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

J Sangeethapriya[1,2 *], Michael Arock[1], U Srinivasulu Reddy[1]
[1]Department of Computer Applications, National Institute of Technology, Trichirappalli-620015, Tamil Nadu, India
[2]Department of Information Technology, Saranathan College of Engineering, Trichirappalli-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 numerous Internet of Things (IoT) applications, but their inherent resource limitations and distributed nature expose them to significant security vulnerabilities. A main 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 methods 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 immense development, hence gaining a much interest both in the academic and industrial domains. A WSN is a self-organized multi-hop network consisting of many sensor nodes which have the following attributes, such as flexibility, fault tolerance, high sensing capabilities, and rapid deployment. These features have led to extensive 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 WSN, every 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 flaws. Wireless communication channels are susceptible to eavesdropping and alteration of data [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 [11], deep learning etc. Kumar et al. [12] 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. [13,29] 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 [14] 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 [15].

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 [18], 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 [17] 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]. The researchers [20] presented a sophisticated approach to overcome security attacks and minimise the unnecessary use of energy in wireless sensor network (WSN) applications, especially those that involve military surveillance and environmental studies. It provides a precise sensor placement. This scheme seems to increase privacy, although at the same time, it improves energy use and latency of information compared to traditional deployment models [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 [23,35], 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. [23,33] combined blockchain and federated learning (FL) for IoT sensor network security. While advanced, FL and blockchain [33] 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 [24,34,25] 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 [28] 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 environments [25] 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. [25] 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 [26] presented a lightweight anomaly detection scheme. Howeverinvolve the integrated routing maintenance and node replacement capabilities that TM-AD would provide. Shi et al. [27] introduced I-CPDA, a data aggregation enhancement of privacy in WSNs, in clusters. Though useful in terms of intra cluster data fusion [33], it mostly focuses on protecting some data, but the detection of minor, network-based malfunctions like routing attacks. TMAD offers a more extensive network-level approach, in that it will monitor the overall node behaviour, and it actively controls routing paths.

2.1 Problem statement

The privacy concerns come about when IoT devices transmit sensitive data through a network channel.

- Current solutions are easily compromised on security and in most cases, they do not offer proper security.
- No records have been made to reflect the intrusion or interference of network transmissions by malicious nodes.
- There is no laid-down procedure in case of a breakdown in transmission on how to deploy an alternative or replace compromised nodes.
- The previous approaches are not reliable to ensure an effective communication with the high Packet Delivery Ratio (PDR), the adequate throughput, and the long working life.

2.2 Research contribution

The proposed work, Token Manager construct is called Token-Based Server Anomaly Detection (TM-AD).

- This paper introduces a detailed discussion of the given technique, which combines the security analysis and experimental outcomes, and, thus, proves its better effectiveness compared with the current methods.
- The routing paths are also strengthened by substituting the affected nodes to ensure a reliable transmission and hence confirming the successful delivery of data.
- The article concentrates on the comparative analysis of the proposed approach, in particular, a variety of efficiency indices is considered.

3 Proposed methodology

The scheme of Anomaly Detection (TM-AD) based on the use of Tokens has been developed to achieve efficient multipath routing, detect unusual node behaviour and react proactively to maintain network integrity within the Wireless Sensor Networks (WSNs). Figure 1 depicts that TM-AD architecture is focusing on a Token Manager (TM) which is a centralized, logically and physically core unit, which is backed by a set of important interacting components.

- **Sensor Nodes:** These are the basic components of the WSN and they are put in place in order to gather environment information and to transmit packets. In TM -AD, they are mainly used to collect data, forward via the TM -established routes and report the necessary status data to the TM. Membership in the network is dictated by tokens.

- **Token Manager (TM):** This fundamental component, which is normally a node that has been chosen based on its greater resources (e.g. energy, bandwidth), serves as the coordinator of the network. The fundamental responsibilities of it are to discover nodes, keep track of their status (e.g., energy, location, activity), issue and manage tokens, compute and maintain optimal routing paths by maintaining a routing table, identify behavioural anomalies or malicious behaviour, and take remedial actions, e.g. isolating or replacing nodes.

- **Tokens:** These are logical objects or messages that are only controlled and transmitted to TM. Sensors are represented by tokens as dynamic permissions to participate in the network, indicating authorization to be actively involved in the network, or to authenticate their current operational status or to designate them to particular routing operations. A token can be flexible to reflect the current network demands.

- **Cooperative Node List:** This is a dynamic registry maintained by the TM, which contains sensor nodes that are currently known to be active and reliable members of network activities, particularly in routing and relaying data. The TM is based on this list when it comes to processing of packet transmission and targeted monitoring.

- **Replacement Nodes:** These are either pre-allocated or dynamically existing sensor nodes that are meant to take the place of identified nodes reported by TM to be permanently malicious or failed. The TM organizes their integration to provide network resilience.

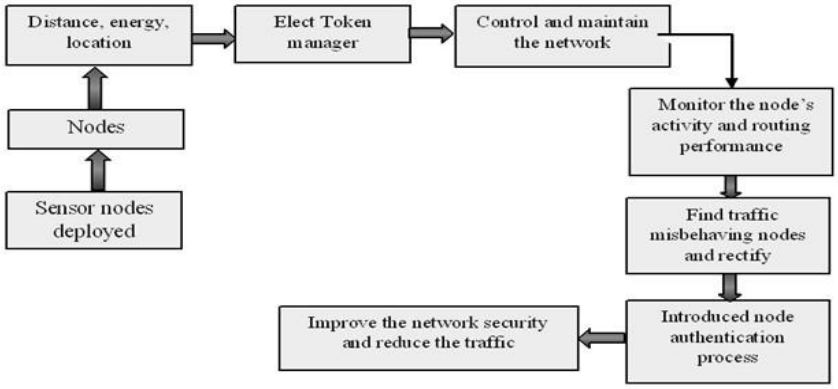

Figure 1: Proposed architecture-token manager-based anomaly detection (TM-AD) system

The components and their interactions are visually described in Figure 1 and point to the TM as the key element of coordination. The following algorithms will outline the operational stages of TM -AD and methods by which these component interactions operate.

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. Select the most worthiest 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

In this section, the sequence of transmitting packets in the network is outlined. A Token Manager is created by a Token broker server, as indicated by Algorithm 1. After that, there are various routing paths which are found under the guidance of the TM. Every routing path is also denoted by a distinct Route ID, which is a concatenation of Token ID and Node ID. Figure 3 points out nodes with low power displays which may pose as sources of unwanted traffic. Table 1 matches the routing IDs with the sets of respective Token and Node IDs and provides an in-depth view of the routing configurations of the network. The algorithm 2 explains how the activities of the nodes are addressed and collected, the transmission of packets facilitated, the harvesting of characteristics as well as the monitoring processes. Algorithm 3 outlines token-based authentications of node and activity monitoring.

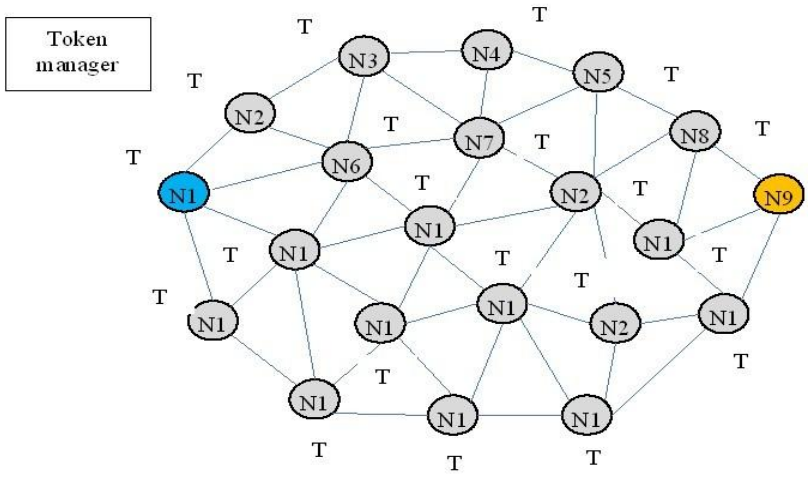

Figure 2: Network topology of the proposed TM-AD scheme

Figure 2 illustrates the network topology for the proposed scheme, showing a random deployment of sensor nodes (e.g., N1 through N21). Here, N1 is the source and N9 the destination. Tokens T01-T21 are issued simultaneously. The status of each node is decided by the message broadcasting mechanism which classifies nodes either as active or inactive considering the distribution of tokens. The nodes responding to the broadcasting of a message containing the word hello are considered as active nodes and the ones that fail to respond are considered as inactive nodes. A dormant node can be activated; therefore, the TM is constantly on alert which makes sure that all the information about the nodes are under observation and updated accordingly. The execution is initiated with the TM which controls the cooperative and non-cooperative node list problems, hence ensuring that tokens are issued to all the active nodes as indicated 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 suitable 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 failed to authenticate")
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 completed, node performance is good.")
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

In this section, the transmission of packets in the network is demarcated. A Token Manager is created by a Token broker server as indicated in Algorithm 1. After this, a sequence of routing paths is found under the supervision of the Token Manager (TM). The routing paths have unique Identifiers called Route ID, which is a combination of Token ID and Node ID. Figure 3 points out nodes that have low energy levels and which could contribute to unwanted traffic.

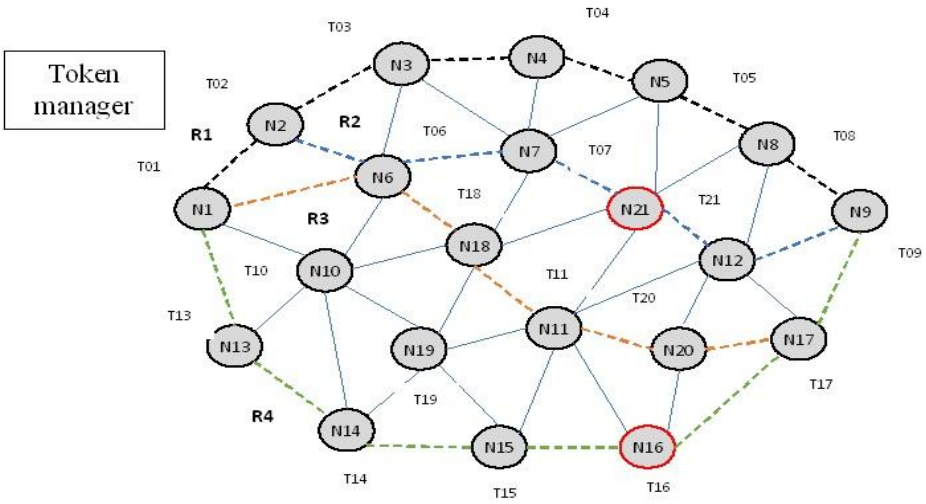

Figure 3: Illustration of multipath routing and anomaly detection

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

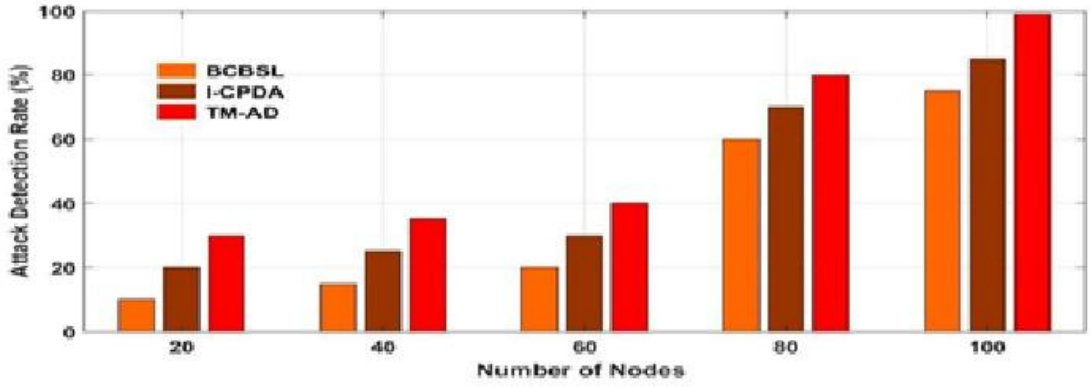

Figure 4: Number of nodes vs. Attack Detection rate

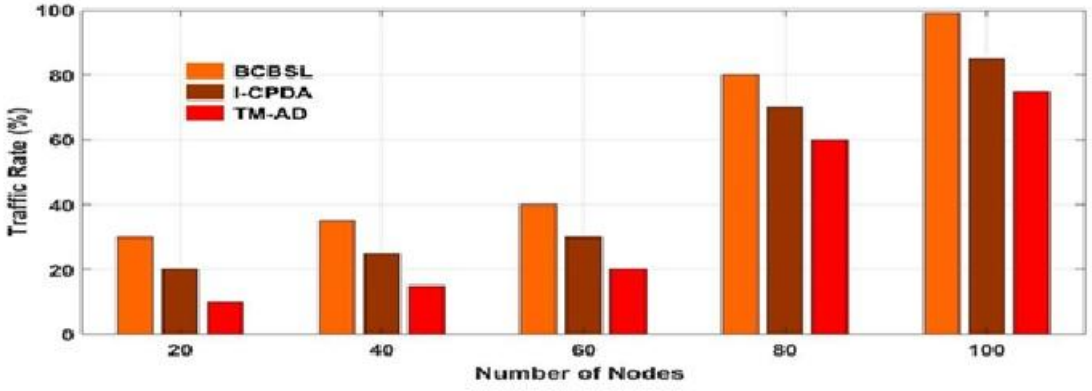

Figure 5: Number of nodes vs traffic rate

Table 3: Simulation parameters

Simulation Parameter	Value
Simulator	NS-2
Simulation time	315 s
Number of nodes	100
Simulation area	1700 × 1700 m^2
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 is a comparison of network traffic rates (percentage) of TM-AD and BCBSL and I-CPDA over a 20 to 100 node network. TM-AD has always shown less traffic rates and this proves to be more efficient. This is mainly due to the fact that the Token Manager at TM-AD has created an efficient network control that reduces the routing overhead as it does not involve a network-wide route change, but instead selectively changes the routes. Additionally, malicious nodes cannot produce disruptive and unwarranted traffic since they can be identified and segregated quickly. TM-AD offers a leaner operational footprint by stabilizing the routes and the volume of control packets resulting in a lower total network load and efficient utilization of bandwidth over other schemes. Figure 6 is a comparison of routing overhead (%) of TM-AD with BCBSL and I-CPDA networks of 20-100 nodes. TM -AD always has lower overhead with 20 to 55 as the range (20 nodes to 100 nodes) being significantly less than its alternatives. This decrease mainly comes as a consequence of the centralized route management of the Token Manager of TM-AD. Routes need to be updated when they need modification and the TM allows specific routes to be updated, thus avoiding floods of control packets on the network that dominate traditional distributed protocols. Proactive monitoring also minimizes route failures and the overhead of reestablishment, which is used effectively to transmit data

instead of unnecessary traffic control, and hence the efficiency of the entire network.

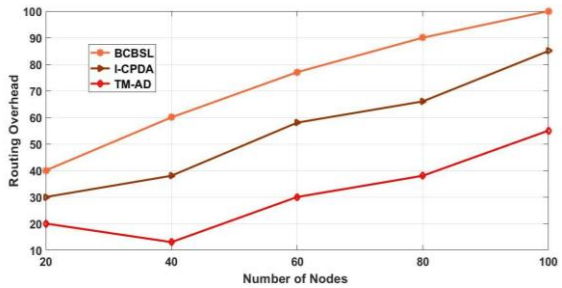

Figure 6: Number of nodes vs. routing overhead

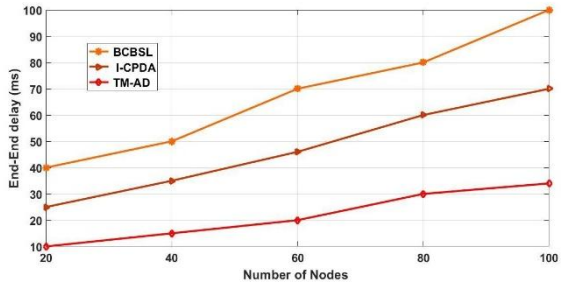

Figure 7: Number of nodes vs end- end delay

In figure 7, the end-to-end delay (ms) of TM-AD is compared to that of BCBSL and I-CPDA in 20-100 node networks. TM-AD has low delay which goes between 10ms (20 nodes) and 24ms (100 nodes) which is extremely low compared to other alternatives. This is less delay caused by the speed at which TM-AD can detect and replace malicious nodes with the Token Manager which will reduce the time that packets spend on bad routes and minimizes the retransmit. Also, optimized routing paths are in place in time to provide efficient data forwarding. This has made TM-AD superior in terms of end-to-end delay performance due to its fast recovery of routes and this is because of its efficiency in packet delivery, and this makes it useful in time sensitive applications with WSNs.

Figure 8 compares network throughput (percentage) between TM-AD and BCBSL and I-CPDA when the number of nodes is between 20 and 100. TM-AD has been shown to be superior to other schemes with 30% throughput at 20 nodes and increasing to 100% throughput at 100 nodes. This is the best performance based on the fact that TM-AD has been able to effectively detect malicious nodes and replace them quickly thus reducing the packets loss and interruption of routes. In addition, the routing paths which are being optimized through the Token Manager and reduction of routing overhead also guarantee that the data transmission is given priority to bandwidth. The Management of TM-AD is proactive, centralized and results in a more stable network, efficient delivery of the data and hence highlights its ability to maximize the throughput of the network through network integrity and efficient routing.

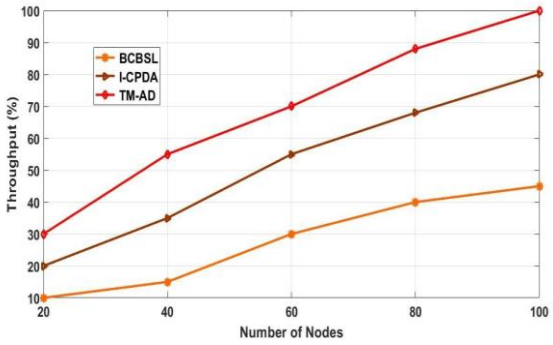

Figure 8: Number of nodes vs throughput

A summary of the performance of TM-AD as compared to BCBSL and I-CPDA in a network of 100 nodes has been shown in table 4. As depicted, TM-AD is always a better scheme compared to its baseline schemes in all the metrics that have been assessed in terms of 100 percent attack detection and network throughput, a much lower delay of 24 percent and 55 percent routing overhead.

Table 4: Comparison of performance metrics at 100 nodes

Metric	TM-AD	BCBSL [25]	I-CPDA [27]
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 cost of computation of TM-AD and the baseline schemes. The topology of TM-AD is such that elaborate calculations on each sensor node can be reduced as all the difficult activities like anomaly detection and routing are centralized at the Token Manager. This is distinctly opposed to the blockchain-based use of solutions such as BCDSL, that subjects all participating nodes to significant cryptographic as well as consensus-related computational demands. Whereas I-CPDA makes use of cryptography and the integration of data, which is usually localized within clusters, the most computing workload in TM-AD is held on the Token Manager, which constitutes a design trade off because it allows sensor node functions to be simplified. Such computational and communication requirements can be detected in the estimated energy consumption, which is presented in Table 6. TM-AD aims at reducing the energy spent by sensor nodes on intensive processing which is offloaded to the Token Manager. The primary energy expenditure by sensor nodes in TM -AD is communication between sensor nodes and the Token Manager. On the contrary, the distributed consensus and cryptographic functions of BCBSL result in an energy drainage on all nodes, compared to the energy profile of I-CPDA which is associated with clustering and aggregating its data. A key consideration for TM-AD is the energy provisioning for the Token Manager, which could be a more powerful node or have access to a more stable power source to sustain its operations.

5 Conclusion

This paper proposed the Anomaly Detection (TM-AD) scheme based on the Token Manager in response to the serious security and efficiency concerns within the Wireless Sensor Networks (WSNs). TM-AD enables proactive monitoring, efficient multipath routing, anomaly detection using a centralized Token Manager and fast replacement of malicious nodes. Comparative experimentation has shown that TM-AD is better than benchmark methods in terms of higher attack-detection rates, network throughput and significant lowering of end to end latency and routing overhead thus highlighting its usefulness in maintaining network integrity through token-based management. However, TM-AD has a number of limitations. The single point of failure and scalability bottleneck in the system might be the central Token Manager itself; the security of the Token Manager itself is paramount; and more research is needed into the

aspect of the resilience to more advanced attacks and the resource requirements placed on the network by it. Future research objectives will thus be to build distributed or hierarchical Token Manager designs, to combine with more advanced machine-learning detection methods, and to consider implementing lightweight biometric authentication to authenticate node-to-Token Manager interactions, and to consider the implementation of Token Manager modules on edge-computers such that the overall objective will be to make TM-AD a stronger, more flexible, and more scalable security solution to WSNs.

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

[35] Nguyen, D. T., Trinh, M. L., Nguyen, M. T., Vu, T. C., Nguyen, T. V., Dinh, L. Q., & Nguyen, M. D. (2025). Security Issues in IoT-Based Wireless Sensor Networks: Classifications and Solutions. *Future Internet*, *17*(8), 350. https://doi.org/10.3390/fi17080350