**Research on Existing Security Solutions & Identifying Gaps in 5G Network Slicing Security**

**1. Existing Security Solutions for 5G Network Slicing**

To secure 5G slices, several companies and research institutions have developed **security frameworks** leveraging **SDN, NFV, deep packet inspection (DPI), and traditional security policies**. However, **most existing solutions rely on static rule-based security**, which is insufficient against **evolving cyber threats**.

Below is a comparison of **leading security solutions for 5G slicing**:

|  |  |  |
| --- | --- | --- |
| Solution | Description | Limitations |
| Ericsson 5G Security | Implements slice-specific security policies and **basic threat detection mechanisms**. | Designed primarily for **enterprise security**, lacks real-time **AI-driven detection**. |
| Huawei 5G Core Security | Uses **SDN-based security policies** for network slice isolation. | Lacks **AI-based anomaly detection**, **rule-based approach** limits adaptability to new attack patterns. |
| Nokia NetGuard Security | Uses **deep packet inspection (DPI)** for real-time **security monitoring** of 5G slices. | DPI **introduces high processing overhead**, making it unsuitable for low-latency applications. |
| OpenDaylight SDN Security | Provides **dynamic network control** and **security policy enforcement** for slices. | **No integration with AI**, lacks **real-time threat analysis**. |

**Key Observations:**

* **Most solutions use static, rule-based security** that is not effective against evolving threats.
* **AI-based, real-time anomaly detection is missing** in most current solutions.
* **Existing frameworks do not integrate SS7 security**, despite SS7 vulnerabilities being a known risk in legacy interconnections.

**2. Existing Security Solutions for SS7 Protection**

While **5G Core uses Diameter and HTTP/2 for signaling**, SS7 remains relevant due to its **role in 2G/3G/4G interconnections**. Several **SS7 security solutions** exist, but they are **not integrated with 5G slice security**.

|  |  |  |
| --- | --- | --- |
| Solution | Description | Limitations |
| AdaptiveMobile SS7 Firewall | Monitors and **blocks suspicious SS7 requests** (e.g., location tracking, SMS hijacking). | Does not integrate **5G slice security**. |
| Positive Technologies SS7 Protection | Uses **pattern recognition** to detect **SS7-based attacks** like location tracking and call/SMS redirection. | **Lacks real-time AI-based threat analysis**. |
| GSMA SS7 Security Guidelines | Provides **recommendations** for securing SS7 interconnections in 5G networks. | **Only guidelines**, does not provide **active security solutions**. |

**Key Observations:**

* **Current SS7 security tools focus only on filtering traffic**, rather than detecting advanced SS7-based attacks.
* **No integration exists between SS7 security and 5G slice security**.
* **A unified security framework for both SS7 and 5G slicing is missing**.

**3. Identifying Gaps in Existing Security Solutions**

Based on the research, **current solutions have several weaknesses**, which this project will address.

| **Existing Weakness** | **Project’s Contribution** |
| --- | --- |
| **No real-time AI-powered anomaly detection for 5G slices.** | Implement AI-driven **real-time monitoring** to detect **cross-slice attacks and SS7 threats**. |
| **No automated response mechanisms for threats.** | Develop a system that **isolates compromised slices dynamically** upon detecting an attack. |
| **SS7 security is not integrated with 5G slice security.** | Create a **unified framework** that **secures both SS7 signaling and 5G network slicing**. |
| **Existing solutions rely too much on DPI and static filtering.** | Use **machine learning-based anomaly detection** instead of just rule-based filtering. |

**Key Takeaways:**

**AI-driven detection is crucial to overcome the limitations of static rule-based security.**  
 **A real-time response system is necessary** to prevent attacks from spreading across slices.  
 **SS7 security must be integrated into 5G slice protection** to prevent inter-network attacks.

**4. How This Project Innovates Beyond Existing Solutions**

This project introduces **three major innovations** compared to existing 5G security solutions.

**A. AI-Driven Anomaly Detection**

**Unlike traditional rule-based security**, this project will use **machine learning (ML) and deep learning** for **real-time detection of threats**.

🔹 **Proposed AI Models:**

* **Unsupervised Learning (Autoencoders, Isolation Forests):** Detects **zero-day attacks** and **unknown anomalies** in network traffic.
* **Supervised Learning (Decision Trees, SVMs):** Classifies **known attack patterns** in slice traffic.
* **Reinforcement Learning (RL):** **Adapts security policies dynamically** based on attack behavior.

**B. Integrated SS7 & 5G Security**

**Unlike existing SS7 firewalls that only filter traffic**, this framework will:

* **Detect SS7-based attacks before they affect 5G slices.**
* **Secure both SS7 signaling and network slicing** to prevent inter-slice threats.
* **Monitor SS7-based SMS hijacking and call forwarding attacks** in real-time.

**C. Automated Threat Response & Dynamic Slice Isolation**

**Unlike current solutions that just issue alerts**, this system will **automatically mitigate threats**.

|  |  |
| --- | --- |
| Threat Type | Automated Response Actions |
| Cross-Slice Attack | **Isolate compromised slice, block unauthorized traffic, adjust SDN policies**. |
| Unauthorized Access Attempt | **Trigger Multi-Factor Authentication (MFA), suspend suspicious accounts**. |
| SS7 Location Tracking Attack | **Block unauthorized SS7 location queries, log attack sources**. |
| SMS Hijacking Attempt | **Redirect SMS authentication to app-based MFA, notify users of possible compromise**. |
| Call Interception Attack | **Encrypt calls, block unauthorized call redirections**. |
| DDoS Attack on a Slice | **Rate-limit traffic, shift high-priority services to redundant slices, blacklist malicious sources**. |

**Key Innovations:**

**Uses AI to detect threats in real-time instead of static filtering.**  
 **Integrates SS7 security with 5G slice security** for a holistic approach.  
 **Automatically isolates compromised slices** to prevent attack spread.

**5. Resources**

To support this research, the following resources will be used:

**Research Papers & Articles**

* **GSMA 5G Security Guidelines** (gsma.com)
* **IEEE Paper: "Security Challenges in 5G Network Slicing"** ([ieeexplore.ieee.org](https://ieeexplore.ieee.org/document/10242032))
* **Whitepaper: "AI for 5G Cybersecurity" (Ericsson)** (ericsson.com)

**Videos & Webinars**

* **YouTube: "Why AI is Needed for 5G Security"** ([youtube.com](https://www.youtube.com/watch?v=5GRuGp6aGmo))
* **Webinar: "5G Security Threats & Countermeasures"** ([5gsecuritywebinar.com](https://www.5gsecuritywebinar.com))