Review Comments: 1

1. Enhanced alert generation system with attacker IP for DOS attacks is the proposed title of this paper

- Yes. *Enhanced Alert Generation System with Attacker IP for DoS Attacks*

2. How to avoid the DDOS attacks?

- To prevent DDoS attacks, our system includes rate limiting, IP blocking, and dynamic threshold adjustments based on traffic patterns.

3. How to achieve the IP tracking process?

- The system uses Pyshark to analyze network traffic in real-time, identifying and logging the attacker's IP for further action.

4. How to enhance the performance?

- Performance is enhanced by optimizing packet processing to reduce false alerts and resource usage, improving detection speed and accuracy.

5. How to achieve the monitoring process?

- Our system performs continuous network monitoring, capturing and analyzing packets in real-time for prompt detection of suspicious activity.

6. Survey of literature is not systematic

- The literature survey has been reorganized to categorize existing techniques by their detection method.

7. How to achieve high accuracy?

- High accuracy is achieved through dynamic threshold tuning and minimizing false positives, helping the system distinguish between normal traffic and attacks effectively. These techniques ensure reliable DoS detection.

8. How the results are validated?

- Results are validated by testing the system in a Virtual network setup, focusing on its accuracy and speed in detecting attacks. This confirms its effectiveness in real-time situations.

9. Figures are of poor resolution and clarity.

- All figures have been updated to high-resolution formats for clear visualization.

Review comments-2

1. What are the critical issues to be considered when selecting the appropriate technique for the research study?

- We considered factors like accuracy, resource efficiency, and scalability when selecting detection techniques.

2. There is no new research statement for this proposed work. Provide the details in the appropriate section.

- This research addresses the need for adaptive DoS detection with real-time alerting and IP tracking to improve network security.

3. The author is not mentioning the research motivation or gap for this current research work. Provide the details.

- Current systems lack real-time IP tracking and adaptive thresholds, which our approach addresses to enhance detection reliability.

4. What is existing system mentioned in the table?

- The table highlights conventional DoS detection methods and their limitations, like high false positives and lack of real-time tracking. Our system addresses these with adaptive thresholds and real-time IP tracking.

5. What are the four methods to detect prevent cybersecurity threats?

- Four key methods include intrusion detection, behavior analysis, anomaly detection, and signature-based detection

6. Manuscript should be edited for proper English language, grammar and punctuation. Avoid using personal pronouns and informal words like landscape. Machine generated words found [For Ex: DoS assaults, DDoS assaults].Some of the figures are blurry.

- The manuscript was checked for formal language, grammar accuracy, and the elimination of informal and machine-generated words.