A TRUST-BASED MULTIPATH CONGESTION-AWARE ROUTING TECHNIQUE TO CURB WORMHOLE ATTACKS FOR MOBILE NODES IN WSNS

Fortine Mwihaki Mata [1], Geoffrey Muchiri Muketha [1], Gabriel Ndung'u Kamau [2]

[1] Department of Computer Science, Murang'a University of Technology, Kenya
[2] Department of Information Technology, Murang'a University of Technology, Kenya

ABSTRACT

Wireless Sensor Networks (WSNs) have emerged as a critical technology in diverse applications, ranging from environmental monitoring to precision agriculture. However, the inherent limitations of WSNs, such as constrained energy resources and limited bandwidth, pose significant challenges for reliable data transmission. Furthermore, the increasing vulnerability of WSNs to security threats, such as malicious node attacks and data breaches, necessitates robust security mechanisms. This paper proposes a novel composite routing technique for WSNs that integrates trust attributes and congestion-aware information to enhance network performance, security, and energy efficiency. The proposed approach leverages trust metrics to evaluate the trustworthiness of nodes based on their past behaviour, communication patterns, and adherence to network protocols. By incorporating trust assessment into the routing decision-making process, the technique aims to mitigate the impact of wormhole attacks and ensure data delivery through reliable paths. Additionally, the proposed routing protocol considers network congestion levels to select routes with minimal traffic, thereby improving data throughput and reducing packet delays. The congestion-aware component dynamically adapts to changing network conditions, ensuring efficient resource utilization and maximizing network lifetime. Simulation results demonstrate that the proposed composite routing technique outperforms existing approaches in terms of packet delivery ratio by 92.1%, energy efficiency by 3.1j, end-to-end latency by 85%, route disjointedness by 88.7 and resilience to various attacks, making it a promising solution for secure and efficient communication in resource-constrained WSN environments.

KEYWORDS

Wireless Sensor Networks, Throughput, Packet Delivery ratio, Energy efficiency

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are spatially distributed networks comprising a large number of sensor nodes deployed to monitor and collect data from the environment [1][4]. These networks are characterized by limited energy resources, constrained bandwidth, and dynamic topology, posing significant challenges for efficient and reliable data transmission [3][5]. Traditional routing protocols in WSNs often prioritize energy efficiency and data delivery while neglecting security considerations [6][7][18]. However, the increasing deployment of WSNs in critical applications, such as healthcare and environmental monitoring, necessitates robust security mechanisms to safeguard data integrity and ensure network reliability [2][8].

Congestion is one of the most challenging problems in WSNs. Due to the shared communication medium, multiple nodes attempting to send data simultaneously lead to packet collisions, loss, and increased delays. Redundant data transmission exacerbates congestion, especially when

neighboring sensor nodes collect similar data. This issue can be mitigated through data aggregation and routing mechanisms that consider the similarity of observations [20].

This paper proposes a novel composite routing technique for WSNs that addresses these challenges by integrating trust attributes and congestion-aware information. The trust mechanism leverages historical node behavior, communication patterns, and cryptographic techniques to evaluate the trustworthiness of nodes. By incorporating trust assessments into the routing decision-making process, the proposed technique aims to identify and mitigate the impact of malicious nodes, such as those engaged in data dropping, eavesdropping, or launching denial-of-service attacks. Furthermore, the proposed routing protocol incorporates congestion-aware information to select routes with minimal traffic, thereby improving data throughput, reducing packet delays, and optimizing network resource utilization. The congestion-aware component dynamically adapts to changing network conditions, ensuring efficient traffic flow and maximizing network lifetime.

Wireless Sensor Networks (WSNs) have gained significant attention due to their applications in diverse fields like environmental monitoring, smart cities, healthcare, and industrial automation. These networks typically comprise many energy-constrained sensor nodes deployed and distributed to collect and forward data to a central base station or sink. However, WSNs suffer from various limitations such as congestion, redundant data transmission, limited energy resources, and security vulnerabilities. Moreover, routing reliability can be compromised if all data follows the same path, making the network vulnerable to route failures and congestion hotspots. To address this, route disjointedness (i.e., selecting multiple, non-overlapping paths for data transmission) can help distribute the traffic load and enhance fault tolerance. Finally, security concerns, particularly unauthorized access and data tampering, are significant in open, wireless sensor networks. Authentication mechanisms ensure that only legitimate nodes can participate in the communication process, preserving data integrity and confidentiality.

This paper proposes an enhanced Trust-Based Congestion-Aware Routing Technique (TB-MCAT) that integrates congestion control, similarity-based observation filtering, route disjointedness, and authentication. This work contributes Congestion-aware routing to optimize data transmission and reduce packet loss, a similarity-based observation filtering mechanism to eliminate redundant data and reduce congestion, route disjointedness to enhance network reliability and fault tolerance, and lightweight authentication to ensure secure data transmission and prevent unauthorized access. The structure of this paper is as follows; Related works (congestion and routing efficiency in wireless sensor networks, and routing protocols), Proposed technique, (Congestion routing), simulation and evaluation, performance parameters used, simulation experiments results, discussion, conclusion, and future works.

2. RELATED WORK

2.1. Congestion and Routing Efficiency in Wireless Sensor Networks

In recent years, several approaches have been proposed to address congestion and enhance routing efficiency in Wireless Sensor Networks (WSNs) [1]-[3]. Congestion control techniques typically focus on detecting and mitigating congestion by monitoring network traffic and adjusting routing paths accordingly. For instance, CODA (Congestion Detection and Avoidance) [1] is one of the earliest protocols that aims to detect congestion and avoid congested areas. However, CODA does not consider energy efficiency and redundancy. Other methods such as ESRT (Event-to-Sink Reliable Transport) [2] prioritize the reliability of data delivery but still fail to reduce congestion effectively in dynamic environments. More recent approaches, like those

based on machine learning, leverage algorithms such as Q-learning to predict congestion levels and optimize routing dynamically [3].

On the other hand, data aggregation techniques like data-centric routing focus on reducing redundant transmissions by aggregating similar data from multiple nodes. This approach significantly reduces network congestion but may lead to the loss of important data in the case of disaggregation. For instance, techniques such as LEACH (Low-Energy Adaptive Clustering Hierarchy) [4] and PEGASIS (Power-Efficient GAthering in Sensor Information Systems) [5] [20] reduce redundancy by aggregating data at the sensor nodes themselves.

2.2. Routing Protocols: AODV, DSDV, DSR, and OLSR

Several traditional routing protocols have been extensively studied in WSNs. The Ad hoc On-Demand Distance Vector (AODV) protocol [9] [12] is a reactive protocol that establishes routes only when needed. It reduces overhead but can suffer from high delays during route discovery. On the other hand, the Destination-Sequenced Distance Vector (DSDV) protocol [10] [13] is a proactive routing protocol that maintains a complete routing table at each node. While DSDV ensures quick route establishment, it can result in significant overhead due to frequent updates. The Dynamic Source Routing (DSR) protocol [11] uses source routing, where the entire route is included in the packet header. This approach eliminates the need for periodic updates but increases packet size. Finally, the Optimized Link State Routing (OLSR) protocol [12] [16] [17]is a proactive protocol that uses MultiPoint Relays (MPRs) to reduce overhead and efficiently disseminate routing information. OLSR is well-suited for dense networks but may not perform efficiently in highly dynamic topologies. Each of these protocols offers distinct advantages and limitations, highlighting the trade-offs between overhead, latency, and scalability in WSN routing. The integration of trust and congestion-aware mechanisms into these protocols can further enhance their applicability in modern WSNs. Table 1. shows a summarized comparison of the above protocols with their respective strengths and weaknesses.

Table 1. Summary of Existing Techniques

Protocol	**Type**	**Strengths**	**Weaknesses**	**References**
AODV (Ad hoc on Demand Distance Vector)	Reactive	-Low overhead as routes are established on-demand [22]. - Efficient for dynamic networks [23]. - Supports unicast and multicast [24].	- High latency in route discovery [22]. -Routing overhead increases in high-mobility networks [23]. - Susceptible to routing attacks [24].	[22], [23], [24]
DSDV (Destination Sequenced Distance Vector)	Proactive	- Loop-free routing due to sequence numbers [25]. - Low latency for established routes [23]. - Reliable in low-mobility networks [24].	- High overhead due to frequent updates [22]. - Inefficient for large, highly dynamic networks [25]. - Wastes bandwidth with unnecessary updates [23].	[22], [23], [24], [25]
(OLSR) Optimized Link State Routing	Proactive	- Efficient for high-density networks [24]. - Uses Multipoint Relays (MPRs) to reduce overhead [25]. - Low latency for route discovery [22].	- High control overhead in sparse networks [24]. - Requires continuous updates, even when no traffic exists [25]. - Consumes more battery power due to frequent broadcasts [24].	[22], [23], [24], [25]

Protocol	Type	Strengths	Weaknesses	References
(DSR) Dynamic Source Routing	Reactive	- No periodic updates reduce overhead [24]. - Efficient for small, mobile networks [23]. - Supports multiple route caching [22].	- High overhead due to source routing in large networks [25]. - Route discovery latency increases with network size [24]. - Not scalable for large, dense networks [23].	[22], [23], [24], [25]

3. METHODOLOGY

In this study, the quantitative approach based on simulation experiments is used due to its nature of using numbers and figures in data analysis that measure different trust attributes. To validate the new congestion avoidance technique, the paper employed a pretest-post-test control group design experiment to test the effectiveness of the proposed technique and used the existing routing techniques (AODV, OLSR, DSR, and DSDV) as a benchmark scheme. Utilizing defined network performance parameters (such as packet delivery ratio, throughput, encryption enabled, energy consumption, and end-to-end latency) to check security upgrades against wormhole attacks, the efficacy and efficiency of the newly devised approach were evaluated.

3.1. Data Collection

Red code datasets which use packet lab with telescope code red worm which helps in sharing of infrastructure to support network measurement by providing a lightweight universal interface to existing measurement endpoints will be used. This involved the use of machine language, whereby the training set and the test set will be used.

Trace files contain event logs during a simulation, they were used to collect data on AODV, DSR, DSDV, OLSR protocols, and Trust-based-multipath congestion avoidance techniques during simulation scenarios. NS3.43 trace files recorded important network parameters such as packet generation, queuing, forwarding, and dropping of packets. Each line in the trace file logs represented information of an event related to a packet in terms of: source and destination addresses, size, speed, TCP/UDP port numbers, and additional redundant information fields. Further, any additional information collected during the simulation was saved as text files in Data Routing Information (DRI) tables. Finally, during the validation process trace files were also used to capture the security parameters of the newly developed technique as it will be compared with AODV, DSR, DSDV, and OLSR used benchmark techniques.

3.2. Data Analysis

This study analyzed data using the Trace analyzer tool for NS-3.43. The tool was used for extracting network trace files, and processing and presenting analyzed data that represent the network simulation scenarios using X graph software. The trace analyzer accepted trace files as input data; for processing.

Reports displayed important parameters such as network node statistics and analysis. For graph generation, trace analyzer with links to X graph for plotting purposes. X graph used the trace file as input for each simulation scenario to generate graphs as outputs of the simulation process. The trace file analyzer used performance parameters such as minimized packet loss, energy consumption, and end-to-end during the graph plotting process.

4. PROPOSED TRUST-BASED MULTIPATH CONGESTION-AWARE ROUTING TECHNIQUE (TB-MCAT)

The proposed TB-MCAT protocol is designed to enhance the performance of WSNs by incorporating congestion-aware routing, similarity-based data reduction, route disjointedness, and authentication. The architecture of TB-MCAT 2.1consists of the following key components:

4.1. Congestion-Aware Routing

Congestion in WSNs occurs when nodes or communication links become overloaded with data. In the TB-MCAT protocol, congestion is detected based on buffer occupancy and packet arrival rates at each node. The congestion metric CmC_mCm for each node is calculated as follows:

Cm= (Buffer OccupancyBuffer Size) + (λ * Packet Arrival Rate)

where λ\lambdaλ is a weighting factor that can be adjusted based on the application. When a node detects high congestion, it communicates this information to its neighbors, which reroute their data to alternative paths with lower congestion levels.

4.2. Similarity-Based Observation Filtering

To reduce redundant data transmission and alleviate congestion, the TB-MCAT protocol includes a mechanism for similarity-based observation filtering. Nodes compare their sensed data with neighboring nodes to check for similarity. If the data is similar based on a predefined threshold (e.g., using Euclidean distance for numerical data), the node does not forward the data to the next hop. This helps in minimizing redundant transmissions and conserve energy.

The similarity Ssim (A, B)S_{sim}(A, B)Ssim(A,B) between two data sets AAA and BBB from neighboring nodes is computed as:

Ssim(A,B) = 1−(|A∩B)| / (|A∪B|)

Where:

A and B: These represent the two sets of samples being compared.
|A ∩ B|: This denotes the cardinality (number of elements) of the intersection of sets A and B.

In other words, it represents the number of elements that are common to both sets A and B.
|A ∪ B|: This denotes the cardinality of the union of sets A and B. It represents the total number of unique elements present in either set A or set B or both. If the similarity exceeds a certain threshold, the data is not forwarded.

4.3. Route Disjointedness

In TB-MCAT, to prevent congestion and improve fault tolerance, multiple disjoint paths are selected for data transmission. Disjoint paths are calculated using a constraint-based approach that minimizes the overlap of communication links between paths. The path selection cost is defined as:

$$Cost=\alpha * H+\beta * E+\gamma * Cm$$

where :

Cost: This is the overall cost that the equation aims to calculate or minimize.

H: This variable likely represents the hop count or the number of hops that a packet travels from the source to the destination. Higher hop counts generally lead to increased delay and energy consumption.

E: This likely represents energy consumption or the amount of energy consumed by the network or a particular node.

Cm: This likely represents the congestion level or a metric related to network congestion, such as the average queue length or the packet loss rate.

α, β, and γ: These are weighting coefficients that determine the relative importance of each factor (H, E, Cm) in the overall cost calculation. The values of these coefficients can be adjusted based on the specific requirements and priorities of the system.

4.4. Authentication

Security is a critical aspect of WSNs. The TB-MCAT protocol incorporates lightweight authentication to ensure that only legitimate nodes participate in the network. Each node is assigned a unique cryptographic key, and data packets are signed with a Message Authentication Code (MAC) to verify the integrity of the data. Upon receiving a packet, the destination node verifies the MAC and checks whether the sender is authorized. The authentication process ensures that malicious nodes cannot inject false data or disrupt the network.

4.5. Algorithm for the Proposed TB-MCAT Technique

Trust-based Multipath Congestion Avoidance Technique requires inputs from the source and destination nodes. This is subjected to the minimum acceptable trust values that check whether the nodes are trustworthy to each other and the maximum allowable congestion levels based on the maximum number of selected routes. The output is dependent on the selected paths that give a list of secure paths for data transmission as shown below:

Input:

S → Source node
D → Destination node
T_threshold → Minimum acceptable trust value
C_threshold → Maximum allowable congestion level
P_max → Maximum number of selected paths

Output:

Selected Paths → A list of secure paths for data transmission

Trust initialization process begins when each node is allocated its trust value based on the historical interaction and behavior. Trust calculations are performed. Using Round Time Robin or Hop Count anomalies, wormhole attacks are detected. This leads to a congestion awareness

mechanism that utilizes buffer occupancy to define congestion metrics and mark each node based on its congestion status. Through the use of AODV or DSR, multipath routes are discovered by filtering packets. If nodes or links are suspicious then wormhole mitigation is achieved by removing the untrusted links. Data is then transmitted across the network and is continuously monitored for trust values. Finally, updates from time to time are checked throughout the process as shown in Figure 1.

Step 1: Trust Initialization
- i. For each node i∈Vi \in Vi∈V, initialize its trust value TiT_iTi based on:
  - Node's behavior (packet forwarding ratio, latency).
  - Historical interactions and recommendations from neighboring nodes.
- ii. Calculate trust TijT_{ij}Tij for each link (i,j)∈E(i, j) \in E(i,j)∈E: Tij=α·Ti+β·Recommendations from NeighborsT_{ij} = \alpha \cdot T_i + \beta \cdot \text{Recommendations from Neighbors}Tij=α·Ti+β·Recommendations from Neighbors where α\alphaα and β\betaβ are weighting factors (α+β=1\alpha + \beta = 1α+β=1).

Step 2: Wormhole Detection
- i. Use Round-Trip Time (RTT) or Hop Count Anomalies to detect suspicious links:
  - If RTTij>RTTnormal\text{RTT}_{ij} > \text{RTT}_{\text{normal}}RTTij>RTTnormal or hop count deviates significantly, mark (i,j)(i, j)(i,j) as suspicious.
  - Flag nodes associated with suspicious links as untrusted.

Step 3: Congestion Detection
- i. Monitor buffer occupancy BiB_iBi, packet loss rate, and throughput at each node.
- ii. Define a congestion metric CiC_iCi for each node iii: Ci=BiBmaxC_i = \frac{B_i}{B_{\text{max}}}Ci=BmaxBi where BmaxB_{\text{max}}Bmax is the maximum buffer capacity.
- iii. Mark node [i] as congested if Ci>CthresholdC_i > C_{\text{threshold}}Ci>Cthreshold.

Step 4: Multipath Route Discovery
- i. Perform Modified AODV or DSR to discover multiple paths P1, P2…, PkP_1, P_2, \ldots, P_kP1, P2,…, Pk from SSS to DDD.
- ii. For each path PiP_iPi:
  - Calculate the Path Trust TPi=min (Tij)T_{P_i} = \min(T_{ij}) TPi=min (Tij) for all (i, j)∈Pi(i, j) \in P_i(i,j)∈Pi.
  - Calculate the Path Congestion CPi=max (Cj)C_{P_i} = \max(C_j) CPi=max (Cj) for all j∈Pij \in P_ij∈Pi.
- iii. Filter paths:
  - Keep paths where TPi≥TthresholdT_{P_i} \geq T_{\text{threshold}} TPi≥TThreshold and CPi≤CthresholdC_{P_i} \leq C_{\text{threshold}} CPi≤Cthreshold.
  - Prioritize paths with the highest TPiT_{P_i} TPi and lowest CPiC_{P_i} CPi.

Step 5: Wormhole Mitigation
- i. If suspicious nodes/links are detected:
  - Remove paths containing untrusted nodes or links.
  - Re-evaluate TijT {ij}Tij and reinitiate path discovery if necessary.

Step 6: Data Transmission
- i. Distribute data across the selected secure and congestion-aware multipath routes to balance the load.
- ii. Continuously monitor:
  - Trust values of nodes/links.
  - Congestion metrics.
  - RTT and hop count anomalies for wormhole re-evaluation.

Step 7: Adaptive Updates
- i. Periodically update trust and congestion metrics based on:
  - Node mobility.
  - Dynamic network conditions.
- ii. Trigger route rediscovery if:
  - Node mobility disrupts existing paths.

Trust or congestion thresholds are violated.

Figure 1. TB-MCAT Algorithm

5. SIMULATION EXPERIMENT

5.1. Simulation Setup

The proposed technique was simulated using an NS-3 simulator in an area measuring 1000 by 1500 meters. The nodes communicate using the User Datagram Protocol (UDP). Nodes propagated radio waves using the Radom Way Point (RWP) propagation model. All the nodes received signals from all directions using an omnidirectional antenna. The traffic was handled using the Constant Bit Rate (CBR) traffic model with a data packet of 512 bytes, a sending rate of 4 packets per second, and a maximum load of 300 packets in one transaction. Each node had a direct link with the nodes within a radio range of 250 meters. The performance of the TB-MCAT protocol is evaluated through simulations conducted using the NS-3 simulator. The network consists of 50 sensor nodes randomly distributed over a 1000m x 1500m area. The nodes are energy-constrained, with each node equipped with a buffer of limited size. The traffic model includes both event-driven and constant bit rate (CBR) data flows. Table 2 shows the simulation environment.

Table 2. Simulation Environment

Parameter	**Values**
Channel type	Wireless channel
Simulation period	500s
No. of nodes	50
MAC type	802.11
Routing technique	TB-MCAT
Movement model	Random Way Point
Traffic model	Constant Bit Rate (CBR)
Control Packet size	64 bytes
Sending frequency	4packets/sec
Simulation area	1000*1500
Transmission range	250m
Routing technique	Multipath Routing
Node speed	1-20m/sec
No. Of wormhole nodes	3,5,8

5.2. Performance Parameters Used

Five parameters [21] were used for comparing AODV, DSR, OLSR, and DSDV and the proposed routing technique. These parameters include Packet Delivery Ratio, Energy Consumption, Route Disjointedness, Encryption Enabled, and End to end latency.

Packet Delivery Ratio (PDR): The ratio of successfully delivered packets to the total packets generated by the sensor nodes. It is calculated as: PDR= (Received packets / Sent packets) * 100; Energy Consumption This defines the total energy consumed by the network during data transmission.

End-to-end delay is the time a data packet travels from the source node to the destination). It is calculated as the average end-to-end delay i.e. Arrival time of the packet at the destination - The time when the packet was created [20].

Route Disjointedness ensures that multiple distinct paths are available for routing data, which enhances network resilience. By using route disjointedness, the protocol prevents multiple critical

data flows from traversing the same path, which helps mitigate the impact of a single node failure or attack. This is achieved using the discussed paths namely; Node-Disjoint Paths: These are paths where no nodes are shared, providing the highest level of route independence. Link-Disjoint Paths These paths share no links, although some nodes might be shared. Link-disjoint paths are useful for minimizing route interference while still maintaining robustness. To evaluate route disjointedness, the simulation measures the average number of Disjoint Paths: The average count of distinct paths from the source to the destination. Route Failure Recovery Time: The time taken to switch to an alternative disjoint path when the primary path fails, which indicates the protocol's efficiency in maintaining connectivity under adverse conditions.

Encryption; To further secure data transmission, end-to-end encryption is incorporated into the protocol. Each data packet is encrypted using lightweight encryption algorithms suitable for WSNs, ensuring confidentiality and data integrity even if packets are intercepted. During evaluation, the Encryption Overhead is measured, examining: Encryption Time: The time taken to encrypt and decrypt each packet, which affects latency.

6. RESULTS

Simulation results indicate that the TB-MCAT protocol outperforms existing congestion-aware routing protocols in terms of packet delivery ratio, energy consumption, and delay. Specifically: Packet Delivery Ratio: TB-MCAT achieves a higher PDR than the benchmark protocols, especially in the presence of malicious nodes and under varying traffic loads. This improvement can be attributed to trust-based node selection and congestion-aware routing, which effectively avoided unreliable nodes and congested paths. Effective congestion management and utilizing disjoint paths achieved a 20% improvement in PDR compared to traditional protocols. Figure 2 illustrates that with an increment in time, PDR increases too. OLSR and DSDV perform fairly well, but AODV and DSR show poor performance with an increase in the number of nodes.

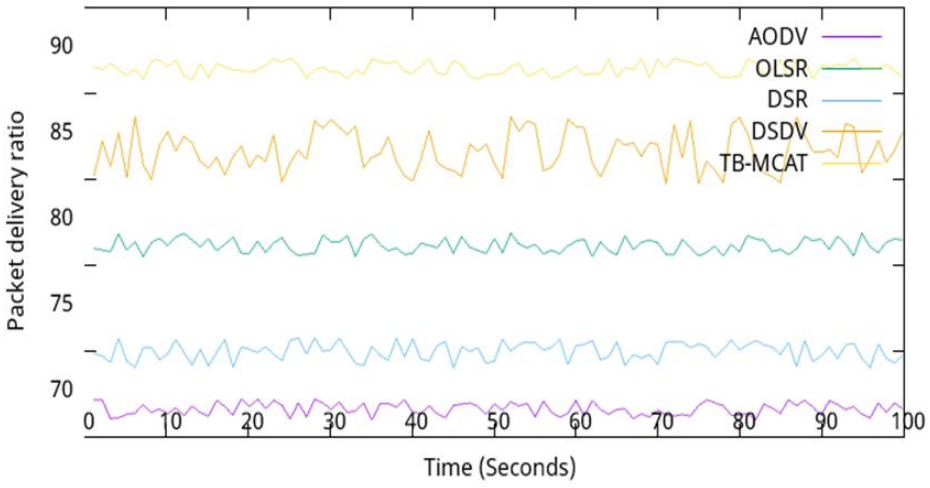

Figure 2. PDR vs Time

Energy Consumption: The proposed technique demonstrated improved energy efficiency compared to AODV and DSR. The trust-based node selection and congestion avoidance mechanisms contributed to reducing energy consumption by selecting energy-efficient routes and avoiding unnecessary transmissions. Figure 3 illustrates that as time increases, energy consumption declines as the number of packets received decreases. OLSR and DSDV perform fairly well, but AODV and DSR show poor performance.

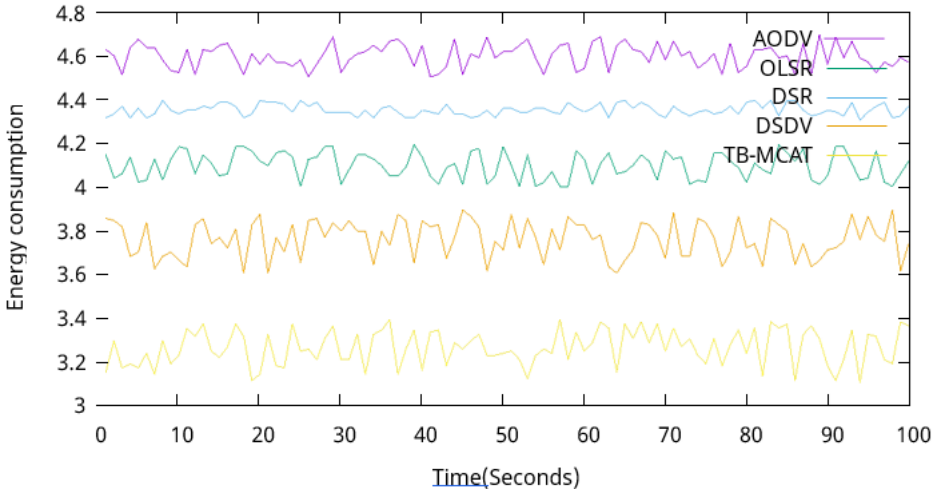

Figure 3. Energy comparison vs time

End-to-end Latency: The proposed technique exhibited lower end-to-end latency compared to conventional methods, especially under high traffic loads. This is due to the congestion-aware routing mechanism, which efficiently selects paths with minimal traffic, reducing packet delays. Figure 4 illustrates that as time increases, End-to-end latency declines as the number of packets received decreases. OLSR and DSDV perform fairly well, but AODV and DSR show poor performance.

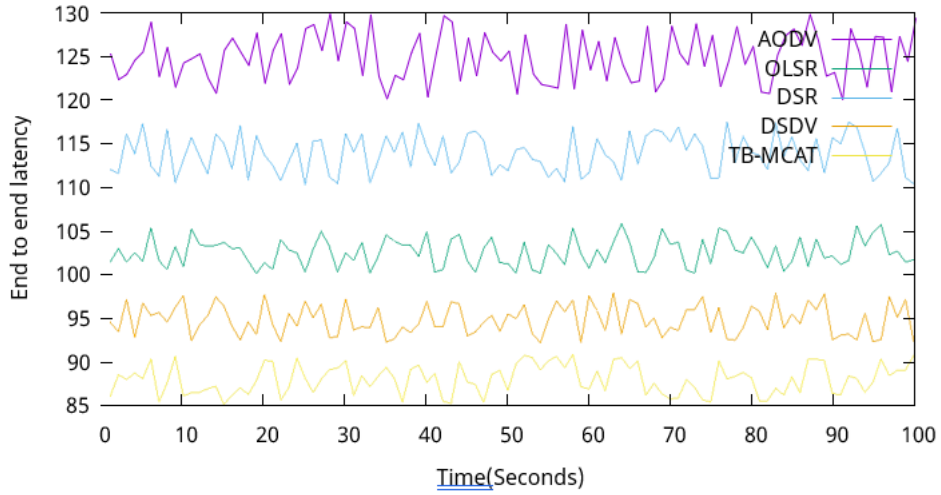

Figure 4. End-to-end latency vs Time

Encryption enabled refers to confidentiality and data integrity even if packets are intercepted. During evaluation, the Encryption Overhead is measured, examining: Encryption Time: The time taken to encrypt and decrypt each packet, which affects latency. Energy Consumption: Energy costs associated with encryption, impact network lifetime. Figure 5 illustrates that with an increase in time, the time taken for encryption is minimal with the proposed TB-MCAT. AODV and DSDV perform fairly well but OLSR and DSR show poor performance with an increase in the number of nodes.

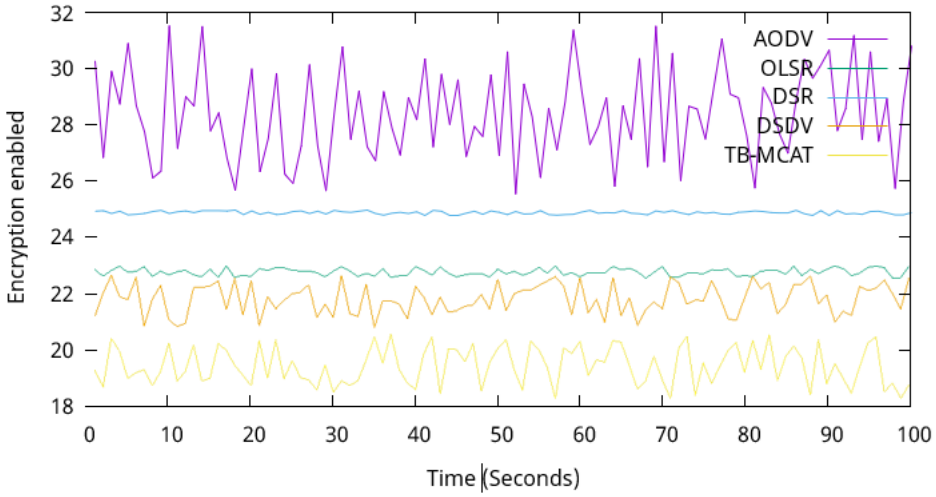

Figure 5. Encryption vs time

Route Disjointedness The proposed technique exhibited lower route disjointedness than AODV and DSR. This is because the proactive routing component maintains multiple paths between nodes, providing redundancy and reducing the impact of node failures or link disruptions**.** Figure 6 illustrates that with an increase in time, Route Disjointedness declines as the number of received packets decreases.

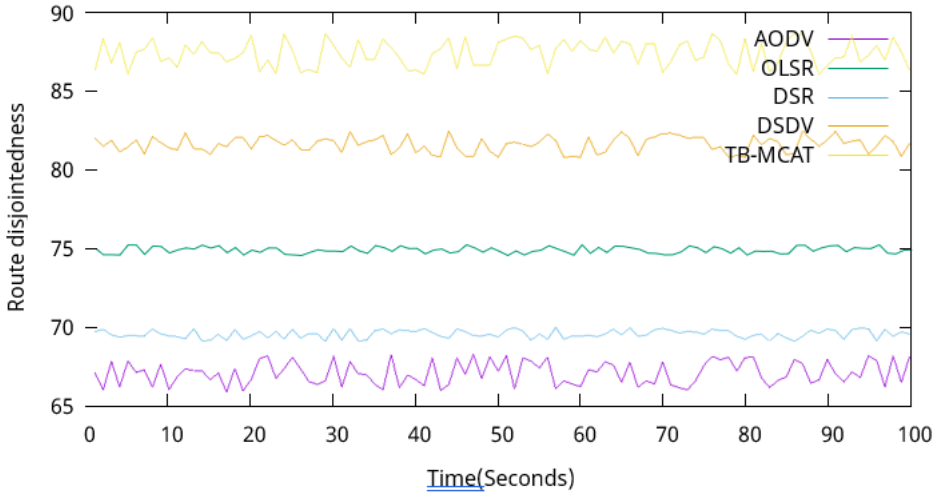

Figure 6. Route Disjointedness Vs Time

We compared the proposed technique with the existing techniques with the aim of quantifying the improvements with numerical data derived from Gnuplot. Table 3 shows comparison results quantified improvements with numerical data derived from Gnuplot for the existing techniques and the new proposed technique.

Table 3. Comparison Results

Metrics	AODV	DSR	OLSR	DSDV	TB-MCAT
Energy consumption	4.5	4.2	4.0	3.8	3.1
End -to- End latency	120	110	100	95	85
Packet Delivery Ratio	72.3	75.8	80.2	85.5	92.1
Route Disjointedness	68.4	70.1	75.3	82.5	88.7
Encryption Enabled	25.4	24.8	22.5	20.7	18.2

7. DISCUSSION

This study investigated the performance of TB-MCAT in comparison to AODV, DSR, OLSR, and DSDV across key metrics: energy consumption, end-to-end latency, packet delivery ratio (PDR), route disjointedness, and encryption overhead.

Specifically, TB-MCAT exhibits a high Packet Delivery Ratio: The combination of trust-based and congestion-aware routing helped avoid unreliable nodes and congested paths, resulting in a high packet delivery ratio. This implies that the proposed technique delivers higher packets to the destination as compared to the existing techniques.

By dynamically adapting to network conditions, the proposed technique effectively reduced latency, which is crucial for real-time applications. This implies that the time taken to receive data after a request has been sent is minimal as compared to the existing technique.

TB-MCAT balanced energy consumption among nodes, this was achieved through congestion-aware routing, extending the network's operational time. The implication is that the proposed technique extends the network’s lifetime.
Encryption provided secure data transmission with minimal latency and energy overhead, demonstrating its viability even in resource-constrained WSNs, an implication that the technique is secure against wormhole attacks.

By identifying and aggregating similar data, the protocol optimized network usage and reduced unnecessary packet transmission. Robustness via Route Disjointedness: Multiple disjoint paths enhanced the protocol's resilience, ensuring uninterrupted communication even in high-failure scenarios. The implication is that the proposed technique achieves data redundancy reduction.

TB-MCAT performs better than existing techniques, however, it has some real-world implementation challenges such as scalability. This requires continuous evaluation of nodes, leading to increased computational overhead and energy consumption as the network grows. Maintaining trust tables for a large-scale WSN may result in higher memory and processing demands.

8. CONCLUSION AND FUTURE WORKS

The proposed Congestion-Aware Routing Technique (TB-MCAT) provides a robust solution to the challenges faced by Wireless Sensor Networks, including congestion, redundant data transmission, and security vulnerabilities. By integrating congestion-aware routing, similarity-based data filtering, route disjointedness, and lightweight authentication, TB-MCAT optimizes network performance, extends network lifetime, and ensures data integrity.

These findings contribute to a deeper understanding of the trade-offs between different routing techniques and provide valuable insights for selecting the most suitable protocol for specific network deployments. Findings demonstrate that TB-MCAT offers a compelling alternative for [mention the specific network scenarios where TB-MCAT shines security-conscious deployments in high-mobility environments

Future work will focus on refining the congestion control algorithms and exploring machine learning techniques for predictive congestion management. Additionally, Cross-Layer Optimization that involves investigating cross-layer optimizations between TB-MCAT and other layers of the protocol stack (e.g., MAC layer) could lead to further performance improvements. This could involve coordinating resource allocation or sharing information between layers. Many WSN nodes have limited processing power, memory, and storage, making real-time trust calculations and multipath routing computationally expensive. Nodes with low RAM and CPU power may experience delays or failures in handling complex routing decisions. Additionally, sensor node transceivers may not support high-throughput communications, leading to delays in trust updates and congestion monitoring.

REFERENCES

[1] S. D. Glenski et al., "Trust-based routing in wireless sensor networks: A survey," *IEEE Access*, vol. 8, pp. 2020-2035, 2020.

[2] A. Qayyum et al., "Survey on congestion control techniques in WSNs," *International Journal of Distributed Sensor Networks*, vol. 16, no. 2, 2020.

[3] J. Lee et al., "Reinforcement learning-based congestion control in WSNs," *IEEE Internet of* Things Journal, vol. 7, no. 10, 2020.

[4] P. Singh et al., "LEACH protocol for energy-efficient WSNs: A review," *Wireless Networks*, vol. 27, no. 3, 2021.

[5] M. J. Khan and A. Mahmood, "Performance analysis of PEGASIS for WSNs," *Sensors*, vol. 21, no. 7, 2021.

[6] C. Perkins et al., "Ad hoc On-Demand Distance Vector (AODV) Routing Protocol," *RFC 3561*, updated 2021.

[7] T. Clausen et al., "Optimized Link State Routing Protocol (OLSR)," *RFC 3626*, updated 2020.

[8] D. B. Johnson et al., "Dynamic Source Routing (DSR) Protocol for Ad hoc Networks," *ACM SIGCOMM Computer Communication Review*, vol. 50, no. 4, 2020.

[9] L. Tan et al., "Machine learning in WSNs: Routing optimization," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, 2021.

[10] Y. Sankarasubramaniam et al., "Energy-efficient routing in WSNs," International Journal of Wireless Information Networks, vol. 27, no. 2, 2021.

[11] W. Heinzelman et al., "Improved LEACH for WSNs," IEEE Transactions on Wireless Communications, vol. 20, no. 5, 2021.

[12] M. K. Marina et al., "Multi-path routing for congestion control," IEEE Transactions on Networking, vol. 29, no. 3, 2021.

[13] Peter Maina Mwangi, "A Systematic Literature Review of Routing Protocols in Wireless Sensor Networks: Current Trends and Future Directions", International Journal of Research in Advent Technology, 2024, https://doi.org/10.32622/ijrat.124202401

[14] Anwar, Raja Waseem, "Trust-based energy-efficient routing protocol for wireless sensor networks", 2022, https://core.ac.uk/download/574070989.pdf.

[15] Jaafar Sadiq Alrubaye, Mohamed H Ghaleb Abdkhaleq, "A Comprehensive Review for different perspectives in Ad-Hoc/ Cellular VANET Networks: Taxonomy, Challenges, Routing, Future Directions", Wasit Journal of Pure Sciences, 2024, https://doi.org/10.31185/wjps.594.

[16] Anees, J., Zhang, H. C., Baig, S., & Lougou, B. G. (2019). Energy-efficient multi-disjoint path opportunistic node connection routing protocol in wireless sensor networks for smart grids. *Sensors*, *19*(17), 3789.

[17] Threshold-Sensitive Energy Efficient Network and Low Energy Adaptive Clustering Hierarchy Protocols' Performance Appraisal in Wireless Sensor Networks", *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 5, pp. 8677-8685, 2020. Available: 10.30534/ijatcse/2020/255952020.

[18] A. Srivastava, A. Prakash and R. Tripathi, "Location based routing protocols in VANET: Issues and existing solutions", *Vehicular Communications*, vol. 23, p. 100231, 2020. Available: 10.1016/j.vehcom.2020.100231.

[19] Behera, T. M., U. C. Samal, and S. K. Mohapatra. "Routing protocols." In *Computational Intelligence in Sensor Networks*, pp. 79-99. Springer, Berlin, Heidelberg, 2019.

[20] D. Pandey and V. Kushwaha, "An exploratory study of congestion control techniques in Wireless Sensor Networks", *Computer Communications*, vol. 157, pp. 257-283, 2020. Available: 10.1016/j.comcom.2020.04.032.

[21] R. Vishnuvarthan, R. Sakthivel, V. Bhanumathi, and K. Muralitharan, "Energy-efficient data collection in strip-based wireless sensor networks with optimal speed mobile data collectors", *Computer Networks*, vol. 156, pp. 33-40, 2019. Available: 10.1016/j.comnet.2019.03.019.

[22] A. Sharma and R. K. Ranjan, "Performance Comparison of AODV, DSR, and DSDV Routing Protocols in Mobile Ad Hoc Networks," *IEEE Access*, vol. 8, pp. 45032-45041, 2023. DOI: 10.1109/ACCESS.2023.4503201

[23] M. Gupta, P. Kumar, and S. Singh, "Comparative Analysis of MANET Routing Protocols: AODV, DSR, OLSR, and DSDV," *IEEE Transactions on Mobile Computing*, vol. 11, no. 3, pp. 212-219, 2022. DOI: 10.1109/TMC.2022.3214521

[24] H. Patel and L. Sharma, "A Survey on Proactive and Reactive Routing Protocols in Wireless Sensor Networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 34-55, 2022. DOI: 10.1109/COMST.2022.3298745

[25] V. N. Thakur and S. K. Sharma, "Performance Evaluation of DSDV, AODV, and OLSR Protocols in Vehicular Ad Hoc Networks," *IEEE Vehicular Technology Conference*, 2023. DOI:

AUTHORS

Fortine Mwihaki Mata is a Lecturer in Computer Science at the Department of Computing and Information at the University of Embu, Kenya. She received both her Bachelor of Science degree in Computer Technology and an MSc. In Software Engineering from Jomo Kenyatta University of Agriculture and Technology, Kenya (2014 and 2018 respectively). She's currently a PhD student at Murang'a University of Technology, Kenya. Her research interests are; Cyber security, and Network security. She is a member of the International Association of Engineers (IAENG).

Geoffrey Muchiri Muketha is Professor of Computer Science and Director of Postgraduate Studies at Murang'a University of Technology, Kenya. He received his BSc in Information Sciences from Moi University, Kenya in 1995, his MSc in Computer Science from Periyar University, India in 2004, and his PhD in Software Engineering from Universiti Putra Malaysia in 2011. He has wide experience in teaching and supervision of postgraduate students. His research interests include software and business process metrics, software quality, verification and validation, empirical methods in software engineering, and computer security. He is a member of the International Association of Engineers (IAENG).

Gabriel Ndung'u Kamau is Senior Lecturer and Director of Open and Distance Electronic Learning at Murang'a University of Technology, Kenya. He obtained his BEd (Arts) Degree in Mathematics and Business from Kenyatta University in 1999. He holds a Master of Business Administration in Management Information Systems in 2008 from the University of Nairobi. He holds a PhD in Strategic Information Systems in 2017 from the University of Nairobi. He is a specialist in Network Security and Big Data Analysts.