Contribution ID: **199** Type: **Poster**

Mobile Network Security: Challenges, Vulnerabilities, and Future Directions

Mobile communication networks have progressed rapidly, from 2G and 3G to 4G and now 5G, with work already underway toward 6G systems. Each generation has brought faster data speeds, reduced latency, and new applications such as video streaming, cloud services, and the Internet of Things (IoT). These advancements have changed the way people connect and businesses operate, but they have also introduced a wide range of security issues that cannot be overlooked. In earlier systems like 2G and 3G, the main problems were weak encryption, poor authentication, and vulnerability to eavesdropping and SIM cloning. The shift to 4G, with its all-IP architecture, offered much better connectivity but also exposed networks to internet-based threats such as denial-of-service attacks, man-in-the-middle interception, and IP spoofing. New challenges also arose in signalling security, handover procedures, and identity protection. With the arrival of 5G, stronger encryption, mutual authentication, and technologies such as network slicing and software-defined networking have improved resilience. However, concerns remain, particularly with backward compatibility, the security of billions of IoT devices, and the risk of advanced cyberattacks. This study examines these security challenges across all generations of mobile networks. It reviews vulnerabilities in authentication, encryption methods, privacy-preserving techniques, and access control, while also analysing the potential of new approaches such as AI-driven intrusion detection and anomaly monitoring. The findings show that although each generation has improved security in some areas, persistent weaknesses remain, especially where older systems coexist with newer ones. Attackers often exploit downgrade flaws or insecure protocols from previous generations, making unified solutions essential. The research highlights the need for stronger cryptographic methods, better authentication protocols, and smarter detection systems, alongside global cooperation between network providers, device manufacturers, and policymakers. It also points to future research directions such as post-quantum cryptography and adaptive, scalable frameworks. Ultimately, the goal is to create mobile networks that are not only faster and more capable but also secure, reliable, and able to protect user privacy in an increasingly connected world.

Author: SANGEETHAM, sujithnarayana (JAIN (Deemed-to-be University))

Co-author: Mr NATARAJAN, VISHNU VENKATESH (JAIN (Deemed-to-be University))

Presenter: SANGEETHAM, sujithnarayana (JAIN (Deemed-to-be University))

Track Classification: Forensic Sciences