International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 12 | Dec - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Comparative Study on Various Authentication Protocols in Wireless Sensor Networks

Soniya Sudarshan Katrale[1], Mr Pradeep Nayak[2], Sowjanya[3],
Srushti Manjunath Ullagaddi[4], Subramanya[5]
Assistant Professor, Department of Information on Science and Engineering[2]
Students, Department of Information on Science and Engineering[1,3,4,5,]
Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka, India

Abstract
Wireless Sensor Networks (WSNs) consist of numerous low-power, low-cost sensor nodes deployed in environments where physical monitoring and security are major challenges. Due to their wireless communication medium, dynamic topology, and limited computational resources, WSNs are highly vulnerable to attacks such as spoofing, Sybil attacks, selective forwarding, replay, and node capture. Authentication, therefore, becomes essential to ensure that data originates from legitimate nodes and remains unaltered during transmission. Various authentication mechanisms—including lightweight schemes, symmetric-key approaches, key management systems, and broadcast authentication techniques—have been proposed to address security requirements such as confidentiality, integrity, freshness, and availability.
This report provides a comprehensive comparative analysis of major authentication protocols used in WSNs. It studies lightweight authentication schemes, ECC-based approaches, trust-based models, TESLA and μTESLA broadcast authentication systems, and identity-based and one-time signature mechanisms. These protocols are evaluated based on communication and computation overhead, robustness to packet loss, resistance to denial-of-service attacks, scalability, and suitability for real-time applications. The findings highlight that while lightweight schemes excel in energy efficiency, public-key-based mechanisms offer stronger security, and TESLA variants provide scalable broadcast authentication. The study concludes that no single method fulfills all requirements, emphasizing the need for hybrid, adaptive, and energy-efficient authentication mechanisms in future WSN deployments.

1.Introduction
Wireless sensor networks (WSNs) are fast rising in popularity due to the low cost solutions for a number of difficulties in the real-world. WSN has no infrastructure support, is swiftly implemented in a region with numerous low-cost sensor nodes, is employed for monitoring the environment, and is rigorous to preserve its security. It is made up of a vast number of resource sensor nodes that are spread out geographically throughout the hostile environment. The sensor nodes' job is to detect physical occurrences in their local vicinity, process the information, and send it to the base stations. Since there are a lot of nodes in WSN and sensor nodes have limitations in terms of power, compute, communication, and storage, multihop communication is preferred.

Security in WSN becomes critical since the nodes after the deployment cannot be manually maintained and watched. This condition becomes a serious concern with WSN due to its network of communication. The authentication is supplied to the data that can be sent or read by any node in the network. Preventing and obtaining information from unauthorized users is also crucial. As new risks and attack models are offered, different kinds of authentication procedures have been created in WSN security. The following standards can be used to distinguish different authentication mechanisms: (i) authenticating unicast, multicast, or broadcasting messages,

(ii) symmetric (shared key) or asymmetric (public key) cryptography mechanism

(iii) WSN features that are mobile, static, or both.

Various works have concentrated on point-to-point authentication mechanisms, which authenticate unicast communications [1–3] in WSN. In spite of being secure, unicast methods cannot be applied straightly to either multicast or broadcast messages. Broadcast messages are straightly acquired from the trusted sources and cannot be modified during transmission. A broadcast authentication process's fundamental steps are

(i)verifying the message's original source identification

(ii)verifying the message's integrity.

Additionally, it offers precaution against (a) forgery, (b) replay attacks, and (c) impersonation, which are main features of the authentication mechanisms. There are two authentication mechanisms based on the cryptographic methods as discussed above. It can either be a symmetric method or an asymmetric method. The former methods use shared key cryptography, where both the sender and the receiver employ similar key in the process of authentication and verification. The latter case uses public key cryptography, where the sender signs a message with the private key and the receivers authenticate it by the respective public key.

In this survey, various existing authentication protocols in wireless sensor networks are discussed. A list of major issues and open research challenges are compared and analyzed. Moreover, an exhaustive survey on the available protocols for authentication in the wireless sensor networks and their applications is provided. The survey also contains the major aspects of examining the protocols on the basis of quality measurement as needed for authentication mechanisms. The comparison tables are provided for decision-making on the most appropriate protocols. It fulfils the requirements of the particular application scenario. This paper reviews several authentication protocols in WSN and its major contributions are listed as follows:

(i)comparison of various authentication protocols

(ii) information about several existing authentication protocols,

(iii) analyses of various schemes with different parameters in the existing methodologies.

2. Security Issues in Wireless Sensor Networks

2.1 Threats and Attacks on Sensor Node Routing

WSN routing protocols are often simple, making them susceptible to many attacks similar to those in ad hoc networks. Common attacks in WSNs include:
(i) spoofing, alteration, or replay of routing data,
(ii) selective packet dropping,
(iii) sinkhole attacks
(iv) Sybil attacks
(v) wormholes
(vi) HELLO flood attacks
(vii) acknowledgment spoofing.

2.1.1. Spoofed, Altered, or Replayed Routing Information

This attack targets routing messages exchanged between nodes. Attackers may create routing loops, inject false updates, increase latency, modify paths, or disrupt the network by partitioning it.

2.1.2. Selective Forwarding

A malicious node may intentionally drop selected packets instead of forwarding them. Acting like a black hole, it discards messages that pass through it, interrupting communication along the data path.

2.1.3. Sinkhole Attacks

Here, an attacker positions a compromised node to appear highly attractive to neighboring nodes, drawing most of the network traffic through itself. Depending on the routing method, the adversary may manipulate reliability or latency metrics to mislead nodes.

2.1.4. Sybil Attacks

In this attack, a single node assumes multiple identities. This undermines redundancy, disrupts fault-tolerant mechanisms, and severely affects geographic routing, as the attacker appears to exist at several locations concurrently.

2.1.5. Wormholes

A wormhole attack involves two colluding malicious nodes that create a low-latency communication tunnel. Messages captured in one part of the network are replayed elsewhere, misleading routing decisions by making nodes seem closer than they are.

2.1.6. HELLO Flood Attack

An attacker with high transmission power sends HELLO packets to convince nodes that it is within their neighbourhood. Nodes assume the adversary is a nearby node and may forward messages to it incorrectly.

2.1.7. Acknowledgment Spoofing

The goal is to mislead the sender into believing that a dead or weak link is functioning properly. By spoofing acknowledgment packets, attackers can redirect traffic toward compromised or unreachable nodes.

2.2. Security Requirements and Challenges in WSNs.

WSNs possess several functionalities similar to conventional computer networks, while also displaying distinctive characteristics of their own. For these networks, ensuring security is essential, and the key security requirements are as follows:

(i) Data confidentiality: ensures that messages transmitted within the network cannot be interpreted by unauthorized entities. It also safeguards privacy across wireless communication mediums, including mobile code, application data, and control messages, thereby preventing eavesdropping.
(ii) Availability: guarantees that the services provided by the entire WSN—or any of its components—remain accessible as needed.
(iii) Authentication: verifies the identities of sensor nodes, cluster heads, and base stations before granting access to restricted resources or sensitive information.
(iv) Authorization: ensures that only legitimate and approved nodes are allowed to perform specific operations.
(v) Integrity: assures that the data remains unchanged during transmission from the sender to the receiver.
(vi) Freshness: ensures that data is up-to-date and protects the network from replay attacks.
(vii) Nonrepudiation: prevents malicious nodes from denying their activities or participation in communication.

Designing strong security mechanisms for WSNs is more challenging compared to wired networks due to several inherent constraints:

(i) wireless nature of communication,
(ii) limited resources of sensor nodes,
(iii) large and densely distributed sensor deployments,
(iv) unpredictable network topology,
(v) continuously changing or dynamic topology.

3. Authentication in Wireless Sensor Networks

Authentication in WSNs is the process of confirming the identity of a node and ensuring that transmitted data or control messages originate from a legitimate source. Authentication procedures generally fall under the following categories:

(i) one-way authentication
(ii) two-way or mutual authentication
(iii) three-way authentication
(iv) implicit authentication

3.1. One-Way Authentication

A single message is sent from the sender to the receiver. This message must prove:
(a) the sender's identity,
(b) that the message was generated by the sender,
(c) that it is intended for the correct receiver, and
(d) that it has not been altered during transmission.

3.2. Two-Way or Mutual Authentication

Here, both communicating nodes authenticate each other. In WSNs, this involves not only the validation between ordinary nodes and the base station but also mutual verification between any two communicating nodes to ensure trust.

3.3. Three-Way Authentication

A third message from the sender to the receiver is exchanged when the nodes' clocks cannot be synchronized, providing an additional verification step.

3.4. Implicit Authentication

This form of authentication occurs indirectly as a result of other operations, such as key establishment. It is beneficial in WSNs because it reduces operational complexity and conserves energy.

Authentication challenges vary based on node deployment strategies.
In static deployment, nodes remain fixed and are susceptible to replay attacks, making them easily traceable; thus, authentication protocols must address these threats.
In dynamic deployment, challenges include:
(a) reauthentication of mobile nodes,
(b) ensuring mobility remains untraceable,
(c) maintaining message integrity,
(d) ensuring data confidentiality, and
(e) handling node capture and compromise.

4.Various Authentication Protocols in Wireless Sensor Networks

This section briefly discusses some of the popular authentication protocol schemes in wireless sensor networks.

4.1. Lightweight Dynamic User Authentication Scheme

In this method, the WSN is deployed in a restricted region divided into multiple zones. Authorized users interact with sensor nodes through mobile devices. The scheme consists of three stages:
(i) registration,
(ii) login, and
(iii) authentication.
A user must first register at the sensor gateway by providing a username and password before making any request to the system. After successful registration, the user may submit queries within a specific time window, which varies based on the application's needs. Once the time limit expires, the user must re-register to begin a new session. This dynamic authentication method allows legitimate users to access sensor data from any node with minimal computational effort. It is secure only against replay and forgery attacks.

An improved lightweight authentication scheme addresses the weaknesses of the earlier method by adding better security while retaining its benefits. This enhanced version includes four phases: registration, login, authentication, and password change. Registration and password update are performed over a secure channel. The system offers protection against replay and forgery attacks, reduces the risk of password exposure, enhances efficiency, and supports password updates.

4.2. Lightweight Trust Model

To minimize energy and memory usage, lightweight trust mechanisms are introduced. The collaborative lightweight trust-based routing protocol (CLT) reduces memory usage through the following steps:
(i) Trust is calculated as a positive integer between 0 and 100, requiring just one byte of memory.
(ii) The trust value is not directly saved in the transaction table.
(iii) Only 3 bits of memory are used to store the trust level, significantly reducing storage needs.
This model increases the packet delivery ratio through trust-based routing and lowers energy consumption by avoiding promiscuous listening mode.

4.3. Lightweight Authentication Scheme for WSNs

This energy-efficient authentication and key establishment approach uses keyed-hash functions (HMAC) and basic encryption methods to provide secure

communication. It also reduces the effect of resource depletion attacks. The scheme includes three phases: (i) a key predistribution stage performed during node manufacturing, (ii) network initialization during deployment where nodes discover neighbors and set up security, and (iii) an authentication phase triggered when a new node attempts to join the network.

The system is strongly resistant to node capture and scales efficiently with very large networks. Similarly, the Secured Energy Conserving Slot-Based Topology Maintenance Protocol uses symmetric key–based authentication to manage sleep/wake cycles, improving energy usage and network lifetime. It is resilient to several attacks such as Sybil, replay, substitution, and sleep deprivation.

4.4. Lightweight Key Management Scheme

This lightweight key management method reduces resource usage and supports other security mechanisms. It uses numeric sequences that allow each sensor node to compute unique pairwise keys with neighboring nodes. The key goals are:
(i) efficient resource usage,
(ii) scalability, and
(iii) support for backward and forward secrecy.
The technique uses minimal key storage and requires fewer message exchanges. It is advantageous because it consumes less memory and energy, performs lightweight key computations, and resists node capture.

4.5. SPINS: Security Protocol for Sensor Networks

SPINS provides two security protocols—SNEP and µTESLA—to secure communication in WSNs. The SNEP protocol offers:
(i) confidentiality,
(ii) integrity,
(iii) authentication,
(iv) weak message freshness, and
(v) replay protection.
SNEP achieves message authenticity and integrity using a Message Authentication Code (MAC). µTESLA requires loose time synchronization between nodes and knowledge of the maximum clock drift.
Implementations require further study on transceiver modulation techniques and memory-performance tradeoffs.

4.6. LEAP: Localized Encryption and Authentication Protocol

LEAP introduces several keying mechanisms to secure different types of packets in WSNs. The protocol provides four keys per node:
(i) an individual key shared with the base station,
(ii) a pairwise key shared with nearby nodes,
(iii) a cluster key shared with a small group of neighbors, and
(iv) a group key shared by all nodes.
µTESLA is used for sink node broadcast authentication, ensuring packets originate from the sink. LEAP uses a predistributed key to establish all four keys. Nodes broadcast IDs, compute shared keys, and distribute cluster and group keys in a multihop manner.LEAP is efficient in terms of storage, key updating, and authentication. Its strengths include µTESLA support, one-way key chains, key revocation, and scalability. A limitation is the assumption that the sink node remains uncompromised.

4.7. Efficient Authenticated Key Establishment Protocols

This approach uses Elliptic Curve Cryptography (ECC) to provide strong security on devices with limited computing power. ECC requires shorter keys while delivering high security, fast processing, low complexity, and small storage needs. The protocol uses two phases:
(i) implicit certificate creation
(ii) hybrid key establishment.
Certificates prevent impersonation by associating a key with a node's identity and expiration time. A drawback is that each node must communicate directly with the Certificate Authority (CA), which may create a bottleneck. Additionally, dynamic reauthentication is not addressed.

4.8. Authentication and Key Establishment in Dynamic WSNs

In dynamic WSNs, nodes may move and encounter new neighbors without having preshared keys. Therefore, a scalable and efficient key establishment protocol is necessary. Each node maintains a key cache to store and manage keys. The procedure includes:
(1) checking for an existing shared key,
(2) performing shared-key detection if no key exists,
(3) creating a key cache entry when needed,
(4) updating session keys and lifetimes upon receiving a notice message,
(5) restarting the process when the key expires, and
(6) deleting old entries to save memory.
This protocol is suitable for both static and dynamic networks and ensures high probability of key sharing with low communication overhead.

4.9. Broadcast Authentication in WSNs

Broadcast authentication is performed using either digital signatures or µTESLA-based techniques. While digital signatures support immediate authentication, µTESLA requires delayed verification. A dynamic window system allows nodes to choose whether to authenticate first or forward a packet first; however, it is partially vulnerable to DoS attacks. To address this, a group key strategy was introduced to protect against malicious nodes. Self-healing key management with broadcast authentication offers stronger security,

reduced resource usage, adjustable window sizes, and adaptable self-healing features.

4.10. Short-Term Public Key System for Broadcast Authentication

This scheme reduces signature verification time by using short-lived public keys. Although the use of shorter keys weakens the security strength, it significantly lowers authentication costs compared to long-term public keys. Due to memory limitations, nodes cannot store all public keys. Therefore, the system transforms broadcast authentication into a public key distribution challenge. The progressive public key distribution mechanism is reliable, efficient, and tolerant to packet loss, allowing the sink node to periodically broadcast and redistribute new public keys.

4.11. Multiuser Broadcast Authentication

Four different public key–based mechanisms have been introduced to provide a detailed comparison of their strengths and weaknesses. In all these methods, user verification is performed using public keys. The approaches include:
(i) a basic certificate-based method,
(ii) a direct storage-based technique,
(iii) a bloom filter–based system, and
(iv) a hybrid system.
In this model, bloom filters are used to store user identities and their corresponding public keys for multiuser authentication. However, bloom filters are vulnerable because they can be manipulated and do not offer protection against DoS attacks.

4.12. Lightweight One-Time Signature Scheme

This scheme enables sensor nodes to authenticate broadcast messages sent by the base station. It uses symmetric cryptographic primitives to provide asymmetric properties for secure broadcast authentication. However, one-time signature systems typically suffer from two major drawbacks: large key sizes and the capability to authenticate only a limited number of messages. Despite this, the scheme reduces storage requirements and includes a rekeying method to allow signing of future messages.

The main steps of the scheme are summarized as follows:
(i) The signer first creates a key pair consisting of private “balls” and public “balls.”
(ii) A verifier can authenticate the private balls using their corresponding public balls.
(iii) The scheme consists of three phases: initialization, signing, and verification.
(iv) The sender produces both private and public keys in the initialization phase.
(v) A pseudorandom generator creates the private key from random numbers.
(vi) A public key is generated by hashing, and the private key is used during the signing process.
(vii) In the verification phase, receivers use the public key to validate the message signature.
(viii) Compared to the HORS scheme, this method uses less storage and communication overhead but requires higher computation.
(ix) Additional hash operations are employed because conserving storage is more critical than saving computation in sensor nodes.

This signature scheme has four key advantages over μTESLA: it does not require time synchronization, avoids receiver-side buffering, authenticates each message individually, and supports immediate authentication. It also strengthens security while maintaining low performance overhead.

4.13. Mutual Authentication and Key Establishment Protocol

This protocol is designed for IP-enabled WSNs operating over 6LoWPAN. Traditional key predistribution techniques are not optimal due to the varying number of devices in the network. To enhance security, the protocol incorporates ECC-based cryptographic methods. To reduce communication overhead and prevent new security threats, the network authenticates an incoming node by generating its authentication key.

Key features of this protocol include:
(i) Offline key assignment: Each device is given a random value and a single share of a public key. ECC is generated using source and destination IP addresses to secure communication.
(ii) Authentication: Only trusted nodes are permitted to access network services.
(iii) Private key generation:
Private key = $(\text{Public key} \oplus \text{Random number})^{-1} \bmod \text{PSN}$.
(iv) Handover: Both public and private keys of nodes are updated to prevent node replication and Sybil attacks.

The system performs effectively against various security threats and reduces the time required for exchanging key establishment packets. Using the Cooja simulator, energy usage and overhead during network connectivity and handover can also be evaluated.

4.14. EIBAS: Efficient Identity-Based Broadcast Authentication Scheme

This scheme consists of a fixed sink, users, and a large number of sensor nodes. The sink acts as a private key generator and is responsible for issuing private keys to users, despite having limited storage. EIBAS aims to meet two major goals: providing user authentication and message integrity, and reducing communication overhead.

The primary contributions of EIBAS are:
(i) System initialization: A prime generator and bilinear pairing are created based on the security parameter, followed by choosing a random number and four cryptographic hash functions.
(ii) Private key extraction: A user obtains a private key generated by the sink along with an identity to join the WSN.
(iii) Signature generation and broadcasting: A timestamp is selected, and the user broadcasts the message to the network.
(iv) Broadcast authentication: Sensor nodes validate the message upon receipt. If verification fails, the message is discarded; otherwise, it is accepted.

EIBAS uses an optimized identity-based signature scheme that reduces communication and computation costs. Among existing techniques, it transmits the smallest broadcast message size and achieves lower energy consumption. It also scales efficiently as the network grows.

4.15. Lightweight Authentication Scheme

Lightweight authentication methods combine key establishment and authentication processes. The key establishment phase is executed during the deployment of the network, while the authentication phase occurs when a new node attempts to join after deployment. These schemes are extremely efficient, impose no special constraints on the network, and follow three main stages:

(i) Key pre distribution: Performed before deployment during node installation.
(ii) Network initialization: Establishes the initial security configuration during deployment.
(iii) Authentication: Executed each time a new node joins the network.

The main advantages include strong resistance to node capture and secure node-to-node identity verification. Only one message exchange is required, making it highly efficient.
Another lightweight scheme, TinyZKP, is specifically designed for wireless body area networks. It uses minimal memory and energy and operates very quickly, making it suitable for resource-constrained embedded devices.

4.16. LOCHA: Lightweight One-Way Cryptographic Hash Algorithm

LOCHA is a lightweight hash algorithm that generates a short, fixed-length hash value from an input message. The main steps include:

(i) Converting the input message into binary ASCII codes for preprocessing.
(ii) Padding the message with bits at the least significant end to make the length divisible by 512.
(iii) If the message already meets this requirement, an extra block of 512 zeros is added for increased robustness.
(iv) The message is divided into three nested levels—512-bit, 64-bit, and 8-bit blocks.
(v) Transformations occur at each nested level to ensure uniformity and reduce storage requirements.
(vi) A three-level swapping mechanism is applied to produce the final hash digest.

5.Discussion on Various Protocols

The evaluation of different authentication protocols for Wireless Sensor Networks (WSNs) shows that each protocol offers unique strengths but also carries certain limitations depending on the operational environment. Lightweight protocols are generally well-suited for sensor nodes because they minimize computational and communication overhead. These protocols make use of symmetric keys, hash functions, and simplified cryptographic operations, allowing them to operate efficiently on devices with limited memory, power, and processing capacity. However, their simplicity can also make them less resilient against advanced security attacks or node capture scenarios.

TESLA-based authentication mechanisms provide efficient broadcast authentication by using delayed key disclosure and one-way key chains. These protocols demonstrate strong scalability and are appropriate for situations involving many receivers. Their major limitation is the absence of immediate authentication due to the delay in key disclosure, which may be problematic in time-critical applications. Public-key-based protocols, including ECC-or identity-based mechanisms, offer higher levels of security and better support for authentication between previously unknown nodes. Although their security is strong, the computational load is heavier, making them less suitable for extremely resource-constrained sensors unless optimization techniques are used.

Key-management-focused protocols provide structured ways to establish secure communication between nodes, enabling individual, pairwise, cluster-level, and group authentication. These protocols tend to provide strong foundational security but may introduce communication overhead during key establishment and rekeying processes, especially in dynamic networks. Trust-based and behavioral-analysis protocols contribute an additional layer of security by evaluating node behavior; however, they may require continuous monitoring and storage resources which increase overhead.

Overall, no single protocol fully satisfies all security and performance requirements of WSNs. Lightweight protocols are good for energy conservation, TESLA-based schemes work well for broadcast authentication, and public-key-based solutions offer robust security. The

discussion clearly indicates that designing hybrid, optimized, and context-specific authentication protocols is essential for achieving an ideal balance between security, efficiency, and resource utilization in wireless sensor networks.

6 .Future Enhancements

A variety of authentication techniques and lightweight security schemes have been evaluated based on several important parameters. These parameters are described below.

6.1. Source Authentication.
Source authentication ensures that broadcasted messages genuinely come from the claimed sender. Each receiving node checks and confirms the sender's identity before accepting the broadcast message.

6.2. Data Integrity.
Data integrity ensures that the message content remains unchanged during transmission. It verifies that no alteration occurred between the sender transmitting the message and the receiver receiving it.

6.3. Immediate Authentication.
Immediate authentication allows a receiver to instantly approve or reject a message the moment it arrives, without any delay. Many MAC-based protocols cannot provide this feature, making them unsuitable for systems that require strict real-time communication.

6.4. Time Synchronization.
This requirement ensures that receivers can verify whether the sender's authentication key was still undisclosed at the time the message was received. Synchronization prevents the acceptance of messages authenticated with prematurely revealed keys.

6.5. Message Cost.
Message cost refers to the total number of messages exchanged to complete the authentication process. A higher number of exchanges results in increased message cost, while fewer exchanges reduce the cost.

6.6. Communication Overhead.
Communication overhead represents the amount of additional communication burden introduced by an authentication protocol. MAC-based schemes generally require very low overhead, whereas digital signature methods depend on large public keys and thus incur more overhead. Protocols like TESLA, µTESLA, multilevel µTESLA, BABRA, unbounded key chains, L-TESLA, XTESLA, TESLA++, and RPT have low communication overhead because they only require two or three messages. Hierarchical key chains and lightweight schemes need just one message, resulting in extremely minimal overhead.

6.7. Computation Overhead.
Computation overhead refers to the processing required for authentication. The sender performs most of the computational work, while the receiver's workload remains very small. Authentication adds extra processing due to signature generation and verification steps. Protocols such as TESLA, µTESLA, multilevel µTESLA, BABRA, L-TESLA, X-TESLA, TESLA++, and RPT have low computational costs because they use MD5, which has linear computational complexity.

6.8. Cryptographic Method.
Authentication protocols may employ either symmetric MAC-based systems or asymmetric digital signature (DS) techniques. Asymmetric approaches can include one-time signature mechanisms or public-key-based systems. The specific symmetric and asymmetric methods used by different protocols are identified in the referenced table.

6.9. DoS Attack Resistance.
A protocol is considered resistant to Denial-of-Service (DoS) attacks if it provides protection against threats like flooding or jamming. Ensuring DoS resistance is crucial so that the broadcast authentication mechanism can function continuously without interruption.

6.10. Robustness to Packet Loss.
This parameter evaluates how well a protocol performs when authentication information is lost. Many TESLA-based protocols use one-way key chains, enabling lost keys to be reconstructed from subsequent keys. This approach enhances robustness and eliminates the need for additional authentication packets.

Based on this analysis, the future direction of our research involves developing a secure lightweight authentication scheme for sensor networks. The proposed system aims to support the following features:
(i) It applies symmetric cryptography with minimal encryption and utilizes hash functions.
(ii) It enables secure identity authentication between individual nodes.
(iii) It maintains low computational and communication complexity during authentication.
(iv) It offers protection against insider threats, such as clone attacks, as well as DoS-based disruptions.

Overall, the proposed lightweight approach is expected to provide improved energy efficiency, reduced communication overhead, and lower computational requirements compared to existing authentication methods.

Conclusion

Security remains a critical challenge in energy-limited Wireless Sensor Networks (WSNs) because of their wide range of security-driven applications. With increasing emphasis on secure communication, designing robust

security protocols has become both essential and difficult. Numerous authentication approaches have been explored to guarantee node confidentiality and authenticity. While many existing mechanisms primarily address security, some also succeed in providing scalability along with reduced communication and computation overhead. Authentication plays an important role in defending against various attacks since it relies on secure key-sharing processes. The existing research clearly shows that effective authentication strategies can lower computational effort and help conserve energy in sensor nodes. However, despite its extensive use, authentication still faces limitations such as the complexity of managing public key infrastructures and significant computational burdens. These challenges highlight the need for continued research to develop more efficient and practical authentication solutions for WSNs.

Reference

[1] X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 24–34, 2007.

[2] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Transactions on Information and System Security*, vol. 8, no. 1, pp. 41–77, 2005.

[3] M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic key management in sensor networks," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 122–130, 2006.

[4] J. Sen, "A survey on wireless sensor network security," *International Journal of Communication Networks and Information Security*, vol. 1, pp. 55–78, 2009.

[5] K. H. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, vol. 1, p. 8, IEEE, Taichung, Taiwan, June 2006.

[6] T.-H. Lee, "Simple dynamic user authentication protocols for wireless sensor networks," in *2008 Second International Conference on Sensor Technologies and Applications (SENSORCOMM '08)*, pp. 657–660, Cap Esterel, France, August 2008.

[7] B. Vaidya, J. Sa Silva, and J. J. P. C. Rodrigues, "Robust dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the 5th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet '09)*, pp. 88–91, ACM, October 2009.

[8] O. Cheikhrouhou, A. Koubaa, M. Boujelben, and M. Abid, "A lightweight user authentication scheme for wireless sensor networks," in *Proceedings of the ACS/IEEE International Conference on Computer Systems and Applications (AICCSA '10)*, pp. 1–7, Hammamet, Tunisia, May 2010.

[9] H.-R. Tseng, R.-H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the 50th Annual IEEE Global Telecommunications Conference (GLOBECOM '07)*, pp. 986–990, Washington, DC, USA, November 2007.

[10] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *Journal of Network and Computer Applications*, vol. 35, no. 5, pp. 1646–1656, 2012.