IEEE Xplore® Digital Library

ISCAS 2020

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

CAS

Detection of Denial of Service Attacks in Communication Networks

Ana Laura Gonzalez Rios, Zhida Li,
Kamila Bekshentayeva, and Ljiljana Trajković

Simon Fraser University

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

Detection of Denial of Service Attacks in Communication Networks

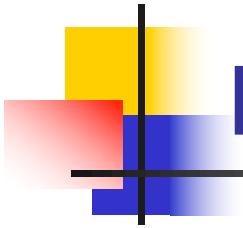
Communication Networks Laboratory

http://www.ensc.sfu.ca/cnl

School of Engineering Science

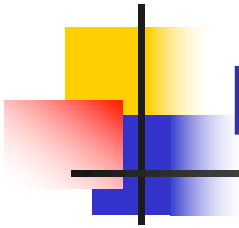
Simon Fraser University, Vancouver, British Columbia

Canada



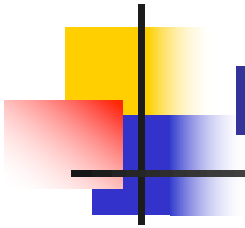
Roadmap

- Introduction
- Intrusion detection testbeds and datasets:
  - CICIDS2017
  - CSE-CIC-IDS2018
- Broad learning system and its extensions
- Experimental procedure and performance evaluation
- Conclusion and references



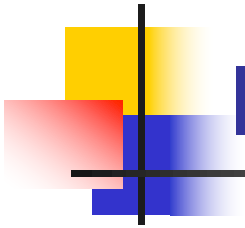
Roadmap

- Introduction
- Intrusion detection testbeds and datasets:
  - CICIDS2017
  - CSE-CIC-IDS2018
- Broad learning system and its extensions
- Experimental procedure and performance evaluation
- Conclusion and references



Introduction

- Primary infrastructure against cybersecurity threats is based on intrusion detection systems:
  - host-based systems protect the host (endpoint) by monitoring the operating system files and processes
  - network-based systems monitor network traffic by analyzing flows of packets and/or inspecting packet headers



Introduction

- Network intrusion detection systems employ diverse deep learning algorithms:
  - Convolutional neural networks: CNNs
  - Recurrent neural networks: RNNs
  - Deep belief networks
  - Autoencoders
- Supervised machine learning algorithms:
  - Support vector machine: SVM
  - Long short-term memory: LSTM
  - Gated recurrent unit: GRU
  - Broad learning system: BLS

Roadmap

- Introduction
- Intrusion detection testbeds and datasets:
  - CICIDS2017
  - CSE-CIC-IDS2018
- Broad learning system and its extensions
- Experimental procedure and performance evaluation
- Conclusion and references

CICIDS2017 and CSE-CIC-IDS2018

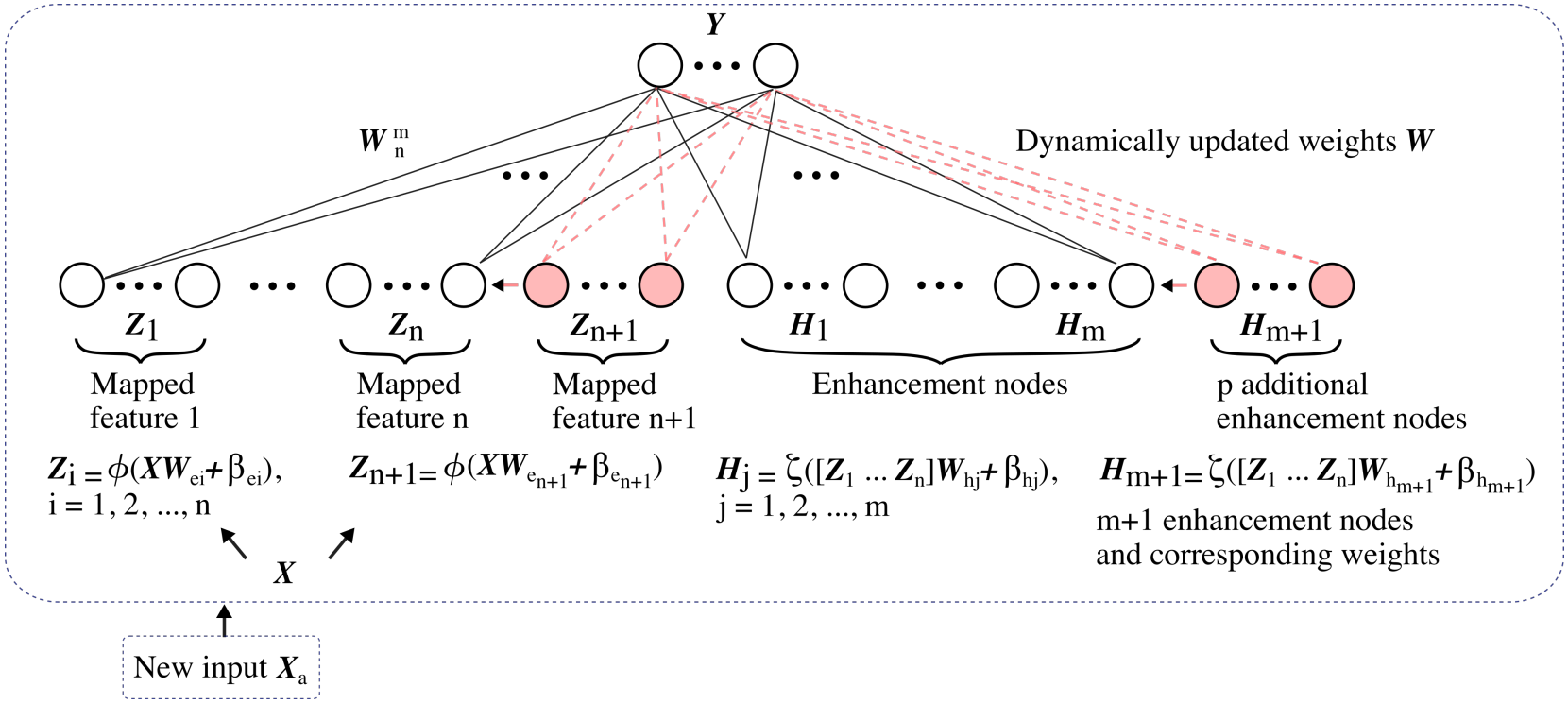
- Testbed used to create the publicly available datasets that include multiple types of recent cyber attacks
- CICIDS2017 DoS data collected on Wednesday, July 05, 2017
- CSE-CIC-IDS2018 DoS data collected on Thursday, February 15, 2018:
  - 09:26 to 10:09
  - 10:59 to 11:40
- Anomalous data points are labeled: GoldenEye, Hulk, SlowHTTPTest, and Slowloris

Roadmap

- Introduction
- Intrusion detection testbeds and datasets:
  - CICIDS2017
  - CSE-CIC-IDS2018
- Broad learning system and its extensions
- Experimental procedure and performance evaluation
- Conclusion and references

Broad Learning System

- Module of the Broad Learning System (BLS) algorithm with increments of mapped features, enhancement nodes, and new input data:



Broad Learning System: BLS

- Matrix $\boldsymbol{A}_x$ is constructed from groups of mapped features $\boldsymbol{Z}^n$ and groups of enhancement nodes $\boldsymbol{H}^m$ as:

$$\begin{aligned}\boldsymbol{A}_x &= [\boldsymbol{Z}^n \mid \boldsymbol{H}^m] \\ &= \left[\phi(\boldsymbol{X}\boldsymbol{W}_{ei} + \beta_{ei}) \mid \xi(\boldsymbol{Z}_x^n \boldsymbol{W}_{hj} + \beta_{hj})\right], \\ &\qquad i = 1, 2, \ldots, n \; and \; j = 1, 2, \ldots, m\end{aligned}$$

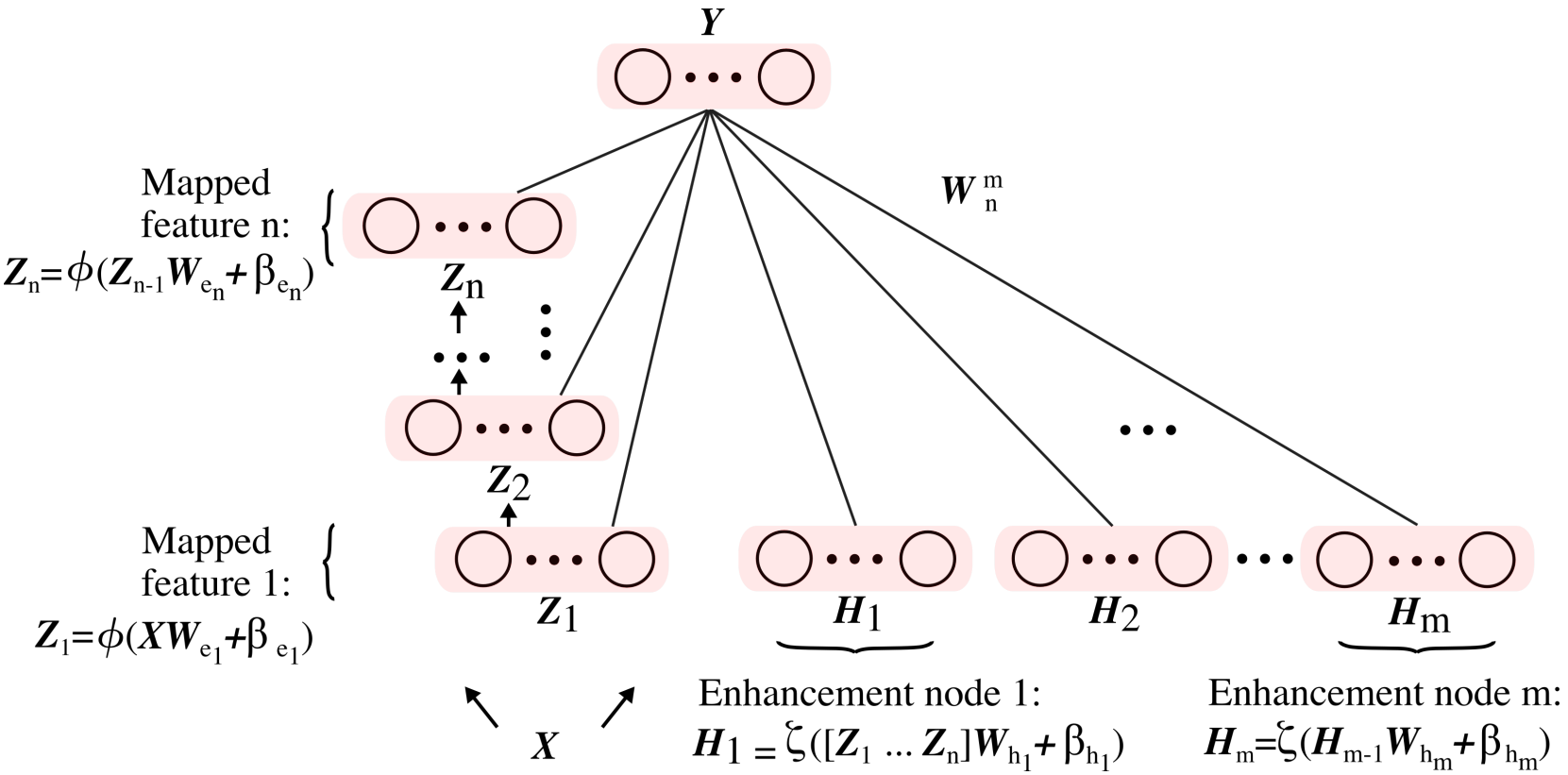
- where:
  - ϕ and ξ: projection mappings
  - $\boldsymbol{W}_{ei}$, $\boldsymbol{W}_{hj}$: weights
  - β_{ei}, β_{hj}: bias parameters
- Modified to include additional mapped features $\boldsymbol{Z}_{n+1}$, enhancement nodes $\boldsymbol{H}_{m+1}$, and/or input nodes $\boldsymbol{X}_a$.

Broad Learning System: BLS

- Moore-Penrose pseudo inverse of matrix $\boldsymbol{A}_x$ is computed to calculate the weights $\boldsymbol{W}_x$ for the given output $\boldsymbol{Y}$
- During testing, data labels are deduced using the calculated weights, mapped features, and enhancement nodes
- The RBF-BLS employs Gaussian function as the enhancement mapping ξ

RBF-BLS: Radial basis function BLS

Cascades of Mapped Features



Cascades of Mapped Features

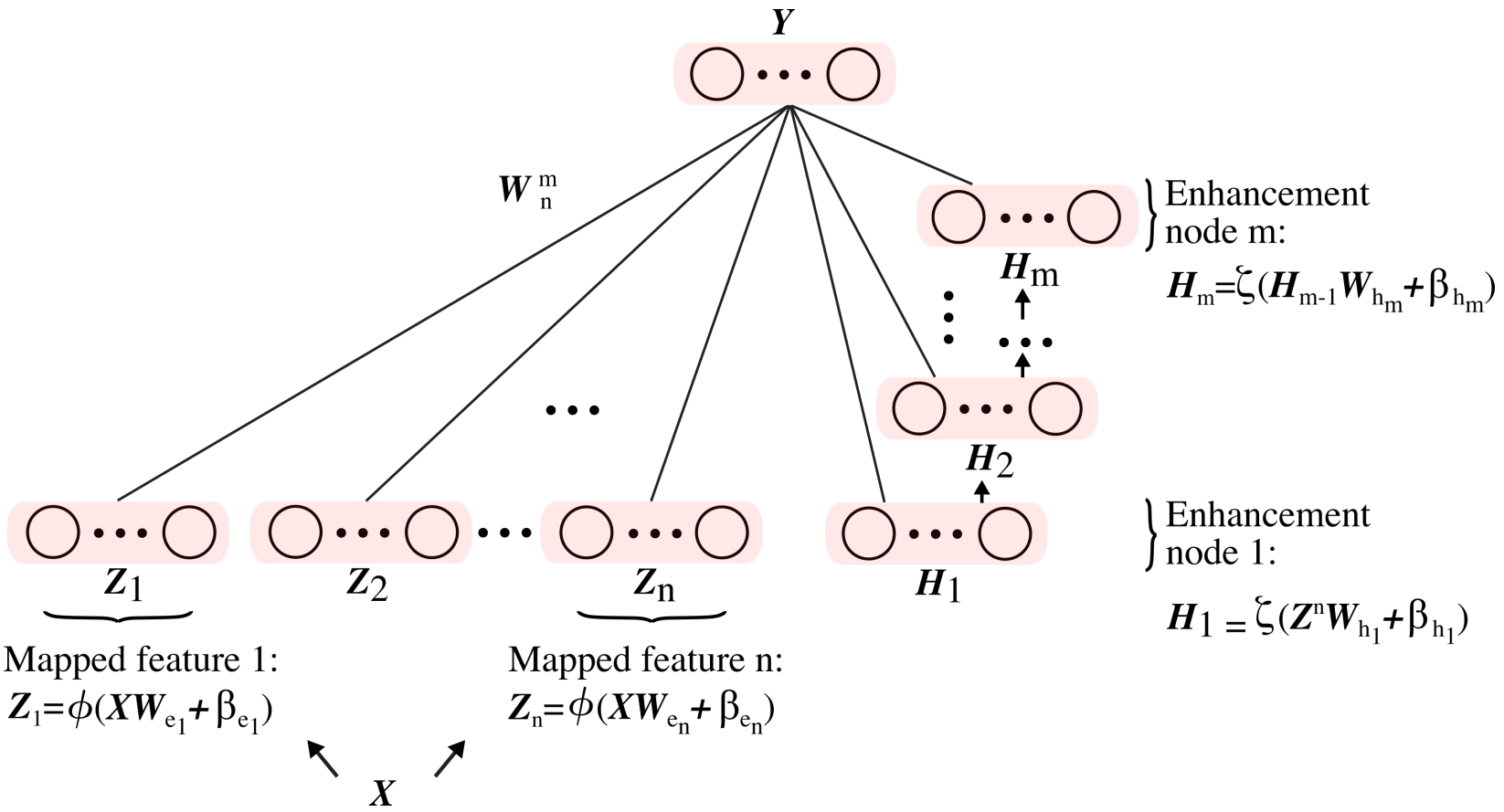
- Cascade of mapped features (CFBLS):

  the new group of mapped features is created by using the previous group $(k\ -1)$.

- Groups of mapped features are formulated as:

$$\boldsymbol{Z}_k = \phi(\boldsymbol{Z}_{k-1}\boldsymbol{W}_{ek}\ +\ \beta_{ek})$$
$$\triangleq\ \phi^k\left(\boldsymbol{X}\,;\{\boldsymbol{W}_{ei},\beta_{ei}\}_{i=1}^{k}\right), for\ k = 1,\ldots,n$$

Cascades of Enhancement Nodes



Cascades of Enhancement Nodes

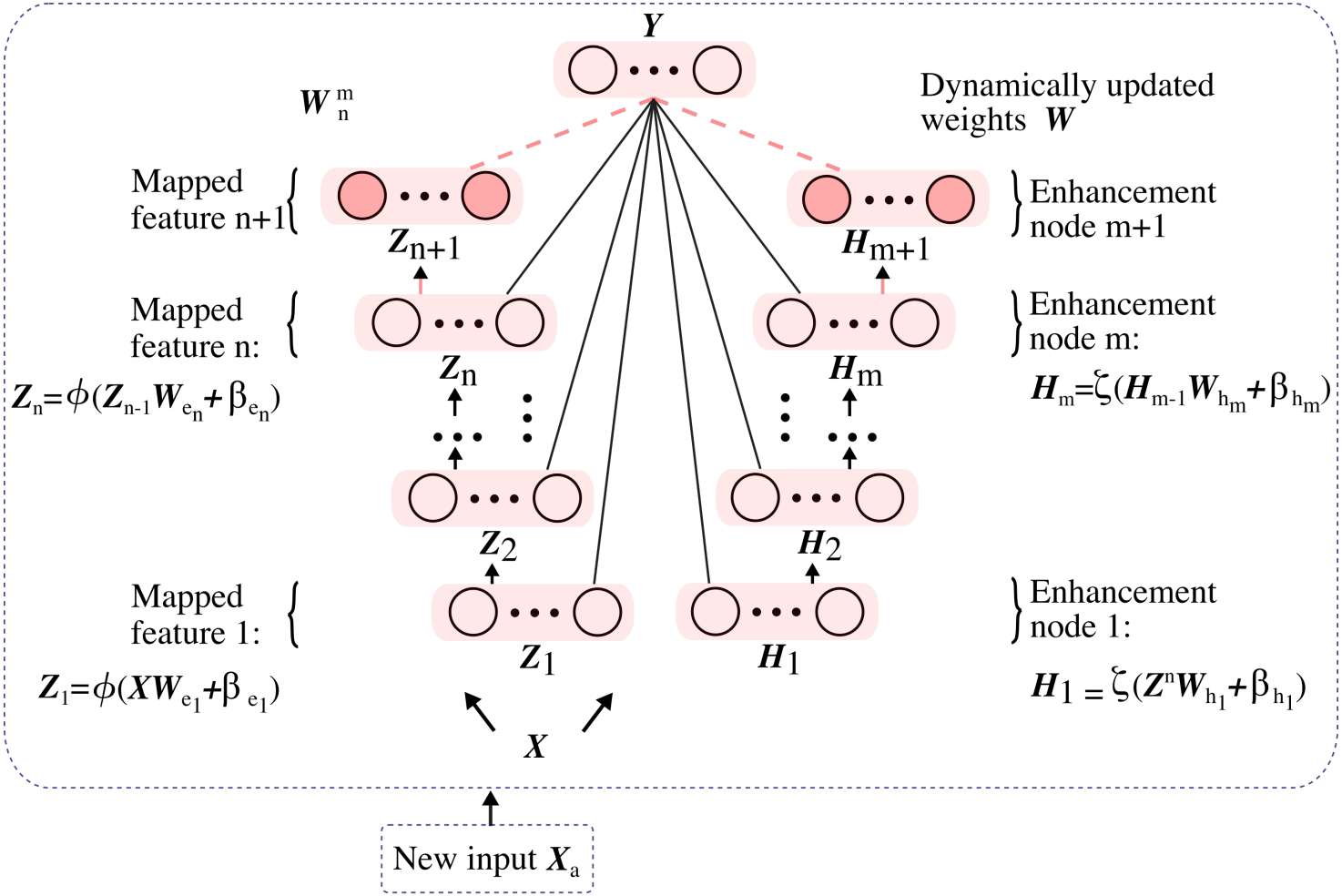
- The first enhancement node in cascade of enhancement nodes (CEBLS) is generated form mapped features
- The subsequent enhancement nodes are generated from previous enhancement nodes creating a cascade:

$$H_u \triangleq \xi^u(\boldsymbol{Z}^n ; \{\boldsymbol{W}_{hi}, \beta_{hi}\}_{i=1}^{u}), \text{for } u = 1, \ldots, m,$$

where:

- $\boldsymbol{W}_{hi}$ and β_{hi} are randomly generated

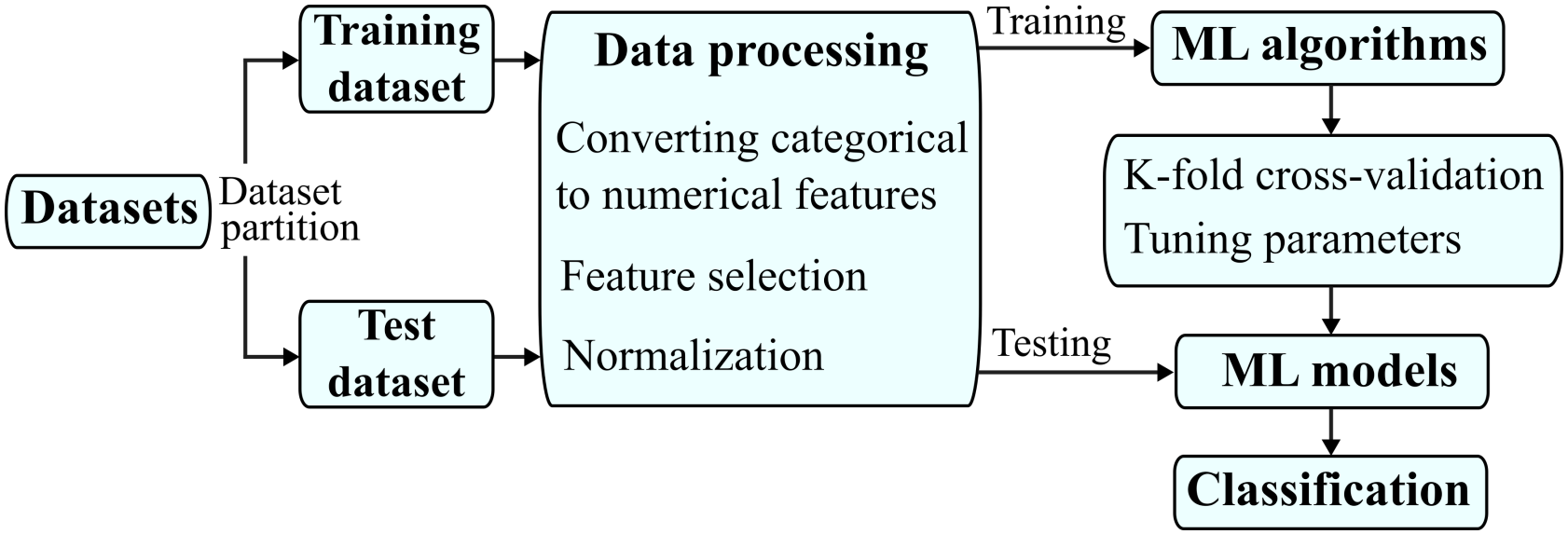
Cascades of Mapped Features and Enhancement Nodes



Roadmap

- Introduction
- Intrusion detection testbeds and datasets:
  - CICIDS2017
  - CSE-CIC-IDS2018
- Broad learning system and its extensions
- Experimental procedure and performance evaluation
- Conclusion and references

Experimental Procedure

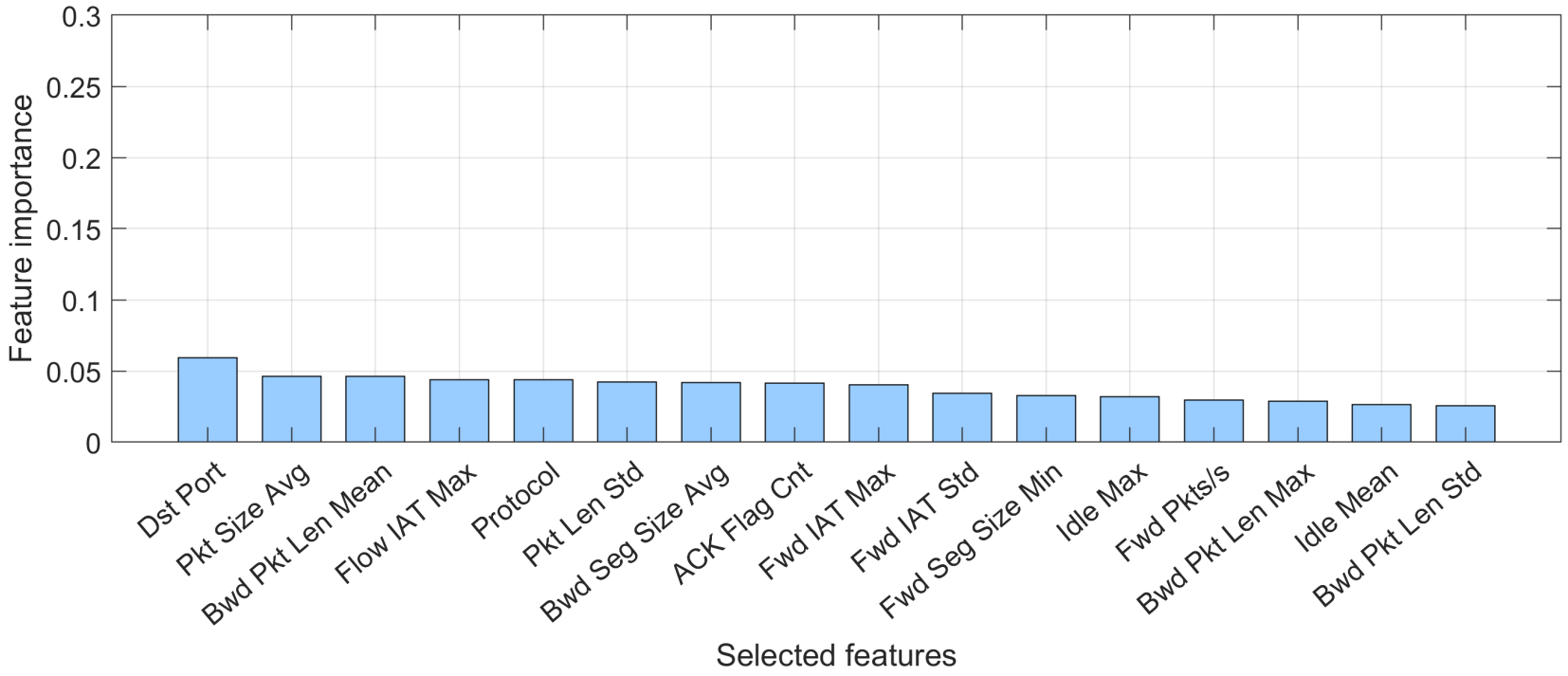


Experimental Procedure

- Step 1: Extracting the CICIDS2017 and CSE-CIC-IDS2018 subsets for training and testing
- Step 2: Removing invalid data, converting categorical to numerical features, and normalizing training and test datasets to have mean 0 and standard deviation 1 employing the z-score function
- Step 3: Using 10-fold validation to train and tune parameters
- Step 4: Testing and evaluating generated machine learning (ML) models based on:
  - Accuracy
  - F-Score

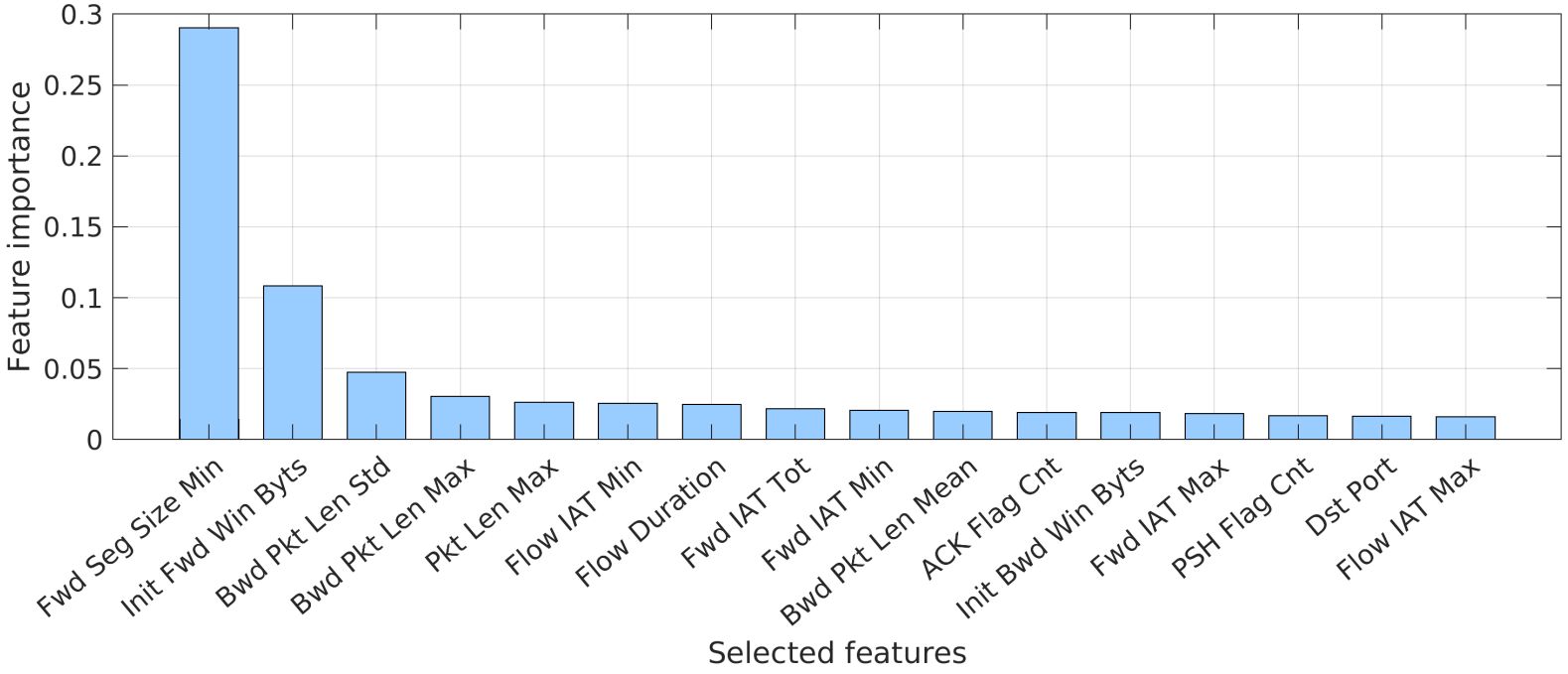
16 Most Relevant Features

- CICIDS2017



16 Most Relevant Features

- CSE-CIC-IDS2018



Best Parameters: Non-Incremental BLS

Parameters	CICIDS2017			CSE-CIC-IDS2018		
	Number of features					
Non-Incremental BLS	**78**	**64**	**32**	**78**	**64**	**32**
Model	RBF-BLS	BLS	CEBLS	CFBLS	RBF-BLS	CEBLS
Mapped features	20	10	10	20	20	15
Groups of mapped features	30	30	10	10	10	20
Enhancement nodes	40	20	40	80	80	80

Best Parameters: Incremental BLS

- Incremental learning steps: 2
- Data points/step: 55,680 (CICIDS2017) and 49,320 (CSE-CIC-IDS2018)
- Enhancement nodes/step: 20

Parameters	**CICIDS2017**			**CSE-CIC-IDS2018**		
	Number of features					
Incremental BLS	**78**	**64**	**32**	**78**	**64**	**32**
Model	CFBLS	CFEBLS	CEBLS	BLS	CEBLS	BLS
Mapped features	10	20	10	15	20	10
Groups of mapped features	20	20	20	30	10	20
Enhancement nodes	40	20	40	20	40	20

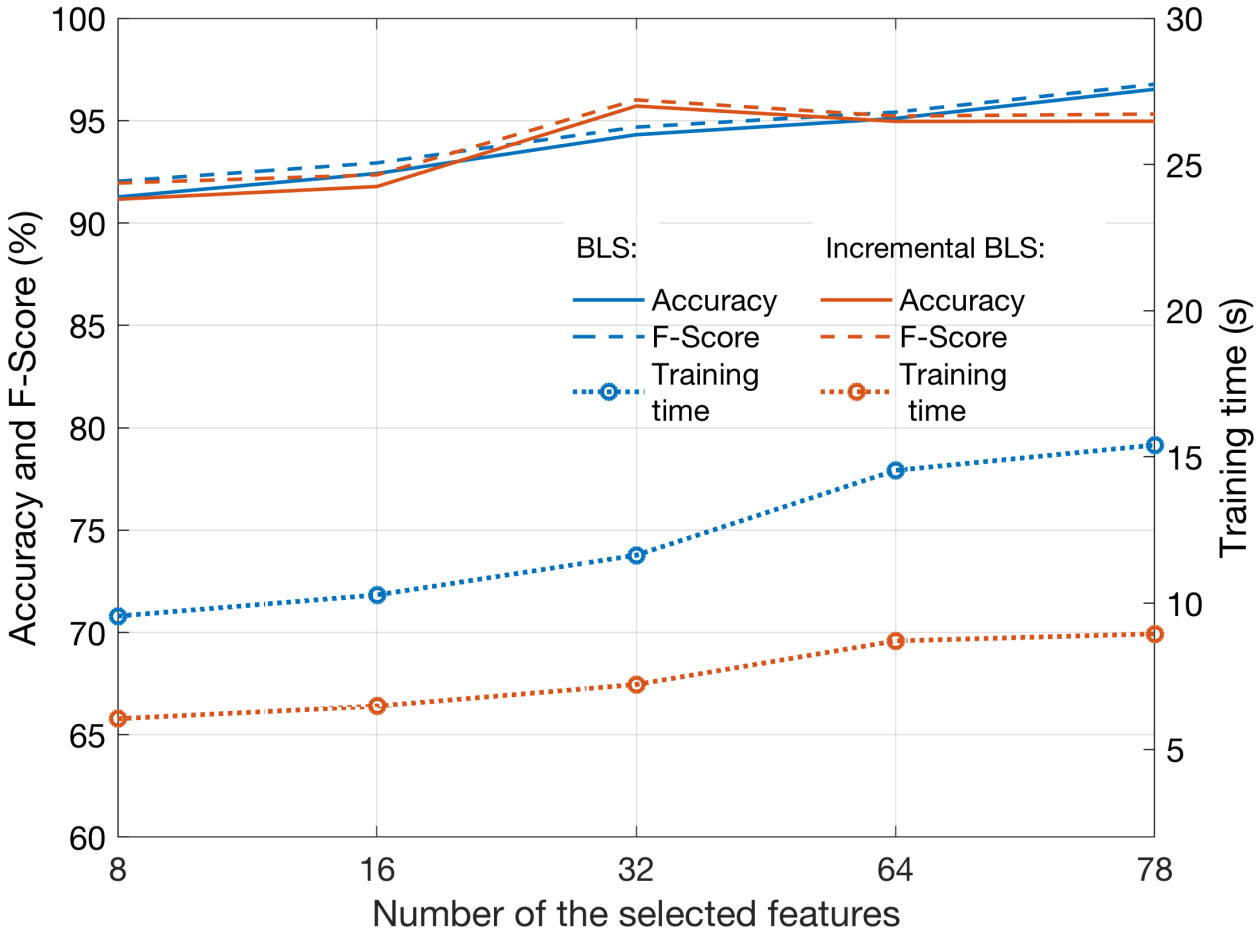
Best Performance: Non-Incremental BLS

Number of features	Dataset	Accuracy (%)	F-Score (%)	Model	Training time (s)
Non-Incremental BLS					
78	CICIDS2017	96.63	96.87	RBF-BLS	15.60
	CSE-CIC-IDS2018	97.46	81.46	CFBLS	4.13
64	CICIDS2017	96.10	96.35	BLS	8.97
	CSE-CIC-IDS2018	98.60	90.49	RBF-BLS	4.65
32	CICIDS2017	96.34	96.62	CEBLS	39.25
	CSE-CIC-IDS2018	98.83	92.26	CEBLS	33.46

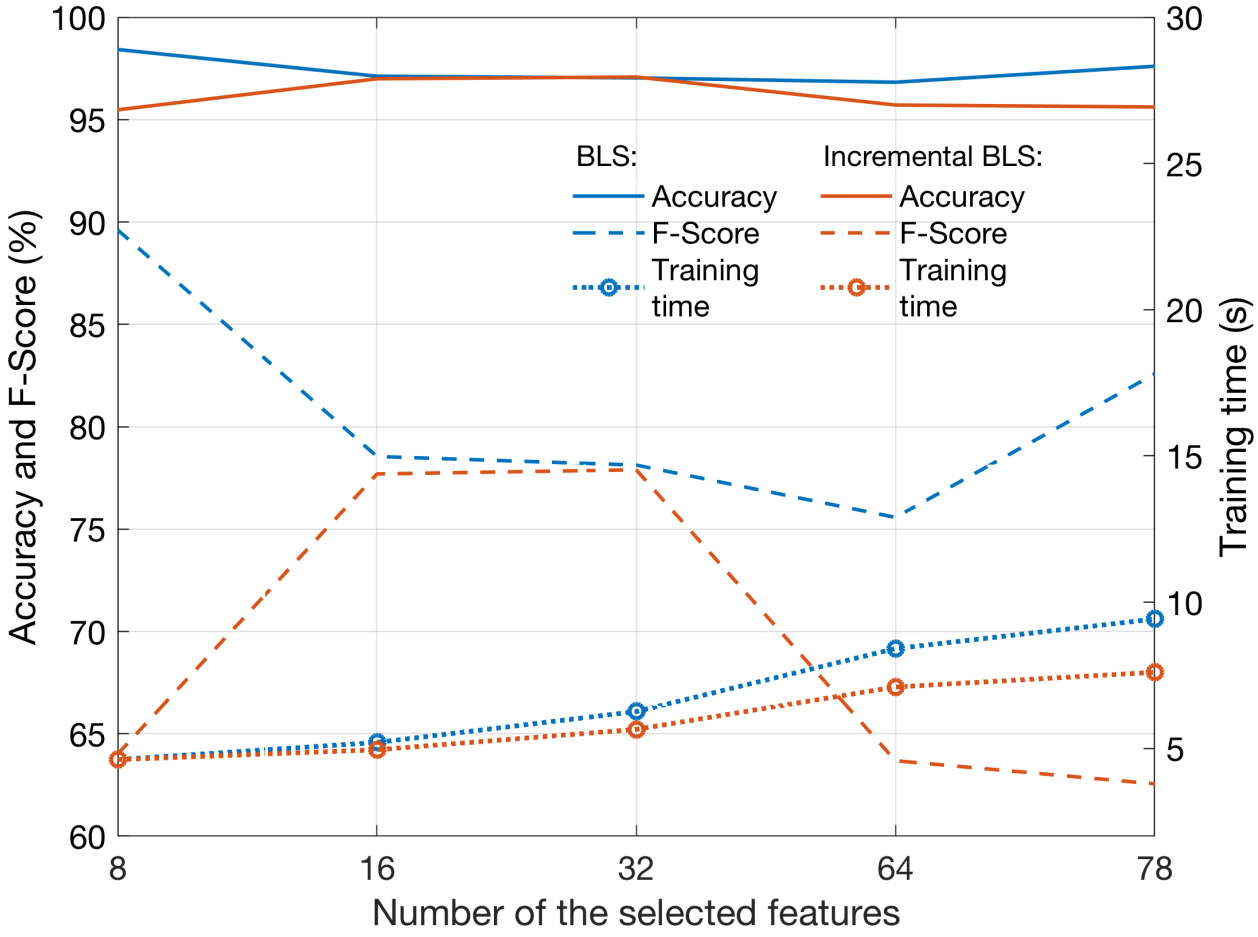
Best Performance: Incremental BLS

Number of features	Dataset	Accuracy (%)	F-Score (%)	Model	Training time (s)
Incremental BLS					
78	CICIDS2017	95.12	95.44	CFBLS	3.69
	CSE-CIC-IDS2018	97.47	81.35	BLS	6.78
64	CICIDS2017	94.44	95.38	BLS	7.39
	CSE-CIC-IDS2018	96.70	74.64	CFBLS	11.59
32	CICIDS2017	95.39	95.75	BLS	6.39
	CSE-CIC-IDS2018	97.08	77.89	BLS	5.65

Performance: BLS and Incremental BLS, CICIDS2017

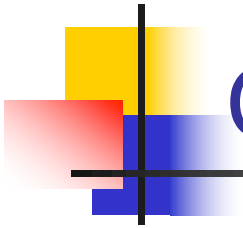


Performance: BLS and Incremental BLS, CSE-CIC-IDS2018



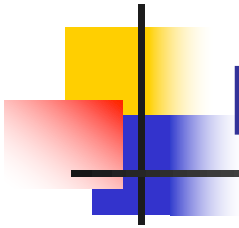
Roadmap

- Introduction
- Intrusion detection testbeds and datasets:
  - CICIDS2017
  - CSE-CIC-IDS2018
- Broad learning system and its extensions
- Experimental procedure and performance evaluation
- Conclusion and references



Conclusion

- We considered malicious intrusions and anomalies in communication networks and evaluated performance of machine learning algorithms
- Models using fewer number of features and models based on the incremental BLS required shorter training time
- Models exhibited comparable performance even when selecting a smaller number of relevant features
- Most generated models achieved accuracy and F-Score above 90%



Roadmap

- Introduction
- Intrusion detection testbeds and datasets:
  - CICIDS2017
  - CSE-CIC-IDS2018
- Broad learning system and its extensions
- Experimental procedure and performance evaluation
- Conclusion and references

References: Data Sources

- CICIDS2017:
  https://www.unb.ca/cic/datasets/ids-2017.html
- CSE-CIC-IDS2018:
  https://www.unb.ca/cic/datasets/ids-2018.html

References: Intrusion Detection and BLS

- M. C. Libicki, L. Ablon, and T. Webb, The Defenders Dilemma: Charting a Course Toward Cybersecurity. Santa Monica, CA, USA: RAND Corporation, 2015.
- V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: a survey,” *ACM Comput. Surv.,* vol. 41, no. 3, pp. 15:1–15:58, July 2009.

- Broadlearning: http://www.broadlearning.ai
- C. L. P. Chen, Z. Liu, and S. Feng, “Universal approximation capability of broad learning system and its structural variations,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 4, pp. 1191–1204, Apr. 2019.
- C. L. P. Chen and Z. Liu, “Broad learning system: an effective and efficient incremental learning system without the need for deep architecture,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 1, pp. 10–24, Jan. 2018.

Publications: http://www.sfu.ca/~ljilja/cnl

- Z. Li, A. L. Gonzalez Rios, and Lj. Trajković, “Detecting Internet worms, ransomware, and blackouts using recurrent neural networks,” in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC 2020)*, Toronto, Canada, Oct. 2020.
- Z. Li, A. L. Gonzalez Rios, G. Xu, and Lj. Trajković, “Machine learning techniques for classifying network anomalies and intrusions,” in *Proc. IEEE Int. Symp. Circuits and Systems*, Sapporo, Japan, May 2019, pp. 1–5.
- A. L. Gonzalez Rios, Z. Li, G. Xu, A. Dias Alonso, and Lj. Trajković, “Detecting Network Anomalies and Intrusions in Communication Networks,” in *Proc. 23rd IEEE International Conference on Intelligent Engineering Systems 2019*, Gödöllő, Hungary, Apr. 2019, pp. 29–34.
- Z. Li, P. Batta, and Lj. Trajković, “Comparison of machine learning algorithms for detection of network intrusions,” in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC 2018)*, Miyazaki, Japan, Oct. 2018, pp. 4248–4253.
- P. Batta, M. Singh, Z. Li, Q. Ding, and Lj. Trajković, “Evaluation of support vector machine kernels for detecting network anomalies,” in *Proc. IEEE Int. Symp. Circuits and Systems*, Florence, Italy, May 2018, pp. 1–4.
- Q. Ding, Z. Li, S. Haeri, and Lj. Trajković, “Application of machine learning techniques to detecting anomalies in communication networks: Datasets and Feature Selection Algorithms” in *Cyber Threat Intelligence,* M. Conti, A. Dehghantanha, and T. Dargahi, Eds., Berlin: Springer, pp. 47–70, 2018.

Publications: http://www.sfu.ca/~ljilja/cnl

- Q. Ding, Z. Li, S. Haeri, and Lj. Trajković, “Application of machine learning techniques to detecting anomalies in communication networks: Classification Algorithms” in *Cyber Threat Intelligence,* M. Conti, A. Dehghantanha, and T. Dargahi, Eds., Berlin: Springer, pp. 71–92, 2018.
- Q. Ding, Z. Li, P. Batta, and Lj. Trajković, “Detecting BGP anomalies using machine learning techniques,” in *Proc. IEEE Int. Conf. Syst., Man, and Cybern. (SMC 2016),* Budapest, Hungary, Oct. 2016, pp. 3352–3355.
- Y. Li, H. J. Xing, Q. Hua, X.-Z. Wang, P. Batta, S. Haeri, and Lj. Trajković, “Classification of BGP anomalies using decision trees and fuzzy rough sets,” in *Proc. IEEE Int. Conf. Syst., Man, Cybern.* (*SMC 2014)*, San Diego, CA, October 2014, pp. 1312–1317.
- N. Al-Rousan, S. Haeri, and Lj. Trajković, “Feature selection for classification of BGP anomalies using Bayesian models,” in *Proc. Int. Conf. Mach. Learn. Cybern. (ICMLC 2012)*, Xi'an, China, July 2012, pp. 140–147.
- N. Al-Rousan and Lj. Trajković, “Machine learning models for classification of BGP anomalies,” in *Proc. IEEE Conf. High Perform. Switching Routing* (*HPSR 2012)*, Belgrade, Serbia, June 2012, pp. 103–108.