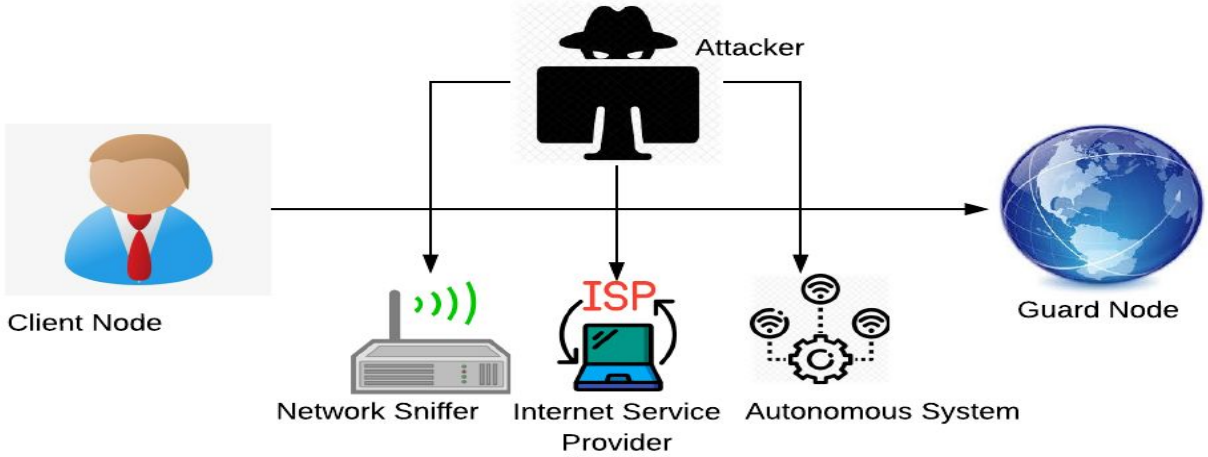
Temporal Analysis of Privacy Enhancing Technology Traffic Using Deep Learning

@SocialSec 2023 University of Kent

Monika Kumari - Goldman Sachs, Bengaluru, India
Mohona Ghosh - IGDTUW, Delhi, India
Niyati Baliyan - National Institute of Technology Kurukshetra,

Privacy on the Internet

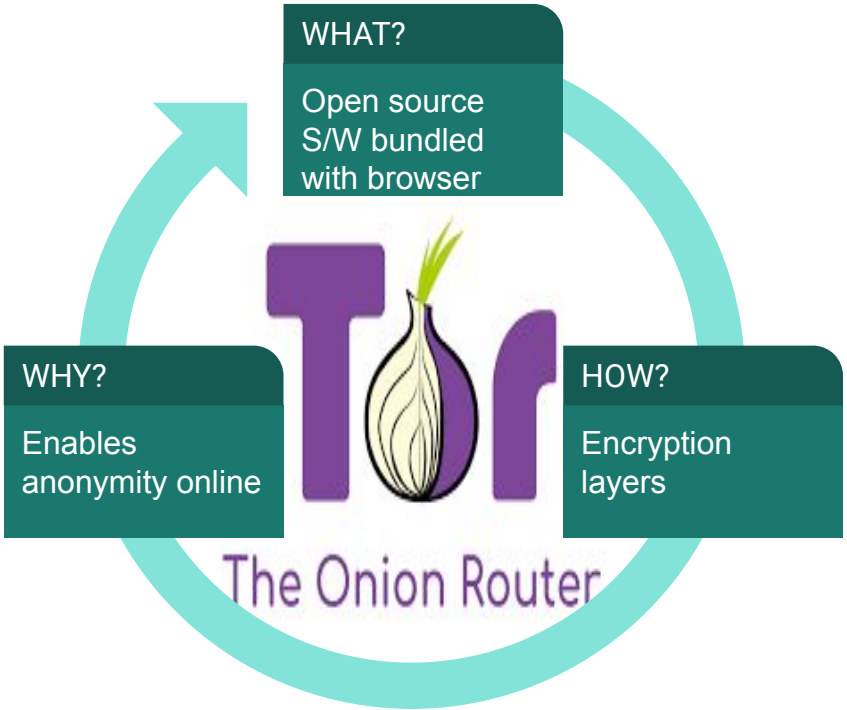
Think you're anonymous online?



Attack vectors sniffing traffic b/w client and guard node in Tor

Contents

Introduction



- common belief: internet users should have private access to an uncensored web.
- Tor instrumental to Snowden's whistleblowing 2013, at that time, Tor could not be cracked.
- PET: Privacy Enhancing Technologies
- TOR : The Onion Router is a PET
  - 8 million users each day.
  - 6500 relays around the world.

Background

➔ Using Tor, criminals keep their activities secret from law enforcement authorities

➔ Challenges in PET traffic classification

- Streaming platforms
- V/R apps
- IoT devices
- Encrypted traffic

} from heterogeneous data sources

Motivation

➔ Valuable insights via classification

- Identify malicious activity and enhance security
- Optimize resource allocation and hence network performance

Problem Statement

- To identify the applications visited by the Tor user using different classification algorithms based on machine learning
- Assumption that different types of application's traffic have different time constraints, allowing us to characterize the traffic being routed through a Tor node
- By classifying the Tor network traffic into different applications, we will be able to downgrade user's privacy to some extent by exposing their activity within Tor.

Objective

- Expose vulnerability of Tor by implementing traffic fingerprinting attack, thereby, classifying traffic into application type

Dataset

- .csv file with 3361 rows and 23 columns.
- 8 different categories of applications.
- Unbalanced Raw Dataset.

duration	total_fiat	total_biat	min_fiat	min_biat	max_fiat	max_biat	mean_fiat	mean_biat	flowPktsP	flowBytes	min_flowi	max_flowi	mean_flov	std_flowia	min_active	mean_acti	max_activ	std_active	min_idle	mean_idle	max_idle	std_idle	class1
10345300	10345257	10345174	60	52	5871778	5870638	517262.9	470235.2	4.253139	2260.447	13	5870638	240588.4	1022685	4092108	4981436	5870764	1257700	3435979	4653309	5870638	1721564	CHAT
14966353	14966200	14966053	7	0	635321	635242	10502.6	5615.78	273.4133	227450.3	0	635042	3658.361	21347.58	-1	0	-1	0	-1	0	-1	0	VIDEO-STREAMING
272867	233627	272820	20303	19353	213324	253467	116813.5	136410	21.98873	8733.192	47	213324	54573.4	90181.74	-1	0	-1	0	-1	0	-1	0	CHAT
14999391	14998887	14999391	0	0	149034	146556	9062.772	4758.69	320.613	277900.9	0	146556	3119.674	9995.782	-1	0	-1	0	-1	0	-1	0	VIDEO-STREAMING
7190597	7189947	7190597	116	492	6555090	6594711	898743.4	898824.6	2.503269	1137.18	12	6555090	422976.3	1582350	7051063	7051063	7051063	0	6555090	6555090	6555090	0	CHAT
14990289	14990249	14990288	0	0	335322	335264	10482.69	5736.811	269.8414	223305.4	0	335264	3706.797	13031.18	-1	0	-1	0	-1	0	-1	0	VIDEO-STREAMING
4894345	4894050	4894345	8600	354	1857545	1857548	444913.6	407862.1	5.107936	2363.953	24	1857504	203931	463960.7	1796398	2139641	2482884	485418.9	1438583	1648044	1857504	296221.9	CHAT
13843963	13842978	13843963	9	0	2192110	2192320	16077.79	8943.129	174.1553	145403.5	0	2191964	5744.383	52777.4	11840857	11800000	11840857	0	2191964	2191964	2191964	0	VIDEO-STREAMING
3334635	3334345	3334447	123	61	1028396	1028363	123494.3	133377.9	16.19368	6876.615	16	1028116	62917.64	160897.9	2322320	2322320	2322320	0	1028116	1028116	1028116	0	CHAT
14997888	14997526	14997032	0	0	132108	131547	5902.214	3006.622	502.1374	438405.5	0	131252	1991.751	7511.201	-1	0	-1	0	-1	0	-1	0	VIDEO-STREAMING
8959011	8920202	8959011	83	57	6093327	6092759	892020.2	895901.1	2.455628	933.8084	15	6092759	426619.6	1362168	1895443	4285731	6676018	3380377	1894923	3993841	6092759	2968318	CHAT
14989818	14989753	14989818	0	0	92205	92167	5415.373	2768.714	545.9706	482524.1	0	92155	1831.824	6492.572	-1	0	-1	0	-1	0	-1	0	VIDEO-STREAMING
2207463	2207400	2207418	14674	14204	2000354	1959996	735800	735806	3.62407	1594.591	45	1959933	315351.9	728474.7	2207400	2207400	2207400	0	1959933	1959933	1959933	0	CHAT
14998525	14998483	14998518	0	0	129551	129362	7586.486	3898.757	388.4382	341171.2	0	129362	2574.854	8572.744	-1	0	-1	0	-1	0	-1	0	VIDEO-STREAMING
14962939	14962891	14962650	0	0	902751	902507	18158.85	11116.38	145.1586	106701.7	0	902074	6892.187	32998.87	-1	0	-1	0	-1	0	-1	0	VIDEO-STREAMING

https://unb.ca/cic/datasets/tor.html

13.

Dataset ~ Application classes

1. Browser 

2. Chat
3. VoIP 

4. File transfer 

5. Email 

6. P2P 

7. Audio 

8. Video 

Dataset ~ Temporal Features from Tor Traffic

- Forward Inter Arrival Time(fiat): It is the time between two packets sent in forward direction.
- Backward Inter Arrival Time(biat):It is the time between two packets sent in backward direction.
- Flow Inter Arrival Time(flowiat): It is the time between two packets sent in either direction.
- Active Time(active): It is the amount of time a flow was active before going idle.
- Idle Time(idle): It is the amount of time a flow was idle before becoming active.
- Flow Bytes per second(flowBytesPerSecond): It is the number of bytes flown per second.
- Flow packets per second(flowPacketsPerSecond): It is the number of packets flown per second .
- Duration of flow(duration): It is the total time duration of the flow.

We take the **minimum**, **maximum**, **standard deviation** and **mean value** of fiat, biat, flowiat, active and idle as the features.

Experimental setup

➔ Dataset : ISCXTor2016 (Temporal data) 3361 rows, 23 columns

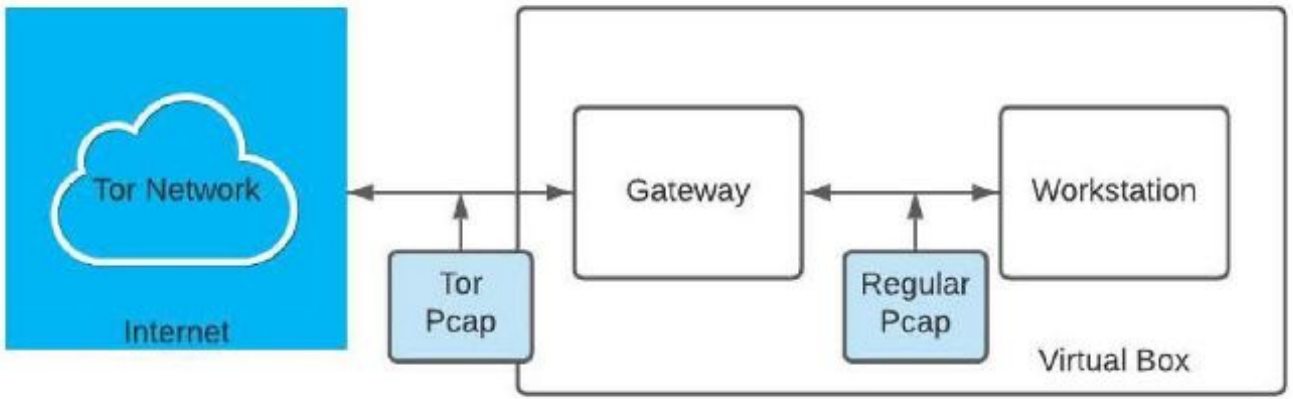
➔ whonix OS routes the traffic through Tor

ISCXFlowmeter

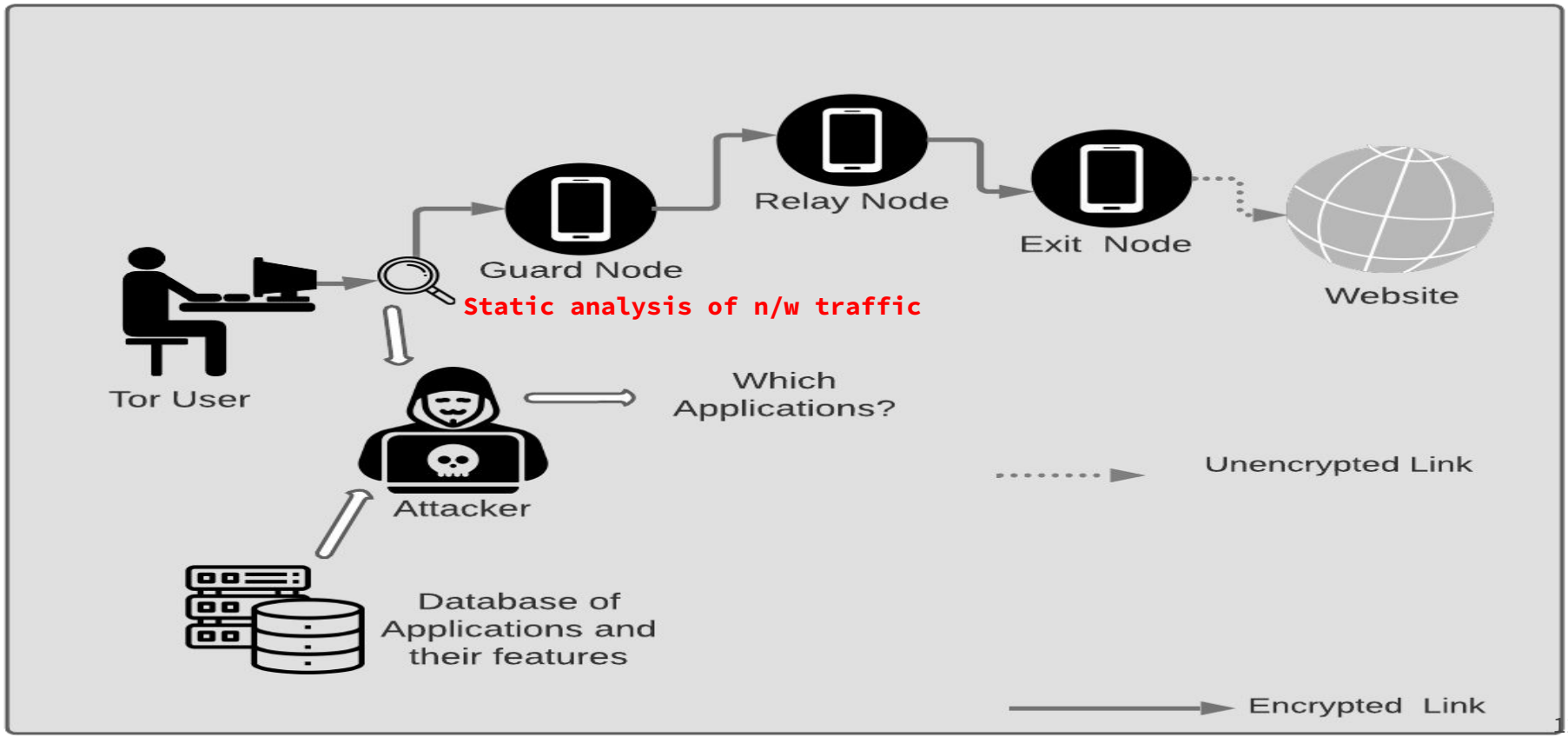
(reduced # features ~ 23)

16 GB RAM

Traffic fingerprinting attack on Tor



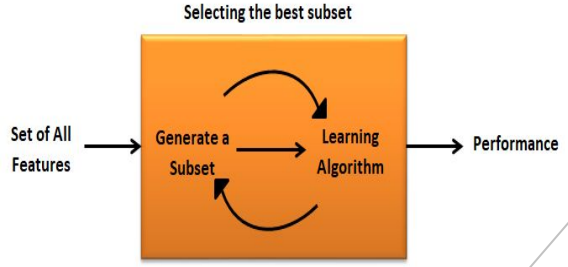
Tor user connecting to a website through three proxy servers

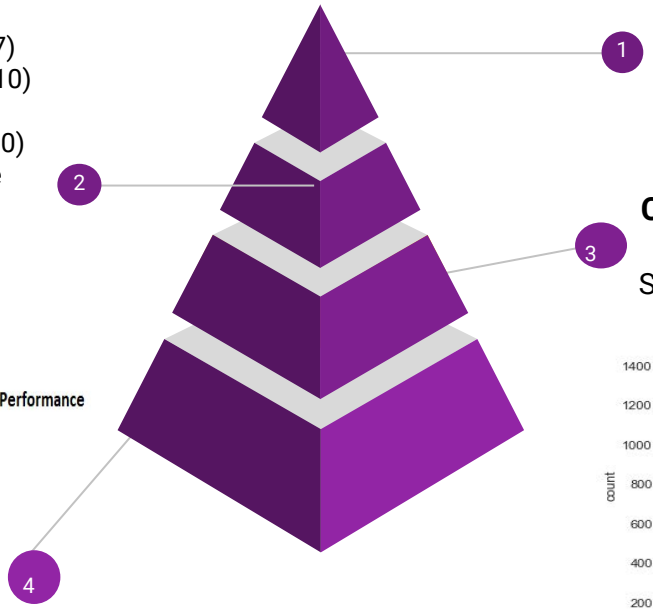


Methodology

Feature Selection

- **FILTER**
  - Correlation FS (7)
  - Mutual Info FS (10)
- **WRAPPER**
  - Sequential FS (10)
  - Tree importance
- **AUTO ENCODER** (12)





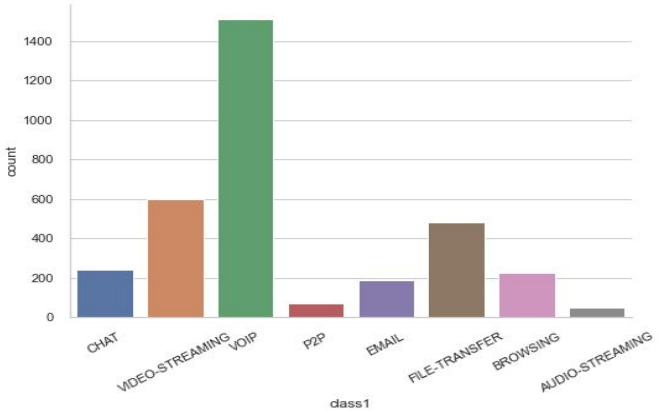
Data Preprocessing

- Complete Case Analysis
- Duplicate value removal

Colour	Make	Doors	Exhaust
Red	Ford	4	1
Red	Ford	4	1
Red	Ford	4	1
Red	Ford	4	1
Green	Ford	5	1

Class balancing

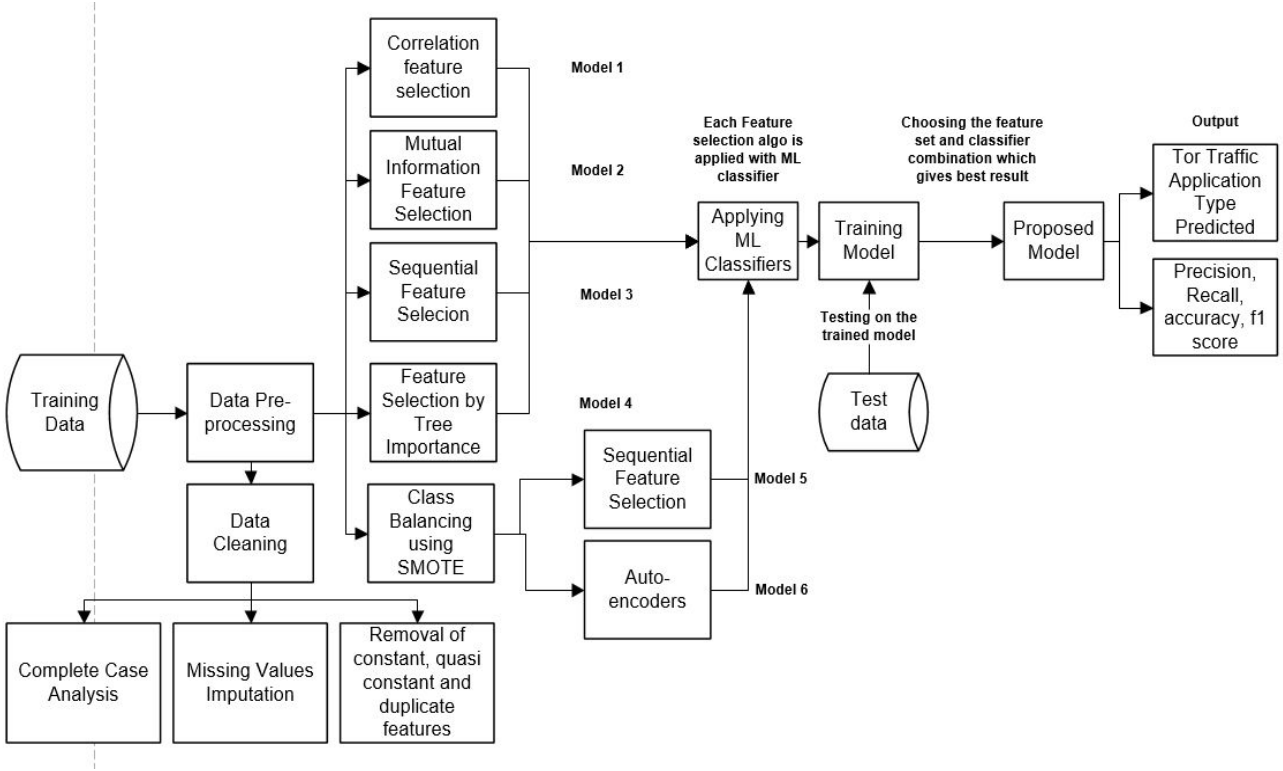
SMOTE :Oversample minority class



Algorithms for classification

Ensemble and DL models
Hyperparameter tuning
F1 + Accuracy metric

Methodology



- Decision tree
- Logistic regression
- Support Vector Machine
- K-nearest neighbour
- **Random Forest**
- AdaBoost
- XGBoost

} Ensemble

Model 1-5 used traditional methods for feature selection. However, model 6 used multilayer perceptron autoencoder for feature selection.

Evaluation metrics

Metric	[1]	[2]	[3]	Our Proposed Model
Precision	0.87	N/A	0.84	**0.96**
Recall	N/A	N/A	0.85	**0.95**
F1-Score	N/A	0.95	N/A	**0.95**
Accuracy	N/A	95.6%	N/A	**95.75%**

Reference:
1. Lashkari, A.H., Draper-Gil, G., Mamun, M.S.I., Ghorbani, A.A.: Characterization of tor traffic using time-based features. In: ICISSP, pp. 253–262 (2004)

2. Xu, J., Wang, J., Qi, Q., Sun, H., He, B.: Deep neural networks for application awareness in sdnbased network. In: 28th International Workshop on Machine Learning for Signal Processing (MLSP), pp. 1–6. IEEE (2018)

3. Sarkar, D., Vinod, P., Yerima, S.Y.: Detection of tor traffic using deep learning. In: IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA), pp. 1–8. IEEE (2020)

Random forest with SMOTE gives best accuracy (95.75%)

Comparative evaluation

Research Work	Feature Selection	Class Balancing	Hyperparameter Tuning	Accuracy	Precision	Recall	F1-Score
[1]	✓	✗	✗	✗	✓	✓	✗
[2]	✗	✗	✗	✗	✓	✗	✗
[3]	✓	✗	✓	✓	✗	✗	✓
Our Work	✓	✓	✓	✓	✓	✓	✓

0.15 % improvement in accuracy over state-of-the-art on given dataset

Scope

1. Compromising the anonymity of Tor user by enabling traffic classification attack.
2. Supervised Machine Learning/Classification Algorithms
   Random Forest, XGBoost, AdaBoost, Decision Tree, K-Nearest, Neighbour, Logistic Regression and Support Vector Machine
3. Feature Selection Algorithms
   Correlation Feature Selection, Mutual Information, Sequential Feature Selection (Step Forward), Tree Importance and Multi-layer Perceptron Autoencoders
4. Using Time Related Features
   focus on temporal statistics of traffic only, as our feature set.
5. Comparative analysis with SOTA
   in terms of accuracy, precision, recall and F-1 score

Conclusion and Future Work

- Analysed that by using time characteristics alone we can classify Tor traffic into different applications like Chat, VoIP, FTP, Video-Streaming, Audio-Streaming, Email, Browsing and P2P.

- Class balancing by SMOTE significantly improved the accuracy of Model 3 by 7.46% and gave best performing proposed model: Model 5

- Model 5 outperformed the models in prior research work by 0.15% in terms of accuracy using the same dataset

- Used Multi layer perceptron autoencoder for traffic classification and inferred that they are not very effective in classifying Tor traffic accurately.

31.

“Those who are motivated only by the desire for the fruits of action are miserable, for they are constantly anxious about the results of what they do” The Bhagwad Gita

Thank you.
Queries and suggestions are welcome.

Reach out : niyatibaliyan@nitkkr.ac.in