Automated System for Detecting Cyber Bot Attacks in 5G Networks using Machine Learning

Thrupthi C.P.[1], Chitra K.[2*], Harilakshmi V.M[3]

[1,2,3]Dayananda Sagar Academy of Technology and Management, Karnataka, India

***Email:** chitra-mca@dsatm.edu.in

Abstract

The automated system for detecting cyber bot attacks in 5G networks relies on cloud servers to store data, facilitating the global access necessary for online transactions and services, but points to the rise of cybercrime with information security flaws and human stealth Attackers known as "Botmasters" spread Trojan malware to grow bots on the network causing DDOS attacks. Botnets are compromised computer networks controlled by attackers that are visible for this reason. Machine learning algorithms have been proposed to identify bot networks with a focus on extracting features from high-dimensional datasets. However, the literature pays little attention to selection methods, which are crucial for developing effective machine-learning models.

Keyword

Bot attacks, 5G network attacks, cyber-attacks, Botnet attacks

Introduction

A Bot is an autonomous program that automatically performs tasks without knowing to areal user (Hadianto et al., 2018). A collection of machines that run such autonomous bots is called a botnet. The bot is remotely controlled by a command-and-control server. The black-hat developers created highly sophisticated malware that is difficult to detect and remove. Bot program is stealthy during its whole life cycle. They had generated a relatively small network footprint and most of the time remained ideal for stealing information. The concept of a remote-controlled computer bot started with Internet Relay Chat (IRC). It provides one too many communications channels and supports a very substantial number of concurrent users. The egg drop was the first bot developed in 1993. As the internet connects billions of computers, tablets, and smartphones to share information across the globe, people are relying on these technologies to share their personal additionally business information. The black hat hackers used their vulnerabilities to perform attacks. The initial intention of these cyber criminals was just to gain fame but over the period they are doing criminal activities to earn money. The phrases "robot" and "network" are the sources of the term "Botnet" In this context, an automated device has been infected by malicious code and is a member of a network, or net, of infected devices under the control of a single attacker or attack group. One term for a bot is a zombie, and another one for a botnet is a zombie army. Both names (bot and zombie) imply the mindless automatic

Submission: 16 October 2024; **Acceptance:** 5 November 2024

propagation of something malicious (malware) by agents that are possessed in some way (by the threat actor). Usually, the botnet virus searches the internet for susceptible devices instead of focusing on certain people, businesses, or sectors. The goal of building a botnet is to infect as many connected devices as you can, and then utilize their resources and processing capacity for automated operations that are typically hidden from the devices' users.

Problem Statement

The web is critical to Internet infrastructure, but it often has security weaknesses and vulnerabilities. Nor is security a key design consideration for many widely deployed 5G network devices. Such analysis makes it especially difficult to detect and control malware bots that can compromise devices. These bots can exploit vulnerabilities in the network, posing a serious security risk. The complexity of 5G networks and sophisticated bot attacks make detecting and mitigating these threats difficult, underscoring the need for comprehensive security measures and detection systems.

Literature Review

Khalid Alissa, Tahir Alyas, Kashif Zafar, Qaiser Abbas, Nadia Tabassum, and Shadman Sakib presented that Internet attacks involving botnets are characterized by multiple forms, often in different IoT environments, beginning with scanning activities and ending with denial of service distributed (DDoS) attacks (Alissa et al., 2022).

Yogita Barse and Dr. Sonali Tidke presented that botnets pose significant security risks and are challenging to identify. Various tools and techniques, such as NetFlow, Snort, Suricata, Entop, and Wireshark, use anomaly and signature-based methods for detection. Additionally, mining-based tools such as Boatminer, Boatsniffer, and Bothnter (powered by Snort) monitor communications between internal and external organizations' versions of Zeus, a popular tool among hackers for studying botnets on the internet (Barse and Tidke, 2020).

Rahmadani Hadianto and Tito Waluyo Purboyo presented SDN architecture that separates the control plane from the data plane and offers several advantages: providing easy changes in network performance by design, lower costs of upgrades and network upgrades, and the flexibility of SDN systems to new technological developments (Hadianto and Purboyo, 2018).

Chaw Su Htwe, Yee Mon Thant, and Mie Mie Su Thwin presented the rapid growth of the Internet of Things gadgets has attracted attackers who target these devices to create networks of bots controlled by bot owners, leading to aggressive attacks on systems Effective systems must be identified, however, most current systems, such as public IDS, based on signatures come and can be circumvented by attackers
(Htwe et al., 2020).

Mads Stege, Jesper Bang, Peter Issam El-Habr, Simon Nam Thanh Vu, and Nicola Dragoni presented the paper on This paper is a systematic update in the literature review of botnets used by a variety of malicious actors for purposes ranging from attack denial to cyber espionage Botnets have adapted to modern platforms such as cars, smartphones, and IoT devices. including advanced countermeasures detection and command control techniques (Thanh et al., 2021).

Ying Xing, Hui Shu, Hao Zhao, Dannong Li, and Li GuoXu introduced a new framework for botnets, summarized the latest botnet detection technologies, and provided a comparison study of the major methods for anomaly-based detection It is important that the paper examines detection strategies in detail and suggest research agendas – Contributions. This highlighted the continued emergence of new botnets and future focus on new technologies and applications (Xing et al., 2021).

Methodology

The approach of identifying cyber bot attacks in 5G networks uses a multi-step approach using Flask for web application interfaces, and Decision Tree algorithms for prediction, firstly collecting and prioritizing network traffic statistics executes the task, which extracts relevant signals of bot activity. A decision tree algorithm is then trained on this pre-processed data to identify the most common dangerous traffic patterns. Once trained, the model is integrated into the Flask web application, enabling real-time predictions of potential bot attacks. Users can interact with the application to upload network traffic data, get instant analytics, and view visual representations of forecast results. This approach ensures that the system is user-friendly and adaptive to evolving threats in 5G environments.

The proposed system is illustrated in figure 1 below. Figure 1 demonstrates the interactions between key system components and external applications. The system itself consists of web data sources that provide raw traffic data to external companies, with users interacting with a web application to enter data and view forecasts, and an alert system that alerts users warning customs about possible threats is analyzed by modules, also f the results are presented to users via the user interface, generated alerts are sent to blast them users are notified of suspicious activities to ensure that threats are detected and responded to in a timely manner This high-level perspective emphasizes data flows and key interfaces within the system.

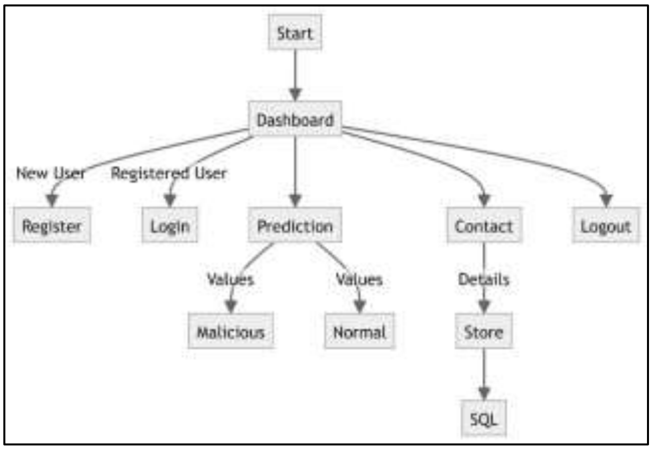

Figure 1: Context Diagram

Results and Discussions

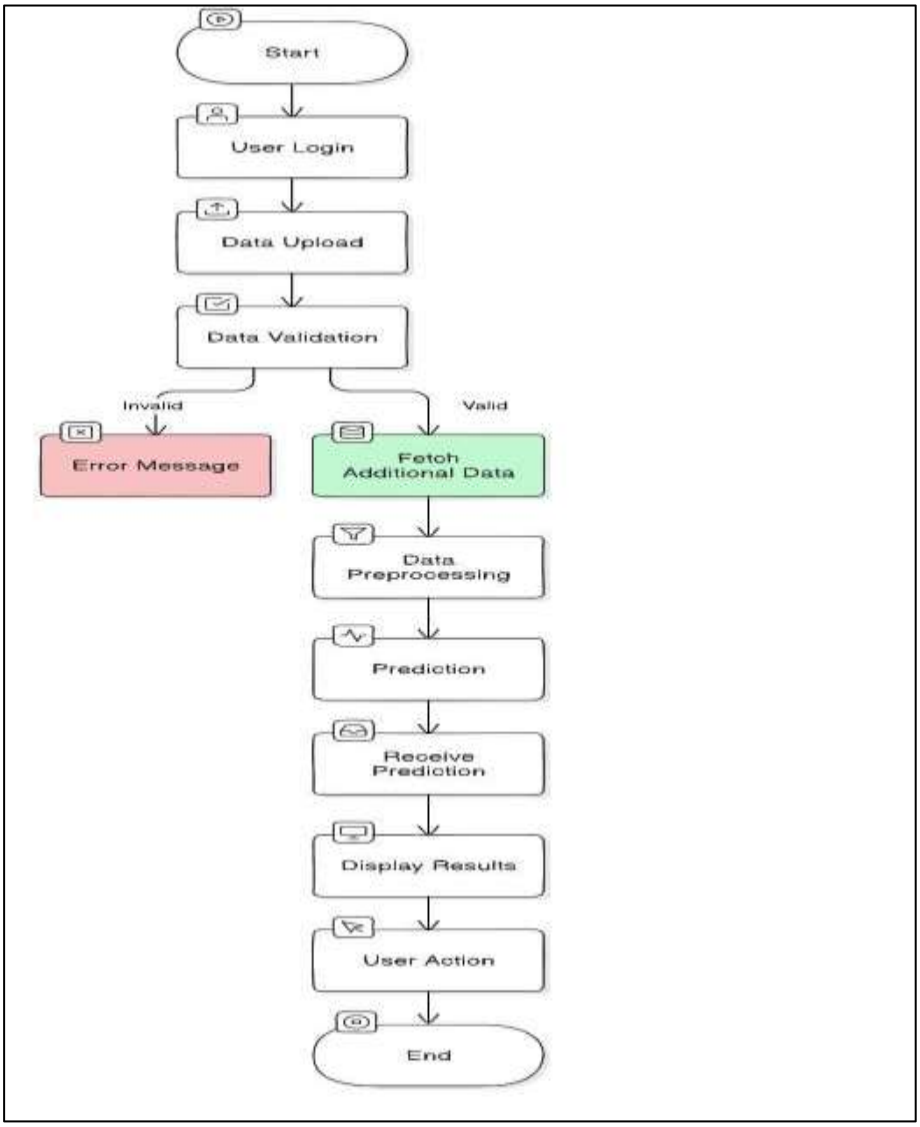

Fig 2: Activity Diagram

Figure 2 shows the workflow and techniques for predicting and detecting malicious network activity through machine learning. This begins with the collection of network traffic data from various sources, which is then pre-processed for troubleshooting purposes It happens. These predictions are displayed to users via a web browser, where they can view detailed insights and visualizations. When something negative is detected, the system issues alerts sent to users. The diagram emphasizes the various activities, decision points, and connections between the sequence of process elements, ensuring a clear comprehension of the procedure from data collection to data processing.

The proposed method for detecting cyber-bot attacks in 5G networks combines a Flask-based web application with a Decision Tree algorithm, forming a robust and scalable solution for real-time monitoring and prediction Flask ensures access to It, additionally, it is user-friendly and provides flexible interfaces for network administrators to address security threats. Decision tree algorithms are chosen because of their robustness and simplicity, providing high accuracy in identifying bot activities by properly classifying data by attributes, and exploiting latency advantages to make faster decisions and reliability required to minimize emergency cyberattacks in 5G deployment environments that continuously analyze network traffic patterns to detect anomalies indicative of bot activity, so that early detection and rapid response can reduce business impact with Flask Integration which supports seamless deployment and scalability, optimizes various network sizes and complexities, while web-application interface to assist managers in reaching logical conclusions on the network -health risk level and enabling transparency to be Increase detection accuracy and performance efficiency security challenges, and provide a scalable framework for future improvements. The proposed method for detecting cyber-bot attacks in 5G networks combines a Flask-based web application with a Decision Tree algorithm, forming a robust and scalable solution for real-time monitoring and prediction Flask ensures access to It, additionally, it is user-friendly and provides flexible interfaces for network administrators to address security threats. Decision tree algorithms are chosen because of their robustness and simplicity, providing high accuracy in identifying bot activities by properly classifying data by attributes, and exploiting latency advantages to make faster decisions and reliability required to minimize emergency cyberattacks in 5G deployment environments that continuously analyze network traffic patterns to detect anomalies indicative of bot activity, so that early detection and rapid response can reduce business impact with Flask Integration which supports seamless deployment and scalability, optimizes various network sizes and complexities, while web-application interface to assist managers in reaching logical conclusions on the network -health risk level and enabling transparency to be Increase detection accuracy and performance efficiency security challenges, and provide a scalable framework for future improvements.

Conclusion

The proposed method for detecting cyber-bot attacks in 5G networks combines a Flask-based web application with a Decision Tree algorithm for real-time monitoring and prediction. This robust and scalable solution ensures access, is user-friendly, and provides flexible interfaces for network administrators to address security threats. Decision Tree algorithms are chosen for their robustness, simplicity, and high accuracy in identifying bot activities. They exploit latency advantages for faster decisions and reliability, minimizing emergency cyberattacks in 5G deployment environments. Flask Integration supports seamless deployment, optimizes network sizes and complexities, and assists managers in determining network health risk levels. This approach increases detection accuracy, performance efficiency, security challenges, and provides a scalable framework for future improvements.

Acknowledgement

The researcher did not receive any funding for this study, and the results have not been published in any other sources.

References

Alissa, K., Alyas, T., Zafar, K., Abbas, Q., Tabassum, N., & Sakib, S.(2022). Botnet attack detection in IoT using machine learning. Computational Intelligence and Neuroscience, 2022(1), ID 4515642. https://doi.org/10.1155/2022/4515642

Barse, Y., & Tidke, S. (2020). A study on BOTNET attacks and detection techniques. IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), 15(3), 1-5. https://doi.org/10.9790/1676-1503020105

Chowdhury, S., Khanzadeh, M., Akula, R., Zhang, F., Zhang, S., Medal, H., … Bian, L. (2017). Botnet detection using graph-based feature clustering. *Journal of Big Data*, *4*(1). https://doi.org/10.1186/s40537-017-0074-7

Gaonkar, S., Dessai, N. F., Costa, J., Borkar, A., Aswale, S., & Shetgaonkar, P. (2020). A Survey on Botnet Detection Techniques. *2020 International Conference on Emerging Trends in Information Technology and Engineering (Ic-ETITE)*. https://doi.org/10.1109/ic-etite47903.2020.id-70

Hadianto, R., & Purboyo, T. W. (2018). A survey paper on botnet attacks and defenses in software-defined networking. International Journal of Applied Engineering Research,13(1), 483-489. https://www.ripublication.com/ijaer18/ijaerv13n1_65.pdf

Htwe, C. S., Thant, Y. M., & Su Thwin, M. M. (2020). Botnets Attack Detection Using Machine Learning Approach for IoT Environment. Journal of Physics: Conference Series, 1646, 012101. https://doi.org/10.1088/1742-6596/1646/1/012101

Ibrahim, W. N. H., Anuar, S., Selamat, A., Krejcar, O., González Crespo, R., Herrera-Viedma, E., & Fujita, H. (2021). Multilayer Framework for Botnet Detection Using Machine Learning Algorithms. IEEE Access, 9, 48753–48768. https://doi.org/10.1109/ACCESS.2021.3060778

Shetu, S. F., Saifuzzaman, M., Moon, N. N., & Nur, F. N. (2019, September). A survey of botnet in cyber security. In *2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT)* (pp. 174-177). IEEE. https://doi.org/10.1109/ICCT46177.2019.8969048

Thanh, S. N., Stege, M., El-Habr, P. I., Bang, J., & Dragoni, N. (2021). Survey on botnets: Incentives, evolution, detection and current trends. *Future Internet*, *13*(8), Article 198. https://doi.org/10.3390/fi13080198

Xing, Y., Shu, H., Zhao, H., Li, D., & Guo, L. (2021). Survey on Botnet Detection Techniques: Classification, Methods, and Evaluation. *Mathematical Problems in Engineering*, *2021*, 1–24. https://doi.org/10.1155/2021/6640499