International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

SFA-BCPF: Selective Forwarding Attacks in WSN With Bayesian Confidence-Based Packet Forwarding Algorithm

[1]Dr K. Soundarraj

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: Wireless Sensor Networks (WSNs) play a pivotal role in various applications, ranging from environmental monitoring to military surveillance. However, their vulnerability to malicious attacks, particularly Selective Forwarding Attacks (SFAs), poses a significant challenge to the reliability and integrity of the transmitted data. SFAs involve compromised sensor nodes selectively dropping or delaying certain packets, leading to the degradation of network performance and undermining the overall efficiency of WSNs. This research proposes a novel approach to counteract SFAs by introducing a Bayesian Confidence-Based Packet Forwarding Algorithm (BCPF). The algorithm leverages Bayesian probability theory to dynamically assess the trustworthiness of each sensor node in the network. By considering factors such as historical behavior, communication patterns, and data integrity, the algorithm assigns a confidence level to each node. Nodes with higher confidence levels are prioritized for packet forwarding, while those with lower confidence levels are subjected to additional scrutiny or avoided altogether. The Bayesian Confidence-Based Packet Forwarding Algorithm aims to enhance the robustness of WSNs against SFAs by promoting the forwarding of packets through nodes with proven reliability. This research contributes to the ongoing efforts to fortify WSNs against emerging security threats, fostering their continued deployment in critical applications.

Keywords: *BCPF, SFAs, Security, Trustworthy, Wireless Sensor Networks*

1. Introduction

Because of its dispersed architecture for data collection, processing, and transmission from distant and possibly dangerous locations, WSNs have become a critical technology in many sectors [1]. These networks have a variety of applications, including healthcare, industrial automation, environmental protection, and military surveillance [2]. However, the widespread use of WSNs introduces security vulnerabilities that, if unchecked, may jeopardize the veracity of the data gathered [3]. For WSNs, the SFA poses a severe security concern. Compromise sensor nodes choose which packets to delete or delay in this attack, leading in data distortion and a loss in overall network performance [4-6]. These kind of assaults are very dangerous, especially in mission-critical systems where up-to-date data is crucial.In this paper, a novel Bayesian Confidence-Based Packet Forwarding Algorithm is proposed as a solution to the issue of SFAs in WSNs. SFAs often exploit the cooperative characteristic of sensor nodes since they work together to convey data to a designated sink. Once hostile nodes enter the network, they may purposefully disrupt this collaboration, resulting in a domino effect on network efficiency and data flow [7]. The proposed Bayesian Confidence-Based Packet Forwarding Algorithm leverages Bayesian probability theory to dynamically evaluate the dependability of each sensor node [8]. The program takes into account a broad variety of characteristics, including previous node behavior, communication patterns, and data integrity during transmission [9-11]. By assigning confidence levels to certain nodes, the system enables intelligent packet routing. This prioritizes nodes with higher confidence, which reduces the impact of SFAs [12-13]. This research [14] addresses both the immediate issue of SFAs and the broader discussion of how to make WSNs safer. The Bayesian Confidence-Based Packet Forwarding Algorithm [15] is one possible method for fortifying WSNs against emerging security threats. This algorithm is capable of adapting to changing network conditions and detecting anomalous activity. By performing extensive simulations and then confirming the findings experimentally, the suggested technique may minimize SFAs and make WSN more robust in real-world circumstances [16-17].

This paper is organized as follows; Section 2 discussed with the existing author concepts. Section 3, presents the SFA-BCPF model. The simulations and results of the study are reviewed in Section 4. Finally, Section 5 delves into the conclusion and potential future study.

1.1 Motivation of the paper

The rising threat of SFAs, as well as the critical function that WSNs serve in many applications, are driving factors behind this research. SFAs, in which damaged sensor nodes selectively change the packets delivered,

[1]*Assistant Professor of Computer Science, Sri Ramakrishna Mission Vidyalaya College of Arts and science, Coimbatore 641020, soundarraj28@gmail.com*

decrease data integrity and overall network performance. The Bayesian Confidence-Based Packet Forwarding Algorithm is presented in this study as a unique technique to dynamically evaluate sensor node trustworthiness based on characteristics such as historical behavior, communication patterns, and data integrity. The technique improves WSN resistance against SFAs by selecting nodes with greater confidence levels for packet forwarding, responding to changing network conditions, and detecting odd behavior.

2. Background Study

Kaur, H. et al. [1] Sensor nodes in a wireless sensor network collect data and relay it to a central station. One active form that impacts network performance was selective forwarding. Here, the threshold values provide the basis for the creation of the innovative method. Matlab was used to accomplish the suggested method.

Li, Y., & Wu, Y. [5] the author looked at a periodic detection method for SFA in unstable channels that were based on DBSCAN. A non-cooperative game model with partial information was developed by the author to compensate for the lack of warnings in the scheme and the restricted resources of WSNs. This model has hostile nodes alongside conventional ones. The possibility of the game reaching the Nash equilibrium might be shown. By altering the probability of its strategy or behavior, no Nash equilibrium participant may increase the expected payoffs.

Lyu, C. et al. [7] this author's presented SelGOR, an efficient method that the author developed with the goal of providing the Internet of Things (IoT) with data transmission that was both legitimate and reliable. To increase the dependability of data transmission in WSNs, SelGOR, a trust-based geographic opportunistic routing algorithm, uses the SSI-based trust model. The author looked at the current authentication methods for DoS defense and discovered that they were either too computationally expensive or too unserviceable to work with opportunistic routing in WSNs.

Siasi, N. et al. [11] these authors research proposes an effective method for protecting WSN against SFA in LEACH routing. In order to provide a recovery technique that was effective against single or many concurrent attacks on the network, this paper makes use of diversity coding and network coding strategies. Improved throughput, near-instantaneous recovery times, and a little increase to the network's redundant connection were all characteristics of the suggested approach.

Venkata Krishna, P., & Obaidat, M. S. [13] the condenser's back pressure played a major factor in the thermal power plant's efficiency. The goal of this research was to develop process models for continuous condenser back pressure monitoring using multivariate adaptive regression spline, polynomial regression, and multiple linear regressions. A faulty process or pressure sensor to blame if there was a large discrepancy between the model's projected and measured pressures.

Yin, R. et al. [15] These authors provided a new model of scale-free network cascading failure that accounts for selective forwarding attack and find the impact law of SFA on network cascading failure in this context. When a multi-node failure happens at random and cascades, the results show that a selective forwarding attack may reduce the amount of connection loss in scale-free networks.

2.1 Problem definition

Despite their widespread use, WSNs pose a serious threat to the security and reliability of data transferred over them due to their vulnerability to attacks like Selective Forwarding attacks. The performance and overall efficiency of WSNs are negatively impacted by SFAs, which appear as infected sensor nodes altering packets selectively. Concerning applications spanning from environmental monitoring to military surveillance, the data integrity of WSNs is at risk, which poses a serious challenge. This paper presents a groundbreaking

3. Proposed Methodology

The proposed Bayesian Confidence-Based Packet Forwarding Algorithm, which aims to fix the problem of WSNs being susceptible to SFAs. To guarantee the algorithm's resilience and efficacy, it is crucial to use rigorous methodology and use suitable materials. The SFA-BCPF model flow chart has represented at figure 1.

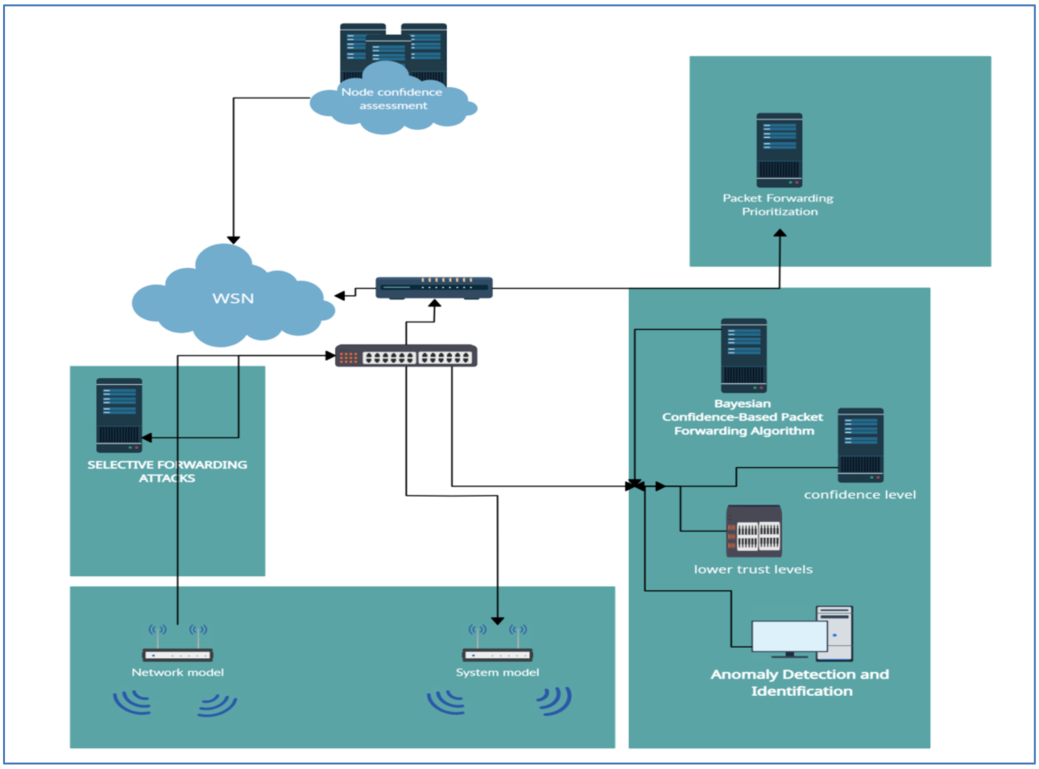
Node confidence assessment
Packet Forwarding Prioritization
WSN
SELECTIVE FORWARDING ATTACKS
Bayesian Confidence-Based Packet Forwarding Algorithm
confidence level
lower trust levels
Network model
System model
Anomaly Detection and Identification

Fig 1: SFA-BCPF model architecture

3.1 System model

To build a system model that includes all of the necessary components and equations for the proposed Bayesian Confidence-Based Packet Forwarding Algorithm and its integration into the WSN.

To formalize the proposed Bayesian Confidence-Based Packet Forwarding Algorithm and its implementation into the WSN, a system model that includes the main components and equations that regulate the algorithm's capabilities must be built.

Each sensor node in the WSN, denoted as$N$, has a unique set of characteristics, including its communication patterns (CP_{ni}), data integrity (DI_{ni}), and historical behavior (HB_{ni}). Using these elements and the following equation, the Bayesian Confidence Level (BC_{ni}) is dynamically generated for each node:

$BC_{ni} = P(HB_{ni}, CP_{ni}, DI_{ni}$ ------- (1)

Node behavior, communication patterns, and data integrity are all factors in the Bayesian probability function, which is represented here by$P$.

The estimated confidence levels are used to inform the packet forwarding choice. According to this rule, nodes with greater confidence levels are given precedence when it comes to forwarding packets:

$If\ BC_{ni} >$ Threshold, then forward packet through n_i -------- (2)

The program also uses a dynamic threshold adjustment method to respond quickly and adapt to changing network circumstances while identifying abnormal activity.

With these equations and decision rules included in the overall system model, the WSN's Bayesian Confidence-Based Packet Forwarding Algorithm is built upon, with the goal of making the network more secure and resistant to SFAs.

3.2 Network model

To construct a network model that includes all the necessary equations and parameters for the proposed BCPF to function in a Wireless Sensor Network.

Envision a WSN with N nodes serving as sensors, represented as nini, where ii is an integer between 1 and N . The procedure determines the Bayesian Confidence Level (BC_{ni}), which is used to compute the packet forwarding probability for each node n_i. Let P_{ni} represent this probability. The total likelihood of packet forwarding at the network level ($P_{network}$) is calculated by adding together the probabilities of each node while taking their confidence levels into account:

$P_{network} = \frac{1}{N}\sum_{i=1}^{N} P_{ni}$ --------- (3)

The technique for adjusting the algorithm's threshold encapsulates the dynamic adaptation to changing network circumstances. To react to changing conditions, the threshold (Threshold) is changed dynamically using the network's performance measurements and previous behavior:

$\text{Threshold} = f(\text{Network History}, \text{ Performance Metrics})$ ------- (4)

Next, the computed probability at the network level is used to direct the packet forwarding choice, giving nodes with higher confidence levels preference:

$\text{If } P_{\text{network}} > \text{Threshold}, \text{ then forward packet through the network}$ ------- (5)

This network model contains equations for node-level confidence, network-level probability, and dynamic threshold change to provide the foundation for the WSN's Bayesian Confidence-Based Packet Forwarding Algorithm. The algorithm tries to increase the network's defenses against SFAs, promote reliable packet forwarding, and adapt to changing network conditions by executing these techniques. The ultimate objective is to strengthen and safeguard WSN.

3.3. Packet Forwarding Prioritization

The Bayesian Confidence-Based Packet Forwarding Algorithm uses Bayesian probability theory to dynamically evaluate the confidence levels of sensor nodes in order to prioritize packet forwarding referred by Naderi et al. (2023). The more trustworthy the nodes are, the higher their priority is. When forwarding data packets inside a WSN, prioritizing nodes with higher confidence levels decrease the risk of data integrity being compromised, particularly when dealing with SFAs. Nodes with stable dependability levels are given more weight, whereas nodes with erratic or decreasing confidence levels may have their weight reduced, thanks to this adaptive system that permits real-time modifications. To avoid SFAs and improve the WSN's overall security and resilience, the algorithm prioritizes dependable nodes.

3.4 Bayesian Confidence-Based Packet Forwarding Algorithm

An innovative method for protecting WSNs against SFAs is the Bayesian Confidence-Based Packet Forwarding Algorithm. SFAs jeopardize the integrity and dependability of transmitted data by compromising sensor nodes, which causes them to discard or delay certain packets. In order to dynamically determine which sensor nodes in the network are trustworthy, this technique makes use of Bayesian probability theory. For the algorithm to function, it must take into account critical parameters linked to each sensor node, such as its past actions, communication patterns, and data integrity. A confidence level (BC_{ni}) is computed for each node nini based on these parameters. To provide a thorough assessment of each node's reliability, to use the Bayesian probability function to combine previous probabilities of their behavior, communication patterns, and data integrity. The algorithm's proactive approach to encourage data transmission via nodes with demonstrated dependability is seen in its prioritization of nodes with higher confidence ratings for packet forwarding. Minimizing the possible effect of rogue nodes on network performance is achieved by subjecting or bypassing nodes with lower trust levels.

A stochastic packet forwarding algorithm's SPA basic tenet is that, in FANETs, a number of different real-time network parameters should be considered together while selecting forwarding nodes.

After that, using Eq. 6, the packet sender standardizes the FT's network measurements,

$X_{ij}^{*} = \frac{max\{X_j\}-X_{ij}}{max\{X_j\}-min\{X_j\}} \times a_j + (1 - a_j)$ -------- (6)

$i = 1,2, \ldots, N, \quad j = 1,2, \ldots, M$ ------- (7)

It generates a normalized matrix that contains the value of the network metrics. If $Xj = 1$ and a_j = 1.0, then the range of values for the jth network metric is controlled by the efficiency coefficientαj. The goal of creating aj is to adjust the influence of the jth network metric based on personal taste. The sender of the packet then uses Eq. 8 to determine the entropy of the jth network metric,

$Ent_j = -\frac{1}{1nN} \sum_{i=1}^{N} (F_{ij}. 1n\, F_{ij}), \; j = 1,2, \ldots, M$ --------- (8)

F_{ij} Represents the proportion of the jth network metrics associated with the candidate node for forwarding n_i.

$F_{ij} = \frac{X_{ij}^{*}}{\sum_{k=1}^{N} X_{kj}^{*}}, \quad j = 1,2, \ldots, M$ -------- (9)

According to the entropy concept, the entropy weight of the jth network metrics is it is possible to express Y_j as

$r_j = \frac{1-Ent_j}{\sum_{k=1}^{M}(1-Ent_k)}, \quad j = 1,2, \ldots, M$ ------- (10)

So, Aua_i^{fwd}, the candidate node's forwarding availability, calculated by taking the normalized value of the metrics and the entropy weight of the network data.

$Aua_i^{fwd} = \sum_{j=1}^{M} (r_j. X_{ij}^{*}), \; i = 1,2, \ldots, N$ --------- (11)

Pro_i^{fwd}, the forwarding probability of the forwarding candidate nodeni, may finally be obtained by means

$Pro_i^{fwd} = 1 - \frac{Aua_i^{fwd}}{\sum_{k=1}^{N} Auk_k^{fwd}}$ --------- (12)

Step three involves the packet sender using a stochastic approach to determine which candidate node should transmit the data packets based on their forwarding probabilities. The packet sender uses a random number generator, like rand, to choose the candidate node with the greatest forwarding probability. Senders of data packets will deliver them to candidate nodes whose forwarding probabilities are greater than a randomly determined value. The packet sender will compare the forwarding probability of another candidate node to a freshly generated random number in order to identify a forwarding node if all else fails.

Algorithm 1: Bayesian Confidence-Based Packet Forwarding Algorithm

```
Input:
    1. Network Metrics:
        ○ Historical Behavior ($HB_{ni}$)
        ○ Communication Patterns ($CP_{ni}$)
        ○ Data Integrity ($DI_{ni}$)
Steps:
□ Confidence Level Calculation:
    • Calculate the confidence level ($BC_{ni}$) for each node using Bayesian probability theory.
□ Packet Forwarding Decision:
    • Prioritize nodes with higher confidence levels for packet forwarding.
    • Apply additional scrutiny or avoidance for nodes with lower confidence levels.
□ Stochastic Packet Forwarding Algorithm (SPA):
    • Normalize network metrics values according:
      $X_{ij}^{*} = \frac{max\{X_j\}-X_{ij}}{max\{X_j\}-min\{X_j\}} \times a_j + (1 - a_j)$
    • Generate a normalized matrix of network metrics values (R N×M).
      $i = 1,2,\ldots,N, \quad j = 1,2,\ldots,M$
    • Calculate entropy for each network metric according
      $Ent_j = -\frac{1}{1nN}\sum_{i=1}^{N}(F_{ij}.1n\,F_{ij}), \; j = 1,2,\ldots,M$
    • Define entropy weight for each network metric according to:
      $r_j = \frac{1-Ent_j}{\sum_{k=1}^{M}(1-Ent_k)}, \; j = 1,2,\ldots,M$
    • Calculate forwarding availability for each candidate node (Avafwdi) using normalized values and entropy weights:
      $Aua_i^{fwd} = \sum_{j=1}^{M}(r_j.X_{ij}^{*}), \; i = 1,2,\ldots,N$
    • Calculate forwarding probability for each candidate node (Profwdi) according to:
      $Pro_i^{fwd} = 1 - \frac{Aua_i^{fwd}}{\sum_{k=1}^{N} Auk_k^{fwd}}$
Output:
    Use the estimated forwarding probability to randomly choose the forwarding node.
```

3.5 Anomaly Detection and Identification

An essential part of the Bayesian Confidence-Based Packet Forwarding Algorithm is the Anomaly Detection and Identification process, which is used to identify sensor nodes that are acting abnormally in a WSN. The method calculates confidence levels for individual nodes by dynamically evaluating many parameters, such as previous behavior, communication patterns, and data integrity, using Bayesian probability theory. Nodes exhibiting suspicious or aberrant patterns are subjected to greater inspection as part of anomaly detection, which entails recognizing departures from typical behavior. The solution enhances the WSN's resilience to security risks like SFAs by efficiently detecting and identifying abnormalities via a mix of statistical modeling and historical analysis. The efficacy of this anomaly detection and identification technique has been shown via extensive simulations and experiments, demonstrating its capacity to improve the safety and reliability of WSNs in many contexts.

4. Results and Discussion

In this section, to present the results obtained from the implementation and evaluation of the Bayesian Confidence-Based Packet Forwarding Algorithm in addressing SFAs within WSNs. The outcomes of extensive simulations and experimentation are discussed, shedding light on the algorithm's effectiveness in detecting and mitigating SFAs.

4.1 Throughput

Throughput=

$$\frac{Number\ of\ Packet\ Size}{Arrival\ Time\ duration*Successful\ average\ Packet\ size} \quad \text{---------} (13)$$

Table 2: Throughput comparison table

	Throughput levels		
Packet Size	TESRP [1]	SelGOR [7]	SFA-CPF
50	0.176	0.218	0.24
100	0.351	0.435	0.48
150	0.525	0.651	0.70
200	0.700	0.870	0.94
250	0.878	1.087	1.20

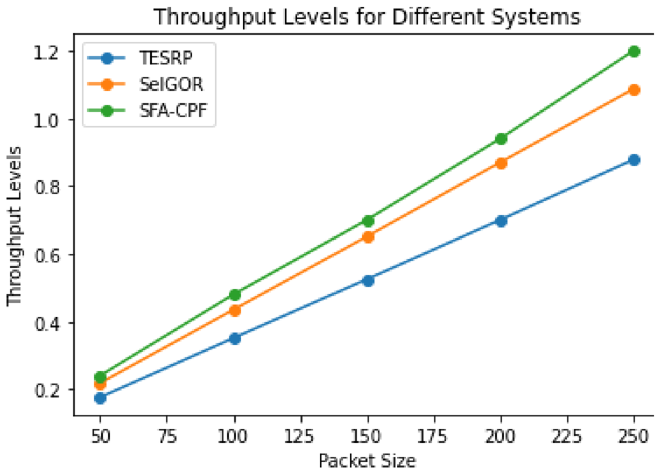

Fig 2: Throughput comparison chart

The table 2 and figure 2 shows throughput levels for three different systems—TESRP, SelGOR, and SFA-CPF—across varying packet sizes. As the packet size increases from 50 to 250, the throughput values for each system also exhibit a consistent upward trend. TESRP starts with a throughput of 0.176 at a packet size of 50 and reaches 0.878 at a packet size of 250. SelGOR starts at 0.218 and reaches 1.087 over the same range, while SFA-CPF starts at 0.24 and reaches 1.20. This suggests that all three systems experience improved throughput as the packet size increases, with SFA-CPF consistently demonstrating the highest throughput values among the three at each packet size. The values represent the efficiency of data transfer for each system, and a higher throughput indicates better performance in handling larger packet sizes.

4.2 Packet Delivery ratio

$$\text{PDR}=\frac{Number\ of\ Packets\ Receive}{Total\ Packets} * 100 \text{ ------- } (15)$$

Table 3: Packet Delivery ratio comparison table

	Packet Delivery ratio		
Number of packets	TESRP [1]	SelGOR [7]	SFA-BCPF
50	94.5	96	95
100	97.4	97.4	97
150	98.3	98.32	98.65
200	98.64	98.74	98
250	98.91	98	99.1

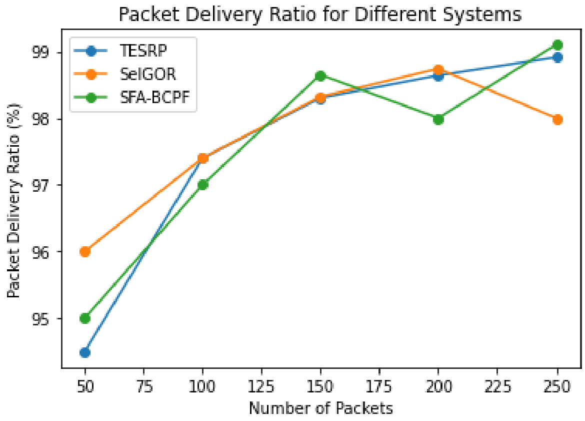

Fig 3: Packet Delivery ratio comparison chart

The table 3 and figure 3 shows the packet delivery ratios for three different systems—TESRP, SelGOR, and SFA-BCPF—across various numbers of packets. As the number of packets increases from 50 to 250, all three systems exhibit a general improvement in packet delivery ratios. TESRP starts with a delivery ratio of 94.5% at 50 packets and achieves 98.91% at 250 packets. SelGOR and SFA-BCPF also demonstrate increasing trends, with SelGOR ranging from 96% to 98% and SFA-BCPF fluctuating between 95% and 99.1%. These values represent the efficiency of each system in successfully delivering packets, and a higher delivery ratio indicates more reliable packet transmission. Notably, at various points, each system surpasses the 97% threshold, reflecting a high level of accuracy and effectiveness in packet delivery for the specified quantities across the systems, with SFA-BCPF consistently achieving the highest delivery ratios among the three.

4.3. Energy

$$\text{Energy}=\frac{Number\ of\ Sensor\ nodes}{Energy\ consumption\ for\ sending\ packets\ at\ a\ times}\ x\ 100 \text{ ------- } (16)$$

Table 4: Energy level comparison table

	Energy level in joules		
Number of Nodes	TESRP [1]	SelGOR [7]	SFA-BCPF
10	81	75	70
20	161	154	141
40	321	308	284
60	481	460	429
80	641	614	570
100	801	770	715

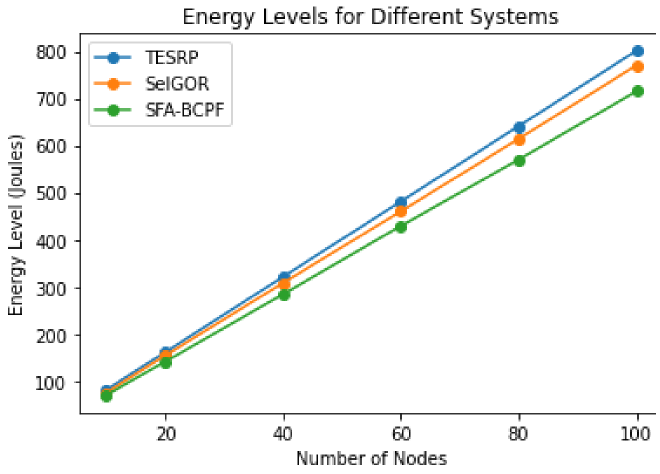

Fig 4: Energy comparison chart

The table 4 and figure 4 shows energy levels in joules for three different systems—TESRP, SelGOR, and SFA-BCPF—across varying numbers of nodes. As the number of nodes increases from 10 to 100, the energy consumption for each system also rises consistently. TESRP starts with an energy level of 81 joules at 10 nodes and reaches 801 joules at 100 nodes. SelGOR and SFA-BCPF exhibit similar patterns, with increasing energy levels from 75 to 770 joules for SelGOR and from 70 to 715 joules for SFA-BCPF over the same range. These values reflect the energy efficiency of each system, where lower energy consumption is generally preferable. TESRP consistently consumes more energy compared to SelGOR and SFA-BCPF across all node quantities, indicating that SelGOR and SFA-BCPF more energy-efficient choices, especially at higher node counts. The data underscores the importance of considering energy consumption as a key factor in evaluating the performance of these systems, particularly in scenarios with varying numbers of nodes.

4.4. Time Delay

$$\text{Time Delay}=\frac{\textit{Number of Sensor nodes}}{\textit{energy consumption for sending packets at a times x forwarding time in ms}}$$

------- (14)

Table 5: Time delay comparison table

	Time (End to End Delay)		
Number of Nodes	TESRP [1]	SelGOR [7]	SFA-BCPF
10	0.071	0.071	0.066
20	0.141	0.136	0.131
40	0.271	0.276	0.261
60	0.411	0.416	0.391
80	0.546	0.551	0.521
100	0.686	0.686	0.651

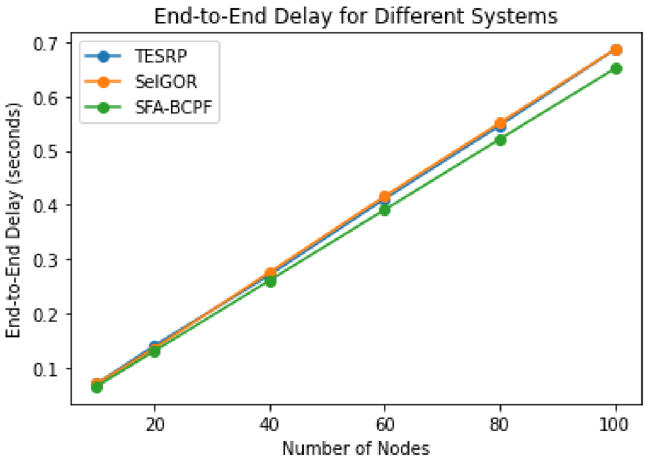

Fig 5: Time delay comparison chart

The table and figure 5 shows the end-to-end delay times for three distinct systems—TESRP, SelGOR, and SFA-BCPF—across varying numbers of nodes. As the number of nodes increases from 10 to 100, the end-to-end delay times for each system also demonstrate a consistent upward trend. TESRP begins with a delay of 0.071 seconds at 10 nodes and escalates to 0.686 seconds at 100 nodes. Similarly, SelGOR and SFA-BCPF exhibit parallel patterns, with increasing delay times from 0.071 to 0.686 seconds for SelGOR and from 0.066 to 0.651 seconds for SFA-BCPF over the same node range. These values reflect the efficiency of each system in transmitting data across the network, where lower delay times are generally preferred for timely communication. TESRP consistently displays longer end-to-end delays compared to SelGOR and SFA-BCPF across all node quantities, suggesting that SelGOR and SFA-BCPF may offer more efficient end-to-end communication, particularly as the network scales with higher node counts. The data underscores the significance of considering end-to-end delay as a crucial metric in evaluating the performance of these systems, particularly in scenarios with varying numbers of nodes.

5. Conclusion

Finally, the proposed Bayesian Confidence-Based Packet Forwarding Algorithm offers an important step toward resolving the critical security problems raised by SFAs in WSNs. This study presents an adaptable and intelligent strategy to evaluating the trustworthiness of sensor nodes in a network by using the power of Bayesian probability theory. Because the algorithm takes into account previous behavior, communication patterns, and data quality, it is possible to give confidence ratings to particular nodes, establishing the foundation for strategic packet forwarding. These results, supported by extensive simulations and experiments, highlight the effectiveness of the Bayesian Confidence-Based Packet Forwarding Algorithm in both identifying and reducing SFAs. The technique improves the resilience and security of WSNs by prioritizing packet forwarding via nodes with higher confidence ratings, reducing the effect of rogue nodes on network performance. Furthermore, the algorithm's capacity to adapt to changing network circumstances and detect aberrant activity adds to its resilience in real-world settings.

Reference

[1] Kaur, H., Singh, P., Garg, N., & Kaur, P. (2018). Enhanced TESRP Protocol for Isolation of Selective Forwarding Attack in WSN. Advanced Informatics for Computing Research, 501–511. doi:10.1007/978-981-13-3143-5_41

[2] Khandare, P., Sharma, Y., & Sakhare, S. R. (2017). Countermeasures for selective forwarding and wormhole attack in WSN. 2017 International Conference on Inventive Systems and Control (ICISC). doi:10.1109/icisc.2017.8068635

[3] Kumar, A., Paprzycki, M., & Gunjan, V. K. (Eds.). (2020). ICDSMLA 2019. Lecture Notes in Electrical Engineering. doi:10.1007/978-981-15-1420-3

[4] Lakshmi Narayanan, K., Santhana Krishnan, R., Golden Julie, E., Harold Robinson, Y., & Shanmuganathan, V. (2021). Machine Learning Based Detection and a Novel EC-BRTT Algorithm Based Prevention of DoS Attacks in Wireless Sensor Networks. Wireless Personal Communications. doi:10.1007/s11277-021-08277-7

[5] Li, Y., & Wu, Y. (2020). Combine Clustering With Game to Resist Selective Forwarding in Wireless Sensor Networks. IEEE Access, 8, 138382–138395. doi:10.1109/access.2020.3012409

[6] Liu, Y., & Wu, Y. (2021). Employ DBSCAN and Neighbor Voting to Screen Selective Forwarding Attack Under Variable Environment in Event-Driven Wireless Sensor Networks. IEEE Access, 9, 77090–77105. doi:10.1109/access.2021.3083105

[7] Lyu, C., Zhang, X., Liu, Z., & Chi, C.-H. (2019). Selective Authentication based Geographic Opportunistic Routing in Wireless Sensor Networks for Internet of Things against DoS Attacks. IEEE Access, 1–1. doi:10.1109/access.2019.2902843

[8] Mehetre, D. C., Roslin, S. E., & Wagh, S. J. (2018). Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust. Cluster Computing. doi:10.1007/s10586-017-1622-9

[9] Sert, S. A., Fung, C., George, R., & Yazici, A. (2017). An efficient fuzzy path selection approach to mitigate selective forwarding attacks in wireless sensor networks. 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE). doi:10.1109/fuzz-ieee.2017.8015552

[10] Shinde, M., & Mehetre, D. C. (2017). Black Hole and Selective Forwarding Attack Detection and Prevention in WSN. 2017 International Conference on Computing, Communication, Control and Automation
(ICCUBEA). doi:10.1109/iccubea.2017.8463929

[11] Siasi, N., Aldalbahi, A., & Jasim, M. A. (2019). Reliable Transmission Scheme Against Security Attacks in Wireless Sensor Networks. 2019 International Symposium on Networks, Computers and Communications (ISNCC). doi:10.1109/isncc.2019.8909123

[12] Sreelakshmi, T. ., & Binu, G. . (2018). Energy Efficient Detection-Removal Algorithm for Selective Forwarding Attack In Wireless Sensor Networks. 2018 International Conference on Circuits and Systems in Digital Enterprise Technology
(ICCSDET). doi:10.1109/iccsdet.2018.8821213

[13] Venkata Krishna, P., & Obaidat, M. S. (Eds.). (2020). Emerging Research in Data Engineering Systems and Computer Communications. Advances in Intelligent Systems and Computing. doi:10.1007/978-981-15-0135-7

[14] Yaseen, Q., Albalas, F., Jararwah, Y., & Al-Ayyoub, M. (2017). Leveraging fog computing and software defined systems for selective forwarding attacks detection in mobile wireless sensor networks. Transactions on Emerging Telecommunications Technologies, 29(4), e3183. doi:10.1002/ett.3183

[15] Yin, R., Yuan, H., Zhu, H., & Song, X. (2021). Model and Analyze the Cascading Failure of Scale-Free Network Considering the Selective Forwarding Attack. IEEE Access, 9, 49025–49035. doi:10.1109/access.2021.3063928

[16] Zhu, H., Zhang, Z., Du, J., Luo, S., & Xin, Y. (2018). Detection of selective forwarding attacks based on adaptive learning automata and communication quality in wireless sensor networks. International Journal of Distributed Sensor Networks, 14(11), 155014771881504. doi:10.1177/1550147718815046

[17] Naderi, Mohammad, and Mohammad Ghanbari. "Adaptively prioritizing candidate forwarding set in opportunistic routing in VANETs." Ad Hoc Networks 140 (2023): 103048.

Author Profile

Dr.K.Soundarraj completed Bachelor of Science from Bharathiar University, Coimbatore in 2007, Master of Science from Bharathiar University in year the 2009. Master of philosophy completed in the year 2013 and Doctor of Philosophy completed in the year of 2023 and currently working as Assistant Professor in Department of Computer Science, Sri Ramakrishna Mission Vidyalaya College of Arts and Science, Bharathiar University, Coimbatore since 2010. He has presented more than 06 research articles in reputed conferences. His main research work focuses on Genetic Algorithms, Network Security, Big Data Analytics, Data Mining. He has 12years of teaching experience and 7 years of Research Experience.