Enhancing Cyber Defense: Using Machine Learning Algorithms for Detection of Network Anomalies

Zhida Li* and Ljiljana Trajković‡

*New York Institute of Technology
Vancouver, British Columbia, Canada

‡Communication Networks Laboratory
http://www.sfu.ca/~ljilja/cnl
Simon Fraser University
Vancouver, British Columbia, Canada

IEEE SMC 2023
Oahu, Hawaii

Roadmap

- Introduction
- CyberDefense tool:
  - high-level architecture
  - implementation
- Experiments and performance evaluation:
  - real-time detection: BGP routing traffic
  - off-line classification: power outage and ransomware attacks
- Conclusions and References

Roadmap

- Introduction
- CyberDefense tool:
  - high-level architecture
  - implementation
- Experiments and performance evaluation:
  - real-time detection: BGP routing traffic
  - off-line classification: power outage and ransomware attacks
- Conclusions and References

Motivation

- Network anomalies and their effect on performance of communication networks have dire economic consequences
- Identifying these anomalous events and their causes is an important step in preventing anomalous routing that affects performance of the Internet border gateway protocol (BGP)
- Classification of anomalous events helps alleviate their effects on network performance

Machine learning algorithms

- Various machine learning algorithms and tools have been used to analyze and classify network anomalies:
  - Internet worms, denial of service attacks, power outages, ransomware attacks
- Machine learning algorithms have been successfully implemented in various intrusion detection systems:
  - support vector machine, naïve Bayes, decision tree, hidden Markov model, extreme learning machine, multilayer perceptron
  - convolutional neural networks, recurrent neural networks, autoencoders
  - broad learning systems
  - gradient boosting decision trees

Intrusion detection systems

- Intrusion detection systems (IDSs) have been implemented as real-time or off-line software tools:
  - Snort, Passban, VMGuard, SwiftIDS, WisdomSDN
- Commercial tools:
  - BGProtect
  - intrusion prevention systems:
    - Cisco
    - FortiGuard
    - Palo Alto Networks advanced threat prevention

Snort: https://www.snort.org
BGProtect: https://www.bgprotect.com
Cisco IPS: https://www.cisco.com/c/en ca/products/security/ngips/index.html
FortiGuard IPS: https://www.fortinet.com/products/ips
Palo Alto Networks IPS: https://www.paloaltonetworks.com/network-security/advanced-threat-prevention

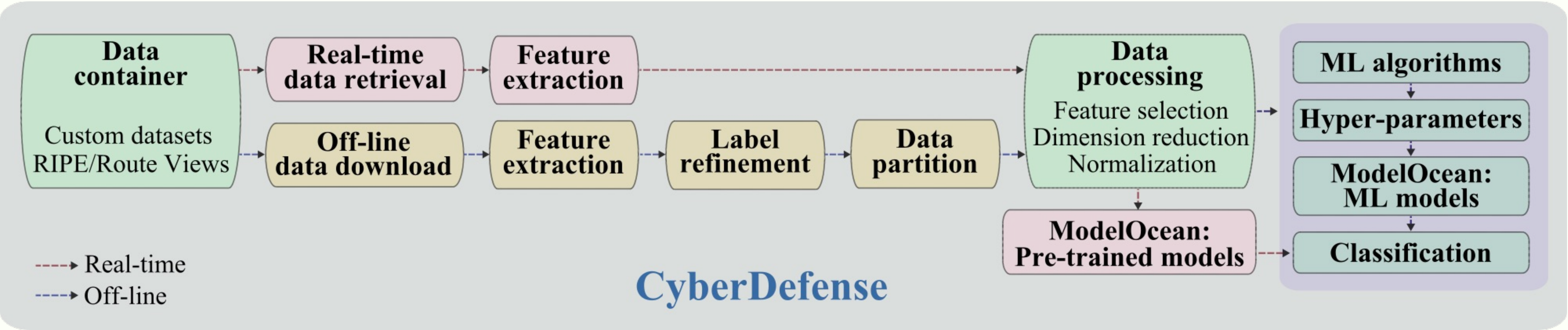
Roadmap

- Introduction
- CyberDefense tool:
  - high-level architecture
  - implementation
- Experiments and performance evaluation:
  - real-time detection: BGP routing traffic
  - off-line classification: power outage and ransomware attacks
- Conclusions and References

CyberDefense

- CyberDefense: integrates various stages of the anomaly detection process
- Modules:
  - data container, real-time data retrieval, off-line data download, feature extraction, label refinement, data partitioning, data processing, machine learning algorithms, hyper-parameter selection, model ocean, and classification
- Includes:
  - real-time anomaly detection and off-line classification based on machine learning algorithms
  - processing datasets based on connection and flow records to create models of intrusion attacks

CyberDefense: architecture



https://github.com/zhida-li/CyberDefense

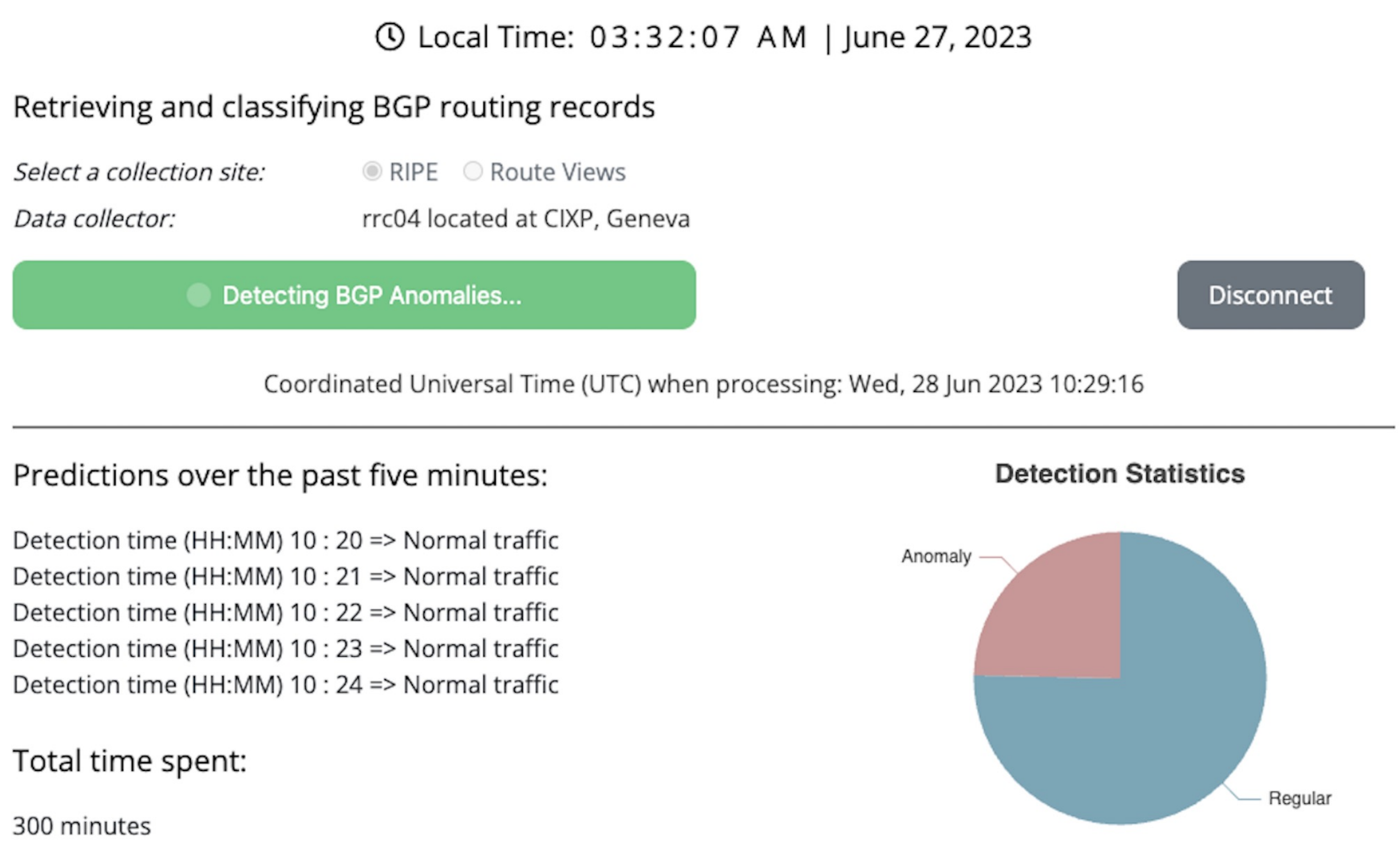
CyberDefense: implementation

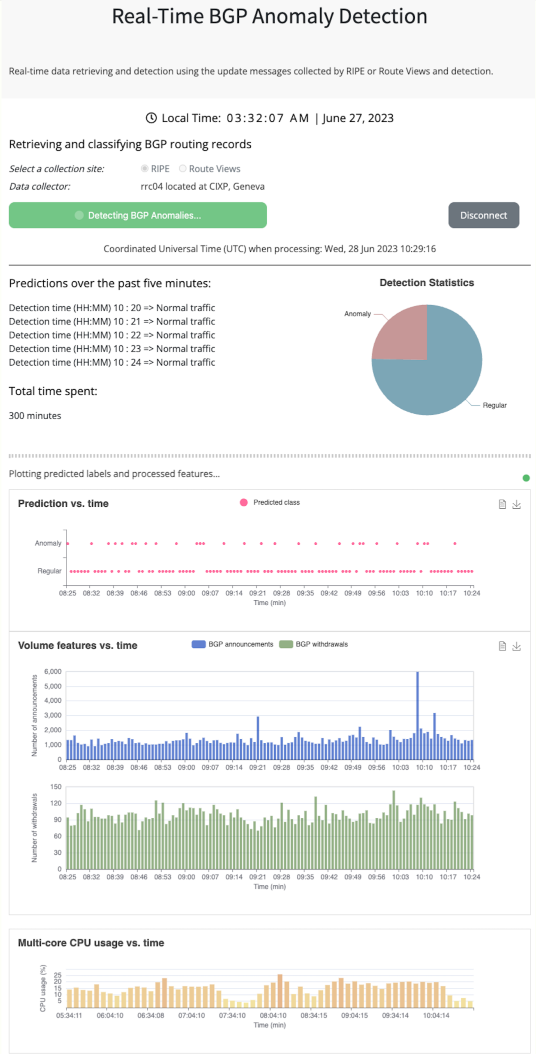
- CyberDefense:
  - offers an interactive interface for monitoring and performing experiments
  - executable on PCs and low-power devices (Raspberry Pi)
- Front-end:
  - HTML
  - Cascading style sheets (CSS): Bootstrap (open-source CSS framework)
  - Socket.IO:
    - transport protocol written in JavaScript for real-time web applications
- Back-end:
  - Flask (Python-based micro web framework)

Roadmap

- Introduction
- CyberDefense tool:
  - high-level architecture
  - implementation
- Experiments and performance evaluation:
  - real-time detection: BGP routing traffic
  - off-line classification: power outage and ransomware attacks
- Conclusions and References

Real-time detection: BGP routing traffic





Datasets

- Réseaux IP Européens (RIPE) and Route Views:
  - Code Red (2001), Nimda (2001), Slammer（2003)
  - Moscow blackout (2005), Pakistan power outage (2021)
  - WannaCrypt (2017), WestRock (2021)
- NSL-KDD (an improvement of the KDD'99 dataset)
- Canadian Institute for Cybersecurity (CIC) collections: CICIDS2017, CSE-CIC-IDS2018, CICDDoS2019
- Various custom datasets

BGP anomalies: power outages

- Pakistan power outage (2021):
  - caused by a cascading effect after an abrupt frequency drop in the power transmission system of the Guddu power plant
  - decreased network connectivity levels in Pakistan to:
    - 62 % within the first hour
    - 52 % after six hours

BGP anomalies: ransomware attacks

- WannaCrypt (2017):
  - malicious attackers encrypted data files
  - ransom was requested
- WestRock (2021):
  - impacted the company’s information and operational technology systems for over six days
  - caused delays in shipments and production levels

Best model parameters: BLS

	Incr. RBF-BLS, Incr. CEBLS
Incremental learning steps	WannaCrypt, WestRock: 2 (RIPE, Route Views)
Data points/step	WannaCrypt: 1,260 (RIPE), 840 (Route Views)
	WestRock: 1,972 (RIPE), 1,195 (Route Views)
Enhancement nodes/step	WannaCrypt, WestRock: 20 (RIPE), 40 (Route Views)

Best model parameters: VFBLS, VCFBLS

	Incr. VFBLS, Incr. VCFBLS
Incremental learning steps	WannaCrypt, WestRock: 2 (RIPE, Route Views)
Data points/step	WannaCrypt: 315 (RIPE), 210 (Route Views)
	WestRock: 448 (RIPE), 229 (Route Views)
Feature weight for initial step	WannaCrypt, WestRock: 0.9 (RIPE, Route Views)
Enhancement nodes/step	WannaCrypt, WestRock: 20 (RIPE, Route Views)

Best model parameters:
XGBoost, LightGBM, CatBoost

	XGBoost, LightGBM, CatBoost
Number of estimators	300, 300, 200
Learning rate	0.1 (none)/0.01 (iForest), 0.05, 0.05

Best performance: Pakistan power outage

Model		Collection site	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)
CNN	No refinement	RIPE	51.00	84.93	7.00	4.64	14.17
		Route Views	52.01	95.00	3.82	8.11	2.50
	k-means	RIPE	50.99	93.50	4.88	5.62	4.31
		Route Views	52.00	95.87	1.59	12.50	0.85
	Isolation forest	RIPE	50.81	86.53	8.18	5.63	15.00
		Route Views	57.15	83.37	6.03	3.89	13.33

Best performance: Pakistan power outage

Model		Collection site	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)
$LSTM_4$	No refinement	RIPE	45.05	92.83	4.44	4.76	4.17
		Route Views	42.29	95.77	14.77	37.93	9.17
$LSTM_2$	k-means	RIPE	32.42	93.93	7.14	8.75	6.03
		Route Views	32.15	95.70	12.24	31.03	7.63
GRU_3	Isolation forest	RIPE	66.47	93.03	3.69	4.12	3.33
$LSTM_4$		Route Views	41.93	95.83	14.97	40.74	9.17

Best performance: Pakistan power outage

Model		Collection site	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)
Bi-$LSTM_2$	No refinement	RIPE	25.83	95.57	9.52	25.93	5.83
Bi-GRU_2		Route Views	41.92	95.60	2.94	12.50	1.67
Bi-$LSTM_3$	k-means	RIPE	29.94	95.57	11.92	25.71	7.76
Bi-$LSTM_2$		Route Views	43.37	95.73	3.03	14.29	1.69
Bi-GRU_3	Isolation forest	RIPE	27.71	95.90	8.89	40.00	5.00
Bi-$LSTM_2$		Route Views	43.40	95.77	3.05	18.18	1.67

Best performance: Pakistan power outage

Model		Collection site	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)
LightGBM	No refinement	RIPE	0.04	95.87	3.13	25.00	1.60
		Route Views	0.05	94.30	5.59	8.47	4.17
	k-means	RIPE	0.01	93.00	7.08	7.27	6.90
		Route Views	0.11	93.77	6.97	8.43	5.93
	Isolation forest	RIPE	0.01	94.33	6.59	9.68	5.00
		Route Views	0.04	91.90	6.90	6.38	7.50

Best performance: WannaCrypt

Model		Collection site	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)
RBF-BLS	No refinement	RIPE	3.67	55.73	56.68	50.48	64.62
Incr. CEBLS		Route Views	16.73	56.65	63.97	50.98	85.85
RBF-BLS	Isolation forest	RIPE	1.02	55.61	56.46	50.37	64.22
Incr. CEBLS		Route Views	14.81	56.82	60.98	51.24	75.29

Best performance: WannaCrypt

Model		Collection site	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)
VFBLS	No refinement	RIPE	6.49	55.06	46.07	49.85	42.82
Incr. VFBLS		Route Views	4.86	56.82	64.10	51.10	85.98
VFBLS	Isolation forest	RIPE	6.36	55.04	46.06	49.80	42.84
Incr. VFBLS		Route Views	4.83	57.09	64.10	51.27	85.46

Best performance: WannaCrypt

Model		Collection site	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)
CatBoost	No refinement	RIPE	1.09	60.31	62.04	54.30	72.35
XGBoost		Route Views	0.87	53.05	59.56	48.51	77.14
LightGBM	Isolation forest	RIPE	0.15	66.08	61.41	54.17	70.88
		Route Views	0.23	52.38	58.95	48.02	76.31

Best performance: WestRock

Model		Collection site	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)
Incr. RBF-BLS	No refinement	RIPE	1.71	58.20	73.55	58.18	99.98
Incr. CEBLS		Route Views	23.33	57.89	73.31	58.05	99.48
Incr. RBF-BLS	Isolation forest	RIPE	33.28	58.20	73.54	58.16	99.98
		Route Views	7.01	58.15	73.52	58.16	99.93

Best performance: WestRock

Model		Collection site	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)
Incr. VCFBLS	No refinement	RIPE	12.04	58.23	73.57	58.19	99.98
		Route Views	9.08	58.30	73.57	58.25	99.85
Incr. VFBLS	Isolation forest	RIPE	11.60	58.27	73.55	58.23	99.80
		Route Views	7.62	58.20	73.55	58.18	99.98

Best performance: WestRock

Model		Collection site	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)
XGBoost	No refinement	RIPE	0.54	60.44	73.38	60.26	93.80
CatBoost		Route Views	0.31	58.17	73.53	58.16	99.95
XGBoost	Isolation forest	RIPE	0.52	59.84	73.05	59.88	93.62
CatBoost		Route Views	0.48	58.24	73.53	58.22	99.78

Roadmap

- Introduction
- CyberDefense tool:
  - high-level architecture
  - implementation
- Experiments and performance evaluation:
  - real-time detection: BGP routing traffic
  - off-line classification: power outage and ransomware attacks
- Conclusions and References

Conclusions

- Machine learning models have been compared using datasets collected during a power outage (Pakistan power outage) and ransomware attacks (WannaCrypt, WestRock)
- Model performance is attributed to the nature of the anomalous events and the unique characteristics of each dataset
- The CyberDefense tool was used to classify various network anomalies using deep learning and fast machine learning algorithms
- CyberDefense enables real-time and off-line detection of anomalies based on routing records downloaded from RIPE and Route Views collection sites and custom datasets

Roadmap

- Introduction
- CyberDefense tool:
  - high-level architecture
  - implementation
- Experiments and performance evaluation:
  - real-time detection: BGP routing traffic
  - off-line classification: power outage and ransomware attacks
- Conclusions and References

References: data sources and tools

- RIPE NCC: https://www.ripe.net
- University of Oregon Route Views project: http://www.routeviews.org
- CIC datasets: https://www.unb.ca/cic/datasets/index.html
- CyberDefense:
  https://github.com/zhida-li/CyberDefense
- BGProtect:
  https://www.bgprotect.com
- Secure IPS (NGIPS):
  https://www.cisco.com/c/en ca/products/security/ngips/index.html
- FortiGuard IPS Security Service:
  https://www.fortinet.com/products/ips
- Advanced Threat Prevention:
  https://www.paloaltonetworks.com/network-security/advanced-threat-prevention

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

Journal publications:

- Z. Li, A. L. Gonzalez Rios, and Lj. Trajkovic, “Machine learning for detecting the WestRock ransomware attack using BGP routing records,” *IEEE Communications* Magazine, vol. 61, no. 3, pp. 20–26, Mar. 2023.
- Z. Li, A. L. Gonzalez Rios, and Lj. Trajkovic, “Machine learning for detecting anomalies and intrusions in communication networks,” *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 7, pp. 2254-2264, July 2021.

Book chapters:

- 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.
- Z. Li, Q. Ding, 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.

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

Conference publications:

- H. Takhar and Lj. Trajković, “BGP feature properties and classification of Internet worms and ransomware attacks,” *IEEE Int. Conf. Syst., Man, Cybern.*, Honolulu, Hi, USA, Oct. 2023, to be presented.
- T. Sharma, K. Patni, Z. Li, and Lj. Trajković, “Deep echo state networks for detecting Internet worm and ransomware attacks” In Proc. *IEEE Int. Symp. Circuits Syst.*, Monterey, CA, USA, May 2023.
- Z. Li, A. L. Gonzalez Rios, and Lj. Trajković, “Classifying denial of service attacks using fast machine learning algorithms,” in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, Melbourne, Australia, Oct. 2021, pp. 1221-1226 (virtual).
- K. Bekshentayeva and Lj. Trajkovic, "Detection of denial of service attacks using echo state networks," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, Melbourne, Australia, Oct. 2021, pp. 1227-1232 (virtual).
- 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.*, Toronto, Canada, Oct. 2020, pp. 2165-2172 (virtual).
- A. L. Gonzalez Rios, Z. Li, K. Bekshentayeva, and Lj. Trajković, “Detection of denial of service attacks in communication networks,” in *Proc. IEEE Int. Symp. Circuits Syst.*, Seville, Spain, Oct. 2020 (virtual).

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

Conference publications:

- 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 Syst.*, Sapporo, Japan, May 2019 (virtual).
- 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 Int. Conf. Intell. Eng. Syst.*, 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.*, 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, P. Batta, and Lj. Trajković, "Detecting BGP anomalies using machine learning techniques," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.,* Budapest, Hungary, Oct. 2016, pp. 3352–3355.

Thank you!