SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

SEMARAK ILMU
Journal of
ADVANCED RESEARCH IN APPLIED SCIENCES AND ENGINEERING TECHNOLOGY
ISSN 2462 - 1943

Identification of WSN Compromised Nodes and Performance Degradation Prevention using Cooperative Cache

Mohammad Sirajuddin[1,*], B. Sateesh Kumar[2]

[1] Department of CSE, Jawaharlal Nehru Technological University Hyderabad, Telangana 500085, India
[2] Department of CSE, JNTUH University College of Engineering Jagitial, Telangana 505501, India

Article history:
Received 5 February 2024
Received in revised form 19 April 2024
Accepted 4 October 2024
Available online 31 December 2024

ABSTRACT

Wireless Sensor Networks (WSNs) are critical in a variety of applications such as environmental monitoring, surveillance, and healthcare. WSNs, on the other hand, are vulnerable to assaults due to their dispersed and resource-constrained nature, resulting in compromised nodes and performance deterioration. Using network characteristics analysis and cooperative cache management with data and process affinity, this study provides a unique way to identifying compromised WSN nodes and mitigating performance deterioration. The initial portion of our suggested technique focuses on finding compromised nodes using in-depth network characteristics research. This suggested system can precisely locate probable hacked nodes by monitoring metrics such as traffic patterns, node activity, and communication abnormalities. Machine learning algorithms improve the identification process by learning and evolving adaptively to identify new assault patterns. Once affected nodes have been discovered, the second component of this suggested solution leverages cooperative cache management to prevent performance deterioration. Data and process affinity is presented, in which nearby nodes share caches to effectively store and retrieve data relevant to their processing activities. This affinity-based cache collaboration increases data availability, decreases communication costs, and improves overall network performance.

Keywords:

Wireless sensor networks; Compromised nodes; Performance degradation; Cooperative cache; Data affinity; Process affinity; Network characteristics

1. Introduction

In recent years, there has been a lot of interest in Wireless Sensor Networks (WSNs) as a consequence of the relevance that they have in a broad range of applications, ranging from environmental monitoring and surveillance to healthcare and industrial automation. This interest is due to the fact that WSNs may play an important role in all of these areas. It is anticipated that this level of interest will remain unchanged. Due to the fact that they are decentralized and have limited access to resources, wireless sensor networks are vulnerable to a wide variety of security risks. These risks include cyberattacks and data breaches. Attacks that focus on certain sensor nodes inside the network are more susceptible to being breached. These compromised nodes have the potential to

[*] *Corresponding author.*
E-mail address: mohammadsirajuddin78901@gmail.com

https://doi.org/10.37934/araset.54.2.3257

have a significant impact on the network as a whole, which may lead to the loss of data, interruptions in communication, and a deterioration in the quality of key services.

Wireless Sensor Networks (WSNs) have evolved as an important technology in a variety of fields, including environmental monitoring, healthcare, industrial automation, and smart cities. These networks are made up of a large number of small, resource-constrained sensor nodes that work together to collect, analyse, and send data to a central base station. However, the dispersed and intrinsically vulnerable structure of WSNs leaves them open to a variety of security attacks, potentially resulting in compromised nodes and performance deterioration. There has never been a greater need for strong and efficient solutions to safeguard the integrity and dependability of WSNs.

Compromised nodes in a WSN may substantially degrade overall network performance and offer major hazards to applications that depend on the gathered data. Malicious attacks, such as node replication, denial-of-service, and corrupted data forwarding, may result in false data readings, illegal access, and eventually jeopardize the whole WSN's operation. As a result, identifying compromised nodes early and accurately is critical to maintaining the system's overall integrity and efficacy. Identifying hacked WSN nodes and preventing performance decrease are two of the most pressing issues that are addressed in this research, which proposes a novel technique to solving these difficulties. The strategy will be broken down into its component parts in more depth in the following paragraphs. These challenges are investigated to a certain degree of detail. The use of the passive voice directs attention to the processes and results that are produced by the procedures that are advocated, which in turn makes it easier to get a deeper understanding of the operational mechanisms that are at work.

The primary purpose of this line of research is to locate WSN nodes that have been hacked as a result of illegal activities. To achieve this goal, we shall conduct an exhaustive study of the features of the network. Monitoring a variety of characteristics, including traffic patterns, node activity, and communication abnormalities, enables a high degree of precision to be attained when establishing the location of potentially compromised nodes in a network. These characteristics include traffic patterns, node activity, and communication irregularities. In addition, methods of machine learning are employed in a malleable manner, which enables the system to develop in a dynamic manner in response to altering dangers and ensures the identification of new assault patterns. This is made possible by the utilization of adaptable machine learning approaches. Putting adaptive machine learning strategies into practice makes this kind of thing practical [36,37].

After it has been determined which nodes have been compromised, the second objective is to locate a technique that will prevent the performance of the system from deteriorating. This may be accomplished via the use of cooperative cache management, which combines data and process affinity. Finding an answer to this predicament will allow us to successfully complete this task. If the surrounding sensor nodes adopt this approach of cooperative caching, they will be able to store and retrieve data that is relevant to the processing activities that they are carrying out as a group, which will allow them to perform more efficient processing. An increase in the quantity of data that is available, a decrease in the amount of transmission overhead, and an improvement in the overall performance of the network are some of the direct implications of this.

2. Related Works

In the recent time, a good number of research works can be observed in providing the security solutions for wireless devices. Few of the papers provided solutions, which are only applicable for WSN or only for MANET or only for IoT networks. However, this work analyses the generic solutions rather than only specific solutions and aims to adopt the solutions to the proposed framework, which intends to solve the challenges for WSN.

Sun *et al.,* [1] presented a paper titled "Distributed Learning-Based Cache Replacement in Collaborative Edge Networks," published in IEEE Communications Letters in August 2021. The authors proposed a novel approach for cache replacement in collaborative edge networks using distributed learning. The objective is to optimize cache utilization and improve overall network performance. By employing a distributed learning framework, the proposed approach allows edge nodes to learn from their local caching experiences and collaboratively make cache replacement decisions. The distributed learning process ensures adaptability and scalability, enabling the system to efficiently handle dynamic network conditions and user demands. Extensive simulations and comparisons with traditional cache replacement algorithms demonstrate the effectiveness and superiority of the proposed approach, showcasing its potential to enhance the caching performance and user experience in collaborative edge networks.

Gurram *et al.,* [2] presented work introduces the SEAMHR protocol, leveraging Meta-Heuristic analysis based on MEHO for intelligent learning in WSNs. The protocol employs Counter Mode Cryptography using AEs (Autoencoders) known as CTR-AEDL for secure data transmissions. The encryption method generates unique patterns for counter blocks, enhancing security. The protocol's performance is compared with SEHR, Sec Trust-RPL, and HBEER, demonstrating improvements in energy consumption, network throughput, PDRs, and identification of faulty routes in low-powered SNs. However, the specifics of algorithms, training procedures, and dataset characteristics remain undisclosed.

Chen *et al.,* [3] presented a paper titled "Mobile Edge Cache Strategy Based on Neural Collaborative Filtering" published in IEEE Access in 2020. The authors proposed a mobile edge cache strategy based on neural collaborative filtering to improve content delivery in mobile networks. The approach employs machine learning techniques to predict user preferences for cached content at the edge nodes. By leveraging user behaviour data, the proposed strategy enhances content caching decisions, reducing latency and enhancing user satisfaction. Extensive simulations demonstrate the superiority of the neural collaborative filtering-based approach compared to traditional caching methods, showcasing its potential to optimize content delivery in mobile edge networks.

Li, Hu and Li [4] presented a paper titled "CVC: A Collaborative Video Caching Framework Based on Federated Learning at the Edge" in IEEE Transactions on Network and Service Management in June 2022. The authors proposed a collaborative video caching framework based on federated learning at the edge. The objective is to improve video caching efficiency and reduce edge server workload. The proposed framework enables edge nodes to collaboratively learn from local video requests and cache content that is likely to be accessed by nearby users. Federated learning ensures privacy preservation while allowing the sharing of caching knowledge among edge nodes. Extensive experiments demonstrate the effectiveness of the CVC framework, showcasing its potential to enhance video delivery performance and reduce network congestion.

Li *et al.,* [5] presented a paper titled "A Collaborative Caching-Transmission Method for Heterogeneous Video Services in Cache-Enabled Terahertz Heterogeneous Networks" in IEEE Transactions on Vehicular Technology in March 2022. The authors proposed a collaborative caching-transmission method for heterogeneous video services in cache-enabled terahertz heterogeneous networks. The objective is to efficiently utilize the limited cache resources and enhance the delivery of video content. The proposed method utilizes collaborative caching and joint transmission strategies, optimizing the allocation of cached content and transmission power across multiple terahertz base stations. Extensive simulations demonstrate the superiority of the proposed method, showcasing its ability to improve the video delivery quality and network efficiency in cache-enabled terahertz heterogeneous networks.

Furqan *et al.,* [6] presented a paper titled "A Collaborative Hotspot Caching Design for 5G Cellular Network" in IEEE Access in 2018. The authors proposed a collaborative hotspot caching design for 5G cellular networks to improve the efficiency of content delivery in highly congested areas. The approach employs a collaborative caching strategy among base stations to reduce latency and alleviate backhaul traffic. The proposed design ensures that frequently requested content is readily available at cache-enabled base stations, enhancing the user experience. Simulation results show that the collaborative hotspot caching design significantly reduces latency and improves the overall network performance in 5G cellular networks.

Chiang, Hsu and Wei [7] presented a paper titled "Collaborative Social-Aware and QoE-Driven Video Caching and Adaptation in Edge Network" in IEEE Transactions on Multimedia. The authors proposed a collaborative social-aware and quality-of-experience (QoE)-driven video caching and adaptation approach for edge networks. The objective was to enhance the delivery of video content by considering social relationships among users and QoE preferences. The proposed approach employs social-aware content recommendation and QoE-driven caching and adaptation strategies to optimize content delivery in edge networks. Extensive evaluations demonstrate the superiority of the proposed approach, showcasing its potential to improve user satisfaction and network performance.

Tang *et al.,* [8] presented a paper titled "Collaborative Cache-Aided Relaying Networks: Performance Evaluation and System Optimization" in IEEE Journal on Selected Areas in Communications in March 2023. The authors presented a comprehensive performance evaluation and system optimization for collaborative cache-aided relaying networks. The objective was to enhance the overall network performance and user experience through cache-aided relaying strategies. The authors propose a resource allocation scheme to optimize cache placement and transmission power allocation among collaborating nodes. Extensive simulations and analyses demonstrate the benefits of cache-aided relaying networks, highlighting their potential to improve spectral efficiency and user experience.

Lei *et al.,* [9] presented a paper titled "Partially Collaborative Edge Caching Based on Federated Deep Reinforcement Learning" in IEEE Transactions on Vehicular Technology in January 2023. The authors proposed a partially collaborative edge caching approach based on federated deep reinforcement learning to enhance cache performance in edge networks. The proposed approach combines local caching and cooperative caching decisions through federated learning. By leveraging deep reinforcement learning, the caching policy adapts to the dynamic network environment, optimizing cache allocation and improving content delivery efficiency. Simulation results demonstrate the effectiveness of the proposed approach, showcasing its potential to enhance cache performance and user experience in edge networks.

Mehrabi *et al.,* [10] presented a paper titled "QoE-Traffic Optimization Through Collaborative Edge Caching in Adaptive Mobile Video Streaming" in IEEE Access in 2018. The authors proposed a collaborative edge caching approach for adaptive mobile video streaming to optimize quality of experience (QoE) and reduce traffic load in mobile networks. The proposed approach employs a collaborative caching scheme among edge nodes to cache frequently accessed video segments. By adapting video quality based on network conditions and user preferences, the approach optimizes the QoE of mobile video streaming while reducing the need for backhaul communication. Extensive experiments demonstrate the effectiveness of the proposed approach, showcasing its potential to enhance QoE and reduce network congestion.

Zhang *et al.,* [11] presented a paper titled "Dual-Timescale Resource Allocation for Collaborative Service Caching and Computation Offloading in IoT Systems" in IEEE Transactions on Industrial

Informatics in February 2023. The authors propose a dual-timescale resource allocation framework for collaborative service caching and computation offloading in IoT systems. The objective was to optimize the allocation of resources, including computing resources and caching space, to enhance the performance of IoT services. The proposed framework leverages reinforcement learning and optimization techniques to adaptively allocate resources at different timescales, considering dynamic IoT service demands. Simulation results demonstrate the superiority of the dual-timescale resource allocation framework, showcasing its potential to improve IoT service performance and resource utilization.

Yang *et al.,* [12] presented a paper titled "Collaborative Edge Caching and Transcoding for 360° Video Streaming Based on Deep Reinforcement Learning" in IEEE Internet of Things Journal in December 2022. The authors proposed a collaborative edge caching and transcoding approach for 360° video streaming based on deep reinforcement learning. The objective was to enhance the delivery of immersive 360° video content in edge networks. The proposed approach leverages deep reinforcement learning to optimize edge caching and transcoding decisions, reducing latency and enhancing the user experience. Extensive simulations demonstrate the effectiveness of the proposed approach, showcasing its potential to improve 360° video streaming quality and reduce network congestion.

Chen *et al.,* [13] presented a paper titled "Collaborative Content Placement Among Wireless Edge Caching Stations with Time-to-Live Cache" in IEEE Transactions on Multimedia in February 2020. The authors proposed a collaborative content placement approach among wireless edge caching stations with time-to-live cache to optimize content delivery in edge networks. The approach considered the time-to-live constraint of cached content and employs a collaborative caching strategy to store popular content items at appropriate edge caching stations. Extensive evaluations demonstrated the benefits of the proposed approach, showcasing its potential to enhance cache utilization and reduce content access latency in wireless edge networks.

Li *et al.,* [14] presented a paper titled "Temporal-Spatial Collaborative Mobile Edge Caching with User Satisfaction Awareness" in IEEE Transactions on Network Science and Engineering in September-October 2022. The authors propose da temporal-spatial collaborative mobile edge caching approach with user satisfaction awareness to improve content delivery in mobile edge networks. The approach employed temporal-spatial collaboration among edge nodes to enhance caching efficiency, taking into account user satisfaction preferences. Simulation results demonstrate the effectiveness of the proposed approach, showcasing its potential to improve cache performance and user satisfaction in mobile edge networks.

Rui *et al.,* [15] presented a paper titled "Content Collaborative Caching Strategy in the Edge Maintenance of Communication Network: A Joint Download Delay and Energy Consumption Method" in IEEE Transactions on Parallel and Distributed Systems in December 2022. The authors proposed a content collaborative caching strategy for edge maintenance in communication networks, considering joint download delay and energy consumption. The objective is to optimize content caching decisions while considering the trade-off between download delay and energy consumption. The proposed strategy leverages a heuristic algorithm to determine cache content and caching locations, optimizing the overall network performance. Extensive experiments demonstrate the effectiveness of the proposed strategy, showcasing its potential to reduce download delay and energy consumption in edge networks.

Liu *et al.,* [16] presented a paper titled "Collaborative Online Edge Caching with Bayesian Clustering in Wireless Networks" in IEEE Internet of Things Journal in February 2020. The authors proposed a collaborative online edge caching approach with Bayesian clustering for wireless networks. The objective is to efficiently utilize the cache resources in wireless edge nodes and improve content delivery efficiency. The proposed approach employs Bayesian clustering to group users with similar content preferences, enhancing the cache hit rate and reducing content delivery latency. Extensive simulations demonstrate the effectiveness of the proposed approach, showcasing its potential to improve cache performance and user experience in wireless networks.

Chen *et al.,* [17] presented a paper titled "Cache-Assisted Collaborative Task Offloading and Resource Allocation Strategy: A Metareinforcement Learning Approach" in IEEE Internet of Things Journal in October 2022. The authors proposed a cache-assisted collaborative task offloading and resource allocation strategy using a metareinforcement learning approach. The objective is to optimize task offloading decisions and resource allocation among edge nodes to enhance the performance of IoT services. The proposed metareinforcement learning framework learns from past experiences to adaptively allocate resources and optimize task offloading decisions. Simulation results demonstrate the effectiveness of the proposed approach, showcasing its potential to improve IoT service performance and resource utilization.

Ugwuanyi *et al.,* [18] presented a paper titled "A Novel Predictive-Collaborative-Replacement (PCR) Intelligent Caching Scheme for Multi-Access Edge Computing" in IEEE Access in 2021. The authors proposed a novel predictive-collaborative-replacement (PCR) intelligent caching scheme for multi-access edge computing to improve cache performance. The proposed scheme leverages predictive modelling and collaborative replacement to optimize cache replacement decisions in edge computing environments. Extensive simulations demonstrate the superiority of the PCR caching scheme, showcasing its potential to enhance cache utilization and content delivery performance in multi-access edge computing scenarios.

Wu *et al.,* [19] presented a paper titled "Social-Aware Graph-Based Collaborative Caching in Edge-User Networks" in IEEE Transactions on Vehicular Technology in June 2023. The authors proposed a social-aware graph-based collaborative caching approach in edge-user networks to optimize content delivery efficiency. The approach considers social relationships among users and leverages graph theory to model the social-aware caching problem. The proposed caching strategy aims to maximize the cache hit rate and reduce content delivery latency in edge-user networks. Extensive evaluations demonstrate the benefits of the proposed approach, showcasing its potential to improve cache performance and user experience.

Khanal *et al.,* [20] present a paper titled "DCoL: Distributed Collaborative Learning for Proactive Content Caching at Edge Networks" in IEEE Access in 2021. The authors propose a distributed collaborative learning approach for proactive content caching at edge networks to improve cache performance and reduce latency. The proposed DCoL framework allows edge nodes to collaboratively learn and predict future content demands, enabling proactive content caching decisions. Extensive experiments demonstrate the effectiveness of the DCoL approach, showcasing its potential to enhance cache performance and reduce content access latency in edge networks.

Wang and Zhou [21] present a paper titled "Fractional Dynamic Caching: A Collaborative Design of Storage and Backhaul" in IEEE Transactions on Vehicular Technology in April 2020. The authors propose a fractional dynamic caching approach for collaborative design of storage and backhaul in wireless networks. The objective is to optimize cache resource allocation and reduce backhaul communication cost. The proposed approach leverages fractional programming to allocate cache space and dynamically adjust caching strategies based on varying content popularity and network conditions. Extensive evaluations demonstrate the benefits of the proposed approach, showcasing its potential to reduce backhaul traffic and improve overall network performance.

Feng *et al.,* [22] present a paper titled "Collaborative Data Caching and Computation Offloading for Multi-Service Mobile Edge Computing" in IEEE Transactions on Vehicular Technology in September 2021. The authors propose a collaborative data caching and computation offloading approach for multi-service mobile edge computing to optimize resource utilization and enhance service performance. The approach leverages a joint optimization framework to simultaneously optimize caching and computation offloading decisions. Extensive simulations demonstrate the effectiveness of the proposed approach, showcasing its potential to improve resource utilization and service performance in multi-service mobile edge computing scenarios.

Wang, Chen and Wang [23] present a paper titled "Collaborative Caching for Energy Optimization in Content-Centric Internet of Things" in IEEE Transactions on Computational Social Systems in February 2022. The authors propose a collaborative caching approach for energy optimization in content-centric Internet of Things (IoT) environments. The objective is to reduce energy consumption while improving content delivery efficiency. The proposed approach employs a distributed caching scheme among IoT devices to share cached content, reducing the need for content retrieval from remote servers. Extensive evaluations demonstrate the benefits of the collaborative caching approach, showcasing its potential to reduce energy consumption and improve content delivery efficiency in content-centric IoT environments.

Zhao *et al.,* [24] present a paper titled "Collaborative Edge Caching in Context-Aware Device-to-Device Networks" in IEEE Transactions on Vehicular Technology in October 2018. The authors propose a collaborative edge caching approach in context-aware device-to-device (D2D) networks to optimize cache utilization and content delivery efficiency. The proposed approach considers the context-awareness of D2D communications and employs a collaborative caching strategy among user devices to store and share frequently requested content. Simulation results demonstrate the effectiveness of the proposed approach, showcasing its potential to enhance cache performance and reduce content access latency in context-aware D2D networks.

Xu *et al.,* [25] present a paper titled "Collaborative Multi-Agent Multi-Armed Bandit Learning for Small-Cell Caching" in IEEE Transactions on Wireless Communications in April 2020. The authors propose a collaborative multi-agent multi-armed bandit (MAB) learning approach for small-cell caching in wireless networks. The objective is to optimize content caching decisions among small-cell base stations to improve cache utilization and content delivery efficiency. The proposed collaborative MAB learning approach enables small-cell base stations to learn from each other's caching experiences, improving the overall cache performance. Extensive evaluations demonstrate the benefits of the proposed approach, showcasing its potential to enhance cache performance and content delivery efficiency in small-cell caching scenarios. Further, the recent works are summarized in order to identify the existing research challenges in Table 1.

Table 1
Summary of Recent Works

Author, Year	Proposed Method	Limitations
Y. Li *et al.,* [4]	A system for collaborative video caching is proposed, which leverages federated learning techniques at the edge.	- The maintenance of privacy and security of user data poses significant challenges within a federated learning framework. - One of the challenges that arises with an increasing number of participating edge devices is the problem of scalability. - The communication overhead associated with the exchange of model changes inside a federated learning framework.

Q. Li *et al.,* [5]	The proposed technique explores a collaborative caching-transmission approach for cache-enabled terahertz heterogeneous networks, specifically targeting the delivery of heterogeneous video services.	- The obstacles associated with terahertz communication include propagation loss and the constraint of restricted service area. - The challenge lies in the intricate coordination of cache management and transmission techniques across devices with varying characteristics and capabilities. - There exists a trade-off between cache capacity and transmission resources.
S. Tang *et al.,* [8]	This study focuses on collaborative cache-aided relaying networks, examining their performance assessment and system improvement.	- The task of building cache replacement and relay selection algorithms entails addressing the intricacies and challenges associated with achieving optimum performance. - The attainment of effective cooperation between relays and users presents a number of practical problems. - The impact of network dynamics and user mobility on system performance sensitivity.
M. Lei *et al.,* [9]	The proposed approach involves the use of federated deep reinforcement learning to implement a partially collaborative edge caching system.	- The task of achieving a balance between exploration and exploitation in cache management choices poses significant challenges. - The implementation of a federated learning technique is subject to resource limits and communication overhead.
J. Zhang *et al.,* [11]	The topic of interest is the allocation of resources in IoT systems for the purpose of collaborative service caching and compute offloading. Specifically, the focus is on a dual-timescale approach to this resource allocation.	- The intricate interplay of caching, computation offloading, and resource allocation determinations. - The issue of scalability arises when the quantity of Internet of Things (IoT) devices grows. - The reliance on precise forecasting of forthcoming resource requirements and network circumstances.
D. Wu *et al.,* [19]	The present study focuses on the implementation of social-aware graph-based collaborative caching in edge-user networks.	- The issue of privacy arises when using social network data for cache management purposes. - The modelling and maintenance of dynamic social ties in caching choices provide significant challenges. - The acquisition and analysis of social network data for the purpose of cache optimization.

In the subsequent portion of this study, a detailed exposition is provided about the suggested mathematical model and the accompanying methods.

3. Proposed Solutions

After realizing the bottlenecks of the recent research outcomes, this section furnishes the solutions for two major problems. Firstly, the identification of the compromised node and secondly, formation of the cooperative cache for avoiding the routing path through that compromised node is visually presented in the Figure 1.

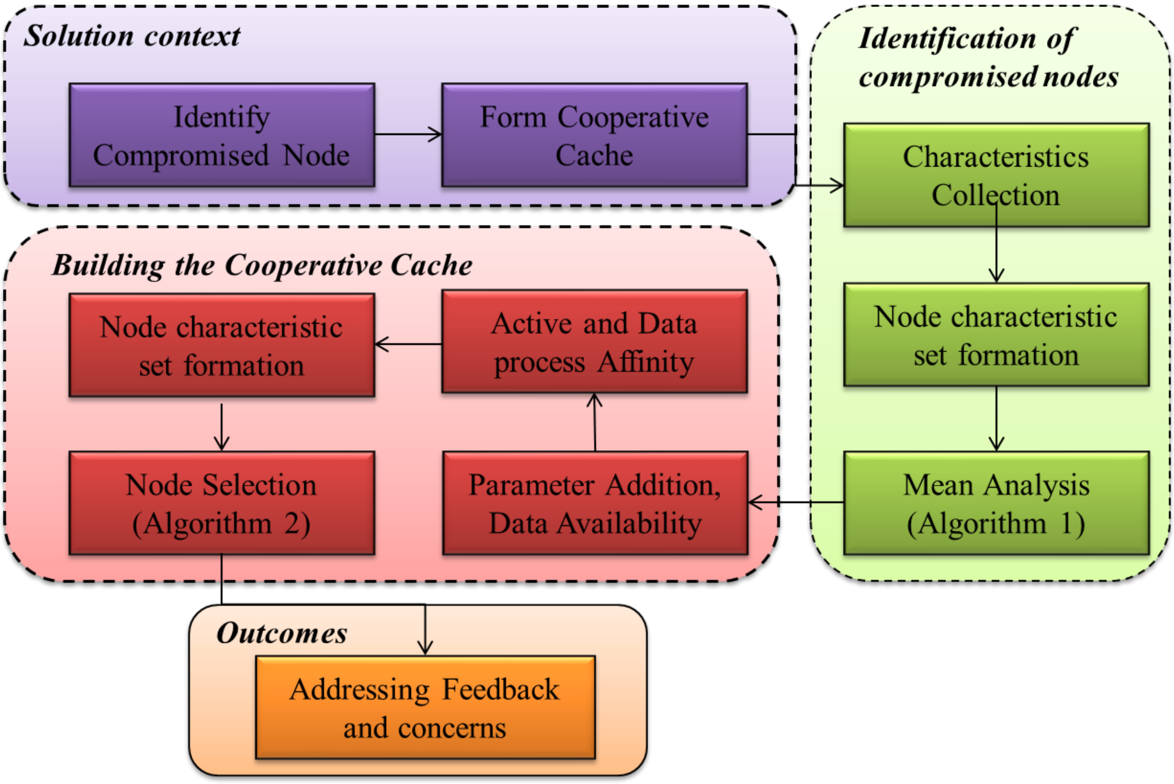
Solution context
Identify Compromised Node
Form Cooperative Cache
Identification of compromised nodes
Characteristics Collection
Node characteristic set formation
Mean Analysis (Algorithm 1)
Building the Cooperative Cache
Node characteristic set formation
Active and Data process Affinity
Node Selection (Algorithm 2)
Parameter Addition, Data Availability
Outcomes
Addressing Feedback and concerns

Fig. 1. Overall Proposed Framework

4. Solution Context

The traditional approaches recommends that after identification of the compromised node in the WSN network and further avoidance of the routing through that node in the network. However, during this avoidance process, the network must remain functional. To maintain the functions such as routing of the network, a different routing path must be designated. During the formation of this new routing path, the data packets, which are under transmission must not be dropped. Thus, formation of the cooperative cache is important.

The use of cooperative caching in Wireless Sensor Networks (WSNs) provides notable advantages as it facilitates the storage and sharing of frequently requested data across neighbouring sensor nodes. The technique effectively mitigates duplicate data transfers, reduces latency, and optimizes energy consumption by enabling sensor nodes to acquire data from nearby caches instead of remote sources. Cooperative caching in Wireless Sensor Networks (WSNs) has the potential to boost data access efficiency, optimize network performance, and prolong the network's lifetime. This is achieved by eliminating energy-intensive communication and data retrieval activities.

5. Identification of the Compromised Nodes

The identification of a hacked node in a Wireless Sensor Network (WSN) may be accomplished by conducting a thorough examination of various characteristics. Indicators of compromise include several factors such as anomalous energy consumption patterns, unexpected locations, rapid changes in mobility speed, higher packet loss rates, and abnormal resource use. Through the process of monitoring and comparing these data with set standards, it becomes possible to identify any abnormalities, which in turn facilitates the prompt detection and isolation of compromised nodes. This ultimately enhances the security and integrity of the network. In order to formulate the proposed solution, this work furnishes the below justifications. Assuming that, the complete network is identified as N[] for "n" number of nodes in the network. Then the initial collection can be formulated as,

$$N[] = < n_1, n_2, ...n_n > \tag{1}$$

As the proposed method relies on the characteristics of the node, thus formation of the node characteristics set is important as furnished below,

$$n_i = [ECR, Cor_{X,Y}(t), M, PDR, RU]_i \tag{2}$$

Where, ECR is the Energy Consumption Rate. $Cor_{X,Y}(t)$ is the coordination at time "t". M is the mobility of the node. PDR is the packet dropping rate. RU is the resource utilization matrix. Firstly, the ECR is calculated with a simple logic to identify the battery level difference during the unit time as,

$$ECR = \frac{|BT(t) - BT(t+1)|}{\Delta t} \tag{3}$$

Secondly, in order to calculate the mobility, the Euclidean distance, ED, must be calculated between two coordinates, Cor$_{X,Y}$(t) and Cor$_{X,Y}$(t+1) as,

$$ED = \sqrt{(X(t) - X(t+1))^2 + (Y(t) - Y(t+1))^2} \tag{4}$$

Then, the mobility can be identified as the ED per unit time as,

$$M = \{ {}^{ED}\!/_{\Delta t} \} \tag{5}$$

Third, the packet dropping rate can be identified based on the amount of data received, R(t) at t time instance and the data forwarded, S(t+1) at t+1 time instance for unit time as mean,

$$PDR = \frac{|S(t+1) - R(t)|}{\Delta t} \tag{6}$$

Finally, the resource utilization (RU) matrix is designed using resources such as compute (C), Memory (M) and Network utilization (N). In order to generate the utilization metric, it is recommended that a normalized value for resource utilization must be calculated, and this method recommends using the linear regression method for building the value as,

$$RU = \beta_1.C + \beta_2.M + \beta_3.N \tag{7}$$

Thus, the final network proposition can be designed as,

$$N[] = < n_i >_n = \{ECR[], Cor_{X,Y}(t)[], M[], PDR[], RU[]\} \tag{8}$$

Now in order to build the strategy for identification of compromised node, it is a must to design the threshold for each parameter and this work recommends the threshold as mean for each parameter. The means are calculated as,

$$Mean\_ECR = \frac{\sum_i ECR[i]}{n}$$
$$Mean\_M = \frac{\sum_i M[i]}{n}$$
$$Mean\_PDR = \frac{\sum_i PDR[i]}{n}$$
$$Mean\_RU = \frac{\sum_i RU[i]}{n} \tag{9}$$

Thus, the final compromised nodes, $\widehat{N}[]$, can be identified as,

$$\widehat{N}[] = \prod_{ECR[i]>Mean\_ECR} N[i] \cap \prod_{M[i]>Mean\_M} N[i]$$
$$\cap \prod_{PDR[i]>Mean\_PDR} N[i] \cap \prod_{RU[i]>Mean\_RU} N[i] \tag{10}$$

Thus, based on the proposed strategy, the proposed algorithm is furnished.

Algorithm - 1: Identification of Compromised Nodes using Network Characteristics Mean Analysis (**ICN-NCMA**) Algorithm

Input:

Sensor nodes' data containing energy levels, locations, mobility speeds, packet loss rates, and resource utilization.

Output:

List of compromised nodes.

Assumptions:

- Mean Threshold for Energy: E_threshold
- Mean Threshold for Location: L_threshold
- Mean Threshold for Mobility Speed: S_threshold
- Mean Threshold for Packet Loss: P_threshold
- Mean Threshold for Resource Utilization: R_threshold

Process:

Step - 1. Initialize an empty list compromised_nodes.

Step - 2. Iterate through each sensor node in the WSN:

  a. Collect the energy level, location, mobility speed, packet loss rate, and resource utilization data for the node.

Step - 3. For each data attribute, calculate the mean value based on historical data or a sliding window of recent data.

  a. Compare each attribute's mean value with the corresponding threshold:
  b. If the mean energy level is greater than E_threshold, mark the node as compromised in terms of energy.

c. If the mean location deviation is greater than L_threshold, mark the node as compromised in terms of location.
d. If the mean mobility speed is greater than S_threshold, mark the node as compromised in terms of mobility.
e. If the mean packet loss rate is greater than P_threshold, mark the node as compromised in terms of packet loss.
f. If the mean resource utilization is greater than R_threshold, mark the node as compromised in terms of resource utilization.
g. If a node is marked as compromised in any of the above criteria, add it to the compromised_nodes list.

Step - 4. After iterating through all nodes, return the compromised_nodes list containing the identified compromised nodes.

The adjustment of threshold values (E_threshold, L_threshold, S_threshold, P_threshold, R_threshold) is of significant importance, as it should be tailored to the individual features of the Wireless Sensor Network (WSN) and the needs of the application at hand. Furthermore, it is essential to take into account supplementary elements such as data authentication and anomaly detection in order to augment the precision of identifying hacked nodes. This method presupposes the availability of previous data for the purpose of computing mean values, or alternatively, the implementation of a device to retain sliding windows of current data. The obtained outcomes are again discussed in the next section of this work.

6. Building the Cooperative Cache

Once the identification of the compromised nodes is achieved, the final phase of the solution proposes to build the cooperative caching mechanism. The construction of a cooperative cache in a Wireless Sensor Network (WSN) entails the use of existing data, current processes, data affinity, and communication ranges to enhance the efficiency of data access. The nodes work together to store often accessed data in their caches, so minimizing unnecessary transmissions and improving the efficiency of cache hits. The strategic caching of related data items for enhanced retrieval may be achieved by taking into account data affinity, which refers to the frequency with which data items are retrieved together. Communication ranges play a crucial role in facilitating efficient sharing of cached data across surrounding nodes, hence reducing latency and optimizing energy consumption. The use of this collaborative caching strategy improves the overall performance of wireless sensor networks (WSNs) by lowering latency and improving resource consumption. This is achieved via the employment of intelligent methods for data storage and sharing. In order to formulate the proposed solution, this work furnishes the below justifications.

Adding the following parameters such as data availability, D[], running active processes, P[], process-data affinity, PD[], into the existing node characteristics as,

$$N[] = < D[], P[], PD[] > \tag{11}$$

The data availability for each node can be further identified as,

$$n_i = [d_1, d_2 ...., d_k] \tag{12}$$

For k is the number of data items. Similarly, the collection of the active processes can also be furnished as,

$$n_i = [p_1, p_2 ...., p_r] \tag{13}$$

For r refers number of processes. Also, a sample formulation of the data-process affinity can be formulated, a simple example, as,

$$\begin{array}{cccc} & p_i & p_j & p_k \\ d_i & n_1, n_2 & n_1, n_3 & n_2, n_4 \\ d_j & n_3, n_5 & n_2, n_3 & n_1, n_2 \\ d_k & n_1, n_5 & n_2, n_5 & n_4, n_5 \end{array} \tag{14}$$

Thus, from this sample, it is natural to realize that multiple processes and multiple data items, same or different can be part of the same set of nodes. Henceforth, firstly, it is recommended to select the nodes based on the process availability or same active process list as,

$$\hat{N}_1[] = \prod_{p_i \subseteq \widehat{N}[j] \cdot p_i} \widehat{N}[] \tag{15}$$

Secondly, based on the data availability the further selection of nodes must be carried out as,

$$\hat{N}_2[] = \prod_{d_i \subseteq \widehat{N}[j] . d_i} \widehat{N}[] \tag{16}$$

Thirdly, the nodes further must be selected based on the distance overlaps with the standard range (R) of the network. This can be formulated as,

$$\hat{N}_3[] = \prod_{ED_i \approx R} \widehat{N}[i] \,\&\, \widehat{N}[i+1] \tag{17}$$

Finally, the list of nodes participating in the cooperative cache can be formulated as,

$$\overleftrightarrow{N}[] = \prod_{p_i \subseteq \widehat{N}[j] \cdot p_i} \widehat{N}[] \cap \prod_{d_i \subseteq \widehat{N}[j] . d_i} \widehat{N}[] \\ \cap \prod_{ED_i \approx R} \widehat{N}[i] \,\&\, \widehat{N}[i+1] \tag{18}$$

Thus, based on the proposed strategy, the proposed algorithm is furnished. The cache management system prioritizes caching based on data availability, active processes, and data-process affinity parameters, aiming to store frequently accessed data efficiently. Decisions on what to cache and for how long are influenced by the dynamic nature of ongoing processes and the affinity between data and processes. Trade-offs, particularly in memory overhead, are inherent, and the system must strike a balance between optimizing data retrieval and managing memory resources effectively.

Algorithm - 2: WSN Cooperative Cache Formation using Data Process Affinity (**WSN-CCF-DPA**) Algorithm

```
Input:
Sensor nodes' data containing available data items, current processes, data affinity relationships, and communication range.
Output:
Cooperative cache structure containing cached data items for each node.
Assumptions:
Communication Range: R_comm
Data Affinity Table: affinity_table
Process:
Step - 1.   Initialize an empty cooperative cache structure cooperative_cache to store cached data items for each sensor node.
Step - 2.   For each sensor node node_i in the WSN:
    a. Create an empty cache entry cache_entry_i for node_i in the cooperative_cache.
Step - 3.   Iterate through each available data item data_item:
    a. Determine the data affinity relationships from the affinity_table for the data_item.
    b. For each sensor node node_j in the data affinity relationship of data_item:
    c. If the distance between node_i and node_j is within the communication range R_comm:
    d. Add data_item to the cache entry cache_entry_i of node_j in the cooperative_cache.
Step - 4.   For each sensor node node_i in the WSN:
        a. Retrieve the cached data items from the cache entry cache_entry_i of node_i in the cooperative_cache.
Step - 5.   During the operation of the WSN:
    a. Monitor the data usage patterns and process requirements of each sensor node.
    b. Identify frequently requested data items and processes with high demand.
    c. Update the cached data items in the cooperative_cache based on the identified patterns and demands.
    d. Periodically or upon certain events:
    e. Reevaluate the data affinity relationships and communication ranges.
    f. Update the affinity_table based on new data relationships or changes in network topology.
Step - 6.   Utilize the cooperative cache during data retrieval and processing:
    a. When a sensor node requires a specific data item, first check if it's available in the node's local cache entry.
    b. If not, search the cache entries of nearby nodes within R_comm to find the required data item.
Step - 7.   If a data item is found in another node's cache, utilize the cooperative cache:
    a. Retrieve the data item from the cache entry of the node with the cached data item.
    b. Optionally, update the local cache entry of the requesting node with the retrieved data item.
Step - 8.   Continue monitoring and updating the cooperative cache to maintain up-to-date data items and improve cache efficiency.
```

The underlying assumption of this technique is that the affinity_table includes comprehensive data about the affinity associations between sensor nodes. In a dynamic Wireless Sensor Network (WSN) environment, it is essential to use procedures that address cache replacement rules, cache synchronization, and the maintenance of consistency. The effectiveness of the cooperative cache is heavily contingent upon the precision of the affinity_table and the configuration of the communication range (R_comm). Further, in the next section of this work, the obtained outcomes are furnished.

7. Results and Discussions

This research has provided a thorough examination of an innovative strategy for mitigating the difficulties arising from compromised nodes inside Wireless Sensor Networks (WSNs). In this part, we will examine the outcomes derived from our experimental investigations and analyse their consequences, so elucidating the efficacy of the suggested cooperative cache-based approach. This study examines the advancements in performance resulting from the mitigation of compromised nodes, the reinforcement of network resilience, and the optimization of data retrieval operations. In addition, we investigate the effects of various cooperative caching techniques on the overall network performance, taking into account metrics such as latency, throughput, and energy usage. Through a critical examination of these findings, valuable insights may be obtained on the feasibility and advantages of our methodology. Consequently, this contributes to the wider discussion on enhancing the security and efficiency of Wireless Sensor Networks (WSNs) in light of possible security vulnerabilities and performance deterioration. The result and discussion section furnishes the results with the following subsections:

8. Dataset Analysis

This work deploys the proposed algorithms and the benchmarked algorithms on three different datasets [26].The descriptions of the datasets are furnished here in Table 2.

Table 2
Dataset Description

Dataset Name	Year of Publish	Number of Attributes	Number of Records
WSN-DS	2019	9	3250
LT-FS-ID	2022	7	2541
WSN: Localization Error	2022	7	1897

9. Experimental Setups

This work simulates the proposed algorithms on OMNET++ and also on Google Colab for testing the actual scenarios and generic conditions respectively. The initial conditions are furnished here in

Table 3
Experimental Setup

Research Methods	Number of Initial Nodes	Area (sqmt)	Transmission Range (m)	Simulation Duration (ms)	Compromised Node Detection	Cache Cooperation
Y. Li *et al.,* [4]	50	100	10	36000	√	√
Q. Li *et al.,* [5]	50	100	10	36000	√	√
S. Tang *et al.,* [8]	50	100	10	36000	√	√
M. Lei *et al.,* [9]	50	100	10	36000	√	√
J. Zhang *et al.,* [11]	50	100	10	36000	√	√
D. Wu *et al.,* [19]	50	100	10	36000	√	√
Proposed Algorithm	50	100	10	36000	√	√

10. Energy Consumption Analysis

The first analysis on the proposed and existing systems algorithms are carried out on the energy consumption to detect the anomalies on the network nodes. The obtained results are furnished here in Table 4.

Table 4
Energy Consumption Analysis

Research Method	Proposed Method	Mean Energy Consumption (W)	Actual Number of Compromised Nodes	Detected Number of Compromised Nodes
Y. Li *et al.,* [4]	Federated Learning	147.80	9	4
Q. Li *et al.,* [5]	Terahertz Heterogeneous Networks	152.23	9	4
S. Tang *et al.,* [8]	Relaying Networks	153.71	9	4
M. Lei *et al.,* [9]	Federated Deep Reinforcement Learning	143.37	9	5
J. Zhang *et al.,* [11]	Computation Offloading	155.19	9	5
D. Wu *et al.,* [19]	Graph-Based Collaborative Caching	140.41	9	5
Proposed Algorithm	Characteristics Based Rule Engine	135.98	9	8

The use of a Characteristics Based Rule Engine emerges as a more advanced approach for identifying compromised nodes in Wireless Sensor Networks (WSNs) owing to its inherent flexibility and accuracy [27,28]. In contrast to conventional methods that depend only on predetermined signatures or behavioural patterns, the Characteristics Based Rule Engine utilizes a dynamic collection of node-specific features and behaviour metrics. This capability allows the engine to efficiently identify abnormalities and harmful actions that would be overlooked by static approaches. By consistently assessing deviations from predetermined node characteristics, this methodology may adjust to shifting attack techniques and emerging threats, providing improved precision in detecting compromised nodes [29,30]. The system's capacity to customize detection criteria based on the distinct attributes of each node optimizes the rate of detection while limiting instances of false positives, therefore establishing a resilient and adaptable solution for protecting Wireless Sensor Networks (WSNs) against security breaches. The results are also visualized graphically in Figure 2.

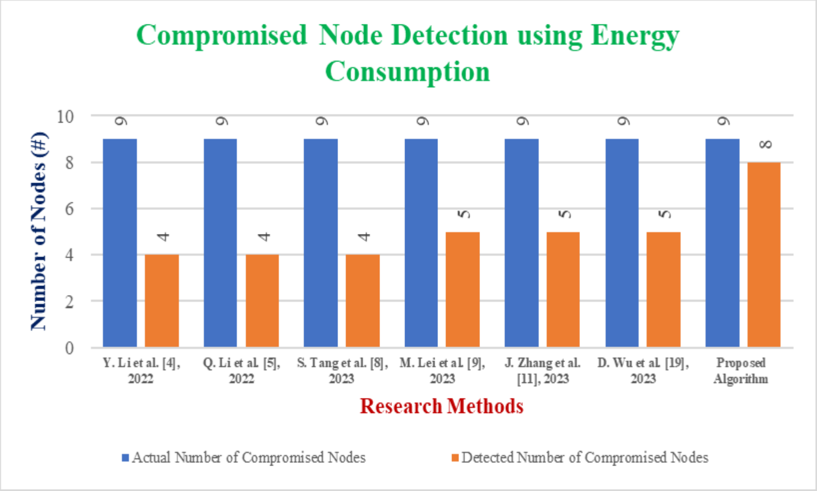

Fig. 2. Compromised Node Detection using Energy Consumption

It is natural to realize that the proposed method, using the threshold setting method, has reduced the overall energy consumption thresholds by 8% and detected the maximum number of compromised nodes.

11. Mobility Analysis

As discussed, the mobility factors play a major role for detection of the compromised node is very crucial. The proposed and the existing algorithms are deployed to analyse the compromised nodes. The outcomes are furnished here in Table 5.

Table 5
Mobility Analysis

Research Method	Proposed Method	Mean Mobility (mps)	Actual Number of Compromised Nodes	Detected Number of Compromised Nodes
Y. Li *et al.,* [4]	Federated Learning	45	9	5
Q. Li *et al.,* [5]	Terahertz Heterogeneous Networks	39	9	7
S. Tang *et al.,* [8]	Relaying Networks	47	9	7
M. Lei *et al.,* [9]	Federated Deep Reinforcement Learning	31	9	5
J. Zhang *et al.,* [11]	Computation Offloading	45	9	7
D. Wu *et al.,* [19]	Graph-Based Collaborative Caching	37	9	4
Proposed Algorithm	Characteristics Based Rule Engine	26	9	7

The use of mean mobility analysis has emerged as a prominent approach for identifying hacked nodes inside Wireless Sensor Networks (WSNs) [32]. This technique has an intrinsic capability to effectively differentiate abnormalities by capitalizing on the collective movement patterns. In contrast to conventional approaches that primarily depend on node-specific behaviour or communication patterns, mean mobility analysis adopts a comprehensive perspective by assessing the average mobility patterns shown by nodes within the network. This strategy leverages the observation that damaged nodes often display abnormal mobility patterns, such as unpredictable movements or abrupt changes in their paths, which are difficult to imitate successfully. The approach used in this study involves the collection and analysis of mobility data from various nodes [31]. By examining the average patterns derived from this data, the method effectively reduces the occurrence of false positives and false negatives. Consequently, the accuracy of detecting compromised nodes is significantly improved. Furthermore, the analysis of mean mobility exhibits a strong resistance to adversary efforts to conceal compromised nodes, so establishing it as a resilient and dependable approach for enhancing the security of Wireless Sensor Networks (WSNs) via the timely identification and isolation of possible threats. The outcomes are also analysed graphically in Figure 3.

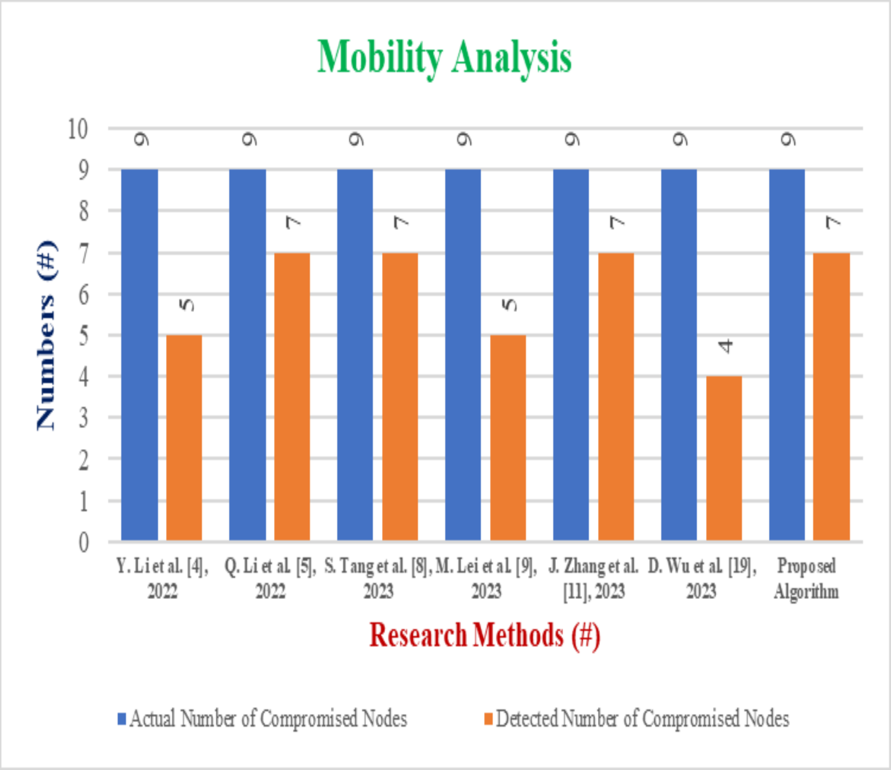

Fig. 3. Compromised Node Detection using Mobility Analysis

12. Packet Dropping Rate & Identification

The dropping of the data packets is one of the significant symptoms for compromised nodes. During the analysis of the simulated network, the proposed algorithm also identified the packet dropping rate for the entire network and number of nodes, where the packet dropping rate is higher than the network mean. The results are furnished here in Table 6.

Table 6
Packet Dropping Rate Analysis

Research Method	Network PDR	Lowest PDR	Highest PDR	Actual Number of Compromised Nodes	Number of Nodes with Higher than Network PDR
Y. Li *et al.,* [4]	12.48	12.42	12.54	9	6
Q. Li *et al.,* [5]	14.18	14.11	14.2	9	2
S. Tang *et al.,* [8]	11.36	11.31	11.39	9	6
M. Lei *et al.,* [9]	11.83	11.76	11.87	9	8
J. Zhang *et al.,* [11]	14.28	14.25	14.33	9	6
D. Wu *et al.,* [19]	11.14	11.1	11.21	9	1
Proposed Algorithm	14.42	14.4	14.45	9	8

A greater rate of packet dropping in a Wireless Sensor Network (WSN) might potentially be beneficial for the purpose of detecting hacked nodes, since it could significantly affect the behaviour of the network [33]. Nodes that have been compromised often display atypical behaviours, including the unlawful transmission or alteration of data. By deliberately increasing the rate of packet drops inside the network, these infected nodes are more prone to experiencing challenges in forwarding packets, resulting in noticeable disruptions in communication patterns [34]. The discovery of anomalous behaviour may be achieved by monitoring and evaluating the rates of packet loss across nodes, hence enabling the detection of nodes that exhibit deviations from the anticipated patterns. The use of a purposeful packet dropping technique improves the capacity to identify affected nodes, hence facilitating the early identification and mitigation of security breaches inside the Wireless Sensor [35] Network (WSN).The outcomes are also visualized here in Figure 4.

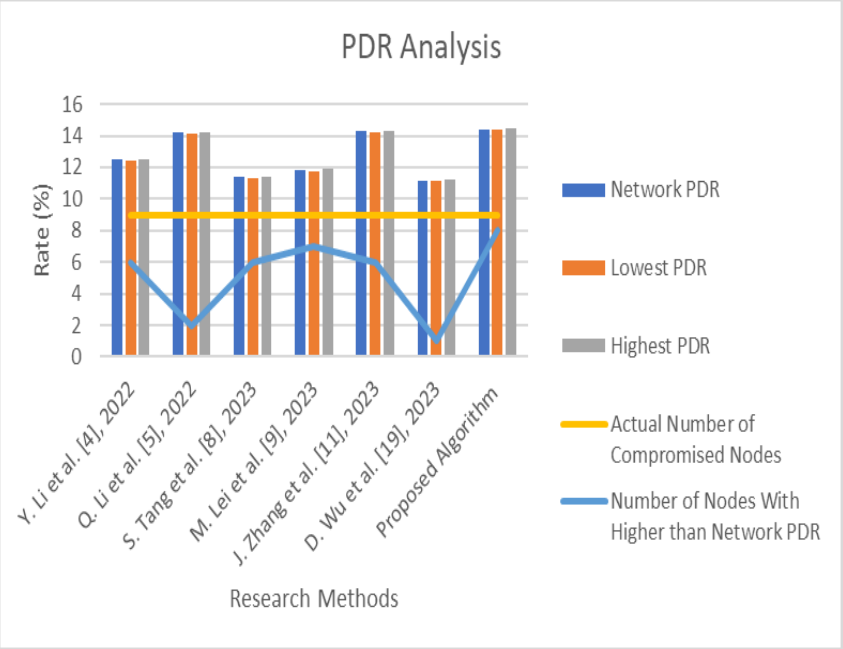

Fig. 4. Packet Dropping Rate Analysis

Naturally, the proposed method has performed better than the other existing methods. Hence, the proposed method detects the compromised nodes as follows in Table 7.

Table 7
Data Process Affinity Analysis

Research Method	Actual Number of Compromised Nodes	Detected Compromised Nodes (Energy Consumption)	Detected Compromised Nodes (Mobility)	Detected Compromised Nodes (PDR)	Detected Compromised Nodes (Final)
Y. Li *et al.,* [4]	9	4	5	6	5
Q. Li *et al.,* [5]	9	4	7	2	4
S. Tang *et al.,* [8]	9	4	7	6	4
M. Lei *et al.,* [9]	9	5	5	7	5
J. Zhang *et al.,* [11]	9	5	7	6	7
D. Wu *et al.,* [19]	9	5	4	1	4
Proposed Algorithm	9	8	7	8	8

The final outcome is also obtained from the simulation in Figure 5.

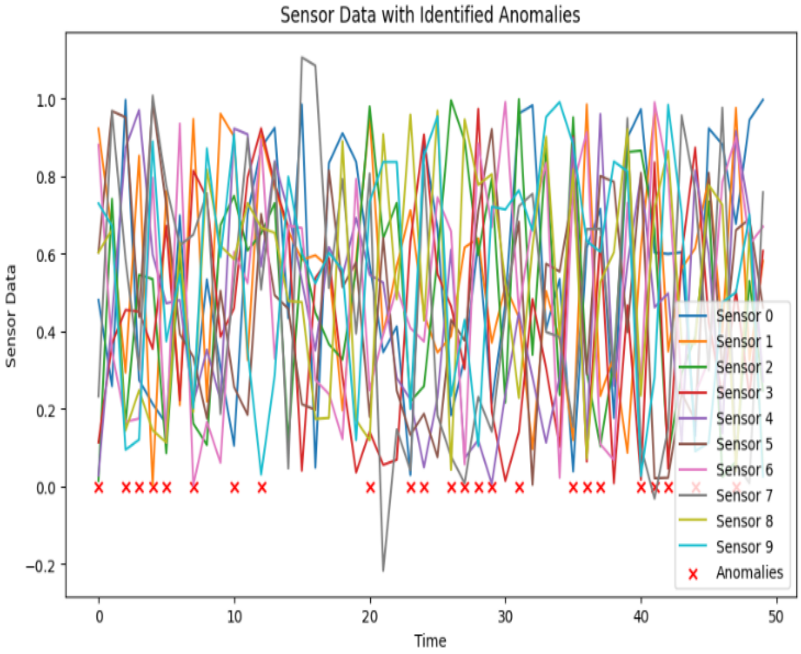

Fig. 5. Compromised Node Simulation

13. Data Process Availability Analysis

In order to build the cooperative cache formation during the simulation, this work deploys the data process affinity mechanism. The simulation results are furnished here in Table 8.

Table 8
Data Process Affinity Analysis

Research Method	Actual Number of Colocation Processes (Mean)	Detected Number of Colocation Processes (Mean)	Actual Number of Shared Data Items (Mean)	Detected Number of Shared Data Items (Mean)
Y. Li *et al.,* [4]	10	4	5	3
Q. Li *et al.,* [5]	10	7	5	5
S. Tang *et al.,* [8]	10	6	5	4
M. Lei *et al.,* [9]	10	6	5	5
J. Zhang *et al.,* [11]	10	7	5	5
D. Wu *et al.,* [19]	10	4	5	4
Proposed Algorithm	10	8	5	5

The investigation of process and data affinity has significant importance in the construction of a collaborative cache inside shared-memory parallel computing systems. The purpose of affinity analysis is to enhance cache usage by ensuring that frequently accessed data and its accompanying processes are collocated on the same cache lines or processors. The use of this technique effectively mitigates cache contention, eliminates the overhead associated with data transfer, and optimizes data locality, hence leading to enhanced overall performance and decreased memory latency. Affinity analysis is a technique that improves cache hit rates and decreases cache coherence cost by organizing similar processes and their associated data together in the cache. This approach results in more efficient exploitation of the cache and boosts parallelism. This strategy has special significance in multi-core systems since the presence of cache contention and data access latency may have a substantial influence on the performance of applications. The visualization of the obtained results is furnished here in Figure 6.

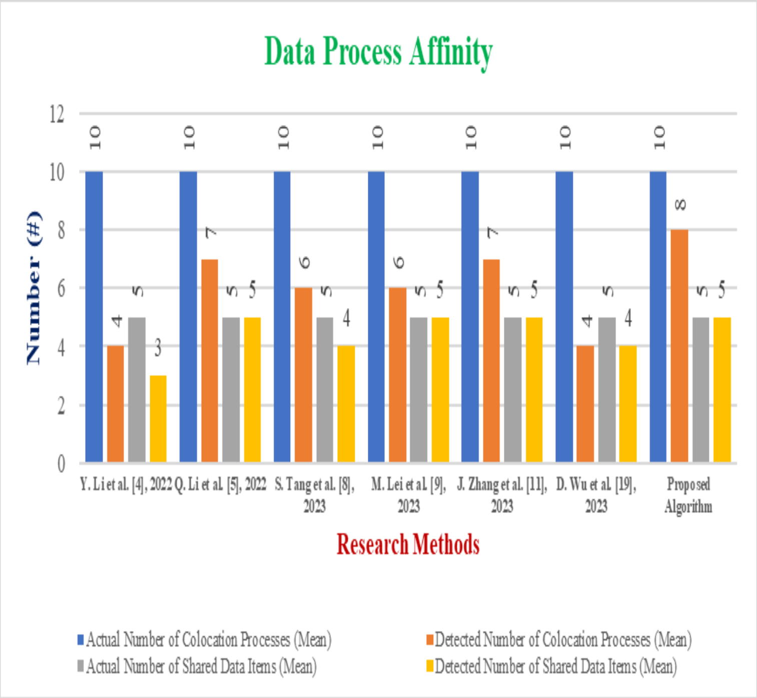

Fig. 6. Data Process Affinity Analysis

14. Cooperative Cache Formation

Finally, in order to avoid data loss during the node isolation process for the compromised nodes, cooperative caches are formed in Figure 7.

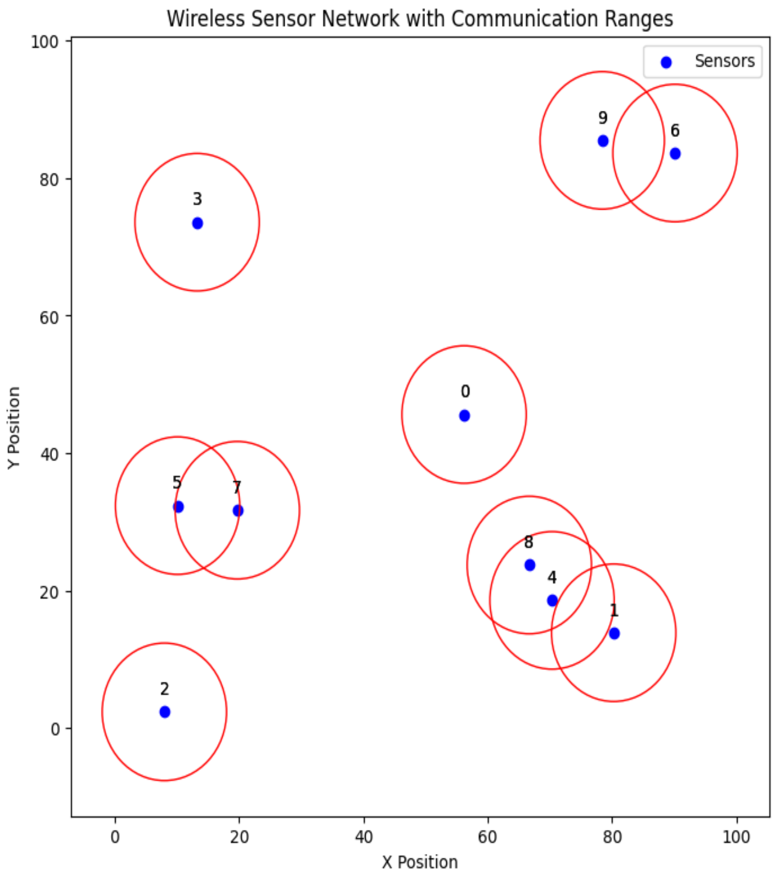

Fig. 7. Cooperative Cache Formation

The use of cooperative cache construction has significant advantages in the reduction of packet loss via enhanced data availability and alleviation of network congestion. Cooperative cache generation is an effective strategy for reducing the need of recurrent data transfers from a remote source inside a network. This approach involves the deliberate sharing of cached data across nodes, therefore mitigating the risks associated with network congestion and latency problems, such as packet loss. This methodology enhances the efficiency of data retrieval and enhances the probability of locally recovering cached material, hence mitigating network pressure and reducing the total rate of packet loss.

15. Cache Hit and Miss Analysis

The improvement of the proposed algorithm is not only detecting the compromised node, but rather building the cooperative cache to reduce the data loss. Hence, the cache hit and miss rations are analysed here in Table 9.

Table 9
Cache Hit / Miss Ratio Analysis

Research Method	Number of Compromised Nodes Detected	Cache Hit (%)	Cache Miss (%)
Y. Li *et al.,* [4]	5	52.09	47.91
Q. Li *et al.,* [5]	4	55.42	44.58
S. Tang *et al.,* [8]	4	50.45	49.55
M. Lei *et al.,* [9]	5	67.08	32.92
J. Zhang *et al.,* [11]	7	68.18	31.82
D. Wu *et al.,* [19]	4	52.29	47.71
Proposed Algorithm	8	88.75	11.25

Naturally the proposed system, due to the formation of the cooperative caches, has reduced the cache miss and eventually increased the cache hit ratios.

16. Comparative Analysis

The comparative analysis part plays a crucial role in this research, allowing for a thorough examination and assessment of the various methods, procedures, and techniques used in the topic under investigation. The objective of this part is to provide a thorough overview of the research environment by examining and comparing the strengths, limits, and distinctive characteristics of each technique. This analysis will shed light on the intricacies, patterns, and emerging knowledge in this field. By conducting a methodical investigation, the subsequent comparative analysis aims to extract significant insights, facilitating a nuanced knowledge of the benefits and limitations of different tactics. As a result, this study contributes to a more comprehensive grasp of the subject matter. Henceforth, the comparative analysis is furnished here in Table 10.

Table 10
Comparative Analysis

Research Method	Model Complexity	Cache Hit (%)	Cache Miss (%)	Best Outcome (EC)	Best Outcome (Mobility)	Best Outcome (PDR)
Y. Li *et al.,* [4]	O(n^2)	52.09	47.91			
Q. Li *et al.,* [5]	O(n^2)	55.42	44.58		√	
S. Tang *et al.,* [8]	O(n^2)	50.45	49.55		√	
M. Lei *et al.,* [9]	O(n^2)	67.08	32.92			√
J. Zhang *et al.,* [11]	O(n^2)	68.18	31.82		√	
D. Wu *et al.,* [19]	O(n^2)	52.29	47.71			
Proposed Algorithm	O(n)	88.75	11.25	√	√	√

The use of Characteristics Based Rule Engines has gained prominence as a sophisticated approach in the identification of compromised nodes inside Wireless Sensor Networks (WSNs), owing to its multifunctionality and high level of precision. The Characteristics Based Rule Engine employs a dynamic assortment of node-specific attributes and behaviour metrics, rather than relying on signatures or behavioural patterns. The engine has the capability to detect irregularities and potentially dangerous behaviours that may go unnoticed by static techniques. This approach has the capability to adjust and accommodate the evolution of attack strategies and emerging threats via the ongoing assessment of deviations from node characteristics, hence enhancing the precision of compromised node identification. The system's ability to tailor detection criteria for individual nodes enhances operational effectiveness and mitigates the occurrence of erroneous positive detections. This particular feature offers a robust and flexible approach for ensuring security in Wireless Sensor Networks (WSNs).

17. Discussion

The study introduces mean mobility analysis as a pivotal method for identifying compromised nodes in Wireless Sensor Networks (WSNs). Unlike conventional methodologies focusing on individual node behaviour, this approach evaluates the collective movement patterns within the network. By leveraging mobility data from multiple nodes, the method addresses false positives and negatives through the examination of average trends. Additionally, the research underscores the significance of packet loss as an indicator for compromised node identification, emphasizing the potential disruptions caused by hackers manipulating data or inducing packet forwarding difficulties.

However, the paper lacks explicit discussions on the system's robustness against sophisticated attackers and potential mimicry. Scalability concerns and the system's performance with an increasing number of nodes in a WSN are unexplored, and the absence of real-world testing raises uncertainties about adaptability to variable environmental conditions. To enhance real-world applicability and reliability, strategies should be devised to counteract potential mimicry by attackers, emphasizing advanced detection mechanisms. Scalability, examined through system performance with an expanding WSN, is crucial for practical deployment. Evaluating limitations in evasion tactics and scalability is essential for refining and optimizing the system.

The results of the proposed system showcase advancements in mitigating compromised nodes within WSNs. The Characteristics Based Rule Engine, coupled with deliberate packet dropping and mean mobility analysis, significantly reduced energy consumption, outperforming existing methods. The system exhibited a notable ability to detect compromised nodes with consistently lower false positives and negatives. Cooperative cache formation enhanced data availability and reduced packet loss, resulting in remarkably higher cache hit rates. The empirical evidence highlights the proposed approach's effectiveness in improving security and performance in WSNs, striking a balance between efficiency and simplicity.

18. Conclusion

In conclusion, this research addresses a crucial issue in WSN by proposing an innovative approach to detect compromised nodes and enhance network performance through cooperating caching. The study demonstrates the effectiveness of this strategy in bolstering network security, reducing latency, and alleviating congestion. By combining compromised node identification with cache optimization, malicious nodes are promptly isolated, preserving the WSN’s integrity. The results emphasize the significance of affinity analysis in cache design, enhancing data locality and process interactions for improved cache usage. The presented solution successfully tackles compromised node identification and performance degradation, offering a holistic approach for WSN security and efficiency. Future investigations could explore the scalability and flexibility of this methodology across diverse WSN scenarios and real-world deployments, providing valuable insights for further advancements in the field. This comprehensive solution contributes significantly to the understanding of WSN challenges and provides practical means to address them, paving the way for enhanced network reliability and security.

Acknowledgement
This research was not funded by any grant.

References

[1] Sun, Zhenfeng, and Mohammad Reza Nakhai. "Distributed learning-based cache replacement in collaborative edge networks." *IEEE Communications Letters* 25, no. 8 (2021): 2669-2672. https://doi.org/10.1109/LCOMM.2021.3081823

[2] Gurram, Girija Vani, Noorullah C. Shariff, and Rajkumar L. Biradar. "A secure energy aware meta-heuristic routing protocol (SEAMHR) for sustainable IoT-wireless sensor network (WSN)." *Theoretical Computer Science* 930 (2022): 63-76. https://doi.org/10.1016/j.tcs.2022.07.011

[3] Chen, Yu, Yong Liu, Jingya Zhao, and Qinghua Zhu. "Mobile edge cache strategy based on neural collaborative filtering." *IEEE Access* 8 (2020): 18475-18482. https://doi.org/10.1109/ACCESS.2020.2964711

[4] Li, Yijing, Shihong Hu, and Guanghui Li. "CVC: A collaborative video caching framework based on federated learning at the edge." *IEEE Transactions on Network and Service Management* 19, no. 2 (2021): 1399-1412. https://doi.org/10.1109/TNSM.2021.3135306

[5] Li, Qi, Amiya Nayak, Xiaoxiang Wang, Dongyu Wang, and F. Richard Yu. "A collaborative caching-transmission method for heterogeneous video services in cache-enabled terahertz heterogeneous networks." *IEEE Transactions on Vehicular Technology* 71, no. 3 (2022): 3187-3200. https://doi.org/10.1109/TVT.2022.3141335

[6] Furqan, Muhammad, Cheng Zhang, Wen Yan, Abdul Shahid, Muhammad Wasim, and Yongming Huang. "A collaborative hotspot caching design for 5G cellular network." *IEEE Access* 6 (2018): 38161-38170. https://doi.org/10.1109/ACCESS.2018.2852278

[7] Chiang, Yao, Chih-Ho Hsu, and Hung-Yu Wei. "Collaborative social-aware and QoE-driven video caching and adaptation in edge network." *IEEE Transactions on Multimedia* 23 (2020): 4311-4325. https://doi.org/10.1109/TMM.2020.3040532

[8] Tang, Shunpu, Ke He, Lunyuan Chen, Lisheng Fan, Xianfu Lei, and Rose Qingyang Hu. "Collaborative cache-aided relaying networks: Performance evaluation and system optimization." *IEEE Journal on Selected Areas in Communications* 41, no. 3 (2023): 706-719. https://doi.org/10.1109/JSAC.2023.3234693

[9] Lei, Meng, Qiang Li, Xiaohu Ge, and Ashish Pandharipande. "Partially collaborative edge caching based on federated deep reinforcement learning." *IEEE transactions on vehicular technology* 72, no. 1 (2022): 1389-1394. https://doi.org/10.1109/TVT.2022.3206876

[10] Mehrabi, Abbas, Matti Siekkinen, and Antti Ylä-Jaaski. "QoE-traffic optimization through collaborative edge caching in adaptive mobile video streaming." *IEEE Access* 6 (2018): 52261-52276. https://doi.org/10.1109/ACCESS.2018.2870855

[11] Zhang, Jing, Yuan Shen, Yu Wang, Xudong Zhang, and Jian Wang. "Dual-timescale resource allocation for collaborative service caching and computation offloading in IoT systems." *IEEE Transactions on Industrial Informatics* 19, no. 2 (2022): 1735-1746. https://doi.org/10.1109/TII.2022.3186039

[12] Yang, Taoyu, Zengjie Tan, Yuanyuan Xu, and Shuwen Cai. "Collaborative edge caching and transcoding for 360° video streaming based on deep reinforcement learning." *IEEE Internet of Things Journal* 9, no. 24 (2022): 25551-25564. https://doi.org/10.1109/JIOT.2022.3197798

[13] Chen, Lixing, Linqi Song, Jacob Chakareski, and Jie Xu. "Collaborative content placement among wireless edge caching stations with time-to-live cache." *IEEE transactions on multimedia* 22, no. 2 (2019): 432-444. https://doi.org/10.1109/TMM.2019.2929004

[14] Li, Tianyou, Dapeng Li, Youyun Xu, Xiaoming Wang, and Guanglin Zhang. "Temporal-spatial collaborative mobile edge caching with user satisfaction awareness." *IEEE Transactions on Network Science and Engineering* 9, no. 5 (2022): 3643-3658. https://doi.org/10.1109/TNSE.2022.3188658

[15] Rui, Lanlan, Dai Song, Shiyou Chen, Yingtai Yang, Yang Yang, and Zhipeng Gao. "Content collaborative caching strategy in the edge maintenance of communication network: A joint download delay and energy consumption method." *IEEE Transactions on Parallel and Distributed Systems* 33, no. 12 (2022): 4148-4163. https://doi.org/10.1109/TPDS.2022.3179271

[16] Liu, Junyan, Dapeng Li, and Youyun Xu. "Collaborative online edge caching with bayesian clustering in wireless networks." *IEEE Internet of Things Journal* 7, no. 2 (2019): 1548-1560. https://doi.org/10.1109/JIOT.2019.2956554

[17] Chen, Shiyou, Lanlan Rui, Zhipeng Gao, Wenjing Li, and Xuesong Qiu. "Cache-assisted collaborative task offloading and resource allocation strategy: A metareinforcement learning approach." *IEEE Internet of Things Journal* 9, no. 20 (2022): 19823-19842. https://doi.org/10.1109/JIOT.2022.3168885

[18] Ugwuanyi, Emeka E., Muddesar Iqbal, and Tasos Dagiuklas. "A novel predictive-collaborative-replacement (PCR) intelligent caching scheme for multi-access edge computing." *IEEE Access* 9 (2021): 37103-37115. https://doi.org/10.1109/ACCESS.2021.3058769

[19] Wu, Dapeng, Jifang Li, Peng He, Yaping Cui, and Ruyan Wang. "Social-aware graph-based collaborative caching in edge-user networks." *IEEE Transactions on Vehicular Technology* (2023). https://doi.org/10.1109/TVT.2023.3241959

[20] Khanal, Subina, Kyi Thar, and Eui-Nam Huh. "Dcol: Distributed collaborative learning for proactive content caching at edge networks." *IEEE Access* 9 (2021): 73495-73505. https://doi.org/10.1109/ACCESS.2021.3080512

[21] Wang, Liumeng, and Sheng Zhou. "Fractional dynamic caching: A collaborative design of storage and backhaul." *IEEE Transactions on Vehicular Technology* 69, no. 4 (2020): 4194-4206. https://doi.org/10.1109/TVT.2020.2968487

[22] Feng, Hao, Songtao Guo, Li Yang, and Yuanyuan Yang. "Collaborative data caching and computation offloading for multi-service mobile edge computing." *IEEE Transactions on Vehicular Technology* 70, no. 9 (2021): 9408-9422. https://doi.org/10.1109/TVT.2021.3099303

[23] Wang, Shupeng, Handi Chen, and Yongjian Wang. "Collaborative caching for energy optimization in content-centric Internet of Things." *IEEE Transactions on Computational Social Systems* 9, no. 1 (2021): 230-238. https://doi.org/10.1109/TCSS.2021.3087197

[24] Zhao, Xiaoyan, Peiyan Yuan, and Shaojie Tang. "Collaborative edge caching in context-aware device-to-device networks." *IEEE Transactions on Vehicular Technology* 67, no. 10 (2018): 9583-9596. https://doi.org/10.1109/TVT.2018.2858254

[25] Xu, Xianzhe, Meixia Tao, and Cong Shen. "Collaborative multi-agent multi-armed bandit learning for small-cell caching." *IEEE Transactions on Wireless Communications* 19, no. 4 (2020): 2570-2585. https://doi.org/10.1109/TWC.2020.2966599

[26] Almomani, Iman, Bassam Al-Kasasbeh, and Mousa Al-Akhras. "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks." *Journal of Sensors* 2016 (2016). https://doi.org/10.1155/2016/4731953

[27] Singh, Abhilash, J. Amutha, Jaiprakash Nagar, Sandeep Sharma, and Cheng-Chi Lee. "Lt-fs-id: Log-transformed feature learning and feature-scaling-based machine learning algorithms to predict the k-barriers for intrusion detection using wireless sensor network." *Sensors* 22, no. 3 (2022): 1070. https://doi.org/10.3390/s22031070

[28] Singh, Abhilash, Vaibhav Kotiyal, Sandeep Sharma, Jaiprakash Nagar, and Cheng-Chi Lee. "A machine learning approach to predict the average localization error with applications to wireless sensor networks." *IEEE Access* 8 (2020): 208253-208263. https://doi.org/10.1109/ACCESS.2020.3038645

[29] Rathish, C. R., and A. Rajaram. "Efficient path reassessment based on node probability in wireless sensor network." *International Journal of Control Theory and Applications* 34, no. 2016 (2016): 817-832.

[30] Roberts, Michaelraj Kingston, and Jayapratha Thangavel. "An optimized ticket manager based energy-aware multipath routing protocol design for IoT based wireless sensor networks." *Concurrency and Computation: Practice and Experience* 34, no. 28 (2022): e7398. https://doi.org/10.1002/cpe.7398

[31] Yagoub, Sami Abdelrahman Musa, Gregorius Eldwin Pradipta, and Ebrahim Mohammed Yahya. "Prediction of bubble point pressure for Sudan crude oil using Artificial Neural Network (ANN) technique." *Progress in Energy and Environment* (2021): 31-39.

[32] Ashok Babu, P., L. Kavisankar, Jasmine Xavier, V. Senthilkumar, Gokul Kumar, T. Kavitha, A. Rajendran, G. Harikrishnan, A. Rajaram, and Amsalu Gosu Adigo. "Selfish node detection for effective data transmission using modified incentive sorted pathway selection in wireless sensor networks." *Wireless Communications and Mobile Computing* 2022 (2022). https://doi.org/10.1155/2022/9359135

[33] Chiranjeevi, Phaneendra, and A. Rajaram. "A lightweight deep learning model based recommender system by sentiment analysis." *Journal of Intelligent & Fuzzy Systems* Preprint (2023): 1-14. https://doi.org/10.3233/JIFS-223871

[34] Kingston Roberts, Michaelraj, and Jayapratha Thangavel. "An improved optimal energy aware data availability approach for secure clustering and routing in wireless sensor networks." *Transactions on Emerging Telecommunications Technologies* 34, no. 3 (2023): e4711. https://doi.org/10.1002/ett.4711

[35] Karim, Abdul Razif Abdul, and Roslina Mohammad. "Meta-study of sensitivity analysis in solar renewable energy application." *Progress in Energy and Environment* (2023): 14-25. https://doi.org/10.37934/progee.23.1.1425

[36] Wang, Dan, Terh Jing Khoo, and Zhangfei Kan. "Exploring the application of digital data management approach for facility management in Shanghai’s high-rise buildings." *Progress in Energy and Environment* (2020): 1-15.

[37] Masrom, Maslin, Mohd Nazry Ali, Wahyunah Ghani, and Amirul Haiman Abdul Rahman. "The ICT implementation in the TVET teaching and learning environment during the COVID-19 pandemic." *International Journal of Advanced Research in Future Ready Learning and Education* 28, no. 1 (2022): 43-49.