Vol. 12-2 (2025) 95-115

International Journal of Computers and Information (IJCI)

Available online at *https://ijci.journals.ekb.eg/*

An Experimental Network Analysis-based Approach for Detection of Jamming Attacks in Wireless Sensor Networks

Elham Elsayed Hamza[a], Arabi Keshk[a], and Anas Youssef[a]

[a] *Computer Science Department, Faculty of Computers and Information, Menoufia University, Shebin El-Kom, Menoufia, Egypt*

Abstract

Wireless sensor networks (WSNs) have emerged as a cutting-edge networking solution with numerous applications in various domains. Such domains include environment, military operations, healthcare, and agriculture. However, WSNs consist of sensor nodes that are susceptible to multiple security risks, because they are often deployed in hostile and unattended locations, and they possess limited resources. The jamming attack is among the most recognized types of attack, which disrupts and diminishes the effectiveness of the normal operations of sensor nodes in WSNs. A jamming attack is characterized by sending signals to interfere with legitimate communications, potentially resulting in a denial of service for one or more nodes in the network. This paper proposes an experimental network analysis-based approach to detect jamming attacks in WSNs. This approach identifies anomalies that indicate the existence of jamming attacks by analyzing a set of network statistics. The analyzed statistics include Packet Delivery Ratio (PDR), Signal to Noise ratio (SNR), and Packet Error Rate (PER) of packets received by sensor nodes. The detection process targets two different types of jamming attacks, namely constant and random jamming attacks. The proposed approach is compared with the Exponentially Weighted Moving Average (EWMA) statistical approach. Simulation results from the trace-based OMNeT++ discrete event simulator demonstrated that the proposed approach effectively and accurately detects jamming attacks in WSNs while reducing detection overhead. The proposed approach is more accurate than EWMA since it is based on an experimental simulation-based analysis of the network as opposed to EMWA which is based on theoretical statistical analysis of the WSN metrics. The Proposed Approach consistently delivers more packets compared to EWMA across all time intervals the Proposed Approach achieves approximately 6000 packets delivered, whereas EWMA is around 5200 packets.

Keywords: *Wireless Sensor Network; Exponentially Weighted Moving Average; Jamming Attack; Constant Jamming; Random Jamming.*

1. Introduction

A Wireless sensor network (WSN) comprises hundreds to thousands of sensor nodes that may be categorized based on their structure, i.e. the environment in which they are deployed, and topology [1]. WSNs are exposed to various security threats and attacks since they are deployed in unattended locations. The jamming attack is one of these attacks. Jamming attacks are a type of denial of service (DoS) attack where an adversary broadcasts a powerful signal to disrupt communications [2].

Typically, jamming can happen unintentionally in a wireless medium due to factors like interference, noise, and collisions. However, a jamming attack in a wireless sensor network is a deliberate effort by an adversary to disrupt the physical transmission of signals during communication [2]. The primary objective of a DoS attack is to target the communication channels of sensor nodes with malicious signals, aiming to deplete their resources, including battery life, storage, and bandwidth. This attack prevents sensor data from being sent from its source to its destination, thus affecting the network availability and performance over the long run.

A jamming attack on a WSN is particularly damaging because it can be executed without the need for specialized hardware or software. This can be accomplished by monitoring the wireless medium passively with the purpose of broadcasting on the same frequency range as normal transmission signal. [2]. A typical jamming attack has a low probability of detection and high energy efficiency. In WSNs, the physical and media-access layers are frequently targeted by jamming attacks [3]. The jamming attack against the physical layer generates a signal with high power of transmission to disrupt the communication medium, since most WSN deployments operate on a single frequency. This attack demands significant resources and is not well-suited for WSNs because of the energy constraints in sensor nodes.

On the other hand, a media-access layer jamming attack is performed either by tampering with control packets or deliberately occupying the communication channel for the maximum allowed number of slots to ensure that other nodes experience reduced throughput due to the channel's inaccessibility. This research suggests that the physical layer generates interference and obtains it from the MAC layer to distinguish between network conditions resulting from jamming attacks or natural sources. Detecting jamming attacks has been a prominent area of research over the past decade in WSNs, whereas commonly proposed methods rely on dedicated hardware or algorithms embedded in the sensing node [4].

These approaches typically rely on pre-existing knowledge of communication behaviour under normal and jammed conditions, which can be monitored using various indicators and metrics from different network layers [5]. Examples of such metrics include the received signal strength at the physical layer and the packet delivery ratio at the application layer. Recently, some methods have introduced a cross-layer architecture to facilitate the collection of jamming attack indicators, while others have combined multiple metrics to enhance the accuracy of jamming attack detection. Related studies have utilized metrics such as Packet Delivery Ratio (PDR), Signal-to-Noise Ratio (SNR), and Packet Error Rate (PER) to identify jamming attacks.

This paper proposes an experimental network analysis-based approach for detecting jamming attacks in WSNs. The proposed approach detects the presence of a jamming attack in a WSN by applying an experimental study that simulates a WSN with different scenarios and computes a set of jamming detection metrics. These metrics include PDR, SNR, and PER. The applied experimental study was concluded by the determination of a set of thresholds for the various metrics used in the study. These thresholds were used to accurately identify jamming attacks in the simulated WSN scenarios used in the experiments. The proposed approach aims to detect two different types jamming attacks namely constant and random jamming attacks. The applied experimental study was implemented using the trace-based OMNeT++ discrete event simulator. The results of the study were compared with the well-known Exponentially Weighted Moving Average (EWMA) theoretical statistical approach. The proposed approach consistently results in a higher packet reception rate compared to EWMA across all time points. For both methods, the number of received packets rises steadily, indicating that packet delivery occurs over time despite on-going jammer. This demonstrates that jammer is effectively identified, even with a higher PDR value. In situations involving constant jamming, networks with a smaller number of nodes can sustain communication for a longer period. However, all network setups ultimately experience performance decline under persistent jamming. In a network with 100 nodes, the packet loss rate could reach as high as 98%. It is noted that the proposed approach is software-based which means it does not need any additional hardware sensors to implement the detection process. This is crucial for the reduction in the power consumed by the limited-power nodes in the WSNs.

The rest of this paper is structured as follows: Section 2 discusses the related works. Section 3 introduces background information about metrics used to detect jamming attacks and describes a classification of the different jamming attacks. Section 4 described the proposed approach. Section 5 describes the simulation setup and environment. The evaluation results are presented and discussed in Section 6. Finally, the paper conclusions and future work are presented in Section 7.

2. Related Work

Jamming attacks are among the most important attacks on WSNs. A jamming attack disrupts the WSN with jamming, collisions, or interference. There by reducing successful packet delivery. This section offers a summary of the detection mechanisms proposed in the literature for identifying jamming attacks on WSNs. A selection of related studies [2, 6, 7, 8, 9] are discussed in this section.

The work in [2] utilized the Exponentially Weighted Moving Average (EWMA) statistical to identify abnormal variations in jamming intensity. The study introduced an innovative jamming detection method by applying EWMA for auto-correlated data and monitoring the packet inter-arrival time (IAT), which is influenced by preceding or subsequent values in a sequence. This approach was implemented at the cluster head to identify jamming attacks on member nodes and at the base station to detect jamming on the cluster heads. The proposed solution effectively and accurately detected jamming attacks in WSNs with minimal or no overhead. In this method, EWMA statistical analysis was used to compare with other techniques for detecting abnormal changes, leveraging various measurements dependent on earlier or later values in a series.

The work proposed in [6] introduced two methods for securing sensor networks against jamming attacks by assessing the damage level of nodes within cluster sensor networks. The first method involves two modules: the certification module and the monitoring module, which work together to assess the level of damage to nodes. The certification module protects the network from jamming devices, while the monitoring module detects which sensor nodes are impacted by jamming. The second approach utilizes fuzzy logic to improve noise metrics, thereby increasing the precision of detecting jamming incidents

The work proposed in [7] introduced two novel methods for jamming detection namely: the Fuzzy Inference System (FIS) and the Adaptive Neuro-Fuzzy Inference System (ANFIS). These systems are designed to identify jamming by assessing two key detection metrics: the packet delivery ratio and the received signal strength index. The FIS method employs Takagi-Sugeno fuzzy logic to optimize noise detection metrics, while the ANFIS method combines fuzzy logic with neural network learning capabilities to enhance jamming detection across various types.

The study proposed in [8] introduced two detection methods designed to identify jamming-style denial of service (J-DoS) attacks, distinguishing between legitimate and malicious situations. These methods leveraged various network parameters and extra packets to differentiate and categorize normal conditions from those caused by adversaries. The initial parameter levels PDR, bad packet ratios (BPR), and energy consumption amounts (ECA) were sampled in the installation phase, and it was assumed that no jammer could disturb the sensor network. It has developed a novel query-based jamming detection algorithm (QUJDA) to identify jamming attacks in WSNs. A query-based jamming detection algorithm (QUJDA) is an attack detection mechanism that uses an anomaly-based approach and operates in a distributed manner. It separates attacking cases from natural network conditions with the help of packet delivery ratio, bad packet ratio, and energy consumption parameters.

The work presented in [9] proposed a jamming detection technique for WSN named physical layer jamming identification using PDR and Received Signal Strength Indicator (RSSI) parameters. This method used only some nodes in the network that had residual energy to monitor. Nevertheless, for monitoring the entire network, the method implemented various monitoring nodes. First, it will broadly categorize the types of jamming attacks using existing detection methods. Then, by analyzing the statistics of packet send rate (PSR) and PDR, it will enhance the current detection mechanism to more accurately identify specific types of jamming attacks when different MAC protocols are employed.

The work proposed in [10] detects jamming using parameters such as Packet Delivery Ratio (PDR), Packet Send Ratio (PSR), Received Signal Strength Indication (RSSI), and Signal-to-Noise Ratio (SNR). Conversely, energy efficiency is a crucial concern in wireless sensor networks (WSNs) and plays a key role in determining their operational lifespan. To extend the network's lifetime, WSNs are structured into clusters, with cluster heads responsible for transmitting aggregated data to the base station either directly or via multi-hop communication. This study focuses on analyzing the impact of a jamming attack within a clustering-based WSN. A jamming attack in a clustered Wireless Sensor Network (WSN) significantly impacts its functionality, rendering clusters ineffective. This can lead to transmission delays and a decline in network throughput. To address these issues, an efficient jamming localization scheme is introduced, leveraging parameters such as Jamming Signal Strength (JSS) and Packet Delivery Ratio (PDR) for jamming detection. The affected area is then identified by constructing a convex hull around the jammed nodes. Additionally, to maintain communication despite jamming, a cluster-based dynamic multi-channel assignment technique is proposed. This method avoids compromised channels and dynamically assigns a new channel to the affected cluster, ensuring uninterrupted transmission.

Table 1 shows a comparison between the proposed approach and earlier cutting-edge research. This paper examines three key network parameters: PDR, SNR, and PER, which will be detailed in Section 5. Utilizing these parameters with a straightforward technique, these metrics effectively differentiate between normal and abnormal instances of jamming attacks. The proposed approach also enables the identification of two kinds of jamming attacks: random and constant jamming attacks.

3. Background

3.1 Jamming Detection Metrics

The detection criteria for jamming attacks are examined in the chosen research, which concentrates on utilizing metrics such as PDR, SNR, and PER to identify jamming incidents in WSNs through meta-heuristic optimization techniques. The rationale behind this selection is thoroughly discussed and summarized.

Table 1. *Comparison with related works*

Reference	Author-Year	Metrics	Jamming Attack	Platform
[2]	Osanaiye, O.; Alfa, A.; Hancke, G- 2018	IAT	Reactive, Constant and Periodic	Trace driven
[6]	Kanagasabapathy, P.M.K.;Kedaluoornachary,V.;Murugan,S.; atesan, A.; Ponnusamy, V -2019	PDR, PLR	Jammed/NoJammed	MatlAB7 and NS2
[7]	Vijayakumar, K. PradeepMohan Kumar, K. Kottilingam, T. Karthick, P. Vijayakumar, P- 2019	PDR, RSSI	Constant, deceptive Random	MATLAB
[10]	An Anti-jamming Technique by Jammer Localization for Multi-channel Wireless Sensor Networks-2024	PDR,PSR, ,RSS,SNR.	Jammer/NoJammer	OMNeT++
Proposed Work		PDR, SNR, PER	Constant, Random	OMNeT++

Packet delivery ratio a metric is utilized to assess the efficiency of packet delivery within a network [11]. It represents the ratio of the number of packets successfully delivered to their intended destinations to the total number of packets sent within a certain timeframe. PDR is defined by equation 1. Higher PDR values indicate better delivery performance, while lower values suggest potential issues with packet loss or network congestion.

$$PDR = \frac{Number\ of\ packets\ successfully\ delivered}{Total\ number\ of\ packets\ sent} \tag{1}$$

The signal-to-noise ratio is a measure used in communications and signal processing to quantify the level of a desired signal relative to the level of background noise [12]. The SNR is usually expressed in decibels (dB). SNR is defined by equation 2.

$$SNR = \frac{Pnoise}{Psignal} \tag{2}$$

Where Psignal is the power of the normal network signal, Pnoise is the power of the noise signal. SNR is defined in decibels using the following equation:

$$SNR = \ 10log10\frac{Pnoise}{Psigna} \tag{3}$$

The packet error rate is defined as the ratio of the number of packets received with errors to the total number of packets sent. A packet is considered to be in error if even a single bit is incorrect. The Packet Error Rate (PER) is solely influenced by the Bit Error Rate (BER) and the number of bits in the packet's data payload, regardless of the data encoding or the events during the transmit-receive process. Consequently, the relationship between PER and BER is defined by equation 4.

$$PER = \frac{Number\ of\ incorrectly\ received\ packets}{Total\ number\ of\ packets\ received} \tag{4}$$

PDR and PER are highly effective metrics that nodes can accurately measure without incurring significant computational overhead. These metrics can effectively detect the presence of different types of jamming attacks. Additionally, SNR assists in determining the viability of the current communication path with neighboring nodes.

3.2 Types of Jamming Attacks in WSNs

WSNs face different types of attacks due to the variety of purposes behind attacking WSNs [16]. In this section, the paper present classification derived from previous attack categorizations. There are four primary types of jamming attacks or, shortly, jammers. [4]. The four types are described as follows. Firstly, a constant jammer continuously transmits radio signals or operates as a typical wireless device that perpetually sends random bits into the channel without adhering to any MAC-layer protocols [13], regardless of whether the channel is busy. Secondly the random jammer randomly alternates between idle and jamming states. Identifying this type of attacks has become difficult due to their unpredictable behaviour. Thirdly, the deceptive jammer continuously injects regular packets into the channel without any gaps between transmissions. This causes a normal communicator to be deceived into thinking there are legitimate packets maintaining it in the receive state. Even if a node has packets to send, it cannot transition to the send state because it will continuously detect incoming packets. Finally, the reactive jammer remains inactive when the channel is idle but begins transmitting a radio signal as soon as it detects activity on the channel.

3.3 Proposed Approach

In this section, the proposed approach for identifying jamming attacks in WSNs is introduced. The objectives of this approach are the detection of the occurrence of a jamming attack and the classification of its type. While there are various types of jamming attacks, the proposed approach focuses on two specific types namely: constant and random jamming attacks. Three key network performance metrics are leveraged which are PDR, SNR, and PER. When the constant jammer occurs in a WSN, this leads to the continuous transmission of interfering signals which disrupts communication. The jamming signal always remains active, leading to persistent interference. When the random jammer occurs, the interfering signal is transmitted intermittently, only at unpredictable intervals. This results in sporadic disruptions to communication, causing varying levels of interference.

The proposed approach detects jammers and classifies their types using the following experimental network analysis-based methodology. Firstly, measurements of PDR, SNR and PER values were collected under normal network conditions, i.e., in the absence of any jammers, to initialize baseline measurements for the three metrics. These collected measurements were then used to serve as reference thresholds for detecting any jamming-induced anomalies. Secondly, network monitoring is applied during suspected jamming activity, and the collected measurements of PDR, SNR and PER were compared with the recorded thresholds.

The experimental study resulted in following general findings. When constant jammer active in the WSN, the PDR was found to continuously decrease and remain at low levels because continuous interference affects all packet transmissions. On the contrary when random jammer was active, the PDR was found to fluctuate where there were periods when the PDR value was normal, i.e., with no signal interference, and periods when it was lower, i.e., when signal interference became active.

When constant jammer was active, the SNR was found to remain low and constant due to the constant jammer interference. When random jammer was active, the SNR was found to fluctuate between high, i.e., normal, and low during periods of jamming signal interference. As shown in PER With constant jamming, the SNR will be constantly high as the interference continually destroys packets. For random interference, the SNR will spike at random intervals and then return to normal levels.

Three threshold values were detected from the above-mentioned experimental findings. The three threshold values are described as follows. If the PDR is consistently below PDR_{th}, this indicates constant jammer interference. If the SNR drops below SNR_{th} and stays there, this indicates constant jammer interference. If it fluctuates, it indicates random jammer interference. If the SNR stays above SNR_{th}, this indicates constant jammer interference. If it rises intermittently, it is considered random jammer interference.

Table 2 shows the behaviour of the three above-mentioned metrics, and they can be used to classify the type of jammers based on the observed behaviour. The pseudo code of the proposed approach is shown in Figure 1. The figure shows a set of comparisons applied to differentiate between normal behaviour and various types of abnormalities, including constant jamming, random jamming, and other network faults in addition to the situation where no jamming is detected.

Table 2. *Behaviour of Metrics for Different Jammer Types*

Metric	Constant Jamming	Random Jamming
PDR	Consistently low	Varying (low during jamming period, normal otherwise)
SNR	Consistently low	Fluctuating (low during jamming period, normal otherwise)
PER	Persistently high	Varying (high during jamming period, normal otherwise)

4. Simulation Environment

4.1. Simulation Setup

To measure the performance of the proposed method against jamming and network attacks, we created different types of jammers in an experimental environment. Network performance can be tested by investigating various values of PDR, SNR, and PER metrics. Table 3 and Table 4 list the configuration of WSN node parameters and jammer simulation parameters, respectively. The effectiveness of the proposed approach is assessed using OMNeT++ simulation. In this research, OMNeT++ was used as the simulation tool. OMNeT++ is a simulation framework that does not include built-in models for network protocols like IP or HTTP. Many third-party frameworks offer major computer network simulation models [19]. The most commonly used is INET, which provides a range of models for various network protocols and technologies, including IPv6 and BGP.

4.2. Simulation Scenarios

This section shows a set of simulation scenarios applied to evaluate and validate the efficacy of the proposed detection approach. By simulating various scenarios, it allows for a comprehensive assessment of the approach's performance, robustness, and adaptability, ensuring it can reliably detect jamming. To limit the effects of an attack, the detection step is crucial. As such, at the beginning of the simulation, we simulate experiments in two scenarios. The two scenarios are as follows. The first scenario involves a WSN with no jamming attacks. In this scenario the following steps are applied in order.

1. Design a WSN scenario in the OMNet++ software.
2. Initialize the number of nodes to 4 sensor nodes.
3. Apply the simulation scale for 60 seconds and check it every 5 seconds.
4. Run and record the behavior, i.e., values, of each parameter.
5. Record the results of PDR, SNR, and PER.
6. Stop Simulation.

In the second scenario involves a WSN with fixed and mobile jamming attacks.

1. Design a WSN scenario in the OMNet ++ software.
2. Initialize the number of nodes to 4 sensor nodes, one jammer.
3. Apply the simulation scale for 60 seconds and check it every 5 seconds.
4. Run and record the behavior i.e. values, of each parameter.
5. Compare Results with a Normal Scenario.
6. Is network performance too much affected?
7. Animated jamming attacks on WSN.
8. Stop Simulations.

Proposed Algorithm

```
// Inputs: PDR, PER and SNR
// Outputs: NetworkFault, ConstantJamming, RandomJamming
Jamming_Detection_Classfication()
IF ($PDR<PDR_{th}$)
  IF ($0<PER<1$ AND $SNR>SNR_{th}$)
    NetworkFault= true              //Network Fault is detected
    ConstantJamming = false
    RandomJamming = false
  ELSEIF ($PER==0$ AND $SNR<SNR_{th}$)
    NetworkFault = false
    ConstantJamming = false
    RandomJamming = true        //Random Jammer is detected
  ELSEIF (PER<1 AND SNR<SNRth)
    NetworkFault = false
    ConstantJamming = true     //Constant Jammer is detected
    RandomJamming = false
  ENDIF
ELSEIF ($PDR>PDR_{th}$)
   Jamming=FALSE                      // No Jamming is detected
ENDIF
```

Fig. 1. *Pseudo code of the proposed detection and classification algorithm*

Table 3. *Configuration of WSN node parameters*

Parameter	Value
Number of Nodes	4,20,50,100,300,500
Performance metric	PDR, PER, SNR
Frequency band	2500MHZ
Packet time interval	1ms
Packet Size	100Byte
Transmit Power	5W,0.5W..0125W
Simulation Time (secs)	5,60,120,180,240,300
Test Plan	100*100,800*600,1000*1000,2000*2000

Table 4: *Jammer simulation parameters.*

Parameter	Value
Number of nodes	1 jammer
SleepInterval	.5ms #(.01ms, .05ms)
Mobility Mode	Fixed/Mobile
Transmit Power	.0125W
Jammer Duration	.1s,.5s

5. Results and Discussion

This section presents a detailed overview of the research findings and their importance in the sequence of jamming detection WSNs. The results demonstrate scenarios involving two types of jamming, i.e., constant and random, jamming. The proposed approach is compared with EWMA in terms of the three previously described metrics including SNR, PDR, and PER.

5.1. Constant Jamming

This section presents and discusses the evaluation results of applying our proposed approach in detecting the constant jamming attack. The results are depicted in Figures 2, 3, and 4. Figure 2 illustrates a comparison of the SNR over time in seconds, where the proposed approach is compared with EWMA, highlighting the superior performance of the proposed algorithm compared to EMWA. Both methods start with a high SNR of around 5.00. The proposed approach shows large fluctuations over time, dropping to 1.00 at several points (20, 30, 40, and 55 seconds). This determines the accuracy and speed of jamming detection. While the fluctuation in the noise rate indicates periods in which no jamming activity is detected due to the influence of the jammer, Noise, since in this case we are applying a constant jammer. But EWMA also fluctuates, but less sharply, maintaining a higher SNR level when compared to the proposed approach. The SNR of EWMA gradually decreases after the initial peak.

Figure 3 shows a comparison of PDR under a continuous noise scenario over time where the Proposed approach is compared with “EWMA." The Suggest method shows a consistently higher number of received packets over time, indicating that it is more robust at determining a higher PDR than proving the presence of persistent interference. Both methods show a linear increase in the number of packets received over time. The proposed approach consistently has more packets received than EWMA at all-time points. The number of packets received increases steadily for both methods, which indicates that packets are delivered over time despite the constant jammer, and this proves that the interference is identified even though PDR value is higher. The gap between the proposed approach and “EWMA” remains constant throughout the observed period, indicating a difference in performance between the two methods.

Figure 4 shows a comparison of the PER under constant jammer scenario over time, the proposed approach is compared with EWMA. The figure for the proposed approach consistently appears lower than the line representing the proposed approach, though both trend slightly downwards over time. This suggests that the average error rate per proposal decreases over time and the proposed approach' data shows a smoother trend.

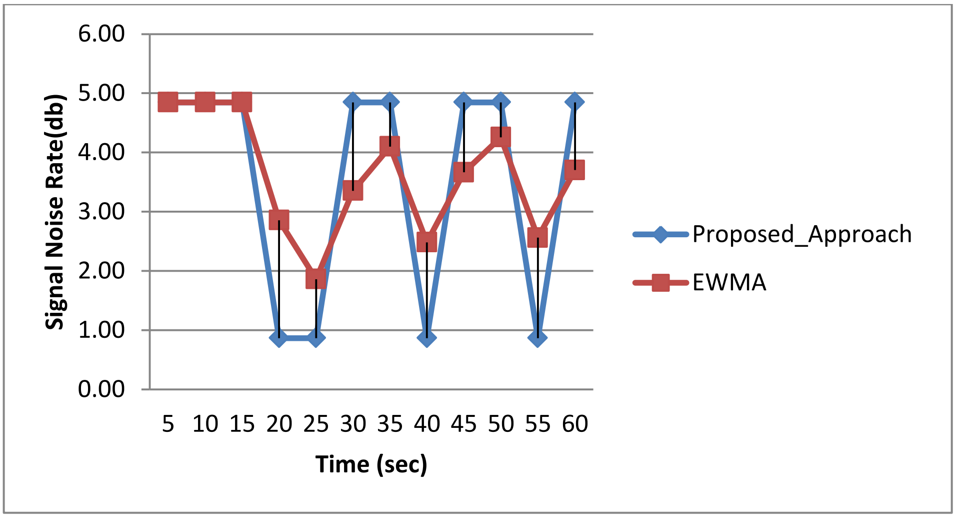

Fig. 2. *Signal to Noise Rate with constant jammer*

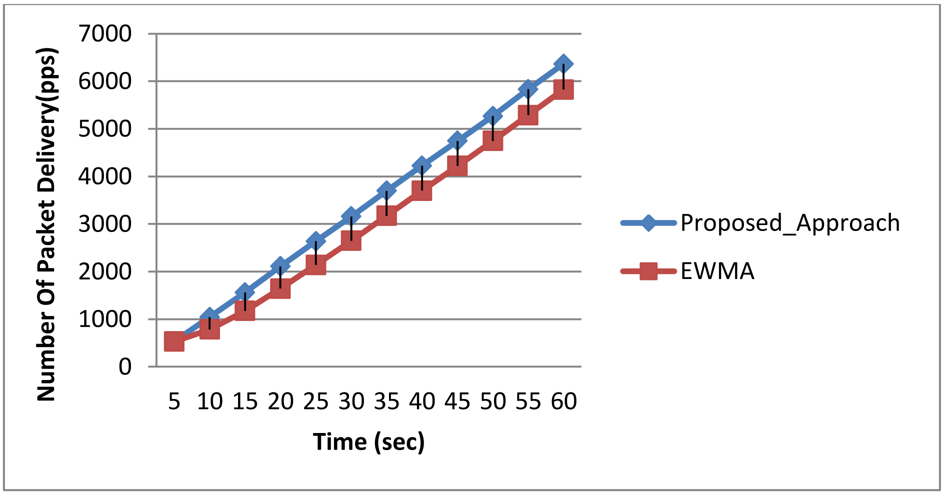

Fig. 3. *Number of Delivered Packets with constant jammer*

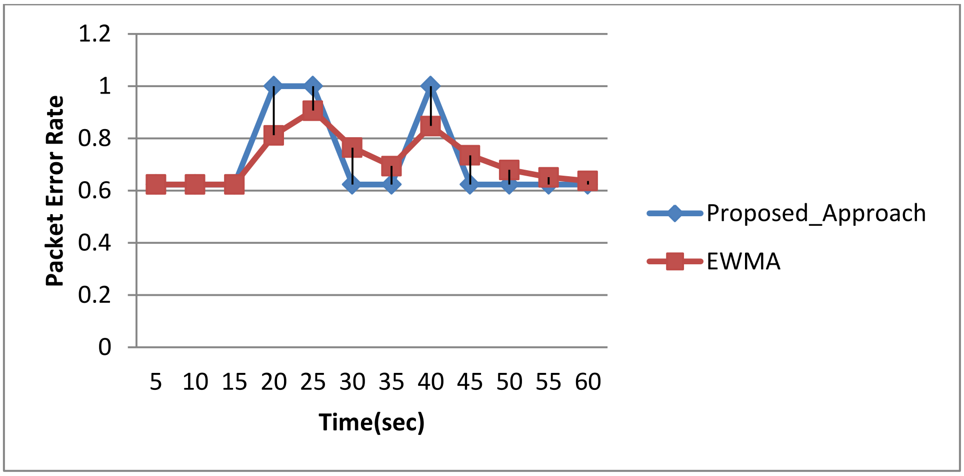

Fig. 4. *Packet Error Rate with constant jammer*

5.2. Random Jamming

This section presents and discusses the evaluation results of applying the proposed approach in detecting the random jamming attack. Figures 5, 6, and 7 show the obtained evaluation results in this case. Nodes targeted by random jammers experience higher levels of jamming compared to typical network behavior, and this difference can be used to differentiate between normal operation and jamming. By repeating the simulation of the SNR parameter in the presence of a random jammer, we can observe its impact on network performance. In Figure 5, the proposed approach shows large peaks on enlightenment (about every 15 s), with SNR values reaching around 120. From these peaks, the proposed approach drops sharply to near zero. This results in a random jamming effect that varies from time to time. “EWMA” is showing more and more consistency, with SNR values ranging between approximately 10 and 40.

The proposed approach method requires a periodic pattern with high peaks with only yellow members, which indicates that it experiences large spikes in SNR under random noise. The SNR method (EWMA) keeps the SNR constant at a much smaller size. While the proposed approach allows higher values for the SNR, which may indicate the safety of random jamming and its limits, including the proposal’s ability to detect jamming even at the lowest value of the noise signal, the detection rate may sometimes range to 58%. It is shown that the noise rate takes a lower rate at some times because no jammer occurred at this time. By repeating the experiment for the simulation of the PDR parameter for a random jammer. In Figure 5, it is shown that the packet Delivery increase with increasing time.

By repeating the experiment for the simulation for the PER parameter. In Figure 7, it is shown that the packet Error rate decreases value 0 and increasing value 1with time. The result of the experiment analysis shows that the proposed algorithm finds in the absence of interference the node receives the packet normally and here the threshold value is 0. Either at time of occurrence of interference the value becomes greater than 0 or equal 1.

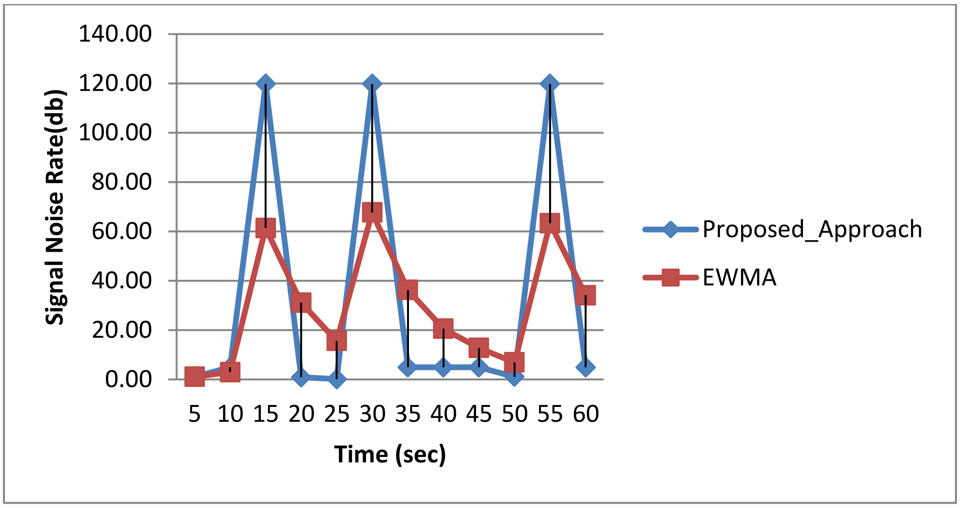

Fig. 5. *Signal to Noise Rate with Random jammer*

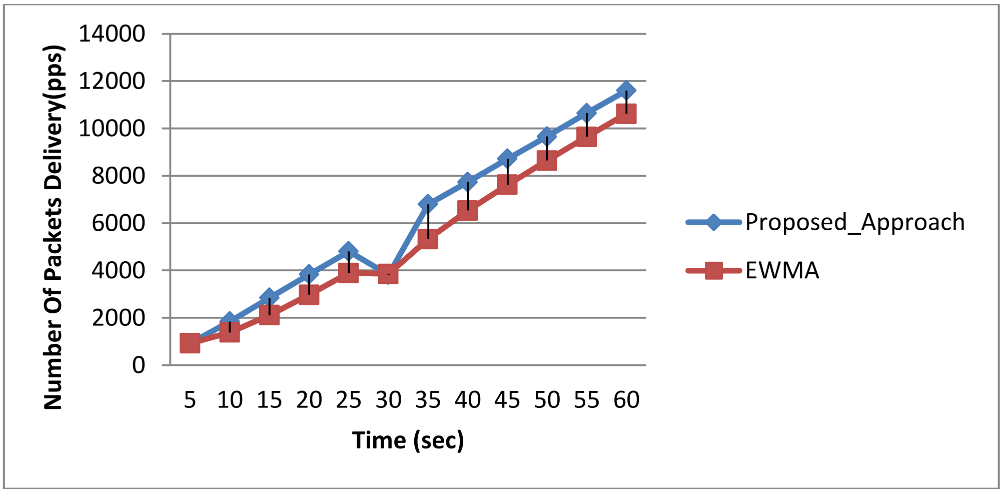

Fig. 6. *Number of Delivered Packets with Random jammer*

5.3. No-Jamming

This section presents and discusses the evaluation results of applying the proposed approach in the absence of a jamming attack. These results can be used to differentiate normal conditions from one another. Figures 8, 9, and 10 present the results of repeated experiments for the SNR, PDR, and PER parameters under the simulation scenario, accounting for background noise but excluding the effects of jamming attacks. In Figure 8, The proposed approach exhibits sharp fluctuations in the signal-to-noise ratio, with peaks around 2500 at certain time intervals (5, 15, 25, 35, 45, and 55 seconds) and drops to zero at other time intervals (10, 30, 40, and 60 seconds).

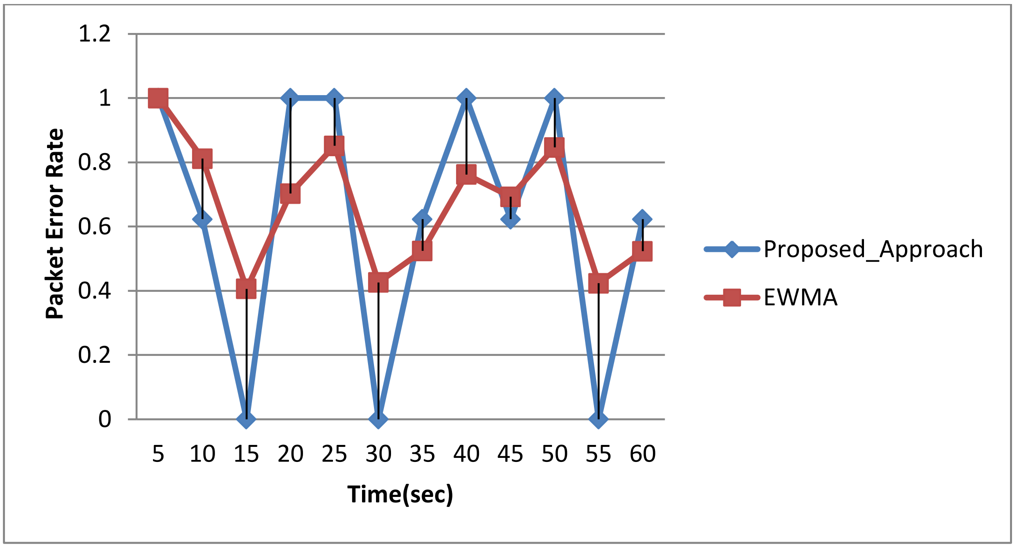

Fig. 7. *Packet Error Rate with Random jammer*

The SNR also exhibits jamming in EWMA but follows a smoother trend compared to the proposed approach. These sharp fluctuations in the signal-to-noise ratio indicate that this method is highly responsive to variations in the environment. It reacts quickly by variations, which may be effective in detecting and responding to noise or other signal interference. However, large drops to zero indicate periods of significant signal degradation. Therefore, the proposed approach is suitable for scenarios that require rapid detection and response to signal changes, even if it results in a temporary decrease in signal quality.

In Figure 9, the proposed approach consistently delivers more packets over time compared to the EWMA approach, as shown by the higher position of its trend line. The difference between the two approaches increases slightly over time, indicating that the Proposed Approach may be more efficient in packet delivery, especially as time progresses. The higher packet delivery rate suggests that this method is more effective in maintaining a high level of packet delivery, possibly due to its more responsive nature in adapting to network conditions and interference.

In Figure 10, the proposed approach shows a series of spikes at designated time intervals (5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, and 60 sec), with PER values reaching 1 at these points. In contrast, the EWMA approach has a more variable PER with peaks and troughs but never reaches a PER of 1. Between these peaks, the proposed approach shows a PER of 0, indicating no packet errors, while EWMA shows a variable PER, generally decreasing over time. The proposed approach has a binary PER pattern either 0 or 1, indicating that it may detect and react to specific jamming or error conditions very effectively but with an all-or-nothing response. EWMA has more latency, indicating that it may be less sensitive to spikes. The proposed approach is therefore designed to detect jamming events or specific conditions that cause packet errors and respond aggressively with a PER of 1. It then recovers quickly PER of 0 until the next event. The proposed approach is suitable for scenarios where rapid detection and response to jamming or errors is critical.

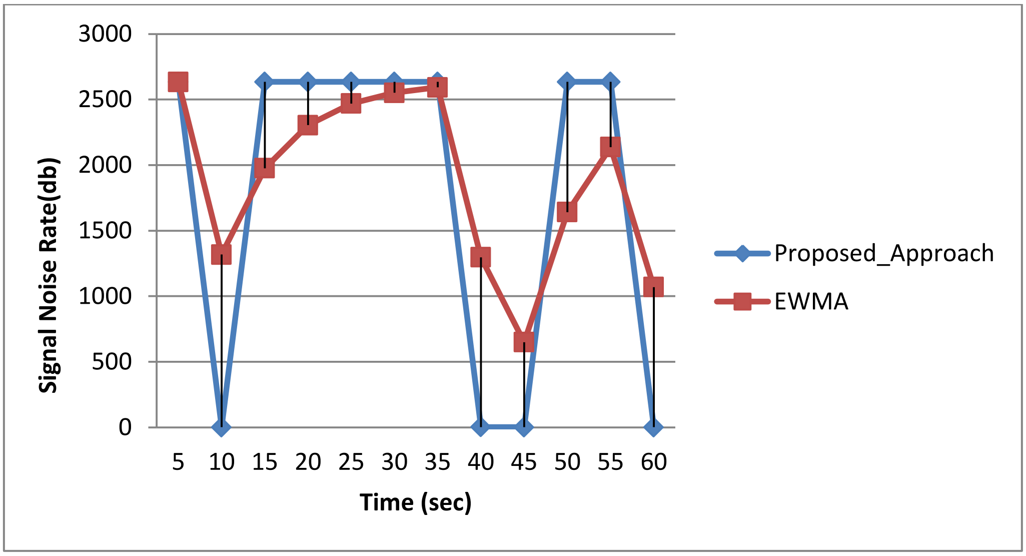

Fig. 8. *Signal to Noise Rate with No-jammer*

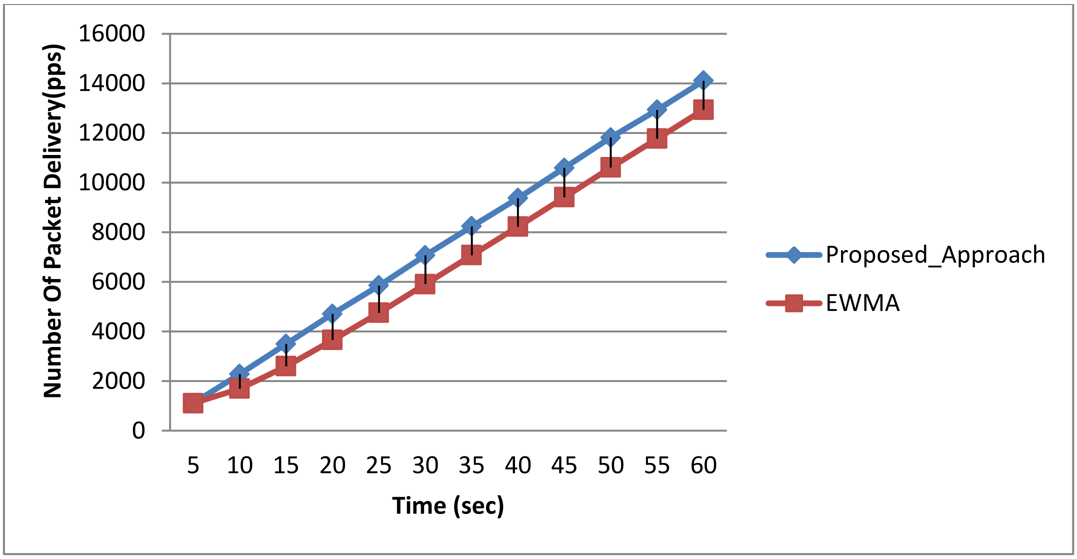

Fig. 9. *Number of Delivered Packets with No-jammer*

5.4. Comparison of Jamming and No-Jamming Scenarios

This section presents and discusses the evaluation results of applying the proposed approach in detecting both constant and random jamming attacks with No-Jammer, figures 11, 12, and 13 illustrate scenarios. By repeating the experiment for the simulation to compare whether there is jamming or No-Jamming.

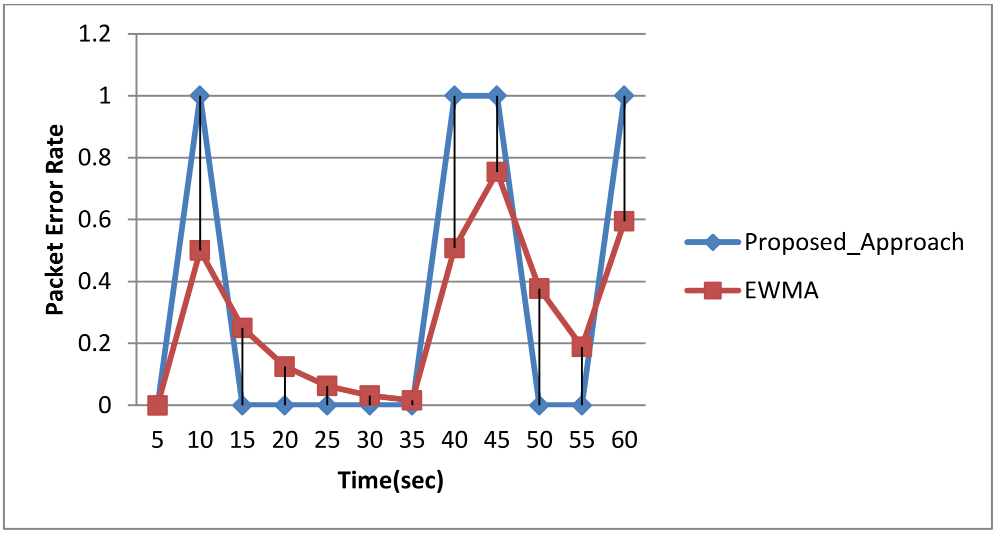

Fig. 10. *Packet Error Rate with No-jammer*

In Figure 11, it is shown that at no jamming, the SNR remains consistently high, around 2500, across all time points (5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, and 60 seconds). The random jamming ratio is also significantly lower, close to 0 due to background noise, across all time points. In the random jamming, no data is shown for the random jamming, indicating that it was not measured or that the SNR is negligible. In the absence of interference, the SNR is consistently high, indicating optimal signal quality. This is because a high and constant SNR results in a clear and strong signal, demonstrating optimal network conditions No-Jamming. The absence of jamming is critical, as evidenced by the high SNR values without any interference. Given the severe impact of random jamming on SNR, it is essential to implement effective anti-jamming measures to protect network performance.

In Figure 12, it is shown that No-Jammer the number of packet deliveries increases steadily over time, reaching approximately 14,000 packets at 60 sec. Random Jammer the number of packet deliveries also increases over time but at a slower rate, reaching about 10,000 packets at 60 sec. But in constant Jammer the number of packet deliveries increases at an even slower rate compared to the random jammer, reaching around 5,000 packets at 60 sec. The presence of a jammer (both random and constant) significantly reduces the number of packet deliveries compared to the scenario without a jammer. In No-Jammer the steady increase in packet deliveries indicates optimal network performance, with no interference affecting communication. Maintaining an environment free of jammers is crucial for achieving the highest number of packet deliveries and optimal network performance. Developing robust anti-jamming techniques is essential, especially to counter the severe impact of constant jammers.

In Figure 13, it is shown that the PER remains constant at 1 over specific time intervals (5, 10, 40, and 60 seconds). At other times, the PER is around 0.6. This is when the presence of jamming is ignored but other influences are present. In the case of random jamming, the PER exhibits a pattern similar to that of the no-jamming scenario, with spikes occurring at the same time intervals but generally staying at 1 throughout the measured periods. In the case of constant interference, the PER is more stable at around 0.6 across all time points, without the high spikes seen in the other two scenarios. Random jamming maintains a high PER of 1 consistently, like the peaks in the no-interference scenario. A high PER in the No-Jamming scenario over specific time intervals can indicate periods of network congestion or other temporary issues that cause packet errors, while a low PER at other times indicates normal operation. A consistently high PER of 1 in the case of random jamming indicates a severe impact on packet delivery, resulting in persistent packet errors during periods of jamming, and a consistent PER of 0.6 in the case of jamming indicates a persistent but moderate impact on packet errors, causing less error rate variability than random jamming. Understanding periods of high PER No-Jamming can help identify underlying issues that need to be addressed to improve network performance.

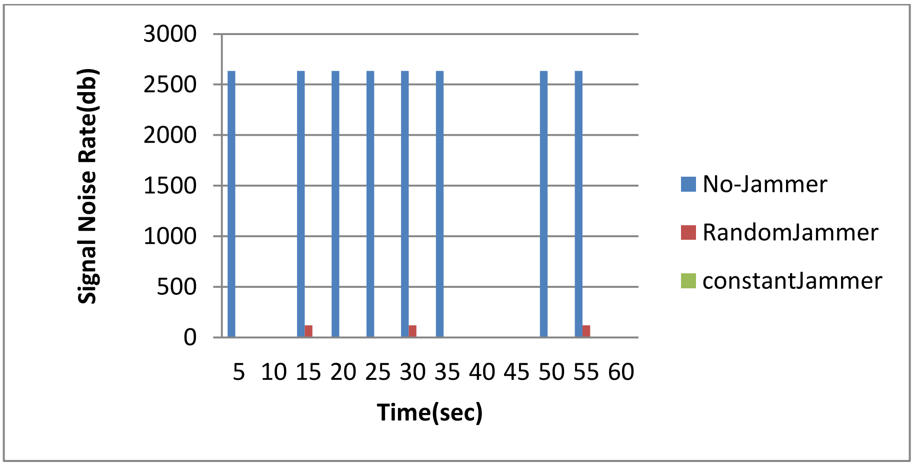

Fig. 11. *Signal to Noise Rate for Jamming and No-Jamming Scenarios.*

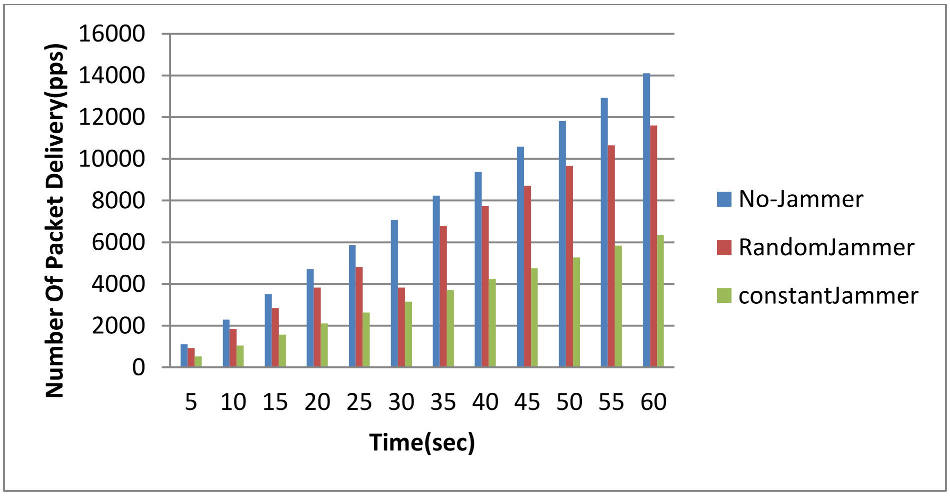

Fig. 12. *Number of Delivered Packets for Jamming and No-Jamming Scenarios.*

5.5. Evaluation using a Complex Network

This section presents and discusses the evaluation results of applying the proposed approach to jamming detection with increasing number of points and running the experiment with different simulation times. Figure 14 shows the PDR observations while a random jammer is applied in the WSN. It is shown that networks with fewer nodes (e.g., 4N) perform better at maintaining packet delivery under random jamming conditions than networks with more nodes (e.g., 100N). Larger networks with more nodes are more susceptible to performance degradation as jamming proceeds, but all node configurations eventually experience a significant decrease in PDR. This version of the figure assumes that N represents the number of nodes in the network, with the figure showing the effect of random jamming on packet delivery over time.

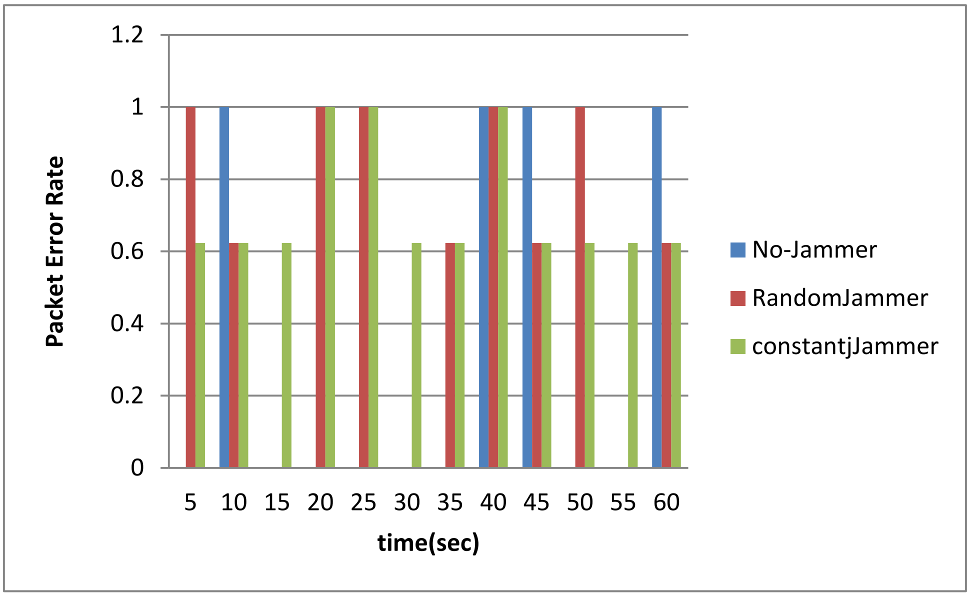

Fig. 13. *Packet Error Rate for Jamming and No-Jamming Scenarios*

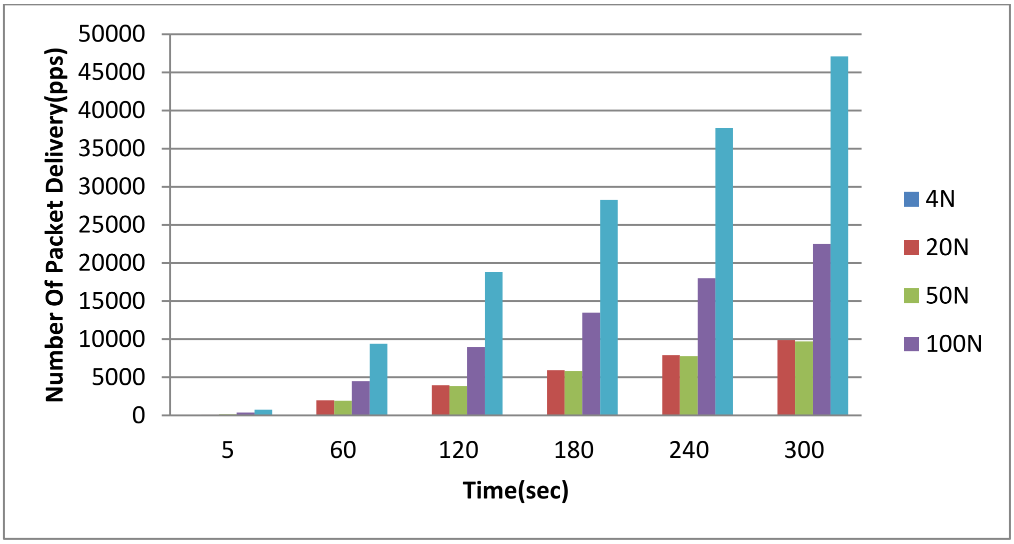

Fig. 14. *PDR observations while Random Jammer is applied in the WSN*

Figure 15 shows PDR observations while a constant jammer is applied in WSN. Figure 15, it is shown that the number of nodes increases, the impact of the constant jammer becomes more significant, as seen by the drastic drop in PDR for networks with higher node counts 100Node. Effect over time that the jamming effect is more prominent over time, reducing PDR values steadily, which shows that the longer the jammer operates the less effective the network becomes. This indicates that in scenarios with constant jamming, networks with fewer nodes maintain communication longer, but all configurations eventually degrade under continuous jamming pressure. The drop rate with 100 nodes may reach 98% loss of packages.

Figure 16 shows the PDR observations while applying the proposed approach in the absence of a jamming attack.it is shown that No-Jammer the number of packet deliveries increases steadily over time. Comparing this graph to the previous PDR under jamming, it is clear that jammer significantly reduces network performance across all configurations.NO-Jammer; PDR values remain significantly higher and degrade at a slower rate, especially for networks with more nodes. Larger networks with 100 nodes consistently deliver more packets over time, as they have higher PDR values throughout the experiment, while smaller networks degrade faster. The absence of jamming allows networks to maintain communication much longer, but PDR still decreases naturally as time progresses, indicating that smaller networks degrade faster.

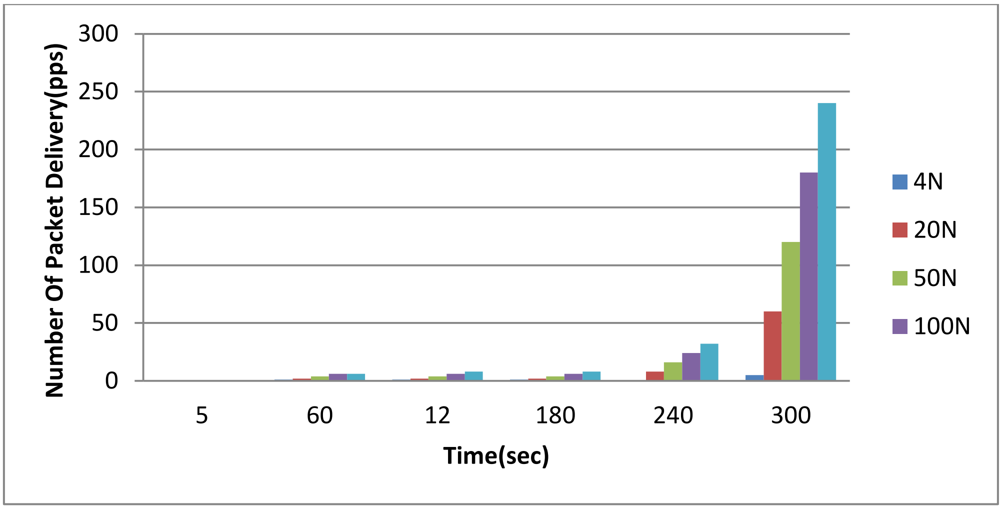

Fig. 15 *PDR observations while Constant Jammer is applied in the WSN*

6. Conclusions and Future Work

This paper presents a comprehensive analysis of the effects of jamming attacks on WSN, with an emphasis on Jamming attacks and the power efficiency of wireless systems is given in this paper. For evaluating network efficiency, three parameters were utilized: the number of packets delivered, noise signal, and packet error of the network. The proposed algorithms can detect network conditions caused by various types of jammers or caused. Using network statistics like PDR, SNR, and PER, this approach can identify signs of jamming attempts. The proposed approach is more accurate than EWMA since it is an empirical analysis of the network as opposed to EMWA which is based on statistical analysis of the network metrics. It has been noticed that jammer significantly reduces network performance across all configurations. With constant jamming, networks with fewer nodes can sustain communication for a longer period, but all configurations eventually degrade under continuous jamming pressure. In the case of 100 nodes, the packet loss can reach up to 98%.

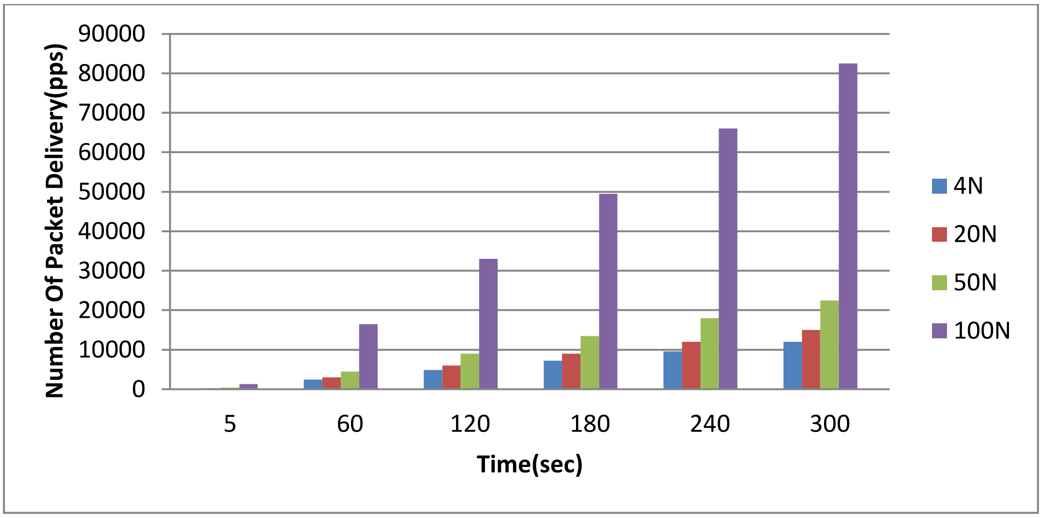

Fig. 16. *PDR Observations while no Jammer is applied in the WSN*

Another advantage is that no additional hardware is needed to implement existing algorithms on wireless sensor nodes. In the subsequent study, the algorithms will be implemented in real-world sensor networks to evaluate their performance. It will provide detailed insights into how the algorithms perform in a real environment. Future research will focus on analyzing a defense framework and exploring ways to adapt it to existing detection devices, aiming to develop unique methods for protecting against this type of attack and to design new energy-efficient MAC protocols.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376,2015.

[2] O. Osanaiye, A. S. Alfa, and G. P. Hancke, “A statistical approach to detect jamming attacks in wireless sensor networks,” Sensors, vol. 18, no. 6, p. 1691, 2018.

[3]. M. Li, I. Koutsopoulos and R. Poovendran, "Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks," in IEEE Transactions on Mobile Computing, vol. 9, no. 8, pp. 1119-1133. 2010.

[4] S. Bagali and R. Sundaraguru, "Efficient Channel Access Model for Detecting Reactive Jamming for Underwater Wireless Sensor Network," 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), Chennai, India, 2019, pp. 196-200.

[5] V. C. Manju and M. S. Kumar, "Detection of jamming style DoS attack in Wireless Sensor Network," 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, Solan, India, 2012, pp. 563-567.

[6] P. M. K. Kanagasabapathy, V. K. Poornachary, S. Murugan, A. Natesan, and V. Ponnusamy, “Rapid jamming detection approach based on fuzzy in WSN,” International Journal of Communication Systems, vol. 35, no. 2,. 2019.

[7]K. Vijayakumar, K. PradeepMohanKumar, K. Kottilingam, T. Karthick, P. Vijayakumar, P. Ganeshkumar, “An adaptive neuro-fuzzy logic based jamming detection system in WSN Soft”. Comput., 23 (8) (2019), pp. 2655-2667.

[8] M. Çakiroğlu and A. T. ÖzceriT, “Design and evaluation of a query-based jamming detection algorithm for wireless sensor networks,” TURKISH JOURNAL OF ELECTRICAL ENGINEERING & COMPUTER SCIENCES, Jan. 2011.

[9] B. Yu and L. Y. Zhang, “An improved detection method for different types of jamming attacks in wireless networks,” 2nd Int. Conf. Syst. Informatics, ICSAI 2014, no. Icsai, pp. 553–558, 2015.

[10] M. Hasana and H. A. Mustafa, “An Anti-Jamming technique by jammer localization for Multi-Channel wireless sensor networks,” International Journal of Computer Networks & Communications, vol. 16, no. 4, pp. 87–107, Jul. 2024.

[11] V. R. M and S. Malladi, “Improving Packet Delivery Ratio in Wireless Sensor Network with Multi Factor Strategies,” International Journal of Advanced Computer Science and Applications, vol. 12, no. 5. 2021.

[12] M.-J. Hao, W.-L. Tsai and Y.-C. Tsai, "Squared envelope-based SNR estimation", J. Chin. Inst. Eng., vol. 36, no. 6, pp. 810-818, 2013.

[13] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," in *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42-56, Fourth Quarter 2009.

[14]. V. C. Manju and M. S. Kumar, "Detection of jamming style DoS attack in Wireless Sensor Network," *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, Solan, India, 2012, pp. 563-567, 2012.

[15]. N. F. A. Al-Shaihk and R. Hassanpour, “Active Defense Strategy against Jamming Attack in Wireless Sensor Networks,” International Journal of Computer Network and Information Security, vol. 11, no. 11, pp. 1–13, 2019.

[16] R. Bhojani and R. Joshi, “An Integrated Approach for Jammer Detection using Software DefinedRadio,” ProcediaComputerScience, vol.79 pp.809–816,2016.

[17] W. Xu et al., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," MobiHoc '05: Proc. 6th ACM Int'l. Symp. Mobile Ad Hoc Net. and Camp., 2005, pp. 46-57.

[18]"INETFramework”. Retrieved 2022-12-22.[Online].Available:https://inet.omnetpp.org/ docs/users-guide.

[19] "INET framework for the OMNeT++ discrete event simulator. Retrieved 2022-12-22. [Online]. Available: https://omnetpp.org.

Vol. 12-2 (2025) 95-115
International Journal of Computers and Information
(IJCI)
Available online at *https://ijci.journals.ekb.eg/*

نهج تجريبي قائم على تحليل الشبكة للكشف عن هجمات التشويش في شبكات الاستشعار اللاسلكية

إلهام السيد حمزة*، عربي كشك*، أنس يوسف*

*قسم علوم الحاسب، كلية الحاسبات والمعلومات، جامعة المنوفية، شبين الكوم، مصر

الملخص باللغة العربية.

ظهرت شبكات الاستشعار اللاسلكية (WSNs) كحل شبكي متطور مع العديد من التطبيقات في مجالات مختلفة. وتشمل هذه المجالات البيئة، والعمليات العسكرية، والرعاية الصحية والزراعة. ومع ذلك، تتكون شبكات الاستشعار اللاسلكية من عقد استشعار معرضة لمخاطر أمنية متعددة، لأنها غالبًا ما يتم نشرها في مواقع معادية وغير مراقبة، ولديها موارد محدودة. يعد هجوم التشويش من بين أكثر أنواع الهجمات شهرة، والذي يعطل ويقلل من فعالية العمليات العادية لعقد الاستشعار في شبكات الاستشعار اللاسلكية. يتميز هجوم التشويش بإرسال إشارات للتدخل في الاتصالات المشروعة، مما قد يؤدي إلى رفض الخدمة لعقدة أو أكثر في الشبكة. يقترح هذا البحث نهجًا تجريبيًا قائمًا على تحليل الشبكة للكشف عن هجمات التشويش في شبكات الاستشعار اللاسلكية. يحدد هذا النهج الشذوذ الذي يشير إلى وجود هجمات تشويش من خلال تحليل مجموعة من إحصائيات الشبكة. تشمل الإحصائيات التي تم تحليلها نسبة توصيل الحزمة (PDR) ونسبة الإشارة إلى الضوضاء (SNR) ومعدل خطأ الحزمة (PER) للحزم التي تستقبلها عقد الاستشعار. تستهدف عملية الكشف نوعين مختلفين من هجمات التشويش، وهما هجمات التشويش المستمرة والعشوائية. تتم مقارنة النهج المقترح بالنهج الإحصائي للمتوسط المتحرك المرجح بشكل أسّي .(EWMA) أظهرت نتائج المحاكاة من محاكي الأحداث المنفصلة ++OMNeT القائم على التتبع أن النهج المقترح يكتشف هجمات التشويش في شبكات الاستشعار اللاسلكية بفعالية ودقة مع تقليل تكلفة الكشف. النهج المقترح أكثر دقة من EWMA لأنه يعتمد على تحليل تجريبي قائم على المحاكاة للشبكة على عكس EMWA الذي يعتمد على التحليل الإحصائي النظري لمقاييس شبكة الاستشعار اللاسلكية. يقدم النهج المقترح باستمرار عددًا أكبر من الحزم مقارنةً بـ EWMA عبر جميع الفترات الزمنية، حيث يحقق النهج المقترح ما يقرب من 6000 حزمة تم تسليمها، في حين يبلغ EWMA حوالي 5200 حزمة.