Cluster Based False Aggregate Detection System in Wireless Sensor Networks

Dr Nagendra Babu[1]
Department of CSE
JAIN (Deemed-to-be University)
Bengaluru, India
nagendra2nag@gmail.com

Chaitanya Kumar V[2]
Department of CSE
JAIN (Deemed-to-be University)
Bengaluru, India
vanamachaitanya246@gmail.com

Gnana Dileep Reddy V[3]
Department of CSE
JAIN (Deemed-to-be University)
Bengaluru, India
dhileep742@gmail.com

Adeebulla Khan K[3]
Department of CSE
JAIN (Deemed-to-be University)
Bengaluru, India
Adeebkhan795@gmail.com

SriRama Vivek[5]
Department of CSE
JAIN (Deemed-to-be University)
Bengaluru, India
sriramavivek5@gmail.com

Siva Sathvik Innamuri[6]
Department of CSE
JAIN (Deemed-to-be University)
Bengaluru, India
sathvikinnamuri777@gmail.com

***Abstract*—Wireless Sensor Networks (WSNs) are becoming increasingly significant in modern applications including environmental monitoring and smart cities. However, these networks confront constraints such as limited power, processing capability, and memory. To circumvent these restrictions, a hierarchical WSN paradigm is presented, where sensor nodes collect data and deliver it to cluster heads. The cluster heads aggregate the data and send it to the base station equipped with a Cluster Based False Aggregate Detection System (CBFADS). This technique improves energy efficiency, network lifespan, and security. The performance of the proposed system is analyzed using the metrics like packet delivery rate, packet loss rate, delay, accuracy, and throughput. Results reveal significant increases in throughput relative to standard approaches. This makes the suggested system a durable, energy-efficient, and secure solution for modern WSN applications.**

Keywords—Accuracy, Precision, Network Intrusion, Performance Evaluation

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have revolutionized the sense of collecting and processing data from the physical world. WSNs include spatially distributed sensor nodes that monitor environmental conditions like temperature, humidity, movement, and more. These networks are used widely in applications such as environmental monitoring, smart agriculture, disaster management, military surveillance, and industrial automation.

One of the important challenges related to WSNs is security, especially against intrusions and malicious behavior. Intrusion Detection Systems (IDS) will therefore come in handy in terms of protecting WSNs against unauthorized access attempts, but current IDSs are inappropriate for massive WSN deployment due to their energy consumption levels, communication overheads, and scalability issues.

Addressing the issues discussed in this paper, this research introduces a dynamic cluster-based intrusion detection strategy Cluster Based False Aggregate Detection System (CBFADS). To optimize energy consumption and enhance scalability, it uses hierarchical clustering and dynamic cluster-head selection. It also uses real-time data analysis at the base station to enhance intrusion detection accuracy. Extensive simulations for the system s performance are evaluated in terms of throughput, energy efficiency, network lifetime, detection accuracy, and latency.

A. Definition of WSN Architecture

WSN Architecture is divided mainly into three parts: it consists of sensor nodes, cluster heads, and a base station. Sensor nodes obtain environment data and forward the data to the cluster head. The cluster head aggregates the received data from its member nodes and sends them to a base station to process them further. This hierarchical structure reduces overhead in communication and improves energy efficiency. The simulation of the WSN architecture is developed in this research using a dynamic clustering approach. The sensor nodes are divided into clusters, each with its unique cluster head. Meanwhile, the base station serves as the central entity for data analysis and intrusion detection.

B. Creating Sensor Nodes

Sensor nodes are considered to be the primitive elements of WSNs. Sensor nodes gather data from their surroundings and send the information to the cluster heads. During the simulation, each sensor node is assigned an identification number and coded to produce random data values for environmental parameters. Wireless links are used for communication between sensor nodes and cluster heads that have specified bandwidth and latency parameters.

C. Establish Cluster Heads

Cluster heads collect data from their member nodes and forward them to the base station. Dynamic cluster head election is used to balance the consumption of energy of the network. It also considers factors such as node energy levels and communication costs for the selection process. Periodically aggregated data are forwarded towards the base station to avoid extra communication overhead.

D. Base Station Design

Base Station is the core that processes the aggregated data received from the cluster heads. It uses threshold value-based intrusion detection algorithms. For example, if the aggregated data exceeds a certain threshold, an intrusion alert message is created. The base station also periodically analyzes the network performance metrics like throughput and energy consumption.

E. Specify Real-World Applications

The system can be applied to many real-life situations. It encompasses like Military surveillance is intended to identify and discourage unlawful entry into secured zones to improve security and protect sensitive installations. Technology is employed in smart agriculture to monitor soil status and intrusions in farms so as to facilitate more efficient and secure

agricultural practice. For industrial automation, the emphasis is on securing procedures in industrial environments, removing risks, and ensuring smooth operations.

Environmental monitoring, however, is geared towards finding anomalies in forests and wildlife areas to preserve ecosystems and prevent unwanted actions.

We measure the system's performance based on critical metrics. Speed of data delivery to the center is an important gauge. Consumption of power by sensors and coordinating units is examined for performance efficiency. We also monitor how long the network stays operational before power sources give way.

Detection accuracy is a measure of the system's reliability to detect intrusions, and latency examines the time for data to move from sensor nodes to the base station.

The NS-2 simulator is employed to analyze the performance of the system implemented, which involves sensor nodes, cluster heads, and a base station. Data collection, aggregation, and intrusion detection are scheduled to be performed to measure system performance. The obtained results are compared with existing research in order to pinpoint increased throughput, energy efficiency, and detection rates as evidence of the system's validity and performance for real-time applications.

II. Literature Survey

An energy-aware intrusion detection system (IDS) of Surraya Khanum et al. (2020) for wireless sensor networks through hierarchical clustering. It is targeted to minimize redundant communication to optimize energy consumption with reliability in intrusion detection. The study reflects the importance of hierarchical models in increasing lifetimes in the network and defending data. Adaptive clustering methods are a central focus to improve system sustainability in resource-limited networks. The proposed solution improves IDS efficiency while optimizing energy consumption[1].

N. Nithyanandan et al. (2019) proposed a dynamic cluster-head selection method for secure IDS in underwater acoustic communication networks. It is residual energy and network density-based for efficient clustering and secure data transmission. The technique is designed to address issues like energy limitations and effective threat detection in underwater networks. The study offers an efficient balanced strategy between security deployments and resource limitation. The suggested approach improves network resilience with efficient energy usage [2].

A. Babu Karuppiah et al. (2021) also proposed a light-weight intrusion detection system for resource-constrained WSNs. The research is founded on minimizing computational overhead and maximizing scalability without losing threat detection capability. Optimized resource utilization guarantees the practicability of the system in dynamic and resource-constrained network environments. The system manages to mitigate scalability and efficiency issues in WSN security. The method is beneficial in scenarios with low resource requirements and efficient threat detection[3].

A hybrid IDS with a combination of anomaly-based and signature-based detection methods with machine learning. The system provides effective threat detection and resilience against varied attacks in wireless networks. Utilizing real-time data analysis, the research provides improved security in critical infrastructure systems. The method proposed by Syeda Gauhar Fatima et al. (2023) effectively secures WSN security frameworks. Its combination of both detection methods provides high reliability against varied attacks[4].

Surraya Khanum et al. (2018) discussed bio-inspired algorithms for adaptive cluster-head selection in WSNs. The study emphasizes the effectiveness of these algorithms in energy consumption optimization and network stability. Adaptive clustering guarantees longer system lifetimes, especially in resource-limited environments. The novel method presents a sustainable security solution for WSNs. It introduces new techniques for maintaining energy efficiency and stability in large-scale WSN deployments[5].

N. Nithiyanandam et al. (2022) presents a multi-cluster architecture that addresses hierarchical intrusion detection systems for large-scale WSNs. This work is centered on developing a highly scalable and stable security system for large wireless sensor networks. Decentralized communication is emphasized to attain stable performance. The framework makes use of dynamic computing methods in order to detect security attacks in real-time and significantly increase the security of inter-connected devices. The results provide important insights on how to create more effective and scalable intrusion detection systems for these advanced networks. [6].

III. Proposed Work

This paper suggests a Cluster Based False Aggregate Detection System (CBFADS) to address the severe issues ofconventional WSNs, i.e., False aggregate and security.

A. System Architecture

The innovative WSN consists of three important modules:

1) Sensor Nodes
These nodes gather environmental data (e.g., temperature, humidity, movement) and relay it to their respective cluster heads.

2) Cluster Heads
Dynamically selected, the cluster heads collect data from their member nodes and relay summarized data with minimal data redundancy and communication overhead.

3) Base Station
Network central node, the base station collects data from cluster heads. Having an Intrusion Detection System (IDS) to check data for malicious activity and security attacks.

B. Dynamic Cluster Management

1) Sensor Node Deployment
The sensor nodes are deployed in such a manner that they observe the environment. Random data are produced at each node for testing, emulating the actual data acquisition.

2) Dynamically selecting cluster heads
Dynamically the cluster heads are selected based on communication costs and present energy level of the cluster head. This keeps the network "alive" a little longer as it spreads energy consumption across the network.

3) Data Aggregation

Data aggregation is done by cluster heads, which minimizes the data sent to the base station, thereby saving energy and enhancing network efficiency.

4) Intrusion Detection and Base Station Processing

A threshold-based intrusion detection system is used in the base station. If aggregated data exceeds a threshold value (say, 0.9) and is believed to indicate a potential security attack, an intrusion alarm is triggered Data values up to and including the threshold are considered normal. The central control point constantly monitors such important network health parameters as data transfer rate, power consumption, and response time in an attempt to maximize the overall efficiency of the system.

The **Fig. 1** illustrates a hierarchical Wireless Sensor Network (WSN) designed for intrusion detection. Sensor nodes transmit data to multiple cluster heads, with the one having the highest energy chosen to relay information to the Base Station, optimizing energy usage. The Base Station processes the incoming data to assess whether an intrusion has taken place. If an anomaly is identified, an "Intrusion Detected" alert is issued; otherwise, it reports "Intrusion Not Detected." This method enhances network longevity, reliability, and balanced load distribution in intrusion detection systems.

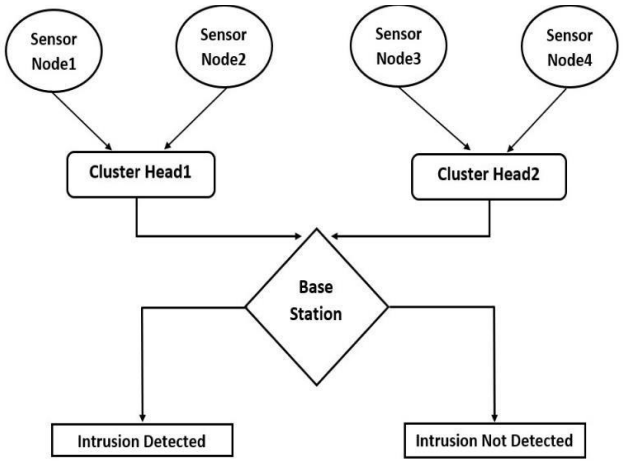

Fig. 1. *Hierarchical Cluster-Based Intrusion Detection System for WSN*

C. Simulation and Performance Evaluation

The system is subjected to a detailed analysis with the help of the NS-2 simulation tool. The following performance metrics are examined:

1) Throughput

Is the amount of data successfully delivered to the base station.

2) Energy Efficiency

Tracks the power usage of sensor nodes and cluster heads.

3) Network Lifetime

Indicates how long the network remains functional before the energy of the nodes is depleted.

4) Detection Accuracy

Refers to the time delay encountered during the transmission of data from sensor nodes to the base station.

IV. PROPOSED METHODOLOGY

A. Sensor Node Deployment Algorithm

```
Initialize Cluster Head:
  Set attribute c_id
  Initialize empty list agg_data
While True:
  Receive Data:
    Call rec_data method with data as a parameter
    Append data to agg_data
    Print received data
  Aggregate Data:
    If agg_data is not empty:
      aggregated_value = Sum of agg_data / Length of agg_data
      Clear agg_data
      Check for the highest aggregate value
      Store highest aggregate value among all cluster heads
      Print "Cluster Head with highest aggregate value: c_id with value max_agg_value"
      Return aggregated_value
    Else:
      Return None
    EndIf
  Send Aggregated Data to Base Station:
    Call send_to_base_station method with base_station as a parameter
    Call aggr_data method to get aggregated_value
    If aggregated_value is not None:
      Print "Sending aggregated data to Base Station"
      Call rec_data method of Base Station with aggregated_value and c_id
    EndIf
  If Stop condition met:
    Terminate process
    Break loop
  EndIf
EndWhile
```

B. Cluster head Deployment Algorithm

```
Initialize Cluster Head:
  Set attribute c_id
  Initialize empty list agg_data
While True:
  Receive Data:
    Call rec_data method with data as a parameter
    Append data to agg_data
    Print received data
  Aggregate Data:
    If agg_data is not empty:
      aggregated_value = Sum of agg_data / Length of agg_data
      Clear agg_data
      Check for the highest aggregate value
      Store highest aggregate value among all cluster heads
      Print "Cluster Head with highest aggregate value: c_id with value max_agg_value"
      Return aggregated_value
    Else:
      Return None
    EndIf
  Send Aggregated Data to Base Station:
    Call send_to_base_station method with base_station as a parameter
    Call aggr_data method to get aggregated_value
    If aggregated_value is not None:
      Print "Sending aggregated data to Base Station"
      Call rec_data method of Base Station with aggregated_value and c_id
```

```
        EndIf
      If Stop condition met:
        Terminate process
        Break loop
      EndIf
    EndWhile
```

C. *Base Station Deployment Algorithm*

```
    Create an instance of Base_Station
  Initialize Cluster Heads and Sensor Nodes:
    Set no_cluster_heads
    Initialize empty lists: c_heads, sensor_nodes
    Set no_sensors_per_cluster
   For ch_id = 1 to no_cluster_heads:
     Create ClusterHead instance with c_id = ch_id
     Append ClusterHead to c_heads
     For node_id = (ch_id - 1) * no_sensors_per_cluster to ch_id *
no_sensors_per_cluster:
       Create SensorNode instance with node_id and assign to
current ClusterHead
       Append SensorNode to sensor_nodes
     EndFor
   EndFor
Run Sensor Nodes and Cluster Heads:
   Set number of iterations
   For iteration = 1 to iterations:
     For each SensorNode in sensor_nodes:
       Call run method
       Collect data
       Send data to Cluster Head
     EndFor
     For each ClusterHead in c_heads:
       Call send_to_base_station with base_station
       Aggregate data
       Send aggregated data to Base Station
     EndFor
     Call intrusion_detect method of BaseStation
     If detected value < 0.9:
       Print "No intrusion detected. Stopping process."
       Break loop
     Else:
       Print "Intrusion detected! Initiating further processing."
       Call alert_authorities() method
       Call log_intrusion_details() method
       Perform necessary countermeasures
     EndIf
     Pause execution for 1 second
   EndFor
Print final aggregated data from base_station.received_data
```

V. PERFORMANCE EVALUATION

The researchers have made significant contributions to the field of Wireless Sensor Networks, leading to the development and implementation of various techniques. This work incorporates three algorithms. Subsequently, we compare the highest accuracy achieved in this study for certain common protocols with the accuracies reported by other researchers for the same parameters.

Fig. 2 Performance comparison of PDR indicates that PEGASIS and CBFADS deliver at a highest efficiency of 85%, LEACH at 80%, and TEEN at 70%.

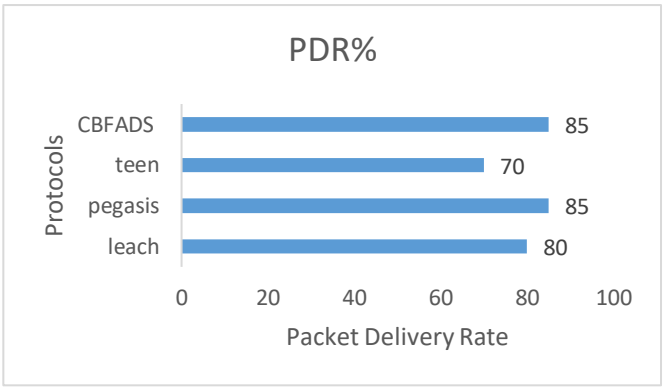

Fig. 2. Packet Delivery Rate

Fig. 3 The Packet Loss Ratio (PLR) comparison indicates that CBFADS shows better performance with the least PLR of 5, then TEEN at 8, PEGASIS at 10, and LEACH showing the greatest PLR of 15.

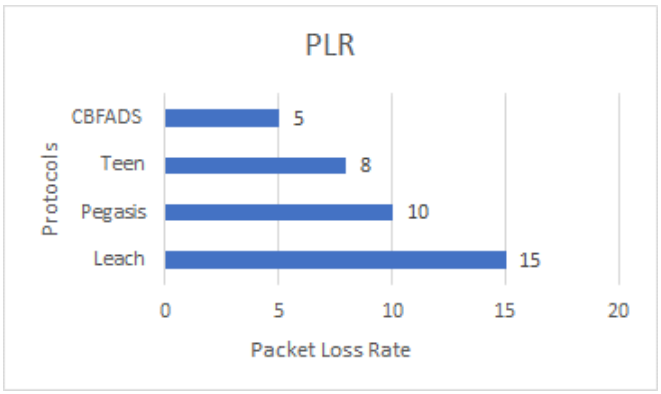

Fig. 3. Packet Loss Rate

Fig. 4 CBFADS performs the best with a maximum end-to-end delay of 200 ms and a delay percentage of 66.67%, better than LEACH (300 ms, 100%), PEGASIS (280 ms, 93.33%), and TEEN (250 ms, 83.33%)

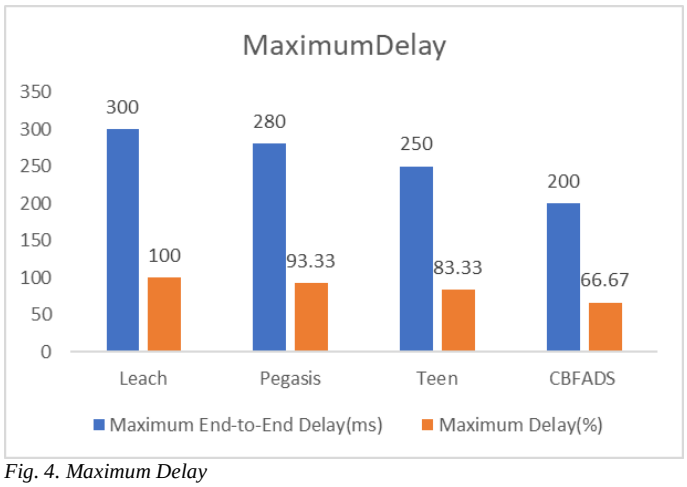

Fig. 4. Maximum Delay

Fig. 5 CBFADS achieves the lowest maximum latency of 250 ms (62.5%), outperforming LEACH (400 ms, 100%),HEED (350 ms, 87.5%), and PEGASIS (300 ms, 75%) in terms of both latency and percentage.

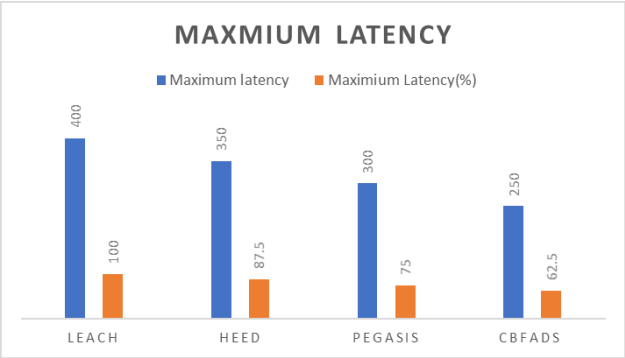

Fig. 5. Maximum Latency

Fig.6, CBFADS records the maximum mean throughput of 1100 bps, corresponding to 100% efficiency, and outperforms LEACH (800 bps, 72.73%) and HEED (950 bps, 86.36%)

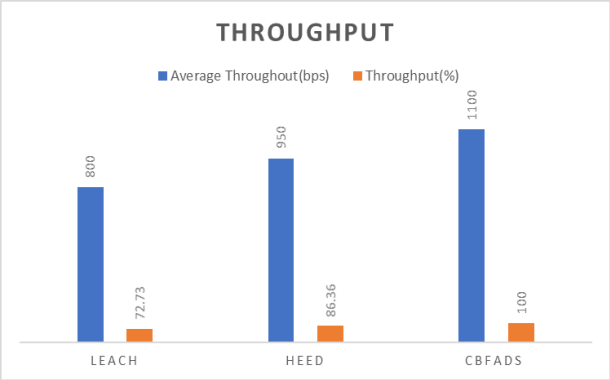

Fig. 7. Throughput

Fig.7, CBFADS gains higher accuracy, precision, and recall than LEACH and HEED with remarkable improvements on the three parameters. CBFADS performs best with accuracy, precision, and recall of 92%, 90%, and 95% outperforming those of LEACH (85%, 80%, 90%) and HEED (88%, 85%, 92%).

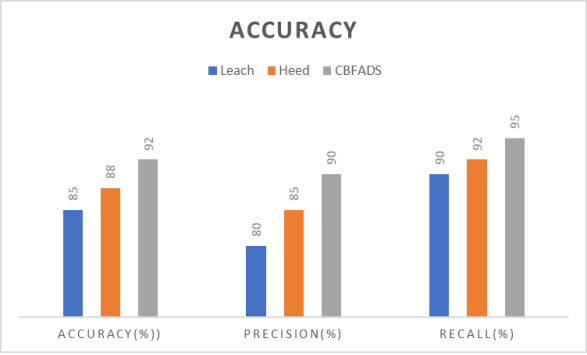

Fig. 7.. Accuracy

VI. Conclusion

The proposed hierarchical WSN model, Cluster Based False Aggregate Detection System (CBFADS) including dynamic clustering and an integrated IDS, provides a resilient, energy- efficient, and secure solution for different real-world applications. Simulation results have revealed considerable increases in key performance measures such as throughput, energy economy, and intrusion detection accuracy compared to traditional WSN techniques, underlining the usefulness of this unique design.

VII. References

[1] *S. Khanum, et al., "Energy-efficient intrusion detection system using hierarchical clustering," Wireless Sensor Systems, 2020. [Online]. Available: https://doi.org/10.1049/wss2.12100.*

[2] N. Nithiyanandam, et al., "Secure acoustic communication with energy-efficient IDS," in Proc. IEEE Wireless Communications and Networking Conference (WCNC), 2019, pp. 1–6. [Online]. Available: https://doi.org/10.1109/WCNC.2019.8909928.

[3] A. B. Karuppiah, et al., "Lightweight IDS for resource-constrained wireless sensor networks," Computer Communications, vol. 176, pp. 10–20, 2021. [Online]. Available: https://doi.org/10.1016/j.comcom.2021.08.015.

[4] S. G. Fatima, et al., "Hybrid intrusion detection systems in WSN," Journal of Network and Computer Applications, vol. 205, 2023, Art. no. 103529. [Online]. Available: https://doi.org/10.1016/j.jnca.2023.103529.

[5] S. Khanum, et al., "Bio-inspired adaptive cluster-head selection for WSNs," in Proc. IEEE Int. Conf. Advances in Computing, Communications and Informatics (ICACCI), 2018, pp. 855–861. [Online]. Available: https://doi.org/10.1109/ICACCI.2018.8554815.

[6] N. Nithiyanandam, et al., "Hierarchical intrusion detection in multi-cluster WSNs," IEEE Internet of Things Journal, 2022. [Online]. Available: https://doi.org/10.1109/IoT.2022.9786345.

[7] L. Yang, Y. Lu, S. X. Yang, T. Guo and Z. Liang, "A secure clustering protocol with fuzzy trust evaluation and outlier detection for industrial wireless sensor networks," IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 4837–4847, July 2021, doi: 10.1109/TII.2020.3019286.

[8] G. Guan, X. Hu, Y. Xu, Q. Luan, C. Li and F. Jiang, "Clustering analysis based power security big data aggregation in ubiquitous power Internet of Things," in Proc. 2020 12th IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Nanjing, China, 2020, pp. 1–5, doi: 10.1109/APPEEC48164.2020.9220667.

[9] H. Pang, K. He, Y. Fu, J.-N. Liu, X. Liu and W. Tan, "Enabling efficient and malicious secure data aggregation in smart grid with false data detection," IEEE Transactions on Smart Grid, vol. 15, no. 2, pp. 2203–2213, Mar. 2024, doi: 10.1109/TSG.2023.3316730.

[10] M. M. Abbas and O. R. Merad-Boudia, "On ensuring data integrity in data aggregation protocols in IoT environments," in Proc. 2022 2nd International Conference on Advanced Electrical Engineering (ICAEE), Constantine, Algeria, 2022, pp. 1–6, doi: 10.1109/ICAEE53772.2022.9962093.

[11] J. Liu and F. Labeau, "Detection of false data injection attacks in industrial wireless sensor networks exploiting network numerical sparsity," IEEE Transactions on Signal and Information Processing over Networks, vol. 7, pp. 676–688, 2021, doi: 10.1109/TSIPN.2021.3122289.

[12] Q. Zhou, X. Qin, G. Liu, H. Cheng and H. Zhao, "An efficient privacy and integrity preserving data aggregation scheme for multiple applications in wireless sensor networks," in Proc. 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), Tianjin, China, 2019, pp. 291–297, doi: 10.1109/SmartIoT.2019.00051.

[13] T. Wang, C. Zhang, Z. Lu, D. Du and Y. Han, "Identifying truly suspicious events and false alarms based on alert graph," in Proc. 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 5929–5936, doi: 10.1109/BigData47090.2019.9006555.

[14] C. Peng, M. Luo, P. Vijayakumar, D. He, O. Said and A. Tolba, "Multifunctional and multidimensional secure data aggregation scheme in WSNs," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2657–2668, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3077866.

[15] N. Komalan and A. Chauhan, "A survey on cluster-based routing, data aggregation and fault detection techniques for locating real-time faults in modern metro train tracks using wireless sensor network," in Proc. 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bengaluru, India, 2017, pp. 116–123, doi: 10.1109/ICIMIA.2017.7975584.

[16] A. Sargolzaei, K. Yazdani, A. Abbaspour, C. D. Crane III and W. E. Dixon, "Detection and mitigation of false data injection attacks in networked control systems," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4281–4292, June 2020, doi: 10.1109/TII.2019.2952067.