MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM) | 979-8-3503-2181-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/MILCOM58377.2023.10356300

Covert and Quantum-Safe Tunneling of Multi-Band Military-RF Communication Waveforms Through Non-Cooperative 5G Networks

Elias Alwan, John Volakis, Md Khadimul Islam, Udara De Silva, and Arjuna Madanayake
Dept. Electrical and Computer Engineering
Florida International University
Miami, FL, USA
{ealwan, jvolakis, misla081, udesi001, amadanay}@fiu.edu

Jose Angel Sanchez, George Sklivanitis, and Dimitris A. Pados
Center for Connected Autonomy and AI
Florida Atlantic University
Boca Raton, FL, USA
{josesanchez2019, gsklivanitis, dpados}@fau.edu

Luke Beckwith, Reza Azarderakhsh
PQSecure Technologies LLC
Boca Raton, FL, USA
{luke.beckwith, razarder}@pqsecurity.com

Madhuvanti Muralkrishan, Rishabh Rastogi, Aniruddha Hore, and Eric W. Burger
Commonwealth Cyber Initiative
Virginia Tech
Arlington, VA, USA
{madhuvantim, rrishabh, aniruddah}@vt.edu

***Abstract*—We have built a prototype universal radio adapter which furnishes seamless and secure wireless communication through non-cooperative indigenous 5G networks for military and government users. The adapter consists of a waveform-agnostic hardware add-on that tunnels DoD terrestrial and satellite data. The adapter uses secure protocols for cross-connecting military-grade wireless RF communications equipment using spectrum in the range from UHF to Ka-band. A 5G data transport channel replaces the captured spectrum for transporting information at the IQ-sample level. In a sense, we replace the antenna-air interface and wireless channel with a transparent 5G data network. A plurarity of legacy military systems can operate through modern 5G networks in a seamless way without any knowledge of the characteristics of military waveforms. The adapter incorporates AI/ML based methods for smart spectrum sensing and autonomous radio reconfiguration. This enables intelligent interconnection of a number of military radios through non-cooperative (potentially adversarial) 5G commercial cellular networks. The adapter is built on four technical pillars: 1) ultra-wideband apertures for multi-functional and flexible software-defined radios (SDRs) with agile, wideband, and dual-band tunable RF transceivers for FR1/FR2 bands; 2) physical layer operation that involve device authentication via deep-learning based RF fingerprinting and compression of acquired IQ data; 3) secure and reconfigurable cryptographic co-processors employing the new quantum-safe algorithms selected by NIST to achieve authentication, key exchange, and encryption with focus on resource-constrained low size, weight, power, and cost (SWaP-C) devices; and 4) generative artificial intelligence and spread-spectrum steganography to hide DoD traffic passed through 5G networks and improve resiliency against real-time traffic analysis by nation-state carriers and intelligence agencies.**

***Index Terms*—5G, security, data hiding, steganography, PQC, IQ signal compression, AI fingerprinting**

I. Introduction

United States DoD personnel and assets deployed in multi-domain environments have maintained maximum operational superiority and warfighting advantages in recent times. Today, the rapidly evolving and expanding technical areas of 5G wireless communication technologies present themselves as inescapable game changers and promise orders of magnitude improvements in multiple areas of operation spanning U.S., allied, and contested regions. The military makes extensive use of spectrum, starting from as low as 3 MHz, through HF, VHF, UHF and X-band, going all the way to mm-wave bands in the tens of GHz. These applications necessitate the integration of transceiver technology of various sizes and bandwidths, as well as the use of unique frequencies and bandwidths. For instance, military satellite communications have typically focused on the C-band (uplink 5.8-6.7 GHz and downlink 3.4 to 4.2 GHz) and X-band (uplink 7.9-8.4GHz and downlink 7.25-7.75 GHz) operations. However, over the years, demand for bandwidth has risen, owing in part to the ongoing development in intelligence needs and the expansion of the use of unmanned aerial systems (UAS). As a result, systems operating at higher frequencies, such as the Ku-band and Ka-band, are increasingly being used.

In particular, the Ka-band (uplink 27.5 to 31 GHz and downlink 18.3 to 18.8 GHz) is being considered for military satellite communications in particular since the frequency band provides a variety of advantages, such as: 1) increased upload and download data transfer speeds, 2) more efficiency in spectral operations, and 3) reduced congestion in the radio

Fig. 1. Communications, EW, and sensing through 5G use cases enabled by wired/wireless versions of ASTRALinQ in U.S., allied, and contested spectrum regions.

This research is supported through the NSF Convergence Accelerator Track G award ITE-2226392.

frequency spectrum band. Military surveillance and reconnaissance systems and signal processing can greatly benefit from the increased speed, reduced latency, and improved reliability of data transfer and transmission that 5G offers. These characteristics will open the door to new command and control applications and streamline logistics. Other examples include augmented and virtual reality (AR/VR), 5G smart warehousing, distributed command and control, and dynamic spectrum utilization. 5G will be able to accomplish all of this by operating on three segments of the electromagnetic spectrum: Among the frequencies used are: 1) low band, which operates at frequencies < 1 GHz; 2) mid band (1-6 GHz); and 3) high band, also known as millimeter-wave (24-300 GHz).

In general, 5G is expected to revolutionize capabilities by enabling a data-connected military. That involves connecting soldiers, vehicles, command posts, ships, satellites, and planes with voice, data, imaging, and signals intelligence. Local and expeditionary 5G networks will be used to connect distant sensors and weaponry. The massive data transfer will assist commanders comprehend, shape, and adapt to disputed settings. Data-rich environments will power and strength algorithms that assist commanders. Because of the benefits of 5G, unmanned and autonomous weapons systems will be enabled by low-latency communications. Warfighters will have more tactical intelligence, allowing even small forces to make a huge impact.

The ubiquity of 5G in urban and suburban environments and the integration of non-terrestrial networks (NTN) in 5G standards present opportunities for the U.S. DoD. Specifically, there is strong interest, and almost a necessity, to leverage existing and future 5G infrastructure for a wide variety of use cases relating to the warfighter, including signals intelligence (SIGINT), cyber, electronic warfare (EW), and communications across contested regions [1]. Public 5G networks can provide an alternative -not necessarily trusted- communication pathway for government operations in contested and otherwise spectral-limited environments. Private 5G networks, open 5G systems, and open radio access networks (O-RANs) can potentially be tailored to meet DoD requirements [2]. However, O-RANs will result in vendor-neutral hardware deployment, increasing security risks. Therefore, securing the operation of DoD devices when transmitting through private and public 5G networks can be a highly cost-effective way to support mission-critical operations while maintaining the integrity of critical infrastructure. The ensuing challenge is that commercially available 5G-capable devices do not implement military standard (MIL-STD) certifications for secure and reliable communications. Also, legacy MIL-STD-certified devices and tactical radios are not interoperable with the 5G RAN/core, as these radios were designed for different frequency bands and communication protocols.

In this paper, we present our recent innovation, ASTRALinQ, which is a device and protocol-agnostic adapter that can acquire any waveform operating at any frequency from UHF to Ka bands and transform it (through acquisition and compression of IQ data) into a 5G compatible waveform. As a result, ASTRALinQ enables any military wireless device operating at any frequency and using any waveform with any security classification to be transparently, covertly, and securely transferred to a remote site via non-cooperative and likely adversarial 5G data transport network. ASTRALinQ allows use of available wireless communications technologies having highly stable and time-tested security protocols and spectral allocations to be used at any location worldwide that has public 5G networks. One mode of operation (as depicted in Fig. 1) improves stealth capability for covert operations as no RF energy is emitted in spectral bands that an adversary will be monitoring. Further, the use of commercial 5G networks as a spectrum transfer pipe allows us to double dip on civil use spectrum allocated by the adversary for non-military use for secure military communications without them finding out about it. This sneaky approach exploits the low-latency and high-capacity offered by 5G networks operating at very specific bands for pushing through classic military waveforms. We achieve this because fundamentally, classic military systems are relatively narrowband but highly-secure in terms of hard cryptography. Our adapter does not break the security level the original military standard specifies as there is no demodulation or decryption involved in our approach. Rather, we transport the secure RF waveforms at baseband IQ-sample level through commercial 5G pipes.

II. Enabling Technology in ASTRALinQ: Replacing RF Channels with 5G Channels

The key enabling idea behind ASTRALinQ is that it offers a transparent pipe between two military wireless systems regardless of spectrum allocations, waveforms, or security classifications by replacing an RF based wireless channel with a 5G network based secure data transport network. In one mode, the signals from a military communications device intended to go to a transmit antenna are diverted to the ASTRALinQ receiver and packetizer. ASTRALinQ then sends the IQ data through the 5G network to a similar adapter at a different location where the packets are reassembled to the original RF waveform and sent to the corresponding military communication device. As far as the military communication system is concerned, nothing has changed as it still continues to transmit and receive RF signals in its allocated spectrum. ASTRALinQ replaces the military wireless RF link with a 5G packet transport pipe through what is conceptually a quantum-safe virtual private network (VPN). We use AI-assisted fingerprinting to authenticate devices that connect to ASTRALinQ and compress acquired IQ samples to reduce the amount of data to be transported through 5G. We use post-quantum cryptography to ensure the forward security of the communications as quantum computers become practical for code breaking. The adapters also use concepts of reverse traffic analysis and steganography to ensure the packets that tunneled through the 5G network are not spotted by traffic monitoring algorithms operated by adversaries.

III. ASTRALinQ SWaP-C Transceiver Hardware

ASTRALinQ reconfigures itself autonomously and intelligently adapts to any military band or protocol. It encrypts, packetizes, and routes the sampled RF data to a selected 5G network. Flexibility in hardware and software is paramount to accommodate different mission requirements (data rates, bandwidth, and security). AI/ML algorithms bring adaptive switching among 5G bands to ensure jamming-free communications to the network core. ASTRALinQ is a low size, weight, power, and cost (SWaP-C) device about the size of a commercial smartphone (i.e., portable). Power consumption is crucial as ASTRALinQ will be mobile and intended to be used in dangerous missions. As shown in Fig. 2, the hardware will be implemented using commercially available integrated circuits (ICs) chips, ensuring low cost and power consumption.

ASTRALinQ will comprise multiple modules for multiband operation. An overview of the RF front-end is shown in Fig. 3. To reduce hardware requirements, RF modules share a wideband antenna, an intermediate frequency (IF) module operating at lower frequencies (*viz.* UHF-S bands), and a digital baseband unit.

A. DoD Compatible Front End

Fig. 3 illustrates a dual-band tunable RF front-end that can process any military/DoD waveform in the UHF to Ka-bands. Each module is designed and implemented separately to operate across a particular frequency range. A reconfigurable RF front end capable of handling signals from all other modules will be relatively straightforward to implement. A tunable band-select filter for each RF front-tend separates all frequency bands. Each band is isolated and fed into a dedicated RF transceiver chain enabling low noise reception. Since a single wideband antenna will be used for transmission and reception in full-duplex mode for each band, a high isolation duplexer will be placed to separate the receive and transmit signals. Hence, signals received (or transmitted) at < 18 GHz will be handled via low-band reconfigurable RF front end. The latter is a homodyne architecture that down-converts these signals to baseband for post-processing using the shared IF module. A heterodyne architecture will be adopted for the higher frequency signals (18-40 GHz). The signal will first undergo a stage of amplification, filtering, and down-conversion at their respective RF modules. Mixing is done using tunable low-frequency local oscillators (LOs) operating from 2-10 GHz. AI/ML control algorithms for tuning will be programmed into a microcontroller and handled by the digital module. For the millimeter-wave (mmWave) signals, frequency multipliers will be employed to translate the LO frequency to these higher bands. The up-converted signals are then pushed to the power amplifier (PA).

B. Multiband AI-assisted 5G Compatible Front-End

The 5G front-end aims to switch adaptively among different bands based on smart network sensing. This front end will be designed separately and integrated with the adapter, as depicted in Fig. 3. To enable a dynamic system with multiband capabilities, AI/ML techniques with smart-decision schemes will be incorporated into our proposed architecture to intelligently predict the state of the spectrum of interest and estimate the parameters, including center frequency, modulation, and waveform type, and transmission power, to reconfigure the proposed transceiver. The IF signals at the output of the chips will then be fed to a switch that connects to a shared IF /baseband hardware before digitization. We will use three commercially available transceiver chips to cover FR1 (sub-6 GHz) and FR2 (K and Ka bands) of the 5G bands. A digitally controlled frequency multiplexer/ demultiplexer will be implemented first to separate the frequency bands. As such, each frequency band is isolated and fed into a dedicated RF transceiver chip. The 5G interface will comply with international 5G standards and be fully licensed to operate on civilian bands (e.g., ATT/ Verizon/ T-Mobile commercial networks). Also, the 5G connection will interface with the adapter using standard protocols (e.g., TCP/IP over 100 Mbps Ethernet).

C. Wideband Reconfigurable Antenna

The military and 5G front ends share an extremely wideband antenna operating from UHF up to 40 GHz. We adopt an

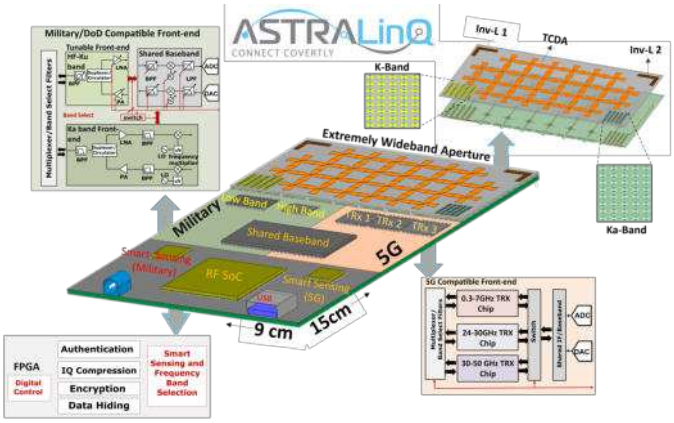

Fig. 2. A 3D rendering of ASTRALinQ including hardware and software IP.

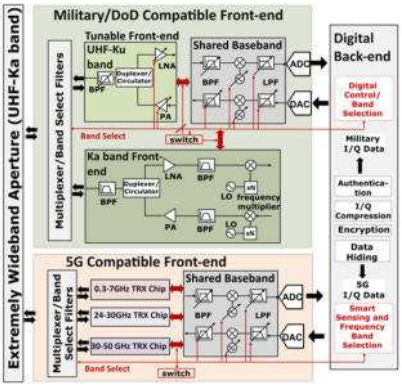

Fig. 3. Schematic of ASTRALinQ's military front-end, 5G front-end, and digital back-end.

embedded antenna system to achieve this wideband operation [13], [14]. Five antennas are co-integrated into a total surface area of 5 cm $\times$ 9 cm: two low-band inverted L antennas operating from 650 MHz to 1.6 GHz and 1.6 GHz to 4 GHz will be placed at the two outer corners of the board.

An RF front-end, operating in the C-band (uplink and downlink) was developed, as a proof of concept, at a TRL 2 (Fig. 4). The experimental setup using two software-defined radios (SDRs) emulating the DoD device and other commercial components was tested for data transmission using BPSK, QPSK, and 64-QAM modulations. Using the first SDR, an encrypted image was transmitted at 3.7 GHz. The received signal was then down-converted to 700 MHz for

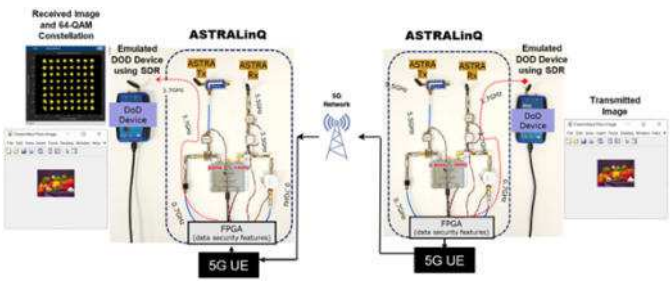

Fig. 4. A benchtop prototype of ASTRALinQ for C-Band operation.

digital processing on FPGA, where security features were added. Subsequently, the secure digital signal was upconverted to 5.5 GHz before transmission to a commercial 5G network. This signal was received using a second SDR, and the data was recovered without errors.

IV. ASTRALinQ Physical Layer Operations

A. Radio Frequency Fingerprinting

We leverage deep neural networks to facilitate radio frequency fingerprinting which aims to identify a device that connects to ASTRALinQ from the originated radio transmission IQ signal. We extract specific features from the transmission generated by the transmit hardware while mitigating the distortions caused by channel effects.

Our device fingerprinting framework is systematically divided into three stages: training, enrollment, and authentication. The initial phase involves training a deep neural network to extract features from channel-independent spectrograms captured from different wireless devices. These spectrograms are obtained after applying a short-time Fourier transform revealing the time-frequency characteristics of a signal. To mitigate channel effects on signals, adjacent columns are divided [12]. We collect multiple packets containing IQ from multiple software-radio devices in a controlled environment to create a diverse dataset for training a convolutional neural network (CNN). The CNN is designed with reference to a ResNet architecture which has been adopted previously for feature extraction. We employ triplet loss during training which aims at minimizing the distance between packets belonging to the same device and maximizing the distance between packets from different devices. The second stage uses the trained neural network for extracting features from legitimate devices to create a database with their radio frequency fingerprints. These RF fingerprints are used for training supervised learning algorithms for device authentication and identification. These include one-class support vector machines (SVM) and K-nearest neighbor (K-NN) for authentication and identification respectively. Authentication is performed by first extracting features from an incoming signal acquired by a legitimate or rogue device using the pre-trained CNN. Then, the one-class SVM algorithm checks whether the extracted features fit into one of the legitimate devices' clusters. We use K-NN to ID the authenticated device by selecting the K nearest neighbors from the legitimate device database.

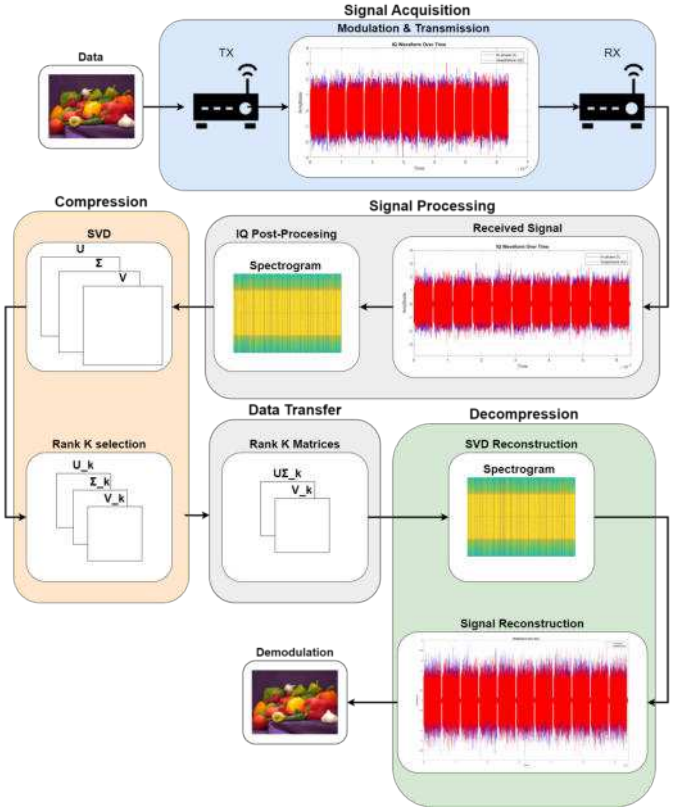

Fig. 5. IQ Compression system diagram.

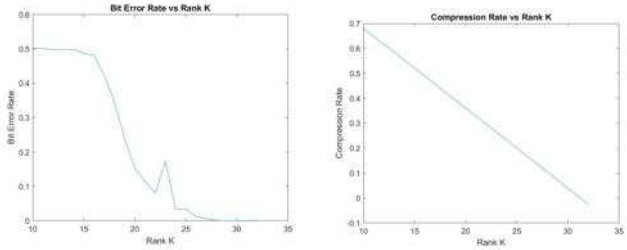

Fig. 6. BER and compression ratio vs. rank-K SVD selection considering 16 QAM OFDM over-the-air transmissions.

B. IQ Compression

In the context of transferring through 5G unprocessed IQ data from the acquired signal, it becomes essential to devise strategies that minimize the volume of stored and re-transmitted data to meet the constraints of storage and data rates within our system. We harness lossy compression methods for representing the originally received information in fewer bits. Our chosen method for accomplishing IQ compression is Singular Value Decomposition (SVD). In order to perform SVD we post-process our data by applying short time Fourier transform (STFT) to the acquired IQ samples. The STFT allows us to represent the IQ data as a decomposable matrix that also enables us to recover the IQ data by applying inverse STFT (ISTFT). This method allows for the efficient decomposition of the received signal, facilitating the selection of the rank that yields the most advantageous compression ratio while ensuring a minimum level of error. Consequently, this approach enables us to transmit information at higher data rates and economize memory consumption when processing IQ data. The end-to-end IQ compression/decompression procedure is shown in Fig. 5. Figure 6 shows bit error rate and compression rate results versus the rank K of SVD considering acquisition of IQ data correspnding to 16-QAM OFDM modulated image data. We observe that depending the desired quality of service (< 0.1) there is almost 35% compression that can be achieved compared to the original IQ data.

V. ASTRALinQ Quantum-Safe Cryptography

Current cryptographic standards, such as RSA and ECC, rely on hard problems which are difficult to solve on classical computers, but become trivial to solve using a large-scale quantum computer to run Shor's algorithm [4]. These legacy cryptographic algorithms provide the basis of secure communications, with key exchange algorithms allowing two parties to safely establish an encryption key and digital signatures

allowing verification of message integrity and authenticity. While there are currently not quantum computers large enough to break the current cryptographic standards, future systems will need to be protected against these attacks and current systems are still vulnerable to "Harvest now, decrypt later" attacks where current traffic is stored for future decryption. Fortunately, there are alternative cryptographic algorithms which are believed to be resistant to both classical and quantum computing attacks. NIST has been evaluating quantum-safe cryptographic algorithms since 2016 and recently announced the first set of these algorithms to be standardized [6]: CRYSTALS-Kyber for key exchange, and CRYSTALS-Dilithium, FALCON, and SPHINCS$^+$ for digital signatures. SPHINCS$^+$ is a hash based algorithm, the other selected algorithms are all based upon the difficulty of lattice problem.

While all four these algorithms will be standardized, only CRYSTALS-Kyber and CRYSTALS-Dilithium are recommended for use by the NSA [3]. Per their recommendations, traditional networking equipment is expected to support these new standards as the preferred algorithms by 2026, and to exclusively use them by 2030 [3]. Thus, all future devices must be built with support for these algorithms.

Implementations of the algorithms must be protected against all relevant side-channel attacks. If not carefully protected, devices may leak information about the secret key during their operation. This may occur through timing side-channels, where the latency of the operations depends on the value of the secret, or through physical leakage such as power consumption. Different operations and differences in input data effect the power consumed by the device and statistical analysis of these differences can allow the secret key to be recovered. If an adversary has physical access to the devices, they can measure the power consumption and perform Simple Power Analysis (SPA) or Differential Power Analysis (DPA) attacks to recover the secret key used by the device. There have already been several successful side-channel attacks against CRYSTALS-Kyber and CRYSTALS-Dilithium [7], and attacks against classical algorithms such as AES and SHA are well known.

Fortunately, there are several well-studied countermeasures to secure implementations against these attacks. Timing attacks can be protected against by ensuring all operations related to the secret key are performed in constant time. Power analysis attacks can be protected against using masking where sensitive data is split into shares using a random value. This breaks the correlation between the power consumption and the sensitive data. Another common countermeasures is shuffling, where the order of operations is randomized each time the algorithm is performed. Implemented countermeasures can be verified by analyzing the latency of the design for changes in timing and by using the Test vector Leakage Assessment (TVLA) test [8]. The TVLA test is a statistical method of analyzing power traces to ensure that there is no observable difference between a constant input and a random input.

ASTRALinQ is equipped with a side-channel protected cryptographic hardware module which implements AES, SHA-3, CRYSTALS-Kyber, and CRYSTALS-Dilithium. The countermeasures were verified using timing analysis and TVLA as previously described. For example, the TVLA results for AES are shown in Figure 7. The CRYSTALS-Kyber and CRYSTALS-Dilithium accelerators enable compatibility with future 5G security standards which will require support for quantum-safe encryption as well support for quantum-safe

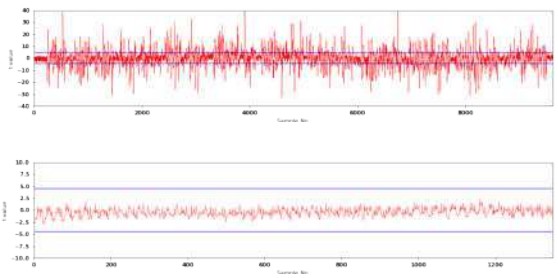

Fig. 7. Example TVLA results for AES-256 hardware implementation. Upper: Failing TVLA for unprotected AES. Lower: Passing TVLA for protected AES.

communication between ASTRALinQ devices. The architecture of the post-quantum hardware modules is discussed in a previous work [5]. SHA-3 is used by the CRYSTALS algorithms hardware modules but also enables support for protocols which hash the message before signing. The AES module provides high throughput encryption for the compressed IQ samples. All the hardware modules are protected against timing attacks through constant time implementation as well first-order power analysis attacks using domain oriented masking (DOM).

VI. ASTRALinQ Data Hiding in Plain Sight

We reduce the likelihood of interception, disruption, or jamming of ASTRALinQ communications over 5G networks using censorship- and detection-resistant applications with traffic patterns that are indistinguishable from local human users. Encryption protects a 5G network when operated by a trusted network operator. ASTRALinQ has strict requirements as it operates through 5G networks. Because ASTRALinQ traffic originates from DOD, it is likely to trigger attention by adversaries. Flagging could target the ASTRALinQ communication for cyber attacks or censorship. Obfuscation of communications through untrustworthy 5G networks is absolutely necessary to prevent espionage or cyber-attacks that may follow when an adversary detects the transport of sensitive information. Thus, we must ensure our communications do not resemble military communications.

ASTRALinQ implements the proven steganographic and network traffic analysis signature-defeating methods developed by DARPA RACECAR, specifically the Raven generative AI traffic dispersion and diffusion approach. [10] This approach embeds the IQ waveform data in popular 5G applications. In our first implementation of ASTRALinQ, we use Gmail as a transport substrate.

Note that it is not sufficient to package captured IQ data as an email. If the email traffic has temporal characteristics of military communications, then a sophisticated adversary can pick out that 'signal' of when and how large the emails are to identify at best that the communication is of interest and at worst identify it as military communications. We defeat this network traffic analysis by using generative AI to create a transmission schedule that appears to be a normal user using a smartphone to send and receive normal emails (Figure 8. When there is no IQ data to transmit, ASTRALinQ will transmit data to mimic real users' behavior. When there is IQ data to transmit, ASTRALinQ will wait for the next scheduled transmission time to send the data. If there is more data than the generated pattern allows, ASTRALinQ waits for a further scheduled transmission to complete the sending.

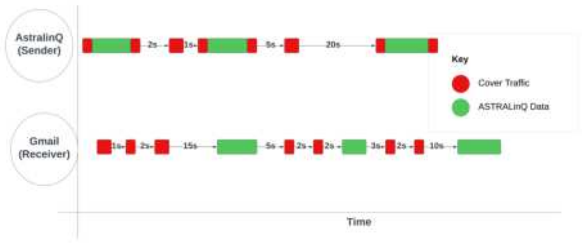

Fig. 8. Email sending schedule.

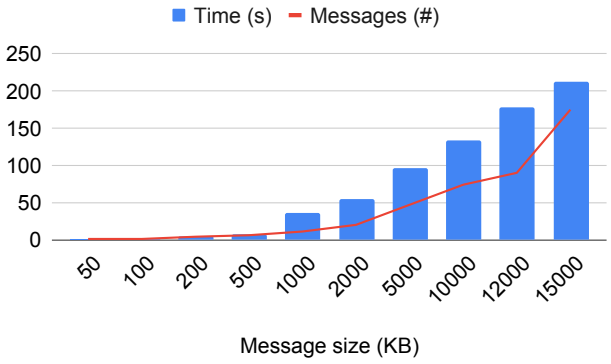

Fig. 9. Email transport latency.

Simulations of Raven encoding demonstrated the ability to hide covert communications by closing matching genuine traffic and by imposing a significant cost in false positives. A pre-Raven approach, Mailet, [9] can be detected for Twitter traffic with total recall with a false positive rate of only 3%. Raven at total recall produces a false positive rate of 50%, making detection computationally infeasible for an adversary, even if the adversary has total network monitoring, as is the case in many foreign countries of interest.

ASTRALinQ enhanced Raven's obfuscation of low-bit-rate messages. The innovation for our Phase 1 deliverable was on the SWaP-C side: RACECAR assumed a high end computer with GPU acceleration for computing the schedule and a capable PC as the client. We implemented the client in one-half the cores of a Raspberry Pi 4, the target architecture and compute resources of the ASTRALinQ FPGA. We measured the performance of the transport system using Gmail and were able to establish latency bounds for ASTRALinQ spectrum transport for messaging applications. Small file transfer (e.g., Link16 command message) may suffer only a few hundred milliseconds of latency. As Fig. 8 notes, opportunities exist to send small messages. Large file transfers, such as a broadband spectrum transfer for a large still image, can suffer longer latencies. Fig. 9 shows the latency we measure during Phase 1 for sending large files through our obfuscator. We have shown that Gmail works as a transport mechanism for relatively short, latency-insensitive military applications.

Does this mean that ASTRALinQ is limited to only short messaging applications? Not at all. The architecture allows for pluggable transports of generative AI-based traffic based on popular applications. Future work includes porting the scheduler to popular interactive streaming media applications, such as Zoom, Teams, Skype. We also address operational issues. For example, the Parrot problem [11] demonstrated that emulations of end user protocols often have detectable signatures. As such, we will look to novel eSIM implementations as well as using actual, in-theatre acquired devices for the 5G interface. Finally, we will explore ASTRALinQ's capability for inter-local device communication to establish multi-path transport to add another layer of obfuscation to our transmissions.

VII. Conclusions

ASTRALinQ provides a "secure bridge" for DoD devices over 5G and leverages zero-trust principles by: 1) authenticating DoD devices connected to ASTRALinQ (source and destination) via artificial intelligence (AI) assisted RF fingerprinting; 2) real-time post-quantum encryption of the digitized IQ of the wireless DoD signal without decoding/accessing data; and 3) disguising the ASTRALinQ packet traffic by data embedding and matching traffic patterns of popular 5G applications.

Acknowledgments

This work was funded by a Joint NSF/DOD Convergence Accelerator Track G Phase-I grant, ITE-2226392. The authors would like to thank our DOD partners and industry contacts who helped shape ASTRALinQ into a viable product that will meet DOD mission needs.

References

[1] Cross-functional Team, "Summary of the Joint All-Domain Command and Control (JADC2) Strategy," Department of Defense, 2022.
[2] USD(R&E), "DoD and the National Telecommunications and Information Administration Luanch 2023 5G Challenge for Open RAN with an Eye Toward Future Base Modernization," 2023.
[3] NSA, "Cybersecurity Advisory Announcing the Commercial National Security Algorithm Suite 2.0," Sep. 07, 2022.
[4] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM J. Comput., vol. 26, no. 5, Oct. 1997.
[5] L. Beckwith, A. Abdulgadir, and R. Azarderakhsh, "A Flexible Shared Hardware Accelerator for NIST-Recommend Algorithms CRYSTALS-Kyber and CRYSTALS-Dilithium with SCA Protection," Topics in Cryptology – CT-RSA 2023. Lecture Notes in Computer Science, vol 13871.
[6] D. Moody, "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 8413, 2022.
[7] P. Ravi, A. Chattopadhyay, J. P. D'Anvers, and A. Baksi, "Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results".
[8] G. Goodwill, B. Jun, J. Jaffe, and P. Rohatgi, "A testing methodology for side channel resistance validation".
[9] S. Li and N. Hopper, "Mailet: Instant Social Networking under Censorship", Proceedings on Privacy Enhancing Technologies (PoPETs), 2016(2).
[10] R. Wails, A. Stange, E. Troper, A. Caliskan, R. Dingledine, R. Jansen, and M. Sherr,"Learning to Behave: Improving Covert Channel Security with Behavior-Based Designs", Proceedings on Privacy Enhancing Technologies (PoPETs), 2022(3).
[11] A. Houmansadr, C. Brubaker, and V. Shmatikov, "The Parrot Is Dead: Observing Unobservable Network Communications", 2013 IEEE Symposium on Security and Privacy (SP 2013).
[12] G. Shen, J. Zhang, A. Marshall and J. R. Cavallaro, "Towards Scalable and Channel-Robust Radio Frequency Fingerprint Identification for LoRa," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 774-787, 2022.
[13] R. Govindarajulu, R. Hokayem, and E. Alwan, "Dual-Band Antenna Array for 5.9 GHz DSRC and 28 GHz 5G Vehicle to Vehicle communication," in 2020 IEEE International Symposium on Antennas and Propagation and North American Radio Science Meeting, pp. 1583-1584, 2020.
[14] R. Govindarajulu, R. Hokayem, Md. Tarek, M. Guerra, and E. Alwan, "Low Profile Dual-Band Shared Aperture Array for Vehicle-to-Vehicle Communication," IEEE Access, vol. 9, pp. 147082-147090, 2021.