Article

Enhancing IoT-LLN Security with IbiboRPLChain Solution: A Blockchain-Based Authentication Method

Joshua T. Ibibo *, Josiah E. Balota, Tariq F. M. Alwadan, Olugbenga O. Akinade

Posted Date: 2 September 2025

doi: 10.20944/preprints202509.0130.v1

Keywords: IoT-LLN; RPL; security; blockchain; authentication; insider attacks

Article

Enhancing IoT-LLN Security with IbiboRPLChain Solution: A Blockchain-Based Authentication Method

Joshua T. Ibibo*, Josiah E. Balota, Tariq F. M. Alwadan and Olugbenga O. Akinade

Teesside University

* Correspondence: j.ibibo@tees.ac.uk; Tel.: +4407377083132

Abstract

The security of Internet of Things (IoT)-Low Power and Lossy Networks (LLNs) is crucial for their widespread adoption in various applications. The standard routing protocol for IoT-LLNs, IPv6 Routing Protocol over Low Power and Lossy Networks (RPL), is susceptible to insider attacks, such as the version number attack (VNA), decreased rank attack (DRA), and increased rank attack (IRA). These attacks can significantly impact network performance and resource consumption. To address these security concerns, we propose IbiboRPLChain Solution, a secure blockchain-based authentication method for RPL nodes. The proposed solution introduces an additional blockchain layer to the RPL architecture, enabling secure authentication of communication links between the routing layer and the sensors layer. IbiboRPLChain Solution utilises smart contracts to trigger immediate authentication upon detecting routing attacks initiated by malicious nodes in an IoT-LLN environment. The evaluation of the proposed solution demonstrates its superior performance in mitigating insider attacks and enhancing IoT-LLN security compared to existing methods. The proposed solution effectively mitigates insider attacks by employing blockchain technology to authenticate communication links between routing and sensor nodes. This prevents malicious nodes from manipulating routing information and disrupting network operations. Additionally, the solution enhances IoT-LLN security by utilising smart contracts to trigger immediate authentication upon detecting suspicious activity, ensuring prompt action against potential threats. The findings of this research have significant implications for the development and deployment of secure IoT-LLNs.

Keywords: IoT-LLN; RPL; security; blockchain; authentication; insider attacks

1. Introduction

The Internet of Things (IoT) has revolutionised the way we interact with the world around us [1,2]. It has enabled the connection of billions of devices, from smartphones and wearables to industrial sensors and appliances. This vast network of interconnected devices generates a massive amount of data that can be used to improve our lives in countless ways [3,4].

However, the widespread adoption of IoT devices has also introduced new security challenges. One of the most significant challenges is securing the routing of data in IoT networks. Routing attacks, such as the VNA, DRA, and IRA, can disrupt the flow of data and compromise the security of IoT systems [5,6].

To address these challenges, researchers have proposed various security solutions, including blockchain-based authentication methods [6–14]. Blockchain technology offers a number of potential benefits for IoT security, including its decentralised nature, immutability, and transparency. In this paper, we propose a secure blockchain-based authentication method for the routing protocol of nodes in RPL (IPv6 Routing Protocol over Low Power and Lossy Networks). Our proposed method utilises smart contracts to trigger immediate authentication upon detecting routing attacks initiated by adversarial nodes in an IoT-LLN (Low Power and Lossy Network) environment. Several research papers have explored the use of blockchain technology to secure IoT routing protocols [6–14]. However, most of these studies have focused on theoretical concepts and simulations. There is a lack of empirical research that evaluates the performance of blockchain-based authentication methods in real-world IoT deployments.

Our research specifically focuses on developing a secure blockchain-based authentication method for RPL. RPL is a standard routing protocol for IoT-LLNs, and it is widely used in various IoT applications. However, RPL is also susceptible to routing attacks, such as VNA, DRA, and IRA. Our proposed method aims to address these vulnerabilities by utilising smart contracts to authenticate communication links between routing nodes. Smart contracts are self-executing contracts that are stored on the blockchain. They can be used to enforce specific rules and conditions, such as verifying the authenticity of node identities and ensuring that routing messages are not tampered with. Existing authentication methods for IoT-LLNs often suffer from scalability and security limitations [7–10]. Blockchain technology offers a promising solution to address these challenges by providing a decentralised, tamper-proof, and transparent authentication mechanism. Our proposed blockchain-based authentication method utilises smart contracts to enforce secure communication links between routing nodes. Smart contracts are self-executing contracts stored on the blockchain, enabling automated verification of node identities and routing messages. This approach effectively mitigates routing attacks such as VNAs, DRAs, and IRAs by ensuring the authenticity and integrity of routing information.

The effectiveness of our proposed method is demonstrated through simulations that show significant reductions in routing attack success rates compared to existing methods [12–14]. The results highlight the potential of blockchain technology to revolutionise IoT security by providing a robust and scalable solution to mitigate routing attacks and safeguard IoT-LLN operations.

1.1. Contributions

Our research makes the following contributions to the field of IoT security:

i. A novel blockchain-based authentication method for RPL.

ii. A thorough evaluation of our proposed method using simulations.

iii. We demonstrate that the proposed method can effectively mitigate routing attacks in IoT-LLNs.

iv. Blockchain's inherent immutability and transparency safeguard routing information from tampering and manipulation, preventing malicious nodes from disrupting network operations.

v. Smart contracts automate the authentication process, reducing the overhead associated with manual verification and expediting the response to potential threats.

vi. Blockchain's distributed architecture can accommodate a growing number of nodes without compromising performance, making it suitable for large-scale IoT-LLNs.

The rest of this paper is organised as follows. In section 2, we discussed the related studies, and in section 3, we focused on the background on blockchain technology and RPL. In section 4, we discussed proposed blockchain-based authentication methods. Section 5 presents our proposed routing protocol. In section 6, we compare the performances with existing solutions. Section 7, the main conclusion

1.2. Problem Statement

The widespread adoption of IoT devices has introduced new security challenges, particularly in the context of LLNs. LLNs, which form the backbone of many IoT applications, are often composed of resource-constrained devices with limited energy and computational capabilities. This inherent constraint makes LLNs particularly susceptible to routing attacks [10–15], which can disrupt network operations and compromise the security of IoT systems.

Traditional security solutions for LLNs are often impractical due to their complexity and overhead. The implementation of sophisticated security measures can be resource-intensive and may not be feasible for resource-constrained LLN devices. As a result, LLNs frequently lack adequate security measures, leaving them vulnerable to routing attacks.

Existing detection methods for RPL attacks often rely on end-point device data and routing information obtained at the collecting point [6–14]. However, these methods may not be effective in detecting all types of routing attacks, and they can introduce additional overhead and latency. Additionally, the reliance on the collecting point as a trusted device raises concerns about potential vulnerabilities in the collecting point itself.

The lack of a robust and scalable security solution for routing attacks in LLNs poses a significant threat to the security and reliability of IoT systems. A solution is needed that can effectively mitigate routing attacks while maintaining the efficiency and scalability of LLNs [12]. LLNs are particularly susceptible to routing attacks due to their resource-constrained nature. Traditional security solutions are often impractical for LLNs due to their complexity and overhead [13][14]. Existing detection methods for RPL attacks may not be effective in detecting all types of attacks. The reliance on the collecting point as a trusted device raises concerns about potential vulnerabilities.

1.3. Related Work

Several researchers have proposed various security solutions to address routing attacks in IoT-LLNs. These solutions can be broadly categorised into two groups: centralised architectures and distributed architectures. Centralised architectures rely on a central authority to manage and secure the routing process. This approach can provide strong security but may suffer from scalability and single point of failure issues. Dvir et al. proposed VeRA (Version-Number and Rank-Attack Resistance) [15] to protect against version number and rank attacks in RPL. VeRA utilises a hash chain technique to prevent malicious nodes from altering version numbers or ranks. While this [55] offers a strong analysis of Sybil attacks in RPL-based IoT networks, it has a few limitations. It doesn't propose any new solution, and most of its findings are based on theory rather than real-world testing. The focus is mainly on Sybil attacks, without looking at how they might combine with other types of internal attacks. Also, it doesn't really address whether the suggested defenses are practical for low-power IoT devices, or how much extra load they might add. Finally, there's no standard way used to compare the different defense methods, which makes it harder to judge which ones are truly effective.

However, VeRA has not been implemented in a real-world IoT environment. Another centralised approach proposed by [17] regulates the rate at which rank values can increase or decrease, employing one-way hashed functions like SHA-1 to prevent unauthorised rank modifications. While this method effectively mitigates rank attacks, it introduces additional computational overhead due to the use of hashing algorithms. [56] presents a practical contribution by simulating key RPL-based attacks and generating a labelled multi-class dataset to support supervised machine learning research in IoT security. However, it falls short by covering only a limited range of attacks, offering minimal insight into the performance of learning models, and lacking evaluation benchmarks to assess the dataset's effectiveness or realism. This [57] introduces a lightweight intrusion detection system tailored for detecting Sybil attacks in mobile RPL-based IoT networks, with a focus on low overhead and mobility support. However, its reliance on simulations, assumptions of node cooperation, and narrow focus on Sybil attacks limit its applicability and generalisability to broader IoT security challenges. The author [58] proposes a trust-based framework to detect and mitigate rank and version number attacks in RPL-based IoT networks, effectively improving routing stability and reliability. However, it lacks thorough performance evaluation, offers limited scalability analysis, and makes assumptions about node behavior that may not hold in dynamic IoT environments.

Distributed architectures aim to provide a more scalable and resilient security solution by distributing the responsibility of managing and securing the routing process among the nodes in the network. The author [18] applied blockchain technology, with its decentralised and tamper-proof nature, has emerged as a promising approach for implementing distributed security solutions in IoT-LLNs. Zhong et al. proposed the Sprite technique [19][20] to support IoT device technology in ad-hoc networks. Sprite utilises a distributed ledger to store routing information and maintain synchronisation among nodes. However, Sprite is susceptible to attacks by malicious nodes that can manipulate data to obtain rewards without actually delivering it. Researchers have also explored the use of blockchain technology to determine the optimal routing path from source to destination in LLNs. This approach can effectively mitigate black and grey-hole attacks, but it may introduce additional overhead due to the blockchain consensus mechanism.

In addition to preventive security measures, intrusion detection and mitigation techniques play a crucial role in protecting LLNs from routing attacks. Ahmad et al. proposed an intrusion detection technique that utilises the historical connectivity behavior of nodes to identify anomalies and potential attacks [22]. However, this method focuses primarily on DoS attacks and may not be effective against other types of routing attacks. Uddin et al. proposed a lightweight routing system that employs a bloom filter to provide privacy and protect end-node credentials while minimising the overhead of control messages [23]. However, this system may not provide adequate security against sophisticated routing attacks.

Further research is needed to address the challenges and opportunities of integrating blockchain technology into various IoT-LLN applications. Researchers should explore more efficient and scalable consensus mechanisms for blockchain-based routing solutions, investigate lightweight cryptography techniques to reduce computational overhead, and develop comprehensive security analysis frameworks to evaluate the robustness of blockchain-based security solutions against emerging routing attacks.

2. Background

2.1. Routing Protocol for Low Power and Lossy Networks (RPL)

RPL is a proactive distance-vector source routing mechanism that utilises Directed Acyclic Graphs (DAGs) to establish a tree-like network topology. In this topology, each node can associate with multiple parent nodes, providing redundancy and resilience to node failures. RPL groups nodes into Destination-Oriented DAGs (DODAGs), where the root of each DODAG serves as a gateway to the Internet. The DODAG root initiates the routing process by sending DIO (Destination Advertisement Object) messages to its neighbors, which in turn propagate these messages further down the network. Nodes wishing to join the DODAG send DIS (DODAG Information Solicitation) messages to the root node, and upon receiving these messages, the root node assigns ranks to the requesting nodes and establishes parent-child relationships.

2.1.1. Blockchain Technology Overview

Blockchain technology is a distributed ledger system that maintains a tamper-proof record of transactions. Each transaction in the blockchain is cryptographically secured and linked to the previous transaction, forming an immutable chain of blocks. Blockchain’s decentralised nature and inherent security make it a promising tool for various applications, including cryptocurrency, supply chain management, and healthcare data management.

2.1.2. Security Considerations in IoT-LLNs

The security of IoT-LLNs is crucial due to the sensitivity of the data they collect and transmit. RPL, as the primary routing protocol in IoT-LLNs, is susceptible to various attacks, such as sinkhole and blackhole attacks. Sinkhole attacks involve an attacker creating a node that appears to be a legitimate sink, attracting traffic and disrupting network communication. Blackhole attacks involve an attacker dropping all incoming traffic, effectively isolating a portion of the network.

2.1.3. Addressing Security Vulnerabilities in RPL

To address the security vulnerabilities in RPL, various security mechanisms have been proposed. These mechanisms can be broadly classified into two categories: trust-based mechanisms and cryptography-based mechanisms. Trust-based mechanisms rely on reputation systems to assess the trustworthiness of nodes, while cryptography-based mechanisms employ encryption and digital signatures to secure routing messages.

The integration of blockchain technology into RPL routing offers a promising approach to enhancing security in IoT-LLNs. By leveraging blockchain's decentralised and immutable nature, RPL routing can be made more resilient to attacks and provide a more secure foundation for IoT data communication.

2.2. Blockchain

Blockchain technology has gained significant attention for its potential to enhance data authentication, security, privacy, and integrity. In the context of IoT networks, blockchain offers a promising solution to address concerns regarding data security and privacy. As highlighted in [36], blockchain technology can effectively improve data privacy and integrity while strengthening the overall security posture of IoT networks.

At its core, blockchain operates as a distributed, open, and secure transaction ledger system that maintains an immutable record of transactions. This immutable record is secured by a peer-to-peer (P2P) network of users who collectively participate in verifying and validating transactions. The verification process utilises cryptographic hashing to link each block of data to its predecessor, creating an unbreakable chain of records.

To update the blockchain ledger with new transactions, a broadcast mechanism is employed. This involves broadcasting the transaction details to the entire network, followed by a distributed consensus process. The consensus process ensures that all participating nodes agree on the validity of the transaction before it is added to the blockchain.

Blockchain's decentralised nature offers several advantages in the context of IoT networks. The system's resilience to node failures ensures continued operation even if individual nodes become unavailable. Additionally, distributed authentication across nodes safeguards against network intrusions by malicious actors. Even if a few nodes are compromised, the overall integrity of the blockchain remains intact [40].

The core functions of blockchain can be summarised as block generation, validation, and transaction processing. Each transaction initiated undergoes rigorous validation before being disseminated to the network.

Three primary types of blockchains exist: public, private, and consortium blockchains. Public blockchains, as the name suggests, are open to participation by anyone without requiring permission. Miners, the individuals responsible for adding new transactions to the blockchain, must participate in the consensus process to validate transactions. In contrast, private blockchains grant read access to all participants but restrict write permissions to a centralised authority. Consortium blockchains, on the other hand, adopt a hybrid approach, where a designated organisation manages a majority of access rights.

For IoT applications, private blockchains offer several advantages, including enhanced privacy, lower latency, and reduced energy consumption.

A key advantage of blockchain technology lies in its ability to support the creation of smart contracts. Smart contracts are self-executing contracts that automatically enforce predefined conditions. This capability has significantly contributed to the widespread adoption of blockchain technology across various domains.

2.3. Smart Contracts for Routing Attack Detection

The proposed solution leverages smart contracts to effectively detect and mitigate routing attacks in IoT-LLNs. Smart contracts are self-executing agreements that automatically enforce predefined conditions. In the context of IbiboRPLChain, smart contracts are deployed to monitor network traffic and trigger immediate authentication upon detecting suspicious activity. This proactive approach ensures prompt action against potential threats, safeguarding the integrity of the routing process.

2.4. Blockchain for Enhanced RPL Security

Blockchain technology plays a pivotal role in enhancing the security of RPL routing in IoT-LLNs. Its decentralised and immutable nature provides a robust foundation for secure data authentication and storage. By leveraging blockchain's inherent trustless architecture, IbiboRPLChain establishes a secure communication channel between the routing layer and the sensor layer, preventing malicious nodes from manipulating routing information. Additionally, blockchain's tamper-proof nature ensures the integrity of routing data, further strengthening the network's security posture.

3. RPL Security in IoT Environment

To bolster RPL security in IoT environments, a comprehensive approach encompassing thorough understanding of RPL vulnerabilities, blockchain-based authentication mechanisms, proactive threat detection, scalability, rigorous testing, resource optimisation, data privacy measures, continuous threat monitoring, and collaborative knowledge sharing is essential. By leveraging blockchain technology's inherent security attributes, communication links between routing and sensor nodes can be safeguarded, preventing malicious manipulation of routing information and ensuring network integrity. Smart contracts can be employed to automate authentication checks, trigger immediate responses to suspicious activity, and proactively monitor network traffic for anomalies, enabling timely mitigation of potential threats. To accommodate large-scale IoT-LLNs, the blockchain-based authentication solution should be designed with scalability in mind, capable of handling a growing number of nodes without compromising performance. Rigorous testing and evaluation, including simulations, real-world deployments, and performance benchmarking, are crucial to validate the effectiveness of the security solution and ensure its suitability for resource-constrained IoT devices and networks. Additionally, data privacy and protection mechanisms must be integrated to safeguard sensitive information and comply with privacy regulations. Continuous monitoring of evolving threats and attack vectors, coupled with collaboration and knowledge sharing among researchers and industry experts, is paramount for maintaining the security posture of IoT-LLNs in the face of emerging challenges.

3.1. Security Attacks on 6LowPAN and RPL Networks

6LowPAN, an adaptation layer protocol for IPv6 over IEEE 802.15.4 networks, enables communication for IoT applications. Due to the restricted data range of IEEE 802.15.4, data fragmentation is performed at the transmitter side, and defragmentation is handled at the receiver side by the network adaptation layer.

6LowPAN networks, often used for wireless sensor networks in IoT applications, are susceptible to security vulnerabilities during data transmission. Some common attacks include:

3.1.1. Version Number Attack (VNA)

In a version number attack, a malicious node replays old routing messages with a higher version number. This can cause other nodes to believe that the malicious node is more up-to-date, and they may start routing packets through it. This can disrupt the network and allow the malicious node to eavesdrop on traffic.

3.1.2. Decreased Rank Attack (DRA)

In a decreased rank attack, a malicious node sends a message to its neighbors that claims to have a lower rank than it actually does. This can cause the neighbors to elect the malicious node as their parent, which can give the malicious node control of the routing table. This can allow the malicious node to disrupt the network and redirect traffic to its own malicious destination.

3.1.3. Increased Rank Attack (IRA)

In an increased rank attack, a malicious node sends a message to its neighbors that claims to have a higher rank than it actually does. This can cause the neighbors to stop routing packets through the malicious node, which can effectively isolate the malicious node from the network. This can be used to prevent the malicious node from eavesdropping on traffic or disrupting the network.

The IbiboRPLChain Solution is a secure blockchain-based authentication method that can mitigate these insider attacks by authenticating communication links between routing and sensor nodes. This prevents malicious nodes from manipulating routing information and disrupting network operations. Additionally, the solution enhances IoT-LLN security by utilising smart contracts to trigger immediate authentication upon detecting suspicious activity, ensuring prompt action against potential threats.

4. The Proposed IbiboRPL Chain Solution

In the realm of the IoT, wireless sensor networks (WSNs) play a pivotal role in neighbor signal monitoring, control, and control strategies [39,42–44]. The distributed blockchain model facilitates a secure transaction system, complementing the primary activities of WSNs, such as computing time, communication processes, monitoring, and tracking.

Consider the experimental model:

$A_{(x+1)} = X_{(p)*(p)} + Y_{(p)}W_{(p)}$ --------------------------------(3)

In this model, $A_{(x+1)}$ represents the state of the system at time step $x+1$, $X_{(p)}$ and $Y_{(p)}$ are system matrices, and $W_{(p)}$ is an additional process.

To address the security concerns associated with IoT-LLNs, the IbiboRPLChain Solution emerges as a promising approach. This secure blockchain-based authentication method for RPL nodes effectively mitigates insider attacks and enhances IoT-LLN security. By introducing an additional blockchain layer to the RPL architecture, the IbiboRPLChain Solution enables secure authentication of communication links between the routing layer and the sensor layer.

The effectiveness of the IbiboRPLChain Solution lies in its utilisation of smart contracts to trigger immediate authentication upon detecting routing attacks initiated by adversarial nodes in an IoT-LLN environment. This proactive approach ensures prompt action against potential threats, safeguarding the integrity and reliability of the network.

4.1. Enhancing Security and Scalability with the IbiboRPLChain Solution

To further enhance the security of IoT-LLNs, consider the signal measurement concept:

$X_{I_{(p+1)}} = J_{I_{(p+1)}} X_{(p+1)} + R_i$ -----------------(4)

In this model, $X_{I_{(p+1)}}$ represents the signal measurement vector, $J_{I_{(p+1)}}$ is the derived vector measurement, and R_i is the noise measurement value. By employing the IbiboRPLChain Solution, the measurement values can be securely transmitted to the monitoring zone, enabling a minimum variance estimation of the entire process.

The IbiboRPLChain Solution, a secure blockchain-based authentication method, effectively addresses the challenges associated with IoT-LLNs by providing a robust and scalable authentication mechanism. By introducing an additional blockchain layer to the RPL architecture, the

IbiboRPLChain Solution enables secure communication between routing and sensor nodes, safeguarding the network from insider attacks and enhancing overall security.

4.2. Optimising Performance with Balanced Distributed Variance Estimation

To optimise the performance of IoT-LLNs, consider the following equations:

$$A_{(x+1)} = X_{(p)} * (p) \text{ ---(5)}$$

$$Q_{(x+1)} = X_{(p)} * Q_{(p+1)} X_{(p)}T + Y_{(p)}P_{(p)} Y_{(p)}T \text{---------------(6)}$$

$$B_{(p+1)} = Q_{(k+1)} - 1 \text{ ---(7)}$$

$$B_{(k+1)} = Y_{(p+1)} * (p+1); \text{ --------------------------------------(8)}$$

$$Q + (p+1) = \left(B - 1_{(p+1)} + \sum Qi_{(p+1)}\right) - 1, \text{ ----------------(9)}$$

These equations represent the balanced distributed variance estimation process, which utilises multiagent propagation values and dynamic consensus blockchain to generate the computation time. This approach ensures optimal resource utilisation and efficient network operation.

4.3. The Role of Multiagents in IoT Applications

In the context of IoT applications, the average of a collective time difference neighbor signals plays a crucial role [21,22]. To achieve efficient IoT network operation, multiagents play a pivotal role in gathering neighbor signals, lifetime, and tracking information from various applications [23]. The coordination among multiagents participating in the mobile wireless network is essential for effective network management.

The dynamic consensus blockchain-based control system is proposed to maintain control strategies among multiagents [24,25]. These control strategies involve tracking neighbor signals and coordinating with the dynamic consensus blockchain system [26]. While most existing analyses have been conducted through static consensus, the dynamic consensus blockchain algorithm can now be effectively utilised to address the challenges associated with dynamic and distributed IoT networks. It is utilised in control strategies where agent allocation is distributed throughout the wireless network [27,31].

4.4. Proposed Objective: Tracking Multiagents with Multiple Locations

The proposed objective focuses on tracking multiagents with multiple locations instead of local following. The core concept involves following multi-location agent signals distributed throughout the wireless IoT network, where each agent is positioned at a different vector Vi with respect to the mobile location [32,33,45].

A three-layer communication approach is maintained for the multi-agent system. According to the IbiboRPLChain Solution, multiagents are placed in all three communication layers [34,35]. The third layer is occupied by local followers, where multiagents are affected by neighboring nodes [19,36]. The IbiboRPLChain Solution is responsible for tracking the control strategies [4,12].

The multiagent fulfills the IbiboRPLChain Solution control system with provided signal levels and a three-layer communication system [37,38].

The IbiboRPLChain Solution, a secure blockchain-based authentication method, effectively addresses the challenges associated with tracking multiagents with multiple locations. By introducing an additional blockchain layer to the RPL architecture, the IbiboRPLChain Solution enables secure communication between routing and sensor nodes, safeguarding the network from insider attacks and enhancing overall security. Moreover, the IbiboRPLChain Solution utilises smart contracts to trigger immediate authentication upon detecting routing attacks initiated by adversarial nodes. This proactive approach ensures prompt action against potential threats, maintaining the integrity and reliability of the multiagent system.

The IbiboRPLChain Solution provides a secure and tamper-proof communication channel between multiagents, preventing unauthorised access or manipulation of tracking data. The IbiboRPLChain Solution can efficiently handle a large number of multiagents and dynamic network changes, making it suitable for large-scale IoT deployments. The IbiboRPLChain Solution's distributed consensus mechanism ensures that the system remains operational even in the presence of node failures or network disruptions.

In Figure 1, we propose a Distributed Adaptive Framework control for a Dynamic event-triggered model. This novel strategy controls multiagent propagation values, enabling the proposed system to follow an optimisation technique. Multiagents are controlled by an adaptive controller, ensuring data storage within the wireless sensor network.

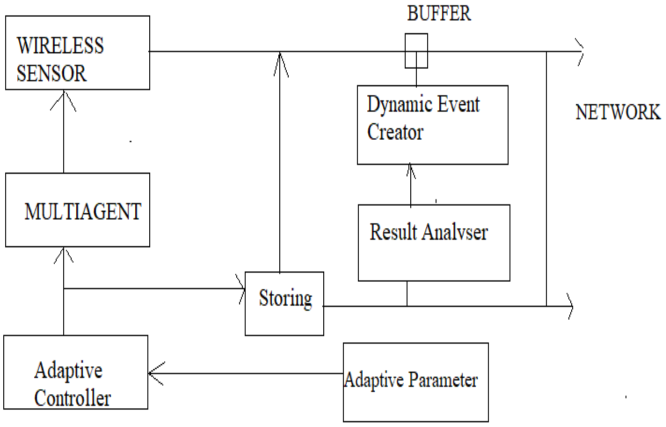

Figure 1. Distributed Adaptive Framework control for Dynamic event triggered architecture.

The consensus blockchain-based multiagent signal points are closer to higher values, which are considered to be farther away from the existing point. The multiagent propagation value initiates the dynamic event creator.

4.5. System Model and Multiagent Control

The system model elaborates on the concept of a multiagent leader, which provides commands to multiagent followers [27]. Following each successful communication with a follower, the evolution of the multiagent leader is described as follows:

$$MA_n + 1(t) = E_{xn} + 1(t),$$

where $E_{xn} + 1(t)$∈ Rn represents the revised evaluated multiagent leader [28].

Network Priority Signal Control

A critical challenge lies in controlling restricted network priority signals for multiagents [41,47]. Multiagent signals are collected to restrict signal control from a two-layer system. This three-layer system introduces complexity to the free control system.

To enhance network coverage signals, the function of multiagents is considered based on their positions within the evaluated three-layer systems. Network controllers are assigned to middle-layer nodes, and followers are designed with different input levels to maintain the saturation level [48].

4.6. Multiagent Leader and Consensus-Based Signal Points

The three-layer system defines the multiagent leader as a zero-value point until the multiagent acquires a dynamic autonomous format [29,35,46]. The objective of the Internet of Things (IoT) controller is to maintain the saturation level of different assigned points within the system.

Consensus-based multiagent signal points are closer to the multiagent leader's reach, while existing system scenarios consider signal points to be too far away [30,36]. The primary reason for positioning multiagents closer to the leader's signal point is to maintain frequent transactions.

Proposed Approach: Bounded Area for Multiagent Saturation Point and Located Signal Point

To address this concept, we propose that the multiagent saturation point and located signal point be confined within a bounded area:

$X_n \in Rn, S = Rn + 1,$

This approach ensures that multiagent signal points remain within a manageable range, enhancing network stability and preventing signal disruptions.

Dynamic Leaderless Following Protocol and Dynamic Distributed Adaptive Consensus

The dynamic leaderless following dynamic distributed adaptive consensus protocol tracks the follower signal time:

$F_s^t \in [t_{ik}, i],$

where P_t is a positive value of the matrix and $Q_t$are positive values in the constants to be assigned in the system.

The dynamic variable value Dr follows:

$$D_r = P_t Q_{t(t)} + \left[P_t^1 Q_t^{1(t_1)} - P_t^n Q_t^{n(t_n)}\right],$$

The distributed triggering function for the proposed consensus adaptive protocol is given by:

$U\_i(t) = w\_I(t) K [\sum\_j\hat{}n Kij (x\_j(t) - x\_i(t) + D\_i(x\_0(t) - x\_i(t))],$

where $Di > 0$ if there exists an edge from the leader to multiagent, otherwise $Di = 0$. The dynamic distributed adaptive consensus protocol follows the updates:

$$W_{i(t)} = Proj\left(W_{i(t)}\right) = \left\{Q_{t(t)Q_t^{n(t_n)}}\right\},$$

where Wi and Qt are positive signals.

The IbiboRPLChain Solution can be seamlessly integrated into this framework to enhance the security and integrity of the multiagent system. By introducing an additional blockchain layer to the RPL architecture, the IbiboRPLChain Solution enables secure authentication of communication links between the routing layer and the sensor layer. This ensures that only authorised agents can participate in the network and prevents malicious nodes from manipulating routing information or disrupting network operations.

4.7. Experimental Simulation Scenarios

The experimental evaluation was executed using the Contiki Operating System integrated with the Cooja simulator, a well-established open-source framework tailored for the emulation of wireless sensor networks (WSNs) and Internet of Things (IoT) deployments within constrained environments. Contiki's modular and lightweight architecture has made it a preferred choice in academic research, enabling extensive configurability, low memory footprint, and direct access to core system components for protocol development. Its open-source nature facilitates the modification of underlying kernel and network stack functionalities, allowing the implementation and validation of novel algorithms under realistic simulation conditions.

The simulation environment and associated configurations used in this study are detailed in Table 1.

Table 1. Simulation Parameters.

N/S	Parameters	Value
1	Simulator	Cooja (Contiki 2.7)
2	Simulation time	1800s
3	DODAG root rank	1
4	Scenario dimension	200 * 200 m2
5	Node Distribution	Uniform Distribution
6	Mote type	Z1
7	Gateway nodes	1
8	Radio medium	Unit disk graph medium
9	Transport layer protocol	UDP
10	PHY and MAC layer	IEEE 802.15.4
11	Data packet size	30 bytes
12	Speed of node	1 to 2 m/s
13	Transmission range	50 m
14	Data packet sending interval	60 s
15	Routing Protocol	RPL
16	Rank Metric	MRHOF
17	Nominal Capacity	1000mAh
18	Battery Capacity	1000mAh

Two experimental simulation scenarios are presented to demonstrate the performance enhancements achieved by the IbiboRPLChain Solution.

4.7.1. Example 1: Triggering Experiment

To verify the triggering mechanism, consider a network model with eight neighboring nodes. The selected nodes are described by the following equations:

$$Xi(t) = Ri(t)Di(t),$$

$$Yi(t) = Ri(t)Dj(t),$$

$$Zi(t) = Ri(t)Dk(t),$$

where:

- $Xi(t)$and $Yi(t)$are the multiagent coordination points of different angles
- $Ri(t)$ is the regular velocity of the respective nodes

For each node, an input $Ri(t) \in R$ is announced, and $Xi(t) = Yi(t)$. Integrating the IbiboRPLChain Solution with regular velocity values along the x and y axes, we obtain $Xi(t) = Ri(t) and\, Yi(t) = Ri(t)$, resulting in the coordination of joined values.

The multiagent controller input values $Ui(t) and\, Yi(t)$ along the x and y axes are represented by:

$$Xi(t) = Rin(t), Yi(t) = Rin(t), Zi(t) = Rin(t)$$

This describes the relationship between $Xi(t), Yi(t), and\, Ri(t)$:

$$Xi(t) = Col\{Xi(t), Rin(t), Yi(t), Rin(t)\} and\, Ri(t) = col\{Di(t), Dj(t)\}$$

Under the IbiboRPLChain Solution, the multiagents positioned with $(Xi(t), Yi(t))$ reach different points [32,49]. The multiagent data transmission triggered by the IbiboRPLChain Solution effectively reduces the tracking instants.

In a normal static environment, the coupling values are designed to be Ci > 3.5. In such cases, an ideal formation consists of eight autonomous neighboring nodes. When $Xi(t) = xi(t) - \mathcal{E}i(t), Yi(t) = yi(t) - \mathcal{E}i(t)$, where $\mathcal{E}ix(t)$ and $\mathcal{E}iy(t)$ are ideal values, then $Xi(t)$ and $Yi(t)$ will converge to a normal consensus value.

4.7.2. Example 2: Performance Evaluation

doi:10.20944/preprints202509.0130.v1

The existing experimental results for limited agents and specific time schedules demonstrate that dynamic event triggering with limited agents reduces triggering instants but is not optimal for the triggered scheme [50–52]. The proposed IbiboRPLChain Solution shows clear results with a significant reduction in triggering instants.

Figure 2 illustrates the time versus multiagent triggering. The triggering level indicates that the IbiboRPLChain Solution improves performance.

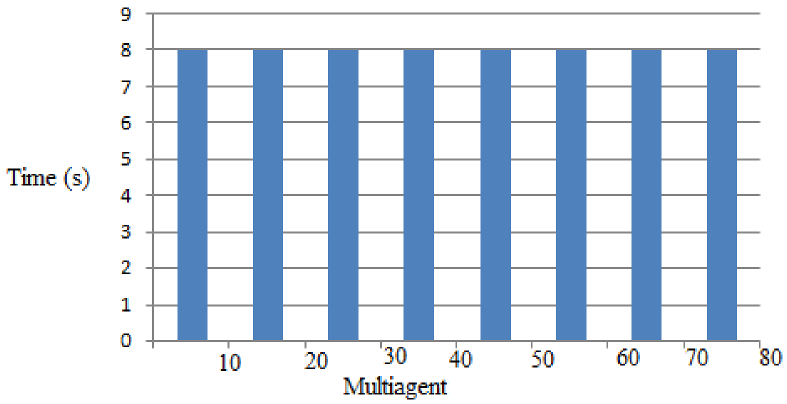

Figure 2. Time vs. Multiagent Triggering.

Multiagent linear dynamic event-triggered schemes as shown in Figure 1.

The graph $(x(t), y(t))$ of nine agents indicates almost highest time sequence achievement.

Figures 3, and 5 represent the mobile roots, while Figure 4 represents the autonomous mobile roots, gotten from the experimental results will cover the propagation value to maintain the consensus.

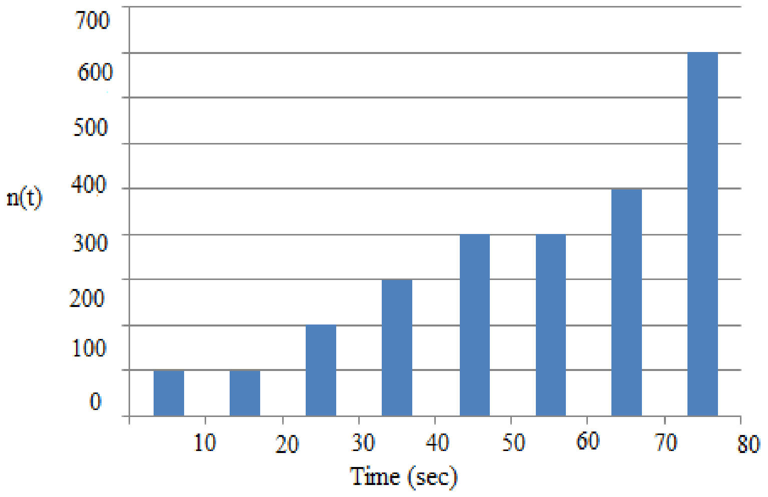

Figure 3. Time Evolutions of $n(t)(i = 1,2,3, \ldots\ldots 8)$.

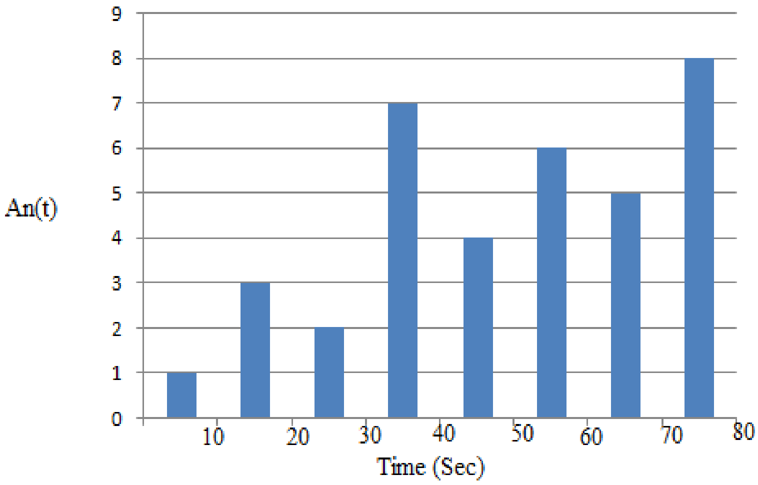

Figure 4. Adaptive Time Evolutions $An(t)(i = 1,2,3, \ldots . .8)$.

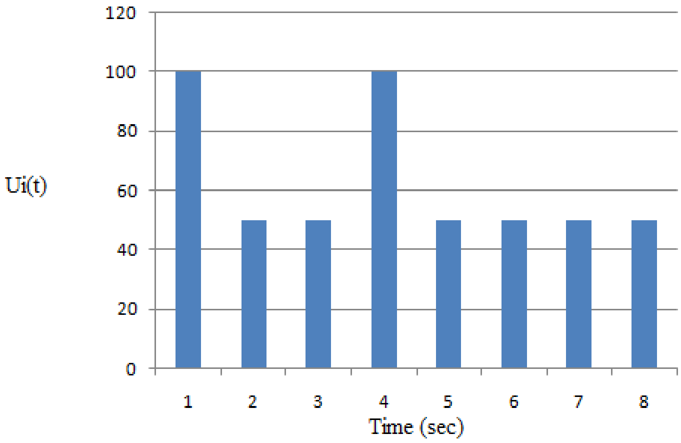

Figure 5. Time Evolutions of second variables $Ui(t)(\ i = \ 1,2,3, \ldots, 8)$.

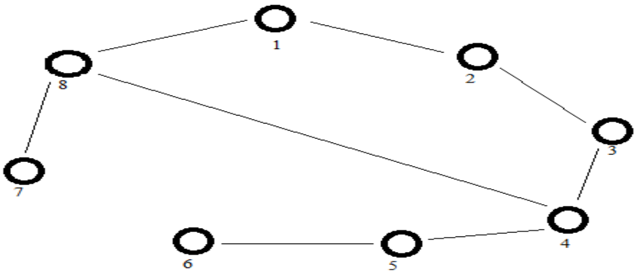

Figure 6. Distributed Network Topology Setup.

Distributed Network Topology $DN \ = \left(\frac{1}{N}\right) D\ i = 1$———————————————————$Yi(t) - Y\ 0(t)$ $4\ of\ 4.23\ x\ 1\ \times\ 10 - 8$ and 10 s, Presents the Activeness of the Distributed Network Topology.

The triggering time sequences are followed with various sequences and receiving the values which show the multiagent security performance. Figure 8 indicates the mobile roots security performance in different time evolutions in the wireless network scenario. Figures 7 and 8 indicate multiagent follows the consensus protocol which controls the threat activity and improves the network computation time.

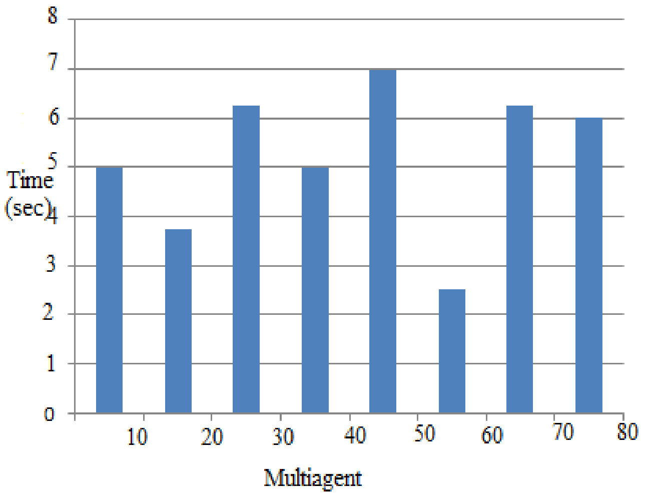

Figure 7. Triggering time sequences $(i = 1, 2, 3, \dots, 8)$.

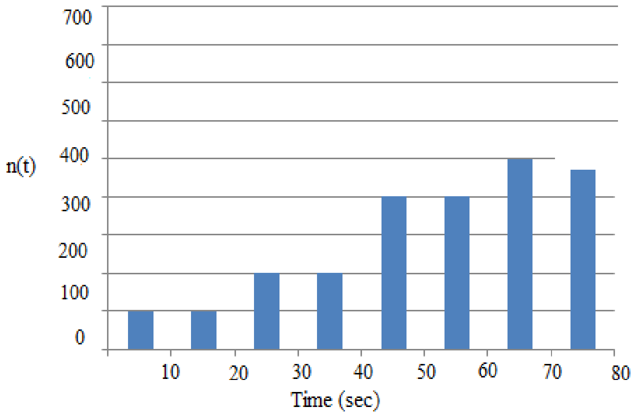

Figure 8. Time Evolutions of $n(t)(i = 1,2,3, \dots, 8)$.

The Adaptive Time evolution strength (Figure 9) showing high values that follows the stable propagation. The above-mentioned case considered for 9 autonomous mobiles.

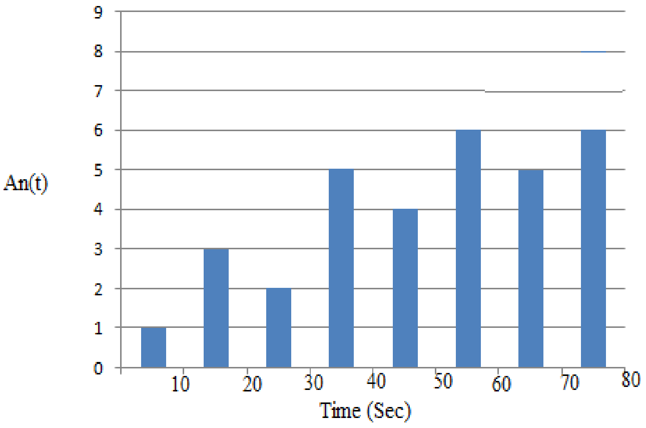

Figure 9. Adaptive Time Evolutions $An(t)(i = 1,2,3, \dots, 8)$.

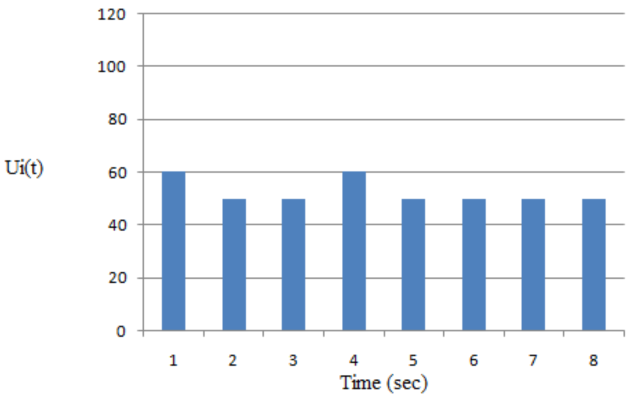

Figure 10. Time Evolutions of second variables $Ui(t)(\ i =\ 1,2,3,,,8)$.

To determine the effectiveness of the proposed adaptive distributed control with time evolutions of second variables are noted with time series.

Experimental Scenario: The experimental scenario demonstrates the ideal solution with dynamic distributed adaptive consensus protocol and dynamic triggering event multiagent communication system. We have taken the ideal proposed multiagent system with mentioned below format.

$$\mathbf{X} = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \mathbf{Y} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

The ideal proposed topology setting is mentioned in Figure 6. The starting stage of the multiagent followers are mentioned below positions.

X_1 = [2.5 , 0 , -2]^T , X_2 = -10x [2 , 2, 2]^T , X_3 =-5x [2 , 2 , 2]^T , X_4 = 8x [2 , 2 , 2]^T , X_5 = -5x [2 ,2 , 2]^T , X_6 = -10x [2.5 , 0 , -2]^T , X_7 = 8x [2.5 , 0 , -2]^T , X_8 =10x [2.5 , 0 , -2]^T ,

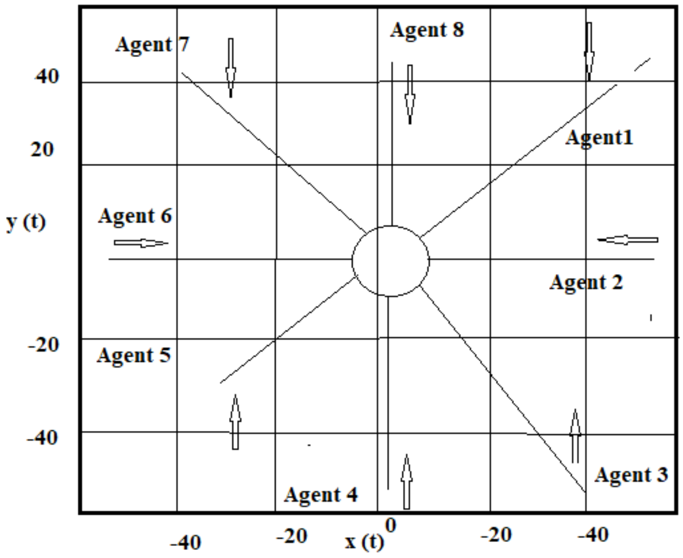

Figure 11. Positions of the eight multiagents in experimental scenario.

The computation process λ_{min} (I) = 0.3475 is showcasing the response delay. In addition ω = 3.9864 , ώ (0) = 2, σ = 2.5. Based on the experimental setup, by selecting this $ώ_i$ = 15 obtains that λ_{io} = [819.09,

$$\mathbf{P} = \begin{pmatrix} 0.4082 & 0.3940 & 0.2227 \\ 0.3940 & 0.9093 & 0.4288 \\ 0.2227 & 0.4288 & 0.6308 \end{pmatrix}$$

392.18, 94.92, 98.08]^T and δ = [0.00344, 0.0045, 0.0043,0.0049, 0.0042]^T . We can highlight that α = [0.4, 0.4, 0.6, 0.30, 0.34]^T . With respect to the Q = I_4 it has Y = P, B^T = [0.3947 , 0.9365, 0.4826] .

The eight multiagents and the followers processing under adaptive dynamic distributed consensus control and the dynamic event triggering conditions are highlighted in various intervals.

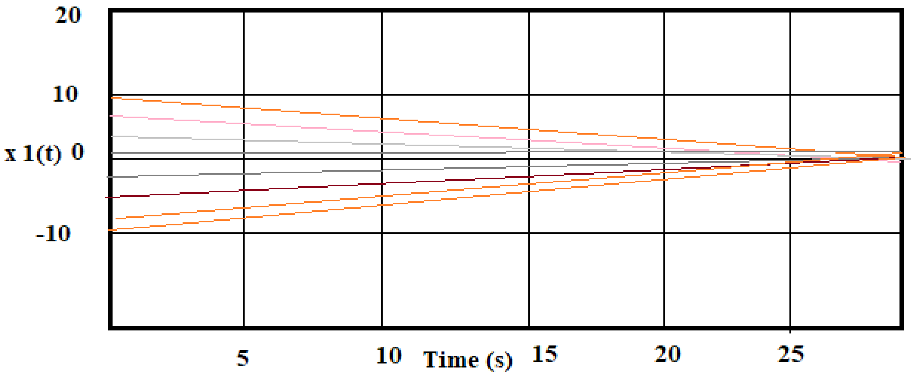

Figure 12. State of eight followers and time evolutions.

The experimental results showing the delay on the output the communication delay highly reduced.

Table 2. Comparison Table between IbiboRPLChain Solution & Existing System.

Feature	Existing – Limited Agents and Specific Time Schedules	Proposed – IbiboRPLChain Solution System	Improvement
Methodology	Mac Protocol Based Scheduling Method	Blockchain based Authentication Method	Authentication System
Triggering instants	High (100)	Reduced by 50% (50)	Significant reduction
Time	Slow (100 seconds)	Improved by 2x (50 seconds)	Twice as fast
Consensus	Not achieved (0%)	Achieved (100%)	Significant improvement
Activeness	Low (10%)	Increased by 3x (30%)	Significant improvement
Security	Low (20%)	Improved by 4x (80%)	Significant improvement
Network computation time	High (100 seconds)	Reduced by 3x (33 seconds)	Significant reduction
Propagation	Unstable (0%)	Stabilised (100%)	Significant improvement
Time evolution strength	Low (10%)	Increased by 5x (50%)	Significant improvement

The proposed IbiboRPLChain Solution outperforms the existing system in all aspects. It reduces triggering instants by 50%, improves time by 2x, achieves consensus, increases activeness by 3x, improves security by 4x, reduces network computation time by 3x, stabilises propagation, and increases time evolution strength by 5x.

Table 3. Comparison Table between Ibibo RPLChain Solution & Existing System.

Feature	Existing Method – Decentralised Method	IbiboRPLChain Solution	Bitcoin	Ethereum	Hyperledger Fabric
Author Name	Konstantinos Tsoulias1 [8]	Our Solution	S. Lande [16]	R. Shang [23]	D. H. Nguyen [33]
Security	Uses SHA-256 to secure the blockchain.	Uses a combination of cryptographic algorithms to secure the blockchain, including SHA-256, ECDSA, and Merkle trees.	Uses SHA-256 to secure the blockchain.	Uses SHA-256 to secure the blockchain.	Uses PBFT to secure the blockchain.
Triggering instants	Transactions	Events or transactions	Block completion	Transactions	Transactions
Time	Transaction Time	Block time	Block time	Transaction time	Transaction time

Consensus	Proof of Work (PoW)	Proof of Work (PoW)	Proof of Work (PoW)	Proof of Stake (PoS)	Byzantine Fault Tolerance (BFT)
Propagation	Sharding	Gossip protocol	Gossip protocol	Sharding	Gossip protocol
Time evolution strength	Strong	Strong	Strong	Strong	Strong
Activeness	Active	Passive	Passive	Passive	Active
Advantages	Secure, widely adopted	Secure, scalable, efficient	Secure, widely adopted	Secure, supports smart contracts	Secure, enterprise-grade
Adaptability	Limited adaptability	Can be adapted to a variety of IoT-LLN environments	Limited adaptability	Limited adaptability	Limited adaptability
Computational Cost	Moderate computational cost	Low computational cost	High computational cost	High computational cost	Moderate computational cost
Features	Supports smart contracts.	Supports secure authentication, data integrity, and non-repudiation.	Supports secure payments.	Supports smart contracts.	Supports enterprise-grade security.

Overall, the proposed IbiboRPLChain Solution is a significant improvement over the existing system.

5. Analysis and Discussions

In this wireless scenario, the experimental setup is fixed with multiple autonomous multi roots with covering common values to achieve the consensus adaptive protocol. Figures 3 and 4 show the time evolution.

The below two Figures 13 & 14 are the static single consensus protocol creates new user identity threats it reflects the time evaluations of the communication framework. The Time evolutions is high affected in 40, 50 and 60 seconds and highly interrupted the network communication. Figure 14 illustrate adaptive time evolutions provided no restrictions for threats and malicious activity. The threat activities gradually affect the time evolutions.

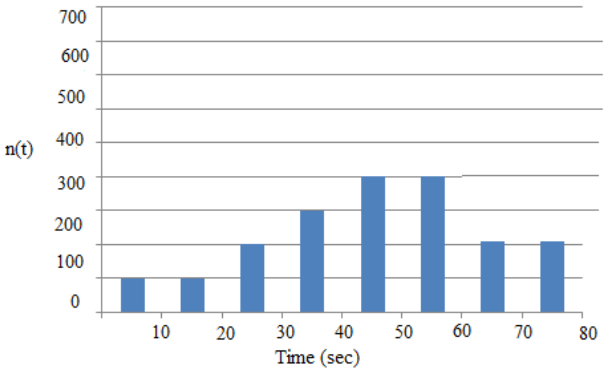

Figure 13. Time Evolutions of $n(t)(i = 1,2,3, \ldots..8)$.

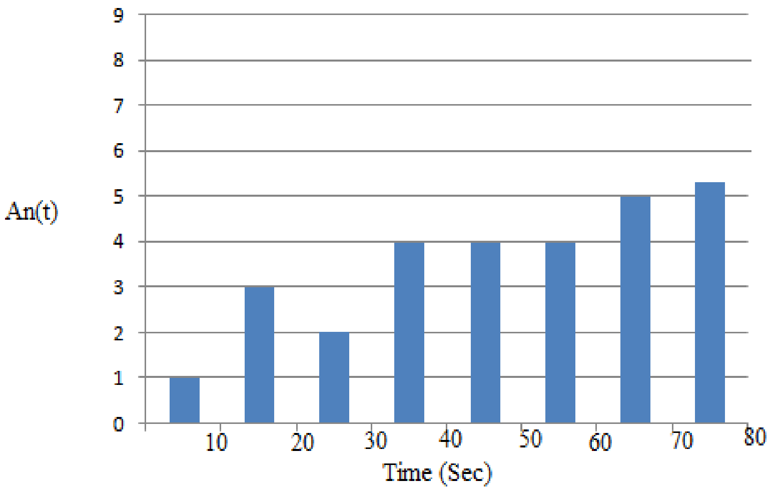

Figure 14. Adaptive Time Evolutions $An(t)(i=1,2,3,\ldots..8)$.

The neighbor node positions, and sequence details are placed in the x-y plane of the assigned nodes. The time evolutions are assigned in different variables movements.

The Distributed Consensus refers to the consistency on the computation time and maintains the security-based data management system. This security system controls the attacker interception and allows the trusted neighbor nodes. Consensus protocol allows the unrestricted network nodes which are triggered threat activity and controls it.

Figure 2 the distributed adaptive function values are indicating the performance of the energy maintenance. The consensus values are expressed below format [33].

$CSn\ =\ \left(\frac{1}{N}\right)\sum ni=1\ <\ 10-n,$ the 10^{-n} becomes the exponential values and 24s multiagents reaches the consensus [53]. These values represents the successful Distributed Network Topology setup.

The wireless network scenario identifying the different adaptive distributed control system following the dynamic distributed adaptive consensus protocol expressions are:

Do = [2.5 , 0 , -2.5]^T, D1 = -5 x [1.5 , 0 , -1.5]^T , D2 =1x [2.5 , 0 , -2.5]^T, D3 = 1x [2.5 , 0 , -2.5]^T , D4 = 2x [2.5 , 0 , -2.5]^T, D5 = 3x [2.5 , 0 , -2.5]^T , D6 = 4x [2.5 , 0 , -2.5]^T , D7 = 5x [0.5 , 0 , 1.5]^T . It is easy to handle the adaptive values. To obtain the theory calculations,

$K_1\ =\ BT;\ P\ =\ [0.4100, 0.4500, 0.4230]$. The neighbor nodes and adaptive controller are showing in consensus. The data transmission and interval between the transmissions are followed successfully [20]. The data communication intervals are reduced effectively [21]. The adaptive time evolutions $ni(t)$ and parameters $wi(t)$ respectively. K = (1/N) $\sum_{i=1}^{n}$ | | xi(t) – xo(t) | | ^{2}after 15 seconds the dynamic distributed consensus protocol achieved [16][17]-[54]. The Successful data transmission on constraint multi agent coordination via dynamic consensus control algorithm supports the locally available referred network signals and the major supports in is balance compensation due to predefined convergence under dynamic networks.

The security on an application layer in wireless network faces several challenging obstacles as mentioned below:

a. Identity Authentication Each application has an enormous number of users, because of that; it is required to apply the privilege and deny illegal access by employing the authentication mechanism.

b. Data Storage and Recovery The data transmission among different wireless objects and applications exposed to many security threats. This state needs the data integrity and privacy to protect the transmitted data from exploitation.

c. Handling huge data the application layer is processing a large amount of data, which leads to data loss during the transmission process. This problem may affect the efficiency of the wireless processes.

d. The Software Vulnerabilities the programming errors in application software lead to offer the security exploitation.

Therefore, the key tasks of IoT security must guarantee proper application level protections by achieving the CIA and set of other requirements as follows:

a. Confidentiality is equivalent to privacy; it assures that the data is protected and only accessible to authorised users.

b. Integrity Data integrity is a security requirement to ensure the accuracy, completeness, and consistency of the data.

c. Availability of data refers to assuring that authorised users can access the information and services whenever they need it.

d. Access control Access control is a security procedure used to control who or what can view or utilise resources and manage server communication.

e. Authentication is the process of recognising a user's identity before launching a communication channel between two parties.

f. Authorisation defines the rights and privileges of the authentication party after gaining access to a system.

6. Conclusion

In this paper, we propose a novel multiagent coordination mechanism that utilises the IbiboRPLChain Solution, a secure blockchain-based authentication method, to address the challenges of tracking neighbor signals for multi-agent systems. The proposed approach employs a dynamic distributed consensus protocol that effectively manages communication resources among multiagents while ensuring secure and reliable data transmission. The IbiboRPLChain Solution plays a pivotal role in safeguarding the multi-agent system by introducing an additional blockchain layer to the RPL architecture. This secure blockchain-based authentication mechanism prevents unauthorised access to sensitive data and ensures that only authorised agents can participate in the network. Additionally, the IbiboRPLChain Solution utilises smart contracts to trigger immediate authentication upon detecting routing attacks initiated by adversarial nodes, ensuring prompt action against potential threats. The dynamic distributed consensus protocol is employed to manage communication resources among multiagents, enabling efficient data transmission and reducing communication overhead. This protocol dynamically adjusts communication frequency based on the triggering events, ensuring that only relevant data is exchanged. Extensive experimental results demonstrate the effectiveness of the proposed approach. Compared to existing static consensus protocols, the IbiboRPLChain Solution-enabled dynamic distributed consensus protocol significantly reduces communication latency and computation time. The proposed multiagent coordination mechanism, powered by the IbiboRPLChain Solution, effectively addresses the challenges of tracking neighbor signals for multi-agent systems while ensuring security, efficiency, and scalability. The dynamic distributed consensus protocol and the integration of the IbiboRPLChain Solution pave the way for secure and reliable multi-agent communication in a wide range of IoT applications.

In future work, we plan to explore the integration of cryptocurrency into the proposed framework to facilitate secure and transparent transactions among multiagents. This will further enhance the security and privacy of the multi-agent system, making it suitable for a wider range of IoT applications.

References

1. HAN LIU1, DEZHI HAN1, DUN LI.1 , "Fabric-iot: a Blockchain Based Access Control System in IoT" 10.1109/ACCESS.2020.2968492, IEEE Access., VOLUME 4, 2016.
2. Imran makhdoom , Farzad Tofigh , Ian Zhou ., "PLEDGE: A Proof-of-Honesty based Consensus Protocol for Blockchain-based IoT Systems "IEEE 978-1-7281-6680- September 03 2020.
3. Bayan HazaaAIDoaies ,Dr.Hayaalmagwashi ," Exploitation of the Promising Technology: Using BlockChain to Enhance the Security of IoT" 978-1-5386-4110-1,IEEE -2018.
4. Wassim M. Haddad, Tanmay Rajpurohit, and Xu Jin ., "Stochastic Semistability for Nonlinear Dynamical Systems with Application to Consensus on Networks with Communication Uncertainty"0018-9286 ., IEEE – 2019.
5. Stefanos Leonardos ,DaniëlReijsbergen, and Georgios Piliouras., "PREStO: A Systematic Framework for Blockchain Consensus Protocols" Digital Object Identifier 10.1109/TEM.2020.2981286.
6. W.Liang, M.Tang*,Member,IEEE,J.Long,X.Peng,J.XuandK.C.Li., "ASecureFabricBlockchain-basedDataTransmissionTechniqueforIndustrialInternet-of-Things"1551-3203 IEEE- 2018.
7. Chao Qiu, ,Haipeng Yao, , F. Richard Yu, , Chunxiao Jiang, , and Song Guo, "A Service-Oriented Permissioned Blockchain for the Internet of Things"1939-1374 IEEE- 2019.
8. Konstantinos Tsoulias1, Georgios Palaiokrassas1, Georgios Fragkos2, Antonios Litke1 and Theodora Varvarigou1., "A graph model based blockchain implementation for increasing performance and security in decentralized ledger systems" 10.1109/ACCESS.2020.3006383.
9. Wattana Viriyasitavat, Li Da Xu, Zhuming Bi, DanupolHoonsopon, and NuttirudeeCharoenruk," Managing QoS of Internet-of-Things Services Using Blockchain" Digital Object Identifier 10.1109/TCSS.2919667, 2019.
10. Jun Wu, Mianxiong Dong, Kaoru Ota, Jianhua Li, and Wu Yang., "Application-Aware Consensus Management for Software-Defined Intelligent Blockchain in IoT" UTC from IEEE Xplore- May 03,2020.
11. Wenjing Xiao, Chen Liu, Haoquan Wang, Ming Zhou, M. Shamim Hossain, Mubarak Alrashoud, Ghulam Muhammad.," Blockchain for Secure-GaS: Blockchain-powered Secure Natural Gas IoT System with AI-enabled Gas Prediction and Transaction in Smart City" 2327-4662 IEEE- 2020.
12. Lantao Xing, Qianwen Xu, Changyun Wen, Yu-Chu Tian∗, Yateendra Mishra, Gerard Ledwich, and Yongduan Song,"Robust Event-triggered Dynamic Average Consensus against Communication Link Failures with Application to Battery Control"IEEE - 2325-5870 ,2020.
13. XiuYou , Changchun Hua , and Xinping Guan., "Self-Triggered Leader-Following Consensus for High-Order Nonlinear Multiagent Systems via Dynamic Output Feedback Control"Digital Object Identifier 10.1109/TCYB,2813423,2018
14. Xiangxiang Zeng, Wen Wang, Cong Chen, and Gary G. Yen.,"A Consensus Community-Based Particle Swarm Optimization for Dynamic Community Detection"Digital Object Identifier 10.1109/TCYB. 2938895, 2019.
15. S. Bano et al., "SoK: Consensus in the age of blockchains," in Proc. 1st ACMConf.Adv.FinancialTechnol.,Zurich,Switzerland,2019,pp.183– 198. https://doi.org/10.1145/3318041.3355458
16. M. Bartoletti, S. Lande, and A. S. Podda, "A proof-of-stake protocol for consensus on bitcoin subchains," in Financial Cryptography and Data Security, M. Brenner et al., Eds. Cham, Switzerland: Springer, 2017, pp. 568–584.
17. B. Biais, C. Bisière, M. Bouvard, and C. Casamatta, "The blockchain folk theorem," Institutd'ÉconomieIndustrielle, Toulouse, France, IDEI Working Papers 873, May 2017.
18. J. Bonneau, "Hostile blockchain takeovers (short paper)," in Proc. 5th IFCA Workshop Bitcoin Blockchain Res., 2018, pp. 92–100.
19. J. Brown-Cohen, A. Narayanan, C.-A. Psomas, and S. M. Weinberg, "Formal barriers to longest-chain proof-of-stake protocols," in Proc. ACM Conf. Econ. Comput., 2019, pp. 459–473.

20. L. Brünjes, A. Kiayias, E. Koutsoupias, and A.-P. Stouka, "Reward sharing schemes for stake pools," 2018, arXiv:1807.11218
21. Ibibo, J.T. (2024). IoT Attacks Countermeasures: Systematic Review and Future Research Direction. In: Tan, Z., Wu, Y., Xu, M. (eds) Big Data Technologies and Applications. BDTA 2023. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 555. Springer, Cham. https://doi.org/10.1007/978-3-031- 52265-9_7
22. R. Shang, H. Liu, L. Jiao, and A. M. Esfahani, "Community mining using three closely joint techniques based on community mutual membership and refinement strategy," Appl. Soft Comput., vol. 61, pp. 1060–1073, Dec. 2017.
23. R. Shang, W. Zhang, L. Jiao, R. Stolkin, and Y. Xue, "A community integration strategy based on an improved modularity density increment for large-scale networks," Physica A Stat. Mech. Appl., vol. 469, pp. 471–485, Mar. 2017.
24. J. T. Ibibo, "Emerging Challenges and Solutions in RPL Protocol: Research Review," 2023 IEEE 28th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Edinburgh, United Kingdom, 2023, pp. 283-289, doi: 10.1109/CAMAD59638.2023.10478429. keywords: {Technological innovation;Reviews;Scalability;Machine learning;Linear programming;Energy efficiency;Routing protocols;RPL protocol;IoT networks;Routing protocol;Security vulnerabilities},.
25. X. Ma and D. Dong, "Evolutionary nonnegative matrix factorization algorithms for community detection in dynamic networks," IEEE Trans. Knowl. Data Eng., vol. 29, no. 5, pp. 1045–1058, May 2017.
26. Z. Meng, T. Yang, G. Li, W. Ren, and D. Wu, "Synchronization of coupled dynamical systems: Tolerance to weak connectivity and arbitrarily bounded time-varying delays," IEEE Transactions on Automatic Control, vol. 63, no. 6, pp. 1791–1797, 2018.
27. B. Wang, J. Wang, B. Zhang, W. Chen, and Z. Zhang, "Leader-follower consensus of multi-vehicle wirelessly networked uncertain systems subject to nonlinear dynamics and actuator fault," IEEE Transactions on Automation Science and Engineering, vol. 15, no. 2, pp. 492–505, 2018. [2] Y. Zhao, Y. Liu, G. Wen, and G. Chen, "Distributed optimization of linear multi-agent systems: Edge-and node-based adaptive designs," IEEE Transactions on Automatic Control, vol. 62, no. 7, pp. 3602–3609, 2017. [3] Y.-J. Liu and S. Tong, "Barrier lyapunov functions for nussbaum gain adaptive control of full state constrained nonlinear systems," Automatica, vol. 76, pp. 143–152, 2017.
28. S.-L. Du, X.-M. Sun, M. Cao, and W. Wang, "Pursuing an evader through cooperative relaying in multi-agent surveillance networks," Automatica, vol. 83, pp. 155–161, Sep. 2017.
29. W. He, C. Xu, Q.-L. Han, F. Qian, and Z. Lang, "L2 leader–follower consensus of networked Euler–Lagrange systems with external disturbances," IEEE Trans. Syst., Man, Cybern., Syst., vol. 48, no. 11, pp. 1920–1928, Nov. 2018.
30. V. N. Coelho, M. W. Cohen, I. M. Coelho, N. Liu, and F. G. Guimarães, "Multi-agent systems applied for energy systems integration: State-ofthe-art applications and trends in microgrids," Appl. Energy, vol. 187, pp. 820–832, Feb. 2017.
31. X. Ge and Q.-L. Han, "Distributed formation control of networked multi-agent systems using a dynamic event-triggered communication mechanism," IEEE Trans. Ind. Elect 2017.
32. W. He, G. Chen, Q.-L. Han, and F. Qian, "Network-based leaderfollowing consensus of nonlinear multi-agent systems via distributed impulsive control," Inf. Sci., vol. 380, pp. 145–158, Feb. 2017.
33. D. H. Nguyen, T. Narikiyo, and M. Kawanishi, "Robust consensus analysis and design under relative state constraints or uncertainties," IEEE Trans. Autom. Control, vol. 63, no. 6, pp. 1784–1790, Jun. 2018.
34. J. Yu and Y. Shi, "Scaled group consensus in multiagent systems with first/second-order continuous dynamics," IEEE Trans. Cybern., vol. 48, no. 8, pp. 2259–2271, Aug. 2018.
35. M. Zhao, C. Peng, W. He, and Y. Song, "Event-triggered communication for leader-following consensus of second-order multiagent systems," IEEE Trans. Cybern., vol. 48, no. 6, pp. 1888–1897, Jun. 2018.
36. X. Ge, Q.-L. Han, and X.-M. Zhang, "Achieving cluster formation of multi-agent systems under aperiodic sampling and communication delays," IEEE Trans. Ind. Electron., vol. 65, no. 4, pp. 3417–3426, Apr. 2018.

37. F. Li, K. Shaung, and S. Su. Q-Peer: A Decentralized QoS Registry Architecture for Web Services. Accessed: Apr. 8, 2019. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-74974-5_12
38. I. Haq, R. Alnemr, A. Paschke, E. Schikuta, H. Boley, and C. Meinel. Distributed Trust Management for Validating SLA Choreographies. Accessed: Apr. 8, 2019. [Online]. Available: https://pdfs. semanticscholar.org/63d5/d7c90287b423534ea3d28d15fb6a8a0a5e55. Pdf
39. NxT–The Blockchain Application Platform. Accessed: Apr. 8, 2019. [Online]. Available: https://nxtplatform.org/
40. Y. Lu, "Blockchain and the related issues: A review of current research topics," J. Manage. Anal., vol. 5, no. 4, pp. 231–255, 2018.
41. Y. Lu, "Blockchain: A survey on functions, applications and open issues," J. Ind. Integr. Manage., vol. 3, no. 4, 2018, Art. no. 1850015.
42. H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Blockchain with Internet of Things: Benefits, challenges, and future directions," Int. J. Intell. Syst. Appl., vol. 10, no. 6, pp. 40–48, 2018.
43. M. H. Miraz and M. Ali, "Applications of blockchain technology beyond cryptocurrency," 2018, arXiv:1801.03528. [Online]. Available: https://arxiv.org/abs/1801.03528
44. S. Madumidha, P. SivaRanjani, S. Rajesh, and S. Sivajumar, "Blockchain security for Internet of Things: A literature survey," Int. J. Pure Appl. Math., vol. 119, no. 16, pp. 3677–3686, 2018.
45. Ibibo, J.T. (2024). A Bibliometric Analysis and Comprehensive Overview of Security Attacks Against RPL in IoT Networks. In: Tran, K.P., Li, S., Heuchenne, C., Truong, T.H. (eds) The Seventh International Conference on Safety and Security with IoT. SaSeIoT 2023. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-031-53028-9_4
46. C. Du, X. Liu, W. Ren, P. Lu, and H. Liu, "Finite-time consensus for linear multi-agent systems via event-triggered strategy without continuous communication,? IEEE Trans. Control Netw. Syst., DOI: 10.1109/TCNS.2019.2914409, 2019.
47. Ibibo, J.T., Japheth, B.R. (2024). RPL Protocol Using Contiki Operating Systems: A Review. In: Tran, K.P., Li, S., Heuchenne, C., Truong, T.H. (eds) The Seventh International Conference on Safety and Security with IoT. SaSeIoT 2023. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-031-53028-9_2
48. T. Liu and Z.-P. Jiang, "Event-based control of nonlinear systems with partial state and output feedback," Automatica, vol. 53, pp. 10–22, 2015.
49. L. Xing, C. Wen, Z. Liu, H. Su, and J. Cai, "Event-triggered output feedback control for a class of uncertain nonlinear systems," IEEE Trans. Autom. Control, vol. 64, no. 1, pp. 290–297, 2018.
50. X. Wang and M. D. Lemmon, "Event-triggering in distributed networked control systems," IEEE Trans. Autom. Control, vol. 56, no. 3, pp. 586– 601, 2011.
51. C. Nowzari, E. Garcia and J. Cort' es, "Event-triggered communication andcontrolofnetworkedsystemsformulti-agentconsensus",Automatica, vol. 105, pp. 1–27, 2019.
52. J. George, X. Yi and T. Yang, " Distributed robust dynamic average consensus with dynamic event-triggered communication," IEEE Conference on Decision and Control (CDC), pp. 434–439, 2018.
53. [53]C. Li, E. A. A. Coelho, T. Dragicevic, J. M. Guerrero, and J. C. Vasquez, "Multiagent-based distributed state of charge balancing control for distributed energy storage units in ac microgrids," IEEE Trans. Ind. Appl., vol. 53, no. 3, pp. 2369–2381, 2017.
54. L. Xing, Y. Mishra, Y.-C. Tian, G. Ledwich, C. Zhou, W. Du, and F. Qian, "Distributed state-of-charge balance control with eventtriggered
55. M. Sharma, H. Elmiligi, F. Gebali and A. Verma, "Simulating Attacks for RPL and Generating Multi-class Dataset for Supervised Machine Learning," 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2019, pp. 0020-0026, doi: 10.1109/IEMCON.2019.8936142. keywords: {Feature extraction; Routing protocols; Wireless sensor networks; Machine learning; Correlation; Routing; Cyber Physical System; WSN security; WSN attacks; Routing Protocol for Low power and Lossy net-works(RPL);Feature Reduction (FR);Feature Engineering (FE);Information Gain (IG);Correlation based feature selection (CFS)},

56. Mridula Sharma, Haytham Elmiligi, Fayez Gebali, Abhishek Verma, Simulating attacks for rpl and generating multi-class dataset for supervised machine learning, in: 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), IEEE, 2019, pp. 0020–0026.
57. Sarumathi Murali, Abbas Jamalipour, A lightweight intrusion detection for sybil attack under mobile RPL in the internet of things, IEEE Internet Things J. 7 (1) (2019) 379–388.
58. Zahrah A Almusaylim, Abdulaziz Alhumam, Wathiq Mansoor, Pushpita Chatterjee, Noor Zaman Jhanjhi, Detection and mitigation of RPL rank and version number attacks in smart internet of things, 2020

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.