5G Network Security Analysis

Nilay Malaviya
202151083
Computer Science and Engineering

Vedant Patel
202151112
Computer Science and Engineering

Raj Kashyap
202151128
Computer Science and Engineering

Vedant Shah
202151143
Computer Science and Engineering

Dev Parmar
202152327
Information Technology

***Abstract*—Rapid adoption of 5G technology brings unprecedented speed and connectivity, while introducing significant security challenges. This project simulates a virtual 5G environment to identify vulnerabilities and assess the resilience of 5G networks against cyber threats. The study focuses on common attack vectors, including eavesdropping, Denial-of-Service (DoS) attacks, and Man-in-the-Middle (MITM) attacks. Using NS3 and Wireshark, the project evaluates the behavior of the packets and provides information on how to mitigate these vulnerabilities. The results underscore the importance of robust encryption, authentication mechanisms, and real-time monitoring to secure 5G networks.**

***Index Terms*—5G, Cybersecurity, Network Simulation, Eavesdropping, DoS, MITM, NS3, Wireshark**

I. Introduction

The primary objective of this experiment is to analyze the security vulnerabilities in 5G networks by simulating common cyberattacks using the ns-3 network simulator. The focus is on three major attacks: Eavesdropping, Denial of Service (DoS), and Man-in-the-Middle (MITM). These attacks were evaluated on a virtual 5G mmWave network setup, designed to replicate real-world scenarios.

The experiment involved setting up a 5G network using ns-3, a discrete-event network simulator, to model a mmWave-based communication system. This setup includes key network elements such as eNodeBs (evolved NodeBs), User Equipment (UEs), and a Packet Gateway (PGW), all connected in a simulation environment.

II. Project Methodology

A. 5G Virtual Environment Creation

The foundation of this research was the creation of a simulated 5G virtual environment using NS3, a discrete-event network simulator widely used for research purposes. The following steps outline the process for setting up the 5G network and integrating attack simulations.

1) Setting Up the Environment: To simulate the 5G environment, we leveraged the NS3-mmWave module, which supports high-frequency communication modeling and mimics realistic 5G network behavior. The mmWave module was cloned and integrated into the NS3 framework for this purpose.

Key Steps:

- **Repository Setup:** The project files and necessary scripts were cloned from the repository to the local machine.
- **Dependencies Installation:** All dependencies required for the NS3 environment, such as the GNU compiler, Python bindings, and relevant libraries, were installed.
- **Wireshark Installation:** Wireshark was used to monitor and analyze the network traffic, providing insights into packet exchanges during simulation.

2) Network Configuration: The virtual 5G network was configured to simulate a realistic environment, consisting of User Equipment (UEs), eNodeBs (base stations), and a Packet Gateway (PGW).

Key Configurations:

- **Base Stations and UEs:** Nodes were equipped with realistic mobility models to reflect varying distances and positions between UEs and eNodeBs.
- **Packet Capture (PCAP):** Network traffic was recorded during the simulation for further analysis.
- **Routing and Connectivity:** Static routing configurations ensured smooth communication between components.

Configuration Commands:

```
./ns3 configure --enable-examples --enable-test
./ns3 build
```

3) Network Design and Simulation Setup: The topology included one or more eNodeBs, UEs, and an attacker node to test vulnerabilities. This setup used the following modules and parameters:

- **Mobility Models:** UEs and attacker nodes were placed at variable distances, using a random uniform distribution to replicate realistic deployments.
- **Data Flow Simulation:** Traffic between UEs and eNodeBs was generated using UDP packets, with parameters such as packet size and transmission intervals adjusted for different scenarios.

The **attack simulation scripts** were integrated into the NS3 environment to enable seamless execution of various attack vectors.

4) Capturing Network Activity: Wireshark and NS3's built-in tracing tools were used to record and analyze network traffic. This allowed us to observe packet flow and identify anomalies caused by attacks. PCAP files generated during the simulation provided detailed insights into packet-level activities.

Thus, the simulation environment adheres to the principles of 5G architecture, which include ultra-high data rates, low latency, and improved connectivity. The mmWave module mimics the physical and MAC layers of 5G, supporting:

- High-frequency wave propagation.
- Beamforming and directional communication.
- Resource allocation and interference modeling.

This realistic representation makes the simulation environment a reliable tool for testing security vulnerabilities, particularly for the high-throughput, low-latency demands of 5G.

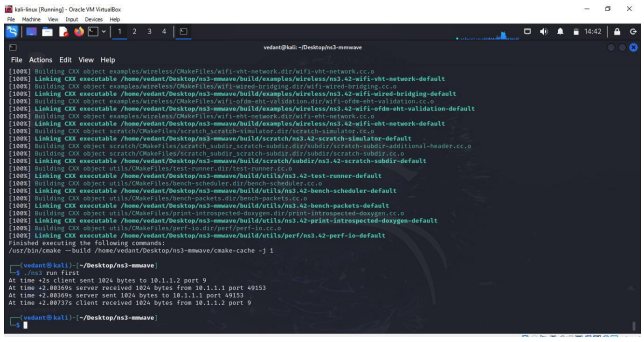

Fig. 1. Setting up network and running test virtual network

B. Eavesdropping

Eavesdropping is a passive attack where an attacker intercepts and listens to the communication between nodes in a network without altering the data being transmitted. The attacker merely collects information, often in the form of packets, and uses it for unauthorized purposes.

Eavesdropping in a network context refers to the act of intercepting and capturing data packets transmitted over the network. The objective is to gain access to information being exchanged between network entities, such as user equipment (UE) and base stations (eNodeBs), without the knowledge of the communicating parties. In a 5G environment, eavesdropping can target the wireless communication channels, which are particularly vulnerable due to their shared medium. The study of eavesdropping is critical for understanding security vulnerabilities, analyzing traffic patterns, and assessing the effectiveness of encryption mechanisms.

We performed eavesdropping to test the ability to intercept 5G communication in a simulated environment, analyze the effectiveness of encryption in preventing sensitive data leakage and understand traffic patterns to identify potential weaknesses in data transmission.

```
206     // Enable PCAP tracing for eNB and UE nodes using p2ph.EnablePcap
207     p2ph.EnablePcap("mmwave-enb", enbmmWaveDevs.Get(0));
208     p2ph.EnablePcap("mmwave-ue", uemmWaveDevs.Get(0));
209
210 // Enable PCAP tracing for the P2P link between PGW and remoteHost
211     p2ph.EnablePcap("mmwave-epc-pgw", internetDevices.Get(0));
212     p2ph.EnablePcap("mmwave-epc-remote", internetDevices.Get(1));
```

Fig. 2. Code snippet for capturing packets

A socket was configured on the attacker node to capture packets being transmitted between the UE and eNB. Despite simulating packet sniffing to intercept data between nodes, no sensitive information or vulnerabilities were identified during the eavesdropping attack.

C. Denial-of-Service (DoS) Attacks

A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal functionality of a network or service by overwhelming it with a massive volume of traffic or resource requests. The primary goal of a DoS attack is to deny legitimate users access to the targeted network, system, or service by consuming its resources, thereby causing service disruptions, downtime, or severely degraded performance. DoS attacks are categorized into several types based on the nature of the attack such as Volume based, Protocol based and Application-layer attacks.

In our experiment, we focus on a Volume-based DoS attack. The basic principle behind a Volume-based DoS attack is to flood the network with a massive amount of traffic, overwhelming the available bandwidth and thereby exhausting the network's resources. The attack does not require exploiting vulnerabilities within the protocols or applications; rather, it is simply a matter of saturating the network's infrastructure with more traffic than it can handle.

In the context of a 5G network, the effects of a Volume-based DoS attack can be particularly detrimental. 5G networks rely on high-speed communication and low latency to offer advanced services such as autonomous driving, smart cities, and real-time data transmission. By sending a large number of packets over the network, the attacker aims to exhaust the available bandwidth, causing high network congestion, latency, and loss of connectivity. The target can be a 5G base station (eNodeB), the User Equipment (UE), or even the entire core network.

The network's max capacity for simulation was 100Gbps so we increased the bandwidth and we also increased the packet size to maximum. We then tried to populate the network by increasing the User Equipments and the attacker nodes which can congest the network.

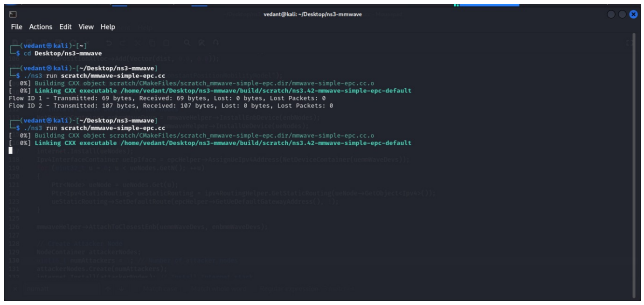

Fig. 3. Simulating DoS first by Increasing Network load and then by populating it.

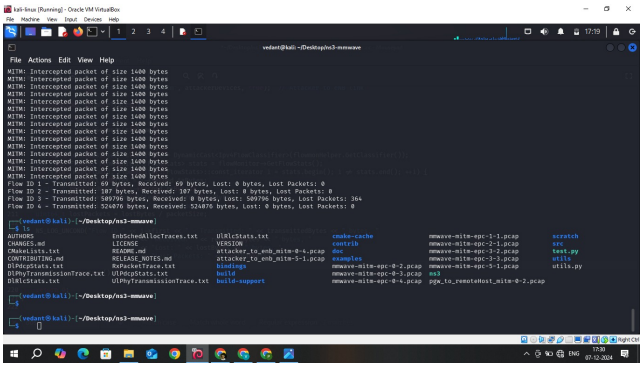

Fig. 4. Simulating the MITM attack

D. Man-in-the-Middle (MITM) Attacks

A Man-in-the-Middle (MITM) attack occurs when a malicious actor intercepts communication between two parties without their knowledge, potentially altering the data being exchanged. The attacker positions themselves between the sender and receiver, acting as a relay to eavesdrop, manipulate, or steal sensitive information. There are two primary types of MITM attacks: passive interception, where the attacker silently listens to the communication, and active interception, where the attacker modifies the data. These attacks exploit vulnerabilities such as weak encryption, poor authentication mechanisms, or outdated protocols.

In the context of 5G networks, MITM attacks can have severe consequences. 5G networks are designed to support high-speed communication, low latency, and highly sensitive applications like autonomous vehicles, remote surgery, and smart city infrastructure. A MITM attack can compromise these services by altering critical communications, causing loss of trust, financial loss, or even harm to human life in the case of mission-critical applications.

It exploit vulnerabilities in network protocols, encryption schemes, or authentication mechanisms used by communicating parties. These attacks are facilitated by weak or outdated encryption, which allows attackers to decrypt sensitive data if the encryption keys are guessable or vulnerable to brute-force attacks. Poor authentication mechanisms also enable attackers to impersonate legitimate participants, intercepting or modifying communication. Insecure protocols, such as those in older systems or improperly implemented Diffie-Hellman key exchanges, provide further opportunities for MITM attacks, where attackers can manipulate the key exchange process and gain access to the communication without detection.

One of the famous Example is of when MITM is the attack performed on Diffie Hellman key exchange algorithm. Where the attacker without knowing the secret key of the Alice and Bob can read and modify their communication.

In order to simulate MITM attack we have created on attacker node which knows the IP address of the UE and eNB. Whenever the packets are transmitted between them the attacker can read the packet and forward it.

III. Results and Observations

A. Eavesdropping

During the simulation, no significant flaws were observed in the eavesdropping scenario. The attacker was unable to successfully intercept any meaningful communication between the nodes, suggesting that the network was secured against passive attacks in this specific setup.

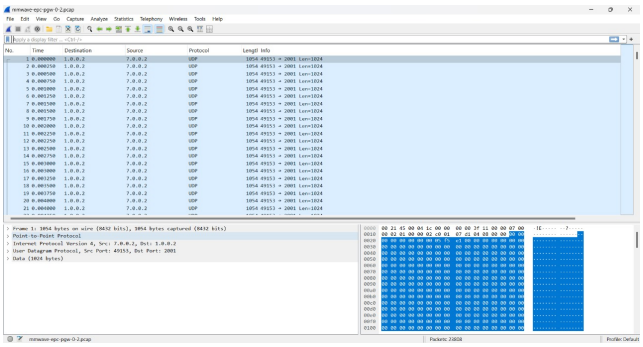

Fig. 5. Analzing packets captured during eaves dropping in wireshark

Some of the results obtained from this attack are as follows:

All captured packets were encrypted, ensuring that no sensitive user data or control information was accessible in plaintext.

Analysis of the captured data revealed distinct traffic patterns, such as packet sizes and inter-arrival times, which could potentially be used for traffic analysis attacks.

The encryption mechanisms employed in 5G communication proved to be effective in preventing unauthorized access to sensitive data.

The presence of strong encryption significantly reduced the effectiveness of the eavesdropping attack, highlighting the importance of secure cryptographic protocols in 5G networks.

While the payload was encrypted, metadata such as packet headers and timing information remained visible, which could still be exploited for certain types of attacks.

Observing the timing and size of packets, an attacker could perform a traffic analysis attack to infer details about user activity or application usage, even without access to the encrypted payload.

Packet headers, which include source and destination IP addresses, port numbers, and protocol types, were accessible despite encryption. This could allow attackers to map communication endpoints or infer relationships between network entities.

B. Denial-of-Service (DoS) Attacks

When the network load was increased by modifying packet sizes and transmission speeds, no significant packet loss or performance degradation was observed initially. The 5G network demonstrated robustness in handling heavy traffic, showcasing its ability to manage high throughput demands efficiently.

Introducing multiple attacker nodes that sent high volumes of malicious traffic caused notable degradation in network performance. The symptoms of network disruption included:

- **Increased Latency:** Communication delays were observed as legitimate packets experienced congestion at bottleneck points.
- **Reduced Throughput:** The average throughput for legitimate users dropped significantly due to resource exhaustion caused by attacker nodes.

The attack resulted in resource starvation, where network resources (e.g., bandwidth and processing power) were consumed by the attacker nodes, leaving limited capacity for legitimate traffic. This effect became more pronounced as the number of attacker nodes and the volume of attack traffic increased.

At peak attack conditions, the network became unusually slow and nearly unusable for legitimate users. Simulated applications, such as video streaming or file transfers, experienced severe interruptions, emphasizing the impact on quality of service (QoS).

The attacker nodes successfully overwhelmed specific network segments, validating the vulnerability of unprotected or poorly configured network layers to DoS attacks.

C. Man-in-the-Middle (MITM) Attacks

In this experiment, we set up a virtual network where an attacker node positioned itself between the eNB and UE. The attacker node successfully intercepted packets transmitted between User Equipment (UE) and the core network. Captured packets contained both control and data plane traffic, demonstrating the feasibility of traffic interception in the absence of proper encryption.

The intercepted packets were analyzed to understand their structure and content. Without proper encryption, sensitive information such as IP addresses, session details, and unencrypted payloads could be extracted.

The attacker node was able to alter the intercepted packets before forwarding them to their intended destination. This demonstrated the potential for data tampering, which could disrupt communication or inject malicious content into the network.

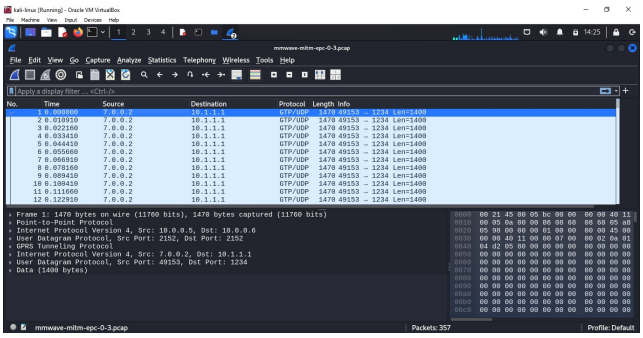

Fig. 6. Analyzing packets captured during MITM attack in wireshark

Modifications introduced by the attacker node caused noticeable delays in communication between UEs and the core network. These delays could degrade the Quality of Service (QoS), particularly in latency-sensitive applications such as video streaming or real-time gaming.

Redirecting traffic through the attacker node introduced inconsistencies in routing, leading to packet loss and reduced throughput. The attack simulated scenarios where legitimate packets were dropped or duplicated, further disrupting the network.

IV. Conclusion and Future Work

In this project, we simulated a virtual 5G network using the NS-3 simulator to analyze potential vulnerabilities and evaluate the resilience of the network against different types of attacks: Eavesdropping, Denial-of-Service (DoS), and Man-in-the-Middle (MITM). The key findings and takeaways

are as follows:

A. Eavesdropping

The eavesdropping simulation highlighted critical vulnerabilities in 5G networks where unencrypted data transmissions could be intercepted and analyzed by malicious entities. While packet capture and traffic analysis were successful in identifying control and data plane traffic, no sensitive or meaningful information could be extracted due to encryption. This reinforces the importance of securing both user and signaling data. The study demonstrated that while modern encryption methods protect data confidentiality, any lapse in implementation leaves the network exposed to privacy breaches and potential exploitation.

Future research should focus on enhancing encryption techniques and implementing advanced security protocols like quantum cryptography to safeguard data in 5G networks. Additionally, employing real-time traffic anomaly detection and deep packet inspection techniques could further mitigate eavesdropping risks. Simulating more complex attack scenarios and testing the robustness of security mechanisms under diverse network conditions will provide deeper insights into potential vulnerabilities and solutions for next-generation networks.

B. Denial of Service (DOS)

The Denial of Service (DoS) attack simulation on the 5G network highlighted the network's susceptibility to congestion and service degradation under excessive traffic load. Increasing the network's packet size and speed did not cause packet loss or noticeable flaws; however, when the network was populated with attacker nodes and UEs, the performance of the network significantly deteriorated. This suggests that while the network can handle typical traffic loads, the introduction of malicious entities can severely impact network efficiency and result in service disruptions. The findings underscore the importance of traffic management and anomaly detection to defend against such attacks in real-world implementations.

Future work should focus on enhancing network resource allocation and optimization strategies to mitigate the impact of DoS attacks. The use of intrusion detection systems (IDS) and traffic filtering mechanisms could be explored to identify and isolate malicious traffic before it causes network congestion. Additionally, investigating the integration of AI-driven anomaly detection systems could provide adaptive defense mechanisms, allowing the 5G network to maintain performance even during high traffic conditions. More comprehensive simulations with larger-scale networks and advanced attack strategies will be beneficial for assessing and strengthening DoS resilience.

C. Man in the Middle Attack

The Man-in-the-Middle (MITM) attack simulation successfully demonstrated how an attacker can intercept, manipulate, and monitor communications between two legitimate nodes in a 5G network. Through packet sniffing and relay, the attacker was able to capture and potentially modify the data exchanged, highlighting critical vulnerabilities in the network's security mechanisms. Despite the implementation of encryption protocols, the simulation showed that without additional safeguards, the network remains vulnerable to MITM attacks. This emphasizes the need for stronger encryption, secure authentication protocols, and traffic integrity verification to prevent unauthorized access and data tampering in a 5G environment.

Future work in mitigating Man-in-the-Middle attacks should focus on implementing end-to-end encryption with more robust authentication mechanisms, such as public key infrastructure (PKI) and mutual authentication. Additionally, integrating network traffic monitoring systems capable of detecting suspicious activities or inconsistencies in communication patterns could further enhance security. The exploration of advanced cryptographic techniques, such as quantum key distribution (QKD), could provide next-generation security solutions for 5G networks. Further research could also involve simulating more complex attack scenarios to evaluate the effectiveness of these mitigation strategies and ensure the overall resilience of the network.

Overall, the project has provided valuable insights into the security challenges of 5G networks. It also highlighted the critical need for robust security mechanisms to safeguard network performance and user data against potential threats. The experiment-based approach reinforced the understanding of 5G vulnerabilities, paving the way for further research and development of advanced security measures in next-generation networks.

V. Project Contribution

The project was a collaborative effort, with each team member contributing to specific aspects of the research and implementation:

- **Nilay Malaviya:** Helped set up the MITM attack code and analyzed intercepted packets for vulnerabilities, ensuring an accurate representation of the attack. Additionally, he contributed to the overall network security analysis, focusing on attack scenarios and vulnerabilities in the simulation.
- **Vedant Patel:** Simulated and implemented the MITM attack, refining its execution for optimal results and logging intercepted data. He also collaborated with the team on identifying attack strategies that could affect the 5G simulation. He also assisted in creating the documentation.
- **Raj Kashyap:** Configured the initial 5G setup using ns-3, focusing on protocol configurations and the eavesdrop-

ping simulation. He also ensured that the network topology was realistic and supported the required simulations for packet capture.

- **Vedant Shah:** Monitored and validated overall network performance during attack simulations, focusing on DoS metrics and logging. He further analyzed the impact of DoS attacks on network latency and the availability of the 5G environment. He also contributed in creating the whole documentation and establishing communication among the team members.
- **Dev Parmar:** Supported simulation runs, conducted performance evaluations, and performed packet analysis of results in Wireshark. He also assisted with effectively communicating the results in a timely manner.

VI. ACKNOWLEDGMENT

We extend our heartfelt gratitude to our professor, Dr. Bhupendra Kumar, for their invaluable guidance, constant encouragement, and insightful feedback throughout the course of this project. Their expertise and unwavering support have been instrumental in shaping our understanding and refining our approach. We are sincerely grateful for the opportunities and resources provided, which greatly contributed to the successful completion of this work.

VII. GITHUB REPO AND VIDEO LINKS

Please find below the project's github repository and presentation video link.

- 5G Network Security Analysis Github Repo
- 5G Network Security Analysis Video

REFERENCES

[1] NS3 Official Documentation
[2] Wireshark User Guide
[3] MMwave Github Repository
[4] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G Security: Analysis of Threats and Solutions," Centre for Wireless Communications, University of Oulu, Finland, pp. 193-198
[5] M. Humayun, B. Hamid, N. Z. Jhanjhi, G. Suseendran, and M. N. Talib, "5G Network Security Issues, Challenges, Opportunities and Future Directions: A Survey", pp. 2-6