Fuzzy Systems and Soft Computing
ISSN : 1819-4362

ANALYZING THE EFFECTS OF ALTERED TOR TRAFFIC ON ONION SERVICE CLASSIFICATION

Pedamutti Rajesh Assistant Professor, Dept of CSE Seshadri Rao Gudlavalleru Engineering College,Gudlavalleru, Andhra Pradesh, India rajpedamutti@gmail.com
Arimanda Mahith Sai Reddy, Chilumuru Yamini Naga Sai Prasanna, Balagam Smily, Balivada Bharath UG Student, Dept of CSE Seshadri Rao Gudlavalleru s Engineering College, Gudlavalleru, Andhra Pradesh, India bharathbalivada4@gmail.com

Abstract: The project's main goal is to determine how changes made to Tor traffic affect the way Onion Service traffic is classified by examining network traffic in darknet settings like the Tor network. It notes that although privacy and anonymity are key features of Tor and Onion Services, they may also be abused, underscoring the need for more awareness and oversight. Three main objectives of the study are to detect Onion Service traffic within Tor traffic, evaluate the impact of traffic alterations, and identify key criteria that are important throughout the categorization process. To accomplish its goals, the initiative probably makes use of machine learning and data analysis tools, with an emphasis on examining network traffic patterns inside the Tor network. The project's conclusions underscore the fine line that must be drawn between protecting user privacy and guaranteeing network security, and they may have an impact on privacy, security, and network monitoring.

1. INTRODUCTION

By rerouting user traffic via intermediary nodes, Tor [1] is able to mask their identities. Using the top-level domain ".onion," Tor offers anonymous onion services, which are also called hidden services. Since Tor may evade censorship, security professionals, network defenders, and law enforcement agencies are working hard to distinguish Tor traffic from encrypted and unencrypted communications [2], [3]. When it comes to Tor traffic, for example, some studies have attempted to classify it according to application type [2, 5, 6], while others have sought to distinguish it from Webmix and I2P traffic [3, 4, 6]. The goal of this study is to distinguish between onion service and Tor traffic using traffic analysis. There are three overarching topics to our study.

Onion services are now botnet command and control servers [7], [8], in addition to hosting unlawful studies like [3] and [6] may become less applicable if the modifications impact the Onion Service's classifiably. We gave time-statistics features top priority. We also make advantage of features that have been applied to identify trends in network traffic [13]. using three different feature selection processes and a battery of feature combinations, we train our classifier to determine which properties are most strongly correlated with the study's traffic type.

2. LITERATURE SURVEY

a) Tor: The Second-Generation Onion Router
https://www.researchgate.net/publication/2910678_Tor_The_Second-Generation_Onion_Router
A low-latency anonymous communication service, Tor is built on circuits. Complete forward secrecy, directory servers, congestion control, integrity testing, adjustable exit rules, and a feasible rendezvous point for location-hidden services are all features of this newest version of Onion Routing. No special permissions or kernel modifications are needed for Tor to operate on the real Internet; no node synchronisation or coordination is required; and anonymity, usability, and efficiency are all balanced. Our international network of about 30 nodes is quickly described. And lastly, we touch on the topic of anonymous communication.

b) Enhancing Tor's performance using real-time traffic classification
https://dl.acm.org/doi/10.1145/2382196.2382208
A low-latency anonymity network that protects users' privacy online is Tor. Every day, hundreds of thousands of clients are served via a worldwide network of routers that are controlled by volunteers.

https://doi.org/10.36893/FSSC.2025.V20.005

Congestion and a poor relay-to-client ratio are causing Tor to run poorly, which might reduce user privacy and prevent its wider adoption.

To make Tor work better, we classify traffic. While the majority of Tor traffic is really interactive web surfing, we are well aware that large-scale downloading consumes an excessive amount of Tor's limited capacity. Because of their unique duration and data transfer limitations, some types of traffic are not eligible for Tor's Quality of Service.

DiffTor is a machine learning approach that dynamically provides distinct service categories to various applications by classifying Tor's encrypted circuits by application. In our tests, we were able to achieve an accuracy level of over 95% when it came to identifying actual Tor network connections. Our straightforward real-time classification and quality of service improve Tor client responsiveness for interactive users by 75% and median download times by 86%.

c) Characterization of Tor Traffic using Time based Features

https://www.semanticscholar.org/paper/Characterization-of-Tor-Traffic-using-Time-based-Lashkari-Draper-Gil/d76f32eb3af1a163c0fde624e9fc229671ca75b6

Although traffic categorisation has been the subject of several research, the ever-increasing sophistication of Internet services and the prevalence of encryption provide a challenge. Recent years have seen an uptick in privacy-enhancing software that uses encryption to keep users' online activities secret. A popular choice, Tor, separates the sender and recipient by encrypting and routing their communication via a distributed network of computers. Here you can see the historical Tor traffic patterns that have occurred between the client and entry node. Applications such as browsing, chatting, streaming, email, voice over IP, peer-to-peer, and file transfer are classified, and Tor traffic detection is detailed. In this work, we additionally evaluate our classifiers using our Tor-labeled dataset.

d) Tor Traffic Classification from Raw Packet Header using Convolutional Neural Network

https://ieeexplore.ieee.org/document/8569113

In order to allocate resources and operate the network effectively, traffic categorisation and analysis are becoming increasingly important due to the exponential growth of network traffic. New security measures, such as the widely used encryption technique Tor, make this endeavour more challenging. According to this research, a convolutional neural network with a hexadecimal raw packet header may be used to categorise Tor data. Our approach is far more precise than competing machine learning approaches. The technique is publicly validated by utilising UNB-CIC Tor network traffic statistics. Our fractionated Tor/non-Tor traffic classification approach achieved a remarkable 99.3% accuracy rate in the testing.

e) Inferring Application Type Information from Tor Encrypted Traffic

https://ieeexplore.ieee.org/document/7176097

Users' internet privacy is protected by the popular anonymous communication method, Tor. To conceal user data, such as the operating application type (Web, P2P, FTP, Others), TCP programs are encrypted and compressed into equal-sized cells. Certain types of applications can compromise anonymity and open the door to additional attacks. Some application behaviours cannot be concealed by Tor, unfortunately. The ability of P2P programs to upload and download at the same time is preserved via Tor traffic. Our study on a novel Tor attack, the traffic categorisation attack, was prompted by this discovery; it can detect the types of applications in Tor traffic. To mimic various apps, an attacker employs a successful machine learning strategy and meticulously selects flow characteristics, such as burst volumes and directions, to mirror application behaviours. Target Tor traffic may be classified and its application type determined by these models. We validated the viability and effectiveness of the traffic categorisation attack by testing it against Tor.

3. METHODOLOGY

i) Proposed Work:

An addition to the conventional system is presented in the form of ADABOOST. By successfully categorizing network traffic into Tor and Onion services with high accuracy, ADABOOST improves the overall performance of the system. When compared to the traditional system's standard machine learning techniques, it performs better. Furthermore, ADABOOST greatly increases classification accuracy, showing that it performs better in terms of accuracy and dependability than the conventional

https://doi.org/10.36893/FSSC.2025.V20.005

methods. The extensions project integrates the Adaboost classifier and improves Tor traffic categorization with a noteworthy 99% accuracy [14, 15], with a particular focus on onion services. With this update, traffic categorization within the Tor network is now much more accurate. A user-friendly Flask framework with SQLite connectivity is created to improve usability in practice by expediting the sign-up and sign-in processes for user testing. This guarantees a smooth and safe experience, preserving user privacy and network security while making the framework usable for realistic Darknet Traffic Analysis.

ii) System Architecture:

According to the project's system design, the procedure is started by a Tor user. In order for the Tor network to receive data from the Tor client, Entry Nodes A and D are used. Through the use of a B-Exit Node, data may leave Tor and reach the outside world. In order to provide secure communication between clients and onion services, a C-Rendezvous Point is necessary [1, 18]. Web services and Tor's Onion are integrated into the system. To categorise and comprehend the impact of Tor traffic on onion service traffic, one needs KNN [3], Random Forest, SVM, and the Adaboost extension. The project's goals will benefit greatly from this extensive architecture, which guarantees an exhaustive examination into the dynamics of darknet traffic, particularly with regard to the classification of Onion services.

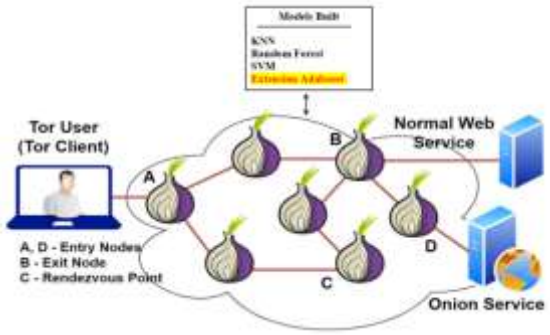

Fig 1 Proposed architecture

iii) Data Processing:

Organisations may gain valuable insights from raw data through data processing. Data scientists collect data, sort it, clean it, verify it, analyse it, and then display the results in written or visual forms. Machines, computers, or humans can process data. Enhancing the value of information and making decision-making easier are the goals. As a result, companies are able to enhance their operations and make critical choices on time. This is mostly due to automated data processing technologies, such computer software development. It may assist in transforming vast volumes of data, especially big data, into insightful understandings for decision-making and quality control.

iv) Feature selection:

Feature selection chooses the most steady, non-repetitive, and pertinent elements for model turn of events. As data sets extend in amount and assortment, purposefully bringing down their size is significant. The fundamental reason for feature selection is to increment prescient model execution and limit processing cost.

One of the vital pieces of feature engineering is picking the main attributes for machine learning algorithms. To diminish input factors, feature selection methodologies take out copy or superfluous elements and limit the assortment to those generally critical to the ML model. Rather than permitting the ML model pick the main qualities, feature selection ahead of time enjoys a few benefits.

v) Algorithms:

K-Nearest Neighbors (KNN) is a simple classification method that classifies data points according to how similar they are to other data points in the area. The "closeness" between samples is calculated using attributes from network traffic, and samples are then assigned to the most frequent class among their KNN. KNN is simple to use and effective in handling intricate data connections; nevertheless, choosing the right number for 'k' and handling high-dimensional data present obstacles [13].

Random Forest is a technique for ensemble learning that combines several decision trees to provide predictions. Every tree is trained via replacement (bagging) on random subsets of data, and the collective votes of all the trees determine the final forecast. Due to its ability to integrate many trees

https://doi.org/10.36893/FSSC.2025.V20.005

for increased accuracy, it is appropriate for categorizing network data. It is resilient, manages high-dimensional data, lessens overfitting, and provides insights into the significance of features.

Support Vector Machines (SVM) [3] is a supervised learning technique that performs well in situations with clear class borders by finding the best hyperplane in high-dimensional space to divide various data classes. It may be used to categorize network traffic, especially in situations with binary or multiple classes. SVM can handle high-dimensional data and clearly define a margin, but it may have trouble with data that is not linearly separable and necessitates careful kernel function selection.

4. Experimental Results

Precision: Precision estimates the level of positive cases or tests precisely sorted. Precision is determined utilizing the recipe:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

Fig 2 Precision comparison graph

Recall: ML recall assesses a model's ability to perceive all significant examples of a class. It shows a model's culmination in catching occasions of a class by contrasting accurately anticipated positive perceptions with complete positives.

$$Recall = \frac{TP}{TP + FN}$$

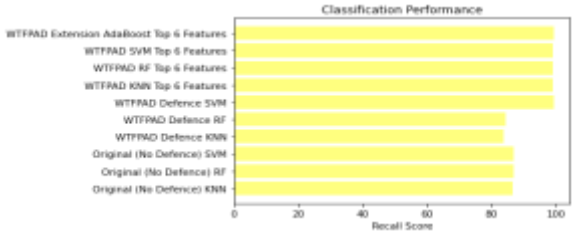

Fig 3 Recall comparison graph

Accuracy: The ability of tests to differentiate between healthy and unhealthy patients is a measure of their accuracy. To determine the accuracy of the test, determine the small percentage of true positives and true negatives in completely broken scenarios. In terms of numbers:

Accuracy = TP + TN TP + TN + FP + FN.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

https://doi.org/10.36893/FSSC.2025.V20.005

Fig 4 Accuracy graph

F1 Score: Machine learning model accuracy is estimated by F1 score. Consolidating model precision and recall scores. The accuracy measurement estimates how frequently a model anticipated accurately all through the dataset.

$$\text{F1 Score} = 2 * \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} * 100$$

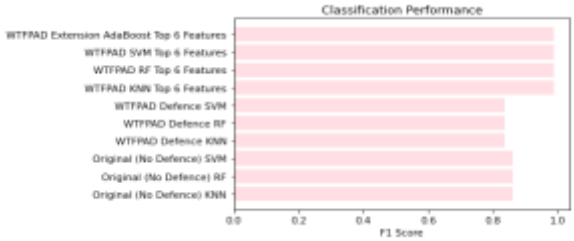

Fig 5 F1Score

ML Model	Accuracy	f1_score	Recall	Precision
Original (No Defence) KNN	0.868	0.860	0.868	0.919
Original (No Defence) RF	0.868	0.860	0.868	0.919
Original (No Defence) SVM	0.868	0.860	0.868	0.919
WTFPAD Defence KNN	0.838	0.838	0.838	0.845
WTFPAD Defence RF	0.838	0.838	0.838	0.845
WTFPAD Defence SVM	0.838	0.838	0.838	0.845
WTFPAD KNN Top 6 Features	0.990	0.990	0.990	0.990
WTFPAD RF Top 6 Features	0.990	0.990	0.990	0.990
WTFPAD SVM Top 6 Features	0.990	0.990	0.990	0.990
Extension WTFPAD Extension AdaBoost Top 6 Features	0.990	0.990	0.990	0.990

Fig 6 Performance Evaluation

Fig 6 User input

https://doi.org/10.36893/FSSC.2025.V20.005

Fig 7 Predict result for given input

5. CONCLUSION

The research effectively examines how changed Tor traffic affects Onion Service traffic classification. Through thorough study, it shows that Tor traffic changes affect categorization accuracy. This finding helps expand darknet traffic dynamics knowledge by explaining Onion Service traffic categorization robustness under different settings ([3], [6]). The project determines and assesses the most important categorization feature combinations. The study identifies important combinations that greatly affect Onion Service traffic categorization accuracy. This knowledge improves models and helps grasp the dataset's complex interactions. Different characteristics and their effects on classifiers are examined in detail. This detailed investigation shows how different characteristics affect classifier performance. Understanding feature performance dynamics improves classification model interpretability and reliability. The project improves Onion Service traffic categorization accuracy by using ensemble techniques, notably Adaboost. Adaboost improves classification system resilience and accuracy by integrating model predictions. This project helps give a robust and accurate darknet traffic analysis solution. The project uses Flask with secure authentication to improve system testing user experience. This interface simplifies user input and secures performance assessment data. User-friendliness and security follow system design best practices, making the project suitable for testing and real-world usage.

6. FUTURE SCOPE

When intentionally modifying Tor traffic with WTFPAD [10] or TrafficSliver, it is necessary to analyse classifier performance in order to analyse the impact of these modifications. Such alterations can impair Tor traffic detection, affecting network monitoring and security. The study may examine how factors impact Onion Service traffic classification performance. This study shows how characteristics affect categorization. To understand the effects of simply recognizing Tor and Onion Service traffic, more study is needed [3], [6]. This understanding should include traffic monitoring and government and sensitive institution limitations, including social and security concerns. The project may use sophisticated methods to identify Onion Service traffic even with obfuscation. This research may lead to new Tor network categorization accuracy approaches.

REFERENCES

[1] In the proceedings of the thirteenth USENIX Security Symposium (SSYM), held in August 2004 in San Diego, California, USA, R. Dingledine, N.Mathewson, and P. Syverson presented "Tor: The secondgeneration onion router" (pp. 303–320).

[2] "Enhancing Tor's performance using real-time traffic classification," in Proc. ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, Oct. 2012, pp. 73-84, created by M. Al Sabah, K. Bauer, and I. Goldberg.

[3] "Characterisation of Tor traffic using time based features," in Proceedings of the 3rd International Conference on Information Security and Privacy (ICISSP), Porto, Portugal, February 2017, pages 253-262, by A. H. Lashkari, G. D. Gil, M. S. I. Mamun, and A. A. Ghorbani.

https://doi.org/10.36893/FSSC.2025.V20.005

[4] "Tor traffic classification from raw packet header using convolutional neural network" (M. Kim and A. Anpalagan, 2018), Proceedings of the 1st IEEE International Conference on Knowledge and Innovation (ICKII), Jeju Island, South Korea, July 2018, pp. 187-190.
[5] "Inferring application type information from Tor encrypted traffic," published in the proceedings of the 2nd International Conference on Advanced Cloud Data (CBD) in November 2014 in Washington, DC, USA, pages 220-227, was written by G. He, M. Yang, J. Luo, and X. Gu.

https://doi.org/10.36893/FSSC.2025.V20.005