# Special Issue on Softwarized Networks and Security: Challenges and Emerging Solutions

## Aims and Scopes

The rapid evolution of communication networks toward highly programmable, virtualized, cloud-native, and intelligent infrastructures has transformed the design, deployment, and operation of modern networking systems. Technologies such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), network slicing, intent-based networking, Quantum Networking, and AI-driven network management are enabling unprecedented flexibility, scalability, and automation in next-generation networks. While these advances offer significant operational benefits, they also introduce new security challenges arising from increased programmability, centralized control architectures, virtualization layers, multi-tenant environments, dynamic service orchestration, and software-defined control mechanisms. Ensuring the security, privacy, trustworthiness, resilience, and dependability of softwarized networks has therefore become a critical research priority for future Internet infrastructures, 5G/6G systems, industrial networks, and cyber-physical systems.

This Special Issue aims to bring together researchers, practitioners, industry experts, and policymakers to present cutting-edge research, innovative methodologies, practical solutions, and emerging trends addressing security challenges in softwarized networking environments. The issue seeks high-quality original contributions that advance the state-of-the-art in securing programmable, virtualized, autonomous, and intelligent networks. This Special Issue welcomes theoretical, experimental, simulation-based, and practical contributions covering, but not limited to the following topics:

**1. Security in Software-Defined Networking (SDN)**

- SDN control plane security
- Secure SDN controllers and controller placement
- East-West and North-South interface protection
- Secure flow rule management
- SDN attack detection and mitigation
- Distributed denial-of-service (DDoS) defense in SDN
- Threat modeling and vulnerability assessment in SDN environments

**2. Security of Network Function Virtualization (NFV)**

- Secure virtual network functions (VNFs)
- VNF isolation and multi-tenancy security
- NFV orchestration and management security
- Hypervisor and container security

- Secure service function chaining
- Trust management in NFV infrastructures

**3. Programmable Data Plane Security**

- P4-based network security mechanisms
- Security of programmable switches
- Data plane monitoring and anomaly detection
- Runtime verification of programmable forwarding behaviors
- Secure in-network computing

**4. 5G, Beyond 5G, and 6G Network Security**

- Security of network slicing
- Open RAN (O-RAN) security
- Security in virtualized radio access networks
- Secure service orchestration in 5G/6G
- AI-native security architectures for 6G
- Security challenges in ultra-low latency and massive IoT deployments

**5. Artificial Intelligence and Machine Learning for Network Security**

- AI-driven threat detection and response
- Federated learning for network security
- Explainable AI for security analytics
- Adversarial machine learning in networking
- Intelligent intrusion detection systems
- Autonomous security orchestration and remediation

**6. Zero Trust and Identity-Centric Networking**

- Zero-trust networking architectures
- Identity and access management
- Continuous authentication and authorization
- Trust frameworks for programmable networks
- Policy-driven security management

**7. Secure Network Automation and Orchestration**

- Intent-based security management
- Secure network automation frameworks
- Policy verification and compliance
- Security-aware orchestration
- Autonomous network security operations

**8. Internet of Things (IoT) and Cyber-Physical Systems Security**

- Secure IoT networking architectures
- Industrial IoT and Industry 4.0 security
- Smart city network security
- Secure edge intelligence
- Trustworthy cyber-physical infrastructures

**9. Emerging Security Challenges**

- Quantum-safe networking security
- Post-quantum cryptography for programmable networks
- Digital twins for network security assessment

- Security of autonomous and self-driving networks
- Green networking and security trade-offs
- Security for integrated terrestrial-satellite networks
- Resilience against advanced persistent threats (APTs)

**10. Security Measurement, Verification, and Testing**

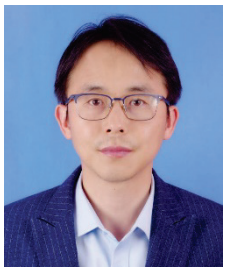
- Formal methods for network security verification
- Security benchmarking and evaluation
- Digital forensics in Softwarized networks
- Security testing and penetration analysis
- Network resilience and survivability assessment

## Special Issue Editors

Guest Editor: Prof. Bishnu Prasad Gautam
Email: gautam_bishnu@rs.sus.ac.jp
Website: https://researchmap.jp/gautambp?lang=en
Suwa University of Science, Nagano, Japan
Interests: Computer Networks, Network Management and Monitoring, AIoT

Guest Editor: Asst. Prof. Babu R. Dawadi
Email: baburd@ioe.edu.np
Website: www.baburd.com.np
Dept. of Electronics and Computer Engineering, Pulchowk Campus, Institute of Engineering, Tribhuvan University, Kritipur, Nepal
Interests: IoT and Edge Network Security, Intelligent Networking, Distributed Computing

Guest Editor: Prof. Li Duan
Email: duanli@bjtu.edu.cn
Website: http://faculty.bjtu.edu.cn/9432/
School of Cyberspace Science and Technology, Beijing Jiaotong University, Beijing, China
Interests: AI Security, Blockchain and Privacy Computing



Guest Editor: Prof. Xuewen Dong
Email: xwdong@xidian.edu.cn
Website: https://faculty.xidian.edu.cn/DXW/zh_CN/index.htm
School of Computer Science and Technology, Xidian University, Xi'an, China
Interests: Blockchain, SDN Security, AI Security,

## Author's Guidelines

The submissions should follow the formatting guidelines of the Journal of Networking and Network Applications (**https://iecscience.org/public/ueditor/php/upload/file/20200202/1580614065642302.zip**). Any questions regarding this special issue should be sent to the guest editors. All submitted papers will be reviewed by at least three reviewers and selected based on their originality, significance, relevance, and clarity of presentation. The manuscript should be prepared in J-NaNA Latex standard and converted into a PDF for auto-submission system. Electronic papers should be submitted to the J-NaNA Submission System at **https://www.manuscriptmanager.net/jnna**.

## Keywords

- Softwarized Networks,
- Network Security,
- SDN Security
- IBN Security
- NDN Security

- Post-Quantum Security,
- Quantum-Safe Networking,
- Zero Trust Networking,
- Security Orchestration,
- Network Slicing Security,
- Open RAN Security,
- Edge Computing Security,
- Container Security,
- Kubernetes Security,
- AI for Cybersecurity,
- Machine Learning for Network Security,
- IoT Security,
- Industrial IoT Security,
- Cyber-Physical Systems Security,
- Secure Telemetry,
- Network Monitoring and Analytics.

## Publication Schedule

Manuscript Submission Deadline: September 15, 2026
Notification of Acceptance/Rejection/Revision: October 20, 2026
Final Manuscript Due: November 20, 2026
Tentative Publication Date: December 20, 2026

## Benefits of Publishing in a Special Issue

- Ease of navigation: Grouping papers by topic helps scholars navigate broad scope journals more efficiently.
- Greater discoverability: Special Issues support the reach and impact of scientific research. Articles in Special Issues are more discoverable and cited more frequently.
- Expansion of research network: Special Issues facilitate connections among authors, fostering scientific collaborations.
- External promotion: Articles in Special Issues are often promoted through the journal's social media, increasing their visibility.
- Special Issues with more than 5 articles can be published, ensuring wide and rapid dissemination.
- The Article Processing Charge (APC) for publication in this open access journal is **No fee**.

## J-NaNA's homepage

- https://iecscience.org/public/journals/J-NaNA
- J-NaNA Submission System: https://www.manuscriptmanager.net/jnna