IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 2 March 2024, accepted 7 March 2024, date of publication 18 March 2024, date of current version 22 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3377144

RESEARCH ARTICLE

Design and Evaluation of Memory Efficient Data Structure Scheme for Energy Drainage Attacks in Wireless Sensor Networks

DAVID SAMUEL BHATTI[1], SHAHZAD SALEEM[2,3], ZULFIQAR ALI[4], TAE-JIN PARK[5], BEOMKYU SUH[6], ALI KAMRAN[7], WILLIAM J. BUCHANAN[8], AND KI-IL KIM[6]

[1]Faculty of Information Technology, University of Central Punjab, Lahore 54000, Pakistan
[2]Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia
[3]School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad 44000, Pakistan
[4]Department of Computer Science, National University of Technology, Islamabad 44000, Pakistan
[5]Nuclear System Integrity Sensing and Diagnosis Division, Korea Atomic Energy Research Institute (KAERI), Daejeon 34057, Republic of Korea
[6]Department of Computer Science and Engineering, Chungnam National University, Daejeon 34134, Republic of Korea
[7]Department of Computer Science, COMSATS University Islamabad, Islamabad 45550, Pakistan
[8]School of Computing, Engineering and the Built Environment, Edinburgh Napier University, EH11 4BN Edinburgh, U.K.

Corresponding author: Ki-Il Kim (kikim@cnu.ac.kr)

This work was supported in part by the National Research Foundation of Korea (NRF) Grant funded by Korean Government, Ministry of Science and ICT (MSIT), under Grant RS-2022-00144000 and Grant RS-2022-00165225; and in part by the Institute for Information and Communications Technology Planning and Evaluation (IITP) Grant funded by Korean Government, MSIT, Convergence Security Core Talent Training Business, Chungnam National University, under Grant 2022-0-01200.

ABSTRACT Wireless Sensor Networks (WSN) are deployed on a large scale and require protection from malicious energy drainage attacks, particularly those directed at the routing layer. The complexity increases during critical operations like cluster head selection where detection of such attacks is challenging. The dependency of WSN on batteries elevates the concern posed by these threats, making detection and isolation crucial, especially within the framework of energy-efficient clustering protocols such as Low Energy Adaptive Clustering Hierarchy (LEACH). Various approaches have been proposed in prior research to deal with such attacks. However, the use of memory-efficient data structures has yet to be effectively addressed. In this article, considering the limitations of WSN, we utilize memory-efficient data structures named Bloom filters, count-min (CM) sketch, and cellular automata (CA) to address abnormal energy drainage. A CA-based trust model is used to choose the legitimate node as the cluster head. CM sketch is used to control the frequency of a node selected as a cluster head, achieving fairness in the cluster head selection process, and Bloom filters maintain the record of malicious nodes blocked from participating in the communication or cluster head selection process. CA and trust functions collectively keep a record of neighbors' energy and their trust in the network. Grayhole, blackhole, and scheduling attacks are three well-known threats that lead to abnormal energy drainage in legitimate nodes. The proposed solution effectively detects and addresses abnormal energy drainage in WSN. Its impact is simulated and observed using ns2 IEEE 802.15.4 medium access control (MAC) and LEACH clustering protocols, specifically in the context of the mentioned attacks. The effectiveness of the proposed model was rigorously analysed, and it was observed that it reduces the energy consumption of WSN by approximately 16.66%, 48.33%, and 43.33% in the cases of grayhole, blackhole, and scheduling attacks, respectively. In terms of space/time complexity, its growth is linear O(n). The proposed solution also consumes 0.08-0.10 J more energy compared to the original LEACH as a cost of the solution, which is not more than 2% of the total initial energy. The trade-off of implementing heightened security is worthwhile, as the proposed approach outperforms the original LEACH and related methods, effectively mitigating abnormal energy drainage in WSN and extending network lifetime, especially in challenging environments with persistent battery recharging challenges.

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

INDEX TERMS WSN, LEACH, cellular automata, CM sketch, Bloom filter, energy drainage, blackhole, grayhole, scheduling attacks, trust model.

I. INTRODUCTION

WSN have transformed communication, finding applications in challenging terrains like defence, health, and industry. These networks exhibit self-healing, self-organization, scalability, and fault tolerance, making them highly adaptable and resilient. In resource-constrained settings, where energy efficiency is crucial due to battery dependency, researchers are diligently working on solutions to maximise the operational longevity of WSN. Clustering is a key organizational structure in WSN where nodes are grouped into clusters and one node within each cluster, often referred to as the cluster head (CH), coordinates communication. The concept of cluster heads alleviates energy consumption in WSN architectures through data aggregation, compression, and transmission to the central sink, as shown in Figure 1. By reducing direct communication between individual sensor nodes and the sink, energy efficiency is improved. Hierarchical routing, such as the LEACH protocol, aims to balance energy consumption among cluster heads, prolonging the overall network lifespan and maintaining consistent performance levels [1]. Due to their broadcast nature, WSN are prone to multiple attacks; among them, routing layer attacks like node misbehaviour, data packet manipulation, and energy drainage are difficult to mitigate. Energy drainage attacks in WSN refer to malicious activities that target and deplete the energy resources of sensor nodes in the network. A few common types of energy drainage attacks are grayhole, blackhole, and scheduling. The objective of the article is to introduce space-time efficient data structures that can enhance the security of WSN, mitigating energy drainage with minimum overheads. Unfortunately, cryptographic techniques can address privacy and integrity concerns, but it is hard for them to thwart such attacks that are mentioned here. These attacks are designed to accelerate the energy consumption of individual nodes, with the ultimate goal of compromising the overall functionality and lifespan of the WSN. Addressing these attacks is crucial due to their potential impact on network performance and reliability in battery dependent scenarios. Numerous strategies have been put forth in previous research to address these attacks. Nevertheless, the effective integration of memory-efficient data structures remains an aspect that requires further attention. This study proposes a trust-based methodology using space-efficient data structures, Bloom filters, CM sketch, and cellular automata to identify and quarantine adversaries involved in unauthorized battery depletion of legitimate nodes in the LEACH protocol routing process, aiming to enhance the resilience of WSN against energy drainage attacks. A Bloom filter is a space-efficient probabilistic data structure used to test if an element is a member of a set, providing false positives but not false negatives. The Count-Min Sketch is a probabilistic data structure used for approximate counting events in data streams. cellular automata are discrete computational models consisting of a grid of cells with finite states evolving over time steps based on rules. Grayhole, blackhole, and scheduling attacks represent three commonly acknowledged threats that result in abnormal energy drainage in legitimate nodes. It is clearly stated that the impact of the proposed approach is specifically simulated and observed in the context of these attacks. The proposed model significantly reduces WSN energy consumption during the mentioned attacks, with a slight increase in energy usage as an implementation cost. Despite this trade-off, the enhanced security justifies deploying the model, outperforming the original LEACH in mitigating abnormal energy drainage.

Rest of the manuscript is formulated as follows: Section II-Contributions, III-WSN challenges, IV-LEACH, V-related work and its conclusion, VI-proposed solution,VII-result analysis and discussion, VIII-Limitations of the proposed solution, IX-conclusion and the future work.

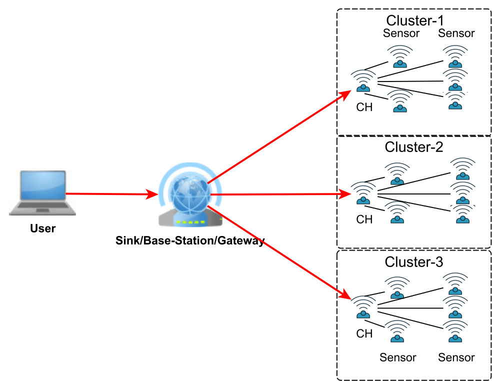


FIGURE 1. WSN Architecture.

II. CONTRIBUTIONS OF THE PROPOSED APPROACH

1) The proposed approach addressed one of the critical concerns in WSN, which is abnormal energy drainage, which, if not dealt with carefully, can cause the network to die earlier.
2) It makes use of space-time efficient probabilistic data structures that fit the resource limitations of WSN nodes.
3) The proposed solution significantly increases the network life by approximately 100 rounds in the case of grayholes, 260 rounds in the case of scheduling, and 280 rounds in the case of blackhole attacks.
4) The proposed solution costs a minute of energy, which is less than 2% of the total assigned energy, which was 6 J per node.

III. WSN CHALLENGES AND SECURITY ISSUES

WSN face numerous challenges in processing, storage, energy, and transmission range, including energy efficiency, network longevity, quality of service, adaptability to hazardous environments, fault tolerance, hardware-software complexity, and security issues. The routing layer is crucial for protecting WSN from energy drainage attacks, which reduce their energy capacity and cause them to die before their actual lifespan. Abnormal battery depletion attacks, such as vampire attacks and cartel attacks, contribute to energy waste and network degradation. Abnormal battery depletion attacks, such as grayhole attacks involving the injection of corrupted routing packets (Vampire attacks) and blackhole attacks targeting source routing protocols (Carousel attacks). Similarly, scheduling attacks that manipulate routing packets to select longer routes contribute to energy waste and network degradation. Denial of service, denial of sleep and wormholes maliciously utilising genuine information for continuous transmission in an unauthorized direction further increase the risk of energy depletion in WSN nodes [2], [3]. These challenges highlight the need to implement robust security measures to safeguard the resilience of WSN.

IV. LEACH

WSN routing protocols include attribute-based, data-centric, geographical, hierarchical, and multipath protocols. LEACH, Power-Efficient GAthering in Sensor Information Systems (PEGASIS), and Threshold-sensitive Energy Efficient sensor Network protocol (TEEN) are popular hierarchical protocols that maintain energy efficiency and extend network lifespan while preserving connectivity [4]. This study focuses on the vulnerability of WSN routing, especially in relation to energy drainage attacks. LEACH is a cross-layer Time Division Multiple Access (TDMA) based MAC protocol. used for longer network lifetimes. It optimizes power dissipation by evenly distributing the energy load among network nodes. The key characteristics of this protocol include: i) localized control and coordination for forming and operating the cluster; ii) rotational and random selection of cluster head and its cluster based on residual energy; iii) adaptive membership with an evenly distributed distribution of energy throughout the sensors; iv) TDMA-based communication of sensors with the cluster head and compression at the cluster head. The LEACH protocol consists of four steps: advertisement, cluster set-up, schedule creation, and data transmission. Each round commences with a set-up phase, followed by a steady-state phase, and concludes with the final data transfer phase. During the advertisement phase, each node decides to become a cluster head, broadcasting an advertisement message to all other nodes using Carrier Sense Multiple Access (CSMA) MAC protocol. In the cluster set-up phase, each node reports to the cluster head, creating a TDMA schedule for data transmission. The data is then sent to the base station. For simplicity, a simple flow of the set-up phase of LEACH has been shown in Figure 2.

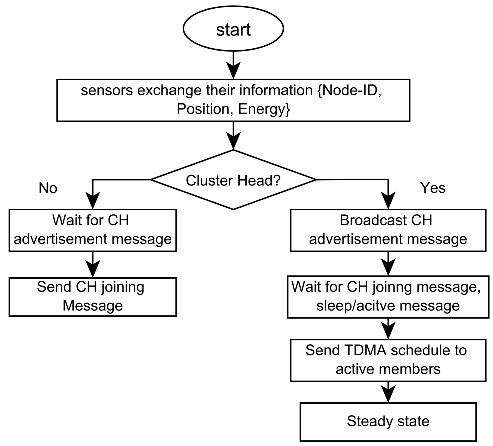


FIGURE 2. LEACH setup phase.

A. LEACH: LIMITATIONS

LEACH has some limitations, like the assumption that all the nodes have the same energy values in a running network, which is not possible for networks working in real-time.

B. LEACH: VULNERABILITY

LEACH is a hierarchical cluster-based protocol that relies on the cluster head for routing and data aggregation, making it vulnerable to routing-based attacks like blackholes, grayholes, and wormholes [5]. Attackers exploit the stochastic cluster head selection phase, which depends on the node energy value and the probability of being a cluster head. An adversary can easily enter LEACH-based WSN by impersonating node IDs or using fake IDs to deceive cluster head selection criteria. A trust-based energy drainage attack detection and prevention scheme is proposed using CM sketch and Bloom filter probabilistic data structures, along with cellular automata. The scheme monitors neighbouring nodes' energy levels, identifies those under attack, and triggers automated state changes upon reaching a threshold. Trust values generated through cellular automata prevent malicious cluster head selection, while the CM sketch ensures fairness in cluster head selection.

V. RELATED WORK

This section explores cluster head selection, focusing on technological frameworks for secure and reliable processes. It emphasizes the importance of this topic and highlights ongoing research in WSN security.

A. TRUST BASED

Since behavioural attacks cannot be addressed by cryptographic approaches, these are expensive and not sufficient to thwart them. These attacks can be easily mitigated with the help of trust-based techniques. Baradaran and Fahimeh [6] introduced NEECH (new energy efficient cluster head protocol) for cluster head selection in WSN. NEECH leverages a synergy of gravity center and mass center principles to identify prospective cluster heads, and it incorporates a genetic algorithm to optimize the selection process, aiming to enhance the overall network lifetime. It utilizes three parameters: energy, distance, and density of nodes. Saravanan et al. [7] proposed "Optimal Cluster_Trust Asymmetric Key Management Protocol (OptCH_TAKMP)" that aims to enhance security and energy efficiency in Mobile Ad Hoc Networks (MANETs) by combining a secure routing mechanism and efficient cluster head selection. This protocol employs Particle Swarm Optimization (PSO) to choose cluster heads and detect malicious nodes, with a focus on building trust among connected nodes. It introduces two specific nodes, the Calculator Key (CK) and the Distribution Key (DK), responsible for generating and sharing secret keys using asymmetric key cryptography. This approach ensures secure communication while maintaining an energy-efficient cluster head selection process. "Trust-based Hybrid Cooperative Routing Protocol for Low Power Lossy Networks (THC-RPL)" to detect malicious Sybil nodes in an RPL-based IoT network is proposed by Arshad et al. [8]. The authors used a combination of trust metrics and secure parent selection mechanisms to identify and avoid malicious nodes. The protocol is designed to be lightweight and scalable, making it suitable for resource-constrained IoT networks. Gurumoorthy et al. [9] proposed a trust-aware, energy-efficient cluster head selection procedure for WSN based on factors like distance, energy, security (risk probability), latency, direct and indirect trust, and Received Signal Strength Indicator (RSSI). The authors used an enhanced Deep Convolutional Neural Network (DCNN) that predicts energy levels to assist in cluster head selection. Narayan and Daniel [10] proposed trust-based clustering and cluster head selection processes whose purpose was to enhance the residual energy and lifetime of the network. So, a node with the maximum residual energy and the minimum distance from the base station becomes a cluster head. The cluster head selection process is completed in two steps: in the first step, a threshold is calculated, and in the second, accurate data is acquired using the trust function from data diffusion. The work showed improvements in lifetime and network stability relative to present clustering techniques in heterogeneous scenarios. Prathapchandran and Janani [11] introduced a protocol designed for IoT-based networks to tackle the same issue. Its protocol is based on logistic regression to calculate the trust score for each node based on their behavior and interactions with other nodes in the network. The trust scores are then used to identify and isolate misbehaving nodes that exhibit malicious behavior or anomalies in RPL networks. Ilyas et al. [12] proposed a trusted-based secure routing protocol for IoT-based WSN that use RPL. The nodes build their trust relationship on the basis of their secure and reliable communication, which is used to guide the selection of routing paths, with more trusted nodes being given priority in the routing process. Moreover, they also proposed energy-efficient data aggregation, which reduces the amount of data transmission and saves energy.

B. AUTOMATA BASED

Reyes et al. [13] introduced an energy-aware cellular automata-based clustering algorithm for routing purposes in WSN. The authors used residual energy, sleep schedule, and the number of active neighbors in the formation of a cluster. In their study, the different behaviors of the networks are simulated with different sets of rules and combined with the A-star algorithm, which exhibits a reduction in energy consumption and increases the life of the network. Khot and Naik [14] proposed a cellular automata-based secure routing algorithm. Their proposed routing algorithm was based on the Particle-based Spider Monkey Optimization algorithm, which was a combination of particle swarm and spider monkey optimization algorithms, so that an optimum route could be selected. The route selection is based on network parameters such as energy, trust, consistency factor, and delay. Doostali and Syed Morteza [15] adopted the clustering technique to reduce energy consumption and increase network performance. Their clustering technique was based on learning automata and sleeping schedules. The parametric criteria included network density, the distance between a node and its nearest neighbor, and the count of nodes situated along the axis connecting the source and the destination. The proposed technique provides scalability, reduced power consumption, and enhanced network life.

C. RESIDUAL ENERGY, DISTANCE, TRANSMISSION RANGE

Aydin et al. [16] proposed a mobile sink solution that goes to every cluster head for data collection; this method mitigates the chances of node isolation. Both types of methods require significant energy consumption. This is the reason that new cluster head formation solutions have been researched for the last couple of years based on residual energy, distance, transmission range, etc. Amutha et al. [17] also presented a simple cluster head selection based on the residual energy and the distance of the cluster head from the nodes. Al-Baz and El-Sayed [18] employ a hybrid approach, utilizing both the RSSI and the distance between nodes, to discern the optimal node for cluster head selection in LEACH-based networks. The proposed algorithm considers the remaining energy of nodes in the network to ensure a fair selection of cluster heads. The new design improves the energy efficiency and lifetime of WSN by selecting the most appropriate cluster head. In mobile scenarios, the challenge of cluster head selection is effectively tackled by Qi et al. [19] through their algorithm, named the "robust, energy-efficient weighted clustering algorithm." This approach employs residual energy and group mobility as key factors for selecting cluster heads. The proposed algorithm incorporates strategies such as imposing a minimum repetition requirement for nodes to become cluster heads, implementing a globally distributed fault detection mechanism, and utilizing a mobility-dependent weight model alongside residual energy considerations. These enhancements collectively contribute to bolstering the reliability of the network. Dongare and Mangrulkar [20] proposed a cluster head selection technique that provides defence against grayhole and blackhole attacks in multi-hop WSN. The technique is based on the LEACH protocol. The cluster head is selected from the nodes that are already compromised but have more residual energy than the non-compromised nodes. The author's reason for choosing high-energy nodes as cluster heads is to maximize the network's life. It is an efficient technique in terms of throughput, packet loss rate, and end-end delay. Gong et al. [21] proposed a resource-conserving routing protocol in WSN called ''energy blocking'' to protect against energy drainage attacks. The protocol incorporates a preventive measure by blocking suspected nodes, aiming to thwart potential energy drainage attacks. This is achieved through a distributed detection algorithm that relies on monitoring data transmission rates. The algorithm selects paths considering the energy levels of nodes and the risk of energy-draining attacks using an analytic hierarchy process. The paper highlights the critical role of cluster head selection in WSN, emphasizing its susceptibility to cross-layer attacks, particularly those targeting energy drainage by exploiting the vulnerability associated with residual energy.

D. OTHERS

Chuhang Wang's ''A Distributed Particle-Swarm-Optimization-Based Fuzzy Clustering Protocol for Wireless Sensor Networks'' named DPFCP [22] employs the ''Mamdani fuzzy logic system'' and the ''Particle Swarm Optimization'' algorithm for cluster head selection, considering factors like residual energy, node degree, distance to base station, and centroid distance for distributed decision-making. The study [23] proposes a Multi-Attribute Decision-Making (MADM) method for cluster head selection, considering multiple attributes simultaneously to address conflicting factors like energy consumption, connectivity, coverage, load balance, base station distance, and neighbor distance, to select the best alternatives. Wu et al. [24] proposed a LEACH-based cluster head selection protocol based on four parameters: cluster distance, sink distance, overall energy consumption, and balance towards cluster head selection. Their protocol outperformed existing multi-objective cluster head selection techniques and enhanced network diversity, convergence, and search.

Summarized and comparative view of existing approaches for mitigating energy drainage in wireless networks is given in Table 1.

E. CONCLUSION FROM THE RELATED WORK

Existing literature on secure cluster head selection in wireless sensor networks has overlooked the crucial aspect of space and storage limitations during the cluster head selection process. Addressing this gap, our research introduces an innovative approach that prioritizes the mitigation of abnormal energy drainage by utilizing space efficient data structures like Bloom filters, cuckoo filters, and cellular automata. This not only prevents inadvertent cluster head selection but also incorporates trust metrics and behavioral evaluations of nominated nodes. Our results demonstrate a notable improvement in both security and efficiency, emphasizing the importance of considering space constraints in mitigating energy drainage attacks in WSN. This contribution represents a significant advancement in building a robust and resource-aware cluster head selection framework for WSN security.

VI. PROPOSED SOLUTION AND ITS KEY COMPONENTS

This section presents a solution to detect abnormal energy drainage from a node and isolate the malicious cluster head that causes this issue. The proposed solution operates under the assumption that nodes are distributed randomly, forming Voronoi regions under the governance of cluster heads. Regular grid patterns are typically used for simulating tessellation in wireless sensor networks, as shown in Figure 3a, but this is impractical in real systems. To model the cellular automata, the spatial or geographical area of the WSN is considered the Voronoi region Figure 3b. The Voronoi spatial model is used to extend and model the regular cellular automata, considering the region as convex cells with different shapes and sizes. The model is essentially a collocation, apposition, or juxtaposition of area divided into smaller Voronoi regions around each object, such as seeds, sites, or generators. In this case, cluster heads form a Voronoi cell containing points closer to the cluster head than any other. A mathematical expression of this definition can be given as Equation 1.

$$\begin{aligned} V(p(x_i, y_i)) = \{p | d((p(x, y), p(x_i, y_i)) \\ \leq d((p(x, y), p(x_j, y_j)), \quad j \neq i, \ j = 1 \ldots n\} \end{aligned} \tag{1}$$

In Equation 1, $V(p(x_i, y_i))$ is the Voronoi region that depicts the cell of point $p(x_i, y_i)$, which is a model of CH_i, a cluster head in our case whose coverage consists of all those points (which are the sensor nodes in this case) that are closer to this cluster head than any other. *The purpose of making all that discussion due to the distance (between sensor node (member) and cluster head (claimant)) being used as one of the parameters in the selection of cluster head*. For two points ($p(x_i, y_i)$ *and* $p(x_j, y_j)$), this distance is Euclidean, which can be computed with the help of the following Equation 2.

$$d((p(x_i, y_i), p(x_j, y_j)) = \sqrt{(x_i - y_i)^2 + p(x_j - y_j)^2} \tag{2}$$

This distance has an inherent relationship with the coverage area of the sensor nodes (cluster heads and members). If $d((p(x_i, y_i), p(x_j, y_j))$ represents the distance between cluster head and a sensor node (S_i) that can be given as Equation 3

$$.d(CH, S_i) \leq R_h \tag{3}$$

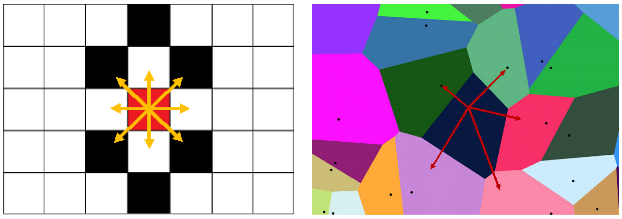
where R_h is the radius of communication coverage range of the cluster head. It implies that for complete radio coverage, there must be at least one sensing node whose distance to its

TABLE 1. Comparison with existing approaches.

Article	Approach based on	Outcome	Comments	Space-efficient data structures? 1	2	3	4
Baradaran and Fahimeh [6]	Trust, Genetic Algorithm	Best cluster head selection	improves network life time	×	×	×	×
Saravanan et al. [7]	Trust, PSO Algorithm, Cryptography	malicious node detection, cluster head selection, secure communication	ensures secure communication maintaining energy efficient cluster head selection	×	×	×	×
Arshad et al. [8]	Trust, secure parent selection	avoid malicious nodes	lightweight, scalable protocol, suitable for low resource IoT devices	×	×	×	×
Sasi Kumar et al. [9]	Trust, DCNN, based on direct and direct trust, energy and distance	energy efficient cluster head selection	RSSI level assist in energy efficient cluster head selection, RSSI values easily available at high layers of TCP/IP even	×	×	×	×
Narayan and Daniel [10]	Trust, residual energy, distance	cluster head with maximum residual energy and minimum distance is selected	improves residual energy and network life-time	×	×	×	×
Prathapchandran et al. [11]	Trust, similar to [10] but uses Logistic Regression	calculates trust-score using logistic regression	identifies and isolates misbehaving nodes from IoT network that is important for its sustainability	×	×	×	×
Ilyas et al. [12]	Trust, secure routing bases on trust	trust calculation on the basis of secure and reliable communication, energy efficient data aggregation	reduces amount of data transmission and energy consumption	×	×	×	×
Reyes et al. [13]	Cellular automata, A-star algorithm, residual energy, sleep schedule, active neighbors	energy efficient cluster formation	increases network life time	✓	×	×	×
Pradeep et al. [14]	cellular automata, Particle Swarm Spider Monkey Optimisation algorithms	optimised routing based on trust, energy, and delay	optimised secure routing is needed in resource constraint scenarios	✓	×	×	×
Syed Morteza [15]	Learning automata, sleeping schedule, network density, distance, clustering	reduces power consumption and enhanced network life	cluster techniques improves scalability	✓	×	×	×
Aydin et al. [16]	mobile sink for data aggregation	reduces the chances of node isolation	significant energy consumption	×	×	×	×
Amutha et al. [17]	residual energy, distance	simple cluster head selection	simple, easy to implement	×	×	×	×
Al-Baz and El-Sayed [18]	RSSI, Distance	suitable cluster head selection	simple, easy to implement, improves network life span	×	×	×	×
Qi et al. [19]	mobile scenario, residual energy, cluster frequency	fair cluster head selection	improves network life span	×	×	×	×
Dongare and Mangrulkar [20]	LEACH, maximum residual energy, compromised nodes	defence against grayhole and blackhole attacks	efficient techniques in terms of throughput, loss rate and end-end delay	×	×	×	×
Gong et al. [21]	energy level, risk of energy drainage	blocks suspected energy drainage nodes	provides protection against energy drainage attacks	×	×	×	×
Chuhang Wang's DPFCP [22]	Fuzy logic, PSO, distance, energy, nodes degree	cluster head selection	results in optimised cluster head selection, but may require more energy due to the repeated nature of PSO	×	×	×	×
A. Srivastava and P. K. Mishra [23]	MADM,distance, load balance, energy consumption, connectivity, coverage	cluster head selection	multi-objectives fitness function may used for optimisation purposes	×	×	×	×
Wu et al. [24]	LEACH, distance, energy consumption, balance towards cluster head selection	cluster head selection	enhances network diversity, convergence, and search	×	×	×	×
Christina et al. [25]	2 level Fuzzy logic	cluster head-based IDS, deals with blackhole	improves network performance	×	×	×	×
Jagnade et al. [26]	LEACH	deals with Vampire attack, which is an energy drainage attack	improves energy consumption	×	×	×	×
Proposed Solution	LEACH, CA, CM sketch, Bloom filter, distance, residual energy, energy consumption	space-time efficient cluster head selection	enhances network life, protection against grayhole, blackhole, and scheduling attacks	✓	✓	✓	×

1-cellular automata, 2-Bloom Filter, 3-CM sketch, 4-Other [Cuckoo Filter, XOR Filters, etc.]

cluster head is not more than the radio range of the cluster head, and there is no sensing hole in the desired system. If the density λ of the WSN is N/A, then the number of neighbours in the radio range of the WSN node would be $[(N-1)(\pi R_s^2)/A]$ [27]. If this is the case, then the probability of radio coverage of a cluster head in N/A dens network can



(a) Rectangular Grid (b) Voronoi Cellular Automata

FIGURE 3. WSN grid vs Varonoi region.

be computed as Equation 4.

$$p_{(cov)} = 1 - e^{-[(N-1)(\pi R_s^2)/A]} \tag{4}$$

where N is the number of sensor nodes in the network and A is the area of the network. Similarly, the probability of isolation of a node can be determined as Equation 5.

$$p_{(iso)} = e^{-[(N-1)(\pi R_s^2)/A]} \tag{5}$$

In this equation, R_s is the sensing range of a sensor node.

The architecture of the proposed solution is elaborated in Figure 4. In this section, we comprehensively discuss the key components of the proposed model, including cellular automata, Bloom filter, CM sketch, trust management and cluster head selection.

A. CELLULAR AUTOMATA (CA)

CA are effective discrete computational models with applications in science and engineering [28]. They originated from the work of John Von Neumann and Stanislaw Ulam in the 1940s. John Conway developed the practical application of CA in 1960, known as "The Game of Life." CA represent a discrete system with time, space, and states. They use a grid structure with individual cells, each holding a binary value of 0 or 1. Cells operate within a finite set of states, determined by neighboring values and specific rules applied at that particular moment in time. cellular automata is defined with the help of quadruplet CA, as shown in Equation 6.

$$CA = \{g, n, s, f\} \tag{6}$$

where:

g: is a Voronoi region tessellation that consists of cells that are occupied by WSN nodes, as shown in Figure 3b.

n: is neighbourhood; in other words, it is a number of nodes that a cluster head covers.

s: is a set of finite states that a sensor node may undergo.

f: is the transition function that governs the change in state of a cell from one to another.

In the proposed model given by Equations {7, 8, 9, 10}:

$$g = V(p(x_i, y_i))\, x \tag{7}$$

$$n = [(N-1)(\pi R_s^2)/A] \tag{8}$$

$$s = \{s_i | i \in \{0 = Trusted, 1 = Untrusted\}\} \tag{9}$$

$$f : s_i(t) \rightarrow s_i(t+1) \tag{10}$$

For the purpose of decision-making regarding the selection of a node as a cluster head, three crucial parameters come into play. These parameters encompass: i) the residual energy of the node being nominated for the cluster head role; ii) the spatial separation between the standard node and the designated node; and iii) the calculated trust value associated with the nominated node. In addition to these primary parameters, the decision-making process also involves two supplementary factors: the outcome of a Bloom filter query and the value contained within the CM sketch. Elementary cellular automata is one of the simplest, which is binary, 1-dimensional, and operates on the nearest neighbours. If the CA consists of three cells, then there would be 2^3 binary states and 2^8 different forms of CA. A 3-neighbourhood cellular automata can be written using Equation 11 [29].

$$S_i(t+1) = f(S_{i-1}(t), S_i(t), S_{i+1}(t)) \tag{11}$$

In this equation, S_i is the specific cell, S_{i-1} represents the left cell, and S_{i+1} the right, respectively. In addition to that, F is the function that produces CA, t is the current, and $t+1$ is the next time. Applying the CA majority rule (voting), if the majority of a node's neighbors observe abnormal energy drainage, the node will be labelled as malicious (CA state) or non-malicious.

B. BLOOM FILTERS: ISOLATION OF MALICIOUS NODES

The discussion on Bloom filters is essential, as our proposed approach relies on them. A Bloom filter is a space-efficient probabilistic data structure utilizing a bit array to determine element membership in a set. Widely used in computer science, software engineering, and network communication, they offer efficiency in representing large elements with minimal space, making them suitable for low-resource networks like WSN. In a Bloom filter, a size m is initialized with zeros. Elements from set S are passed through k hash functions, with their outputs marking corresponding indices as 1. Membership is checked similarly. While never yielding false negatives, false positives are possible due to the "Element Does Exist" response for elements not in S. The false-positive rate (FPR) can be managed by adjusting filter size and hash functions, with collision-resistant hashing further reducing FPR. The trade-off among size (m), hash functions (k), and FPR is defined. With input size (n) and error probability, m and k can be determined. The probability of not setting an index as 1 after adding n elements is $e^{-kn/m}$, with the converse around $1 - e^{-kn/m}$. The probability of false positives can be calculated using k and m in Equation 12 [30].

$$P_{FP} = \left(1 - (1 - 1/m)^{kn}\right)^k \approx \left(1 - e^{-kn/m}\right)^k \tag{12}$$

The values of 'k' and 'm' can significantly reduce the FPR, as evidenced by Lu's research on low-cost Bloom filters [31]. Thus, given the input size "n" and the desired FPR, one can estimate "k" and "m" using Equations 13

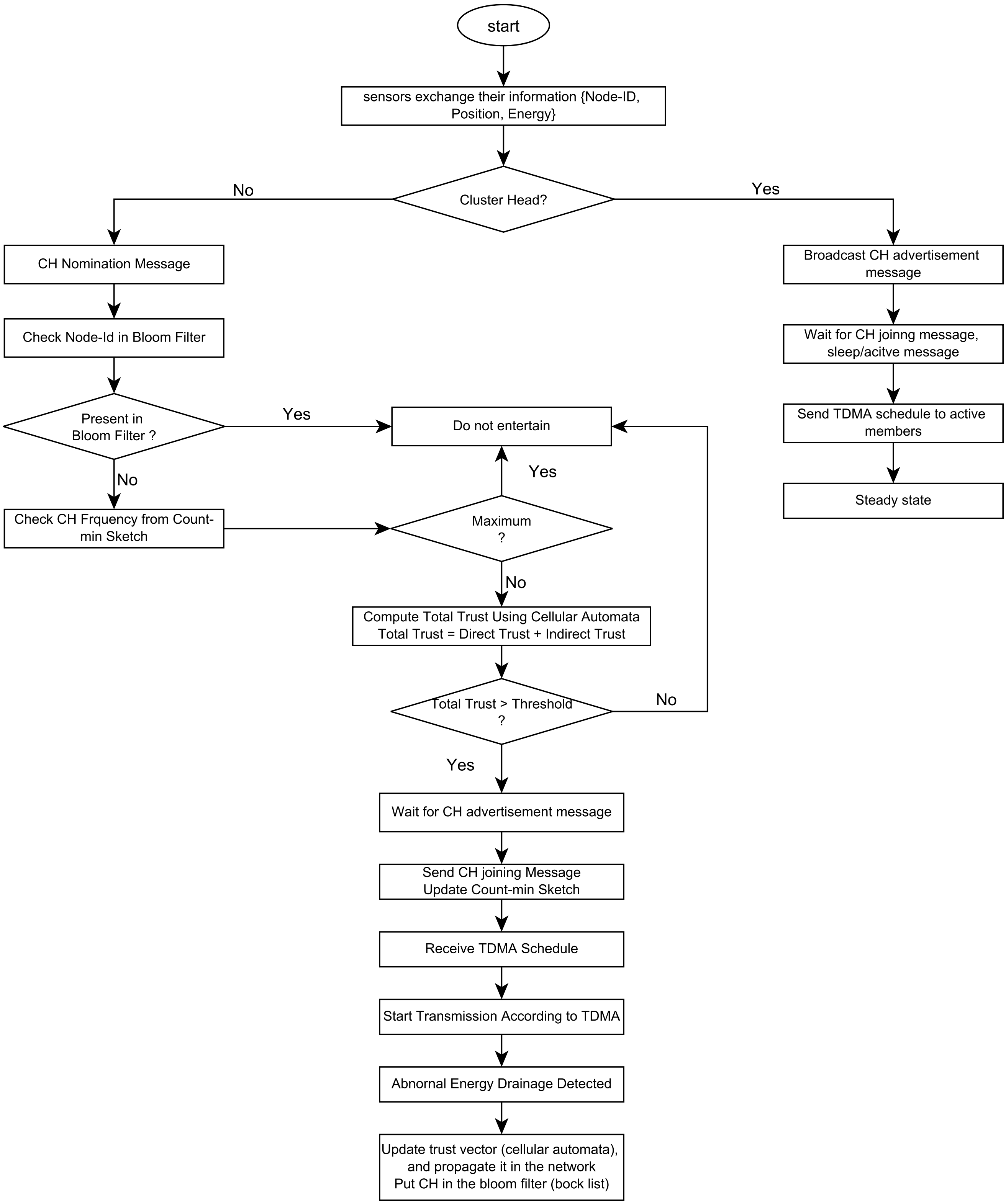


FIGURE 4. Architecture of the proposed model.

and 14 respectively.

$$k = \log 2 \times m/n \tag{13}$$

$$m = -n \log P_{FP}/(\log 2)^2 \tag{14}$$

Since k is some hash function, for the optimal value of k, the false-positive-rate is given by Equation 15.

$$\left(\frac{1}{2}\right)^k = (0.6185)^{\frac{m}{n}}. \tag{15}$$

The derivation of these equations is beyond the scope of this article, but can be found in Broder's work on Bloom filter network applications and the examination and applications of Bloom filters by Mitzenmacher and others [32], [33], [34]. Note that these equations provide only approximate values, and it is highly recommended that users configure m and k based on a specific desired error probability instead of relying solely on the theoretical values derived from these equations. Figure 5 shows that attackers A1, A2, and A3 are added to the Bloom filter using the hash functions h1, and h2, and how attacker A2 is successfully queried using the same set of hash functions.

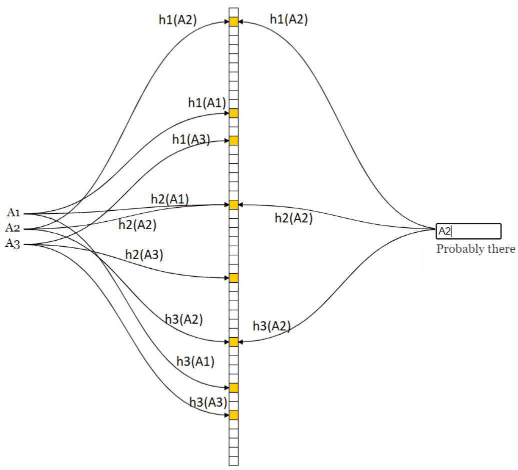


FIGURE 5. Bloom filter: Attacker insert and query.

C. CM SKETCH: FAIRNESS

The Count-Min Sketch is a probabilistic data structure designed to add elements and estimate the frequency of items in a set. It operates using two key parameters, m and k, where m signifies the count of buckets per hash function h_i, and K represents the number of hash functions with k being much smaller than m. The memory space needed for a CM sketch is $(m \times k)$ counters. It differs from Bloom filters as it uses a 2-dimensional array with X columns (corresponding to M) and Y rows (corresponding to k), providing a trade-off between accuracy and probability by adjusting X and Y. Adding or querying an item has a time complexity of $O(k)$, assuming each hash function operates in constant time. To maintain an acceptable error probability δ, k should be greater than or equal to $\log_n \frac{1}{\delta}$. CM sketch has been used by AT&T for network traffic analysis with limited memory and by Google atop its Map-Reduce parallel processing framework. Similarly, Clayton et al. [35] have discussed the use of CM sketches in adversarial scenarios of network security.

Algorithm 1 is applied for inserting cluster heads, and Algorithm 2 is employed for querying their frequencies.

D. TRUST MANAGEMENT SYSTEMS

It is a well-established fact that confidentiality, integrity, and authentication attacks can be handled with cryptographic techniques, but it is hard to fix the misbehaviour of malicious nodes such as packet-dropping, unjust routing, abnormal energy drainage, etc. Studies have shown that, in such cases, trust-based security solutions are quite effective [36]. A typical trust-based security solution consists of five steps [37]: i) collects values that can be used as trust elements, such as node interaction, position, energy, etc. These elements are used to calculate the trust-value; ii) collects values that can be used as trust elements, such as node interaction, position, energy, etc. These elements are used to calculate the trust-value; iii) nodes store the trust-value, trust elements, and reputation for later use; here, the storage constraint of WSN becomes very significant; iv) trust management system creates a trust model based on different parameters such as trust-value, trust-freshness, weights of trust for each element, nature of the attack, etc. The model should be simple, as the WSN nodes are very low in resources; v) trusts are transferred between nodes; vi) a node takes some decision.

Algorithm 1 CM Sketch for Node Insertion

Require: data stream N of nodes, w hash functions, and d hash tables
Ensure: CM sketch for N

Initialize all cells in the CM sketch to 0: $C[i, j] \leftarrow 0$ for $i \in \{1, \ldots, d\}$ and $j \in \{1, \ldots, w\}$.
for each node x in N **do**
  for $j \leftarrow 1$ to w **do**
    $h(x, j) \leftarrow$ hash value of x using hash function h_j
    for $i \leftarrow 1$ to d **do**
      $C[i, h(x, j)] \leftarrow C[i, h(x, j)] + 1$
  return CM sketch C

Algorithm 2 CM Sketch for Finding the Least Frequent Node

Require: CM sketch C, set of items N
Ensure: the least frequent node in N based on C

Initialize minCount $\leftarrow \infty$ and leastFreqItem $\leftarrow$ null.
for each item x in N **do**
  itemCount $\leftarrow$ the minimum count for x across all hash table-cell pairs: itemCount $\leftarrow \min\{C[i, h(x, j)]\}$ for $i \in \{1, \ldots, d\}$ and $j \in \{1, \ldots, w\}$ where $h(x, j)$ is the hash value of x using the hash function h_j.
  if itemCount $<$ minCount **then**
    minCount $\leftarrow$ itemCount
    leastFreqItem $\leftarrow x$
  return leastFreqItem

In this study, cellular automata and trust management technologies, along with probabilistic data structures (CM sketch, Bloom filter), have been exploited to address an illegal energy drainage issue for the LEACH protocol without modifying the original one.

Every member of the LEACH cluster at the start of each round has the provision to be or not be a cluster head. This decision is stochastic, based on the prior computed value of the number of cluster heads suggested for the network and the number of turns for which the nodes have been chosen as a cluster head so far. If n is the node that needs to take this decision, then it chooses a random number between 0 and 1. If the chosen value of this number is less than some $Threshold(n)$ computed using Equation 16, then the node is elected as a cluster head for the current round; otherwise, it is not.

$$Threshold(n) = \begin{cases} \dfrac{P_{CH}}{1 - P_{CH}(R \; Mod \; \frac{1}{P_{CH}})} & \text{if } n \in G \\ = 0 & \text{otherwise} \end{cases} \tag{16}$$

In Equation 16, P_{CH} is the percentage of cluster heads recommended for the WSN under discussion. R is the number of rounds in which node n has been selected as a cluster head until a particular round. G is the group of sensor nodes to which node n belongs.

The proposed algorithm for cluster head selection deviates from the conventional LEACH protocol by incorporating trust values of potential cluster heads. These trust values are determined based on factors such as past energy consumption, distance from the node, and residual energy. The trust value is calculated using cellular automata to monitor node behavior and performance and exchange information between nodes. Cellular automata keep track of node behavior and performance in terms of energy drainage. The solution does not alter any aspect of the LEACH protocol. Nodes start with a trust value of 1 for each other, and in the first round, nodes monitor their energy value and share this with neighbors. The nodes keep their neighbors information in their neighborhood vector. If a node detects an energy drainage attack, it inserts that cluster head in the Bloom filter, stops communicating with it, and waits for the next round. In the next round of cluster head selection, no frame is received from the cluster head listed in the Bloom filter; rather, a new cluster head is selected. Subsequently, the nodes engage in the monitoring of their respective energy levels while facilitating the exchange of status-related information. The standard behavior of nodes is further elaborated in Section VII.

E. TRUST CALCULATION AND PROPAGATION

There are two ways to calculate trust in a node: direct and indirect. Node's direct trust in node is determined by comparing the energy consumed in the previous round when it was selected as a cluster head and the energy consumed in the present round when it is nominated for cluster head. At the end of each round, we find the difference in energy consumption to calculate the direct trust, which is placed in the CA lattice after combining with indirect trust. All other nodes used this CA lattice for the selection of cluster in the next round, meaning the CA previous state determines the new state of the node who wishes to be a cluster head. Indirect trust is computed from trust information received from neighbours, provided the nodes belong to the same cluster. This condition provides a more accurate trust value. Total trust is the sum of direct and indirect trust. CA previous state determines the new state of node who wishes to be a cluster head. Figure 6 shows that Node $N_{i=1}$ desires to find its trust on $N_{i=5}$; hollow lines show the computation of direct trust and dotted indirect using neighbourhood vector $N_{i=2,3,4,6,7}$. But $N_{i=1}$ does not consult $N_{i=8}$ for calculating indirect trust on $N_{i=5}$ because $N_{i=8}$ does not belong to cluster $N_{i=1}$.

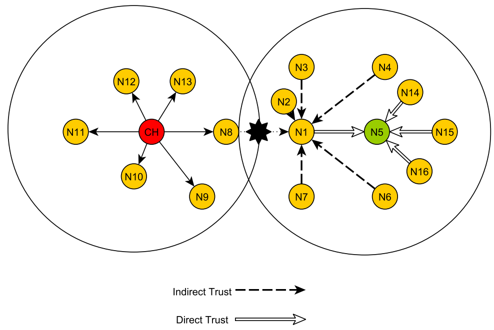


FIGURE 6. **Direct and indirect trust.**

Following Equations 17, 18, 19, and 20 are used to compute direct and indirect trust values. In Figure 6, it is considered that node N5 takes the initiative to self-nominate for the role of a cluster head, prompting node N1 to assess N5's trustworthiness through the subsequent process:

$$Trust_{N1-N5} = DT_{N1-N5} + IT_{N1-N5} \tag{17}$$

Here, the notation DT_{N1-N5} denotes the measure of direct trust, while IT_{N1-N5} signifies the evaluation of N1's indirect trust in N5. The indirect trust is obtained using the recommendations of neighbour nodes in the same cluster [38].

Where:

$$IT_{N1-N5} = \sum_{i}^{n} DT_i \rightarrow N2 \tag{18}$$

In Equation 18, n is the list of neighbouring nodes $N1$ [39]. Equations 19 and 20 are used to compute direct trust one node (N1 in this case) over the other (N5 in this case).

$$DT_{N1-N5} = 1 - T(cal) \tag{19}$$
$$T(cal) = Econ(t-1) - Econ(t) \tag{20}$$

In the presented model, Algorithm 3 is employed to generate a list of neighbors, while Algorithm 4 is utilized for the detection and isolation of malicious nodes, state alteration of a node, and the maintenance of trust factors through CA. Additionally, Algorithm 5 illustrates the process of nodes joining with cluster heads, eventually forming a secure cluster.

The energy consumption of WSN is crucial for maintaining the system's functionality. Energy models used in the network aim to minimize energy consumption to prolong its life. It is utilized to determine the power required for data transmission

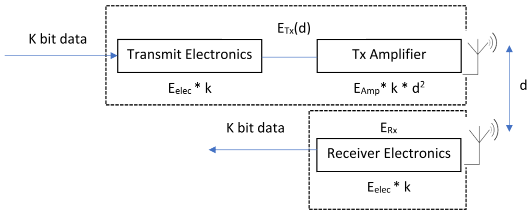


FIGURE 7. **Energy model.**

TABLE 2. **Sensor components and their operating modes.**

State	Processor	Memory	Sense unit	Radio
Active	active	active	on	tx
Listen	idle	sleep	on	rx
Sensing	sleep	sleep	on	off
Sleep	sleep	sleep	off	off

and reception within WSN, which rely on radio waves for communication between nodes. It consists of two types of channels: i) multi-path fading, and ii) free space. The choice between these channels depends on whether the distance (d) between the transmitter and receiver is less than or greater than a designated threshold value (d_0). Equation 21 can be used to calculate the energy required for transmitting a message of length k bits over a distance d and Equation 22 for receiving the same number of bits [40].

$$E_T(k,d) = \begin{cases} k * E_{\text{elec}} + k * E_{\text{fs}} * d^2, & \text{if } d \leq d_0 : \textit{freespace} \\ k * E_{\text{elec}} + k * E_{\text{mp}} * d^4, & \text{if } d \geq d_0 : \textit{multipath fading} \end{cases} \tag{21}$$

E_{elec}, E_{fs}, and E_{mp} represents energy used by electronic circuitry, free space, and multi-path fading channels, respectively.

$$E_R(k) = k * E_{elec} \tag{22}$$

The classical energy model considered in this study is shown in Figure 7. The operating modes of the WSN node are given in Table 2, which helps to compute the energy consumption of the node using $E_{consumed} = P_{tx} \times t_{tx} + P_{rx} \times t_{rx} + P_{idle} \times t_{idle}$.

Algorithm 3 Create Neighbourhood Vector

Require: current node *node*, maximum distance radius *radius*
Ensure: neighbourhood vector *neighbourhood*
neighbourhood ← empty list;
for each *n* in *network.nodes* **do**
  if $n \neq node$ **and** $distance(node, n) \leq radius$ **and** *n* **not in** *neighborhood* **then** add *n* to *neighborhood*;
Return *neighborhood*;

F. CH SELECTION PROCEDURE

In this research study, the selection of cluster head is made on the basis of the following parameters: i) the residual energy of the node that wishes to be a cluster head; ii) the distance between the normal node and the one that nominates itself as the cluster head; iii) trust in the nominated node; and iv) Bloom filter information. In the beginning, all nodes have full trust in each other, which is taken as 1. Upon a node's initial

Algorithm 4 CA and Trust Management

procedure Maintain CA
  for each *cluster* in *network* **do**
    for each *n* in *cluster.nodes* **do**
      `E`$_{remaining}$ `= E`$_{initial}$ `- E`$_{consumed}$
      if $E_{remaining} < ThresholdLevel1$ **then**
        procedure CHECK ENERGY DRAINAGE
          `E(t+1)(i,j) = E(t)(i,j) - C(S(t)(i,j), Neighbor. Nodes(i,j))`
          if `CA Lattice does not satisfy` conditions **then**
            `Set Node`$_{ij}$ `Energy Consumption State = Abnormal`
          `update CA lattice`
        if More than 50% nodes report Abnormal Energy Consumption **then**
          `stop communication with present` *CH*
          `insert this CH in the Bloom filter`
          `wait for the next CH selection round`
      else if $Erem < Ethres2$ **then**
        `Mark Current State of the Node = Isolate`
      procedure CALCULATE TRUST
        $T_{cal} = E_{con}(t-1) - E_{con}(t)$
        `WT` $\leftarrow T_{cal}$

Algorithm 5 Clustering Algorithm

`Initialise state of nodes` //CH selection
for Each Node **do**
  if (Residual energy $\geq$ 0) && (Flagcandidate = TRUE) **then**
    `Select CH using equation 23;`
    `Broadcast advertisement (CH`$_{id}$`);`
for Each Node **do**
  if (Residual energy > 0) && (Flagnormalnode = TRUE) **then**
    if Distance ≤ CH communication range **then**
      `Normal nodes send join messages;`
*After receiving all the join messages
for Each CH **do**
  `CH sends a TDMA message to its member nodes;`

broadcast designating itself as the cluster head, a validation procedure is initiated. This procedure assesses the level of trust the receiving nodes have in the advertised node by referencing the cellular automata maintained collectively by all nodes in the network. Equation 23 is used to select the cluster head from the RSSI value. RSSI has been found equally valid for cluster head selection in other research as well, such as [41].

$$WT_{j-i} = \alpha[\frac{Erem_i}{D(node_j, node_i)}] + \beta(Tnode_{j-i}) \tag{23}$$

where:

1) $Erem_i$: remaining energy of $node_i$ that wants to be a cluster head
2) $D(node_j, node_i)$: distance between $node_j$ and $node_i$ in a cluster
3) WT_{j-1}: Weighted trust of $node_j$ on $node_i$, a final trust value with which one node trusts over the other in its neighbourhood in the same cluster head
4) α and β: These weight values serve as determining factors in assigning appropriate significance to trust values.

Nodes in the cluster keep records of their trust in each other in their respective neighbourhood regions. Equation 23 ensures that only a node $node_j$ nominated as cluster head will be selected as cluster head that has the highest energy and trust value but the lowest distance value from the cluster node $node_j$. In other words, the given equation gives the optimised value for the selection of the cluster head. Moreover, abnormal energy on one round of drainage is communicated in the network, and all nodes update their cellular automata of that node, which results in the loss of network nodes on that cluster head node. The malicious node is recorded in the Bloom filter using Algorithm 6, and in the future, no frame will be entertained sent from this node. If a malicious node nominates itself for selection of cluster head, its presence is first seen in the Bloom filter. Algorithm 7 is used to check the presence of malicious nodes in the Bloom filter; if found, it will not be entertained. If not found, the cellular automata will be seen, and with lower trust, it will be negated.

Algorithm 6 Malicious Node Insertion in Bloom Filter

`B: Bloom filter`
`l: size of Bloom Filter`
`t: total number of attackers`
`A: Attacker`
for Index=0 to S-1 STEP 1 **do**
    $B[Index] \leftarrow 0$ `//Initialize Bloom filter locations to 0`
for j=0 to t STEP 1 **do**
    for i=0 to k STEP 1 **do**
        $B[h_i(A_j)\ mod\ S] \leftarrow 1$

Algorithm 7 Malicious Node Membership Query

`B: Bloom filter`
`l: size of Bloom Filter`
`A: Attacker`
`Bloom filter` B`, Attacker` A
`True if` $AttackerA$ `is probably in` B`,`
`False otherwise`
for $i \leftarrow 1$ to k **do**
    if $B[h_i(A)\ mod\ S] = 0$ **then return** False
return True

TABLE 3. Simulation setup.

Properties	Value
Channel Type	Wireless Channel
Radio-Propagation Model	Two Ray Ground
Antenna Model	Omni-Directional
Protocol	LEACH
Topology	100m × 100m
Simulation	500 rounds
No. of Nodes (Nn)	100
Node chance to be a CH (P)	10%
Number of CHs	P×Nn
Node Initial Energy	2000 mJoules
E(sensing)	0.083 J/s
E(aggregation)	5 nJ/bit/signal
E(amplification)	10 pJ/bit/m2
Nodes Radio Range	3-4 m
Frame Size	25-30 Bytes (frame larger than 100 bytes dropped by 802.15.4 in ns2)
Data Rate	64 Kbps
Number of attackers	1
MAC	IEEE 802.15.4

VII. SIMULATION AND RESULTS ANALYSIS

A. PROOF OF CONCEPT

LEACH routing protocol is used in the IEEE 802.15.4 network [42]. The proposed protocol is simulated in NS-2.34, and a complete list of simulation setup parameters is given in Table 3. The results of the simulation show that the proposed protocol mitigates the abnormal energy drainage issue and provides a secure way for the selection of an optimised cluster head. The cellular automata precisely model the dynamic energy drainage behaviour of the malicious node, and the Bloom filter is cost-effective in terms of space and time complexity.

B. ENERGY DRAINAGE ANALYSIS WITHOUT SOLUTION

1) ENERGY DRAINAGE OF DEFAULT LEACH

The simulation was run for 500 rounds using the original LEACH protocols without any attacks. It is observed that energy consumption per bit is higher in large network areas as compared to smaller ones. The comparison is shown in Figure 8.

The wireless networks are erroneous, and the chance of frame losses is always higher. So, in the case of packet drop, the sender will have to consume more energy to re-transmit

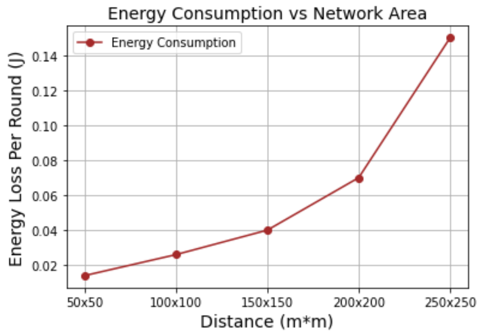


FIGURE 8. Energy consumption vs. network area m^2.

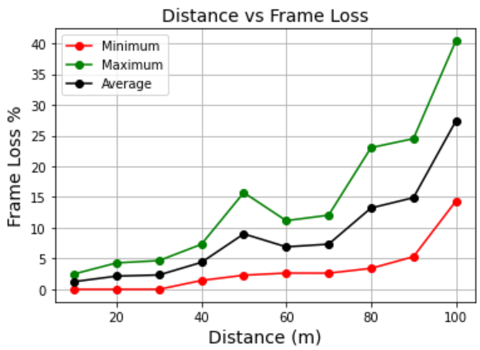


FIGURE 9. Distance vs. frame loss.

the unsuccessfully transmitted frames. In simulation, it is considered that all the nodes are identical and suffer almost similar frame losses, which are inherently associated with WSN [43]. The frame loss with respect to distance is shown in Figure 9.

The results of energy consumption in the case of original LEACH in the absence of any attack are shown in Figure 10. It is observed that a legal node on average consumes about 0.00000111 J/bit, 0.000222 J/packet, and 0.010878926J-0.0111J per round. Furthermore, it was observed that the network energy dropped to 0 within 550 rounds, the whole network ceased to exist, and 6×100J network energy was completely consumed. It is important to note that 6J is the initial node energy. Since there are 100 nodes in the network, 6×100J represents the total network energy. In the simulation, a 25-byte frame is used for transmission. We configured the normal node to send only 50 packets in one round to its cluster head; $25 \times 8 \times 50$ bits were transmitted in one round.

For the detection of abnormalities in the drainage of node energy, the node keeps track of the energy drainage of each transmission against the number of frames transmitted in that transmission. In our proposed model, we considered that a node transmits 50 frames in a round. Since more transmission power is required for distance transmission, the node consumes $\approx$0.56μJ for short distances such as 50m_2 and $\approx$800μJ for long distances such as 250m_2. At the same time, the frame loss is higher in the case of

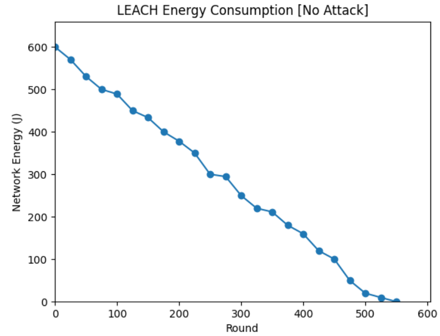


FIGURE 10. Original LEACH protocol without attack.

long-distance transmission as compared to short-distance transmission, which also results in the consumption of more energy for making re-transmissions. On average, 27% frame loss is considered to communicate with the long-distance cluster head. It is already established that long-distance transmission consumes more energy compared with short-distance transmission. In addition to all this, it is worth considering that the size of the payload also plays an important role in energy consumption during transmission because bigger frames consume more energy compared with smaller frames. In addition to this, the number of clusters also affects energy consumption; the greater the number of clusters, the higher the energy consumption. It is observed that the residual energy also depends upon the number of rounds that nodes complete and even when they become cluster heads. So, when a legitimate node finds that its energy is draining quickly, it will inquire with its neighbors about their rate of energy drainage. The issue becomes more critical when a malicious node becomes a cluster head. If neighbors belonging to the same cluster report abnormal energy drainage, meaning greater than the normal energy drainage threshold, communication is stopped with the cluster head. The trust of member nodes is lowered over the cluster, and the CA is updated accordingly.

2) BLACKHOLE ATTACK ON LEACH

In this attack, the malicious node attempts to capture the maximum data traffic of the network and intentionally drops it instead of sending it to the base station. Consequently, the malicious node conserves energy, potentially leading to a higher likelihood of being selected as the cluster head in each round. To mitigate the impact of this attack, it becomes imperative to remove the malicious node from the network. To simulate this attack, a single malicious node was introduced into the network, with a data packet drop rate set between 80% and 90%. As the cluster head refrains from forwarding data frames to the sink and instead transmits a drop frame message to the source node, the latter is compelled to engage in re-transmissions. Consequently, the node experiences rapid energy drainage, exceeding 80% of the original LEACH model. Figure 11 illustrates the

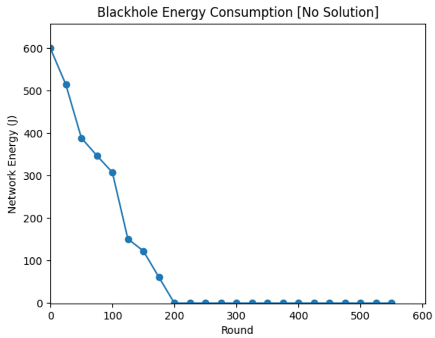


FIGURE 11. LEACH [without solution]: Blackhole attack.

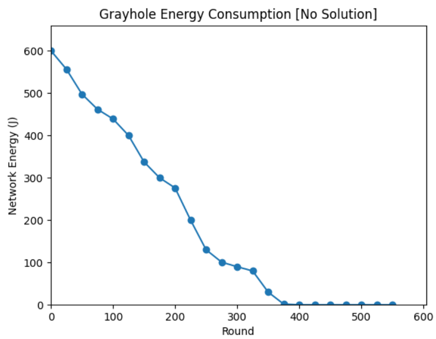


FIGURE 12. LEACH [Without solution]: Grayhole attack.

complete network collapse within 200 rounds. Fortunately, this abnormal energy drainage is easily detectable and confirmable by neighboring nodes within the same cluster, leading to an immediate halt in ongoing transmissions with the current cluster head.

3) GRAYHOLE ATTACK ON LEACH

In a grayhole attack, an attacker advertises itself with a high probability of becoming a cluster head and selectively drops data packets when it becomes a cluster head. A grayhole attack is simulated by deploying a malicious node with 50% drop rate that consequently requires the member nodes to make more re-transmission and lose more energy as compared to normal transmission in a round. It is observed that 25%-30% more energy is drained, which causes the death of the entire network within 400 rounds. The effect of this attack is shown in Figure 12, which shows the drainage of almost half of the network energy in the first 100 rounds.

4) SCHEDULING ATTACK ON LEACH

In a grayhole attack, an attacker increases the likelihood of becoming a cluster head and selectively drops data packets when it does. The grayhole attack is simulated by deploying a malicious node with a 50% drop rate. Consequently, member nodes are required to engage in more re-transmissions, leading to greater energy loss compared to normal transmission in rounds. It has been observed that this results in a 25%-30% increase in energy drainage, ultimately

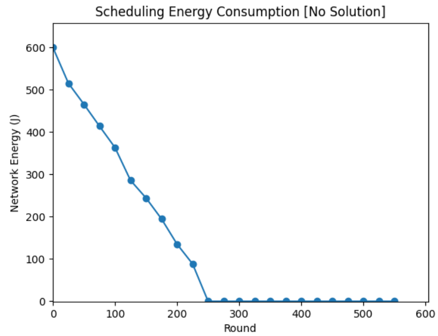


FIGURE 13. LEACH [without solution]: Scheduling attack.

leading to the network's demise within 400 rounds. The impact of this attack is depicted in Figure 13, which illustrates the depletion of nearly half of the network's energy within the first 100 rounds.

C. ENERGY DRAINAGE ANALYSIS WITH PROPOSED SCHEME: COMPARISON AND DISCUSSION

The simulation results demonstrated a notable enhancement in the original LEACH protocol's performance. The proposed solution was tested alongside the original LEACH protocol, both under normal conditions and while facing blackhole, grayhole, and scheduling attacks. The objective of these tests was to identify any abnormal energy drainage in legitimate nodes caused by malicious cluster heads within a cluster. Our solution suggests that legitimate nodes should monitor their energy drainage, preventing the selection of any node as a cluster head that caused abnormal energy drainage in previous transmission rounds. When a malicious cluster head refrains from forwarding data to the sink (base station), it conserves its own battery and consequently has a higher likelihood of being selected as a cluster head in the next round. To address this issue, the CM sketch assumes a crucial role in the equitable selection of a cluster head based on its frequency of being chosen. This data structure aids in selecting a cluster head with the least frequency. Furthermore, the malicious nodes are isolated and stored in an efficient bit array data structure named the Bloom filter. If any member node of a cluster identifies a nominated cluster head in its Bloom filter, no node is designated as a cluster head.

In the case of scheduling, as shown in Figure 14, the proposed solution is sufficient to increase WSN life by more than 260 rounds, saving $\approx$ 2.78 J energy of the network.

Figure 15 shows the energy drainage of the network with the original LEACH and the proposed one in the presence of a grayhole attack. It is observed that the proposed model significantly improves the network life of WSN. In the absence of the proposed solution, the whole network dies out within about 380 rounds. But with the proposed model, the network lives for about 490 rounds. Thus, the proposed solution enhances network life by more than 100 rounds. In other words, it saves $\approx$ 1.1J network energy.

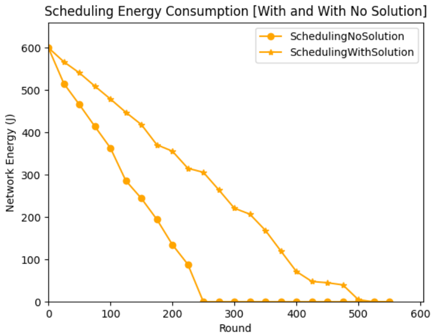


FIGURE 14. LEACH [with solution]: Scheduling attack.

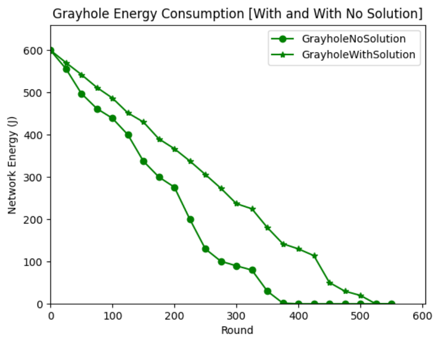


FIGURE 15. LEACH [with solution]: Grayhole attack.

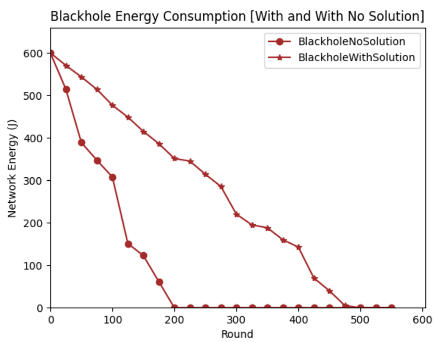


FIGURE 16. LEACH [with Solution]: Blackhole attack.

Similarly, in the case of a blackhole attack, the WSN life increases by more than 280 rounds, thus saving $\approx$ 3J of network energy, which is shown in Figure 16.

Figure 17 shows the energy drainage proposed model when there is no attacking node in the network. In this case, our proposed model consumes more energy as compared to the default LEACH protocol. On average, the proposed protocol consumes $\approx$ 0.08J - 0.12J more energy as compared to the default LEACH. In other words, network life is reduced by 8-11 rounds in the proposed model when compared with the default LEACH. This cost, which is paid to thwart the energy drainage attacks, is negligible compared to the benefits obtained from the solution. Nevertheless, results show that the proposed solution is sufficient to outperform

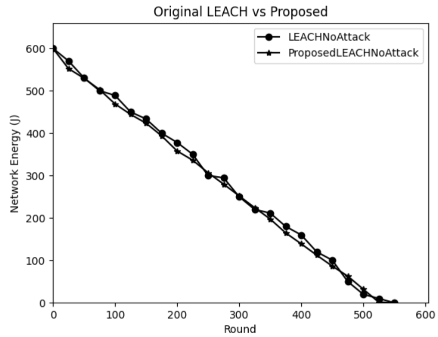


FIGURE 17. LEACH [with solution].

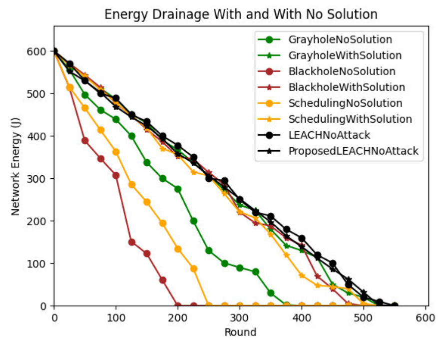


FIGURE 18. Energy drainage comparison.

default LEACH in terms of mitigation of abnormal energy drainage issues and optimisation of energy consumption.

A comprehensive comparison of energy drainage caused by blackhole, grayhole, and scheduling attacks is illustrated in Figure 18, both in the presence and absence of the proposed solution. The figure shows that the proposed LEACH consumes more energy than the original, and a significant amount of energy is saved from blackhole, grayhole, and scheduling attacks, as already discussed individually.

D. ENERGY IMPROVEMENT COMPARISON WITH CLOSE STUDIES

Comparing our proposed solution to previous studies, particularly Joseph et al. [25], indicates a notable 2.12 times improvement in energy utilization. Furthermore, our approach surpasses the performance of Jagnade et al. [26] by approximately 1.09 times. In the context of blackhole scenarios, a comparison with Dongare and Mangrulkar [20] reveals that our proposed approach outperforms theirs by about 1.03 times, while in the case of grayhole attack, Dongare et al. [20] outperforms our model by more than double. It's important to note that Dongare et al.'s [20] data rate is 5 kbps, whereas ours is 64 Kbps. This disparity influences higher frame loss at elevated data rates, necessitating re-transmission and consequently leading to increased energy consumption. Additionally, our proposed memory-based model, incorporating the Bloom filter, CM sketch, and CA_{t-1}, stores evolving system states over time, culminating in enhanced defence mechanisms.

E. APPLICATION SCENARIOS

Proposed security model is highly suitable for the following and similar cases

1) PROXIMITY

In multi-hop WSN, nodes near the sink or base station must transmit or forward more traffic than those farther away. This leads to energy depletion in these nodes, potentially forming energy holes within the network. This results in outer layer sensor nodes abstaining from forwarding data to the sink, reducing the network's lifespan, even with abundant residual energy.

2) EXCESSIVE TRANSMISSION/RECEPTION

Energy holes occur when certain nodes receive or transmit more packets than their counterparts, potentially leading to network collapse in multi-hop settings.

3) ATTACK SCENARIOS

Vampire attacks are malicious attacks that stealthily target the gradual depletion of network energy resources, typically batteries within nodes. These threats pose a significant threat to WSN applications operating in challenging environments, such as environmental surveillance or enemy detection, where battery replacement is often difficult or impossible.

VIII. ASSUMPTIONS AND LIMITATIONS

The proposed model assumes that all nodes are randomly deployed and have equal energy levels in the network, which is not possible in all scenarios. A Bloom filter used to identify and block malicious cluster heads may generate false positives, mistakenly categorizing legitimate nodes as malicious, but these can be significantly reduced to a tolerable level by adjusting the filter size and the number of hash functions. In addition, Bloom filters do not support element deletion, so once a cluster head is added, it cannot be removed. Fortunately, this limitation can be addressed by using counting Bloom filters.

IX. CONCLUSION AND THE FUTURE WORK

The proposed CA-based trust management is a decentralized and adaptive approach to handling trust in WSN, making it more robust against various threats. It uses probabilistic data structures for space efficiency and is crucial in selecting trust metrics, designing CA rules, updating trust rates, and propagating it in the network. The study focuses on challenges in WSN and energy efficiency issues, resulting in an enhancement of the LEACH protocol with the help of the Bloom filter, CM sketch, and cellular automata structure to counter energy drainage attacks. Cellular automata are effective for modeling system dynamics, while probabilistic data structures are useful for space and time efficiency. These techniques help devise an optimized solution for mitigating abnormal energy drainage issues (grayhole, blackhole, and scheduling attacks) in WSN; may encounter false positives but to tolerable extent with no false negatives. The proposed approach outperforms the original LEACH, demonstrating its efficacy and practical viability.

Bloom filters are space-efficient data structures, and CM sketch solves the counting problems probabilistically. Cellular automata are good for simulating dynamic systems in the real world. In the future, we want to enhance the trust model so other attacks may also be mitigated in other routing protocols like Sensor Protocols for Information via Negotiation (SPIN), Multi Path and Multi SPEED (MMSPEED), Geographical and Energy-aware Routing (GEAR), Distributed Energy Efficient Clustering (DEEC) and Enhanced Distributed Energy Efficient Clustering (EDEEC). In the future, we also want to make use of some optimization techniques, such as PSO for the best cluster head selection.

REFERENCES

[1] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, 2000, p. 10.

[2] M. Keerthika and D. Shanmugapriya, "Wireless sensor networks: Active and passive attacks–Vulnerabilities and countermeasures," *Global Transitions Proc.*, vol. 2, no. 2, pp. 362–367, Nov. 2021.

[3] S. S. Qasim and S. M. NSAIF, "Advancements in time series-based detection systems for distributed denial-of-service (DDoS) attacks: A comprehensive review," *J. Netw. Secur.*, vol. 2024, pp. 1–9, Jan. 2024. [Online]. Available: https://mesopotamian.press/journals/index.php/BJN/article/view/255/223

[4] N. Sabor, S. Sasaki, M. Abo-Zahhad, and S. M. Ahmed, "A comprehensive survey on hierarchical-based routing protocols for mobile wireless sensor networks: Review, taxonomy, and future directions," *Wireless Commun. Mobile Comput.*, vol. 2017, pp. 1–23, Jan. 2017, doi: 10.1155/2017/2818542.

[5] J. Gutiérrez, J. F. Villa-Medina, A. Nieto-Garibay, and M. Á. Porta-Gándara, "Automated irrigation system using a wireless sensor network and GPRS module," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 1, pp. 166–176, Jan. 2014.

[6] A. A. Baradaran and F. Rabieefar, "NEECH: New energy-efficient algorithm based on the best cluster head in wireless sensor networks," *Iranian J. Sci. Technol., Trans. Electr. Eng.*, vol. 47, no. 3, pp. 1129–1144, Sep. 2023, doi: 10.1007/s40998-022-00587-1.

[7] S. Saravanan, D. Prabakar, and S. S. Sathya, "Trust aware ad hoc routing protocol with key management based mechanism and optimal energy-efficient cluster head selection in mobile ad hoc networks," *Concurrency Comput. Pract. Exper.*, vol. 35, no. 7, p. e7599, Mar. 2023.

[8] D. Arshad, M. Asim, N. Tariq, T. Baker, H. Tawfik, and D. Al-Jumeily OBE, "THC-RPL: A lightweight trust-enabled routing in RPL-based IoT networks against Sybil attack," *PLoS ONE*, vol. 17, no. 7, Jul. 2022, Art. no. e0271277.

[9] S. Gurumoorthy, P. Subhash, R. Pérez De Prado, and M. Wozniak, "Optimal cluster head selection in WSN with convolutional neural network-based energy level prediction," *Sensors*, vol. 22, no. 24, p. 9921, Dec. 2022.

[10] V. Narayan and A. K. Daniel, "A novel approach for cluster head selection using trust function in WSN," *Scalable Comput., Pract. Exper.*, vol. 22, no. 1, pp. 1–13, Feb. 2021.

[11] K. Prathapchandran and T. Janani, "A trust-based security model to detect misbehaving nodes in Internet of Things (IoT) environment using logistic regression," *J. Phys., Conf. Ser.*, vol. 1850, no. 1, May 2021, Art. no. 012031.

[12] M. Ilyas, Z. Ullah, F. A. Khan, M. H. Chaudary, M. S. A. Malik, Z. Zaheer, and H. U. R. Durrani, "Trust-based energy-efficient routing protocol for Internet of Things–based sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 10, Oct. 2020, Art. no. 155014772096435, doi: 10.1177/1550147720964358.

[13] J. Reyes, F. García, M. E. Lárraga, J. Gómez, and L. Orozco-Barbosa, "Game of sensors: An energy-efficient method to enhance network lifetime in wireless sensor networks using the game of life cellular automaton," *IEEE Access*, vol. 10, pp. 129687–129701, 2022.
[14] P. S. Khot and U. L. Naik, "Cellular automata-based optimised routing for secure data transmission in wireless sensor networks," *J. Experim. Theor. Artif. Intell.*, vol. 34, no. 3, pp. 431–449, May 2022.
[15] S. Doostali and S. M. Babamir, "An energy efficient cluster head selection approach for performance improvement in network-coding-based wireless sensor networks with multiple sinks," *Comput. Commun.*, vol. 164, pp. 188–200, Dec. 2020.
[16] M. A. Aydin, B. Karabekir, and A. H. Zaim, "Energy efficient clustering-based mobile routing algorithm on WSNs," *IEEE Access*, vol. 9, pp. 89593–89601, 2021.
[17] S. Amutha, B. Kannan, and M. Kanagaraj, "Energy-efficient cluster manager-based cluster head selection technique for communication networks," *Int. J. Commun. Syst.*, vol. 34, no. 5, p. e4741, Mar. 2021.
[18] A. Al-Baz and A. El-Sayed, "A new algorithm for cluster head selection in LEACH protocol for wireless sensor networks," *Int. J. Commun. Syst.*, vol. 31, no. 1, p. e3407, Jan. 2018.
[19] H. Qi, F. Liu, T. Xiao, and J. Su, "A robust and energy-efficient weighted clustering algorithm on mobile ad hoc sensor networks," *Algorithms*, vol. 11, no. 8, p. 116, Aug. 2018.
[20] S. P. Dongare and R. S. Mangrulkar, "Optimal cluster head selection based energy efficient technique for defending against gray hole and black hole attacks in wireless sensor networks," *Proc. Comput. Sci.*, vol. 78, pp. 423–430, Jan. 2016.
[21] P. Gong, T. M. Chen, and P. Xu, "Resource-conserving protection against energy draining (RCPED) routing protocol for wireless sensor networks," *Network*, vol. 2, no. 1, pp. 83–105, Feb. 2022.
[22] C. Wang, "A distributed particle-swarm-optimization-based fuzzy clustering protocol for wireless sensor networks," *Sensors*, vol. 23, no. 15, p. 6699, Jul. 2023.
[23] A. Srivastava and P. K. Mishra, "Load-balanced cluster head selection enhancing network lifetime in WSN using hybrid approach for IoT applications," *J. Sensors*, vol. 2023, pp. 1–29, May 2023, doi: 10.1155/2023/4343404.
[24] D. Wu, S. Geng, X. Cai, G. Zhang, and F. Xue, "A many-objective optimization WSN energy balance model," *KSII Trans. Internet Inf. Syst. (TIIS)*, vol. 14, no. 2, pp. 514–537, 2020.
[25] C. Joseph, P. C. Kishoreraja, and R. Baskar, "Cluster head based intrusion detection system for black hole attacks in wireless ad hoc networks using 2 level fuzzy logic system," in *Proc. 1st Int. Conf. Comput., Commun. Control Syst.*, 2021, pp. 1–16.
[26] G. A. Jagnade, S. I. Saudagar, and S. A. Chorey, "Secure VANET from vampire attack using LEACH protocol," in *Proc. Int. Conf. Signal Process., Commun., Power Embedded Syst. (SCOPES)*, Oct. 2016, pp. 2001–2005.
[27] S. Mohdpuzi, S. Salleh, R. Ishak, and S. Olariu, "Neighborhood discovery in a wireless sensor networks," in *Proc. 9th Int. Conf. Adv. Mobile Comput. Multimedia*, Dec. 2011, pp. 80–86.
[28] M. Ghosh, R. Kumar, M. Saha, and B. K. Sikdar, "Cellular automata and its applications," in *Proc. IEEE Int. Conf. Autom. Control Intell. Syst. (I2CACIS)*, Oct. 2018, pp. 52–56.
[29] T. Toffoli and N. Margolus, "Cellular automata," in *Cellular Automata Machines: A New Environment for Modeling*. Stanford, CA, USA: Stanford Univ. Press, 2021, pp. 5–11.
[30] D. Randall. (Oct. 22, 2006). *CS 6550 ? Design and Analysis of Algorithms*. Accessed: Oct. 15, 2018. [Online]. Available: http://people.math.gatech.edu/~randall/AlgsF09/bloomfilters.pdf
[31] J. Lu, T. Yang, Y. Wang, H. Dai, X. Chen, L. Jin, H. Song, and B. Liu, "Low computational cost Bloom filters," *IEEE/ACM Trans. Netw.*, vol. 26, no. 5, pp. 2254–2267, Oct. 2018.
[32] A. Broder and M. Mitzenmacher, "Network applications of Bloom filters: A survey," *Internet Math.*, vol. 1, no. 4, pp. 485–509, Jan. 2004.
[33] J. Honorof. (2006). *An Examination of Bloom Filters and Their Applications*. Accessed: Mar. 28, 2022. [Online]. Available: https://cs.unc.edu/
[34] D. S. Bhatti and S. Saleem, "Ephemeral secrets: Multi-party secret key acquisition for secure IEEE 802.11 mobile ad hoc communication," *IEEE Access*, vol. 8, pp. 24242–24257, 2020.
[35] D. Clayton, C. Patton, and T. Shrimpton, "Probabilistic data structures in adversarial environments," in *Proc. ACM SIGSAC Conf. Comput. Commun.*, 2019, pp. 1317–1334.
[36] A. Turower, "Trust management method for wireless sensor networks," Ph.D. dissertation, pp. 1–148, 2017. [Online]. Available: https://pbc.gda.pl/Content/63004/phd_turower_alan.pdf
[37] W. Fang, W. Zhang, W. Chen, T. Pan, Y. Ni, and Y. Yang, "Trust-based attack and defense in wireless sensor networks: A survey," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–20, Sep. 2020, doi: 10.1155/2020/2643546.
[38] J. M. Corchado, J. Bajo, D. I. Tapia, and A. Abraham, "Using heterogeneous wireless sensor networks in a telemonitoring system for healthcare," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 2, pp. 234–240, Mar. 2010.
[39] W. Li, L. Ma, and Q. Yu, "Cellular automata-based multi-hop WSN routing protocol energy saving technology," in *Proc. Int. Conf. Commun., Circuits Syst. (ICCCAS)*, vol. 1, Nov. 2013, pp. 113–117.
[40] B. Suresh and G. S. C. Prasad, "An energy efficient secure routing scheme using LEACH protocol in WSN for IoT networks," *Measurement, Sensors*, vol. 30, Dec. 2023, Art. no. 100883.
[41] K. Jain and A. Kumar, "An optimal RSSI-based cluster-head selection for sensor networks," *Int. J. Adapt. Innov. Syst.*, vol. 2, no. 4, p. 349, 2019.
[42] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," *Security*, vol. 3, pp. 162–175, Nov. 2004.
[43] C. Cirstea, M. Cernaianu, and A. Gontean, "Packet loss analysis in wireless sensor networks routing protocols," in *Proc. 35th Int. Conf. Telecommun. Signal Process. (TSP)*, Jul. 2012, pp. 37–41.

DAVID SAMUEL BHATTI received the Ph.D. degree in computer science (information security) from the School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2020. He is currently an Assistant Professor with the University of Central Punjab (UCP), Lahore, Pakistan. His research interests include networks, mobiles, and smartphone security. His expertise extends to secure routing protocols, secret key establishment, and device authentication, particularly in low-resource devices, such as wearable, body-worn, and wireless body area networks (WBAN) devices. His current research endeavors involve the design of security protocols using probabilistic data structures. The aim is to optimize time and space complexity in low-resource devices, enhancing their efficiency and robustness in the realm of information security.

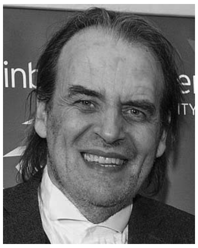
SHAHZAD SALEEM received the M.S. degree in information and communication systems security from The Royal Institute of Technology, Sweden, and the Ph.D. degree in digital forensics from the Department of Computer and Systems Sciences, Stockholm University, Sweden. He is formerly associated with the School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan, where he is currently on an extended leave from SEECS. He is actively engaged in research with the Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia, focusing on information security with a keen interest in digital forensics. His expertise includes extensive work with industry-standard digital forensics tools, such as i2 Analyst Notebook, EnCase, FTK, XWays, UFED, XRY, and Device Seizure.

ZULFIQAR ALI received the Ph.D. degree in computer science from the National University of Computer and Emerging Sciences, Islamabad. He is currently an accomplished Assistant Professor with the National University of Technology, where he has extensive teaching experience. He has supervised research projects and published extensively in reputable journals. His commitment to academic excellence is evident in his continuous contributions to the field of computer science. Apart from his teaching roles, he actively contributes to conferences, including the Frontiers of Information Technology. His research interests include optimization, networks, and particularly in computational intelligence and swarm intelligence. He received the Research Exchange Fellowship from Arizona State University, in 2014.

TAE-JIN PARK was born in Seoul, South Korea. He received the B.Sc. and M.Sc. degrees in chemistry from Yonsei University, in 1997 and 1999, respectively, and the Ph.D. degree from the Department of Chemistry, The State University of New York at Stony Brook (SUNY Stony Brook), in 2007, under the supervision of Prof. Stanislaus S. Wong. After completing compulsory military service, in 2001, he was a Research Scientist with Korea Institute of Science and Technology (KIST). After finishing a Postdoctoral Fellowship with the University of California at Davis (UC Davis) with Prof. Alexandra Navrotsky, he held the position of a Senior Researcher with Korea Atomic Energy Research Institute (KAERI), since 2011. He has been continuing his work at KAERI as a Principal Researcher, since 2017. His research interests include wireless technology relevant to smart sensing and diagnosis for safety-related instrumentations in nuclear power plants, thermochemistry, nano/materials sciences, and safety in radwaste disposal relevant to nuclear energy.

BEOMKYU SUH received the B.S. and M.S. degrees in computer engineering from Chungnam National University, Daejeon, South Korea, in 2022 and 2024, respectively, where he is currently pursuing the Ph.D. degree. His research interests include wireless sensor networks and deep reinforcement learning.

ALI KAMRAN received the Engineering degree from COMSATS University Islamabad, Pakistan, in 2012. Since then, he has been working in IT domain with cutting-edge technologies and well-known firms across the globe. As young dynamic Entrepreneur has more than ten years of proven experience in IT, Digital Transformation, Artificial Intelligence, and Machine Learning, is currently the Country Head for a multinational IT firm. He has worked with renowned organizations like Faronics, Infosys, Microsoft, SAP, Veeam, VMware, Oracle, DELL-EMC, Cisco, and others. He has also initiated his own start-up, focused on cutting-edge technologies, Net Zero carbon, and state-of-the-art solutions for modern problems with less human intervention. He is keen on using technology for Corporate Social Responsibility (CSR) and improving human life.



WILLIAM (BILL) J. BUCHANAN is currently a Professor with the School of Computing, Edinburgh Napier University, Edinburgh, U.K. He also leads the Blockpass ID Laboratory and the Centre for Cybersystems and Cryptography. He has published more than 30 academic books and over 300 academic research papers. He works in the areas of blockchain, cryptography, trust, and digital identity. He has one of the most extensive cryptography sites in the World (asecuritysite.com). He is involved in many areas of novel research and teaching. Along with this, his work has led to many areas of impact, including three highly successful spin-out companies, along with awards for excellence in knowledge transfer, and teaching. He was awarded the "Outstanding Contribution to Knowledge Exchange" Award and an OBE. He is a fellow of British Computer Society (BCS).

KI-IL KIM received the M.S. and Ph.D. degrees in computer science from Chungnam National University, Daejeon, South Korea, in 2002 and 2005, respectively. He is currently with the Department of Computer Science and Engineering, Chungnam National University. He has been with the Department of Informatics, Gyeongsang National University, since 2006. His research interests include machine learning for networks, wireless/mobile networks, fog computing, MANET, QoS for wireless, and wireless sensor networks.