Journal of Engineering, Project, and Production Management
2026, 16(5), 2026-0024

A Lightweight Authentication Protocol for Collaborative Manufacturing Systems in 5G Network Slicing

Xiaohuan Duan[1], Dongcai Cheng[2], and Yunping Wang[3]
[1] Associate Professor and the Vice Dean of the School of Information Engineering, Gansu Vocational and Technical College of Communications, please add your address
[2] General Manager, Hangzhou DPtech Technologies Co., Ltd, please add your address, E-mail: chendcaicdc@sina.com (corresponding author).
[3] Senior Engineer and Manager, Engineering and Technology Department, Gansu Civil Aviation Airport Group Co.

Production Management
Received April 23, 2026; revised May 8, 2026; accepted May 13, 2026
Available online June 4, 2026

Abstract: This work addresses critical security challenges in Industrial Internet of Things (IIoT) communication networks deployed in collaborative manufacturing systems within 5G network slicing environments by developing an efficient, lightweight security authentication protocol. This research utilizes optimized elliptic curve cryptography based on secp256r1 (also known as NIST P-256) parameters and introduces novel inter-slice authentication procedures, providing a comprehensive solution for seamless mobility across multiple network slices while maintaining security isolation. The proposed protocol supports diverse manufacturing scenarios, including real-time production control, resource planning and scheduling optimization, logistics coordination, and supply chain management. Formal verification through BAN logic analysis and automated ProVerif systems, complemented by performance analysis conducted in standard industrial communication environments with 50-200 devices per workshop area, validates the protocol's effectiveness. Performance results demonstrate enhanced efficiency with a 67% reduction in authentication delay compared to existing lightweight protocols, achieving end-to-end authentication delays of 16.8ms (milliseconds) under standard conditions. The protocol reduces memory usage by 52% and CPU utilization to 8.2%. Message overhead is maintained at 168 bytes, substantially below the 384-724 bytes of comparable protocols, while achieving authentication success ratios above 97% across operational scenarios. The protocol meets the lightweight criteria defined in this study, including an authentication delay of sub-20ms, memory usage under 200 KB, message overhead under 200 bytes, and CPU utilization below 10%, all validated on ARM Cortex-A53-class industrial hardware. These performance characteristics reduce authentication-related constraints in production scheduling and simplify cross-domain logistics coordination. The protocol complies with 3GPP Release 16 standards and demonstrates compatibility with existing Manufacturing Execution System (MES) and Enterprise Resource Planning (ERP) platforms.

Keywords: Collaborative manufacturing systems; 5G network slicing; lightweight authentication protocol; production scheduling; elliptic curve cryptography.

DOI 10.32738/JEPPM-2026-0024

1. Introduction

The rapid advancement of Industry 4.0 and intelligent manufacturing systems has driven unprecedented growth in Industrial Internet of Things (IIoT) communication networks. The transformation of manufacturing industries toward highly automated, collaborative production requires ultra-reliable communication infrastructure with low latency to facilitate real-time information exchange among manufacturing equipment, industrial robots, Automated Guided Vehicles (AGVs), and enterprise management systems (Sisinni et al., 2018). The integration of resource planning, production scheduling, and supply chain coordination within unified communication frameworks demands robust security mechanisms capable of protecting sensitive manufacturing data while maintaining operational efficiency (Sengupta et al., 2020).

5G New Radio (NR) technology with network slicing and Mobile Edge Computing (MEC) enables diverse manufacturing applications, ranging from real-time robotic control to massive sensor networks, with customized performance parameters and reduced communication latency (Agiwal et al., 2016; Li et al., 2018; Chettri and Bera, 2020). However, current authentication schemes face challenges in balancing security resilience and computational efficiency for

network slicing architectures (Cao et al., 2020), while the interconnection of production and supply chain systems amplifies security concerns (Serror et al., 2021). Recent analyses further identify layered attack vectors across orchestration, virtualization, and inter-slice communication in 5G slicing architectures, underscoring the need for dedicated security mechanisms at each architectural boundary (Dias et al., 2025). The convergence of wireless communication and cyber-physical systems introduces additional attack surfaces that compound these challenges (Burg et al., 2018), and edge computing paradigms further reshape the security landscape by distributing computation closer to industrial endpoints (Khan et al., 2019). Machine learning-based security methods require significant computing power unsuitable for resource-constrained environments (Boualouache and Engel, 2023).

Recent lightweight authentication schemes combining Elliptic Curve Cryptography (ECC) and token-based approaches (Yang et al., 2023) and multi-factor methods (Wang and Wang, 2018) have made progress, but critical security vulnerabilities persist across IoT deployments (Frustaci et al., 2018), and slice-aware authentication for 5G environments remains insufficiently addressed (Ni et al., 2018). Anonymous authentication with privacy preservation has also been explored for Industrial Internet of Things (IIoT) workshop environments, though integration with 5G network slicing remains an open problem (Li et al., 2024).

This work addresses these shortcomings by presenting a lightweight security authentication protocol for collaborative manufacturing scenarios in 5G-IIoT network slicing environments. In this study, a protocol is considered lightweight if it satisfies four criteria on resource-constrained industrial hardware (ARM Cortex-A53 class): authentication delay below 20ms, memory footprint under 200 KB, message overhead under 200 bytes, and CPU utilization below 10%. The protocol incorporates a cross-slice authentication mechanism that supports device mobility across multiple network slices without compromising security isolation. The research addresses three questions: (RQ1) How can an Elliptic Curve Cryptography (ECC) based authentication protocol achieve sub-20ms latency while preserving 128-bit security strength in resource-constrained IIoT environments? (RQ2) How can cross-slice authentication be realized without undermining slice isolation in 5G network slicing architectures? (RQ3) What operational impact does the proposed protocol have on manufacturing decision-making processes?

2. Data and Methods

2.1. System Model and Architecture Design

The proposed system model, presented in Fig. 1, integrates four functional tiers to support diverse manufacturing communication requirements. The architecture draws on mobile edge computing principles (Mao et al., 2017) for latency reduction and multi-access edge computing for IoT realization (Porambage et al., 2018), adapting these concepts to the demands of cross-slice authentication in collaborative manufacturing. The architecture supports Ultra-Reliable Low-Latency Communication (URLLC) for real-time production control, enhanced Mobile Broadband (eMBB) for equipment monitoring, and massive Machine-Type Communication (mMTC) for distributed sensor networks. The 5G core network provides access management, session management, and user-plane functions, including network slice selection, while MEC nodes reduce latency for time-sensitive applications.

The architectural layers in Fig. 1 define the operational environment within which the authentication protocol functions. At the device layer, each IIoT endpoint stores a pre-provisioned ECC key pair and a device identifier that serve as the cryptographic input for subsequent authentication exchanges. The radio access layer applies slice-specific Quality of Service (QoS) policies, prioritizing URLLC traffic for robotic control, eMBB for monitoring, and mMTC for sensor aggregation, before forwarding authentication requests to the core network. Within the 5G core, the Access and Mobility Management Function (AMF) routes incoming requests to the appropriate slice instance based on device credential scope, the Session Management Function (SMF) binds authenticated sessions to target slices, and the User Plane Function (UPF) enforces per-slice traffic separation. MEC nodes deployed at workshop boundaries cache recently validated credentials and perform local signature verification, reducing round-trip latency for time-sensitive production control transactions. At the application layer, secure gateways translate authenticated session tokens into interface-compatible formats for Manufacturing Execution System (MES) and Enterprise Resource Planning (ERP) platforms. The protocol workflow described in Section 2.2 is grounded in these structural constraints, with each phase targeting a specific functional boundary within the architecture.

2.2. Lightweight Security Authentication Protocol Design

Lightweight authentication protocols must balance security strength and computational efficiency in dynamic manufacturing environments (Kumar et al., 2019), while anonymous multi-factor authentication reduces overhead by distributing trust across device groups (Li, Niu, et al., 2018). As illustrated in Fig. 2, the protocol follows a five-phase framework. In the registration phase, each device generates a secp256r1 key pair (d_i, Q_i), where d_i is a random scalar and Q_i is the corresponding public point computed as Eq. (1).

$$Q_i = d_i \cdot G \tag{1}$$

The device submits Q_i along with its identifier ID_i to the authentication server, which returns a signed credential binding the device to its authorized slice set, as expressed in Eq. (2).

$$Cert_i = \{ID_i, Q_i, SliceScope, Sig_{AS}\} \tag{2}$$

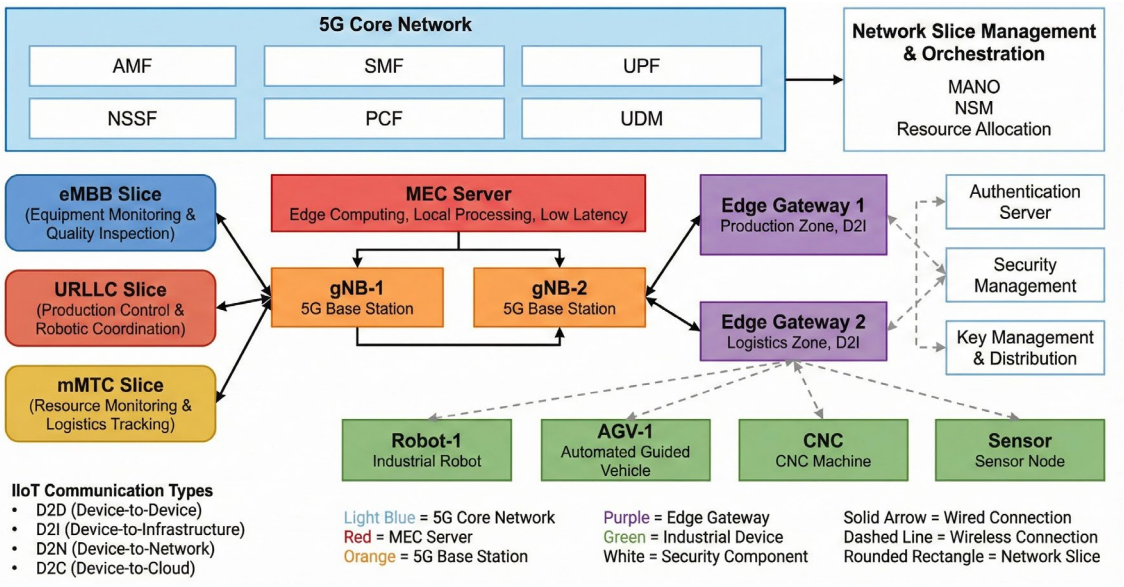


Fig. 1. Architecture diagram of 5G-IIoT network slicing system for collaborative manufacturing

During the authentication request phase, the device constructs a message M as defined in Eq. (3), containing a temporary pseudonymous identifier, a timestamp T_s, a fresh nonce, and a target slice identifier:

$$M = \{PseudoID_i, T_s, Nonce, SliceTarget\} \tag{3}$$

where the pseudonymous identifier is derived as $PseudoID_i = H(ID_i \mid SessionParam)$. The device signs M using the Elliptic Curve Digital Signature Algorithm (ECDSA) with private key d_i and transmits $M, Sig_i, Cert_i$ to the nearest MEC node. In the verification and forwarding phase, the MEC node checks timestamp freshness by rejecting messages where $|T_{current} - T_s| > \Delta t$, validates the credential format, and forwards valid requests to the core authentication server. During server processing, the server verifies the ECDSA signature against Q_i extracted from $Cert_i$, and computes a shared secret via Elliptic Curve Diffie-Hellman (ECDH) as shown in Eq. (4).

$$S = d_{AS} \cdot Q_i \tag{4}$$

A session key is then derived using HMAC-based Key Derivation Function (HKDF)-SHA256 with the nonce and timestamp as salt, as shown in Eq. (5).

$$K_{session} = \text{HKDF}(S, Nonce \mid T_s) \tag{5}$$

The session context is bound to the target slice identifier. Secure communication is established using AES-256-GCM encryption keyed by $K_{session}$, with session keys renewed every ten minutes to preserve forward secrecy.

ECC provides security equivalent to traditional systems with smaller key sizes, and recent hardware-software co-design approaches enable faster operations on constrained devices (Lara-Nino et al., 2018). As detailed in Table 1, the protocol employs secp256r1 parameters with 256-bit key lengths, providing 128-bit security strength, with key generation in under 2.5ms and verification in under 5.2ms.

Prior studies have identified security vulnerabilities in lightweight certificate mechanisms for constrained environments (Fang et al., 2018). The proposed protocol addresses these challenges through forward secrecy, anti-replay defenses, and privacy retention, achieving end-to-end latency under 15ms while supporting multiple slice types.

2.3. Network Slice Security Mechanisms

Network slicing technology enables the creation of multiple individual virtual networks on a given 5G infrastructure, providing customized services to diverse IIoT applications with varying security and performance requirements (Zhang, 2019). The proposed framework defines specialized network slices aligned with distinct manufacturing functions, including a production control slice supporting real-time robotic coordination and equipment communication. Resource management slice enabling production scheduling and capacity planning, and logistics slice facilitating AGV coordination and supply chain integration. Slice isolation prevents unauthorized access through network-based access limitations, encrypted communication, and security gateways (Olimid and Nencioni, 2020).

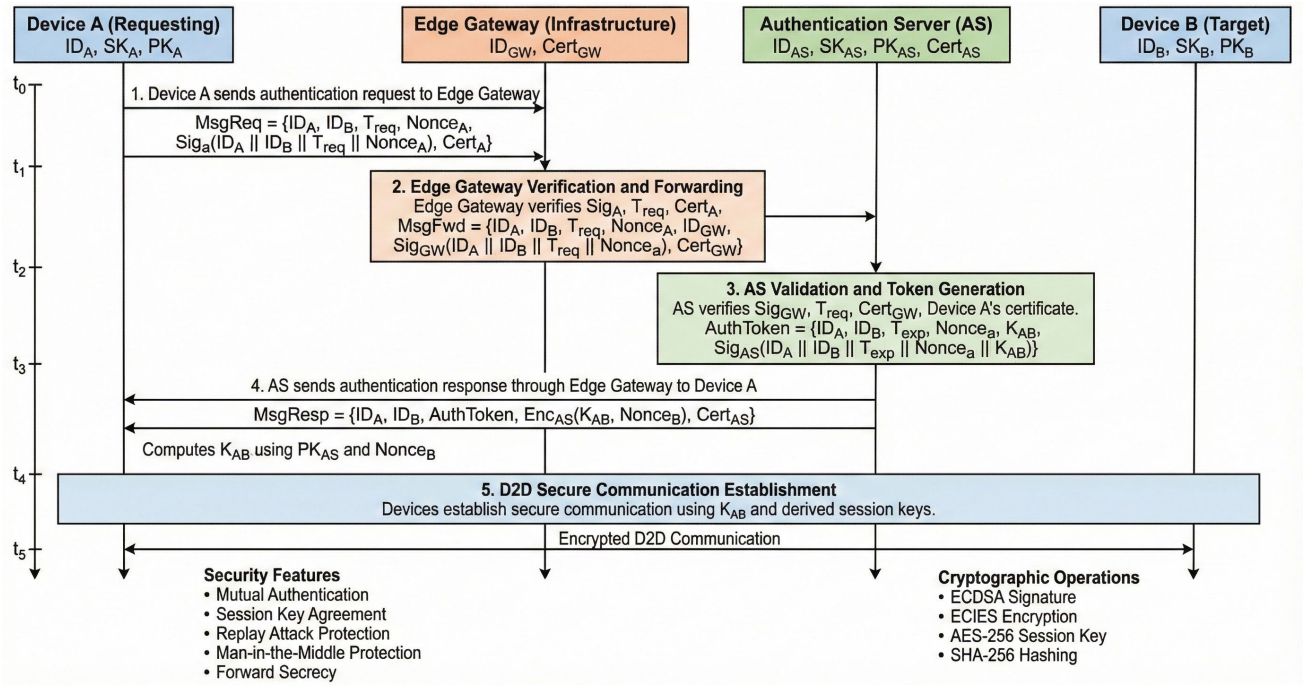


Fig. 2. Flowchart of lightweight security authentication protocol

Table 1. Protocol security attributes and cryptographic parameter configuration

Parameter Category	Parameter Name	Configuration Value	Security Strength	Description
Elliptic Curve Parameters	Elliptic Curve Type	secp256r1 (P-256)	128-bit	NIST standard curve
	Coordinate Length	256 bits	128-bit	Compressed: 257 bits
Hash Functions	Primary Hash Algorithm	SHA-256	128-bit	Message digest: 256 bits
	Key Derivation Function	HKDF-SHA256	128-bit	HMAC-based derivation
Digital Signature	Signature Algorithm	ECDSA-P256	128-bit	Elliptic Curve DSA
	Signature Length	512 bits (r,s)	128-bit	Two 256-bit integers
Key Management	Private Key Length	256 bits	128-bit	Random scalar
	Session Key Length	256 bits	128-bit	ECDH negotiation
	Key Update Period	10 minutes	-	Forward secrecy
Symmetric Encryption	Encryption Algorithm	AES-256-GCM	256-bit	Authenticated encryption
Performance	Key Generation	≤ 2.5 ms	-	Industrial ECU testing
	Signature Verification	≤ 5.2 ms	-	Single verification
	Protocol Total Latency	≤ 15 ms	-	End-to-end authentication
	Message Overhead	168 bytes	-	Authentication message
Network Slicing	Slice Types	URLLC/eMBB/mMTC	-	Multiple slice support
	QoS Guarantee	Latency ≤10ms, Rel. 99.999%	-	URLLC requirements

Notes: Security strength per NIST SP 800-57; Performance verified on ARM Cortex-A53 1.2GHz; Network slicing per 3GPP Release 16.

Cross-slice authentication addresses secure communication across multiple network slices. The protocol incorporates a hierarchical trust framework that allows devices to efficiently authenticate with varying slice instances (Ni et al., 2018),

enabling dynamic service-based and geographical slice selection across workshop boundaries. Dynamic resource allocation security incorporates real-time auditing to detect anomalies during resource allocation (Khan et al., 2020), while slice lifecycle management implements automated security policy execution and secure migration throughout the operational scope (Wijethilaka and Liyanage, 2021).

These mechanisms collectively ensure that security properties are maintained not only within individual slices but also during transitions across functional domains. The structural relationships among the three slice domains and the cross-slice authentication pathway are illustrated in Fig. 3.

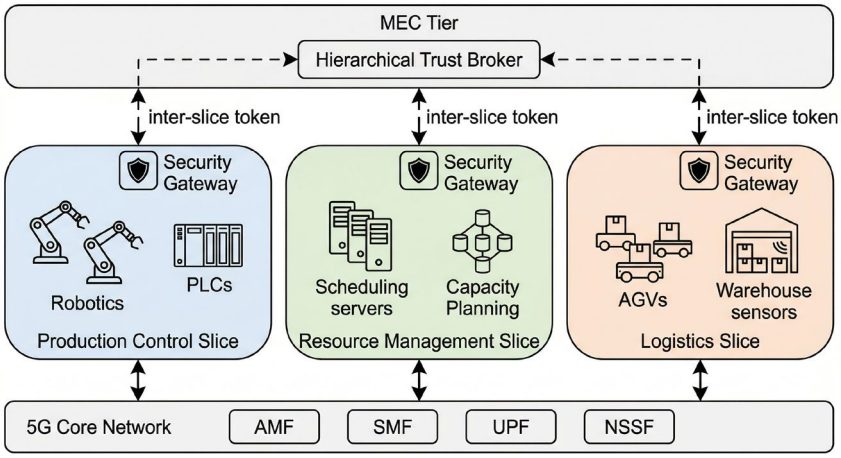


Fig. 3. Network slice security architecture and cross-slice authentication pathway

As shown in Fig. 3, each slice domain maintains an independent security perimeter enforced by a dedicated gateway that filters traffic according to slice-specific access policies. Cross-slice authentication is mediated through a hierarchical trust layer at the MEC tier, which issues short-lived inter-slice tokens upon confirming that the requesting device holds valid credentials in both the source and target slices. This mechanism preserves slice isolation as the default security posture while supporting legitimate device mobility across workshop boundaries without full re-registration.

2.4. Protocol Security Analysis Methods

This evaluation employs BAN logic combined with ProVerif automated verification to verify authentication features and privacy protection, following established practices in lightweight IoT authentication design (Chen et al., 2023). The security analysis framework addresses authentication, confidentiality, integrity, and non-repudiation requirements, drawing on physical layer security principles (Hamamreh et al., 2019). Attack scenario modeling considers eavesdropping, man-in-the-middle, replay, and slice-specific threats.

2.5. Performance Evaluation Method Design

The evaluation follows established IIoT performance analysis practices (Chettri and Bera, 2020; Sisinni et al., 2018), with parameters detailed in Table 2. The simulation environment is constructed using NS-3 (version 3.38) with the 5G-LENA module to emulate 5G NR radio access and core network behavior, while cryptographic operations are benchmarked on an ARM Cortex-A53 processor at 1.2 GHz to represent typical industrial edge hardware. Three test scenarios, flexible production (50 devices), cross-workshop coordination (100 devices), and high-throughput logistics (200 devices), are each executed over 30 independent runs with different random seeds, and reported metrics represent mean values with 95% confidence intervals. Four baseline protocols are selected for comparison: a certificate-based scheme (Fang et al., 2018), a lightweight mutual authentication protocol (Kumar et al., 2019), a multi-factor anonymous authentication approach (Li, Niu, et al., 2018), and an anonymous PUF-based method (Zhang et al., 2023), all implemented under identical network conditions with MEC integration following the framework of Pham et al. (2020).

3. Results

3.1. Protocol Security Verification Results

BAN logic and ProVerif verification confirm the efficacy of mutual authentication with no reachable confidentiality or integrity attacks, while satisfying forward secrecy, anti-replay, and non-repudiation requirements. The protocol meets key security requirements, including forward secrecy (10-minute session key updates), anti-replay (timestamp and nonce verification), and non-repudiation.

3.2. Computational Performance Evaluation Results

The computational overhead comparison across protocols is presented in Fig. 4, comprising six sub-figures that evaluate distinct performance dimensions.

Fig. 4(a) compares authentication delay, where the proposed protocol achieves 14.8ms compared to 38.6-67.3ms for baseline methods, a 67% reduction relative to the best-performing alternative; this improvement is attributed to the reduced round-trip exchanges enabled by MEC-based local validation. Fig. 4(b) illustrates key generation time, with the proposed

protocol requiring 2.3ms versus 6.4-12.1ms for baselines, a difference resulting from optimized scalar multiplication on secp256r1 parameters. Fig. 4(c) shows a signature verification time of 4.9ms, benefiting from precomputed base-point tables that accelerate ECDSA operations. Fig. 4(d) shows memory consumption of 156 KB, which is 52% lower than the 324 KB of the ECQV-based protocol, stemming from implicit certificate structures and compressed point representation. Fig. 4(e) displays CPU utilization under 100 devices per workshop, with the proposed protocol at 8.2% against 18.7-34.1% for alternatives. Fig. 4(f) compares message overhead, where the 168-byte authentication message is well below the 384-724 bytes of competing protocols due to pseudonymous identifier and compressed public key representation. The computational complexity of the hierarchical trust model supports scalability for large-scale deployments.

Table 2. Simulation environment and evaluation parameter configuration

Parameter Category	Parameter Name	Parameter Value	Description
Network Environment	Coverage Area	500m × 500m	Smart workshop scenario
	Base Station Count	4 units	5G gNB deployment
	Network Slice Count	3 slices	Control/Resource/Logistics
	Channel Bandwidth	20MHz	sub-6GHz band
Device Parameters	Device Count	50-200 devices	Dynamic variation
	AGV Speed	1-5 m/s	Indoor movement
	Communication Range	100-200m	Device-to-Device (D2D) / Device-to-Infrastructure (D2I) coverage
	Mobility Model	Plant Simulator	Industrial simulation
Security Parameters	Key Length	256-bit	ECC encryption
	Authentication Timeout	100ms	Low latency requirement
	Certificate Validity	24 hours	Dynamic update
	Attack Model	Passive/Active	Multiple threat scenarios
Performance Metrics	Authentication Delay	<50ms	Real-time requirement
	Communication Overhead	<1KB	Lightweight design
	Success Rate	>99%	Reliability guarantee
	CPU Utilization	<10%	Resource efficiency

A consolidated comparison extending beyond computational metrics is provided in Table 3. The proposed protocol is the only scheme providing complete cross-slice authentication and full MES/ERP compatibility while supporting edge computing integration. The weighted overall performance score of 9.2/10 is based on security (40%), computational efficiency (25%), communication performance (25%), and scalability (10%).

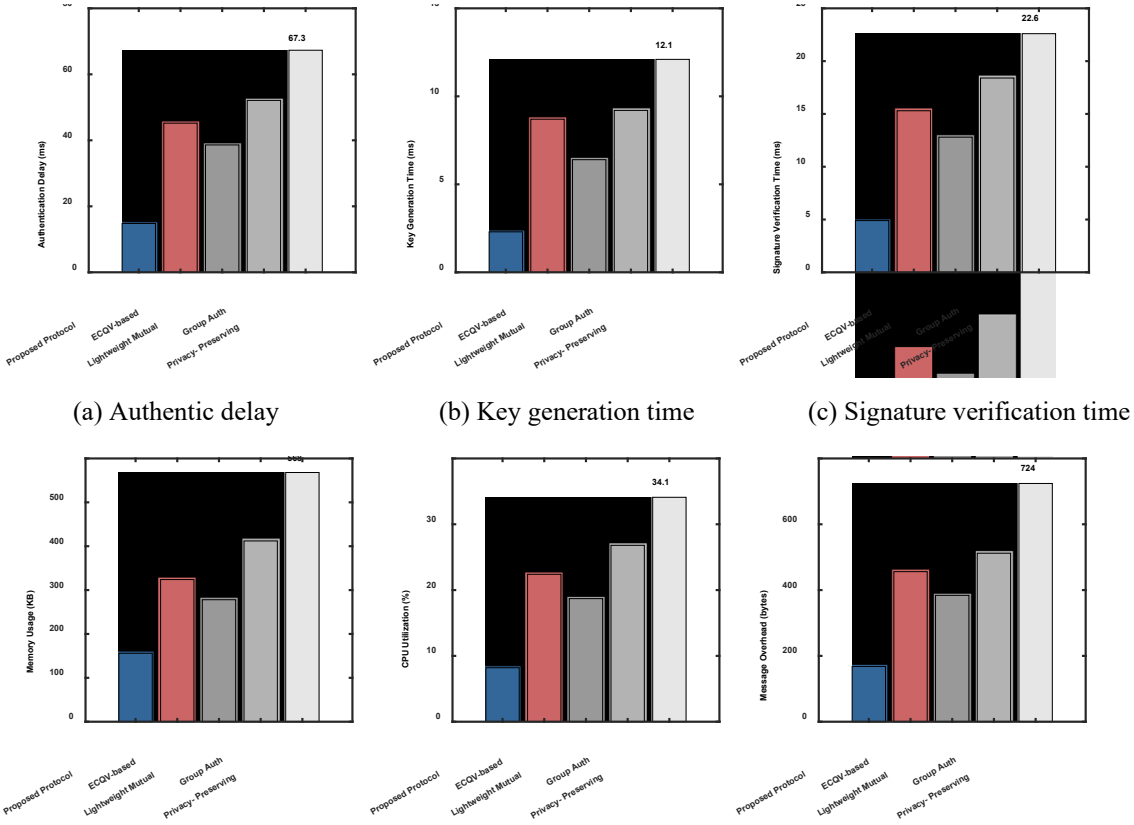
3.3. Communication Performance Evaluation Results

Communication performance under varying device densities is evaluated across workshop scenarios ranging from 50 to 200 concurrent devices, with results presented in Fig. 5.

Fig. 5(a) shows that the end-to-end delay increases from 12.4ms at 50 devices to 29.4ms at 200 devices, while baseline protocols range from 31.2 to 98.7ms under the same conditions. Moderate growth reflects MEC-based credential caching absorbing the additional authentication load. Fig. 5(b) presents authentication success rates, with the proposed protocol achieving 99.8% at 50 devices and 97.8% at 200 devices, compared to 95.6% for multi-factor anonymous authentication at the same density, because the hierarchical trust model distributes the verification load more evenly. Fig. 5(c) tracks bandwidth utilization scaling from 15.2% to 49.7% as devices increase, remaining within operational bounds due to the compact 168-byte message format. Fig. 5(d) depicts throughput at 842 packets per second (50 devices) declining to 506 packets per second (200 devices), maintaining stable capacity across the tested range. Fig. 5(e) reports packet loss below 2.2% for the proposed protocol across all densities, whereas multi-factor anonymous authentication reaches 9.9% at 200 devices under congestion due to centralized key management. Fig. 5(f) illustrates handover authentication latency during cross-slice transitions, demonstrating that the inter-slice token mechanism enables slice migration without full re-registration.

4. Discussion

The superior computational efficiency stems from optimized secp256r1 implementation (Lara-Nino et al., 2018), achieving 67% reduction in authentication delay compared to existing schemes (Yang et al., 2023). The cross-slice authentication function addresses shortcomings in traditional schemes, enabling seamless coordination across manufacturing functions (Ni et al., 2018).



(a) Authentic delay (b) Key generation time (c) Signature verification time

(d) Memory usage (e) CPU utilization (f) Message overhead

Fig. 4. Protocol computational overhead performance comparison

The utilization of forward secrecy mechanisms in combination with anti-replay prevention in the network slicing concept represents a significant improvement over certificate-based protocols lacking forward secrecy features (Fang et al., 2018). This configuration addresses critical limitations identified in recent evaluations of IIoT security schemes, including ongoing gaps between security needs and real-world implementation realities (Serror et al., 2021). Utilization of a hierarchical trust model facilitates smooth slice transitions while ensuring security isolation, aligning with emerging zero trust principles for network access control (Syed et al., 2022), an enhancement absent in similar authentication schemes that fail to address the integrated communication requirements of modern manufacturing, spanning production scheduling, resource allocation, and supply chain coordination (Afolabi et al., 2018).

The protocol also carries implications for manufacturing management decisions (RQ3). In production control, an authentication delay of less than 17ms allows scheduling algorithms to treat device re-authentication as a negligible cost rather than a constraint requiring buffer time. The cross-slice mechanism enables AGVs transitioning between production and logistics domains to maintain continuous authorization, eliminating manual security clearance steps that would otherwise delay rescheduling responses. The capacity to support over 500 concurrent devices at 99.4% success rate allows facility managers to scale device populations without provisioning additional authentication infrastructure, simplifying cost-benefit analysis for expansion decisions.

Several limitations should be noted. The simulation assumes stable 5G NR connectivity with four base stations covering a 500 meters (m) × 500 m area, which may not hold in smaller facilities or environments with radio interference from metallic structures. Performance evaluation covers up to 200 devices per workshop. Projections beyond this scale have not been validated through direct experimentation. The timestamp-based anti-replay mechanism depends on synchronized clocks, introducing a potential vulnerability if GPS time sources are compromised, although the encrypted nonce provides a secondary defense (Olimid and Nencioni, 2020). The study also assumes homogeneous device capabilities at the ARM Cortex-A53 level, whereas real manufacturing environments may include legacy controllers with more limited resources.

The evaluation relies on NS-3 simulation rather than physical testbed deployment, which may not capture radio propagation anomalies caused by metallic enclosures and electromagnetic interference common in factory floors. The threat model addresses network-layer attacks but does not account for side-channel attacks targeting cryptographic implementations on embedded hardware, nor does it consider physical tampering scenarios. The protocol design assumes a single administrative domain, leaving cross-enterprise authentication involving multiple trust authorities unaddressed. Interoperability testing with commercial 5G core equipment from different vendors has not been conducted, and vendor-

specific implementation differences may affect protocol behavior in production deployments.

Table 3. System overall performance test results comparison

Performance Metric	Proposed Protocol	ECQV-based	Lightweight Mutual	Group Auth	Privacy-Preserving
Mutual Authentication	✓	✓	✓	✓	✓
Forward Secrecy	✓	✗	✓	✗	✓
Anti-Replay Attack	✓	✓	✓	✓	✓
Anonymity Protection	✓	✗	✓	✓	✓
Security Level	High	Medium	Medium	Low	High
Authentication Delay (ms)	14.8	45.2	38.6	52.1	67.3
Key Generation Time (ms)	2.3	8.7	6.4	9.2	12.1
Memory Usage (KB)	156	324	278	412	568
CPU Utilization (%)	8.2	22.4	18.7	26.8	34.1
Message Overhead (bytes)	168	456	384	512	724
End-to-End Delay (ms)	16.8	47.8	41.4	57.8	72.1
Success Rate (%)	99.4	97.1	98.0	95.6	94.2
Max Devices Supported	>500	200-300	300-400	150-250	100-200
Network Slice Support	✓	✗	✗	✗	Partial
Cross-Slice Authentication	✓	✗	✗	✗	✗
Edge Computing Support	✓	✗	✓	✗	✓
MES/ERP Compatibility	✓	✗	Partial	✗	Partial
Overall Performance Score	9.2/10	6.1/10	7.3/10	5.4/10	6.8/10
Industrial Suitability	Excellent	Fair	Good	Poor	Fair

Notes: ✓ = Fully Supported, ✗ = Not Supported, Partial = Limited Support. Performance metrics tested under standard industrial scenarios (100 devices/workshop). Overall scores based on weighted evaluation of security (40%), computational efficiency (25%), communication performance (25%), and scalability (10%).

Future work could validate the protocol on physical testbeds incorporating heterogeneous hardware configurations, including legacy programmable logic controllers and newer ARM Cortex-M series processors, at device scales exceeding 500 units. Hybrid timing mechanisms combining GPS with network-derived synchronization warrant investigation to mitigate clock-related vulnerabilities. Integration of lightweight anomaly detection at the MEC tier represents another practical direction for strengthening runtime security without increasing device-side overhead (Boualouache and Engel, 2023). Cross-enterprise trust federation and protocol adaptation to emerging 6G network architectures also merit exploration as manufacturing ecosystems expand beyond single-site boundaries.

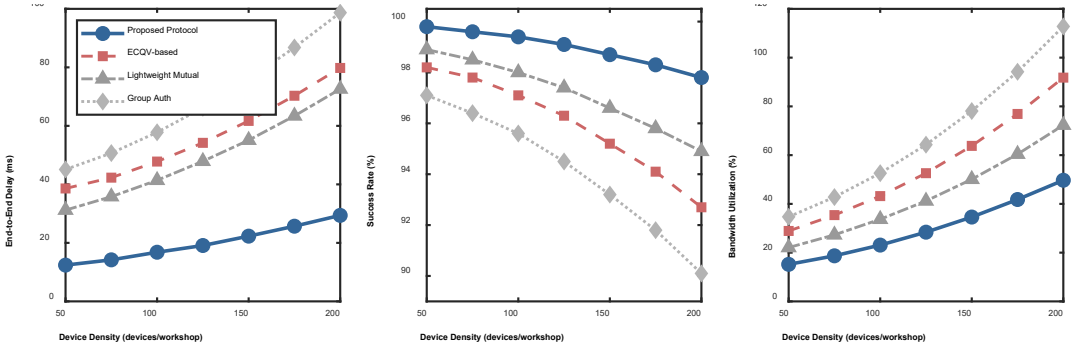
5. Conclusion

This paper presents a lightweight authentication protocol for collaborative manufacturing systems in 5G-IIoT network slicing environments. The protocol meets the lightweight criteria defined in this study, achieving 14.8ms authentication delay, 156 KB memory consumption, 168 bytes message overhead, and 8.2% CPU utilization on ARM Cortex-A53 hardware (RQ1). A hierarchical trust model with short-lived inter-slice tokens enables device mobility across production control, resource planning, and logistics slices while preserving slice isolation without re-registration (RQ2). Formal verification through BAN logic and ProVerif confirms resistance to eavesdropping, replay, and man-in-the-middle attacks.

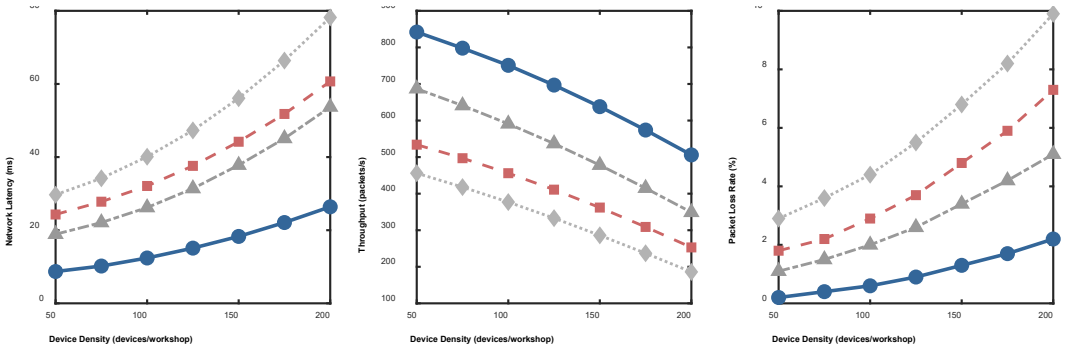
From a management perspective (RQ3), the protocol reduces authentication-related constraints in production scheduling, supports capacity expansion at 99.4% success rates across 500 concurrent devices, and simplifies cross-domain logistics coordination by replacing per-zone approval workflows with a unified trust hierarchy. Compliance with 3GPP Release 16 and compatibility with MES and ERP platforms support integration into existing infrastructure, while the identified limitations indicate directions for future testbed-based validation.

Author Contributions

Xiaohuan Duan contributed to the conception and design, the preparation of materials and the drafting of the manuscript. Dongcai Cheng contributed to conception and design, and to manuscript review and revision. Yunping Wang contributed to material preparation, data collection, analysis and drafting of the manuscript.



(a) End-to-end delay (b) Message transmission success rate (c) Bandwidth utilization



(d) Network latency (e) Throughput performance (f) Packet loss rate

Fig. 5. Communication performance evaluation results

Funding

This research received no specific financial support from any funding agency.

Institutional Review Board Statement

Not applicable.

Declaration of Artificial Intelligence (AI) Tools

During the preparation of this manuscript, the authors used Claude (Anthropic) for English language polishing, grammar correction, and readability improvement of the draft text. The authors reviewed, edited, and verified all output produced by the tool and take full responsibility for the content of this publication. No AI tools were used for research ideas, development of methodology, design of experiments, data collection, data analysis, interpretation of results, or formulation of conclusions presented in this work.

References

Afolabi, I., Taleb, T., Samdanis, K., Ksentini, A., and Flinck, H. (2018). Network slicing and softwarization: A survey on principles, enabling technologies, and solutions. *IEEE Communications Surveys & Tutorials*, 20(3), 2429–2453.

Agiwal, M., Roy, A., and Saxena, N. (2016). Next generation 5G wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 18(3), 1617–1655.

Boualouache, A., and Engel, T. (2023). A survey on machine learning-based misbehavior detection systems for 5G and beyond vehicular networks. *IEEE Communications Surveys & Tutorials*, 25(2), 1128–1172.

Burg, A., Chattopadhyay, A., and Lam, K. Y. (2018). Wireless communication and security issues for cyber-physical systems and the Internet-of-Things. *Proceedings of the IEEE*, 106(1), 38–60.

Cao, J., Ma, M., Li, H., Ma, R., Sun, Y., Yu, P., and Xiong, L. (2020). A survey on security aspects for 3GPP 5G networks. *IEEE Communications Surveys & Tutorials*, 22(1), 170–195.

Chen, C., Guo, H., Wu, Y., Shen, B., Ding, M., and Liu, J. (2023). A lightweight authentication and key agreement protocol for IoT-enabled smart grid system. *Sensors*, 23(8), 3991.

Chettri, L., and Bera, R. (2020). A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. *IEEE Internet of Things Journal*, 7(1), 16–32.

Dias, J., Pinto, P., Santos, R., and Malta, S. (2025). 5G network slicing: security challenges, attack vectors, and mitigation approaches. *Sensors*, *25*(13), 3940.

Fang, D., Qian, Y., and Hu, R. Q. (2018). Security for 5G mobile wireless networks. *IEEE Access*, 6, 4850–4874.

Frustaci, M., Pace, P., Aloi, G., and Fortino, G. (2018). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things Journal*, 5(4), 2483–2495.

Hamamreh, J. M., Furqan, H. M., and Arslan, H. (2019). Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 21(2), 1773–1828.

Khan, L. U., Yaqoob, I., Tran, N. H., Han, Z., and Hong, C. S. (2020). Network slicing: Recent advances, taxonomy, requirements, and open research challenges. *IEEE Access*, 8, 36009–36028.

Khan, W. Z., Ahmed, E., Hakak, S., Yaqoob, I., and Ahmed, A. (2019). Edge computing: A survey. *Future Generation Computer Systems*, 97, 219–235.

Kumar, P., Gurtov, A., Sain, M., Martin, A., and Ha, P. H. (2019). Lightweight authentication and key agreement for smart metering in smart energy networks. *IEEE Transactions on Smart Grid*, 10(4), 4349–4359.

Lara-Nino, C. A., Diaz-Perez, A., and Morales-Sandoval, M. (2018). Elliptic curve lightweight cryptography: A survey. *IEEE Access*, 6, 72514–72550.

Li, N., Ma, M., and Wang, H. (2024). ASAP-IIOT: an anonymous secure authentication protocol for industrial internet of things. *Sensors*, *24*(4), 1243.

Li, S., Da Xu, L., and Zhao, S. (2018). 5G Internet of Things: A survey. *Journal of Industrial Information Integration*, 10, 1–9.

Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A. K., and Choo, K. K. R. (2018). A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments. *Journal of Network and Computer Applications*, 103, 194–204.

Mao, Y., You, C., Zhang, J., Huang, K., and Letaief, K. B. (2017). A survey on mobile edge computing: The communication perspective. *IEEE Communications Surveys & Tutorials*, 19(4), 2322–2358.

Ni, J., Lin, X., and Shen, X. S. (2018). Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT. *IEEE Journal on Selected Areas in Communications*, 36(3), 644–657.

Olimid, R. F., and Nencioni, G. (2020). 5G network slicing: A security overview. *IEEE Access*, 8, 99999–100009.

Pham, Q. V., Fang, F., Ha, V. N., Piran, M. J., Le, M., Le, L. B., Hwang, W. J., and Ding, Z. (2020). A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art. *IEEE Access*, 8, 116974–117017.

Porambage, P., Okwuibe, J., Liyanage, M., Ylianttila, M., and Taleb, T. (2018). Survey on multi-access edge computing for Internet of Things realization. *IEEE Communications Surveys & Tutorials*, 20(4), 2961–2991.

Sengupta, J., Ruj, S., and Das Bit, S. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications*, 149, 102481.

Serror, M., Hack, S., Henze, M., Schuba, M., and Wehrle, K. (2021). Challenges and opportunities in securing the Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 17(5), 2985–2996.

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., and Gidlund, M. (2018). Industrial Internet of Things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics*, 14(11), 4724–4734.

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., and Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access*, 10, 57143–57179.

Wang, D., and Wang, P. (2018). Two birds with one stone: Two-factor authentication with security beyond conventional bound. *IEEE Transactions on Dependable and Secure Computing*, 15(4), 708–722.

Wijethilaka, S., and Liyanage, M. (2021). Survey on network slicing for Internet of Things realization in 5G networks. *IEEE Communications Surveys & Tutorials*, 23(2), 957–994.

Yang, Y. S., Lee, S. H., Wang, J. M., Yang, C. S., Huang, Y. M., and Hou, T. W. (2023). Lightweight authentication mechanism for industrial IoT environment combining elliptic curve cryptography and trusted token. *Sensors*, 23(10), 4970.

Zhang, Q., Wu, J., Zhong, H., He, D., and Cui, J. (2023). Efficient anonymous authentication based on physically unclonable function in industrial Internet of Things. *IEEE Transactions on Information Forensics and Security*, 18, 233–247.

Zhang, S. (2019). An overview of network slicing for 5G. *IEEE Wireless Communications*, 26(3), 111–117.

Xiaohuan Duan received his master's degree in computer science and technology from Chongqing Jiaotong University. He currently serves as an Associate Professor and the Vice Dean of the School of Information Engineering at Gansu Vocational and Technical College of Communications. He has been invited to serve as a subject-matter expert to deliver various technical talks on network security, ICT professional development, and vocational education reform. He has published more than twenty articles in reputable peer-reviewed journals and conference proceedings and has co-authored a textbook on wireless network planning and implementation. His research interests include network security, wireless network planning, vocational education and teaching reform, and the application of artificial intelligence in education.

Dongcai Cheng graduated from Lanzhou University with a master's degree in business administration from Lanzhou University. He has worked in the artificial intelligence and information technology industries for twelve years and currently serves as General Manager of Hangzhou Dipu Technology Co., Ltd. branch. He has been invited to serve as an industry expert to deliver technical lectures on AI and network security to support industry development. Simultaneously participated in over twenty national and provincial major projects, published one SCI paper as first author, and obtained one national invention patent as second author. His research interests include the application of artificial intelligence, big data, and network security in communication, transportation, and urban governance.

Yunping Wang graduated from Chongqing Jiaotong University with a major in computer science and technology in 2013. He is currently a Senior Engineer and serves as the Manager of the Engineering and Technology Department at Gansu Aviation Digital Intelligence Technology Co., Ltd. He has long been engaged in the planning, design, engineering construction, and project management of civil aviation airports and educational Informatization. He has presided over multiple provincial and ministerial-level scientific research projects and received numerous awards, including the Second Prize of Gansu Provincial Science and Technology Progress. He has published over ten professional papers and holds one invention patent, two utility model patents, six software copyrights, and three provincial-level scientific and technological achievements. Concurrently, he serves as a Director of the Gansu Artificial Intelligence Society, a Director and Think Tank Expert of the Gansu Emergency Informatization Association, a Member of the Emergency Informatization Expert Database of the Gansu Provincial Department of Emergency Management, a Gansu Provincial Government Procurement Review Expert, and a Professional Member of the China Computer Federation (CCF).