LoRaWAN & The Helium Blockchain: A Study on Military IoT Deployment

Michael A. Reyneke, Mark G. Reith, and Barry E. Mullins

Air Force Institute of Technology, Wright-Patterson AFB, USA

Michael.Reyneke@afit.edu
Mark.Reith@afit.edu
Barry.Mullins@afit.edu

Author Note: The authors thank the reviewers for their helpful comments**.** The views expressed are those of the authors and do not reflect the official policy or position of the US Air Force, Department of Defense, or the US Government.

Abstract: Technology is evolving at a rapid pace, and the demand for a reliable, far-reaching Internet of Things (IoT) network has never been higher. Low Power Wide Area Network (LPWAN) offers an energy-efficient, low-cost, long-range wireless communication protocol catered to IoT devices. A subset of LPWAN, Long Range Wireless Access Network (LoRaWAN), is being rapidly adopted due to its effortless integration into existing system architectures and real-world success. The Helium Network cryptocurrency blockchain's financial incentives have been used to speed up the LoRaWAN adoption and deployment in urban and rural areas by financially incentivizing gateway owners to establish a redundant network based out of their homes and businesses. In addition to ease of deployment, the Helium Network allows for enhanced security by utilizing a public blockchain ledger to verify the identities of both sender and recipient to combat packet replay and man-in-the-middle attacks. This research argues for the effectiveness of LoRaWAN and Helium Network technology fusion based on real-world examples of a robust and dependable worldwide network. Further, this research advocates for adoption and modification of this technology by the Department of Defense (DoD), to enhance environmental sensing, establish real-time tactical networks, and critical infrastructure and logistics monitoring. If the DoD chooses to integrate these two technologies with its existing IoT infrastructure; it can reliably, securely, and anonymously use LoRaWAN nodes and routers as both a long-range and backup encrypted communication network capable of supporting end-to-end encryption up to AES-128 (DoD SECRET-classification standard). The DoD could capitalize on these successes to advance information dominance in both domestic and international environments. The demonstrated performance and low adoption cost of LoRaWAN and Helium Network technologies could greatly enhance the DoD's mission of maintaining its lethality and dominance in information warfare.

Keywords: Blockchain, Cryptocurrency, Defense, Helium Network, Internet, Internet of Things (IoT), LoRaWAN, Military, Sensors, UHF Communication

1. Introduction

The Internet of Things (IoT) is an ever-evolving wave of technology that is replacing traditional sensor-related technology with low-cost, low-energy, wireless solutions designed for continual use in multiple conditions. Around the world, commercial and industrial sectors have been quick to adopt and adapt IoT technologies to expand their businesses and offer new capabilities to their clienteles. However, world governments have been slow and adverse to adopting or entertaining IoT integration for military purposes. The United States military is interested in warfighting integration with new weapon systems and communications networks but has thus far limited its investment into IoT technologies that support smart military bases, critical infrastructure monitoring, and ruggedized sensors in deployed environments.

IoT devices have distinct requirements such as radio coverage, scalability, and power consumption that can make device deployment difficult. Low Power Wide Area Network (LPWAN) (Raza, et al., 2017) is an emerging technology that is the next step in evolution of wide area, low power wireless communications. LoRaWAN, an open specification subset of LPWAN and Long Range (LoRa), operates within globally unlicensed frequency bands (see Table 1), which eliminates licensing costs and makes this technology affordable and globally deployable-- (Adelantado, et al., 2017) (Sornin, et al., 2015) similar to current long-range IoT wireless communications technologies.

When comparing common wireless communication technologies, as shown in Table 1, Figure 1, and Figure 2, LoRaWAN devices exhibit the following characteristics:

1. *Low Power:* LoRaWAN protocol's low power consumption makes it an excellent candidate for a scalable platform to support IoT devices. In fact, IoT devices with LoRaWAN capabilities consume significantly less power than those using 4G/5G or ZigBee communication protocols.

2. *Low Cost:* The low operating and manufacturing costs of LoRaWAN allow for more resources to be spent on manufacturing IoT sensors and enable the end-user to deploy more or higher quality IoT devices for the same net cost.
3. *Long-Range:* As shown in Figures 1 and 2, LoRaWAN has considerable range (3-5 km in urban areas, 20 km in suburban areas) when compared to more common wireless communications protocol such as Wi-Fi & Bluetooth. While this range is significant, it requires minimal obstructions and preferably a direct line-of-sight between access points and IoT devices utilizing the network. One unique attribute of LoRaWAN is that the signal can reflect off a limited number of buildings, water sources, and hills effectively, which further increases its range.
4. *Enhanced Propagation & Signal Penetration:* LoRaWAN operates under an unlicensed spectrum under the Sub-GHz ISM band (see Table 1). This band provides enhanced signal propagation properties that enable adequate coverage in urban or crowded areas because the signal can penetrate through natural and man-made obstructions without a great deal of signal loss.

Table 1: Comparison of common wireless communication technologies

	Bluetooth *(Bluetooth Inc., 2020)*	**LoRaWAN** *(LoRa Alliance, 2015; Libelium, 2015)*	**Wi-Fi** *(IEEE, 2020)*	**Zigbee** *(ZigBee Alliance, 2015)*
Bandwidth	1 MHz	125 kHz 250 kHz	22 MHz	300 kHz 600 kHz 2 MHz
Frequencies	2.4 GHz	433-434 MHz [EU] 863-870 MHz [EU] 902-928 MHz [NA] 915-928 MHz [AU] 2.4 GHz [Global]	2.4 GHz 5.1 GHz	868 MHz 915 MHz 2.4 GHz
Modulation	GFSK	CSS	BPSK QPSK	O-QPSK
Max Data Rate	1 Mbps	50 kbps	9.6 Gbps	250 kbps
Range (Urban)	10 m	3-5 km	100 m	10 m
Range (Rural)	100 m	20 km	200 m	100 m
Transmit Current (Max)	300 mA	135 mA	700 mA	285 mA
Transmit Power (Max)	10 dBm	14 dBm	20 dBm	20 dBm

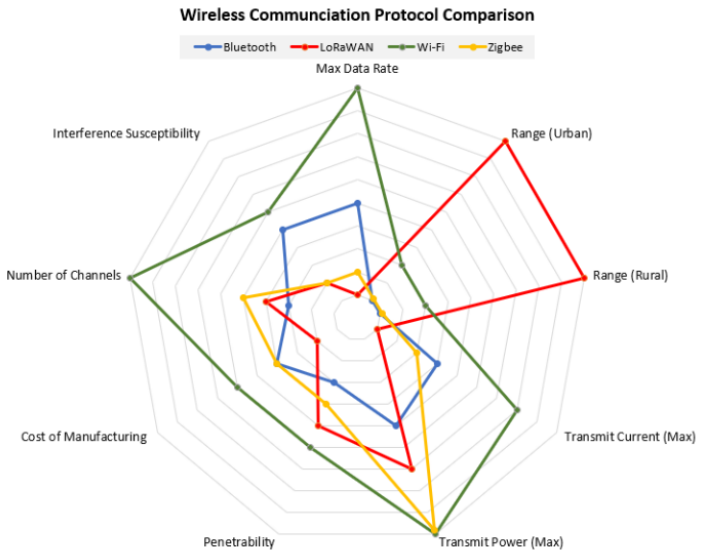

Figure 1: Radar Chart comparing Bluetooth, LoRaWAN, Wi-Fi, and Zigbee wireless communications protocol.

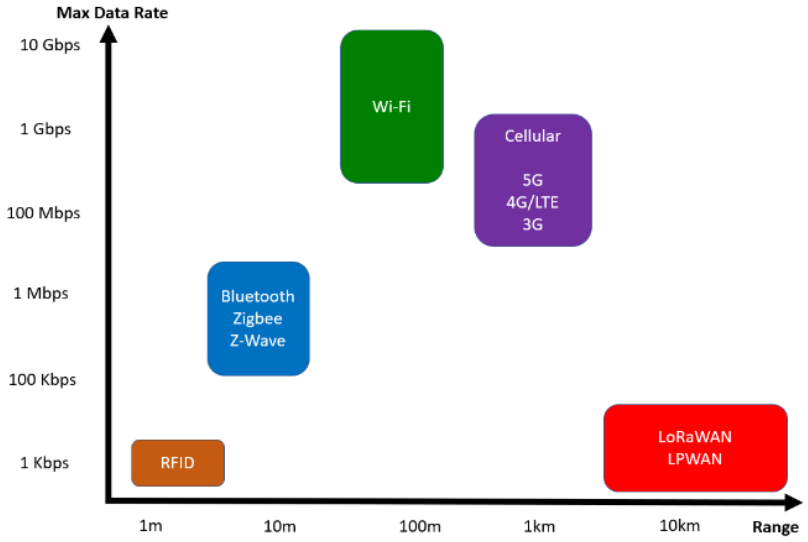

Figure 2: Max data rate and range graph comparing common wireless communication technologies

Integrating the benefits of LoRaWAN with a crypto blockchain, such as the Helium blockchain, can help people and organizations worldwide establish dependable IoT communications built around security and redundancy.

2. The Versatility of the Long-Range LoRaWAN Network

LoRa is the physical layer protocol used in LoRaWAN. LoRa features low power operation, which enables certain devices to last approximately 10 years on a single charge. Compared to other communication technologies, LoRa has a low data rate, between 20-50 kbps, depending on its modulation. However, LoRa makes up for this low-data rate by having an exceptionally long communication range (3-5 km in urban areas, 20 km in rural areas) (Adelantado, et al., 2017). The LoRaWAN network functions on a star topology with LPWAN-enabled access points, gateways, and nodes and maintains a network server connection to the Internet via IP over Cellular or Ethernet. LoRaWAN expands on LoRa capabilities by using AES-128 for end-to-end encryption and adds a frame counter to the packets (Blenn & Fernando, 2017) for verification and to prevent playback attacks. The added security and long-range capabilities make LoRaWAN favored in remote locations where routine access is limited or where sensitive data may be intercepted.

As listed in Table 2, there are three different device classes of LoRaWAN (Class A, B, & C) that can be used for different purposes in various applications:

1. *Class A:* Supports bi-directional communication between an end-device and a gateway. Uplink messages from the device can be sent at any time. The device opens two receive windows at *Rx1 Delay* and *Rx2 Delay* following the uplink transmission. The server chooses to respond in either window. Whatever window it chooses, the other one will close. Class A devices are often battery-powered and have the lowest energy consumption when compared to the other device classes. Class A devices mostly operate in sleep mode, which results in long intervals between uplinks.
2. *Class B:* Extends Class A communication by time-synchronizing receive windows for downlink messages from the server and introduces multicast capabilities. Class B devices are low latency, reachable at preconfigured times, and can receive a downlink at any time. Since these devices are periodically accessed, their battery lives are shorter, and the devices spend more time in an active state.
3. *Class C*: Extends Class B by making receive windows persistent unless the end-device is transmitting. This increases energy consumption but establishes a reliable data stream between devices and gateways. Class C devices are normally AC powered and have no downlink latency due to their always active state.

Table 2: Comparison of LoRaWAN

	LoRa Class A	*LoRa Class B*	*LoRa Class C*
Communication	Bi-directional, occasional	Bi-directional, scheduled	Bi-directional, persistent
Interval Size	Long Intervals	Long Intervals	Short Intervals
Message Type	Unicast	Unicast, Multicast	Unicast, Multicast
Power Type	Battery (high latency)	Battery, AC (low latency)	AC (no latency)
Server Relationship	Server establishes downlink, predetermined response windows	Server initiates communication at periodic intervals	End-device constantly receiving/ transmitting

As seen in Figure 3, as of July 2022, there are 173 network operators in 177 countries who provide full LoRaWAN coverage for all three LoRaWAN classes (LoRa Alliance, 2022). This coverage is more than sufficient for global DoD operations and LoRaWAN system deployment.

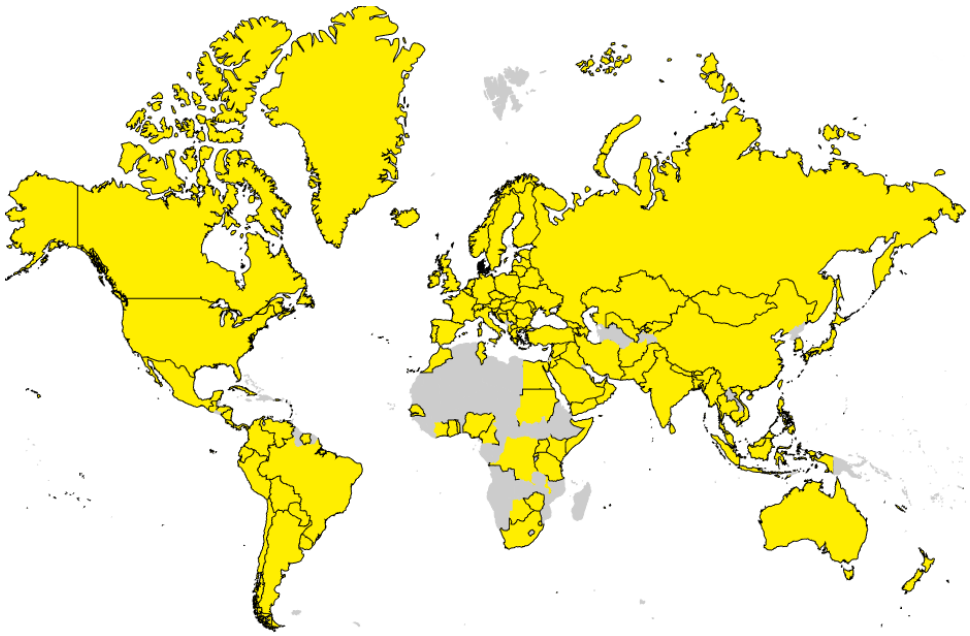

Figure 3: Worldwide LoRaWAN Coverage Map in yellow (LoRa Alliance, 2022)

The security of a communication system is equally important as its availability and reliability. For this reason, the LoRaWAN standard is designed with security in mind "to adhere to state-of-the-art principles: use of standard, well-vetted algorithms, and end-to-end security." (LoRa Alliance, 2017) The network join policy requires mutual authentication before a LoRaWAN end-device can connect to the LoRaWAN network. To prevent traffic from being altered, LoRaWAN messages are origin authenticated, integrity and replay protected, and encrypted up to AES-128 standards.

There are multiple layers of security implemented in the LoRaWAN network at both the software and hardware levels. As with most devices, the effectiveness of a system's security is dependent on the physical access of a malicious actor. If a device (e.g. node, gateway, relay) is subjected to physical intrusion, the encryption keys are stored in Secure Element, a tamper-resistant storage, which makes them extremely difficult to extract (LoRa Alliance, 2017) (Coman, et al., 2019).

3. The Helium Network, Cryptocurrency, and Blockchain

The Helium Network is a cryptocurrency-backed, wide-area networking system that uses protocol tokens for data transmissions (Haleem, et al., 2018). The Helium blockchain is a decentralized wireless network ledger designed to support LoRaWAN IoT devices. The Helium Network utilizes an open-source, standards-compliant wireless network protocol, called *WHIP* (Haleem, et al., 2018), to exchange LoRaWAN traffic for a subset of Helium cryptocurrency called a *Data Credit (DC).* DCs are spent when establishing bi-directional data transfer

between end-devices and the Internet. The process works as follows: (1) End-devices spend DCs to transfer data between the Internet, (2) Gateway operators (miners) earn tokens for providing network coverage and supporting data transfers, and (3) Miners earn Helium ($HNT) tokens for validating the coverage and data integrity of the Helium Network to prevent fraudulent proof-of-coverage or illegitimate geographical placement. $HNT tokens can then be exchanged for other cryptocurrencies or sold on crypto exchanges for fiat currencies

To establish a network proof-of-coverage, as seen in Figure 4, the Helium Network components go through the following process:

An end-device requesting to transmit data across the Internet uses a *Transmitter* to ping the Helium Blockchain. Another node, called a *Challenger*, verifies the Transmitter is a reliable node on the LoRaWAN network. Nearby nodes called *Witnesses* verify both the Challenger and Transmitter can communicate effectively. The Challenger issues a challenge to a node on the Helium Network and the Transmitter sends a beacon to witnesses. Then, the Witnesses receive the beacon and send back a proof-of-coverage receipt of Transmitter's network coverage back to the Challenger. The Challenger then validates the information and informs the Helium Blockchain of its success or failure. Lastly, if the Transmitter provided proper proof-of-coverage, they get rewarded with $HNT.

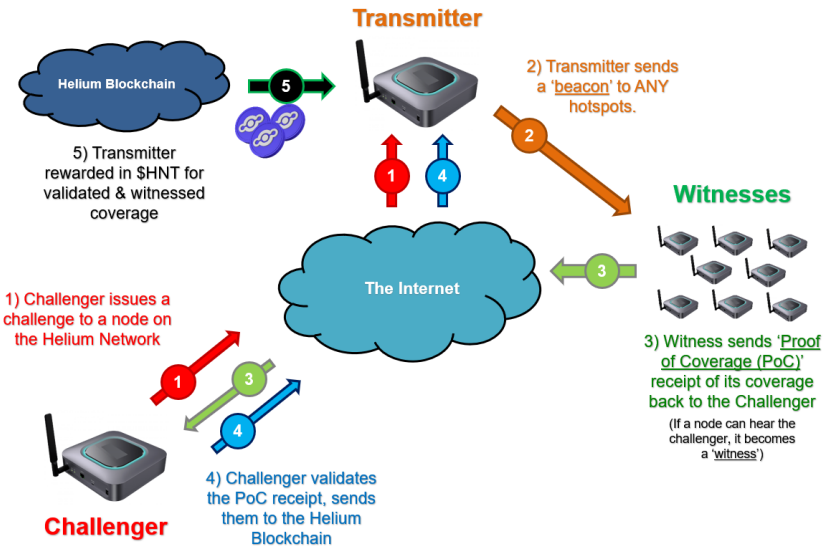

Figure 4: Helium Network Ecosystem

For an end-device to utilize the Helium Network for data transfer, as seen in Figure 5, the end-device must be able to communicate with LoRaWAN gateways and the Helium blockchain (Haleem, et al., 2018) The Helium Network uses a pay-to-communicate model, exhausting DCs, for network utilization. Without connection to the Helium Network, data cannot be exchanged between end-devices and the Internet.

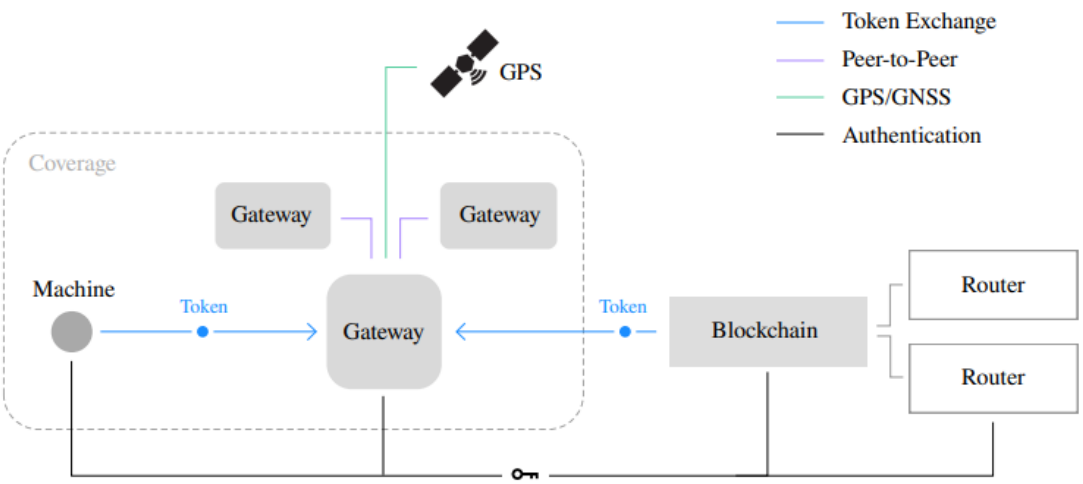

Figure 5: Helium Network Overview (LoRa Alliance, 2017)

4. Military Application of LoRaWAN & Helium Network

The military is fueled by information and demands the information be provided in a timely manner, whether in war or peacetime. By introducing an IoT ecosystem backed by or modelled after the Helium Blockchain, the DoD can create opportunities to obtain critical information otherwise deemed difficult to obtain. The three primary applications for DoD use of LoRaWAN IoT devices are as follows:

1. Environmental Sensing: There have been proven examples of accurate and timely environmental data collection such as real-time urban flood monitoring (Garcia, et al., 2015) and early earthquake detection and monitoring via QuakeSense (Boccadoro, et al., 2019). Utilizing this technology would allow for the real-time monitoring of both natural disaster precursor events and environmental parameters, which could help the DoD to coordinate timely evacuations. With this added information capability, the DoD could effectively evacuate US citizens prior to deadly events such wildfires, tornados, floods, and earthquakes that affect DoD assets. Extending the sensing capabilities in the bioenvironmental field to bolster DoD's monitoring of migration patterns, weather conditions, and environmental viability would be invaluable for global operations. To ensure DoDs smart bases and smart cities comply with environmental laws and policies, LoRaWAN allows the DoD to "pervasively monitor the air quality in urban areas by exploiting public means of transportation as mobile sensor nodes" (Addabbo, et al., 2019). Additionally, this type of monitoring can be deployed during tactical and humanitarian operations to validate information from forward-advance teams and weather personnel to enhance mission success and operational safety.
2. Real-Time Tactical Information: The long-range attributes of LoRaWAN allow IoT devices to be placed in multiple locations and on multiple assets such as personnel, vehicles, and buildings to receive, transmit, and verify data. Since there are normally no reliable sources of Ethernet in deployed or training locations, a satellite uplink would be necessary to manage the Internet uplink for these devices (Abdullahi, et al., 2019). When paired with other communication protocol combinations, such as LoRaUAV's use of Wi-Fi and LoRaWAN, real-time information such as GPS and biometric data can be successfully received and transmitted from firefighters carrying portable LoRaWAN tags (Stellin, et al., 2020). Defensively, LoRaWAN devices could be ruggedized and placed on deployed personnel to monitor human factors such as stress and vitals, as well as location to prevent friendly fire incidents (Stellin, et al., 2020). Offensively, LoRaWAN devices could be integrated into adversarial infrastructure to monitor their movement, capabilities, and identify potential opportunities for the neutralization/exploitation of their assets (Kott, et al., 2016).
3. Special consideration must be had when implementing ruggedized LoRaWAN devices in the field as they have a risk of being lost, captured, or reverse-engineered by hostile groups. A ruggedized LoRaWAN device would need obfuscated hardware and software modules to discourage and frustrate any reverse-engineering attempts. Additionally, these ruggedized devices would require additional encryption protocols to prevent signal interception and detection.

4. Critical Infrastructure: LoRaWAN's wireless signal range and broad support of multiple devices could prove to be effective in streamlining the monitoring of critical infrastructure such as electricity, natural gas, water, and sewage. (Conceição, et al., 2020) (Michaelis, et al., 2019). One such example utilizes LoRaWAN for smart infrastructure to monitor physical access to city sewer systems to increase civic response (Chaudhari, et al., 2021). LoRaWAN's ability to process Message Queuing Telemetry Transport (MQTT) messages means existing IoT infrastructure need minimal modification as they may only require a LoRaWAN antenna module, as seen in Figures 6 and 7, to connect (Fathoni, et al., 2020) (Black Hills Information Security, 2022). It is important to note that if DoD implements this technology, adoption costs and upgrade time will be extremely low.

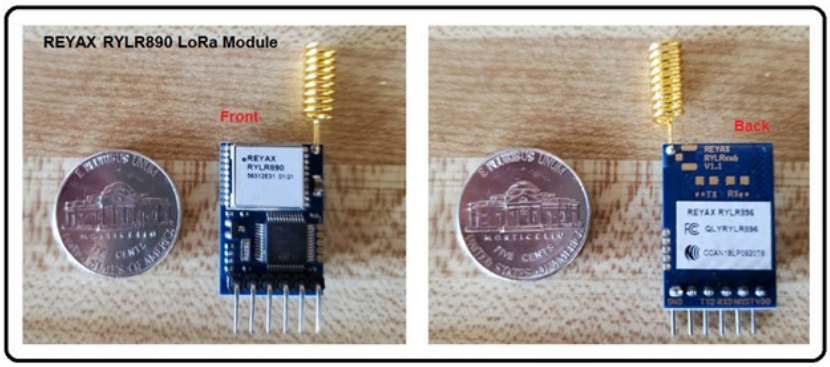

Figure 6: REYAX RYLR890 LoRa Radio Module (Black Hills Information Security, 2022)

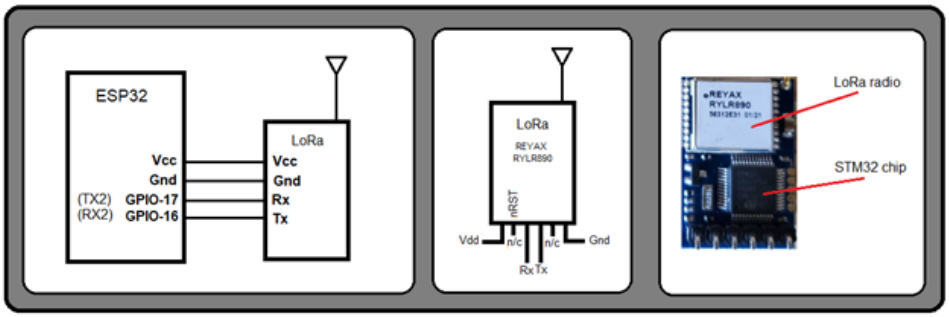

Figure 7: REYAX RYLR890 Pin-Out Diagram (Black Hills Information Security, 2022)

In November 2021, the DoD experienced a hazardous environmental disaster where over 14,000 gallons of jet fuel spilled at the Red Hill Bulk Fuel Storage Facility inside an access tunnel at Joint Base Pearl Harbor-Hickam (JBPHH), HI, USA. (The Associated Press, 2021) While the spill was being cleaned up, the jet fuel had already integrated with the Navy's water distribution system at JBPHH which serves over 93,000 people. This fuel spill contaminated residential and commercial water systems with contaminants found to be at double Hawaii's health limits for drinking water (The Associated Press, 2021). Initially undetected, the jet fuel infused water caused multiple health problems in military members, DoD contractors, and their families, and resulted in the evacuation of over 3,000 families until the problem was resolved. If LoRaWAN and Helium Network IoT sensors were installed in the service tunnels where the spill occurred and at the water distribution plant, the contaminants would have been detected sooner and the consumption of the contaminated water could have been mitigated.

5. *Logistics Monitoring:* LoRaWAN end-devices and routers could also be integrated into stationary cargo aircraft and vehicles to actively generate $HNT cryptocurrency. Additionally, end-devices could be integrated with cargo to automatically transmit logistical data to delivery and refueling locations to verify shipment integrity and provide accurate delivery timeframes. For example, an end-device could be programmed to contain the item information of a cargo pallet, be placed on the pallet or in the pallet, and be able to transmit its location, handling conditions, and package contents to an aircraft's LoRaWAN gateway or a LoRaWAN gateway at an aerial or naval port. This would automate and standardize the inventory management process while ensuring accurate delivery timeframes, proper cargo handling,

and up-to-date inventory listings. Additionally, shipping logs would automatically be kept on the blockchain.

5. Analysis of LoRaWAN and Helium Network Hybridization

By contributing to the Helium Network and adding the LoRaWAN wireless communication standard to the DoD's toolbox, we not only increase the resiliency and availability of digital communications but also introduce the risk of data exfiltration and interception.

1. *LoRa Device Classes:* With the three available LoRa devices classes, DoD would be able to selectively tailor each system to a specific environment and use-case model. Class A end-devices are excellent for environmental data collection, water monitoring, natural disaster early warning, and location tracking. DoD could embed Class A devices in training environments where access is irregular and data demands are low. Additionally, these devices could be used to detect seismic activities such as heavy vehicle use or explosions. The presence of CBRN agents could also be detected and recorded by Class A devices. A downside to using Class A devices in remote locations is the battery's integrity and ability recharge or replace an expended energy source. Class B end-devices could prove useful in smart bases and smart cities by wirelessly connecting smart metering on major utilities while having a public blockchain validate the readings and timing. This system would improve resource audit integrity and provide accurate statistics to identify system faults or utility misuse. Interconnectivity of systems remains difficult in subterranean and urban conditions, but LoRaWAN's long-range capabilities solve this problem. Class C end-devices shine where power consumption is not a concern. In addition to adding dedicated Class C devices to its IoT ecosystem, DoD also has the option could integrate a LoRaWAN module (Black Hills Information Security, 2022) into existing IoT and SCADA devices. This would introduce long-range monitoring and real-time configuration capabilities to critical infrastructure systems. This integration also provides an additional communication platform while establishing a blockchain-backed record to verify system changes, detect unauthorized access, and report system abnormalities in real-time. This persistent class of LoRaWAN devices could link geographically separated critical infrastructure nodes where traditional wireless networks cannot reach.
2. *Hybridization of Civilian and Government Gateways*: By distributing the network setup and maintenance to gateway owners, the military can save significant money and time. As discussed previously, due to the sensitivity of DoD information, enhancements may need to be made (end-point encryption and covert communications) to ensure security and functionality. While the Helium Network is maintained primarily by civilians and disinterested parties, the DoD cannot rule out the possibility of malicious actors hosting gateways to commit espionage or sabotage. The DoD would be able to assist with network reliability and increase its own data security by purchasing gateways and maintaining its own infrastructure. Additionally, DoD communications units or other government agencies could maintain gateways for cryptocurrency incentives, which could alleviate budget constraints.
3. *Pay-To-Communicate Model*: One benefit to the pay-to-communicate model is the cost-effectiveness of LoRa Class A devices since they do not transfer at regular intervals. A disadvantage of this model is that the devices cannot transmit on the network if they expend their DC balance or cannot access the Helium Network. This remains as a major hurdle to DoD integration as the appropriate amount of DCs would need to be pre-loaded to the end-devices and then replenished, as necessary. Additionally, depending on the mining capabilities of the LoRaWAN gateways, the DoD may need pay for DCs out-of-pocket to keep devices functional. The Helium Network's pay-to-communicate model requires continual maintenance and monitoring, which would add a large administrative burden to DoD personnel. With these constraints, it would be beneficial for DoD to establish a government-specific LoRaWAN network, modeled after the Helium Network, to allow only white-listed devices to connect to their network without the pay-to-communicate model.
4. *Ruggedized LoRaWAN and Sensitive Operations:* In deployed or austere environments, the DoD would need to maintain a subset of ruggedized LoRaWAN devices with enhanced security features. Ideally, the DoD would establish non-Helium Network devices to prevent the disclosure of DoD presence and communications capabilities on publicly available blockchains. Since most LoRaWAN devices operate with and without the Helium Network, we recommend utilizing this network for smart military bases/cities, critical infrastructure, humanitarian roles, and non-combat expeditionary operations. Modifications to Helium Network and LoRaWAN devices would be necessary to prior to use in combat environments to prevent inadvertently disclosing sensitive information or asset locations.

5. *Cybersecurity Concerns:* Attacks on LoRaWAN include replay, eavesdropping, packet modification, ACK spoofing, and battery exhaustion (Coman, et al., 2019). The greatest vulnerability to LoRaWAN end-devices and gateways is unauthorized physical access. "If an attacker gets access to a node, a gateway, or a server, and if strong hardware security policies are not used, the whole device or even the network must be assumed as compromised." (Coman, et al., 2019) Regarding signals intelligence (SIGINT), these attacks are less prevalent but Yang (Yang, et al., 2018) expands upon these attack vectors discussing how trivial it is for an adversary to successfully execute a message replay attack.

As seen in Figure 8, if an adversary can successfully record the wireless LoRaWAN communications between an end-device and gateway, they can retransmit a malicious version of the message that mimics the following attributes: 1) Device Address 2) Session Keys and 3) Incremented Counter Value (Yang, et al., 2018). A replay attack can be devastating as it can cause service denial and may reveal end-device configurations and locations.

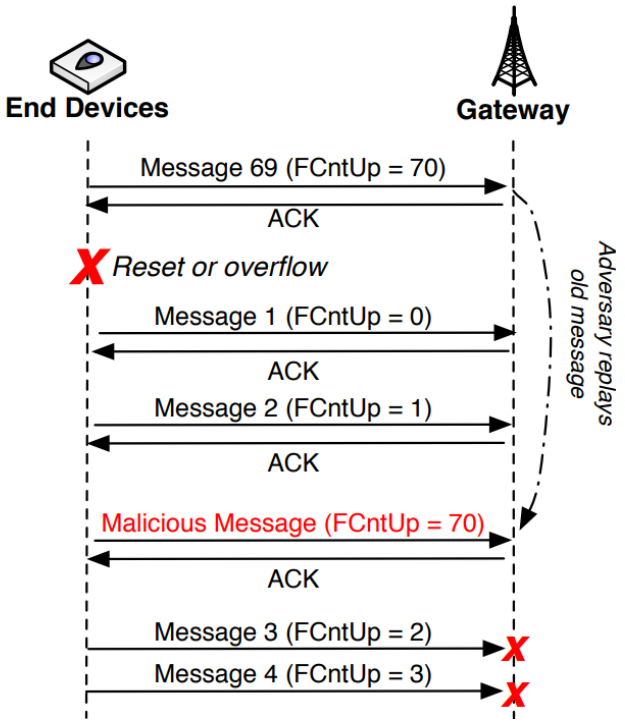

Figure 8: Example of Replay Attack for ABP (Yang, et al., 2018)

If an attacker is unable to successfully intercept and decode messages, they can use an ACK spoofing attack to selectively jam LoRaWAN end-devices. Additionally, an attacker may choose to introduce malicious end-devices into the network ecosystem with random or extreme wakeup time values causing the target's end-device batteries to be expended at a rapid rate (Coman, et al., 2019) (Yang, et al., 2018). This attack can also cause network congestion and increase the wireless transmission footprint, which would make LoRaWAN transmissions easier to triangulate and intercept.

LoRaWAN is one of the few IoT networks using standardized AES-128 cryptographic algorithms, specifically AppKey (Blenn & Fernando, 2017), for end-to-end encryption up to the DoD-SECRET level. This encryption level provides DoD the ability to transmit sensitive data if traditional communication methods become unavailable. Additionally, LoRaWAN's high physical security supports DoD's anti-tampering mission, which makes it an attractive candidate for worldwide deployment.

6. Future Work

LoRaWAN and the Helium Network are two technologies that provide secure end-to-end encryption while also building upon existing IoT communication infrastructure. This current combination limits safe use to domestic infrastructure and non-sensitive operations. In the future, the DoD may explore the possibility of creating its own blockchain for tamper-resistant communications and increased anonymity and control. Additionally, the DoD could research integrations into existing communications infrastructure for human monitoring and critical infrastructure sensing and enhancing MQTT IoT end-devices. Lastly, the DoD could also assist in building both

the Helium Network and its own proprietary blockchain-backed network to further the strengthen its information dominance and establish partnerships with both public and private entities.

To further research DoD adoption of LoRaWAN and blockchain-based technology, it would be beneficial to conduct experimentation on the reliability of communication system as well as the security of both hardware and software components. While this technology has been found favorable amongst civilian users, stressing this system for continual use in various environments is required. As with any wireless communication standard, security concerns for use with sensitive data and operations must be researched and addressed.

7. Conclusion

A unique combination of LoRaWAN and Helium Network technologies could be employed to combat IoT challenges faced by the DoD to enhance its lethality and information dominance. With a properly built IoT ecosystem, the DoD would be able to build upon existing Helium Network technologies to create a new wireless communication standard. This technological fusion provides excellent solutions for emergency management, real-time battlefield information, and critical infrastructure protection and monitoring. With minimal setup and maintenance costs, the DoD could effectively field high-quality, minimally modified devices to provide critical support to warfighters and base populi. The DoD would greatly benefit from and expand on the high potential of LoRaWAN and Helium Network technologies to create smart military bases, save additional lives, and effectively monitor the nation's critical infrastructure at home and abroad.

References

Abdullahi, U. S. et al., 2019. Exploiting IoT and LoRaWAN Technologies for Effective Livestock Monitoring in Nigeria. *Ariz Zone Journal of Engineering, Technology, and Environment,* 15(1), pp. 1-14.

Addabbo, T. et al., 2019. Smart Sensing in Mobility: A LoRaWAN Architecture for Pervasive Environmental Monitoring. *2019 IEEE 5th International Forum on Research and Technology for Society and Industry (RTSI),* pp. 1-6.

Adelantado, F. et al., 2017. Understanding the Limits of LoRaWAN. *IEEE Communications Magazine #55*, pp. 34-40.

Black Hills Information Security, 2022. *Introducting LoRa (Long Range) Wireless Technology - Part 1.* [Online] Available at: https://www.blackhillsinfosec.com/introducing-lora-long-range-wireless-technology-part-1/ [Accessed 22 July 2022].

Blenn, N. & Fernando, K., 2017. LoRaWAN in the Wild: Measurements from the Things Network. *arXiv preprint,* pp. 1-9.

Bluetooth Inc., 2020. *Specification of the Bluetooth System.* s.l.:s.n.

Boccadoro, P., Montaruli, B. & A, G. L., 2019. QuakeSense, a LoRa-Compliant Earthquake Monitoring Open System. *2019 IEEE/ACM 23rd International Symposium on Distributed Simulation & Real Time Applications (DS-RT),* 1(1), pp. 1-8.

Chaudhari, P., Tiwari, A. K., Pattewar, S. & Shelke, S. N., 2021. Smart Infrastructure Monitoring using LoRaWAN Technology. *2021 International Conference on System, Computation, Automation and Networking (ICSCAN),* pp. 1-6.

Coman, F. L., Malarski, K. M., Petersen, M. N. & Ruepp, S., 2019. Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT. *3rd Global IoT Summit,* pp. 1-6.

Conceição, A. F., de Oliveira, L. R., de Moraes, P. & Neto, L. P., 2020. *Review of LoRaWAN Applications.* [Online] Available at: https://arxiv.org/pdf/2004.05871.pdf [Accessed 12 August 2022].

Farrell, S., 2018. Low-Power Wide Area Network (LPWAN) Overview (RFC 8376). *IEEE.*

Fathoni, H., Miao, H.-Y., Chen, C.-Y. & Yang, C.-T., 2020. A Monitoring System of Water Quality Tunghai Lake Using LoRaWAN. *2020 International Conference on Pervasive Artificial Intelligence (ICPAI),* pp. 1-3.

Garcia, F. C. C., Retamar, A. E. & Javier, J. C., 2015. *A Real Time Urban Flood Monitoring System for Metro Manila.* IEEE, s.n.

Haleem, A. et al., 2018. *Helium: A Decentralized Wireless Network.* [Online] Available at: http://whitepaper.helium.com [Accessed 21 July 2022].

IEEE, 2020. *IEEE 802.11- IEEE Standard for Information Technology.* [Online].

Kott, A., Swami, A. & West, B. J., 2016. The Internet of Battle Things. *IEEE Computer,* 49(12), pp. 70-75.

Libelium, 2015. *Libelium Waspmote LoRa 868Mhz-915Mhz SX1272 Networking Guide.* [Online] Available at: http://www.libelium.com/development/waspmote/documentation/waspmote-lora-868mhz-915mhz- sx1272-networking-guide/ [Accessed 21 August 2022].

LoRa Alliance, 2015. *Technical Overview of LoRa & LoRaWAN,* s.l.: s.n.

LoRa Alliance, 2017. White Paper on LoRaWAN Security. *LoRa Alliance,* 1(1), pp. 1-4.

LoRa Alliance, 2019. *Coverage and Operator Maps. https://lora-alliance.org/.* [Online] Available at: https://lora-alliance.org/ [Accessed 31 July 2022].

Michaelis, J. et al., 2019. Leveraging LoRaWAN to Support IoBT in Urban Environments. *IEEE 5th World Forum on Internet of Things (WF-IoT),* pp. 207-212.

Noura, H. et al., 2020. LoRaWAN Security Survey: Issues, Threats and Possible Mitigation Techniques. *IEEE Internet of Things,* Volume 12.

Petajajarvi, J. et al., 2017. Evaluation of lora lpwan technology for indoor remote health and wellbeing. *International Journal of Wireless Information Networks,* 24(2), pp. 153-165.

Raza, U., Kulkarni, P. & Sooriyabandara, M., 2017. Low Power Wide Area Networks: An Overview. *IEEE Communications Surveys Tutorials,* 1(1), pp. 1-19.

Sornin, N. et al., 2015. *LoRa Specification 1.0.* [Online] Available at: www.lora-alliance.org [Accessed 15 July 2022].

Stankovic, J. A., 2014. Research directions for the Internet of Things. *IEEE Internet of Things,* 1(1), pp. 3-9.

Stellin, M., Sabino, S. & Grilo, A., 2020. LoRaWAN Networking in Mobile Scenarios Using a WiFi Mesh of UAV Gateways. *MDPI Electronics Journal,* 9(630), pp. 1-19.

The Associated Press, 2021. *Navy Blames Hawaii Water Contamination on Jet Fuel Spill.* [Online] Available at: https://www.armytimes.com/news/your-military/2021/12/12/navy-blames-hawaii-water-contamination-on- jet-fuel-spill/ [Accessed 7 August 2022].

Tikhvinskiy, V. et al., 2017. Spectrum sharing in 800 MHz band: Experimental estimation of LoRa networks and air traffic control radars co-existence. *International Symposium on Electromagnetic Compatibility - EMC EUROPE,* pp. 1-6.

Yang, X., Karampatzakis, E., Doerr, C. & Kuipers, F., 2018. Security Vulnerabilities in LoRaWAN. *IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI),* pp. 1-13.

ZigBee Alliance, 2015. *ZigBee Specification Document 05-3474-21,* s.l.: s.n.