Poster: Advanced Features for Real-Time Website Fingerprinting Attacks on Tor

Donghoon Kim
Arkansas State University
Jonesboro, Arkansas, USA
dhkim@astate.edu

Andrew Booth
Arkansas State University
Jonesboro, Arkansas, USA
andrew.booth@smail.astate.edu

Euijin Choo
University of Alberta
Edmonton, AB, Canada
euijin@ualberta.ca

Doosung Hwang
Dankook University
Yongin-si, Gyeonggi-do, South Korea
dshwang@dankook.ac.kr

ABSTRACT

The Tor network has been identified as vulnerable to website fingerprinting (WF) attacks. Existing WF attacks have proven effective against the Tor network. However, prior research has mostly been limited to controlled experimental settings, leading to questions about the practicality of WF attacks in real-time environments. Recent advancements in feature engineering and machine learning aim to address this by exploring real-world scenarios, though they often overlook the preprocessing time required to design features from raw network traffic data. To tackle these issues, this research focuses on developing more efficient and high-performing feature vectors for WF attacks in real-time by analyzing previously successful feature vectors. The results indicate that advanced features, particularly those in a compact feature set, deliver competitive performance with reduced training times for real-time WF attacks. This study enhances our understanding of the feasibility of real-time WF attacks on Tor networks in practical settings and may inform future security improvements.

CCS CONCEPTS

• **Security and privacy → Network security**.

KEYWORDS

Tor network, onion service, real-time website fingerprinting attack

ACM Reference Format:
Donghoon Kim, Andrew Booth, Euijin Choo, and Doosung Hwang. 2024. Poster: Advanced Features for Real-Time Website Fingerprinting Attacks on Tor. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3658644.3691373

1 INTRODUCTION

Tor (The Onion Router) is a network and software tool that enables users to browse the Internet anonymously, protecting their privacy and security. Tor browser, built on Firefox, can access both general websites (non-hidden) and onion services (hidden) [7, 10]. General websites, such as "www.google.com," are accessible through standard web browsers like Chrome, Safari, and Mozilla Firefox. In contrast, onion services are only accessible via the Tor network using the Tor Browser. Instead of traditional DNS resolution, they use unique addresses with ".onion" extensions, resulting in URLs like "vnwf42cmztzqfojlrehvyd45bts.onion." [2, 3, 13, 15].

Previous research has demonstrated that website fingerprinting (WF) attacks leveraging machine learning can effectively extract information to identify onion services by analyzing extensive network traffic on the Tor network [7, 10, 16]. However, questions have been raised about the feasibility of such WF attacks in real-time environments due to the preprocessing time required to convert raw network traffic data into feature vectors [6]. To address these issues, this study aims to create a more efficient and high-performing feature vectors for WF attacks in real-time by combining two feature vectors that have previously demonstrated good performance: Panchenko *et al.*'s CUMUL [10], which uses packet quantity and number, and Kim *et al.*'s 125 features [6], which leverage various packet information. The contributions of this study are as follows:

- Our framework includes the collection of a comprehensive dataset of genuine onion services. This dataset forms the basis for our analysis, offering real-world examples essential for evaluating the effectiveness of our methods.
- We propose empirical methods to convert data into low-dimensional features by leveraging previously proven features for WF attacks. These features are carefully developed through empirical experimentation with onion service network traffic data.

2 RELATED WORK

This study employs two main sets of features to evaluate and enhance real-time WF attacks: CUMUL and 125 features. Panchenko *et al.* [10] designed the CUMUL feature. CUMUL has 104 features derived from the total number and size of packets. These features include 4 basic elements: the quantity of incoming and outgoing packets, and the total size of incoming and outgoing packets. Additionally, there are 100 additional features that are calculated as cumulative sums of packets using linear interpolation [10]. The 125 features consist of diverse information, including packet general information, cell sequence length, packet inter-arrival time, burst

CCS '24, October 14–18, 2024, Salt Lake City, UT, USA

ACM ISBN 979-8-4007-0636-3/24/10
https://doi.org/10.1145/3658644.3691373

Table 1: Extracted Features

Features	Contents in a Feature	Count
104 CUMUL [10]	The number of incoming packets	1
	The number of outgoing packets	1
	The sum of incoming packets	1
	The sum of outgoing packets	1
	Cumulative sum of packets based on linear interpolation	100
125 features [6]	Packet general information	44
	Cell sequence length	4
	Packet Inter arrival time	4
	Burst information	22
	Cell ordering	18
	Concentration	8
140 features	Burst information	9
	Concentration	9
	Packet ordering	18
	CUMUL	104

information, cell ordering, and concentration based on 103 features [6, 9]. Oh *et al.* [9] found that the 103 features outperformed CUMUL when analyzing data from websites that frequently update their content over time. Detailed descriptions for each feature are provided in Table 1.

Many researchers demonstrated that WF attacks on the Tor network are successful in identifying both general websites and onion services with high performance metrics and high volume of dataset [7], various features [10], under closed [8, 10, 14, 17, 18] and open [5, 11, 12] world models. As the performance of WF attacks has improved, researchers have expanded their studies from controlled environments to real-world environments [4]. Despite their success in executing WF attacks in real-world environments, no research is currently focused on studying the feasibility of real-time WF attacks.

3 METHODOLOGY

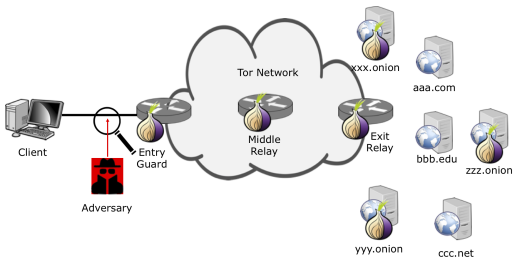


Figure 1: The Threat Model

Threat Model. An attacker can monitor traffic between the client and the first router (entry guard) in the Tor network [10], as well as between the last router and the destination client, without needing to decrypt the packets. The attackers may be the owner of a Tor router, an internet service provider, or a network administrator. In this study, we consider the scenario where an attacker is monitoring the traffic within the same broadcast domain as the client and the entry guard as the threat model illustrated in Figure 1. Because it highlights the significant risks and vulnerabilities associated with user identity exposure. By focusing on attackers such as the owner of a Tor router, an internet service provider, or a network administrator, we address a range of potential threats that are particularly relevant in today's digital landscape. This scenario emphasizes the importance of understanding how WF attacks can compromise user anonymity on Tor networks.

Approach. Our research approach involves a comprehensive analysis, focusing on the feasibility and effectiveness of real-time WF attacks. First, in order to find the optimal number of interpolation in CUMUL, we experimented with CUMUL features using various numbers of interpolations, specifically 6, 16, 26, and 36, instead of just 100. Second, we combine the optimal number of CUMUL features with 36 features selected from a pool of 125, based on feature importance determined by a random forest classifier. These 36 features are less related to the numbers and sizes of packets, which are the main components of CUMUL.

Data Collection. We utilize the network traffic collection system that we developed to collect data. We collected 25 onion services using `ahmia.fi` [1], each with 150 instances, with the primary objective of ensuring a broad and varied set of services with non-overlapping content, thus capturing the full spectrum of available services without redundancy.

4 EXPERIMENTS

Experiment 1 (EX1): CUMUL-ish. We conducted experiments with CUMUL by varying the number of interpolations, as shown in Table 2. In the table, RF stands for Random Forest, ACC stands for accuracy, PRE stands for precision, REC stands for recall, F1 stands for the F1-score, and Train stands for training time. Additionally, we use accuracy to visualize the data presented in Table 2. Although trends may be hard to discern through tables and graphs, it's evident that a larger number of interpolations does not necessarily result in better performance. For instance, with 30 (4+26) interpolations and MLP, the highest accuracy achieved is 73.73%. However, for training time, a larger number of features tends to result in longer training times.

Table 2: EX1: CUMUL's Variation

CUMUL-ish	Models	ACC	PRE	REC	F1	Train (s)
10 (4+6)	**RF**	68.13	68.41	68.63	68.21	201.30
	MLP	73.41	74.73	73.92	73.14	100.95
	CNN	71.46	72.24	63.11	65.34	39.04
20 (4+16)	**RF**	68.85	69.38	69.41	69.07	144.34
	MLP	72.37	73.03	72.68	72.20	90.49
	CNN	66.79	66.96	57.46	59.43	36.19
30 (4+26)	**RF**	68.19	68.46	68.73	68.23	254.90
	MLP	73.73	75.21	73.87	73.68	106.84
	CNN	71.13	72.82	63.72	65.81	44.36
40 (4+36)	**RF**	67.60	67.92	68.14	67.63	306.00
	MLP	70.93	71.54	71.43	70.39	119.96
	CNN	70.23	73.07	63.70	65.66	49.58

Experiment 2 (EX2): Advanced Features We created new features by combining CUMUL with the 125 features, resulting in two sets: 140 features and 66 features which compose of 36 features from the 125 features and 30 (4+26) selected from Table 2 as it achieved the highest accuracy. Figure 3 shows the confusion matrix on Random Forest using 25 websites. The experimental results indicate that 66 features outperform 140 features in terms of accuracy while requiring less training time.

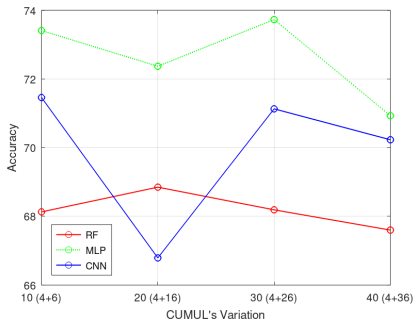
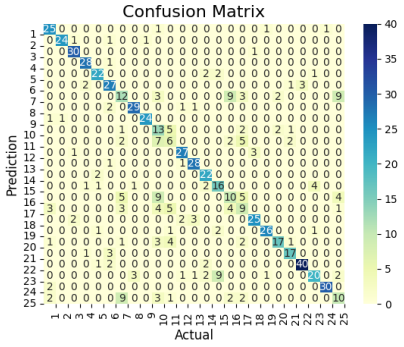


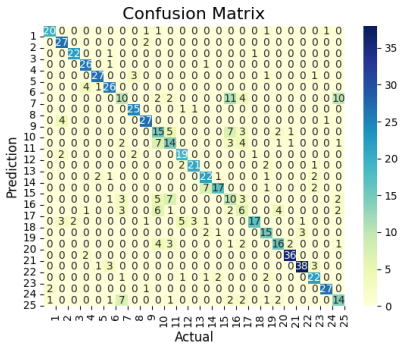
Figure 2: EX1: Visualizing CUMUL's Variation

Table 3: EX2: Advanced Feature Vectors

Features	Models	ACC	PRE	REC	F1	Train (s)
140 (104+36)	**RF**	70.88	70.68	71.03	70.41	10.69
	MLP	66.88	67.47	66.92	66.61	6.67
	CNN	64.84	66.22	63.70	64.33	235.33
66 (30+36)	**RF**	73.73	74.54	74.29	73.89	7.03
	MLP	70.23	71.61	71.18	70.76	8.40
	CNN	67.67	70.41	63.46	65.36	60.52



(a) 140 (104+36)



(b) 66 (30+36)

Figure 3: EX2: Confusion Matrix on Random Forest

5 CONCLUSION

This study investigated advanced features by leveraging previously proven features for website fingerprinting attacks. The conducted experiments reveal key insights into the performance of different feature sets and interpolation strategies. This underscores the effectiveness of the more compact feature set in optimizing both performance and efficiency. However, the study also faced some limitations, including a lack of diverse combinations and a large-scale dataset. These limitations indicate that, despite significant progress, there is still much work to be done to further explore WF attacks.

ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Award No. OIA-1946391.

REFERENCES

[1] (accessed June 21, 2024). *Tor Hidden Service Search.* https://ahmia.fi.
[2] Mashael AlSabah and Ian Goldberg. 2016. Performance and security improvements for tor: A survey. *ACM Computing Surveys (CSUR)* 49, 2 (2016), 1–36.
[3] Mohamad Amar Irsyad Mohd Aminuddin, Zarul Fitri Zaaba, Azman Samsudin, Nor Badrul Anuar Juma'at, and Sazali Sukardi. 2020. Analysis of the paradigm on tor attack studies. In *2020 8th International Conference on Information Technology and Multimedia (ICIMU).* IEEE, 126–131.
[4] Giovanni Cherubin, Rob Jansen, and Carmela Troncoso. 2022. Online website fingerprinting: Evaluating website fingerprinting attacks on tor in the real world. In *31st USENIX Security Symposium (USENIX Security 22).* 753–770.
[5] Marc Juarez, Sadia Afroz, Gunes Acar, Claudia Diaz, and Rachel Greenstadt. 2014. A critical evaluation of website fingerprinting attacks. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.* 263–274.
[6] Donghoon Kim, Loc Ho, Young-Ho Kim, Won-gyum Kim, and Doosung Hwang. 2021. Poster: A Pilot Study on Real-Time Fingerprinting for Tor Onion Services. In *The Network and Distributed System Security Symposium (NDSS).*
[7] Albert Kwon, Mashael AlSabah, David Lazar, Marc Dacier, and Srinivas Devadas. 2015. Circuit fingerprinting attacks: Passive deanonymization of tor hidden services. In *24th {USENIX} Security Symposium ({USENIX} Security 15).* 287–302.
[8] Arash Habibi Lashkari, Gerard Draper-Gil, Mohammad Saiful Islam Mamun, and Ali A Ghorbani. 2017. Characterization of Tor Traffic using Time based Features.. In *ICISSP.* 253–262.
[9] Hyungseok Oh, Donghoon Kim, Won-gyum Kim, and Doosung Hwang. 2020. Performance Analysis of Tor Website Fingerprinting over Time using Tree Ensemble Models. In *2020 International Conference on Computational Science and Computational Intelligence (CSCI 2020).*
[10] Andriy Panchenko, Fabian Lanze, Jan Pennekamp, Thomas Engel, Andreas Zinnen, Martin Henze, and Klaus Wehrle. 2016. Website Fingerprinting at Internet Scale.. In *NDSS.*
[11] Andriy Panchenko, Lukas Niessen, Andreas Zinnen, and Thomas Engel. 2011. Website fingerprinting in onion routing based anonymization networks. In *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society.* 103–114.
[12] Antonio Pescape, Antonio Montieri, Giuseppe Aceto, and Domenico Ciuonzo. 2018. Anonymity services tor, i2p, jondonym: Classifying in the dark (web). *IEEE Transactions on Dependable and Secure Computing* (2018).
[13] Florian Platzer, Marcel Schäfer, and Martin Steinebach. 2020. Critical traffic analysis on the tor network. In *Proceedings of the 15th International Conference on Availability, Reliability and Security.* 1–10.
[14] Vera Rimmer, Davy Preuveneers, Marc Juarez, Tom Van Goethem, and Wouter Joosen. 2017. Automated website fingerprinting through deep learning. *arXiv preprint arXiv:1708.06376* (2017).
[15] Yixin Sun, Anne Edmundson, Laurent Vanbever, Oscar Li, Jennifer Rexford, Mung Chiang, and Prateek Mittal. 2015. {RAPTOR}: Routing attacks on privacy in tor. In *24th {USENIX} Security Symposium ({USENIX} Security 15).* 271–286.
[16] Tao Wang. 2020. High Precision Open-World Website Fingerprinting. In *2020 IEEE Symposium on Security and Privacy (SP).* 152–167. https://doi.org/10.1109/SP40000.2020.00015
[17] Wang, Tao. 2016. Website Fingerprinting: Attacks and Defenses. http://hdl.handle.net/10012/10123
[18] Zhongliu Zhuo, Yang Zhang, Zhi-li Zhang, Xiaosong Zhang, and Jingzhong Zhang. 2018. Website Fingerprinting Attack on Anonymity Networks Based on Profile Hidden Markov Model. *Trans. Info. For. Sec.* 13, 5 (May 2018), 1081?1095. https://doi.org/10.1109/TIFS.2017.2762825