscillation." Frequency can further be represented by the equation $f = \frac{1}{T}$, where "f" represents the frequency and "T" is the time (University of California, n.d.). The transmission frequency chosen for the transceiver is fundamental for several reasons. First, the Orbital-1 already has an antenna selected that can only tolerate a specific frequency range. Next, as noted in the RF Spectrum variable description, agencies like the FCC in the U.S. and the International Telecommunications Union (ITU) determine the authorized purpose for a particular frequency. Further, the frequency determines if a signal transmitted to space is susceptible to interferences like ionospheric scintillation or atmospheric absorption (Crook, PowerPoint slides, 2011).

James Jones et al. (2015) explain scintillation as the “random modulation imparted to propagating wave fields by structures in the propagating medium” (p. 1). Ionospheric scintillation is most problematic at the lower end of the frequency spectrum (200-400 MHz) (Jones et al. 2015). However, episodes of ionospheric scintillation have been strong enough to disrupt satellite navigation operations transmitting near the 1.5 GHz range (Jones et al., 2015). Scintillation has been further noted to diminish signals transmitting at frequencies up to the Ku-band (10.7-18 GHz) (Gordon & Morgan, 1993; Smith & Flock, 1993). Atmospheric absorption is caused by water vapor in the air. Zubair et al. (2011) note that rain droplets both absorb and scatter RF waveforms. The effects of atmospheric absorption are most severe in the higher frequencies (above 10 GHz), where the height of the sinusoidal wave is small and approaching the size of a raindrop (Zubair et al., 2011).

d. Physical Size

The physical size of the replacement transceiver is a very specific requirement for the Orbital-1 payload PCB. The current Orbital-1 transceiver is a Pycom L04, which is 40mm x 16 mm x 2.7 mm. As shown in Figure 7, the payload PCB is 85 mm x 70 mm with some spare space on the board for a slightly larger replacement transceiver.

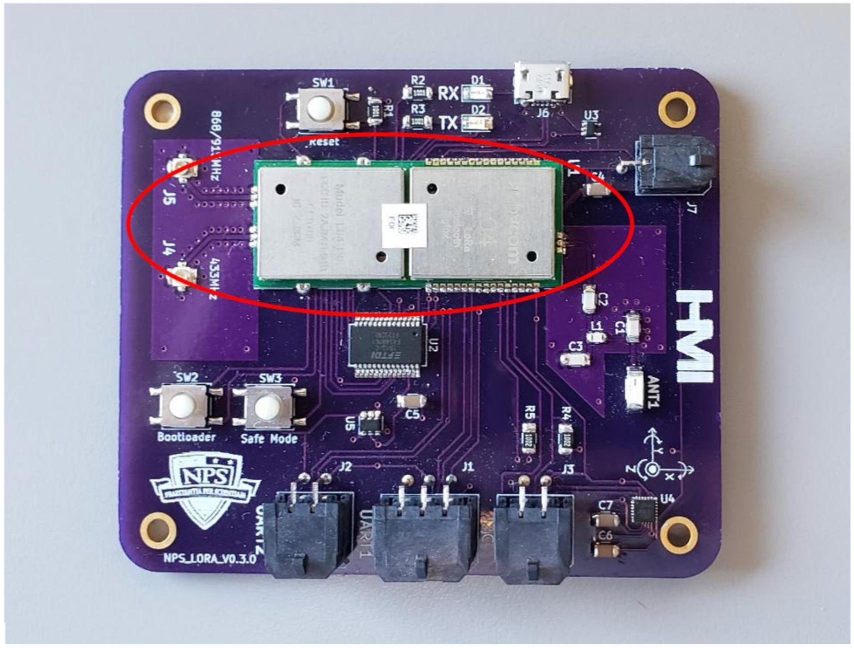

Figure 7. NPS Orbital-1Original Payload PCB. The Red Circle Encompasses the Pycom L04 Transceiver which Houses the Problematic Semtech LoRaWAN Chip Inside of It.

e. FY19 NDAA and EO 13873 Compliant

The limitations on covered telecommunications equipment and services were covered in depth in Chapter II. This is an important variable to consider for a transceiver to be authorized for use by the DOD. Not only is the use of covered parts illegal, but they also represent a significant threat to U.S. intelligence, critical infrastructure, communications systems, cybersecurity, and by extension, military personnel. The challenge, nevertheless, is the accurate assessment of a company's risk to the U.S. as defined in EO 13873. This study conducted a preliminary search for transceiver manufacturer ties to the Republic of China. However, the ultimate authority lies with the Federal Acquisition Regulation (FAR) Council to determine the threat of a system or service (Federal Acquisition Regulation, 2020).

The two secondary variables for the Orbital-1 transceiver or CSS chip are as follows:

f. Cybersecurity and Encryption

Cybersecurity and encryption are described in Section C.1. They are of secondary concern in the selection of a transceiver due to the threat mitigation approaches they can provide. Transceivers capable of enabling virtual private networks (VPNs) through Session layer encryption like transport layer security (TLS) or gateway-to-gateway encryption like internet protocol security (IPSec) provide enhanced protection for the data in-transit (J. Fulp, PowerPoint slides, March 2022). Moreover, components that can also offer encryption are able to meet confidentiality, integrity, and availability requirements for protecting the data both at rest and in-transit.

g. Memory

The final variable for consideration in a replacement transceiver is the memory available on the component. Memory for the Orbital-1 transceiver has two primary forms: flash memory and random access memory (RAM). Flash memory is non-volatile storage predominantly used to keep firmware on embedded systems (Yang, 2019). RAM is a volatile store typically used for primary data storage and retrieval in support of applications, processes, and programs (Ibrahim, 2014; Villinger, 2022). Due to the complexity of the modulation schemes that the transmission waveform must support, the transceiver requires a small amount of on-component RAM to manage the transmission timing (Eberle, 2008). The memory for the transceiver is significant to the Orbital-1 payload PCB due to its essential functions. The PCB must contain firmware to guide the hardware's operations, and RAM is necessary to support the transceiver's radiations.

4. Operationalization of Transceiver Variables

Like the IoT waveform variables, Siedlecki's (2020) research guidance was the foundation for the operationalization of the transceiver variables. The variable's operational definitions are closely aligned to their conceptual descriptions, while providing a standardized, measurable reference. Table 4 illustrates the association between these definitions for each of the transceiver variables.

Table 4. Conceptual and Operations Definitions for Alternative Component Variables

Variable	Conceptual Definition	Operational Definition
Power Consumption	The amount of energy used per unit of time (Harris & Harris, 2022).	Energy in Watt hours (Wh)
Transmission Range	The maximum distance between any two nodes such that the signal emanating from one node could directly reach the other node with strength appreciable enough to correctly extract the encoded information. (Meghanathan, 2014, p. 274)	Theoretical maximum range in kilometers (km)
Frequency	The number of cycles per unit of time for a wave or oscillation (University of California, n.d.).	Cycles per second in Hertz Million Hertz: Mega (MHz) Billion Hertz: Giga (GHz)
Physical Size	The dimensions of the replacement component.	Physical surface area measured in millimeters (mm) squared
FY19 NDAA & EO 13873 Compliant	Equipment cannot be “designed, developed, manufactured, or supplied by owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.” (EO 13873, 2019, pp. 22689-22690)	Manufacturer has no ties to FCC Designated Covered Companies: Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, AO Kaspersky Lab, China Mobile International USA Inc, China Telecom (Americas) Corp., PacificNetworks Corp., ComNet (USA) LLC (FCC, 2022c; FCC, 2022d; NDAA, 2018, p. 132 STAT 1918)
Cybersecurity	Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform	Application of security protocols such as SSL, TLS, HTTPS, and IPSec.

Variable	Conceptual Definition	Operational Definition
	information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (JCS, 2018, p. II-2)	Application of encryption algorithms such as SHA, AES, and RSA.
Memory	Flash memory is non-volatile storage predominantly used to keep firmware on embedded systems (Yang, 2019). RAM is a volatile store typically used for immediate data storage and retrieval in support of applications, processes, and programs (Ibrahim, 2014; Villinger, 2022).	Data storage capacity measured in Bytes Thousand Bytes: Kilo (KB) Million Bytes: Mega (MB)

D. SUMMARY

This chapter outlined the research design, methods, and key variables used in this study. The research is founded on a quantitative, descriptive comparative approach based on postpositivist worldviews. The data collection focused on the two primary research questions and involved searching through existing academic and commercial datasets, which yielded limitations like gaps in data points and varying results for a single element. Five primary and four supporting variables were first identified to classify and assess alternative IoT waveforms. Then five primary and two secondary variables were noted to evaluate substitute IoT transceivers. The next chapter presents two tables based on these variables to synthesize the results and conduct analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RESULTS AND ANALYSIS

This chapter presents the results and analysis of the data necessary to address this study's primary research questions. The chapter beings with a description of the data collected on alternative IoT waveforms, followed by an analysis of that data. Based on the research methods described in Chapter IV, the study identifies three feasible waveforms to replace LoRaWAN in the Orbtial-1 CubeSat: NB-IoT, LTE-M, and Ingenu. The three waveforms are then used to identify six possible IoT transceivers to supersede the Pycom L04. Three of the transceivers are designed to support NB-IoT and LTE-M. They are Murata LBAD0ZZ1SE, Thales DIS EMS31-X, and Thales DIS TN-23. The remaining three transceivers function with the Ingenu waveform: Compal RU-232, Gemtek GR1036, and U-blox SARA-S200. A comparative analysis is then performed amongst the six transceivers with a special emphasis on their FY19 NDAA and EO 13873 compliance. Based on the security analysis three transceivers are determined feasible to replace the Orbtial-1 Pycom L04, the two Thales DIS transceivers: EMS31-X and TN-23, and the U-blox SARA-S200 transceiver.

A. IOT WAVEFORM RESULTS AND ANALYSIS

The following subsections detail the results and analysis of the alternative IoT waveforms. The study's findings conclude three IoT waveforms are viable to replace LoRaWAN in the Orbital-1 CubeSat: NB-IoT, LTE-M, and Ingenu.

1. Standardized Raw Data for IoT Alternative Waveforms

Table 5 displays the results for the primary and secondary waveform variables for six waveforms based on 16 different scholarly and private sector sources. LoRaWAN was used as the baseline reference to compare the Sigfox, NB-IoT, LTE-M, Wi-sun and Ingenu waveforms against. These alternative waveforms were selected due to their membership to LPWAN and cellular IoT protocol categories, and the relative range of these protocol categories, presented in Figure 3 of Chapter II.

Table 5. Alternative IoT Waveform Parameters

Variables	Waveforms					
	LoRaWAN	Sigfox	NB-IoT	LTE-M	Wi-sun	Ingenu
Protocol Type	LPWAN [c,j,k]	LPWAN [c,j,k]	LPWAN/Cellular [c, g,j,k]	Cellular [c,g]	LR-WPAN [p]	LPWAN [k]
Standard	LoRa Alliance [a, h]	Sigfox [a,e,f,h,i]	3GPP [a,e,g,h,i,m]	3GPP [e,g,i,m]	Wi-sun Alliance [p]	RPMA [a,f]
RF Spectrum (MHz)	Unlicensed/ISM [e,h,o] 915 MHz US [a,b,e,h,i] 868 MHz EU [a,b,e,h,i] 433 MHz Asia [b,e,h,i]	Unlicensed/ISM [e,h,o] 915 MHz US [e,h] 868 MHz EU [a,e,h,i] 433 MHz Asia [e,h]	Licensed [a,e,h,i,o] LTE frequency bands [e,h,k]	Licensed [e,i,k,o] LTE frequency bands [e,k]	Unlicensed/ISM [n] 915 MHz US n 868 MHz EU [n]	Unlicensed/ISM [o] 2,400 MHz [a]
Tx Range (km)	5 km urban [e,h,o] 15-45 km rural [e,k, o]	10 km urban [e,f,h,o] 30-50 km rural [a,f,o]	1 km urban [e,h] 20-40 km rural [a]	5 km urban [e,f] 50 km rural [f]	2-3 km rural [m]	3 km urban [f,k] 50 km rural [a,f]
Max data rate (kbps)	UL: 50 [e,f,h,k,m] DL: 290 [e]	UL: 0.100 [a,e,h,i,k,o] DL: 0.600 [a,e,i,m]	UL: 64 [a,o] DL: 128 [o]	UL: 1,000 [e,f,i,m,o] DL: 1,000 [e,f,i,m,o]	50-300 [m, p]	UL: 624 [a,f,o] DL: 156 [a,f,o]
Max payload (bytes)	243 [e,h]	UL: 12 [a,e,h,i] DL: 8 [a,e,h,i]	1600 [e,h]	1000 [e]	Not limited [m]	64 [a]
Latency (seconds)	10s of seconds [m,o]	10s of seconds [m,o]	>10 seconds [o]	0.10 seconds [m,o]	0.010 seconds [m]	10s of seconds [o]
Bandwidth (kHz)	125 kHz [a,b,e,h,m] 250 kHz [a,b,h] 500 kHz [a,b,e]	0.100 kHz [a,h,i] 0.600 kHz [a,e]	180 KHz [a,e,i,k]	1,400 kHz [e,i,k,m] 20,000 kHz [e,i]	100 kHz [m] 600 kHz [m]	1,000 kHz [a]
Spread Spectrum Modulation Scheme	CSS [a,e]	UNB [i,m]	OFDM [m]	OFDM [m]	No data available	DSSS [a]
Cybersecurity	AES 128b [a,e,h,i,l,p]	Not supported [a,h]	AES 256 [e,i,p]	AES 256 [e,i]	Public Key Encrypt, AES [p]	AES 256b [a]
Pwr Consumption (mA)	120 mA [d] Very low [a]	11mA rx [d] 125 mA tx [d] Very low [a]	300 mA [d] Low [a]	No data available No data available	No data available No data available	No data available High [a]
Battery lifetime 2000 mAH	105 months [e]	150 months [e]	90 months [e] > 10 yrs [o]	18 months [e] > 10 yrs [o]	No data available	No data available

Note: Adapted from Almuhaya, Jabbar, Sulaiman, and Abdulmalek, 2022[a]; Andrade and Yoo, 2019[b]; Centenaro, Costa, Granelli, Sacchi, and Vangelista, 2021[c]; Ferrer, Céspedes, and Becerra, 2019[d]; Khalifeh, Aldahdouh, Darabkh, and Al-Sit, 2019[e]; Kuzlu, Pipattanasomporn, and Rahman, 2018[f]; Liberg et al., 2020[g]; Mekki, Bajic, Chaxel, and Meyer, 2019[h]; Oliveira, Rodrigues, Kozlov, Rabêlo, and Albuquerque, 2019[i]; Purnama, Nashiruddin, and Murti, 2020[j]; Putland, 2020[k]; Queralta, Gia, Zou, Tenhunen, and Westerlund, 2019[l]; Sendin, Matanza, and Ferrus, 2021[m]; Texas Instruments, n.d[n]; Wang and Fapojuwo, 2017[o]; Wi-sun Alliance, 2019[p].

2. Analysis of IoT Waveform Results

Figure 8 provides a flow chart of this study's analysis process for addressing research question 2 and determining if a feasible alternative IoT waveform exists to replace LoRaWAN for the Orbtial-1 CubeSat. The flow chart implements the five primary waveform variables as discrimination filters to assess the five alternative waveforms against LoRaWAN. Each variable has a determined threshold, if the threshold is met, the waveform progresses to the next discrimination filter, if the threshold is not met, the waveform is rejected from the vertical flow and noted on the side. This flow chart also acts as an initial step towards developing a rule-based artificial intelligence (AI) model for machine learning (ML) in software defined radios (SDR) that switch between various IoT waveforms in order to optimize the selected waveform to the defined conditions.

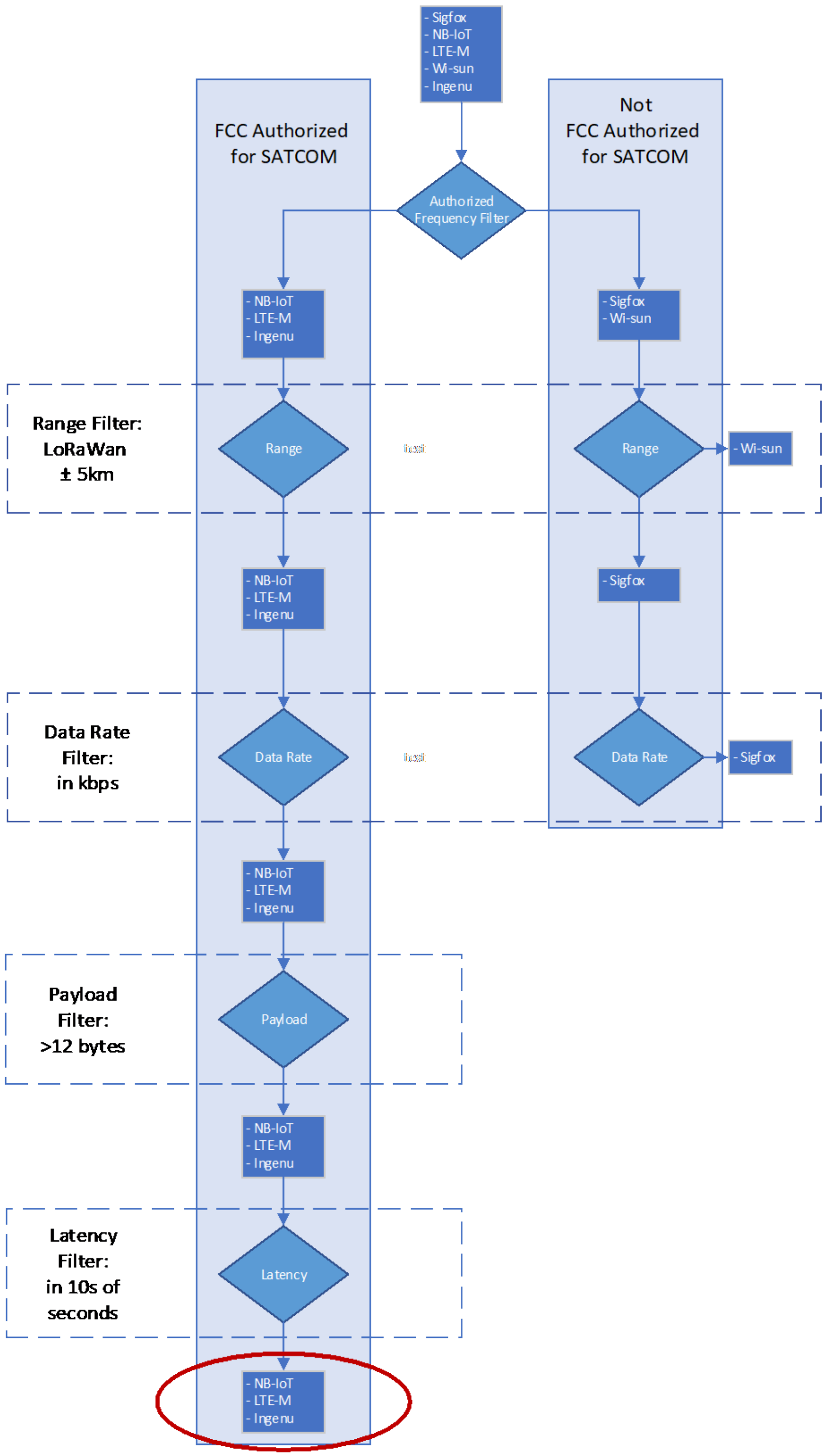

Figure 8. IoT Waveform Analysis Flow Chart.

As shown in Figure 8, the first waveform variable was whether the IoT waveform operates at a frequency currently authorized for SATCOM by the FCC. The flow chart divides the results into “FCC Authorized for SATCOM” and “Not FCC Authorized for SATCOM.” The authorized waveforms include NB-IoT, LTE-M, and Ingenu. NB-IoT and LTE-M operate in LTE frequency bands, which are defined based on the frequency spectrum that a cellular company owns and can consist of typical SATCOM frequency bands like the C-band (Verizon, 2021). Ingenu operates at 2.4 GHz, which the FCC approves for both terrestrial and space-based communications (FCC, 2022a). Sigfox and Wi-sun are unauthorized waveforms for SATCOM because they operate at 915 MHz in the U.S., and this frequency is not presently permitted to radiate to space. However, the results are shown as two parallel paths since this study anticipates that the FCC regulations will likely change to support these IoT waveforms over SATCOM in the future and the use cases for the waveforms considered is also expected to expand.

Range was the next discrimination filter applied to the IoT waveforms. The threshold was determined to be plus or minus five kilometers from 45 km, the range of LoRaWAN in Table 5. This threshold was chosen based on LoRaWAN’s success in transmitting to space (Lacuna Space, n.d.). NB-IoT, LTE-M, Ingenu, and Sigfox successfully passed this filter. However, Wi-sun was significantly below the threshold range at 2–3 km and therefore rejected from the rest of the assessment.

Following range, the data rate filter was set to kilobits per second (kbps) based on the LoRaWAN data rates in Table 5: 50 kbps for uplink transmissions and 290 kbps for downlink transmissions and definitions from Jie Ding et al.’s study, *IoT Connectivity Technologies and Applications: A Survey* (2020). Ding et al. classify “low data rates” for machines as “up to hundreds of kbps” and “higher data rates” as “tens of Mbps.” These ranges were used to establish the acceptable deviation from the LoRaWAN standard and justify the data rate threshold in kbps. Figure 9 displays several potential IoT applications and the data rates required to support these applications. Sigfox does not pass this filter because its data rate is considerably lower than the LoRaWAN threshold at 100 bps for uplink transmissions and 600 bps for downlink transmissions. In fact, the Sigfox uplink transmission is approximately 500 times slower than LoRaWAN’s uplink transmission data rate. On the other hand, NB-IoT, LTE-M, and Ingenu all pass this filter, with kbps data rates for NB-IoT and Ingenu and Mbps data rates for LTE-M.

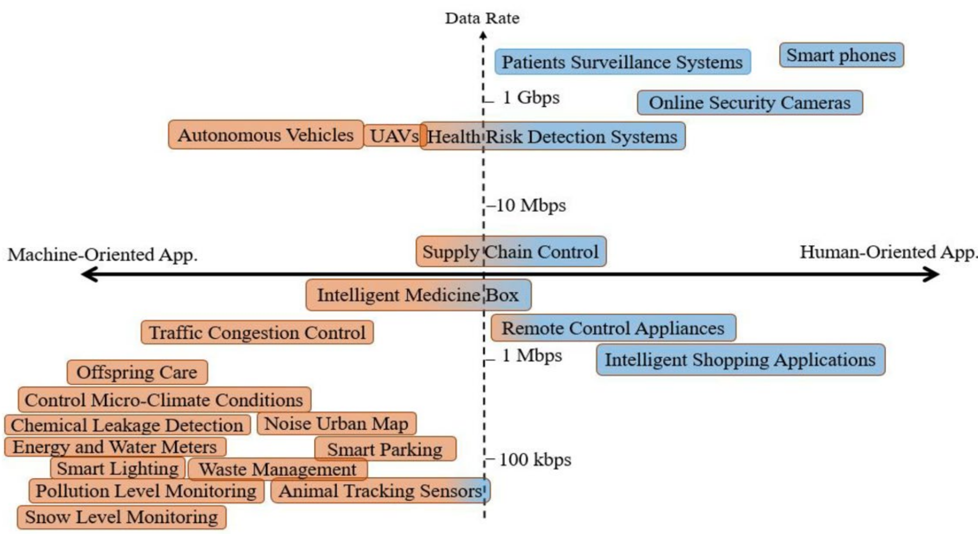

Figure 9. IoT Applications and Their Data Rates. Source: Ding et al. (2020).

The fourth IoT waveform filter is the payload size. The threshold for this filter is based on the Electronic Product Code Global (EPCglobal) (2005) General Identifier with 96 bits (GID-96) standard. This standard was chosen to set the lower threshold limit for payload size because it is a universal standard that supports one of the least data intensive IoT applications, RFID. This threshold identifies what the smallest relevant IoT payload is that can be transmitted, and which waveforms can support it. RFID tags with the GID-96 standard provide asset tracking through a General Identifier*,* which is broken into 28 bits for a general manager number, 24 bits for the object class, and 36 bits for the serial number (EPCglobal, 2005). The remaining 8 bits of the GID-96 are used as a packet header (EPCglobal, 2005). In total, the 96 bits translate to a 12-byte payload. Based on this threshold, no additional IoT waveforms were discarded. NB-IoT, LTE-M, and Ingenu all offer data payloads much larger than 12 bytes. Ingenu offers approximately a five times larger payload than the GID-96 requirement at 64 bytes, and NB-IoT and LTE-M provide payloads in the thousands of bytes.

The final discrimination filter for the alternative IoT waveforms is latency. The latency threshold was determined to be tens of seconds. Although different IoT applications have varying latency tolerances, this decision was based on LoRaWAN's latency of tens of seconds, in Table 5, and Ding et al.'s 2020 study. Ding et al. divide IoT applications into delay-sensitive and delay-tolerant categories. They classify technologies like self-driving cars as delay-sensitive and sensors for agriculture and waste management as delay-tolerant. Ding et al. further state that delay-tolerant IoT systems can support latency greater than one second, while delay-sensitive IoT applications require less than one second of latency, often tens of milliseconds. Ding et al.'s classifications help define the acceptable range of the LoRaWAN latency threshold. Most of the applications that the Orbital-1 CubeSat can support will be delay-tolerant. Two of the remaining IoT waveforms meet Ding et al.'s definition of delay-tolerant: NB-IoT and Ingenu. They both offer latency within tens of seconds. LTE-M meets the delay-sensitive characterization based on latency values of around ten milliseconds.

Thus, after running six potential IoT waveforms through the five primary waveform filters, three waveforms remained: NB-IoT, LTE-M, and Ingenu. Examination of these waveforms' secondary variables did not eliminate any of the three remaining waveforms. All three had bandwidth comparable to LoRaWAN's, better encryption algorithms than LoRaWAN's, and similar power consumption. The spread spectrum modulation scheme is not a factor at this stage; It was only noted in Table 5 for the initial attempt to find a direct replacement for LoRaWAN based on a CSS modulation scheme.

NB-IoT, LTE-M, and Ingenu therefore meet the requirements to address research question 2 and the defined standards for a feasible replacement to the LoRaWAN waveform for the Orbital-1 CubeSat. Two of the three waveforms belong to the cellular IoT protocol class and require a licensed frequency spectrum to operate: NB-IoT and LTE-M. The last waveform, Ingenu, is part of the LPWAN class and operates in the unlicensed frequency spectrum. The CENETIX team must decide if licensed or unlicensed is preferable, especially since licensed spectrum costs approximately $490M per MHz of bandwidth compared to free for unlicensed spectrum (Mekki et al., 2019).

B. IOT TRANSCEIVER RESULTS AND ANALYSIS

The following sections describe the identified potential IoT transceivers and analyze their ability to replace the Pycom L04 in the Orbital-1 CubeSat. This study's findings determine three transceivers from two different companies are viable options: Thales DIS EMS31-X and TN-23 which support NB-IoT and LTE-M waveforms, and U-blox SARA-S200 which implements the Ingenu waveform.

1. Alternative IoT transceivers for the Orbital-1

Six potential IoT transceivers were selected based on the feasible waveforms found in Chapter V Section A and the transceiver variables defined in Chapter IV Section C.3. These transceivers were compared against the Pycom L04 transceiver from the Orbtial-1 CubeSat. The six transceivers are manufactured by five different companies. Three are compatible with NB-IoT and LTE-M and three were designed for the Ingenu RPMA waveform. Table 6 displays the results of the primary and secondary waveform variables for the L04 and the six potential alternative IoT transceivers.

Table 6. Potential IoT Transceivers Compatible with NB-IoT, LTE-M, or Ingenu

Variable		Manufacturer & Model Number						
		Pycom L04	Murata LBAD0ZZ1SE	Thales DIS EMS31-X REL.3	Thales DIS TN-23 (Preliminary)	Compal RU-232 (Preliminary)	Gemtek GR1036	U-blox SARA-S200
IoT Waveform		NB-IoT/ LTE-M[m,n]	NB-IoT/ LTE-M[g,i,j]	NB-IoT/LTE-M[q]	NB-IoT/LTE-M[s,t]	Ingenu[b]	Ingenu[d]	Ingenu[v,w]
Power Consumption	Tx	18 mA[m]	"enables 10 yr battery"[g,j]	210 mA[q]		125-330 mA[b]	83 mA[a]	320 mA[w]
	Rx	12 mA[m]				65-100 mA[b]	62 mA[a]	105 mA[w]
	Sleep	0.2 µA[m]	3 µA[j]	2 mA[q]	80 uA eDRX[t]	<1 mA[b]	41 mA/ 5 µA[a]	19 µA[w]
Tx Range		>50 km[n]	No data available	No data available	No data available	12.8 km[b]	No data available	No data available
Tx Frequency		868 MHz EU, 915 MHz US[m,n]	Low Bands 5,8,12,13,14(CAT M1 Only),17,18,19,20, 26,28[g,i] Mid Bands 1,2,3,4,25[g,i]	EMS31-US LTE Bands 2,4,12[q] EMS31-W LTE Multiband[q]	Bands 1, 2, 3, 4, 5, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 66, 85[t]	2.4 GHz[b]	2.4 Ghz[a,d]	2.4 GHz[v,w]
Physical Size		40 mm x 16 mm x 2.7 mm[n]	15.4 mm x 18 mm x 2.5 mm[j]	27.6 mm x 18.8 mm x 2.1 mm[q]	15.3 mm x 15.3 mm x 2.9mm[s]	36 mm x 36 mm x 4 mm[b]	20.5 mm x 18 mm x 2.35 mm[d]	16 mm x 26 mm x 2.4 mm[v,w]
FY19 NDAA & EO 13873 Compliant		no[o]	probably yes[h,k]	yes[r,u]	yes[r,u]	probably no[c,l,p]	probably no[e,f]	most likely yes[x,y]
Cybesecurity		SSL/TLS, AES[m,n]	SSL/TLS[i]	TLS[q]	TLS 1.3, DTLS 1.2[s,t]	SSL[b]	AES 128[d]	No data available
Memory	Flash	8 MB[n]	1 MB[g]	No data available	256 KB[t]	No data available	No data available	No data available
	RAM	520 KB + 4 MB[n]	512 KB + 160 KB[g]	No data available	128 KB[t]	No data available	No data available	8 MB[w]

Note: Adapted from Airhoa, 2006[a]; Compal, 2017[b]; Compal, n.d.[c]; Gemtek, n.d-a[d]; Gemtek, n.d.-b[e]; Gemtek, 2021[f]; Murata, n.d.-a[g]; Murata, n.d.-b[h]; Murata, 2018[i]; Murata, 2021[j]; Obe, 2022[k]; Orgio Inc., n.d[l]; Pycom, n.d.-a[m]; Pycom, n.d.-b[n]; Semtech, n.d.[o]; Shen & Lee, 2022[p]; Thales DIS, 2018[q]; Thales DSI, n.d.[r]; Thales Group, n.d.-a[s]; Thales Group, n.d.-b[t]; Thales Group, n.d.-c[u]; U-blox, 2017[v]; U-blox, 2018[w]; U-blox, 2022a[x]; U-blox, 2022b[y].

2. Analysis of IoT Transceiver Results

While there are many transceiver options available, this study selected six that were technically suitable and met the physical parameters on initial assessment. Three were chosen to further examine that were compatible with NB-IoT and LTE-M and an additional three were chosen that support Ingenu. All six of the selected IoT transceivers were determined to be technologically feasible. Although the power consumption for all of the alternative IoT transceivers is greater than the L04, the rates are all well below the CENETIX team's requirement of 1.2 amps (Bourakov, personal communication, September 20, 2022). The physical size of the alternatives is smaller than the L04 and therefore they would all fit on the Orbital-1 PCB. The transmission range was absent from almost all manufacture datasheets and was therefore unusable as a delimitator of the transceivers. Cybersecurity was comparable to the L04 on five of the six transceivers.

The U-blox SARA-S200, however, will require a deeper investigation to determine its security since it was not specified on its data sheet. Memory was absent for three of the six IoT transceivers. For those that had memory listed, their flash and RAM were adequate to support IoT operations. This determination is based on Nilesh Badodekar and Girija Chougala (2019) who state IoT controllers usually require 64–265 kilobytes to support their data processing, storage, and retrieval.

Among the transceivers that are technically viable, the primary concern for a replacement IoT transceiver is whether it is compliant with the FY19 NDAA and EO 13873 regulations. Of the six, two are determined to be compliant and one is most likely compliant. The Compal RU-232 and Gemtek GR1036 were both determined to likely not meet the standards of these regulations. Compal's chairman holds several positions in China such as "President of the China Productivity Center" and "Chairman of the General Chinese National Federation of Industries" (Origio Inc., N.d.). Gemtek's ties to China are less defined, however, their 2021 Annual Report notes several manufacturing and research and development shops in mainland China. Murata and U-blox are deemed probably compliant and most likely compliant respectively. Murata is a Japanese company with primarily sales offices in China instead of manufacturing, but in an interview given in January 2022, the company's president expressed continued interest in business with either China or the U.S., depending on who will win the trade war (Obe, 2022). Although Murata's president's perspective could be a matter of profit, the business relationship with China could entail a security implication for the U.S. U-blox is a Swiss company that has a very large set of "partners and allies" that are all from the European Union (EU) and the U.S. (U-blox, 2022b). The company's board members are also all from the EU (U-blox, 2022a). U-blox does not present any overt compliance concerns, however, they aren't clearly presented as a defense contractor. Therefore, out of an abundance of caution, U-blox is regarded as most likely compliant. The only company this study determined compliant is Thales Group. Thales developed a "proxy-regulated company Free of Foreign Ownership, Control, or Influence (FOCI)" called Thales Defense and Security, Inc., which is based in the U.S. (Thales DSI, n.d.). This company is specifically designed to be able to sell parts to the U.S. government and military.

Based on the security analysis of these five IoT transceiver manufacturers, this study found three feasible components to recommend as replacements for the L04 for the Orbital-1 CubeSat: the possible solutions include Thales DSI EMS31-X REL.3, Thales DSI TN-23, and U-blox SARA-S200. The IoT application and domain will determine the best transceiver for the Orbtial-1. The Thales DSI transceivers are limited to operations in locations where cellular networks currently exist, however they NB-IoT and LTE-M offer higher data rates and less capacity. The U-blox Ingenu transceiver can operate independent of other networks, but Ingenu requires smaller payloads and more power.

C. SUMMARY

Five alternative waveforms—Sigfox, NB-IoT, LTE-M, Wi-sun, and Ingenu—were assessed through the use of a flow chart with the five primary variables set as discrimination filters. NB-IoT, LTE-M, and Ingenu were determined to meet the threshold to be a feasible alternative to address research question 2 and replace the LoRaWAN waveform in the Orbital-1 CubeSat. Based on these results, six potential IoT transceivers were identified to replace the Pycom L04. The transceivers were assessed based on both the primary and secondary transceiver variables defined in Chapter IV. The primary limitation was their likely compliance with the FY NDAA and EO 13873 regulations. Two transceivers made by Thales group for the NB-IoT and LTE-M IoT waveforms were determined to be compliant. One transceiver from U-blox for the Ingenu waveform was deemed "probably compliant." Their use cases and limitations were briefly discussed, however, all three are feasible options for the CENETIX team to further examine. The following chapter will discuss the implications of this analysis and conclusions to this study.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

This chapter translates the results and analysis of this study into actionable recommendations for the DOD and the Information Science community. The first section of this chapter summarizes the established problem statement, provides answers to the research questions, and identifies contributions to DOD academia. The following section discusses the study's limitations and future research proposals. Finally, the last section relays actionable recommendations and provides a conclusion.

A. SUMMARY

The DOD requires that Armed Forces be able to operate effectively anywhere in the world. Most DOD operations are data intensive and require more bandwidth than is currently available. To further complicate these missions, many take place in remote environments where terrestrial communications are unavailable or severely lacking, which results in a high reliance on SATCOM to provide C2 to these operations.

The DOD has numerous IoT-friendly data types that could be transitioned to IoT waveforms. Historically, the military has used both WSNs and RFID to improve battlespace situational awareness and asset tracking (CASCOM, 2020). These are just two examples of data that now fall under the IoT umbrella. The challenge remains of how to ascertain an IoT waveform capable of transmitting to satellites while also providing a secure communication link for the DOD user.

1. Answers to Research Questions

In an effort to work towards the ultimate solution of identifying an ideal IoT waveform for DOD SATCOM, this study answered two research questions directly related to the Orbital-1 CubeSat, with broader implications for the DOD as a whole. These questions discussed in the order they were laid out in the Methods Chapter.

a. *Research Question 2: Is there an alternative to the LoRaWAN waveform that will meet the requirements for long-distance, low-power communications required for the Orbital-1 CubeSat?*

This study identified three waveforms as possible alternatives to LoRaWAN that would be capable of meeting the long-distance, low-power communication requirements of the Orbital-1 CubeSat. The primary discriminator that determined the feasibility of the alternative waveforms was their compatibility with FCC frequency allocations for SATCOM transmissions. The IoT waveforms were designed to operate in FCC SATCOM-friendly frequencies as well as meet the range, data rate, payload, and latency thresholds determined in this study, which include NB-IoT, LTE-M, and Ingenu.

Two of the three waveforms, NB-IoT and LTE-M, are cellular-based IoT protocols and therefore require licensed frequency spectrum to operate. Ingenu is from the LPWAN class and operates in the unlicensed frequency spectrum. This study did not make a determination on the use of licensed or unlicensed spectrum and, therefore, left all three waveforms as feasible alternatives to LoRaWAN for both the Orbital-1 CubeSat and greater DOD SATCOM.

b. *Research Question 1: Is there an alternative chirp spread spectrum (CSS) transceiver with the same form, fit, and function as the Semtech-based LoRaWAN transceiver that can meet the DOD requirements for use on the Orbital-1 CubeSat?*

Preliminary research in this study ruled out the feasibility of replacing the Pycom L04 LoRaWAN transceiver with a substitute CSS transceiver. Therefore, after examining alternative waveforms to LoRaWAN, this study selected three of the six assessed transceivers as viable alternatives. They are designed to operate with either NB-IoT/LTE-M or Ingenu waveforms.

Like the waveform analysis, there was also a primary differentiator for the transceivers: security. The security threat of the selected transceivers was assessed based on FY19 NDAA and Executive Order 13873 compliance. Two of the three feasible transceivers were determined “compliant”: Thales DIS EMS31-X and TN-23, which support NB-IoT and LTE-M waveforms. The other one was determined “likely compliant”: U-blox SARA-S200, which implements the Ingenu waveform. In addition to meeting the security requirements of this study, these transceivers also met the thresholds set for power, transmission frequency, physical size, and cyber security.

2. Contributions

To the best of the researcher’s knowledge, the outcomes of this research have yielded one of the first comprehensive, comparative analyses of current and near-term IoT waveforms for DOD SATCOM applications. This study provided unique insight into the limitations of FCC frequency regulations and legislative and executive branch compliance requirements unique to government telecommunications and services. Further, over the course of this research, a valuable data pool on IoT waveforms was established that could be used for subsequential, obliquely-related research.

This study also adds to the body of knowledge on which IoT protocols are best suited for communications with satellites in LEO. Throughout the research process, the study designed a rule-based flow chart to assess IoT waveforms. This flow chart can become the foundation for an AI/ML model for SDR IoT waveform switching. Like the Information Scientists and public sector companies discussed during the literature review, this study found value in both cellular and LPWAN IoT protocols for space-based communications. Although this research identified more cellular waveforms than LPWANs as feasible protocols, the expense of paying for frequency allocation is significant. Unless the DOD performs a broader acquisition of the licensed spectrum, it seems LPWAN is ideal for experimentation and academic studies.

B. LIMITATIONS AND FUTURE RESEARCH

Due to the emergent nature of this topic, this study was primarily limited by the reliable data available. When assessing the alternative waveforms to LoRaWAN, several waveforms had variables with “no data available” or only one to two sources to reference. Similar challenges occurred when comparing transceiver options. Since data sheets are not required to be developed in a standardized form, manufacturers choose what they want to be included. This problem was significant enough to cause the abandonment of two transceiver variables: transmission range and memory.

This study was further limited by time. Since the research was cross-sectional, the study was restricted to the current works available at the time. With such an evolving topic, the timeline restriction can be significant. Most of the works cited, especially in the IoT protocols section, are from 2019 to 2022, with an increasing number of references from 2022.

These limitations, in addition to discoveries made throughout the research process, lead to several future research recommendations. First, researchers will need to further define the security requirements and threats. Next, researchers should examine the viable transceivers via modeling and simulation and then bench testing. Lastly, there is a necessity for researchers to design an operational concept for a DOD LEO IoT CubeSat mesh network.

Although this study touches on the significance of security and communications resilience, a more thorough examination must be completed before any of the proposed IoT waveforms can be utilized by the DOD for mission purposes. Broadly, security protocols should be explored to ensure confidentiality, integrity, and availability through system design, physical security, and network security lenses (Dimov, 2021). Additionally, further research can be done to determine a more definitive answer to the FY19 NDAA and EO 13873 compliance requirements.

To further refine the selection pool for the Orbital-1 transceiver replacement, it would be valuable to first model and simulate the circuit card assemblies and then bench-test actual PCBs from the identified companies. The IoT transceivers are relatively inexpensive (less than $30 per unit), and some companies will offer free prototype PCBs in exchange for access to the test result data (Digi-key Electronics, n.d.). Access to the physical PCB will yield more precise data on how the component actually performs and if it is truly compatible with the Orbital-1.

Finally, this study forms a critical foundation to build upon in the development of an operational concept for a DOD LEO IoT CubeSat mesh. The concept could explore the requirements on an enterprise level to manage the architecture, discuss the operational benefits of an IoT CubeSat mesh; show integration challenges with existing DOD

SATCOM architecture; and demonstrate multiple applications for the network, such as communication relays, remote network monitoring, and transport for various IoT sensor data.

C. CONCLUSION

This study examined the DOD SATCOM capacity problem through the lens of implementing IoT waveforms on a theoretical IoT LEO CubeSat constellation in order to diversify and add resiliency to DOD communications in remote territories. The research identified and then examined ten waveform and eight transceiver variables to ultimately select three viable alternatives to the LoRaWAN L04 transceiver for the Orbital-1 CubeSat. The field of IoT is emerging, and there is still much to examine and test, but this study adds to the body of knowledge on space-based IoT, especially in regard to DOD use.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1-3 OSI reference model. (2013, December 12). Retrieved September 4, 2022, from https://www.freeccnastudyguide.com/study-guides/ccna/ch1/1-3-osi-reference-model/

Airoha. (2006). AL2236 2.4 GHz RF transceiver [Data Sheet]. Retrieved September 25, 2022, from https://www.datasheets360.com/pdf/-217205260247329252

Asif, S. (2018). Radio Frequency Spectrum. In *5G Mobile Communications: Concepts and Technologies* (pp. 15–24). CRC Press. doi:https://doi.org/10.1201/9780429466342-3

Adame, T., Bel, A., Bellalta, B., Barcelo, J., & Oliver, M. (2014). IEEE 802.11ah: The WIFI approach for M2M communications. *IEEE Wireless Communications, 21*(6), 144–152. doi:10.1109/mwc.2014.7000982

Address to joint session of Congress May 25, 1961. (n.d.). Retrieved July 25, 2022, from https://www.jfklibrary.org/learn/about-jfk/historic-speeches/address-to-joint-session-of-congress-may-25-1961

Afhamisis, M., & Palattella, M. R. (2022). Salsa: A scheduling algorithm for Lora to LEO satellites. *IEEE Access, 10*, 11608-11615. doi:10.1109/access.2022.3146021

Almuhaya, M. A., Jabbar, W. A., Sulaiman, N., & Abdulmalek, S. (2022). A survey on LoRaWAN technology: Recent trends, opportunities, simulation tools and future directions. *Electronics, 11*, 1–32. doi:10.3390/electronics11010164

Andrade, R. O., & Yoo, S. G. (2019). A comprehensive study of the use of LoRa in the development of smart cities. *Applied Sciences, 9*(22), 1–39. doi:10.3390/app9224753

Arifin, J. (2021). Study of CUBESAT systems for IOT. *2021 12th International Renewable Engineering Conference (IREC)*. doi:10.1109/irec51415.2021.9427817

Asia Satellite. (n.d.). Hughes 9502 BGAN M2M external antenna terminal - 2 piece (3500509-0001). Retrieved August 25, 2022, from https://www.asiasatellite.co/Hughes-9502-BGAN-M2M-Terminal-2-Piece-p/Hughes-9502-Fixed-BGAN-Termina.htm#whats_included

Australian Space Academy. (n.d.). *Radio frequencies for space communication*. Retrieved September 13, 2022, from https://www.spaceacademy.net.au/spacelink/radiospace.htm

Badodekar, N., & Chougala, G. (2019, December 23). Ensuring fail-safe data storage in battery-powered IOT sensor nodes. Retrieved September 25, 2022, from https://www.embedded.com/ensuring-fail-safe-data-storage-in-battery-powered-iot-sensor-nodes/

Barros, S. (2019, June 23). *12 use cases for 5G ultra reliable communications*. Retrieved August 26, 2022, from https://www.linkedin.com/pulse/12-use-cases-5g-ultra-reliable-communications-sebastian/

Bauer, B., & Patrick, A.S. (2002). A Human factors extension to the seven-layer OSI Reference Model. Retrieved September 4, 2022 from https://www.semanticscholar.org/paper/A-Human-Factors-Extension-to-the-Seven-Layer-OSI-Bauer-Patrick/74d13837b2dd0bdd47e1255a8ed91e4de14caba1

Bechtold, L. (1994, December 31). Bit rate and frequency in data communications. Retrieved September 8, 2022, from https://www.cablinginstall.com/connectivity/rj45-utp-shielded/article/16469695/bit-rate-and-frequency-in-data-communications

Bizon Franco de Almeida, I., Chafii, M., Nimr, A., & Fettweis, G. (2021). Alternative chirp spread spectrum techniques for LPWANs. *IEEE transactions on green communications and networking, 5*(4), 1846–1855. doi:10.1109/tgcn.2021.3085477

Bloechl, M. (n.d.). *What is LoRaWAN [2022 update]: Link labs*. Retrieved September 14, 2022, from https://www.link-labs.com/blog/what-is-lorawan

Bocker, S., Arendt, C., Jorke, P., & Wietfeld, C. (2019). LPWAN in the context of 5G: Capability of LoRaWAN to contribute to MMTC. *2019 IEEE 5th World Forum on Internet of things (WF-IoT)*. doi:10.1109/wf-iot.2019.8767333

Britannica. (n.d.). *American radio goes to war.* Retrieved September 5, 2022, from https://www.britannica.com/topic/radio/American-radio-goes-to-war

California State University, San Bernardino [CSUSB]. (n.d.). Statement of the Shannon-Hartley theorem. Retrieved September 13, 2022, from http://cse.csusb.edu/ykarant/courses/f2010/csci530/shannon-hartley-theorem.html

Cameron, B. G., Crawley, E.F. (2018, October 1). A technical comparison of three low earth orbit satellite constellation systems to provide global broadband [Presentation]. Massachusetts Institute of Technology. https://web.archive.org/web/20210225093826/http://www.mit.edu/~portillo/files/Comparison-LEO-IAC-2018-slides.pdf

Carter, J. (1978, May 11). National Space Policy (1978). (United States of America, President). Washington, DC. https://csps.aerospace.org/sites/default/files/2021-08/PD-37%20National%20Space%20Policy%2011May78.pdf

Centenaro, M., Costa, C., Granelli, F., Sacchi, C., & Vangelista, L. (2021). A survey on technologies, standards and open challenges in satellite IOT. *IEEE Communications Surveys & Tutorials, 23*(3), 1693–1720. doi:10.1109/comst.2021.3078433

Chapman, T., Larsson, E., Von Wrycza, P., Dahlman, E., Parkvall, S., & Sköld, J. (2015). High-order modulation. In *HSPA evolution: The fundamentals for mobile broadband* (pp. 219–233). Academic Press. doi:https://doi.org/10.1016/B978-0-08-099969-2.00010-7

Chaudhari, B., & Borkar, S. (2020). Design considerations and network architectures for low-power wide-area networks. *LPWAN technologies for IoT and M2M applications,* 15–35. doi:10.1016/b978-0-12-818880-4.00002-8

Chaudhari, B., & Zennaro, M. (2020). *LPWAN technologies for IOT and M2M applications*. Academic Press.

Cisco. (2022, February 09). *What is encryption? explanation and types*. Retrieved September 9, 2022, from https://www.cisco.com/c/en/us/products/security/encryption-explained.html

Cocco, G., & Ibars, C. (2012). On the feasibility of satellite M2M systems. *30th AIAA International Communications Satellite System Conference (ICSSC)*. doi:10.2514/6.2012-15074

Coleman, D. D., & Westcott, D. A. (2021). Wireless LAN topologies. In *CWNA: Certified Wireless Network Administrator Study Guide: Exam CWNA-108* (pp. 247–270). Indianapolis, IN: Sybex, a Wiley brand.

Combined Arms Support Command [CASCOM]. (2020, July 13). In-transit visibility (ITV). United States Army. Retrieved September 5, 2022, from https://cascom.army.mil/g_staff/cdi/esd/itv/

Compal. (n.d.). *Investor relations*. Retrieved September 25, 2022, from https://www.compal.com/investor-relations/company-info/

Compal. (2017). RU232 [Data Sheet Preliminary]. Retrieved September 25, 2022, from https://www.ingenu.com/wp-content/uploads/2017/12/RU232-brochure.pdf

Council on Foreign Relations [CFR]. (n.d.). *The history of communications*. Retrieved September 5, 2022, from https://world101.cfr.org/global-era-issues/globalization/two-hundred-years-global-communications

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage.

Crook, M. (2011, May). SATCOM Overview_May2011_cut [PowerPoint slides]. Space Systems Academic Group, Naval Postgraduate School. Sakai@NPS.

Clark, S. (2022, May 13). *SpaceX passes 2,500 satellites launched for Starlink internet network*. Retrieved July 12, 2022, from https://spaceflightnow.com/2022/05/13/spacex-passes-2500-satellites-launched-for-companys-starlink-network/

Dailey, J. (2022, July 6). *AFRL spacecraft recurve launches on Virgin Orbit Space Force mission*. Retrieved August 27, 2022, from https://www.afrl.af.mil/News/Article-Display/Article/3083678/afrl-spacecraft-recurve-launches-on-virgin-orbit-space-force-mission/

De Sanctis, M., Cianca, E., Araniti, G., Bisio, I., & Prasad, R. (2016). Satellite communications supporting internet of remote things. *IEEE Internet of Things Journal, 3*(1), 113–123. doi:10.1109/jiot.2015.2487046

Department of Defense [DOD]. (2022, March). Summary of the Joint All-Domain Command and Control (JADC2) Strategy.

Digi-key Electronics. (n.d.). *EMS31-x REL.3: Digi-key electronics*. Retrieved November 16, 2022, from https://www.digikey.com/en/products/detail/thales-dis-formerly-gemalto/EMS31-X-REL-3/10494211

Dimov, I. (2021, August 10). *Guiding principles in information security*. Retrieved November 16, 2022, from https://resources.infosecinstitute.com/topic/guiding-principles-in-information-security/

Ding, J., Nemati, M., Ranaweera, C., & Choi, J. (2020). IOT connectivity technologies and applications: A survey. *IEEE Access, 8*, 67646-67673. doi:10.1109/access.2020.2985932

Dubrawsky, I. (2010). Wireless networks. In *Eleventh hour Security+: Exam SYO-201 study guide* (pp. 77–88). Burlington, MA: Syngress. doi:https://doi.org/10.1016/B978-1-59749-427-4.00006-X

Dunbar, B. (2004, October 4). *SpaceShipOne wins X-Prize*. Retrieved July 25, 2022, from https://www.nasa.gov/vision/space/gettingtospace/SpaceShipOne.html

Eberle, W. (2008). Efficient Digital VLSI signal processing for OFDM. In *Wireless transceiver systems design* (pp. 79–131). New York, NY: Springer. doi:https://doi.org/10.1007/978-0-387-74516-9

Electronic Product Code Global [EPCglobal]. (2005, May 10). *EPC Generation 1 Tag Data Standards Version 10 1.1 Rev.1.27*. https://www.gs1.org/sites/default/files/docs/epc/tds_1_1_rev_1_27-standard-20050510.pdf

European Space Agency [ESA]. (2020, February 3). *Low earth orbit*. Retrieved September 5, 2022, from https://www.esa.int/ESA_Multimedia/Images/2020/03/Low_Earth_orbit

Eutelsat. (n.d.). *Eutelsat Leo satellite network*. Retrieved August 27, 2022, from https://www.eutelsat.com/en/satellites/elo-fleet.html

Executive Order No. 13873, 84 F.R. 96. (2019, May 17). Securing the information and communications technology and services supply chain. https://www.govinfo.gov/content/pkg/FR-2019-05-17/pdf/2019-10538.pdf

Executive Order No. 13914, 85 F.R. 20381 (2020). Encouraging international support for the recovery and use of space resources. https://www.federalregister.gov/documents/2020/04/10/2020-07800/encouraging-international-support-for-the-recovery-and-use-of-space-resources

Faludi, R. (2021, December 10). *Long range vs. short range wireless communications: What's best for your project?*. Retrieved September 8, 2022, from https://www.digi.com/blog/post/long-range-vs-short-range-wireless-communications#:~:text=Range%20is%20defined%20as%20the,antennas%20in%20a%20wireless%20network.

Fawkes, S. (2006). The second space race. *Journal of the British Interplanetary Society* (JBIS), 59, 364–367.

Federal Communications Commission [FCC]. (2020, April 24). *FCC opens 6 GHz band to WiFi and other unlicensed uses*. Retrieved August 11, 2022, from https://www.fcc.gov/document/fcc-opens-6-ghz-band-wi-fi-and-other-unlicensed-uses

Federal Communications Commission [FCC]. (2022a, July 1). FCC Online Table of Frequency Allocations, 47 C.F.R. 2.106 (2022). https://transition.fcc.gov/oet/spectrum/table/fcctable.pdf

Federal Communications Commission [FCC]. (2022b, August 9). Industrial, Scientific, and Medical Equipment, 47 C.F.R. Part 18 (2022). https://transition.fcc.gov/oet/spectrum/table/fcctable.pdf

Federal Communications Commission [FCC]. (2022c, March 25). List of equipment and services covered by section 2 of the Secure Networks Act. Retrieved September 4, 2022, from https://www.fcc.gov/supplychain/coveredlist

Federal Communications Commission [FCC]. (2022d, March 23). Order on the revocation and termination of Pacific Networks Corp. and ComNet USA (LLC) [FCC 22–22]. Retrieved September 4, 2022, from https://www.fcc.gov/document/fcc-revokes-pacific-networks-comnets-telecom-service-authority-0

Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment. 85 Fed Reg. 135. (2020, July 14). in § 48 CFR Parts 1, 4, 13, 39, and 52 https://www.federalregister.gov/documents/2020/07/14/2020-15293/federal-acquisition-regulation-prohibition-on-contracting-with-entities-using-certain.

Ferrer, T., Céspedes, S., & Becerra, A. (2019). Review and evaluation of MAC protocols for satellite IOT systems using nanosatellites. *Sensors, 19*(8), 1947. doi:10.3390/s19081947

Fierce Electronics, S. (2013, May 21). *Orbcomm M2M devices target transportation market.* Retrieved August 21, 2022, from https://www.fierceelectronics.com/components/orbcomm-m2m-devices-target-transportation-market

Fraire, J. A., Céspedes, S., & Accettura, N. (2019). Direct-to-satellite IOT - A survey of the state of the art and future research perspectives. *Ad-Hoc, mobile, and wireless networks,* 241–258. doi:10.1007/978-3-030-31831-4_17

Fraire, J. A., Henn, S., Dovis, F., Garello, R., & Taricco, G. (2020). Sparse satellite constellation design for LoRa-based direct-to-satellite Internet of things. *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*. doi:10.1109/globecom42002.2020.9348042

Froehlich, A., & Loshin, P. (2021, October 25). *What is a payload?* Retrieved September 13, 2022, from https://www.techtarget.com/searchsecurity/definition/payload

Fund, F. (2019, January 29). *Frequency hopping spread spectrum. Wireless implementation testbed lab at the NYU Polytechnic School of Engineering*. Retrieved September 14, 2022, from https://witestlab.poly.edu/blog/frequency-hopping-spread-spectrum/

GeeksforGeeks. (2022, June 15). *Layers of OSI model*. Retrieved September 4, 2022, from https://www.geeksforgeeks.org/layers-of-osi-model/

Gemtek. (n.d.-a). GIoT RPMA Module [Data Sheet]. Retrieved September 25, 2022, from https://www.gemteks.com/en/products/3gXZJ6/download

Gemtek. (n.d.-b). *About gemtek*. Retrieved September 25, 2022, from https://www.gemteks.com/en/about/about

Gemtek. (2021). Gemtek Technology Co., Ltd. 2021 Annual Report. Retrieved September 25, 2022, from https://www.gemteks.com/en/ir/years/EJy4qo/download

General Dynamics Information Technology [GDIT]. (2022, June 9). *GDIT completes software defined network implementation at the Pentagon*. Retrieved August 25, 2022, from https://www.gdit.com/about-gdit/press-releases/gdit-completes-software-defined-network-implementation-at-the-pentagon/

Goldstein, P. (2021, July 29). *Why Disa has embraced SDN for the Pentagon*. Retrieved August 25, 2022, from https://fedtechmagazine.com/article/2018/09/why-disa-has-embraced-sdn-pentagon-perfcon

Gomez, C., Darroudi, S. M., Naranjo, H., & Paradells, J. (2021). On the energy performance of Iridium satellite IOT technology. *Sensors*, 21(21), 7235. doi:10.3390/s21217235

Gratton, D. A. (2013). *The Handbook of Personal Area Networking technologies and protocols*. Cambridge: Cambridge University Press. doi:https://doi.org/10.1017/CBO9780511979132

Hackmann, G. (2006, March 21). *802.15 Personal area networks*. Retrieved August 11, 2022, from https://www.cse.wustl.edu/~jain/cse574-06/ftp/wpans/index.html#Section2

Hamad, S. (2011). Creativity: Method or magic? In 2026523007 1406502646 H. Cohen & 2026523008 1406502646 B. Stemmer (Authors), *Consciousness and Cognition: Fragments of Mind and Brain* (pp. 127–137). Academic Press. doi:https://doi.org/10.1016/B978-012373734-2/50010-8

Harris, S. L., & Harris, D. M. (2022). *Digital design and computer architecture*. Elsevier.

History.com Editors. (2010, February 22). *The space race*. Retrieved July 25, 2022, from https://www.history.com/topics/cold-war/space-race#:~:text=By%20landing%20on%20the%20moon,with%20Sputnik's%20launch%20in%201957.

Höyhtyä, M., & Mustonen, M. (2018). Applications of TV white space networks and cognitive radio techniques to satellite communications. *TV white space communications and networks,* 193–208. doi:10.1016/b978-0-08-100611-5.00012-6

Hughes. (2013). *Hughes 9502 BGAN M2M terminal* [Brochure]. Hughes Network Systems. https://www.asiasatellite.co/hughes-9502-bgan-m2m-brochure-pdf

Hwang, Y. (2022, March 28). *Cellular IOT explained - NB-IoT vs. LTE-M vs. 5G and more*. Retrieved August 11, 2022, from https://www.iotforall.com/cellular-iot-explained-nb-iot-vs-lte-m

Ibrahim, D. (2014). Microcomputer systems. In *Designing embedded systems with 32-bit PIC microcontrollers and mikroc* (pp. 1–39). Kidlington, Oxford, UK: Newnes. doi:https://doi.org/10.1016/B978-0-08-097786-7.00001-4.

Institute of Electrical and Electronics Engineers (IEEE). (n.d.). IEEE 802.15 WPAN task group 4 (TG4). Retrieved August 11, 2022, from https://www.ieee802.org/15/pub/TG4.html

Institute of Electrical and Electronics Engineers (IEEE). (1984, March 22). IEEE standard letter designations for radar-frequency bands. Retrieved September 13, 2022 from https://ieeexplore-ieee-org.libproxy.nps.edu/stamp/stamp.jsp?arnumber=29086

Institute of Electrical and Electronics Engineers (IEEE) P802.15 Working Group (WG). (2003, July). Principles and benefits of css [PowerPoint]. IEEE. https://www.ieee802.org/15/pub/03/15-03-0312-00-0040-principles-and-benefits-css.ppt

Inmarsat. (2012, January 25). *New BGAN M2M offers global IP data for M2M communications*. Retrieved August 21, 2022, from https://www.inmarsat.com/en/news/latest-news/enterprise/2012/new-bgan-m2m-offers-global-ip-data-for-m2m-communications.html

Inmarsat. (2022). *Our roadmap*. Retrieved August 21, 2022, from https://www.inmarsat.com/en/about/technology/our-roadmap.html

International Telecommunication Union Radiocommunication Sector [ITU-R]. (2015, August). *Nomenclature of the frequency and wavelength bands used in telecommunications*. https://www.itu.int/dms_pubrec/itu-r/rec/v/R-REC-V.431-8-201508-I!!PDF-E.pdf

Internet Engineering Task Force. (2015, May 27). *Towards a definition of the Internet of Things (IoT) Rev. 1*. https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

Iqbal, M. A., Hussain, S., Xing, H., & Imran, M. A. (2021). Internet of things (IoT) Fundamentals. In *Enabling the Internet of Things fundamentals, design, and applications*. Hoboken, NJ: Wiley.

Iridium. (2020, August 03). *Timeline*. Retrieved August 21, 2022, from https://www.iridiummuseum.com/timeline/

Iridium. (2021, August 25). *Iridium short burst data (SBD)*. Retrieved August 21, 2022, from https://www.iridium.com/services/iridium-sbd/

Iridium. (2020). Iridium edge part#1601 [Datasheet]. Retrieved August 25, 2022, from https://www.iridium.com/products/iridium-edge/

John S. McCain National Defense Authorization Act [NDAA] for Fiscal Year 2019, P.L. 115–232, 132 STAT. 1636. (2018). https://www.govinfo.gov/content/pkg/PLAW-115publ232/pdf/PLAW-115publ232.pdf

Joint Chiefs of Staff [JCS]. (2018, June 8). *Cyberspace Operations* (JP 3-12). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Jones, J., Scro, K., Payne, D., Ruhge, R., Erickson, B., Andorka, S., . . . Starks, M. (2015, October 18). Research to operations of ionospheric scintillation detection and forecasting. Retrieved September 17, 2022, from https://ui.adsabs.harvard.edu/abs/2015amos.confE..38J/abstract

Kellermann, T., Centelles, R. P., Camps-Mur, D., Ferrus, R., Guadalupi, M., & Auge, A. C. (2022). Novel architecture for cellular IOT in future non-terrestrial networks: Store and forward adaptations for enabling discontinuous Feeder Link Operation. *IEEE Access, 10*, 68922-68936. doi:10.1109/access.2022.3184720

Khalifeh, A., Aldahdouh, K., Darabkh, K., & Al-Sit, W. (2019). A survey of 5G Emerging wireless technologies featuring LoRaWAN, Sigfox, Nb-IOT and LTE-M. *2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET),* 561–566. doi:10.1109/wispnet45539.2019.9032817

Khan, S. (n.d.). *The scientific method (article)*. Retrieved September 5, 2022, from https://www.khanacademy.org/science/biology/intro-to-biology/science-of-biology/a/the-science-of-biology

Krebs, G. (2008, May 7). *Orbcomm FM101, ..., FM119 (OG2)*. Retrieved August 21, 2022, from https://space.skyrocket.de/doc_sdat/orbcomm-2.htm

Kua, J., Loke, S., Arora, C., Fernando, N., & Ranaweera, C. (2021). Internet of things in space: A review of opportunities and challenges from satellite-aided computing to digitally-enhanced space living. *Sensors, 21*(23), 8117th ser., 1–33. doi:10.3390/s21238117

Kuzlu, M., Pipattanasomporn, M., & Rahman, S. (2018). Assessment of communication technologies supporting smart streetlighting applications. *2018 IEEE International Smart Cities Conference (ISC2)*. doi:10.1109/isc2.2018.8656979

Lacuna Space. (n.d.). *About Lacuna Space*. Retrieved August 27, 2022, from https://lacuna.space/about/

Large, D., & Ciciora, W. S. (2004). Home networks. In *Modern cable television technology video, voice and data communications* (pp. 955–983). Amsterdam: Elsevier/Morgan Kaufmann. doi:https://doi.org/10.1016/B978-155860828-3/50027-8

Launching a new space industry. (n.d.). Retrieved July 25, 2022, from https://www.xprize.org/prizes/Ansari

Lee, J. (2020). Statistics, descriptive. In *International encyclopedia of human geography (second edition)* (pp. 13–20). Elsevier. doi:https://doi.org/10.1016/B978-0-08-102295-5.10428-7

Liberg, O., Sundberg, M., Wang, Y. E., Bergman, J., Sachs, J., & Wikström, G. (2020). Cellular Internet of things: From massive deployments to critical 5G applications. London, UK: Academic Press.

Meghanathan, N. (2014). Algorithms to determine stable connected dominating sets for mobile ad hoc networks. In 2029873452 1408565945 M. A. Matin (Author), *Handbook of research on progressive trends in wireless communications and networking* (pp. 249–274). Hershey, PA: IGI Global. doi:https://doi-org.libproxy.nps.edu/10.4018/978-1-4666-5170-8.ch009

Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IOT deployment. *ICT Express, 5*(1), 1–7. doi:10.1016/j.icte.2017.12.005

Milenkovic, M. (2020). Internet of things: Concepts and system design. Dublin, CA: Springer. doi:https://doi.org/10.1007/978-3-030-41346-0

Minoli, D. (2015). M2M developments and satellite applications. In *Innovations in satellite communications and satellite technology: The industry implications of DVB-S2X, high throughput satellites, Ultra HD, M2M, and IP* (pp. 221–295). John Wiley & Sons.

Moltz, J. C. (2013). From theory to policy. In 1998769489 1389798904 E. Sadeh (Author), *Space strategy in the 21st century: Theory and policy* (p. 23). London: Routledge.

Murata. (n.d.-a). Type 1SE(LBAD0ZZ1SE): Product lineup [Data Sheet]. Retrieved September 25, 2022, from https://www.murata.com/en-us/products/connectivitymodule/lpwa/overview/lineup/type-1se#anchor-2

Murata. (n.d.-b). *Affiliated companies greater China and east Asia*. Retrieved September 25, 2022, from https://corporate.murata.com/en-us/company/muratalocations/affiliated_eastasia

Murata. (2018). LBAD0ZZ1SE LTE CAT M1/NB-IoT Module [Data Sheet]. Retrieved September 25, 2022, from https://media.digikey.com/pdf/Data%20Sheets/Murata%20PDFs/LBAD0ZZ1SE_DS.pdf

Murata. (2021). Product brief type 1SE end device [Data Sheet]. Retrieved September 25, 2022, from https://www.mouser.com/datasheet/2/281/1/Murata_05182021_End_Device_1SE_ProductBrief-2326842.pdf

Murugan, P., & Agrawal, Y. (2020). Small satellites applications, classification and technologies. International Journal of Science and Research (IJSR), 9(7), 1683–1687. doi:10.21275/SR20723213825

National Institute of Standards and Technology [NIST]. (2019, March). Cyber-physical systems and Internet of things (NIST SP1900-202). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf

National Institute of Standards and Technology Computer Security Resource Center [NIST CSRC]. (n.d.). Spread spectrum – Glossary: CSRC. Retrieved September 14, 2022, from https://csrc.nist.gov/glossary/term/spread_spectrum

National Reconnaissance Office [NRO]. (2019, November 1). *CubeSat Fact Sheet* [Fact Sheet]. https://www.nro.gov/Portals/65/documents/news/NRO%20Fact%20Sheets_CubeSat%201%20Nov%2019.pdf?ver=2019-11-01-073813-603#:~:text=NRO's%20CubeSats,of%20new%20technologies%20in%20space.

The National Space Policy, 85 Fed. Reg. 81755 (2020, December 9) (FR. Doc 2020–27892). https://www.federalregister.gov/documents/2020/12/16/2020-27892/the-national-space-policy

Obe, M. (2022, January 10). *Murata's Thailand move heralds Japan tech shift from China.* Retrieved September 25, 2022, from https://asia.nikkei.com/Spotlight/Supply-Chain/Murata-s-Thailand-move-heralds-Japan-tech-shift-from-China

Office of Research Integrity [ORI]. (n.d.). *Model 3 elements of research section 1. U.S. Department of Health and Human Services.* Retrieved September 5, 2022, from https://ori.hhs.gov/module-3-elements-research-section-1

Oliveira, L., Rodrigues, J., Kozlov, S., Rabêlo, R., & Albuquerque, V. (2019). Mac layer protocols for Internet of things: A survey. *Future Internet, 11*(1), 16. doi:10.3390/fi11010016

OneWeb. (2022, June 14). *Experience oneweb.* Retrieved July 12, 2022, from https://oneweb.net/our-network/experience-oneweb

Onireti, O., & Imran, M. A. (2018). Satellite communications in the 5G ERA. In *Satellite communications in the 5G era* (pp. 1–23). London: The Institution of Engineering and Technology. doi:10.1049/PBTE079E_ch1

Onomondo. (2021, July 22). *NB-IOT vs. LTE-M: A comparison*. Retrieved August 11, 2022, from https://www.iotforall.com/nb-iot-vs-lte-m-a-comparison#:~:text=NB%2DIoT%20can%20be%20deployed,to%20be%20available%20on%205G.

Orbcomm. (2021a). ST6100 Satellite Terminal [Datasheet]. Retrieved August 25, 2022, from https://www.orbcomm.com/PDF/datasheet/st-6100.pdf

Orbcomm. (2021b). ST2100 [Datasheet]. Retrieved Septmeber 5, 2022 from https://www.orbcomm.com/PDF/datasheet/st-2100.pdf

Orbcomm satellites. (n.d.). Retrieved August 21, 2022, from https://www.n2yo.com/satellites/?c=16

Orgio Inc. (n.d.). *Rock Hsu - Chairman at Compal Electronics*. Retrieved September 25, 2022, from https://theorg.com/org/compal-electronics-inc/org-chart/rock-hsu

Park, H., & Kim, E. (2015). Location-oriented multiplexing transmission for capillary machine-to-machine systems. *Multimedia tools and applications,* 75(22), 14707-14719. doi:10.1007/s11042-015-2833-9

Pegulu, M. (2022, July 29). *How to brand your lora-enabled application*. Retrieved September 14, 2022, from https://blog.semtech.com/how-to-name-and-brand-your-lora-application

Perez, Z. (2022, August 18). *Spaceflight experiment recurve launches in support of warfighter comms*. Retrieved August 27, 2022, from https://www.defensenews.com/battlefield-tech/space/2022/07/06/spaceflight-experiment-recurve-launches-in-support-of-warfighter-comms/

Peterson, K. (2003). Satellite communications. *Encyclopedia of physical science and technology,* 413–438. doi:10.1016/b0-12-227410-5/00673-6

Purnama, A. A., Nashiruddin, M. I., & Murti, M. A. (2020). Feasibility study of the IOT-connectivity deployment for AMI service: A case study in Surabaya City. *2020 IEEE International Conference on Communication, Networks and Satellite (Comnetsat)*. doi:10.1109/comnetsat50391.2020.9328934

Putland, P. (2020). Connecting devices: Access networks. In J. Davies & C. Fortuna (Eds.), *The Internet of Things: From data to insight* (pp. 9–19). Hoboken, NJ: Wiley. https://ieeexplore-ieee-org.libproxy.nps.edu/book/9259568

Pycom. (n.d.-a). L04 Spec sheet v2 [Data Sheet]. Retrieved September 25, 2022 from https://docs.pycom.io/gitbook/assets/specsheets/Pycom_002_Specsheets_L04_v2.pdf

Pycom. (n.d.-b). L04 [Data Sheet]. Retrieved September 25, 2022 from https://pycom.io/wp-content/uploads/2017/10/L04SpecsheetN.pdf

Qu, Z., Cao, H., Cheng, Y., Wu, S., & Zhang, G. (2019). A Lorawan-based network architecture for LEO satellite Internet of things. *2019 IEEE International Conference on Consumer Electronics – Taiwan (ICCE-TW)*. doi:10.1109/icce-tw46550.2019.8991826

Queralta, J. P., Gia, T., Zou, Z., Tenhunen, H., & Westerlund, T. (2019). Comparative study of LPWAN technologies on unlicensed bands for M2M communication in the IOT: Beyond LoRa and LoRaWAN. *Procedia Computer Science, 155*, 343–350. doi:10.1016/j.procs.2019.08.049

Reagan, R. (1982, July 4). National Space Policy (1982). (United States of America, President). Washington, DC. https://csps.aerospace.org/sites/default/files/2021-08/National%20Space%20Policy%20Jul82.pdf

Reynders, B., & Pollin, S. (2016). Chirp spread spectrum as a modulation technique for long range communication. *2016 Symposium on Communications and Vehicular Technologies (SCVT)*. doi:10.1109/scvt.2016.7797659

Saeed, N., Elzanaty, A., Almorad, H., Dahrouj, H., Al-Naffouri, T. Y., & Alouini, M. (2020). Cubesat communications: Recent advances and future challenges. *IEEE Communications Surveys & Tutorials, 22*(3), q3, 1839–1862. doi:10.36227/techrxiv.12179397

Salih, A. (n.d.). *Channel and signal bandwidth [Class Handout]*. College of Engineering, University of Anbar. https://www.uoanbar.edu.iq/eStoreImages/Bank/4815.pdf

Sateliot. (n.d.). *Overview – Sateliot*. Retrieved August 26, 2022, from https://sateliot.space/en/overview/

Sciddurlo, G., Petrosino, A., Quadrini, M., Roseti, C., Striccoli, D., Zampognaro, F., . . . Piro, G. (2022). Looking at NB-IoT over LEO satellite systems: Design and evaluation of a service-oriented solution. *IEEE Internet of Things Journal, 9*(16), 14952-14964. doi:10.1109/jiot.2021.3135060

Semtech. (n.d.). *Leadership: Ye Jane Li member of the Compensation Committee*. Retrieved September 17, 2022, from https://www.semtech.com/company/executive-leadership/ye-jane-li

Sendin, A., Matanza, J., & Ferrus, R. (2021). Wireless IoT technologies. In *Smart grid telecommunications: Fundamentals and Technologies in the 5G Era* (pp. 293–337). Hoboken, NJ: Wiley-IEEE Press. doi:10.1002/9781119755401.ch8

Shen, S., & Lee, A. (2022, August 19). U.S., *China in Thucydides trap: Q&A with Rock Hsu, chairman of Kinpo-Compal Group*. Retrieved September 25, 2022, from https://www.digitimes.com/news/a20220810PD209/compal-electronics-kinpo-compal-group-rock-hsu-thailand-vietnam.html

Siedlecki, S. L. (2020). Understanding descriptive research designs and methods. *Clinical Nurse Specialist, 34*(1), 8–12. doi:10.1097/nur.0000000000000493

Silicon Labs. (n.d.). *AN971: EFR32 Radio Configurator Guide for RAIL in Simplicity Studio v4* [Brochure]. Austin, TX: Author. Retrieved September 14, 2022, from https://www.silabs.com/documents/public/application-notes/an971-efr32-radio-configurator-guide.pdf

Smith, E. & Flock, W. (1993). *Effects of the equatorial ionosphere on L-Band earth-space transmissions* (Document ID: 19940010198). National Aeronautics and Space Administration. https://ntrs.nasa.gov/citations/19940010198

Sorensen, R., Moller, H., & Koch, P. (n.d.). 5G NB-IoT via low density LEO constellations. *35th Annual Small Satellite Conference,* 1–9. Retrieved September 1, 2022, from https://arxiv.org/abs/2108.06172

Soret, B., Leyva-Mayorga, I., Cioni, S., & Popovski, P. (2021). 5G satellite networks for Internet of things: Offloading and backhauling. *International Journal of Satellite Communications and Networking, 39*(4), 431–444. doi:10.1002/sat.1394

Space Policy Directive-5 Cybersecurity Principles for Space Systems. 85 Fed. Reg. 56155 (2020, September 10) (FR Doc. 2020–20150). https://www.federalregister.gov/documents/2020/09/10/2020-20150/cybersecurity-principles-for-space-systems

SpaceX. (n.d.). Retrieved July 12, 2022, from https://www.starlink.com/satellites

Stanford University. (n.d.). *Bits and bytes*. Retrieved September 13, 2022, from https://web.stanford.edu/class/cs101/bits-bytes.html

Strout, N. (2022, August 19). *With all three Gunsmoke-J satellites on orbit, the Army is ready to test space-based targeting*. Retrieved August 27, 2022, from https://www.c4isrnet.com/battlefield-tech/space/2021/07/12/with-all-three-gunsmoke-j-satellites-on-orbit-the-army-is-ready-to-test-space-based-targeting/

Swinhoe, D. (2021, June 9). *Skylo partners with Inmarsat and Softbank to provide satellite based narrowband IOT services - newsroom*. Retrieved September 2, 2022, from https://www.skylo.tech/newsroom/skylo-partners-with-inmarsat-and-softbank-to-provide-satellite-based-narrowband-iot-services

Telesat. (2022, May 06). *Telesat Lightspeed LEO Network*. Retrieved August 26, 2022, from https://www.telesat.com/leo-satellites/

Tetcos. (n.d.). *Internet of Things (IOT) and Wireless Sensor Networks (WSN)* [Handbook]. https://www.tetcos.com/downloads/v12/IOT-WSN.pdf

Texas Instruments. (n.d.). *Wi-Sun Products*. Retrieved September 21, 2022, from https://www.ti.com/wireless-connectivity/wi-sun/overview.html

Thales Digital Identity and Security [Thales DIS]. (2018). MTC LTE Cinterion EMS31 Wireless Module LTE Cat. M1 for Highly Efficient 4G [Data Sheet]. Retrieved September 25, 2022, from Connectivityhttps://storage.pardot.com/128881/202589/Thales_Cinterion_EMS31_Datasheet.pdf

Thales Defense & Security Inc. [Thales DSI]. (n.d.). *About Thales Defense & Security, Inc.*. Retrieved September 25, 2022, from https://www.thalesdsi.com/about-company-2/

Thales Group. (n.d.-a). *TN23-W efficient MTC module (LTE Cat.NB2) global*. Retrieved September 25, 2022, from https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/iot-connectivity/products/iot-products/tn23-w

Thales Group. (n.d.-b). Cinterion TN23 IoT Module LTE Cat NB1 and NB2 in breakthrough "Things" [Preliminary Data Sheet]. Retrieved September 25, 2022, from footprinthttps://iot.thalesgroup.com/Thales_TN23_Datasheet?_ga=2.27972089.491504852.1664060144-1729355293.1664060123

Thales Group. (n.d.-c). *Management and board*. Retrieved September 25, 2022, from https://www.thalesgroup.com/en/global/group/management-and-board

The Things Network. (n.d.). *Device classes*. Retrieved September 11, 2022, from https://www.thethingsnetwork.org/docs/lorawan/classes/

The Things Network. (2021, November 26). *Spreading factors*. Retrieved September 14, 2022, from https://www.thethingsnetwork.org/docs/lorawan/spreading-factors/

U-blox. (2017). SARA-S200 Size and power optimized RPMA module for the machine network [Data Sheet]. Retrieved September 25, 2022, from https://content.u-blox.com/sites/default/files/SARA-S200_DataSheet_%28UBX-17048649%29.pdf

U-blox. (2018). Product Summary SARA-S200 Size and power optimized RPMA module for the machine network [Data Sheet]. Retrieved September 25, 2022, from https://content.u-blox.com/sites/default/files/SARA-S200_ProductSummary_%28UBX-17013042%29.pdf

U-blox. (2022a, May 12). *New composition of board of directors and executive committee*. Retrieved September 25, 2022, from https://www.u-blox.com/en/press-releases/new-composition-of-board-of-directors-and-executive-committee#:~:text=Thereafter%2C%20the%20Executive%20Committee%20will,previously%20taken%20by%20Thomas%20Seiler

U-blox. (2022b, June 08). *Partners and alliances*. Retrieved September 25, 2022, from https://www.u-blox.com/en/alliance-memberships-partnerships

Ugwuanyi, S., Paul, G., & Irvine, J. (2021). Survey of IOT for developing countries: Performance analysis of LoRaWAN and cellular NB-IoT Networks. *Electronics,* 10(18), 2224. doi:10.3390/electronics10182224

Ullah, M. A., Mikhaylov, K., & Alves, H. (2022). Enabling MMTC in remote areas: LoRaWAN and LEO satellite integration for offshore wind farm monitoring. *IEEE transactions on industrial informatics, 18*(6), 3744–3753. doi:10.1109/tii.2021.3112386

United States Air Force [UASF]. (2015). *MILSTAR Satellite Communications System* [Fact Sheet]. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104563/milstar-satellite-communications-system/

United States Space Force [USSF]. (2021). *MILSTAR Satellite Communications System* [Fact Sheet]. Space Operations Command. https://media.defense.gov/2022/Apr/08/2002973443/-1/-1/1/MILSTAR%20FACTSHEET.PDF

University of California. (n.d.). *Understanding waves*. Retrieved September 8, 2022, from http://earthguide.ucsd.edu/wav/frequency.html

University of Cambridge. (2022, August 16). *A technique to guide the development of faster and longer lasting next-generation batteries*. ScienceDaily. Retrieved September 14, 2022 from www.sciencedaily.com/releases/2022/08/220816120249.htm

Verizon. (2021, March 3). *Verizon announces C-band auction results*. Retrieved September 17, 2022, from https://www.verizon.com/about/news/verizon-announces-c-band-auction-results

Villinger, S. (2022, September 09). *What is RAM and Why is it important?* Retrieved September 9, 2022, from https://www.avast.com/c-what-is-ram-memory#

Voxco. (2022, August 30). *What is descriptive research*. Retrieved September 5, 2022, from https://www.voxco.com/blog/descriptive-research

Waghmare, P. (2022, July 13). *Bandwidth of a signal: Learn definition, formula, applications*. Retrieved September 13, 2022, from https://testbook.com/learn/physics-bandwidth-of-a-signal/

Wang, H., & Fapojuwo, A. O. (2017). A survey of enabling technologies of low power and long range machine-to-machine communications. *IEEE Communications Surveys & Tutorials, 19*(4), 2621–2639. doi:10.1109/comst.2017.2721379

Weik, M. H. (2000). Radio frequency bandwidth. *Computer science and communications dictionary,* 1402–1402. doi:10.1007/1-4020-0613-6_15369

Weissberger, A. (2021, October 01). *Phantom space to build/launch 72 LEO satellites to deliver Ingenu's RPMA IIOT payloads anywhere on earth*. Retrieved September 2, 2022, from https://techblog.comsoc.org/2021/10/01/phantom-space-to-build-launch-72-leo-satellites-to-deliver-ingenus-rpma-iiot-payloads/

West, J., Dean, T., & Andrews, J. (2019). *Comptia Network+ guide to networks*. Cengage.

White House (2022, April). *In-Space Servicing, Assembly, and Manufacturing National Strategy* (2022). National Science and Technology Council. https://www.whitehouse.gov/wp-content/uploads/2022/04/04-2022-ISAM-National-Strategy-Final.pdf

White House (2021, December 1). *United States Space Priorities Framework* (2021). https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Space-Priorities-Framework-_-December-1-2021.pdf

Wi-Sun Alliance. (2019). *Comparing IoT networks at a glance* [Brochure]. Author. Retrieved September 16, 2022, from https://www.wi-sun.org/wp-content/uploads/WiSUN-Alliance-Comparing-IoT-Networks-2019-Nov-A4.pdf

Wu, Y., He, Y., & Shi, L. (2020). Energy-saving measurement in LoRaWAN-based wireless sensor networks by using compressed sensing. *IEEE Access,* 8, 49477-49486. doi:10.1109/access.2020.2974879

Yang, X. (2019). Programming for I/O and storage. In 2031281606 1409427428 R. Oshana & 2031281607 1409427428 M. Kraeling (Authors), *Software Engineering for Embedded Systems: Methods, Practical Techniques, and Applications* (pp. 817–877). Amsterdam: Newnes. doi:https://doi.org/10.1016/B978-0-12-415917-4.00023-2

Yoon, Z., Frese, W., & Briess, K. (2019). Design and implementation of a narrow-band intersatellite network with limited onboard resources for IOT. *Sensors, 19*(19), 4212th ser., 1–25. doi:10.3390/s19194212

Zito, P. (2013, May 3). *What is the OSI model*. Retrieved September 4, 2022, from https://blog.smartbuildingsacademy.com/what-is-the-osi-model

Zorzi, M., & Chockalingam, A. (2003). Wireless communications. *Encyclopedia of Physical Science and Technology,* 851–874. doi:10.1016/b0-12-227410-5/00827-9

Zubair, M., Haider, Z., Khan, S., & Nasir, J. (2011). Atmospheric influences on satellite communications. *PRZEGLĄD ELEKTROTECHNICZNY, 87*, 261–264. Retrieved September 8, 2022, from http://pe.org.pl/articles/2011/5/64.pdf

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California