The AI Security Paradox: Protecting Networks with AI and Protecting AI in Networks

Madhusanka Liyanage *Senior Member, IEEE*
Assistant Professor/Ad Astra Fellow, School of Computer Science, University College Dublin, Ireland
Email: madhusanka@ucd.ie
Engin Zeydan, *Senior Member, IEEE,*
Centre Tecnològic de Telecomunicacions de Catalunya, Castelldefels, Barcelona, Spain, 08860.
Email: engin.zeydan@cttc.cat

I. Objectives, Motivation, Timeliness and Intended Audience

A. Objectives and Motivation

Artificial Intelligence (AI) and machine learning (ML) are rapidly transforming the landscape of modern telecommunications and network management. Networks today face an unprecedented scale of complexity, with billions of connected devices, dynamic traffic patterns, and sophisticated adversarial threats. At the same time, AI-driven systems are increasingly embedded in critical network infrastructure, making the security of AI systems themselves a matter of paramount importance. This tutorial addresses the dual relationship between AI and network security: how AI can be leveraged as a powerful tool to strengthen network security, and how networks must be secured to protect the AI systems that operate within them.

The first dimension of this tutorial, *AI for Network Security*, examines how AI and ML techniques can be applied to detect, prevent, and respond to network threats. Traditional rule-based and signature-driven security tools are increasingly outpaced by the volume, velocity, and variety of modern cyberattacks. AI-powered approaches, including deep learning-based intrusion detection, anomaly detection, federated learning for privacy-preserving threat intelligence sharing, and reinforcement learning for adaptive cyber defence, offer a new generation of tools capable of operating at network scale in real time. We will explore concrete use cases spanning intrusion detection systems (IDS), malware classification, network traffic analysis, and zero-trust architectures.

The second dimension, *Network Security for AI*, addresses the growing recognition that AI systems deployed in network environments are themselves vulnerable to a wide range of attacks. Adversarial machine learning, data poisoning, model inversion, and model stealing are just a few of the threat vectors that can compromise AI-driven network functions. As AI becomes the backbone of network automation, intelligent resource management, and autonomous network operations (e.g., in 5G, 6G, and Open RAN), ensuring the integrity, robustness, and trustworthiness of AI models is critical. This portion of the tutorial will discuss threat taxonomies specific to AI systems in networking contexts, as well as defences including adversarial training, differential privacy, robust aggregation, and explainable AI for anomaly accountability.

Together, this tutorial provides a comprehensive, balanced, and forward-looking perspective on the interplay of AI and network security, two of the most strategically important technical areas of our time. Attendees will leave with both a conceptual framework and practical insights applicable to research, standardisation, and industry deployment.

B. Timeliness and Intended Audience

1) Why is the topic current and important?: The intersection of AI and network security is among the fastest-growing areas in both academic research and industry practice. Several converging trends make this tutorial particularly timely. First, the proliferation of AI-native network architectures in 5G and the emerging 6G vision, including AI-driven RAN management, autonomous network slicing, and self-optimising networks, means that AI is no longer an optional enhancement but a fundamental component of next-generation network infrastructure. Second, the threat landscape has evolved dramatically: state-sponsored advanced persistent threats (APTs), ransomware-as-a-service, supply-chain attacks, and large-scale distributed denial-of-service (DDoS) campaigns are growing in frequency and sophistication. Traditional perimeter-based defences are insufficient; AI-powered, adaptive security mechanisms are now a necessity.

Third, the adversarial AI threat has moved from academic theory to practical reality. Recent incidents have demonstrated that ML models deployed in production environments can be manipulated through carefully crafted inputs, poisoned training data, or model extraction techniques, resulting in failures with potentially severe consequences in network contexts. Regulatory bodies, standardisation organisations (including ETSI, 3GPP, and ITU-T), and national cybersecurity agencies are increasingly publishing frameworks that address both the use of AI in security and the security of AI systems. This tutorial is therefore not only timely but essential for the community to navigate this rapidly evolving space.

2) Why the tutorial may attract a good number of attendees?: Both AI and network security are individually among the most popular research themes at major IEEE conferences. Their intersection amplifies interest considerably. Researchers working in network management and automation are increasingly aware that security is an inseparable concern;

likewise, the security community recognises that AI tools are becoming indispensable. This tutorial bridges the two communities, offering value to both.

This tutorial will be of key interest for:

- **Network Security Researchers:** Seeking to understand how ML and AI methods can augment or replace classical security tools such as firewalls, IDS/IPS, and SIEM systems, and how to evaluate the robustness of AI-driven security mechanisms.
- **AI and Machine Learning Researchers:** Interested in applying their expertise to high-impact, real-world network security problems, and in understanding the unique threat models and robustness requirements of networked deployment environments.
- **Network Operators and Service Providers:** Responsible for securing increasingly complex and softwarised network infrastructures, and looking to understand the practical deployment considerations of AI-based security tooling.
- **Standards and Policy Professionals:** Engaged in the development of AI security frameworks, responsible AI guidelines, and cybersecurity standards for telecommunications, including those active in ETSI, 3GPP, ITU-T, and national cybersecurity agencies.
- **Early-career Researchers and Graduate Students:** Looking to identify promising and impactful research directions at the intersection of AI and network security, and to build foundational knowledge in both domains.

No stringent prerequisites are required, though a foundational background in either networking or machine learning will help attendees get the most from the tutorial.

II. Name and a Short Biography of Each Tutorial Presenter

Dr. Madhusanka Liyanage received his Doctor of Technology degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. He is currently an assistant professor/Ad Astra Fellow and Director of Graduate Research at the School of Computer Science, University College Dublin, Ireland. He is also acting as an adjunct Processor at the Center for Wireless Communications, University of Oulu, Finland. He was also a recipient of the prestigious **Marie Skłodowska-Curie Actions Individual Fellowship** during 2018-2020. During 2015-2018, he has been a Visiting Research Fellow at the CSIRO, Australia, the Infolabs21, Lancaster University, U.K., Computer Science and Engineering, The University of New South Wales, Australia, School of IT, University of Sydney, Australia, LIP6, Sorbonne University, France and Computer Science and Engineering, The University of Oxford, U.K. He is also a senior member of IEEE. In 2020, he received the "**2020 IEEE ComSoc Outstanding Young Researcher**" award by IEEE ComSoc EMEA. In 2021, he was ranked among **the World's Top 2% Scientists (2020)** in List prepared by Elsevier BV, Stanford University, USA. Also, he was awarded a **Irish Research Council (IRC) Research Ally Prize** as part of the IRC Researcher of the Year 2021 awards for the positive impact he have made as a supervisor. He has co-authored over **125+ publications**, including four edited books with Wiley and one patent (Google Citations: 4000+, h-index : 30+). Moreover, He has received **two Best Paper Awards** for SDMN security (at NGMAST 2015) and 5G Security (at IEEE CSCN 2017). Additionally, he has been awarded two research grants and 19 other prestigious awards/scholarships during his research career. Liyanage has worked for more than fifteen EU, international and national projects in the ICT domain. In 2015, 2016, 2017, and 2018, he won the Best Researcher Award at the Centre for Wireless Communications, the University of Oulu, and the school of computer science in 2020 for his excellent contribution to project management and research activities. Additionally, two of the research projects (MEVICO and SIGMONA projects) received the **CELTIC Excellence and CELTIC Innovation Awards** in 2013, 2017, 2018 and 2021 respectively. He is also currently an **expert consultant** at European Union Agency for Cybersecurity (ENISA) for 5G security topics including Open RAN security and Privacy. In 2021, Liyanage was elevated as **Funded Investigator** of Science Foundation Ireland CONNECT Research Centre, Ireland. Moreover, he is an expert reviewer at different funding agencies in France, Qatar, UAE, Sri Lanka, and Kazakhstan. In addition, Madhusanka has been nominated as a **Named Supervisor** of the SFI Centre for Research Training in Machine Learning to supervise the doctoral students at the center. In addition, Madhusanka is a member of the Graduate School Board (GSB), College Graduate Research Forum and Equity, Diversity, and Inclusion (EDI) Committee at UCD. URL: http://madhusanka.com

Dr. Engin Zeydan is a Senior Researcher in the Services as networks (SaS) at Centre Tecnologic de Telecomunicacions de Catalunya (CTTC) in Barcelona, Spain. He received his PhD degree from the Department of Electrical and Computer Engineering at Stevens Institute of Technology, Hoboken, NJ, USA in 2011 and M.S. and B.S. degrees from the Department of Electrical and Electronics Engineering at Middle East Technical University, Ankara, Turkey, in 2006 and 2004, respectively. Before joining CTTC in 2018, he worked as an R&D Engineer for Avea (a Turkish mobile operator) between 2011 and 2016, as Senior R&D Engineer in Turk Telekomunikasyon A.S between 2016 and 2018 and a part-time instruction at Electrical and Electronics Engineering department of Ozyegin University between January 2015 and June 2018. Dr. Zeydan has been primarily responsible for carrying out European Commission and nationally funded research activities at CTTC, Türk Telekomunikasyon, Avea. He is currently the Project Coordinator of the Horizon Europe UNITY-6G European Project (January 2025-December 2027). He was the Project Coordinator of the Horizon 2020 MonB5G European Project (November 2021-April 2023). He has also been involved in other European level projects such as H2020 projects 5Growth (2019-2022) and Clear5G (as WP leader, 2017-2018), FP7 projects MOTO (as WP leader, 2012-2015) and CROWD (2014-2015) in collaborations with various industries and universities. He is co-author of over 150+ papers in international journals and conferences and 12

patents (11 granted in Turkish Patent Institute and 1 granted under European Patent Office). His research interests are in the areas of telecommunications, data engineering/science and network security.

III. A Description of the Topics the Tutorial Will Address

The tutorial will address the following technical topics, emphasising their timeliness and relevance to the research and practitioner communities:

- **AI for Intrusion Detection and Prevention:** Application of supervised, unsupervised, and semi-supervised ML methods for network intrusion detection systems (NIDS); deep learning architectures for real-time traffic classification; comparison with classical signature-based approaches.
- **Anomaly Detection in Network Traffic:** Autoencoders, generative adversarial networks (GANs), and statistical learning methods for identifying anomalous behaviour in high-dimensional, high-volume network telemetry data.
- **Federated Learning for Privacy-Preserving Threat Intelligence:** Collaborative threat detection without centralising sensitive network data; challenges of non-IID data distributions in federated security settings; secure aggregation protocols.
- **Reinforcement Learning for Adaptive Cyber Defence:** Game-theoretic and multi-agent reinforcement learning for autonomous intrusion response; moving target defence; attack graph navigation.
- **AI in Zero-Trust and Identity-Aware Networking:** Role of ML in continuous authentication, behavioural biometrics, and dynamic access control within zero-trust architectures.
- **Adversarial Machine Learning and Attack Taxonomies:** Evasion attacks, poisoning attacks, model inversion, and model stealing; threat modelling for AI systems deployed in network environments.
- **Robustness and Defences for AI in Networking:** Adversarial training, certified robustness, input sanitisation, differential privacy, and secure multi-party computation as defences against AI-targeted attacks.
- **AI Security in 5G/6G and Open RAN:** Specific threat vectors arising from AI-driven network automation, intelligent RAN control, and open interfaces; standardisation efforts at 3GPP, ETSI, and O-RAN Alliance.
- **Explainable and Trustworthy AI for Security:** Interpretability requirements in security-critical applications; explainability as an audit and accountability mechanism; regulatory and governance implications.
- **Future Research Directions and Open Challenges:** Large language models (LLMs) for security operations, AI-generated attack synthesis, AI watermarking, and the road to trustworthy AI-native networks.

IV. An Outline of the Tutorial Content, Including Its Tentative Schedule

The tutorial is planned as a half-day event lasting 3 hours of technical content. The outline is presented in Table I.

TABLE I
Outline and Schedule of the Tutorial

Time Duration	**Broad Topic to be Covered**
00 – 15 min	Introduction: The AI–Security Nexus in Modern Networks
15 – 30 min	AI for Intrusion Detection: Methods, Architectures, and Benchmarks
30 – 45 min	Anomaly Detection and Network Traffic Analysis with ML
45 – 60 min	Federated Learning for Collaborative and Privacy-Preserving Security
60 – 75 min	Reinforcement Learning for Adaptive Cyber Defence
	Break (15 Mins)
75 – 90 min	Adversarial ML: Attack Taxonomies and Threat Models for AI in Networks
90 – 115 min	Defences for AI Systems: Robustness, Privacy, and Trust
115 – 135 min	AI Security in 5G, 6G, and Open RAN: Standards and Deployment Considerations
135 – 155 min	Explainable and Trustworthy AI for Network Security
155 – 180 min	Conclusion, Future Directions, and Open Research Challenges

V. A Description of the Past and Relevant Experience of the Speakers

Dr Madhusanka has extensive research experience in 5G and beyond security domains and has organised numerous tutorials at various IEEE conferences, including:

- Tutorial on "The Role of Distributed Ledger Technology (DLT) for Beyond 5G Networks" at IEEE ICIN 2022 [1]
- Tutorial on "6G Security and Privacy Vision Towards Reality" at IEEE CCNC 2022 [2]
- Tutorial on "6G Security and Privacy Vision Towards Reality" at IEEE 5GWF 2021 [3]
- Tutorial on "Blockchain, IoT and 5G – The Trio to Mitigate Current and Post COVID-19 Challenges" at IEEE 5GWF 2021 [4]

[1] https://www.icin-conference.org/tutorials/
[2] https://ccnc2022.ieee-ccnc.org/program/tutorials
[3] https://ieee-wf-5g.org/2021-applications-tutorials/#TUT-8
[4] https://ieee-wf-5g.org/2021-applications-tutorials/#TUT-4

- Tutorial on "Security and Privacy of 5G and Beyond 5G Networks" at IEEE CCNC 2021 [5]
- Tutorial on "5G Security and Privacy: Issues, Potential Solutions and Future Directions", IEEE Globecom 2020 [6]
- Workshop on "5G Security and Privacy" at ICAC 2020 [7]
- Tutorial on "Blockchain-powered 5G-IoT Ecosystem vis-à-vis COVID-19: Opportunities and Challenges" at IEEE ANTS 2020 [8]
- Tutorial on "Role of Blockchain in Beyond 5G Networks" at IEEE 5GWF 2020 [9]
- Tutorial on "5G Security and Privacy: Issues, Potential Solutions and Future Directions" at IEEE Netsoft 2020 [10]
- Tutorial on "Blockchain for 5G and IoT: Use cases, Opportunities and Challenges" at IEEE CCNC 2020 [11]
- 3-day Workshop on "Security of 5G and SDN" at SSIC 2019 Conference[12]
- Special Session on "Secure 5G Telecommunication Networks" at ICCT'19 conference[13]
- 3-day Workshop on "Road to 5G Security" at LPU 2019 [14]

Dr Zeydan has also given more than 10 tutorials on data engineering for network management and orchestration in various conferences such as NoF 2024, IEEE SM 2024, CITS 2024, ICMLCN 2024, MeditCom 2024, HPDC 2024, WF-IoT 2023, IEEE HPSR 2023, COST CA20120 INTERACT, NOMS 2023, CNSM 2022, NoF 2022, NOMS 2016. Dr Zeydan has also instructed several courses given to undergraduate/graduate students at Özyğin University with tutorial related topics focusing on design principles of telecommunication networks, programmable networks (SDN, NFV), big data, IoT and virtualization.

VI. A Description of Previous Tutorial Experience of the Speakers

Since 2021, Dr Madhusanka has been working as an expert consultant at the European Union Agency for Cybersecurity (ENISA) for 5G security topics including Open RAN security and privacy. Dr. Zeydan has an expertise in quantum security and next-generation wireless networks and has presented tutorials on Quantum Secure 6G: The Framework and Proof-of-Concept at various conferences (outlined below). The presentations covered critical aspects of integrating quantum security into 6G networks, highlighting theoretical frameworks and real-world proof-of-concept implementations.

In addition to previous ones mentioned in Section V, the following tutorials were conducted by the speakers:

- Tutorial on "Open RAN Security and Privacy: Opportunities and Challenges" at IEEE Globecom 2022
- Tutorial Presentation by E. Zeydan, "Quantum Secure 6G: The Framework and Proof-of-Concept" presented at IEEE Consumer Communications & Networking Conference (CCNC 2025), 10–13 January 2025, Las Vegas, NV, USA and the 40th ACM/SIGAPP Symposium On Applied Computing, Sicily, Italy, March 31 – April 4, 2025.

[5] https://ccnc2021.ieee-ccnc.org/program/tutorials#security
[6] https://globecom2020.ieee-globecom.org/program/tutorials#tut01
[7] https://icac.lk/
[8] https://ants2020.ieee-comsoc-ants.org/wp-content/uploads/sites/223/2020/12/Tutorials.pdf
[9] https://ieee-wf-5g.org/5g-applications-tutorials/#TUT03
[10] https://netsoft2020.ieee-netsoft.org/program/tutorials/
[11] https://ccnc2020.ieee-ccnc.org/program/tutorials#tut-03
[12] https://ssic2019.com/gworkshop.html
[13] https://www.icct.co.in/specialsession3.php
[14] http://www.spadelpu.com/Roadto5GSecurity-SPADE.html