



Security and Privacy for Modern Wireless Communication Systems, 2nd Edition

Tao Huang ^{1,*}  and Jusak Jusak ² ¹ College of Science and Engineering, James Cook University, Cairns, QLD 4878, Australia² School of Science and Technology, James Cook University, Singapore 387380, Singapore; jusak.jusak@jcu.edu.au

* Correspondence: tao.huang1@jcu.edu.au

1. Introduction

Wireless communication systems are undergoing rapid transformation, driven by the advent of 6G technologies, the proliferation of Internet of Things (IoT) devices, and the growing reliance on intelligent and connected infrastructure. As wireless networks expand in complexity and capability, ensuring security and privacy becomes increasingly vital—not only to protect sensitive data but also to maintain trust, system integrity, and operational reliability in critical applications such as remote healthcare, autonomous vehicles, and smart manufacturing.

This Special Issue, titled “Security and Privacy for Modern Wireless Communication Systems, 2nd Edition”, aims to address urgent challenges by highlighting the latest innovations in protocols, architectures, software, and hardware solutions designed to enhance the security and privacy of contemporary wireless networks. Unlike traditional systems, modern wireless environments must accommodate a diverse array of resource-constrained devices, ultra-low-latency applications, and emerging vulnerabilities introduced by technologies such as intelligent reflective surfaces, blockchain, edge/fog/cloud computing, and artificial intelligence (AI).

The 12 papers published in this Special Issue discuss a wide range of research topics. Several contributions focus on lightweight and quantum-resistant cryptography. These include discussions on the use of the CHERI architecture to create memory-safe intrusion detection systems and MLWE-based key exchange methods for post-quantum secure authentication. Other papers address network-level threats, proposing innovative solutions such as hybrid communication architectures, blockchain-based security for supply chains, and frameworks for cyber insurance to handle catastrophic cyber incidents. Additionally, this Special Issue highlights advancements in physical-layer security and edge security, including methods for physical-layer fingerprinting of LoRa devices, detection of covert communications, and the development of trust models within 6G edge-node-cloud ecosystems. Practical aspects of cybersecurity are also examined; several studies explore log-based forensic analysis, testbed validation, and real-time monitoring to detect remote access and file exfiltration.

Collectively, the papers cover foundational research and applied solutions across topics such as 5G/6G communications, physical-layer key generation, lightweight cryptography, blockchain networks, anonymity in data transmission, the use of machine learning/deep learning, and security and privacy designs tailored for Vehicle-to-Everything (V2X), supply chain, and LoRa networks. Furthermore, this Special Issue underscores the importance of prototyping, forensic tools, and testbed evaluations to ensure real-world viability.



Received: 6 June 2025

Accepted: 9 June 2025

Published: 11 June 2025

Citation: Huang, T.; Jusak, J. Security and Privacy for Modern Wireless Communication Systems, 2nd Edition. *Electronics* **2025**, *14*, 2379. <https://doi.org/10.3390/electronics14122379>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

By collating these contributions from leading researchers, this Special Issue provides a comprehensive and timely overview of the state of the art while also identifying emerging research directions that will shape the future of secure and private wireless communication systems.

2. Summary of the Contributions

The first contribution, provided by Yoon et al., proposes a cooperative autonomous driving system tailored for urban environments by leveraging a V2X network-based framework. Unlike previous studies that primarily focus on highway scenarios, this work addresses the unique challenges of urban driving, such as managing traffic lights, pedestrian interactions, and dynamic vehicle clusters. A key innovation is the introduction of the Throttle–Steer–Brake (TSB) driving technique, which enables following vehicles to replicate the control commands of a leading vehicle, significantly reducing computational overhead and improving real-time responsiveness. The system also incorporates an HSV-based traffic light perception method, which outperforms AI-based models in speed and accuracy, and a pedestrian detection mechanism using V2P communication to trigger emergency braking when necessary. The system employs pseudonymized vehicle identifiers, AES encryption, and EdDSA digital signatures to ensure secure and reliable communication. Validated in the CARLA simulator, the proposed approach demonstrated approximately 466 times faster computation using TSB driving compared to waypoint-based methods and achieved 99.58% accuracy in traffic light recognition. The results confirm the feasibility of real-time, safe, and secure cooperative autonomous driving in urban settings. Future work will focus on deploying the system in real-world conditions, accounting for network latency and failures, and enhancing TSB driving in complex traffic scenarios.

The second contribution, provided by Kalutharage et al., explores the enhancement of automotive intrusion detection systems (IDSs) by integrating CHERI (Capability Hardware Enhanced RISC Instructions), a hardware-enforced memory protection architecture. Motivated by the growing cybersecurity risks in connected vehicles, especially threats like IP spoofing and rule manipulation, the authors propose a CHERI-enabled IDS that isolates memory and safeguards detection rules from unauthorized access. The system enforces strict spatial and temporal memory safety by embedding capability-based access controls directly into the IDS design, effectively blocking advanced attacks. Experimental results show that the CHERI-enhanced IDS achieves 100% detection of spoofed packets and prevents all unauthorized rule modifications, even under real-time constraints. Implemented on the ARM Morello board, the solution operates within the latency thresholds required for automotive applications. Compared to traditional software-based IDS solutions, this hardware-centric approach ensures rule integrity, enhances detection robustness, and maintains system performance in resource-constrained environments. The authors conclude that CHERI-based IDS frameworks offer a scalable, secure foundation for future automotive cybersecurity systems, with potential for further optimization and integration with machine learning for anomaly detection.

The third contribution, authored by Kim et al., introduces LazyNTT, a novel approach to optimizing the Number Theoretic Transform (NTT), which is fundamental to lattice-based post-quantum cryptographic schemes. Traditional NTT relies heavily on Montgomery multiplication for modular reduction, which, while efficient, is still more costly than standard integer multiplication. To solve this problem, the authors propose two variants, SM-LazyNTT and SSM-LazyNTT, which strategically replace certain Montgomery multiplications with standard multiplications during intermediate stages of the NTT computation. These “lazy” replacements postpone modular reductions without affecting the final correctness, reducing computational overhead. SM-LazyNTT alternates between

standard and Montgomery multiplications, while SSM-LazyNTT allows two consecutive standard multiplications before performing a Montgomery multiplication. The method is validated using parameters from Falcon and Kyber cryptosystems, showing performance improvements of up to 9% and 28%, respectively. The approach is generalizable to more complex variants and incurs only minimal additional memory requirements. Experimental results confirm that LazyNTT significantly reduces cycle counts while preserving output correctness, making it a promising optimization for post-quantum cryptography and potentially homomorphic encryption.

The fourth contribution, produced by Scalise et al., presents an applied study on enhancing the cybersecurity of 5G and future 6G core networks by integrating post-quantum cryptography (PQC), specifically Key Encapsulation Methods (KEMs), into the free5GC open-source platform. Recognizing that the virtualized nature of modern 5G Core Networks increases the attack surface, the authors aim to address the threat posed by quantum computing, especially the risk of “Store Now, Decrypt Later” (SNDL) attacks, by replacing vulnerable key exchange methods in TLS with quantum-resistant alternatives like CRYSTALS-Kyber. The team implements these PQC KEMs into TLS 1.3 for inter-VNF communication within free5GC, leveraging the Open Quantum Safe (OQS) project and modifying the system using Go-OpenSSL bindings for compatibility. The evaluation demonstrates that PQC integration results in only a minimal increase in latency and bandwidth overhead during UE (User Equipment) connection establishment. Specifically, standalone Kyber KEMs outperform the widely used elliptic curve X25519 in latency performance. The authors conclude that PQC-enabled 5G cores are both feasible and beneficial, offering strong quantum-resilient security with negligible impact on real-time system performance. This work sets a precedent for integrating PQC in production-grade 5G and 6G systems to future-proof their cryptographic integrity.

The fifth contribution, authored by Park et al., introduces a provably quantum-secure three-party mutual authentication and key exchange protocol based on the Modular Learning with Error (MLWE) problem. Motivated by the limitations of existing work in the literature, which is vulnerable to several attacks, including replay attacks, impersonation attacks, insider attacks, and denial-of-service attacks, the authors develop a more robust and efficient protocol that integrates biometric data for three-factor authentication. The proposed scheme ensures that users and servers can mutually authenticate and securely exchange session keys even with quantum adversaries. Formal security validation is conducted using BAN logic, the Real-or-Random (RoR) model, and the AVISPA tool, confirming resistance against various attacks and verifying mutual authentication. Performance analysis demonstrates computational efficiency and improved security features compared to related protocols. By leveraging the strengths of MLWE in combination with biometric authentication and secure hash-based operations, the protocol offers a scalable and practical solution for post-quantum secure communications in multi-party settings.

The sixth contribution, provided by Thakur et al., presents IoT-GChain, a blockchain- and IoT-assisted grain supply chain framework aimed at enhancing transparency, traceability, and security in grain distribution. The system addresses long-standing issues in traditional supply chains, such as middleman exploitation, record tampering, and lack of real-time grain condition monitoring, by integrating non-fungible tokens (NFTs), smart contracts, and sensor data. Each grain lot is tokenized as an NFT containing critical information, including quality metrics, weight, and environmental conditions (e.g., temperature and humidity) collected via DHT22 sensors and GPS modules. These NFTs are dynamically updated as grain moves through a multi-tiered supply chain, from central authorities to local retailers. Smart contracts deployed on the Ethereum blockchain automate verification, traceability, and ownership transfer, with real-time updates stored in Firebase and metadata

hosted on IPFS. The framework includes a user interface with QR code scanning for grain status verification and integrates with MetaMask for secure interaction. Security is assessed using SolidityScan, with a reported security score of 84.56. Experimental validation confirms the system's capability to streamline operations, enhance user trust, and prevent fraud. This layered, decentralized design demonstrates a scalable and tamper-resistant model for modernizing grain supply chains in developing economies.

The seventh contribution, provided by Zadobrischi et al., explores a hybrid communication architecture that enhances the scalability and interoperability of vehicular communication protocols, specifically C-V2X, DSRC, and LoRa 2.4 GHz, within urban Intelligent Transportation Systems (ITS). The paper is motivated by the need to improve road safety, reduce traffic congestion, and support smart city development amidst increasing urbanization. The authors assess the strengths and limitations of each protocol: DSRC offers low latency for short-range safety-critical applications; C-V2X, built on LTE/5G, supports high-throughput and long-range communication; and LoRa 2.4 GHz provides energy-efficient, long-distance communication ideal for non-critical infrastructure monitoring. Through simulation and field experiments, the study demonstrates that LoRa 2.4 GHz can complement DSRC and C-V2X by filling communication gaps in high-mobility or obstructed urban areas. Using advanced signal modeling and ray tracing, the authors validate LoRa's effectiveness under urban interference and confirm its low bit error rate and acceptable latency. A proposed architecture integrates LoRa nodes across vehicles, infrastructure, and pedestrians, linking them to a gateway that communicates with cloud-based analytics platforms. The study concludes that combining these technologies offers a scalable, low-cost, and resilient communication framework for future ITS applications and recommends further research into interoperability, dynamic parameter tuning, and security to support autonomous vehicle networks and smart city infrastructure.

The eighth contribution, produced by Aroon et al., proposes the Enhanced Profiling Assurance (EPA) architecture to address the limitations of the Manufacturer Usage Description (MUD) standard in detecting malicious activity within IoT networks. While the MUD framework enforces stateless access control rules based on predefined profiles, it fails to inspect the state of ongoing communications, potentially allowing traffic amplification and other attacks to bypass detection. To overcome this, the EPA incorporates a two-layer Intrusion Detection and Prevention System (IDPS) that combines both stateless and stateful inspection. It leverages three-way decision theory—allow, deny, and uncommitted—to support ongoing analysis of uncertain network behaviors rather than forcing binary decisions. The architecture also integrates a Network Behavior Analysis (NBA) system that consults dynamically updated knowledge bases of normal, abnormal, and uncertain behaviors. This enables real-time packet inspection and adaptive rule updates for improved security enforcement. Experimental evaluations demonstrate that the EPA significantly reduces false negatives compared to the conventional MUD approach. The study provides a flexible and scalable implementation model for small-scale IoT networks, with potential for broader application in securing edge environments against evolving cyber threats.

The ninth contribution, provided by Bace et al., offers a comprehensive multistakeholder analysis on how the United States can enhance resilience against catastrophic cyber incidents (CCIs) through the strategic use of cyber insurance and potential federal intervention. Using content analysis of 56 public comments submitted in response to a U.S. Treasury Department Request for Information, the authors investigate four key areas: how CCIs are defined, how they can be mitigated, whether the current cyber insurance sector can manage such risks, and what role the government should play. The study finds that while stakeholders agree that CCIs involve large-scale financial loss, cross-sector impact, and critical infrastructure disruption, no consistent definition complicates risk modeling. Many

comments support the use of basic cybersecurity measures (e.g., MFA, patching, employee training) to mitigate CCI and suggest that insurers should mandate such practices. Most respondents believe the private insurance sector lacks the capacity or willingness to manage CCIs alone, advocating for a federal backstop, modeled partly on the Terrorism Risk Insurance Program (TRIP), to stabilize the market. Concerns such as moral hazard, physical loss exclusions, and excessive regulation are acknowledged but seen as manageable through careful design. The study concludes with a proposed framework for a federal backstop and offers actionable insights for policymakers to strengthen national cybersecurity resilience.

The tenth contribution, authored by Tripi et al., provides a comprehensive analysis of security, privacy, and trust challenges in 6G networks, structured around a layered security architecture that spans the physical, connection, and application layers. The paper begins by highlighting the transformative potential of 6G, including its ultra-low-latency capabilities, massive connectivity, and support for emerging technologies like XR, CRAS, BCI, and blockchain, while emphasizing that these advances demand a proactive approach to security from the ground up. At the physical layer, the authors detail vulnerabilities like eavesdropping, jamming, and spoofing and propose mitigations including Reconfigurable Intelligent Surfaces (RISs), Friendly Jamming, NOMA, frequency hopping, and reinforcement learning. Key risks such as DoS, MitM, and replay attacks for the connection layer are countered through Quantum Key Distribution (QKD), network slicing, and deep learning-based intrusion detection systems (IDSs). The application layer faces threats like social engineering, for which biometric authentication, Quantum Homomorphic Cryptography (QHC), and Authentication and Key Agreement (AKA) protocols are proposed. The paper also explores trust management models involving blockchain, smart contracts, and trust anchors, advocating for decentralized, transparent mechanisms. The authors offer a forward-looking blueprint for building secure, resilient, and trustworthy 6G infrastructures by integrating Zero Trust Architecture- and AI-driven defense strategies.

The eleventh contribution, from Baldini et al., presents a novel hybrid machine learning and deep learning approach for Radio Frequency Fingerprinting (RFF) of LoRa devices, leveraging the residuals from Variational Mode Decomposition (VMD) instead of the commonly used modes. The authors argue that residual signals, which exclude common modulation components, better capture device-specific physical characteristics essential for accurate fingerprinting. The authors propose a feature-driven segmentation method to handle the computational burden of applying CNNs to spectrograms derived from these signals. This involves calculating Local Binary Pattern (LBP) and Shannon entropy to identify and extract the most discriminative regions of the spectrograms for input into a multi-head attention CNN. The method is evaluated on a public dataset of 10 LoRa devices, each contributing 500 signal bursts. Experimental results show that this residual-based and segmented spectrogram approach significantly improves classification accuracy (up to 91.9%) while reducing computational time compared to baseline methods using full spectrograms or original signals. The study concludes that combining residual analysis with targeted image reduction and deep learning leads to a more efficient and accurate RFF framework suitable for IoT environments with constrained resources.

The final contribution, from Pañeda et al., presents a forensic analysis of file exfiltration activities using three widely used remote desktop applications: TeamViewer, AnyDesk, and Chrome Remote Desktop. Motivated by the surge in remote work during the COVID-19 pandemic and the associated cybersecurity risks, the authors investigate whether digital forensics can effectively determine what files were exfiltrated, as well as when and by whom, using such tools. The study simulates both push (the user exfiltrates data to an external device) and pull (the external user accesses internal data) scenarios on virtual machines. Using Wireshark, forensic evidence is collected from application logs, system

event logs, browser histories, and network traffic. Key findings show that TeamViewer provides detailed logs, including file names, paths, and timestamps, while AnyDesk reveals connection details and remote IPs but lacks file names in logs. Chrome Remote Desktop, being browser-based, offers the least forensically useful logging, with evidence primarily found in browser histories and system events. Network behavior, such as traffic patterns and acknowledgement timings, can be analyzed to infer exfiltration events despite encryption. The study concludes that while some evidence is partial, combining multiple sources (logs, audits, traffic) can yield legally viable digital evidence and early warning indicators for unauthorized data transfers.

3. Conclusions

This Special Issue features a diverse collection of cutting-edge research that addresses the evolving challenges of security and privacy in modern wireless communication systems. The selected papers strike a balance between theoretical advancements and practical solutions, covering a wide range of topics, including post-quantum cryptography, physical-layer security, network intrusion detection, and forensic analysis. As wireless technologies advance toward 6G and beyond, and as the integration of AI, IoT, and edge computing deepens, ensuring secure and trustworthy communication infrastructures remains a critical priority. Through this collection, we not only hope to platform current research but also inspire further innovation in this vital field.

Author Contributions: Writing—original draft preparation, T.H.; writing—review and editing, J.J. and T.H. All authors have read and agreed to the published version of the manuscript.

Funding: This article received no external funding.

Acknowledgments: We would like to express our sincere gratitude to all the Guest Editors of this Special Issue for their invaluable contributions throughout the editorial process. Their expertise, dedication, and thoughtful oversight were instrumental in ensuring the high quality and thematic coherence of the published works. We also extend our appreciation to the reviewers for their time and constructive feedback and to the authors for submitting their outstanding research. Finally, we thank the editorial team at *Electronics* for their continuous support and professionalism in managing this Special Issue.

Conflicts of Interest: The authors declare no conflicts of interest.

List of Contributions

1. Yoon, M.; Seo, D.; Kim, S.; Kim, K. V2X Network-Based Enhanced Cooperative Autonomous Driving for Urban Clusters in Real Time: A Model for Control, Optimization and Security. *Electronics* **2025**, *14*, 1629. <https://doi.org/10.3390/electronics14081629>.
2. Kalutharage, C.S.; Mohan, S.; Liu, X.; Chrysoulas, C. Enhancing Automotive Intrusion Detection Systems with Capability Hardware Enhanced RISC Instructions-Based Memory Protection. *Electronics* **2025**, *14*, 474. <https://doi.org/10.3390/electronics14030474>.
3. Kim, G.; Seo, E.; Lee, Y.; Kim, Y.-S.; No, J.-S. Lazy Modular Reduction for NTT. *Electronics* **2024**, *13*, 4887. <https://doi.org/10.3390/electronics13244887>.
4. Scalise, P.; Garcia, R.; Boeding, M.; Hempel, M.; Sharif, H. An Applied Analysis of Securing 5G/6G Core Networks with Post-Quantum Key Encapsulation Methods. *Electronics* **2024**, *13*, 4258. <https://doi.org/10.3390/electronics13214258>.
5. Park, H.; Son, S.; Park, Y.; Park, Y. Provably Quantum Secure Three-Party Mutual Authentication and Key Exchange Protocol Based on Modular Learning with Error. *Electronics* **2024**, *13*, 3930. <https://doi.org/10.3390/electronics13193930>.

6. Thakur, K.S.; Ahuja, R.; Singh, R. IoT-GChain: Internet of Things-Assisted Secure and Tractable Grain Supply Chain Framework Leveraging Blockchain. *Electronics* **2024**, *13*, 3740. <https://doi.org/10.3390/electronics13183740>.
7. Zadobrischi, E.; Havriliuc, Ș. Enhancing Scalability of C-V2X and DSRC Vehicular Communication Protocols with LoRa 2.4 GHz in the Scenario of Urban Traffic Systems. *Electronics* **2024**, *13*, 2845. <https://doi.org/10.3390/electronics13142845>.
8. Aroon, N.; Liu, V.; Kane, L.; Li, Y.; Tesfamicael, A.D.; McKague, M. An Architecture of Enhanced Profiling Assurance for IoT Networks. *Electronics* **2024**, *13*, 2832. <https://doi.org/10.3390/electronics13142832>.
9. Bace, B.; Dubois, E.; Tatar, U. Resilience against Catastrophic Cyber Incidents: A Multistakeholder Analysis of Cyber Insurance. *Electronics* **2024**, *13*, 2768. <https://doi.org/10.3390/electronics13142768>.
10. Tripi, G.; Iacobelli, A.; Rinieri, L.; Prandini, M. Security and Trust in the 6G Era: Risks and Mitigations. *Electronics* **2024**, *13*, 2162. <https://doi.org/10.3390/electronics13112162>.
11. Baldini, G.; Bonavitacola, F. LoRa Radio Frequency Fingerprinting with Residual of Variational Mode Decomposition and Hybrid Machine-Learning/Deep-Learning Optimization. *Electronics* **2024**, *13*, 1925. <https://doi.org/10.3390/electronics13101925>.
12. Pañeda, X.G.; Melendi, D.; Corcoba, V.; G. Pañeda, A.; García, R.; García, D. Forensic Analysis of File Exfiltrations Using AnyDesk, TeamViewer and Chrome Remote Desktop. *Electronics* **2024**, *13*, 1429. <https://doi.org/10.3390/electronics13081429>.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.