Botnet Detection Through Periodic Patterns in Command-and-Control Network Traffic

Dominik Oškera[1], Josef Koumar[1,2,*], Alžběta Pokorná[4], Kamil Jeřábek[2,3], and Tomáš Čejka[2]

[1]Czech Technical University in Prague, Prague, Czech Republic
[2]CESNET, a.l.e., Prague, Czech Republic
[3]Brno University of Technology, Brno, Czech Republic
[4]Czech University of Life Sciences, Prague, Czech Republic
[*]Corresponding author email: josef.koumar@fit.cvut.cz

***Abstract*—Detecting botnet Command-and-Control (C&C) communication in encrypted network traffic is a persistent challenge in cybersecurity, particularly in environments without endpoint visibility. We present a novel approach for botnet detection based on the inherent periodic communication patterns of C&C channels. Leveraging the Lomb-Scargle periodogram, we identify periodic behaviour in multiflow time series and extract periodic-based features for classification using machine learning. To address limitations in existing datasets, we introduce CESNET-CC25, a comprehensive and publicly available dataset comprising real-world botnet C&C traffic and benign traffic collected from an ISP backbone and controlled laboratory settings. Our method achieves high precision across both the widely used CTU-13 dataset and CESNET-CC25, with significant improvements in recall on long-duration captures. The results demonstrate that periodicity is a reliable indicator of C&C behaviour, even in modern, encrypted network environments, and that CESNET-CC25 provides a realistic benchmark for future botnet detection research.**

***Index Terms*—botnet, Lomb-Scargle periodogram, network traffic analysis, periodic network traffic, multiflow classification, network traffic classification**

I. Introduction and Background

Command and Control (C&C) is the communication channel usually established for malicious activities through backdoors or remote shells. The C&C allows attackers to maintain persistent access to compromised systems, issue commands, and exfiltrate data. Detection of C&C communication in network traffic has become essential for maintaining the security of enterprises [1]. Most of the recent threats, including Advanced Persistent Threat (APT) [2], use some form of C&C. APT groups consistently employ C&C techniques to maintain persistent access to compromised systems, exfiltrate data, and coordinate further malicious activities [3]. Analysis of documented APT groups in the MITRE ATT&CK framework[1] reveals that virtually all such groups rely on at least one C&C mechanism, ranging from standard protocols (e.g., HTTP, HTTPS, DNS) to more covert channels such as custom encrypted tunnels or legitimate services like cloud storage and social media platforms [4].

Detecting botnet activity on individual devices using antivirus or Endpoint Detection and Response (EDR) systems is not feasible in environments where direct access to endpoint devices is not possible. This challenge is prevalent among ISPs, organizations managing large-scale networks, and operators of public WiFi infrastructures. Nevertheless, botnet detection in network traffic is challenging due to the high adoption of encryption to increase the privacy of users on the Internet [5].

Relying solely on blacklists of known C&C server IP addresses is inadequate, as botnets frequently alter their infrastructure within days [6]. Therefore, the adoption of Machine Learning (ML) is a viable option in both packet-based and flow-based detection [7]. In the packet-based detection, multiple approaches were evaluated, for example, a small set of packet-level features with an explainable gradient-boosted tree model [8], and a semi-supervised One-Class SVM trained on packet-header features [9], and aggregated packet time series per 1s interval with a k-NN model [10]. In the flow-based detection, multiple features and models were adopted, for example, time-series statistics and XGBoost model [11], graph-based features with self-organizing map model [12], transfer learning approach by clustering of tabular features [13], multimodal features with random forest model [14], and sequence of packet lengths with deep learning models [15].

However, more resilient botnets, particularly those leveraging advanced architectures [16], further complicate detection efforts. Despite sophisticated evasion techniques, such as encryption, protocol obfuscation, and random padding, the periodic nature of botnet communication remains a detectable trait [17]–[19].

Our approach focuses on identifying periodic communication patterns, a fundamental characteristic of botnet activity. Specifically, we enhance existing periodic behaviour detection

This work was supported by the Student Summer Research Program 2024 of FIT CTU in Prague. This research was partially funded by the Ministry of Interior of the Czech Republic in project "Flow-Based Encrypted Traffic Analysis" (VJ02010024), by the Ministry of Education, Youth and Sports of the Czech Republic in project "e-Infrastructure CZ" (LM2023054), and also by the Grant Agency of the CTU in Prague, grant No. SGS23/207/OHK3/3T/18 funded by the MEYS of the Czech Republic. Computational resources were provided by the e-INFRA CZ project (ID:90254), supported by the Ministry of Education, Youth and Sports of the Czech Republic.

[1]https://attack.mitre.org/

978-3-903176-75-1 ©2025 IFIP

techniques using the Lomb-Scargle periodogram [20], [21]. This method allows us to effectively identify periodic network behaviours associated with botnet C&C communication. Furthermore, we construct a novel dataset by capturing real-world traffic from multiple botnet families in a controlled environment. Our approach is evaluated on the well-known dataset CTU-13 [22] and our newly created dataset CESNET-CC25, demonstrating its efficiency in real-world scenarios.

The key contributions of this paper are as follows:

- We create and publish a novel dataset of real-world botnet communication, enabling further research in the field of multiflow detection approaches.
- We evaluate our approach on both existing and newly created datasets, demonstrating its effectiveness in detecting periodic C&C communication patterns.
- We provide a detailed analysis of botnet behaviours in encrypted network traffic and propose potential improvements for threat detection systems.

This paper is organized as follows: Section II describes details about the datasets used for evaluation, mainly focused on the novel CESNET-CC25 dataset. Section III describes our methodology, including periodic behaviour detection and machine learning-based classification. Section IV presents experimental results and analysis. Finally, Section V provides conclusions and outlines potential future research directions.

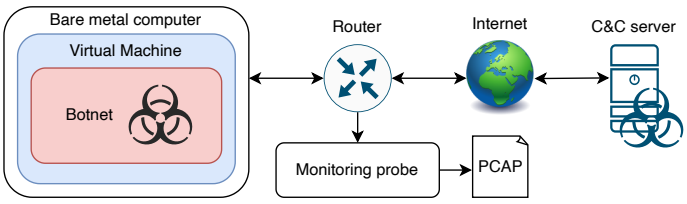
II. Datasets

Using two datasets, we evaluated the detection approach based on the periodic nature of botnet communications. The first is the widely recognized CTU-13 dataset [22], which has become a standard benchmark in botnet detection research due to its extensive collection of real-world network traffic with labelled botnet activities. Despite its widespread use, CTU-13 is over a decade old, and its relevance to current cybersecurity threats is limited. Over the years, botnet architectures, C&C techniques, and evasion strategies have evolved significantly [7], causing the dataset to be less representative of modern botnet behaviours. Additionally, most scenarios in CTU-13 have a short time length, which restricts their suitability for evaluating multi-flow detection methods to uncover persistent C&C communication.

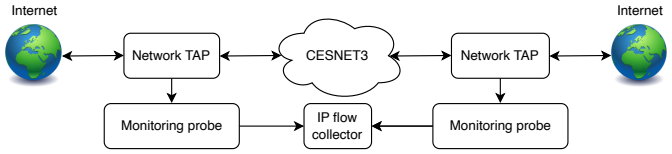
To overcome these limitations, we introduce a novel dataset—CESNET-CC25—explicitly designed to reflect contemporary botnet C&C traffic patterns. CESNET-CC25 offers a richer and more representative set of real-world threats, capturing modern behaviours such as decentralized (peer-to-peer) architectures and encrypted communication channels. This enables more accurate and robust evaluation of detection methods under realistic and current conditions. To promote reproducibility and encourage further research in this domain, CESNET-CC25 is publicly available via the Zenodo platform [23]–[25].

A. Capturing Process of CESNET-CC25 Dataset

Capturing and distinguishing botnet communications in real-world network environments poses a significant challenge,



(a) Capture architecture of botnet traffic in laboratory environment



(b) Capture architecture of benign traffic from ISP network CESNET3

Fig. 1: Capturing process of the CESNET-CC25 dataset

as C&C traffic typically constitutes only a negligible fraction of the total network flow. Nevertheless, capturing realistic benign traffic in a controlled laboratory setting is equally problematic, as such environments cannot faithfully replicate the diversity and scale of real-world communication patterns. To address these limitations, we designed and deployed two distinct traffic capture architectures, enabling the collection of authentic C&C traffic from active botnets and representative benign traffic from operational networks.

The first architecture is dedicated to capturing botnet C&C communication, as illustrated in Fig. 1a. In this setup, botnet binaries were executed within isolated virtual machines. Upon activation, most botnets immediately initiated communication with their respective C&C servers. This traffic was intercepted at the router level using port mirroring and recorded with tcpdump on a dedicated monitoring probe. Continuous traffic supervision ensured timely intervention, and all malicious activities were promptly identified and blocked. For instance, the Gafgyt botnet typically initiates attack traffic within seconds of execution.

The second architecture was designed to collect benign traffic from the CESNET3 network, as depicted in Fig. 1b. This infrastructure, deployed within a live ISP network, enabled us to obtain real-world benign communication patterns. Such an approach provides a more authentic representation of legitimate traffic than synthetically generated traffic in laboratory settings, which often fails to capture the complexity and variability of real network behaviour. Importantly, it also addresses the standard limitation of existing malware communication datasets, which often include benign traffic crafted under artificial conditions.

B. Content of CESNET-CC25 Dataset

The CESNET-CC25 dataset contains traffic from 32 distinct botnet binaries representing five different botnet families that were among the most prevalent at the time of writing. Each capture, along with associated traffic statistics, is summarized in Table I. The raw botnet communication traffic is provided

TABLE I: Botnet captures inside CESNET-CC25 dataset

No.	Family	Dur. [h]	C&C packets	C&C IP flows
1	Gafgyt	138.21	33 793	8 290
2	Mirai	24.71	92 346	22 263
3	Mirai	25.43	10 767	1 954
4	Mirai	25.23	6 256	1 532
5	Mirai	25.07	10 527	1 879
6	Kaiji	167.01	145 787	3 635
7	Mirai	20.43	121 308	17 464
8	Mirai	20.17	116 199	16 609
9	Miori	8.60	19 889	4 938
10	Hailbot	54.57	16 024	3 946
11	Gafgyt	3.12	3 462	975
12	Mirai	1.98	548	126
13	Hailbot	22.02	4 300	1 056
14	Hailbot	35.25	6 851	1 663
15	Mirai	47.32	50 138	583
16	Gafgyt	10.39	21 368	125
17	Hailbot	70.02	10 858	2 540
18	Mirai	111.44	28 078	6 970
19	Mirai	68.98	14 695	3 412
20	Gafgyt	15.41	3 738	928
21	Mirai	22.49	77 691	18 918
22	Gafgyt	42.94	10 640	2 610
23	Gafgyt	4.05	987	245
24	Mirai	150.22	36 415	9 040
25	Xorbot	43.39	156 215	2 646
26	Gafgyt	14.51	9 892	2 826
27	Hailbot	2.03	338	94
28	Gafgyt	42.49	53 901	11 089
29	Mirai	103.99	26 103	6 291
30	Gafgyt	1.23	298	75
31	Gafgyt	30.41	7 697	1 825
32	Mirai	27.34	15 634	4 196
	Total	**1 380.44**	**996 743**	**160 743**

in PCAP format and publicly available on Zenodo [23] for detailed analysis.

Furthermore, the CESNET-CC25 dataset is available in two formats—IP flows extracted by the `ipfixprobe`[2] exporter, available on Zenodo [24], and time series features distilled for the purpose of our periodicity detection approach[3], available on Zenodo [25], both in CSV format.

C. Analysis of CESNET-CC25 Dataset

The dataset consists of IP flows representing both benign and botnet communications, as previously described. These IP flows serve as the fundamental layer upon which time series features are subsequently extracted and the detection method is built. A detailed explanation of the feature extraction and detection methodology is provided in Section III.

To support reproducible evaluation, the dataset is already split chronologically into training and testing subsets, following an approximate 70:30 ratio of time. Detailed statistics on the number of flows in each split are presented in Table II.

[2]https://github.com/CESNET/ipfixprobe

[3]https://github.com/koumajos/EnhancedDeCrypto

TABLE II: Standardized train and test split of IP flows in dataset.

Traffic	Train IP Flows	Test IP Flows	Total
Benign	132 683 119	61 467 627	194 150 746
Botnet	97 120	63 623	160 743

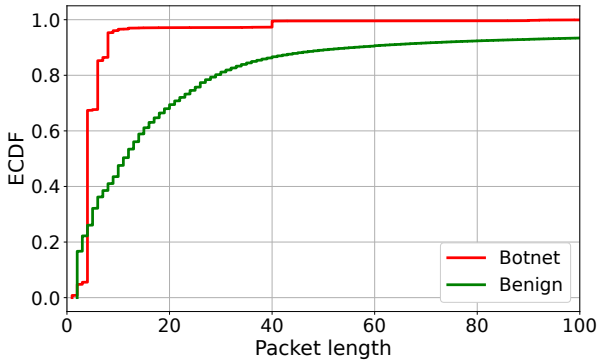


Fig. 2: Distribution of packet lengths of IP flows of benign and botnet communication.

The majority of botnet flows in the dataset are short, with 95% containing up to 10 packets. These short flows primarily represent repeated establishment of connections with C&C servers. In contrast, a noticeable spike in longer flows around 40 packets indicates connections where some data was exchanged, for example, an attack order. Overall, botnet traffic exhibits relatively uniform patterns across the dataset, whereas benign traffic is significantly more diverse in its characteristics, as illustrated in Fig. 2.

When examining individual IP flows and their characteristics, botnet and benign traffic can often appear indistinguishable due to low variability in their observable features. As demonstrated by Jeřábek et al. [26], packet sequence metadata—commonly used in traffic classification—tends to exhibit a high degree of duplication. This observation holds true in our dataset as well. The botnet portion, comprising 160,745 flows, contains only 2,458 unique packet length and direction sequences. In contrast, the benign traffic is substantially more diverse, with 54,987,920 unique sequences.

Furthermore, these sequences are from some part shared between botnet and benign classes, making direct classification based on a single IP flow unreliable. This overlap further motivates the need for alternative detection strategies, such as our approach based on multiflow time series and periodicity proposed in this paper.

D. Recommendation for Using CESNET-CC25 Dataset

When working with the CESNET-CC25 dataset, we recommend focusing on the extracted statistical features for method development, while omitting general identifiers such as IP addresses, port numbers, and protocol types. These identifiers are often short-lived and do not reflect consistent or generalizable communication behaviour across different contexts.

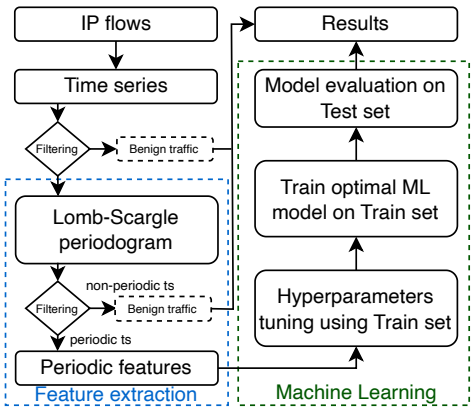


Fig. 3: Methodology of botnet detection using periodicity behaviour in multiflow time series

Additionally, the dataset was captured using flow exporters deployed at two distinct locations within the network infrastructure. This setup may introduce unintended bias, particularly when analysing inter-packet times. Due to differences in capture points, the timing characteristics of botnet and benign flows may vary, potentially leading to unwanted overfitting if inter-packet timing is used directly as a classification feature. Nevertheless, we have retained the inter-packet time information in the IP flow records to support detailed, flow-level analyses of botnet and benign behaviours when appropriate.

III. Our approach

Our approach focuses on detecting periodic communication patterns, a core behavioural trait of many botnets. We adopt the methodology proposed in our previous work [20], [21], which is illustrated in Fig. 3. After packet capture, traffic is aggregated into IP flows as described in earlier sections. For the CTU-13 dataset, we utilize the flow representations already prepared by the original authors.

The IP flows are chronologically divided into training and testing sets using a 70:30 split along the time axis. Subsequently, flows are segmented into fixed-length time windows of duration t—a key hyperparameter of the method. Within each time window, IP flows are transformed into multiflow time series, each corresponding to a specific network dependency. A network dependency is defined as a client-server relationship where the client accesses a particular service on the server (e.g., DNS queries to a DNS server).

To detect periodic behaviour in these time series, we employ the Lomb–Scargle periodogram along with Scargle's Significance Test, using a significance level of 0.1 and a periodicity threshold of 0.995. Only the time series deemed periodic by this test are retained for further processing.

Next, we perform feature engineering on the periodic time series to generate a feature vector comprising 44 statistical metrics. These features provide a rich characterization of the observed network behaviour and include basic statistical, temporal, spectral, and periodic features.

These features collectively enable robust characterization of network dependencies. The CESNET-CC25 dataset already includes these extracted features, which we use directly as input to a machine learning pipeline. The pipeline outputs a binary decision indicating whether the periodic time series represents botnet C&C communication or benign activity.

Crucially, we assume that C&C traffic exhibits periodic patterns. Therefore, any time series with an insufficient number of data points or lacking significant periodicity is pre-classified as benign before the feature extraction stage.

IV. Experimental evaluation

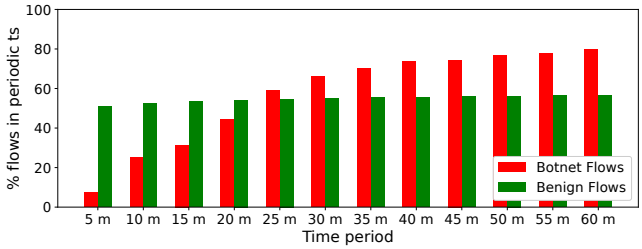
We construct multiple datasets of periodic features by varying the time window length $t \in [300, 3600]$ seconds. For each selected time period, we extract periodic time series and evaluate the performance of three machine learning algorithms commonly used for tabular data: k-Nearest Neighbors (k-NN), Random Forest, and XGBoost. All models are evaluated on both datasets (CTU-13 and CESNET-CC25) across all time periods. Among the tested algorithms, XGBoost consistently achieved the highest performance on the validation set; therefore, the results reported in this paper are based on XGBoost performance on the test set.

The choice of the time window t significantly affects the results. As t increases, the number of detected periodic time series, as well as the proportion of IP flows contained within them, increases—this trend is shown in Fig.4a and Fig.4b. This effect is especially evident in the long-term CESNET-CC25 dataset, where almost 100% of C&C flows are captured within periodic time series as the time window grows. In contrast, the CTU-13 dataset includes multiple short-duration scenarios with a limited number of C&C samples, leading to many C&C flows being missed in the periodic time series extraction.

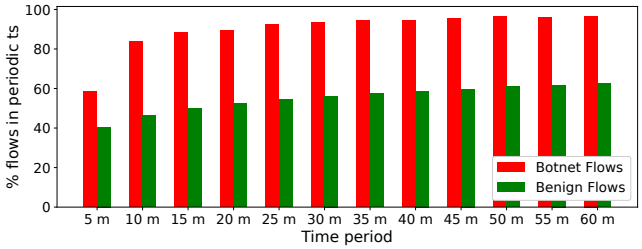
This discrepancy directly impacts the classification results presented in Fig.4c and Fig.4d. For both datasets, Accuracy and Precision exceed 99.9% across most time periods. However, Recall is significantly affected by the proportion of C&C flows in the periodic time series. On the CESNET-CC25 dataset, Recall consistently exceeds 90% for most time windows. Conversely, on CTU-13, Recall often remains below 60% due to the sparse representation of C&C communication in periodic time series.

The issue becomes more pronounced when the results are translated to the per-flow level. In this setup, we label all flows not part of a periodic time series as benign by default. This leads to a further drop in Recall on the CTU-13 dataset, as shown in Fig.4e and Fig.4f. Specifically, we observe an average 25% decrease in Recall for CTU-13, and even the best-performing configuration fails to reach 60% Recall. In contrast, CESNET-CC25 does not exhibit such a drop, confirming its robustness and suitability for periodicity-based detection.

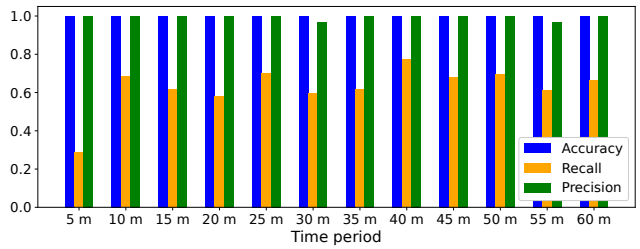
Our evaluation demonstrates that periodic C&C behaviour can be effectively detected in multiflow time series. Importantly, when the model classifies a time series as C&C based on its periodic nature, the confidence is extremely high. We



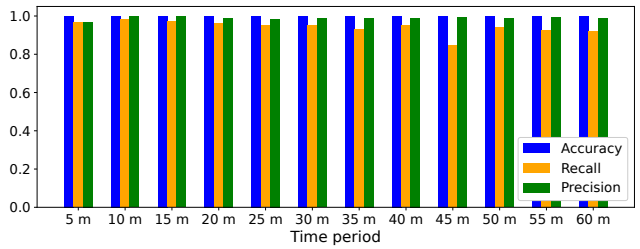
(a) Ratio of periodic IP flows in the CTU-13 dataset.



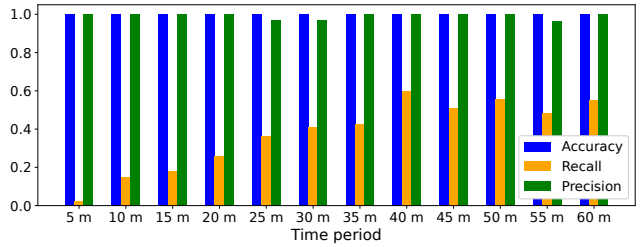
(b) Ratio of periodic IP flows in the CESNET-CC25 dataset.



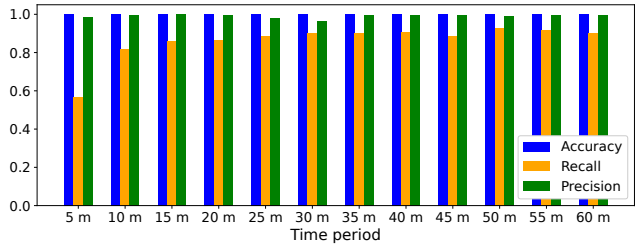
(c) Results of detection based on periodicity on the time series features for the CTU-13 dataset.



(d) Results of detection based on periodicity on the time series features for the CESNET-CC25 dataset.



(e) Results of detection based on periodicity transferred from the time series features to the IP flows for the CTU-13 dataset.



(f) Results of detection based on periodicity transferred from the time series features to the IP flows for the CESNET-CC25 dataset.

Fig. 4: Experimental evaluation of detecting C&C communication through periodic behaviours

consistently achieve 100% Precision across both datasets. This makes our approach highly reliable for confirming the presence of C&C activity, even if it may under-detect sparse or short-lived attacks. Moreover, our approach defeats the problem that identical flows are shared between botnet and benign classes, because on the multiflow level, this phenomenon does not occur.

Finally, we compare our results with existing work on the CTU-13 dataset in Table III. While our method achieves comparable Accuracy, the F1-score is slightly lower, which can be attributed to the limited recall caused by sparse C&C presence in periodic flows, as discussed earlier. Nevertheless, our approach uniquely offers 100% Precision on CTU-13, underscoring its value for high-confidence botnet detection.

V. Conclusions

In this paper, we proposed a novel approach for detecting botnet Command-and-Control (C&C) communication by leveraging the inherent periodicity of such traffic. By applying the Lomb-Scargle periodogram to multiflow time series, we were able to detect characteristics of botnet activity, even in encrypted traffic where deep inspection is not feasible. Our method demonstrated high precision and robustness, particularly when applied to long-duration traffic captures.

To overcome the limitations of existing datasets, we introduced CESNET-CC25. This new, publicly available dataset captures modern botnet C&C traffic in realistic conditions, including benign traffic from ISP networks and malicious traffic from active botnet samples. Our evaluation on both CTU-13 and CESNET-CC25 datasets showed that while CTU-13 suffers from short capture durations and low recall, CESNET-CC25 enables highly effective detection due to its extensive and realistic capture of botnet activity.

The results confirm that periodicity-based detection is a feasible and scalable method for identifying botnet communications. Furthermore, CESNET-CC25 lays the groundwork for future research on flow-based and encrypted traffic analysis.

References

[1] M. Lyu, H. H. Gharakheili, and V. Sivaraman, “A survey on enterprise network security: Asset behavioral monitoring and distributed attack detection,” *IEEE Access*, 2024.

[2] MITRE, “Groups,” https://attack.mitre.org/groups/, n.d., accessed: 2025-06-20.

TABLE III: Comparison of botnet detection methods on the CTU-13 dataset

Related work	Used Features	Model	Accuracy (%)	F1-score (%)
Koumar et al. [27]	NetTiSA flow	XGBoost	99.95	99.79
Stergiopoulos et al. [28]	Flow-based features	CART	99.85	99.90
Nugraha et al. [29]	Flow-based	CNN, LSTM	99.01	99.02
Jiang et al. [13]	Heuristic + learned features	Transfer learning	–	88.6
Chinta et al. [30]	Flow-based, behavior-based	Decision Tree	99.9	–
Gunawan et al. [31]	Flow-based features	k-NN	97.2	–
Shamshirband et al. [32]	Statistical, frequency-based features	HP-ELM	96.25	–
Our approach	Multiflow Periodicity	XGBoost	99.99*	74.81*

* The results were obtained for our multiflow approach. Thus, we transfer the results to the flow by using the flow count in the multiflow time series as a weight.

[3] Z. Ma, Q. Li, and X. Meng, "Discovering suspicious apt families through a large-scale domain graph in information-centric iot," *IEEE Access*, vol. 7, pp. 13 917–13 926, 2019.

[4] M. Li, Q. Li, G. Xuan, and D. Guo, "Identifying compromised hosts under apt using dns request sequences," *Journal of parallel and distributed computing*, vol. 152, pp. 67–78, 2021.

[5] C. Patsakis, F. Casino, and V. Katos, "Encrypted and covert dns queries for botnets: Challenges and countermeasures," *Computers & Security*, vol. 88, p. 101614, 2020.

[6] R. Tanabe, T. Tamai, A. Fujita, R. Isawa, K. Yoshioka, T. Matsumoto, C. Gañán, and M. Van Eeten, "Disposable botnets: examining the anatomy of iot botnet infrastructure," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1–10.

[7] S. N. Thanh Vu, M. Stege, P. I. El-Habr, J. Bang, and N. Dragoni, "A survey on botnets: Incentives, evolution, detection and current trends," *Future Internet*, vol. 13, no. 8, p. 198, 2021.

[8] M. M. Alani, "Botstop: Packet-based efficient and explainable iot botnet detection using machine learning," *Computer Communications*, vol. 193, pp. 53–62, 2022.

[9] A. A. Korba, A. Diaf, and Y. Ghamri-Doudane, "Ai-driven fast and early detection of iot botnet threats: A comprehensive network traffic analysis approach," in *2024 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2024, pp. 1779–1784.

[10] W. N. H. Ibrahim, S. Anuar, A. Selamat, O. Krejcar, R. G. Crespo, E. Herrera-Viedma, and H. Fujita, "Multilayer framework for botnet detection using machine learning algorithms," *IEEe Access*, vol. 9, pp. 48 753–48 768, 2021.

[11] J. Koumar, K. Hynek, and T. Čejka, "Network traffic classification based on single flow time series analysis," in *2023 19th International Conference on Network and Service Management (CNSM)*. IEEE, 2023, pp. 1–7.

[12] S. Chowdhury, M. Khanzadeh, R. Akula, F. Zhang, S. Zhang, H. Medal, M. Marufuzzaman, and L. Bian, "Botnet detection using graph-based feature clustering," *Journal of Big Data*, vol. 4, pp. 1–23, 2017.

[13] J. Jiang, Q. Yin, Z. Shi, M. Li, and B. Lv, "A new c&c channel detection framework using heuristic rule and transfer learning," in *2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC)*. IEEE, 2019, pp. 1–9.

[14] M. A. R. Putra, T. Ahmad, and D. P. Hostiadi, "Analysis of botnet attack communication pattern behavior on computer networks." *International Journal of Intelligent Engineering & Systems*, vol. 15, no. 4, 2022.

[15] C. Wei, G. Xie, and Z. Diao, "A lightweight deep learning framework for botnet detecting at the iot edge," *Computers & Security*, vol. 129, p. 103195, 2023.

[16] C. Nunnery, G. Sinclair, and B. B. Kang, "Tumbling down the rabbit hole: Exploring the idiosyncrasies of botmaster systems in a multi-tier botnet infrastructure." in *LEET*, 2010.

[17] Z. Zha, A. Wang, Y. Guo, D. Montgomery, and S. Chen, "Botsifter: an sdn-based online bot detection framework in data centers," in *2019 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2019, pp. 142–150.

[18] B. AsSadhan, J. M. Moura, and D. Lapsley, "Periodic behavior in botnet command and control channels traffic," in *GLOBECOM 2009-2009 IEEE Global Telecommunications Conference*. IEEE, 2009, pp. 1–6.

[19] G. Gu, J. Zhang, and W. Lee, "Botsniffer: Detecting botnet command and control channels in network traffic," in *15th Annual Network and Distributed System Security Symposium*, 2008.

[20] J. Koumar and T. Čejka, "Network traffic classification based on periodic behavior detection," in *2022 18th International Conference on Network and Service Management (CNSM)*. IEEE, 2022, pp. 359–363.

[21] J. Koumar, R. Plnỳ, and T. Čejka, "Enhancing decrypto: Finding cryptocurrency miners based on periodic behavior," in *2023 19th International Conference on Network and Service Management (CNSM)*. IEEE, 2023, pp. 1–7.

[22] S. Garcia, M. Grill, J. Stiborek, and A. Zunino, "An empirical comparison of botnet detection methods," *computers & security*, vol. 45, pp. 100–123, 2014.

[23] D. Oškera, J. Koumar, A. Pokorná, K. Jeřábek, and T. Čejka, "Cesnet-cc25: Long-term capture of c&c communication of botnets in the pcap format," Aug. 2025. [Online]. Available: https://doi.org/10.5281/zenodo.16752462

[24] ——, "Cesnet-cc25: Dataset for detection of c&c communication of botnets in the ip flow format," Aug. 2025. [Online]. Available: https://doi.org/10.5281/zenodo.16753890

[25] ——, "Cesnet-cc25: Dataset for detection of c&c communication of botnets in the periodic behavior features from multiflow time series format," Aug. 2025. [Online]. Available: https://doi.org/10.5281/zenodo.16753981

[26] K. Jerabek, J. Luxemburk, R. Plny, J. Koumar, J. Pesek, and K. Hynek, "When simple model just works: Is network traffic classification in crisis?" *arXiv preprint arXiv:2506.08655*, 2025.

[27] J. Koumar, K. Hynek, J. Pešek, and T. Čejka, "Nettisa: Extended ip flow with time-series features for universal bandwidth-constrained high-speed network traffic classification," *Computer Networks*, vol. 240, p. 110147, 2024.

[28] G. Stergiopoulos *et al.*, "Automatic Detection of Various Malicious Traffic Using Side Channel Features on TCP Packets," in *ESORICS 2018*, vol. 11098. Springer, 2018, pp. 346–362.

[29] B. Nugraha, A. Nambiar, and T. Bauschert, "Performance evaluation of botnet detection using deep learning techniques," in *2020 11th International Conference on Network of the Future (NoF)*. IEEE, 2020, pp. 141–149.

[30] S. R. Chinta, V. B. Polinati, and P. Srinivas, "Detecting bots inside a host using network behavior analysis," *International Journal of Computer Applications*, vol. 975, p. 8887, 2018.

[31] D. Gunawan, T. Hairani, and A. Hizriadi, "Botnet identification based on flow traffic by using k-nearest neighbor," in *2019 International Conference on Advanced Computer Science and information Systems (ICACSIS)*. IEEE, 2019, pp. 95–100.

[32] S. Shamshirband and A. T. Chronopoulos, "A new malware detection system using a high performance-elm method," in *Proceedings of the 23rd international database applications & engineering symposium*, 2019, pp. 1–10.