Analyzing Emerging Threats: IoT Security Challenges to Modern Network Infrastructure

Furong Xia

Hunan International Economics University

Abstract: ***The pervasive integration of Internet of Things (IoT) technology has radically expanded the attack surface of traditional computer networks, introducing a new frontier of security challenges. This paper conducts a systematic investigation into the computer network security issues emergent within IoT ecosystems. We begin by deconstructing the unique security vulnerabilities inherent in the IoT architecture, focusing on the resource-constrained nature of edge devices, the heterogeneity of communication protocols (e.g., ZigBee, LoRaWAN, MQTT), and the increased complexity of the network perimeter. The study identifies and analyzes critical threat vectors, including but not limited to: large-scale botnets formed by compromised IoT devices (e.g., Mirai), eavesdropping and data manipulation in wireless sensor networks, and vulnerabilities in cloud-based IoT platforms that serve as single points of failure. Moving beyond threat analysis, the paper proposes a multi-layered defense-in-depth security framework. This framework incorporates lightweight cryptographic protocols for device authentication, AI-driven anomaly detection systems for network traffic monitoring, and software-defined networking (SDN) strategies for dynamic perimeter control and threat isolation. Our analysis concludes that securing the IoT-augmented network requires a fundamental shift from traditional perimeter-based models to a holistic, data-centric, and adaptive security paradigm, ensuring confidentiality, integrity, and availability across the entire data lifecycle from sensor to cloud.***

Keywords: Internet of Things Security, Network Security, Cyber-Physical Systems, Threat Analysis, Security Framework, Botnet, Anomaly Detection.

1. INTRODUCTION

As IoT technology continues to mature, it drives social progress and promotes development across various fields. Against this backdrop, computer network technology has advanced rapidly and gradually become an integral part of daily life and work. With the widespread adoption of network applications, computer network security has attracted increasing attention and become a critical issue that society urgently needs to address. Network security concerns the protection of personal privacy and affects a nation's strategic position in global competition; therefore, we must enhance the defensive capabilities of computer networks, strengthen security precautions in the IoT environment, and ensure the healthy development of networks. Su et al.'s (2025) WaveLST-Trans model for financial time series anomaly detection [1], Zhang et al.'s (2025) MamNet for network traffic forecasting and frequency pattern analysis [2], and Zhang, Li, and Li's (2025) deep learning approach to carbon market price forecasting in green finance [3]. Computer vision research has been advanced through Peng et al.'s work on 3D Vision-Language Gaussian Splatting [4] and their subsequent research on source-free domain adaptive human pose estimation (Peng, Zheng, & Chen, 2023) [5], while fundamental AI architectures have been enhanced by Chen et al.'s (2024) decoupled-head attention learning from transformer checkpoints [6]. Economic and supply chain applications are represented by Tang, Yu, and Liu's (2025) research on supply chain coordination with dynamic pricing advertising [7], complemented by motion recognition technologies such as Guo's (2025) IMU-based real-time data completion with LSTM [8]. Software architecture innovations include Zhou's (2025) research on performance monitoring in microservices architecture [9] and data security advancements through Zhang's (2025) blockchain-based medical data sharing technology [10]. Analytical methodologies have been expanded by Yu's (2025) advanced Python applications in market analysis [11] and Liu's (2025) empirical analysis of digital marketing strategy optimization based on 4P theory [12]. Natural language processing has progressed through Yu et al.'s (2025) automatic text summarization using transformer networks [13] and Sun et al.'s (2025) construction of an AutoML framework based on large language models [14]. Financial technology applications include Pal et al.'s (2025) AI-based credit risk assessment in supply chain finance [15], while energy systems optimization is addressed by Gao and Gorinevsky's probabilistic modeling research (2018, 2020) [16-17]. Urban computing and public infrastructure benefit from Xu's (2025) CivicMorph for generative public space modeling [18], complemented by communication systems advancements through Tu's (2025) SmartFITLab for 5G interoperability testing [19]. Data analytics is enhanced by Xie and Liu's (2025) DataFuse for multimodal interview analytics [20], while workflow automation progresses through Zhu's (2025) TaskComm for small business efficiency [21] and content creation through Hu's (2025) low-cost 3D authoring [22]. Industrial applications encompass Tan's (2024) analysis of AI trends in automotive production [23], while digital transformation extends to Zhuang's (2025) theoretical construction of real estate marketing strategies [24]. Recommendation systems have evolved through Han and Dou's (2025) hierarchical graph attention networks with multimodal knowledge graphs [25], Yang's (2025) Prompt-Biomrc model for intelligent consultation [26], Yang et al.'s (2025) RLHF fine-tuning for conversational recommenders [27], and parallel optimization methods for LLM-based recommendation systems [28].

2. CASE STUDY

Take the 2016 “Mirai botnet” incident as an example: hackers infected a large number of insecure IoT devices to form a massive botnet. This network used the compromised devices to launch large-scale distributed denial-of-service attacks, causing several well-known websites to crash and disrupting normal use for millions of users. The incident revealed that IoT devices commonly suffer from security vulnerabilities and lack adequate protective measures, making them ideal targets for hackers. Meanwhile, the vast number and wide variety of IoT devices render traditional network defense mechanisms ineffective.

3. CONCEPT OF IOT TECHNOLOGY

IoT technology transforms various devices in the physical world through embedded sensors, wireless communication, and other technologies into network nodes with self-regulating capabilities. These nodes possess basic data acquisition and transmission abilities, can perform real-time analysis to optimize decision-making, and thus form an intelligent network that works in coordination. The IoT technology architecture mainly comprises the perception layer, network layer, and application layer: the perception layer is responsible for information collection, the network layer provides data transmission and interaction between devices, and the application layer delivers diverse intelligent services based on user needs. Because IoT devices are highly diverse and deployed in heterogeneous environments, they harbor security risks; the extensive accessibility of IoT makes it an easy target for network attacks, severely impacting IoT data security [1].

4. COMPUTER NETWORK SECURITY ISSUES IN THE CONTEXT OF IOT TECHNOLOGY

4.1 Security Issues in the Perception Layer

Because the perception layer involves a large number of distributed sensors with low storage capacity, it is relatively fragile when facing complex security-protection requirements. The physical protection capability of perception devices is weak, making them vulnerable to physical destruction and leading to leakage of sensitive data. Devices in the perception layer use wireless communication technologies for data transmission, and the susceptibility of wireless signals to interference exposes them to eavesdropping, signal hijacking, and other attacks. The lack of effective encryption mechanisms in wireless communication allows attackers to forge transmitted data via man-in-the-middle attacks, thereby undermining data reliability. Perception-layer devices in IoT systems are often highly heterogeneous; differences in device types lead to inconsistent security mechanisms, increasing the complexity of security protection. Some perception devices lack proper access-control measures and can easily become entry points for unauthorized devices, creating potential security vulnerabilities. Attackers can impersonate legitimate devices to carry out intrusions. The maintenance cycle of perception-layer devices is short and updates are not timely; some devices do not consider future security requirements at the time of manufacture, leaving unpatched vulnerabilities. Remaining in an unpatched state for a long time, these devices are powerless against known attacks.

4.2 Issues in Data Protection

IoT systems use a large number of perception devices to collect and transmit massive amounts of sensitive data, which involve user privacy and corporate secrets, so the protection requirements are extremely stringent. Because IoT devices are diverse and widely distributed, the data's transmission and storage throughout the system often face multiple security risks. Data transmission in IoT relies on wireless communication, making the data vulnerable to eavesdropping, tampering, and other attacks during transit. Due to the open nature of wireless channels, unencrypted data streams can easily be altered by attackers through man-in-the-middle attacks, compromising data integrity. IoT devices have limited computing power and scarce storage resources, resulting in weak support for data encryption. Some devices fail to provide end-to-end encryption, and effective encryption measures are absent for data transmission between different nodes, thereby increasing the risk of data leakage. Data protection in IoT also faces problems of device authentication and access control. Lacking strict authentication mechanisms, attackers can forge legitimate devices and tamper with device identities to gain access to data. For unauthorized devices, attackers can remotely manipulate them to steal sensitive data stored on the devices [2].

4.3 Communication Security Issues

IoT communications rely on multiple wireless technologies such as Wi-Fi and Bluetooth, which are susceptible to interference and signal tampering. Wireless signals propagate without physical boundaries, allowing attackers to access the communication channel through various means, launch man-in-the-middle attacks, and thereby intercept or disrupt communication content. A vast number of IoT devices connect to the network; their sheer volume and wide distribution, together with diverse and complex communication links, make effective control of the network topology difficult. In such an environment, the data-encryption mechanisms between devices are often inadequate, and unencrypted communication data can be maliciously altered, compromising communication integrity. IoT communications employ lightweight protocols that prioritize low power consumption and high efficiency during design, yet fail to give sufficient consideration to security, making them easy entry points when facing specific attacks. Some protocols do not provide strict encryption for data, resulting in plaintext transmission issues that allow data to be tampered with during communication. Moreover, IoT devices frequently rely on public networks for connectivity, and the inherently low security of these public networks makes them vulnerable to large-scale network attacks, thereby undermining the availability of IoT communication links.

4.4 The Attack Surface of IoT Systems Has Expanded

IoT systems connect a large number of devices and sensors to the network, dramatically enlarging the attack surface. Traditional computer networks mainly face threats against end devices and servers, whereas IoT devices are diverse, widely distributed, and interconnected. The fusion of physical and virtual spaces allows attackers to operate across a much broader range. IoT devices themselves have limited storage capacity, and some lack adequate security measures, enabling attackers to compromise them with ease and thus broaden the scope of attacks. The heterogeneity of IoT devices makes it difficult to patch security vulnerabilities uniformly; attackers can exploit differences among devices to breach system defenses and achieve large-scale intrusions. As IoT systems continue to scale, attackers can launch assaults from a single device and propagate laterally through the network, leveraging other devices to create a chain reaction that magnifies the impact. IoT systems' cloud platforms tie IoT to traditional data centers; compromising the security of edge nodes can indirectly disrupt the entire IoT system [3].

5. COUNTERMEASURES FOR COMPUTER NETWORK SECURITY UNDER IOT TECHNOLOGY

5.1 Strengthening the Application of Firewalls and Intrusion Detection Systems

Firewalls are the first line of defense for IoT network security and must be custom-designed according to the characteristics of the IoT. Traditional firewalls control traffic based on ports, but some IoT devices communicate over non-standard ports, so firewalls need deep packet inspection capabilities to identify and filter abnormal traffic. IoT firewalls should support dynamic access control, adjusting in real time based on device identity and behavior patterns to counter ever-changing attack modes. For low-power devices in the IoT, firewall design must account for resource constraints, adopting lightweight yet efficient security policies to minimize impact on device performance. Complementing firewalls is intrusion detection technology; intrusion detection systems in IoT should provide multi-layer detection, identifying potential attacks at different levels. Network-traffic-based intrusion detection can analyze traffic patterns to uncover signs of malicious attacks, while host-based intrusion detection can delve into each device's operating system to detect malware, data tampering, and other behaviors. To improve detection accuracy, intrusion detection systems should support behavioral analysis, modeling normal device behavior patterns to promptly spot anomalous activities. Intrusion prevention systems can be tightly integrated with IDS, actively blocking attack traffic upon detecting intrusion signs to ensure system availability. Given the heterogeneity of IoT devices, intrusion detection technology should enable cross-platform collaboration, performing joint analysis with multi-dimensional data sources to enhance overall defense capabilities; the figure shows intrusion detection technology.

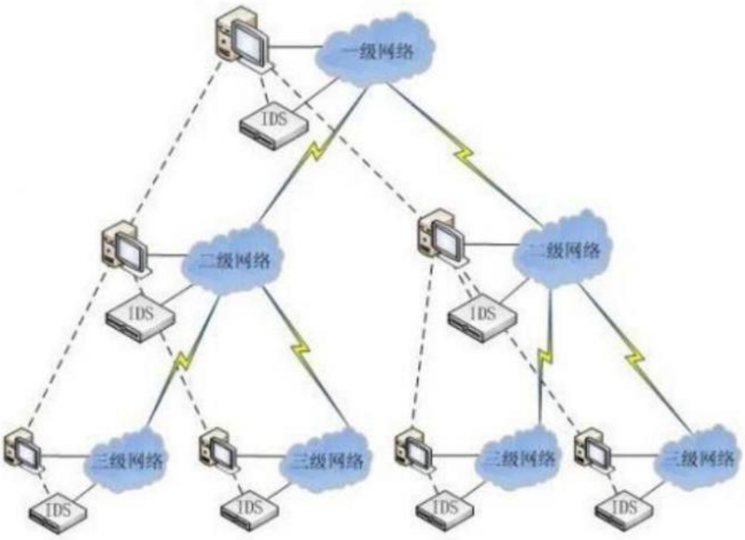

Figure 1: Intrusion Detection Technology

5.2 Strengthening the Management of Network Security Defense Mechanisms

The security defense mechanism of an IoT system should establish a sound management framework that clearly defines security roles and permissions, ensuring that all types of devices and nodes comply with strict security requirements during access, communication, and data exchange. Under this framework, a risk-based security assessment model should be adopted to periodically inspect and evaluate the security status of every link in the network, promptly identify potential vulnerabilities in the system, and formulate corresponding remediation measures. The security defense mechanism of an IoT network should implement comprehensive access control, dynamically monitoring all access points based on device identity to prevent unauthorized devices from taking control of the system. For different categories of IoT devices, access control should adopt lightweight, low-latency methods while ensuring the effectiveness of protective measures. Strengthen network traffic monitoring and analysis by deploying intelligent traffic analysis tools to identify potential attack patterns in real time, ensuring rapid response and defensive measures at the earliest stage of an attack. Traffic analysis tools should have self-learning capabilities, dynamically adjusting according to the network's normal communication patterns to adapt to ever-changing network threats. To improve the management level of the defense mechanism, a multi-layered protection system should be reinforced, setting up multiple defense layers at the network boundary and on terminal devices to form a closed-loop defense, ensuring that when one layer is breached, other layers can continue to function. For the management requirements of large-scale IoT systems, adopt a security management approach that combines centralized and distributed methods, leveraging the advantages of edge computing platforms to achieve centralized monitoring and distributed protection of IoT devices, thereby effectively enhancing the system's defense capability against large-scale attacks [4].

5.3 Real-time monitoring and control of the system

The IoT system should deploy a comprehensive real-time monitoring mechanism to ensure that anomalous behavior is detected at the earliest possible moment. Real-time monitoring should be combined with network traffic analysis, performing deep packet inspection and behavioral analysis on network traffic to promptly identify signs of attacks such as abnormal traffic and data tampering, preventing the attack from spreading within the system. The system should be equipped with intelligent intrusion detection and intrusion prevention systems to continuously monitor and analyze network behavior in real time, immediately triggering alerts and initiating automated defenses when an attack attempt is discovered, isolating the compromised devices to effectively block the propagation of the attack. To control the IoT system in real time, the security operations and maintenance platform should integrate centralized and distributed monitoring mechanisms, leveraging edge computing to process data at the network edge in real time, reducing data transmission latency and increasing response speed, ensuring that the cloud platform can centrally aggregate and analyze all security events and optimize defense strategies from a global perspective. Device performance monitoring should also be embedded in the real-time control mechanism, periodically obtaining device firmware versions and vulnerability scan results, and using automated update and remediation mechanisms to ensure that devices remain in the latest secure state.

5.4 Establishing Secure Routers

Secure routers should integrate deep packet inspection capabilities to analyze data packets in transit in real time, detecting and blocking potential attacks. By monitoring network traffic in real time, the secure router can identify anomalous behavior and promptly defend against threats from both internal and external sources. For the wireless communication technologies common in IoT environments, the router must support advanced encryption algorithms to ensure the confidentiality of data during transmission and prevent data tampering. To prevent the router itself from becoming an attack target, it should have firmware protection features, regularly patching vulnerabilities to prevent remote attacks via router flaws. The secure router should be able to automatically detect and isolate potential threats, automatically severing malicious connections upon detecting an attack, mitigating the impact and preventing the attack from spreading, while also supporting cross-protocol security protection to provide security assurance across different communication standards [5].

6. CONCLUSION

In summary, computer network security is a crucial component of IoT systems and the core element for ensuring information security. In the current IoT environment, computer network security still faces many challenges, leading to risks of data leakage. When building IoT systems, it is necessary to apply firewall technologies, implement intrusion detection mechanisms, and establish a comprehensive network security protection system, using dynamic monitoring to track system operation in real time, thereby effectively enhancing the security of IoT systems and promoting their steady development.

REFERENCES

[1] Su, Tian, et al. "Anomaly Detection and Risk Early Warning System for Financial Time Series Based on the WaveLST-Trans Model." (2025).

[2] Zhang, Yujun, et al. "MamNet: A Novel Hybrid Model for Time-Series Forecasting and Frequency Pattern Analysis in Network Traffic." arXiv preprint arXiv:2507.00304 (2025).

[3] Zhang, Zongzhen, Qianwei Li, and Runlong Li. "Leveraging Deep Learning for Carbon Market Price Forecasting and Risk Evaluation in Green Finance Under Climate Change." Journal of Organizational and End User Computing (JOEUC) 37.1 (2025): 1-27.

[4] Peng, Q., Planche, B., Gao, Z., Zheng, M., Choudhuri, A., Chen, T., Chen, C. and Wu, Z., 3D Vision-Language Gaussian Splatting. In The Thirteenth International Conference on Learning Representations.

[5] Peng, Qucheng, Ce Zheng, and Chen Chen. "Source-free domain adaptive human pose estimation." Proceedings of the IEEE/CVF International Conference on Computer Vision. 2023.

[6] Chen, Yilong, et al. "Dha: Learning decoupled-head attention from transformer checkpoints via adaptive heads fusion." Advances in Neural Information Processing Systems 37 (2024): 45879-45913.

[7] Tang, H., Yu, Z., & Liu, H. (2025). Supply Chain Coordination with Dynamic Pricing Advertising and Consumer Welfare An Economic Application. Journal of Industrial Engineering and Applied Science, 3(5), 1–6.

[8] Guo, Y. (2025, May). IMUs Based Real-Time Data Completion for Motion Recognition With LSTM. In Forum on Research and Innovation Management (Vol. 3, No. 6).

[9] Zhou, Z. (2025). Research on Software Performance Monitoring and Optimization Strategies in Microservices Architecture. Artificial Intelligence Technology Research, 2(9).

[10] Zhang, T. (2025). Research and Application of Blockchain-Based Medical Data Security Sharing Technology. Artificial Intelligence Technology Research, 2(9).

[11] Yu, Z. (2025). Advanced Applications of Python in Market Trend Analysis Research. MODERN ECONOMICS, 6(1), 115.

[12] Liu, Huanyu. "Research on Digital Marketing Strategy Optimization Based on 4P Theory and Its Empirical Analysis."

[13] Yu, Z., Sun, N., Wu, S., & Wang, Y. (2025, March). Research on Automatic Text Summarization Using Transformer and Pointer-Generator Networks. In 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT) (pp. 1601-1604). IEEE.

[14] Sun, N., Yu, Z., Jiang, N., & Wang, Y. (2025). Construction of Automated Machine Learning (AutoML) Framework Based on Large LanguageModels.

[15] Pal, P. et al. 2025. AI-Based Credit Risk Assessment and Intelligent Matching Mechanism in Supply Chain Finance. Journal of Theory and Practice in Economics and Management. 2, 3 (May 2025), 1–9.

[16] Gao W and Gorinevsky D 2020 Probabilistic modeling for optimization of resource mix with variable generation and storage IEEE Trans. Power Syst. 35 4036–45

[17] W. Gao and D. Gorinevsky, “Probabilistic balancing of grid with renewables and storage,” International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), 2018.

[18] Xu, Haoran. "CivicMorph: Generative Modeling for Public Space Form Development." (2025).

[19] Tu, Tongwei. "SmartFITLab: Intelligent Execution and Validation Platform for 5G Field Interoperability Testing." (2025).

[20] Xie, Minhui, and Boyan Liu. "DataFuse: Optimizing Interview Analytics Through Multimodal Data Integration and Real-Time Visualization." (2025).

[21] Zhu, Bingxin. "TaskComm: Task-Oriented Language Agent for Efficient Small Businesses Workflows." (2025).

[22] Hu, Xiao. "Low-Cost 3D Authoring via Guided Diffusion in GUI-Driven Pipeline." (2025).

[23] Tan, C. (2024). The Application and Development Trends of Artificial Intelligence Technology in Automotive Production. Artificial Intelligence Technology Research, 2(5).

[24] Zhuang, R. (2025). Evolutionary Logic and Theoretical Construction of Real Estate Marketing Strategies under Digital Transformation. Economics and Management Innovation, 2(2), 117-124.

[25] Han, X., & Dou, X. (2025). User recommendation method integrating hierarchical graph attention network with multimodal knowledge graph. Frontiers in Neurorobotics, 19, 1587973.

[26] Yang, J. (2025, July). Identification Based on Prompt-Biomrc Model and Its Application in Intelligent Consultation. In Innovative Computing 2025, Volume 1: International Conference on Innovative Computing (Vol. 1440, p. 149). Springer Nature.

[27] Yang, Zhongheng, Aijia Sun, Yushang Zhao, Yinuo Yang, Dannier Li, and Chengrui Zhou. "RLHF Fine-Tuning of LLMs for Alignment with Implicit User Feedback in Conversational Recommenders." arXiv preprint arXiv:2508.05289 (2025).

[28] Yang, Haowei, Yu Tian, Zhongheng Yang, Zhao Wang, Chengrui Zhou, and Dannier Li. "Research on Model Parallelism and Data Parallelism Optimization Methods in Large Language Model-Based Recommendation Systems." arXiv preprint arXiv:2506.17551 (2025).