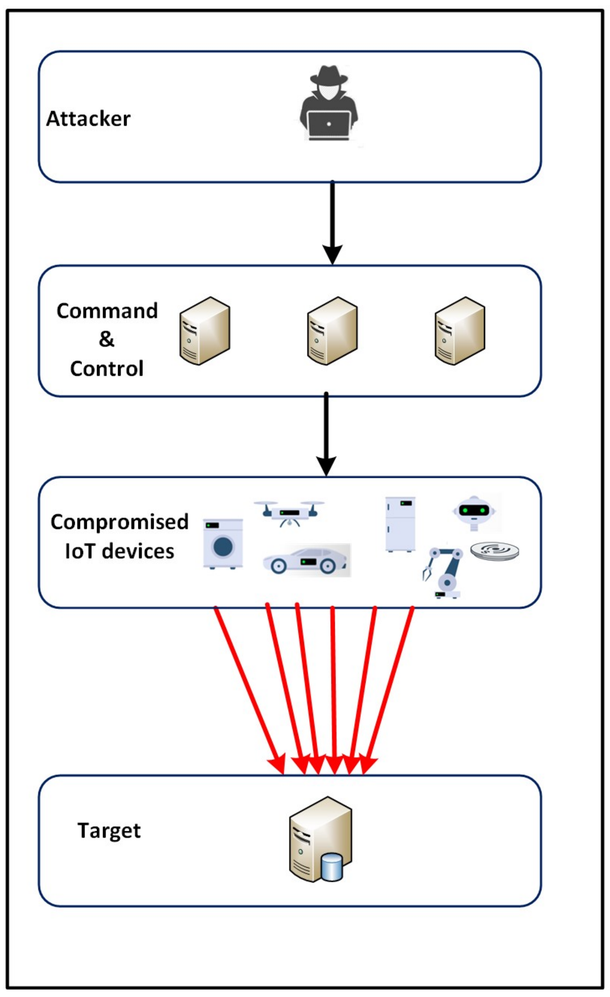
Mitigating Cyber Threats at the Network Edge

Toyin Sofoluwe, Fung Po Tso, Iain Phillips

Loughborough University

Problem



1. Single point DDoS detection requires high compute resources
2. Wastes significant resources as attack traffic traverse multiple networks only to be dropped.
3. Attack easily re-route around point-based detection systems
4. Eemphasis not been placed on quantitative measurements of compute requirements needed for DDoS detection

Contributions

The main contributions of this paper are:

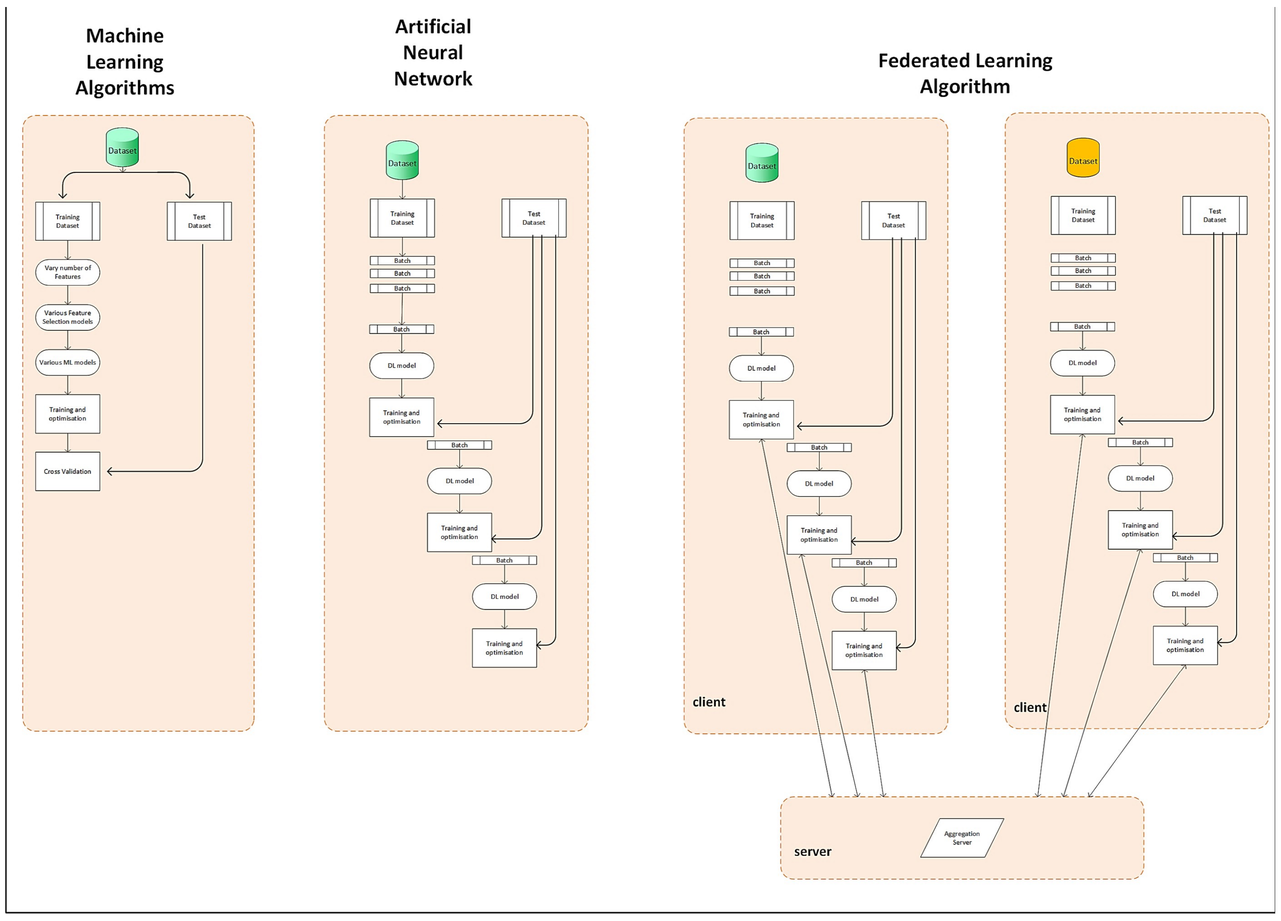
1. Quantitative measurements of compute requirements of the inference stage of ML based DDoS detection.
2. Identify suitable combination of ML algorithms which is suitable for use in a cloud-based IoT environment with minimal compute and memory resource requirements.
3. Identify suitability of utilising deep learning based Federated learning algorithms and measure the resource requirement of FL algorithms.

Utilising knowledge gained to develop a lightweight framework of interconnected edge devices able to share minimal non-confidential data required in a DDoS detection model.

Future Work

- Hyper-parameter tuning to verify impact on the performance.
- Develop a lightweight collaborative network framework to detect DDoS attacks close to the source.

Method



Labelled dataset UNSW-NB15 utilized, transformed with scikit-learn MinMaxScaler and StandardScaler . The 4 feature extraction techniques used : Anova-F, Chi-squared **(Chi2)**, Recursive Feature Elimination **(RFE)** and Mutual Information Classifier **(MIC)**.

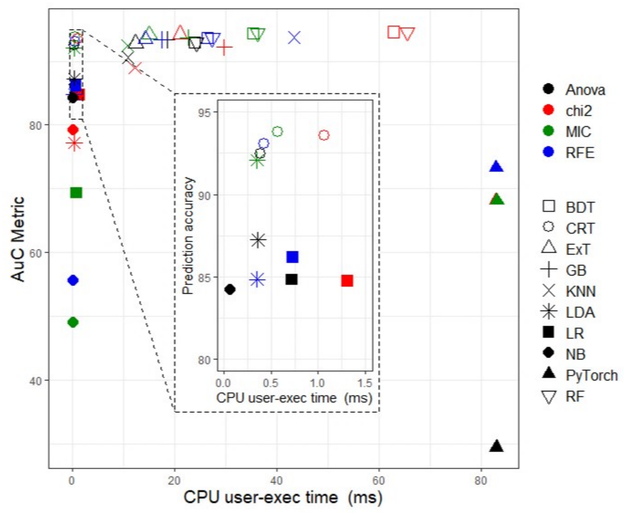
Combined with 10 lightweight ML, ANN & FL algorithms. Then trained and tested with binary classification metrics such as prediction accuracy, area under ROC curve (AuC) and Confusion matrix while measuring the resource requirements of each combination.

Federated Learning: Resource utilisation measured on each client node

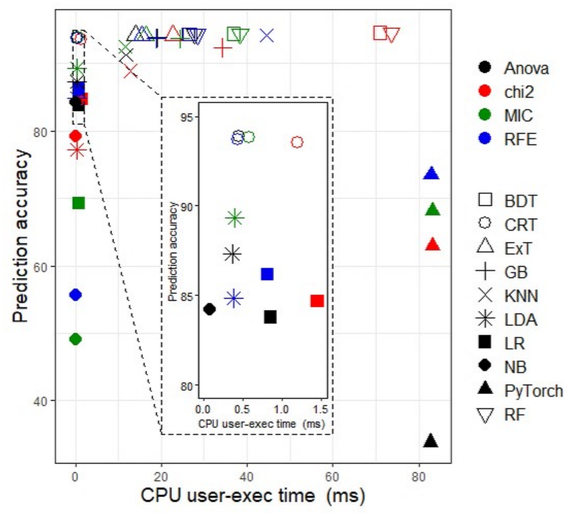
Algorithm combinations

Feature Selection	Machine Learning
Anova-F	Bagging Decision Tree (BDT)
Chi2	Decision Tree Classifier (CRT)
RFE	Extra Tree (ExT)
MIC	Gradient Boosting (GB)
	K-Nearest Neighbours (KNN)
	Linear Discriminant Analysis (LDA)
	Logistic Regression (LR)
	GaussianNB (NB)
	PyTorch
	Random Forest algorithms (RF)

Results



Prediction vs CPU



AuC vs CPU

- **Selected Features:** vary significantly when using fewer than five features.
- **Memory Utilization:** was not significantly different across different combinations.
- **Prediction Results:** DL and ensemble ML gave higher accuracy at the cost of CPU

Promising DDoS detection using simple, low compute resource ML algorithms. We aim to aggregate outputs from low resource edge nodes to further improve overall detection

References

[1] Doshi, R. and Apthorpe, N. and Feamster, N. IEEE: Machine learning DDoS detection for consumer internet of things devices. In *EEE Symposium on Security and Privacy Workshops*

[2] Mishra, N. and Pandya, S. Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review In *IEEE Access , IEEE Press 2021*

[3] The University of New South Wales https://research.unsw.edu.au/projects/unsw-nb15-dataset In *June 2021*