INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY
Monthly Peer-Reviewed, Refereed, Indexed Journal
Volume - 8, Issue - 2

ISSN(O): 2456-6683
[Impact Factor: 7.148]
February - 2024

DOIs:10.2017/IJRCS/202402028 --:-- Research Paper / Article / Review

An Experimental Analysis based on Node localization techniques and Fuzzy rules to tackle Black Nurse attack

[1]Shikha Bhardwaj, [2]Nikhil Mariwala, [3]Abdul Hai

[1,2,3] Department of Electronics & Communication Engineering, UIET, Kurukshetra University, Kurukshetra, Haryana.
[1]Email - sbhardwaj2015@kuk.ac.in

Abstract: *Distributed Denial of Service (DDoS) and Denial of Firewalling (DoF) attacks pose substantial threats to network security and performance. In this research, the operation of Low-Rate DDoS attacks, with a particular focus on the emerging Black Nurse attack, and the challenges posed by static firewall rule activity have been discussed. To address these challenges, a system based on dynamic mechanism that analyzes network traffic patterns using fuzzy logic rules and implements Node Localization Techniques to detect and isolate malicious nodes has been developed. The dynamic mechanism utilizes fuzzy logic rules which are generated based on real-time network data, allowing for the adaptive detection and isolation of attacks. Additionally, Node Localization Techniques are employed to establish secure paths from source to destination while eliminating compromised nodes. Through experimental evaluation, the proposed approach has been compared with related and previous works, considering metrics such as delay, throughput, packet loss, overhead, and energy consumption.*

Key Words: *DDoS attack, DoF attack, Black Nurse attack, stateful firewall, Node Localization Technique, Fuzzy Rules.*

1. INTRODUCTION:

The relentless advancement in information security practices has underscored the need for innovative offensive techniques to develop effective security solutions. These solutions play a pivotal role in enhancing the confidentiality, integration, and reliability of computer systems [1]. To achieve this, it is imperative to continually update security methodologies with the latest insights into emerging threats, attack methodologies, and countermeasures. Within the realm of security, one of the most pressing challenges is the mitigation and detection of Distributed Denial of Service (DDoS) attacks, which pose substantial risks to various sectors including finance, healthcare, retail, entertainment, and politics. The impact of DDoS attacks has been substantial, with statistics revealing a significant surge in their occurrence, including a 273% increase in 2019 alone [2],[3],[5]. These attacks, characterized by their intent to overwhelm target systems by consuming essential resources like bandwidth, memory, and CPU, pose a formidable threat to modern IT infrastructures.

In the realm of Intrusion Detection Systems (IDS), the detection of DDoS attacks has been a longstanding issue, prompting extensive research efforts to develop effective mitigation and detection strategies [6],[7]. DDoS attacks manifest in three primary categories: Volume-Based Infrastructure Attacks, Application Attacks, and Network Infrastructure Vulnerability Attacks. Each category exploits vulnerabilities at different layers of the IT architecture, causing varying degrees of disruption. This paper focuses on an increasingly relevant facet of DDoS attacks, Denial of Firewalling (DoF) attacks, with particular attention given to the emerging Black Nurse attack. Firewalls serve as the first line of defense against DDoS assaults and network threats, acting as gatekeepers that filter network traffic based on predefined rules. However, even these essential security components are susceptible to DoF attacks, where malevolent actors exploit vulnerabilities to inundate firewalls with redundant packets, leading to performance degradation and hindered genuine traffic flow[8],[9].

The Black Nurse attack, a recent addition to the DoF attack repertoire, takes aim at network firewalls. It employs low-volume ICMP packets, specifically crafted to overload firewall processors, rendering them unresponsive [10], [11]. This paper delves into the mechanics of the Black Nurse attack and its variants, shedding light on their intricacies and potential impact on network security.

The subsequent sections of this paper present a comprehensive exploration of DoF attacks, with a primary focus on the Black Nurse attack. Additionally, it outlines the research gaps, methodologies, and findings that contribute to a deeper understanding of these emerging threats and paves the way for enhanced security measures.

The rest of this paper is structured as follows: Section 2 presents related work. Methodology is presented in Section3. The implementation, evaluation, and results are presented in Section 4. Section 5 concludes the work with future.

2. RELATED WORK :

In this section, an overview of related research efforts that address Denial of Firewalling (DoF) attacks, particularly focusing on the BlackNurse attack has been presented and also discusses the gaps in the existing literature.

2.1. History of DoF Attacks

The emergence of the Black Nurse attack in 2016 marked a significant milestone in network security threats [1]. It utilizes low-rate ICMP packets to overwhelm firewall resources, exposing vulnerabilities in firewall systems. Black Nurse gained recognition due to its disruptive nature, even affecting advanced firewalls [1].

2.2. Firewall Fingerprinting and Machine Learning

Liu et al. (2017) introduced techniques for deducing firewall implementation based on unusual flags in TCP packets and employing machine learning [8]. They emphasized enhancing firewall implementations for better defense against attacks [8]. However, this work does not specifically address Black Nurse attacks.

2.3. Stateful Session Table (SST) Models

Trabelsi et al. (2018) proposed an SST model for detecting Denial of Stateful Firewall (DoSF) attacks [17]. This approach employed a stateful firewall and multilevel filtering paths to reduce packet filtering time. While effective for some attacks, it does not directly tackle BlackNurse attack.

2.4. NFV-Based DDoS Defense

Rashidi et al. (2018) introduced an NFV-based defense framework for mitigating Distributed Denial of Service (DDoS) attacks [19]. They focused on verifying packet source authenticity and scalable packet dispatching. This approach showed promise but did not specifically address Black Nurse attacks.

2.5. Early Rejection Rules

Z. Trabelsi et al. (2019) discussed a mechanism for defending against Black Nurse attacks using early rejection rules based on current attack statistics [7]. The experimental results indicated the effectiveness of this approach in mitigating Black Nurse attacks [7].

2.6. Non-Bayesian Classifier for DDoS

Frazier et al. (2019) recommended a Non-Bayesian Classifier algorithm for detecting DDoS attacks, effectively separating attackers from non-attackers [18]. While useful for general DDoS detection, its applicability to Black Nurse attacks is not explored.

2.7. Summary of Research Gaps

The existing literature provides valuable insights into DoF attacks and various mitigation techniques. However, there are research gaps that need to be addressed:

The static nature of rule activity affects network performance, and dynamic rule generation methods are needed. Detection techniques based on attack patterns need to consider the severity and impact of attacks triggered through these patterns. Firewalls should adaptively generate rules based on real-time packet exchange patterns to improve efficiency.

In this paper, we aim to address these gaps by proposing a dynamic scheme for the isolation of Black Nurse attacks using fuzzy logic and node localization techniques, considering packet delivery ratio, delay evaluation, packet loss, packet throughput, overhead, and energy consumption as evaluation metrics.

3. METHODOLOGY:

In this section, a comprehensive research methodology for the detection and isolation of malicious nodes in wireless sensor networks (WSNs) has been presented. The methodology encompasses three main phases: Node Localization Technique, Detection and Isolation Process, and Continual Monitoring and Isolation.

3.1. Node Localization Technique

The research process commences with the Node Localization Technique, which plays a crucial role in accurately identifying the positions of sensor nodes and their transmission delays. This phase ensures the foundation for subsequent malicious node detection and isolation.

3.1.1. Sensor Network Deployment

The research begins by deploying a finite number of sensor nodes within the wireless sensor network infrastructure. This deployment forms the basis for the subsequent security measures.

3.1.2. Firewall Activation for Security

To enhance network security, each sensor node is equipped with an activated firewall. This protective measure safeguards the network against potential malicious activities that could compromise its integrity.

3.1.3. TCP Packet Generation

Sensor nodes within the network generate TCP packets for communication purposes. These packets serve as the medium for data exchange within the wireless sensor network.

3.1.4. Establishment of Secure and Shortest Paths

The Node Localization Technique focuses on the establishment of secure and shortest paths from source nodes to destination nodes while routing through cluster heads. This routing strategy forms the basis for efficient and secure communication.

3.2. Detection and Isolation Process

The Detection and Isolation Process is a critical phase of the research methodology, responsible for identifying and isolating potential malicious nodes within the wireless sensor network.

3.2.1. Information Gathering by the Sink

In this step, the sink node, acting as the base station, collects essential network information. This information includes sensor node locations, which are crucial for the localization and isolation of malicious nodes.

3.2.2. Per-Hop Delay Information Collection

The base station gathers information regarding per-hop delays occurring within the network. This data is instrumental in identifying potential malicious nodes responsible for causing delays exceeding a predefined threshold.

3.2.3. Isolation of Nodes with Increased Delay

Nodes whose delay surpasses the specified threshold of 2 milliseconds are identified as potential malicious nodes. These nodes are subsequently isolated from the network to prevent further disruptions.

3.2.4. Continuous Monitoring and Isolation

The methodology includes a continuous monitoring mechanism. If a node's delay does not exceed the 2 ms threshold, it is still assessed for abnormal delays. Nodes causing such delays are isolated to ensure network integrity.

3.3. Continual Monitoring and Isolation

The Continual Monitoring and Isolation phase ensures the ongoing security and stability of the wireless sensor network.

3.3.1. Iterative Monitoring

The research methodology continuously monitors each hop within the network for potential malicious nodes. Nodes identified as malicious are isolated promptly to maintain network security.

3.3.2. Conclusion of Methodology

The research methodology concludes when the entire network topology has been traversed, and all malicious nodes have been detected and isolated. This phase ensures the overall security and stability of the wireless sensor network.

The localization formula relies on range free localization and represented as a set of equations.

The expected delay, calculated using node distances and the time-to-live parameter, helps identify malicious nodes by comparing it with a predicted delay. Multi-path routing is employed to circumvent paths containing malicious nodes, ensuring the establishment of secure communication routes.

The expected delay is calculated with the equation 1.

$$Expected\ Delay = Time\ to\ live * Distance\ between\ each\ node \quad (1)$$

The distance between each node is calculated with the equation 2.

$$Distance = [a(i+1) - a(i)]^2 + [a(y+1) - a(y)]^2 \quad (2)$$

The predicted delay is defined with the equation (3).

$$Predicted\ Delay = \frac{Distance\ between\ each\ node}{Total\ number\ of\ message\ exchange} \quad (3)$$

When the predicted delay > the expected delay then the malicious node is detected from the network. By solving these equations, the coordinates of sensor nodes are obtained. The research aims to address the challenge of detecting and isolating malicious nodes in wireless sensor networks (WSNs). Previous techniques, such as monitor mode and delay tolerance, have shown limitations due to undefined detection conditions and increased system complexity. To overcome these challenges, a comprehensive approach is proposed, involving node localization, network throughput monitoring, and multi path routing.

This comprehensive methodology addresses the challenge of detecting and isolating malicious nodes in wireless sensor networks, offering a structured approach to enhance network security and integrity. The flowchart of the methodology is shown in figure 1.

4. PERFORMANCE EVALUATION AND RESULTS :

The proposed algorithms used to defend against low-rate Internet Control Message Protocol (ICMP) error message attacks using Node localization technique and Network monitoring, are implemented using Network Simulation Version 2. Despite this, there are times when low-rate attacks are not launched, and as a result, the triggering procedure is not successful. Calculations and modifications from the most recent time period in which the relevant low-rate attack had happened are retained. The parameters (Expected Delay, Distance, Network Throughput, and predicted delay) are used in proposed model to define the skill level of attacker. For the occurrence of each ICMP low rate attacks the following parameters are calculated (Predicted delay, Expected delay, Network Throughput, and each node distance) to be used for the detection and preventing same kind of attacks.

ISSN(O): 2456-6683
[Impact Factor: 7.148]
February - 2024

4.1 Delay Evaluation

For delay evaluation, a graph has been obtained and analysed. In this graph, the purple line corresponds to the delay outlined in compared technique, AER_TTD. This delay, as indicated by the coordinates (Time=6.48354, Delay=29.0144), serves as a reference point. Conversely, the green line portrays the revised delay, achieved through the application of new methodologies.

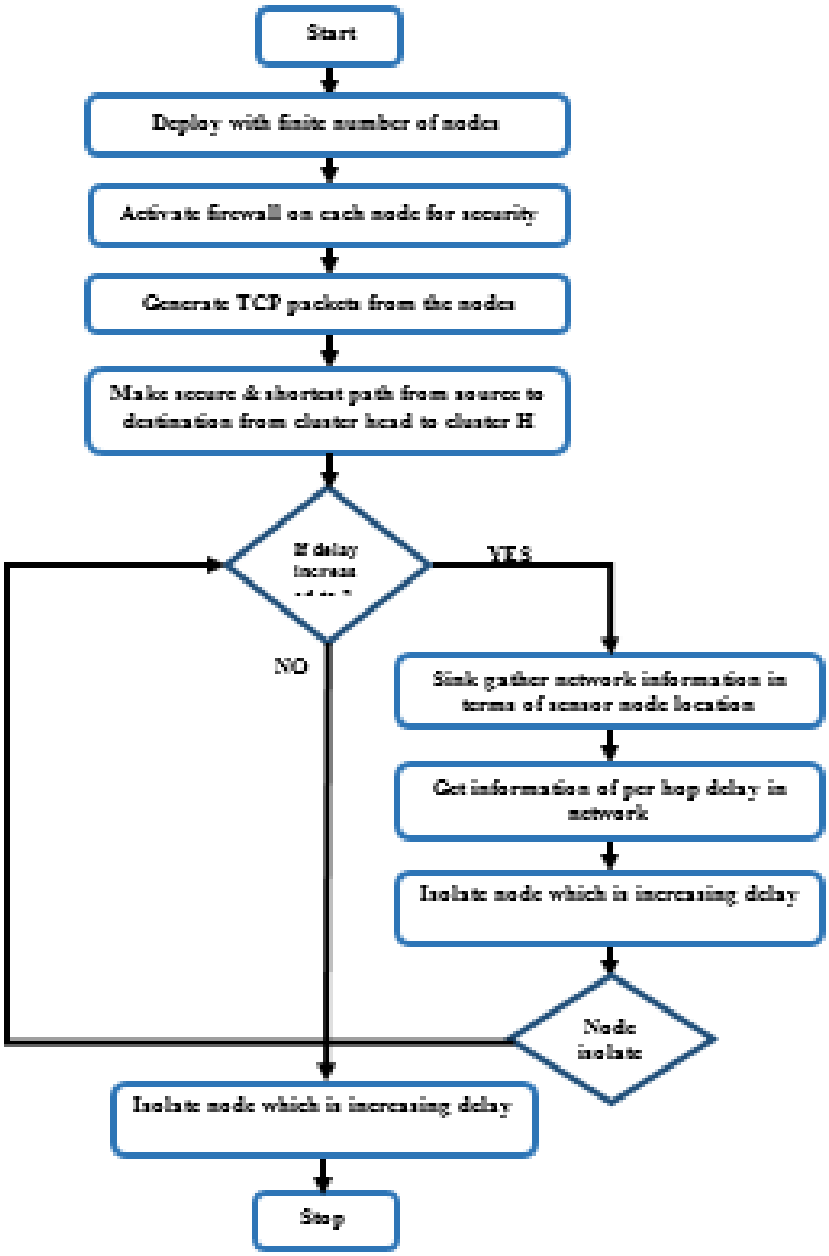

Fig. 1 Flowchart of Methodology

The screenshots from the NS2 software for malicious nodes is shown in Fig. 2 which depicts the start of communication between source and destination. After identification of malicious nodes, the same nodes are isolated and a new path is formed from the source to destination as shown in Fig. 3

ISSN(O): 2456-6683
[Impact Factor: 7.148]
February - 2024

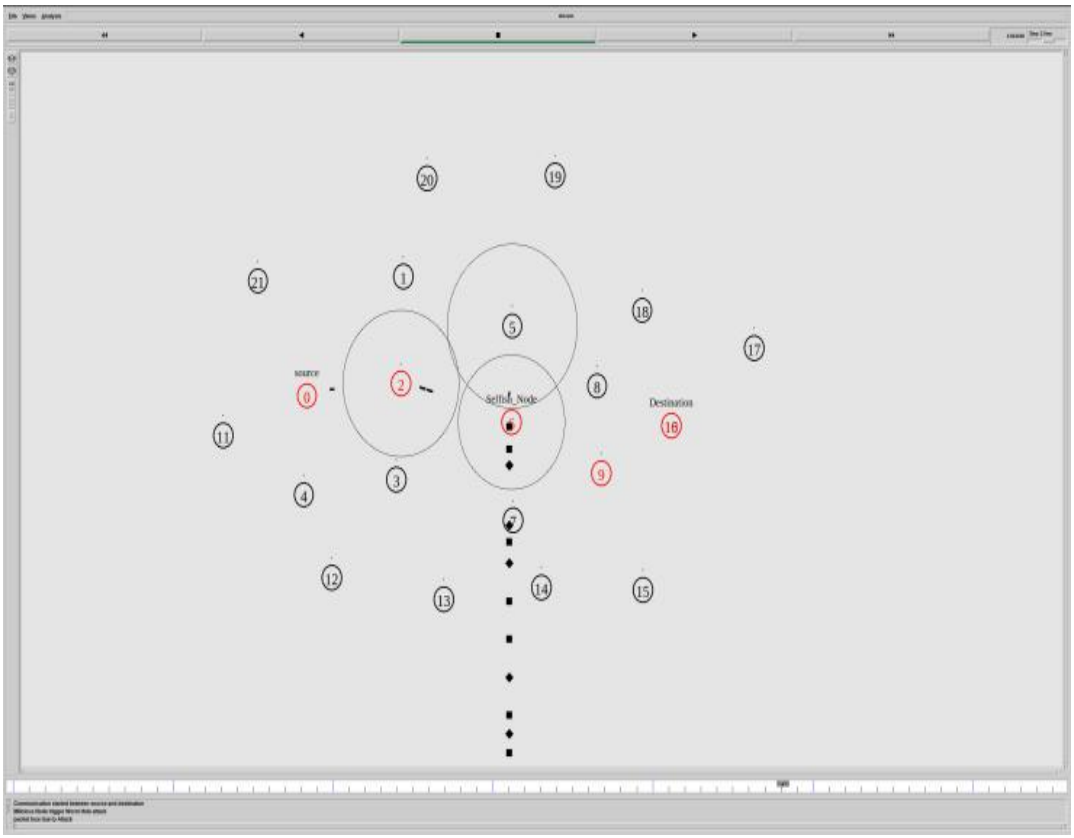

Fig. 2 Communication Started between source and destination, Malicious Node Trigger ICMP low-rate Attack, Packet-loss due to Attack

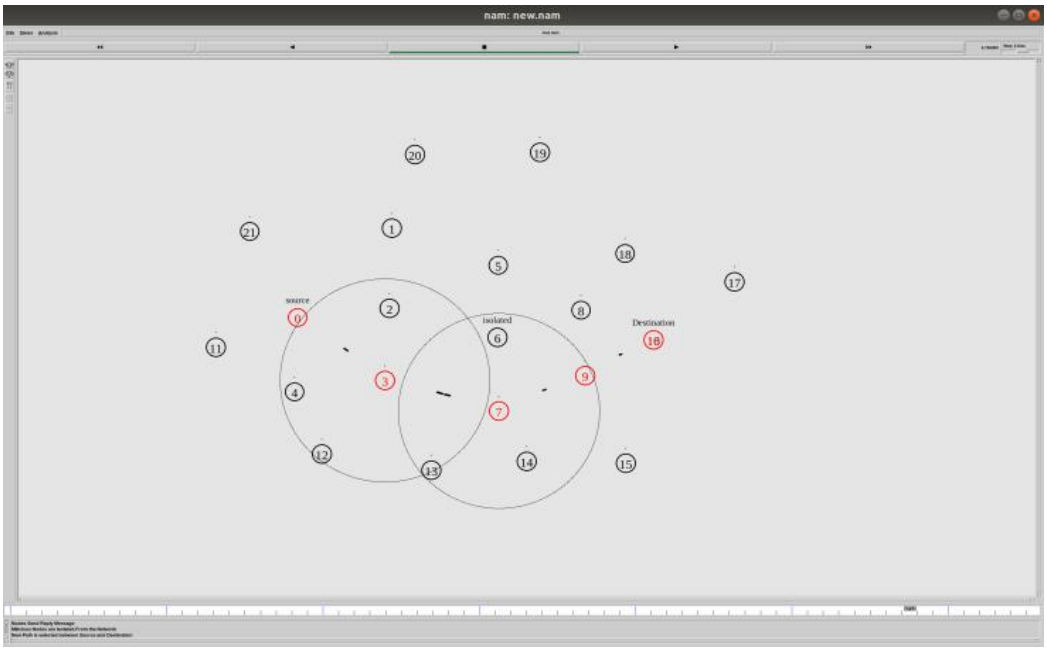

Fig. 3 Malicious Node are Isolated from Network, New path is selected between source and destination, Node Sends Reply Message

The coordinates (Time=6.48354, Delay=17.5487) pertain to this adjusted delay as shown in Fig. 4. Notably, the unit of measurement for delay is joules. This modification has resulted in a discernible reduction in delay magnitude.

ISSN(O): 2456-6683
[Impact Factor: 7.148]
February - 2024

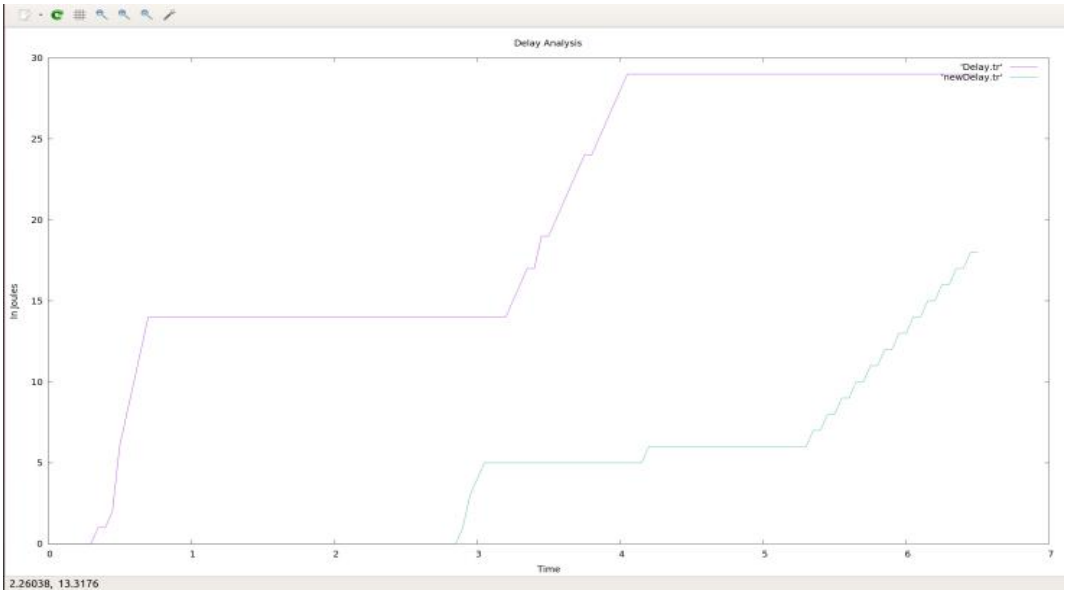

Fig.4 Comparison of existing technique AER_TTD and proposed technique in terms of their delay.

4.2 Minimizing the Packet-loss

Again, the proposed technique has been compared in terms of its packet loss. The purple line depicts the representation of Packet-loss in accordance with the parameters outlined in the compared technique. Specifically, at the time interval of (Time=6.48354, Packet loss=24.9123), this phenomenon is recorded. In contrast, the green line serves to portray the updated scenario of Packet-loss, a result attained through the implementation of novel methodologies. This revised representation is characterized by the coordinates (Time=6.48357, New Packet-loss=2.95612). Notably, the proposed model has proven effective in significantly mitigating the occurrence of Packet-loss in legitimate packets. A comparative analysis with the compared related work further underscores this improvement, highlighting a substantial reduction in the incidence of Packet-loss as shown in Fig. 5.

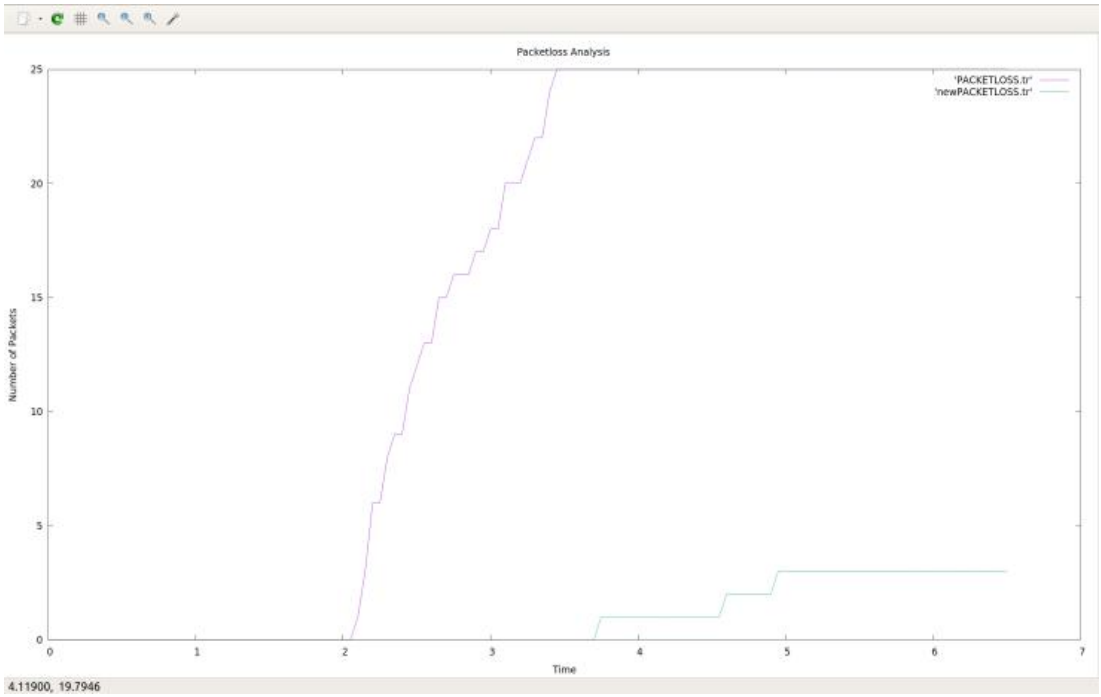

Fig.5 Comparison of existing technique and proposed technique in terms of their Packet-loss.

4.3 Throughput

The comparison in terms of throughput is represented in Fig. 6. The purple line within the graph serves to depict the representation of Packet Throughput as outlined in the compared related technique, AER_TTD. Precisely, at the time marker (Time=6.49436, Packets=28.9514), this particular metric is recorded. Conversely, the green line assumes the role of illustrating the updated scenario of New Throughput. This newly derived representation, obtained at the same time point (Time=6.49436, New Throughput=36.7390), reflects the outcomes resultant from the application of advanced methodologies. Noteworthy is the fact that the proposed model has demonstrated its effectiveness in significantly augmenting the throughput of authentic packets. A comprehensive juxtaposition with the compared work further accentuates this enhancement, showcasing a substantial reduction in the extent of degradation experienced by the throughput metric.

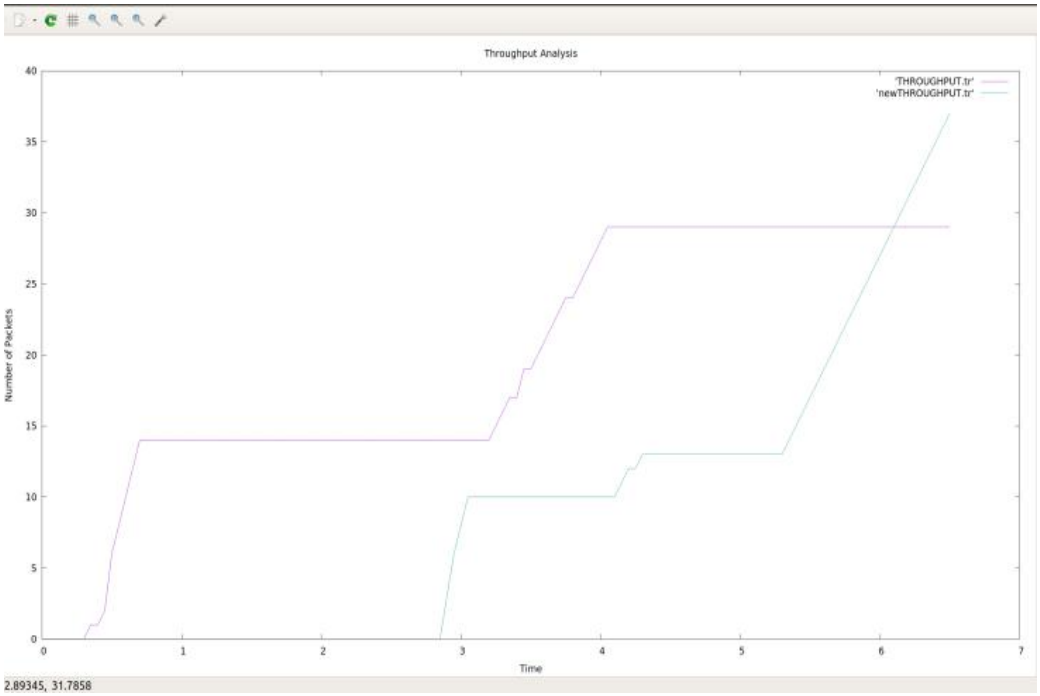

Fig.6 Comparison of existing technique and proposed technique in terms of its Packet Throughput.

4.4 Overhead

Comparison in terms of overhead is given in Fig. 7. The purple line portrayed within the graph delineates the representation of Packet Overhead derived from the compared related work. Specifically, this depiction captures the state at (Time=6.48354, Packets=53.9489). In contrast, the green line assumes the role of illustrating the novel New Overhead. This updated portrayal, attained at the time instance (Time=6.49436, New Overhead=27.4941), is an outcome of the implementation of advanced methodologies. Notably, the proposed model has proven its efficacy in significantly mitigating the Overhead associated with legitimate packets transiting through the designated node. A comparative analysis with the chosen related work underscores this improvement, highlighting a substantial reduction in the extent of Overhead loss experienced. The measurement of this reduction is quantified in joules.

4.5 Energy

In the graph shown in Fig. 8, the purple line signifies the portrayal of Energy Consumption pertaining to the operational state of the node, as outlined in the related work, AER_TTD. Precisely, the data point at (Time=6.48895, Energy=20.9219) captures the energy consumption metric during this operational phase. Conversely, the green line serves the purpose of illustrating the revised metric denoted as New Energy consumption. This updated representation, derived at the same time reference (Time=6.48895, New Energy=13.9611), stems from the implementation of advanced methodologies. Noteworthy is the demonstrated efficacy of the proposed model in significantly minimizing the energy consumption of nodes. A comparative evaluation with the related research work substantiates this enhancement, revealing a substantial reduction in energy consumption magnitude. The quantification of this decrease is expressed in joules.

ISSN(O): 2456-6683
[Impact Factor: 7.148]
February - 2024

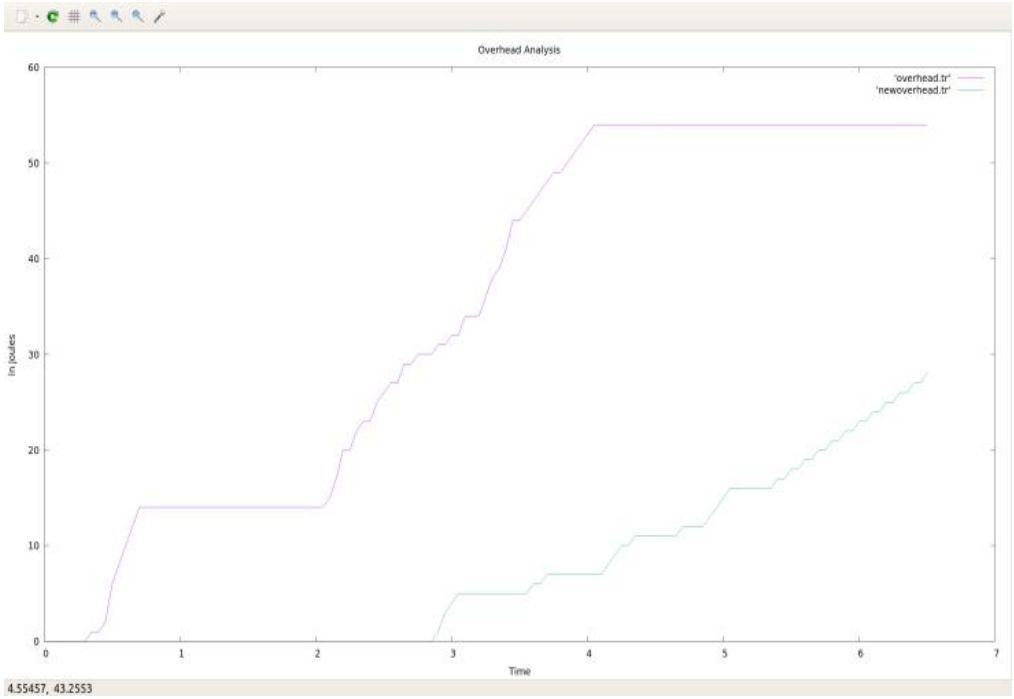

Fig.7 Comparison of existing technique and proposed technique in terms of their Overhead.

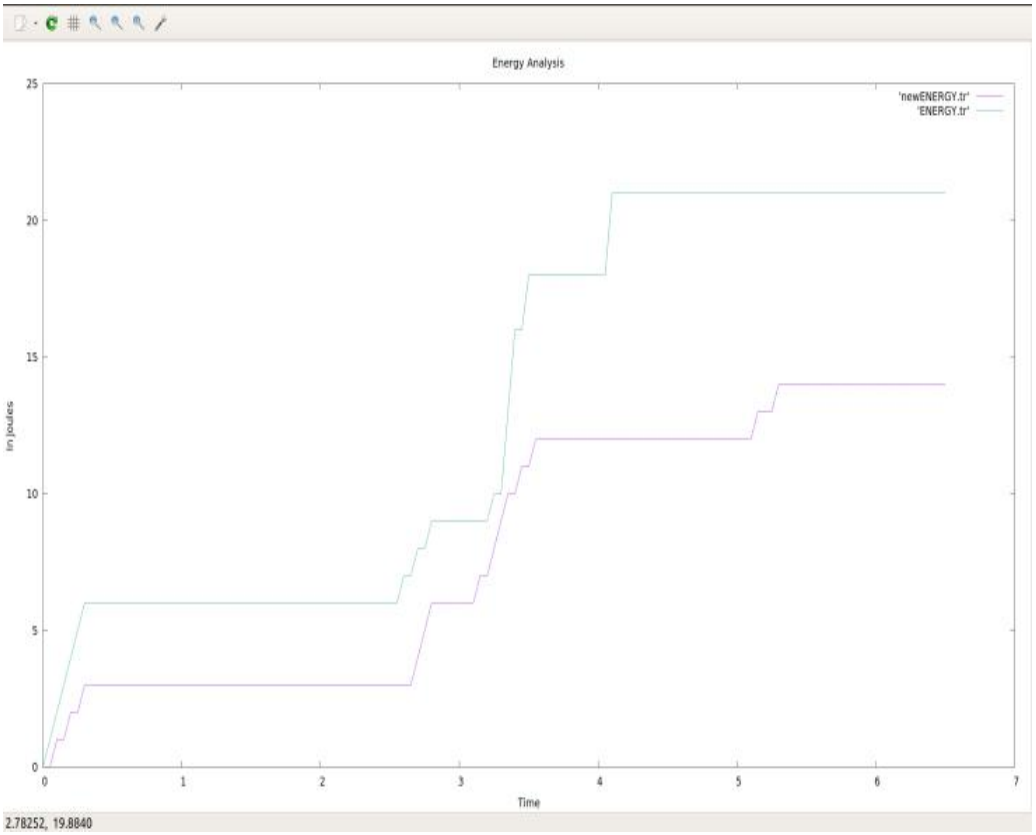

Fig.8 Comparison of existing technique, AER_TTD and proposed technique in terms of their Energy.

A comparison of all the taken evaluation metrics together with the compared technique, AER_TTD is given in Table 1.

Table 1. Comparison of related technique, AER_TTD with the Proposed Technique

Sr. No.	Time	Performance Metrics	Related Technique, AER_TTD	Proposed Technique
1.	6.48354s	Delay	29.0144	17.5487
2.	6.48354s	Packet loss	24.9123	2.9561
3.	6.49356s	Throughput	28.9514	36.7390
4.	6.48354s	Overhead	54.9489J	27.4941J
5.	6.48895s	Energy	20.9219J	13.9611J

5. CONCLUSION AND FUTURE SCOPE :

In this research, the focus is on analyzing the operation of Low Rate DDoS and DoF Attacks, especially the Emerging Black Nurse Attack, specifically, comparing Fuzzy logic and Node Localization Techniques under uniform and partially shaded conditions. The Node localization techniques offers betterment in detecting compromised nodes during DDoS attacks. However, in previous related works, it has been analyzed that rule activity is static in nature, there is no histogram of real-time data based on which firewall can accept and reject the packet, which affects the performance of the network to address these limitations. In comparison to previous works, the dynamic mechanism is used in the proposed work which will analyze patterns and detect attacks from the network. To analyze these patterns from the network, fuzzy rules are generated based on the network. These fuzzy rules detect and isolate attacks from the network. In Addition, Node localization Technique is also used to detect and isolate malicious nodes from the network and establish the best and most secure path from source to destination. The performance of the proposed system based on Node localization technique encapsulating fuzzy rules has been successfully compared with the previous research work in terms of many evaluation metrics like Delay, Throughput, Packet loss, Overhead, and Energy. These results indicate that the proposed Node localization Technique exhibits a significantly low Delay, packet loss and overhead with a high volume of throughput, which uses low energy during the process in comparison to related work. In future, a system based on generalization of early rejection rules with time to defend duration, to cover other classes of low-rate DoF attacks can be developed. Also, an open source firewall can be implemented in the future work.

REFERENCES:

1. R. C. Diovu and J. T. Agee (2017), "Quantitative analysis of firewall security under DDoS attacks in smart grid AMI networks," *IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON)*, Owerri, Nigeria, pp. 696-701.
2. E. C. Amadi, G. E. Eheduru, F. U. Eze, C. Ikerionwu and K. C. Okafor (2017), "Anti- DDoS firewall; A zero-sum mitigation game model for distributed denial of service attack using Linear programming," *IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, Iran*, pp. 0027-0036
3. J. Ramprasath, A. B. Arockia Christopher, M. Balakrishnan and A. S. M. Murugavel (2022), "Denial of Service Malevolent Traffic Identification and Prevention in Software Defined Networking," *2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Greater Noida, India, pp. 400-405
4. N. Naik, P. Jenkins, R. Cooke, D. Ball, A. Foster and Y. Jin (2017), "Augmented windows fuzzy firewall for preventing denial of service attack," *IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, Naples, Italy, pp. 1- 6

5. N. Naik and P. Jenkins (2016), "Fuzzy reasoning based Windows Firewall for preventing denial of service attack," *IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, Vancouver, BC, Canada, pp. 759-766
6. M. Sinha, P. Bera and M. Satpathy (2021), "An Anomaly Free Distributed Firewall System for SDN," *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Dublin, Ireland, pp. 1-8
7. Z. Trabelsi, S. Zeidan and K. Hayawi (2019), "Denial of Firewalling Attacks (DoF): The Case Study of the Emerging Black Nurse Attack," in *IEEE Access*, vol. 7, pp. 61596- 61609.
8. A. X. Liu, A. R. Khakpour, J. W. Hulst, Z. Ge, D. Pei and J. Wang (2017), "Firewall Fingerprinting and Denial of Firewalling Attacks," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1699-1712.
9. Z. Trabelsi and S. Zeidan (2019), "Resilence of Network Stateful Firewalls against Emerging DoS Attacks: A Case Study of the BlackNurse Attack," *IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, Abu Dhabi, United Arab Emirates, pp. 1-8
10. Z. Trabelsi, S. Zeidan and H. Saleous (2019), "Teaching Emerging DDoS Attacks on Firewalls: A Case Study of the BlackNurse Attack," *IEEE Global Engineering Education Conference (EDUCON)*, Dubai, United Arab Emirates, pp. 977-985
11. K. Hayawi, Z. Trabelsi, S. Zeidan and M. M. Masud (2020), "Thwarting ICMP Low- Rate Attacks Against Firewalls While Minimizing Legitimate Traffic Loss," in *IEEE Access*, vol. 8, pp. 78029-78043.
12. G. Vira Yudha and R. Wisnu Wardhani (2021), "Design of a Snort-based IDS on the Raspberry Pi 3 Model B+ Applying TaZmen Sniffer Protocol and Log Alert Integrity Assurance with SHA-3," *9th International Conference on Information and Communication Technology (ICoICT)*, Yogyakarta, Indonesia, pp. 556-561
13. M. R. Amal and P. Venkadesh (2022), "H-DOCTOR: Honeypot based firewall tuning for attack prevention", *Measurement: Sensors*, vol. 3, no. , pp. 24-30.
14. M. Dimolianis, D. K. Kalogeras, N. Kostopoulos and V. Maglaris (2022), "DDoS Attack Detection via Privacy-aware Federated Learning and Collaborative Mitigation in Multi-domain Cyber Infrastructures," *IEEE 11th International Conference on Cloud Networking (CloudNet)*, Paris, France, pp. 118-125
15. Y. Fu, M. H. Au, R. Du, H. Hu and D. Li (2020), "Cloud Password Shield: A Secure Cloud-based Firewall against DDoS on Authentication Servers," *IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, Singapore, Singapore, pp. 1209-1210
16. T. V. Krishna and P. Karthik (2022), "Dominance of Hardware Firewalls and Denial of Firewall Attacks (Case Study BlackNurse Attack)", *International Journal of Science and Research (IJSR)*, vol. 11, no. 4, pp. 6263-6271.
17. Z. Trabelsi, S. Zeidan, K. Shuaib and K. Salah (2018), "Improved Session Table Architecture for Denial of Stateful Firewall Attacks," in *IEEE Access*, vol. 6, pp. 35528-35543.
18. G. L. Frazier, J. A. McGill, R. Zarookian, S. Robertson, B. Floyd and P. M. McNeely (2019), "The NNBC Anti-DDoS Firewall," MILCOM 2019, *IEEE Military Communications Conference (MILCOM)*, Norfolk, VA, USA, 2019, pp. 1-7
19. B. Rashidi, C. Fung and M. Rahman (2018), "A scalable and flexible DDoS mitigation system using network function virtualization," NOMS 2018 - 2018 *IEEE/IFIP Network Operations and Management Symposium*, Taipei, Taiwan, pp. 1-6
20. J. He, Y. Tan, W. Guo and M. Xian (2020), "A Small Sample DDoS Attack Detection Method Based on Deep Transfer Learning," *International Conference on Computer Communication and Network Security (CCNS)*, Xi'an, China, 2020, pp. 47- 50
21. A. E. Cil, K. Yildiz and A. Buldu (2020), "Detection of DDoS attacks with feed forward based deep neural network model", *Expert Systems with Applications*, vol. 7, no. 2, pp. 619-624.
22. K. Singh, K. S. Dhindsa and D. Nehra (2020), "T-CAD: A threshold based collaborative DDoS attack detection in multiple autonomous systems", *Journal of Information Security and Applications*, vol. 9, pp. 37075-37085.
23. N. M. Yungaicela-Naula, C. Vargas-Rosales and J. A. Perez-Diaz (2021), "SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning," in *IEEE Access*, vol. 9, pp. 108495-108512.
24. S. Yeom, C. Choi and K. Kim (2022), "LSTM-Based Collaborative Source-Side DDoS Attack Detection," in *IEEE Access*, vol. 10, pp. 44033-44045.