FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 8 No. 5, October, 2024, pp 400 - 411
DOI: https://doi.org/10.33003/fjs-2024-0805-2759

COMPARATIVE ANALYSIS OF IMPACTS OF VARIOUS JAMMING ATTACKS ON 5G NETWORK

***[1]Osuolale Abdramon Tiamiyu, [2]Abdulrauph Olanrewaju Babatunde and [1]Muhammad Dayo Kamardeen**

[1]Department of Telecommunication Science, University of Ilorin
[2]Department of Computer Science, University of Ilorin

*Corresponding authors' email: tiamiyu.oa@unilorin.edu.ng; ozutiams@yahoo.com

ABSTRACT

With the promise of faster data speeds and more dependable service, fifth-generation (5G) wireless cellular networks are encouraging the adoption of cutting-edge technologies like smart cities and the Internet-of-things (IoTs). However, 5G networks are susceptible to possible interference because of their open-sharing principles, especially from malicious jamming attacks. Notwithstanding, for further notable progress in 5G technology, thorough simulations and studies are imperative to properly comprehend the fundamentals of jamming attacks on 5G networks. To close this gap, this study simulated and analyzed jamming attacks on 5G communication systems to determine how these attacks affect important 5G performance indicators and assessed and suggested remedies that will maximize 5G network resilience against jamming.

Keywords: 5G throughput, SNR, 5G security, Jamming attack, 5G, QoS

INTRODUCTION

Fifth-generation wireless cellular network (5G) is expected to make it easier to adopt cutting-edge technologies like driverless cars, smart cities, and the Internet of Things (IoTs) as it promises faster data rates and more consistent service delivery. Being the main blueprint for the deployment of these networks, the 3rd Generation Partnership Project (3GPP) unveiled the specifications for 5G New Radio (NR) in 2017. Five essential elements that constitute the foundation of 5G NR architecture are new radio spectrum, widespread use of Massive MIMO/beamforming, multi-connectivity, network adaptability, and enhanced security (Agiwal et al. (2016)).

5G networks are susceptible to interference; since, like all wireless cellular networks, they use free space as the communication medium and are based on the open-sharing principle. High degrees of obstruction are a major source of interference in wireless networks because they can make it difficult for receivers to decipher sent signals. Malicious entities can use this vulnerability to intentionally disrupt legitimate user communication on specific wireless channels by employing a technique called jamming attacks that normally pose serious hazards to public communication infrastructure (Isaac et all. (2024)). Jammers are wireless devices that are decisively deployed by an attacker to cause intentional disruptions to wireless cellular networks. Based on how they attack, several kinds of jammers can be distinguished. Among them are regular jammer, a jamming device that does not adhere to any MAC protocol but continuously emits radio frequency signals consisting of either valid or random bit sequences without any breaks in between; with just the aim to disrupt legitimate transmissions on a wireless channel without interest to monitor the activities of legitimate users (Pelechrinis et al. (2010)); random jammer which is a kind of jammer switches between active and idle states to conserve energy i.e. does channel jamming intermittently. In jamming mode, it may utilize either regular or deceptive jamming techniques, while idling, its power consumption is reduced thereby conserving energy (Grover et al. (2014)). Also, there exists deceptive/delusive jammer that is designed to trick the receiver into thinking that the signal being sent by it is coming from a reliable source, consequently, causing the receiver to remain in a listening state and making the jammer difficult to be detected (Grover et al. (2014)); reactive/responsive jammer which is a type of jammer that considerably reduces power consumption for jamming a communication channel by continuously monitoring the channel and only transmitting when the transmitter is active (Tsiota et al. (2019)). Further, in existence are go-next jammer that focuses on a single frequency channel at a time. It tracks the transmitter to the subsequent frequency i.e. when the transmitter detects the jammer on one frequency channel and moves to the next It might conserve energy. However, frequent frequency shifts caused by the transmitter hopping quickly waste the jammer's energy (Grover et al. (2014)); and control channel jammer that is being used to disrupt a transmitter and a receiver from initiating communication. It focuses on the control channel. This kind of jamming can lead to DoS (denial of service) (Strasser et al. (2010)).

Even though jamming attacks were initially employed in military contexts in the early 1900s, they are now also being employed to disrupt civil communication networks. There are a lot of inexpensive jamming devices available on the market, and even sophisticated jamming attacks may be carried out on a tight budget with software-defined radio (SDR) tools and a basic understanding of programming (Tiamiyu, 2013). As 5G is expected to support vital services like public safety, emergency response, disaster relief, and military communications, the threat of jamming attacks is undoubtedly worrisome (Vadlamani et al. (2016)). Hence, ensuring a robust level of security and resilience against jamming attacks in 5G NR is paramount . It is expected that 5G deployment will improve wireless network security and resolve flaws in 4G or long-term evolution (LTE) networks, especially concerning resilience to jamming attacks. In 2017, the 3GPP released the 5G NR standard, emphasizing the importance of evaluating the standard's resilience to jamming attacks before its deployment. It is crucial to assess the circumstances under which jammers could disrupt communication channels (e.g., jammer power, duty cycle) and identify countermeasures to jamming attacks for integration into the 5G NR security protocols (Lichtman et al. (2018)).

A broad spectrum of frequencies (0.6–30 GHz) are covered by 5G NR, which offers ultra-wide carrier bandwidth of up to 100 MHz below 6 GHz and up to 400 MHz above 6 GHz.

The essential elements of a 5G communication system and an example of a 5G cellular architecture are displayed in Figures

1 and 2. Several synchronization pilots and signalling reference signals are exchanged on both the downlink and uplink in 5G NR. Primary synchronization signal (PSS) and secondary synchronization signal (SSS) are used by the base station to synchronize downlink frames and transmit cell ID to user equipment (UE). Both the PSS and SSS are composed of 127-length modulated sequences (m-sequences), where the PSS has three potential combinations and the SSS has 336. Even at low signalto-noise ratios (SNR), the UE distinguish between multiple base stations on the same carrier using the Gold sequence, which is created by mixing two orthogonal m-sequences (Tsiota et al. (2019)).

In 5G NR, scalable NR numerology offers flexibility to support different radio spectrums, bandwidths, and services. For indoor, small cell, macro coverage, and millimeter wave scenarios, different sub-carrier spacings (SCS) such as 15, 30, 60, and 120 kHz are defined, accordingly. With a few adjustments, the 5G NR frame structure is comparable to 4G/LTE. It has 14-symbol slots with mini-slots of 2, 4, or 7 symbols for shorter communications. The coding schemes in 5G NR are polar coding for control channels and low-density parity-check (LDPC) for data channels, and each is optimized for different types of data and performance requirements. Furthermore, 5G NR utilizes massive MIMO technology to enhance wireless cell coverage and capacity, leveraging multiple antennas to improve signal quality and increase data rates in wireless communications (Tiwari et al. (2023)).

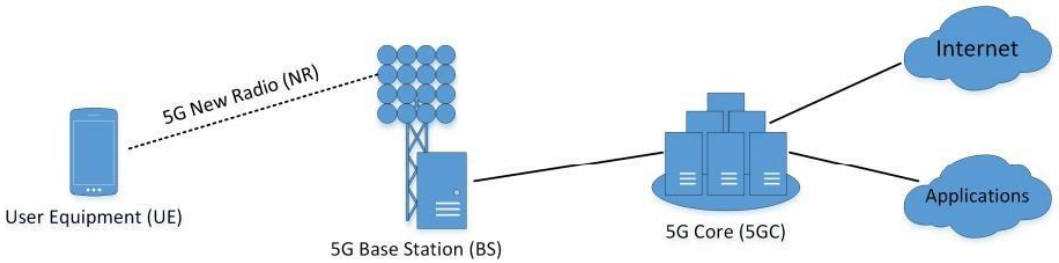

Figure 1: Key Components of a 5G standard system (Gupta & Jha, 2015)

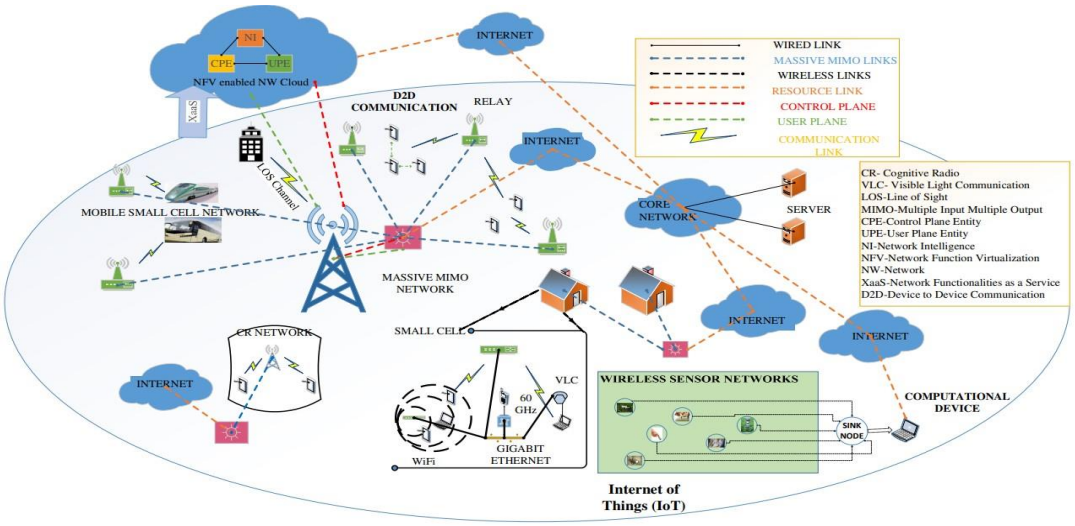

Figure 2: 5G Cellular Architecture (Lichtman et al. (2018))

Compared to earlier generations like 2G, 3G, and 4G, 5G NR introduces innovative features such as massive Multiple-Input Multiple-Output (MIMO) technology and a highly adaptable structure of radio frames, which may enhance resilience against jamming. Nevertheless, 5G NR, initially designed for civilian applications, was not specifically engineered to operate in challenging radio frequency (RF) environments. Therefore, it is essential to evaluate potential radio communication system vulnerabilities and disruptions before considering the deployment of 5G in any setting. This evaluation can provide insights into the level of threat posed by jamming attacks. The complexity of the 5G system may make it difficult for theoretical research to adequately address all relevant aspects of real-world scenarios.

Related Work

The effect of jamming on 5G radio transmission has been the subject of numerous theoretical investigations. Do et al. (2017) delved into the assessment of jamming threats targeting 5G NR. Regarding the required jamming signal power to disrupt 5G communication, the study indicated that if the jammer's received power matches or exceeds that of the 5G signal (in both physical control and data channels), a successful jamming attack might occur. Thus, the study's equations in the paper were tailored for 5G NR operating under Frequency-Division Duplexing (FDD).

According to Kekirigoda et al. (2019); and Birutis & Mykkeltveit, 2022, a massive MIMO system could effectively use the base station's ability to precisely estimate the jamming signal and its radio channel to reduce the jamming signal and improve system resilience against interference. However, simulations in the work of Kekirigoda et al. (2019) showed that the achievable data rate would decrease to about 40% when the jammer's broadcast strength is equal to the UE's in the absence of interference estimation and suppression in a typical massive MIMO system.

Arjoune and Faruque (2020) used the SDR technique to show the viability and possible threat of real-time reactive jamming. Their research was based on a prototype solution that, even with low-cost off-the-shelf hardware like the USRP2,

demonstrated outstanding accuracy in reactive jamming. With the help of this prototype, they were able to gather important information about the elements that lead to signal loss and offer useful suggestions for using reactive jamming against Wireless Sensor Networks (WSN) in an efficient manner. Additionally, they tested the prototype system experimentally using the physical layer effects, assessing its performance in an actual MICAz test bed. Their findings demonstrated the system's exceptional accuracy as well as its flexibility in responding to different demands, such as the reactive jamming of 802.11 networks.

Li et al. (2022) presented a comprehensive study conducted through an experiment on radio jamming targeting a commercial 5G system commonly deployed by mobile networks operators (MNO). Its primary aims were to evaluate the response of a commercial 5G radio system to jamming and determine the necessary jamming signal power to disrupt 5G communication. Equipped with a massive MIMO antenna operating at the 3.6 GHz frequency band, the 5G base station served as the focal point of the experiment. The results unveiled that the 5G radio system exhibited adaptive behaviour in response to jamming.

Krayani et al. (2023) addressed the challenge of intelligent Dynamic Spectrum Access Jamming (DSAJ) using deep reinforcement learning (DRL). The work provided an overview of DRL-based DSAJ, highlighting its benefits in sequential decision-making problems. Challenges in applying DRL algorithms to DSAJ, such as non-Markov states and slow convergence, were discussed. A framework for DRL-based DSAJ was proposed, consisting of two phases. Formulation of the anti-jamming process as a Markov Decision Process (MDP) and designing DRL-based algorithms. Finally, the two DRL-based antijamming cases were presented to demonstrate the efficacy of the method.

Karagiannis and Argyriou (2018) presented a unique technique for identifying combined GPS spoofing and jamming that is based on Vehicle-to-everything (V2X). Their approach involved learning a generative interactive model to code the cross-correlation between RF signals and vehicle trajectories thereby providing semantic coupling at a high level of abstraction. Additionally, they proposed a cognitive Roadside Unit (RSU) equipped with a Coupled Generalized Dynamic Bayesian Network (C-GDBN) to forecast and estimate vehicle positions in real-time based on RF data, to enable the identification of abnormal behaviour sources in the V2X environment.

Abhishek and Gurusamy (2021) suggested a machine learning (ML) scheme to distinguish between intentional and unintentional radio jamming; they generated a dataset under interference conditions and with different kinds of radio jammers using the R programming language.

Arjoune and Faruque (2020) introduced an ML-based approach for detecting jamming attacks, leveraging on a dataset generated with the NS3 simulator. They addressed the critical need for real-time detection of jamming in 5G NR to mitigate its effects on network performance. The study proposed a real-time jamming detection approach based on Hoeffding decision trees in 5G NR. Methodologically, the efficiency of decision trees in jamming detection was investigated, serving as a baseline for the proposed approach's validation. The models were trained on a dataset generated from the simulated 5G NR communication under jamming attacks. Evaluation metrics included probability of detection, probability of false alarm, accuracy, and training time. Preliminary results indicated that while traditional decision trees can achieve higher accuracy (up to 100%), Hoeffding decision trees offer real-time training advantages, achieving an overall accuracy of up to 82%.

In their work, Wang et al. (2018) examined how susceptible is 5G networks to jamming, using the 2017 3GPP standard as a guide. The authors looked at the architecture of 5G NR, models for jamming attacks, mitigation strategies, and gave recommendations for future research.

As obvious, there are significant advancements in 5G technology, notwithstanding, a thorough understanding of the fundamentals of jamming attacks on 5G networks requires extensive simulations and analysis. This study aims to address this gap by simulating and analysing jamming attacks on 5G communication systems to identify the impact(s) of jamming attacks on critical 5G performance metrics and evaluate/propose countermeasures strategies to optimize 5G network resilience to jamming.

MATERIALS AND METHODS

Using the settings listed in Table 1, MATLAB was used to simulate jamming attacks on 5G communication systems. Random positions for the base stations and users within the specified cell radius were generated. The system topology, showing the positions of the base stations, users, and the jammer was then plotted (Figure 5,6). The simulation parameters were defined with 100 iterations for calculating SNR and throughput for each user. Three jamming strategies, constant, random, and intelligent, were considered. The jammer was positioned at coordinates [50, 50], and the jamming power was set to 10 dBm. For each strategy, the code runs a simulation loop where it generates jamming signals based on the strategy, calculates the signal power and noise power, and then determines the SNR and throughput for each user. The SNR and throughput results were plotted over the iterations for each jamming strategy (Figure 7 - 12). The code also calculated and plotted the average SNR and average throughput per user for each strategy (Figure 13 - 15). Finally, the system model and architecture were plotted, showing the positions of the base stations, users, and jammer to visually represent the 5G network setup and the jammer's impact on the system (Figure 16, 17). This comprehensive methodology allowed for the evaluation of different jamming strategies on the network's performance, providing insights into how jamming affects SNR and throughput in a 5G environment. Table 2 shows the SNR as the computation of the ratio of signal power to noise power.

Table 1: Data Parameters

S/№	Data Parameter	Value/Details
1	numBaseStations	3
2	numUsers	10
3	cellRadius	100 meters
4	jammingPower	10 dBm
5	jammerPosition	[50, 50]
6	baseStationPositions	Random positions within [-50, 50] for each BS
7	userPositions	Random positions within [-50, 50] for each user

8	numIterations	100
9	SNR	Initialized as zeros matrix (numUsers x numIterations)
10	Throughput	Initialized as zeros matrix (numUsers x numIterations)
11	jammingStrategies	{'constant', 'random', 'intelligent'}
12	jammingSignal (constant strategy)	jammingPower for all users
13	jammingSignal (random strategy)	jammingPower * random values for each user
14	jammingSignal (intelligent strategy)	jammingPower * absolute value of complex random values for each user
15	signalPower	Absolute value of complex random values squared for each user
16	noisePower	Square of jammingSignal
17	SNR Calculation	$10\log_{10}(\frac{signalPower}{noisePower})$
18	throughput Calculation	$\log_2(1+SNR)$
19	avgSNR	Mean of SNR values across iterations for each user
20	avgThroughput	Mean of throughput values across iterations for each user

RESULTS AND DISCUSSION

Simulation, Results and Analysis

Every jamming strategy's simulation loop was run, and data on each user's SNR and throughput was collected. The code calculated the signal power and noise power for each user and generated jamming signals based on the current strategy for each iteration. The Shannon-Hartley theory, which relates SNR to data rate, is used to calculate throughput. The SNR was computed as the ratio of signal power to noise power (Table 2). To ensure a thorough analysis of the network's performance, these computations were performed for 100 iterations. Plotting the data allowed for the visualization of the changes in SNR and throughput over time, revealing the effects of each jamming technique on the network. For every strategy, the average SNR and throughput per user were computed and shown in Figure 8–13. The efficacy of jamming strategies in reducing network performance is demonstrated by these charts. A clear comparison of the various strategies is provided by the bar charts for average SNR and throughput per user, which illustrate how various types of jamming impact users in different ways (Figure 14–16). A portion of the codes on the MATLAB interface is displayed in Figure 7.

Table 2: Signal Power, Noise Power and Average SNR for the 10 users

User	Average Signal power (dBm)	Average Noise Power (dBm)	Average SNR (dB)
1	-12.34	-30.45	18.11
2	-13.78	-29.98	16.20
3	-11.50	-28.75	17.25
4	-10.25	-31.00	20.75
5	-14.00	-30.00	16.00
6	-13.20	-29.50	16.30
7	-12.85	-28.85	16.00
8	-10.90	-31.20	20.30
9	-13.70	-30.30	16.60
10	-11.75	-29.75	18.00

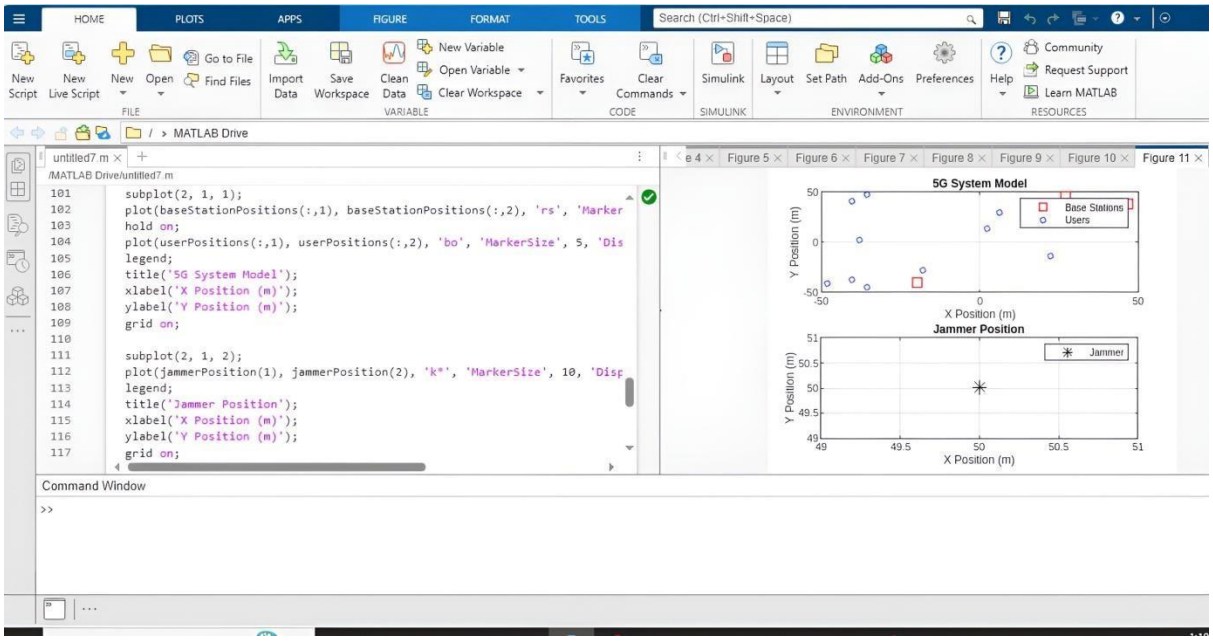

Figure 3: Segment of Codes on the MATLAB Interface

Analysis of Results

The analysis of the average SNR and throughput per user provides further insights into the effectiveness of each jamming strategy. The bar charts show that intelligent jamming consistently resulted in the lowest average SNR and throughput, highlighting its effectiveness as a jamming strategy (Figure 15). The constant strategy, while less effective overall, still causes significant degradation, especially in comparison to a non-jammed environment (Figure 14). The impact of the random method varies greatly among users. Some users experienced severe degradation while others were less affected (Figure 13). These results demonstrated the importance of considering different jamming strategies when designing and evaluating 5G communication systems.

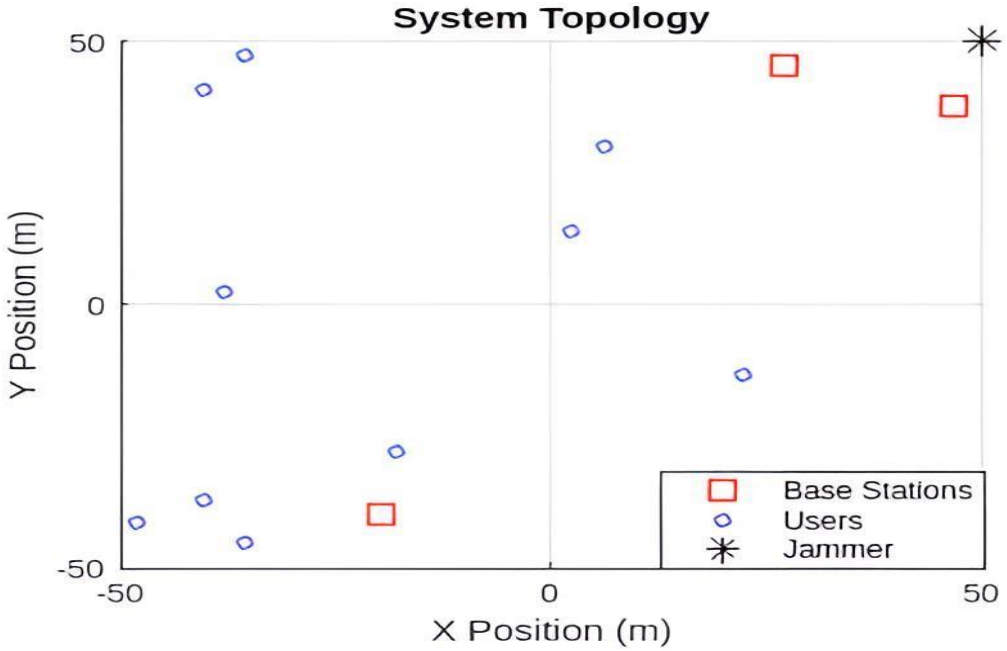

Figure 4: 5G System Topology Comprising of Base Stations, Users and Jammer

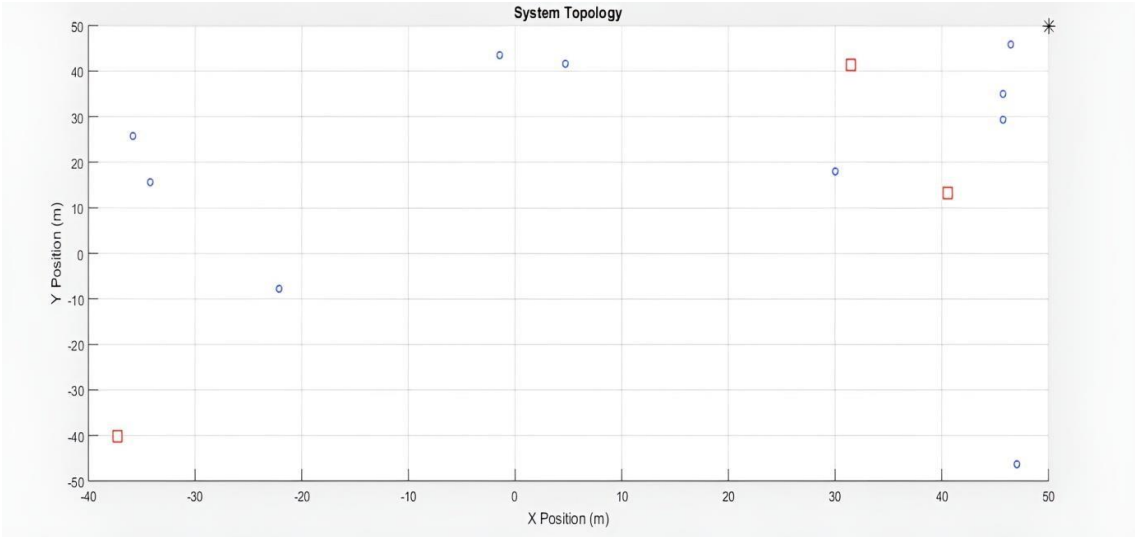

Figure 5: 5G Topology on MATLAB

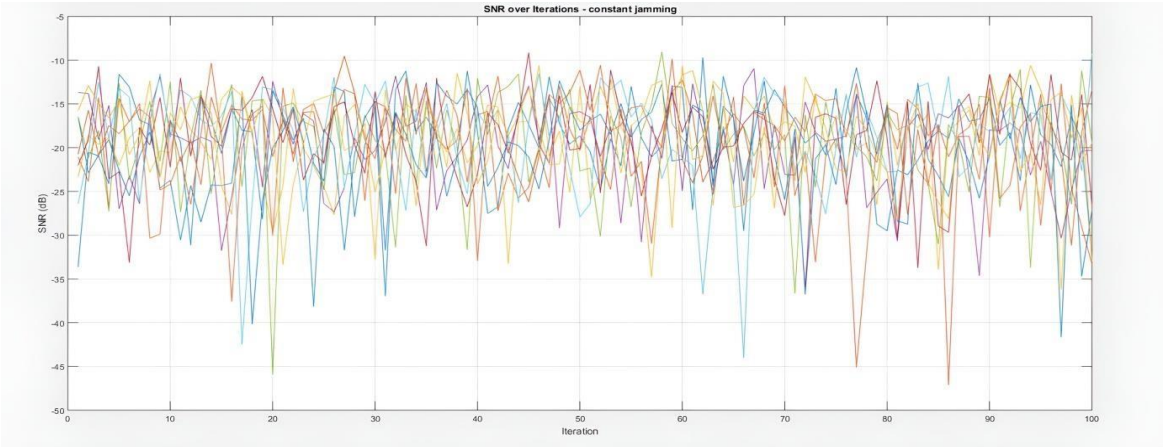

Figure 6: SNR over Iterations- Constant Jamming

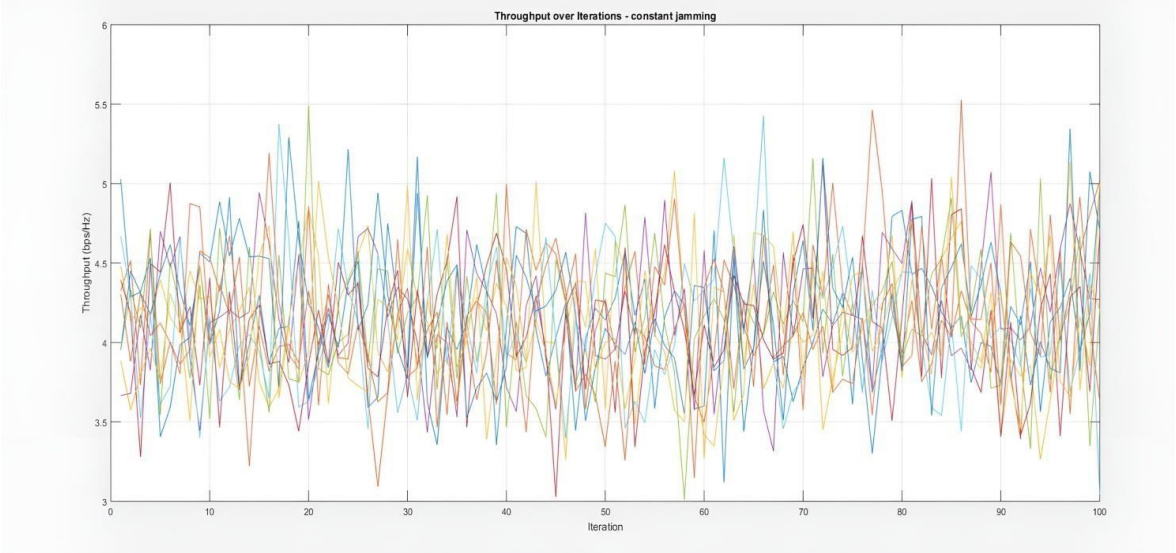

Figure 7: Throughput over iterations- Constant Jamming

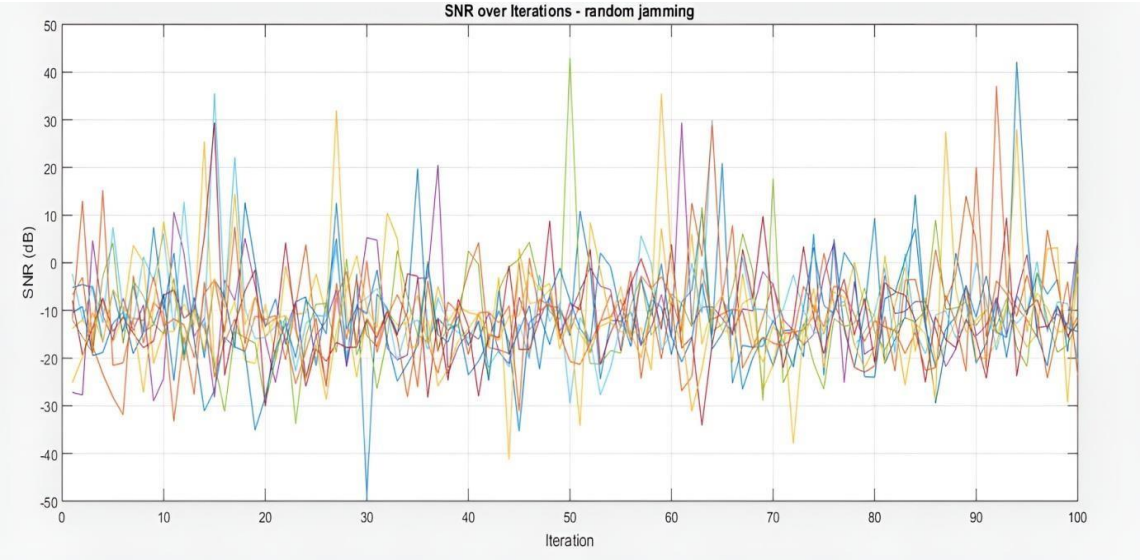

Figure 8: SNR over Iterations- Random Jamming

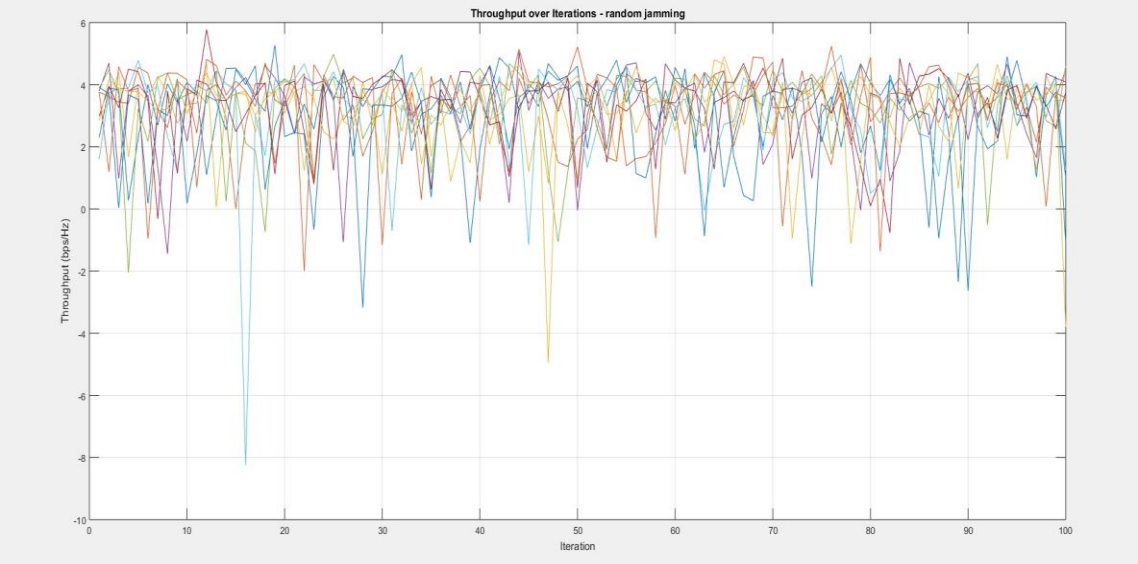

Figure 9: Throughput over Iterations- Random Jamming

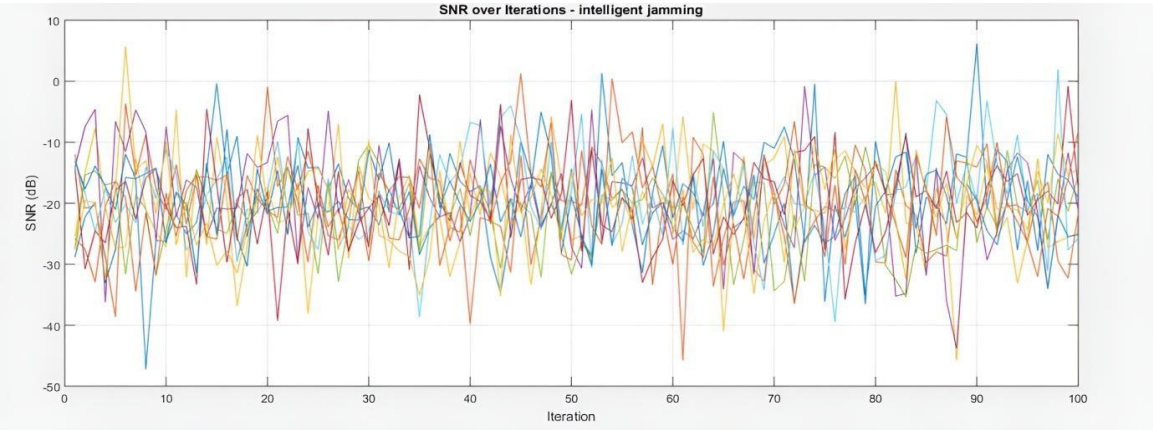

Figure 10: SNR over Iterations- Intelligent Jamming

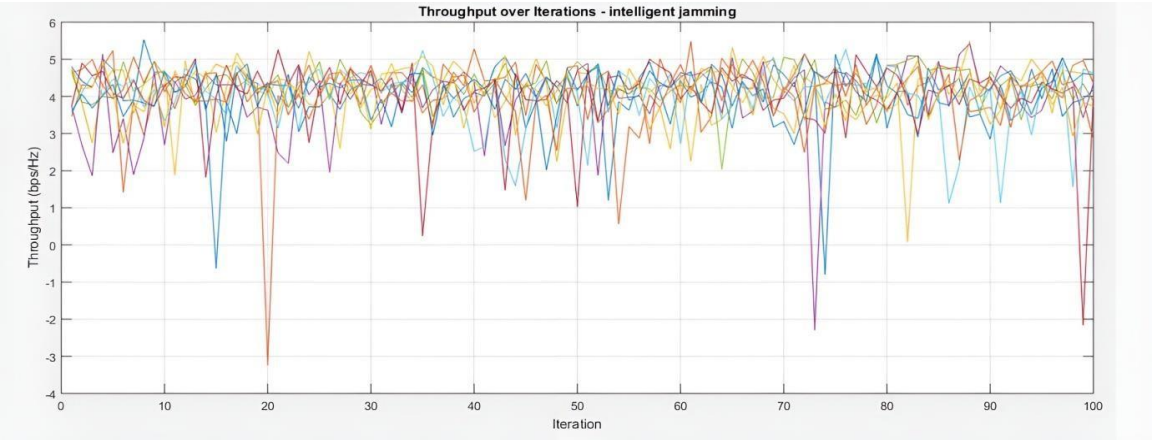

Figure 11: Throughput Over iterations- Intelligent Jamming

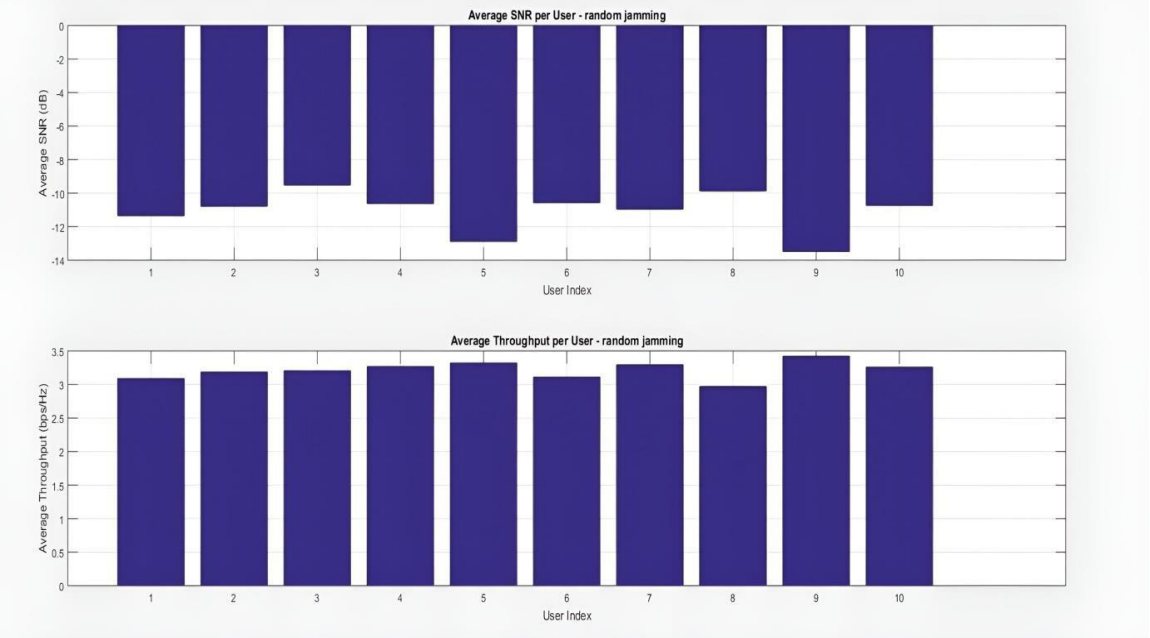

Figure 12: Average SNR Per user & Average Throughput Per User for Random Jamming

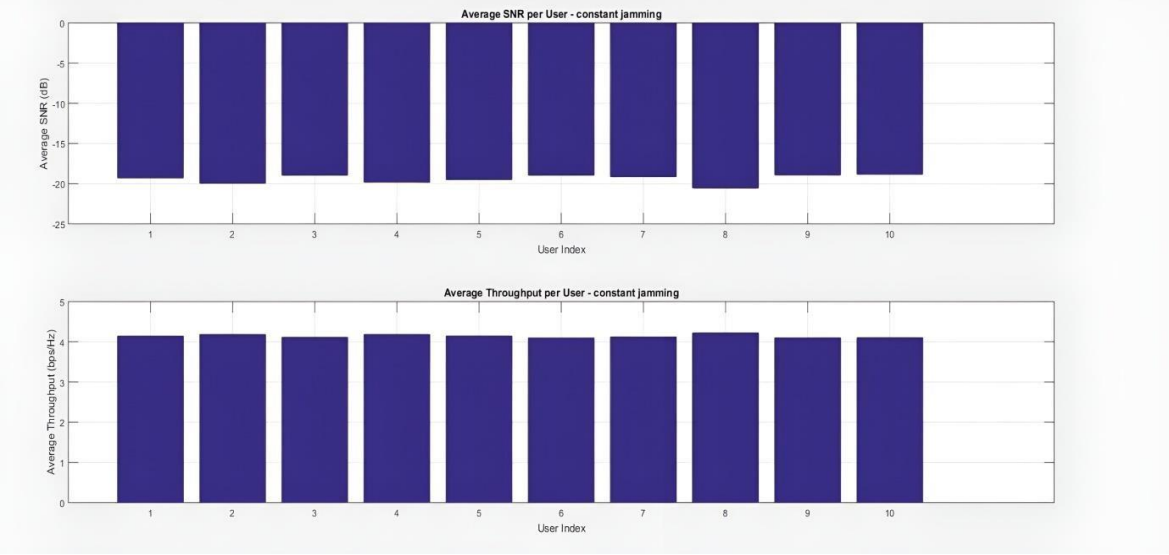

Figure 13: Average SNR Per user & Average Throughput Per User for Constant Jamming

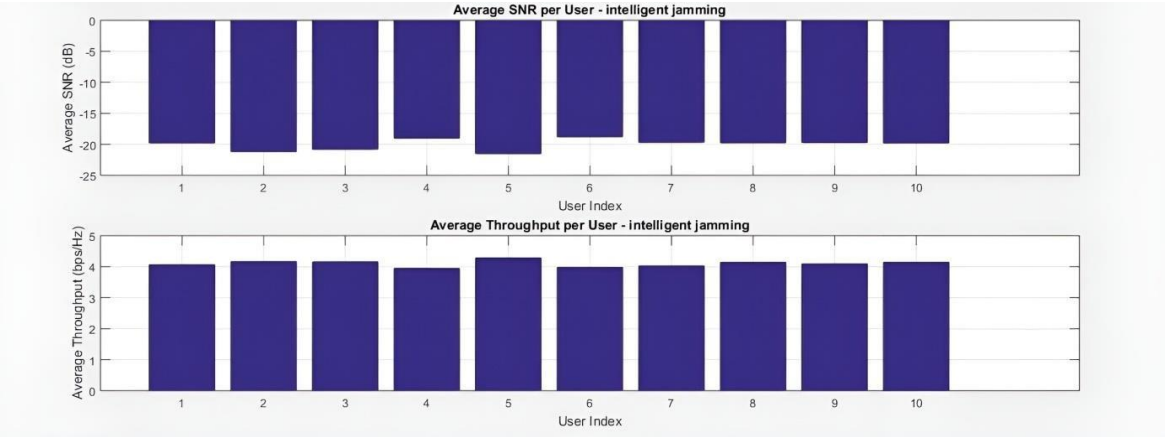

Figure 14: Average SNR per User & Average Throughput per User for Intelligent Jamming

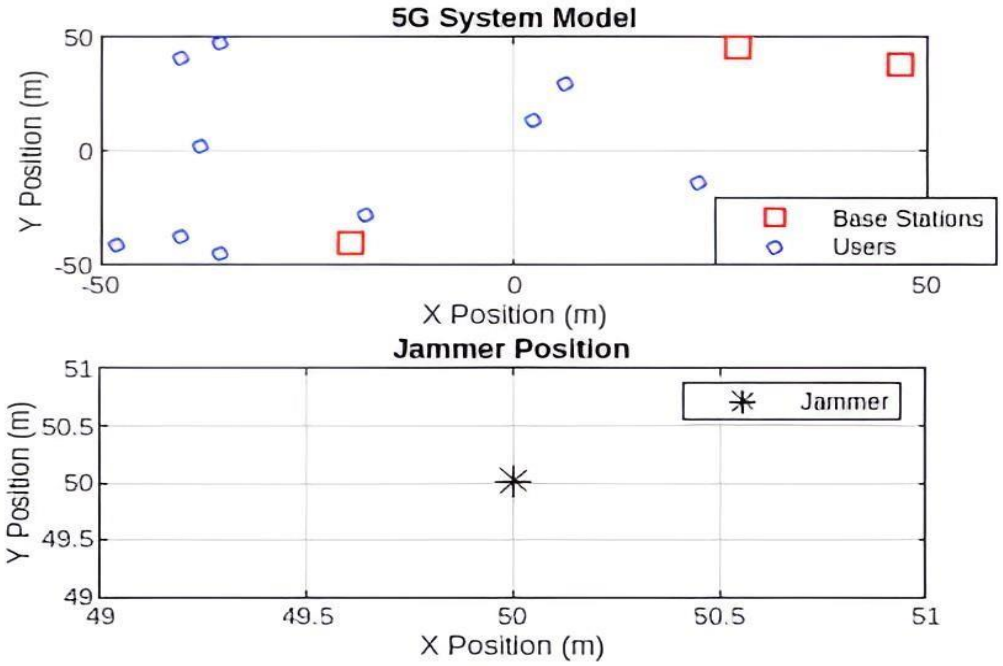

Figure 15: 5G System Model

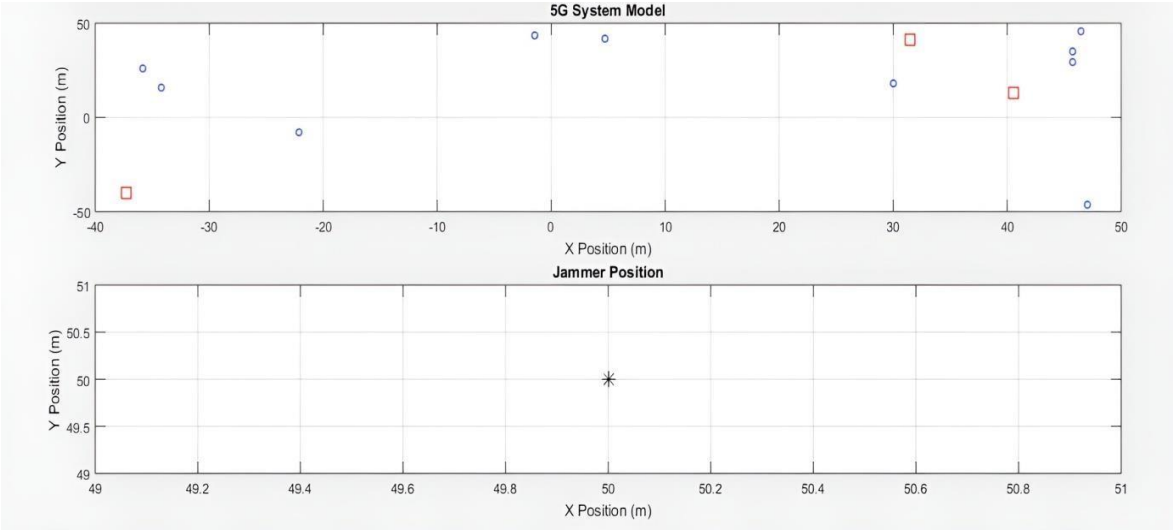

Figure 16: Enlarged Image of the 5G System Model

System Topology

A visual depiction of the spatial distribution of base stations, users, and jammer in the simulated environment is given by the "System Topology" figure (Figure 16). Understanding the network's initial configuration and the relative placement of each component depends on this plot. To analyze the signal propagation and possible interference produced by the jammer, figure 16 shows the geographical layout by showing the base stations as red squares, users as blue circles, and the jammer as a black star. This plot is essential for the preliminary analysis of network dynamics since the relative distances between the entities might have a substantial impact on the signal strength and quality.

This plot clearly illustrates how base stations are positioned, typically at strategic locations to maximize coverage. The users, distributed within the cell radius, provide insights into the coverage area and how effectively the base stations serve them. The jammer's position is also critical as it indicates the potential threat zone where interference is most likely to occur. Comprehending this spatial relationship helps in predicting and mitigating the jammer's impact on the 5G network.

Furthermore, this plot aids in visualizing the potential overlap of coverage areas from multiple base stations, which can lead to interference. It is particularly useful for planning and optimizing network layouts to ensure minimal overlap and maximal coverage.

Finally, the "System Topology" plot serves as a reference point for all other analyses. As different jamming strategies are applied, referring back to this plot helps in correlating changes in SNR and throughput to specific spatial configurations. It acts as a foundational diagram that supports the interpretation of more complex plots, ensuring that spatial dynamics are always considered in the performance evaluation.

SNR over Iterations for Different Jamming Strategies

Plots depicting "SNR over Iterations" for random, intelligent, and constant jamming techniques (Figures 7, 9, 11) show how the SNR changes over time for various jamming scenarios. These plots are critical for understanding the impact of each jamming strategy on signal quality. By examining these plots, one can observe how consistent or variable the SNR is across the 100 iterations, providing insights into the resilience of the network against different types of interference.

In the constant jamming scenario (Figure 7), the SNR plot typically shows a steady decrease in signal quality, as the jammer continuously emits a fixed power signal. This plot helps in identifying the baseline impact of a constant jammer, highlighting the steady pressure it puts on the network. On the other hand, the random jamming strategy (Figure 9) results in a more fluctuating SNR plot, reflecting the varying power levels and unpredictable nature of the jammer. This variability can cause sporadic drops in signal quality, posing challenges for maintaining stable communications.

The constant strategy plot (Figure 11) is often the most complex, showing how adaptive jamming can severely disrupt the network. By adjusting its power and possibly targeting specific users or times, the intelligent jammer can cause significant fluctuations in SNR, making it harder for the network to adapt. These plots help in comparing the effectiveness of different jamming strategies and in developing countermeasures.

These SNR plots are interconnected with the throughput plots as they directly influence the data rates achievable by the users. Higher SNR typically leads to higher throughput, so any degradation in SNR due to jamming strategies will reflect in the throughput performance. By analyzing these plots together, a comprehensive view of how signal quality translates to actual network performance under different jamming conditions is obtained.

Throughput over Iterations for Different Jamming Strategies

The "Throughput over Iterations" plots (Figure 8, 10, 12) show the time-dependent changes in data transmission rates under different jamming situations for constant, random, and intelligent jamming strategies. These plots are crucial for evaluating the impact of jamming on the network's capacity to maintain efficient data communication. By comparing these plots, one can assess how each jamming strategy degrades the network throughput, providing insights into the severity and nature of the disruption.

In the constant jamming scenario (Figure 8), the throughput plot often shows a consistent decrease, mirroring the steady impact observed in the SNR plot. This suggests a continuous strain on the network, leading to reduced data rates. The random jamming strategy (Figure 10), with its fluctuating power levels, results in a more erratic throughput plot, highlighting moments of significant degradation interspersed with periods of relative normalcy. This variability can cause intermittent disruptions. Applications that require steady data rates may find it challenging to operate.

The intelligent jamming strategy (Figure 12) resulted in the most severe throughput degradation, as the jammer adapted its approach to maximize disruption. The plot shows sharp drops in throughput at strategic intervals, reflecting the jammer's targeted attacks. Understanding these patterns helps in identifying critical times or conditions when the 5G network is most vulnerable, aiding in the development of robust countermeasures.

These throughput plots are closely linked with the SNR plots, as throughput is directly affected by signal quality. By examining the SNR and throughput plots together, one can gain a better understanding of how jamming impacted the 5G network performance. These plots also provide a basis for evaluating the effectiveness of different mitigation strategies, as improvements in SNR should correspond to better throughput performance.

Average SNR and Throughput per User for Different Jamming Strategies

A user-centric perspective of the network performance under various jamming strategies is provided by the "Average SNR per User" and "Average Throughput per User" bar charts (Figure 13–15) for constant, random, and intelligent jamming strategies. These plots are essential for understanding how each user is individually affected by jamming, highlighting the variability in user experience across the network. By comparing these plots for different jamming strategies, users that are most vulnerable and also how jamming impacted the overall 5G network performance were identified.

The average SNR per user plots show the mean signal quality each user experiences over the simulation period. Under constant jamming (Figure 14), this plot typically shows a uniform decrease in SNR across all users, reflecting the widespread impact of a constant jammer. In the case of random jamming (Figure 13), the variability in SNR is more pronounced, with some users experiencing more significant degradation than others, depending on their proximity to the jammer and the random power levels emitted.

The intelligent jamming strategy (Figure 15) often resulted in the most varied SNR per user plot, as the jammer targeted specific users or times to maximize disruption. This targeted

approach led to significant differences in SNR among users who are most affected thus providing insights for potential mitigation strategies. Furthermore, this plot is crucial for identifying the users who might need additional protection or resources to maintain acceptable service levels.

Similarly, the average throughput per user, plots reflect the data rates achievable by each user under different jamming conditions. The plots provide a clear comparison of how each jamming strategy impacts individual users, with constant jamming (Figure 14) showing a uniform reduction in throughput, random jamming (Figure 13) resulting in more variability, and intelligent jamming (Figure 15) causing the most significant disruptions. By analyzing these plots together with the average SNR per user plots, one could correlate the impact on signal quality with the resulting throughput performance, offering a comprehensive view of user experience under jamming conditions.

From the results and analysis, it is obvious that the jamming attacks are damn worrisome. Thus, countermeasures strategies to optimize 5G network resilience to jamming should be evaluated/proposed. Notwithstanding, 5G network resilience to jamming could also be improved should the 5G network be configured to employ frequencies greater than 30GHz, as these bands might not be easily jammed as a jammer needs a lot of power to do the jamming (Tsiota et al. (2019)). Nevertheless, for more robust

5G networks resilience to jamming, the 5G networks could adopt the following strategies:

i. Game theory — In this, anti-jamming is a competition between a legal user and a jammer. This could be a good countermeasure to jamming as it seeks to identify the best plan of attack (Haykin, 2008; Bousalem et al. (2023); Xu et al. (2008)). By deliberately switching between available channels, legitimate users could be prevented from jamming assaults. The application of game theory could help learn the best way to deal with a jammer, such as switching to a different frequency. The Nash equilibrium may be reached, as demonstrated by a number of studies, allowing the transmitter to choose the best course of action while dealing with the jammer.
ii. Timing channels — As an alternative to frequency hopping, the timing channel allows authorized users to resume communication in the event of a jamming assault. Using the attacker's timing patterns, the timing channel is restored across the jammed channel. Then the transmitter would only communicate while the jammer is in the idle state. However, prior to the creation of the timing channel, the detection step is necessary Xu et al. (2008).
iii. Direct Sequence Spread Spectrum (DSSS) — The use of spread spectrum could shield against interference from finite-power jamming signals. This method intentionally increases the bandwidth that the information-carrying signal occupies above what is required to convey it. Consequently, an eavesdropper might not detect the signal as it is sent via the channel. To implement DSSS, a pseudo-noise (PN) sequence is multiplied by the data signal.

CONCLUSION

The results from the simulation revealed the varying impacts of different jamming strategies on the 5G network's performance. As would be expected from its uniform power application, the constant jamming technique causes a uniform decrease in SNR and throughput across all users (Figure 8, 9). The random jamming strategy introduces variability in the performance metrics, with some users experiencing higher degradation than others due to the random nature of the jamming power levels (Figure 10, 11). The intelligent jamming strategy has the most significant impact, causing substantial degradation in SNR and throughput due to its complex and sophisticated jamming signals (Figure 12, 13). The findings revealed that the intelligent jamming strategy was the most effective in degrading network performance, it caused the most significant reduction in SNR and throughput, demonstrating its potential as a powerful jamming strategy. The constant jamming strategy, while less effective than the intelligent jamming strategy, still had a noticeable impact. The random strategy's effects were more variable. These results buttressed the need for robust security measures in 5G communication systems to mitigate the effects of jamming attacks. This study provides valuable insights for network designers and engineers, emphasizing the importance of considering various jamming strategies when evaluating/designing robust and resilient 5G communication systems.

RECOMMENDATIONS

Future research could explore additional jamming strategies and their impact on different types of wireless networks, as well as develop advanced mitigation techniques to counteract these attacks. Based on the findings, it is recommended that 5G communication systems incorporate advanced detection and mitigation techniques such as adaptive signal processing algorithms, machine learning-based detection methods, dynamic frequency hopping strategies and more to counteract intelligent jamming attacks.

REFERENCES

Agiwal, M., Roy, A., & Saxena, N. (2016). Next generation 5G wireless networks: A comprehensive survey. *IEEE communications surveys & tutorials*, 18(3), 1617-1655.

Abhishek, N. V., & Gurusamy, M. (2021). JaDe: Low power jamming detection using machine learning in vehicular networks. *IEEE Wireless Communications Letters*, 10(10), 2210-2214.

Arjoune, Y., & Faruque, S. (2020, December). Real-time machine learning based on hoeffding decision trees for jamming detection in 5G new radio. In 2020 IEEE International Conference on Big Data (Big Data) (pp. 4988-4997). IEEE.

Arjoune, Y., & Faruque, S. (2020, January). Smart jamming attacks in 5G new radio: A
review. In 2020 10th annual computing and communication workshop and conference (CCWC) (pp. 1010-1015). IEEE.

Birutis, M. A., & Mykkeltveit, A. (2022). Practical jamming of a commercial 5G radio system at 3.6 GHz. *Procedia Computer Science*, 205, 58-67.

Bousalem, B., Sakka, M. A., Silva, V. F., Jaafar, W., Letaifa, A. B., & Langar, R. (2023, October). DDoS attacks mitigation in 5G-V2X networks: A reinforcement learning-based approach. In 2023 19th International Conference on Network and Service Management (CNSM) (pp. 1-5). IEEE.

Do, T. T., Björnson, E., Larsson, E. G., & Razavizadeh, S. M. (2017). Jamming-resistant receivers for the massive MIMO uplink. *IEEE Transactions on Information Forensics and Security*, 13(1), 210-223.

Grover, K., Lim, A., & Yang, Q. (2014). Jamming and anti–jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing*, 17(4), 197-215.

Gupta, A., & Jha, R. K. (2015). A survey of 5G network: Architecture and emerging technologies. *IEEE access*, 3, 1206-1232.

Haykin, S. (2008). Communication systems. John Wiley & Sons.

Isaac, S., Ayodeji, D. K., Luqman, Y., Karma, S. M., & Aminu, J. (2024). CYBER SECURITY ATTACK DETECTION MODEL USING SEMI-SUPERVISED LEARNING. FUDMA JOURNAL OF SCIENCES, 8(2), 92-100.

Karagiannis, D., & Argyriou, A. (2018). Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning. *vehicular communications*, 13, 56-63.

Kekirigoda, A., Hui, K. P., Cheng, Q., Lin, Z., Zhang, J. A., Nguyen, D. N., & Huang, X. (2019, November). Massive MIMO for tactical ad-hoc networks in RF contested environments. In MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM) (pp. 658-663). IEEE.

Krayani, A., Barabino, G., Marcenaro, L., & Regazzoni, C. (2023, March). Integrated sensing and communication for joint gps spoofing and jamming detection in vehicular v2x networks. In 2023 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-7). IEEE.

Li, W., Chen, J., Liu, X., Wang, X., Li, Y., Liu, D., & Xu, Y. (2022). Intelligent dynamic spectrum anti-jamming communications: A deep reinforcement learning perspective. *IEEE Wireless Communications*, 29(5), 60-67.

Lichtman, M., Rao, R., Marojevic, V., Reed, J., & Jover, R. P. (2018, May). 5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation. In 2018 IEEE international conference on communications workshops (ICC Workshops) (pp. 1-6). IEEE.

Pelechrinis, K., Iliofotou, M., & Krishnamurthy, S. V. (2010). Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications surveys & tutorials*, 13(2), 245-257.

Strasser, M., Danev, B., & Čapkun, S. (2010). Detection of reactive jamming in sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 7(2), 1-29.

Tiwari, P., Gahlaut, V., Kaushik, M., Rani, P., Shastri, A., & Singh, B. (2023). Advancing 5G connectivity: a comprehensive review of MIMO antennas for 5G applications. International Journal of Antennas and Propagation, 2023(1), 5906721.

Tiamiyu, O. A. (2013). An Overview of Modern Telecommunication Networks Security Challenges. National Security and Strategic Planning (Национальнная Безопасность и Стратетическое Планирование). National Security and Strategic Planning (Национальнная Безопасность и Стратетическое Планирование), 2(2), 37-43.

Tsiota, A., Xenakis, D., Passas, N., & Merakos, L. (2019). On jamming and black hole attacks in heterogeneous wireless networks. *IEEE Transactions on Vehicular Technology*, 68(11), 10761-10774.

Vadlamani, S., Eksioglu, B., Medal, H., & Nandi, A. (2016). Jamming attacks on wireless networks: A taxonomic survey. *International Journal of Production Economics*, 172, 76-94.

Wang, Q., Nguyen, T., Pham, K., & Kwon, H. (2018). Mitigating jamming attack: A game-theoretic perspective. *IEEE Transactions on Vehicular Technology*, 67(7), 60636074.

Xu, W., Trappe, W., & Zhang, Y. (2008, March). Anti-jamming timing channels for wireless networks. In Proceedings of the first ACM conference on Wireless network security (pp. 203-213).

©2024 This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license viewed via https://creativecommons.org/licenses/by/4.0/ which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is cited appropriately.