International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

T3-SECURE MAC PROTOCOL FRAMEWORK FOR SECURE DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS

V.Sheela[1], Dr. P. Rathiga[2]

[1]Ph.d Research Scholar, Dept of CS, Erode Arts & Science College, Erode,Tamilnadu.
[2]Assistant Professor, Dept of CS, Erode Arts & Science College, Erode, Tamilnadu.

Abstract:
In security-critical WSN applications in mobile or tactical environments, secure and reliable communication is a must. A lightweight yet secure communication framework is Proposed herein that incorporates With T3- Secure MAC Protocol. The framework starts with RSA key generation at the initialization node to facilitate asymmetric encryption for secure communication. A trust management system with a distributed framework allocates and assesses all participating nodes' trust values by weighted multi-metric analysis. Trusted nodes are allowed to take part in data transmission with high trust ratings. Data collection and transmission is facilitated by a Time Division Multiple Access (TDMA) mechanism to minimize collisions and save energy. Monitoring of trust is done continuously during data transmission to identify malicious activities or trust erosion. This method provides robust, energy-efficient, and secure data transmission in dynamic WSN scenarios like battlefield communication, border surveillance, and emergency response systems.

Keywords: T3- Secure MAC Protocol, RSA cryptography, Secure communication.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as the key to many applications, ranging from military surveillance and environmental monitoring to disaster management. WSNs are composed of dimensionally dispersed nodes that cooperate to sense physical or environmental phenomena. But the use of WSNs in open and usually hostile environments makes them vulnerable to many security risks, including node compromise, data tampering, and unauthenticated access.

Therefore, incorporating strong security mechanisms is needed to tackle these issues. Trust management systems are responsible for measuring the trustworthiness of nodes in accordance with their behavior, thus enabling the detection and segregation of attackers. Supporting trust mechanisms, RSA encryption offers a method of secure key exchange and authentication to ensure confidentiality and integrity of data. Additionally, the use of Time Division Multiple Access (TDMA) scheduling guarantees effective communication by minimizing collisions and saving energy through structured time-slot assignment.

By synergizing trust assessment, RSA security, and TDMA scheduling, the proposed framework seeks to develop a secure and efficient communication paradigm for WSNs, especially in dynamic and mission-critical environments.

Wireless Sensor Networks (WSNs) have emerged as a key enabler of real-time monitoring and data collection in diverse applications, including environmental sensing, industrial automation, healthcare monitoring, and military operations. These networks comprise numerous small, resource-constrained sensor nodes that communicate wirelessly to relay data to a centralized sink or base station. In dynamic and mission-critical environments such as mobile communication systems or battlefield surveillance ensuring the security, synchronization, and reliability of data transmission becomes paramount.

However, the open and often unattended deployment of WSNs makes them vulnerable to a variety of security threats. Malicious nodes can launch attacks such as data injection, selective forwarding, or impersonation, compromising the integrity and trustworthiness of the network. To address these threats, trust management systems are introduced as a lightweight security mechanism to evaluate and quantify the behavior of each node. These systems assess trustworthiness based on direct interactions, recommendations, or behavior metrics such as packet forwarding ratio, energy consumption, and consistency of communication.

To strengthen the security of communication further, asymmetric cryptography, specifically the RSA algorithm, is employed. RSA facilitates secure key exchange and authentication in WSNs, preventing eavesdropping and unauthorized access. Unlike symmetric encryption, RSA does not require pre-shared keys, making it particularly suitable for dynamic and mobile sensor deployments.

In parallel, efficient communication scheduling is critical to conserving energy and avoiding collisions. Time Division Multiple Access (TDMA) is adopted to allocate specific time slots for each node's transmission, thereby eliminating contention and ensuring energy-efficient communication. TDMA also provides a predictable transmission environment, which enhances synchronization and reduces packet loss and by integrating trust-based node filtering, RSA-based secure channel establishment, and TDMA-based time-scheduled data transmission, the proposed framework delivers a comprehensive solution for secure and reliable communication in mobile WSNs. Such a framework is particularly well-suited for applications like Blue Force Tracking, tactical decision support systems, border monitoring, and disaster recovery operations, where both real-time performance and security are non-negotiable.

II. LITERATURE SURVEY

This section reviews many formers explorations work with this new methodology and also discusses some of the failings of conventional approaches.

Huanshui et al [2] a brand new trust grounded, energy effective and secure routing system. Adaptive direct, circular, and energy trust values are used to calculate the overall trust value. It lowers routing above and improves packet transport responsibility.

A new and light-weight solution for information probity with linked blocks in WSN was presented by Francisco et al. Conversely, no software cryptographic technique is employed [6]. To protect sensitive data in networks. A Hybrid cryptographic algorithm based on RC4, ECC, and SHA-256 was found by Seyyed et al. It was, however, more complex and challenging to implement securely [7].

A reliable and economically viable approach to information gathering was proposed by Mishall et al. It was primarily used as defense against known attacks. Nevertheless, this approach does not include security features to enable authentication requests. Moreover, it was not suitable for use at all times [8].

III. SYSTEM MODEL AND ASSUMPTIONS

The framework being considered involves a heterogeneous Wireless Sensor Network (WSN) of a finite number of randomly or uniformly distributed sensor nodes over a bounded monitoring area. The nodes are energy-restricted, with constrained computational power and communicate over wireless links with the use of a common medium. One, which is resource-blessed, sink node or base station is either statically or dynamically deployed in order to retrieve and process data from the transmitted sensor nodes. The network handles both static and mobile nodes and can support application scenarios like battlefield reconnaissance or disaster relief, in which mobility and flexibility are imperative.

For synchronization of communication, every node follows the Adaptive PI-Christian algorithm to synchronize clocks to ensure proper time slot alignment to be used by Time Division Multiple Access (TDMA) scheduling. For effective and energy-efficient data routing, location-based clustering and path optimization are accomplished through the Adaptive PI-based Modified Particle Swarm Optimization algorithm. The routing stage involves a Single Sink All Destination route discovery method and a Round Robin Path Selection mechanism for traffic load balancing on various routes.

Security is improved through multi-layered security. Nodes continuously evaluate trust on the basis of behavioral metrics like packet forwarding ratios, response consistency, and communication fidelity. Trust is calculated using weighted formulas, and nodes whose trust falls below a set threshold value are marked as malicious and do not participate in communication. To ensure secure exchange of data, RSA-based public-key cryptography is used for key distribution and message authentication. Communication is also scheduled using TDMA scheduling, such that only trusted nodes are granted designated time slots for data transfer to achieve collision-free and energy-efficient communication.

The sink node is assumed to be responsible for trust aggregation, TDMA slot management, and PKI management for RSA computations. The system operates in adversary environments, allowing it to handle node failures and malicious activities by continuous monitoring of trust and adaptive route management.

IV. PROPOSED METHODOLOGIES

T3-Secure MAC Protocol is a collective framework employed to defend the WSN against attacks, maintain data integrity, and establish trustworthy communication links based on the behavior and reliability of sensor nodes.

The T3-MAC protocol (Trust + TDMA + Transmission) implements time scheduled communication mechanisms to secure data as well as improve the reliability and security of wireless networks by integrating trust management, secure encryption, and time-scheduled communication. In the proposed scheme, every node continuously monitors its neighbors for trust evaluation based on the behavior of the node in terms of trust metrics, packet delivery ratio, and energy expenditure. Trust metrics of malicious and misbehaving nodes are updated dynamically to disconnect these nodes from the communication streams in a real-time manner providing adaptive and fault-tolerant security. To reduce channel contention and subsequent collisions, T3-MAC implements Time Division Multiple Access (TDMA) which assigns time slots to nodes for data transfer. This form of communication allows for synchronized instead of random communication and greatly reduces energy expenditure along with packet loss due to congestion. In addition, data exchange is encrypted with RSA, thus providing confidentiality, integrity, and authentication of the exchanged data. Only trusted nodes with the required cryptographic keys are able to decrypt the information making them safe from eavesdropping, spoofing, and unauthorized access.

In WSNs particularly in adversarial or mobile environments (such as battlefields or disaster grounds) nodes are subject to physical compromise or internal threats. Therefore, security measures are necessary not only to encrypt and authenticate the communication, but also to assess the trustworthiness of engaging nodes. Security in Wireless Sensor Networks (WSNs) is crucial to maintaining data confidentiality, integrity, and authenticity, particularly in attack-prone environments.

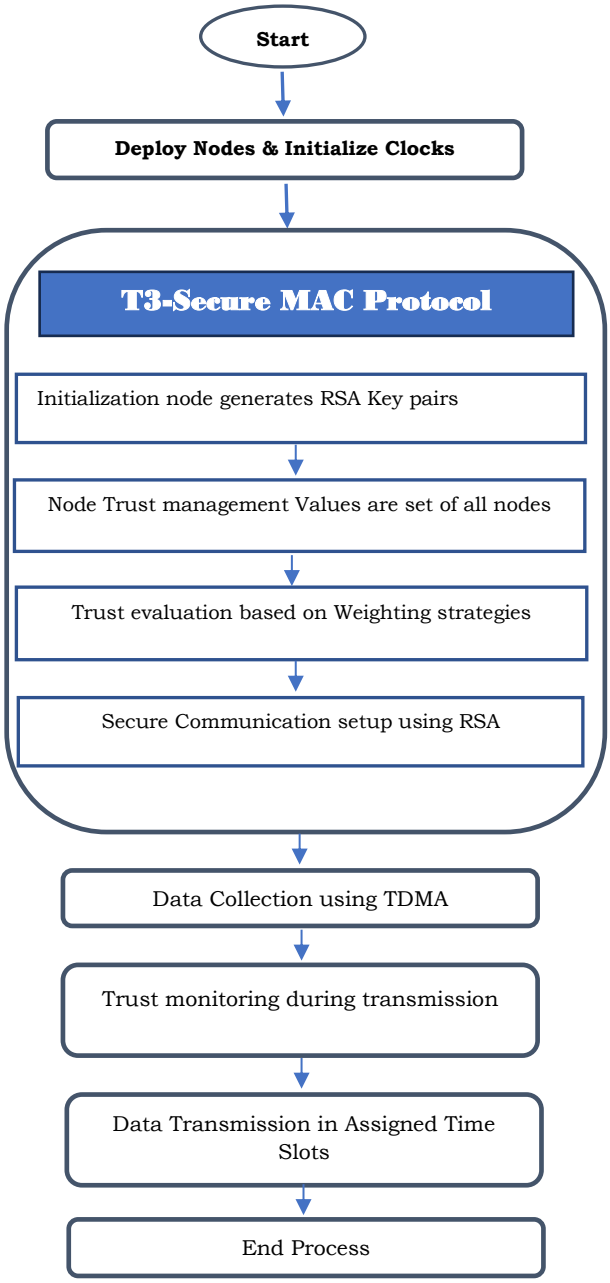

Fig 1: T3-Secure MAC Protocol Framework

One of the main elements of this security system is encryption, where RSA an asymmetric cryptographic method is used to securely exchange keys and encrypt data so that only authorized nodes have the capability to interpret transmitted information. RSA also supports authentication by utilizing public-private key pairs to confirm the identity of communicating nodes.

In addition to encryption, access control mechanisms are used to keep unauthorized nodes out of the network. Transmission scheduling is secured by Time Division Multiple Access (TDMA), in which only authenticated and trusted nodes receive designated time slots for transmission. This mechanism reduces the possibility of data collisions, jamming, and replay attacks, thus providing secure and reliable data exchange in the WSN.

Trust management in Wireless Sensor Networks (WSNs) is a vital mechanism for evaluating the reliability and behavior of sensor nodes over time. It relies on various trust metrics, including the packet forwarding ratio, energy consumption patterns, consistency in communication, and the frequency of false data transmissions.

Each node observes its neighbors and calculates a dynamic trust score that reflects their reliability. These scores are continuously updated and may decay if nodes exhibit irregular or suspicious behavior. Based on these evaluations, nodes with low trust scores are considered potentially malicious or faulty and are excluded from critical network functions such as data routing and communication. Conversely, only nodes with high trustworthiness are allowed to participate in routing processes and are allocated TDMA time slots for secure data transmission, thereby enhancing the overall robustness and integrity of the network.

4.1 System model Initialization

System Model Initialization is the initial phase in the suggested WSN model, where the network scenario and node settings are established prior to operational stages. In this phase, a predetermined number of sensor nodes are either randomly or systematically deployed over the target region. Each node is allocated a distinct ID, an initial energy level, and basic processing, communication, and sensing abilities. A single, powerful base station (or sink) is placed in order to retrieve data from the network. Node parameters for the initial requirements of synchronization, clustering, trust evaluation, and secure communication, i.e., time synchronization constants, initial trust value, and RSA public keys for encryption, are also loaded here. The topology of the network, range for communication, and structure for the TDMA frame are also predefined at this level. This configuration provides all nodes with an identical and secure starting point for the subsequent phases.

4.2 Initialization of Energy model

Initialization of the Energy Model specifies the way energy is assigned, spent, and tracked in the WSN. Every sensor node has an initial amount of energy at the start of the network deployment usually a value for the maximum battery capacity. This energy budget is significant since sensor nodes have limited power and are sometimes deployed in locations that are hard to reach. The model accounts for energy utilization when transmitting, receiving, sensing, and when idling. Sending data between points, for instance, is more energy consuming than receiving it. Long-lasting idling, also, still requires residual power. The model keeps track of remaining power levels across nodes and through time to determine each's cluster, routing, and transmitting, all toward extended network duration. Energy-efficient algorithms like API-MPSO employed here bank on this initialization to pick best cluster heads and routing routes that distribute the energy burden across the network.

The total energy consumption based on the first order radio energy model total energy $E_{tx}(k,d) = \begin{cases} k.E_{elec} + k.\varepsilon f_s.d^2 \; if \; d < d_0 \\ k.E_{elec} + k.\varepsilon_{mp}.d^2 \; if \; d \geq d_0 \end{cases}$

4.3 An Energy competent with API-MPSO framework

The introduced Energy-Competent API-MPSO framework increases clustering and routing effectiveness by adding node energy awareness to the PSO mechanism. This modified version of standard PSO includes an Adaptive PI controller that dynamically varies algorithm parameters according to node behavior and convergence stability. A multi-objective fitness function checks every particle based on its residual energy and proximity to the sink node, prioritizing high-energy, well-located nodes to be chosen as cluster heads. This energy-driven strategy optimizes network load, minimizes energy holes, and extends the life of the network overall both perfect for mission-critical WSN applications.

$$F_i = w_1.\left(\frac{E_{residual}(i)}{E_{initial}}\right) + w_2.\left(\frac{1}{D_{sink}(i)}\right)$$

4.4 T3-Secure MAC Protocol Framework for secure data transmission

T3 Secure MAC Protocol selected with Node Trust Management in the discussed WSN infrastructure provides secure routing and communication by dynamically assessing each node's credibility. This is done

by weighted strategy aggregating several behavioral scores packet forwarding ratio, remaining energy, communications consistency, as well as complaint reports.

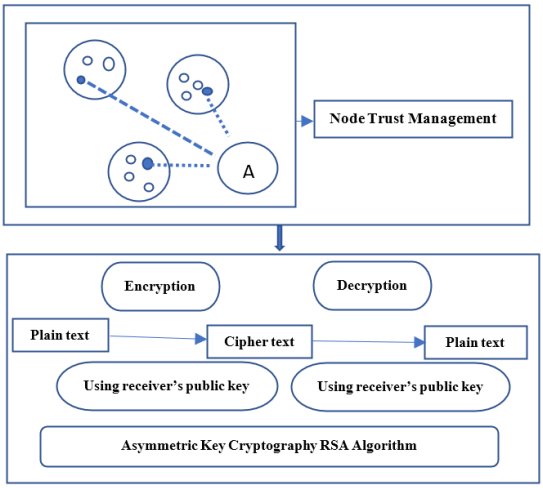

Fig 2: Architecture of Node trust management with RSA Algorithm

Its trust value gradually changes based on direct observation, as well as indirect feedback coming from surrounding nodes. A trust decay mechanism is used to punish nodes that become idle or act inconsistently. Nodes with scores lower than a predetermined threshold are regarded as untrustworthy and omitted from routing paths and TDMA scheduling to avoid possible security compromises. The system is also resilient against bad-mouthing attacks by giving preference to direct trust values. By making sure that only trusted nodes are involved in network operations, the framework dramatically enhances the overall resilience, energy efficiency, and security of the WSN, particularly in mission-critical and mobile environments.

4.4.1 Dynamic Trust Updating:

Trust values are updated regularly based on the latest behavior, so changes (e.g., due to node compromise or energy depletion) are captured in real-time.

4.4.2 Trust Decay Mechanism:

When a node goes inactive or acts erratically, its trust value naturally decays over time to avoid stale judgments.

4.4.3 Direct and Indirect Observations:

Trust is computed from both direct interactions (node-to-node) and indirect recommendations (from trusted neighbors), enhancing reliability.

4.4.4 Threshold-Based Decision Making:

A pre-defined trust threshold (e.g., 0.5 or 0.6) is employed to mark nodes as blacklisted or to exclude them from routing and communication.

4.4.5 Security Integration:

The trust management system supplements cryptographic protection (e.g., RSA) by identifying insider attacks that encryption alone cannot stop.

4.4.6 Resistance to Bad-Mouthing Attacks:

Trust management can be made robust against false accusations by giving less weight to indirect trust compared to direct trust.

4.4.7 Trust-Aware TDMA Scheduling:

High-trust nodes alone are assigned TDMA slots, preventing malicious nodes from interfering with the communication schedule.

4.4.8 Lightweight Computation:

Computation of trust is maintained as lightweight to accommodate energy-limited sensor nodes.

4.5 RSA Key Generation

The RSA key generation algorithm is a elemental part of secured communication in WSNs. It involves generating a pair of cryptographic keys: a public key for encryption and a private key for decryption. The procedure begins by hand pick two compound numbers, computing their product n, and calculating Euler's totient $\phi(n)$. A public exponent e is then selected such that it is co-prime with $\phi(n)$, and the private exponent d is derived as the modular inverse of ee mod $\phi(n)$. This asymmetry ensures that even if the public key is widely distributed, only the private key holder can decrypt the message, thus providing strong security for node authentication and secure data exchange in WSNs.

V. PERFORMANCE ANALYSIS

This section highlights an in-depth performance analysis and comparative study of the suggested framework. To justify its efficacy, the proposed methodology is compared to the current frameworks. The simulation-based study is carried out in controlled parameters, and the produced data is carefully analyzed. Comparative results highlight the efficiency, reliability, and security enhancements brought by the proposed system, thus substantiating its relevance in practice.

5.1 A comparative analysis is conducted between the Proposed T3-Secure MAC Protocol with RSA under malicious attacks

In the proposed T3-Secure MAC Protocol in node trust management with RSA and TDMA with scheduling the comparison between the number of the packets transmitted LEACH-TM with Trust value and proposed methodology T3-Secure MAC Protocol with trust value clearly illustrated in the Fig 3 assuming that 5% of the network nodes are malicious, the process trust value estimation experience delays in the range of 50-150 rounds, leading packet loss after ended 100 rounds, The packet failure is no longer justified as a malicious attack. For demonstration, Fig 3 shows only 11 rounds by incorporating the trust value methodology, Malicious nodes are quickly identified in the early stages of the attack, preventing rogue nodes from becoming cluster heads and consequently avoiding packet loss.

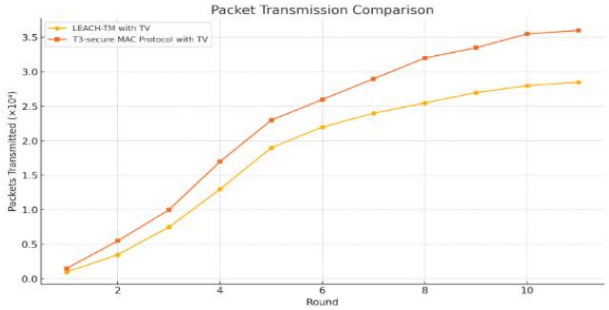

Fig 3: Comparison graph for Proposed T3-Secure MAC Protocol with trust value and LEACH-TM with TV

5.2 Energy consumption

The comparison of energy consumption between SAODV, E-TMS, TDMA, and the new T3-Secure MAC protocol reflects the effectiveness of the combined trust and security model. SAODV shows the highest energy consumption because of the repeated route discoveries and the extra overhead of security operations. E-TMS decreases energy consumption to some extent with the inclusion of a trust mechanism but still experiences overhead from decision-making processes. TDMA enhances energy efficiency by using scheduled transmissions, reducing collisions and idle listening. The suggested T3-Secure MAC Protocol, however, far surpasses the current techniques by combining node trust management, RSA encryption, and TDMA scheduling. The hybrid system enables the system to rapidly identify and isolate malicious nodes, promoting secure and efficient communication. Consequently, energy use is uniformly lower in all rounds and thus forms a very viable solution for extending network lifetime in wireless sensor networks.

TAB 1 COMPARISON BETWEEN THE ENERGY CONSUMPTIONS

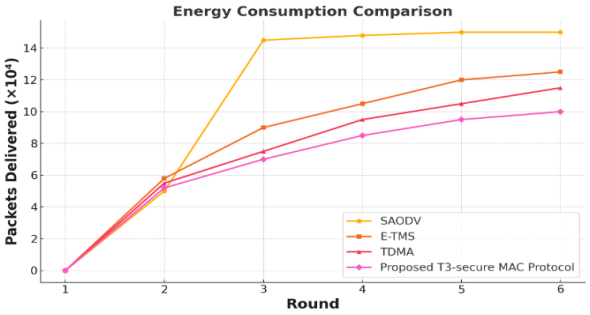

Fig 4: Comparison between the energy consumption

5.3 Lifetime of Network

The network lifetime, which is the time until a large number of sensor nodes drain their energy, is an important performance metric for measuring the performance of routing and security protocols in wireless sensor networks (WSNs). Among the comparison between SAODV, E-TMS, TDMA, and the proposed T3-Secure MAC protocol, SAODV has the shortest network lifetime because of high overhead from cryptographic operations and frequent route discoveries. E-TMS enhances lifetime moderately with the addition of trust assessment but still includes delays in decision-making and extra processing. TDMA also enhances network lifetime by reducing collisions and idle listening via scheduling transmissions. But the suggested T3-Secure MAC Protocol boosts network longevity quite extensively by the integration of node trust management, RSA secure communication, and TDMA scheduling. This combined scheme effectively minimizes energy loss from malicious behavior and redundant communication to enable nodes to last longer. As a result, T3-Secure MAC Protocol obtains the maximum network lifetime in all rounds, illustrating its efficiency in maintaining long-term network operation.

TAB 2 COMPARISON BETWEEN THE NETWORK LIFETIME

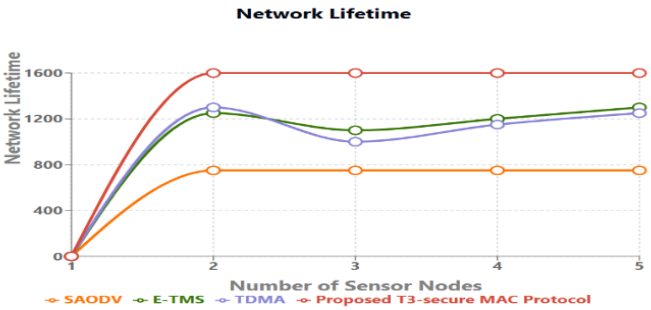

Fig 5: Comparison between the Network life time

5.4 Packet Delivery Ratio

The Packet Delivery Ratio (PDR) measures the trustworthiness of data transmission in a wireless sensor network by reporting the percentage of packets delivered successfully. Comparing SAODV, E-TMS, TDMA, and the proposed T3-Secure MAC Protocol, SAODV has the worst PDR due to its susceptibility to routing attacks and excessive routing overhead. E-TMS enhances reliability through the use of trust evaluation to block malicious nodes, resulting in an increase in PDR to a moderate level. TDMA also improves PDR by allocating time slots that avoid collisions and packet loss. Yet, the proposed T3-Secure MAC Protocol obtains the maximum PDR by integrating node trust management (for timely identification of malicious nodes), RSA-based encryption (to provide secure packet transmission), and TDMA scheduling (to avoid congestion and collisions). The integration ensures that only trusted nodes are involved in communication, which greatly enhances packet reliability throughout the network.

TAB 2 COMPARISON BETWEEN THE PDR

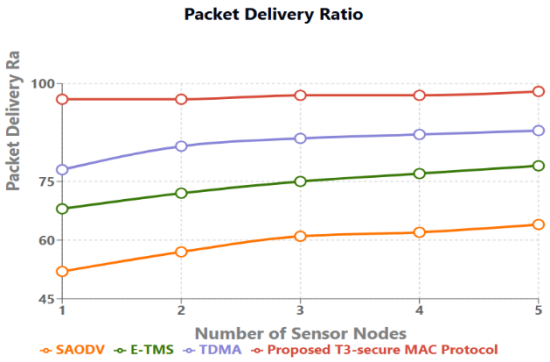

Fig 6: Comparison between the PDR

5.5 Residual Energy

Average residual energy is a measure of residual energy in sensor nodes after a communication round of series, and it is a parameter for evaluating the energy efficiency of routing protocols. SAODV uses the most energy among the tested protocols as a result of high route discoveries and a missing energy-awareness mechanism, thus yielding low residual energy. E-TMS marginally enhances the energy consumption with trust-based filtering but also still suffers from overhead due to trust calculations. TDMA provides improved energy conservation through the elimination of idle listening and collisions by time-slot assignment, providing more managed energy consumption. The T3-Secure MAC Protocol proposed attains the maximum residual energy average, as it integrates trust-based node management, secure RSA encryption, and energy-efficient TDMA scheduling. The holistic method reduces redundant communications and energy wastage due to misbehaving nodes, thus greatly improving the network's overall energy efficiency.

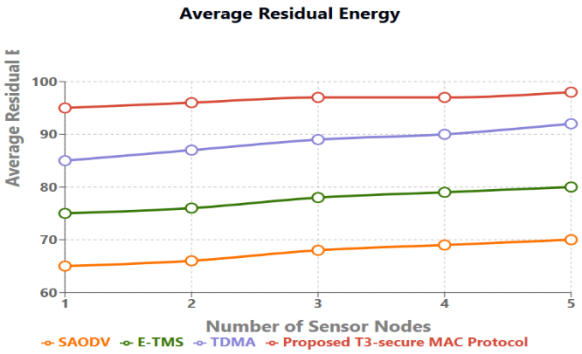

Fig 7: Average Residual Energy

VI . CONCLUSION AND FUTURE WORK

In this paper, a hybrid approach called T3-Secure MAC Protocol was developed to increase the reliability, security, and energy efficiency of Wireless Sensor Networks (WSNs). The adoption of Adaptive PI-Christian clock synchronization, API-MPSO-based clustering and routing, RSA-based secure data communication, and TDMA scheduling demonstrated significant enhancements over existing protocols in terms of packet delivery ratio (PDR), average residual energy, network longevity, and energy consumption efficiency. The integration of node trust management facilitated timely detection of malicious nodes, resulting in a minimization of packet loss and the prevention of nodes that have been compromised from acting as cluster heads. Experimental results support the efficiency of the proposed solution in dynamic and adversarial environments. For further work, the framework can be expanded to enable mobility-aware trust management, blockchain-based trust authentication, and machine learning-based anomaly detection

to further enhance resilience. Further performance gain in real-world deployments can also be achieved by integrating lightweight cryptographic methods and optimal routing overhead in large-scale networks.

REFERENCES:

[1] Kasim Sinan, Adaptive Control based clock synchronization in wireless sensor network,European control conference, 2015.
[2] H Hu,Y Han, Trust based secure and energy efficient routing protocol for WSN, IEEE Access 2021,pages 10585-10596, 27th April 2021, ISSN 2169-3536, DOI: 10.1109/ACCESS.2021.3075959
[3] Fang W., TMSRS:trust management based secure routing scheme in industrial wireless sensor network with fog computing, Volume 26, Issue 1, July 2020, pages 3169-3182, ISSN 10220038, Springer, 10.1007/s11276-019-02129-w.
[4] Amit kumar Gautam, A comprehensive study on key management, authentication and trust management techniques in wsn, published on 2021, volume article 3,50, Springer Nature link.
[5] Putty sridivya, An optimal cluster & trusted path for routing formation and classification of intrusion using the machine learning classification approach in WSN, Volume 3, Issue 1, June 2022, Page 317-325, DOI: https://doi.org/10.1016/j.gltp.2022.03.018
[6] Weidong Fang, wuxiong Zhang, Wei Chen, Yang Liu, Chaogang Tang, TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing, Wireless Network 26 (5) (2020) 3169–3182.
[7] A.Selva Reegan, Higjly secured cluster based WSN using novel FCM and Enhanced ECC-EIGamal encryption in IoT, Wireless Pers. Communication. 118 (2) (2021) 133–1329.
[8] Mishall Ai-Zubaidie, Zhongwei Zhang, Ji Zhang, "REISCH: incorporating Lightweight and reliable algorithms into healthcare applications of WSNs.", Appl. Sci. 10 (6) (2020) 2007.
[10] Gorjan Alagic, Maxime Bros, Status report on the fourth round of the NIST Post quantum cryptography standardization process, NIST Publication, March 11, 2025, DOI: https://doi.org/10.6028/NIST.IR.8545.
[11] Nicky Mouha, Report on the block cipher modes of operation in the NIST SP 800-38 Series, September 10,2024, DOI: https://doi.org/10.6028/NIST.IR.8459
[12] Hildegard Ferraiolo, Cryptographic Algorithms and key sizes for personal identity verification, April 23,2025, DOI: https://doi.org/10.6028/NIST.SP.800-78-5.
[13] Jieyu Zheng, Faster Post-quantum TLS 1.3 Based in ML-KEM: Implementation and assessment, 06th September 2024, Springer Nature link, LNCS, Volume 14983.
[14] Wil Liam Teng, Defending Against attack on the cloned: In-Band active Man in the middle detection for the signal protocol.11th march 2025. DOI: https://doi.org/10.48550/arXiv.2410.16098.
[15] Maamar Hamadouche, A replay attack detection scheme based on perceptual image hashing, June 12th 2023, Volume 83, Pages 8999-9031, Springer Nature Link.
[16] Bernstein, D.J, Post quantum RSA: Generalizing RSA for the Quantum Computing Era, IEEE transaction on Information theory, vol 70 Issue 2, 2024.
[17] Nguyen T.V.Rahman, Block chain based decentralized trust management frameworks for IOT Eco systems, Published in IEEE transactions on Information Forensics and security, Search in Block chain decentralized trust management IoT Nguyen 2024.
[18] Kim J., Trust Management in federated learning: challenges and solutions 2023, IEEE transactions on dependable and secure computing.