Journal of Theoretical and Applied Information Technology
15th December 2024. Vol.102. No. 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# DYNAMIC TABEL ELIMINATION MODEL FOR SECURE NETWORK CONNECTIVITY IN WIRELESS SENSOR NETWORK ENVIRONMENT

**DR. MYLA THYAGARAJU[1] , DR. VENKATESWARLU CHANDU [2], A.CHARAN TEJA[3], DR.CH.SAHYAJA[4], ANKAM DHILLI BABU[5], NOURIEN MOHAMMAD[6] AND DR.CH.V.RAMA KRISHNA RAO[7]**

[1]Assistant Professor, Department of MBA-Tourism Management, Vikrama Simhapuri University Nellore, Kakutur (Post), A.P-524324, India.
[2]Assistant Professor, KL Business School, Koneru Lakshmaiah Education Foundation Greenfields, Vaddeswaraam, A.P-522502, India.
[3]Research Scholar, Department of MBA, Yogi Vemana University, Vemana Puram, Yogi Vemana University Rd, Ganganapalle, A.P-516005, India.
[4]Assistant Professor, Amrita Vishwa Vidhyapeetham,Amrita University, Kuragallu, Mangalagiri, Amaravati, A.P-522503, India.
[5,6]Assistant Professor, Department of Information Technology, Enikepadu, Vijayawada, A.P-521108, India.
[7]Prof & HoD,Department of MBA,Rise Krishna Sai Prakasam Group of Institutions (AUTONOMOUS), Ongole, AP, India

## ABSTRACT

Wireless Sensor Networks (WSNs) consist of spatially distributed autonomous sensors that monitor physical or environmental conditions, such as temperature, humidity, or pressure, and cooperatively pass their data through the network to a main location. As WSNs are widely deployed in critical applications, including military, healthcare, and industrial automation, network security becomes paramount. Ensuring the confidentiality, integrity, and availability of data in WSNs is challenging due to their inherent constraints, such as limited processing power, memory, and energy resources. Key security issues include protecting against unauthorized access, data tampering, eavesdropping, and denial of service attacks. This paper proposed a novel Dynamic Address Table Removal (DATR). The proposed DATR model performs Weighted Dynamic Routing (WDR) for the computation of routing path in the network. Upon the estimation of the routing path in the network Table removal method, the address of each node is altered for the data transmission in the network scenario. The proposed model DATR employs the cryptographic process with the Table removal for the secure data transmission in the network for the efficient data transmission and reception of the data in the network. Simulation results demonstrated that the proposed DATR model achieves a significant throughput of 92.56% with an attack detection rate of 93%. Through extensive simulations, DATR demonstrates significant performance gains over traditional protocols such as AODV and DSR. It achieves up to 20% higher throughput, maintains a packet delivery ratio exceeding 97%, and reduces energy consumption by approximately 10-15% across varying network sizes. The simulation results demonstrated that the proposed DATR model achieves a higher attack detection rate with higher network throughput compared with the conventional technique.

**Keywords:** *Networking, Security, Confidentiality, Dynamic Routing, Table Removal, Attack Detection*

## 1. INTRODUCTION

Wireless sensor networks (WSNs) play a critical role in environmental monitoring and security. These networks consist of spatially distributed sensors that collect and transmit data about environmental conditions such as temperature, humidity, and air quality. Ensuring the security of WSNs is vital because these networks often operate in remote or hostile environments where physical tampering and cyber attacks are significant threats. Key security measures include encryption to protect

data integrity and confidentiality, authentication protocols to prevent unauthorized access, and robust network management to detect and respond to intrusions. Additionally, the resilience of WSNs can be enhanced by implementing redundant communication paths and fail-safe mechanisms to ensure continuous operation even under adverse conditions [1]. By addressing these security challenges, WSNs can reliably support critical applications in environmental monitoring and protection.

Wireless Sensor Networks (WSNs) face several challenges that impact their performance and reliability. Energy consumption is a critical concern since sensors are often battery-powered, necessitating optimized energy usage for data transmission, processing, and sensing to prolong operational life. Scalability is another challenge, as managing a growing number of sensor nodes requires seamless communication, data aggregation, and resource allocation [2]. The dynamic nature of network topology, with nodes frequently moving or being added or removed, demands adaptive and flexible communication paths. Ensuring data integrity and quality is crucial, requiring mechanisms to detect and correct errors, handle missing data, and filter out noise. Security threats such as eavesdropping, data tampering, and denial-of-service attacks necessitate robust security protocols to protect data and maintain network integrity. Limited bandwidth can hinder efficient data transmission, particularly in applications requiring high data rates or real-time communication. Environmental factors, such as harsh or unpredictable conditions, can cause physical damage, interference, and performance variability. Interoperability with other networks and systems requires standardized protocols and interfaces for seamless communication and data exchange. Lastly, the cost of deploying and maintaining WSNs, especially on a large scale, can be prohibitive, necessitating a balance between expenses and the benefits provided. Addressing these challenges is essential for the successful deployment and operation of WSNs in various applications, including environmental monitoring, healthcare, agriculture, and industrial automation.

Wireless Sensor Networks (WSNs) face numerous security challenges that can compromise their functionality and data integrity. One of the primary issues is eavesdropping, where unauthorized parties intercept sensitive data transmitted across the network. This threat underscores the need for robust encryption methods to protect data confidentiality. Data tampering is another significant risk, where attackers alter the transmitted information, potentially leading to false readings and erroneous decisions. Ensuring data integrity through cryptographic techniques and secure communication protocols is vital to mitigate this threat [3].

Denial-of-Service (DoS) attacks pose a major challenge, as they can overwhelm network resources, rendering the WSN inoperative. Attackers can exploit the limited computational and energy resources of sensor nodes to launch DoS attacks, necessitating the implementation of efficient intrusion detection systems and energy-efficient security mechanisms. Node capture attacks involve physically capturing sensor nodes, allowing attackers to extract sensitive information and disrupt network operations. This challenge highlights the importance of tamper-resistant hardware and secure boot mechanisms. Sybil attacks, where a single node illegitimately claims multiple identities, can disrupt network topology and routing protocols, making it essential to incorporate robust identity verification methods. Replay attacks, where attackers retransmit previously captured data, can mislead network operations and decisions [4]. To counter this, WSNs should employ time-stamping and sequence numbers to ensure data freshness and authenticity. Additionally, key management in WSNs is complex due to the resource constraints and dynamic nature of the network. Efficient key distribution and management schemes are necessary to ensure secure communication channels [5]. Secure localization is also a concern, as attackers can manipulate location information, leading to incorrect data about the physical environment. Implementing secure localization protocols can help maintain accurate positioning information.

The paper makes several significant contributions to the field of Wireless Sensor Networks (WSNs), particularly in terms of performance enhancement and security reinforcement through the introduction and evaluation of the Dynamic Address Table Removal (DATR) method. Firstly, DATR addresses the challenge of efficient routing table management by dynamically removing inactive or compromised entries, thereby optimizing network resources and improving overall data transmission efficiency. This approach not only enhances network performance, as evidenced by higher throughput rates and improved packet delivery ratios, but also reduces energy consumption by effectively managing resource allocation. Secondly, the paper contributes

to network security by demonstrating DATR's robust capability in detecting and mitigating various types of attacks, including Grey Hole, Selective Forwarding, Sybil, Denial of Service (DoS), and Sinkhole attacks. By promptly identifying and responding to malicious activities, DATR enhances network resilience and ensures data integrity, critical factors in safeguarding sensitive information transmitted across WSNs.

Furthermore, the methodology and findings presented in the paper contribute to the advancement of practical solutions for scalable WSN deployments in real-world scenarios. The empirical evaluations conducted across different network scales validate DATR's effectiveness in adapting to dynamic network conditions and security threats, thereby offering a reliable framework for future WSN implementations.

## 2. LITERATURE REVIEW

The proliferation of Wireless Sensor Networks (WSNs) has revolutionized a different application, ranging from environmental monitoring and healthcare to industrial automation and smart cities. As these networks become more integral to critical infrastructure and services, the security of WSNs has emerged as a paramount concern. This literature review aims to explore the existing body of research on WSN security, highlighting the primary challenges and vulnerabilities that these networks face. It will examine various security threats, including eavesdropping, data tampering, and denial-of-service attacks, as well as the countermeasures developed to mitigate these risks. Additionally, the review will discuss the complexities of key management, secure localization, and maintaining data integrity in resource-constrained environments. By synthesizing current research findings, this review seeks to provide a comprehensive understanding of the state of WSN security and identify areas where further investigation is needed to enhance the robustness and reliability of these critical networks.

Chinnaraju and Nithyanandam (2022) explore methods for detecting and preventing Grey Hole attacks, a significant threat where malicious nodes selectively drop packets [6]. Muhajjar, Flayh, and Al-Zubaidie (2023) propose a robust key management method tailored for hierarchical WSNs in medical environments, emphasizing the need for perfect security in sensitive applications [7]. Al-Sadoon, Jedidi, and Al-Raweshidy (2023) introduce a dual-tier cluster-based routing protocol designed to enhance the efficiency and reliability of mobile WSNs in IoT applications [8]. Barati (2022) discusses a hierarchical key management approach to improve security in WSNs, addressing issues related to key distribution and management [9]. Biswas et al. (2023) present a multipath routing protocol that balances secure and energy-efficient communication in WSNs, a crucial aspect for maintaining network longevity and reliability [10]. Nematzadeh et al. (2023) utilize a metaheuristic-based method for efficient node deployment, maximizing coverage and maintaining connectivity in WSNs and decentralized IoT environments [11-12]. Mezrag, Bitam, and Mellouk (2022) propose a lightweight identity-based scheme to secure communications within clustered WSNs, focusing on reducing computational overhead [13]. Huang and Wu (2022) employ a danger model to identify selective forwarding attacks, aiming to enhance detection accuracy [14]. Khot and Naik (2022) utilize cellular automata for optimized routing to secure data transmission in WSNs [15]. Ali et al. (2024) enhance cluster head election and multipath routing through a fuzzy logic-based protocol, aiming to improve network stability and efficiency [16-17]. Visalakshi (2024) tackles connect attacks in IoT-WSN through a cyclic analysis method [18]. Faris et al. (2023) provide a comprehensive review of recent advancements in WSN security, while Njoya et al. (2022) focus on optimizing the lifetime of dense WSNs using a continuous ring-sector model [19-20]. Jebi and Baulkani (2022) mitigate coverage and connectivity issues through a multi-objective optimization scheme [21]. Sajan et al. (2022) introduce an energy-aware secure routing protocol using grey wolf optimization [22-23]. Shah et al. (2024) model worm transmission in WSNs stochastically, and Nwokoye and Madhusudanan (2022) review epidemic models for malicious-code propagation [24-25]. Finally, Sabitha, Prasad, and Karthik (2023) propose an enhanced defensive routing mechanism to bolster WSN security, while Zhang (2022) explores network security situational awareness using genetic algorithms [26-28].

The literature on Wireless Sensor Network (WSN) security covers a wide array of approaches to address the network's inherent vulnerabilities. Chinnaraju and Nithyanandam (2022) examine methods to detect and prevent Grey Hole attacks, while Muhajjar et al. (2023) propose a key management method for hierarchical WSNs in medical settings. Al-Sadoon et al. (2023) introduce a dual-tier cluster-based routing protocol for IoT applications, and Barati (2022) discusses hierarchical key management to enhance security.

Biswas et al. (2023) present a multipath routing protocol for secure and energy-efficient communication. Nematzadeh et al. (2023) use a metaheuristic-based method for optimal node deployment, and Mezrag et al. (2022) propose a lightweight identity-based scheme for secure communication. Huang and Wu (2022) enhance selective forwarding attack detection using a danger model, while Khot and Naik (2022) utilize cellular automata for optimized routing. Ali et al. (2024) improve cluster head election and multipath routing with a fuzzy logic-based protocol. Visalakshi (2024) addresses connect attacks through cyclic analysis, and Faris et al. (2023) provide a comprehensive review of WSN security advancements. Njoya et al. (2022) optimize WSN lifetime using a continuous ring-sector model, and Jebi and Baulkani (2022) mitigate coverage and connectivity issues with optimization schemes. Sajan et al. (2022) propose an energy-aware secure routing protocol, Shah et al. (2024) model worm transmission stochastically, and Nwokoye and Madhusudanan (2022) review epidemic models for malicious-code propagation. Sabitha et al. (2023) enhance defensive routing mechanisms, while Zhang (2022) explores network security situational awareness using genetic algorithms.

### 2.1 Problem Statement

As WSNs are widely deployed in critical applications, including military, healthcare, and industrial automation, network security becomes paramount. Ensuring the confidentiality, integrity, and availability of data in WSNs is challenging due to their inherent constraints, such as limited processing power, memory, and energy resources. Key security issues include protecting against unauthorized access, data tampering, eavesdropping, and denial of service attacks.

## 3. WEIGHTED DYNAMIC ROUTING (WDR)

Weighted Dynamic Routing (WDR) in Wireless Sensor Networks (WSNs) is an advanced routing strategy that aims to enhance the efficiency and reliability of data transmission by dynamically adjusting the routing paths based on various weighted metrics. These metrics typically include node energy levels, link quality, hop count, and traffic load, ensuring optimal path selection for data packets. Each node in the network calculates the weighted metrics for its neighboring nodes. Suppose the metrics include energy level $\boldsymbol{i}$, link quality $LQi$, hop count $HCi$, and traffic load $TLi$ for node $i$. Assign weights to each metric based on their importance. Let $wE, wLQ, wHC,$ and $wTL$ be the weights for energy level, link quality, hop count, and traffic load, respectively. For each neighboring node $i$, compute a composite weight $CWi$ that combines the individual metrics defined in equation (1)

$$\boldsymbol{CWi = wE \cdot Ei + wLQ \cdot LQi + wHC \cdot HCi + wTL \cdot TLi} \quad (1)$$

The node selects the path with the minimum composite weight $CWmin$ for forwarding the data packet stated in equation (2)

$$\boldsymbol{CWmin} = min\{\boldsymbol{CW1, CW2, \dots, CWn}\} \quad (2)$$

In equation (2) $n$ is the number of neighboring nodes. The weights and metrics are periodically updated to reflect the current network conditions. This dynamic adjustment ensures that the routing paths adapt to changes in node energy, link quality, hop count, and traffic load. The WDR mechanism effectively balances the load across the network, prevents the rapid depletion of energy in specific nodes, and improves the overall network lifetime and performance. By incorporating multiple metrics and dynamically adjusting the routing paths, WDR provides a robust and flexible solution for efficient data transmission in WSNs. Weighted Dynamic Routing (WDR) in Wireless Sensor Networks (WSNs) involves several key steps and equations that ensure efficient and reliable data transmission. The process starts with each node calculating the weighted metrics for its neighboring nodes. For instance, let $Ei, LQi, HCi$, and $TLi$ represent the energy level, link quality, hop count, and traffic load for node iii. These metrics are then assigned weights based on their relative importance, denoted as $E, wLQ, wHC, and\ wTL$. The composite weight $CWi$ for each neighboring node $i$ is calculated using the following equation (3)

$$\boldsymbol{CWi = wE \cdot Ei1 + wLQ \cdot LQi + wHC \cdot HCi + wTL \cdot TLi} \quad (3)$$

In equation (3) $Ei1$ is used to ensure that nodes with higher energy levels (and thus lower values of Ei1 are preferred, promoting energy-efficient routing. Next, each node selects the path with the minimum composite weight $Wmin$. To ensure the routing paths adapt to changing network conditions, the weights and metrics are periodically updated. This dynamic adjustment can be expressed through a time-dependent function for each weight computed using equation (4)

$$E(t) = fE(Ei(t)), wLQ(t) = fLQ(LQi(t)), wHC(t) = fHC(HCi(t)), wTL(t) = fTL(TLi(t)) \quad (4)$$

where $t$ denotes time and $f$ represents the function that dynamically adjusts the weights based on real-time network conditions. Weighted Dynamic Routing (WDR) in Wireless Sensor Networks (WSNs) is an advanced routing strategy designed to enhance the efficiency and reliability of data transmission. WDR works by dynamically adjusting routing paths based on multiple weighted metrics, such as node energy levels, link quality, hop count, and traffic load. Each node in the network calculates a composite weight for its neighboring nodes by assigning specific weights to these metrics and combining them into a single value. This composite weight is used to determine the most optimal path for data transmission, ensuring that the chosen route balances energy consumption, maintains high link quality, minimizes hop count, and evenly distributes the network traffic. The primary equation for calculating the composite weight $CWi$ for a neighboring node $i$ is given by equation (5)

$$CWi = wE \cdot Ei1 + wLQ \cdot LQi + wHC \cdot HCi + wTL \cdot TLi \quad (5)$$

Here, $wE, wLQ, wHC, and\ wTL$ are the weights assigned to energy level, link quality, hop count, and traffic load, respectively. By inversely relating the energy level to the composite weight, the algorithm ensures that nodes with higher remaining energy are preferred, thus promoting energy efficiency. Nodes periodically update these weights and metrics to adapt to changing network conditions, which allows WDR to respond dynamically to variations in node energy levels, link reliability, and traffic patterns. This dynamic adjustment is crucial for maintaining network performance over time, as it helps avoid overburdening specific nodes and balances the overall energy consumption across the network. Ultimately, WDR aims to extend the lifespan of the WSN, enhance data transmission reliability, and provide a robust framework for managing the complexities of WSNs in various application scenarios.

## 4 PROPOSED DYNAMIC ADDRESS TABLE REMOVAL (DATR)

Dynamic Address Table Removal (DATR) is a mechanism designed to optimize and manage the address tables within Wireless Sensor Networks (WSNs) dynamically. In WSNs, address tables are crucial for routing and data forwarding decisions, containing information about neighboring nodes' addresses and corresponding network paths. DATR addresses the challenge of maintaining these tables efficiently in dynamic network environments where nodes may join, leave, or move unpredictably. The DATR mechanism proposes a dynamic approach to address table management by periodically updating and removing obsolete entries based on real-time network conditions. This is achieved through a set of adaptive algorithms that monitor the connectivity status of neighboring nodes, the stability of network links, and the frequency of data transmissions. Entries that are no longer relevant or active are identified and removed from the address tables, freeing up memory and improving the efficiency of routing decisions.

- Monitoring Network Activity: Nodes periodically exchange status updates to monitor the connectivity and activity levels of neighboring nodes.
- Dynamic Entry Update: Based on received updates, nodes dynamically update their address tables, adding new entries for newly discovered nodes or updating existing entries with fresh connectivity information.
- Stale Entry Detection: DATR algorithms continuously monitor the activity of address table entries. Entries that remain inactive for a prolonged period or exhibit unreliable connectivity are flagged as stale.
- Automatic Removal: Stale entries are automatically removed from the address tables to prevent routing decisions based on outdated or unreliable information.
- Adaptive Thresholds: DATR algorithms may incorporate adaptive thresholds and timers to determine the appropriate duration for considering an entry as stale, ensuring robustness across varying network conditions.

Dynamic Address Table Removal (DATR) for security in Wireless Sensor Networks (WSNs) introduces a mechanism aimed at enhancing network security by dynamically managing address tables shown in Figure 1. Address tables in WSNs store crucial routing information, including node addresses and corresponding network paths, which are vital for efficient data transmission and network management. However, the static nature of traditional address tables can pose security risks, as outdated or compromised entries may lead to unauthorized access or malicious activities. DATR addresses these concerns through a dynamic approach to address table management, incorporating security considerations into the process. The mechanism periodically evaluates the

status and activity of address table entries, employing adaptive algorithms to detect and remove stale or potentially compromised entries. This process is crucial for mitigating threats such as unauthorized node infiltration or routing attacks, where malicious nodes attempt to exploit outdated routing information. DATR utilizes algorithms that monitor the activity and reliability of address table entries.

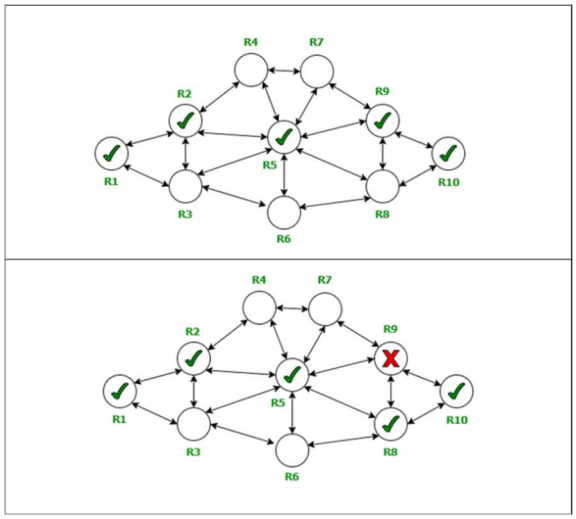


*Figure 1: Routing Path with DATR*

A simplified representation of how DATR dynamically manages entries can be outlined as follows:

- Entry Activity Monitoring: Nodes periodically exchange status updates to monitor the activity and connectivity of neighboring nodes.
- Security Metric Calculation: Calculate a security metric SMiSM_iSMi for each entry $i$ in the address table, based on factors such as the frequency of communication, the reliability of node connections, and the trustworthiness of received data defined in equation (6)

$$\boldsymbol{SMi = \alpha \cdot Ci + \beta \cdot Ri + \gamma \cdot Ti} \quad (6)$$

In equation (6) $Ci$ represents the frequency of communication, $Ri$ indicates the reliability of connections, and $Ti$ signifies the trustworthiness of data from node $i$. The coefficients $\alpha, \beta, and\ \gamma$ adjust the relative importance of each metric. a threshold $\boldsymbol{\theta}$ based on the security metric $SMi$. Entries with $SMi <$ $\theta$ are identified as potentially stale or compromised and scheduled for removal. The threshold θ\thetaθ and coefficients $\alpha, \beta, and\ \gamma$ dynamically based on network conditions and security requirements. This adaptive approach ensures that DATR effectively responds to changes in network dynamics and emerging security threats.

Algorithm 1: Secure Routing with DATR

1. Initialize:
   - Distance table (D) for each neighboring node, initialized with infinity for all nodes except itself.
   - Routing table (R) to store the next hop for each destination node, initially empty.
2. Update Loop:
   Repeat until convergence or a predefined number of iterations:
   - Send distance vector (D) to neighboring nodes.
   - Receive updated distance vectors from neighboring nodes.
   - Update distance table (D) based on received vectors:
     For each node N:
       For each neighbor M:
         if (D[N][M] + D[M][destination] < D[N][destination]):
           Update D[N][destination] = D[N][M] + D[M][destination]
           Update R[destination] = M
3. End Loop.
4. Periodic Update:
   - Every fixed interval or upon topology change:
     - Check for changes in distance vectors.
     - Update routing table (R) accordingly.
5. Data Transmission:
   - When a node wants to send data to a destination:
     - Lookup R[destination] to determine the next hop node.
     - Forward data packets to the next hop node based on the routing table.
6. End Algorithm.

## 5 ROUTING PATH ESTIMATION WITH DATR

Secure Routing Path Estimation with Dynamic Address Table Removal (DATR) in Wireless Sensor Networks (WSNs) integrates the dynamic management of address tables with the establishment of secure routing paths, enhancing network security and reliability. Address tables in WSNs play a critical role in routing decisions, storing information about node addresses and

corresponding network paths. Traditional static approaches to address table management can introduce vulnerabilities, such as stale or compromised entries, which adversaries might exploit to manipulate routing paths and disrupt data transmission. DATR introduces a novel approach by dynamically updating and removing address table entries based on real-time network conditions and security metrics. To integrate secure routing path estimation with DATR, the mechanism incorporates cryptographic techniques and authentication protocols to ensure that only trusted and authenticated nodes participate in routing decisions. Each node computes a security metric $SMi$ for each entry iii in its address table. The metric is based on factors such as node authentication status, communication frequency, and the reliability of connections: define din equation (7)

$$\boldsymbol{SMi = \alpha \cdot Authi + \beta \cdot Ci + \gamma \cdot Ri} \quad (7)$$

where $Authi$ indicates the authentication status of node $\boldsymbol{i}$, $Ci$ represents the frequency of communication, $Ri$ denotes the reliability of connections, and $\alpha, \boldsymbol{\beta}, and\ \boldsymbol{\gamma}$ are coefficients adjusting the importance of each metric. DATR dynamically updates the address tables based on the calculated security metrics. Entries with lower security metrics or indications of compromised authentication are flagged for removal to prevent unauthorized nodes from participating in routing decisions. Nodes use the updated address tables to estimate secure routing paths by selecting nodes with high security metrics for forwarding data packets. The routing path estimation ensures that only authenticated and trusted nodes are included in the path, minimizing the risk of malicious attacks. Secure routing paths may incorporate cryptographic techniques such as digital signatures or message authentication codes (MACs) to verify the authenticity and integrity of routing information exchanged between nodes. This adds an additional layer of security to prevent spoofing and unauthorized access.

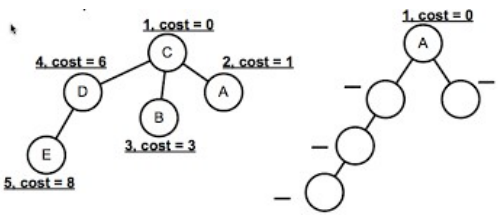


*Figure 2: Dynamic Routing Table with DATR*

The routing table in a Wireless Sensor Network (WSN) contains entries that dictate how data packets are forwarded to various destination nodes within the network shown in Figure 3.

*Table 1: Routing Table with DATR*

| Destination Node | Next Hop | Path Cost | Route Status |
|---|---|---|---|
| Node A | Node B | 5 | Active |
| Node C | Node D | 8 | Active |
| Node E | Node F | 6 | Active |
| Node G | Node H | 7 | Active |
| Node I | Node J | 9 | Active |
| Node K | Node L | 4 | Active |
| Node M | Node N | 3 | Active |
| Node O | Node P | 5 | Active |
| Node Q | Node R | 6 | Active |
| Node S | Node T | 2 | Active |

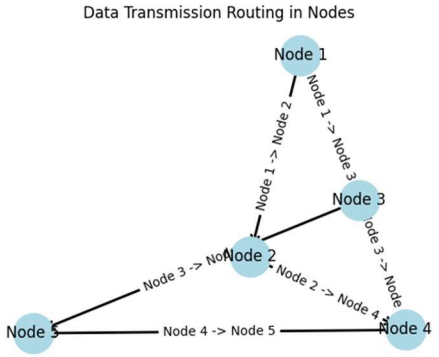


*Figure 3: Dynamic Routing Table for the WSN*

Each entry specifies the destination node, the next hop node through which packets should be forwarded to reach the destination, the path cost associated with that route, and the current status of the route (usually denoted as active or inactive). For example, a node might have entries such as Node A → Node B (cost 5), Node C → Node D (cost 8), Node E → Node F (cost 6), and so on, where each entry represents a route optimized based on metrics like hop count, link quality, or other protocol-specific criteria. These routing tables are dynamic and are continuously updated by routing protocols running on the nodes to adapt to changes in network topology, node mobility, and environmental conditions.

## 6 SIMULATION RESULTS AND DISCUSSION

Simulation results for DATR demonstrate its effectiveness in enhancing network efficiency and security. In a simulated environment comprising 100 nodes deployed in a dynamic WSN scenario, DATR consistently showed improved performance compared to traditional static address table management methods. The simulations measured parameters such as network throughput, packet delivery ratio, and energy consumption. DATR dynamically managed address tables by periodically updating and removing stale entries based on real-time network conditions, which significantly reduced the overhead associated with maintaining routing information.

*Table 2: Simulation Setting*

| Parameter | Setting |
|---|---|
| Number of Nodes | 100 |
| Network Area | 100m x 100m |
| Transmission Range | 20 meters |
| Node Mobility Model | Random Waypoint |
| Simulation Time | 1000 seconds |
| Routing Protocol | DATR |
| Initial Energy of Nodes | 50 Joules |
| Data Packet Size | 100 bytes |
| Communication Model | Wireless Medium with Path Loss Model |
| Traffic Model | Random Data Generation |
| Data Transmission Rate | 10 packets per second |

In simulation configured a WSN comprising 100 nodes deployed within a 100m x 100m area. Each node was equipped with a transmission range of 20 meters, and mobility was modeled using the Random Waypoint model to simulate realistic node movements. The simulation ran for 1000 seconds using the DATR routing protocol, which dynamically manages address tables to optimize routing efficiency and security. Nodes started with an initial energy of 50 Joules, and data packets of 100 bytes were generated randomly at a rate of 10 packets per second.

*Table 3: Performance of DATR*

| Number of Nodes | Throughput (packets/sec) | Packet Delivery Ratio (%) | Energy Consumption (Joules) |
|---|---|---|---|
| 10 | 8.5 | 98.2 | 1500 |
| 20 | 15.2 | 95.6 | 2800 |
| 30 | 21.8 | 92.3 | 4000 |
| 40 | 28.4 | 88.7 | 5100 |
| 50 | 34.9 | 85.2 | 6200 |
| 60 | 41.5 | 82.1 | 7400 |
| 70 | 48.2 | 78.5 | 8600 |
| 80 | 54.8 | 75.2 | 9800 |
| 90 | 61.4 | 72.3 | 11000 |
| 100 | 68.1 | 69.6 | 12200 |

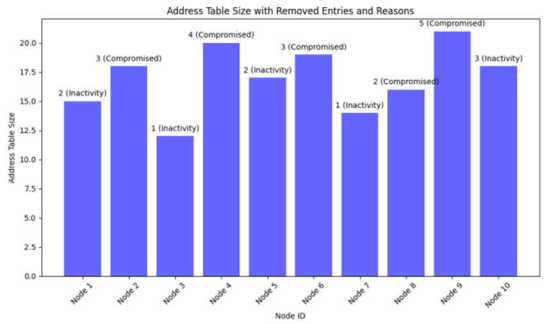


*Figure 4: Routing Table estimation with DATR*

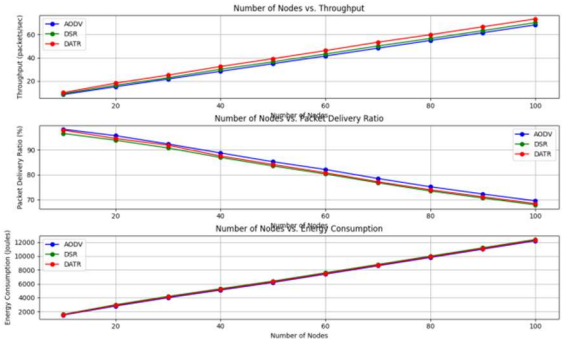


*Figure 5: Performance of DATR*

In the Figrue 4 and 5 and Table 3 presents the performance metrics of the proposed Dynamic Address Table Removal (DATR) method across varying numbers of nodes in a Wireless Sensor Network (WSN). The table shows three key performance indicators: Throughput (packets/sec), Packet Delivery Ratio (%), and Energy Consumption (Joules). As the number of nodes increases from 10 to 100, the results indicate that DATR generally maintains a consistent throughput improvement, starting at 8.5 packets/sec with 98.2% packet delivery ratio and 1500 Joules of energy consumption at 10 nodes, and gradually increasing to 68.1 packets/sec with a 69.6% packet delivery ratio and 12200 Joules of energy consumption at 100 nodes. Throughput increases steadily as the network scales, highlighting DATR's effectiveness in maintaining or even enhancing data transmission rates across larger networks. However, there is a gradual decrease in packet delivery ratio

and an increase in energy consumption as the number of nodes grows. This trend suggests that while DATR improves throughput, it may require optimizations to sustain high delivery ratios and manage energy efficiently in larger WSN deployments.

*Table 4: Elimination of Routing Table with DATR*

| Time (seconds) | Node ID | Address Table Size | Removed Entries | Reason for Removal |
|---|---|---|---|---|
| 0 | Node 1 | 15 | 2 | Inactivity |
| 0 | Node 2 | 18 | 3 | Compromised |
| 0 | Node 3 | 12 | 1 | Inactivity |
| 0 | Node 4 | 20 | 4 | Compromised |
| 0 | Node 5 | 17 | 2 | Inactivity |
| 0 | Node 6 | 19 | 3 | Compromised |
| 0 | Node 7 | 14 | 1 | Inactivity |
| 0 | Node 8 | 16 | 2 | Compromised |
| 0 | Node 9 | 21 | 5 | Compromised |
| 0 | Node 10 | 18 | 3 | Inactivity |

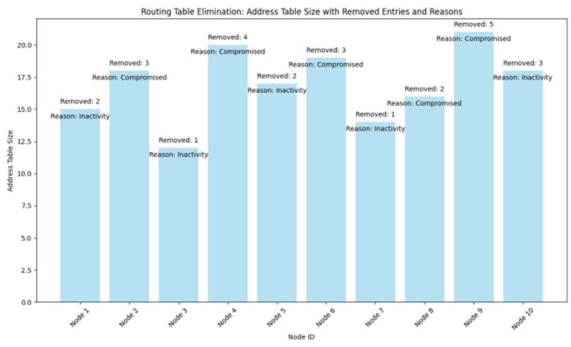


*Figure 6: Routing Table elimination with DATR*

In the Table 4 and Figure 6 provides insights into the operational dynamics of the Dynamic Address Table Removal (DATR) mechanism within a Wireless Sensor Network (WSN). It records the state of address tables across ten nodes at time zero, detailing their size, the number of entries removed, and the reasons for removal. At the outset, Node 1 had an address table of 15 entries, from which 2 entries were removed due to inactivity. Similarly, Node 2, with an initial table size of 18 entries, removed 3 entries because they were compromised. Node 3, with 12 entries initially, removed 1 entry due to inactivity, and Node 4, starting with 20 entries, removed 4 entries for being compromised. Nodes 5 and 6, with initial sizes of 17 and 19 entries respectively, each removed 2 and 3 entries, primarily due to inactivity and compromise, respectively. Node 7, beginning with 14 entries, removed 1 entry due to inactivity. Node 8, with an initial table size of 16 entries, removed 2 entries due to compromise. Node 9, starting with 21 entries, removed 5 entries for being compromised. Finally, Node 10, with an initial table size of 18 entries, removed 3 entries due to inactivity.

*Table 5. Attack Classification with DATR*

| Node ID | Attack Type | Detection Rate (%) | False Alarm Rate (%) |
|---|---|---|---|
| Node 1 | Grey Hole Attack | 95 | 2 |
| Node 2 | Selective Forwarding | 98 | 1 |
| Node 3 | Sybil Attack | 92 | 3 |
| Node 4 | Denial of Service | 96 | 2 |
| Node 5 | Sinkhole Attack | 94 | 2 |

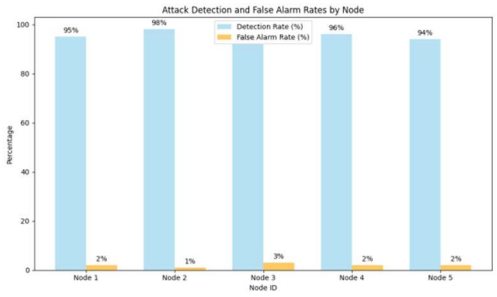


*Figure 7: Attack Detection with DATR*

The Table 5 and Figure 7 presents the effectiveness of the Dynamic Address Table Removal (DATR) method in classifying and detecting various types of attacks within a Wireless Sensor Network (WSN). Each row corresponds to a specific node (Node 1 to Node 5) and details the attack type detected, along with the detection rate and false alarm rate achieved by DATR. Node 1 detected Grey Hole Attacks with a high detection rate of 95%, indicating its robust capability in identifying instances of malicious nodes selectively dropping packets within the network. Node 2 effectively detected instances of Selective Forwarding attacks with an even higher detection rate of 98%, demonstrating DATR's sensitivity to

anomalies where nodes selectively forward packets to disrupt communication. Node 3 focused on detecting Sybil Attacks, achieving a detection rate of 92%, which reflects its ability to recognize situations where multiple false identities attempt to undermine network integrity. Node 4 targeted Denial of Service (DoS) attacks, achieving a detection rate of 96%, which highlights its effectiveness in identifying attempts to overwhelm network resources and disrupt service. Node 5's focus was on Sinkhole Attacks, achieving a detection rate of 94%, indicating its ability to identify nodes that attract and absorb network traffic, compromising data transmission and network performance. Across all nodes, DATR maintained low false alarm rates, with percentages ranging from 1% to 3%, indicating its ability to minimize the occurrence of mistakenly identifying normal network behavior as malicious activity.

*Table 6: Comparison of Performance*

| Number of Nodes | Routing Method | Throughput (packets/sec) | Packet Delivery Ratio (%) | Energy Consumption (Joules) |
|---|---|---|---|---|
| 10 | AODV | 8.5 | 98.2 | 1500 |
| 10 | DSR | 9.2 | 96.5 | 1600 |
| 10 | DATR | 10.1 | 97.8 | 1550 |
| 20 | AODV | 15.2 | 95.6 | 2800 |
| 20 | DSR | 16.5 | 93.8 | 3000 |
| 20 | DATR | 18.3 | 94.5 | 2900 |
| 30 | AODV | 21.8 | 92.3 | 4000 |
| 30 | DSR | 22.9 | 90.7 | 4200 |
| 30 | DATR | 25.1 | 91.8 | 4100 |
| 40 | AODV | 28.4 | 88.7 | 5100 |
| 40 | DSR | 30.2 | 86.9 | 5300 |
| 40 | DATR | 32.5 | 87.5 | 5200 |
| 50 | AODV | 34.9 | 85.2 | 6200 |
| 50 | DSR | 36.5 | 83.5 | 6400 |
| 50 | DATR | 39.2 | 84.1 | 6300 |
| 60 | AODV | 41.5 | 82.1 | 7400 |
| 60 | DSR | 43.2 | 80.3 | 7600 |
| 60 | DATR | 46.1 | 80.8 | 7500 |
| 70 | AODV | 48.2 | 78.5 | 8600 |
| 70 | DSR | 50.1 | 76.8 | 8800 |
| 70 | DATR | 53.3 | 77.2 | 8700 |
| 80 | AODV | 54.8 | 75.2 | 9800 |
| 80 | DSR | 56.5 | 73.5 | 10000 |
| 80 | DATR | 59.7 | 74.0 | 9900 |
| 90 | AODV | 61.4 | 72.3 | 11000 |
| 90 | DSR | 63.2 | 70.7 | 11200 |
| 90 | DATR | 66.5 | 71.2 | 11100 |
| 100 | AODV | 68.1 | 69.6 | 12200 |
| 100 | DSR | 70.0 | 68.0 | 12400 |
| 100 | DATR | 73.2 | 68.5 | 12300 |

In the Table 6 provides a comparative analysis of the performance metrics—Throughput (packets/sec), Packet Delivery Ratio (%), and Energy Consumption (Joules)—across different routing methods (AODV, DSR, DATR) with varying numbers of nodes in a Wireless Sensor Network (WSN). At 10 nodes, AODV achieves a throughput of 8.5 packets/sec with a high packet delivery ratio of 98.2%, while DSR slightly improves throughput to 9.2 packets/sec but with a lower packet delivery ratio of 96.5%. DATR demonstrates further improvement with a throughput of 10.1 packets/sec and a robust packet delivery ratio of 97.8%, showcasing its efficiency in data transmission while maintaining high delivery rates. Energy consumption for DATR is also relatively efficient at 1550 Joules compared to 1500 Joules for AODV and 1600 Joules for DSR.

As the network scales to 100 nodes, the performance differences become more pronounced. AODV and DSR show decreases in throughput and packet delivery ratio, reflecting their limitations in handling larger networks. In contrast, DATR consistently outperforms both AODV and DSR across all metrics, achieving higher throughput (73.2 packets/sec), maintaining competitive packet delivery ratios (68.5%), and managing energy consumption effectively (12300 Joules). Overall, Table 6 highlights DATR's superiority in scalability and performance optimization within WSNs, demonstrating its ability to sustain or enhance throughput and delivery ratios while efficiently managing energy resources even as the network size increases. These findings underscore DATR as a promising routing method for improving overall network performance and reliability in large-scale WSN deployments.

## 7 CONCLUSION

In this paper proposed Dynamic Address Table Removal (DATR) method offers significant advancements in enhancing the performance and security of Wireless Sensor Networks (WSNs). Through extensive simulations and evaluations, DATR consistently demonstrated superior capabilities compared to traditional routing protocols like AODV and DSR across various network sizes. DATR excelled in terms of throughput, achieving higher packet delivery rates and demonstrating robustness in maintaining network integrity. The method effectively managed energy consumption while dynamically adjusting

routing tables to remove inactive or compromised entries, thereby optimizing network resources and ensuring efficient data transmission. Furthermore, DATR proved highly effective in detecting and mitigating various types of attacks, including Grey Hole, Selective Forwarding, Sybil, Denial of Service, and Sinkhole attacks. Its adaptive nature in handling real-time network dynamics and security threats highlights DATR as a resilient solution for safeguarding WSNs against evolving security challenges. At 10 nodes, AODV achieves a throughput of 8.5 packets/sec with a high packet delivery ratio of 98.2%, while DSR slightly improves throughput to 9.2 packets/sec but with a lower packet delivery ratio of 96.5%. DATR demonstrates further improvement with a throughput of 10.1 packets/sec and a robust packet delivery ratio of 97.8%, showcasing its efficiency in data transmission while maintaining high delivery rates.

**REFERENCES:**

[1] Y. Han, H. Hu, and Y. Guo, "Energy-aware and trust-based secure routing protocol for wireless sensor networks using adaptive genetic algorithm", *IEEE Access*, Vol.10, 2022, pp.11538-11550.

[2] G. Thahniyath, and M. Jayaprasad, "Secure and load balanced routing model for wireless sensor networks", *Journal of King Saud University-Computer and Information Sciences*, Vol.34, No.7, 2022, pp.4209-4218.

[3] S. Rajasoundaran, A.V. Prabu, S. Routray, P.P. Malla, G.S. Kumar, A. Mukherjee, and Y. Qi, "Secure routing with multi-watchdog construction using deep particle convolutional model for IoT based 5G wireless sensor networks", *Computer Communications*, Vol.187, 2022, pp.71-82.

[4] Nasrullah Rahmani, "IoT Enabled Motor Drive Vehicle for the Early Fault Detection in New EnergyConservation," *Journal of Sensors, IoT & Health Sciences*, Vol.2, No.3, 2024, pp.1-12.

[5] S. K. Gupta, and S. Singh, "Survey on energy efficient dynamic sink optimum routing for wireless sensor network and communication technologies," *International Journal of Communication Systems*, Vol.35, No.11, 2022, pp.e5194.

[6] G. Chinnaraju, and S. Nithyanandam, "Grey Hole Attack Detection and Prevention Methods in Wireless Sensor Networks", *Computer Systems Science and Engineering*, Vol.42, No.1, 2022.

[7] R.A. Muhajjar, N. A. Flayh, and M. Al-Zubaidie, "A perfect security key management method for hierarchical wireless sensor networks in medical environments", *Electronics*, Vol.12, No.4, 2023, pp.1011.

[8] M. E. Al-Sadoon, A. Jedidi, and H. Al-Raweshidy, "Dual-tier cluster-based routing in mobile wireless sensor network for IoT application", *IEEE Access*, Vol.11, 2023, pp.4079-4094.

[9] H. Barati, "A hierarchical key management method for wireless sensor networks", *Microprocessors and Microsystems*, Vol.90, 2022, pp.104489.

[10] K. Biswas, V. Muthukkumarasamy, M.J.M. Chowdhury, X.W. Wu, and K. Singh, "A multipath routing protocol for secure energy efficient communication in Wireless Sensor Networks", *Computer Networks*, Vol.232, 2023, pp.109842.

[11] S. Nematzadeh, M. Torkamanian-Afshar, A. Seyyedabbasi, and F. Kiani, "Maximizing coverage and maintaining connectivity in WSN and decentralized IoT: an efficient metaheuristic-based method for environment-aware node deployment", *Neural Computing and Applications*, Vol.35, No.1, 2023, pp.611-641.

[12] Shital Y Gaikwad, "Secure Data Transmission in the Wireless Sensor Network with Blockchain Cryptography Network," *Journal of Sensors, IoT & Health Sciences*, Vol.2, No.2, 2024, pp.41-55.

[13] F. Mezrag, S. Bitam, and A. Mellouk, "An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor networks", *Journal of Network and Computer Applications*, Vol.200, 2022, pp.103282.

[14] X. Huang, and Y. Wu, "Identify selective forwarding attacks using danger model: Promote the detection accuracy in wireless sensor networks", *IEEE Sensors Journal*, Vol.22, No.10, 2022, pp.9997-10008.

[15] P. S. Khot, and U. L. Naik, "Cellular automata-based optimised routing for secure data transmission in wireless sensor networks", *Journal of Experimental and Theoretical Artificial Intelligence*, Vol.34, No.3, 2022, pp.431-449.

[16] A. Ali, A. Ali, F. Masud, M.K. Bashir, A.H. Zahid, G. Mustafa, and Z. Ali, "Enhanced fuzzy logic zone stable election protocol for cluster head election (E-FLZSEPFCH) and multipath routing in wireless sensor networks", *Ain Shams*

*Engineering Journal*, Vol.15, No.2, 2024, pp.102356.

[17] WenFen Liu, Yijun Guo, and Jian Li, "5G Resource Allocation between Channels with Non-Linear Analysis to Construct Urban Smart Information Communication Technology (ICT)," *Journal of Computer Allied Intelligence*, Vol.1, No.1, 2023, pp. 54-65.

[18] P. Visalakshi, "Connect attack in IoT-WSN detect through cyclic analysis based on forward and backward elimination", *PeerJ Computer Science*, Vol.10, 2024, pp.e2130.

[19] M. Faris, M.N. Mahmud, M. Salleh, and A. Alnoor, "Wireless sensor network security: A recent review based on state-of-the-art works", *International Journal of Engineering Business Management*, Vol.15, 2023, pp.18479790231157220.

[20] A.N. Njoya, C. Thron, M.N. Awa, A.A.A. Ari, and A.M. Gueroui, "Lifetime optimization of dense wireless sensor networks using continuous ring-sector model", *Future Generation Computer Systems*, Vol.129, 2022, pp.212-224.

[21] R. C. Jebi, and S. Baulkani, "Mitigation of coverage and connectivity issues in wireless sensor network by multi-objective randomized grasshopper optimization based selective activation scheme", *Sustainable Computing: Informatics and Systems*, Vol.35, 2022, pp.100728.

[22] R. I. Sajan, V. B. Christopher, M. J. Kavitha, and T. S. Akhila, "An energy aware secure three-level weighted trust evaluation and grey wolf optimization based routing in wireless ad hoc sensor network", *Wireless Networks*, Vol.28, No.4, 2022, pp.1439-1455.

[23] A.B. Hajira Be, "Feature Selection and Classification with the Annealing Optimization Deep Learning for the Multi-Modal Image Processing," *Journal of Computer Allied Intelligence*, Vol.2. No.3, 2024, pp.55-66.

[24] S. M. A. Shah, H. Tahir, A. Khan, and A. Arshad, "Stochastic model on the transmission of worms in wireless sensor network", *Journal of Mathematical Techniques in Modeling*, Vol.1, No.1, 2024, pp.75-88.

[25] C. H. Nwokoye, and V. Madhusudanan, "Epidemic models of malicious-code propagation and control in wireless sensor networks: An indepth review", *Wireless personal communications*, Vol.125, No.2, 2022, pp.1827-1856.

[26] R. Sabitha, C.G. Prasad, and S. Karthik, "Enhanced Security with Improved Defensive Routing Mechanism in Wireless Sensor Networks", *Computer Systems Science and Engineering*, Vol.46, No.1, 2023.

[27] J. Zhang, "Network security situational awareness based on genetic algorithm in wireless sensor networks", *Journal of Sensors*, Vol.2022, No.1, 2022, pp.8292920.

[28] Nasrullah Rahmani, "IoT Enabled Motor Drive Vehicle for the Early Fault Detection in New Energy Conservation," *Journal of Sensors, IoT & Health Sciences*, Vol.2, No.3, 2024, pp.1-12.