Keynote

Securing the Intelligent 6G Era: From AI-Driven Threats to Autonomous Resilience

6G is expected to become the first truly AI-native communication ecosystem, where intelligence is deeply embedded into network design, management, orchestration and service delivery. While this transformation will unlock unprecedented levels of automation, adaptability and efficiency, it will also expand the cyber threat landscape. Future 6G infrastructures will need to defend not only the network itself, but also the AI models, data pipelines and decision-making mechanisms that increasingly drive network operations. This keynote explores the emerging security challenges of the intelligent 6G era and argues that security must evolve from reactive protection to secure-by-design, autonomous and resilient-by-design architectures. It will discuss how AI can strengthen 6G security through anomaly detection, intrusion detection, threat intelligence, adaptive defence and automated response, while also examining the new vulnerabilities introduced by AI-driven systems, including adversarial manipulation, poisoning attacks, model inversion, model theft and trustworthiness concerns. The keynote will further highlight the need for autonomous cyber resilience in 6G, where networks are expected to anticipate threats, maintain critical services under attack or failure, recover rapidly from disruptions, and continuously adapt to dynamic operating conditions. In this context, explainable AI, trustworthy orchestration, zero-trust security models, distributed threat intelligence, and cross-domain resilience mechanisms will play a central role in building dependable 6G infrastructures. Aligned with the broader vision of European 6G-SNS projects, this keynote will present a forward-looking perspective on how intelligence, security and resilience must be co-designed to support trustworthy future networks. The talk will conclude by outlining key research directions toward self-defending, explainable and resilient 6G systems capable of securing both the network and the intelligence embedded within it.

Speaker Bio

Professor Madhusanka Liyanage is a Professor and Ad Astra Fellow at the School of Computer Science, University College Dublin (UCD), Ireland, where he leads the UCD Network Softwarization and Security Labs (NetsLab). His research focuses on the security, privacy and resilience of next-generation communication systems, with particular emphasis on 5G/6G security, AI and explainable AI for cybersecurity, federated learning, Open RAN, network softwarization, IoT, blockchain, and edge/cloud systems.

Prof. Liyanage has established an internationally recognised research profile in mobile network security and has authored more than 250 publications, including books, edited volumes and patents. He has received several prestigious recognitions, including the IEEE ComSoc Outstanding Young Researcher Award (EMEA), the IRC Research Ally Prize, and the SFI CONNECT Tom Brazil Excellence in Research Award. He has also been listed among the World's Top 2% Scientists and recognised as a Highly Cited Researcher.

He currently coordinates and contributes to several major national and European research initiatives in secure and intelligent future networks, including SHIELD-6G and other 6G-related projects. Prof. Liyanage is also an active contributor to the wider research and innovation community through his roles with ENISA, ETSI, and international collaborative research networks. His keynote and invited talks regularly address the future of trustworthy, explainable and resilient AI-native communication systems.