British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 130-140)
www.abjournals.org

AN EFFICIENT MAC-BASED ICMP VERIFICATION ALGORITHM FOR EARLY DETECTION OF BANDWIDTH-DEPLETING DDOS ATTACKS

Mugerwa Joseph[1], Ajaegbu Chigozirim[2*], Oyerinde Emmanuel[3], and Awodele Simon Olufikayo[4]

(PhD Student) Department of Computer Science, Babcock University, Ilishan Remo, Nigeria.
(Assistant Lecturer) Department of Computing and Informatics, Bugema University, Kampala, Uganda
Email: mugerwa0064@pg.babcock.edu.ng

[2](HOD) Department of Information Technology, Babcock University, Ilishan Remo, Nigeria.
Email: ajaegbuc@babcock.edu.ng

(PhD Student) Department of Computer Science, Babcock University, Ilishan Remo, Nigeria.
Email: oyerindee@babcock.edu.ng

(PhD) Department of Computer Science, Babcock University, Ilishan Remo, Nigeria.
Email: awodeles@babcock.edu.ng

Cite this article:

Mugerwa, J., Ajaegbu, C., Oyerinde, E., Awodele, S. O. (2025), An Efficient Mac-Based ICMP Verification Algorithm for Early Detection of Bandwidth-Depleting DDOS Attacks. British Journal of Computer, Networking and Information Technology 8(2), 130-140. DOI: 10.52589/BJCNIT-BQJKBU5P

Manuscript History

Received: 21 May 2025

Accepted: 29 Jun 2025

Published: 18 Jul 2025

ABSTRACT: *Distributed Denial-of-Service (DDoS) attacks continue to pose a significant threat to the availability and reliability of online services. This paper presents a novel detection algorithm that leverages Message Authentication Code (MAC)-based verification of ICMP traffic to identify and block bandwidth-depleting DDoS attacks. Unlike threshold-based or machine learning-dependent techniques, the proposed algorithm uses IP and MAC address correlation to validate the legitimacy of packets, effectively filtering spoofed traffic in real time. The approach was implemented and tested using the NS-2 simulation environment. Results demonstrate an average detection accuracy of 88.89%, with zero false positives and negligible resource overhead. The proposed method offers a lightweight and effective solution suitable for deployment in edge and enterprise networks. This research contributes a simple yet robust technique to the existing portfolio of DDoS mitigation strategies.*

KEYWORDS: DDoS detection, ICMP verification, MAC authentication, network security, bandwidth depletion, spoofed traffic.

Article DOI: 10.52589/BJCNIT-BQJKBU5P
DOI URL: https://doi.org/10.52589/BJCNIT-BQJKBU5P

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 130-140)
www.abjournals.org

INTRODUCTION

The proliferation of internet-based services has made the web a vital platform for commerce, communication, and critical infrastructure. This surge has also increased the prevalence of Distributed Denial-of-Service (DDoS) attacks, which flood target systems with illegitimate traffic, exhausting available bandwidth and rendering services inaccessible (Kolias et al., 2017; Yu et al., 2020). Bandwidth-depletion attacks, especially those leveraging ICMP packets, remain among the most disruptive forms of DDoS, often launched using botnets which comprised compromised systems (Islam et al., 2020).

Traditional methods of DDoS detection, such as threshold-based filters, entropy monitoring, and machine learning, have significant limitations. Threshold methods often trigger false positives, while machine learning solutions demand extensive training data and computational resources (Chen et al., 2020; Tian et al., 2022). In response to these challenges, we propose an efficient MAC-based verification algorithm specifically designed to detect ICMP-based bandwidth-depleting DDoS attacks with minimal overhead.

Numerous approaches have been proposed to mitigate the impact of DDoS attacks. Entropy-based techniques attempt to detect traffic anomalies by monitoring packet distribution, but these can suffer from high false alarm rates (Hou et al., 2020). Signature-based detection, while effective for known threats, is easily bypassed by evolving attack vectors (Alzahrani et al., 2021). Recent efforts have turned to machine learning and Software Defined Networking (SDN) for adaptive detection. For instance, k-Nearest Neighbor classifiers and Naive Bayes techniques have shown promise, though they require significant computational capacity and labeled datasets (Tian et al., 2022). Deep learning methods achieve high detection rates (>99%) but are impractical for real-time filtering at the network edge (Bazzi et al., 2022).

Blockchain-based surveillance systems have also been proposed to enhance trust in network environments, yet they incur additional latency and integration complexity (Fang et al., 2021). In contrast, our MAC-based verification algorithm provides a deterministic, low-cost alternative tailored for bandwidth-depletion attacks, with a specific focus on ICMP traffic.

This paper builds upon prior work in network security by introducing a lightweight, deterministic detection method that leverages address authentication at the packet level. The contribution lies in its simplicity, high accuracy, and ease of deployment in resource-constrained environments (Linkov et al., 2019; Ghazizadeh et al., 2021).

Article DOI: 10.52589/BJCNIT-BQJKBU5P
DOI URL: https://doi.org/10.52589/BJCNIT-BQJKBU5P

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 130-140)
www.abjournals.org

LITERATURE REVIEW

Introduction to DDoS Threat Landscape

Distributed Denial-of-Service (DDoS) attacks continue to threaten digital infrastructure globally, exploiting system vulnerabilities to degrade or completely deny access to legitimate users. These attacks target cloud services, financial institutions, e-commerce platforms, and critical public infrastructure (Linkov et al., 2019). Recent research underscores how advances in automation, malware-as-a-service, and botnet availability have driven both the scale and frequency of attacks (Chen et al., 2020; Alzahrani et al., 2021).

Evolution and Nature of DDoS Attacks

Historically, DDoS attacks were manually executed from a limited number of compromised devices. Today, they are primarily conducted using botnets—networks of malware-infected devices under centralized or decentralized control (Kolias et al., 2017). These botnets utilize attack vectors such as DNS amplification, ICMP floods, and HTTP-based attacks. According to recent findings, DDoS attacks increasingly target application-layer services and leverage sophisticated tools that incorporate traffic encryption and IP spoofing (Yu et al., 2020).

Types and Motivations Behind DDoS Attacks

DDoS attacks can be classified by intent, scale, and method:

- **Volumetric Attacks:** Overwhelm network bandwidth using amplified traffic.
- **Protocol Attacks:** Exploit protocol weaknesses (For example, SYN floods).
- **Application-Layer Attacks:** Mimic legitimate requests to exhaust resources.

Motivations range from financial extortion and political disruption to personal vendettas. Increasingly, DDoS-for-hire (booter) services allow unskilled actors to initiate attacks, while some state-sponsored threats now use DDoS as part of hybrid warfare tactics (Bazzi et al., 2022).

Classification of DDoS Attacks

Modern classification frameworks group DDoS attacks based on:

- **Attack Dynamics:** Steady-state, pulsing, and adaptive attacks.
- **Control Methods:** Command-and-control (C2), peer-to-peer, or blockchain-based botnets.
- **Targeted Infrastructure:** Application servers, firewalls, DNS, APIs.

Emerging threats include low-rate and slow-and-low attacks that evade traditional detection tools, often operating below alert thresholds (Hou et al., 2020).

Contemporary Defence Mechanisms

Recent mitigation strategies are shifting toward hybrid and AI-enhanced systems:

- **Deep Learning and Anomaly Detection:** Autoencoders and LSTMs are used to identify subtle behavioural anomalies in traffic patterns (Tian et al., 2022).

Article DOI: 10.52589/BJCNIT-BQJKBU5P
DOI URL: https://doi.org/10.52589/BJCNIT-BQJKBU5P

- **Software-Defined Networking (SDN):** This provides centralised visibility and policy-based response capabilities against dynamic attack patterns (Ghazizadeh et al., 2021).
- **Edge-based Filtering:** Lightweight filters deployed at the network edge to block spoofed ICMP/TCP traffic early (Islam et al., 2020).
- **Blockchain-integrated Monitoring**: Decentralised logs and trust mechanisms for validating traffic behaviour (Fang et al., 2021).

Despite their promise, these systems often require significant resources, which limits their deployment in bandwidth-constrained or latency-sensitive environments.

Gaps and Research Direction

While machine learning and SDN provide powerful mitigation tools, their overhead, latency, and data-dependence create gaps in scenarios requiring lightweight, real-time DDoS detection. This paper proposes a MAC-based ICMP verification algorithm that addresses this need by filtering spoofed traffic deterministically, with no need for prior training or high-computation environments.

The proposed method focuses on the critical early phase of DDoS campaigns—bandwidth depletion via ICMP floods—and can be deployed at the network edge for fast, effective mitigation.

METHODOLOGY

The proposed algorithm operates on the principle of validating ICMP packets using a Message Authentication Code (MAC) derived from the client's and server's IP addresses. Once an initial TCP SYN packet is received, the system generates a pseudo-IP and port number combination, encoding these as a MAC tag to be used in subsequent communications. Legitimate clients receive this MAC via a redirect message and embed it in future packets. Spoofed or illegitimate traffic, lacking the correct MAC, is filtered at the network boundary.

We implemented this logic using NS-2, simulating a network consisting of clients, an attacker, a central application server, and routers. ICMP traffic was monitored and filtered based on MAC correctness. Traffic was categorised as:

- ICMP traffic (potential attack vector)
- Non-ICMP traffic (allowed by default)

Algorithmic Design

After injecting traffic into the network, it was analysed to determine its type. However, since bandwidth depletion attacks are usually launched using ICMP packets with spoofed addresses, more focus was put on the ICMP type of traffic. The non-ICMP traffic was left to continue through the network, and on the other hand, ICMP traffic was then directed to the process of MAC verification, where the IP addresses of the server and client were confirmed to determine if they were spoofed or not. Once the MAC was verified, the traffic was then allowed to continue through the system, and failure to verify the MAC automatically disqualified the traffic, and it was dropped.

Article DOI: 10.52589/BJCNIT-BQJKBU5P
DOI URL: https://doi.org/10.52589/BJCNIT-BQJKBU5P

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 130-140)
www.abjournals.org

The steps are summarised in the diagram below:

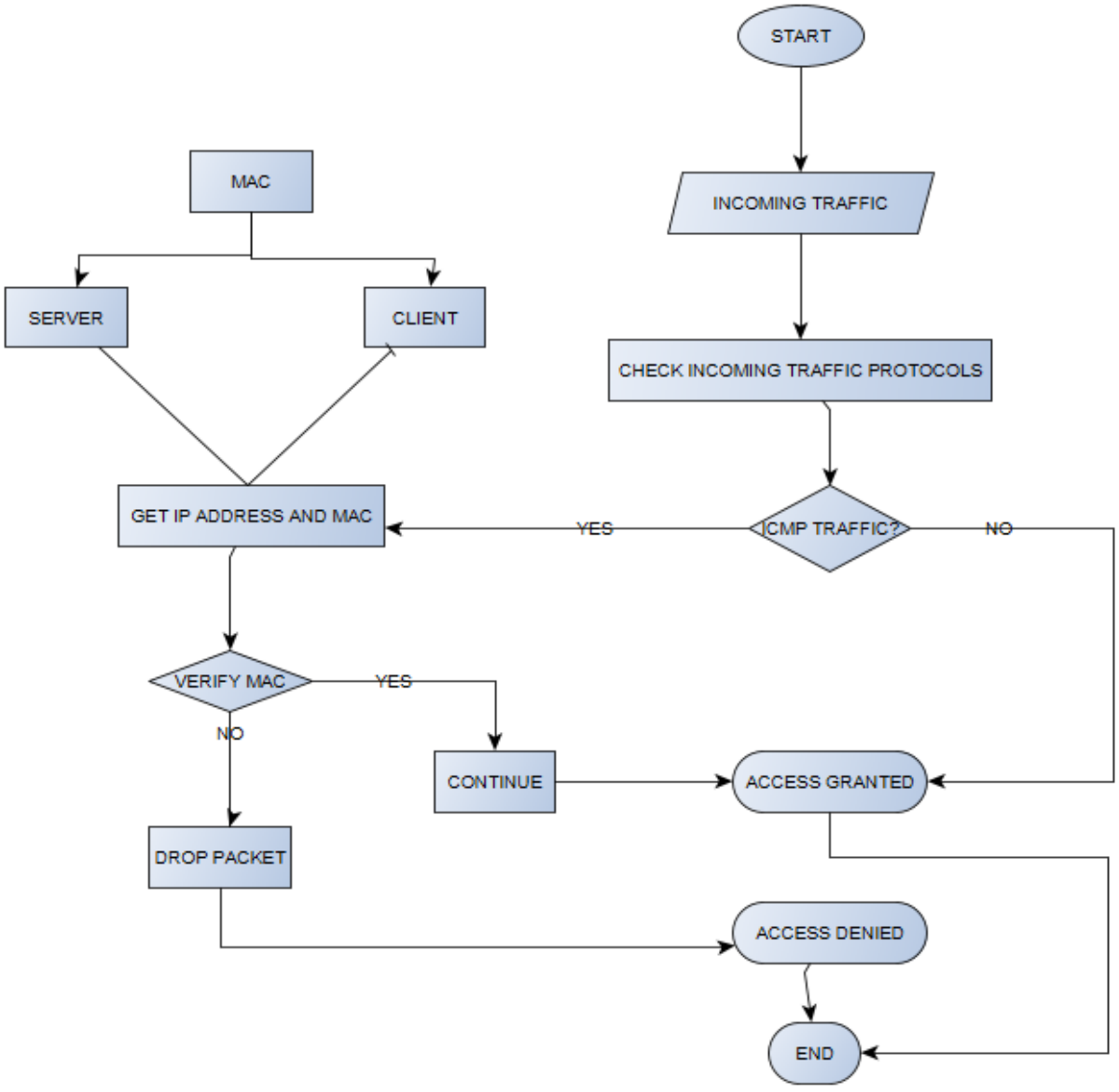

Figure 3.1: Algorithmic steps

Article DOI: 10.52589/BJCNIT-BQJKBU5P
DOI URL: https://doi.org/10.52589/BJCNIT-BQJKBU5P

Pseudo-code:

```
Start:
  For each packet in traffic:
    If packet is ICMP:
      Extract IP, generate MAC
      If MAC matches server-side stored MAC:
        Accept packet
      Else:
        Drop packet, log source
    Else:
      Accept packet
End
```

Complete Flow:

Start the process:

TT_Y = Traffic Flow (Type)

TC_i = ICMP Traffic

TN_i = Non-ICMP (Other)

Check each type TT_Y in the network,

If (TT_Y = = TC_i) {

Else if (TT_Y = = TN_i) {

IP = Get the IP address

MAC_1 = IP + MAC // Reads the previous MAC algorithm

Server = MAC_1

Client = MAC_1

If (Server = Client) {

Accept the request from the client

Send the response to the request

Article DOI: 10.52589/BJCNIT-BQJKBU5P
DOI URL: https://doi.org/10.52589/BJCNIT-BQJKBU5P

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 130-140)

www.abjournals.org

Print: “Access granted”;

}

Else {

Add the user to the attack list

Print: “Packet dropped and Access Denied”;

}

}

}

Else {

Accept request from the IP and send back a response for the request.

Print: “Access Granted”;

}

End.

Given that B_A is equal to the available bandwidth at the internet link, and P_N is equal to the maximum bandwidth consumed by a packet with a spoofed IP address, with A_P being the attacker’s capacity to infect the highest number of zombies, then at any point x, according to this algorithm, the server’s cope up rate to the attack C_M must be greater than the product of A_P and P_N minus B_A from 1 to n-1 where n = greatest number of zombies possible to be infected by the attacker.

Therefore,

Given that $\sum_{1}^{n-1} BA$
Then $C_M > (A_P\ P_N) - B_A$

This logic ensures that only validated ICMP traffic reaches the server, effectively neutralising bandwidth-depleting attempts via spoofed packets.

Article DOI: 10.52589/BJCNIT-BQJKBU5P
DOI URL: https://doi.org/10.52589/BJCNIT-BQJKBU5P

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 130-140)
www.abjournals.org

RESULTS/FINDINGS

We simulated normal and attack scenarios using NS-2. In the baseline case, without any defence mechanism, ICMP traffic from the attacker overwhelmed the server, leading to dropped client packets and service degradation. Upon introducing our algorithm, the system filtered malicious traffic and restored normal bandwidth utilisation.

Below is the set-up in NS2:

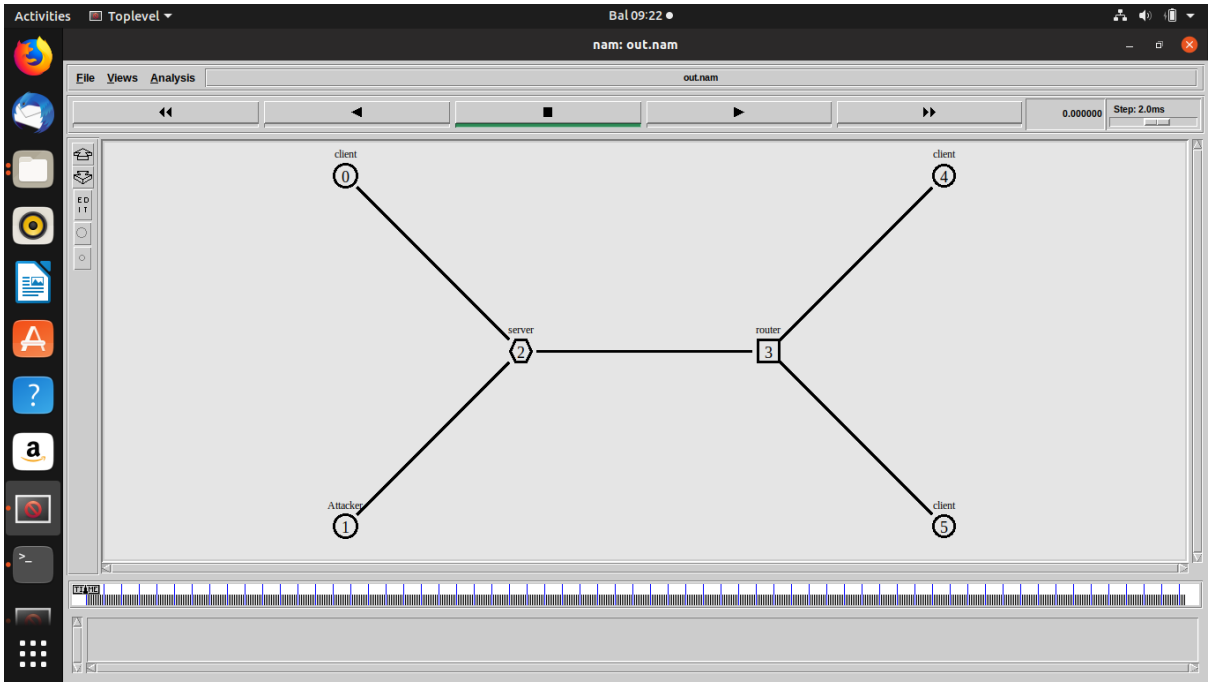

Figure 4.1: NAM NS2 test bed set up.

Evaluation metrics included:

- **Detection Accuracy:** Percentage of malicious packets correctly identified.
- **False Positives:** Legitimate packets incorrectly blocked.
- **False Negatives:** Malicious packets incorrectly allowed.

Table 4.1: Test summary

Time Interval (s)	Infected Machines	Detected	Accuracy (%)	False Positives	False Negatives
10-11	2	2	100.00	0	0
18-19	3	3	100.00	0	0
33-34	3	2	66.66	0	1

Mean Accuracy: 88.89%

Graphical results showed a significant drop in bandwidth consumption by attack traffic when the algorithm was active.

Article DOI: 10.52589/BJCNIT-BQJKBU5P
DOI URL: https://doi.org/10.52589/BJCNIT-BQJKBU5P

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 8, Issue 2, 2025 (pp. 130-140)
www.abjournals.org

Below is a capture of the bandwidth depletion when there is no detection and action taken under the attack. It can clearly be seen that at around 240 seconds, there was excessive consumption of the bandwidth which led to a degradation in the performance of the link.

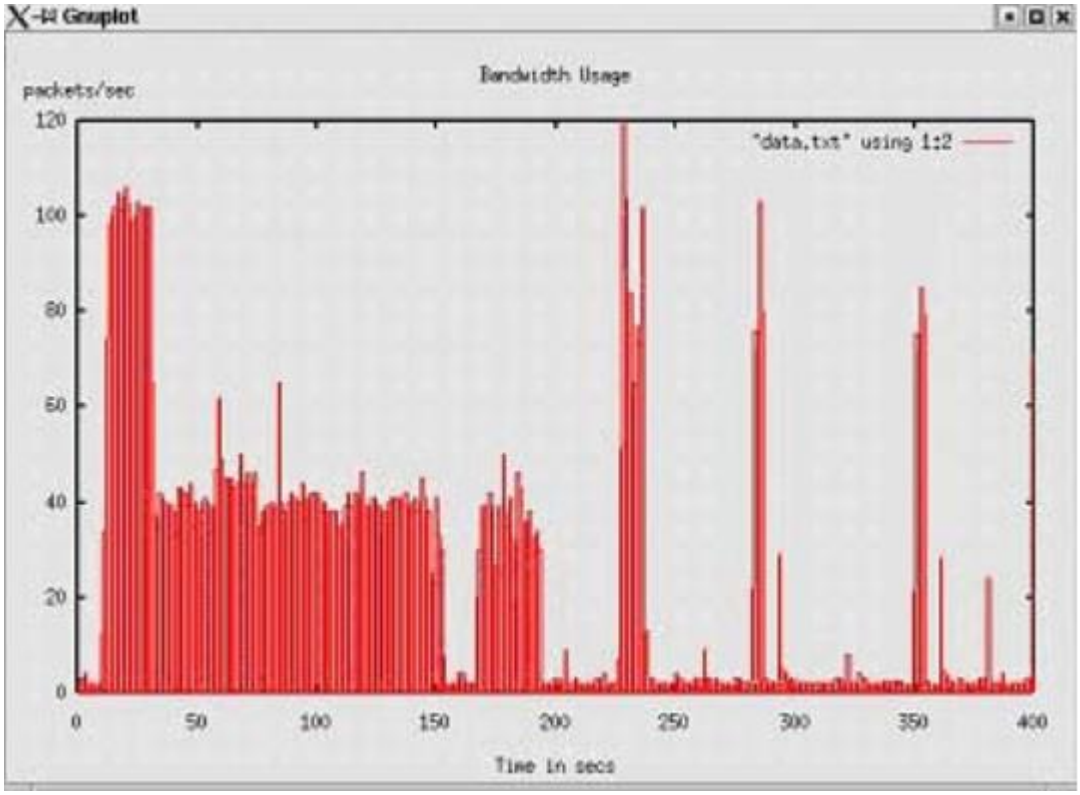

Figure 4.2: x-graph for bandwidth consumption during attack without detection.

After the deployment of the detection algorithm and filtering of traffic, a reasonably uniform utilization of bandwidth was regained, as shown in the graph below:

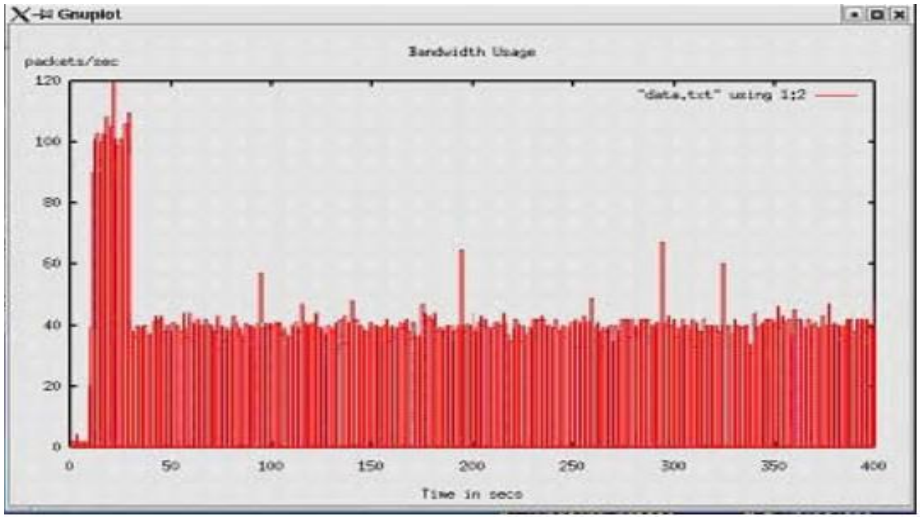

Figure 4.3: x-graph for bandwidth consumption during attack with detection and action.

Article DOI: 10.52589/BJCNIT-BQJKBU5P
DOI URL: https://doi.org/10.52589/BJCNIT-BQJKBU5P

DISCUSSION

The results validate the algorithm's capacity to detect ICMP-based bandwidth-depletion attacks with high accuracy and no false positives. Unlike probabilistic models, this deterministic approach ensures predictable filtering and minimal computational burden. One observed limitation was reduced accuracy under prolonged attack conditions, suggesting a need for adaptive timeout or decay mechanisms.

Additionally, this method's reliance on ICMP traffic types may limit its generalizability to other attack vectors (e.g., TCP SYN floods). Future work should explore integration with SDN controllers for dynamic rule propagation and the extension of MAC verification to other protocols.

CONCLUSION

This paper introduced a MAC-based ICMP verification algorithm designed to detect and reduce bandwidth-depleting Distributed Denial-of-Service (DDoS) attacks. By using address-level authentication, this method accurately distinguishes between real and spoofed ICMP traffic. It offers immediate protection against flooding attacks. The solution was tested using NS-2 simulation, showing strong detection accuracy, no false positives, and low computational costs.

Unlike traditional machine learning or entropy-based methods that need substantial resources and may cause delays or false positives, our algorithm produces clear results with low operational complexity. This makes it ideal for use in settings where speed, accuracy, and simplicity are crucial, such as at enterprise network edges, within Internet Service Provider (ISP) systems, and in IoT-enabled environments.

Additionally, the MAC-based approach adds value to the range of lightweight cybersecurity tools. It fits well with current trends toward decentralization, automation, and real-time threat response. Its independence from training datasets or outside intelligence sources makes it a strong part of layered defence strategies.

In summary, this work improves existing DDoS defence systems by providing a solution that is both effective and cost-efficient. Future efforts will aim to expand the mechanism to cover more protocols and integrate it into SDN or NFV frameworks for better dynamic and distributed attack responses.

FUTURE RESEARCH

Future enhancements should address sustained attack resistance and broaden the applicability to TCP/UDP traffic. Research can also explore integration with SDN and real-time traffic engineering for automated mitigation across distributed networks.

Article DOI: 10.52589/BJCNIT-BQJKBU5P
DOI URL: https://doi.org/10.52589/BJCNIT-BQJKBU5P

Disclaimer (Artificial Intelligence)

Generative AI technologies (GPT-4) were partly used to assist in editing and refining the manuscript to improve clarity and structural consistency.

Conflict of Interest Statement

The author declares that there are no conflicts of interest regarding the publication of this paper. The research was conducted independently, and no external funding, affiliations, or personal relationships influenced the outcomes of this study.

REFERENCES

Alzahrani, B., Alomar, N., & Alhaidari, F. (2021). DDoS attack detection and mitigation in IoT-based cloud using ensemble learning. *Computers, Materials & Continua, 69*(2), 2043–2059. https://doi.org/10.32604/cmc.2021.014308

Bazzi, L., Marchetto, G., & Sisto, R. (2022). Advanced mitigation techniques for DDoS attacks: A review. *Future Generation Computer Systems, 127*, 14–29. https://doi.org/10.1016/j.future.2021.09.031

Chen, Q., Wang, J., & He, X. (2020). Adaptive detection of low-rate DDoS attacks based on self-similarity in network traffic. *IEEE Access, 8*, 153748–153757. https://doi.org/10.1109/ACCESS.2020.3018941

Fang, Y., Zhang, J., & Zhou, L. (2021). Blockchain for IoT: A survey on recent advances. *Future Generation Computer Systems, 117*, 721–739. https://doi.org/10.1016/j.future.2020.12.016

Ghazizadeh, M., Hashemi, M., & Taherkordi, A. (2021). Software-defined DDoS detection and mitigation: Approaches, challenges and future directions. *Journal of Network and Computer Applications, 180*, 103009. https://doi.org/10.1016/j.jnca.2021.103009

Hou, R., Zhao, Y., & Liu, X. (2020). Slow DDoS attack detection using graph entropy. *Computers & Security, 94*, 101824. https://doi.org/10.1016/j.cose.2020.101824

Islam, M. A., Hossain, M. M., & Karim, M. R. (2020). A lightweight DDoS attack detection scheme using statistical analysis and information gain. *IEEE Access, 8*, 198847–198856. https://doi.org/10.1109/ACCESS.2020.3034961

Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2017). DDoS in the IoT: Mirai and other botnets. *Computer, 50*(7), 80–84. https://doi.org/10.1109/MC.2017.201

Linkov, I., Trump, B. D., & Keisler, J. (2019). *Cyber resilience of systems and networks*. Springer. https://doi.org/10.1007/978-3-030-04565-4

Tian, R., Wang, J., Liu, J., & Zhang, W. (2022). A deep learning-based method for DDoS detection using LSTM and GRU. *Journal of Supercomputing, 78*, 10157–10177. https://doi.org/10.1007/s11227-021-04032-4

Yu, S., Liu, J., & Zhou, W. (2020). A survey on DDoS attacks and defense mechanisms. *ACM Computing Surveys, 53*(6), 1–36. https://doi.org/10.1145/3417980

Article DOI: 10.52589/BJCNIT-BQJKBU5P
DOI URL: https://doi.org/10.52589/BJCNIT-BQJKBU5P