Efficient Multipath Routing and Anomaly Detection with a Token-Managed Certificateless Authentication Scheme (TM-AD) in WSNs

J Sangeethapriya[1,2 *], Michael Arock[2], U Srinivasulu Reddy[1]
[1]Research Scholar, Department of Computer Applications, National Institute of Technology, Trichirappalli-620015, Tamil Nadu, India
[2]Assistant Professor, Department of Information Technology, Saranathan College of Engineering, Tiruchirappalli-620012, Tamil Nadu, India
E-mail: sangeethapriya.nitt@gmail.com, michael@nitt.edu, usreddy@nitt.edu
*Corresponding author

Keywords: WSN, TM-AD, IoT, anomaly detection, security

Received: April 20, 2025

Wireless Sensor Networks (WSNs) are crucial for diverse Internet of Things (IoT) applications, but their inherent resource constraints and distributed nature expose them to significant security vulnerabilities. A primary challenge is the effective and timely detection and mitigation of malicious or misbehaving nodes, which can disrupt network operations, compromise data, and reduce network lifespan. Existing approaches often face obstacles in efficiently addressing these threats. This paper proposes the Token Manager-based Attack Detection (TM-AD) scheme, to enhance WSN security and operational efficiency. The TM-AD system features a "Token Manager" (TM), a dedicated entity responsible for continuous network monitoring, assessing node behavior based on defined parameters, and managing node participation through a token-based mechanism. Upon identifying malicious or anomalous activity, TM-AD facilitates uninterrupted network transmission by orchestrating the replacement of compromised nodes with designated "replacement nodes." The efficacy of the proposed TM-AD system is evaluated through comparative analysis. At 100 network nodes, TM-AD achieved a 100% attack detection rate and 100% network throughput, alongside a reduction in routing overhead of up to 43.8% and in end-to-end delay of up to 74.7% compared to benchmark schemes. These results affirm that TM-AD effectively identifies malicious nodes and significantly enhances network performance across these key metrics, thereby ensuring a more robust and reliable WSN operation.

Povzetek: Učinkovit večpotni usmerjevalni in varnostni mehanizem za brezžična senzorska omrežja združuje zaznavanje anomalij s certifikatno-neodvisno avtentikacijo, upravljano z žetoni (TM-AD). Predlagani pristop izboljša varnost, zanesljivost prenosa in energijsko učinkovitost v IoT okoljih.

1 Introduction

In recent years, WSN technology has undergone significant development, capturing the attention of both academic and industry communities. A WSN is a self-organized multi-hop network consisting of numerous sensor nodes with distinct attributes, such as flexibility, fault tolerance, high sensing capabilities, and rapid deployment. These features have led to diverse applications of WSN, including environmental monitoring, agriculture, military, Smart Grids, and healthcare [1, 2]. The WSN system comprises three key elements: aggregation nodes (sink nodes), sensor nodes, and management nodes, as depicted in Figure 1. Sensor nodes are strategically placed within the monitored area, manually or by drone dispersal, forming a WSN through Wireless Self-Organization. In this network, each node acts as a router, establishing and restoring connections as needed [1]. WSNs collect data from sensor nodes, transmitting it to sink nodes in a single-hop or multi-hop fashion. Sink nodes conduct preliminary data processing and information fusion before transferring the data to users via satellite or wired networks [1].

Despite their utility, WSNs face significant security challenges. Wireless communication channels are susceptible to eavesdropping and data manipulation [3, 4]. Furthermore, sensor nodes often operate in unsupervised or hostile environments, making them vulnerable to physical capture and compromise by malicious actors [4-6]. Traditional cybersecurity mechanisms are often ill-suited for WSNs due to their unique threat landscape and severe resource constraints, including limited bandwidth, processing power, and storage [7, 8]. Ensuring data integrity, authentication, and non-repudiation under these limitations is a considerable challenge [1]. To address these security requirements, various cryptographic techniques have been considered. While Public Key Infrastructure (PKI) offers strong security, its certificate management overhead is problematic for WSNs [4]. Identity-Based Cryptography (IBC) simplifies this but introduces key escrow concerns [9]. Certificateless Public

Key Cryptography (CL-PKC) has emerged as a promising alternative, as it avoids certificates and the key escrow problem by having a Key Generation Centre (KGC) issue only partial private keys [10, 11]. While direct implementation of full CL-PKC schemes can still be demanding for all WSN operations, the principles of minimizing reliance on heavy infrastructure and distributing trust are valuable. This paper introduces the Token Manager-based Attack Detection (TM-AD) scheme, a novel approach that focuses on efficient anomaly detection and routing maintenance through a token-based system. While not a direct implementation of CLS for all node communications, TM-AD is designed with lightweight operation in mind, concentrating on behavioral analysis and adaptive routing managed by a central Token Manager to enhance WSN security and resilience.

2 Related work

Several researchers have examined and applied various kinds of strategies for protection like machine learning [12], deep learning etc. Kumar et al. [13] used blockchain and deep learning for vehicular network security. While robust, its high computational/communication overhead and vehicular focus make it ill-suited for resource-constrained WSNs needing lightweight, real-time anomaly detection. TM-AD, using a central Token Manager, offers a WSN-tailored, low-overhead alternative for behavioral anomaly detection and routing maintenance.

Mahdavisharif et al. [14,29] used deep learning for intrusion detection in general networks, achieving high accuracy. However, its reliance on substantial data storage and processing makes it impractical for resource-constrained WSNs. WSNs require lightweight solutions. TM-AD offers this via localized, token-managed behavioral analysis, minimizing resource use on sensor nodes.

A low-power 3D WSN privacy protection technique [15] aimed to enhance data security with low energy use and improved data fusion. Despite these merits, its privacy protection ability was identified as needing significant improvement. TM-AD complements such fusion-focused privacy by addressing node misbehavior and routing integrity, crucial for overall network security.

In [16]. introduced research on monitoring methods related to WSN applications. In this work, the Sensors distinguish an attenuated (unknown) deterministic signal when the target is fixed, and the signal depends on the unknown distance between the sensor and the target. Therefore, the simulation results ensure the promising performance of the proposed method.

In [17], the long-range transmission issue that WSNs encounter was examined, leading to the development of an optimized system for WSNs for fuzzy subordinate support systems. There is a discussion on the system's precise level. For WSN data aggregation, Lakshmi and Deepthi [18] proposed a channel code-based privacy scheme. However, it lacks mechanisms to detect malicious nodes that could falsify data or disrupt routes. TM-AD addresses this by providing node-level behavioral analysis and ensuring routing integrity.

The information security issue about WSNs in the power grid was tackled by [19], and his team members also proposed a blockchain-based data-sharing paradigm. It is crucial to remember that the analysis evaluated how well and safely the data-sharing model shares, stores, and protects sensitive information [19]. An enhanced approach was developed by Jiang et al. [20] to address security flaws and excessive energy consumption in WSN applications, including military surveillance and habitat monitoring. The scheme carefully distributes the sensors. In contrast with traditional deployment plans, this approach may have improved privacy while optimizing energy consumption and information latency [20,32].

For data compression in WSNs, a data clustering method that adapts characteristics such as adaptive recursion and smooth data compression was developed [21,30]. Experiments demonstrate that this kind of technique can compress data with as minimal space-time complexity as possible. The system accurately predicts the failure intensity of landslides, according to the optimized WSN presented in [22,31].

Research in [23], A blockchain-based trust management model was proposed to detect malicious WSN nodes and improve beacon node relationships explored blockchain-based trust management for WSN malicious node detection using various assessment metrics. While robust, the overhead and latency for localization. Though it establishes a trust evaluation model, its primary application to secure localization and the overhead of blockchain may limit associated with blockchain operations might hinder real-time responsiveness in dynamic WSNs. TM-AD aims for quicker detection through a centralized Token Manager and behavioral analysis.

Abubaker et al. [24,33] combined blockchain and federated learning (FL) for IoT sensor network security. While advanced, FL and blockchain introduce significant computational and communication overhead. For WSNs needing rapid, low-latency responses with minimal node burden, TM-AD's direct, token-managed centralized analysis offers potentially faster reaction times.

In [25,34] proposed a blockchain technology of an authenticated group key agreement mechanism for the IoTs. The novel concept called the device manager mediates communications between IoT gadgets and blockchain infrastructures is the proposed protocol and it has been secured after being subjected to various assaults, as indicated by the security analysis. The time expenditures of protocol operations are fair and appropriate for IoT settings shown in the simulation. Its primary focus on key agreement, does not address ongoing behavioral monitoring or routing attacks once keys are established.

Gebremariam et al. [26] integrated blockchain/FL for secure WSN localization and malicious node detection. While powerful, this combines FL's computational demands with blockchain's overhead, posing complexity for resource-constrained WSNs needing immediate responses. TM-AD offers a simpler, centralized token

management for direct behavioral monitoring and lower latency.

For WSNs, Cheng and Zhu [27] presented a lightweight anomaly detection scheme. However, its scope may not fully cover the integrated routing maintenance and node replacement that TM-AD offers.

Shi et al. [28] introduced I-CPDA, improving privacy in WSN cluster-based data aggregation. While effective for data fusion within clusters, its primary focus is on data protection, not detecting subtle network-wide misbehaviors like routing attacks. TM-AD offers a broader network-level approach by monitoring overall node behavior and actively managing routing paths.

2.1 Problem statement

Privacy issues arise when IoT devices exchange sensitive data over a network channel.

- Existing approaches are easily susceptible to security levels and may not provide sufficient protection.
- No documented evidence that any malicious nodes intruded and disrupted the network transmission
- If any transmission fails there is no established system for implementing alternatives or replacing malicious nodes.
- Previous approaches do not guarantee any reliable communication with a High Packet Delivery Ratio (PDR), throughput, and lifespan.

2.2 Research contribution

The Token manager concept introduces a method known as Token-Based Server Attack Detection (TM-AD).

- This work reveals a thorough evaluation of the proposed technique combining security analysis and experimental findings, thereby demonstrating its superior effectiveness in comparison to existing techniques.
- To ensure reliable transmission, the routing path are upgraded by replacing the malicious nodes with the replacement nodes, affirming successful transmission.
- The article emphasizes a comparative analysis of the proposed technique, with a specific focus on assessing various efficiency parameters.
- Promotes secure IoT transmission, by employing encrypted data through a reliable and lightweight pathway to elevate network performance.

3 Proposed methodology

The Token Manager-based Anomaly Detection (TM-AD) scheme is engineered to establish efficient multipath routing, identify anomalous node behaviour, and proactively uphold network integrity within Wireless Sensor Networks (WSNs). As depicted in Figure 1, the TM-AD architecture is cantered around a **Token Manager (TM)**—a pivotal, logically centralized entity—supported by several key interacting components.

- **Sensor Nodes:** These are the WSN's fundamental units, deployed for environmental data acquisition and packet relay. Within TM-AD, their primary functions include data collection, forwarding data along TM-established routes, and reporting necessary status information to the TM. Their active network participation is governed by tokens.

- **Token Manager (TM):** This critical entity, typically a node selected for its superior resources (e.g., energy, bandwidth, as detailed in Sec 3.2), acts as the central network orchestrator. Its core responsibilities encompass discovering nodes, continuously monitoring their status (e.g., energy, location, activity), issuing and managing tokens, establishing and maintaining optimal routing paths (via a routing table), detecting behavioral anomalies or malicious activities, and initiating corrective actions such as node isolation or replacement.

- **Tokens:** These are logical constructs or messages exclusively managed and distributed by the TM. Tokens serve as dynamic authorizations for sensor nodes, signifying their permission for active network participation, validating their current operational status, or assigning them to specific routing tasks. The nature of information conveyed by a token is adaptable to current network needs.

- **Cooperative Node List:** Maintained by the TM, this is a dynamic registry of sensor nodes currently verified as active and trustworthy participants in network operations, particularly for routing and data forwarding. The TM uses this list as a basis for packet transmission processing and targeted monitoring.

- **Replacement Nodes:** These are pre-designated or dynamically available sensor nodes intended to assume the functionality of other nodes that the TM has identified as irrecoverably malicious or failed. Their integration is orchestrated by the TM to ensure network resilience.

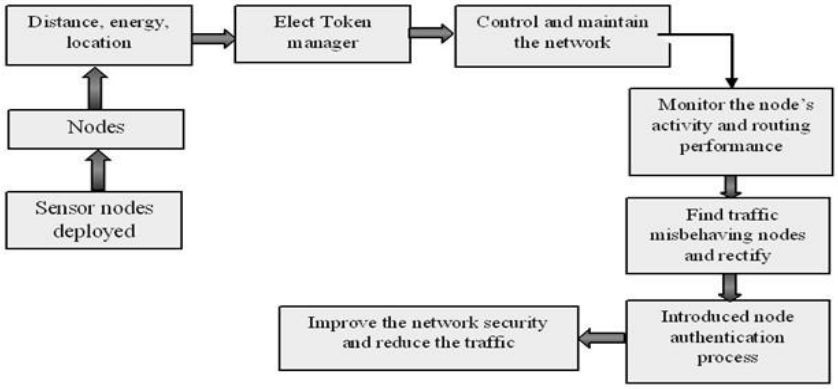

Figure 1: Proposed architecture-token manager-based anomaly detection (TM-AD) system

Figure 1 visually represents these components and their interactions, highlighting the TM's central coordination. The subsequent sections will detail TM-AD's operational phases and the algorithms dictating these component interactions.

Algorithm 1: Token manager (Tm) creation and initial network setup

Input: Randomly deployed nodes Nodes_Deployed = {N1, N2, N3 ... Nn}.

Output: Designated Token Broker node (Tm_selected), Cooperative Node List (Cooperative_List), Idle Node List (Idle_List), Initial Token Distribution.

Procedure Procedure Initial_Network_Setup(Nodes_Deployed)

// **1. Elect the most capable node to be the Token Manager (TM)**
// This function internally checks energy (>65%) and centrality.
TM ← Find_Best_TM_Candidate(Nodes_Deployed)

If TM is null:
Return Failure("Network setup failed: No suitable TM found.")
End If

// **2. TM discovers the network to build lists of active and idle nodes**
// This function internally broadcasts a "HELLO" and waits for "ACK" responses.
// It only considers nodes with sufficient energy (>45%) to be potentially active.
(Cooperative_List, Idle_List) ← TM.Discover_Network(Nodes_Deployed)

// **3. TM distributes initial tokens to all active nodes**
// This function generates and sends a unique token to each node.
TM.Distribute_Initial_Tokens(Cooperative_List)

// Return the key outputs of the setup process
Return TM, Cooperative_List, Idle_List

End Procedure

This section delineates the process of packet transmission within the network. As already mentioned in the Algorithm, 1 Token broker server initializes the creation of a Token manager. Then, under the guidance of the Token Manager (TM), multiple routing paths are discovered. Each routing path is identified by a unique Route ID, which comprises a combination of Token ID and Node ID. Above, figure 3 highlights the nodes with low energy levels that potentially generate unwanted traffic. Table 1 illustrates each routing ID is associated with its respective set of Token and Node IDs representing a detailed overview of the network's routing configurations. Algorithm 2 describes the process of addressing and gathering nodes' activities, facilitating packet transmission, collecting characteristics, and monitoring processes. Token Manager-based Node Authentication and Activity Monitoring is explained in algorithm 3

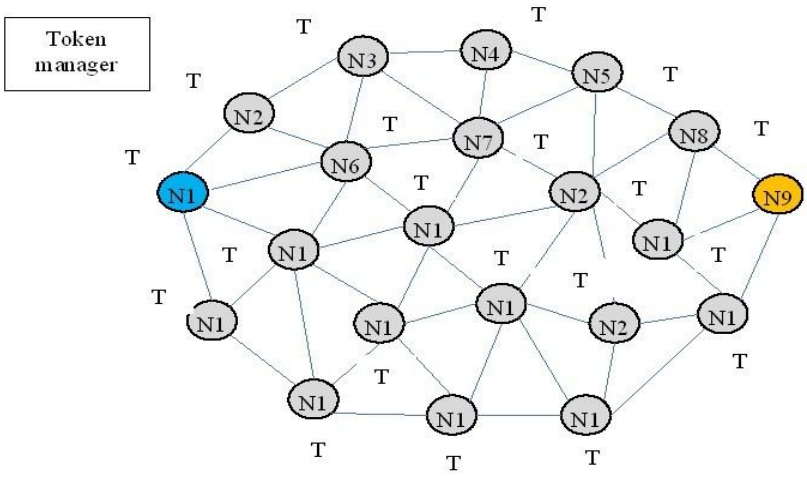

Figure 2: Network topology of the proposed TM-AD scheme

Figure 2 illustrates the network topology for the proposed scheme, showing a random deployment of sensor nodes (e.g., N1 through N21). According to this deployment, N1 acts as the source and N9 as the destination. The tokens T01 to T21 are issued parallelly. The message broadcasting mechanism determines each node's status, classifying them as either active or inactive, through the token distribution process. Following the broadcast of the "hello" message, the nodes that respond are “active nodes”, whereas those which doesn’t respond are “inactive nodes”. It’s important to note that an idle node has the potential to attain the active status; hence, TM maintains a continuous vigil, by ensuring all node information is monitored and updated accordingly. The execution operation is initiated by TM, which controls both cooperative and non-cooperative node list problems, thereby affirming the issuance of tokens to all active nodes as described in the algorithm.

Algorithm 2: Routing Maintenance by Token Broker

Input: Token Broker (TB), Set of available routes R = {R1, R2, ..., Rn} to D_node, Network size N. **Output:** Packet delivery, Misbehaving node handling**.**

Procedure

```
Maintain_Routing_And_Detect_Anomalies(TM, Available_Routes, Destination_Node)

    For each Route R in Available_Routes:

        // Phase 1: Monitor data transmission on the current route
        Transmission_Status ← TM.Monitor_Transmission_On_Route(R, Destination_Node)

        // Phase 2: Assess performance and take action if needed
        Switch (Transmission_Status):

            Case "SUCCESSFUL":
                // No action needed, move to the next route or finish
                Continue

            Case "ISSUES_DETECTED":

                // Phase 3: Identify the source of the problem
                Misbehaving_Node ← TM.Identify_Problem_Node_On_Route(R)

                If Misbehaving_Node is not null:

                    // Phase 4: Authenticate and handle the problematic node
                    Is_Authenticated ← TM.Authenticate_Node(Misbehaving_Node)

                    If Is_Authenticated:
                        TM.Action_On_Node(Misbehaving_Node, action="TEMPORARY_HOLD")

                    // Phase 5: Find a new route to complete the transmission
                    New_Route ← TM.Find_Alternative_Route(Destination_Node)
                    If New_Route is not null:

                        TM.Monitor_Transmission_On_Route(New_Route, Destination_Node)
                    End If
                End If
            End If

        End Switch
    End For

End Procedure
```

Algorithm 3: Token Manager-based Node Authentication and Activity Monitoring

Input: A specific Node (N_check), Token Manager (TM).
Output: Node participation eligibility, Registered Node/Token IDs, Monitored packet transmission status, Potential node holding.

Procedure Check_Single_Node(N_check, TM, Task)

// **Phase 1: Check node's eligibility to participate**
Is_Eligible ← (N_check.Energy > 0.50) AND Is_Position_Suitable(N_check.Distance)

If NOT Is_Eligible:
Return Failure("Node is not eligible for participation.")
End If

// **Phase 2: Verify node's identity and authorization**
Is_Verified ← TM.Verify_Node_Credentials(N_check.ID, N_check.Token)

If NOT Is_Verified:
Return Failure("Node verification failed.")
End If

// **Phase 3: Monitor the node's performance during a live task**

Performance_Outcome ← TM.Monitor_Node_During_Task(N_check, Task)

// Phase 4: Respond to performance issues

If Performance_Outcome is "GOOD":
Return Success("Monitoring cycle complete, node performed well.")
Else:
// Performance was poor (e.g., packet drops, energy drain)
TM.Action_On_Node(N_check, action="TEMPORARY_HOLD")

Alternative_Node ← TM.Find_Eligible_Alternative_Node()

If Alternative_Node is not null:
TM.Reassign_Task(Task, Alternative_Node)
Return Success("Task re-allocated to alternative node.")
Else:
Return Failure("No suitable alternative node found.")
End If
End If

End Procedure

This section delineates the process of packet transmission within the network. As already mentioned in the Algorithm, 1 Token broker server initializes the creation of a Token manager. Then, under the guidance of the Token Manager (TM), multiple routing paths are discovered. Each routing path is identified by a unique Route ID, which comprises a combination of Token ID and Node ID. Above, figure 3 highlights the nodes with low energy levels that potentially generate unwanted traffic.

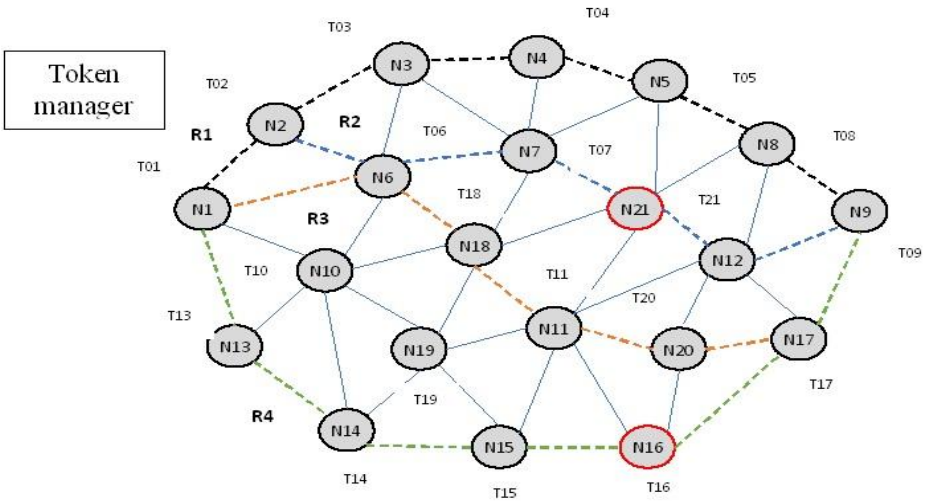

Figure 3: Illustration of multipath routing and anomaly detection

Table 1: Routing information and find misbehaving nodes

Routing ID	Token-ID	Node ID	Misbehaving nodes
R1	T01, T02, T03, T04, T05, T06, T07, T08, T09	N01, N02, N03, N04, N05, N06, N07, N08, N09	NIL
R2	T01, T02, T06, T07, T21, T12, T09	N01, N02, N06, N07, N21, N12, N09	N21
R3	T01, T06, T18, T11, T20, T17, T09	N01, N06, N18, N11, N20, N17, N09	NIL
R4	T01, T13, T14, T15, T16, T17, T09	N01, N13, N14, N15, N16, N17, N09	N16

Table 2: Token manager-based node authentication structure

Misbehaving node	Token-ID	Source -ID token	Destination ID token
N21	T21	TSID 12	TDID 21
N16	T16	TSID 61	TDID 16

This Figure 3 demonstrates the dynamic process of multipath routing and anomaly detection by the Token Manager (TM). It depicts four potential routes (R1, R2, R3, R4) from the source node (N1) to the destination (N9). The TM actively monitors traffic along these paths. Nodes circled in red **N21** on Route 2 (R2) and **N16** on Route. The packet processing begins with multipath routing in R1, that contains N01, N02, N03, N04, N05, N06, N07, N08, N09. The R2 includes nodes N01, N02, N06, N07, N21, N12, N09. TM in R2 detects unwanted traffic and checks the node's activity, identifying the misbehaving nodes N21. After finding this node, the node might be temporarily stopped or removed from the network. Moving to R3 comprises of N01, N06, N18, N11, N20, N17, N09. Finally, R4 includes nodes such as N01, N13, N14, N15, N16, N17, and N09 this route saw some normal traffic, prompting a check of node activity and ultimately identifies the node N16 as a misbehaving node and it temporarily holds from the network.

Once the misbehaving nodes are identified, the new source IDs and destination IDs are generated for these nodes to intimate a TM. Finally, the security scheme is improved by reinforcing the following algorithm's 3 steps. After finding the misbehaving node there is an enhancement in the new security scheme. Before the network communication the nodes' parameters such as $(N_d(medium), N_e(medium) threshold\ level\ (\geq 50\%)\ are\ assessed$. Only the nodes meeting this threshold are eligible to participate in the network, while others are excluded from the network. In the Second step, the fresh source IDs, destination IDs, and token iDs are registered by TM. After a registration packet transmission process commences and continues after a specified travel time, nodes' parameters, $N_d$and N_e, are re-evaluated only if they meet the threshold criteria. If this condition doesn't meet the requirement, then, the new nodes which satisfies the threshold criteria are addressed in the network, meanwhile, it temporarily eliminates the older and energy-depleted nodes. The same steps will be repeated and ultimately, calculating the packet delivery ratio, attack detection rate, and end-end delay. Table 1 shows the misbehaving nodes. Table 2 illustrates the structure for creating the source IDs and destination IDs after finding the misbehaving node.

4 Experimental results and discussions

The simulation environment emulates a dynamic network, with 100 nodes using the Random Way mobility model. The network occupies a 1700 x 1700 m2 space, allowing the nodes to roam freely within this area. Based on the simulation adheres to the IEEE specifications for the 802.11 Mac protocol, analyzing that the simulation's link-layer protocol is in accordance. To generate network traffic, a constant bit ratio multicast approach is employed. The experiment consists of both IEEE 802.11b and 802.11e WLAN heterogeneous traffic scenarios. Data connections are employed using either a TCP or UDP network topology, with the nodes exhibiting a mobility range between 10-35 m/s. The value of packet size is 512 bytes, and the data rate is 24 Mbps. The various simulation parameters utilized during the execution are explained elaborately in the provided Table 3.

Figure 4 compares attack detection rates (%) for TM-AD against BCBSL and I-CPDA, across networks of 20 to 100 nodes. TM-AD demonstrates robust performance, achieving 30% detection at 20 nodes and an impressive 100% at 100 nodes, consistently outperforming alternatives. This superior capability stems from the Token Manager's continuous, proactive monitoring of node behavior and attributes against established baselines, as detailed in its algorithms. The TM's centralized analysis of network-wide interactions allows for effective identification of deviations indicative of attacks. This vigilance, improving with network density, and TM-AD's ability to swiftly isolate threats, underpins its high attack detection efficacy across all scales

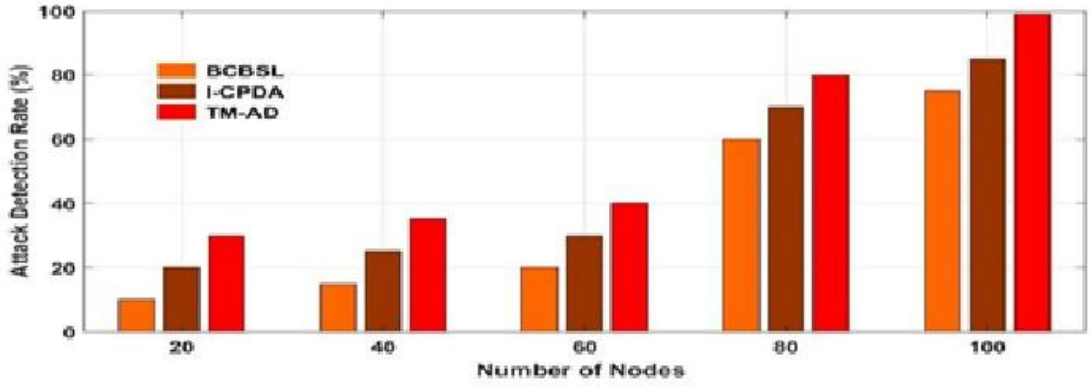

Figure 4: Number of nodes vs. Attack Detection rate

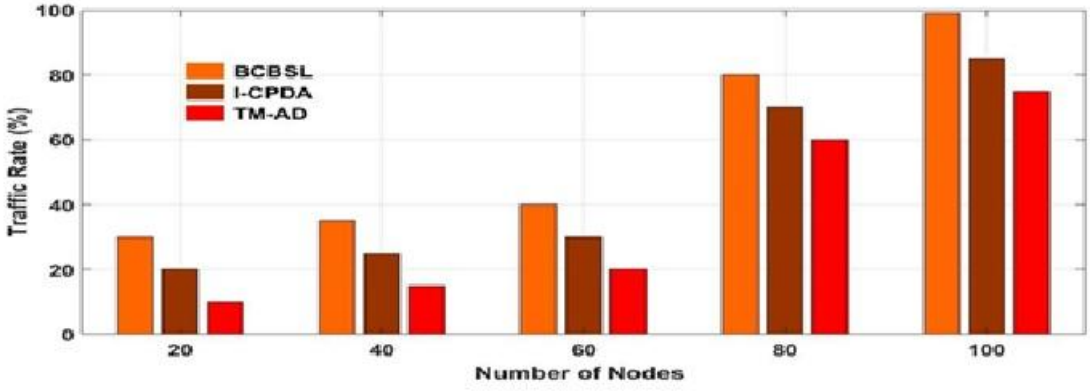

Figure 5: Number of nodes vs traffic rate

Table 3: Simulation parameters

Simulation Parameter	Value
Simulator	NS-2
Simulation time	315 s
Number of nodes	100
Simulation area	1700 × 1700 m2
Mac Protocol	IEEE 802.11
Data rate	24 Mbps
Radio range	110m
Mobility model	Random waypoint Model
Antenna	Omnidirectional antenna
Node speed	10-35 m/s
Packet size	512 bytes
Traffic type	Multicast constant bit Ratio

Figure 5 compares network traffic rates (%) for TM-AD against BCBSL and I-CPDA across networks of 20 to 100 nodes. TM-AD consistently exhibits lower traffic rates, demonstrating superior efficiency. This reduction is primarily due to TM-AD's efficient network management by the Token Manager, which minimizes routing overhead through targeted updates instead of network-wide broadcasts. Additionally, rapid detection and isolation of malicious nodes prevent them from generating disruptive or unnecessary traffic. By maintaining stable routes and reducing control packet volume, TM-AD ensures a leaner operational footprint, leading to lower overall network load and more efficient bandwidth utilization compared to alternatives. Figure 6 compares routing overhead (%) for TM-AD against BCBSL and I-CPDA in networks of 20 to 100 nodes. TM-AD consistently demonstrates lower overhead, from 20% (20 nodes) up to 55% (100 nodes), significantly outperforming alternatives.This reduction is chiefly due to TM-AD's centralized route management by the Token Manager. When routes need adjustment or malicious nodes are replaced, the TM facilitates targeted updates, minimizing network-wide control packet floods common in distributed protocols. Proactive monitoring further reduces route failures and associated re-establishment overhead, ensuring efficient bandwidth use for data rather than excessive control traffic, thus enhancing network efficiency.

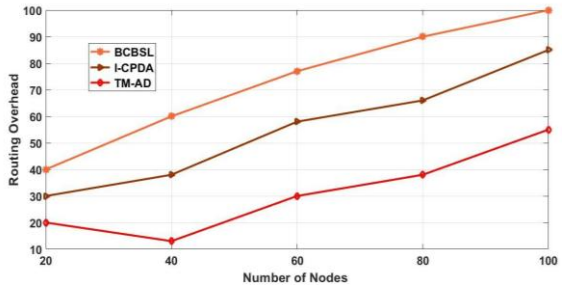

Figure 6: Number of nodes vs. routing overhead

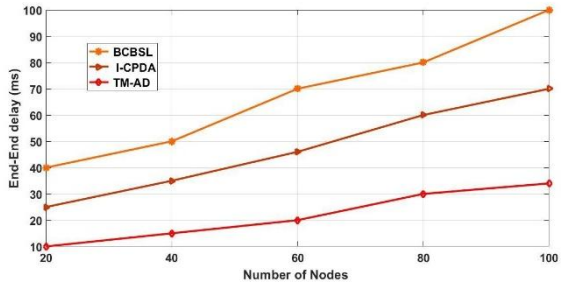

Figure 7: Number of nodes vs end- end delay

Figure 7 compares end-to-end delay (ms) for TM-AD against BCBSL and I-CPDA across networks of 20 to 100 nodes. TM-AD consistently exhibits minimal delay, ranging from 10ms (20 nodes) to 24ms (100 nodes), significantly outperforming alternatives. This reduced delay is attributed to TM-AD's rapid malicious node detection and replacement by the Token Manager, which minimizes packet time on compromised routes and reduces retransmissions. Furthermore, proactively maintained optimized routing paths ensure efficient data forwarding. TM-AD's capability to quickly restore stable routes and ensure efficient packet delivery underpins its superior end-to-end delay performance, demonstrating its effectiveness in time-sensitive WSN applications.

Figure 8 compares network throughput (%) for TM-AD against BCBSL and I-CPDA, with node counts from 20 to 100. TM-AD consistently outperforms others, achieving 30% throughput at 20 nodes and scaling to 100% at 100 nodes. This superior performance stems from TM-AD's efficient malicious node detection and rapid replacement, minimizing packet loss and route.
Furthermore, optimized routing paths. maintained by the Token Manager and lower routing overhead ensure bandwidth is prioritized for data transmission. TM-AD's proactive, centralized management leads to enhanced network stability and effective data delivery, underscoring its capability to maximize throughput across various network densities by maintaining network integrity and efficient routing.

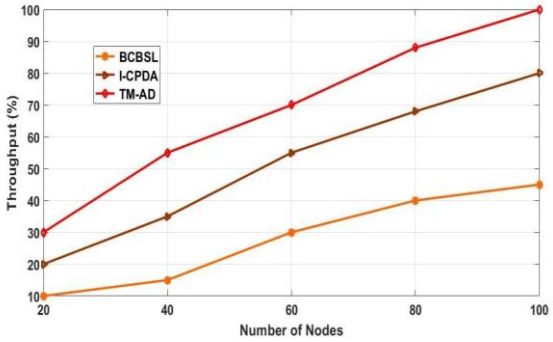

Figure 8: Number of nodes vs throughput

Table 4 Summarizes the performance of TM-AD against BCBSL and I-CPDA for a network of 100 nodes. As shown, TM-AD consistently outperforms both baseline schemes across all evaluated metrics, achieving 100% attack detection and network throughput, significantly lower delay such as 24% and 55% routing overhead.

Table 4: Comparison of performance metrics at 100 nodes

Metric	TM-AD	BCBSL [ref]	I-CPDA [ref]
Attack Detection Rate (%)	100	~82-85	~90
Network Throughput (%)	100	~50	~85
End-to-End Delay (ms)	24	~95	~70
Routing Overhead (%)	55	~98	~82
Traffic Rate (Overall Load) (%)	76	~81	~98

Table 5: Computation cost comparison

Scheme	Component	Key Operations Involved	Estimated Cost (Unit/Scale)
TM-AD	Sensor Node	Token validation, status reporting	Low
TM-AD	Token Manager	Anomaly detection, routing updates, token mgmt.	Medium (centralized load)
BCBSL	Sensor Node	Hashing, consensus participation, ledger interaction	High
I-CPDA	Sensor Node	Data slicing, encryption, intra-cluster communication	Medium
I-CPDA	Cluster Head	Data fusion, aggregation logic	Medium

Table 6: Estimated energy consumption comparison

Scheme	Component	Primary Energy Consumers	Estimated Energy (Unit/Scale)
TM-AD	Sensor Node	Radio (Tx/Rx for TM comms, data), low computation	Low-Medium
TM-AD	Token Manager	Radio (high comms), computation	Medium-High (if node-based)
BCBSL	Sensor Node	Radio (Tx/Rx for consensus, ledger), high computation	High
I-CPDA	Sensor Node	Radio (intra-cluster, data), medium computation	Medium
I-CPDA	Cluster Head	Radio (inter-cluster, sink), medium computation	Medium

Table 5 provides a comparative overview of the estimated computational costs associated with TM-AD and the baseline schemes. TM-AD is designed to minimize computational load on individual sensor nodes by centralizing complex tasks like anomaly detection and routing management at the Token Manager. This contrasts sharply with blockchain-based approaches like BCBSL, which typically impose significant cryptographic and consensus-related computational burdens on all participating nodes. While I-CPDA involves operations like encryption and data fusion, these are often localized within clusters. The primary computational load in TM-AD is on the TM, which is a design trade-off for simplifying sensor node operations. The estimated energy consumption, outlined in Table 6, reflects the computational and communication demands. TM-AD aims for lower energy expenditure on sensor nodes by offloading intensive processing to the Token Manager. Communication between sensor nodes and the TM constitutes the main energy cost for nodes in TM-AD. In contrast, BCBSL's distributed consensus and cryptographic operations lead to higher energy drain across all nodes. I-CPDA's energy profile is tied to its clustering and data aggregation tasks.

5 Conclusion

This paper introduced the Token Manager-based Attack Detection (TM-AD) scheme to address critical security and efficiency challenges in Wireless Sensor Networks (WSNs), leveraging a centralized Token Manager for proactive monitoring, efficient multipath routing, anomaly detection, and rapid malicious node replacement. Comparative evaluations demonstrated TM-AD's superior performance, achieving high attack detection rates and network throughput while significantly reducing end-to-end delay and routing overhead against benchmarks, highlighting its efficacy in maintaining network integrity through token-based management.

However, TM-AD faces limitations, including the Token Manager's potential as a single point of failure and scalability bottleneck, the paramount importance of TM security, and the need for further study on its resilience against highly sophisticated attacks and its own resource demands. Future work will target these by exploring distributed/hierarchical TM architectures, advanced machine learning for detection, integrating lightweight biometric authentication for secure node-to-TM communication within TM-AD, and investigating TM component deployment on edge computing nodes, aiming to establish TM-AD as a more robust, adaptive, and scalable WSN security solution.

Acknowledgement

The authors would like to express their sincere gratitude to the Department of Computer Applications, National Institute of Technology Tiruchirappalli, for providing the necessary facilities and research support throughout this work. The authors also thank their colleagues and reviewers for their valuable feedback, which helped improve the quality and clarity of this paper.

References

[1] Aldosari, S.S. and L.S. Aldawsari, PQ-LEACH: A novel post-quantum protocol for securing WSNs communication. International Journal of Engineering Business Management, 2024. 16: p. 18479790241301163. https://doi.org/10.1177/18479790241301163

[2] Temene N, Sergiou C, Georgiou C, Vassiliou V. A survey on mobility in wireless sensor networks. *Ad Hoc Networks.* 2022; 125:102726. doi: 10.1016/j.adhoc.2021.102726

[3] Zarpelão BB, Miani RS, Kawakani CT, de Alvarenga SC. A survey of intrusion detection in Internet of Things. J Netw Comput Appl. 2017; 84:25–37. doi: 10.1016/j.jnca.2017.02.009

[4] Shiraly D, Pakniat N, Noroozi M, Eslami Z. Pairing-free certificateless authenticated encryption with keyword search. J Syst Archit. 2022; 124:102390. doi: 10.1016/j.sysarc.2021.102390

[5] Tomić I, McCann JA. A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet Things J.* 2017;4(6):1910–1923. doi:10.1109/JIOT.2017.2749883

[6] Sethi P, Sarangi SR. Internet of things: architectures, protocols, and applications. J Electr Comput Eng. 2017; 2017:9324035. doi:10.1155/2017/9324035

[7] Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications.

IEEE Commun Surv Tutor. 2015;17(4):2347–2376. doi:10.1109/COMST.2015.2444095

[8] Shamir A. Identity-based cryptosystems and signature schemes. In: Chaum D, Blakley GR, editors. *Advances in Cryptology – CRYPTO 84* (Lecture Notes in Computer Science, vol. 196). Springer; 1985. p. 47–53. doi:10.1007/3-540-39568-7_5

[9] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: *Advances in Cryptology – ASIACRYPT 2003*, Lecture Notes in Computer Science; 2003. p. 452-473. doi:10.1007/978-3-540-40061-5_29

[10] Challa S, Wazid M, Das AK, Kumar N, Reddy AG, Yoon EJ, Yoo KY. Secure signature-based authenticated key establishment scheme for future IoT applications. *IEEE Access.* 2017; 5:3028–3043. doi:10.1109/ACCESS.2017.2684620

[11] Haque A, Chowdhury MN-U-R, Soliman H, Hossen MS, Fatima T, Ahmed I. Wireless sensor networks anomaly detection using machine learning: a survey. *arXiv* [Preprint]. 2023. arXiv:2303.08823.

[12] Kumar R, Kumar P, Tripathi R, Gupta G, Neeraj K, Hassan MM. A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system. *IEEE Trans Intell Transp Syst.* 2022;23(9):16492–16503. doi:10.1109/TITS.2021.3098636

[13] Mahdavisharif M, Jamali S, Fotohi R. Big data-aware intrusion detection system in communication networks: a deep learning approach. *J Grid Comput.* 2021;19(4):46. doi:10.1007/s10723-021-09581-z

[14] Feng L, Liu B. Low-energy data fusion privacy protection algorithm for three-dimensional wireless sensor network. *Mob Inf Syst.* 2022; 2022:3580607. doi:10.1155/2022/3580607.

[15] Ciuonzo D, Rossi PS, Varshney PK. Distributed detection in wireless sensor networks under multiplicative fading via generalized score tests. *IEEE Internet Things J.* 2021;8(11):9059–9071. doi:10.1109/JIOT.2021.3056325

[16] Nasurulla I, Kaniezhil R. Integration of fault-tolerant feature to OMIEEPB routing protocol in wireless sensor network. *Int J Intell Comput Cybern.* 2022;15(3):414–424. doi:10.1108/IJICC-09-2021-0189

[17] Lakshmi V, Deepthi P. A secure channel code-based scheme for privacy preserving data aggregation in wireless sensor networks. *Int J Commun Syst.* 2019;32(1):e3832. doi:10.1002/dac.3832

[18] Zhang X, Zhao L, Gao X, Zhang X. A data-sharing model based on blockchain for power grid big data. *J Phys.: Conf. Ser.* 2021;1792(1):012051. doi:10.1088/1742-6596/1792/1/012051

[19] Jiang S, Li M, Tang Z. A new scheme for source-location privacy in wireless sensor networks. *Int J Netw Secur.* 2018;20(5):879–889. doi:10.6633/IJNS.201809_20(5).09

[20] Alam MK, Abd Aziz A, Abd Latif S, Abd Aziz A. Error-control truncated SVD technique for in-network data compression in wireless sensor networks. *IEEE Access.* 2021; 9:13829–13844. doi:10.1109/ACCESS.2021.3051978

[21] Giri P, Ng K, Phillips W. Wireless sensor network system for landslide monitoring and warning. *IEEE Trans Instrum Meas.* 2019;68(4):1210–1220. doi:10.1109/TIM.2018.2888295

[22] Kim T-H, Goyat R, Rai MK, Kumar G, Buchanan WJ, Saha R, Thomas R. A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks. *IEEE Access.* 2019;7:184133–184144. doi:10.1109/ACCESS.2019.2960609

[23] Abubaker Z, Javaid N, Almogren A, Akbar M, Zuair M, Ben-Othman J. Blockchained service provisioning and malicious node detection via federated learning in scalable Internet of Sensor Things networks. *Comput Netw.* 2022; 204:108691. doi: 10.1016/j.comnet.2021.108691

[24] Chen CM, Deng X, Gan W, Chen J, Islam SK. A secure blockchain-based group key agreement protocol for IoT. *J Supercomput.* 2021; 77:9046–9068. doi:10.1007/s11227-020-03561-y

[25] Gebremariam GG, Panda J, Indu S. Blockchain-Based Secure Localization against Malicious Nodes in IoT-Based Wireless Sensor Networks Using Federated Learning. *Wireless Commun Mobile Comput.*2023:8068038. doi:10.1155/2023/8068038

[26] Cheng P, Zhu M. Lightweight anomaly detection for wireless sensor networks. *Int J Distrib Sens Netw.* 2015;11(8) doi:10.1155/2015/653232

[27] Shi L, Li K, Zhu H. Data fusion and processing technology of wireless sensor network for privacy protection. *J Appl Math.* 2023;2023:1046050. doi:10.1155/2023/1046050.

[28] M. B. Begum, J. Eindhumathy, J. S. Priya, M. Padmaa, N. R. Nagarajan and S. J. M. Suhail, Reconfigurable Architecture Application Using Machine Learning in Edge Computing for IoT Devices,*2024 Eighth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Waknaghat, Solan, India, 2024, pp. 755-760, doi: 10.1109/PDGC64653.2024.10984266

[29] Baritha Begum M. Real-time security in sensor networks in sequential approach with BWT compression, Huffman coding, and reduced array encryption. *J Syst Sci Syst Eng.* 2025;1–45. doi:10.1007/s11518-025-5661-0

[30] Baritha Begum M, Muhamed Suhail SJM, Priya JS, Eindhumathy J, Sivakannu G, Kesavan A. Innovative IoT solutions for vehicle maintenance and tracking. In: *Proc. 2024 International Conference on Big Data Analytics in Bioinformatics (DABCon 2024), Kolkata, India.* 2024: pp. 1–6. doi:10.1109/DABCon63472.2024.10919361

[31] Baritha Begum M, Suganthi B, Sivagamasundhari P, Arunmozhi SA, Muhamed Suhail SJM. An enhanced heterogeneous local directed acyclic graph

blockchain with recalling enhanced recurrent neural networks for routing in secure MANET-IoT environments in 6G. *Int J Commun Syst.* 2025;38(4). doi:10.1002/dac.6110

[32] Aravinth RB, Victor P, Arokiasamy A. Energy aware routing in wireless sensor network-based healthcare systems using optimized CGRNN. *IETE J Res.* 2025. doi:10.1080/03772063.2025.2531956

[33] Venkatasubramanian S, Raja S, Sumanth V, Dwivedi JN, Sathiaparkavi J, Modak S, Kejela ML. Fault diagnosis using data fusion with ensemble deep learning technique in IIoT. *Math Probl Eng.* 2022; 2022:1682874. doi:10.1155/2022/1682874

[34] Manojkumar V, Sastry VN, Srinivasulu Reddy U. Security, privacy challenges, and solutions for various applications in blockchain distributed ledger for wireless-based communication networks. In: *AI and Blockchain Technology in 6G Wireless Network*. Cham: Springer; 2022. p. 117–135. https://content.e-bookshelf.de/media/reading/L-18559651-cb1000bf31.pdf