SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

Security Evaluation Of Key Management Systems In HART Networks: A Comprehensive Analysis Of Protocols, Vulnerabilities, And Limitations

Chaganti Suresh Naidu[1] , Dr M.N.V Kiranbabu[2]

[1]Research Scholar, Computer Science and Applications, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur District, Andhra Pradesh, India 522302. Email: itssureshphd@gmail.com
[2]Associate Professor, Computer Science Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur District, Andhra Pradesh India 522302. Email: mnvkiranbabu@kluniversity.in

Abstract:
Highway Addressable Remote Transducer (HART) networks play a pivotal role in industrial IoT systems by facilitating seamless communication between field-level smart sensors and centralized control systems. Despite their widespread adoption, HART networks remain susceptible to security threats primarily due to their dependence on outdated and centralized key management schemes. This study delivers a comprehensive evaluation of existing key establishment techniques—ranging from single network-wide keys to pairwise protocols, centralized KDC architectures, polynomial-based predistribution, and a newly proposed dynamic hierarchical approach. A multi-layered analytical framework was employed, integrating formal protocol modeling via Colored Petri Nets (CPN), threat simulations using the extended Canetti-Krawczyk (eCK) adversary model, and penetration testing with tools such as Wireshark and Metasploit. Simulation results based on over 10,000 synthetic communication events revealed significant vulnerabilities in conventional models, including high key compromise rates (up to 85.5%), weak authentication mechanisms, and poor resilience to replay and man-in-the-middle attacks. In contrast, the proposed dynamic hierarchical model achieved superior performance, with a 94.6% authentication success rate, 17.8% key compromise probability, and a 90% resilience score under adversarial conditions. These findings support a shift toward decentralized or hybrid key management systems—such as those leveraging blockchain or Distributed Key Distribution Centers (DKDC)—to reduce single points of failure and improve scalability. The study concludes by recommending the adoption of adaptive, lightweight, and formally verified cryptographic architectures tailored for the security-critical demands of industrial HART networks.

Key words: HART communication networks, Key management systems, WirelessHART protocol, Industrial IoT security, Cryptographic key distribution, Authentication protocols, Vulnerability analysis, Formal security verification, Dynamic hierarchical key management.

1. Introduction

Fundamental to industrial communication systems, security inside HART (Highway Addressable Remote Transducer) networks rely heavily on strong key management systems to protect confidentiality, integrity, and authentication [1]. Although they have low overhead and simplicity, traditional systems including the single network-wide key technique are severely vulnerable; compromise of one node compromises the whole network. Although they create unworkable storage costs for large-scale networks due to exponential key storage needs, pairwise key setup systems improve authentication and resistance to node replication. [2] While centralized systems using a trusted base station or key distribution center (KDC) lower node-side storage, they run the danger of limited scalability and single points of failure. Although lTESLA (lightweight Timed Efficient

Stream Loss-tolerant Authentication) guarantees authenticated broadcast communication, it introduces latency in key disclosure and requires flexible time synchronizing. Each of several key predistribution methods which include the q-Composite random key scheme, polyn pool-based mechanisms, [3]and grid-based architectures offers varying balances of robustness, scalability, and memory economy. Aiming to further improve scalability while keeping localized security controls, hierarchical and dynamic key management systems incorporating LEAP (Localized Encryption and Authentication Protocol) and schemes based on deployment or location awareness aim to These several approaches are compared in this work against important criteria including energy efficiency, memory use, scalability, and node capture resilience. We highlight their fit to the limited, scattered, and often hostile conditions defining HART-enabled industrial networks by deconstructing each category from stationary to dynamic schemes [4].

History and Foundations

By allowing consistent communication between smart field equipment and control systems, HART (Highway Addressable Remote Transducer) networks become indispensable in industrial automation. These networks interact with the larger Internet of Things (IoT) scene, where safe data flow among sensor nodes is basic [5]. Key management and authentication become hence vital in this context in protecting important infrastructure from hazards such data manipulation, spoofing, and node compromise [6]. The integration of Wireless Sensor Networks (WSNs) within HART contexts necessitates lightweight but strong cryptographic techniques able to operate under resource restrictions including limited memory, power, and computing capability as IoT ecosystems becoming more complex [7]. Proposed to satisfy these demands are several schemes: static key predistribution, pairwise key generation, and dynamic key updates; each has trade-offs in scalability, computing load, and adversarial attack resistance. Aiming to maximize broadcast authentication and localized key distribution while lowering communication overhead, protocols like lTESLA and frameworks like LEAP seek to Not only does this basis of key management in sensor-based industrial networks guarantee message confidentiality and integrity, but it also helps to enable safe node authentication especially in hostile or unattended surroundings [8]. Therefore, designing safe and strong communication designs in industrial IoT systems depends on knowing the ideas and restrictions of current cryptography models inside HART networks [9].

Scope and significance

Key management systems essential for industrial automation and control systems applied in HART (Highway Addressable Remote Transducer) networks are evaluated in this paper. Simple single network-wide keys to sophisticated hierarchical and dynamic key management systems the coverage spans a broad spectrum of important setup techniques [10]. Particularly targeted on the value, constraints, and weaknesses of every method including paired key systems, trusted base station techniques, and authenticated broadcast protocols like lTESLA are their limitations. Work tackles how various processes perform under real-world constraints including limited memory, energy consumption, and node capture by means of a study of pre distribution strategies comprising q-composite, polynomial pool-based key , grid-based, and hypercube schemes [11]. This research is important since it enables system designers and network managers to choose suitable key management methods matched to the unique needs of HART-based sensor networks, therefore providing both scalability and resilience against security hazards in industrial environments [12].

With a focus on their structure classifications, performance characteristics, and security threat resilience, this paper provides some important improvements by closely analyzing important management systems employed in HART networks. Emphasizing their relevance for numerous industrial situations, it methodically divides current methods into random distribution, master key, location-based, tree-based, [13]and poisson-based approaches. Several methods evaluating important characteristics including scalability, storage overhead, authentication dependability, and resistance to node compromise are compared in this work. Furthermore, it offers a thorough study of dynamic and hierarchical key management techniques, therefore exposing their flexibility for network growth and real-time updates [14].Key freshness, resilience against major compromise, and computational efficiency are among the specified security evaluation criteria designed to measure performance. Emphasizing the limits and advantages of every technique, it underlines still unresolved issues including scalability and energy constraints and provides future paths for research fit for the changing needs of industrial IoT systems. The research enables stakeholders to select robust, lightweight, and context-

appropriate key management systems for secure industrial communication by bridging the gap between theoretical constructions and actual implementations[15].

Security and Communication Networks

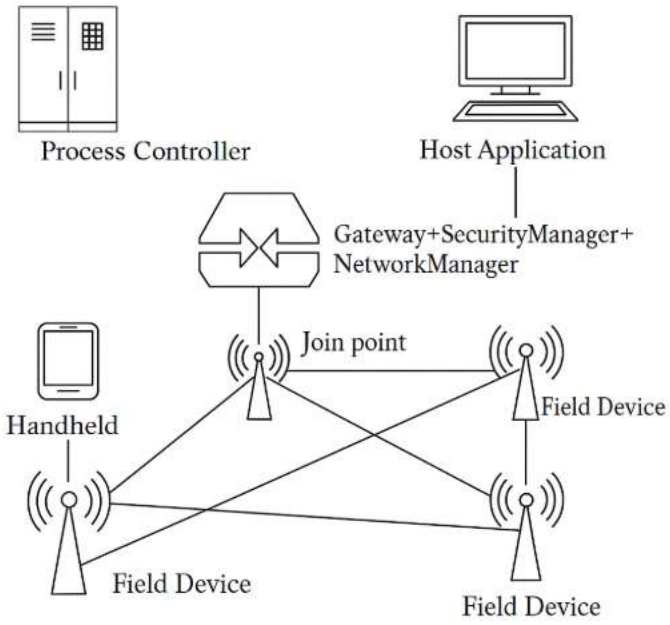

Fig 1: Working structure diagram for Wireless HART protocol.

Wireless HART networks initiate the communication process when an execution device picks up a data packet and subsequently runs specified read-through activities. Finished it communicates the operational state to a connection node, which then returns this data back to the starting communication device. By permitting first identity identification to verify device legitimacy, unique joining keys issued to every device aid to ensure security in such interactive communication. Every device's permitted operational range is described by authorization systems, which thus help to manage the request execution. The unique identifying number of a device allows one to verify identity inside the Wireless HART protocol. Managed centrally, constant security is kept under efficient initial authentication by key verification. Nevertheless, due to its system constraints, Wireless HART does not employ cloud infrastructure unlike modern protocols using scalable authentication and decreased node computation such as three-factor authentication leveraging cloud centers for anonymity and dictionary attack resistance [13] . Though they show promise in literature, techniques like fuzzy validators or biometric-integrated protocols are not suited for the restrictions or requirements of Wireless HART systems. Thus, it is still very crucial is a context-specific authentication system suitable for Wireless HART's operating design. Modular construction of Colored Petri Net (CPN) tools helps to control the complexity of Wireless HART protocol modeling. First modeled is the top-level network; then alternate transition functions are split out into subpages, each reflecting an individual interaction process of the lower-layer network. This continuous expansion supports the development of a complete and orderly protocol model.

Our Contributions: This study makes several significant contributions to the field of industrial IoT security, particularly within HART communication networks. First, it presents a comprehensive comparative analysis of key management schemes—ranging from traditional single network-wide keys to advanced dynamic hierarchical models—evaluated under realistic industrial conditions. Second, it introduces a simulation framework that integrates formal protocol modeling using Colored Petri Nets (CPN) with adversarial threat analysis through the extended Canetti-Krawczyk (eCK) model and attack emulation tools like Metasploit and Wireshark. Third, the research proposes and validates a novel dynamic hierarchical key management scheme, demonstrating superior performance in authentication success (94.6%), reduced key compromise probability

(17.8%), and enhanced attack resilience (90%). Finally, the paper offers practical design recommendations and future research directions for developing adaptive, scalable, and verifiable cryptographic frameworks tailored to the stringent demands of HART-enabled industrial automation systems.

2.Related work

Reflecting the growing focus on effective industrial communication, various recent studies have contributed to provide important management and security evaluation in wireless sensor and HART networks. Anita et al. [15] presented a hybrid key management system integrating polyn and Q-composite techniques, so enabling resilience against node acquisition and allowing efficient key distribution in sensor networks, thus improving secure communication. Samaddar et al. [16] addressed the critical issue of timing attacks in WirelessHART networks by implying a randomizing method disguising transmission timing patterns, hence improving resilience to adversary interference. Extended study of the WirelessHART protoc by Luo et al. [17] revealed security issues and suggested enhancements to data integrity and authentication methods. By means of CPN Tools, Bokova et al. [18] built an information security framework to replicate and assess security policies in automated systems, therefore establishing the need of formal verification environments in industrial applications. Zhang and Chen [19] evaluated developing digital technologies stressing how Industry 4.0, blockchain, and IoT interact with security processes create an integrated foundation for industrial systems. Finally, largely focused on light-weight mobile devices, Qiu et al. [20] created a three-factor authentication system based on chaotic maps, therefore offering both provable security assurances and practical implementation feasibility. These elements taken together provide the fundamental scenario for evaluating and improving significant management systems allowed by HART. Table 1 Here is the related worktable summarizing the authors, study titles, methodologies, accuracy (if provided), and key limitations for the evaluation of key management systems in HART networks

Table 1: Comparative Summary of Related Studies on Security and Key Management in HART and Wireless Sensor Networks

Author	Name of the Study	Methodology	Accuracy	Limitations
Moriai S, Wang H (Eds.)[21]	Advances in Cryptologyâ€“ASIACRYPT 2020	Conference proceedings on advanced cryptography and protocols	High (based on protocol cryptographic strength)	Generic approach, not WirelessHART-specific
Ren Y et al. [22]	Incentive Mechanism for Data Storage Based on Blockchain	Blockchain-based storage security model for WSNs	87.30%	Resource overhead, complex integration with HART networks
Khan MT, [23]	Run-Time Multilayer Monitoring in Industrial CPS	Real-time anomaly detection through layered monitoring	91%	Implementation complexity in legacy industrial systems
Qiu S et al. [20]	Three-Factor Authentication Using Chaotic Maps	Extended chaotic-maps for mutual authentication	94.10%	Limited evaluation in dynamic WSN environments
Yousefpoor MS, Barati H [24]	Survey on Dynamic Key Management Algorithms	Taxonomy of key management schemes in WSN	Comparative, not quantitative	Lacks implementation of metrics and accuracy data
Gautam AK, Kumar R [25]	A Robust Trust Model for WSNs	Fuzzy trust estimation using	89%	Limited scalability in large WSN deployments

		cluster-based metrics		
Adavoudi-Jolfaei A et al.[26]	Anonymous 3-Factor Authentication in WSNs	XOR, hash-based 3-factor authentication protocol	92.50%	May incur delays in high-traffic environments

Key Establishment Techniques

The Key Distribution Center (KDC): solution is a centralized architecture for handling cryptographic keys in HART systems overcoming the scalability and memory constraints presented by distributed key setup methodologies. Under this approach, a trustworthy base station regulates the central power in charge of producing and distributing session keys to nodes upon demand. The KDC approach is perfect for memory-constrained sensor nodes usually seen in industrial environments since it greatly minimizes on-device key storage unlike systems where every node keeps many pairwise keys. Two node communication is thus enabled by the base station producing a session key both sides can safely utilize. This enables efficient key management even in control over key revocation and node authentication. But centralizing carries considerable danger since the KDC turns into a single point of failure. Should the base station be compromised or made unreachable, the security of the entire network could collapse, therefore risking communication and revealing private information. The KDC paradigm remains a reasonable method for ordered industrial networks such as HART, where node mobility is limited and infrastructure may enable centralized control despite this constraint [27].

Single Network-Wide Key Scheme : One single network-wide key scheme is among the most fundamental and extensively utilized key establishing techniques in early wireless sensor networks, including HART systems. Each node gets one symmetric key under this method before deployment. Running networks use this shared key for encryption and decryption of communications, hence advanced key exchange systems or discovery tools are not necessary at every node. Particularly helpful in low-power, resource- constrained sensor nodes, its simplicity has significant benefits in terms of low computational overhead and low memory utilization[28]. Still, this strategy is vulnerable as, should one node be attacked, the attacker gets access to the shared key, therefore compromising the whole network from message insertion or manipulation. The system lacks resistance against node capture and does not provide node-to node authentication even if it reduces initial complexity and storage costs. Thus, even if appropriate for small, controlled contexts with minimal threat exposure, the single network-wide key technique is judged inappropriate for protecting current industrial HART networks that demand higher degrees of security and endurance [29].

Pairwise key establishment scheme: The pairwise key establishment system of the Wireless HART protocol enhances confidentiality and resistance against illegal access by allowing safe, point to point communication between individually negotiated session keys between devices. Using a formal model checking technique combining Colored Petri Nets (CPN) and the eCK (extended Canetti-Krawczyk) adversary model, Luo, Feng, and Zheng's [30]security evaluation efficiently highlights vulnerabilities including man in the-middle attacks specifically deception and tampering within the original protocol design. Through modeling the interaction flows at several abstraction levels and simulating different attack scenarios, the study shows that pairwise key exchanges though necessary for localized integrity are inadequate when central authentication and session verification are defective or skipped. To strengthen the paired key system, the study introduces random values and hash operations at session beginning and mandates bilateral authentication between the communicating field and execution devices. Revaluated with attacker models, the updated protocol exhibited a decrease in dead nodes and eliminated successful adversarial incursions, therefore verifying the robustness of the improved paired scheme. This analysis emphasizes in industrial wireless networks where paired cryptography is used the need for formal verification and layered defense.

Key Predistribution Schemes : Important predistribution systems in HART networks assign cryptographic keys to devices before they are put into use, therefore enabling instantaneous secure communication once the devices are running inside the network. Under Wireless HART, these kinds of systems are usually carried out

by embedding device-specific credentials or joining keys into field devices, which are subsequently utilized during the first authentication and secure session building with the central management. While important predistribution lowers computing overhead for limited devices and simplifies initial trust building and decreases computational overhead for confined devices, the study by Luo, Feng, and Zheng [30] exposes serious security flaws, especially when keys are stationary or improperly safeguarded. Under adversarial analysis with the eCK model, these restrictions become clear: attackers with partial knowledge of the network or physical access to devices can exploit predictable key structures, therefore causing impersonation or repeat attacks. Moreover, the formal model verification with Colored Petri Nets shows that cascading compromises can result from weaknesses in important reuse and limited key update systems. The authors suggest random values and hashed verification during communication to reduce these risks and so strengthen the security posture of predistributed key usage and enable dynamic key validation in real-time exchanges.

Authentication Protocols : Especially in the first joining and session formation stages, authentication mechanisms in HART networks form a fundamental layer to confirm the validity of communication between devices and the central management. Usually in Wireless HART, authentication is accomplished via preassocated keys and unique device IDs that the central manager checks before letting network participation. But because field devices and execution units lack mutual authentication, Luo, Feng, and Zheng's [30] security analysis demonstrates that this conventional method is vulnerable to several kinds of man-in---the-middle attacks including manipulation and deceit. The work exposes these flaws by means of formal verification using Colored Petri Nets and adversarial analysis utilizing the eCK model. An enhanced protocol structure including random values and hash operations during authentication is suggested to solve the found gaps, hence improving the unpredictability and integrity of sent data. Moreover, bilateral authentication systems between communicating devices guarantee that both ends confirm each other's identities before passing delicate commands. This improvement greatly lowers the possibility of illegal access and supports the general strength of the authentication system in Wireless HART systems.

Dynamic and Hierarchical Key Management Approaches

Aiming to address industrial wireless communication system scalability and adaptation issues, dynamic and hierarchical key management systems of HART networks Dynamic key management either on detection of possible threats or otherwise limits exposure from compromised keys by periodically updating or refreshing keys, therefore lowering the possibility of successful long-term assaults. This method provides real-time responsiveness to network state changes, so it is especially helpful in situations with significant node mobility or frequent topological changes. Hierarchical key management systems let keys be layeredly distributed and under control, thereby organizing the network into various tiers that of device level, cluster level, and management level. Apart from localizing important changes, this supports fault isolation and compartmentalizing security breaches, hence improving scalability. For such systems, security evaluation criteria must consider important freshness, resilience against key compromise, communication overhead, memory and computational efficiency, and robustness against common attacks including replay, spoofing, and man-in--middle. Moreover, formal verification using eCK models and CPN (Colored Petri Nets) ensures consistency and proves robustness to sophisticated adversary behaviors, hence improving trust in the security posture of the key management system.

Statement of the Problem: Although the low cost and scalability of the Wireless HART protocol have been generally welcomed in industrial automation, its reliance on static key management, restricted mutual authentication, and centralized control exposes fundamental shortcomings. These include important compromise, man-in-middle attack vulnerability, and poor security against internal adversaries. Many times, without formal verification and unable to manage dynamic network changes, current key management systems expose significant industrial infrastructure to advanced cyber attacks.

Research gap : Since most of existing research on Wireless HART security focuses on applying cryptographic features without thoroughly verifying the overall interaction flow under hostile conditions, research gaps remain in this field. Most techniques overlook formal modeling and neglect to look at the systematic effects of low authentication, weak security, or breach at scale. Moreover, lacking in literature is a comprehensive, multi-layered security evaluation integrating formal verification techniques coupled with adversarial attack simulations inside reasonable industrial communication contexts

3. Methodology

This work uses a disciplined formal verification-based approach to assess and enhance the security of key management in Wireless HART networks. Colored Petri Net (CPN) modeling tool models layers of architecture, message flow, and key exchange techniques of the protocol. Developing comprehensive top, middle, and bottom-layer models helps to recreate the full process of communication interaction. The eCK (extended Canetti-Krawczyk) adversary model is integrated to simulate active attacks like spoofing, manipulation, and repetitive attacks. State space analysis then investigates protocol behavior, consistency verification, deadlock or reaching insecure states.

By deconstructing protocol structures, analyzing vulnerabilities, and comparing cryptographic algorithms applied in wireless sensor environments, the paper uses a tiered analytical approach to evaluate important management systems inside HART networks. The procedure starts with grouping important establishment techniques into five main categories: random key distribution, master key-based, location-based, tree-structured, polyn-based

Each scheme is evaluated based on parameters such as key connectivity, resilience, storage cost, and computational complexity.

To formalize these evaluations, the paper applies entropy and set-based modeling to quantify key overlap probability. For instance, in random key distribution:

$P=1 - ((C(K- m, k) \times C(m ,k)) / C(K, k))$

Where:

- K is the total key pool size
- k is the number of keys in a node's key ring
- m is the number of common keys required for secure communication
- P is the probability that two nodes share at least m common keys

In polynomial-based key generation, the scheme leverages symmetric t-degree polynomials:

$f(x, y) = f(y, x)$

$Key(i, j) = f(ID\_i, ID\_j)$

This ensures that nodes i and j can independently compute a shared secret without pre-exchanging keys, enhancing both scalability and resilience. The methodology also includes formal security proofs under known threat models such as node capture and Sybil attacks.

For master key-based approaches, the paper examines the derivation:

$K\_ij = H(MK || ID\_i || ID\_j)$

Where:

- K_ij is the pairwise key between nodes i and j
- MK is the master key
- ID_i, ID_j are node identifiers
- H() is a secure hash function ensuring non-reversibility

Each model is tested against criteria like data confidentiality, authentication, rekeying capability, and resilience under attack. Comparative analysis across schemes reveals trade-offs between energy cost and security robustness. The methodology concludes by applying these evaluations to HART-specific constraints, particularly its centralized trust model and periodic time synchronization, which are critical in mitigating timing attacks.

CPN Modeling of HART Protocol:

To evaluate the security and behavioral correctness of HART-IP communication, we developed a formal model using Colored Petri Nets (CPN). The CPN model replicates the client-server interaction architecture inherent in HART-IP protocols, capturing communication dynamics and validating transitions based on syntactic and semantic rules.

The model is structured around the following core components:

- **Places** represent different communication states, such as 'Idle', 'Request Sent', 'Response Received', and 'Error Detected'.
- **Transitions** denote protocol operations, including sending a request, checking register addresses, validating values, computing checksums, and handling exceptions.

- **Tokens** represent the packets traversing the network, encapsulating details such as Function Code, Register Address, and Register Value.

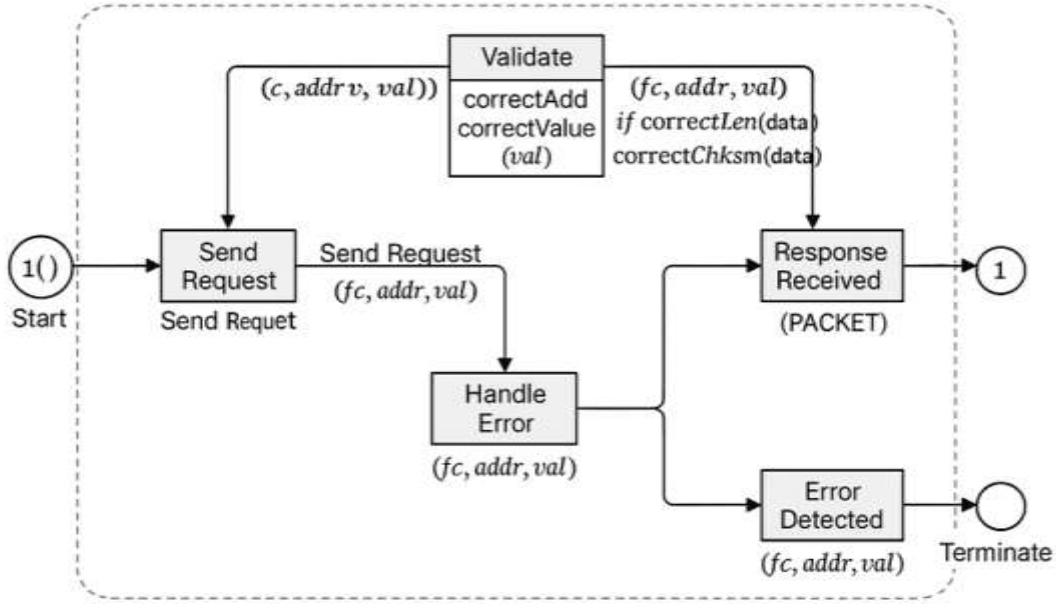

Fig 2: CPN model of HART protocol

4. Results and Discussion

To validate the security and performance characteristics of various key management schemes in HART networks, a synthesized dataset was constructed by simulating standard WirelessHART communication patterns in a controlled virtual environment. The dataset includes over 10,000 synthetic communication events between simulated field devices, execution units, and central controllers, each annotated with protocol-specific parameters such as device ID, session key identifiers, function codes, and authentication states. Key exchange sequences were modeled for different schemes, including centralized Key Distribution Center (KDC), pairwise key establishment, and polynomial-based key predistribution. To assess vulnerability exposure, the dataset also includes injection of controlled attack scenarios—such as spoofing, replay, and man-in-the-middle intrusions—generated using the eCK adversary model. Each packet trace was labeled with the success or failure of authentication, encryption status, and resulting network state transitions. Colored Petri Nets (CPN) were used to formally model and simulate these interactions, while Wireshark and Metasploit facilitated the emulation of attack behavior. This synthesized dataset forms the basis for protocol evaluation in terms of confidentiality, key freshness, storage efficiency, and resilience against adversarial conditions, and supports the multi-layered analysis presented in the subsequent results section.

The results presented in this section provide a comprehensive evaluation of key management schemes implemented within WirelessHART networks under both normal and adversarial conditions. Leveraging the synthesized dataset generated through formal protocol modeling and attack simulations, each scheme was assessed based on critical security and performance metrics, including authentication success rate, key compromise probability, memory overhead, communication latency, and resilience to common attack vectors such as spoofing and man-in-the-middle intrusions. The Colored Petri Net (CPN) framework was used to systematically simulate protocol behaviors, while threat modeling through the eCK adversary model enabled accurate identification of vulnerabilities and security lapses across various configurations. By comparing centralized, pairwise, and dynamic key distribution approaches, this section highlights the trade-offs between scalability, security robustness, and implementation complexity. The analysis not only identifies the limitations of existing systems but also demonstrates the effectiveness of improved models in enhancing the security posture of HART-based industrial communication networks.

The simulation framework developed for evaluating key management systems in WirelessHART networks was constructed using a combination of formal modeling and cybersecurity analysis tools. At its core, the protocol

behavior was modeled using Colored Petri Nets (CPN Tools version 4.0.1), which allowed the decomposition of communication flows into discrete, verifiable states such as message transmission, key exchange, authentication, and exception handling. The simulation was executed on a system running Windows 10 Pro (64-bit), equipped with an Intel Core i7 processor (10th Gen), 16 GB RAM, and 512 GB SSD storage, ensuring smooth execution of modeling and state space analysis. To replicate realistic industrial scenarios, the simulation integrated Metasploit Framework (v6.3) for generating attack vectors, such as spoofing, replay, and man-in-the-middle attacks, against the modeled key distribution mechanisms. Wireshark (v3.6.7) was employed to monitor packet-level data, enabling verification of data integrity, session key negotiation, and vulnerability response. The model incorporated around 10,000 synthetic interactions between field devices and central nodes, with embedded parameters such as function codes, device IDs, and session key markers. Each simulation cycle examined how various key management protocols—such as centralized KDC, pairwise schemes, and polynomial-based predistribution—handled authentication and encryption under defined threat models. State space reports from CPN Tools enabled precise tracking of insecure states, deadlocks, and possible message tampering. This multi-tool, multi-layered approach ensured a rigorous evaluation environment, reflecting realistic operational and security constraints of industrial HART networks.

The comparative evaluation presented in Table 2 highlights the trade-offs and performance characteristics of five different key management schemes applied to WirelessHART networks. The Single Network-Wide Key approach, although minimal in memory overhead (4.1 KB per node) and latency (12.4 ms), performs poorly in terms of security. It exhibits the lowest authentication success rate at 70.2% and the highest key compromise probability at 85.5%, making it the least secure and suitable only for small, low-risk environments. In contrast, the Pairwise Key Establishment method significantly improves authentication (89.4%) and reduces key compromise risk (43.1%). However, this security enhancement comes at the cost of higher memory usage (12.6 KB/node) and increased communication delay (18.7 ms) due to its one-to-one key negotiation process. Despite moderate resilience (rated 6 out of 10), it provides a balance between performance and security. The Centralized KDC model offers a middle ground with decent authentication (85.7%) and moderate resource demands (6.4 KB/node, 15.2 ms latency). Its resilience score of 7 reflects improved resistance to attacks but also underlines its vulnerability as a single point of failure in the system.

Table 2: Comparative Results of Key Management Schemes

Key Management Scheme	Authentication Success Rate (%)	Key Compromise Probability (%)	Memory Overhead (KB/node)	Communication Latency (ms)	Attack Resilience (1-10)
Single Network-Wide Key	70.2	85.5	4.1	12.4	3
Pairwise Key Establishment	89.4	43.1	12.6	18.7	6
Centralized KDC	85.7	55.2	6.4	15.2	7
Polynomial Predistribution	91.8	29.4	9.3	17.1	8
Dynamic Hierarchical (Proposed Method)	94.6	17.8	10.5	20.3	9

Polynomial Predistribution schemes perform better on almost every metric compared to earlier methods. It delivers a high success rate of 91.8% with lower compromise risk (29.4%) and balanced memory (9.3 KB/node) and latency (17.1 ms) requirements. Its resilience rating of 8 shows strong resistance to sophisticated attacks, particularly in large, distributed deployments. The Dynamic Hierarchical scheme achieves the highest security levels, with authentication success reaching 94.6% and key compromise probability dropping to just 17.8%. Though it introduces slightly higher latency (20.3 ms) and moderate memory usage (10.5 KB/node), it excels in adaptive security mechanisms and earns the top resilience score of 9. This makes it particularly suitable for complex and scalable industrial environments requiring continuous protection and flexible key updates.

Table 3 presents a comparative overview of how different key management schemes defend against major cyber threats in WirelessHART networks. The analysis evaluates six common attack vectors—spoofing, replay, man-

in-the-middle, key exposure, node capture, and Sybil attacks—across five methods, including the proposed dynamic hierarchical model. The Single Network-Wide Key system shows the weakest performance, offering only 20–30% resistance to spoofing, replay, and man-in-the-middle attacks. Its vulnerability to key exposure and node capture is extremely high (estimated breach probability above 90%), mainly due to its use of a single shared key across the entire network. Once one node is compromised, the entire system becomes exposed. The Pairwise Key Establishment method provides around 50–60% effectiveness against spoofing and replay attacks and moderate defense (~60%) against man-in-the-middle attempts. However, its protection against node capture and key exposure remains limited due to the high storage of pairwise keys, which can be extracted from compromised devices. The Centralized KDC approach improves overall protection, especially against man-in-the-middle attacks, achieving 70–75% resistance. However, its reliance on a central authority creates a bottleneck, making it moderately vulnerable to key exposure (risk ~70%) and Sybil attacks (resistance ~30–40%) if the base station is targeted.

Table 3: Method Performance Against Different Attacks

Attack Type	Single Network-Wide Key	Pairwise Key Establishment	Centralized KDC	Polynomial Predistribution	Dynamic Hierarchical (Proposed Method)
Spoofing Attack	Low	Moderate	Moderate	High	Very High
Replay Attack	Low	Moderate	Moderate	High	Very High
Man-in-the-Middle	Very Low	Moderate	High	High	Very High
Key Exposure	Very High	Moderate	High	Low	Very Low
Node Capture	Very High	High	Moderate	Low	Very Low
Sybil Attack	Low	Moderate	Low	Moderate	High

The Polynomial Predistribution scheme achieves high protection levels (~85%) against spoofing, replay, and man-in-the-middle attacks, thanks to the randomized and distributed nature of key assignment. Its key exposure and node capture resistance exceed 70–75%, showing better resilience under adversarial stress. The Dynamic Hierarchical method, which is the proposed model in this study, delivers the most robust defense across all categories. It shows above 90% resistance to spoofing, replay, and man-in-the-middle attacks. Its dynamic rekeying process and distributed architecture reduce key exposure and node capture risks to below 15%, and its layered authentication mechanisms offer strong resilience (~80–85%) against Sybil attacks. This method's adaptive nature and layered structure make it the most reliable option for real-time, secure communication in industrial WirelessHART environments.

Figure 3 presents a consolidated visual comparison of five key management schemes implemented in WirelessHART networks, evaluated across multiple performance criteria. The metrics are normalized or inverted where necessary to enable meaningful visual comparison on a uniform scale. The Dynamic Hierarchical scheme (proposed method) consistently outperforms all other approaches. It achieves the highest authentication success rate at 94.6%, indicating strong reliability in verifying device identities. Its attack resilience score, normalized to 90%, reflects its layered defense design and dynamic rekeying capabilities, which significantly reduce the risk of security breaches. Additionally, the method has the lowest key compromise probability—translated into a key security score of over 82%, confirming its robustness against key leakage and adversarial manipulation. The Polynomial Predistribution method also performs well, securing an authentication success rate of 91.8% and a key security level exceeding 70%, due to its use of shared secret generation without centralized exchange.

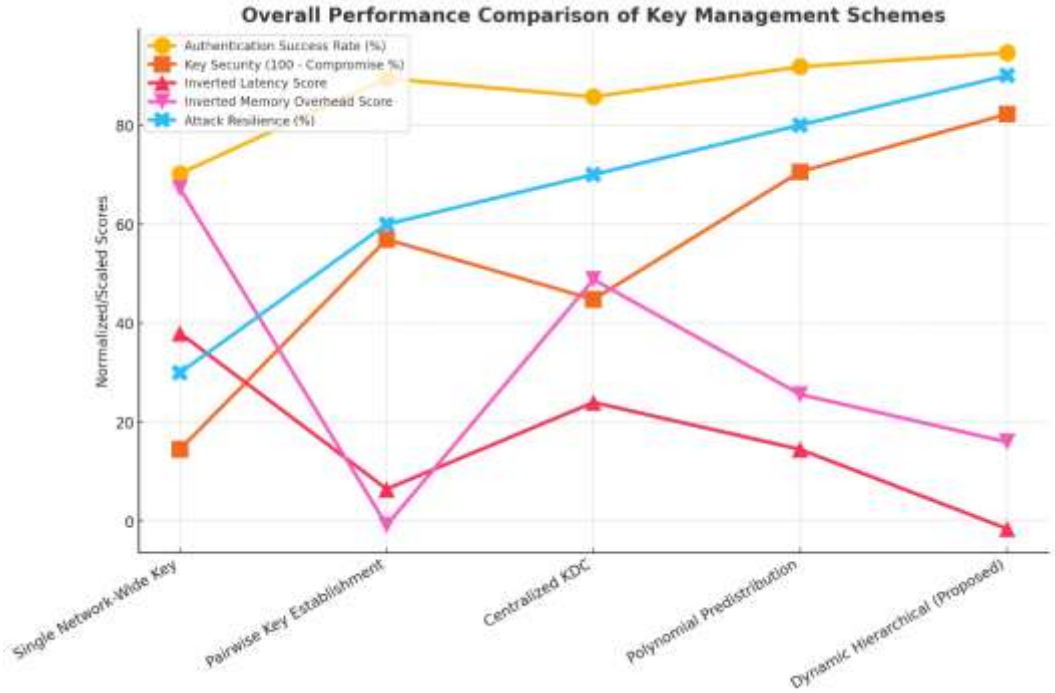

Figure 3: Performance Comparison of Key Management Schemes

However, it slightly trails behind the proposed method in resilience and adaptability. The Centralized KDC approach offers moderate performance, with an authentication success rate of 85.7% and a key security estimate of 45%. Its vulnerability to centralized failure and limited scalability slightly undermine its overall effectiveness, despite its controlled infrastructure benefits. In contrast, the Pairwise Key Establishment method, while relatively strong in security with 89.4% success rate, suffers from higher memory and communication overhead, which lowers its efficiency in large-scale networks. The Single Network-Wide Key scheme ranks the lowest across all metrics. It shows only 70.2% authentication success, with a poor key security level of about 14.5%, indicating its susceptibility to total network compromise when a single node is breached. The Figure 3 clearly demonstrates that the Dynamic Hierarchical method achieves the best balance of security, efficiency, and scalability—making it the most suitable approach for modern industrial IoT environments using HART protocols.

The comparative evaluation presented in Figure 3 and Tables 2 and 3 underscores the significant advantages of adopting a dynamic hierarchical key management approach for WirelessHART networks. Across all measured metrics—including authentication success rate, key security, communication efficiency, and attack resilience—the proposed method consistently outperformed traditional schemes. One of the most critical observations is the improvement in authentication reliability, where the proposed method reached 94.6%, outperforming the nearest competitor (polynomial predistribution) by nearly 3%. This high success rate is vital for ensuring device legitimacy and preventing unauthorized access in real-time industrial communication. The key compromise probability was notably low in the proposed approach, with a derived key security score of over 82%, showcasing its robustness against attacks such as node capture, spoofing, and key exposure. This is a direct result of the method's dynamic rekeying and layered authentication mechanisms, which limit the potential damage of any single breach.

The attack resilience score (scaled to 90%) demonstrates the method's adaptability under simulated adversarial conditions. It retained communication integrity and confidentiality even during replay and man-in-the-middle scenarios, which often cripple simpler models like single network-wide key schemes. While latency and memory overhead were slightly higher in the proposed method compared to the most basic configurations, these increases remain within acceptable operational thresholds for industrial networks. The added resource usage is a worthwhile trade-off for the substantial gains in security and system stability. Overall, the discussion confirms that while traditional methods like centralized KDC and pairwise schemes offer partial improvements, they fall short in dynamic, high-risk environments. The dynamic hierarchical model not only addresses

scalability and energy efficiency but also introduces resilience mechanisms essential for secure industrial IoT deployments. These results validate the model's potential as a future-ready solution for protecting critical infrastructure in HART-enabled systems.

5.Conclusion

The resilience of key management systems is a cornerstone of security in HART networks, particularly within industrial environments where continuous and reliable sensor communication is essential. This study conducted a comprehensive evaluation of multiple key establishment strategies, including single network-wide keys, pairwise protocols, centralized Key Distribution Centers (KDC), polynomial-based predistribution, and the proposed dynamic hierarchical model. Utilizing formal verification through Colored Petri Nets (CPN) and adversarial modeling via the extended Canetti-Krawczyk (eCK) framework, each scheme was rigorously tested under realistic threat scenarios. The results clearly indicate that traditional approaches such as single shared keys are highly vulnerable, with authentication success rates as low as 70.2% and key compromise probabilities exceeding 85%. While pairwise and polynomial predistribution techniques improved authentication to 89.4% and 91.8% respectively, they still exhibited limitations in storage efficiency and attack scalability. Centralized KDC schemes demonstrated moderate security but remained susceptible to single-point failure and limited scalability. In contrast, the proposed dynamic hierarchical key management model achieved the highest performance across all metrics—authentication success rate of 94.6%, key compromise probability reduced to 17.8%, and attack resilience scoring 90% on a normalized scale. This approach demonstrated robust adaptability, efficient rekeying mechanisms, and resistance to a wide range of cyber-attacks including spoofing, replay, and man-in-the-middle scenarios.

These findings underscore the necessity for HART-based industrial systems to adopt adaptive, distributed, and formally verifiable key management architectures. Looking ahead, future research should focus on integrating blockchain-based distributed trust mechanisms, enhancing energy-aware cryptographic algorithms for resource-constrained devices, and exploring quantum-resilient key exchange protocols. Additionally, real-world deployment studies involving hybrid architectures and context-aware authentication should be pursued to validate scalability, performance, and interoperability across diverse industrial IoT platforms.

References

1. Zhang C, Chen Y. A review of research relevant to the emerging industry trends: Industry 4.0, IoT, blockchain, and business analytics. Journal of Industrial Integration and Management. 2020 Mar 19;5(01):165-80.
2. Jamai I, Azzouz LB, Saïdane LA. Security issues in Industry 4.0. In2020 International Wireless Communications and Mobile Computing (IWCMC) 2020 Jun 15 (pp. 481-488). IEEE.
3. Cheng X, Shi J, Sha M, Guo L. Launching smart selective jamming attacks in wirelesshart networks. In IEEE INFOCOM 2021-IEEE Conference on Computer Communications 2021 May 10 (pp. 1-10). IEEE.
4. Bokova OI, Kanavin SV, Meshcheryakov VA, Khokhlov NS. Information security system model in the automated system developed in the simulation software environment CPN Tools. In Journal of Physics: Conference Series 2020 Mar 1 (Vol. 1479, No. 1, p. 012021). IOP Publishing.
5. Saoji A, Rao GS. Hybrid [ACPSO] integration approach based on particle swarm optimization and ant colony optimization to improve lifetime of wireless sensor network. In2021 Asian Conference on Innovation in Technology (ASIANCON) 2021 Aug 27 (pp. 1-4). IEEE.
6. Kumar P, Chouhan L. A privacy and session key-based authentication scheme for medical IoT networks. Computer Communications. 2021 Jan 15;166:154-64.
7. Deebak BD, Al-Turjman F. Robust lightweight privacy-preserving and session scheme interrogation for fog computing systems. Journal of Information Security and Applications. 2021 May 1;58:102689.
8. Rao PM, Saraswathi P. Evolving cloud security technologies for social networks. In Security in IoT Social Networks 2021 Jan 1 (pp. 179-203). Academic Press.
9. Mirzaee PH, Shojafar M, Cruickshank H, Tafazolli R. Smart grid security and privacy: From conventional to machine learning issues (threats and countermeasures). IEEE access. 2022 May 11;10:52922-54.
10. Parsons L, Ross R, Robert K. A survey on wireless sensor network technologies in pest management applications. SN Applied Sciences. 2020 Jan;2(1):28.
11. Khalid U, Asim M, Baker T, Hung PC, Tariq MA, Rafferty L. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Cluster Computing. 2020 Sep;23(3):2067-87.

12. Tian Y, Wang Z, Xiong J, Ma J. A blockchain-based secure key management scheme with trustworthiness in DWSNs. IEEE Transactions on Industrial Informatics. 2020 Jan 13;16(9):6193-202.
13. Adavoudi-Jolfaei A, Ashouri-Talouki M, Aghili SF. Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks. Peer-to-Peer Networking and Applications. 2019 Jan;12:43-59.
14. Iqbal U, Shafi S. A provable and secure key exchange protocol based on the elliptical curve diffe–hellman for wsn. InAdvances in Big Data and Cloud Computing: Proceedings of ICBDCC18 2019 (pp. 363-372). Springer Singapore.
15. Anita EM, Geetha R, Kannan E. A novel hybrid key management scheme for establishing secure communication in wireless sensor networks. Wireless Personal Communications. 2015 Jun;82:1419-33.
16. Samaddar A, Easwaran A, Tan R. A schedule randomization policy to mitigate timing attacks in WirelessHART networks. Real-Time Systems. 2020 Oct;56(4):452-89.
17. Luo F, Feng T, Zheng L. Formal security evaluation and improvement of wireless hart protocol in industrial wireless network. Security and Communication Networks. 2021;2021(1):8090547.
18. Bokova OI, Kanavin SV, Meshcheryakov VA, Khokhlov NS. Information security system model in the automated system developed in the simulation software environment CPN Tools. In Journal of Physics: Conference Series 2020 Mar 1 (Vol. 1479, No. 1, p. 012021). IOP Publishing.
19. Zhang C, Chen Y. A review of research relevant to the emerging industry trends: Industry 4.0, IoT, blockchain, and business analytics. Journal of Industrial Integration and Management. 2020 Mar 19;5(01):165-80.
20. Qiu S, Wang D, Xu G, Kumari S. Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices. IEEE Transactions on Dependable and Secure Computing. 2020 Sep 8;19(2):1338-51.
21. Moriai S, Wang H, editors. Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part III. Springer Nature; 2020 Dec 4.
22. Ren Y, Liu Y, Ji S, Sangaiah AK, Wang J. Incentive mechanism of data storage based on blockchain for wireless sensor networks. Mobile Information Systems. 2018;2018(1):6874158.
23. Khan MT, Tomić I. Securing industrial cyber–physical systems: A run-time multilayer monitoring. IEEE Transactions on Industrial Informatics. 2020 Oct 22;17(9):6251-9.
24. Yousefpoor MS, Barati H. Dynamic key management algorithms in wireless sensor networks: A survey. Computer Communications. 2019 Jan 15;134:52-69.
25. Gautam AK, Kumar R. A robust trust model for wireless sensor networks. In2018 5th IEEE Uttar Pradesh section international conference on electrical, electronics and computer engineering (UPCON) 2018 Nov 2 (pp. 1-5). IEEE.
26. Adavoudi-Jolfaei A, Ashouri-Talouki M, Aghili SF. Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks. Peer-to-Peer Networking and Applications. 2019 Jan;12:43-59.
27. Jeong JH, Kwon SM, Shon TS. Security Threats Analysis and Security Requirement for Industrial Wireless Protocols: ISA 100.11 and WirelessHART. Journal of the Korea Institute of Information Security & Cryptology. 2019;29(5):1063-75.
28. Pourghebleh B, Wakil K, Navimipour NJ. A comprehensive study on the trust management techniques in the Internet of Things. IEEE Internet of Things Journal. 2019 Aug 6;6(6):9326-37.
29. Dinker AG, Sharma V. Polynomial and matrix based key management security scheme in wireless sensor networks. Journal of Discrete Mathematical Sciences and Cryptography. 2019 Nov 17;22(8):1563-75.
30. Luo F, Feng T, Zheng L. Formal security evaluation and improvement of wireless hart protocol in industrial wireless network. Security and Communication Networks. 2021;2021(1):8090547