**Literature Survey**

**Team:** F-33

**Paper 1: 5D-NIDD: A comprehensive network Intrusion detection dataset generated over 5G Wireless network**

The abstract highlights the increasing complexity of 5G technology, posing challenges due to its sophistication and susceptibility to intelligent attacks facilitated by machine learning (ML) and artificial intelligence (AI). The authors advocate for proactive security measures to counter these threats and introduce the 5G-NIDD dataset for implementing AI/ML solutions. The introduction shifts to the evolution towards 6G, emphasizing intelligence integration into wireless connections and amplifying security risks. The necessity for real-time, adaptable security measures is stressed, alongside the lack of suitable datasets reflecting complex network behaviors. The 5G-NIDD dataset, developed in Oulu, Finland, is presented as a solution due to its real-world network scenario representation and integration of various attack scenarios and benign traffic, allowing for the application of multiple ML techniques.

The background and related work section discusses the inadequacies of existing threat detection mechanisms for 5G and 6G networks. Conventional signature-based methods are deemed ineffective against novel threats, while ML-based approaches require extensive data for accurate results. Existing datasets like DARPA, KDD, and DEFCON are criticized for their lack of relevance, redundancy, and inability to reflect real-time conditions. The authors stress the importance of high-quality datasets for accurate ML-based intrusion detection.

Furthermore, the research paper discusses different types of attacks, mainly focusing on Denial of Service (DoS) attacks and Port Scans, which are common threats in 5G networks. DoS attacks aim to slow down or completely block legitimate users' access to a network or device by overwhelming them with traffic. Various DoS attacks include ICMP Flood, UDP Flood, SYN Flood, HTTP Flood, and Slowrate DoS. Each attack targets different aspects of the network or applications. Additionally, Port Scans are used to identify open ports on a target system, which attackers can exploit for further attacks. The paper discusses different port scans like SYN Scan, TCP Connect Scan, and UDP Scan, each with its method of identifying open ports. The research uses tools like Hping3, Goldeneye, and Nmap to simulate these attacks and scans for evaluation purposes.

**Paper 2: AI\_and\_6G\_Security\_Opportunities\_and\_Challenges**

The paper explores the integration of Artificial Intelligence (AI) to secure 6G networks, emphasizing proactive threat discovery, mitigation techniques, and overall security. It discusses the transition from softwarization/cloudification to intelligentization in network architecture and the critical role of AI in achieving "connected intelligence" in 6G. The introduction underscores the necessity of sophisticated security mechanisms to meet the demands of future wireless applications.

The security threat landscape of 6G is delineated, covering pre-6G security issues, the security of 6G architecture, and 6G technologies. It highlights challenges such as the denser deployment of cells, mesh networks, and the reliance on AI, exposing vulnerabilities to attacks like data manipulation and privacy breaches. Strategies, including hierarchical security mechanisms and blockchain integration, are proposed to mitigate these threats.

The paper delves into AI's role in enhancing security and privacy in 6G systems, addressing pre-6G security issues, security within 6G architecture, and technology-specific security measures. Techniques like deep reinforcement and federated learning are suggested for intrusion detection and privacy preservation. Furthermore, it discusses security and privacy concerns in AI systems, proposing countermeasures like adversarial machine learning and federated learning to mitigate threats. Ethical considerations regarding fully automated AI-based networks, potential AI-based attacks on 6G networks, and corresponding defense mechanisms are also examined.

In conclusion, the paper advocates integrating AI into 6G networks to bolster security and privacy measures. It offers insights into challenges and opportunities in implementing intelligent security measures in 6G systems and suggests future research directions.

**Paper 3: A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems**

This research paper discusses what the next generation of cell phone networks, called 6G, might look like. While some improvements will come naturally from the current network, new ideas like better ways to talk between phones and smart surfaces that talk to implants in our bodies will need exploring. The paper gives five suggestions for making 6G a reality: making phones work better at super-high frequencies, changing how we design the whole network, focusing on different kinds of applications instead of just making things faster, using smart surfaces more, and improving how we measure the network's performance. Overall, it's a big plan for making cell phones even better in the future.

In essence, this paper guides researchers and industry experts in navigating the terrain of future wireless networks, offering insights into the diverse array of challenges and opportunities. By proposing forward-thinking recommendations and highlighting the need for interdisciplinary collaboration, it aims to steer the trajectory of 6G development towards enhanced performance and greater adaptability to the evolving needs of society.

**Paper 4: Robust and Resilient Federated Learning for Securing Future Networks**

This paper proposes a defense mechanism in case of an adversarial attack via adding noise; we explore this facet of 5g network intrusion too.

Proposed Defense Mechanisms: Recent studies have proposed innovative defense mechanisms to augment existing FL security measures. These mechanisms often leverage advanced techniques, such as threshold-based clustering, to enhance the detection and mitigation of malicious activities within FL environments. Additionally, researchers have conducted comprehensive analyses to evaluate the efficacy of proposed defense strategies under varying attack scenarios, shedding light on their practical applicability and performance metrics.

Future Research Directions: The literature emphasizes the importance of ongoing research efforts to address the evolving threat landscape surrounding FL security. Future research endeavors aim to explore novel grouping strategies for attackers, optimize noise insertion techniques, and investigate dynamic defense mechanisms capable of adapting to sophisticated poisoning attacks in real time. Moreover, a growing emphasis is on collaborative research initiatives supported by funding agencies and industry partners to advance state-of-the-art FL security.

In conclusion, this paper provides a comprehensive overview of the research landscape surrounding Federated Learning in telecommunications, focusing on security challenges, defense mechanisms, and avenues for future research. This review sets the stage for continued exploration and innovation in securing future networks against emerging threats by synthesizing existing knowledge and identifying critical research gaps.