Detection and Characterization of DDoS Attacks using Time-based Features

Team/Students: James Halladay, Drake Cullen, and Nathan Briner | Professor: Dr. Ram Basnet

Abstract

In today's evolving cybersecurity landscape, distributed denial-of-service (DDoS) attacks have become one of the most prolific and costly threats. Their capability to incapacitate network services while causing millions of dollars in damages has made effective DDoS detection and prevention imperative for businesses and government entities alike. Prior research has found shallow and deep learning classifiers to be invaluable in detecting DDoS attacks; however, there is an absence of research concerning time-based features and classification among many DDoS attack types. We propose and study the efficacy of 25 time-based features to detect and classify 12 types of DDoS attacks using binary and multiclass classification. Furthermore, we ran experiments to compare the performance of eight traditional machine learning classifiers and one deep learning classifier using two different scenarios. Our findings show that the majority of models provided 99% accuracy on both the control and time-based experiments in detecting DDoS attacks while yielding 70% accuracy in classifying specific DDoS attack types. Training on the proposed time-based feature subset was found to be effective at reducing training time without compromising test accuracy; thus, the smaller time-based feature subset alone is beneficial for near-real time applications that incorporate continuous learning.

Our Contributions

- We train nine classifiers on a time-based feature subset to detect and classify DDoS attacks by analyzing temporally related features in traffic flows. To our knowledge, the time-based feature set has not been investigated in the domain of DDoS attacks.
- The smaller time-based feature set reduces overall training time, decreases dimensionality and noise, reduces the necessary computational resources, and promotes the viability of continuous learning.
- We've found few related works concerning multiclass classification in the domain of DDoS detection. One such study by Chen et al. focused on differentiating five types of DDoS attacks whereas our classifiers differentiate 12 different attack types.
- Our binary classifiers produced comparable or higher accuracy results than the ones published in existing literature, and our multiclass classifiers' performances are in line with Chen et al.'s classifiers despite using seven more attack types.
- Lashkari et al. found the time-based feature set to be effective in classifying Tor and VPN traffic. We have filled in the knowledge gap in the domain of DDoS attacks by finding the time-based feature subset alone to be comparably effective and providing much better training time.

Dataset

The CICDDoS2019 dataset, provided by the Canadian Institute of Cybersecurity, contains benign and DDoS attack flows from 13 modern DDoS attack types. Approximately 112,000 of the 70 million samples are benign. Our time-based experiments train on a subset of 25 out of the original 88 features. The time-based features include forward inter arrival time, backward inter arrival time, flow inter arrival time, active time, idle time, flow bytes per second, flow packets per second, forward inter arrival time total, backward inter arrival time total, and duration. Note, the first five features (forward inter arrival time through idle time) are made up of four features. These features include the mean, min, max, and standard deviation of that feature; thus, there are a total of 25 time-based features.

Experiment Scenarios

We conduct our experiments in two separate scenarios and compare the results of several classifiers on a time-based feature set. Scenario A aims to detect DDoS attacks.

Experiment Scenarios Continued

This is done using binary classification where benign flows are mixed with a basket of 12 different DDoS attack types. Control results were established by training the nine models (Random Forest (RF), K-Nearest Neighbors (KNN), LightGBM (LGBM), XGBoost (XGB), Adaptive Boosting (ADA), Linear Discriminant Analysis (LD), Gaussian Naïve Bayes (GNB), Support Vector Machine (SVM) and a Deep Neural Network (DNN)) on all 70 features in the processed and cleaned dataset. Next, the same nine models were trained on the 25 time-based features. Scenario B focuses on characterizing a given DDoS attack using multiclass classification. The nine models were trained to differentiate between UDP-Lag, UDP Flood, TFTP, SYN Flood, SSDP, SNMP, Portmap, NetBIOS, NTP, MSSQL, LDAP, and DNS attacks. Like Scenario A, the first set of models were trained on every feature and subsequent models were trained on time-based features.

Results

Every model in Scenario A performed exceptionally well on the control features. The models performed in the range of 98-99% accuracy with F1-scores and AUC values of at least 0.99.

Table 1: Results for Scenario A control experiments

Metrics	LD	LGBM	XGB	RF	DNN	ADA	SVM	KNN	GNB
Accuracy	.99	.9999	.9998	.9997	.9989	.9987	.9985	.9951	.9862
F1	1	1	1	1	1	1	1	1	.99
AUC	1	1	1	1	1	1	1	1	.99
Training Time (s)	1.33	1.34	8.93	12.03	185.61	12.91	203.28	30.36	.14

In contrast to the Scenario A control experiments, the baseline multiclass experiments saw a great divergence in model performance. Referring to table 2, XGB, LD, and LGBM achieved the highest accuracies and F1 scores of just over 70% and 0.7, respectively. For differentiating among 12 attack types, these are exceptional results.

Table 2: Results for Scenario B control experiment (Metrics are the same as Table 1)

XGB	LGBM	LD	KNN	RF	DNN	SVM	ADA	GNB
.7408	.7346	.7334	.7038	.6994	.6362	.6302	.5149	.3849
.7342	.7257	.7258	.7	.6858	.65	.5958	.4525	.29
.98	.97	.97	.97	.97	.96	.96	.86	.92
1569.45	71.96	59.037	27,525.78	218.77	1,566.47	189,733.14	125.01	2.94

Transitioning to the time-based data as seen in Table 3, most classifiers performed like their control experiment yielding only a small decrease in accuracy. The training time difference between the time-based and control experiments becomes more apparent in the Scenario B experiments. This could result from the fact that differentiating among multiple classes is a more computationally demanding task compared to binary classification; therefore, any improvements in training speed will be compounded.

Table 3: Results for Scenario B control experimentation (Metrics are the same as Table 1)

XGB	RF	LGBM	LD	KNN	ADA	SVM	DNN	GNB
.9858	.9858	.9844	.9843	.9792	.9578	.9051	.698	.5784
.99	.99	.98	.98	.98	.96	.905	.69	.5
1	1	1	1	.99	.99	.96	.94	.85
5.69	13.06	.65	.65	28.69	6.27	1728.08	187.34	.05

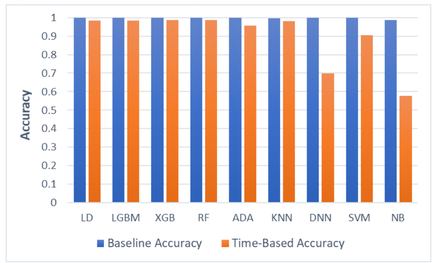
Results Continued

Observing the time-based Scenario B results seen in Table 4, accuracy and F1-score saw a slight degradation across all classifiers. Training times saw moderate to substantial improvements across all classifiers except for RF which maintained a similar time.

Table 4: Results for Scenario B time-based experimentation (Metrics are the same as Table 1)

XGB	RF	LD	LGBM	KNN	SVM	ADA	DNN	GNB
.6905	.6898	.6843	.6838	.6743	.5427	.5151	.4955	.1139
.6733	.6742	.6642	.6642	.67	.4950	.4483	.48	.0658
.97	.97	.97	.97	.96	.88	.87	.87	.66
624.01	229.31	44.11	56.38	13,696.92	209,182.82	71.8	1401.08	.062

Figures 1 and 2: Comparison of accuracies in Scenario A and Scenario B



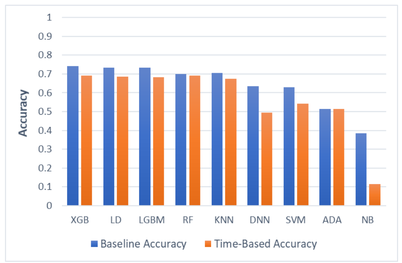


Table 7: Training time comparisons for the top 5 models

	Scenario A			Scenario B		
	Control training time (s)	Time-based training time (s)	% Difference	Control	Time-based	% Difference
XGB	8.93	5.69	-36.28%	1569.45	624.01	-60.24%
KNN	30.36	28.69	-5.50%	27,525.78	13,696.92	-50.24%
LD	1.33	.65	-51.13%	59.04	44.11	-25.29%
LGBM	1.34	.65	-51.48%	71.96	56.38	-21.65%
RF	12.03	13.06	8.56%	218.77	229.21	4.77%

Conclusion

Our work demonstrated time-based features viability in the domain of DDoS detection. The results found in research indicate that time-based features warrant further experimentation in traffic-based research where a smaller dataset may prove beneficial to prevent overfitting, potentially improve accuracy, and promote the viability of continuous training.

References

T. Mahjabin et al., "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," 2017, doi: https://doi.org/10.1177/1550147717741463

S. Mohammed et al., "A new machine learning-based collaborative ddos mitigation mechanism in software-defined network," 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications, 2018, doi: https://doi.org/10.1109/wimob.2018.8589104

A. Callado et al., "A survey on internet traffic identification," IEEE Communications Surveys & Tutorials, 11(3), 37–52, 2009, doi: https://doi.org/10.1109/surv.2009.090304

X. Ying, "An Overview of Overfitting and its Solutions. Journal of Physics: Conference Series," 2019, 1168. 022022. doi: 10.1088/1742-6596/1168/2/022022.

A. Lashkari et al., "Characterization of tor traffic using time based features," 2017, doi: https://doi.org/10.5220/0006105602530262

I. Sharafaldin et al., "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," IEEE 53rd International Carnahan Conference on Security Technology, Chennai, India, 2019, Available: https://ieeexplore.ieee.org/abstract/document/8888419

S. Elsayed et al., "DDoSNet: A Deep-Learning Model for Detecting Network Attacks,"2020, doi: https://doi.org/10.1109/wowmom49955.2020.00072

Department of Computer Science and Engineering

COLORADO MESA UNIVERSITY

Cybersecurity Education & Research Center (CybER)