Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
March 2024 5(3), 212–224

# A COMPREHENSIVE RESEARCH PAPER ON THE IN-DEPTH ANALYSIS OF WI-FI NETWORK SECURITY AND THE IDENTIFICATION OF POTENTIAL THREATS

Teg Singh [1], Dr. Rajesh Chauhan [2]

[1] Research Scholar, Career Point University, Alaniya Kota, Rajasthan, India
[2] Assistant Professor, UIIT, HPU, Shimla, Himachal Pradesh, India

**Corresponding Author**

Teg Singh, tejuit9@gmail.com

**DOI**
10.29121/shodhkosh.v5.i3.2024.1740

**Funding:** This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.



## ABSTRACT

This research paper delves into the critical aspects of Wi-Fi network security, providing a thorough analysis of the vulnerabilities and risks associated with wireless networks. As Wi-Fi technology continues to expand globally, ensuring robust security measures has become increasingly vital to protect sensitive data and maintain the integrity of network communications. The paper explores the various security protocols employed in Wi-Fi networks, evaluates their effectiveness, and highlights the common threats that these networks face, including unauthorized access, data interception, and cyber-attacks. Through a detailed examination of case studies and current security practices, the paper identifies potential weaknesses in existing Wi-Fi security frameworks and proposes strategies for mitigating these risks. By addressing both technical and practical considerations, this research aims to contribute to the ongoing efforts to enhance Wi-Fi network security, ensuring safer and more reliable wireless communication in both personal and professional environments. Recent tools and methods have proven to be beneficial in the research study area, with a particular focus on utilizing tools like OPNET. The study emphasizes the hardware requirements necessary for conducting MANET and OPNET simulations, which are crucial for enhancing network security and developing robust mechanisms to defend against attacks and hacking attempts. Researchers must employ powerful hardware systems, scalable techniques, and advanced simulators to meet the high computational demands of modern state-of-the-art application domains.

**Keywords:** Wi-Fi Security, Network Vulnerabilities, Wireless Communication, Cybersecurity, Encryption, Wep, Wpa, Access Control, Data Protection, Network Threats, Attacks, Opnet, Integrity, Hacking, Case Studies

## 1. INTRODUCTION

Wi-Fi networks have become essential for modern connectivity, enabling wireless communication in both personal and professional settings. The convenience and flexibility offered by Wi-Fi make it a popular choice for internet access and network connections. However, this widespread use also brings significant security challenges, making it crucial to understand the vulnerabilities and threats associated with Wi-Fi networks. Wi-Fi technology allows devices to connect to the internet and communicate with each other without the need for physical cables. It supports a wide range of applications, from home networking to enterprise environments, facilitating seamless access to information and services. The proliferation of smartphones, tablets, laptops, and IoT devices has further increased reliance on Wi-Fi networks. Wi-Fi provides a fast connection to the

internet without the need for cables or wires. The technology is built on three fundamental components: radio waves, transceivers, and the data transfer path, with radio frequency (RF) signals playing a central role alongside intermediate network modules. This technology ensures seamless connectivity and compatibility, allowing users to access networks efficiently within its coverage area. In practical use, Wi-Fi is typically connected through a well-organized setup involving stereo systems and high-quality connecting mediums. It enables users to connect from various locations such as resorts, libraries, schools, universities, private institutions, and coffee shops, enhancing business opportunities and connectivity. Wi-Fi's compatibility allows for efficient internet browsing at relatively low costs compared to other methods.

**Figure 1**

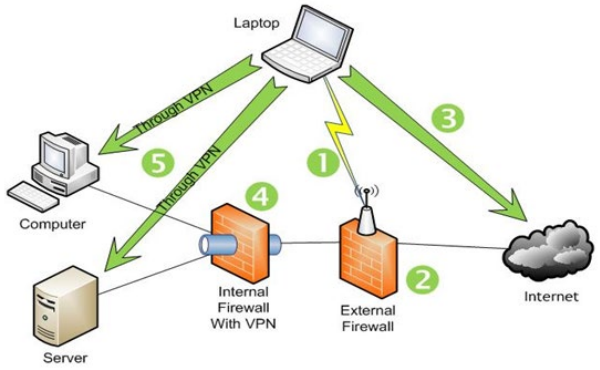


**Figure 1** Wi-Fi Connections

Fig: 1 shows the Wi-Fi connections receivers, located in antennas and routers, transmit radio signals to establish connections within a range of 100-150 feet. The effectiveness of this connection depends on the surrounding environment, and the connection speed may vary based on the distance from the source. Wi-Fi enables wireless internet connectivity using radio waves, allowing devices to connect and communicate without physical cables. It works through a wireless router or access point that transmits radio signals, which are picked up by Wi-Fi-enabled devices like laptops and smartphones. These devices connect to the network by selecting its SSID (network name) and entering a password for authentication.

Wi-Fi operates on two main frequency bands: 2.4 GHz, which offers longer range but can be slower, and 5 GHz, which provides faster speeds but a shorter range. The range typically extends 100-150 feet indoors and can be enhanced using extenders or mesh networks. Security is crucial for Wi-Fi networks and is managed using encryption protocols like WPA2 or WPA3 to protect data and prevent unauthorized access. Wi-Fi is used in various settings, from homes and public spaces to businesses, providing flexible and convenient internet access.

## 2. OBJECTIVES

The primary focus of the MANET environment is to enhance both the security and performance of the network. Despite numerous protocols designed to ensure network security, all of them are vulnerable to Jellyfish Attacks. No protocol has yet been developed that entirely eradicates the Jellyfish Attack problem. MANETs (Mobile Ad Hoc Networks) are not widely implemented. These networks are self-organized and operate autonomously without infrastructure support. In a MANET,

nodes move freely and frequently alter their topology. Without a fixed routing path, every node in the network must also function as a router.

The goal of this research is to develop a secure Wi-Fi network that improves performance and ensures security. The study demonstrates that implementing a secure OSPF protocol in MANETs enhances network performance. Research has been conducted on Jellyfish attacks and secure OSPF protocols in MANETs. Comparisons show that OSPF in MANETs outperforms traditional MANET configurations in various aspects. Simulations were carried out using OPNET (Optimize Network Performance).

The objective of this thesis is to implement a methodology that provides improved results over previous security solutions. This research applies a secure OSPF protocol to MANETs to boost network performance and security. The MANET network was initially designed, and then OSPF was integrated to enhance performance and security. Jellyfish attacks were used to assess their impact on the network. Comparisons were made between standard MANETs and those utilizing secure OSPF under Jellyfish attack conditions. The main objectives of the thesis are summarized as follows:

- Study the Structural and Behavioral Properties of the MANET Network:
- Understand how to create a Wi-Fi network.
- Explore the deployment of MANET networks.
- Examine the operation of wireless nodes in an autonomous environment.
- Investigate the MANET Network with the OLSR Routing Protocol:
- Analyze how protocols function within a WiFi network.
- Configure various protocols in a WLAN network.
- Examine the OSPF Secure Routing Protocol in the MANET Environment:
- Study various secure protocols within a WLAN network.
- Understand how to deploy the OSPF protocol in a wireless network.

## 3. RESEARCH METHODOLOGY

A research plan outlines the guidelines for conducting the study, detailing the what, when, where, and how of the process. It assists in planning ahead and selecting methods that best achieve research goals. This study adopts a flexible research strategy, enabling both qualitative and quantitative data collection. This section covers the need, scope, goals, methodology, data collection tools, sampling methods, and analytical tools.

### 3.1. TYPES OF RESEARCH DESIGN

- **Experimental Research Design:** Involves manipulating one variable while controlling others to establish cause-and-effect relationships. It includes control groups, random assignment, and pre- and post-testing. It can be conducted in controlled or natural settings and is valued for isolating and measuring the impact of variables.
- **Descriptive Research Design:** Focuses on describing characteristics of a population or phenomenon, answering "what" questions. It includes surveys, case studies, observational research, and cross-sectional studies, useful for identifying trends and patterns.

- **Correlational Research Design:** Examines relationships between variables without manipulation, identifying patterns and predicting variables based on others. It cannot determine causality and uses methods like surveys and archival data analysis.
- **Longitudinal Research Design:** Studies the same subjects over time to observe changes and developments. It can be descriptive, correlational, or experimental and provides insights into temporal sequences and causality.
- **Cross-Sectional Research Design:** Observes a population at a single point in time, assessing prevalence and relationships between variables without tracking changes over time. It is quick and cost-effective for preliminary research.
- **Qualitative Research Design:** Collects non-numerical data through interviews, focus groups, and open-ended surveys to gain in-depth insights into behaviors, motivations, and attitudes. It is flexible and provides detailed contextual understanding.
- **Mixed-Methods Research Design:** Combines quantitative and qualitative approaches for a comprehensive analysis. It integrates the strengths of both methods for a more complete understanding of complex phenomena.

### 3.2. STATEMENT OF PROBLEM

In Mobile Ad Hoc Networks (MANETs), security is a major concern due to frequent topology changes and moving nodes. MANETs face various attacks such as Black Hole, Worm, Flooding, Jellyfish, and Gray Hole Attacks. Most research focuses on improving routing protocols to enhance performance and mitigate attacks. This study specifically examines the impact of applying a secure OSPF protocol with an OLSR-based routing protocol in MANETs under Jellyfish attack conditions.

### 3.3. NEED FOR STUDY

As network technologies evolve, new security threats emerge, impacting organizations such as research agencies, banking systems, and increasing cybercrime globally. This study aims to address these security challenges by analyzing network threats and gaps in Wi-Fi security. Network security is crucial for protecting data from unauthorized access and ensuring system integrity against malicious attacks. Enhancing network security involves safeguarding both data and computer systems from threats such as viruses, spyware, and hacking. Understanding and addressing these security needs is essential for developing robust and secure networks.

## 4. PROPOSED SYSTEM DESIGN

### 4.1. CURRENT LIMITATIONS OF IDS TOOLS

Modern IDS tools primarily focus on Signature Detection (SD), but they struggle with rapid advancements in bandwidth, attack complexity, and volume. Many IDS devices are limited to monitoring mode, detecting but not preventing attacks, presenting several challenges for network security administrators:

1) **Incomplete Attack Coverage:** Most IDS solutions focus on signatures, anomalies, and denial-of-service (DoS) attacks, requiring multiple solutions from various vendors for comprehensive protection.

2) **Inaccurate Detection:** IDS tools often emphasize DoS attacks, anomalous traffic, and signatures, necessitating integration of different solutions to avoid breaches.
3) **Detection, Not Prevention:** Current systems are designed for attack detection rather than prevention, which may lead to damage by the time preventive measures are implemented.
4) **Performance Issues:** Generic hardware limits IDS performance, leading to false identifications and packet loss, especially on low-bandwidth networks.
5) **Limited High Availability:** IDS products with single ports fail to handle asymmetric data transmission and lack adequate backup systems for production networks.
6) **Poor Scalability:** Modern IDS tools are not scalable for large networks, facing challenges with bandwidth, network segments, sensors, and alert rates.
7) **Single Policy Enforcement:** Most IDS solutions apply one security policy system-wide, lacking support for multiple policies across different departments.
8) **High IT Resource Requirement:** IDS products demand significant operator involvement, making maintenance and updates resource-intensive.

There is a pressing need to address these shortcomings by developing IDS systems that can handle advanced threats and provide better real-time responses. Anomaly-based systems offer broader threat detection but often require professional intervention, impacting performance.

## 4.2. IDS REQUIREMENTS

Effective IDS systems must automate data analysis and adapt to the large volume of network data. Key requirements include:

1) **Detection Efficiency:** Automated and efficient analysis of network behavior.
2) **System Adaptation:** Adaptation to evolving threats and system maintenance.
3) **Distributed Solutions:** Integration with other security mechanisms and support for distributed IDS components.

## 4.3. PROBLEMS IN DETECTING NETWORK ATTACKS

Current IDS tools face several issues:

1) **Noisy Internet Environment:** High data volume and noise lead to high false alarm rates.
2) **Specificity of Network Attacks:** Attacks often target specific software versions, requiring a constantly updated signature library.
3) **Commercial Purchase Trends:** Organizations may buy IDS to meet regulatory or insurance requirements without proper evaluation.
4) **Encrypted Traffic Analysis:** Network-based IDS struggle with encrypted communications, which can only be monitored by host-based IDS.

5) **Packet Capture and Preprocessing:** Fragmented packets and high computation requirements affect the efficiency of capturing and analyzing data.

The higher-level architecture of the proposed framework is shown in Figure 2.

**Figure 2**

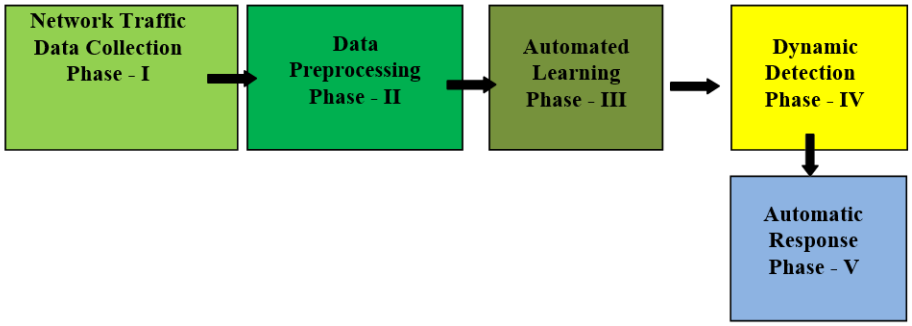


**Figure 2** General Framework of Proposed IDS

At the core of architectural design is creating a strong structural foundation. This involves identifying the system's key components and their interactions. Typically, a TCP connection involves two links: one from the sender to the receiver and another from the receiver to the sender. However, a connection does not necessarily require the TCP protocol.

**Figure 3**

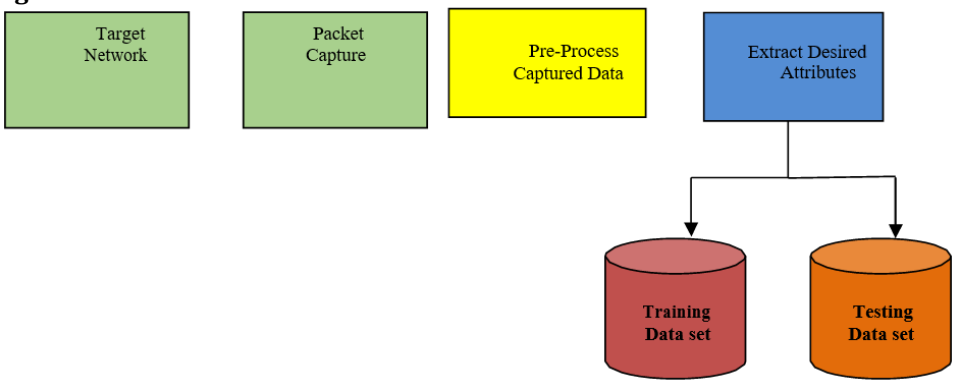


**Figure 3** Framework for Packet Capture Process

Incoming packets are captured from the network and processed by the preprocessing module, which extracts the necessary features. The IDS operates in two phases: training and testing. For the dataset collection, a one-week window is used for both phases. Given the week-long window, the initial learning period should span at least a week. The deviation threshold is set to a pre-calculated standard deviation, as data typically falls within these boundaries. Outlier and CP thresholds are determined through trial and error. The steady period is used to detect behavioral changes in the network, representing the time during which the data should remain stable or normal. Thresholds are fine-tuned by averaging them for each day within the dataset. Monitoring every data request in real-time can be challenging due to the high volume of data accesses. To detect intruders, an IDS can monitor either application requests, data requests, or both.

## 5. RESULT AND DISCUSSION

Analyze the payload of the abnormal traffic to identify any indicators of a DDoS attack. This may include analyzing the type of traffic, the source IP addresses, the size of the packets, and the frequency of the traffic features. Detect and analysis data traffic by ensemble classifier model and analysis accuracy, precision and recall.

**Figure 4**

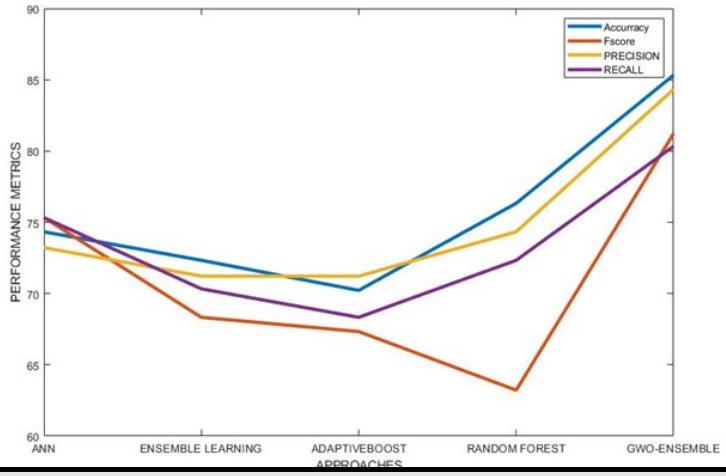


**Figure 4** Proposed (GWO-Ensemble) and Existing Classifier Intrusion Classification Performance Metrics

The graph displayed above compares the performance metrics of the proposed (GWO-Ensemble) and existing approaches. The proposed (GWO-ENSENBLE) method obtained the highest accuracy, precision, recall, and F-score in terms of performance metrics. As shown in the graph, the proposed approach performed better than all existing rival strategies. As illustrated in the graph, the accuracy, precision, and recall values are all favorable; however, the F-score values accomplished a marginally weak response in all cases.

**Figure 5**

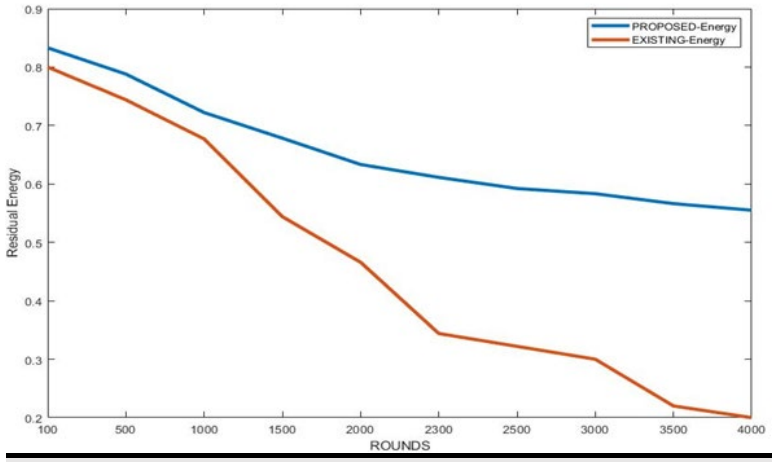


**Figure 5** Proposed (GWO-Ensemble) and Existing Intrusion after Prevention Residual Energy

Figure 5 depicts the proposed (GWO-Ensemble) and existing residual energy systems for different rounds. The proposed (GWO-Ensemble) approach, results in

residual energy that is both somewhat greater and more uniform than the approaches that are currently in use. This indicates that a lower quantity of energy is used for the transmission of packets in accordance with the proposed method.

**Figure 6**

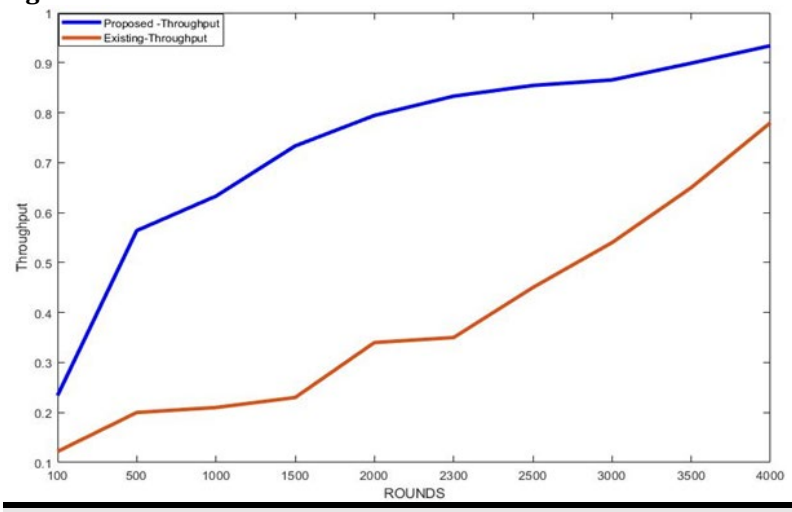


**Figure 6** Proposed (GWO-Ensemble) and Existing Intrusion after Prevention Throughput

Figure 6 illustrates the proposed (GWO-Ensemble) and existing approach throughput for various rounds. Here, we can see the network system throughput improvements. The proposed (GWO-Ensemble) strategy outperformed the current strategy. After 3500 rounds, the throughput of the proposed methodology is nearly 90% compared to the present approach, which is roughly above 70%.

**Figure 7**

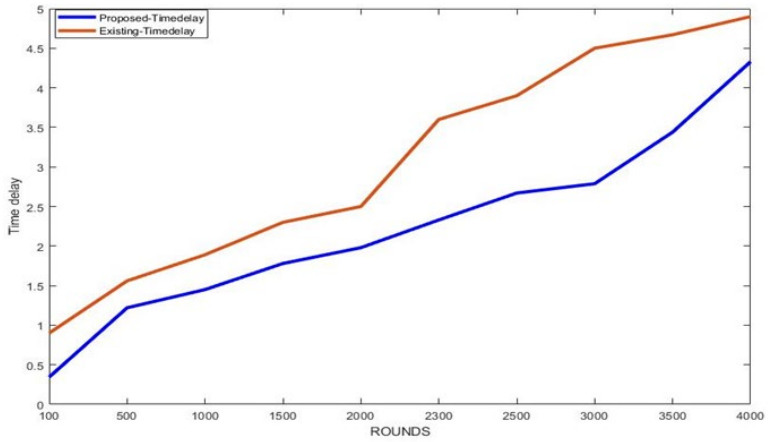


**Figure 7** Proposed (GWO-Ensemble) and Existing Intrusion after Prevention Time Delay

Figure 7 illustrates the proposed (GWO-Ensemble) and existing approach time delay function for various rounds. Here, we can see how the proposed approach will cut down on delays in time. At the 4000th round, the recommended (GWO-Ensemble) strategy had a time delay of about 4.3 seconds, while the existing approach had a time delay of about 4.9 seconds. This shows that the proposed approach had less delay time improving network performance.

**Table 1**

**Table 1 Proposed (GWO-Ensemble) and Existing Classifier Intrusion Classification Performance Metrics**

| APPROACHES | ACCURACY | PRECISION | RECALL | F-SCORE |
|---|---|---|---|---|
| ANN | 74.33 | 73.22 | 75.33 | 75.33 |
| ENSEMBLE LEARNING | 72.33 | 71.222 | 70.33 | 68.33 |
| ADAPTIVEBOOST | 70.222 | 71.22 | 68.33 | 67.33 |
| RANDOM FOREST | 76.33 | 74.33 | 72.33 | 63.22 |
| GWO-ENSEMBLE | 85.322 | 84.33 | 80.334 | 81.22 |

Table 1 displays the performance metrics of the proposed (GWO-Ensemble) and existing approaches. The GWO-ENSENBLE approach achieves the highest accuracy of 85.322, followed by the RF (76.33), AB (70.222), EL (72.33), and ANN (74.40). In terms of precision value, the proposed GWO-ENSENBLE method achieves the highest precision of 84.33, followed by the RF (74.33), ANN (73.22), EL (71.222), and AB (71.22). The model with the highest recall value is GWO-ENSEMBLE (80.334), followed by ANN (75.33), RF (72.33), EL (70.33), and AB (68.33). The proposed approach obtained the highest F-score value (81.22), while the RF achieved the lowest value (63.22). The proposed strategy did better than all the other ones. As shown in the table, the accuracy, precision, recall and F-score values for each case are all favorable. On the other hand, the F-score values for each case are slightly below average.

**Figure 8**

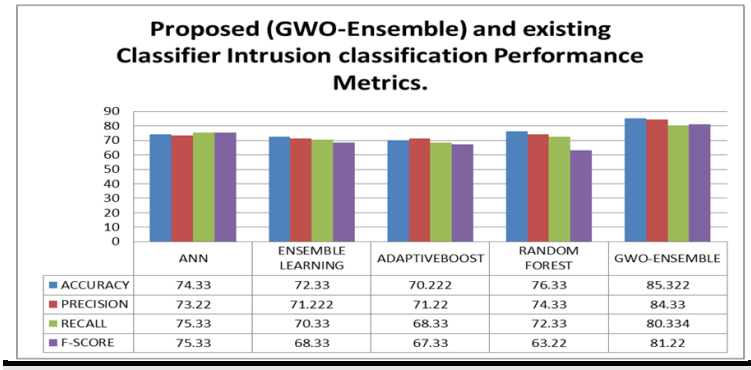


**Figure 8** Proposed (Gwo-Ensemble) snd Existing Classifier Intrusion Classification Performance Metrics

A MANET Network work with OLSR convention was made in OPNET and it was checked how jellyfish assaults influence the OLSR convention. In this way, we made two situations, in the primary situation, as appeared in Fig 8 we made a MANET network with the OLSR convention and checked the rate at which the information transmission is traded between the hubs. MANET network with 5 hubs and a versatile worker was made in which all the hubs are associated with them. Two different hubs, for example, Application Configuration and Profile Configuration have been utilized to characterize the application definition and profile definition and characterize the geography and setup needed for the organization. OLSR convention deals with an organization and shows how information bundle goes in the organization. The Configured Hyperlink Country Routing is a desk-driven link state routing protocol for the hoc population of cell advertising in figure 9. It uses Multipoint Relays as a tool to overwhelm the community with manipulations and traffic messages. The security concerns are not now considered in the layout of the

protocol with the help of RFC. The numerous authentication and encryption techniques help to make this protocol comfortable with attacks by intruders outside the gate. The protected OLSR architecture contains a safety module that provides minimal overhead for defence. Through minimizing the large range of Multipoint Relay nodes within the network and providing protection for the chosen nodes, the overhead is minimized. Security is largely based on the method of threshold cryptography.

**Figure 9**

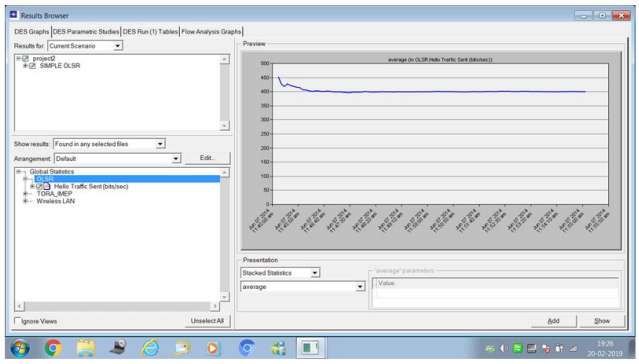


**Figure 9** Data Packet Exchange in OLSR Protocol

The consequence of the scenario is uncovered in fig 9 in which the welcome message parcel goes into the organization at the pace of 400b/s. The Optimized Hyperlink Kingdom Routing (OLSR) convention for specially appointed organization cells is characterized in this article. The convention is an advancement of the calculation of the traditional realm of hyperlinks fit to the necessities of a versatile remote LAN. The principle term utilized inside the convention is that of multipoint transfers (MPRs). MPRs are resolved throughout the flooding convention on hubs that hand off transmission messages. As opposed to a traditional flooding system, this technique incredibly diminishes the message overhead, where every hub retransmits each message while accepting the essential replication of the message. Association nation insights are made in OLSR exclusively by hubs picked as MPRs. For course assessment, this information is then utilized. Ideal courses are given by OLSR (in expressions of the amount of bounces). Specifically, the convention is ideal for enormous and thick organizations, since the MPR strategy works well in this sense.

The Optimized Hyperlink Kingdom Routing (OLSR) convention for impromptu organization cells is characterized in this article. The convention is an advancement of the traditional calculation of the hyperlink domain, adjusted to the necessities of a versatile MANET, a self-arranging bunch that utilizes multi-jump steering for discussion with measurements. Gathering recognition is precarious with no centralization, leaving it helpless against attacks that include attack by Jellyfish. The IPSec convention can in this manner be utilized as one of its insurance techniques. The objective of this paper is to investigate the presentation of MANET utilizing OLSR and TORA steering conventions close by the IPSec utility when the MANET is under Jellyfish attack, to see which directing convention is least affected by the assault and to see which directing convention most picked up from the utilization of Riverbed Modeler e utilizing IPSec. In view of the reenactments, apparently with the utilization of IPSec, OLSR performs best under Jellyfish assault, and TORA favors the cutoff.

**Figure 10**

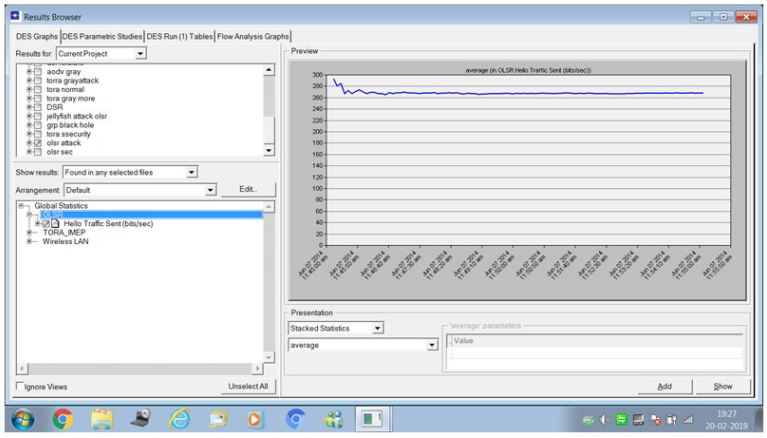


**Figure 10** Data Packet Exchange in OLSR Protocol with Jellyfish Attack

It has been shown in Fig 10 that when a black hole is applied to the network, the Hello packet exchange bit rate will be reduced to 270b/s. The nodes with the ideal values of consideration enable the MANET's trust tables to be calculated to detect jellyfish attacks. More appropriate security can be trusted through secured key management throughout the manner of transmission of facts. The overall performance assessment of the current approach is carried out primarily on the basis of one kind of metric that includes the use of the NS-2 simulator platform for the lifetime, overhead, and packet transport ratio. The result obtained suggests the better efficiency in minimizing jellyfish assaults of the proposed ACO-CBRP technique.

## 6. CONCLUSION

Security and threats are major concerns in wireless networks. I evaluated the impact of the Jellyfish attack on WLAN performance and implemented the OSPF secure protocol to measure its effectiveness in mitigating this threat. The findings indicate that OSPF considerably enhances network performance compared to a typical WLAN.

- **WLAN with OLSR Protocol:** Packet delivery rate is 400 bits/sec.
- **WLAN with Secure OSPF:** Performance improves to 560 bits/sec.
- **WLAN under Jellyfish Attack**: Performance decreases to 270 bits/sec.

Therefore, WLAN with OSPF provides superior performance and better threat control than a standard WLAN.

Moving forward, the following measures are recommended:

- Implement distributed key management for enhanced attack mitigation.
- Use acknowledgment-based schemes to protect against cooperative attacks.
- Identify the most effective routing protocols to mitigate Jellyfish attacks.
- Consider additional types of attacks associated with Jellyfish threats.
- Continue research on detection and removal strategies for Jellyfish attacks.

## CONFLICT OF INTERESTS

None.

## ACKNOWLEDGMENTS

None.

## REFERENCES

Aneja Akshika, Sodhi Garima (2016)",," A Study of Security Issues Related With Wireless Fidelity (WI-FI )",International Journal of Computer Science Trends and Technology (IJCST) – Volume 4 Issue 2, ISSN: 2347-8578 www.ijcstjournal.org.

ttps://www.elprocus.com/how-does-wifi-work/

ekhande Vandana (2006)," WI-FI TECHNOLOGY: SECURITY ISSUES "RIVIER ACADEMIC JOURNAL, VOLUME 2, NUMBER 2, ISSN 1559-9388.

ttps://www.tutorialspoint.com/wi-fi/wifi_ieee_standards.htm

ttps://www.tutorialspoint.com/wi-fi/wifi_service_quality.htm

ong Shagun, Biju (2014), "ANALYSIS OF WIFI AND WIMAX AND WIRELESS NETWORK COEXISTENCE" International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.6, pp. 64-65.

itesh Sai, Kakkar Ashna (2016), "International Journal of Advanced Research in Computer Science and Software Engineering Research Paper , Volume 6, Issue 3.

han H. Afaq, Qadeer A. Mohammed(2009)," 4G as a Next Generation Wireless Network".

umar Ashish, Aswal Ankit, Singh Lalit (2013)," 4G Wireless Technology: A Brief Review", Quoted in International Journal of Engineering and Management Research, Volume-3, Issue-2, ISSN No.: 2250-0758 , Pages: 35-43. Available at: www.ijemr.net.

Ghazal Shatha, S Alkhlailah Raina (2016)," 5th Generation Wi-Fi", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 8.

Alawi Dr. (2006) ," WiFi Technology: Future Market Challenges and Opportunities ",Journal of Computer Science 2 (1): 13-18, ISSN 1549-3636.

Enad nassar, Muhanna (2013)," Computer Wireless Networking and Communication "International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, IJARCCE .

Helen D., Arivazhagan D. (2014)," Applications, Advantages and Challenges of Ad Hoc Networks" Journal of Academia and Industrial Research (JAIR), Volume 2, Issue 8.

Salfi Rahman, Ur Mohsin (2015)," A STUDY OF MOBILE AD-HOC NETWORKS - ISSUES AND CHALLENGES" International Journal of Advanced Research in Computer Science, 93-96 Available Online at www.ijarcs.info.

Singh Teg, Chauhan Rajesh(2019), "A Review Paper of Dropping the Consequence of Jellyfish Attack in MANET using AODV and OLSR Routing Protocol" , INTERNATIONAL JOURNAL OF RESEARCH IN ELECTRONICS AND COMPUTER ENGINEERING A UNIT OF I2OR, VOL. 7 ISSUE 2 , ISSN: 2348-2281

Khan Ruzaina ,Hasan Mohammad (2017)," NETWORK THREATS, ATTACKS AND SECURITY MEASURES: A REVIEW", quoted in International Journal of

Advanced Research in Computer Science RESEARCH PAPER , Volume 8, No.8.

G. Poornima, Mr. M. Raja Senathipathi (2013)," REVIEW ON ROUTING PROTOCOLS FOR MOBILE AD HOC NETWORKS", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, 2281 www.ijarcet.org.

Chithik M., Yasin Mohamed, Ponnurajan P. (2011)" A Review on Ad-hoc Network Security", International Journal of Mathematics and Computational Methods in Science & Technology, Vol. 1, No.6

Sonu (2016)," The Review Paper on Securing Wireless Network from External Threats", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.5.

Parte Smita, Pandya Smriti (2012)," A Comprehensive Study of Wi-Fi Security – Challenges and solutions", INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 3, ISSUE 8.

Sharma Nidhi. , Sharma R.M. (2010),"Provisioning of Quality of Service in MANETs Performance Analysis &Comparison (AODV and DSR)". 978-1-4244-6349-7/10\ IEEE.

Pandey Shailja (2011)," MODERN NETWORK SECURITY: ISSUES AND CHALLENGES, quoted in International Journal of Engineering Science and Technology (IJEST), ISSN: 0975-5462 Vol. 3 No.

Om prakash (2011), "wireless home security system with mobile", Quoted in international journal of advanced engineering technology, Volume 2, issue 4.

Promila, Chhillar Dr. R. S. (2012), "Review of Wi-Fi security Techniques", Quoted in International Journal of Modern Engineering Research (IJMER), Volume 2, issue.5.

Alsoufi Delan, Elleithy Khaled, Abuzaghleh Tariq and Nassar Ahmad (2012), "Security in Wireless Sensor Networks", Quoted in International Journal of Computer Science & Engineering Survey (IJCSES), Volume3, and No.3.

Vamsi Ram, Venkaterwarlu Bala (2012),"Network security management in wireless networks through zero knowledge proof", quoted in international journal of advanced research in computer science and software engineering, Volume 2, Issue 9.

Kour Parmjit, Panwar Chand Lal (2012), "A review on security challenges and attacks in wireless sensor networks", Quoted in international journal of science and research, Volume 3, issue 5.

Khandakar Amith (2012), "Step by Step Procedural Comparison of DSR, AODV and DSDV Routing protocol", 4th International Conference on Computer Engineering and Technology (ICCET 2012) IPCSIT vol.40.

rnal of Communications and Network 6(2): 7-17.