STM JOURNALS

International Journal of
Wireless Security and Networks

ISSN: 2584-0703
Volume 3, Issue 1, 2025
January–June
DOI (Journal): 10.37591/IJWSN

https://journals.stmjournals.com/ijwsn

Review IJWSN

Network Security Secure Communication in Industrial Networks

V. Basil Hans*

Abstract

In an era dominated by rapid industrial digitization, ensuring the security of communication in industrial networks has become a critical challenge. Industrial networks, which facilitate seamless communication between machines, devices, and systems, are increasingly targeted by cyber threats that can disrupt operations, compromise sensitive data, and jeopardize safety. This article delves into the key aspects of secure communication in industrial networks, emphasizing the role of advanced encryption techniques, robust authentication protocols, and real-time monitoring systems. It explores the unique vulnerabilities inherent in industrial control systems (ICS) and operational technology (OT) environments, highlighting the need for tailored security measures that align with industry standards like IEC 62443 and NIST Cybersecurity Framework. The article also examines emerging trends such as zero-trust architectures, blockchain for immutable data exchange, and the integration of artificial intelligence for predictive threat detection. By addressing the challenges of scalability, interoperability, and legacy system security, this work provides actionable insights for enhancing the resilience of industrial networks. Ultimately, the discussion underscores that secure communication is not merely a technical requirement but a strategic imperative for safeguarding industrial operations in a connected, data-driven world.

Keywords: Data exchange, industrial operations, secure communication, industrial networks, internet of things (IoT)

INTRODUCTION TO INDUSTRIAL NETWORKS

Industrial networks are an essential but often overlooked component of modern-day automation. These networks constitute the infrastructure supporting the communication and interaction between a broad range of different device types, varying from traditional sensors and actuators to advanced programmable logic controllers and operator panels, but also comprising drives, servo controllers, and robot controllers, to name only a few. This interaction is essential for any kind of automation task carried out in a factory. Industrial networks are the systems responsible for sending control signals to actuators on the base of sensor readings, thereby making a factory "intelligent." Besides this, they usually control or implement closed-loop control processes, maintaining the desired state steady.

The first industrial networks came into existence with the third industrial revolution, leading to the introduction of programmable logic controllers (PLCs) that streamlined the automation of manufacturing processes. With the PLCs and the factory network, communication among controllers, drives, and operator panels was carried out. These traditional systems generally work over legacy physical media and accelerate the adoption of digital networks as their communication channels. Even though these networks have limitations compared to new networks based on Ethernet or long-term evolution (LTE) like reliability,

***Author for Correspondence**
V. Basil Hans
E-mail: vhans2011@gmail.com

Research Professor, Department of Management & Commerce, Srinivas University, Mangaluru, Karnataka, India

Received Date: January 22, 2025
Accepted Date: January 29, 2025
Published Date: February 24, 2025

Citation: V. Basil Hans. Network Security Secure Communication in Industrial Networks. International Journal of Wireless Security and Networks. 2025; 3(1): 1–8p.

scalability, and most of the required services in modern factory networks, they will still persist, creating islands of digital networks with gates among them. With the advent of the fourth industrial revolution, often referred to as industry 4.0, modern digital networks will be greatly expanded and exposed to the internet, thus alarming the need for a well-defined communication.

LITERATURE REVIEW

The literature on network security, particularly in the context of industrial networks, has evolved significantly in recent years, reflecting the increasing complexity and sophistication of cyber threats. The exploration of internet of things (IoT) security has become particularly pertinent as IoT devices proliferate in critical infrastructures and everyday environments. In a foundational contribution, Hamza et al. [1] present a thorough examination of IoT network security requirements, threats, and countermeasures. Their work emphasizes the necessity for a robust IoT security framework, highlighting the unique vulnerabilities posed by IoT devices as compared to traditional information technology (IT) systems. By surveying various attack vectors and categorizing them based on their potential impact, the authors provide a critical resource for network operators seeking to enhance their understanding of IoT security challenges.

Building upon this understanding, Li et al. [2] offer a comprehensive survey of network security within Industrial Control Systems (ICS). Their analysis includes a detailed review of prevalent network protocols, identifying vulnerabilities and proposing defense mechanisms. This paper underscores the importance of multi-layered security strategies, including data encryption and intrusion detection systems, which are essential for safeguarding ICS against increasingly sophisticated cyber threats. The authors' focus on defense-in-depth strategies complements the insights provided by Hamza et al. [1], reinforcing the notion that a nuanced approach is necessary for effective network security in industrial settings.

Further contributing to the discourse, Okporokpo et al. [3] conducted a systematic literature review on trust-based approaches to IoT security. They categorize various trust-based systems into observation-based, knowledge-based, and cluster-based techniques, providing a critical analysis of their effectiveness and associated challenges. This review highlights the ongoing research into trust management as a vital component of IoT security, particularly within industrial contexts. The authors also identify key gaps in existing literature, such as the need for more robust mechanisms to manage untrustworthy entities within IoT networks. Their findings resonate with the earlier works by emphasizing the necessity of innovative approaches to address the evolving landscape of cyber threats.

Together, these articles illustrate the multifaceted nature of network security in industrial environments, emphasizing the critical need for comprehensive strategies that integrate various security measures and frameworks. The collective insights from these studies underscore the urgency of advancing research and development in network security to effectively mitigate the risks posed by increasingly sophisticated cyber threats in both IoT and ICS domains.

In the article "IoT Network Security: Requirements, Threats, and Countermeasures" by Hamza et al. [1], the authors provide a comprehensive examination of the security challenges posed by the increasing integration of IoT devices within critical infrastructures, enterprises, and households. The paper effectively underscores the urgency for robust IoT network security solutions, particularly in light of the sophisticated cyber-attacks that have been reported, which exploit vulnerabilities in both active and passive forms.

The authors begin by delineating the fundamental differences between IoT and traditional IT systems, emphasizing that IoT environments often incorporate a diverse array of devices with varying security capabilities. This distinction is crucial as it sets the stage for understanding the unique vulnerabilities that IoT networks face [1]. The paper highlights that many existing security measures are insufficient

when applied to IoT systems, which necessitates the development of tailored security solutions that address the specific needs of these networks.

One of the key contributions of the article is its detailed survey of IoT attack vectors and cyber threats. The authors categorize various attack techniques, providing examples of how these attacks can compromise network security. This classification serves as a valuable resource for network operators, enabling them to identify potential threats and implement appropriate countermeasures. The discussion on the shortcomings of existing security solutions is particularly insightful, as it reveals gaps that need to be addressed to enhance the overall security posture of IoT networks [1].

Moreover, the authors propose a framework for IoT network security system architecture that includes essential components necessary for mitigating risks. This framework is a significant contribution, as it not only outlines the requirements for effective security measures but also encourages stakeholders to collaborate in enhancing IoT security. The emphasis on stakeholder perspectives is a noteworthy aspect of the paper, as it recognizes that a multi-faceted approach involving various parties is essential to fortifying IoT security [1].

The article titled "Network Security in the Industrial Control System: A Survey" authored by Li et al. [2] provides a thorough examination of the current landscape of network security within ICS. The authors systematically categorize and analyze prevalent network protocols utilized in ICS, highlighting their inherent vulnerabilities and proposing potential defense mechanisms. This foundational approach is critical, as it lays the groundwork for understanding the unique security challenges faced by industrial networks.

One of the significant contributions of this paper is its detailed exploration of defense strategies, specifically focusing on data encryption, access control policies, and intrusion detection systems. The authors emphasize the importance of a "defense in depth" strategy, which integrates multiple layers of security controls to protect against various types of threats. This multifaceted approach is particularly relevant in the context of ICS, where the convergence of operational technology and information technology creates complex security scenarios.

The authors effectively illustrate the vulnerabilities associated with widely used protocols, which can serve as entry points for cyberattacks. By analyzing these vulnerabilities, the article not only raises awareness but also guides practitioners in selecting appropriate defense mechanisms tailored to their specific network configurations. The discussion on data encryption is particularly pertinent, as it underscores the necessity of securing sensitive data transmitted across industrial networks. Furthermore, the evaluation of access control policies highlights the need for stringent user authentication and authorization processes to mitigate unauthorized access.

However, while the article provides a comprehensive overview, it could benefit from a deeper exploration of the practical implementation challenges associated with the proposed defense measures. For instance, the integration of advanced intrusion detection systems within existing ICS infrastructure may face operational hurdles that are not sufficiently addressed in the survey. Additionally, a discussion on the evolving nature of cyber threats and how these defense strategies can adapt over time would enhance the article’s relevance in a rapidly changing security landscape.

The article "Trust-based Approaches Towards Enhancing IoT Security: A Systematic Literature Review" by Okporokpo et al. [3] provides a comprehensive examination of trust-based methodologies aimed at improving the cybersecurity of IoT networks. This systematic literature review (SLR) categorizes various trust-based systems into three primary types: observation-based, knowledge-based, and cluster-based systems. Each category is critically analyzed, shedding light on the strengths and weaknesses inherent in these approaches.

The authors effectively highlight the significance of trust in managing IoT networks, emphasizing that trust-based management techniques are crucial for identifying and eliminating untrustworthy entities within these systems. This is particularly pertinent as the evolution of IoT technology continues to introduce new threats and vulnerabilities, necessitating robust security frameworks. The article underscores the dynamic nature of cybersecurity challenges in IoT, where emerging threats require continuous adaptation of security measures.

Moreover, the authors identify several open issues and challenges related to trust and reputation management in IoT, paving the way for future research. This identification of gaps is critical as it not only informs the academic community but also assists practitioners in understanding the limitations of current methodologies. The discussion on the industrial internet of things (IIoT) security architecture, referencing the work of Tan and Azman, further enriches the review by contextualizing trust-based approaches within a broader security framework. The four-layer security architecture based on the CIA+ (Confidentiality, Integrity, Availability, and additional parameters) model provides a structured perspective on addressing security requirements specific to IIoT technologies.

The article also incorporates insights, which enhances the discussion on trust management strategies by outlining their respective advantages and disadvantages. This comparative analysis is invaluable as it equips readers with a nuanced understanding of the trade-offs involved in implementing different trust-based systems.

The reviewed literature highlights the critical advancements and ongoing challenges in network security, particularly within the realms of ICS and the IoT. The foundational work by Hamza et al. [1] lays the groundwork for understanding the unique security requirements and vulnerabilities associated with IoT devices. They emphasize the necessity for a tailored security framework that addresses the distinct characteristics of IoT networks, which differ significantly from traditional IT systems. Their comprehensive survey of attack vectors offers valuable insights for network operators, enabling them to identify potential threats and implement effective countermeasures.

Li et al. [2] build upon this foundation by examining network security in ICS. Their analysis of prevalent network protocols and defense mechanisms underscores the importance of a multi-layered security approach, including data encryption and intrusion detection systems. Further enriching the discourse, Okporokpo et al. [3] provide a systematic literature review on trust-based approaches to IoT security. They categorize trust-based systems into observation-based, knowledge-based, and cluster-based techniques, highlighting their respective strengths and weaknesses. Their identification of gaps in existing literature, particularly regarding the management of untrustworthy entities in IoT networks, points to the need for innovative security solutions. The incorporation of trust management into the broader security framework for IoT is crucial as it addresses the dynamic nature of cybersecurity challenges in these networks.

In conclusion, the collective insights from these studies illustrate the multifaceted nature of network security in industrial contexts. The emphasis on tailored security frameworks, multi-layered defense strategies, and trust-based management approaches underscores the urgency for continuous research and development in this field. As cyber threats become increasingly sophisticated, the need for comprehensive and adaptive security measures in both IoT and ICS domains is paramount.

IMPORTANCE OF SECURE COMMUNICATION IN INDUSTRIAL NETWORKS

Industrial networks play a fundamental role in the interaction and control of physical entities in modern industrial environments. When these processes are automated, the interaction is mediated by networks, so that industrial control systems can operate in a more efficient and flexible way. However, the associated communication between field devices also introduces several risks. Given the increasing complicity of industrial networks, attacks against them can compromise the confidentiality, integrity and availability of the exchanged information, and therefore hinder dependable operation of the

connected devices [4]. Traditional automation and control solutions do not address the attack vectors in modern industrial networks and there are several complementary technologies, implementations and regulations for effective protection. Beside the financial losses, the possible consequences of an attack in industrial networks are so catastrophic that there exists a specific need for the research in intrusion detection and other counteracting. Industrial networks differ in terms of technology, features and applicability, and provide an environment with critical security requirements. These characteristics, together with the potential consequences of an attack, make them a challenging target for an attacker, so that the number of security incidents is continuously increasing [5]. However, most of the research works and security technologies have been developed for public or controlled communication infrastructures. Industrial networks, in contrast, are dedicated solutions with their own infrastructure and protocols, and manage critical processes. Industrial networks aim toward a robust, real-time and determinate communication between field devices that operates in harsh environments and follows specific standards. The possible consequences of an attack in industrial networks can be more catastrophic than in other sectors.

COMMON THREATS AND VULNERABILITIES IN INDUSTRIAL NETWORKS

In recent years, there have been large scale security incidents and an increase in the number of cyber threats on ICS. These incidents have shown that industrial networks are under risk of a broad range of attacks. ICSs are vulnerable to forensic attacks executed locally via USB (universal serial bus) or internet. Also, components already deployed cannot be replaced or modified. In this context, protective and detective solutions must be implemented. Sensor coverage is an important task for the trust model. Industrial companies using IT as well as operational technology (OT) are prone to ransomware attacks. Operation Aurora, Stuxnet, and the Maroochy Water Services cyberattack demonstrated that wide spread damages can be inflicted onto industrial infrastructures. Industrial networks have been evaluated as critical infrastructures under threat. Small- and medium-size companies are under attack, as they usually have less security personnel with industrial IT knowledge. Almost 83% of companies are being compromised in a spear-phishing related attack.

Cyber threats can be categorized into the following groups: computer aided manipulation, man-in-the-middle/local attacks, network attacks, and social and personnel engineering attacks. Attack vectors and data could be used by intrusion detection systems as possible events of interest. The taxonomy must be abstract and apply to all attack types. An indicative generic taxonomy would be: data-based attacks, which are also known as availability attacks; device-based attacks, that is, hardware-focused attacks [6]; exploitation-based attacks, that is, known vulnerabilities being exploited; sniffing-based attacks, that is, man-in-the-middle related attacks; social-based attacks; traffic-based attacks, including issues like transmission control protocol (TCP)-state-based attacks; and trend-based attacks. When categorizing attacks, the ultimate goal is to define types of processable, meaningful data that will be used as preliminary input to the algorithm or mathematics model of a detection system [4]. There is an ongoing debate about the maintenance mode state of the attacks in the taxonomy, and how insightful the taxonomy should be in order to be effectively used for cyber threat identification scenarios. As the attacks are massively evolving, it is not feasible to have a fixed inventorial of description entries, which an IDS will be able to detect. In effect, the focus of the presentation is not at the feature level of the attacks, but more to their meta-information.

KEY TECHNOLOGIES FOR SECURE COMMUNICATION IN INDUSTRIAL NETWORKS

Constant economic and technological changes make industries continuously adapt to new scenarios. Previously, ICS environment requirements were mainly focused on availability and reliability, leaving security into the background. However, with the convergence of IT and OT, ICS has partially lost its isolation and proprietary characteristics, and new threats may leverage IT exposed services. Additionally, since the creation of the IIoT and the expansion of sensor industrial networks, massive ground for risks is opened. Malware in the OT network, (domain name server) DNS tunnels, internet protocol version 6 (IPv6) floods over automation devices, VxLan (virtual extensible lacal area network)

encapsulation, or covert channels over communication protocols are some of the risks risen in the previous years. Besides, some sectors like critical infrastructures (CI) must adopt more ambitious measures, such as energy suppliers, transportation systems, or water facilities.

A remaining problem concerns the communication among industrial devices, which is frequently not secure. This is, data is sent in plain text among devices that may be located in different areas of the factory but may also be physically distant. Obviously, sensitive devices like controllers, remote I/O (input/output) or LAN modules, sensors and edge devices collect and exchange sensitive data. On the one hand, proprietary services may depend on the communicated data. On the other, sensitive information related to the manufacturing process should not be exposed to unauthorized parties. According to it, a defence architecture based on Defence-in-Depth is developed, involving the application at several levels of the security pyramid, including policies, perimeter security, network and device security, and key transfer [7]. Data encryption and the use of secure protocols are explored at network and device level to assure that if a seized device does not contain likely pairs of keys, traffic cannot be decrypted during the time that the remaining active nodes regenerate a new key and send it among them. With the perspective of simplicity, key management is restricted to manual methods, understanding the practice under a real scenario. Light encryption ciphers are proposed attending to existing limitations of the automation devices in terms of operations, as well as the restrictions of the most widely used automation communication technologies. This last statement implies a greater compromise from the research community to provide industrial automation devices with firewall capabilities or even TLS (transport layer security) support in advanced devices. An alerting system is implemented at the network level regarding the violation of protocol logic. Decentralized SCADA (supervisory control and data acquisition) systems and protocols are studied. Unencrypted ICS protocols are widespread. It is not possible to rely on proprietary security mechanisms supported by manufacturers, and industrial automation often uses proprietary or semi-proprietary technologies, closing the ground to third parties seeking to improve security. In such scenarios, network intrusion detection systems (NIDS) specially crafted for ICS networks are investigated. Industrial switches with embedded IDS capabilities are still limited, being an industrial alternative in the use of Test Access Points (TAPs). It ends up with the analysis of some covert channels over Modbus TCP embedded inside UDP (user datagram protocol) or ICMP (internet control message protocol) packets.

RESULTS

Network Security in Industrial Networks

Industrial networks, such as those used in manufacturing and critical infrastructure, require robust security measures due to the rise of threats like malware, ransomware, and targeted cyberattacks.

Key Components of Network Security

- *Authentication:* Ensuring only authorized devices and users can access the network.
- *Data Integrity:* Preventing unauthorized alterations to transmitted data.
- *Confidentiality:* Encrypting sensitive data to prevent unauthorized access.
- *Availability:* Protecting the network from attacks that could disrupt operations (e.g., distributed denial of service [DDoS] attacks).

Challenges in Industrial Network Security

- Legacy systems with outdated security features.
- Increasing integration of IoT devices, which often lack robust security mechanisms.
- Need for real-time operation with minimal downtime, making patching and updates challenging.
- Diverse protocols like Modbus, OPC-UA (Open Platform Communications Unified Architecture), and Profinet, which may have vulnerabilities.

Secure Communication in Industrial Networks

Secure communication ensures the safe exchange of information across industrial networks, vital for maintaining operational integrity.

Techniques for Secure Communication

Encryption

- Use of algorithms like AES (advanced encryption standard) and RSA (Rivest–Shamir–Adleman) to encrypt data during transmission.
- Ensures data confidentiality over potentially insecure channels.

Virtual Private Networks (VPNs)

- Creates secure tunnels for communication between remote sites or users and the industrial control system.

Firewalls and Intrusion Detection Systems (IDS)

- Protects network perimeters and monitors traffic for suspicious activity.

Use of Secure Protocols

- Transition from legacy protocols (e.g., HTTP, FTP) to secure ones (e.g., HTTPS, SFTP, TLS).

Public Key Infrastructure (PKI)

- Ensures secure identity management using digital certificates.

Role-Based Access Control (RBAC)

- Limits access to network resources based on user roles and permissions.

Emerging Trends

- *Artificial Intelligence and Machine Learning:* For anomaly detection and real-time threat mitigation.
- *Zero Trust Architecture:* Ensures continuous authentication and least privilege access.
- *Blockchain:* Enhances data integrity and traceability in communication.
- *Post-Quantum Cryptography:* Preparing for threats posed by quantum computing.

BEST PRACTICES FOR IMPLEMENTING SECURE COMMUNICATION IN INDUSTRIAL NETWORKS

Industrial networks are evolving faster than ever. While the industry is focusing on the most recent technological advances related to the industry 4.0 concept, it often neglects the consequences in terms of cybersecurity. To guarantee uninterrupted production, the availability, reliability, and integrity of the data within the industrial networks are vital [8]. However, attacks on industrial networks happen every day for different reasons, ranging from competition between industries to cyber-experts' games. Moreover, new vulnerabilities appear every time the system changes. Therefore, an industrial network must have a periodically updated well-defined strategy to make it secure [4].

Conducting a risk assessment and identifying cybersecurity measures should be the preliminary phase in defining a cybersecurity strategy for an industrial network. Beyond the definition of barriers and methodologies to maintain cybersecurity measures, operations and tasks to prevent undesired events should also be identified. In order for a system to be secure and resilient, barriers should also possess a controlling mechanism. A company providing any type of service to an industrial network should meet at least a basic security level and should periodically undergo inspections and audits in that sense. The development and the distribution of a security check list are considered a best practice to make it feasible [9].

Whenever a new security breach in system software is discovered, it is immediately disseminated to constitute a potential risk. Security updates and patches must be regularly shared by the producer company and systematically updated on the system. Ensuring secure communication in OT systems also means making operational personnel aware of the problematics, risks, modalities, and means to

prevent possible industrial cyberattacks [10]. Companies sharing sensitive, business-related, industrial data have to establish a technology readiness level (TRL) agreement. Furthermore, companies managing sensitive data must guarantee its protection.

CONCLUSION

In today's interconnected world, ensuring the security of communication within industrial networks is more critical than ever. Industrial environments are increasingly adopting advanced technologies, such as IoT and cloud-based systems, which introduce significant vulnerabilities. Ensuring network security is essential for protecting sensitive information, securing vital infrastructure, and maintaining uninterrupted operations.

Effective secure communication in industrial networks requires a multi-layered approach, combining robust authentication protocols, encryption techniques, real-time monitoring, and regular updates. Promoting cybersecurity awareness among employees is crucial for reducing risks associated with human error.

As industrial systems continue to evolve, proactive investment in advanced security solutions and adherence to global standards will be vital. By prioritizing network security, industries can not only prevent cyberattacks but also build trust and resilience in their operations, paving the way for sustainable and secure digital transformation.

REFERENCES

1. Hamza A, Gharakheili HH, Sivaraman V. IoT network security: requirements, threats, and countermeasures. arXiv preprint arXiv:2008.09339. August 21, 2020.
2. Li Y, Wu S, Pan Q. Network security in the industrial control system: a survey. arXiv preprint arXiv:2308.03478. August 7, 2023.
3. Okporokpo O, Olajide F, Ajienka N, Ma X. Trust-based approaches towards enhancing IoT security: a systematic literature review. arXiv preprint arXiv:2311.11705. November 20, 2023.
4. Anton SD, Schotten HD. Putting together the pieces: a concept for holistic industrial intrusion detection. In: ECCWS 2019 18th European Conference on Cyber Warfare and Security, Coimbra, Portugal, July 4–5, 2019. p. 178.
5. Meshram A. Deterministic Industrial Network Communication: Fundamentals. Karlsruhe, Germany: KIT Scientific Publishing; 2018.
6. Kayan H, Nunes M, Rana O, Burnap P, Perera C. Cybersecurity of industrial cyber-physical systems: a review. ACM Comput Surveys. 2022; 54 (11s): 1–35.
7. Mosteiro-Sanchez A, Barcelo M, Astorga J, Urbieta A. Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0. J Manuf Syst. 2020; 57: 367–378.
8. Asghar MR, Hu Q, Zeadally S. Cybersecurity in industrial control systems: issues, technologies, and challenges. Computer Netw. 2019; 165: 106946.
9. Borhani M, Liyanage M, Sodhro AH, Kumar P, Jurcut AD, Gurtov A. Secure and resilient communications in the industrial internet. In: Rak J, Hutchison D, editors. Guide to Disaster-Resilient Communication Networks. New York, NY, USA: Springer; 2020. pp. 219–242.
10. Li S, Xu LD. Security architecture in the internet of things. In: Securing the Internet of Things. New York, NY, USA: Elsevier; 2017. pp. 27–48.

