International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

Analysis of Behavioral Characteristics of Jammers to Detect Malicious Nodes in Mobile ADHOC Networks

Dr. Adilakshmi Yannam[1], Basaveswara Mukesh Suryadevara[2], Thabassum[3], V. Mohan Sai[4], Manoj Vatturi[5]
[1]Professor, Department of Computer Science and Engineering. Seshadri Rao Gudlavalleru Engineering College
Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru
Gudlavalleru, India
laxmi072003@gmail.com
[2]Student, Department of Computer Science and Engineering. Seshadri Rao Gudlavalleru Engineering College
Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru
Gudlavalleru, India
suryadevarabasaveswaramukesh@gmail.com
[3]Student, Department of Computer Science and Engineering. Seshadri Rao Gudlavalleru Engineering College
Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru
Gudlavalleru, India
thabassumbaig7722@gmail.com
[4]Student, Department of Computer Science and Engineering. Seshadri Rao Gudlavalleru Engineering College
Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru
Gudlavalleru, India
vutukurimohansai@gmail.com
[5]Student, Department of Computer Science and Engineering. Seshadri Rao Gudlavalleru Engineering College
Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru
Gudlavalleru, India
manojvatturi10@gmail.com

Abstract— Wireless ADHOC Networks are used to establish a wireless connection between two computing devices without the need for a Wi-Fi access point or router. This network is decentralized and uses omnidirectional communication media, which makes it more vulnerable to certain types of attacks compared to wired networks. Jamming attacks, a subset of denial-of-service (DoS) attacks, involve malicious nodes that intentionally interfere with the network, blocking legitimate communication. To address this issue, the proposed method analyzes various characteristics of nodes, such as packets sent, received, and dropped, at each node. Using the packet delivery ratio and packet drop ratio, the method detects jamming nodes from normal nodes, improving network performance. The network is simulated in NS2 environment.

Keywords - ADHOC, DoS, Jamming attack, and NS2.

I. INTRODUCTION

Wireless networking is crucial for achieving ubiquitous computing, which enhances the quality of human life by providing uninterrupted connectivity and services through network devices embedded in various environments. However, wireless networks are more susceptible particular attacks. Radio frequency signals have a particular characteristic such that all devices within the spatial coverage receive the signals. This makes the wireless signal vulnerable to attacks. Attackers often prefer more sophisticated attacks, like the MitM (Man-in-the-Middle) attack, where they attempt to secretly place themselves between the sender and receiver to gain data control and potentially alter or develop it. Furthermore, the exposed nature of wireless links makes them susceptible to jamming attacks, which can result in Denial-of-Service (DoS) problems and higher-layer security issues that are not always adequately addressed.

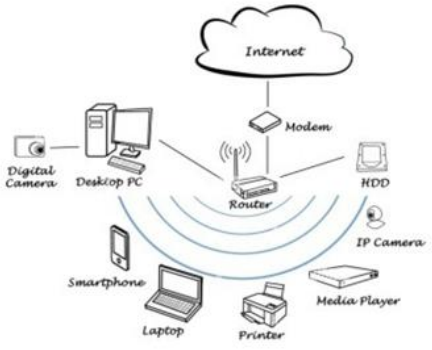


Fig. 1.1

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

In the present day, any node or device connected to the internet can be accessed from anywhere in the world, which makes them susceptible to attacks. This vulnerability is particularly true for personal computers (PCs) or laptops, which are highly susceptible to various attacks, including Ransomware, Malware, Fileless Attacks, Phishing, MitM (Man-in-the-Middle) Attack, Malicious Apps, DoS (Denial of Service) Attack, and Zero-Day Exploit.

Wireless jamming is a term that describes the act of intentionally interfering with wireless signals to disrupt ongoing wireless communication. This can lead to a decrease in the signal-to-noise ratio at the receiver's end. In contrast to unintentional interference that can be caused by microwaves or other wireless devices, jamming is a deliberate attempt to disrupt communication. Typically, an attacker initiates this kind of interference to disrupt communication. Jamming can cause disruptions in various ways, such as hindering transmission or distorting legitimate communication packets. Jamming is distinct from typical network interference because it is a intentional attempt to disrupt communication using wireless signals, whereas interference is an unintentional form of disruption.

To explore wireless network jamming, two primary aspects need to be investigated: 1) the types of jammers that are currently in use and 2) the challenges created by jamming attacks. It is essential to comprehend how jammers can affect wireless networks, and for that reason, we scrutinize the different techniques that jammers can use to jam networks. This involves a detailed analysis of constant jammers, periodic jammers, and random jammers. Additionally, we explore the problems that arise during or after a jamming attack.

The act of jamming involves the deliberate usage of radio signals to disrupt wireless communications by either maintaining the communication medium occupied or affecting the turn off the transmitter when the medium is busy. Jamming is mainly aimed at attacks on the physical layer, but attacks on other layers are also possible. This section contains, details on different types of jammers.

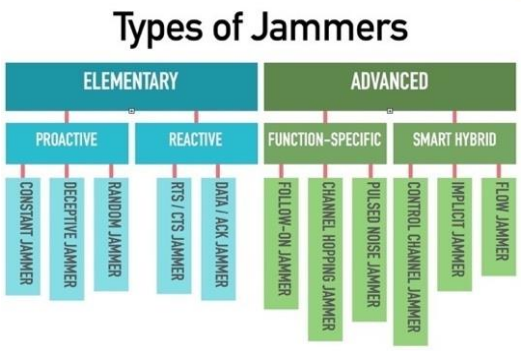


Fig.1.2

II. LITERATURE SURVEY

The researchers *Y. Adilakshmi et al.* (2022) of the paper [1] proposes A new and innovative method for address the problem of nodes that act maliciously in Mobile Ad-hoc Networks (MANET) by employing the algorithms used in Machine Learning, in particular Decision Tree and SVM (Support Vector Machine). One of the most common attacks in MANET is the Blackhole attack, where a malicious node enters the network and drops packets instead of forwarding them. The proposed approach detects attacker nodes using machine learning algorithms and compares the network's performance parameters before and after applying the ML algorithms, including Residual Energy, Throughput, Packet Delivery Ratio, and Average End to End delay. The outcomes demonstrated that the suggested approach is effective for networks in order to detecting malicious nodes and improves its overall efficiency of the network. By improving the security of MANET against malicious attacks, this research contributes to the advancement of network security.

The current study by author *Abinaya R. et al.* (2021) [2] suggests a digital healthcare system that allows patients to create, compile, and save PHR (Personal Health Records). There is a need for greater focus on cost-effectiveness and faster response times in the public cloud platform. The suggested model for healthcare systems utilizes the publisher-observer pattern, which enables patients to review and amend their personal health records (PHRs) before any computations are performed. The cloud system operates as a backend framework that provides an accessible and transparent environment.

In [6], the authors *S. Shrestha et al.* (2020) proposed an innovative algorithm called RREP which modifies the information in control packets such as sequence number typically used in the AODV (Ad-Hoc On-Demand Distance Vector) routing protocol. The presented algorithm's performance was evaluated and compared to conventional intrusion detection techniques, resulting in its superiority over them. The paper was published in the International Electrical Engineering Congress (IEEE) and can be a valuable reference for researchers interested in securing Mobile Ad-hoc Networks (MANETs) against blackhole attacks using the RREP algorithm.

The authors *Y. Adilakshmi et al.* (2019) in reference [7] proposed a method to detect intrusion attacks during the communication between mobile nodes in order to ensure uninterrupted data transmission. In their approach, they selected a monitoring node based on a trust value metric, which is a measure of the node's reliability and reputation. To further enhance the security of the data content, the authors also used a new secret key generation method for encryption. By using this

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

method, the data transmission was protected from intruders who might try to intercept and access the data without authorization. Overall, the proposed method provides a robust solution for securing data transmission in mobile ad-hoc networks.

The paper [8] presented by *Y. Adilakshmi et al.* (2019) introduces a CIDS (Cooperative Intrusion Detection System) to improve or increase the level of security Mobile Ad-hoc Networks (MANETs). To avoid computation overhead and network failure, a secondary server is selected to perform intrusion detection. The paper proposes the use of a Modified Ant colony algorithm to determine the optimal secondary server. Intrusion detection is performed by learning the traffic variation between different traffic patterns using a modified Support Vector Machine (SVM) approach. Simulation results using NS2 indicate that CIDS has a better intrusion detection probability than existing works. The proposed system can help in improving the security of MANETs by detecting intrusions in a timely and efficient manner.

The research work presented by *Y. Guo et al.* in 2019 [9] proposed an incentive-based intrusion detection method aimed at enhancing the level of security in the system by increasing the intrusion detection ratio. A game-theoretic method was utilized to effectively carry out intrusion detection in this approach. The method also introduced a punishment appeal mechanism that further improved the efficiency of intrusion detection. By implementing this approach, the research aimed to improve the security level of the system as a whole in terms of its performance, and the findings demonstrated that this method was effective in achieving this goal.

The paper [10] proposed by *S. Bambang et al.* (2019) states a method for detecting fake access points in wireless networks by analyzing the Media Access Control and Basic Service Set Identifier addresses in beacons. This approach provides the benefit of being lightweight and simple to implement, making it suitable for use on mobile devices. However, the authors acknowledge that this method has limitations and may not be able to detect fake access points created by advanced attackers who can replicate all the static information of a legitimate access point. While this method may not be foolproof, it still offers a valuable tool in the arsenal of wireless network security and can help detect basic types of fake access points.

In [15], the authors *B. Alotaibi et al.* (2016) highlight that as per the guidelines of the IEEE 802.11 protocol, there exist only a available data rates and modulation types are restricted in number. The likelihood is high that transmission rate adaptation algorithm of the attacker's fake access point will use the identical data rate or modulation scheme as the authorized access point, particularly in the case that they are functioning on the identical frequency channel and are located in close proximity. As a result, the fake access point of attacker's may go undetected using the modulation-based detection method.

In some studies, authors have proposed methods for Identifying fraudulent access points by measuring and evaluating the beacon signals received. For example, in *Kao et al.* (2014) [16], researchers suggest that detecting deviations in the beacon interval can be utilized for the identification of counterfeit access points. However, researchers assumed may be attacker has already succeeded in order to synchronize sequence numbers, clock skew elimination, and copy all static information. The proposed method involves examining numerous beacon frames, the interval between the beacon frames of either the fake access point or the authentic access point will eventually deviate. However, the method by which the attacker can synchronize the sequence number is not described by the authors and prevent the clock skew of fake access point. Furthermore, In the event that the attacker has the ability to precisely control the timing of the bogus access point, they can quickly detect any deviation and adjust the beacon interval accordingly.

In (2013) [17], *Jadhav and Patil Jadhav* proposed a new technique in order to detect attacks like DDOS, called the OEB (Objective Entropy-Based) method. This technique works by predicting DDOS attacks which has low rate variation in packet transfers between destination and the source nodes is used to learn about the network. The approach finds more effective than detecting DDoS attacks in the traditional methods. However, one of major drawbacks by the specified technique is that intrusion detection may be imprecise due to the slight difference between attack and normal traffic. Compared to other methods, this approach is more likely to produce false positive rate.

The author *N. Sufyan et al.* (2013) [18] proposed a three-dimensional model for detection of attacks in 802.11b radio networks such as jamming. This model considers three parameters, Packet Delivery Ratio, PW (pulse width) , and signal strength of the signal, which leads to a notable enhancement in precision and better classification of jamming attacks. The authors highlight pulse width, signal strength variation, and Packet Delivery Ratio and were observed to produce results that are consistent with the findings. Model that is presented has shown to be effective in detecting attacks in wireless networks such as jamming attacks and its types.

In their work (2013) [19], *Khairnar and Kotecha* emphasize the difficulties of deploying VANETs and mechanisms for routing efficiently. They contrast the results of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

three protocols for routing, they are AODV, DSR, and GPSR, where they are based on discovery of different gateway and topology updating algorithms. They conduct simulations using SUMO and NS2 simulators to evaluate the protocols based on measures like throughput, loss of packets, packet delivery ratio, and end-to-end delay for different scenarios. The authors analyze the simulation results to provide useful insights for the development and deployment of VANET protocols. Overall, their study highlights the importance of effective routing mechanisms for the successful deployment of VANETs.

In their study, *Cheng T et al.* (2012) [21] produced a method known as Double Circle Localization (DCL) for addressing an issue on localization of the jammer in wireless networks. The authors considered a scenario where all nodes are static in the nature in the network and deployed randomly and can detect if they are being jammed. For detecting the jammer location, proposed algorithm computes the minimum bounding circle and maximum inscribed circle for the all the compromised nodes convex hull. Algorithm's performance was tested through experiments, evaluating its accuracy, efficiency, and robustness using the free-space propagation model. The results showed, DCL approach performs better compared to other methods, this makes it a potentially effective method for identifying the location of jammers in wireless networks.

Author *D. Torrieri et al.* (2012) [22] suggests a different approach for locating compromised nodes in a wireless network. Unlike many existing methods that rely on the information about the group of nodes that have been intentionally disrupted (jamming nodes) this method focuses on locating the node that has been breached (compromised node) can be identified by analyzing its spread-spectrum signal transmission with a recognized key. One main advantages of this approach is it does not require any assumptions regarding the propagation model of the signal. This approach can be useful in situations where there is little or no information about the jammer or the jammed nodes.

In the article [23], the authors *Han C et al.* (2012) present a method of verifying the authenticity of a wireless access point by comparing its information from beacon, like the service set identifier, type of authentication, and type of cipher. They argue that authentication type and cipher type are vendor-specific and added using the firmware of WLAN card, making it difficult to the attackers to copy them. However, some authors have published tutorials on modification of firmware of different WLAN cards, suggesting that this information may not always be reliable. To improve accuracy, the combination of other methods comparison of information such as IP addresses from static beacon information or identifiers of environment, which are located on remaining layers of the Open Systems Interconnection model. These additional pieces of information are used to enhance the accuracy of identifying fake access points.

The authors of the paper [25] *Chumchu P et al.* (2011) proposed a method to detect the Man-in-the-Middle (MITM) attacks. They did this by analyzing the information provided in beacon frames such as data rate and modulation type, the transmission rate adaptation algorithm defines it. The researchers claimed that their approach is created by the manufacturers of Wireless LAN cards and that modulation type and the data rate change based on the channel's status, so it's not easy to the attackers for manipulating. The writers presented method is effective in finding out attacks such as MITM by conducting experiments in various environments and under different scenarios.

The paper [26] by *Liu Hongbo et al.* (2011) presents the Virtual Force Iterative Localization algorithm, so it aims to enhance the accuracy of the Centroid Localization method. VFIL considers the jammed nodes distribution and uses a iterative method called as virtual-force to adjust the estimation of the jammer's location. The study conducted by the authors involves comparing the performance of VFIL with other localization algorithms, such as CL. The results indicate that VFIL performs better than CL when it comes to localization accuracy, particularly in situations where only a small number of nodes are jammed. These findings offer valuable insights into enhancing jammer localization techniques in wireless networks.

Y. Xiang et al. (2011) [27] suggested a novel approach for identifying and projecting Distributed Denial of Service attacks in low rate on a network by utilizing metrics based on entropy. This method measures the generalized entropy between the traffic of normal network and DDoS attack traffic to accurately predict the presence DDoS attacks with a low rate. The authors also compare their method with the traditional Shannon entropy method and explained their presented approach has a better performance. The evaluation of this method is based on two metrics, namely false positive rate and distance gap, and the latter is adjusted to ensure reliable and accurate prediction of DDoS attacks. The study shows that this method can effectively detect and predict low-rate DDoS attacks, which are difficult to detect using traditional techniques.

The authors *C. Arackaparambil et al.* (2010) [28] present a technique for detecting fake access points by using clock difference, also known as clock skew. The authors explain that they can differentiate between the beacons transmitted by the genuine access point and those emitted by using the timestamp clock skew between beacons for analyzing the fake access. Even though this methodology is dependable in recognizing counterfeit access points, its implementation may

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

pose a challenge. Furthermore, other researchers have discovered that attackers clock skew can be altered in order to reducing their before creating a fake access point by doing this attackers project them self's as legitimate nodes, rendering this technique less effective.

A innovative strategy for analysing ad hoc networks whether there is a jamming attack performed was presented by *A. Hamieh et al.* (2009) in reference [29]. Their method relies on analyzing the relationship between the duration of error and the time of correct reception. The concept of this paper is to identify a particular jamming type where the jammer only emits when valid radio activity is detected from its radio hardware. To detect such attacks, the transmission node measures the Error Probability and the Correlation Coefficient between the reception error time and the correct reception time. Provided that the Correlation Coefficient is greater than the relative Error Probability, then the network can be classified as jammed. This method allows for detecting jamming attacks without relying on signal strength or channel characteristics, making it a valuable tool in environments with high levels of noise or interference.

The paper by *J. Blumenthal et al.* (2007) [30] introduces the Weighted Centroid Localization method, which enhances the traditional Centroid Localization technique by considering the influence of jammed nodes during the localization process. WCL assigns weights to each jammed node and modifies its contribution when determining the network's centroid. These weights are calculated using the estimated distance between both the jammer as well as the impacted nodes, which might be calculated by evaluating the radio signal's strength coming in. If the jammed node is nearer to the jammer, the higher its weight will be. This approach provides a more accurate estimation of the jammer's location than CL, which assumes equal contribution from all nodes in the network.

In their paper [31], *Guo and Chiueh* (2005) proposed a technique for identifying fraudulent access points through examining the gaps between sequence numbers in beacon frames. The authors found that in usual conditions, the difference in sequence numbers between two consecutive beacons is usually less than or equal to 8. If the difference between sequence numbers is larger than 8, then it indicates the presence of a fake access point. While this method is reliable, attackers can potentially examine the time-based variation in the gap between sequence numbers, predict it, and modifying the beacon interval of a fake access point to avoid triggering sequence number gap significant fluctuations. In addition, they may employ jamming signals or requests for probe to interfere with the mechanism for detecting or counting the legitimate access point.

III. PROPOSED METHODOLOGY

Jamming is a type of harmful act where wireless communications are disrupted intentionally by lowering the signal-to-noise ratio at the recipient side with the use of disrupting radio waves. Jamming is different from unintentional interference as it is a deliberate attempt to disrupt wireless communications. The interference can occur due to wireless transmissions between devices within a network or from auxiliary devices like microwaves and radio frequency controllers. In contrast, deliberate interference is usually done by attackers to disrupt network communications. Jamming can have different effects on communications, ranging from impeding transmission to distorting packets in genuine communications. The present work examines three types of jamming attacks: constant, periodic, and random attacks, investigating their characteristics, effects on wireless communications, and the most effective placement of jammers to increase the area impacted by jamming.

In the context of wireless communications, a Constant Jammer is a malicious entity that continuously sends arbitrary bits without adhering to the CSMA protocol, which legitimate nodes use to determine the state of the radio frequency spectrum prior to transmission. When the network is idle for a DCF Interframe Space interval, a node is expected to transmit a frame, and if busy, it should abstain from transmitting. However, a Constant Jammer constantly occupies the medium, obstructing legal nodes from collaborating. Despite being inefficient in terms of energy consumption and easy to detect, this form of attack can still result in significant harm to network communications, culminating in communication breakdowns. This research focuses on the influence of constant jamming breaches on wireless interference as well as investigates methods for detecting and mitigating them.

A periodic jammer disrupts wireless communication by generating jamming signals, in which the duration of the period of inactivity that occurs between consecutive transmissions follows the jamming rate R specifies an exponential distribution.. This allows the jammer to adjust the timing of its transmissions to create periodic interference. Like the constant jammer, the periodic jammer also ignores the CSMA protocol and keeps the channel constantly busy, making it difficult for legitimate nodes to communicate with each other. However, periodic jamming is a more efficient way to attack wireless networks because it can cause significant disruption to network communications while conserving energy. Since it can imitate the behaviour of legitimate network traffic, the periodic jamming attack is also challenging to detect.

Random jamming attacks are a type of malicious activity where wireless networks are interrupted by sporadically

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

transmitting unpredictable bits or normal packets to interfere with communication. Unlike constant and periodic jammers, this jammer's primary goal is to save energy by switching between two states: sleep and jamming phases. During the sleep phase, the jammer conserves energy, while in the jamming phase, it transmits jamming signals intermittently. The length of time for sleep and jamming can be predetermined or randomized, and the jammer needs to balance the amount of disruption with energy conservation because jamming is not feasible during the sleep periods. To optimize the trade-off between effectiveness and efficiency, the jammer can control the proportions of the sleep and jamming intervals. The random jamming attack is challenging to detect since it can mimic the behaviour of legitimate network traffic, making it an effective way to disrupt wireless communications while conserving energy.

The performance of a network can be negatively impacted by jamming attacks, the development of a new detection method was prompted by this. Identifying malicious nodes in wireless mobile networks susceptible to jamming attacks, the behavioural characteristics of nodes of type normal, constant, periodic and random jammers were observed with 10 number of nodes among which some nodes behaving like genuine and one will behave like abnormal node in one simulation later two of them behave like malicious nodes and again five of them showing abnormal attitude .From this network implementation, the characteristics such as the count of packets that were transmitted, received, or lost at specific nodes during simulation times are collected and analyzed with the help of line graphs. These characteristics were collected from normal nodes and jamming nodes under various simulation times. Based on the analysis of these characteristics in a simulated network environment, he ratio of packets that are delivered successfully and the ratio of packets that are dropped were calculated and observed at each node to identify malicious behaviour.

The process starts with the creation of a network and assigning properties to it. Later, at the beginning of the simulation, both benign and malicious nodes are created, each with specific characteristics. Once the connections are established, all nodes, including the malicious ones, start their communication. After the simulation is completed in the NS2 environment, a trace file is generated, containing data such as packets sent, received, and dropped by all nodes. From this data, the packet delivery ratio and packet drop ratio are calculated. Based on these ratios, jammers are detected. The process of the proposed work is illustrated in the flowchart that has been given below.

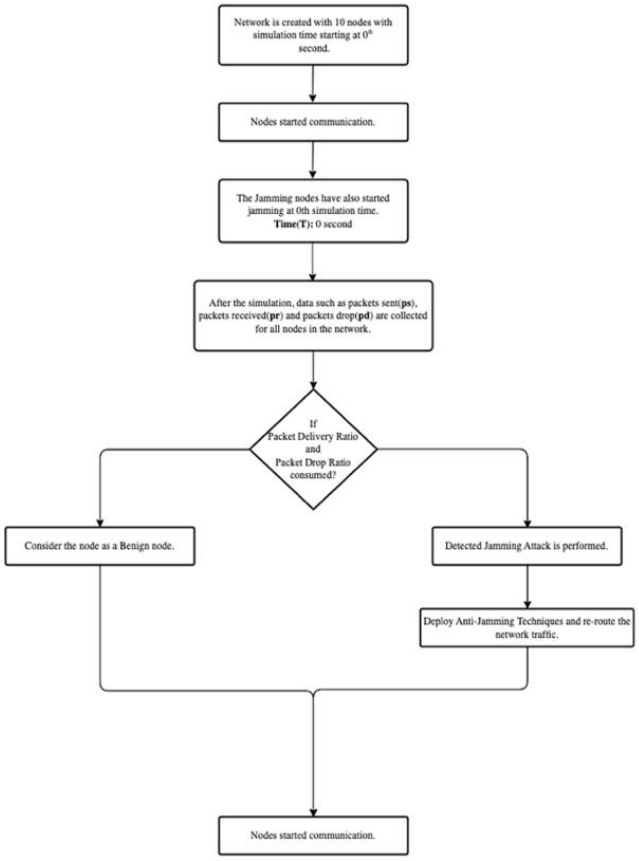


Fig. 3.1

IV. RESULTS

The network that was established includes a total of 10 nodes, which comprise both malicious and legitimate nodes, and each node has specific properties that were taken into consideration during their creation.

```
set val(chan)     Channel/WirelessChannel      ;# Channel type
set val(prop)     Propagation/TwoRayGround     ;# Radio-Propagation model
set val(netif)    Phy/WirelessPhy              ;# Network interface type
set val(mac)      Mac/802_11                   ;# MAC Type
set val(ifq)      Queue/DropTail/PriQueue      ;# Interface Queue Type
set val(ifqlen)   1048576;                     ;# 1 MB Queue Length (2^20 bytes)
set val(ll)       LL                           ;# Link Layer Type
set val(ant)      Antenna/OmniAntenna          ;# Antenna Model
set val(rp)       DSDV                         ;# Routing Protocol
set mal_per       [lindex $argv 1]             ;# Initializing the malicious percentage
```

Fig. 4.1

This is the simulation of a wireless network consisting of 10 nodes with randomized positions for each simulation. The lines connecting the nodes indicate that they can communicate with each other within the network.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

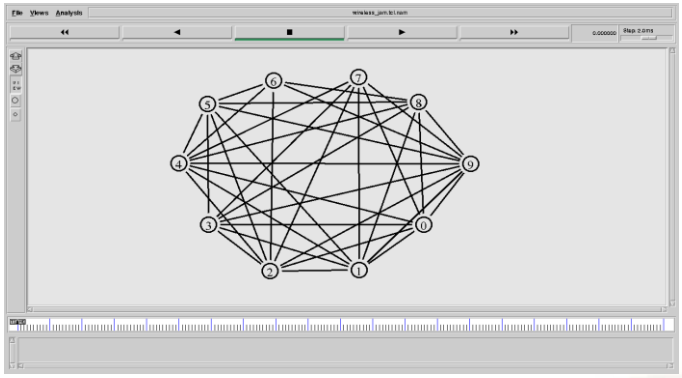


Fig. 4.2

The network with 10 nodes is simulated, and the behavioural characteristics are observed and analyzed based on various factors to detect the presence of malicious nodes, such as constant, periodic, and random jamming attacks. The observed results for packets sent, received, and dropped at various nodes were plotted and discussed in the following order.

1. Network simulation with presence of normal nodes and two attacker nodes.
2. Network simulation with presence of normal nodes and five attacker nodes.

I. *Constant Attack*

1. *Packets Sent*

a. *Benign node*

1. A plot, labeled as Fig 4.3(C).1.1.1, represents the behaviour of a benign node 2 under constant attack by two attackers. Over the course of 20 seconds of simulation time, the packets sent by node 2 remain approximately constant.

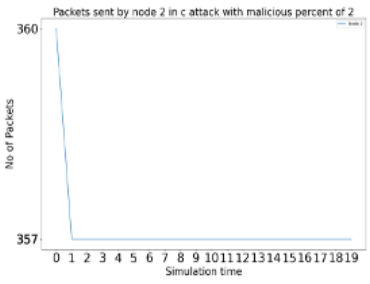


Fig. 4.3(C).1.1.1

2. Fig 4.3(C).1.1.2 displays the behavior of benign node 2 during a constant attack with 5 attackers. The graph shows that the quantity of packets transmitted by the particular node 2 remains constant over the entire 20-second simulation period. This behavior is similar to that observed when there are only 2 attackers, but the count of packets that have been transmitted varies with the count of individuals performing malicious activities.

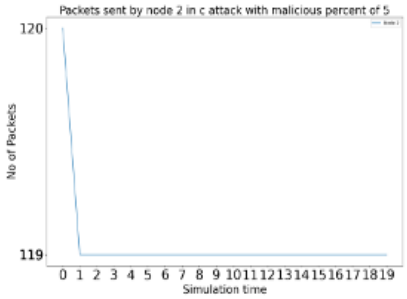


Fig. 4.3(C).1.1.2

b. *Malicious nodes*

1. Two Figs, namely Fig 4.3(C).1.2.1(a) and Fig 4.3(C).1.2.1(b), are drawn to represent the packets sent by malicious nodes 8 and 9 under a constant attack with two attackers. The behavior of packets sent by both malicious nodes is identical, showing a meandering pattern and keeping the number of packets sent approximately constant throughout the simulation time.

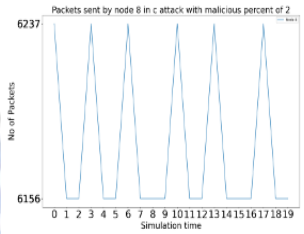


Fig. 4.3(C).1.2.1(a)

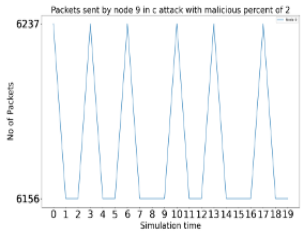


Fig. 4.3(C).1.2.1(b)

2. Figs 4.3(C).1.2.2(a), (b), (c), (d), and (e) show the results for malicious nodes 5, 6, 7, 8, and 9, respectively, under constant attack by five attackers. The packets sent by all these malicious nodes exhibit similar behaviour, with the number of packets sent remaining constant in a meandering pattern throughout the 20-second simulation period.

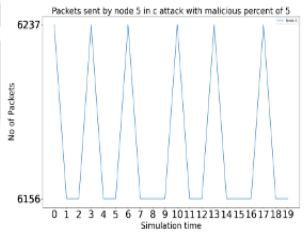


Fig. 4.3(C).1.2.2(a)

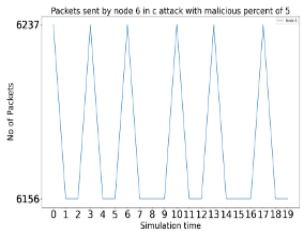
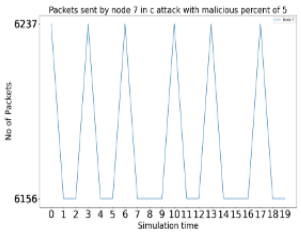


Fig. 4.3(C).1.2.2(b)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*



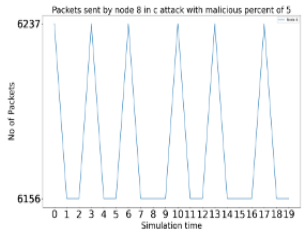


Fig. 4.3(C).1.2.2(c) Fig. 4.3(C).1.2.2(d)

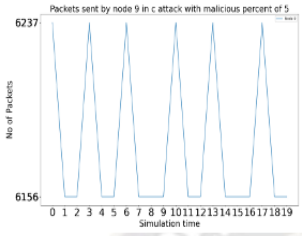


Fig. 4.3(C).1.2.2(e)

2. *Packets Received*
   a. *Benign node*
      1. Throughout the simulation time, the packets received by node 2 with two attacker nodes are decreasing in a meandering manner.

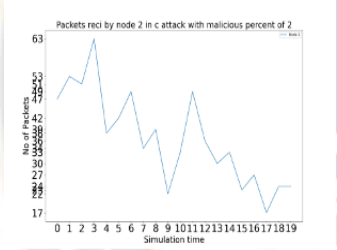


Fig. 4.3(C).2.1.1

      2. While simulating a network that had 5 attacker nodes, the packets received by node 2 demonstrated an upward trend that was simple to examine.

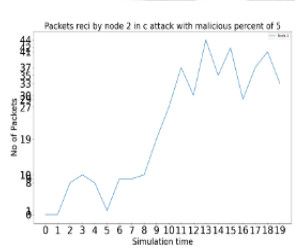
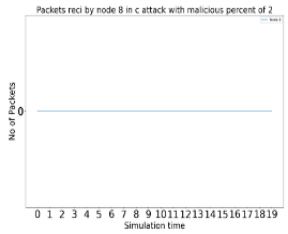


Fig. 4.3(C).2.1.2

   b. *Malicious nodes*
      1. Throughout the simulation, nodes 8 and 9 did not receive any packets at any point in time.



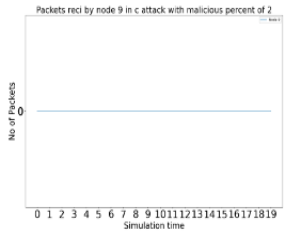
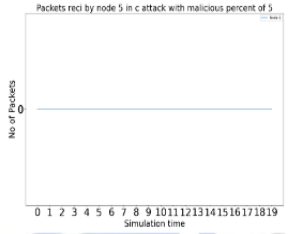


Fig. 4.3(C).2.2.1(a) Fig. 4.3(C).2.2.1(b)

      2. During the simulation with 5 attacker nodes, the malicious nodes 5, 6, 7, and 9 did not receive any packets throughout the simulation time. However, node 8 received some packets in an irregular manner, with a maximum of 9 packets received.



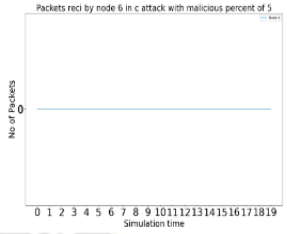
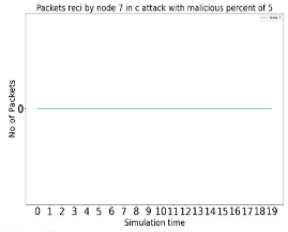


Fig. 4.3(C).2.2.2(a) Fig. 4.3(C).2.2.2(b)



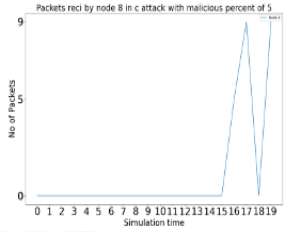


Fig. 4.3(C).2.2.2(c) Fig. 4.3(C).2.2.2(d)

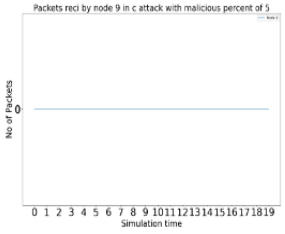


Fig. 4.3(C).2.2.2(e)

3. *Packets Dropped*
   a. *Benign nodes*
      1. Initially, during the beginning of the simulation time, the node 2 experienced a high quantity of packets that were not successfully transmitted. However, as the simulation time nears its conclusion, which was 15 to 20 seconds duration, there was a significant reduction in the quantity of packets that were not successfully delivered at node 2.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

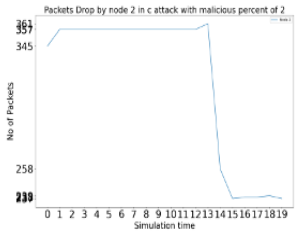


Fig. 4.3(C).3.1.1

2. During the entire duration of the simulation, the quantity of packets that were not successfully transmitted by node 2 with 5 attacker nodes remained constant.

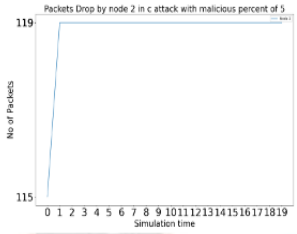


Fig. 4.3(C).3.1.2

b. *Malicious nodes*

1. The quantity of packets that were not delivered by the nodes considered to be malicious, specifically nodes 8 and 9 is exhibiting a similar behaviour to that of the benign node 2, where there is a notable reduction in the amount of packets that are not delivered.

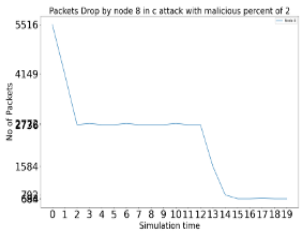


Fig. 4.3(C).3.2.1(a)

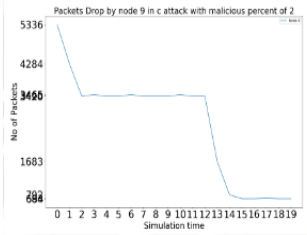


Fig. 4.3(C).3.2.1(b)

2. The behavior of the packets dropped by malicious nodes 5, 6, 7, 8, and 9 is the same as that of the packets dropped by malicious nodes 8 and 9 when there are 2 attacker nodes present.

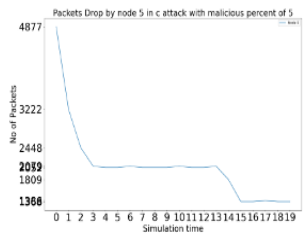


Fig. 4.3(C).3.2.2(a)

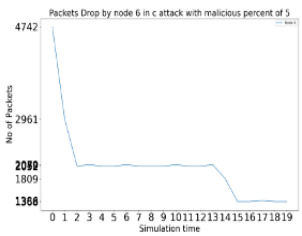


Fig. 4.3(C).3.2.2(b)

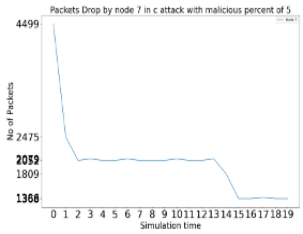


Fig. 4.3(C).3.2.2(c)

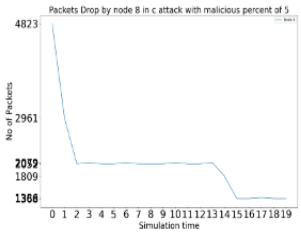


Fig. 4.3(C).3.2.2(d)

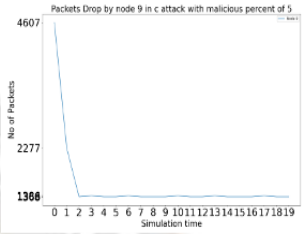


Fig. 4.3(C).3.2.2(e)

II. *Periodic Attack*

1. *Packets Sent*

a. *Benign node*

1. The Fig 4.4(P).1.1.1 illustrates the behaviour of benign node 2 in the presence of two attackers under periodic attack. The packets sent by the node 2 show a similar characteristic to the packets sent by benign node 2 in constant attack. However, there is a slight variation in the number of packets sent.

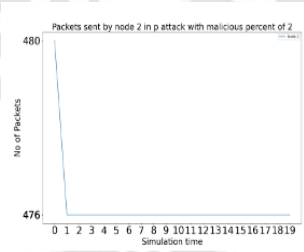


Fig. 4.4(P).1.1.1

2. Fig 4.4(P).1.1.2 displays the behaviour of a benign node 2 when under periodic attack by 5 attackers. The number of packets sent by node 2 remains almost constant throughout the entire 20-second simulation period. Similar to the behaviour observed in a benign node 2 under constant attack by 2 attackers, the node exhibits similar characteristics under periodic attack.

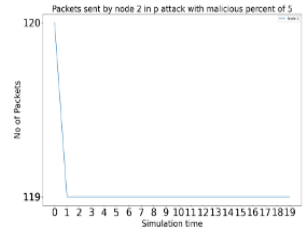


Fig. 4.4(P).1.1.2

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

b. *Malicious nodes*

1. The Figs 4.4(P).1.2.1(a) and 4.4(P).1.2.1(b) show the behaviour of malicious nodes 8 and 9, respectively, under periodic attack in a network simulation. The packets sent by these nodes exhibit periodic behaviour throughout the simulation time. This is because each node has its own time period for transmitting packets, and when there is an augmentation in the quantity of data packets sent during a particular second, it indicates that the corresponding malicious node is active during that period of simulation time.

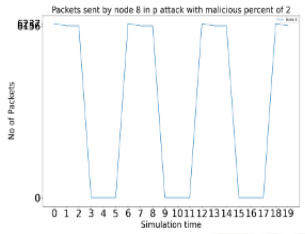


Fig. 4.4(P).1.2.1(a)

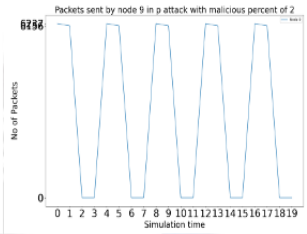


Fig. 4.4(P).1.2.1(b)

2. Fig 4.4(P).1.2.2(a) represents the behaviour of malicious node 5, Fig 4.4(P).1.2.2 (b) shows the behaviour of malicious node 6, Fig 4.4(P).1.2.2 (c) depicts the behaviour of malicious node 7, Fig 4.4(P).1.2.2 (d) displays the behaviour of malicious node 8, and Fig 4.4(P).1.2.2 (e) shows the behaviour of malicious node 9 during a periodic attack scenario with 5 attackers. The packets sent by all the malicious nodes 5, 6, 7, 8, and 9 exhibits a periodic behaviour, but the number of packets sent remains constant throughout all the malicious nodes.

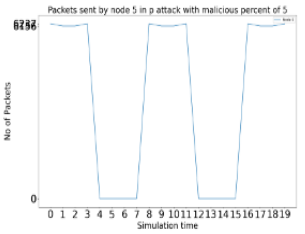


Fig. 4.4(P).1.2.2(a)

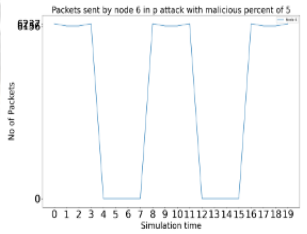


Fig. 4.4(P).1.2.2(b)

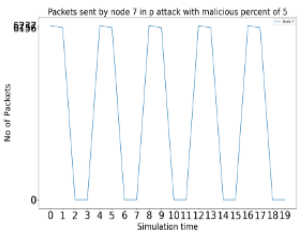


Fig. 4.4(P).1.2.2(c)

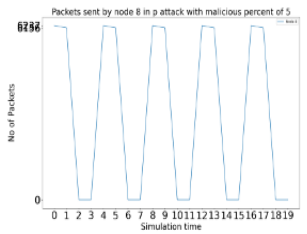


Fig. 4.4(P).1.2.2(d)

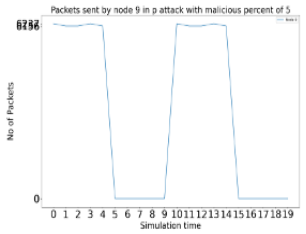


Fig. 4.4(P).1.2.2(e)

2. *Packets Received*

a. *Benign node*

1. During the entire 20-second simulation duration, the packets received by node 2 display a fluctuating pattern, gradually decreasing. This behaviour is similar to that of packets received by benign node 2 under constant attack.

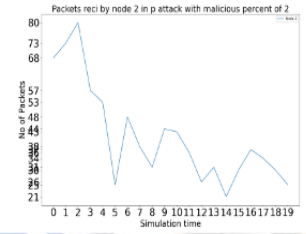


Fig. 4.4(P).2.1.1

2. The simulation, node 2 did not receive any packets at any point in time.

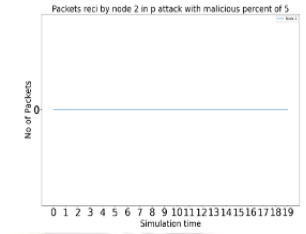


Fig. 4.4(P).2.1.2

b. *Malicious nodes*

1. The malicious nodes 8 and 9 did not receive any packets.

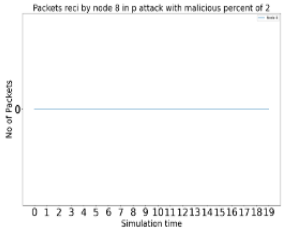


Fig. 4.4(P).2.2.1(a)

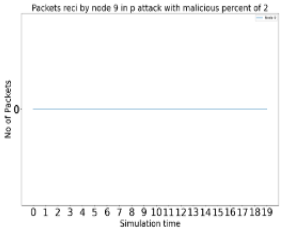


Fig. 4.4(P).2.2.1(b)

2. Throughout the simulation time with 5 attacker nodes, the malicious nodes 5, 6, 7, and 9 did not receive any packets. However, node 8 received some packets, specifically 14 packets.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

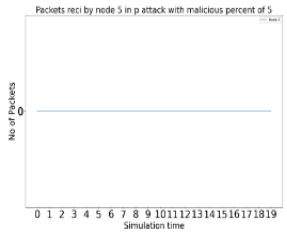


Fig. 4.4(P).2.2.2(a)

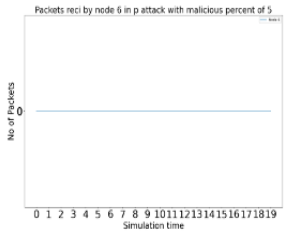


Fig. 4.4(P).2.2.2(b)

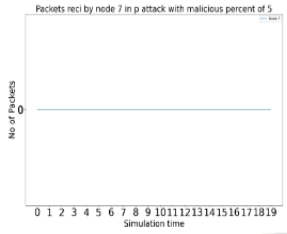


Fig. 4.4(P).2.2.2(c)

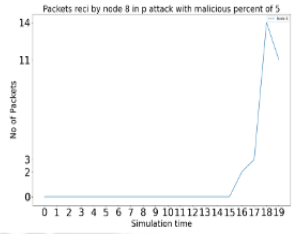


Fig. 4.4(P).2.2.2(d)

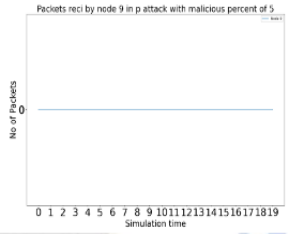


Fig. 4.4(P).2.2.2(e)

3. *Packets Dropped*
   a. *Benign nodes*
      1. At the beginning of the simulation period, the number of packets dropped by node 2 was initially high. However, as the simulation progresses, it has been noticed that there is an exponential decrease in the number of dropped packets.

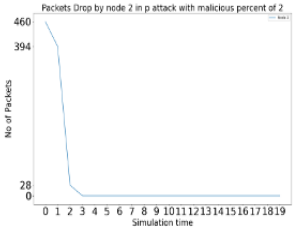


Fig. 4.4(P).3.1.1

      2. The packet drop rate of node 2 in the presence of 5 attacker nodes decreases gradually as the simulation time increases, and this behaviour is similar to that of benign node 2 when there are only 2 attackers present.

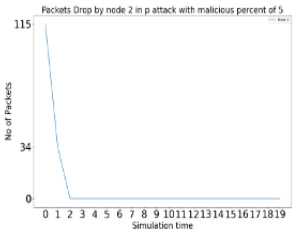
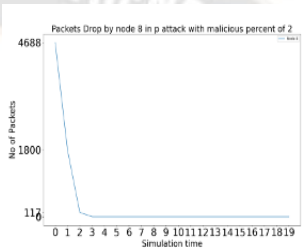


Fig. 4.4(P).3.1.2

   b. *Malicious nodes*
      1. There is a decrease in the count of packets that were not successfully delivered by the nodes 8 and 9, which are considered malicious.



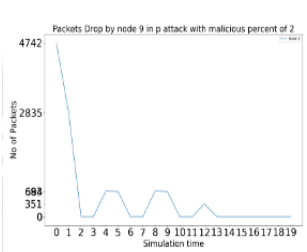
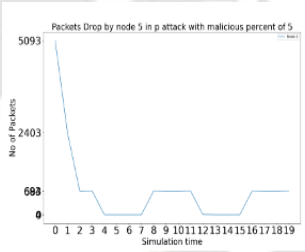


Fig. 4.4(P).3.2.1(a) Fig. 4.4(P).3.2.1(b)

      2. The packets dropped by all of the malicious nodes, including nodes 5, 6, 7, 8, and 9, exhibit a similar behaviour to that of attacker nodes 8 and 9. Initially, number of dropped packets exhibits a notable reduction.



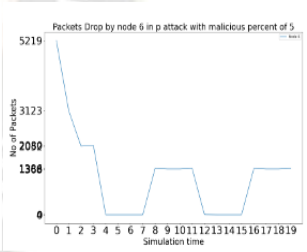
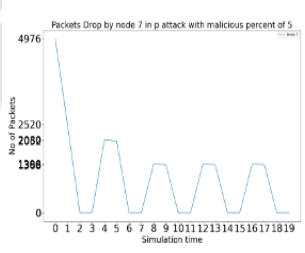


Fig. 4.4(P).3.2.2(a) Fig. 4.4(P).3.2.2(b)



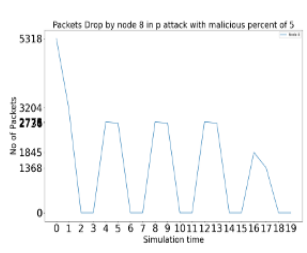


Fig. 4.4(P).3.2.2(c) Fig. 4.4(P).3.2.2(d)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

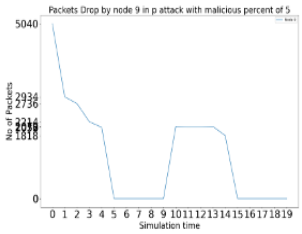


Fig. 4.4(P).3.2.2(e)

III. *Random Attack*

1. *Packets Sent*

a. *Benign node*

1. The Fig 4.5(R).1.1.1 depicts the behavioural characteristics of benign node 2 in a network simulation with 2 attackers under random attack. The packets sent by node 2 show a similar pattern as those sent by benign node 2 in constant and periodic attacks, but with a slight variation in the number of packets sent.

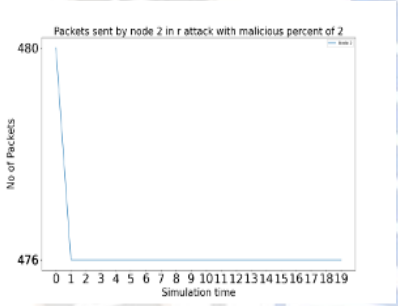


Fig. 4.5(R).1.1.1

2. The following information pertains to a simulation conducted on a network with 5 attackers under random attack. A Fig, denoted as 4.5(R).1.1.2, was created to represent the behaviour of a benign node, specifically node 2. The packets sent by node 2 are approximately constant throughout the entire 20-second simulation period. Furthermore, it was observed that the behavioural characteristics of node 2 with 5 attackers were similar to those of node 2 with 2 attackers, with the only difference being the number of packets sent.

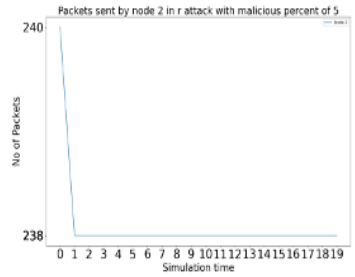


Fig. 4.5(R).1.1.2

b. *Malicious nodes*

1. Figs 4.5(R).1.2.1(a) and 4.5(R).1.2.1(b) show the performance of malicious nodes 8 and 9 in a network simulation with 2 attackers under random attack. It can be observed from the Figs that the packets sent by the malicious nodes 8 and 9 demonstrate an random behavior during the entire simulation time, which cannot be attributed to any specific pattern.

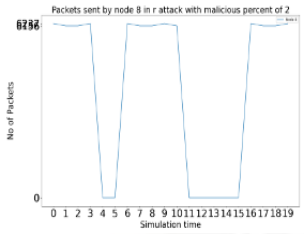


Fig. 4.5(R).1.2.1(a)

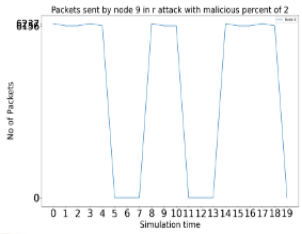


Fig. 4.5(R).1.2.1(b)

2. The Fig 4.5(R).1.2.2(a) corresponds to the behaviour of malicious node 5, Fig 4.5(R).1.2.2 (b) corresponds to the behaviour of malicious node 6, Fig 4.5(R).1.2.2 (c) corresponds to the behaviour of malicious node 7, Fig 4.5(R).1.2.2 (d) corresponds to the behaviour of malicious node 8, and Fig 4.5(R).1.2.2 (e) corresponds to the behaviour of malicious node 9 when there are 5 attackers under random attack. The packets sent by all the malicious nodes 5, 6, 7, 8 and 9 exhibit similar pattern as of when there are 2 attackers but maintain a constant number of packets sent throughout the simulation time.

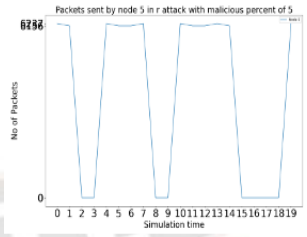


Fig. 4.5(R).1.2.2(a)

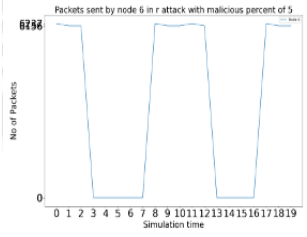


Fig. 4.5(R).1.2.2(b)

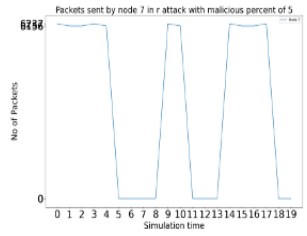


Fig. 4.5(R).1.2.2(c)

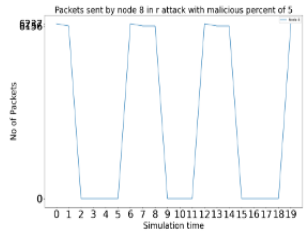


Fig. 4.5(R).1.2.2(d)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

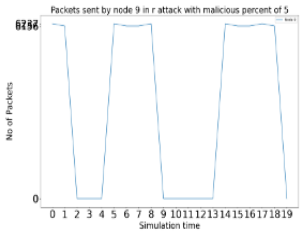


Fig. 4.5(R).1.2.2(e)

2. *Packets Received*
   a. *Benign node*
      1. Throughout the simulation time, the packets received by node 2 are observed to decrease in a meandering manner. This behaviour is similar to the packets received by nodes under constant and periodic jamming attacks.

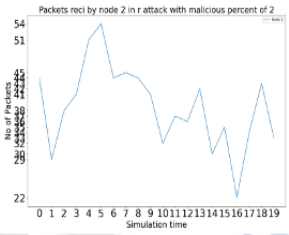


Fig. 4.5(R).2.1.1

      2. There are no packets received by node 2 when there are 5 attackers.

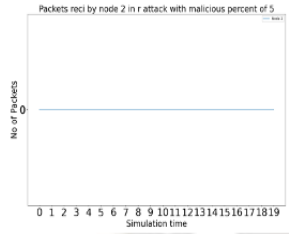


Fig. 4.5(R).2.1.2

   b. *Malicious nodes*
      1. Nodes 8 and 9, which are malicious nodes, did not receive any packets.

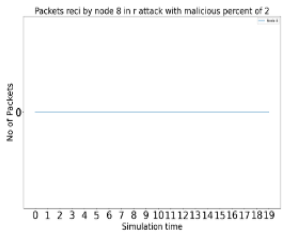


Fig. 4.5(R).2.2.1(a)

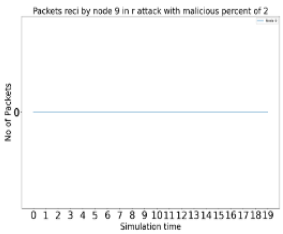


Fig. 4.5(R).2.2.1(b)

      2. Throughout the simulation time with 5 attacker nodes, the malicious nodes 5, 6, 7, 8, and 9 did not receive any packets.

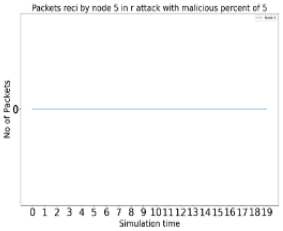


Fig. 4.5(R).2.2.2(a)

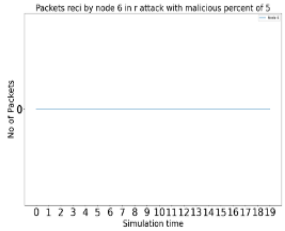


Fig. 4.5(R).2.2.2(b)

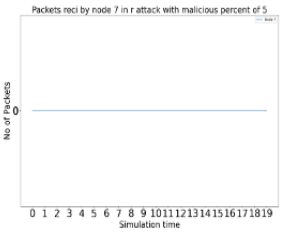


Fig. 4.5(R).2.2.2(c)

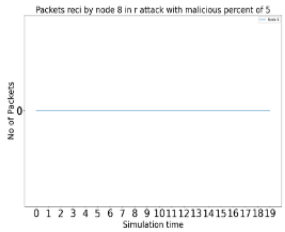


Fig. 4.5(R).2.2.2(d)

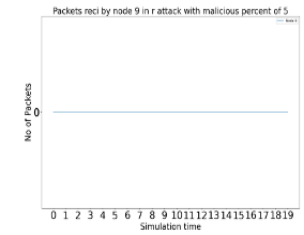


Fig. 4.5(R).2.2.2(e)

3. *Packets Dropped*
   a. *Benign nodes*
      1. The packets dropped by node 2 shows a gradually decrease in a stepwise manner over the course of the simulation time.

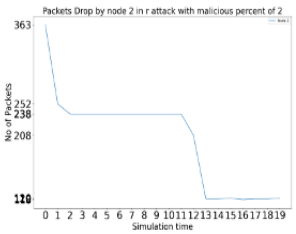


Fig. 4.5(R).3.1.1

      2. The behaviour of packet dropping by node 2 with the presence of 5 attacker nodes is observed, and it is noted that the number of packets dropped decreases in steps with the simulation time.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

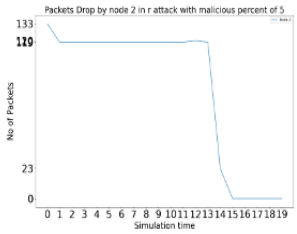


Fig. 4.5(R).3.1.2

b. *Malicious nodes*

1. There is a decrease in the count of packets that were not successfully delivered by the nodes 8 and 9, which are considered malicious following a similar pattern.

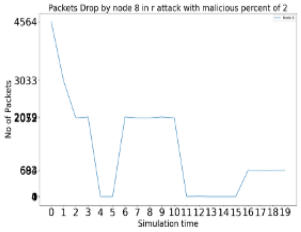


Fig. 4.5(R).3.2.1(a)

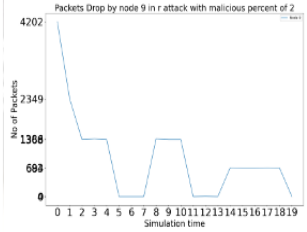


Fig. 4.5(R).3.2.1(b)

2. All the malicious nodes have dropped a certain number of packets, including nodes 5, 6, 7, 8, and 9, exhibit similar behaviour, demonstrating a notable reduction in the quantity of packets that were not successfully transmitted.

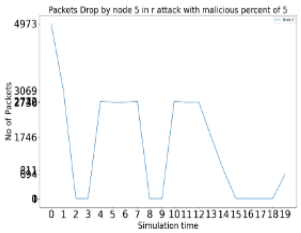


Fig. 4.5(R).3.2.2(a)

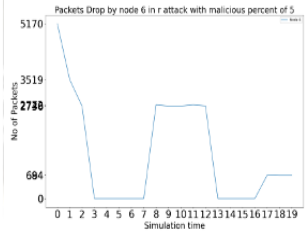


Fig. 4.5(R).3.2.2(b)

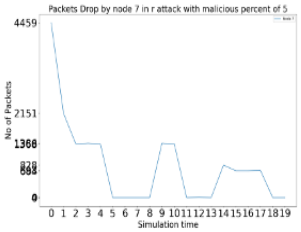


Fig. 4.5(R).3.2.2(c)

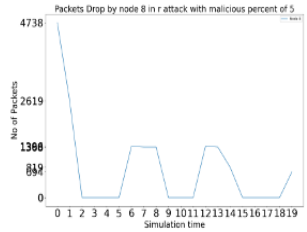


Fig. 4.5(R).3.2.2(d)

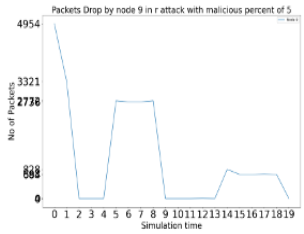


Fig. 4.5(R).3.2.2(e)

Packet Delivery Ratio:

Packet delivery ratio (PDR) is a crucial metric that measures the effectiveness of data transmission in a network by determining The proportion of packets that were effectively transmitted to their intended destination compared to the total number of packets sent. A high PDR suggests an efficient network, whereas a low PDR indicates a problem that needs to be addressed. This metric is especially critical in applications where data transmission reliability is vital, providing a quantitative measure of the network's reliability to ensure that packets are being delivered reliably and efficiently.

$$\text{Packet Delivery Ratio} = \frac{\sum(\text{Number of Packets Delivered to Destination})}{\sum(\text{Total Number of Packets Sent})} * 100$$

The packet delivery ratio is calculated using the data extracted from the trace file. The data collected provides a representative sample of the actual data, including different percentages of malicious nodes ranging from 0.0 to 0.5, along with their behaviour during constant, periodic, and random attacks. The collected data is presented in the following section.

Packets Sent:

Malicious Nodes	Nodes	0	1	2	3	4	5	6	7	8	9	Total Sent
0	0	0	2383	2383	2383	0	0	0	0	2383	0	9532
	1	2383	0	2383	0	2383	0	2383	2383	0	0	11915
	2	0	2383	0	0	2383	0	2383	0	0	2383	9532
	3	2383	2383	2383	0	0	0	2383	0	2383	2383	14298
	4	0	0	2383	0	0	0	2383	2383	2383	0	9532
	5	2383	2383	0	0	2383	0	0	0	0	0	7149
	6	2383	2383	2383	2383	2383	2383	0	0	0	0	14298
	7	2383	0	2383	0	2383	0	0	0	0	0	7149
	8	2383	2383	2383	2383	0	0	2383	2383	0	2383	16681
	9	2383	2383	2383	2383	0	2383	2383	2383	0	0	16681
1	0	0	2383	0	0	2383	0	0	0	2383	0	7149
	1	2383	0	2383	0	2383	0	0	0	0	0	7149
	2	0	2383	0	2383	2383	0	0	0	2383	0	9532
	3	0	2383	0	0	0	0	2383	2383	0	0	7149
	4	2383	2383	2383	2383	0	0	2383	0	0	0	11915
	5	0	2383	2383	2383	0	0	2383	0	2383	0	11915
	6	0	2383	2383	0	2383	0	0	2383	2383	0	11915
	7	0	0	0	2383	0	0	2383	0	0	0	4766
	8	2383	2383	2383	2383	2383	2383	2383	0	0	0	16681
	9	13743	13743	13743	13743	13743	13743	13743	13743	13743	0	123687

Fig. 4.6.1

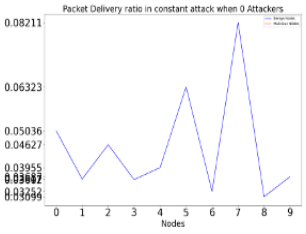
Packets Received:

Malicious Nodes	Nodes	0	1	2	3	4	5	6	7	8	9	Total Received
0	0	0	189	0	291	0	0	0	0	0	0	480
	1	232	0	0	0	0	0	157	42	0	0	431
	2	0	136	0	0	0	0	188	0	0	117	441
	3	214	88	0	0	0	0	142	0	0	71	515
	4	0	0	0	0	0	0	246	131	0	0	377
	5	290	162	0	0	0	0	0	0	0	0	452
	6	202	74	0	177	0	12	0	0	0	0	465
	7	298	0	289	0	0	0	0	0	0	0	587
	8	156	25	123	128	0	0	78	0	0	7	517
	9	201	77	0	180	0	14	129	14	0	0	615
1	0	0	209	0	0	233	0	0	0	0	0	442
	1	247	0	186	0	143	0	0	0	0	0	576
	2	0	107	0	0	130	0	0	0	0	0	237
	3	0	123	0	0	0	0	173	49	0	0	345
	4	179	51	98	0	0	0	101	0	0	0	429
	5	0	64	183	111	0	0	114	0	0	0	472
	6	0	94	210	0	118	0	0	21	0	0	443
	7	0	0	0	312	0	0	258	0	0	0	570
	8	177	53	115	22	76	0	103	0	0	0	546
	9	397	0	0	0	0	0	0	0	0	0	397

Fig. 4.6.2

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

The packet delivery ratios are calculated for all the nodes and displayed below.



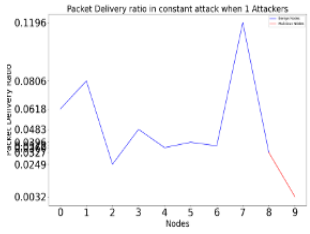
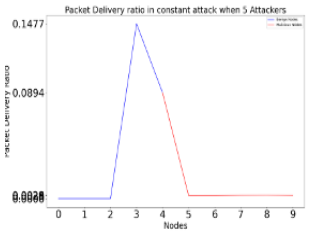


Fig: 4.6.3 (constant attack 0 attackers) Fig: 4.6.4 (constant attack 1 attackers)



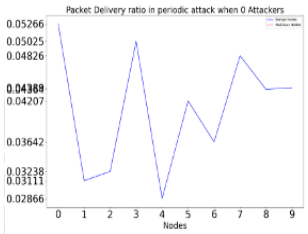
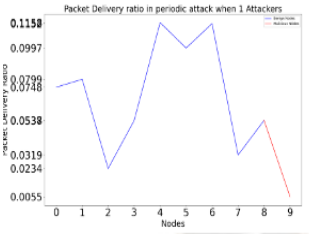


Fig: 4.6.5 (constant attack 5 attackers) Fig: 4.6.6 (periodic attack 0 attackers)



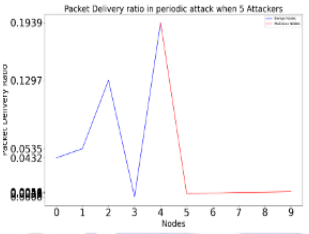
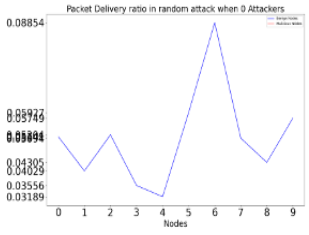


Fig: 4.6.7 (periodic attack 1 attackers) Fig: 4.6.8 (periodic attack 5 attackers)



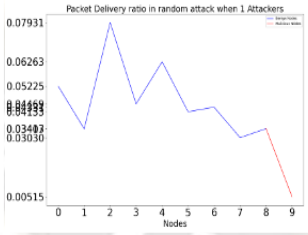


Fig: 4.6.9 (random attack 0 attackers) Fig: 4.6.10 (random attack 1 attackers)

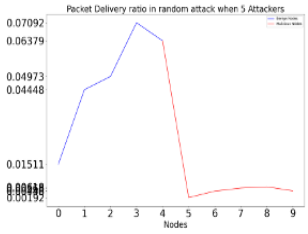


Fig: 4.6.11 (random attack 5 attackers)

Packet Drop Ratio:

Packet drop ratio (PDR) is a crucial metric that calculates the percentage of lost or dropped packets during network transmission. It indicates the efficiency and quality of the network and is particularly significant in applications where data transmission reliability is essential. High PDR can cause poor application performance or complete data loss, while low PDR ensures reliable data transmission and optimal network performance. PDR helps network administrators to identify and troubleshoot network issues promptly, making it an essential metric for measuring network reliability and efficiency.

$$\text{Packet Drop Ratio} = \frac{\sum(Number\ of\ Packets\ Not\ Delivered\ to\ the\ Destination)}{\sum(Total\ Number\ of\ Packets\ Sent)} * 100$$

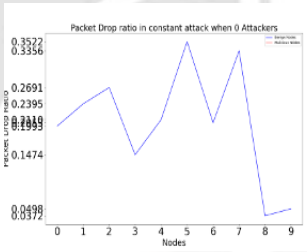
The packet drop ratio is calculated using the same data collected for calculating the ratio of packets that are successfully transmitted and received, which includes The quantity of data packets sent. The data that has been collected is utilized to compute the ratio of packets that were dropped.

Packets Dropped:

Malicious Nodes	Nodes	0	1	2	3	4	5	6	7	8	9	Total Drop	Packet Drop Ratio
0	0	0	132	195	29	0	0	0	0	1544	0	1900	0.199328577
	1	5	0	194	0	2382	0	79	194	0	0	2854	0.239530004
	2	0	132	0	0	2204	0	79	0	0	150	2565	0.26909358
	3	8	133	194	0	0	0	79	0	1544	150	2108	0.147433207
	4	0	0	194	0	0	0	79	194	1544	0	2011	0.210973563
	5	4	132	0	0	2382	0	0	0	0	0	2518	0.352217093
	6	4	132	194	29	2382	194	0	0	0	0	2935	0.205273465
	7	4	0	13	0	2382	0	0	0	0	0	2399	0.335571409
	8	2	132	34	29	0	0	79	194	0	150	620	0.037168035
	9	8	132	194	29	0	194	79	194	0	0	830	0.049757209
1	0	0	129	0	0	105	0	0	0	1798	0	2032	0.284235557
	1	1	0	62	0	105	0	0	0	0	0	168	0.02349979
	2	0	129	0	1228	106	0	0	0	1798	0	3261	0.342110785
	3	0	129	0	0	0	0	78	202	0	0	409	0.057210799
	4	1	129	81	376	0	0	78	0	0	0	665	0.055812002
	5	0	129	9	81	0	0	78	0	1798	0	2095	0.175828787
	6	0	129	13	0	105	0	0	202	1798	0	2247	0.188585816
	7	0	0	0	25	0	0	78	0	0	0	103	0.021611414
	8	5	129	66	159	105	206	78	0	0	0	748	0.044841436
	9	17	769	1007	13742	625	1210	472	1192	10399	0	29433	0.237963569

Fig. 4.7.1

The packet drop ratios are calculated for all the nodes and displayed below.



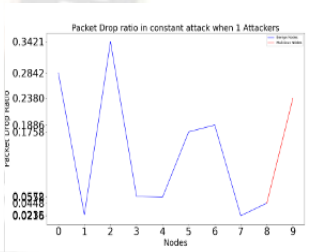
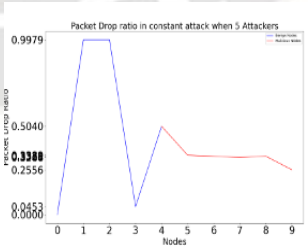


Fig: 4.7.2 (constant attack 0 attackers) Fig: 4.7.3 (constant attack 1 attackers)



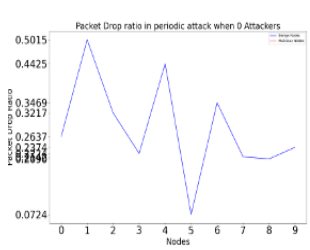


Fig: 4.7.4 (constant attack 5 attackers) Fig: 4.7.5 (periodic attack 0 attackers)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

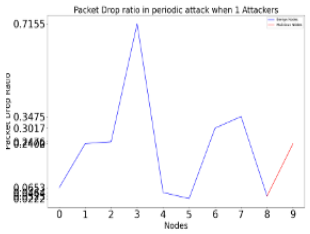


Fig: 4.7.6 (periodic attack 1 attackers)

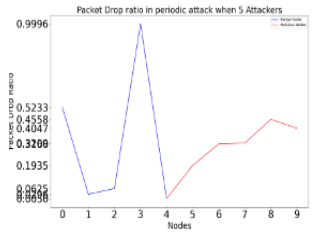


Fig: 4.7.7 (periodic attack 5 attackers)

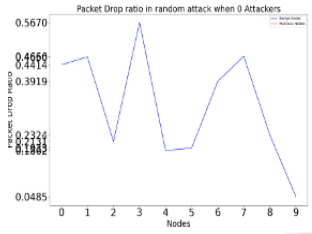


Fig: 4.7.8 (random attack 0 attackers)

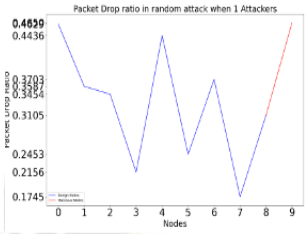


Fig: 4.7.9 (random attack 1 attackers)

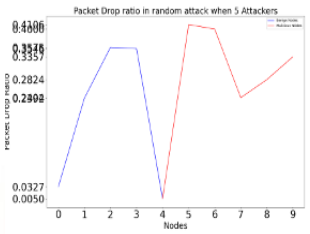


Fig: 4.7.10 (random attack 5 attackers)

V. CONCLUSION

The paper presented the detection mechanism to detect various jamming attack nodes in MANET. The network is created and simulated in NS2 tool with 10 nodes out of which all the nodes are behaving like normal nodes at one time later some of the nodes shows normal behavior and other nodes shows different jamming behavior like constant, periodic and random jammers varying from single attack node to multiple attack nodes. Then the like packet sent, received and dropped collected from trace file and analyzed using python scripts, from these characteristics the packets delivery ratio and packet drop ratio calculated and based on this behavior the malicious node was detected by this the network performance can be unproved by re-routing the network. In future, the behavioral analysis of jamming nodes can also be classified using Machine Learning Algorithms.

REFERENCES

[1] Adilakshmi, Y. (2022). Node Behaviour Classification Using SVM & Decision Tree to Detect Malicious Nodes in MANET. The International Journal of Analytical and Experimental Modal Analysis, ISSN NO: 0886-9367.

[2] Indira, D.N.V.S.L.S., Abinaya, R., et al. (2021). Secured Personal Health Records using Pattern Based Verification and 2-Way Polynomial Protocol in Cloud Infrastructure. International Journal of Ad Hoc and Ubiquitous Computing, 40(3), 86-93. ISSN: 1743-8233.

[3] Singh, S. ., Wable, S. ., & Kharose, P. . (2021). A Review Of E-Voting System Based on Blockchain Technology. International Journal of New Practices in Management and Engineering, 10(04), 09–13. https://doi.org/10.17762/ijnpme.v10i04.125.

[4] Kim, J., Biswas, P. K., Bohacek, S., Mackey, S. J., Samoohi, S., & Patel, M. P. (2021). Advanced protocols for the mitigation of friendly jamming in mobile ad-hoc networks. Journal of Network and Computer Applications, 181, 103037.

[5] Bhavani M., & M. Durgadevi. (2023). Streamlined Classification of Microscopic Blood Cell Images. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 57–62. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2477.

[6] S. Shrestha, R. Baidya, B. Giri, and A. Thapa, "Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol," in 2020 8th International Electrical Engineering Congress (iEECON), Chiang Mai, Thailand, 2020, pp. 1-4, doi: 10.1109/iEECON48109.2020.229555.

[7] Adilakshmi, Y., & Prasad, G. V. S. N. R. V. (2019). Trust aware intrusion detection system to defend attacks in MANETs. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(6), 1298-1304.

[8] Adilakshmi Y, & G. V. S. N. R. V. Prasad. "Cooperative intrusion detection system to enhance the security in MANET." Journal of Advanced Research in Dynamical and Control Systems 11, no. 2 (2019): 100-109.

[9] Guo, Y., Zhang, H., Zhang, L., Fang, L., & Li, F. (2019). A game theoretic approach to cooperative intrusion detection. Journal of Computational Science, 30, 118-124.

[10] B. S. M. Y, R. Ibrahim, and A. Amiruddin, "Lightweight method for detecting fake authentication attack on Wi-Fi," in 2019 6th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), pp. 280-285, 2019. doi: 10.23919/EECSI48112.2019.8976975.

[11] Basaligheh, P. (2021). A Novel Multi-Class Technique for Suicide Detection in Twitter Dataset. Machine Learning Applications in Engineering Education and Management, 1(2), 13–20. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/14.

[12] Mark White, Kevin Hall, Ana Silva, Ana Rodriguez, Laura López. Predicting Educational Outcomes using Social Network Analysis and Machine Learning . Kuwait Journal of Machine Learning, 2(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/182.

[13] A. S. A. Alghamdi, S. R. Hasan, M. F. Hassan, and M. S. Ali, "Jamming and anti-jamming techniques in wireless sensor networks: a comprehensive study," Wireless Personal Communications, vol. 105, no. 2, pp. 581-616, 2019.

[14] Bhunia, S., Regis, P.A., & Sengupta, S. (2018). Distributed Adaptive Beam Nulling to Survive Against Jamming in 3D UAV Mesh Networks. Computer Networks, 133, 153-166. DOI: 10.1016/j.comnet.2018.03.011

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7111
***Article Received**: 16 March 2023 **Revised**: 20 May 2023 **Accepted**: 28 May 2023*

[15] Alotaibi B, & Elleithy K,"Rogue access point detection: Taxonomy, challenges, and future directions" Wireless Personal Communications, 2016, 90(3), 1261–1290.

[16] Kao K. F, Chen W. C, Chang J. C, & Chu, H. T, "An accurate fake access point detection method based on deviation of beacon time interval", 2014 IEEE Eighth international conference on software security and reliability-companion (pp. 1–2), http://dx.doi.org/10.1109/SERE- C.2014.13.

[17] Jadhav P. N, &Patil, B. M, "Low-rate DDoS attack detection using optimal objective entropy method", International Journal of Computer Applications, 2013, 78(3).

[18] N. Sufyan, N. A. Saqib, and Z. Muhammad, "Detection of jamming attacks in 802.11b wireless networks", EURASIP Journal on Wireless Communications and Networking, vol. 2013, article 208, 2013.

[19] Khairnar, V. D, & Kotecha, K,"Simulation-Based Performance Evaluation of Routing Protocols in Vehicular Ad-hoc Network" International Journal of Scientific and Research Publications, 2013, 3(10), ISSN: 2250-3153.

[20] Ali Ahmed, Machine Learning in Healthcare: Applications and Challenges , Machine Learning Applications Conference Proceedings, Vol 1 2021.

[21] T. Cheng, P. Li, S. Zhu, "An algorithm for jammer localization in wireless sensor networks", Proceedings of the 26th IEEE International Conference on Advanced Information Networking and Applications (AINA), Fukuoka, Japan, March 2012.

[22] D. Torrieri, S. Zhu, S. Jajodia, "Moving Target Defense: Application of Game Theory and Adversary Modeling", Springer, 2012, pp. 87–96 (Chapter Cyber Maneuver Against External Adversaries and Compromised Nodes).

[23] Han C, In-Jang J, feng Shao J, Chae K, Seong-Soo B, & Jung S,"A scheme of detection and prevention rogue AP using comparison security condition of AP", 2012.

[24] Faris, W. F. . (2020). Cataract Eye Detection Using Deep Learning Based Feature Extraction with Classification. Research Journal of Computer Systems and Engineering, 1(2), 20:25. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/7.

[25] Chumchu P, Saelim T, &Sriklauy C,"A new MAC address spoofing detection algorithm using PLCP header", In The International conference on information networking 2011 (pp. 48–53), IEEE.

[26] H. Liu, Z. Liu, Y. Chen, W. Xu, "Determining the position of a jammer using a virtual-force iterative approach", Wireless Networks. 17 (2) (2011) 531–547.

[27] XiangY, Li K, & Zhou W,"Low-rate DDoS attacks detection and traceback by using new information metrics", IEEE transactions on information forensics and security, 2011, 6(2), 426-437.

[28] Arackaparambil C, Bratus S, Shubina A, &Kotz D,"On the reliability of wireless fingerprinting using clock skews", In Proceedings of the third ACM Conference on wireless network security (pp. 169–174), 2010.

[29] Hamieh A, Ben-othman J, "Detection of Jamming Attacks in Wireless Ad Hoc Networks Using Error Distribution", in IEEE International Conference on Communications, 2009 ICC '09, pp.1-6, 14-18 June 2009.

[30] J. Blumenthal, R. Grossmann, F. Golatowski, D. Timmermann, "Weighted centroid localization in zigbee-based sensor networks", Proceedings of the IEEE International Symposium on Intelligent Signal Processing (WISP 2007), October 2007.

[31] Guo F, &Chiueh T,"Sequence number-based MAC address spoof detection. In International workshop on recent advances in intrusion detection" (pp. 309–329), 2005, Springer.