Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 9
September 2023

Detecting Selective Forwarding Attack in Cluster-Based Wireless Sensor Networks Using Composite Reputation Value Algorithm

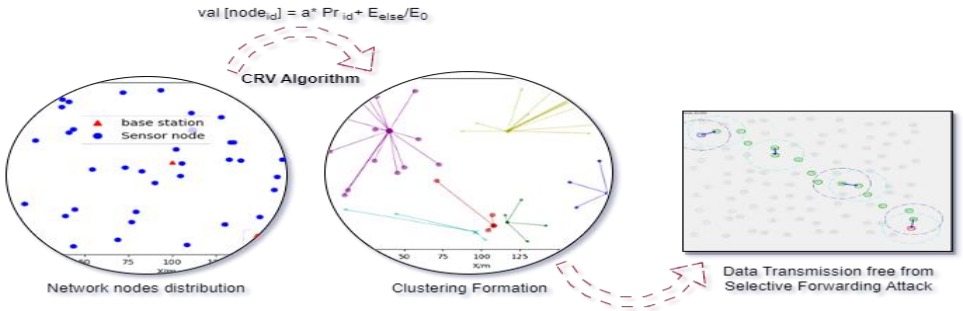
Hriday Banerjee,[1*] Surendra Yadav[2]

1*Research Scholar, computer science and Engineering, Vivekananda Global University (VGU), Sector 36, NRI Colony Rd, V I T Campus, Jagatpura, Seesyawas, Rajasthan 303012

2 Professor, computer science and Engineering, Vivekananda Global University (VGU), Sector 36, NRI Colony Rd, V I T Campus, Jagatpura, Seesyawas, Rajasthan 303012

Abstract

Wireless sensor networks (WSNs) consist of a generous number of small sensor nodes with low energy consumption, poor computing capabilities, and little storage. In large-scale data-gathering WSNs, cluster-based WSNs have been widely used. To identify a selective forwarding attack, the author used Composite Reputation Values (CRVs). The proposed technique has two phases of detection and correction working together to prevent attacks and increase the effective data transmission of the system. There are specific properties of WSN nodes, such as stable neighbors' information, that aid in detecting anomalies. When suspicious activity is detected, nodes report it to the Cluster Head (CH) for further investigation. Using the standard CRV Algorithm, the currently active nodes are grouped. This study also investigates whether or not it is possible to use the leaching method to examine the selective forwarding attack in the WSN. During the experiment, the highest forwarding rate of the CRV algorithm was observed in the range from 0.1000 to 0.9612, with 0.9612 being the highest forwarding rate.0.96



Hriday Banerjee, Research Scholar, computer science and Engineering, Vivekananda Global University (VGU), Sector 36, NRI Colony Rd, V I T Campus, Jagatpura, Seesyawas, Rajasthan 303012

Keywords: Wireless sensor network, Composite reputation value algorithm, Clustering, Selective forwarding attack, Malicious Nodes

Introduction

Several operating systems, such as medical applications and wildfire monitoring, are harmed by node capture attacks in Wireless Sensor Network (WSN).

Malevolent nodes in these assaults seem to be perfectly innocent, but they delete crucial packets on purpose, such as one that records the activities of a different power, making it more difficult to determine whether they are indeed malicious[1]. Current methods for detecting Selective Forwarding Attacks() rely on randomly selecting checkpoints that are reachable between nodes on the forwarding path and are responsible for issuing

classifications as Inspector Node (IN), Cluster Head (CH), and Member Node (MN) according to each supported protocol feature and capability (MNs)[2]. Since CH is assumed to be the most susceptible node and the whole cluster would begin functioning in the network once CH is hacked, node IN is now considered to be listening in on every one of the operations[3]. The IN is trained according to predetermined norms and criteria that ascertain whether or not the CH or MN is malevolent and then behaves accordingly. When the suggested techniques verify the project design, many network simulators can be used as a simulation tools [4]. In most of the methods, two distinct stages detection and correction are factored in as working to combat attacks and nearly taking into consideration the system's efficiency. The attack's impact is mitigated by various techniques, which improve data transfer and enhancement[5]. The CRV algorithm can also be used for clustering and attack detection in WSN.

The CRV of each node is determined by the node's forwarding rate and excess energy, with the node with the highest forwarding rate being chosen as CH and the node with the second highest forwarding rate being chosen as IN.

$$Val\ [node_{id}] = a * Pr_{id} + b * \frac{E_{else}}{E_0}$$

where a and b are parameters and 0 < a < 1, 0 < b < 1, a + b = 1. Initial energy, denoted by E_0, and excess energy, denoted by E_{else}; CRV, represented by Val[$node_{id}$]; forwarding rate, denoted by Pr_{id}. The beta trust model assigns a trust value Tr (0 < Tr < 1) to a node based on its observed behavior of forwarding the packet s times and dropping the packet f times[6], as shown below.

$$T_r = (s + 1)/(s + f + 2)$$

The simulation employs the beta trust model for Prid, where Prid = Forward_pks / Receive_pks.

A WSN is a network system that self-organizes and is distributed in a particular region. A WSN is important in both military and civilian settings. The cheap node's open connectivity and limited computational power make the WSN especially susceptible to various cyberattacks[7]. The hardest to recognize among them is a selective forwarding assault while hostile nodes drop data packets at unpredictable times, in variable quantities, and with selective implies[8]. Data packet loss due to poor channels adds to the challenge, and the malicious node's mastery of the environment means it will do all it can to pass for a good node to avoid detection. Figure 1 shows the processing of the secure CH selection into the secure routing base selection below.

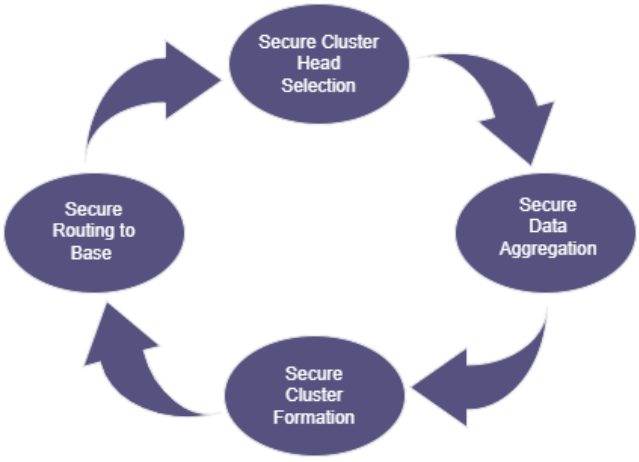


Figure 1. Initialize CH selection [9]

Scientists have previously incorporated Artificial Intelligence (AI) into attack detection techniques. AI-based techniques wiped out malicious nodes by observing harmful activities and contrasting them with appropriate ones [10]. Many AI techniques such as support vector machine and many encryption, decryption algorithms are helpful in creating security mechanisms that enhance the effectiveness of the attack detection technique[11]. Systematically analyzed machine learning in attacker sensing devices and suggested a novel WSN environment to improve attack detection and lower energy usage on the node. However, these AI-based methods include complex learning and modeling procedures for harmful behaviors, which would significantly use network resources if hostile nodes continued to change their behavior ingeniously[12].

The need to protect these networks is emphasized by the fact that WSNs have a sizeable market in both the military and the civilian sectors. Because of their exposed nature and lack of security measures, the networks of sensors in WSNs are susceptible to a broad variety of assaults. The data transfer between sensor devices and sink nodes can be prevented as various attacks, which result in significant damage. The selective forwarding attack is a highly consequential form of internal attack that specifically aims at compromised nodes, compelling them to selectively discard portions or the entirety of sent data[13].

Many reputation-based methods could identify selective forwarding attacks but generally struggled to address the aforementioned issue by comparing the reputations of the nodes with predefined or adaptive criteria. Recently, many scientists have been concentrating on employing various approaches for intrusion detection[14]. Since low-quality channels are a direct effect of their surrounding environment, they are restricted to densely populated regions with many nodes, while malicious acts appear spontaneously. Therefore, a data clustering technique can identify these harmful actions. Some data clustering approaches that have shown a lot of promise in the past for use in attack detection and prevention include K-means, K Nearest Neighbor (KNN), K-medoids,, and Density-Based Spatial Clustering of Programs with Noise (DBSCAN)[15].

Literature Of Review

This section examines the literature on a learning-based safety solution for a selective forwarding attack (SFA) in clustered WSNs, discussing and analyzing the relevant work by different authors.

Khan et al., (2023)[16] provide a well-structured and motivating secure, reliable trust assessment (SDTS) scheme for commercial WSNs to deal with unexpected behavior such as an on-off attack, garnished attack, bad-mouthing attack etc., by using the use of strong trust assessment components like success ratio and node misconduct. The frequency with which sensor nodes exchange data is a key factor in determining SDTS's overall performance. The proposed model (SDTS) incorporates anomalous absorption and dynamic slide distances to better handle a variety of natural calamities and internal attacks. When compared to three recently proposed state-of-the-art methods, SDTS performed better in terms of average energy consumption (0.40 J), throughput (108 Kbps according to the load of 500 nodes with sensors alongside 50% malicious nodes), detection of attacks percentage (90%), detection efficiency (91%), false-positive rate (2.5%), and false-negative rate (2%). Success with this method has been demonstrated through studies.

Ding et al., (2022) [17] simulate a targeted forwarded attack by maliciously intelligent nodes using RL. The author comes up with the double-threshold density peaks clustering (DT-DPC) method to find out about selective forwarding attacks in tough situations. Due to repeated abnormalities, abnormal nodes are suspected of being malicious and segregated. Neighbor voting is used to identify potentially malicious nodes since harmful activities manifest independently and a harsh environment uniformly upsets all nodes. DT-DPC increases network performance even if maliciously intelligent nodes evade detection by an RL algorithm. According to the simulation findings, the false detection rate (FDR) and missing detection rate (MDR) for DT-DPC are both under 1% and 10%, respectively. Network throughput improves by roughly 4% under extreme conditions.

Huang et al., (2022)[18] designed a synthetic immune system based on threat models to detect network attacks. The authors propose a screen-confirm approach to improve detection accuracy while simultaneously basing it on the risk signals obtained from the nodes' power consumption, forwarding rate, connect duration, transmission frequency, and transmission time. The authors choose an appropriate risk threshold and compute the suspect results in the verification phase. The findings are then checked against the threshold established by the authors. The simulation results show that with a 10% malicious ratio, the proposed method still maintains a false rate of detection (FDR) of less than 4.3% and an MDR of close to 1.3%. The suggested solution also has a lower algorithm complexity than previous efforts in this area

Madhuri et al., (2022)[19] proposed a novel intrusion detection system as a certificate revocation approach for efficient node operation and key distribution. A certificate revocation technique has been implemented, invalidating the keys of the malicious nodes. The malicious nodes were unable to transmit with the rest of the network because they lacked valid keys. The suggested method compares Network Simulator-2 with more conventional security algorithms while simulating its use in a variety of situations designed to improve network security. Simulation findings indicated that the suggested approach outperformed current methods in terms of throughput, packet delivery ratio, end-to-end latency, energy usage, and routing overhead.

Xueyan et al., (2022)[20] introduce the Lightweight Selective Forwarding Attack Detection (LSFAD) technique for WSNs. By determining the average packet loss rate of the attack path and comparing it to the normal packet loss rate of the attack path, the LSFAD scheme can identify the path of the SFA and pinpoint the malicious nodes or links responsible for the attack. The LSFAD scheme has a much lower communication cost compared to previous schemes, and it is secure against passive and active selective forwarding attacks, as shown by security and performance studies. The tentative simulation outcomes confirm that the LSFAD scheme can perceive the SFA path with a normal packet loss rate of 0.125 and that malicious nodes or malicious links can be detected and localized by the base station with a normal packet loss rate of 0.025 or higher.

Alkwai et al., (2022)[21] introduce a hybrid clustering method, authentication-based routing protocol, and probabilistic fuzzy chain set for optimizing network data. To defend against the expanding number of vampire attacks that use sophisticated mathematical formulas, this study proposes a solution that uses a fuzzy-based chain rule set. The authenticated routing protocol has improved the safety of routing in a network. Network energy consumption has been minimized thanks to the suggested method (PFCS-ARP_HC). The suggested model has been tested through simulation in NS2, and the results reveal that it achieves 98% throughput, 89% packet delivery ratio, 67% energy usage, 46% latency, 53% control overhead, and 87.9% attack detection ratio.

Premkumar et al., (2022)[22] show how to utilize geographical information to identify and locate a group of opponents using a single or many node IDs. This research presents the scalable and energy-efficient cluster-based anomaly detection (SEECAD) method for spotting DoS assaults and extending network lifetimes without using key management systems. Several various indicators, such as a network's detection rate, its false positive rate, its packet delivery ratio, its overhead, its energy consumption, and the average delay of packets, might be used to evaluate the performance of a network. Authors show that this system is not only more accurate than previous ones but also has a high hit rate when it comes to identifying and identifying the location of many potential threats.

Ding et al., (2021)[23] created a method for detecting selective forwarding attacks called Noise-Based Density Peaks Clustering (NB-DPC). The Cumulative Forwarding Rates (CFRs) from all the sensor nodes combined might reveal attacks that selectively forward data. In order to improve the NB-DPC method, the author eliminated unnecessary processing actions in the Density Peaks Clustering (DPC) algorithm and specified noise points for identifying fraudulent activity. Simulation studies show that the NB-DPC has an extremely low Missed Detection Rate (MDR) and FDR of less than 1%.

Liu et al., (2021)[24] presented a comprehensive technique for identifying selective forwarding attacks under challenging conditions in WSNs. This approach uses a data clustering algorithm (DCA) to filter out bad nodes by grouping them based on their CFRs, and it also incorporates a voting decision mechanism to shield nodes from being labeled as bad in hostile environments. The simulation findings demonstrate that under a local changeable hostile environment, the system achieves a 1% FDR and a 5% MDR with minimal energy usage in WSNs.

Janakiraman et al., (2021)[25] described a Markov Process-based Opportunistic Trust Factor Estimation Mechanism (MPOTFEM) that is developed for attaining optimum CH selection to improve the likelihood of preserving network longevity and power constancy. It is suggested to use MPOTFEM to guarantee effective CH selection and extend the WSNs' operational lifespan. The projected MPOTFEM depends on the strengths of the Markov process to compute the Opportunistic and Trust factors, which evaluate the extreme probability of nodes that might be chosen as the CH via the examination of a variety of transition states in the networks upon which they operate. By analyzing the proposed MPOTFEM, the author finds that it significantly increases the network's lifetime.

Wei et al., (2021)[26] suggested a trust with a negative binomial distribution, taking energy constraints into account. The suggested approach is minimal in size and power consumption, making it ideal for use with discrete healthcare sensors. Simulations demonstrate that it can efficiently handle internal threats while still conserving power.

The paper's authors suggest studying how to determine the size of ΔT as the next step for their research. However, while a lower ΔT will have a negative impact on the effectiveness of mischievous node detection, a larger ΔT would have a negative impact on the storage capacity of sensor nodes.

Gautam et al., (2021)[27] proposed a new trust model based on a ranking mechanism for recommending a safe neighbor node among a network's nodes. The author employs a voting mechanism and a combination of the AHP and TOPSIS approaches to determine the relative merits of the several nearby options. The paper's case study shows how the recommended approach, which is designed to optimize defense against internal threats, works in practice. The advantage of the suggested strategy has been shown by a complex analysis. The suggested approach has a time complexity of O(n2), whereas the comparable algorithm has a growth rate of O(n2).

Li et al., (2020)[28] presented a method of grouping nodes in a clustered WSN into bad, suspicious, and good categories. The suggested approach cuts out bad nodes from the network to prevent them from launching selective forwarding attacks. Authors plan uses a non-cooperative game with partial knowledge to coerce suspicious nodes toward increasing their forwarding rates. Attackers' expected income and faith in the game are reduced by the structure of rewards and punishments in place. The suggested clustering strategy will compel suspect nodes to forward packets to avoid detection. This demonstrates that the game between trusted nodes and questionable ones has reached its Nash equilibrium. Simulations indicate that the suggested technique increases network performance and extends network longevity.

Fu et al., (2019)[29] proposed a data clustering technique (DCA-SF) for spotting attacks that selectively convey data. By grouping their CFRs, it is possible to identify hostile CHs that have initiated selective forwarding assaults and then isolate them. By dynamically adjusting the DCA parameters (Eps, Minpts), the DCA-SF algorithm's performance has been improved. The results of the model illustrate that the DCA-SF utilizes very small power while having a little missed detection rate of just 1.04% and a low FDR of only 0.42%.

Robinson et al., (2019) [30] established a threshold rate and fuzzy logic-based power-conscious routing strategy for WSN to reduce power consumption. The possibility values of each node in a WSN are determined by the amount of energy each node still has, and these values are then used to elect the cluster leaders. The current network phase's mean energy is determined by adding the energy of all remaining nodes. As packets are sent from cluster members to the leader through single-hop communication, the leader is more likely to be a high-probability node. The cluster's epicenter relays information to its destination via fuzzy management and multi-hop communication. Three variables are used in fuzzy control: queue length, distance to the base station, and node energy. Experiments show that MLSEEP, an energy-efficient cluster-based routing system, outperforms current protocols by supplementing such approaches.

Problem Formulation And Objectives

In this study, the author focuses on investigating the effects of a clustering algorithm in WSNs with a good forwarding rate, which can help find and stop the selective forwarding attack. SFA is one in which hostile nodes alter the regular operation of the network by dropping or forwarding packets selectively. The goal is to provide a learning-based security method for clustered WSNs that can identify and prevent such attacks. The method should help to recognize the traits and patterns associated with selective forwarding attacks, allowing for continuous monitoring and protection. This study intends to improve the security and resilience of clustered WSNs in the face of selective forwarding attacks, paving the way for more trustworthy and dependable network operations.

The objectives of the given study are:

- To optimize the CRV calculation algorithm to achieve faster and more accurate computation of the Composite Reputation Value, taking into account the Senior Node (SN) data and other relevant variables.
- To implement a novel and efficient initial-level development strategy for Senior Nodes (SN) that enables them to quickly establish a strong network presence and facilitate smooth cluster formation.
- Enhance the Neighboring List generation process and commitment key assignment for each sensor node (N) in the network to ensure robust and secure communication within clusters.
- Develop and deploy an intelligent and adaptive clustering network with a refined CRV-based clustering head, enabling it to resist selective forwarding attacks.

Research Methodology

In this section, various steps of the suggested methodology are discussed. Figure 2 shows a flowchart of the method that was meant to be used, from the first stage of SN development to the source authenticity valid key by clustering networks below with guard nodes.

In the first step, the network gets equipped with a collection of wireless sensor nodes (SN) that can monitor and record activity in their immediate vicinity. After the sensor nodes are set up, they compile a list of other nodes within their range of communication and generate commitment keys to ensure private conversations between them. After this step, the network clusters form groups of similar sensor nodes for easier management and coordination. To determine which nodes should serve as Cluster Heads (CHs), we use the Cluster-Head Rotation Value (CRV) technique. A Guard Node is tasked with securing the confidentiality, integrity, and validity of data within a cluster by acting as a gateway and enforcing communication rules. Node S sends a route request to Node D, the destination, to begin the connection setup process. The commitment key is checked at the designated node Z after the request has made its way across the network. The route request is then refreshed and sent out to the local nodes if it still holds water. Along the way to the final or intermediate nodes, the route request checks the validity of the source node. Upon receiving confirmation that the source is legitimate; the final destination or intermediaries will send a route reply outlining the best way to get there. A Cluster Head's performance can be assessed in part by measuring its forwarding efficiency, which is calculated as a percentage of the total forwarding rate. To evaluate the efficacy of data forwarding and the efficiency of the clustering algorithm, the author looked at CRVs. Missing Detection Rate (MDR) and False Detection Rate (FDR) calculations are also used to evaluate the system's performance in spotting network events and anomalies.

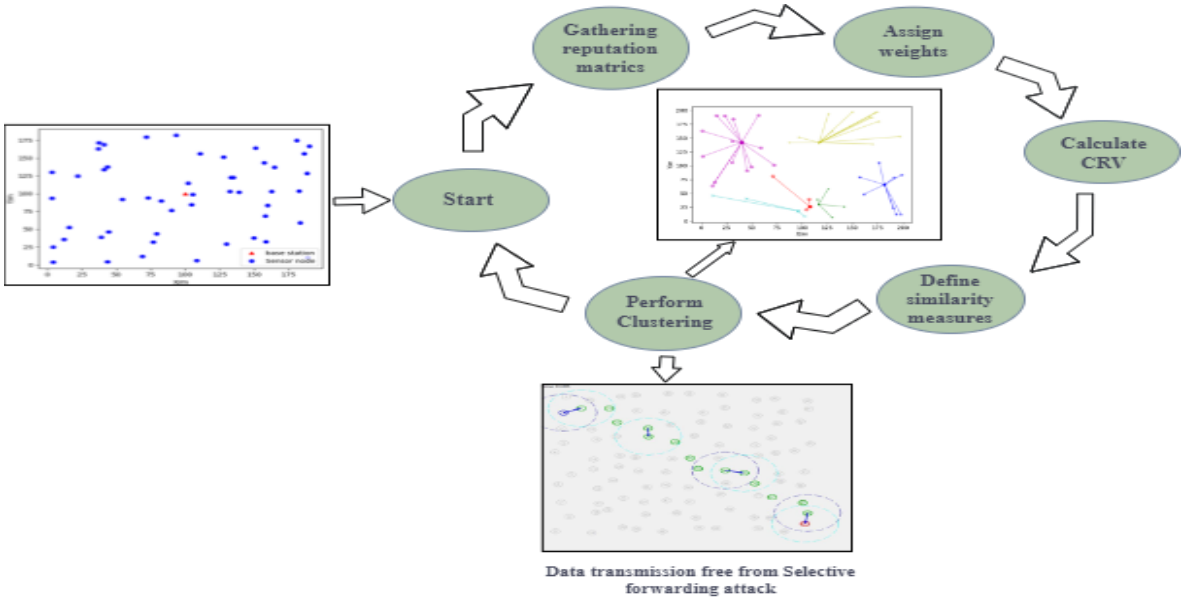


Figure 2: Composite Reputation Value Model for Selective Forwarding Attack Prevention

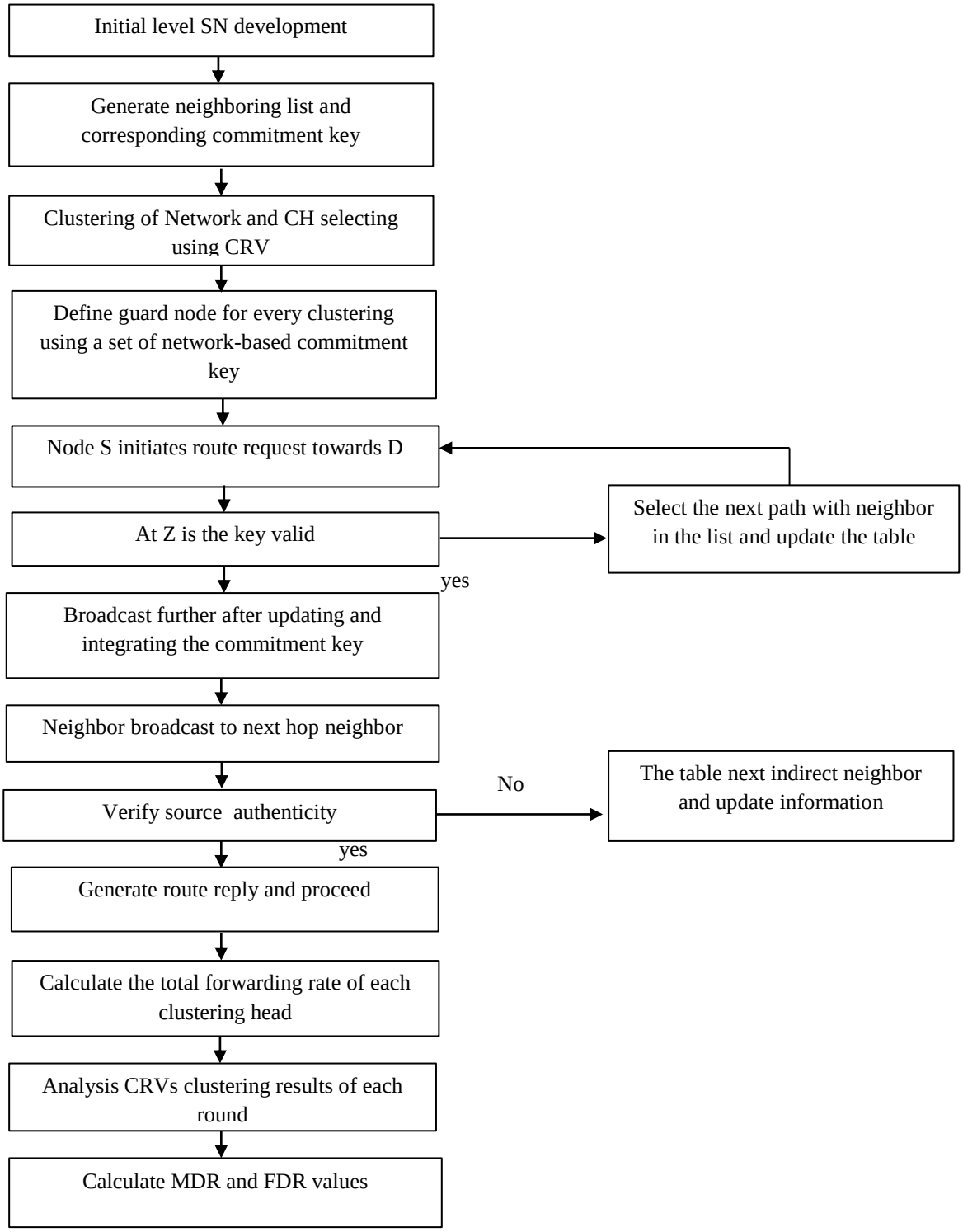


Figure 3. Proposed Methodology

The algorithm for the suggested methodology is given below :

ALGORITHM:	**C**omposite **R**eputation **V**alue **A**lgorithm for **S**elective **F**orwarding **A**ttack **P**revention

Start

1. Input variable SN → Senior node, CRV → Composite Reputation Value
2. Initial level SN development.

3. For each N(sensor node) generate a Neighboring list and commitment key.
4. Create a clustering network and clustering head using the CRV algorithm.
5. Define G (guard node) for every cluster using the Network based communication rule.
6. Node S (source node) initiates route request towards D(Destination node).
7. **At** Z (node) **If** (key is valid):
8. Update and integrate the commitment key for each neighbor (Z)
9. **Else,**
10. Select the next path from the list (i) and update the table.
11. **End**
12. For each Neighbor (Z) broadcast R to its next hop neighbor. R→ set of route request
13. Verify the authenticity of the source node(S) for each set of received route requests (R_received).
14. **If** (source is valid):
15. Generate route, reply, and proceed.
16.
17. **Else,**
18. Update information and shows the table, next indirect neighbor.
19. **End**
20. Calculate the total forwarding rate of each CH.
21. Analyze CRV clustering results in each round.
22. Calculate MDR and FDR values.
23. **End**

End

Results

A. An Example of Simulation

Figure 4 shows the simulation diagram, which will further present clustering and data transmission. It depicts the nodes before clustering in the network. This diagram shows how sensor nodes and base stations must be present in the network before clustering or data transmission can take place.

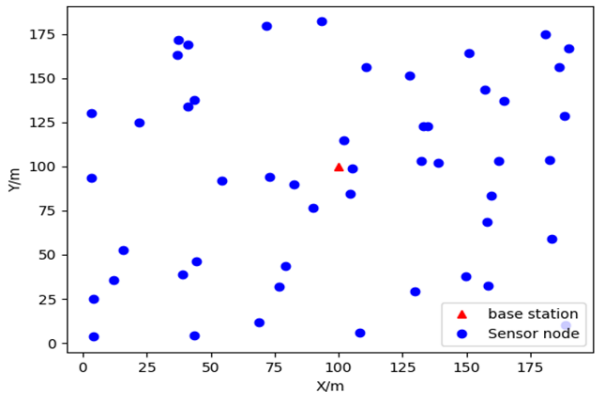


Figure 4: Network nodes distribution

Figure 5 shows clusters that formed when configuring the optimal system. Nodes are arranged into clusters using CRV algorithm and CH is chosen during the cluster construction process. At the end of each simulation, new clusters are formed with new CHs.

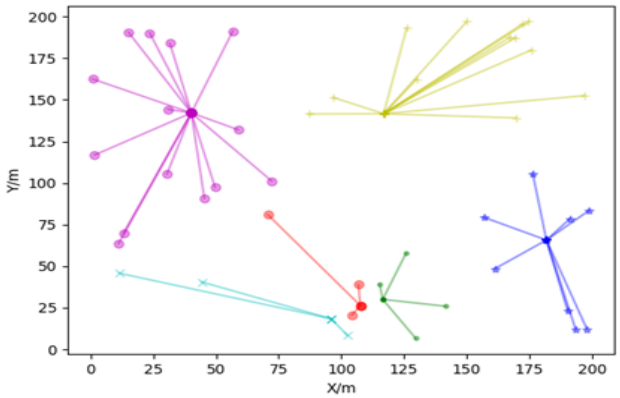


Figure 5: Clustering Formation

Proposed CRV's forwarding ratio. The speed at which data packets are delivered or conveyed within the cluster is known as its forwarding rate. The greatest forwarding rate is 0.9612, with the values ranging from 0.1000 to 0.9612.

Cumulative Forwarding Rates (CRF's) [29] forwarding rate. Like the proposed CRV, it evaluates the speed or effectiveness of data packets sent across nodes in a cluster. The maximum forwarding rate is indicated by the value of 0.9402. Values are in the series of 0.1468 to 0.9402.

Table 1 displays the outcomes of a random generator for total forwarding rates. The global forwarding rates of CHs are calculated by simulation.

Table 1: CH total forwarding rate

No. of CH	Forwarding rate (CRV)	Forwarding rate (CRF) [29]
1	0.8850	0.8755
2	0.6599	0.6299
3	0.70333	0.9074
4	0.502	0.8057
5	0.8211	0.8052
6	0.9612	0.9402
7	0.8014	0.9030
8	0.9111	0.1468
9	0.1000	0.8456

Table 2 (a) shows how each CH was classified after a final round of analysis using the proposed CRV clustering method. For each CH, the table indicates whether or not clusters were created. Cluster development is indicated by a value of 1, while the absence of clusters is indicated by a value of 0.

The fact that it is stated that CH9 is part of a group with zero others indicates that there were no other nodes in the first round that clustered with CH9. CH9 failed to form any clusters with any of the other sensor nodes on the first attempt.

Furthermore, the CH9 had significant packet loss in the first phase. This indicates that CH9 had difficulties during data transmission, leading to a high rate of packet losses.

Table 2 (a): Proposed CRV clustering results in each round.

ROUNDS / CH	1	2	3	4	5	6	7	8	9	10	...	49	50
1	1	1	1	1	1	1	1	1	1	1	...	0	1
2	1	1	1	1	1	1	1	1	1	1	...	0	0
3	1	1	1	0	1	1	1	1	1	1	...	0	0
4	1	1	1	0	1	1	0	1	1	1	...	0	0
5	1	1	1	0	0	1	0	1	1	1	...	0	0
6	0	0	1	0	0	0	0	0	0	1	...	0	0
7	0	0	1	0	0	0	0	0	0	1	...	0	0
8	0	0	0	0	0	0	0	0	0	1	...	0	0
9	0	0	0	0	0	0	0	0	0	1	...	0	0

The results of the CRF[29] clustering method's final analysis on each CH are shown in Table 2 (b).

Table 2 (b): CRF [29] clustering results in each round s

ROUNDS / CH	1	2	3	4	5	6	7	8	9	10	...	49	50
1	1	1	1	1	1	1	1	1	1	1	...	1	1
2	1	1	1	1	1	0	0	0	0	0	...	0	0
3	1	1	1	1	1	1	1	1	1	1	...	1	1
4	1	1	1	1	1	1	1	1	1	1	...	1	1
5	1	1	1	1	1	1	1	1	1	1	...	1	1
6	1	1	1	1	1	1	1	1	1	1	...	1	1
7	1	1	1	1	1	1	1	1	1	1	...	1	1
8	0	0	0	0	0	0	0	0	0	0	...	0	0
9	1	1	1	1	1	1	1	1	1	1	...	1	1

B. Results of Detection Analyzed against Other DCAs

Figure 6 demonstrates that the proposed CRV outperforms K-means and DBSCAN in terms of MDR and that all three of these DCAs have O(log n) time complexity (m).

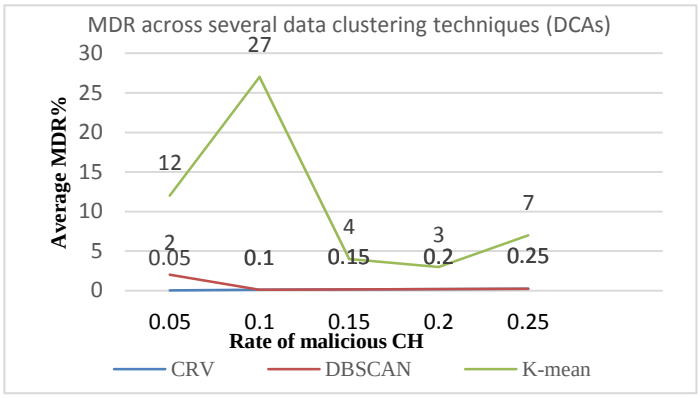


Figure 6: Analyzing MDR across several data clustering techniques

(DCAs)

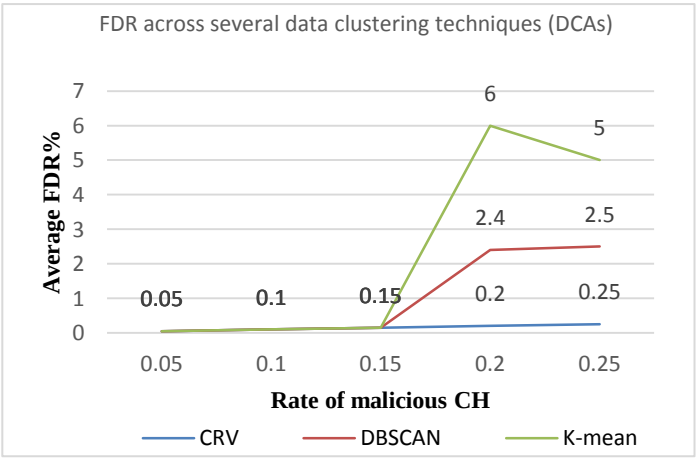


Figure 7 shows a comparison of FDRs across several DCAs. Compared to K-means and DBSCAN, the proposed CRV's FDR yields superior results.

Figure 7: Analyzing FDR across several data clustering techniques (DCAs)

Conclusion

In summary, this study has provided a technique for defending cluster-based Wireless Sensor Networks (WSNs) against attacks that involve selective forwarding. WSNs have become popular for large-scale data collection projects because of their self-organizing nature and abundance of inexpensive, low-power sensor nodes. The suggested method makes use of the CRV (Cluster-based Reliable Voting) algorithm to detect attacks and uses a two-stage detection and correction procedure to improve the system's performance. The suggested approach uses information from reliable neighbors and network node cooperation to spot malicious activity. The working nodes are grouped together using the CRV technique, allowing for quicker and more effective information exchange within the network. An experiment was run to examine the forwarding rate of each Cluster Head (CH) in order to assess the effectiveness of the suggested approach. The forwarding rate is a metric for assessing a CRV's ability to send data packets between cluster nodes. The outcomes were 0.1000 to 0.9612, with 0.9612 being the highest forwarding rate attained. The results of this study show that the suggested CRV algorithm can thwart selective forwarding attacks on cluster based WSNs. The method improves the security and dependability of data transmission in WSNs by identifying and mitigating harmful network activity. The use of reliable neighbor data and cooperative node actions increases the system's resilience and resistance to malicious behavior. To explore the scalability and applicability of the suggested method in larger WSN deployments, additional research can be done in the future. By investigating the potential addition of additional security features like intrusion detection systems or encryption algorithms, cluster based WSNs can also be made more secure.

Acknowledgments

The authors of this work would like to say their sincere appreciation to all of those who made valuable contributions to this research article. The invaluable contributions and assistance provided by the individuals were vital in the effective culmination of this research endeavor.

References And Notes

[1] 1. W. Yuanming. An energy-balanced loop-free routing protocol for distributed wireless sensor networks. *International Journal of Sensor Networks* **2017**, 23(2), 123-31.

[2] 2. Y. Liu, Y. Wu. A key pre-distribution scheme based on sub-regions for multi-hop wireless sensor networks. *Wireless Personal Communications* **2019**, 1091161-80.

[3] 3. Y. Liu, M. Ma, X. Liu *et. al.* Design and analysis of probing route to defense sink-hole attacks for Internet of Things security. *IEEE Transactions on Network Science and Engineering* **2018**, 7(1), 356-72.

[4] 4. Z. Lu, Y.E. Sagduyu, J.H. Li In *2015 IEEE Conference on Computer Communications (INFOCOM)*; IEEE: 2015, p 253-61.

[5] 5. H. Zhou, Y. Wu, L. Feng, D. Liu. A security mechanism for cluster-based WSN against selective forwarding. *Sensors* **2016**, 16(9), 1537.

[6] 6. Y. Hu, Y. Wu, H. Wang. Detection of insider selective forwarding attack based on monitor node and trust mechanism in WSN. *Wireless Sensor Network* **2014**, 6(11), 237.

[7] 7. C. Pu, S. Lim. A light-weight countermeasure to forwarding misbehavior in wireless sensor networks: design, analysis, and evaluation. *IEEE Systems Journal* **2016**, 12(1), 834-42.

[8] 8. J. Ren, Y. Zhang, K. Zhang, X. Shen. Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks. *IEEE Transactions on Wireless Communications* **2016**, 15(5), 3718-31.

[9] 9. S. Singh, H.S. Saini. Learning-based security technique for selective forwarding attack in clustered WSN. *Wireless Personal Communications* **2021**, 118(1), 789-814.

[10] 10. B. Jiang, G. Huang, T. Wang *et. al.* Trust based energy efficient data collection with unmanned aerial vehicle in edge network. *Transactions on Emerging Telecommunications Technologies* **2022**, 33(6), e3942.

[11] 11. Y. Chen, S. Tang, N. Bouguila *et. al.* A fast clustering algorithm based on pruning unnecessary distance computations in

DBSCAN for high-dimensional data. *Pattern Recognition* **2018**, 83375-87.

[12] 12. J. Gan, Y. Tao In *Proceedings of the 2015 ACM SIGMOD international conference on management of data* 2015, p 519-30.

[13] 13. M.S. Yousefpoor, E. Yousefpoor, H. Barati *et. al.* Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review. *Journal of Network and Computer Applications* **2021**, 190103118.

[14] 14. A. Rodriguez, A. Laio. Clustering by fast search and find of density peaks. *science* **2014**, 344(6191), 1492-96.

[15] 15. H. El Alami, A. Najid. ECH: An enhanced clustering hierarchy approach to maximize lifetime of wireless sensor networks. *Ieee Access* **2019**, 7107142-53.

[16] 16. T. Khan, K. Singh, K. Ahmad, K.A.B. Ahmad. A secure and dependable trust assessment (SDTS) scheme for industrial communication networks. *Scientific Reports* **2023**, 13(1), 1910.

[17] 17. J. Ding, H. Wang, Y. Wu. The Detection Scheme Against Selective Forwarding of Smart Malicious Nodes With Reinforcement Learning in Wireless Sensor Networks. *IEEE Sensors Journal* **2022**, 22(13), 13696-706.

[18] 18. X. Huang, Y. Wu. Identify selective forwarding attacks using danger model: Promote the detection accuracy in wireless sensor networks. *IEEE Sensors Journal* **2022**, 22(10), 9997-10008.

[19] 19. K. Madhuri. A New Level Intrusion Detection System for Node Level Drop Attacks in Wireless Sensor Network. *Journal of Algebraic Statistics* **2022**, 13(1), 159-68.

[20] 20. C. Xueyan, Z. Zhiming, Y. Wei *et. al.* Lightweight Selective Forwarding Attack Detection for Wireless Sensor Networks. *Journal of Frontiers of Computer Science & Technology* **2022**, 16(4), 865.

[21] 21. L.M. Alkwai, A.N. Mohammed Aledaily, S. Almansour *et. al.* Vampire attack mitigation and network performance improvement using probabilistic fuzzy chain set with authentication routing protocol and hybrid clustering-based optimization in wireless sensor network. *Mathematical Problems in Engineering* **2022**, 2022.

[22] 22. M. Premkumar, S. Ashokkumar, V. Jeevanantham *et. al.* Scalable and Energy Efficient Cluster Based Anomaly Detection against Dos Attacks in WSN. **2022**.

[23] 23. J. Ding, H. Zhang, Z. Guo, Y. Wu. The DPC-based scheme for detecting selective forwarding in clustered wireless sensor networks. *IEEE Access* **2021**, 920954-67.

[24] 24. Y. Liu, Y. Wu. Employ DBSCAN and neighbor voting to screen selective forwarding attack under variable environment in event-driven wireless sensor networks. *IEEE Access* **2021**, 977090-105.

[25] 25. S. Janakiraman, M.D. Priya, S.S. Devi *et. al.* A Markov process-based opportunistic trust factor estimation mechanism for efficient cluster head selection and extending the lifetime of wireless sensor networks. *EAI Endorsed Transactions on Energy Web* **2021**, 8(35), e5-e5.

[26] 26. Z. Wei, S. Yu, W. Ma. Defending against internal attacks in healthcare-based WSNs. *Journal of Healthcare Engineering* **2021**, 2021.

[27] 27. A.K. Gautam, R. Kumar. A trust based neighbor identification using MCDM model in wireless sensor networks. *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)* **2021**, 14(4), 1336-51.

[28] 28. Y. Li, Y. Wu. Combine clustering with game to resist selective forwarding in wireless sensor networks. *IEEE Access* **2020**, 8138382-95.

[29] 29. H. Fu, Y. Liu, Z. Dong, Y. Wu. A data clustering algorithm for detecting selective forwarding attack in cluster-based wireless sensor networks. *Sensors* **2019**, 20(1), 23.

[30] 30. Y.H. Robinson, E.G. Julie, R. Kumar, L.H. Son. Probability-based cluster head selection and fuzzy multipath routing for prolonging lifetime of wireless sensor networks. *Peer-to-Peer Networking and Applications* **2019**, 121061-75.