Machine Learning for Detecting Network Anomalies and Intrusions

Dr. Zhida Li

zli74@nyit.edu

www.nyit.edu/bio/zli74 | zhidali.me

Department of Computer Science

New York Institute of Technology

Vancouver, British Columbia, Canada

NEW YORK INSTITUTE OF TECHNOLOGY

Vancouver

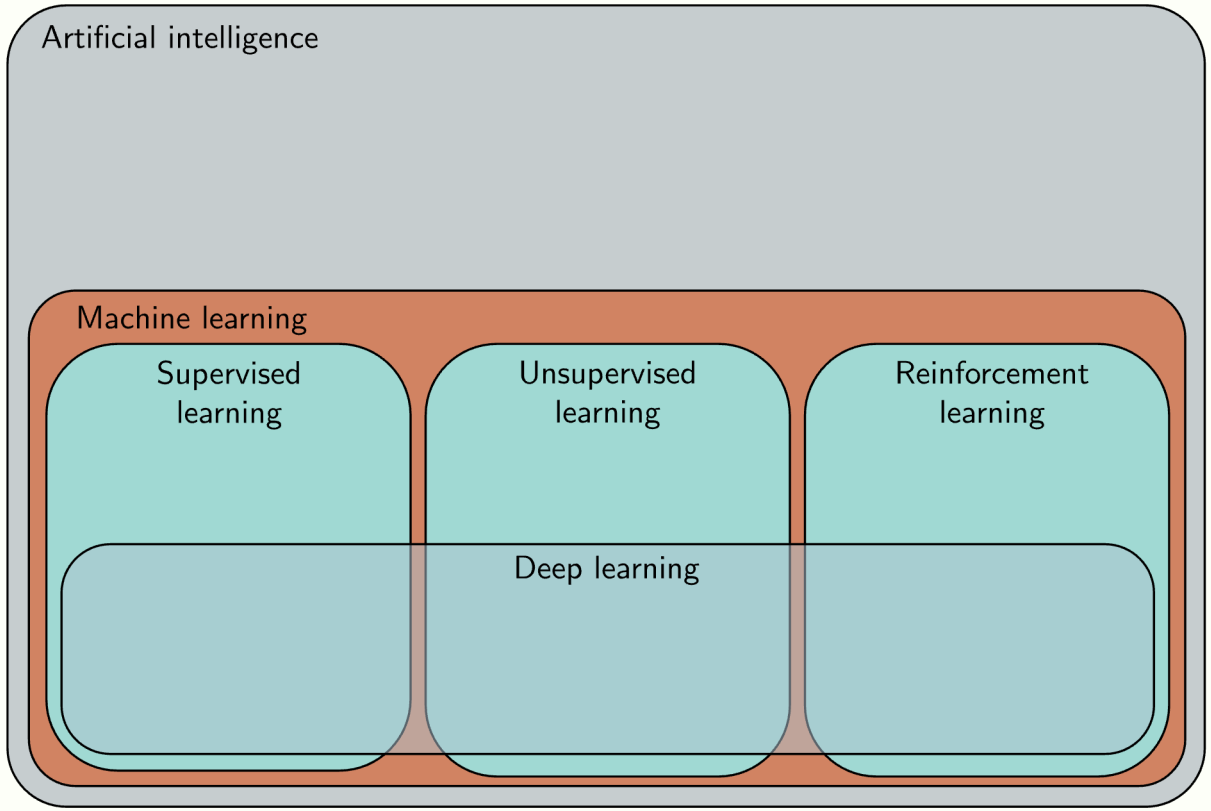
Roadmap

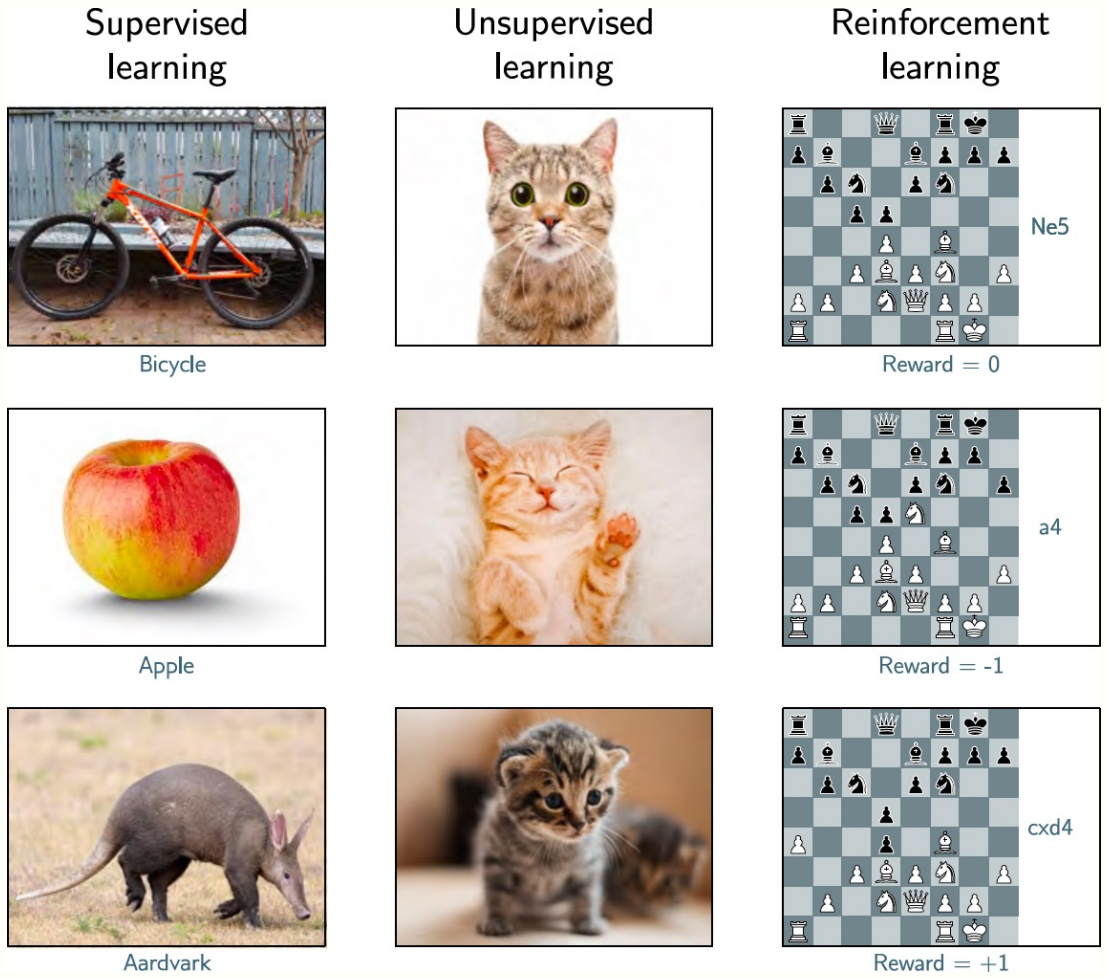
- Introduction
- Network anomalies and intrusions
- Applications of machine learning algorithms
- CyberDefense tool
- Conclusions and References

Roadmap

- Introduction
- Network anomalies and intrusions
- Applications of machine learning algorithms
- CyberDefense tool
- Conclusions and References

AI and machine learning





Motivation

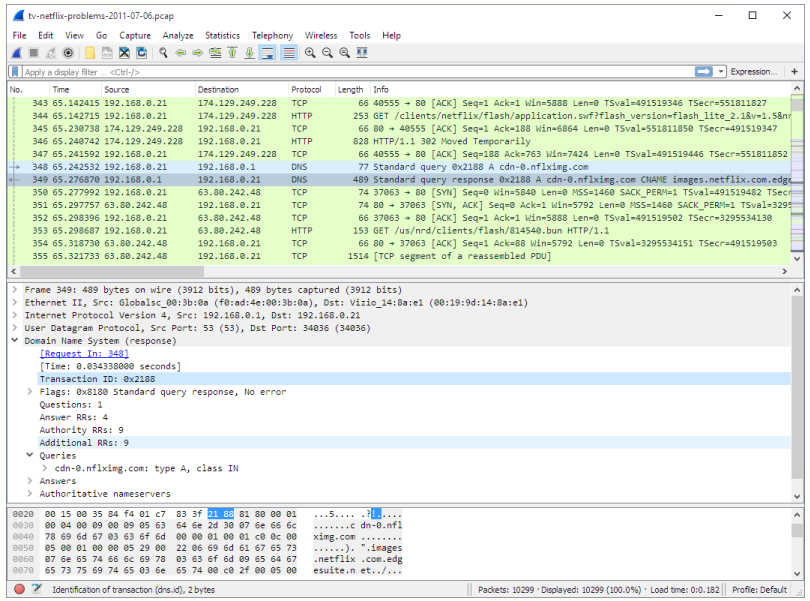
- The Internet is highly susceptible to failures and attacks
- Various machine learning models have been implemented to enhance cybersecurity
- Using machine learning techniques to detect network intrusions is an important topic in cybersecurity

Intrusion detection systems

- The Intrusion detection systems (IDS) monitors the traffic for malicious activities, sending alerts when suspicious activities are found
- Signature-based IDS
  - detects known attacks by comparing traffic against established rules and patterns
- Anomaly-based IDS:
  - detects both known and unknown intrusions by comparing traffic against a pre-defined baseline of behaviors

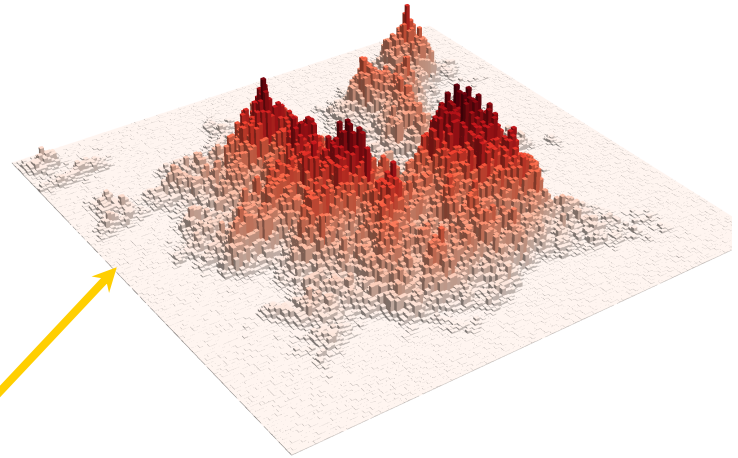
Cybersecurity: data transformation and analysis

Network raw data

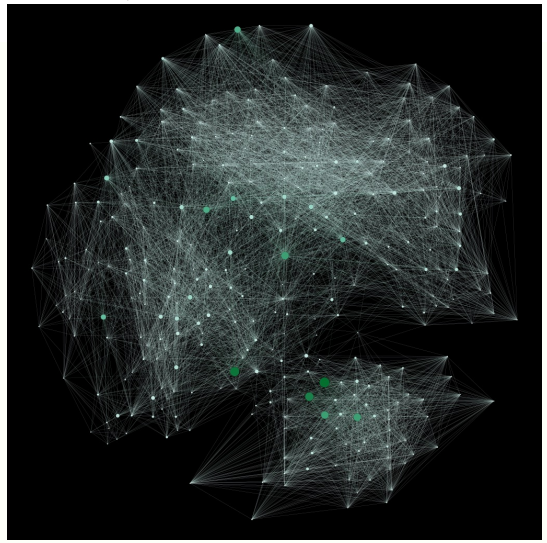


Field	Value
TIME	2022-1-16 01:40:06
TYPE	BGP4MP/BGP4MP_MESSAGE_AS4 AFI_IP
FROM	192.65.185.195
TO	192.65.185.40
BGP PACKET TYPE	UPDATE
ORIGIN	IGP
AS-PATH	15547 6939 4788 45259 10094 10030
NEXT-HOP	192.65.185.195
ANNOUNCED	183.171.121.0/24
ANNOUNCED	183.171.120.0/24

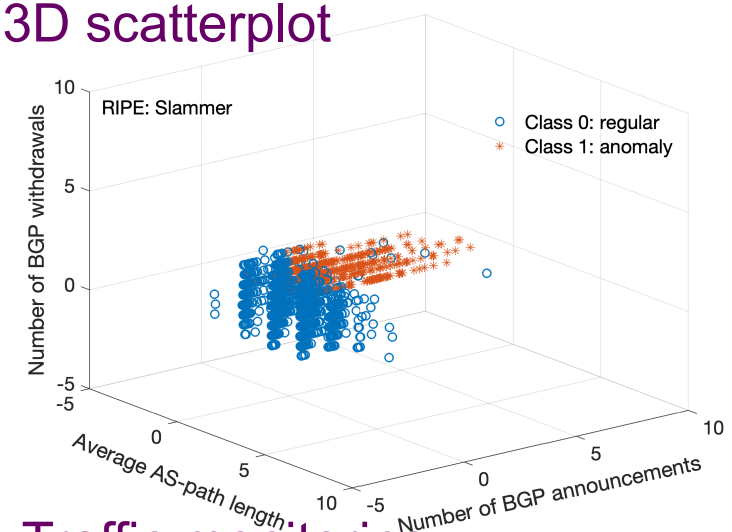
3D data



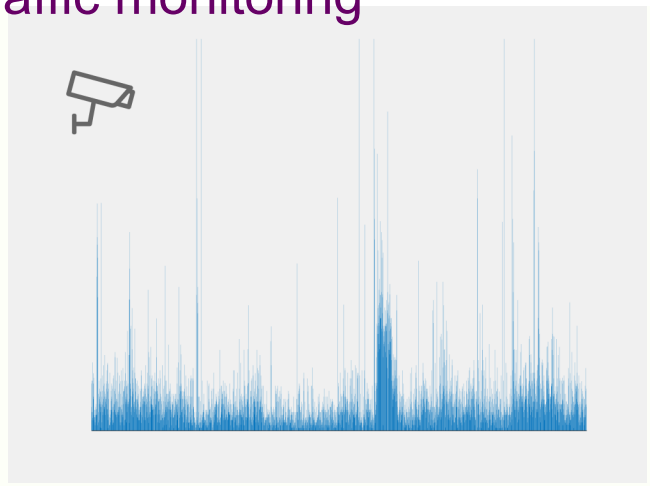
graph



3D scatterplot



Traffic monitoring



Machine learning techniques

- A variety of network-based intrusion detection systems (NIDSs) have been designed using:
  - supervised, unsupervised, and semi-supervised learning
- They help detect the malicious intentions of network users
- Detection of attacks:
  - require updating or retraining generated models to capture deviations from regular network activities
- Training time:
  - important for the decision-making process

Roadmap

- Introduction
- Network anomalies and intrusions
- Applications of machine learning algorithms
- CyberDefense tool
- Conclusions and References

Network traffic datasets

- Anomalies affect performance of the Internet Border Gateway Protocol (BGP)
- Réseaux IP Européens (RIPE) and Route Views:
  - Slammer（2003）, Nimda (2001), Code Red (2001)
  - 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
- UNSW-NB15
- BCNET

BGP anomalies: Internet worms

- Slammer (2003):
  - infected Microsoft SQL servers through a small piece of code that generated IP addresses at random
- Nimda (2001):
  - exploited vulnerabilities in the Microsoft Internet Information Services (IIS) web servers for Internet Explorer 5
- Code Red (2001):
  - attacked Microsoft IIS web servers by replicating itself through the IIS server weaknesses

BGP anomalies: power outages

- Moscow blackout (2005):
  - caused a complete shutdown of the Chagino substation of the Moscow energy ring
  - caused the failure of the Internet traffic exchange
- 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 and to 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

Network traffic datasets: data collection

- Route Views collector map: collectors are located in 5 RIR regions

https://www.routeviews.org/routeviews/map/

Network traffic datasets

BGP datasets:

- Anomalous data: days of the attack
- Regular data: two days prior and two days after the attack
- 37 numerical features from BGP update messages

Sample of a BGP *update* message

Field	Value
TIME	2022-1-16 01:40:06
TYPE	BGP4MP/BGP4MP_MESSAGE_AS4 AFI_IP
FROM	192.65.185.195
TO	192.65.185.40
BGP PACKET TYPE	UPDATE
ORIGIN	IGP
AS-PATH	15547 6939 4788 45259 10094 10030
NEXT-HOP	192.65.185.195
ANNOUNCED	183.171.121.0/24
ANNOUNCED	183.171.120.0/24

BGP datasets: Internet worms

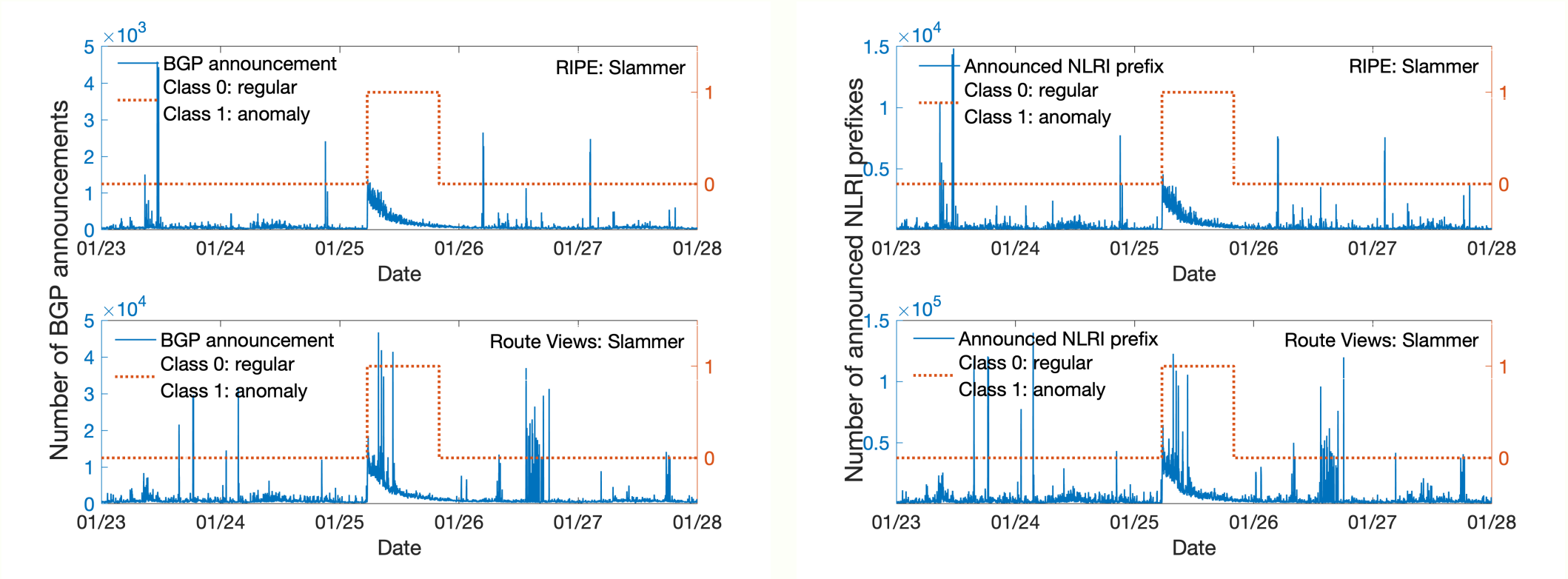
- Slammer, Nimda, Code Red:

Collection site	Dataset	Regular (min)	Anomaly (min)	Regular (training)	Anomaly (training)	Regular (test)	Anomaly (test)	Start	End
RIPE	Slammer	6,331	869	3,210	530	3,121	339	23.01.2003 00:00:00	27.01.2003 23:59:59
	Nimda	7,308	1,301	3,673	827	3,635	474	16.09.2001 00:00:00	21.09.2001 23:59:59
	Code Red	6,880	320	4,000	200	2,880	120	17.07.2001 00:00:00	21.07.2001 23:59:59
Route Views	Slammer	6,319	869	3,198	530	3,121	339	23.01.2003 00:00:00	27.01.2003 23:59:59

Route Views data collection began in 2003.

BGP dataset: Slammer (2003)

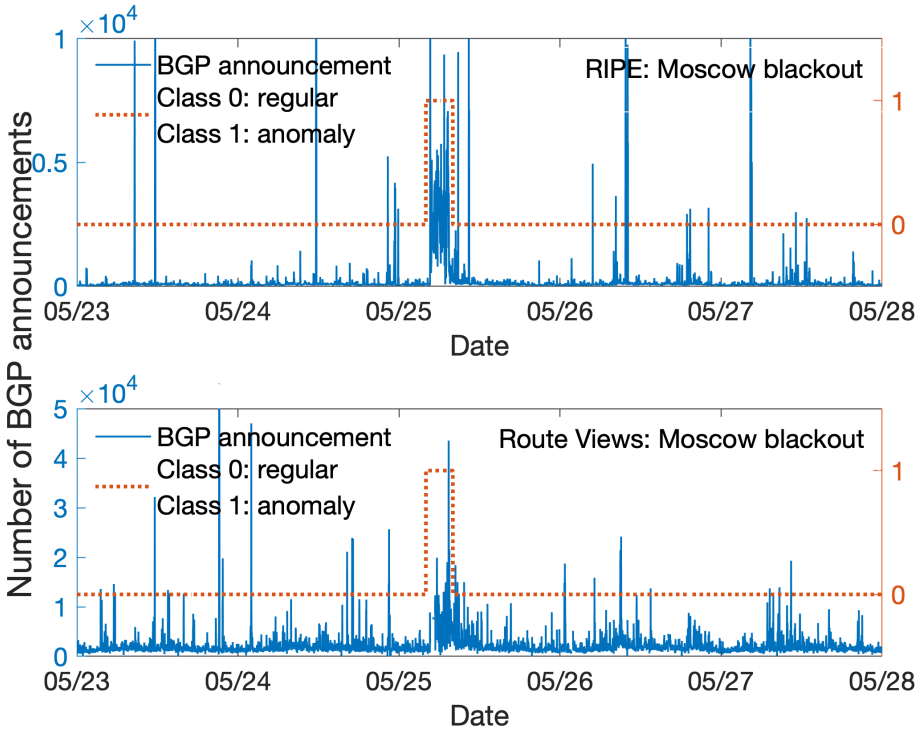
- Number of BGP announcements and announced NLRI prefixes vs. date:

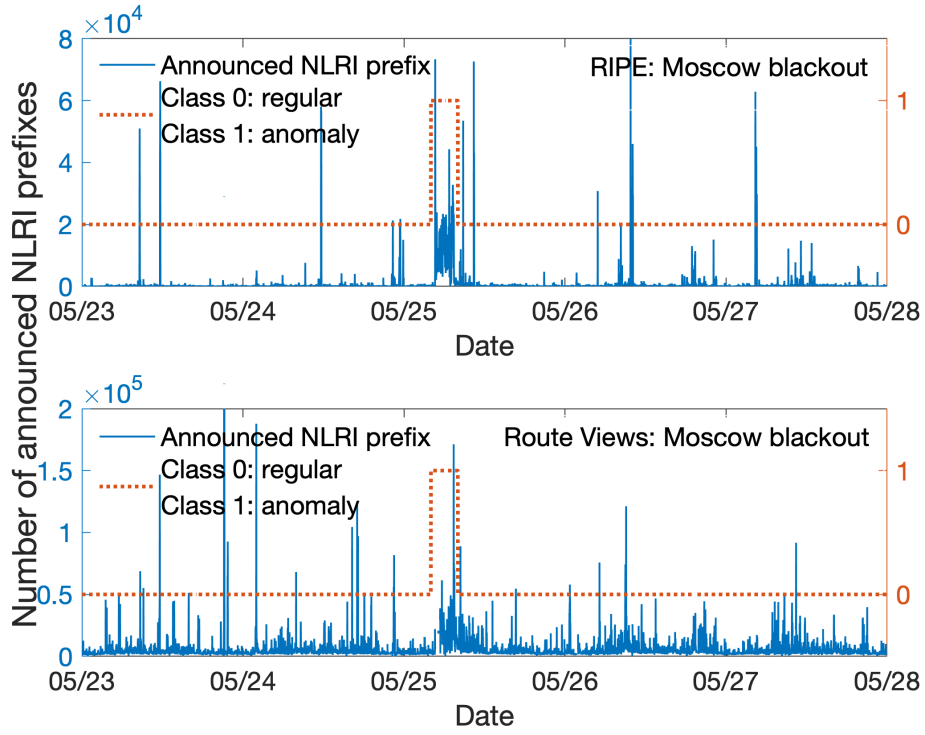


BGP: Border Gateway Protocol
NLRI: Network Layer Reachability Information

BGP dataset: Moscow blackout (2005)

- Number of BGP announcements and announced NLRI prefixes vs. date:

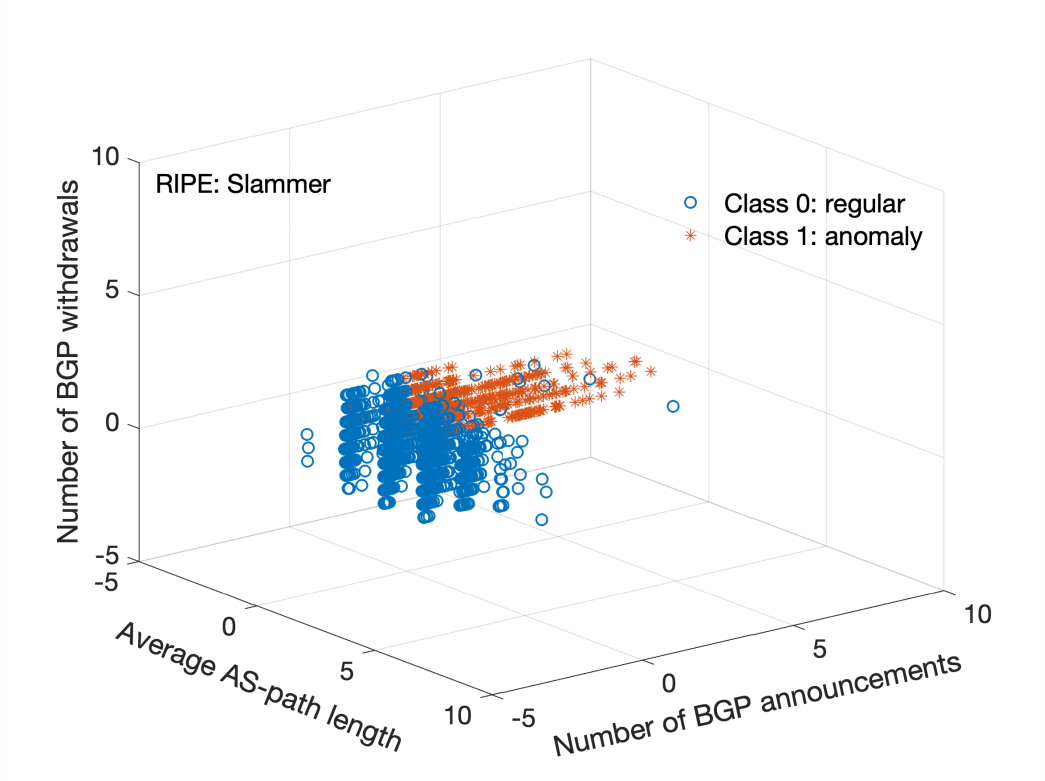




BGP: Border Gateway Protocol
NLRI: Network Layer Reachability Information

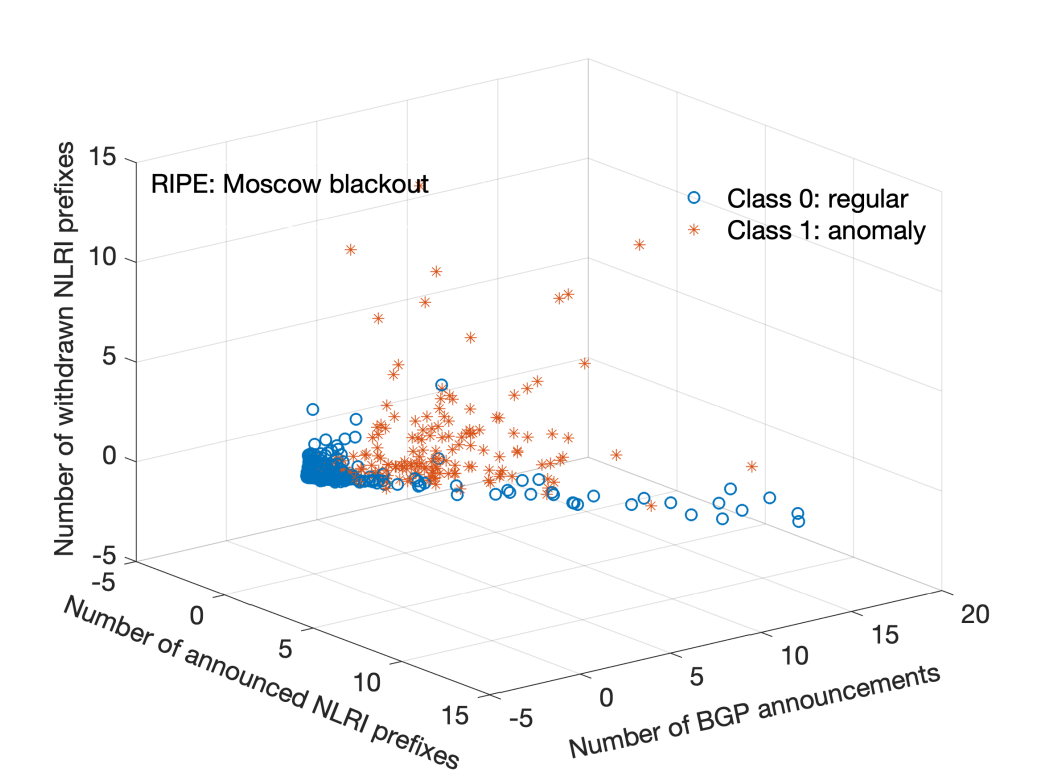
BGP dataset: Slammer

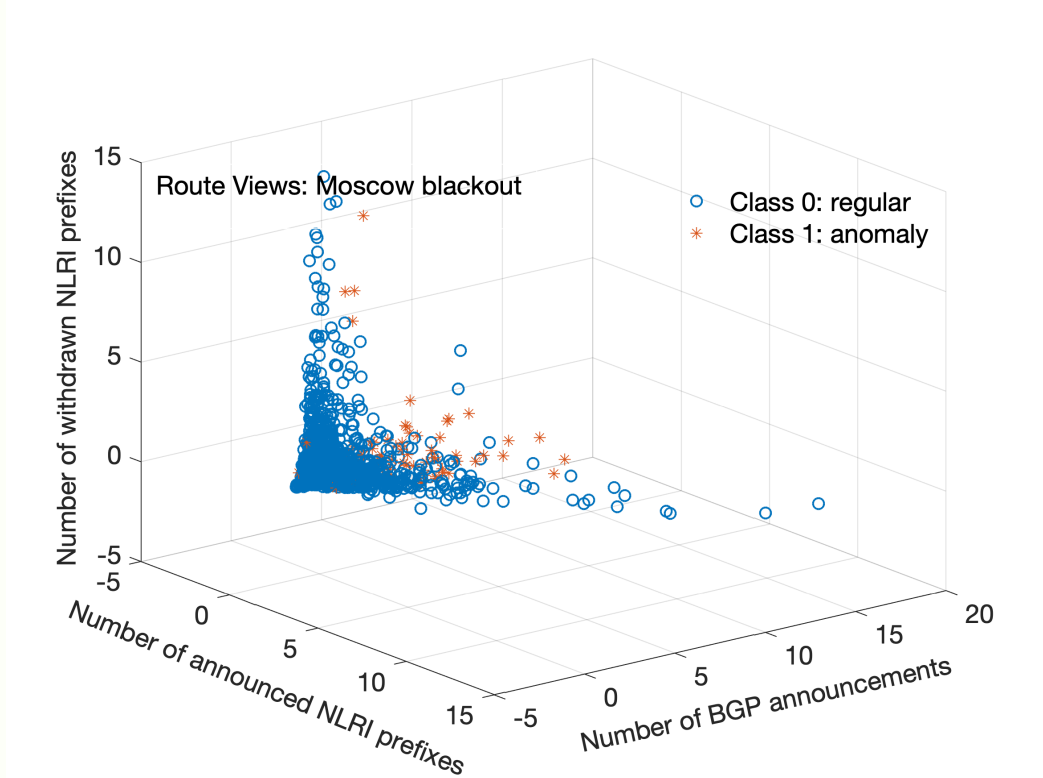
- Average AS-path length vs. number of BGP announcements vs. number of BGP withdrawals:



BGP dataset: Moscow blackout

- Number of announced NLRI prefixes vs. number of BGP announcements vs. number of withdrawn NLRI prefixes:





NSL-KDD datasets

- NSL-KDD dataset: an improvement of the KDD'99 dataset that was used in various intrusion detection systems
- NSL-KDD dataset: a benchmark used for evaluating anomaly detection and intrusion techniques

	Regular	DoS	U2R	R2L	Probe	Total
KDDTrain^{+}	67,343	45,927	52	995	11,656	125,973
KDDTest^{+}	9,711	7,458	200	2,754	2,421	22,544
KDDTest^{-21}	2,152	4,342	200	2,754	2,402	11,850

Canadian Institute for Cybersecurity datasets

CICIDS2017, CSE-CIC-IDS2018, and CICDDoS2019:

- Testbed used to create the publicly available dataset that includes multiple types of recent cyber attacks
- Dataset features: extracted from collected TCP and UDP network flows with a network traffic flow analyzer
- Each dataset: over 80 features including destination IP and port, protocol type, flow duration, and maximum/minimum packet size
- Network traffic collected:
  - Monday, 03.07.2017 to Friday, 07.07.2017
  - Wednesday, 14.02.2018 to Friday, 02.03.2018
  - Saturday, 03.11.2018 and Saturday, 01.12.2018

CIC datasets: DoS and DDoS attacks

- Application-layer DoS and TCP/UDP DDoS attacks

Dataset	Attack	Number of Data Points
	GoldenEye	10,293
CCIDS2017	Hulk	230,124
July 05, 2017	SlowHTTPTest	5,499
	Slowloris	5,796
CSE-CIC-IDS2018	GoldenEye	41,508
February 15, 2018	Slowloris	10,990
CICDDoS2019	Domain Name System	5,071,011
December 01, 2018	Lightweight Directory Access Protocol	2,179,930
	Network Time Protocol	1,202,642

UNSW-NB15 dataset

- Developed by the Cyber Range Lab of UNSW Canberra, the UNSW-NB15 dataset serves as a benchmark for research in network intrusion detection systems:
  - includes a mixture of real contemporary normal activities and synthetic attack behaviors
  - 49 features divided into categories such as flow, basic, content, time, additional generated, and labeled features
- Distribution of normal and attacks in the UNSW-NB15 dataset:

Value	Counts	Percentage
Normal	2,218,764	87.35 %
Attack	321,283	12.65 %

UNSW-NB15 dataset

- Nine types of attacks: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms

Attack Type	Counts	Percentage
Normal	2,218,764	87.35 %
Generic	215,481	8.48 %
Exploits	44,525	1.75 %
Fuzzers	24,246	0.95 %
DoS	16,353	0.64 %
Reconnaissance	13,987	0.55 %
Analysis	2,677	0.11 %
Backdoors	2,329	0.09 %
Shellcode	1,511	0.06 %
Worms	174	0.01 %

Roadmap

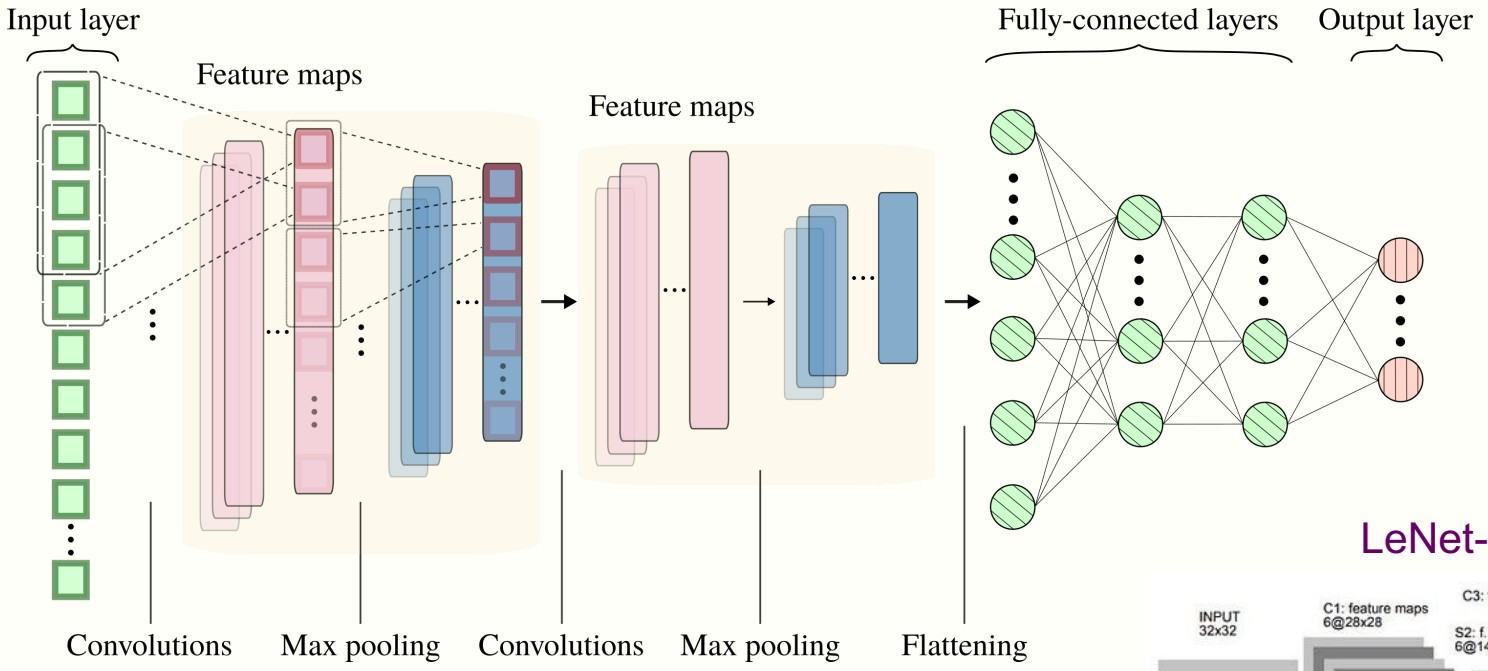
- Introduction
- Network anomalies and intrusions
- Applications of machine learning algorithms
- CyberDefense tool
- Conclusions and References

Machine learning algorithms

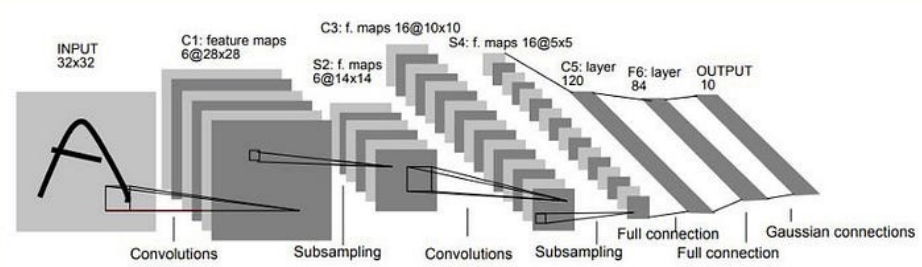
- Various machine learning algorithms and tools have been used to analyze and classify network anomalies:
  - Internet worms, denial of service attacks, power outages, ransomware attacks
- Machine learning algorithms have been successfully implemented in various intrusion detection systems:
  - support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

Convolutional neural network

- High-level structure of a CNN using one-dimensional input data:

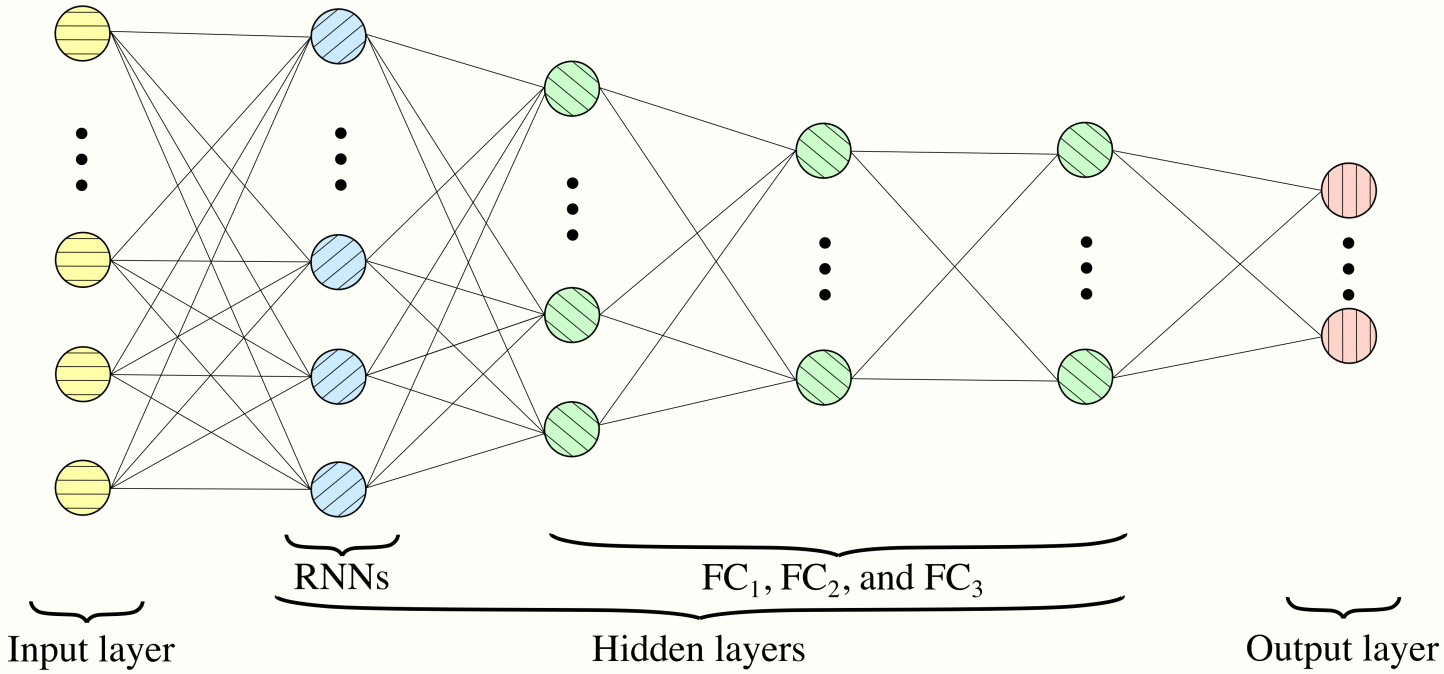


LeNet-5 CNN architecture



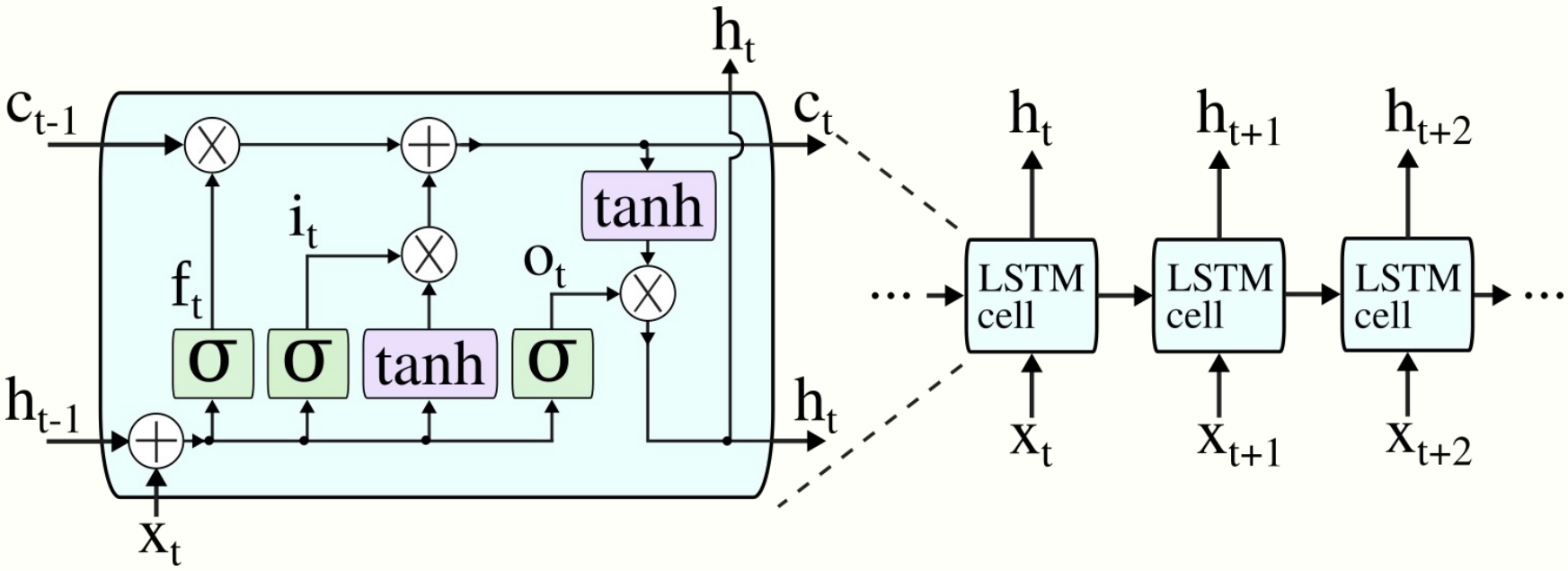
Deep learning neural network

- 37 (BGP)/109 (NSL-KDD) RNNs, 64 FC_1, 32 FC_2, and 16 FC_3 fully connected (FC) hidden nodes:



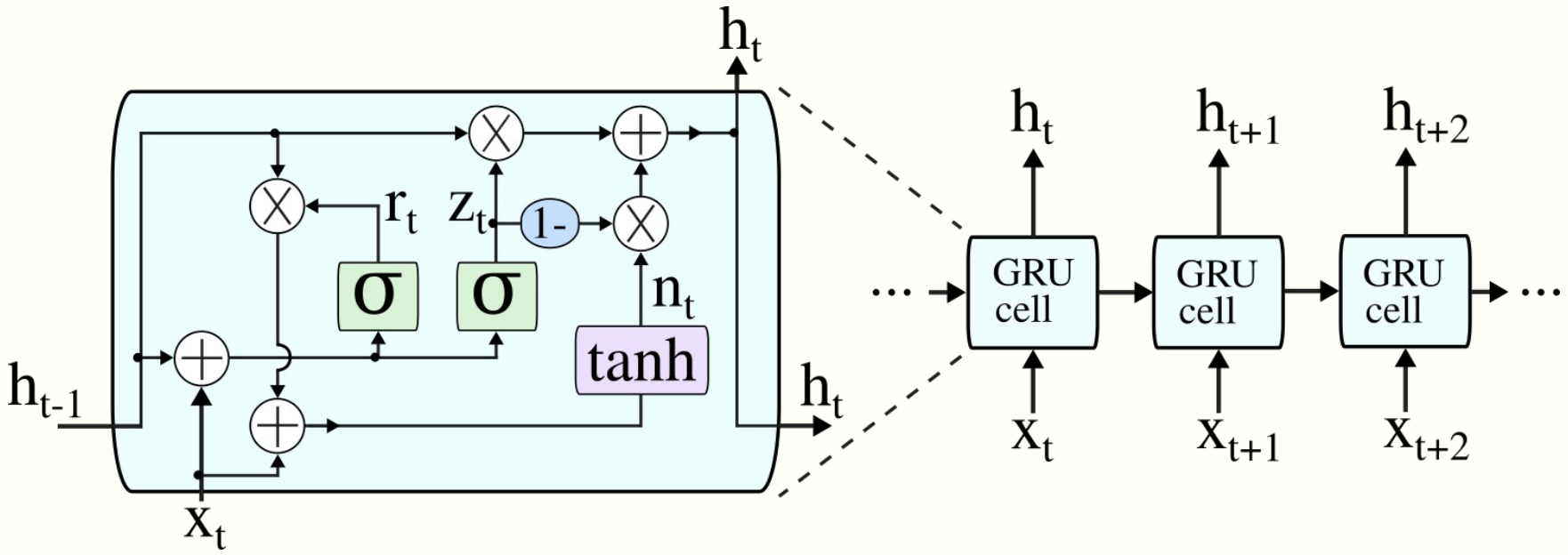
Long short-term memory: LSTM

- Repeating module for the LSTM neural network:



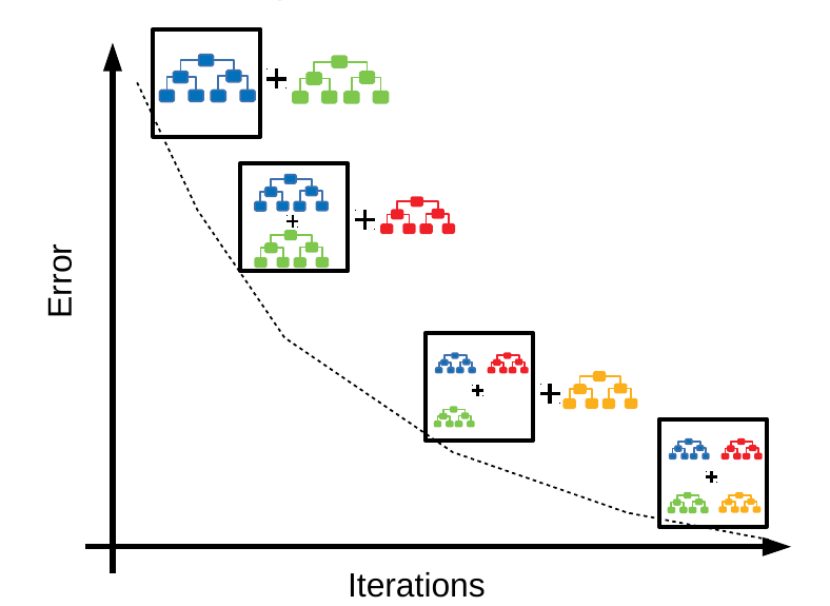
Gated recurrent unit: GRU

- Repeating module for the GRU neural network:



Gradient boosting machines

- Gradient boosting machines (GBMs): boosting algorithms that employ functional gradient descent to minimize the loss function
- GBDT: GBM variant that employs decision trees as estimators
- Generating a gradient boosting model:



https://medium.com/swlh/gradient-boosting-trees-for-classification-a-beginners-guide-596b594a14ea

Gradient boosting decision trees: GBDT

- When training a GBDT model with K estimators using N data points, the predicted output for the i^{th} data point $\boldsymbol{x}_i$ is:

$$\hat{\mathrm{y}}_i = \sum_{k=1}^{K} f_k(\boldsymbol{x}_i),$$

where:

- f_k: the k^{th} decision tree
- $\boldsymbol{x}_i$: a row vector of matrix $\boldsymbol{X}$ containing input data and represents one collection sample

Gradient boosting decision trees: GBDT

- In the k^{th} iteration, predicted output is evaluated using the k^{th} estimator and k^{th} decision tree:

$$\hat{y}_i^{(k)} = \hat{y}_i^{(k-1)} + f_k(\boldsymbol{x}_i),$$

where:

- $\hat{y}_i^{(k)}$: predicted output of the i^{th} data point
- $\hat{y}_i^{(k-1)}$: previously predicted output
- f_k: the k^{th} decision tree

Gradient boosting decision trees: GBDT

- Goal of the GBDT models is to minimize the objective function:

$$\mathcal{L}^{(k)} = \sum_{i=1}^{N} l\left(y_i - \hat{y}_i^{(k)}\right) + \Omega(f_k),$$

where:

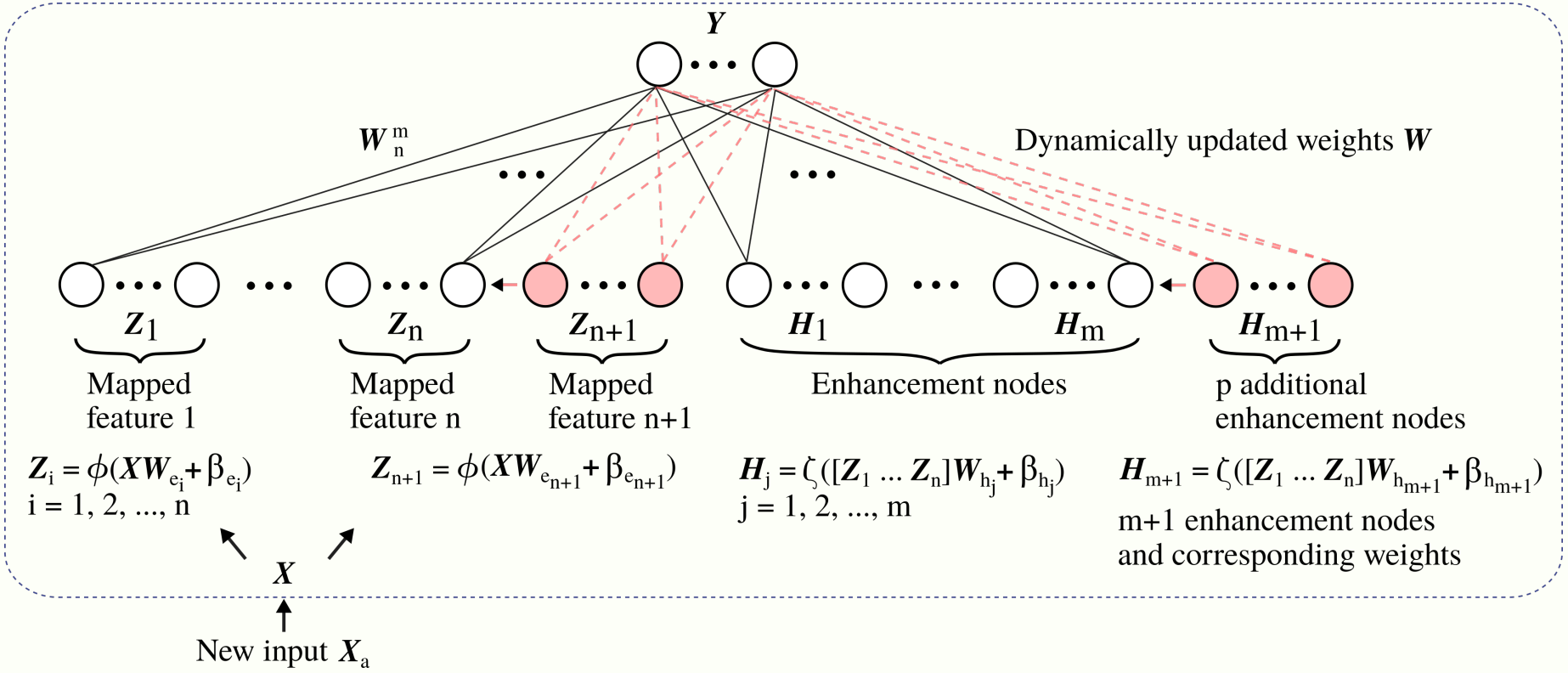
- $l(\cdot)$: loss function
- y_i: true value of the i^{th} data point
- $\hat{y}_i^{(k)}$: predicted output of the i^{th} data point for the kth iteration
- $\Omega(f_k)$: (optional) regularization term

GBDT: XGBoost, LightGBM, CatBoost

- XGBoost:
  - adds an L^2 norm regularization term to avoid over-fitting
  - employs the second-order Taylor series to approximate its objective function
- LightGBM:
  - accelerate the training speed by using gradient-based one-side sampling (GOSS) and exclusive feature bundling (EFB)
- CatBoost:
  - deals with categorical features
  - employs target statistic to convert categorical to numerical features
  - employs ordered boosting

Broad learning system

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



Original BLS

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

$$\boldsymbol{A}_x = [\boldsymbol{Z}^n \mid \boldsymbol{H}^m]$$

$$= \left[\phi\left(\boldsymbol{X}\boldsymbol{W}_{e_i} + \boldsymbol{\beta}_{e_i}\right) \mid \xi\left(\boldsymbol{Z}_x^n \boldsymbol{W}_{h_j} + \boldsymbol{\beta}_{h_j}\right)\right],$$

$$i = 1, 2, \ldots, n \text{ and } j = 1, 2, \ldots, m,$$

where:

- ϕ and ξ: projection mappings
- $\boldsymbol{W}_{e_i}$, $\boldsymbol{W}_{h_j}$: weights
- $\boldsymbol{\beta}_{e_i}$, $\boldsymbol{\beta}_{h_j}$: bias parameters

Original BLS

- Moore-Penrose pseudo inverse of matrix $\boldsymbol{A}_x$ is computed to calculate the weights of the output:

$$\boldsymbol{W}_n^m = [\boldsymbol{A}_n^m]^+ \boldsymbol{Y}$$

- Calculated using ridge regression:

$$\boldsymbol{W}_n^m = [(\boldsymbol{A}_n^m)^T \boldsymbol{A}_n^m + \lambda \boldsymbol{I}]^{-1} (\boldsymbol{A}_n^m)^T \boldsymbol{Y}$$

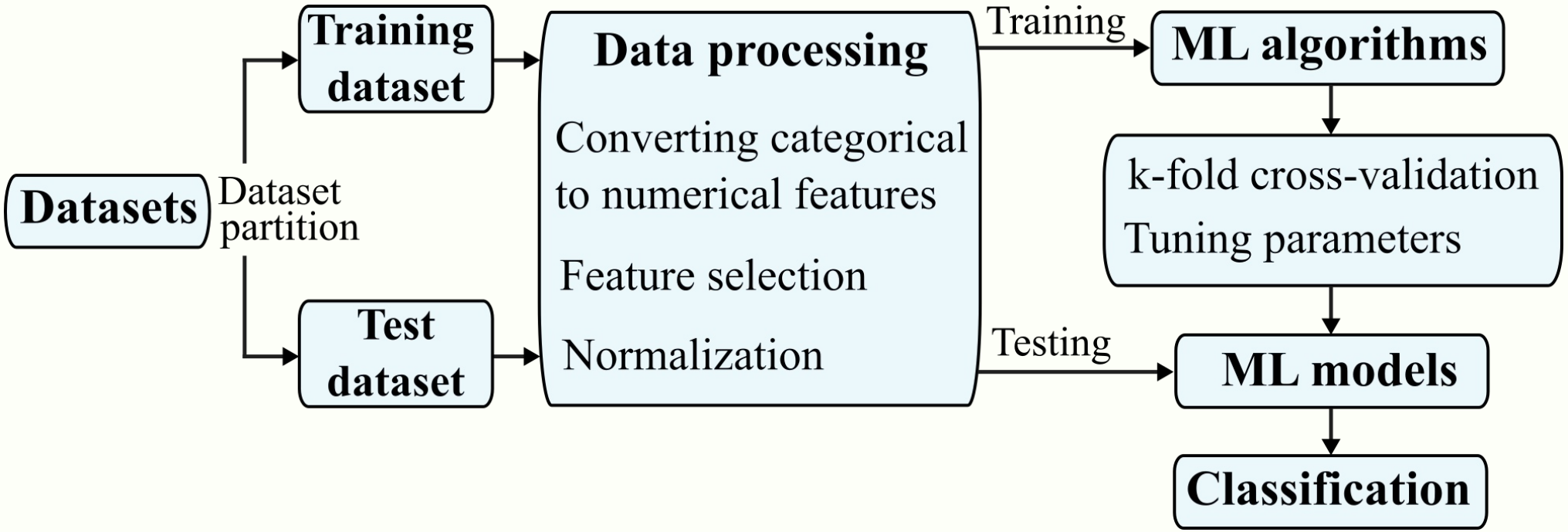
- During the testing process, data labels are deduced using the calculated weights $\boldsymbol{W}_n^m$, mapped features $\boldsymbol{Z}_n$, and enhancement nodes $\boldsymbol{H}_m$:

$$\begin{aligned} \boldsymbol{Y} &= \boldsymbol{A}_n^m \boldsymbol{W}_n^m \\ &= [\boldsymbol{Z}_1, \dots, \boldsymbol{Z}_n | \boldsymbol{H}_1, \dots, \boldsymbol{H}_m] \boldsymbol{W}_n^m \end{aligned}$$

- Modified to include additional mapped features $\boldsymbol{Z}_{n+1}$, enhancement nodes $\boldsymbol{H}_{m+1}$, and/or input nodes $\boldsymbol{X}_a$

Experimental procedure

- Experimental framework for intrusion detection:



Performance metrics

- Accuracy:
  - (TP + TN) / (TP + TN + FP + FN)
- F1-Score signifies harmonic mean between precision and recall (precision):
  - 2 x (precision x recall) / (precision + recall)

where:

  - Precision: TP / (TP + FP)
  - Recall: TP / (TP + FN)
- Confusion matrix: TP, FP, TN, FN
- Training Time and Test Time
- Receiver operating characteristic (ROC) curve

Performance comparison: RNN and BLS

	Datasets	$LSTM_2$	$LSTM_3$	$LSTM_4$	GRU_2	GRU_3	GRU_4
		Python (CPU)					
Training time (s)	Slammer	224.52	259.91	819.78	54.12	60.76	759.82
	NSL-KDD	4,481.73	4,614.66	11,478.62	1,108.31	1,161.80	11,581.30

	Datasets	BLS	RBF-BLS	CFBLS	CEBLS	CFEBLS
		Python (CPU)				
Training time (s)	Slammer	21.53	18.68	18.89	32.36	32.13
	NSL-KDD	99.47	98.27	98.13	108.23	108.14

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.

Performance comparison: RNN and BLS

- RNN and BLS models: NSL-KDD dataset

	Accuracy (%)		F-Score (%)	
Model	KDDTest^{+}	KDDTest^{-21}	KDDTest^{+}	KDDTest^{-21}
$LSTM_4$	82.78	66.74	83.34	76.21
GRU_3	82.87	65.42	83.05	74.06
CFBLS	82.20	67.47	82.23	76.29

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.

Best performance: CNN, RNN, and Bi-RNN models

- BGP dataset: WestRock ransomware attack

Model	Collection site	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)	TP	FP	TN	FN
CNN	RIPE	18.79	55.33	70.96	57.04	93.85	3,754	2,827	53	246
CNN	Route Views	18.66	57.67	72.96	58.04	98.23	3,929	2,841	39	71
GRU_4	RIPE	13.99	75.23	80.24	74.84	86.48	3,459	1,163	1,717	541
$LSTM_4$	Route Views	18.95	55.42	70.72	57.20	92.60	3,704	2,771	109	296
Bi-GRU_4	RIPE	20.59	78.49	81.92	80.10	83.83	3,353	833	2,047	647
Bi-GRU_3	Route Views	21.89	62.50	69.70	65.73	74.18	2,967	1,547	1,333	1,033

Z. Li, A. L. G. Rios, and Lj. Trajković, "Machine learning for detecting the WestRock ransomware attack using BGP routing records," *IEEE Commun. Mag.*, vol. 61, no. 3, pp. 20–26, Mar. 2023

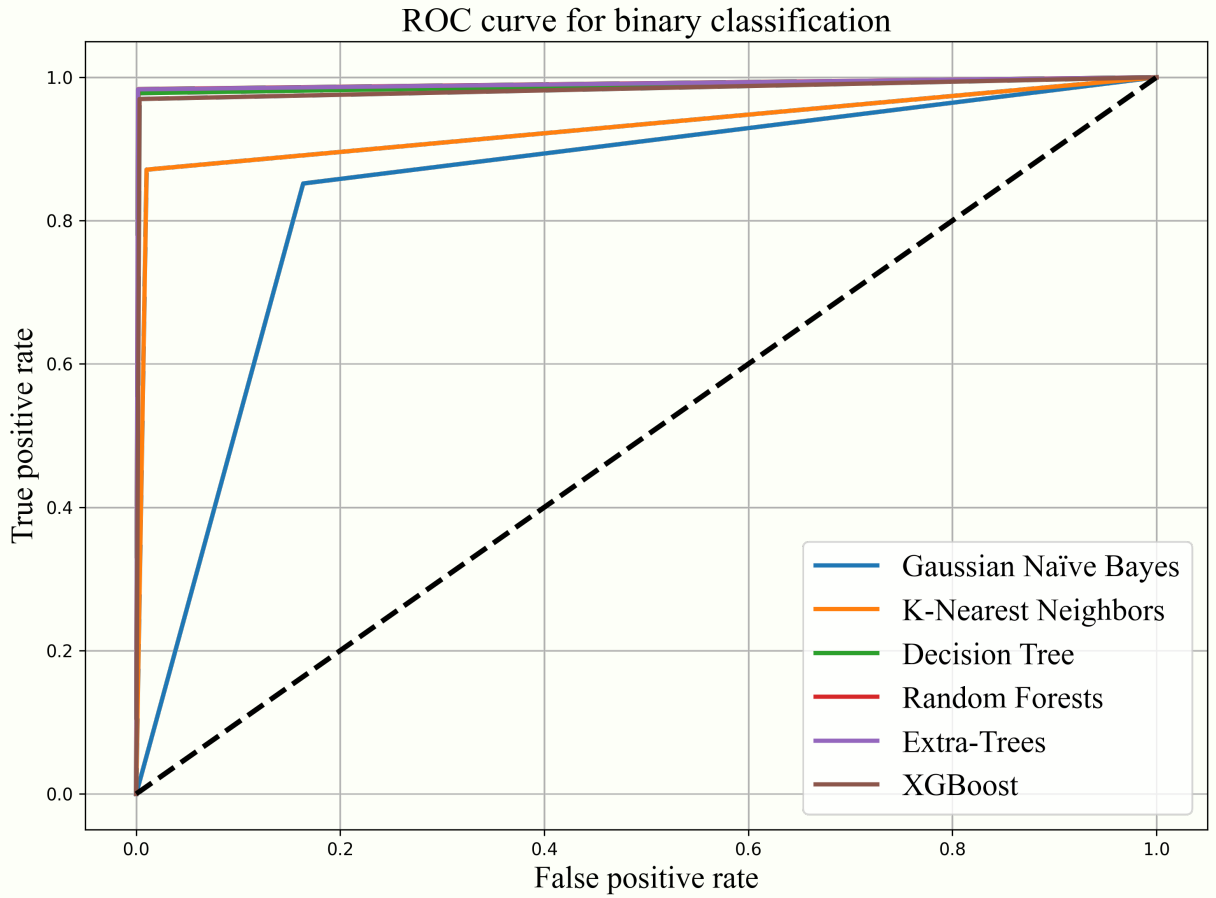
Best performance: XGBoost, LightGBM, and CatBoost models

- CICIDS2017, CSE-CIC-IDS2018, CICDDoS2019

Model	Dataset	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)	TP	FP	TN	FN
XGBoost	CICIDS2017	24.49	98.62	98.72	99.43	98.02	98,684	568	84,359	1,989
	CSE-CIC-IDS2018	14.43	99.90	99.39	99.99	98.79	20,731	1	240,314	254
	CICDDoS2019	62.99	99.99	99.99	99.99	99.99	2,541,767	7	1,151	6
LightGBM	CICIDS2017	3.35	97.93	98.06	99.94	96.25	96,896	60	84,867	3,777
	CSE-CIC-IDS2018	1.73	98.73	91.44	99.99	84.23	17,675	1	240,314	3,310
	CICDDoS2019	8.12	99.99	99.99	99.99	99.99	2,541,767	8	1,150	6
CatBoost	CICIDS2017	20.27	98.01	98.13	99.91	96.41	97,056	83	84,844	3,617
	CSE-CIC-IDS2018	19.03	99.95	99.72	99.97	99.46	20,872	6	240,309	113
	CICDDoS2019	17.38	99.99	99.99	99.99	99.99	2,541,762	19	1,139	11

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.

Network intrusion detection:
ROC curves of models for binary classifications



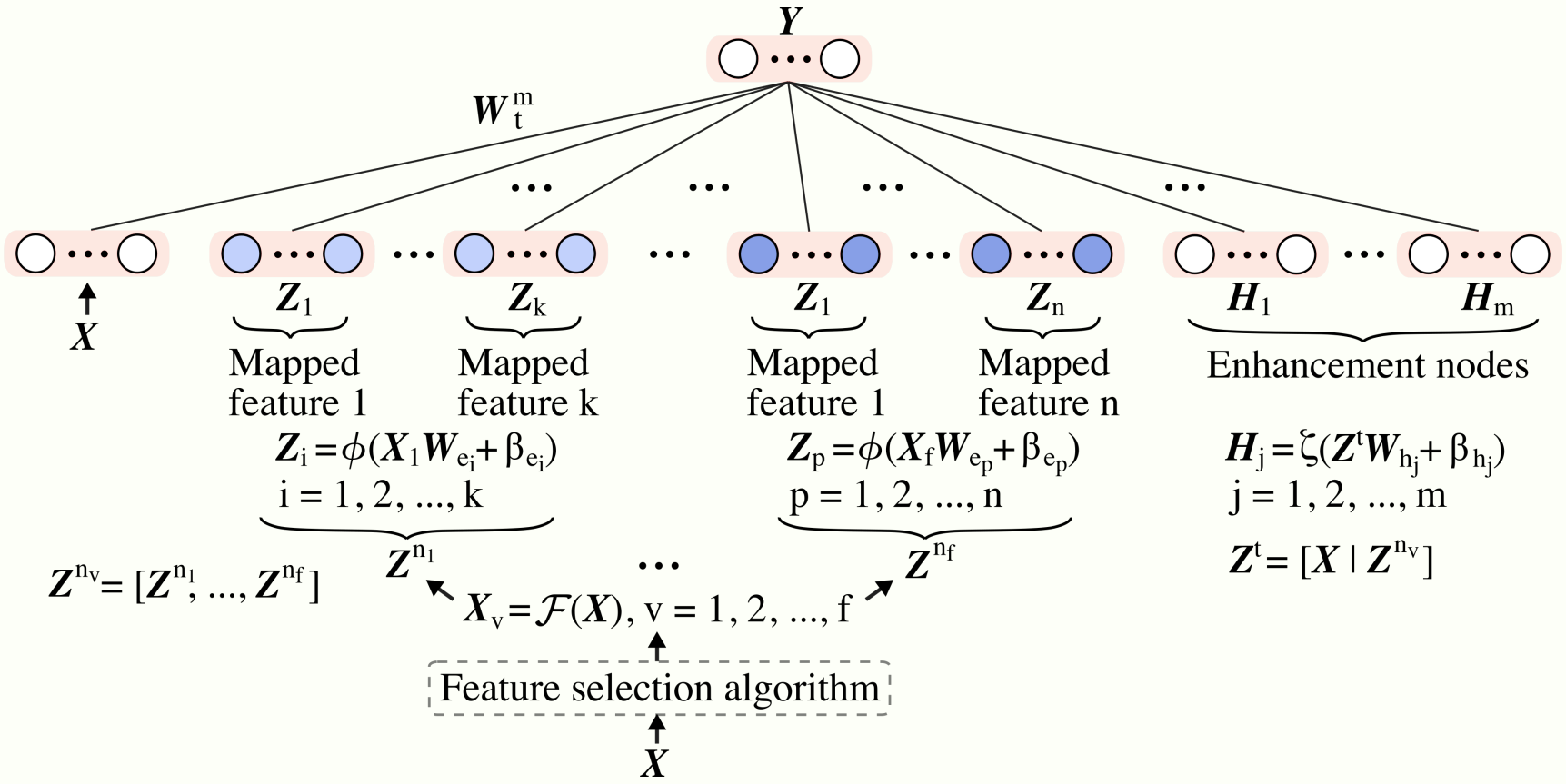
Z. Li, W. Han, Y. Shao, and A. Makanju, "Enhancing cybersecurity through fast machine learning algorithms," in *Proc. IEEE Canadian Conf. Elect. Comput. Eng. (CCECE)*, Kingston, ON, Canada, Aug. 2024, pp. 905–909.

Variable features broad learning system

- Variable features BLS without (VFBLS) and with cascades (VCFBLS) with and without incremental learning consist of:
  - variable number of mapped features and groups of mapped features
  - a feature selection algorithm to create subsets of input data
- VFBLS and VCFBLS enable:
  - derivation of generalized models
  - integration of selecting features and generating models
  - reduction of the training time by employing a smaller number of features

Z. Li, A. L. Gonzalez Rios, and Lj. Trajkovic, "Machine learning for detecting anomalies and intrusions in communication networks," *IEEE JSAC*, vol. 39, no. 7, pp. 2254-2264, July 2021.

Variable features broad learning system: VFBLS



Z. Li, A. L. Gonzalez Rios, and Lj. Trajkovic, "Machine learning for detecting anomalies and intrusions in communication networks," *IEEE JSAC*, vol. 39, no. 7, pp. 2254-2264, July 2021.

Variable features broad learning system: VFBLS

- Subsets of input data $\boldsymbol{X}$ using a feature selection algorithm $\mathcal{F}$:

$$\boldsymbol{X}_v = \mathcal{F}(\boldsymbol{X}), \qquad v = 1, 2, \ldots, f$$

- Sets of groups of mapped features: $\boldsymbol{Z}^{n_v} = [\boldsymbol{Z}^{n_1}, \ldots, \boldsymbol{Z}^{n_f}]$
- Concatenation of $\boldsymbol{X}$ and $\boldsymbol{Z}^{n_v}$: $\boldsymbol{Z}^t = [\boldsymbol{X} \mid \boldsymbol{Z}^{n_v}]$
- Enhancement nodes:

$$\boldsymbol{H}_j = \xi\left(\boldsymbol{Z}^t \boldsymbol{W}_{h_j} + \boldsymbol{\beta}_{h_j}\right), \qquad j = 1, 2, \ldots, m$$

where:

- f: number of subsets
- n_v: number of sets of mapped features
- ξ: projection mapping

Variable features broad learning system: VFBLS

- State matrix $\boldsymbol{A}_t^m$: concatenation of $\boldsymbol{Z}^t$ and $\boldsymbol{H}^m$
- Ridge regression algorithm is employed to compute the weights $\boldsymbol{W}_t^m$ based on $\boldsymbol{A}_t^m$ and given labels $\boldsymbol{Y}$
- Error function, minimized during the training process:

$$\boldsymbol{E}(\boldsymbol{W}_t^m) = (||\boldsymbol{W}_t^m - \boldsymbol{Y}||_2)^2 + (\lambda||\boldsymbol{W}_t^m||_2)^2$$

- Output weights:

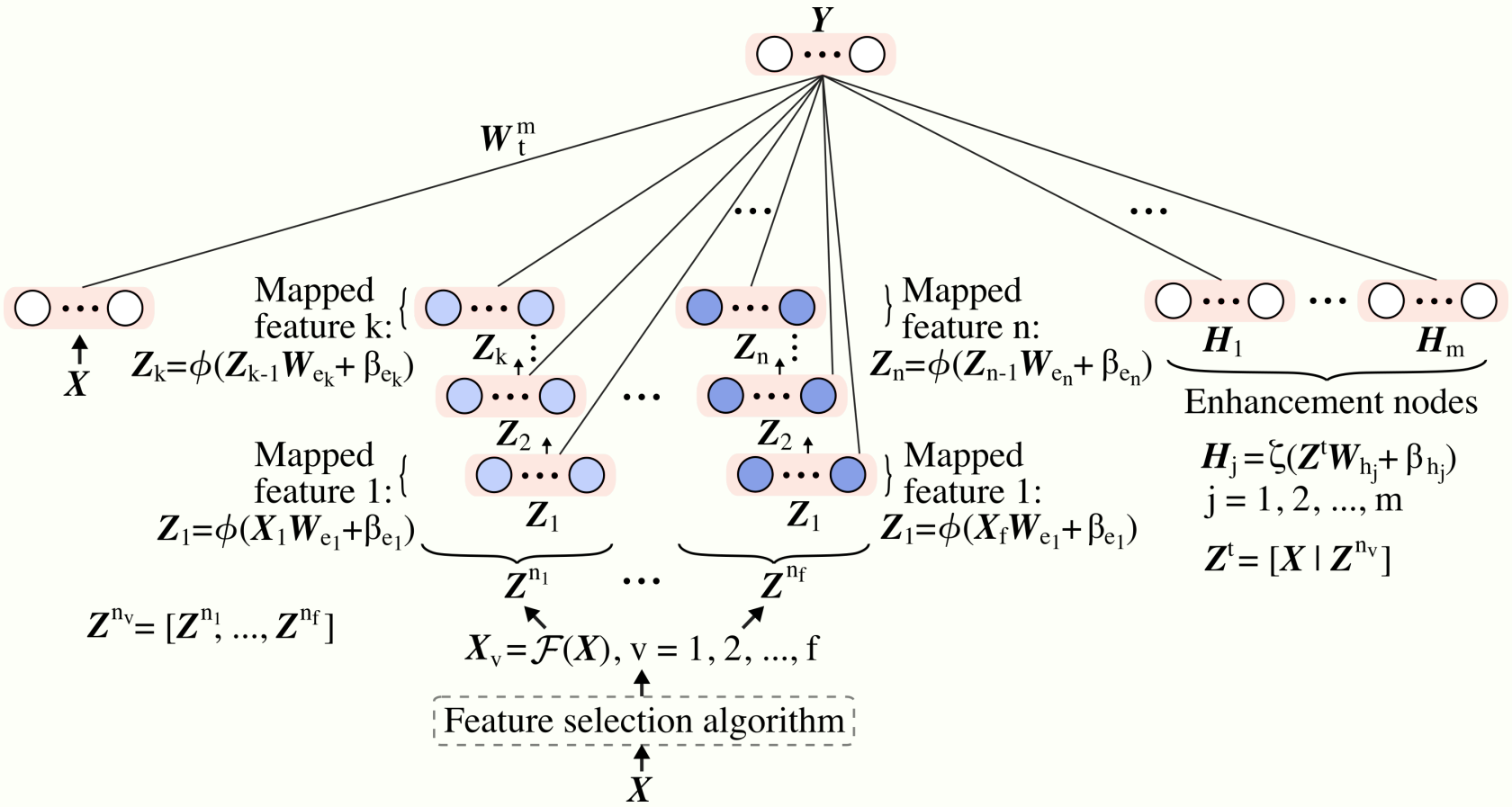
$$\boldsymbol{W}_t^m = (\lambda\boldsymbol{I} + (\boldsymbol{A}_t^m)^T\boldsymbol{A}_t^m)^{-1}(\boldsymbol{A}_t^m)^T\boldsymbol{Y}$$

where:

- λ is the sparse regularization coefficient

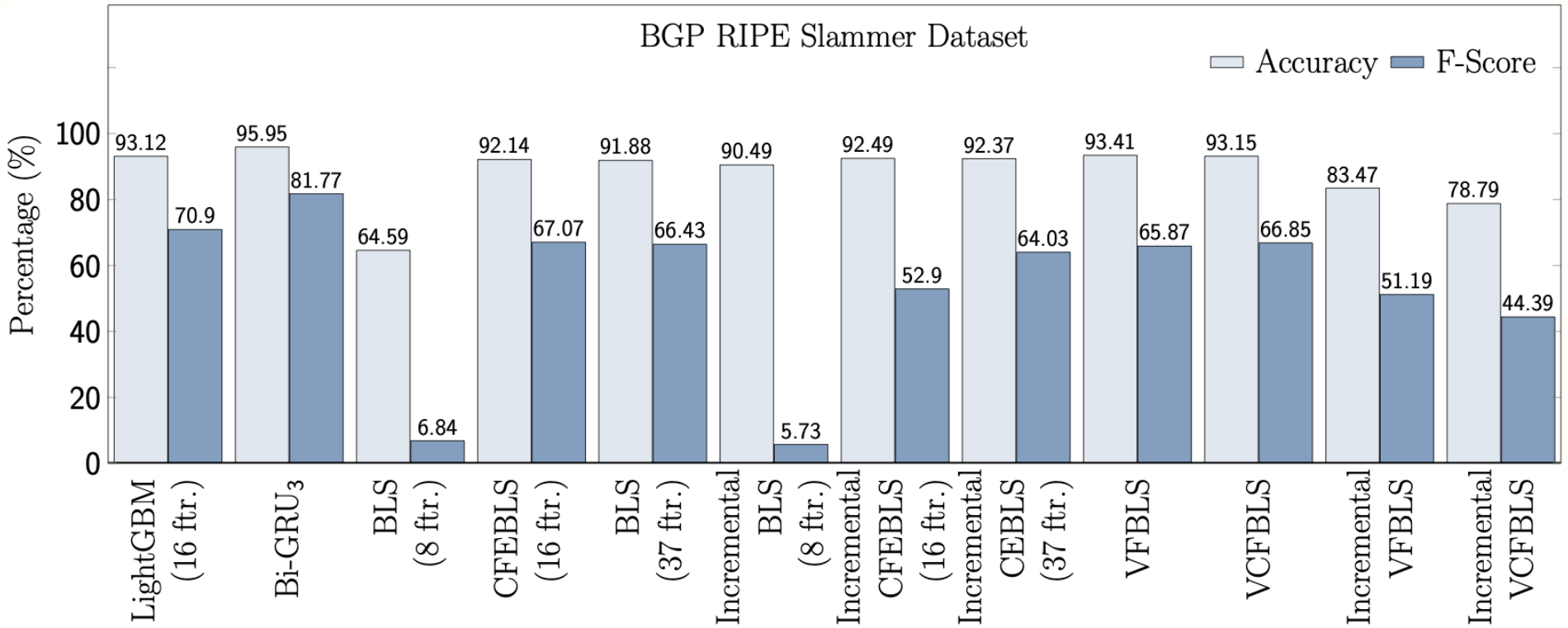
Z. Li, A. L. Gonzalez Rios, and Lj. Trajkovic, "Machine learning for detecting anomalies and intrusions in communication networks," *IEEE JSAC*, vol. 39, no. 7, pp. 2254-2264, July 2021.

Variable features broad learning system: VCFBLS



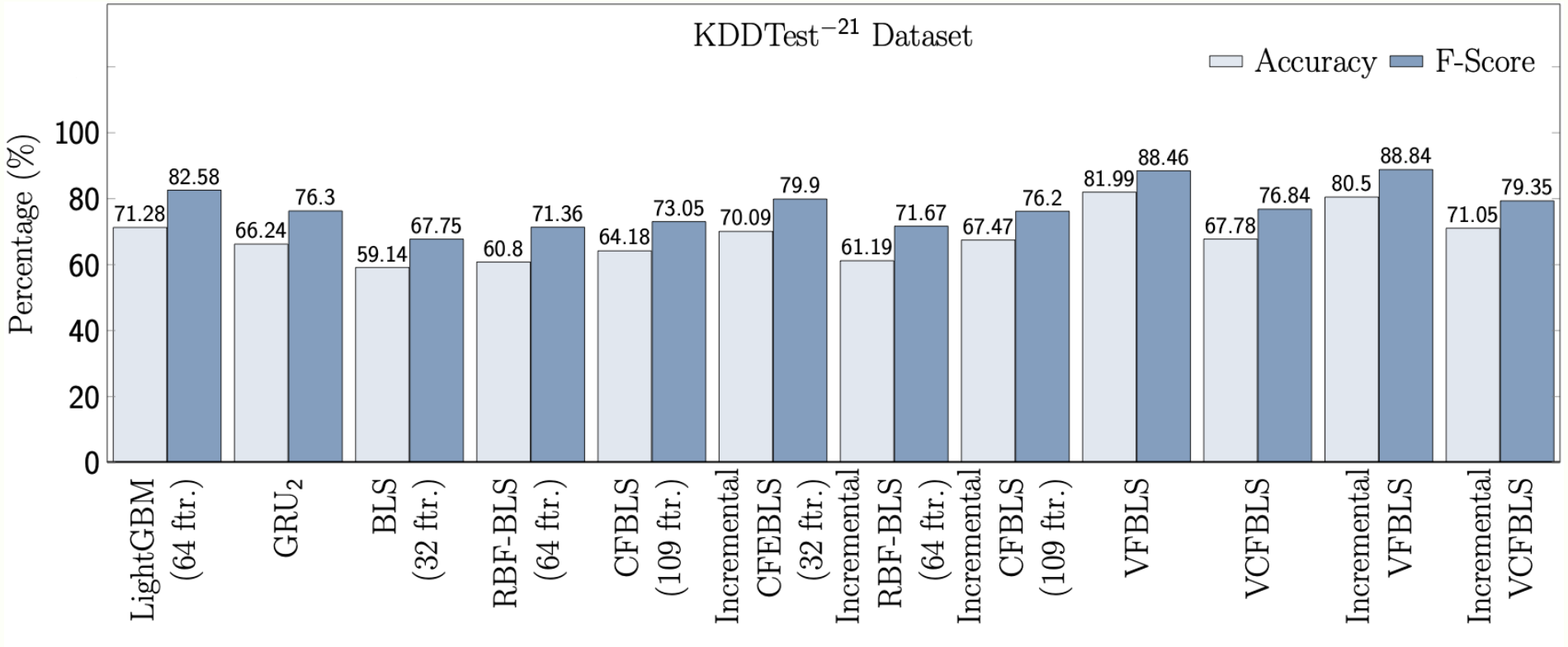
Z. Li, A. L. Gonzalez Rios, and Lj. Trajkovic, "Machine learning for detecting anomalies and intrusions in communication networks," *IEEE JSAC*, vol. 39, no. 7, pp. 2254-2264, July 2021.

Best performance: Slammer



Z. Li, A. L. Gonzalez Rios, and Lj. Trajkovic, "Machine learning for detecting anomalies and intrusions in communication networks," *IEEE JSAC*, vol. 39, no. 7, pp. 2254-2264, July 2021.

Best performance: KDDTest^{-21} (NSL-KDD)



Z. Li, A. L. Gonzalez Rios, and Lj. Trajkovic, "Machine learning for detecting anomalies and intrusions in communication networks," *IEEE JSAC*, vol. 39, no. 7, pp. 2254-2264, July 2021.

Performance comparison: training time

- Datasets: Slammer, NSL-KDD, and CICIDS 2017

Dataset		LightGBM	RNN	BLS			Incremental BLS			Variable BLS		Incremental Variable BLS	
Slammer	Model		Bi-GRU_3	BLS	CFEBLS	BLS	BLS	CFEBLS	CEBLS	VFBLS	VCFBLS	VFBLS	VCFBLS
	(No. ftr.)	(16)		(8)	(16)	(37)	(8)	(16)	(37)				
	Time (s)	0.02	212.83	6.47	24.09	15.38	216.62	37.83	8.75	9.22	13.86	1.82	1.66
NSL-KDD	Model		GRU_2	BLS	RBF-BLS	CFBLS	CFEBLS	RBF-BLS	CFBLS	VFBLS	VCFBLS	VFBLS	VCFBLS
	(No. ftr.)	(64)		(32)	(64)	(109)	(32)	(64)	(109)				
	Time (s)	0.92	4,831.55	39.77	11.10	24.84	26.05	36.74	83.03	31.21	31.32	28.92	60.43
CICIDS 2017	Model		GRU_2	CEBLS	BLS	RBF-BLS	CFBLS	CFEBLS	CFBLS	VFBLS	VCFBLS	VFBLS	VCFBLS
	(No. ftr.)	(32)		(32)	(64)	(78)	(32)	(64)	(78)				
	Time (s)	1.43	15,483.96	39.25	8.97	15.60	6.39	7.39	3.69	25.25	26.05	25.55	24.19

Z. Li, A. L. Gonzalez Rios, and Lj. Trajkovic, "Machine learning for detecting anomalies and intrusions in communication networks," *IEEE JSAC*, vol. 39, no. 7, pp. 2254-2264, July 2021.

Roadmap

- Introduction
- Network anomalies and intrusions
- Applications of machine learning algorithms
- CyberDefense tool
- Conclusions and References

Intrusion detection systems

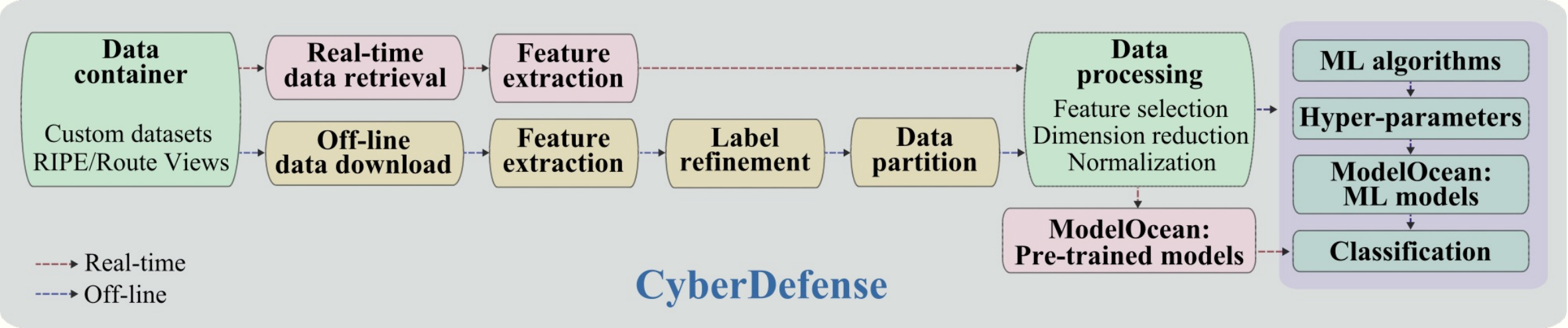
- Intrusion detection systems (IDSs) have been implemented as real-time or off-line software tools:
  - Snort, Passban, VMGuard, SwiftIDS, WisdomSDN
- Commercial tools:
  - BGProtect
  - intrusion prevention systems:
    - Cisco
    - FortiGuard
    - Palo Alto Networks advanced threat prevention

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

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



Z. Li and Lj. Trajković, "Enhancing cyber defense: using machine learning algorithms for detection of network anomalies," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, Honolulu, USA, Oct. 2023, pp. 1658–1663.

Real-time detection: BGP routing traffic

Local Time: 03:32:07 AM | June 27, 2023

Retrieving and classifying BGP routing records

Select a collection site: RIPE Route Views

Data collector: rrc04 located at CIXP, Geneva

Detecting BGP Anomalies... Disconnect

Coordinated Universal Time (UTC) when processing: Wed, 28 Jun 2023 10:29:16

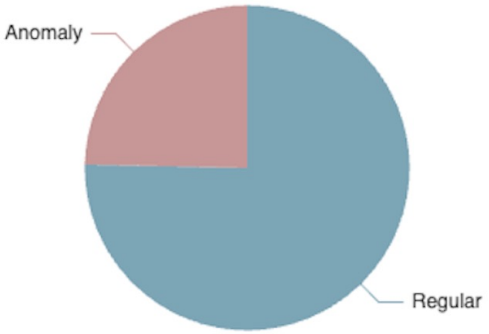
Predictions over the past five minutes:

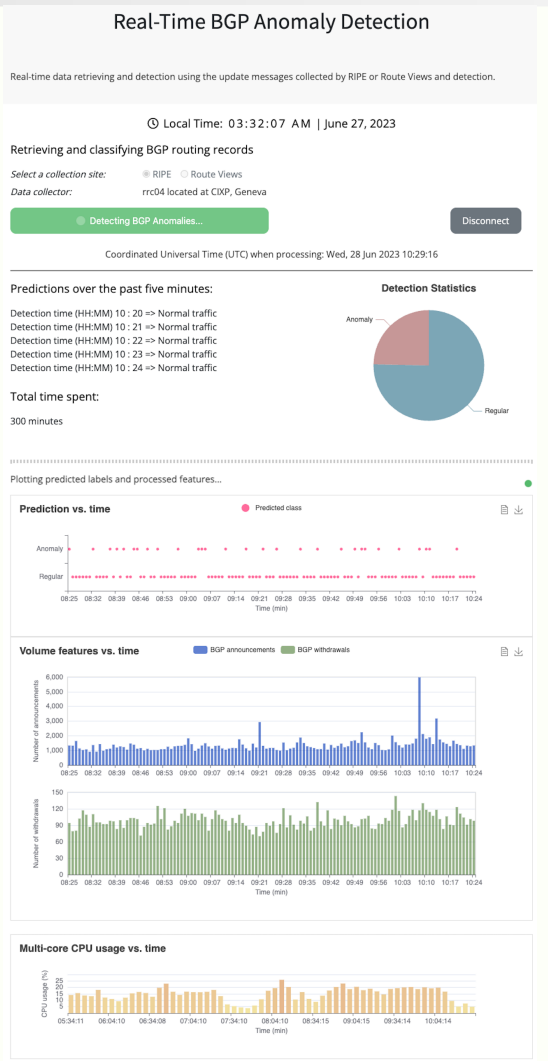
Detection time (HH:MM) 10 : 20 => Normal traffic
Detection time (HH:MM) 10 : 21 => Normal traffic
Detection time (HH:MM) 10 : 22 => Normal traffic
Detection time (HH:MM) 10 : 23 => Normal traffic
Detection time (HH:MM) 10 : 24 => Normal traffic

Total time spent:

300 minutes

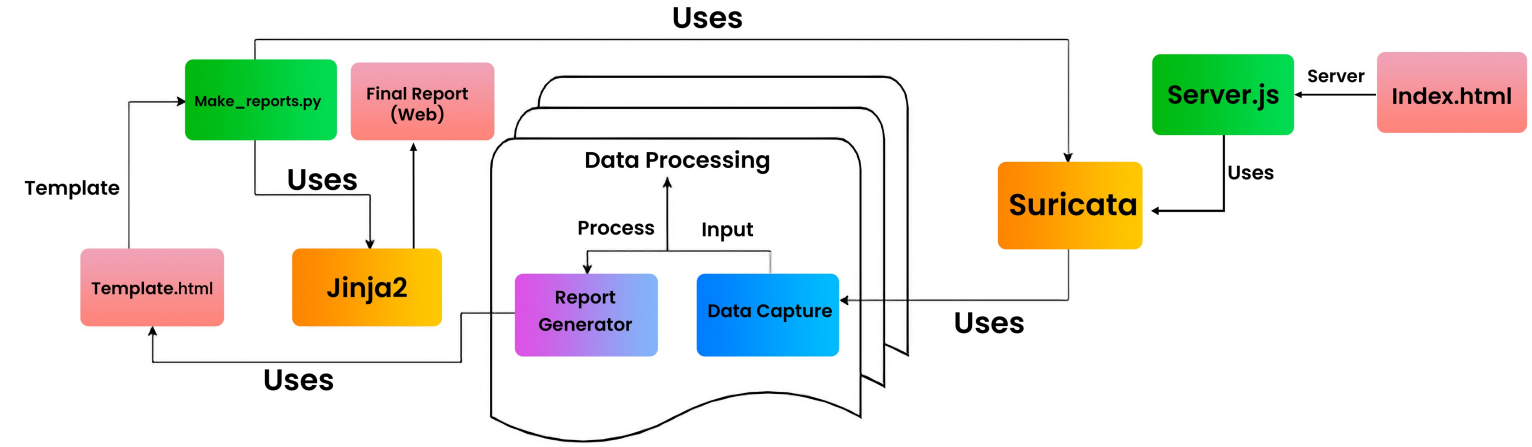
Detection Statistics

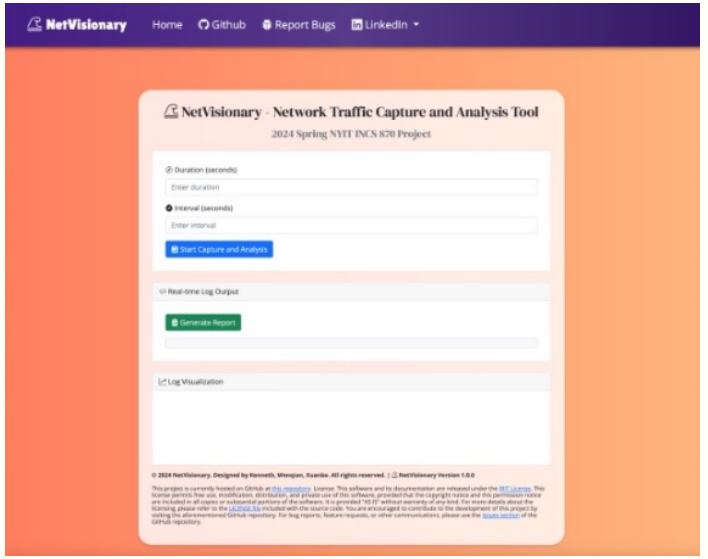




Other platform: NetVisionary

- *NetVisionary*: An Automated and Scalable Suricata-Based IDS Platform

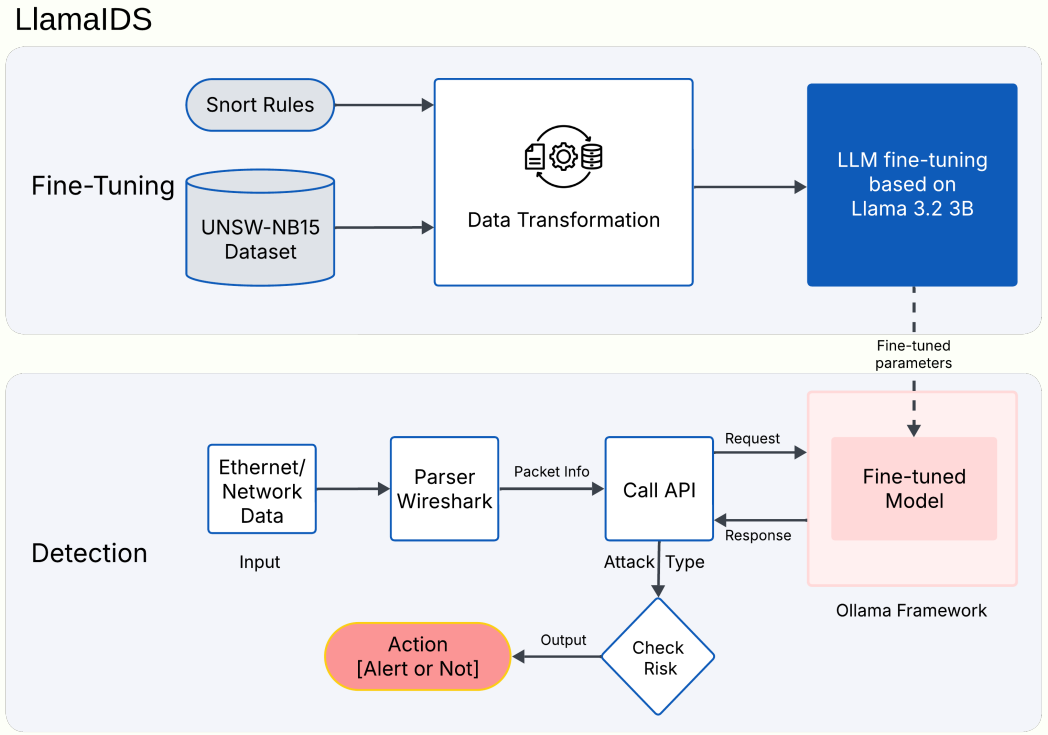




G. Zhu, W. Dai, X. Guo, C. Wang, Y. Shao, A. Makanju, and Z. Li, "NetVisionary: An Automated and Scalable Suricata-Based IDS Platform," *IEEE Canadian Conf. Elect. Comput. Eng. (CCECE)*, Vancouver, Canada, May 2025, to be published.

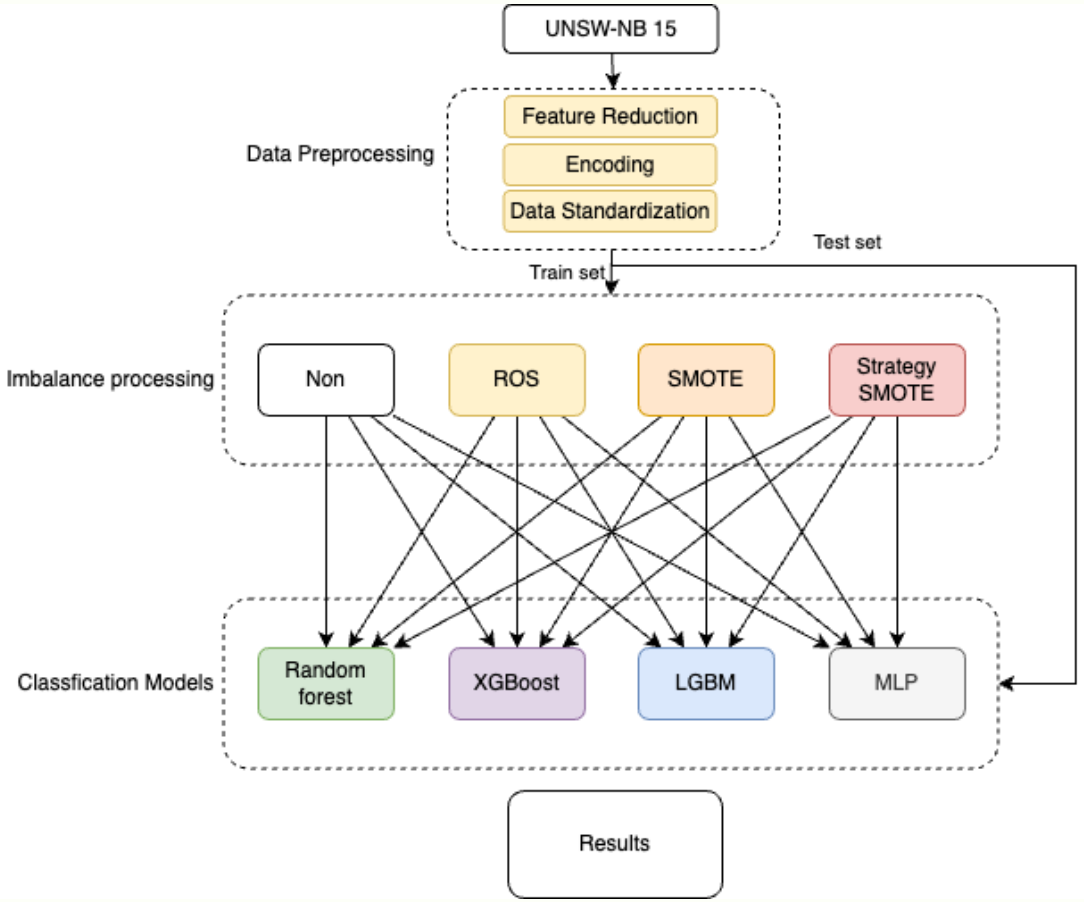
Other platform: LlamaIDS

- *LlamaIDS: Real-Time Detection Model of Zero-Day Intrusions Using Large Language Models*



F. Wang, Q. Weng, M. Zhang, Y. Shao, Z. Alomari, A. Makanju, and Z. Li, "LlamaIDS: Real-Time Detection Model of Zero-Day Intrusions Using Large Language Models," *IEEE Canadian Conf. Elect. Comput. Eng. (CCECE)*, Vancouver, Canada, May 2025, to be published.

Other technique: Optimization of class imbalance



NUMBER OF EACH CLASS IN TRAINING DATESET BEFORE AND AFTER RESAMPLED

Class	Class Code	Count (Original)	Percentage (Original)	Count (Resampled)	Percentage (Resampled)
Normal	0	74319	36.05%	74319	31.56%
Generic	1	47126	22.86%	47126	20.01%
Exploits	2	35724	17.33%	35724	15.17%
Fuzzers	3	19441	9.43%	19441	8.26%
DoS	4	13085	6.35%	13085	5.56%
Reconnaissance	5	11096	5.38%	11096	4.71%
Analysis	6	2129	1.03%	11096	4.71%
Backdoor	7	1851	0.90%	11096	4.71%
Shellcode	8	1227	0.60%	11096	4.71%
Worms	9	140	0.07%	1400	0.59%

H. Xie, Y. Shao, Z. Li, Z. Alomari, and A. Makanju, "Optimization of Class Imbalance Techniques in Machine Learning Models for Network Intrusion Detection," *IEEE Int. Conf. Cryptography, Security and Privacy (CSP)*, Okinawa, Japan, April 2025, to be published.

Roadmap

- Introduction
- Network anomalies and intrusions
- Applications of machine learning algorithms
- CyberDefense tool
- Conclusions and References

Conclusions

- We presented and evaluated the performance of:
  - traditional, deep learning, and fast machine learning algorithms
- Datasets collected from deployed network traffic and testbeds
- BLS models offer comparable performance to deep learning RNNs (LSTM, GRU, Bi-LSTM, Bi-GRU) models while requiring shorter training time
- LightGBM models required the shortest training time
- VFBLS and VCFBLS algorithms: employed variable number of mapped features and an integrated feature selection algorithm
- The CyberDefense tool was used to classify various network anomalies

Roadmap

- Introduction
- Network anomalies and intrusions
- Applications of machine learning algorithms
- CyberDefense tool
- Conclusions and References

References: data sources

- 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
- UNSW-NB15 Dataset:
  https://research.unsw.edu.au/projects/unsw-nb15-dataset
- IEEE DataPort:
  Border Gateway Protocol (BGP) datasets:
  https://ieee-dataport.org/open-access/border-gateway-protocol-bgp-routing-records-reseaux-ip-europeens-ripe-and-bcnet
  https://ieee-dataport.org/open-access/border-gateway-protocol-bgp-routing-records-route-views

References: tools

- Python:
  https://pypi.org
- PyTorch:
  https://pytorch.org/docs/stable/nn.html
- CyberDefense:
  https://github.com/zhida-li/CyberDefense
- 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

References: intrusion detection

- L. N. Tidjon, M. Frappier, and A. Mammar, “Intrusion detection systems: a cross-domain overview,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3639–3681, Fourth quarter 2019.
- P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, “A detailed investigation and analysis of using machine learning techniques for intrusion detection,” *IEEE Commun. Surveys Tut.*, vol. 21, no. 1, pp. 686–728, First quarter 2019.
- J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, “A review of intrusion detection systems using machine and deep learning in Internet of things: challenges, solutions and future directions,” *Electronics*, vol. 9, no. 7, July 2020.
- D. Han, Z. Wang, Y. Zhong, W. Chen, J. Yang, S. Lu, X. Shi, and X. Yin, “Evaluating and improving adversarial robustness of machine learning-based network intrusion detectors,” *IEEE J. Sel. Areas Commun.*, vol. 39, no. 8, pp. 2632–2647, Aug. 2021
- 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.

References: machine learning

- K. P. Murphy, *Probabilistic Machine Learning: An Introduction*. Cambridge, MA, USA: The MIT Press, 2022.
- I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning. Cambridge*, MA, USA: The MIT Press, 2016.
- G. E. Hinton, N. Srivastava, A. Krizhevsky, I. Sutskever, and R. R. Salakhutdinov, “Improving neural networks by preventing co-adaptation of feature detectors,” *Computing Research Repository (CoRR)*, abs/1207.0580, pp. 1–18, Jul. 2012.
- K. Greff, R. K. Srivastava, J. Koutnik, B. R. Steunebrink, and J. Schmidhuber, “LSTM: a search space odyssey,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 10, pp. 2222–2232, Oct. 2017.
- P. Geurts, D. Ernst, and L.Wehenkel, “Extremely randomized trees,” *Mach. Learn.*, vol. 63, no. 1, pp. 3–42, Apr. 2006.
- G. Louppe, L. Wehenkel, A. Sutera, and P. Geurts, “Understanding variable importances in forests of randomized trees,” in *Proc. Int. Conf. Neural Inform. Process. Syst.*, Lake Tahoe, NV, USA, Dec. 2013, pp. 431–439.

References: BLS and GBDT

- 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.
- 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.

- T. Chen and C. Guestrin, “XGBoost: a scalable tree boosting system,” in *Proc. 22nd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, San Francisco, CA, USA, Aug. 2016, pp. 785–794.
- G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye and T.-Y. Liu, “LightGBM: a highly efficient gradient boosting decision tree,” in *Proc. Int. Conf. Neural Inform. Process. Syst.*, Long Beach, CA, USA, Dec. 2017, 3146–3154.
- L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush, and A. Gulin, “CatBoost: unbiased boosting with categorical features,” in *Proc. Int. Conf. Neural Inform. Process. Syst.*, Montreal, Quebec, Canada, Dec. 2018, 6639–6649.

Publications: https://zhidali.me/

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: https://zhidali.me/

Conference publications:

- Z. Alomari, Z. Li, A. Makanju, “Lightweight machine learning-based IDS for IoT environments,” *IEEE Cyber Security in Networking Conference (CSNet)*, Paris, France, Dec. 2024.
- Z. Li, W. Han, Y. Shao, and A. Makanju, “Enhancing cybersecurity through fast machine learning algorithms,” in *Proc. IEEE Canadian Conf. Elect. Comput. Eng. (CCECE)*, Kingston, ON, Canada, Aug. 2024, pp. 905–909.
- Z. Li and Lj. Trajković, "Enhancing Cyber Defense: Using Machine Learning Algorithms for Detection of Network Anomalies," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, Honolulu, USA, Oct. 2023, pp. 1658–1663.
- 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.
- 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.

Publications: https://zhidali.me/

Conference publications:

- 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.
- 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.
- 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.*, Gödöllö, 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.