Fast-Fourier Transform in 5G Network*

Davit Begashvili[1,*,†], Giorgi Akhalaia[2,†], Avtandil Gagnidze[3,†] *and* Sergiy *Gnatyuk*[4,†]

[1] *Kutaisi International University*
[2] *Caucasus University, Caucasus School of Technology*
[3] *East-west teaching university*
[4] *National Aviation University*

Abstract

The advent of 5G technology has ushered in a new era of high-speed wireless communication, bringing unprecedented connectivity and capabilities. However, the inherent vulnerabilities of 5G networks pose significant cybersecurity challenges that demand innovative solutions. This research explores the utilization of Fast Fourier Transform (FFT) as a foundational element in addressing cybersecurity concerns within the 5G paradigm. The paper begins with an overview of 5G technology and its pivotal role in contemporary communication systems. Emphasis is placed on the evolving security landscape, highlighting the distinctive threats posed to 5G networks. Against this backdrop, the research establishes its primary objective: to investigate the application of FFT techniques in fortifying the security infrastructure of 5G networks. A comprehensive literature review examines existing research in both 5G security and signal processing, identifying gaps that underscore the need for advanced security mechanisms. The theoretical framework elucidates the role of FFT in the modulation/demodulation process, channel estimation, and signal processing within the 5G context. This theoretical foundation serves as the basis for proposing innovative FFT-based security mechanisms. The paper delves into specific cybersecurity threats faced by 5G networks, presenting FFT as a viable solution to mitigate these threats. Intrusion detection, anomaly detection, and enhanced encryption and decryption processes are explored as key applications of FFT in bolstering cybersecurity measures.

To validate the effectiveness of the proposed FFT-based solutions, the research outlines an experimental setup, including simulations or case studies conducted in realistic scenarios. Results and analysis are presented, comparing the efficacy of FFT-based security mechanisms with existing solutions, and interpreting findings in the context of the research objectives. In conclusion, this research contributes to the evolving field of 5G cybersecurity by showcasing the potential of FFT as a strategic tool for addressing vulnerabilities and fortifying network defences. The findings open avenues for further research, offering insights into the integration of signal processing techniques in the pursuit of resilient and secure 5G communication networks.

Keywords

FFT, 5G Network, Radio-waves, Cyber Security, Mobile Communication

1. Introduction

The fifth generation of wireless technology, commonly referred to as 5G, heralds a new era of connectivity that promises to revolutionize how we communicate, interact, and experience the world around us. With its unprecedented speed, ultra-low latency, and massive connectivity capabilities, 5G stands poised to transform not only the telecommunications industry but also various sectors of society, including healthcare, transportation, manufacturing, and entertainment. But before we start digging about 5G deeper let's review predecessors. 1G refers to the first generation of cellular network (wireless) technology.[1] These are mobile telecommunications standards that were introduced in the 1980s and were superseded by 2G. The main difference between these two mobile cellular generations is that the audio transmissions of 1G networks were analog, while 2G networks were entirely digital. In early 2000s third generation of wireless mobile telecommunication technology 3G was offered with faster data transfer, and better voice quality.

*IVUS2024: Information Society and University Studies 2024, May 17, Kaunas, Lithuania
[1,*] Corresponding author
[†] These author contributed equally.
d.begashvili@yahoo.com (D. Begashvili); gakhalaia@cu.edu.ge (G. Akhalaia); gagnidzeavto@yahoo.com (A. Gagnidze); s.gnatyuk@nau.edu.ua (S. Gnatyuk)
0000-0002-4194-2681 (G. Akhalaia)

Last but not least, 4G LTE ushered in the era of mobile broadband. 4G networks offered faster data download and upload speeds compared to 3G. Reduced latency, resulting in more responsive user experiences.
Enhanced network capacity allowing more simultaneous connections. Use of MIMO (Multiple Input Multiple Output) and beamforming for better signal quality and improved spectral efficiency. Unlike its predecessors, 5G is not merely an incremental upgrade but represents a fundamental leap forward in wireless communication technology. Building upon the foundations laid by 4G LTE networks, 5G networks leverage advanced technologies.

Innovating upon existing protocols, my approach introduces a sophisticated three-way handshake mechanism between the client, RF radar, and server. This strategic addition aims at fortifying the defense against potential man-in-the-middle (MITM) attacks, a prevalent concern in contemporary digital communication landscapes. Moreover, to bolster security measures further, an additional stratum of encryption is proposed during the implementation of the Fast Fourier Transform (FFT).[2] This involves integrating a matrix multiplication process with an extra constant, a proactive measure aimed at elevating the security quotient. Notably, the transmission of this augmented security parameter is encrypted within the handshake process, ensuring robust protection throughout the communication exchange. This multi-layered approach signifies a significant stride towards enhancing the integrity and confidentiality of data transmissions within RF radar systems.[3]

2. Literature overview

This presents ideas that have been thoroughly researched and developed, drawing on the latest scientific literature, technical documents. Furthermore, my main friand was AI which helped me to develop this idea and to give more thoughts about the security aspects of the 5G. Mathematical part for this approach is still to be done to measure the complexity and the cost of the operations. Implementing extra layer of encryption to 5G ideally and theoretically is more secure.

3. How is 5G better than 4G

There are several reasons that 5G will be better than 4G: 5G is significantly faster than 4G, has more capacity, has significantly lower latency, is a unified platform that is more capable, uses spectrum better.[3] It's even better visible in numbers:

Speed and Bandwidth:

- 4G: Fourth-generation networks typically offer peak download speeds of up to 100 Mbps, with some advanced variants reaching up to 1 Gbps under optimal conditions.
- 5G: Fifth-generation networks boast substantially higher speeds, with peak download speeds exceeding 10 Gbps. This dramatic increase in bandwidth enables ultra-high-definition video streaming, immersive gaming, and other data-intensive applications with minimal latency.

Latency:

- 4G: 4G networks typically exhibit latency ranging from 30 to 50 milliseconds, which, while relatively low, may still be noticeable in real-time applications such as online gaming and video conferencing.
- 5G: 5G networks drastically reduce latency, with estimates ranging from 1 to 10 milliseconds. This near-real-time responsiveness is critical for applications like autonomous vehicles, remote surgery, and augmented reality, where split-second decisions are paramount.

Connectivity and Capacity:

- 4G: Fourth-generation networks support a limited number of simultaneous connections per square kilometer, which can lead to congestion in densely populated areas or during large-scale events.
- 5G: Fifth-generation networks are designed to accommodate a vastly greater number of connected devices, thanks to technologies like massive MIMO and beamforming. This enhanced connectivity enables the Internet of Things (IoT), smart cities, and other scenarios with a high density of connected devices.

Spectrum and Infrastructure:

- 4G: Fourth-generation networks primarily operate within sub-6 GHz frequency bands, utilizing existing infrastructure such as cell towers and base stations.
- 5G: Fifth-generation networks leverage a broader spectrum, including millimeter wave frequencies (mmWave), to achieve higher data rates and lower latency. However, mmWave signals have shorter propagation distances and are susceptible to interference, necessitating the deployment of additional infrastructure like small cells. [4]

4. 5G threat landscape

Increased Attack Surface: With the proliferation of connected devices and the expansion of the Internet of Things (IoT), 5G networks significantly increase the attack surface. More devices connected to the network mean more potential entry points for attackers.
Distributed Architecture: 5G networks utilize a distributed architecture with virtualized network functions, which introduces new vulnerabilities and potential points of attack compared to traditional centralized architectures.
Network Slicing Vulnerabilities: Network slicing, a key feature of 5G, allows operators to create multiple virtual networks on a single physical infrastructure to meet different service requirements. However, vulnerabilities in the implementation of network slicing could lead to unauthorized access or disruption of services.[7]
Edge Computing Risks: 5G enables edge computing, which brings computational resources closer to the end-users. While edge computing offers benefits such as reduced latency, it also introduces security risks, including data breaches and unauthorized access to edge devices.
Authentication and Identity Management: Secure authentication and identity management become more challenging in 5G networks due to the dynamic nature of network elements and the increased use of virtualized infrastructure. Weak authentication mechanisms could lead to identity theft and unauthorized access.
Privacy Concerns: 5G networks transmit vast amounts of data, including sensitive personal and business information. Privacy concerns arise from the potential interception or unauthorized access to this data, leading to breaches of confidentiality and privacy regulations.
Supply Chain Risks: The global nature of 5G supply chains introduces risks related to the integrity of hardware and software components. Malicious actors could exploit vulnerabilities in supply chains to compromise the security of 5G networks.[8]
Nation-State Threats: There are concerns about nation-state actors leveraging 5G technology for espionage, sabotage, or cyber warfare purposes. The deployment of 5G infrastructure by foreign vendors raises questions about the security of critical communications infrastructure. [10]

5. How 5G works

5G transmission consists of 3 main part time domain, frequency domain, radio frequency signals. Let's now discuss all of them and see where extra layer of encryption can be added.
In 5G communication, the time domain refers to the representation of signals in terms of their variations over time. In wireless communication systems like 5G, information is transmitted using electromagnetic waves, which can be characterized by various parameters such as frequency, amplitude, and phase. Time domain specifically relates to the time-varying behavior of these electromagnetic waves. The Fast Fourier Transform (FFT) is a mathematical algorithm used to transform a signal from the time domain to the frequency domain. FFT plays a crucial role in modulation and demodulation processes. Here's how FFT is used to transfer data from the time domain to the frequency domain in 5G networks:

- Digital Modulation: In 5G and other wireless communication systems, data is typically transmitted in the form of digital symbols. These symbols are represented by variations in the amplitude, phase, or frequency of a carrier signal. Before transmission, the digital data is modulated onto the carrier signal using modulation techniques such as Quadrature Amplitude Modulation (QAM) or Phase Shift Keying (PSK).[5]
- Conversion to Analog Signal: The modulated digital signal represents variations in the time domain, where the amplitude of the signal changes over time according to the modulating data. This signal needs to be converted into an analog signal suitable for transmission over the air.
- FFT Processing: The modulated digital signal is segmented into small time-domain intervals known as time windows or frames. Each frame typically contains a finite number of digital samples. The FFT algorithm is then applied to each frame to convert the signal from the time domain to the frequency domain.
- Frequency Domain Representation: The output of the FFT operation is a set of complex numbers representing the signal's frequency components. Each complex number corresponds to a specific frequency bin in the frequency spectrum. The magnitude and phase of these complex numbers indicate the amplitude and phase of the signal at each frequency. [6]
- Transmission: The frequency-domain representation of the signal is transmitted over the communication channel. In wireless communication systems like 5G, the signal may undergo further processing, such as channel encoding, modulation, and multiple access techniques, before transmission.
- Reception and Demodulation: At the receiver side, the transmitted signal is received and processed to extract the frequency-domain representation. The Inverse FFT (IFFT), which is essentially the reverse operation of the FFT, is applied to convert the signal from the frequency domain back to the time domain.
- Digital Demodulation: The demodulated signal in the time domain contains the modulated digital symbols, which can be processed further to recover the original digital data.

Next step is to turn frequency domain into radio frequency (RF) signals. It involves the process known as up conversion. this process takes place after digital modulation and frequency domain representation. Quadrature Amplitude Modulation (QAM) is a widely used modulation scheme in 5G and other modern communication systems for transmitting digital data over radio frequency (RF) channels. Before modulation, the binary symbols are mapped to complex symbols, where each complex symbol represents a unique amplitude and phase combination. QAM utilizes a two-dimensional constellation diagram to represent these symbols, with one dimension representing the in-phase (I) component and the other representing the quadrature (Q) component. The mapped symbols are modulated onto a carrier signal using QAM modulation. In QAM, the in-phase and quadrature components of the carrier signal are modulated independently based on the amplitude and phase of the complex symbols. This allows multiple bits to be transmitted per symbol, resulting in increased data throughput compared to simpler modulation schemes like binary phase shift keying (BPSK) or quadrature phase shift keying (QPSK). The number of symbols in the constellation diagram, or the size of the QAM constellation, determines the modulation order and the number of bits transmitted per symbol. Common modulation orders used in 5G include 16-QAM, 64-QAM, and 256-QAM, which respectively transmit 4, 6, and 8 bits per symbol. To ensure reliable communication over noisy channels, error correction coding and detection techniques are employed in conjunction with QAM modulation. Forward Error Correction (FEC) codes add redundancy to the transmitted data, allowing receivers to detect and correct errors introduced during transmission. 5G networks often employ adaptive modulation and coding techniques, where the modulation scheme and coding rate are dynamically adjusted based on channel conditions such as signal strength and interference levels. QAM modulation allows for flexible adaptation of modulation order to optimize data throughput and spectral efficiency under varying channel conditions.[9]

By utilizing FFT and its inverse (IFFT), 5G systems efficiently transfer data between the time domain and the frequency domain, enabling high-speed data transmission and efficient use of the frequency spectrum. After that, QAM modulation plays a crucial role in 5G networks by enabling the transmission of digital data at high data rates over RF channels. Its flexibility, efficiency, and compatibility with advanced communication techniques make it

well-suited for the requirements of 5G communication systems.

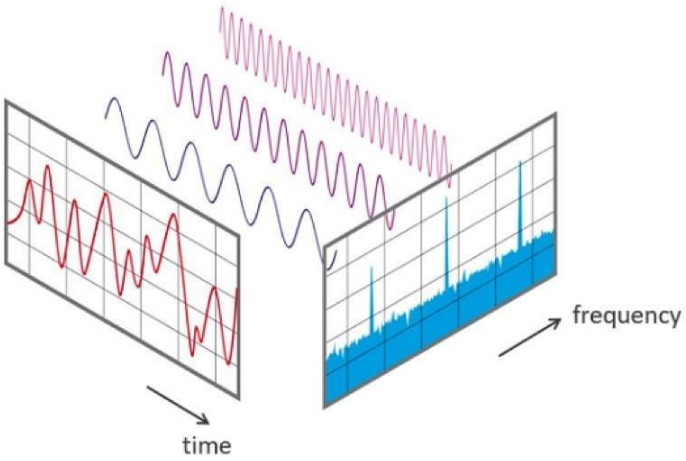

Figure 1: Turning Time domain into frequency domain

6. Fast Fourier transform

FFT is a fast algorithm that transforms a signal from its time-domain representation to its frequency-domain representation.
FFT helps us uncover the hidden frequency components within a signal, enabling us to understand its composition. Used in various applications like audio processing, image analysis, and communication systems.
Divides the signal into smaller components, reducing the computational complexity.
Utilizes a divide-and-conquer approach to efficiently compute the Discrete Fourier Transform (DFT).
Involves complex numbers to represent both amplitude and phase information at different frequencies. [6]

$$X_k = \sum_{m=0}^{n-1} x_m e^{-i2\pi km/n} \qquad k = 0, \ldots, n-1$$

Figure 2: FFT

Direct approach with FT would give us complexity of O(n^2), but FFT gives complexity of O(n*logn).

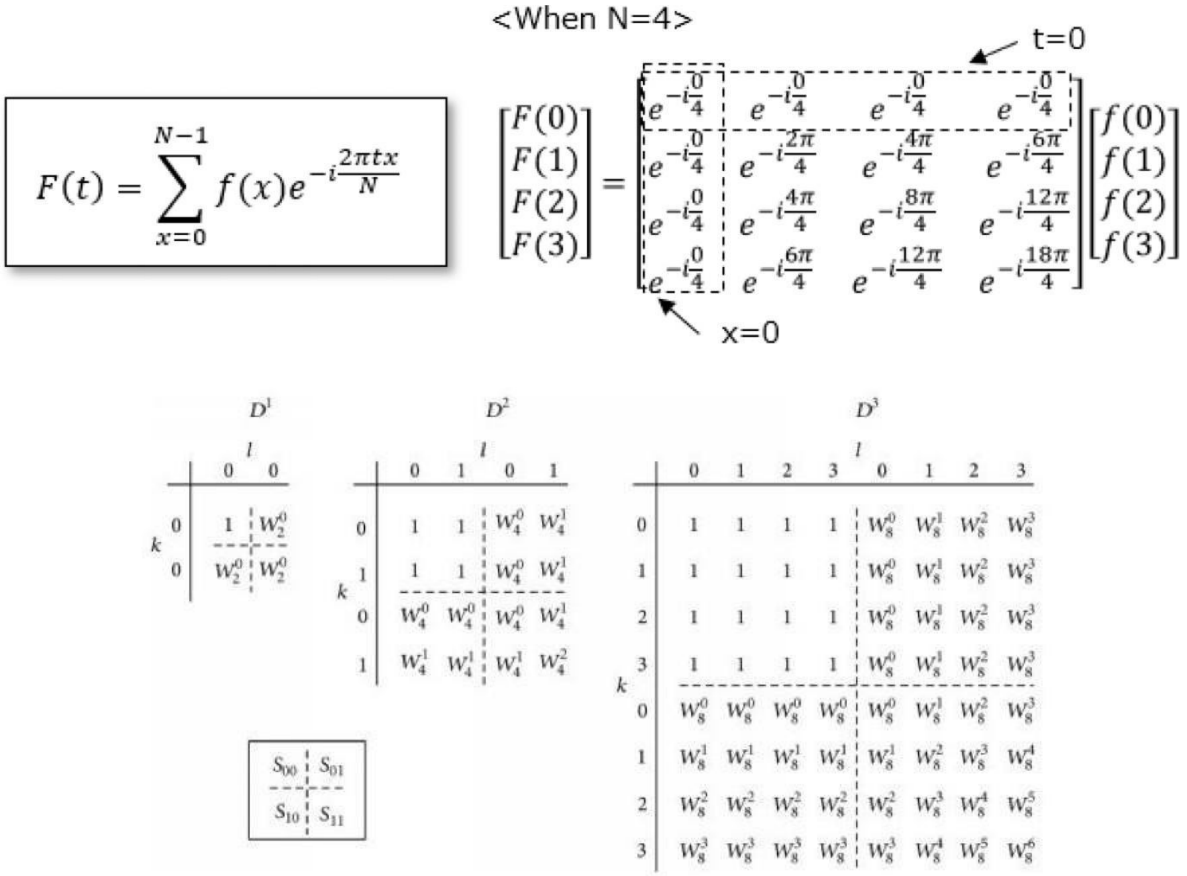

Figure 3: Splitting matrix in quadratic matrices

7. Complexity of this idea

Modern smartphones equipped with multicore processors and hardware-accelerated computation capabilities can perform FFT operations quite efficiently. For typical signal lengths encountered in audio or communication applications, such as 1024, 2048, or 4096 samples, the computational time for FFT on a smartphone is typically negligible and can be executed in milliseconds or even microseconds. For example, let's consider a smartphone with a quad-core processor running at 2.5 GHz. If we assume that the FFT algorithm is well-optimized and can effectively utilize multiple cores, the time taken to compute an FFT for a signal with 2048 samples could be on the order of microseconds to low milliseconds. [5]

However, for longer signals or more computationally intensive applications, the time required could be slightly longer. Advanced optimization techniques, hardware acceleration, and efficient memory access patterns can further reduce the computational time. As shown previously fft complexity is O(nlogn) so multiplying FFOT on constant will not change the complexity because multiplying happens in linear time and O(nlogn) dominates on it.

In a typical scenario with optimized implementations and efficient network conditions, the total time taken for a three-way handshake involving certificate-based authentication with an RF tower could range from a few milliseconds to tens of milliseconds (e.g., 10-50 milliseconds) per round-trip time (SYN + SYN/ACK+ ACK). [11] This communication will be like this:

Client Hello (Round-trip Time: RTT1):

- The client sends a "Client Hello" message to the RF tower.
- The RF tower responds with a "Server Hello" message and its certificate.
- The time taken for this initial exchange depends on the network latency (SYN) between the client and the RF tower.

Certificate Verification and Key Exchange (RTT2):

- The client verifies the authenticity and validity of the RF tower's certificate.
- The client may also perform key exchange and negotiation of cryptographic parameters during this step.
- The time taken for certificate verification and key exchange can vary based on the complexity of the certificate chain, the efficiency of the cryptographic algorithms, and the computational capabilities of the client device.

Completion of Handshake (RTT3):

- Upon successful verification and key exchange, the client sends a "Finished" message to the RF tower.
- The RF tower responds with its own "Finished" message.
- The time taken for this final exchange depends on the network latency (ACK) between the client and the RF tower.

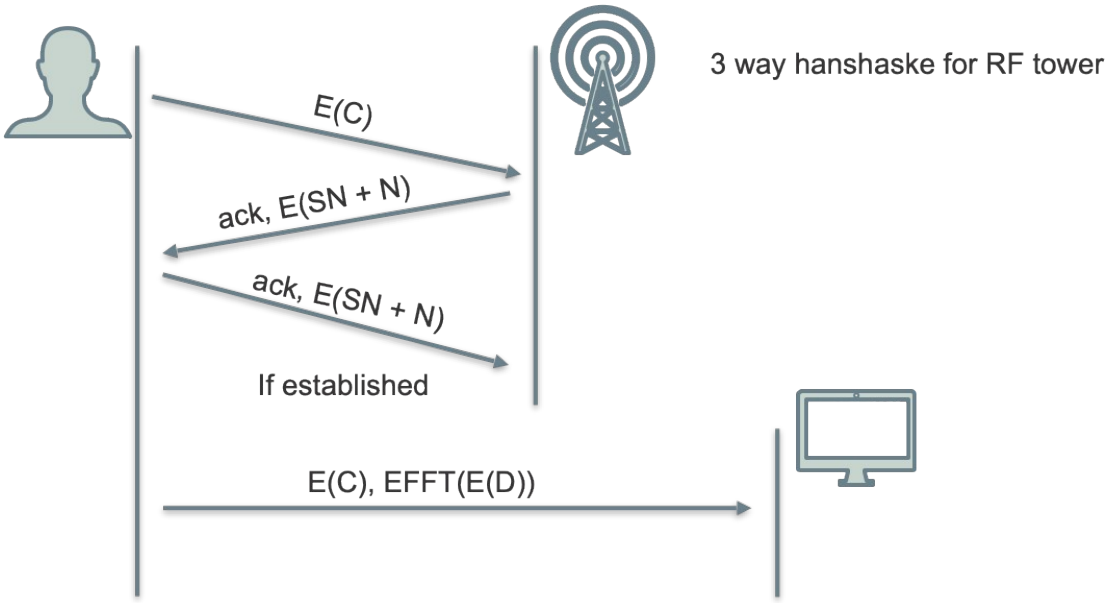

Figure 4: 3 way handshake with RF tower

Moreover, we should take notice of encryption methods and how it will affect this communication, we are discussing this with AES encryption.

If we have a constant number the size of a digital certificate can range from a few hundred bits to several thousand bits (e.g., 1-5 KB) based on the cryptographic algorithms, key sizes, and encoding formats used. When considering the size of certificates in a communication

system, it's essential to account for the size of the individual certificates, the certificate chain, and any additional metadata or headers required for the communication protocol.

Size considerations for AES encryptions:

1. **Block Size:** AES operates on fixed-size blocks of data, with each block being 128 bits (16 bytes) in size. If the plaintext data does not align perfectly with the block size (e.g., is not a multiple of 16 bytes), padding may be required to bring the plaintext data to the nearest block size before encryption.
2. **Ciphertext Size:** The size of the ciphertext produced by AES encryption will be the same as the size of the plaintext data (including any required padding). For example, if you encrypt a 1 MB file using AES-128 or AES-256 encryption, the size of the resulting ciphertext will also be approximately 1 MB.
3. **Key Size:** AES supports key sizes of 128 bits, 192 bits, and 256 bits. While increasing the key size can enhance the security of the encryption, it does not affect the block size or the size of the encrypted data. The size of the ciphertext remains the same regardless of the key size used.

Business model of this idea is also interesting because it can be costly but internet providers can create a special service. There can be two ways: one is to create subscription based service and another is to create new line of pricing for internet purchase. That means implementing this kind of technology will buy itself and security will be on higher level. [12]

8. Extra Layer of security

Before starting approach to the idea let's define some notations.

Certificate = N(name of the holder) + SN(serial number) + pk(copy of public key) + CA(certificate authority) + ED(expiration date)

E(encryption) - EAS 128bit or 256bit

EFFT - Fast Fourier Transform encryption with serial number (SN will be used as constant multiple for vector to turn into frequency domain)

Extra layers consist of two parts, one is to add 3 way handshake between client and tower or server and tower, and second part consists of adding hidden constant during the FFT transformation.

For the first part, client sends the encrypted certificate to the RF tower, it gets back acknowledgment and encrypted serial number plus name of holder, then client responds with same kind of response. Client finally sends the encrypted certificate and EFFT with encrypted data.

Here is the UML graph that will show the entire logical process:

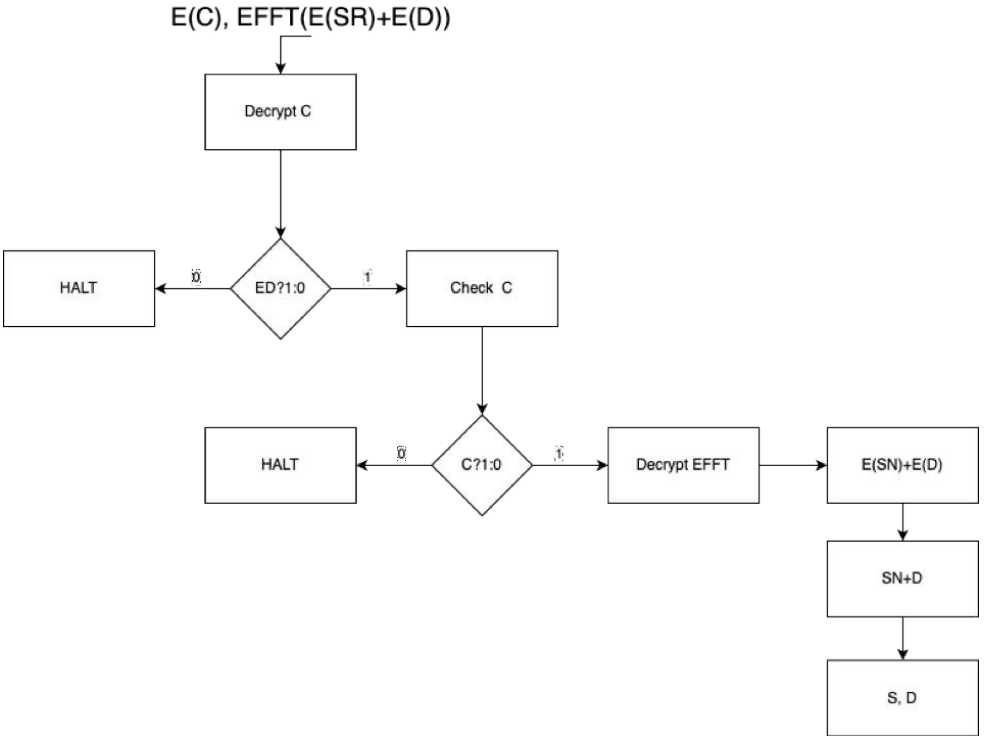

Figure 5: UML diagram of communication model

9. Conclusion

MITM attacks represent 19% of all successful cyber-attacks, according to a 2021 study. A 2022 report by F5 found that over 50% of all MITM attacks involve the interception of sensitive information such as login credentials and banking information. MITM attacks are responsible for an estimated $2 billion in annual losses worldwide, according to a 2020 report by Accenture. Therefore, creating new technologies such as 5G creates new risks.[8]

As 5G networks continue to evolve and expand, the imperative for robust security measures escalates. With the ever-increasing volume of data traversing these networks, safeguarding sensitive information against cyber threats becomes paramount. In response to this challenge, the integration of advanced encryption techniques within fundamental processes like the Fast Fourier Transform (FFT) emerges as a promising solution, poised to fortify data security in 5G communication systems.

By embedding encryption directly into the FFT algorithm, a formidable barrier is erected against potential breaches in the confidentiality and integrity of transmitted data. This additional layer of security serves as a defensive wall, restricting unauthorized access, interception, and tampering attempts during data transmission, thereby preserving the sanctity of sensitive information.

Furthermore, the strategic incorporation of encryption within FFT architecture addresses security concerns without incurring detrimental impacts on the efficiency and performance metrics of 5G networks. Leveraging the computational prowess inherent in FFT operations, encryption can be seamlessly woven into existing communication protocols, ensuring minimal disruption to data transmission speeds and latency levels(It still requires mathematical and practical testing to be proven).

In essence, the fusion of encryption and FFT not only reinforces the resilience of 5G networks against evolving cyber threats but also underscores a proactive approach towards safeguarding the integrity and confidentiality of data in the digital realm. This symbiotic relationship between security and technological innovation heralds a new era of fortified

communication infrastructures, poised to navigate the complexities of an increasingly interconnected world with confidence and assurance.

10. Acknowledgment

The work was conducted for the cybersecurity conference in Caucasus University (Georgia, Tbilisi).

11. References

[1] Qualcomm, “What is 5G?”
[2] Eoin O'Connell, Denis Moore, Thomas Newe, “Challenges Associated with Implementing 5G in Manufacturing”, June 2020, Telecom
[3] Cisco, “ What is 5G technology?”
[4] Cisco, “5G news”
[5] Juha Yli-Kaakinen, Toni Levanen, Markku Renfors, Mikko Valkama, “FFT-domain signal processing for spectrally-enhanced CP-OFDM waveforms in 5G new radio”, November 2018
[6] NTI-Audio, “Fast Fourier Transformation FFT”
[7] M. Ivezic, L. Ivezic, “5G Security & Privacy Challenges” in 5G.Security Personal Blog, 2019. https://5g.security/cyber-kinetic/5g-security-privacy-challenges/
[8] Akhalaia, G., Iavich, M., Gnatyuk, S. (2022). “Location-Based Threats for User Equipment in 5G Network”. Advances in Computer
Science for Engineering and Education. ICCSEEA 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 134. Springer, Cham. https://doi.org/10.1007/978-3- 031-04812-8_11
[9] Huawei Technologies CO,. LTD in “5G Network Architecture – A high Level Perspective”,
2016 [10]M. Iavich, G. Akhalaia, S.Gnatyuk. Method of Improving the Security of 5G Network Architecture Concept for Energy and Other Sectors of the Critical Infrastructure, In: Zaporozhets A. (eds) Systems, Decision and Control in Energy III. Studies in Systems, Decision and Control, vol 399. Springer, Cham. https://doi.org/10.1007/978-3-030-87675-3_14,
[11] Todo, Y., Aoki, K. (2014). FFT Key Recovery for Integral Attack. In: Gritzalis, D., Kiayias, A., Askoxylakis, I. (eds) Cryptology and Network Security. CANS 2014. Lecture Notes in Computer Science, vol 8813. Springer, Cham. https://doi.org/10.1007/978-3-319-12280-9_5
[12] Jin, C., Zhou, Y. Enhancing non-profiled side-channel attacks by time-frequency analysis. Cybersecurity 6, 15 (2023). https://doi.org/10.1186/s42400-023-00149-w