A Survey of Malicious Traffic Detection Techniques Based on the CTU-13 Dataset

Kadirhan Özdemir, Mete Birol Albayram, Alperen Özgür Özkan
Erzurum Technical University
Erzurum, Türkiye

***Abstract*—This paper [1] aims to present a survey of existing literature regarding the CTU-13 dataset, its source, purpose, and how following research added to it. First, the CTU-13 dataset is introduced with its source, purpose, and relevance to cybersecurity. Then, a survey of other relevant research is presented. Finally, insights are summarized based on existing materials.**

I. Introduction

This paper aims to present a survey of existing literature regarding the CTU-13 dataset its source purpose and how following research added to it. First section of this paper introduces the CTU-13 dataset with its source, purpose and relevance to cyber security. In the second section we give a survey of the other pieces of relevant research on the topic. In the third section we give a summary of what insights can be concluded from the existing material on this subject.

II. Dataset Introduction

The CTU-13 dataset first proposed with the research paper "An empirical comparison of botnet detection methods" is a dataset that provides network traffic from a botnet to aid in botnet detection research. Some important features of the dataset include the following:

- Includes real-world botnet traffic, normal traffic, and background traffic.
- Contains 13 scenarios representing various botnet behaviors (e.g., IRC, HTTP, and P2P-based communication, spam, DDoS, fast flux).
- Labels traffic as botnet, normal, or background, ensuring clear ground truth.
- Traffic was collected using virtualized Windows XP environments bridged to a university network, capturing genuine attack behaviors.

A. Dataset Features

The CTU-13 dataset includes many important features that distinguish it from other datasets and was produced with the following design goals:

- Must have real botnet attacks and not simulations.
- Must have unknown traffic from a large network.
- Must have ground-truth labels for training and evaluating the methods.
- Must include different types of botnets.
- Must have several bots infected at the same time to capture synchronization patterns.
- Must have NetFlow files to protect the privacy of the users.

Dataset captures real botnet attacks rather than simulations making it a more realistic botnet traffic example and includes synchronized botnet activities to represent real-world network behaviors accurately. Traffic is labeled as botnet, normal, or background, with clear ground truth to aid method evaluation. Each scenario represents specific botnet behaviors (e.g., IRC-based communication, HTTP-based attacks, spam, DDoS, port scanning, fast-flux techniques). Traffic data was converted from raw packet capture (pcap) format to NetFlow format for scalability and ease of analysis. Some scenarios include over 70 million packets and over 11 million NetFlows. Duration varies from a few minutes to several hours per scenario.

B. Relevance of Botnet Detection Methods for Cybersecurity

Botnet detection methods are critical for maintaining robust cybersecurity defenses. Botnets, networks of compromised devices controlled by attackers, enable various malicious activities, including:

1) **Distributed Denial of Service (DDoS) Attacks:** Overwhelming servers with traffic.
2) **Credential Stuffing and Brute Force Attacks:** Stealing user credentials or breaking into systems.
3) **Spam Campaigns and Phishing Attacks:** Propagating malware or stealing sensitive data.
4) **Data Theft:** Extracting confidential information from targeted systems.

Given their versatility and impact, detecting and mitigating botnets is essential for protecting individual, corporate, and national information security. Benefits to be had from improvements in botnet detection include:

- Preventing Large-Scale Attacks: Early detection of botnets can stop attackers from launching large-scale DDoS attacks or phishing campaigns, thereby protecting organizations from downtime and reputation damage.
- Mitigating Economic Costs: Botnets are often used for financial crimes, including ad fraud and extortion. Detecting them minimizes economic losses.
- Enhancing Network Integrity: Botnet detection ensures the integrity of network operations, preventing the misuse of organizational or personal devices.
- Protecting Critical Infrastructure: Advanced botnets target critical infrastructure, such as power grids or healthcare

systems. Detecting them safeguards public safety and essential services.

C. Botnet Detection Methods Tested

The research paper examined tests three different detection methods for comparison: CAMNEP, BClus, and BotHunter.

CAMNEP and **BClus** generalize well to new botnet behaviors, thanks to their adaptable and clustering-based approaches. **BotHunter** excels at recognizing known botnets but struggles with new or unconventional behaviors due to its reliance on predefined rules. CAMNEP balances adaptability and low false positives, while BClus captures temporal and behavioral patterns effectively. The study highlights the complementary strengths of these methods, emphasizing the importance of dataset quality and evaluation methodology for fair comparisons.

1) CAMNEP: CAMNEP is a behavior-based anomaly detection system that models network and user behaviors to detect deviations as anomalies. Uses multiple detection algorithms, including entropy-based measures, Principal Component Analysis (PCA), and fuzzy classifiers. It uses a three layer Architecture to detect anomalies :

- Anomaly Detectors: Detect anomalies using various traffic features and algorithms.
- Trust Models: Group traffic into behavioral clusters and assess anomalies over time to reduce false positives.
- Aggregators: Combine outputs from trust models into a composite anomaly score.

Its strengths include its ability to be highly adaptable to different network environments and is effective at detecting previously unseen botnet behaviors.

2) BClus: BClus BClus is a clustering-based method that aggregates NetFlows by source IP address to identify behavioral patterns indicative of botnet activity. Aggregates features like source ports, destination IPs, packet counts, and bytes transferred for each source IP. Identifies clusters that exhibit bot-like behavior (e.g., synchronized actions, repeated connections to a Command and Control (C&C) server). It is effective at detecting botnets with synchronized behaviors and its unsupervised clustering allows adaptation to different traffic environments.

3) BotHunter: BotHunter is a rule-based system that detects botnets by tracking the infection and coordination stages of malware. Monitors specific stages of botnet activity: scanning, exploitation, malware download, C&C communication, and attack propagation. Correlates warnings across multiple detection stages to assign an infection score to hosts. It relies on rules based on known malware infection sequences. It is effective against well-known botnet behaviors has high precision in detecting infections when its predefined rules apply but struggles against novel or unconventional behaviors.

III. Other Research in the Relevant Area

CTU-13 dataset is often used by other researchers in detecting cyber threats.

A. Adversarial Machine Learning for NIDS

The research paper titled "Adversarial Machine Learning for Network Intrusion Detection Systems: A Comprehensive Survey" [2]discusses how adversarial machine learning impacts the effectiveness of Network Intrusion Detection Systems (NIDS), which are critical in detecting and mitigating network-based cyber-attacks. Its findings include the following :

Vulnerability of Deep Learning (DL)-Based NIDS:

-
- While DL models enhance NIDS by accurately detecting malicious traffic, they are vulnerable to adversarial attacks, which use imperceptible perturbations to evade detection. Challenges in Applying Adversarial Learning from Computer Vision (CV) to NIDS:
- Adversarial attack methods designed for CV are not directly applicable to NIDS due to differences in data structures, feature spaces, and attack vectors. For instance, network traffic features are structured and constrained, unlike pixel values in images.

Evaluation of Defence Mechanisms:

- The paper reviews various defences like adversarial training, input reconstruction, and feature reduction, but notes that many are either computationally expensive or impractical for real-world application in NIDS.

B. Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research

The paper [3] provides a detailed examination of Explainable Artificial Intelligence (XAI) techniques applied to cybersecurity, addressing gaps in current research, presenting applications, challenges, and proposing future directions.

The increase in internet usage has amplified cybersecurity risks, such as malware, spam, and phishing attacks. AI methods (especially ML and DL) are widely used in cybersecurity for their effectiveness over traditional rule-based techniques. AI systems, though effective, often operate as "black boxes," making their decision-making processes opaque. This lack of explainability undermines user trust, regulatory compliance, and adoption in critical sectors like healthcare and financial services. The paper bridges the research gap by providing a comprehensive review of XAI methods applied to cybersecurity, a domain that has been inadequately addressed compared to XAI applications in fields like healthcare or finance.

It shows various advantages for XAI in cybersecurity AI models (e.g., neural networks) improve malware detection, but XAI tools like Grad-CAM, SHAP, and LIME add interpretability, ensuring decisions are understandable and justifiable. XAI enhances botnet identification models by explaining decisions through visual tools (e.g., scatterplots for retweet patterns) or dimensionality reduction techniques like PCA. XAI explains the decisions of intrusion detection models, helping analysts understand potential vulnerabilities in network traffic.

IV. Conclusion

Botnet detection methods are indispensable for cybersecurity as they enable proactive defense against evolving threats. They help mitigate risks, protect sensitive data, and ensure the reliability of digital infrastructure. Continuous advancements in AI and threat intelligence are making botnet detection more effective, enabling organizations to stay ahead of sophisticated cybercriminals. As cyber threats get more sophisticated it is crucial that improvement in malicious traffic detection methods stay capable. Some steps that can be taken to improve such system include developing resistant and robust AI models. Standardize evaluation metrics for explainability. Address ethical and legal concerns to ensure fair and compliant AI applications. Explore interdisciplinary approaches for improved adoption across industries. Developing methods to generate examples that adhere to real-world network constraints. Combining multiple defence strategies to improve robustness without excessive computational costs. Creating standardized datasets and metrics to evaluate adversarial attacks and defences in realistic NIDS environments. Bridging the gap between theoretical adversarial methods and practical implementations that can be deployed in live networks.

References

[1] Sebastian Garcia, Martin Grill, Jan Stiborek, and Alejandro Zunino. An empirical comparison of botnet detection methods. *computers & security*, 45:100–123, 2014.

[2] Ke He, Dan Dongseong Kim, and Muhammad Rizwan Asghar. Adversarial machine learning for network intrusion detection systems: A comprehensive survey. *IEEE Communications Surveys Tutorials*, 25(1):538–566, 2023.

[3] Zhibo Zhang, Hussam Al Hamadi, Ernesto Damiani, Chan Yeob Yeun, and Fatma Taher. Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access*, 10:93104–93139, 2022.