Zero Trust Security Methods for Wireless Networks





Moayad Aloqaily Helen Paik Willian T. Lunardi Cihan Tunc Fang He

Wireless networks have evolved significantly over time, enabling a wide range of advanced services and applications in various areas, including communications, healthcare, industry, and transportation. These applications have a tremendous impact on our daily lives, making us overly dependent on wireless technologies, hence, emphasizing the need for security. Wireless networks are vulnerable to a wide range of security threats and attacks that can compromise the confidentiality, integrity, and availability of data. The complexity of these threats increases exponentially as the current wireless network infrastructure evolves, such that security attacks target network resources, confidential data, and exploit user privacy. For this reason, new security models are highly needed to overcome these threats and provide a secure environment for wireless applications.

Zero trust is a contemporary security model that provides a new cybersecurity strategy to eliminate implicit trust. It assumes that all users, devices, applications, and their network traffic, internal and external, are untrusted and should be continuously verified and validated at every stage of a digital interaction before granting admission to network resources. Zero Trust Security Methods for Wireless Networks offer a paradigm shift in cybersecurity, focusing on continuous verification, least privilege access, and dynamic enforcement of security policies. By adopting these methods, wireless networks can significantly improve their resilience against evolving cyber threats and protect their sensitive assets effectively.

The purpose of this Special Issue (SI) is to elaborate on and emphasize the key aspects of zero-trust methods for wireless networks, understanding the principles of Zero Trust Security and how they can be applied to wireless networks and implementation of Zero Trust Security in wireless networks - best practices and challenges. This SI has carried significant importance, impact, and practical usefulness in today's digital landscape for several reasons:

- Enhanced wireless networks security posture.
- Protection against insider threats and adaptability to dynamic environments.
- Scalability and flexibility.
- Reduction of risk and data breaches.

The focus and purpose of this special issue are particularly relevant to both research communities and the security industry at this time. The peer-review process has made a significant contribution to the emerging field of zero-trust within wireless network infrastructures. Through its approach, the review process underwent multiple rounds, resulting in the acceptance of ten articles. The selection of these articles was based solely on their scientific quality, alignment with the special issue theme, and their contributions to the field. A range of papers addressing topics pertinent to the special issue were solicited, including:

- "Integrative Federated Learning and Zero-Trust Approach for Secure Wireless Communications," by M. Asad *et al.*, presents an innovative approach that integrates federated learning with zero-trust security to enhance the security of wireless communications. By leveraging the decentralized data processing capabilities of federated learning and the strict access controls of zero-trust models, our research offers a robust framework capable of significantly strengthening resistance against potential breaches. The significance of our work lies in its ability to address the escalating complexity of cyber threats with a novel, adaptable security model. The practical usefulness stems from the framework's applicability across various wireless communication networks, promising to revolutionize security measures and inspire future research in the field.
- "Industrial Wireless Internet Zero Trust Model: Zero Trust Meets Dynamic Federated Learning with Blockchain," by H. Xie *et al.*, proposes a comprehensive framework for ensuring industrial Internet of Things (IIoT) data security by combining the principles of zero-trust authentication, federated learning, and blockchain technology. The contribution of this article lies in its innovative integration of blockchain, federated learning, and zero trust principles to enhance data privacy and security in the Industrial Internet of Things. The utility of this framework lies in its ability to better defend against internal and external threats, improve anomaly detection, and enable secure collaboration among distributed nodes in an industrial Internet environment.
- "Federated Zero Trust Architecture using Artificial Intelligence," by S. Pal *et al.*, address the growing significance and impact of zero trust architecture (ZTA) in the context of evolving trends in cloud computing, remote work, and personal device usage. This article proposes a novel research direction by leveraging federated artificial intelligence to develop a Zero Trust (ZT) algorithm. This innovative approach aims to enhance enterprise infrastructure security, ensuring Dynamic access control and continuous monitoring in alignment with the principles of never trusting and consistently verifying. The practical utility of this research lies in its potential to fortify cybersecurity measures in the face of evolving organizational landscapes and increased reliance on cloud services and remote work scenarios.
- "Distributed Edge Caching for Zero Trust-Enabled Connected and Automated Vehicles: A Multi-Agent Reinforcement Learning Approach," by X. Xuanhong *et al.*, presents D-ECMA, a Distributed Edge Caching method with Multi-Agent reinforcement learning for Zero Trust-enabled Connected and

Automated Vehicles (CAVs). Addressing the challenge of real-time data processing delays in Zero Trust-Enabled CAVs, D-ECMA utilizes Multi-Agent Deep Deterministic Policy Gradient approach to obtain caching policies. In addition, Spatial-Temporal Fusion Graph Neural Networks for predicting demand and collaboration graph for acquiring collaborations are proposed to optimize the caching policies. Comparative experiments demonstrate the effectiveness of D-ECMA in reducing response delays.

- "Domain-Agnostic Hardware Fingerprinting-Based Device Identifier for Zero-Trust IoT Security," by A. Elmaghbub *et al.*, proposed EPS-CNN fingerprinting framework marks a significant leap forward in increasing the security of such networks under the Zero Trust (ZT) security model. EPS-CNN does so by leveraging a Convolutional Neural Network (CNN) in conjunction with the power spectrum of the signal's envelope or Envelope Power Spectrum (EPS) for short, a novel representation of RF signals, to achieve high device identification performances. EPS-CNN's ability to maintain over 99% accuracy across changing operational domains is what showcases its significance in fulfilling the stringent ZT model requirements. More than enhancing IoT network security, EPS-CNN underscores the critical role of domain-specific insights in the integration of deep learning into the security infrastructure of modern wireless networks.
- "SLIP: Self-supervised Learning based model Inversion and Poisoning Detection based Zero-Trust Systems for Vehicular Networks," by K. Dev *et al.*, proposes a Self-Supervised Learning based Model Inversion and Poisoning (SLIP) detection based zero-trust framework. The proposed framework implicitly scrutinizes each model at the server side to rate its security and then decides which model should be allowed to participate in aggregation process. The framework leverages state-of-the-art image generative networks along with networks that perform model inversion attacks to train the pretext task, which is responsible for differentiating between generated and original data. The downstream task is responsible for identifying corrupt samples that have undergone poisoning attack. The fusion rating module is also proposed to categorize the samples into white, grey, and black lists, respectively.
- "Softwarized Resource Allocation of Tailored Services With Zero Security Trust in 6G Network," by Cao *et al.*, investigated allocating resources of tailored slices with zero security trust in 6G networks. The authors proposed one tailored softwarized resource allocation method, labeled as Tail-ZeSec-6G. Comparing with existing softwarized resource allocation methods, the Tail-ZeSec-6G conducts the security checking procedure. Then, the Tail-ZeSec-6G does the formal softwarized resource allocation. After completing the allocation, zero security verification of all physical appliances will be conducted by Tail-ZeSec-6G. The checking procedure is conducted, based on zero security trust. In order to validate the security merits of Tail-ZeSec-6G, simulation work is conducted. Results vividly demonstrate that Tail-ZeSec-6G achieves better security performance, while guaranteeing high acceptance ratio.
- "ZTRAN Prototyping Zero Trust Security xApps for Open Radio Access Network Deployments," by A. Aly *et al.*, proposes the utilization of zero trust principles within the O-RAN architecture, the article introduces the concept of ZTRAN as a novel approach to enhancing network security through the integration of service authentication, intrusion detection, and secure slicing subsystems encapsulated as xApps. This innovative framework not only addresses the emerging security challenges posed by the disaggregated and software-defined nature of O-RAN but also sets a new standard for securing advanced wireless networks. The practical demonstration of ZTRAN on the Open Artificial Intelligence Cellular (OAIC) research platform showcases its feasibility and effectiveness in improving legitimate user throughput and latency figures. By bridging the gap between theoretical concepts and real-world applications, this article offers valuable insights for researchers and practitioners seeking to navigate the complex landscape of wireless network security.
- "Toward Zero-Trust 6GC: A Software Defined Perimeter Approach with Dynamic Moving Target Defense Mechanism," by A. Refaey, describes and discusses the most common and forecasted security threats for 6G networks, hence laying the key importance of a much-needed framework, such as Software Defined Perimeter, that adopts the Zero Trust Architecture (ZTA) model where access requests undergo authentication and continuous monitoring to enable the network providers to secure their networks against attackers, giving them a stress-free solution. Also proposed are Moving Target Defense mechanisms within SDP, which make the static nature of 6G networks vanish, in return, mitigating more serious cyber attacks and further enhancing the network security. Providing a deployment model that is fully scalable on large networks without additional cost and paving the way for more research toward more secure 6G networks.
- "Zero Trust-bBased Mobile Network Security Architecture, by Y. Liu *et al.*, presents a zero trust-based 6G security architecture to establish direct trust relationships between user equipment and service networks. Then, the article explores the opportunities offered by artificial intelligence and novel air interface technologies, which promote robust and efficient identity authentication, access control, and confidential data transmission for 6G. Finally, the article validates the performance of the zero trust architecture through a case study on 6G-enabled vehicular networks.

Biographies

Moayad Aloqaily (maloqaily@ieee.org) Moayad Aloqaily received a Ph.D. degree in Computer Engineering from the University of Ottawa, Canada, in 2016. He is currently with the Machine Learning Department, at Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), UAE. He was the recipient of many honors and awards, such as best paper awards of 2020 Ad Hoc Networks Journal, 2021 Computer Networks, 2022 IEEE IWCMC, 2022 IEEE MeditCom, 2022 IEEE Globecom, and 2023 IEEE Metaverse. His current research interests include the applications of AI and ML, blockchain solutions, and sustainable energy and data management.

Hye-Young (Helen) Paik (h.paik@unsw.edu.au) is Associate Professor at School of Computer Science and Engineering, UNSW, Sydney Australia. Helen is also a member of Cybersecurity Cooperative Research Centre. Her research background comes from areas such as middleware, distributed process integration and Service-Oriented architectures. Recently, Distributed Ledger Technology have become main focus, looking into various security and privacy enabling technologies such as Decentralised Identity Management and privacy-preserving data analytics and platforms, privacy and security in cyber physical systems.

Fang He (fanghe.fjnu@hotmail.com) received her Ph.D. degree in Electrical and Computer Engineering from Western University, Canada, in 2020. She is currently a Full Professor at Fujian Normal University, China. Her research interests include intelligent security provision and trust management. She serves as an AE of China Communications, and a GE of several journals. She was involved in many IEEE conferences as a Track Chair or Session Chair. She won the Best Paper Award from IEEE GLOBECOM 2023.

Cihan Tunc (Cihan.Tunc@unt.edu) is an assistant professor at the Department of Computer Science and Engineering at the University of North Texas (UNT). Dr. Tunc received his Ph.D. from the University of Arizona in 2015 and continued as a research assistant professor until his appointment at UNT in 2020. Dr. Tunc's research interests include cybersecurity and resiliency in the topics of IoT, drones, and cloud computing, and social media analysis.

Willian T. Lunardi (WillianTessaro.Lunardi@tii.ae) received the Ph.D. degree in computer science from the University of Luxembourg. He is currently a Machine Learning Researcher with the Secure Systems Research Centre, Technology Innovation Institute, Abu Dhabi, United Arab Emirates. He is also working on machine learning for network security, physical layer security, and jamming detection. He has published over 25 research papers in scientific international journals, conferences, and book chapters. His research interests include machine learning and combinatorial optimization.