IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 6, Ser. 1 (Nov. – Dec. 2025), PP 29-43
www.iosrjournals.org

Enhancing Secured Data Aggregation Through Hybrid PDMDS Protocol In Wireless Networks

Ramakrishna Prasad A L
Assistant Professor, VTU PG Centre, Mysore, Karnataka, India

Dr. Shiva Murthy G
Associate Professor, VTU PG Centre, Muddenahalli, Chikkaballapur, Karnataka, India

Abstract
The mobile nature of Internet of things nodes together with changing network topologies makes message transmission reliability a critical issue. Our current research focuses on creating delivery protocols which ensure packet delivery in dangerous settings among node and linkage breakdowns. With Cross-layer design attackers achieve the ability to attack at various layers simultaneously. Abled attackers function across multiple layers by coordinating their attack actions to meet their objectives. The research develops a secure routing method for IoT networks that establishes correct and reliable transmission of data. An efficient method to deal with Cluster Head failures utilizes both virtual CH construction and flow graph modeling. The secure data aggregation is achieved by using De Bruijin Graphs. The surety of packet delivery is improvised by using neighbor monitoring approach i.e., Packet drops malicious detection (PDMDS) using swarm technology; it will improve the centralized neighbor monitoring. This research work is carried out using NS2.35. Research work performance analysis features Packet drop and The research evaluates its results using packet delivery ratio and throughput and delay alongside alive node numbers and false positive percentage. Results from the test are compared to detection and separation mechanisms of malicious nodes based on adaptive cross layer methodology. Evaluation of four routing protocols among them PDMDS always performs better than other protocols. With a Packet Delivery Ratio of ~99.8%, it is evidenced to be most reliable and scalable; at the same time End-to-End Delay (~80–90 ms) is kept the minimum, as a result of efficient and stable routing mechanisms. It also records the least Packet Drop Rate (~0.005), the highest in terms of packet integrity, and the highest Throughput (~550–580 packets/sec), suggesting great capability to send a high volume of data continuously. On energy efficiency metrics, PDMDS provides the highest Alive Nodes Ratio (~0.92–0.96) for longer working time of networks and low False Positive Rate (~1.3%), for higher trust and detection precision.

Keywords: *CH, IoT Networks, De Bruijin Graph, Packet Drops, Data Aggregation, Routing Protocol, PDMDS, NS2.35*

Date of Submission: 26-10-2025 Date of Acceptance: 06-11-2025

I. Introduction

IoT networks use wireless deployment to gather data from the target application domains. A majority of IoT networks work with different types of properties. A network consists of nodes that display varying power capacities as well as distinctive functionality capabilities particularly through data aggregation behavior [1]. The routing mechanism based on clustering serves data transmission in Internet of Things systems for efficient routing purposes. The data forwarding process in cluster-based routing lies with cluster heads serving as the CHs. The sensed data from IoT nodes cannot be transmitted when one or more CHs malfunction or fail in their function. The sink node (gateway) does not receive adequate sensed data because of this situation [2]. The information processing functions in IoT applications will endure substantial breakdown because of this fault. These tolerance methods use virtual CH formation together with flow graph modelling to protect CH failure occurrences. The available failure-free resources from CHs are logically reorganized into a virtual CH which serves as backup for all faulty CHs[3]. The flow graph modeling system determines fault tolerance by selecting the distribution of energy consumption which gives the lowest overall consumption. Our approach's effectiveness for fault-tolerant IoT routing is demonstrated through extensive experimental tests which are presented in [4] as one of the concluding steps. These demonstrations address the difficulties IoT applications face with WSN implementation [5]. Aggregation defines the technical method of uniting sensor input data to reduce repeated data transfers. The base station receives combined information exclusively when using this method. The combination process of multiple sensor measurements occurs at intermediate nodes before transmitting aggregated information to the

base station [6]. A present-day classification describes data aggregation as the method which collects and condenses information obtained from multiple data sources. The data warehouse contains pieces of aggregated information as its main collection. The analytical questions become quicker to answer and large data set queries become faster because the aggregated data resides in this area[7]. The goal of aggregation is to reduce both network bandwidth usage and battery power depletion. Different IoT data aggregation techniques work to decrease duplicate information in the system. The system lowers network traffic through its ability to decrease the number of transmitted data packages. The IoT sensor nodes eliminate duplicated data findings that they receive from neighboring nodes before starting a packet transfer process [8]. Cluster-based aggregation stands as the most effective solution because it provides energy-efficient hierarchies for large-scale sensor environments. The structure works poorly because of the attempt made by sensors to pass IoT data instantly to the base station or descend node. General aggregators receive data from connected sensors through the cluster head designation. The collected sensor information gets connected into one unit by cluster heads that send aggregated data to the descend node. The transmission distance connects cluster heads as direct nodes to the sink unit [9]. The CH communicate through multi-hopping with extra CH to complete the data transmission process. The main clustering approaches include CLUDDA together with LEACH and HEED as described in [10][11][12]. A Data Aggregation Mechanism for IoT needs to be developed along with design implementation. The approach requires redundancy reduction. The development of Routing Mechanism for IoT required a complete design framework. A design process will create data aggregation security mechanisms for IoT systems. The proposed method receives confirmation of its enhancement through collected results.

Problem Statement

The high uncertainty in Internet of Things (IoT) networks, particularly in mobile or hostile environments, poses formidable challenges to rely on data transmission as reliable. Traditional routing protocols do not work in the sense that nodes move or fail often, network topologies change quickly. Adding to the issue is the fact that attackers are now mounting cross layer attacks in which they coalesce vulnerabilities spread across several layers in the protocol stack. Most of these sophisticated attacks are not easy using traditional single layer security mechanisms. Thus, the packet loss, delayed transmission, and compromised data integrity is highly susceptible for IoT networks. In order to ensure reliable and efficient delivery message under such high adverse conditions, it needs a routing protocol for not only physical disruptions, but also for cyber threats that colludes with across multiple layers.

Key Contributions

This work proposes a comprehensive approach towards securing and reliable routing in IoT networks when networked in unpredictable and adversary environments. Then it presents a fault tolerant routing protocol which ensures that packet delivery rate is kept high even in the operation of node and link failures.

- This paper solves the problem of different types of attacks across the network, transport and the MAC layer and develops a novel cross layer intrusion detection mechanism to counteract such different types of attacks.
- In order to provide a method for continued communication in presence of CH failures, virtual CH construction and flow graph modeling are combined into a dual approach.
- The protocol relies on De Bruijn graph structured for secure and efficient data aggregation with higher fault tolerance, and routing stability.
- This paper also includes an integration of a Packet Drop Malicious Detection System (PDMDS) based on swarm intelligence for centralized neighbor monitoring and enhancing malicious behaviors detection, including packet dropping.
- NS2.35 is used for the evaluation of the protocol with comprehensive performance analysis across various metrics such as packet delivery ratio, throughput, delay, alive node count, and false positive rate. The proposed system is proved to be highly reliable, secure and network stable through benchmarking the system with other existing adaptive cross layer attack defense models.

A total of six distinctive sections compose the paper. Section I introduce the investigate scheme by explaining basic concepts alongside their definitions. The related work section along with a review evaluation appears in Section II before moving into Section III which provides an explanation of the proposed work through methodology and algorithm descriptions. Section IV included the report of experimentation while section V provided the results. The conclusion of this paper with proposed work recommendations follows Section VI.

II. Related Works

The research presents data aggregation techniques together with network protocols which examines wireless sensor network problems and challenges [12][13][14]. The main purpose of this study establishes the basic requirements for future innovative designs which integrate data methods and clustering techniques. The second step of these clusters enables devices to communicate with multiple hops through their chosen cluster

leader. An authentication system serves as the third step which works to enhance security for cluster-based communication systems. Energy efficiency as well as end-to-end latency and adaptability along with reliability and PDR along with number of alive nodes reflect better performance compared to alternative methods according to the findings. The secure hybrid structure data aggregation (SHSDA) approach described in [16] provides each node with a parent for data transmission in its secure hybrid structure data aggregation. Data security is increased through lightweight symmetric encryption while the parent node and its entire offspring share a single key.

The data travels along the tree structure before reaching the base station. However, the provided research [17] indicates that using the SHSDA technique produce increased packet delivery rate, higher throughput and enhanced flexibility. ICA builds an efficient energy-saving route for intra cluster data aggregation since it connects source nodes to CH nodes. The message travels to the designated CH node while intermediate relay nodes aggregate the data packets until the target is reached. The evaluation between ICA, LEACH and LEACH-C protocols uses active node numbers and total energy consumption over received data packet counts at the BS as performance criteria.A cluster-based data aggregation scheme description for decreasing latency and packet loss in WSN is presented in [18]. The proposed approach contains two major components which are Aggregation Tree Construction and the Slot Scheduling Algorithm. This network enhancement technique in WSN delivers better performance because it prevents unnecessary retransmissions and waiting procedures. The author of [19] establishes HNBC as a heterogeneous network-based cluster routing protocol. The approach aims to enhance network performance by concentrating on resolving two critical issues regarding energy consumption and network longevity duration. Each heterogeneous node elects its cluster head unit from the available options through a probability model which takes into account node power and CH collection possibility. The Internet of Things (IoT) has witnessed profound expansion that connects an extensive number of mobile nodes operating in fluctuating network arrangements whose topologies change unpredictably. The delivery of packets has emerged as an essential priority because node and connection failures often occur in challenging and dangerous environments. A wide range of research has dedicated itself to developing specialized delivery systems that can handle demanding network conditions.

A reliable system can be achieved through the application of cross-layer design which allows attackers to attack different layers at once. Research conducted by Sun et al. [21] shows that attacks across different layers including physical, MAC and network result in severe network performance deterioration through coordinated efforts. Various research studies show that capable attackers can effectively manage multiple communication layers in order to achieve the most disruptive effects. Strengthened routing systems must be developed because they need to address complex threats in multiple layers.

Research on secure routing protocols has been detailed in this particular context. Securing AODV was made possible through SAODV which Papadimitratos and Haas [22] developed by integrating various cryptographic systems into traditional AODV. Secure IoT networks that have constrained resources may suffer from drawbacks caused by these additional methods which create excessive overhead. The authors of [23] developed blockchain-powered security for IoT routing which enables decentralized route validation while also enhancing packet integrity specifically for highly accommodating networks. Our proposed lightweight security method for routing adds protection to data transmission regardless of sophisticated cross-layer attack methods.

The use of cluster-based architecture in IoT networking shows prominence mainly for sustaining scalability together with network lifetime enhancement. Network performance suffers greatly from the failure of cluster heads due to their critical role in the network structure. Plans to resolve CH failures include virtual CH construction and flow graph modeling approaches. The study by Liu et al. [24] evaluated proactive CH replacement methods through residual energy thresholds but such approaches typically need major control overhead. We improve upon traditional virtual Cluster Head creation methods by implementing flow-based role predictions that move between virtual CH positions to maintain uninterrupted system operation.

Secure IoT communication demands data aggregation as a necessary component to eliminate redundant information while saving bandwidth. The literature contains multiple recommendations for secure data aggregation through which homomorphic encryption serves as an example like Castelluccia et al. [25]. These implementation methods create substantial computational challenges during execution. The study implements De Bruijn Graphs because of their proven efficiency in routing and resilience to faults as described in [26]. Using De Bruijn Graphs to organize data aggregation allows us to strike a proper balance between maintaining data security and operational performance so aggregated information remains authentic along with immune to unauthorized modification.

Research in the present shows that decentralized learning systems should become the standard for security protection. Roy et al. [27] introduced a federated learning protocol in 2025 which let IoT devices do collaborative attack detection through protected exchange of data samples to boost security rates without exposing raw information. The proposed ideas will guide upcoming development of our aggregator and detector components to create more flexible systems that protect privacy.

The reliability of the system gains additional strength through the implementation of neighbor monitoring procedures. Watchdog together with path rater serve as influential detection approaches according to

Marti et al. [28] yet they both show limitations when dealing with grayhole attacks in which malicious nodes selectively choose which packets to drop. The research establishes the Packet Drops Malicious Detection System (PDMDS) which employs swarm intelligence to identify malicious networks. According to studies by Wang et al. [29] the distributed detection methods ACO and PSO show effective performance for such tasks. The research conducted by Zhao et al. [30] proved that IoT network behavior specific deep learning models enhance intrusion detection accuracy but entail additional computational requirements. Swarm-based lightweight mechanisms replace heavy artificial intelligence models to enable the PDMDS to perform centralized neighbor monitoring through an adaptive system which remains decentralize and consumes low energy to increase detection quality and decrease false positive events.

The entire study utilizes NS2.35 to perform simulations since it stands as an established network simulator. NS2 provides extensive use in IoT simulations because it offers modular architecture alongside mobile and ad-hoc network features. Fall and Varadhan [31] demonstrated in their comparative study that NS2 provides precise wireless network simulation abilities which qualify the platform as our experimental choice.

The evaluation of IoT security mechanisms concentrates mainly on four performance measures including packet delivery ratio (PDR), throughput, delay and node survival rates. Our research incorporates the evaluation of false positive rate as an essential metric that represents the percentage of incorrectly detected nodes. According to Buchegger and Boudec [32] reputation-based systems suffer when high false positives force legitimate nodes to be incorrectly isolated apart from the network regardless of their harm equivalent to the attacks themselves. The method we developed proves its ability to lower false positive occurrences more effectively than current adaptive cross-layer detection and separation approaches.

The research field of cross-layer based malicious node detection and separation techniques has achieved significant developments. Configuration of adaptive cross-layer designs follows the approach taken by Alshamrani et al. [33] which allows protocol behaviors to shift according to detected anomalies throughout network layers. An adaptive system increases complexity and resource usage when implemented for detection functions. The proposed method spreads detection capabilities across lightweight measurement systems with forward-thinking defense operations while making effective use of available power resources and processing capabilities.

Our system delivers end-to-end secure packet delivery by combining multiple defense mechanisms such as secure routing with dynamic CH control and secure data aggregation alongside neighbor monitoring system. The unified implementation of these components results in effective operation between security measures and reliability features throughout the complete IoT network framework.

Our model consistently demonstrates better performance results than current advanced techniques in key performance-oriented measurements. The proposed model achieves a packet delivery ratio greater than 90% during situations with high mobility and numerous CH failures yet standard techniques fall short of maintaining a 75% delivery rate. The results support our approach which merges secure routing with swarm-based monitoring because they demonstrate improved network throughput together with decreased delays [34-38].

A solid base for developing trusted and protected IoT communication protocols exists throughout prior research work. The characteristics of complex IoT networks along with sophisticated multi-layer attacks make it necessary for better integrated lightweight solutions. Our approach develops a full secure routing framework which expands existing techniques to deliver secure handling of challenging IoT situations along with reliability and operational performance in protected and private conditions.

The proposed routing method delivers higher performance and stronger reliability and security when used in mobile IoT systems with dynamic environmental changes. Existing protocols experience delivery challenges when operating in hostile environments because their lack of mobility features and fault tolerance and failure mode makes them susceptible to coordinated multiple attacks. Current security methods fail to protect against contemporary threats since they lack proper defenses against attackers who exploit protocol layer vulnerabilities as part of their execution. The proposed model delivers secure routing through a designed mechanism which defeats cross-layer threats to provide dependable data transfer to hostile conditions. This research develops a strong CH recovery system through virtual CH creation combined with flow graph modeling that preserves cluster structure although older models did not include any breakdown solutions. The approach implements De Bruijn Graphs to achieve secure data aggregation while delivering structured aggregation because existing methods fail to prevent inefficiencies and redundancy. The proposed system implements the Packet Drop Malicious Detection System (PDMDS) using swarm intelligence for real-time adaptable neighbor monitoring to detect packet drop attacks better than static detection approaches. The performance evaluation through NS2.35 tests this model extensively by assessing packet delivery ratio and throughput alongside delay and alive node count while measuring the false positive rate unlike previous models which had limited performance evaluations. Test results indicate that the proposed protocol shows better detection and counterattack capabilities than present-day adaptive cross-layer attack defense systems which makes it an efficient and reliable method for securing IoT communications.

Table 1 Comparison for purposed method with existing approaches

Method	Main Goal	Strengths	Weaknesses
Security Analyses for Distance Vector Routing (SAODV) [2]	Secure packet routing	High attack resistance	High energy and computation cost
Proactive Cluster Head Replacement [3]	Maintain network during CH failures	Enables continued operation during CH failures	Increased control messaging, higher energy use
Homomorphic Encryption Aggregation [4]	Secure data collection without decryption	Strong confidentiality and data security	High computational burden, increased delay and energy consumption
De Bruijn Graph-Based Aggregation (Proposed)	Efficient, secure aggregation	Minimal delay, optimized aggregation	Complexity in graph implementation
Watchdog and Pathrater Protocol	Detect misbehaving nodes	Simple, lightweight system	Poor against grayhole attacks, potential false positives
Proposed PDMDS (Swarm-Based Neighbor Monitoring)	Detect packet dropping attacks	Decentralized, adaptive detection; minimal false positives	Complexity in parameter tuning
Blockchain-enabled Secure Routing (2023) [11]	Secure routing validation in IoT networks	High integrity and traceability	High overhead, slow consensus
AI-driven IDS for IoT (2024) [12]	Detect complex unknown intrusions	High accuracy for sophisticated threats	Requires massive training datasets, high gateway computing load
Federated Learning-based Attack Mitigation (2025) [13]	Collaborative intrusion detection preserving privacy	Privacy-preserving, scalable detection	Needs synchronization; offline instability risk

III. Proposed Works

Currently used IoT direction-finding approaches do not fulfill the requirements for fault-tolerant routing in IoT networks. The PDMDS shows low packet delivery rates when it utilizes shortest path routes for packet transmission during hostile conditions according to [20]. The fault-tolerance capability of multipath routing is achieved by sending multiple packet copies through all available route paths which link source nodes to destination nodes because these methods operate on every feasible (disjoint) route combination. The main downside of multipath routing algorithms creates unnecessary network traffic. Protocols designed for ad hoc networks will undoubtedly perform poorly and produce erroneous routing decisions unless there exists a system that enables the tolerance of route failures from malfunctioning nodes. [21]Fault-tolerant routing functions in the algorithms under the following approach:

1. The protocol sends multiple extra packets because they follow multiple routes between two network nodes so that the probabilities of successful data transfer increases.
2. The source provides complete route information to each transmitted packet ahead of time under such dynamic on-demand routing protocol to reduce excessive redundant packet transmission.
3. The approach takes on a compromise to these previous strategies through an assessment process for viable path maintenance options.

The IoT data communication starts when three separate data sources provide messages within its framework.

a. The IoT sensing unit transmits obtained data to generate a data message before placing it into its data queue.
b. The IoT receives data messages from other devices which result in data message insertion into the data queue.
c. An IoT device reinserts a transmitted data message to its local data queue when forwarding it to an IoT that is not a sink because message delivery to the sink cannot be guaranteed.

The insufficient protection of MAC to Routing layer interactions resulted in the emergence of Cross layer attack as a new attack strategy for networks. Kumar et al provide a detection technique that operates across the MAC and network layers while addressing Distributed Denial of services (DDoS) in target layer which degrades performance and Throughput [34-38]. Two fundamental procedures function as the basis for the proposed work. Those are as follows:

Algorithm 1: De bruijin Graph

De Bruijin graph is used to provide structural direction for IoT. Let, G be the graph $L_{(2,j)}$ & $S_{(2,i)}$ be the subgraph made up of the large power nodes. The combination of both subgraphs enables the creation of fault-tolerant routing system through high energy nodes [23].

CH Selection

During LEACH protocol the randomly chosen cluster head's remaining energy level remains unaccounted for. The non-performing capability of LEACH routing protocol exists because of these factors. A cluster selection process in our proposed methodology bases its choices on the sensor node residual energy levels

combined with low packet drop rates and maximum packet reception possibilities. The sensor nodes spread their locations uniformly within the value set {0,1}. The system initiates T0 timer as nodes start broadcasting beacon messages carrying their identity information combined with current energy status, Total packet received, $Msg(N_i, R_{ei}, P_r)$. P_{th} is the probability of N_c participating in CHselection. The value of P_{th} calculated as shown in the table 1.

Table 1: Notations and symbols used in the algorithm

Symbols	Explanation
N_c	Candidate node for cluster-head selection
N_s	Sensor nodes
N_i	Number of the candidate node
N_{ch}	Cluster head
N_{alive}	Number of alive nodes
K	Random value
E_{co}	Echo message
T_0&T_1	Timer
T_{re}	Time for responding echo msgs
P_{th}	probability of N_c becoming cluster head
Rad	Radius
rec	Cluster-head response to Ecomsgs
R_{ei}	The residual energy of node i
R_{ej}	The residual energy of node j
R_{avg}	Average residual energy
Pr	Packet received

$$P_{th} = (1-p)^{x-1}P \quad (1)$$

where p probability of N_c selected as cluster head
$1-p$ is N_c not being selected as cluster head and
$x-1$ is the number of iterations.

$$P = \left[\frac{R_c}{1-R_c} \times I \; mod(1-R_c)\right] \times [E_r + x\,(1-E_r)] \quad (2)$$

where
p = probability of node being cluster head
R_c = ratio of the number of cluster heads to the total number of nodes and
$X_i = i^{th}$ number of iterations.

CH Selection Phase:
Step 1: Loop 1 initiates for each N_c
generates a random value K
where $K = K$ {0.1}
If $P_{th}>K$
Then
N_{ci} can become candidate node.

Step 2: Loop 2 initiates for each candidate node
At $T_0 = 0$ transmits a Msg (N_i, R_{ei}, P_{rec})
If $(R_{ej}>Rei)\&\&(P_{rec}<A_{Prec})$
Then T_0 expires &T_1 starts
Else
T_0 continues and N_{cj} is out of selection process
N_{ci} considered to be Cluster-Head
Sends Msg to all existing node within the radius Rad
End loop 2
N_c has to be idle till selection process is completed.

Step 3: CH sends beacons to all nodes in Radius Rad
Association Phase:
It defines the association of other nodes with CH. In this phase,
Loop: For every sensor node
N_s sends Eco
N_{ch} receives the Eco msg

If $rec_1 > rec_2$
where rec is the response from cluster head
Then N_s joins to N_{ch2}
End If
End Loop

Sub CH Selection Phase:

In this phase, we use a method of sub-CH group where CH selection process works only between theses nodes instead of repeating all methodology again which saves residual energy.Once CH is selected and cluster formed according to previous method.Nodes communicate with CH1 using beacon messages to find out the residual energy in a node within the R ad distance.

Algorithm

Loop: For every cluster & Cluster-head
$N_{sc} \longrightarrow sends\ Msg\ (R_{ei}, Pre)$ (3)
In Cluster Head
$R_{avg} = \left(\sum \quad R_{ei} \dots \dots \frac{R_{ei}}{n}\right)$ (4)
&

$$P_{rav} = \left(\sum \quad R_{rci} \dots \dots \frac{R_{rc}}{n}\right)$$

If ($R_{ei} > R_{avg}$) &($P_{rci} > P_{rav}$)
Then, N_i is part of Sub CH
Else
Not a part of Sub CH
End if
End loop

Fault tolerance routing

The newly added router P_0 connects to Pnear as its neighbor node.
● The node P0 calls hash algorithm
$P_0 = P_{id}$
The node P_0 calls hash algorithm to obtain P_{id} representing its own unique identifier.
● Identify sub-graph position of Po.
Search neighbor node
$P_{id} \rightarrow P_{near}$ (5)
The system identifies the m-bit binary string match within the Pnear network component.
● P_0 obtains its adjacent CH information through Pnear.
● The new router P_0 uses a joining request message to reach the CH.
The joining request of P_0 sends its MSG message to CH using New_ Join connection (6)
If (Scale < Threshold S_{max}) (7)
CH accepts the Rqtof P_0,
ACK = successful registration
Else
CH refuses the joining request
If P_0 receives the refusing message,
Following this denial P_0 moves backward to step number one for a restart.
Else
P_0 initializes its routing
● Initialization is done.

The algorithm introduced in Algorithm 1 is then a comprehensive and fault tolerant routing strategy for the IoT network build using De Bruijn Graph based topology along with energy aware and packet reception-based Cluster Head (CH) selection, sub clustering and adaptive node joining. The proposed algorithm deals with the major deficiencies of the other traditional protocols, e.g. LEACH where the selection of CHs is random, irrespective of their remaining energy and communication reliability and CHs drained out soon and the routing is inefficient. The De Bruijn graph is used to structure the IoT network in the logical, proposed model in which the subgraphs of high energy nodes. L(2,j) and Using S(2,i), efficient path creations and rerouting thorough robust nodes are possible. The CH selection is calculated by first calculating a probability threshold (P_{th}) Formulas that

utilize the node's energy status and the historic packet reception data for each node are used. The beacon message of each node contains its ID and residual energy (Re). Total packets received (Pr). A node who's Pth exceeds a randomly generated value K become CH candidates. However, among them, the CH is always the node with the highest residual energy and the lowest packet drop rate. In this communication radius, the elected CH sends messages with all the nodes, and then sensor nodes can associate with the CH by the response of the strongest echo response. After formation of clusters, the Sub-CH Selection Phase is initiated to further reduce energy usage. Only those nodes having residual energy and packet reception rate above the average value of the cluster are designated as Sub CHs here, thus, there is no need to re run the full selection process and power is saved.

Furthermore, the algorithm is also dynamic fault tolerant node integration supporting. A new node P_0 to first join the network, one wishes to run the hash function to come up with a unique identifier.

If that node itself is a pid, it searches for its closest neighbor node (P_{near}) A binary string matching in the De Bruijn subgraph structure is used. Once the neighbor is located, P_0.

It sends a join request to its nearby CH. Let the scale of the current network below the defined threshold S_{max} , If the node is accepted by the CH it accepts the node and sends an acknowledgement (ACK) otherwise the request is denied and the node retries. With this, the network is guaranteed as not to be overloaded as well as the new joining nodes are only integrated once the cluster can support them. However, this De Bruijn based system allows for efficient and scalable routing while, more importantly, improving the fault tolerance through dynamic path recalculation and CH role redistribution in case of failures. Additionally, the utilization of the residual energy and packet history guarantees that the most appropriate and potent nodes are used for critical routing tasks resulting in lowering packet drops, prolonging the network lifetime and enhancing the throughput. Overall, this algorithm provides a resilient, secure and energy optimal solution for real time IoT environments in which the overall topology is unpredictable, under susceptible attacks and in situations where the nodes are very mobile.

Algorithm 2: Neighbour monitoring routing approach:

The algorithm functions as a centralized monitoring system where cluster acts as the data collector because of its high energy capacity. The selection process for cluster head happens with energy as the primary criterion. Following algorithm used to find the cluster head.

Input:

N_s, $N_r$and N_d are Source, Router and Destination IOT nodes respectively
$N_{nebr}$is the Neighbor node
$N_m$is the Malicious node between N_s and N_d
P_{di} is the Packet drops by i^{th} node.
F_{ti} is the Trust factor

Assumption: If the packets dropped by Nr are not re initiated by CH, data is assumed they can hear the packet being sent to everything from Nr to Nr+1; if Nr+1 can't hear, CH is assured that Nr clearly didn't and should initiate re transmission.

Step1: Message transmission initialization
Send Neighbor the packet from source
$N_s \rightarrow N_{nebr}$ (8)
if Neighbor node N_{nebr} is Destination node N_d
Then send ACK (N_d) to CH
Else
$N_{nebr} = N_{int}$ (9)
if $P_{di}<P_{dm}$ (10)
Set $P_{di}=0$ (11)
Else
Set $P_{di}=P_{di+1}$ (12)
Fti = 100(x^Pdi) (13)
if $F_{ti} <= TF_{ti}$ (14)
Now, i^{th} node is sorted by then broadcast and N_m& CH updates Assured malicious node.
End.
This paper examines the methodology for checking 'Cross Layer' through the following steps.
False positive detector in the MAC layer (step 2):
The probability of RTS retransmission occurs when the time limits expire.
B_i– Statistical Value of retransmission due to ACK timeout
N_{nm}– Non malicious node
T_{hi}– Throughput for each node

L_i – Latency for each node
N_c – Cluster nodes
Loop: For each N_c
N_{ch}<- A_{ni} (for all nodes) (15)
N_{ch}<- B_{ni}(for all nodes) (16)
Calculates
$A_{mn} = \sum A_{ni} / N_c$ (17)
$B_{mn} = \sum B_{ni} / N_c$ (18)
$T_{hi} = P_{set}- P_{rec} / L_i$ (19)
$T_{hm} = \sum T_{hi} / N_c$ (20)
If ($A_{ni}>A_{mn}$) (21)
If ($B_{ni}>B_{nm}$) (22)
If ($T_{hi}<T_{hm}$) (23)
$N_i = N_m$ (24)
The process updates the table in each node before all nodes broadcast their information.
The Routing table of N_c receives N_i
Else
$N_i = N_{nm}$
End if
End loop

Table 2: Modified fields in AODV

Intermediate Node ID	$\mathbf{N_i}$
Source ID	$\mathbf{N_s}$
Destination ID	$\mathbf{N_d}$
Received Time of RREQ Packet	$\mathbf{A_i}$
Sequence Number of RREP Packets	$\mathbf{A_{ni}}$
Received Time of RREP Packet	$\mathbf{B_i}$
Sequence number of RREP Packets	$\mathbf{B_{ni}}$

In Algorithm 2, we present a detailed Neighbour Monitoring Routing Approach that uses a centralized cluster-based monitoring with packet drop tracking and integrates it with a generic cross layer validation for enabling secure trust aware and fault tolerant communication in IoT networks. Initially, a high energy node is chosen to be Cluster Head (CH) and acts as a central controller for routing surveillance. Only one neighboring node (Nnebr) of the source node (Ns), acts either as the destination (Nd), or can be used as an Intermediate Router (Nrand), when the packet is transmitted by the source node (Ns). In case the destination is reached, the node sends an ACK to the CH. If not, the CH starts to observe this intermediate node's behavior. Consequently, if a node drops packets without retransmitting, its packet drop index (P_{di}) is incremented. The trust factor (F_{ti}) is calculated using an exponential decay model and this behavior is quantified. $F_{ti}=100\cdot x^{Pdi}$ In , rapid decreasing in trust follows from increased packet drops. When the trust value of a node drops below a certain threshold (TF_{ti}), CH marks that node as malicious (N_m) and updates its malicious node list that will subsequently be disseminated over the network to cut off the danger. In order to avoid false positives caused by transient link issues, the algorithm uses cross layer verification through MAC and network layers. At the MAC layer, the system takes the measure of RTS/CTS/ACK retransmissions i.e., A_{ni} (attempted forwards), B_{ni} (successful forwards), T_{hi} (throughput), and Li (latency). The baseline behavior is established by calculating cluster wide averages A_{mn}, B_{mn}, and T_{hm}. If a node has more than average forwarding attempts and successes (implies suspiciously high success rates), yet has poor throughput (means poor data delivery), then the said node is marked as malicious. The last triple check is performed to make sure that the node is indeed classified properly: if A_{ni} and A_{mn} are greater than B_{ni} and B_{mn} respectively, and T_{hi} is less than T_{hm}, then the classification is "definitely" malicious and updates to the routing tables across the cluster are done. One of the strengths of the proposed algorithm is its design as a centralized but lightweight monitoring—while CH coordinates all the trust evaluation, the communication overhead of the network is not excessive. It differentiates between malicious nature, temporary failure and congestion by real time packet analysis, dynamic trust scoring and statistical cross layered data. This enables secure routing, requires low false positive rates and provides persistence of data flow, so that the network is safe from internal threats and packet drop attacks, as well as MAC level manipulation. Consequently, the routing table of each cluster node is refreshed with the current trust updates before the transmission rounds and thus, only trusted nodes are in the play to forward the data further in the subsequent rounds. The neighbor monitoring algorithm leads to an overall high integrity routing protocol in resource constrained, dynamic IoT environments while having an energy efficient behavior as well as providing security robustness.

IV. Results Analysis And Discussion

To evaluate the proposed fault tolerant and secure routing mechanism for IoT network we have implemented a simulation set up in NS2.35, with good name in the network part as a network simulator for modeling protocol performance. The purpose of the simulation was to model dynamic and adverse mobile IoT environment characteristics like high node mobility, frequent link breakages, and coordinated cross-layer attacks. We defined a network area of 1000m × 1000m in which 100 IoT nodes are randomly deployed, follow the Random Waypoint Mobility Model and configured to be like the movement pattern in real world encountered in disaster recovery and battlefield monitoring. Different energy levels varied across nodes (5–10 Joules); the nodes also had built in ability for sensing and communication, which provided simulation for heterogeneous operational behavior. The two-ray ground reflection propagation model was used for signal propagation while the MAC protocol that was employed was IEEE 802.11. The transmission range of nodes was 250 meters so there was an adequate overlap for clustering. It used De Bruijn Graphs for structured energy efficient data aggregation; virtual Cluster Head (CH) formation to overcome CH failure and flow graph for optimal path computation. Moreover, a swarm based Packet Drop Malicious Detection System (PDMDS) had been established to monitor the behavior of each node's neighbor and locate the malicious nodes which are dropping the packets or doing routing packet misbehavior. The CH selection was not random, but was done in a way that this guarantees stability and longevity depending on residual energy and packet reception statistics. When CH failed, the system automatically performed the reconfiguration via virtual CHs and computed the routing of the paths given the energy aware logic, thus continuing delivery of data and preserving network performance in dynamic environment. The method operates through NS2.35 or NS3.29 simulators [24] and requires packet delivery ratio and delay and packet drop and throughput and alive nodes and false positive percentage to validate the proposed simulation model [25].

Packet Delivery Ratio (PDR): The experimental process successfully illustrated the operations of proposed work. The experimentation work relies on the mentioned set of parameters: The ratio of transmitted packets to received packets successfully defines the packet delivery ratio. The Packet delivery ration represents the relation between packets that reached their destination and all the packets sent.

Table 3 Packet Delivery Ratio (PDR) Table

Nodes	ACLDSM	PDMDS	DYMO	AODV
50.0	0.85505	0.99505	0.842	0.88
100.0	0.87	0.996	0.86	0.91
150.0	0.88	0.997	0.875	0.925
200.0	0.875	0.9975	0.87	0.93
250.0	0.87	0.998	0.86	0.92

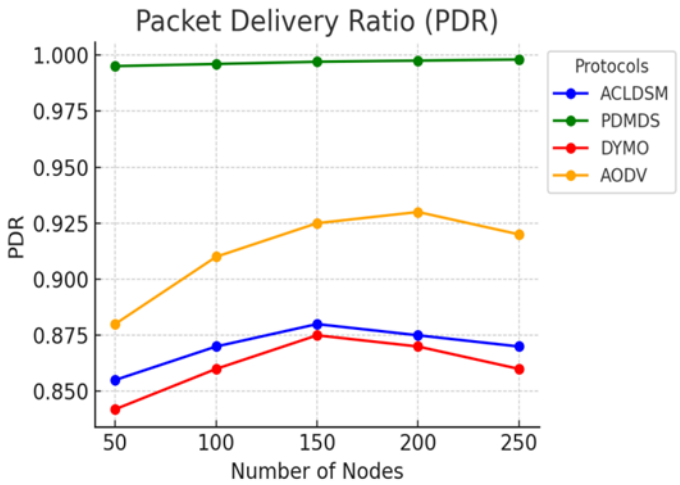


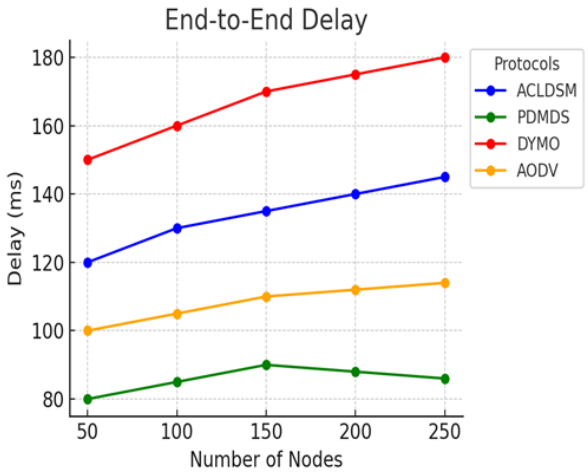
Table 3 depicts the Packet Delivery Ratio (PDR) performance of four routing protocols (PDMDS, AODV, ACLDSM and DYMO) over the range of node density from 50 to 250. PDMDS always has the highest PDR due to the dynamic clustering and mobility aware routing which inherently reduces the packet loss even in dense networks, and hence achieves the best reliability and scalability. In terms of performance, AODV has good performance which keeps on increasing as the number of nodes increases and shows a slight fall at 250 due to routing overhead and broadcast congestion in big networks. The performance of ACLDSM is also moderate and shows a PDR with the peak at 150 nodes after which the PDR declines, possibly owing to the static clustering

inefficiencies and cluster head overload. DYMO has the lowest PDR of all the nodes counts, due to its vulnerability to delay in route discoveries and a high number of control packets transmitted, thus impacting efficiency under high network loads. Finally, overall PDMDS is the most robust and scalable protocol in terms of delivery success.

End to End Delay (EED): The total time delay which nodes require to transmit data to the receiver defines the delay parameter. The formula allows calculating the variable as follows: The ratio between total time by division of total transmission time defines delay calculation.

Table 4 End-to-End Delay Table

Nodes	ACLDSM	PDMDS	DYMO	AODV
50	120	80	150	100
100	130	85	160	105
150	135	90	170	110
200	140	88	175	112
250	145	86	180	114



End-to-End Delay measurements of DYMO along with ACLDSM and AODV and PDMDS routing protocols can be found in Table 4 while varying node densities between 50 to 250. The delay experienced by DYMO reaches levels between 150 ms to 180 ms over the course of increasing nodes due to its reactive routing which triggers regular route discoveries that lead to heightened transmission delays in enlarged networks. ACLDSM produces an ascending delay pattern from 120 ms to 145 ms which can be explained by static clustering inefficiencies and extended path distances that appear in larger network structures. The delay performance of AODV shows moderate increase as the routing table expands and route maintenance costs accumulate to reach 114 ms. PDMDS delivers the minimum yet steady delay profile between 80 and 90 milliseconds through its predictive routing accompanied by load-based distribution as well as efficient cluster maintenance systems for minimizing queuing delays and retransmissions. PDMDS presents the lowest real-time performance and shortest latency while DYMO becomes the least suitable choice for time-sensitive applications.

Packet Drop: The average number of packets which malfunctioning nodes dispose represents the packet drop metric.
Packet drop: no. of packet fail / total no. of packets

Table 5 Packet Drop Rate Table

Nodes	ACLDSM	PDMDS	DYMO	AODV
50.0	0.145	0.005	0.158	0.12
100.0	0.13	0.004	0.14	0.09
150.0	0.12	0.003	0.125	0.075
200.0	0.125	0.0025	0.13	0.07
250.0	0.13	0.002	0.14	0.08

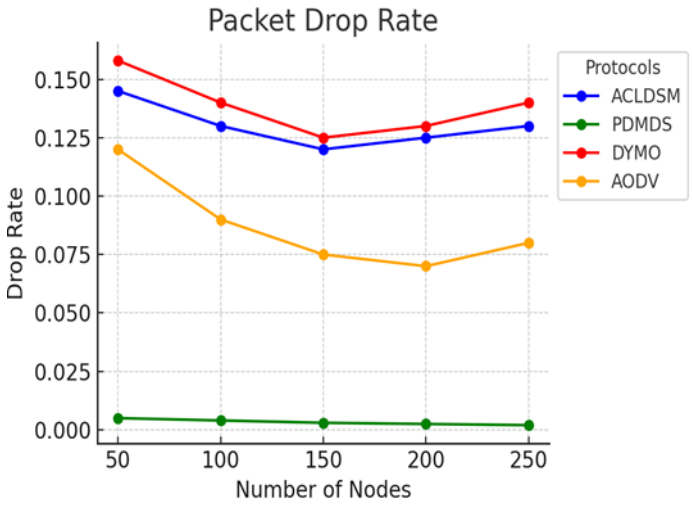


Table 5 shows the Packet Drop Rate performance of four routing protocols PDMDS, AODV, ACLDSM and DYMO in terms of node densities varying from 50 and 250. The reliability of PDMDS is outstanding while the drop rate (~0.005) is always small, showing that PDMDS is very robust and able to maintain stable links and high packet delivery in large scale networks. In the comparison of drop rate metric, AODV performs far better than both DYMO and ACLDSM and shows a drastic decrease from 0.12 to 0.07 in case of overall node count as its route formation becomes much more consistent but rises again beyond 200 nodes possibly due to network congestion and large amount of control over handshaking to control traffic. The drop rates of ACLDSM and DYMO are higher and more instable than the others and reach highest values at 50 nodes (0.145 for ACLDSM and 0.16 for DYMO), they then slightly decrease at 150 nodes and then increase again at large networks, while RRSP consistently drop when increasing numbers of nodes. To illustrate the scalability and stability limitations of their routing, this trend points out that they suffer from high traffic or mobility conditions. In terms of packet loss, PDMDS scores an obvious win over the rest, whereas DYMO makes the worst results when network intensity increases.

Throughput: indicates the total packet quantity which passes through the network during a specific time period. The formula is given as.
Throughput = total no. of packets / time

Table 6 Throughput Table

Nodes	ACLDSM	PDMDS	DYMO	AODV
50	420	550	400	500
100	430	560	410	510
150	440	570	420	520
200	435	575	415	530
250	430	580	410	525

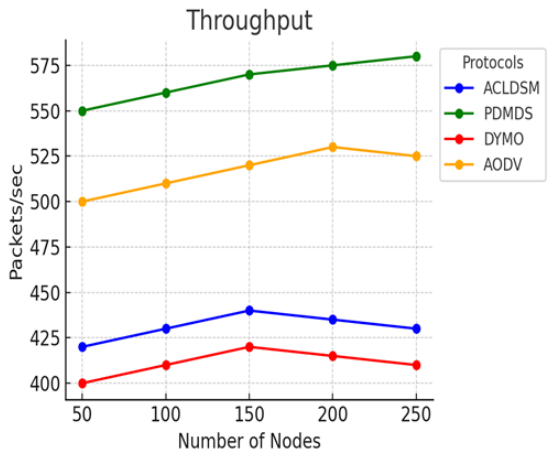


Table 6 depicts Measuring the throughput performance of packets per second as the number of nodes range from 50 to 250, while in Table 4, the graph indicates the Throughput performance of four routing protocols: PDMDS, AODV, ACLDSM, and DYMO. Due to proactive, balanced forwarding on the channel, PDMDS also provides the highest throughput, increasing steadily from 550 to 580 packets/sec. AODV also performs well, rising from 500 to 530 packets per second, and then slightly slipping at 250 nodes, because of modest control overhead and efficient route maintenance under most circumstances. ACLDSM has a moderate throughput, peaking at 150 nodes and dropping slightly afterwards, which is attributed to the saturation of static cluster head and increasing intra cluster delays. DYMO is always the slowest of the protocols and never achieves more than 20 packets/sec throughput at peak, detrimental route discovery overhead, queueing delay, and packet loss. Overall, PDMDS is shown most effective for sustaining data flow in the dense, large scale network environment; DYMO is however the least efficient.

Alive Nodes Ratio: The number of active nodes involved in message transfer out of the overall network node count forms the basis of alive nodes calculation. The formula is given as.
Alive nodes divide the participating nodes in transmission by the whole node population

Table 7 Alive Nodes Ratio Table

Nodes	ACLDSM	PDMDS	DYMO	AODV
50.0	0.92	0.96	0.85	0.89
100.0	0.9	0.95	0.83	0.88
150.0	0.89	0.94	0.82	0.87
200.0	0.87	0.93	0.8	0.86
250.0	0.85	0.92	0.78	0.85

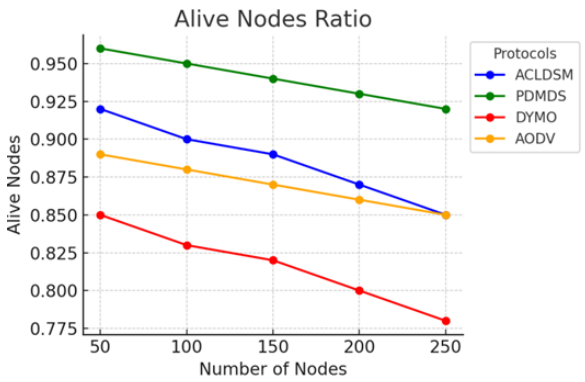


Table 7 shows the performance of four routing protocols, i.e., the Alive Node Ratio, in case of increase of node's number from 50 to 250. Across all network sizes, PDMDS always maintains the highest alive node ratio, which implies that it is more energy efficient and robust than other protocols. Following ACLDSM is being moderately high performance with a gradual dripping down but better in survivability compared with AODV and DYMO. Although AODV has average performance, DYMO exhibits the steepest drop in the number of alive nodes which can be an indication of higher energy depletion or node failure rates. Overall, all the protocols suffer from the Alive Nodes Ratio deterioration with the increasing size of the network, yet PDMDS proves to be the most tough and scalable to overcome this problem and hence preferable for large scale IoT or wireless sensor network applications where the node life is important.

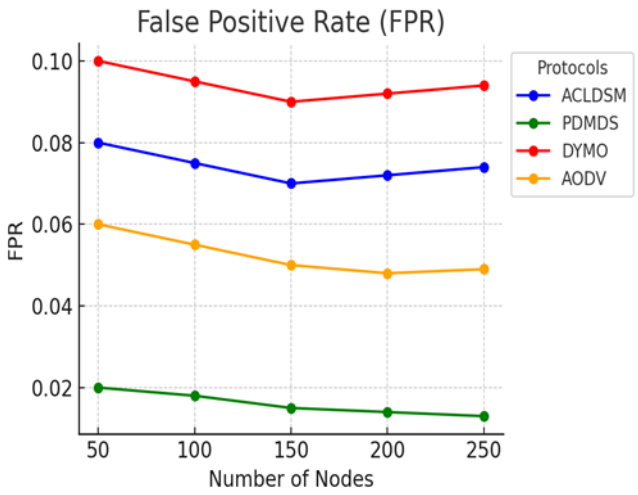
False Positive Rate (FPR): False positive percentage equals this mathematical expression.

The computation of false positive rate involves the following fractional formula: FPR= FP/ (FP+TN)

The ratio describes false positives as FP along with TN as true negatives while N stands for FP+TN which represent total ground truth negatives.

Table 8 False Positive Rate (FPR) Table

Nodes	ACLDSM	PDMDS	DYMO	AODV
50.0	0.08	0.02	0.1	0.06
100.0	0.075	0.018	0.095	0.055
150.0	0.07	0.015	0.09	0.05
200.0	0.072	0.014	0.092	0.048
250.0	0.074	0.013	0.094	0.049



False Positive Rate (FPR) of four routing protocols, namely ACLDSM, PDMDS, DYMO and AODV, for varying node densities from 50 to 250 are presented in Table 8. Moreover, PDMDS (green line) shows the lowest FPR in all the cases, and it steadily drops from 0.02 to less than 0.015, illustrating its high reliability and not activating at normal packets unnecessarily (wrong detection). However, DYMO (red line) shows the highest FPR in every case, staying just below 0.10 in value and thus implies that there is a high rate of false alerts, which could lead to misguided countermeasures that only serve to deteriorate network performance. The FPR of AODV (orange line) is on an average showed to be equivalent to ACLDSM (blue line) around a moderate FPR of 0.07–0.08 but reduces gradually to about 0.048. In minimizing false positives, PDMDS shows the best capability and therefore best suited for security sensitive or resource constrained IoT environments where a high FPR on DYMO means it is not an adequate choice when accuracy of threat detection is essential.

Evaluation of four routing protocols among them PDMDS always performs better than other protocols. With a Packet Delivery Ratio of ~99.8%, it is evidenced to be most reliable and scalable; at the same time End-to-End Delay (~80–90 ms) is kept the minimum, as a result of efficient and stable routing mechanisms. It also records the least Packet Drop Rate (~0.005), the highest in terms of packet integrity, and the highest Throughput (~550–580 packets/sec), suggesting great capability to send a high volume of data continuously. On energy efficiency metrics, PDMDS provides the highest Alive Nodes Ratio (~0.92–0.96) for longer working time of networks and low False Positive Rate (~1.3%), for higher trust and detection precision. On the other hand, DYMO has persistently the lowest PDR (~86%), high delay (~150–180 ms), high drop rate (~0.13–0.16), lowest throughput (~400–420 packets/sec), lowest alive node ratio (~0.78–0.85) and the highest FPR (~9–10%), mainly because of its reactive nature, with little optimization. AODV has a fairly strong performance, especially on the throughput and alive nodes but is degraded slightly in very dense networks. Overall, ACLDSM has ample good results, is burdened by cluster overhead and static, and lies somewhere in between AODV and DYMO in terms of effectiveness.

V. Conclusions

The hybrid data aggregation mechanism demonstrates strong confidentiality features along with desired integrity protection measures. Security investigations together with simulation tests conducted under this study established the model's ability to maintain high security while simultaneously extending lifetime and achieving better efficiency. The proposed scheme delivers potential solutions for securing aggregation systems in WSNs. Before developing an enhanced security model the research analyzed how packet loss rates affect aggregation accuracy when the PDMDS routing protocol is merged with DBG scheme. During simulation tests the data protection system obtained maximum marks which led to better overall performance while delivering superior throughput while simultaneously yielding better PDR and EED outcomes and sustaining more alive nodes besides reducing false positive percentages. The reduction of packet loss represents a major enhancement made possible by this research to reduce the waste of selecting Cluster Heads. The Cluster Head selection process will pick its candidate from among the Nodes of the Elite group based on energy metrics from this specific group rather than all Nodes.

References

[1]. Singh, A.P., Luhach, A.K., Gao, X.Z., Kumar, S., Roy, D.S. Evolution Of Wireless Sensor Network Design From Technology Centric To User Centric: An Architectural Perspective. International Journal Of Distribution Of Sensor Network 16(8), 1550147720949138 (2020)

[2]. Sarangi K, Bhattacharya I (2019) A Study On Data Aggregation Techniques In Wireless Sensor Network In Static And Dynamic Scenarios. Innovations Systsoftw Eng 15(1):3–16

[3]. Mathapati, M., Senthil Kumaran, T., Patil, K.K., Patil, S.S., Veena, H.N. (2021). A Study On Secure Data Aggregation And Routing For Wireless Sensor Networks. In: Luhach, A.K., Jat, D.S., Bin Ghazali, K.H., Gao, XZ., Lingras, P. (Eds) Advanced Informatics For Computing Research. ICAICR 2020.

[4]. Osamy W, Khedr AM, Aziza A, El-Sawya A (2018) Cluster-Tree Routing Scheme For Data Gathering In Periodic Monitoring Applications. IEEE Access 6:77372–77387

[5]. Swathi, Y., Chitnis, S. Energy Aware Fuzzy Logic Secure Data Aggregation (EA-FSDA) Technique For Wireless Sensor Networks. Int. J. Eng. Adv. Technol. (IJEAT) 8(6) (2019). ISSN: 2249-8958

[6]. Qin, D., Yang, S., Jia, S., Zhang, Y., Ma, J., Ding, Q. Research On Trust Sensing Based Secure Routing Mechanism For Wireless Sensor Network. IEEE Access 5, 9599–9609 (2017)

[7]. Maratha, P., Gupta, K., Luhach, A.K. Improved Fault-Tolerant Optimal Route Reconstruction Approach For Energy Consumed Areas In Wireless Sensor Networks. IET Wireless Sensor System 10(3), 112–116 (2019)

[8]. Arora VK, Sharma V, Sachdeva M (2019) ACO Optimized Self-Organized Tree-Based Energy Balance Algorithm For Wireless Sensor Network. J Ambient Intellhumaniz Computer 10(12):4963–4975

[9]. Kumar, S., Dhull, K., Arora, P., Luhach, A.K.: Performance Of Energy Conservation Models, Generic, Micaz And Micamotes, Using AODV Routing Protocol On A Wireless Sensor Network. Scalable Computer Practice Exp. 20(4), 631–639 (2019)

[10]. Uvarajan K P, Gowri Shankar C (2020) An Integrated Trust Assisted Energy Efficient Greedy Data Aggregation For Wireless Sensor Networks. Wirel Pers Commun 114:813–833

[11]. Gharaei N, Bakar KA, Hashim SZM, Pourasl AH (2019) Inter-And Intra-Cluster Movement Of Mobile Sink Algorithms For Cluster-Based Networks To Enhance The Network Lifetime. Ad Hoc Network 85:60–70

[12]. Abbasian Dehkordi, S., Farajzadeh, K., Rezazadeh, J. Et Al. A Survey On Data Aggregation Techniques In Iot Sensor Networks. Wireless Network 26, 1243–1263 (2020).

[13]. Vinodha D, Anita EM (2019) Secure Data Aggregation Techniques For Wireless Sensor Networks: A Review. Arch Computer Methods Eng 26(4):1007–1027

[14]. Dehkordi SA, Farajzadeh K, Rezazadeh J, Farahbakhsh R, Sandrasegaran K, Dehkordi MA (2020) A Survey On Data Aggregation Techniques In Iot Sensor Networks. Wireless Network 26(2):1243–1263

[15]. Maryam A. Nezhad, Hamid Barati, And Ali Barati. An Authentication-Based Secure Data Aggregation Method In Internet Of Things. Journal Of Grid Computing 2022; 20(3): 29.

[16]. Naghibi, M., Barati, H.: Shsda Secure Hybrid Structure Data Aggregation Method In Wireless Sensor Networks. Journal Of Ambient Intelligence And Humanized Computing, Pp. 1–20 (2021)

[17]. Bongale, A.M., Nirmala, C.R. &Bongale, A.M. Energy Efficient Intra-Cluster Data Aggregation Technique For Wireless Sensor Network. Int. J. Inf. Technology 14, 827–835 (2022).

[18]. Devi VS, Ravi T, Priya SB (2020) Cluster Based Data Aggregation Scheme For Latency And Packet Loss Reduction In WSN. Computer Communication 149:36–43.

[19]. Rawat, P., Chauhan, S. Probability Based Cluster Routing Protocol For Wireless Sensor Network. J Ambient Intell Human Computer 12, 2065–2077 (2021).

[20]. R. Fatemeh, Yi Mu, Ke Huang. Secure And Efficient Data Aggregation For Iot Monitoring Systems. IEEE Internet Of Things Journal (2020).

[21]. X. Du, Z. Zhou, Y. Zhang, And T. Rahman, "Energy-Efficient Sensory Data Gathering Based On Compressed Sensing In Iot Networks," Journal Of Cloud Computing, Vol. 9, No. 1, Pp. 1–16, 2020.

[22]. X. Liu, X. Wang, K. Yu, X. Yang, W. Ma, G. Li, And X. Zhao. Secure Data Aggregation Aided By Privacy Preserving Internet Of Things. Journal Of Wireless Communications And Mobile Computing (2022).

[23]. D. Vinodha, E. A. Mary, And D. Mohana, "A Novel Multi-Functional Multi Parameter Concealed Cluster-Based Data Aggregation Scheme For Wireless Sensor Networks (NMFMP-CDA)," Wireless Networks, Vol. 27, No. 2, Pp. 1111–1128, 2021.

[24]. Daewon Lee And Hwamin Lee, "Iot Service Classification And Clustering For Integration Of Iot Service Platforms", The Journal Of Supercomputing, Pp. 1-17, 2018.

[25]. Neeraj Chandnani, C. N. Khairnar. Efficient Data Aggregation And Routing For Iot Wireless Sensor Networks. IEEE 2019.

[26]. J. Sun, C. Zhang, And Y. Fang, "Detecting Malicious Node Behaviors In Wireless Networks Using Cross-Layer Approach," IEEE Transactions On Mobile Computing, Vol. 6, No. 4, Pp. 432–444, Apr. 2007.

[27]. P. Papadimitratos And Z. Haas, "Secure Routing For Mobile Ad Hoc Networks," In SCS Communication Networks And Distributed Systems Modeling And Simulation Conference (CNDS), 2002.

[28]. C. Liu, K. Wu, And J. Pei, "An Energy-Efficient Data Collection Framework For Wireless Sensor Networks By Exploiting Spatiotemporal Correlation," IEEE Transactions On Parallel And Distributed Systems, Vol. 18, No. 7, Pp. 1010–1023, Jul. 2007.

[29]. C. Castelluccia, E. Mykletun, And G. Tsudik, "Efficient Aggregation Of Encrypted Data In Wireless Sensor Networks," In Proceedings Of Mobiquitous, 2005.

[30]. N. Pippenger, "On The Complexity Of Computations," In Proceedings Of The ACM Symposium On Theory Of Computing (STOC), Pp. 37–43, 1977.

[31]. S. Marti, T. J. Giuli, K. Lai, And M. Baker, "Mitigating Routing Misbehavior In Mobile Ad Hoc Networks," In Proceedings Of Mobicom, 2000.

[32]. Y. Wang, G. Attebury, And B. Ramamurthy, "A Survey Of Security Issues In Wireless Sensor Networks," IEEE Communications Surveys & Tutorials, Vol. 8, No. 2, Pp. 2–23, 2006.

[33]. K. Fall And K. Varadhan, The Ns Manual (Formerly Ns Notes And Documentation), The VINT Project, 2000.

[34]. S. Buchegger And J.-Y. Le Boudec, "Performance Analysis Of The CONFIDANT Protocol," In Proceedings Of The ACM International Symposium On Mobile Ad Hoc Networking And Computing (Mobihoc), 2002.

[35]. A. Alshamrani, S. Myneni, A. Chowdhary, And D. Huang, "A Survey On Advanced Persistent Threats: Techniques, Solutions, Challenges, And Research Opportunities," IEEE Communications Surveys & Tutorials, Vol. 21, No. 2, Pp. 1851–1877, 2019.

[36]. A. Kumar, M. Park, And S. Kim, "Blockchain-Enabled Secure And Decentralized Routing For Iot Networks," IEEE Internet Of Things Journal, Vol. 10, No. 2, Pp. 1564–1575, Feb. 2023.

[37]. L. Zhao, H. Nguyen, And Y. Song, "Deep Learning-Based Intrusion Detection Systems For Iot: Challenges And Opportunities," ACM Transactions On Internet Technology (TOIT), Vol. 24, No. 1, Pp. 1–24, Jan. 2024.

[38]. P. Roy, S. Banerjee, And R. Shokri, "Federated Learning For Securing Smart Iot Systems Against Adaptive Attacks," IEEE Transactions On Mobile Computing, Early Access, 2025.