Machine Learning for Detecting Ransomware Attacks Using BGP Routing Records

Ana Laura Gonzalez Rios
anag@sfu.ca

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

Roadmap

- Introduction
- Border Gateway Protocol: anomalies and datasets
- Relational database for Border Gateway Protocol
- Ransomware attacks
- Supervised and semi-supervised algorithms
- Performance evaluation and experimental results
- Conclusion
- Future Work
- References and publications

Roadmap

- Introduction
- Border Gateway Protocol: anomalies and datasets
- Relational database for Border Gateway Protocol
- Ransomware attacks
- Supervised and semi-supervised algorithms
- Performance evaluation and experimental results
- Conclusion
- Future Work
- References and publications

Motivation

- The Internet:
  - highly susceptible to failures and attacks
- Border Gateway Protocol (BGP):
  - incremental path vector Internet routing protocol
  - manages network reachability information
  - optimally routes data between Autonomous Systems (ASes)
  - implementation of routing policies is complex and error-prone
  - lacks security mechanisms to verify legitimate route updates
  - is prone to anomalies

Motivation

- Machine learning: used to address a variety of engineering and scientific problems
- Classified as:
  - supervised
  - unsupervised
  - semi-supervised
- BGP anomalies classified using various supervised machine learning algorithms:
  - Recurrent neural networks (RNNs)
  - Broad learning system (BLS)
  - Gradient boosting decision trees (GBDT)

Research contributions

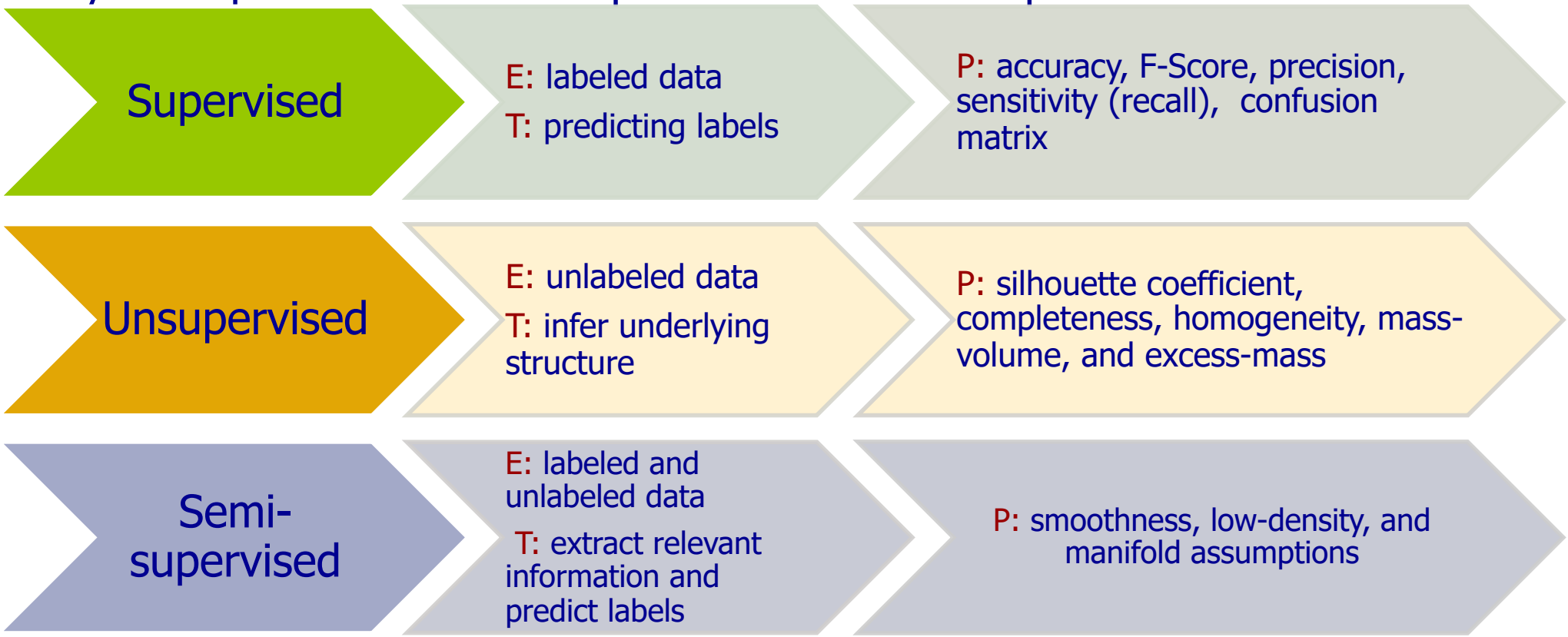
- Relational database (BGP-RDB) based on BGP messages and TCP connection states:
  - Open
  - Update
  - Notification
  - Keepalive
- Supervised and semi-supervised machine learning:
  - WannCrypt: May 12, 2017
  - WestRock: January 23, 2021

Border gateway protocol (BGP): an overview

- The Internet consists of numerous ASes:
  - single technical administration domain
  - unified routing policy
  - exchange network reachability information
- BGP routers (peers) are classified as:
  - internal
  - external
- Transport Control Protocol (TCP) sessions using port 179
- Routing information is stored in Routing Information Bases: Adj-RIB-In, Loc-RIB, Adj-RIB-Out

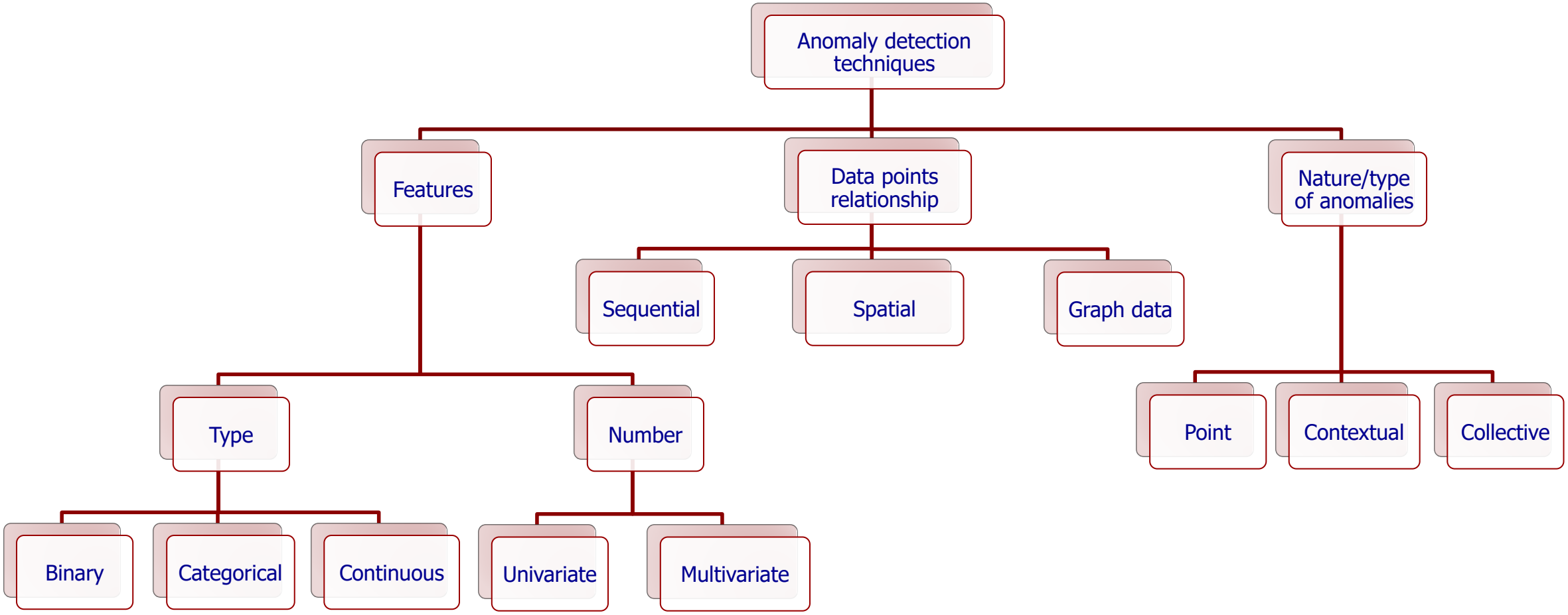
Machine learning approaches

- Rely on experience E with respect to a task T and performance measure P:



T. M. Mitchell, Machine Learning. New York, NY, USA: McGraw-Hill, 1997.
J. E. van Engelen and H. H. Hoos, "A survey on semi-supervised learning," *Mach Learn*, vol. 109, no. 2, p. 373–440, Feb. 2020.

Anomaly detection



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.

Anomaly detection in communication networks

Classification-based techniques:

- Consist of training and testing phase
- One-way classification:
  - regular data are inside a boundary
  - anomalies are outside
- Multi-way classification:
  - used when there are multiple regular or anomalous classes
- Computational complexity depends on the classification algorithm
- Performance relies on accuracy of available labels

Anomaly detection in communication networks

Clustering-based techniques:

- Use unsupervised or semi-supervised machine learning
- Anomalies detected based on:
  - location with respect to a cluster
  - proximity to nearest cluster centroid
  - size and sparsity of a cluster
- Computational complexity may be quadratic or linear
- Disadvantages:
  - ineffectiveness of algorithm, lack of optimization, small clusters with anomalies, high complexity

Anomaly detection in communication networks

Statistics techniques:

- Anomalies are observations not generated by used statistical model
- Models may be developed using techniques:
  - parametric: based on scores or null hypothesis
  - non-parametric: determine statistical model based on the given data
- Computational complexity depends on selected statistical model
- May be used for unsupervised detection

Anomaly detection in communication networks

Information theory:

- Employ measures such:
  - Kolmogorov complexity
  - entropy
  - relative entropy
- Assume that irregularities in the information content are caused by anomalies
- Computational complexity may be exponential or linear
- May be used for unsupervised detection without assuming the underlying statistical distribution of the data

Roadmap

- Introduction
- Border Gateway Protocol: anomalies and datasets
- Relational database for Border Gateway Protocol
- Ransomware attacks
- Supervised and semi-supervised algorithms
- Performance evaluation and experimental results
- Conclusion
- Future Work
- References and publications

Border gateway protocol: data

- BGP routing data used to:
  - analyze the Internet topology and hierarchy
  - infer AS relationships
  - evaluate various intrusion and anomaly detection mechanisms
- BGP routing messages are available from global BGP monitoring systems:
  - Réseaux IP Européens (RIPE)
  - Route Views
- BGP messages are stored in Multi-threaded Routing Toolkit (MRT) format and collected using Quagga routing software
- Network traffic anomalies affect BGP update messages and result in harmful changes in the protocol's that degrade the Internet performance and reliability

Border gateway protocol: anomalies

- BGP anomalies may be caused by:
  - infrastructure (link) failures: power outages (Moscow blackout, Pakistani power outage) or physical damage to network elements (Mediterranean cable break)
  - router misconfigurations: directly modify BGP routing configuration (hijacked or leaked prefixes) and result in packet loss, unintended paths between routers, and forwarding loops
  - network intrusions: worms (Slammer, Nimda, Code Red) and ransomware attacks (WannaCrypt, WestRock) targeting Internet components that result in an increased number of prefix announcements, prefix withdrawals, and changes in AS-Path length and packet size
- BGP anomalies caused by network intrusions do not modify BGP routing configuration

BGP data collection sites: RIPE

RIPE (Routing Information Service (RIS) project):

- Established in 2001 to collect and store routing data from ASes worldwide
- Main collection site at the Network Coordination Center (NCC)
- 25 remote route collectors at major topologically interesting Internet points
- Messages:
  - collected every 15 minutes before July 23, 2003
  - every 5 minutes afterwards
- Routing tables:
  - collected every 8 hours

BGP data collection sites: Route Views

Route Views (University of Oregon project):

- Cisco and Juniper backbone routers configured as IPv4 or IPv6 route servers
- Employs FRRouting, Quagga, and Cisco collectors
- Messages: collected every 15 minutes
- Routing tables: collected every 2 hours
- 31 collectors across 5 regional Internet registries (RIRs):
  - America
  - Latin America
  - Asia-Pacific
  - Africa
  - Europe

BGP datasets: data processing and feature extraction

- BGP datasets: extracted from BGP update messages downloaded from RIPE and Route Views data collection sites
- Data collected during periods of Internet anomalies include:
  - days of the attack (anomalous data)
  - 2 days prior and after the attack (regular data)
- Employed collection sites are located near a considered anomalous event
- zebra-dump-parser tool is used to transform MRT to ASCII format
- Tool written in C# to extract 37 continuous, categorical, and binary features classified as:
  - AS-Path and volume
- Granularity of generated datasets: based on 1-minute intervals of routing records

List of features extracted from BGP update messages

Feature	Name	Type	Category
1	Number of announcements	continuous	*volume*
2	Number of withdrawals	continuous	*volume*
3	Number of announced NLRI prefixes	continuous	*volume*
4	Number of withdrawn NLRI prefixes	continuous	*volume*
5	Average *AS-Path* length	categorical	*AS-Path*
6	Maximum *AS-Path* length	categorical	*AS-path*
7	Average unique *AS-Path* length	categorical	*AS-Path*
8	Number of duplicate announcements	continuous	*volume*
9	Number of implicit withdrawals	continuous	*volume*
10	Number of duplicate withdrawals	continuous	*volume*
11	Maximum edit distance	categorical	*AS-Path*
12	Arrival rate	continuous	*volume*
13	Average edit distance	categorical	*AS-Path*
14-23	Maximum *AS-Path* $= n$, $n = (11, ..., 20)$	binary	*AS-Path*
24-33	Maximum edit distance $= n$, $n = (7, ..., 16)$	binary	*AS-Path*
34	Number of Interior Gateway Protocol (IGP) packets	continuous	*volume*
35	Number of Exterior Gateway Protocol (EGP) packets	continuous	*volume*
36	Number of incomplete packets	continuous	*volume*
37	Packet size (B)	continuous	*volume*

Roadmap

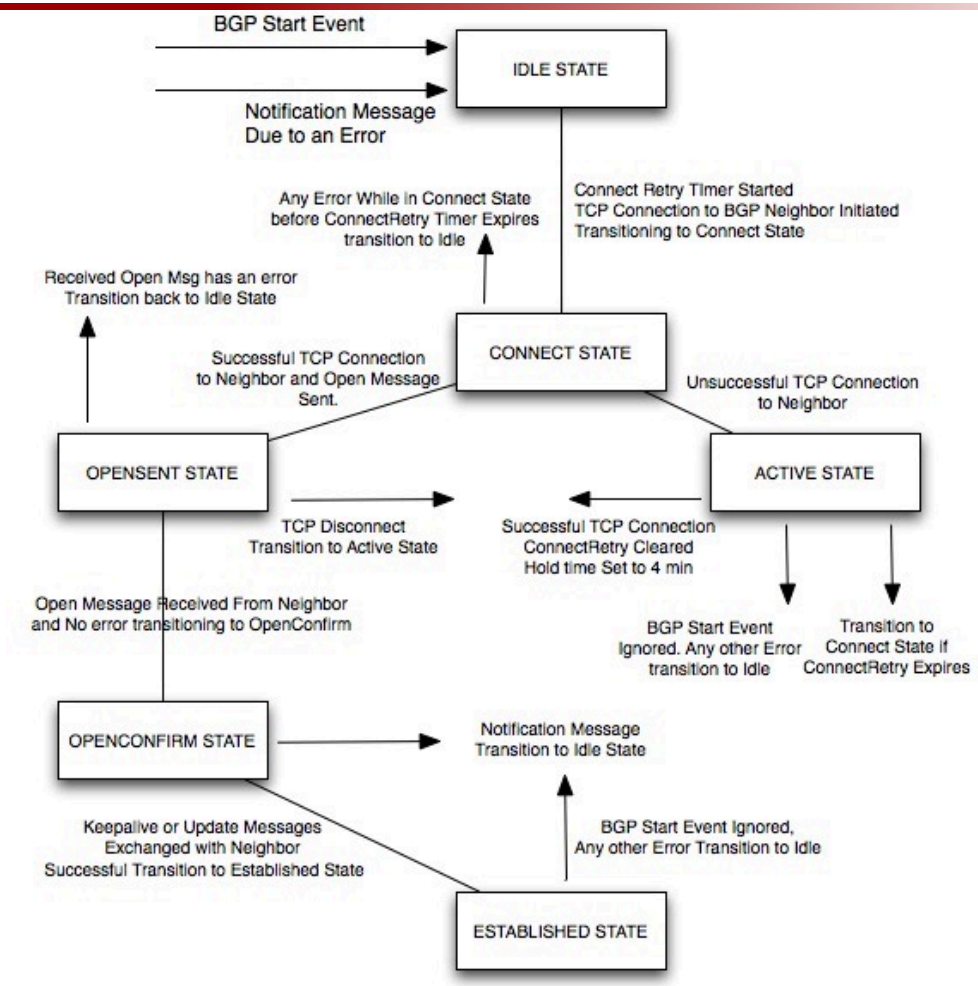
- Introduction
- Border Gateway Protocol: anomalies and datasets
- Relational database for Border Gateway Protocol
- Ransomware attacks
- Supervised and semi-supervised algorithms
- Performance evaluation and experimental results
- Conclusion
- Future Work
- References and publications

Border gateway protocol: messages

- Understanding elements of BGP messages important to:
  - analyse changes in the protocol
  - identify anomalies and intrusions
- Past analysis of BGP datasets consider only changes in BGP update messages
- Open: sent after establishing a TCP connection and upon confirmation of its receipt
- Keepalive: sent upon successfully establishing a TCP connection and periodically afterwards to ensure that BGP peers are reachable
- Update: used for routing advertisements and withdrawals exchange between BGP peers
- Notification: sent when an error condition is detected followed by closing the BGP connection

Border gateway protocol: finite state machine

- BGP finite state machine (FMS): used to describe the process of establishing a TCP connection between peers
- Outgoing: active or connecting peer sending the first TCP SYN packet
- Incoming: passive or listening peer sending the first SYN/ACK
- BGP peers initialize a TCP connection unless configured to remain:
  - in the Idle state
  - as passive peer



BGP routing protocol overview: http://gponsolution.com/bgp-routing-protocol-overview.html.

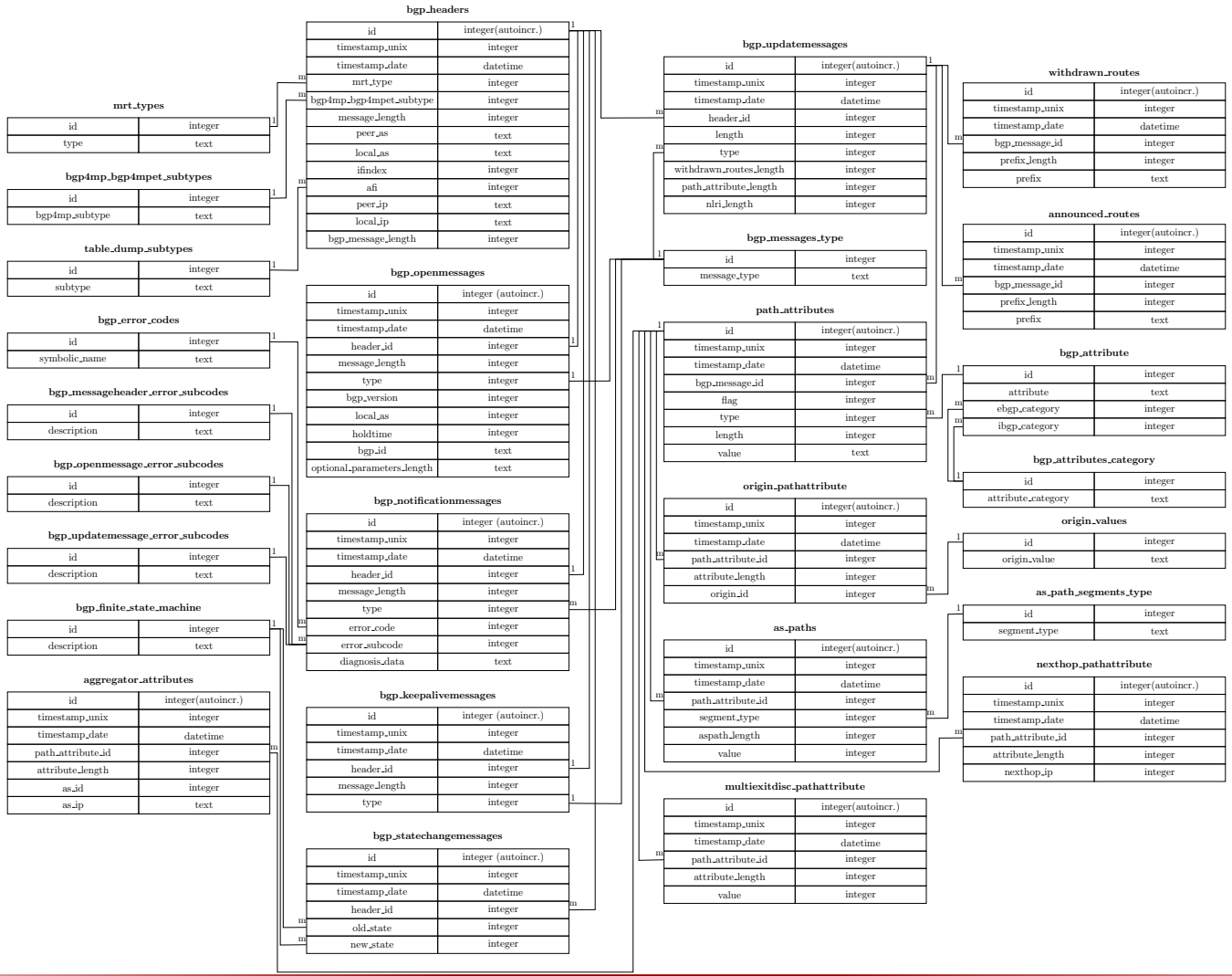
Relational database: data processing

- BGP data: downloaded from RIPE and Route Views collection sites
- Use the module dataDownload.py that employs the Python Requests HTTP library
- The mrtparser Python module used to:
  - convert raw BGP data from MRT to ASCII using the object class Reader
  - store converted data in YAML files by using the mrt2yaml.py script
- An ingestion engine is used to:
  - initialize the database tables
  - insert entries based on processed data in the generated YAML file

Relational database: model

- Relational databases: employed to create links between multiple tables
- Links between tables are defined using:
  - logical keys: used to search for a specific row and are typically defined using unique strings
  - primary keys: unique integer values that may be defined when creating a table or automatically assigned by the database when adding a new row
  - foreign keys: have number values that refer to a primary key of a row in a different table
- Primary and foreign keys: employed to generate queries that require joining multiple tables
- The BGP-RDB database:
  7 core, 7 lookup, 7 list, and 8 detail tables

Relational database: schema



Roadmap

- Introduction
- Border Gateway Protocol: anomalies and datasets
- Relational database for Border Gateway Protocol
- Ransomware attacks
- Supervised and semi-supervised algorithms
- Performance evaluation and experimental results
- Conclusion
- Future Work
- References and publications

Ransomware attacks

- Advanced cryptography algorithms to lock victims' data until a ransom is paid
- Types of ransomware attacks:
  - Cryptoworm: replicate themselves to targeted hosts for maximum reach and impact
  - Ransomware as a Service (RaaS): sold on the dark web as distribution kits, typically deployed via malicious spam e-mails or exploit kits
  - Automated active adversary: attackers scan the Internet for systems with weak protection, enter the system, and plan the attack for the maximum damage
- Rely on tools and processes: runtime packers and exploits
- During the encryption: data are partially or fully renamed
- Store the encrypted data on the used (overwrite) or available (copy) disk sectors

WannaCrypt ransomware attack

- Cryptoworm ransomware that affected systems running Microsoft Windows 7:
  - works by gaining administrative privileges
  - employs the EternalBlue exploit and DoublePulsar backdoor
- May 12, 2017 to May 15, 2017
- Infected over 230,000 computers in 150 countries
- Spreads throughout a network by attempting to connect to TCP port 445
- Replicates by querying for the non-existing domains:
  - www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
  - www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
- Replication: prevented if the victims receive a response indicating that these domains are registered

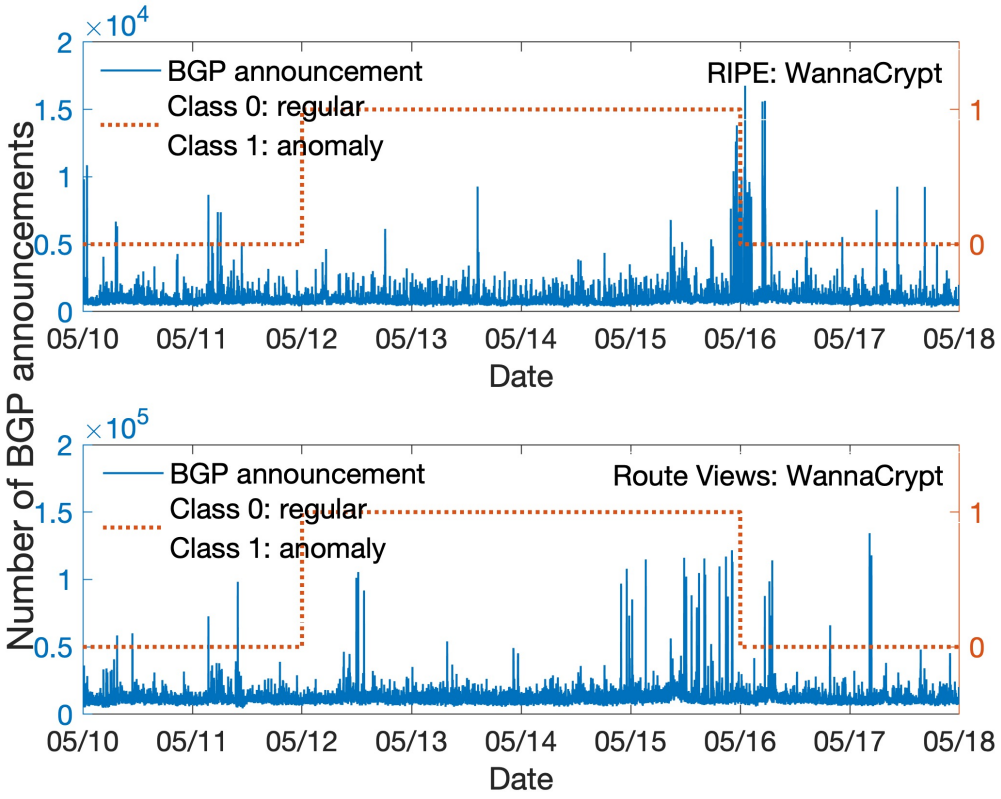
WestRock ransomware attack

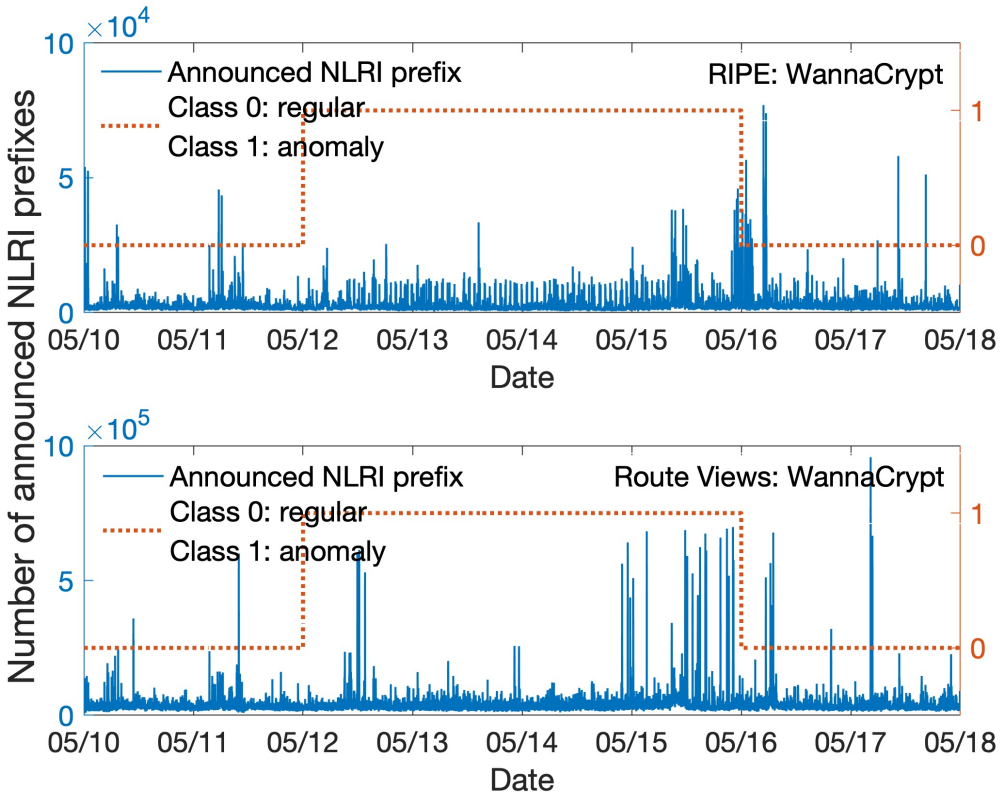
- WestRock Company second largest packaging company in USA:
  - over 320 manufacturing facilities worldwide
  - experienced a ransomware attack detected on January 23, 2021
- Over 6 days, the attack impacted the company's systems:
  - information technology (IT): store, process, maintain, and operate data
  - operational technology (OT): monitor and control industrial processes, events, and devices
- Caused delays in shipments of goods and production levels
- Controlled remediation plan: executed in phases including systems shutdown and security measures enhancements
- Between 1:12 UTC on 23.01.2021 and 23:59 UTC on 29.01.2021

Datasets: data collection

- Collected BGP update messages:
  - 8 days during the WannaCrypt
  - 11 days during the WestRock
- Data downloaded from RIPE collection site:
  - rrc04 (WannaCrypt): Geneva, Switzerland with 20 peer ASes
  - rrc14 (WestRock): Palo Alto, CA, USA with 28 peer ASes
- Data downloaded from Route Views collection site:
  - route-views2 (WannaCrypt): Oregon, USA with 77 peer ASes
  - telxatl (WestRock): Atlanta, GA, USA with 36 peer ASes

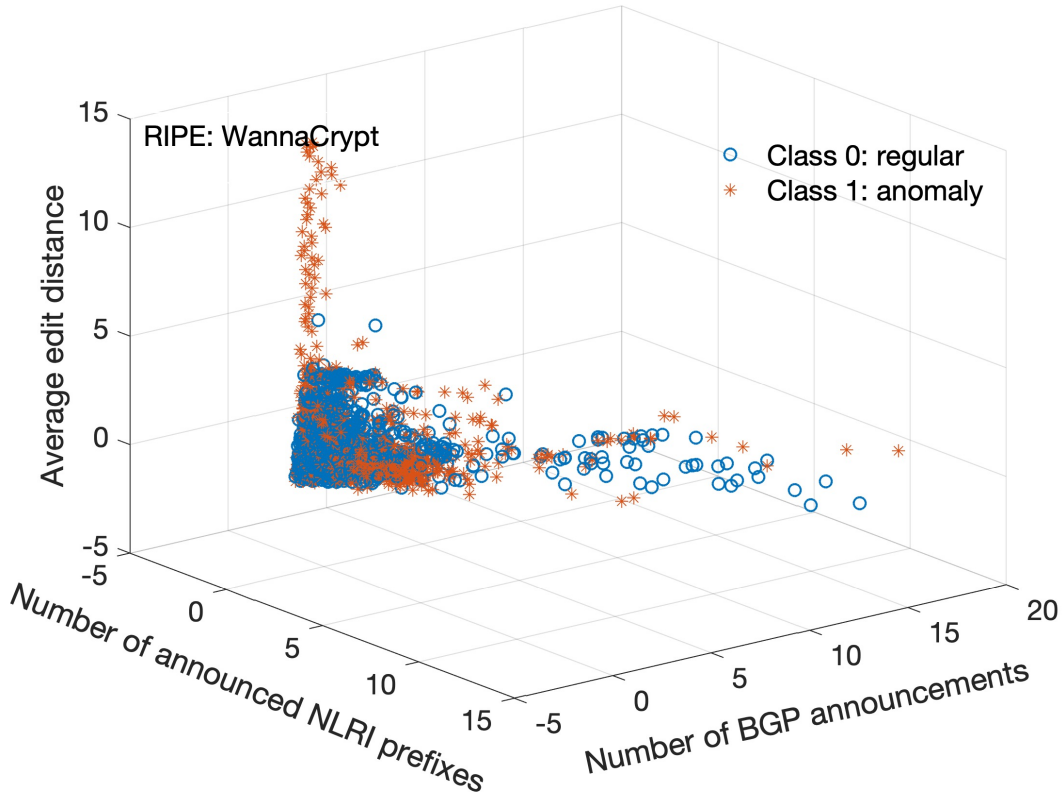
WannaCrypt data visualization: patterns during regular and anomalous events

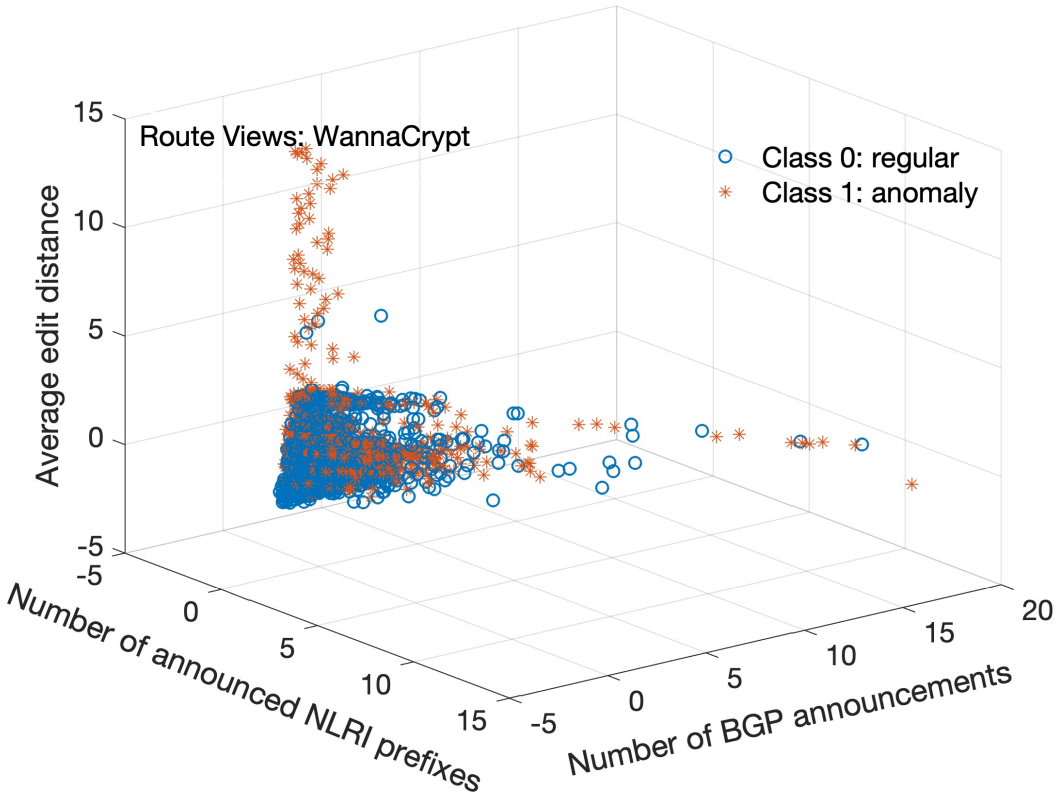




WannaCrypt datasets: 11,520 data points, attack lasted 5,760 minutes

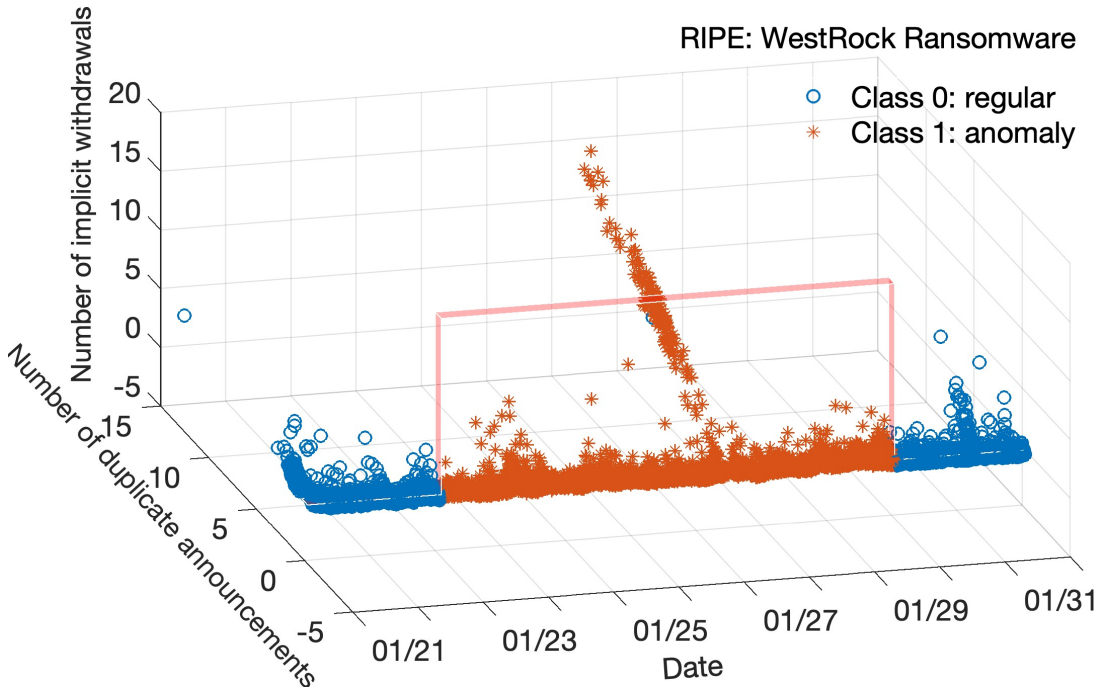
WannaCrypt data visualization: spatial separation for regular and anomalous classes

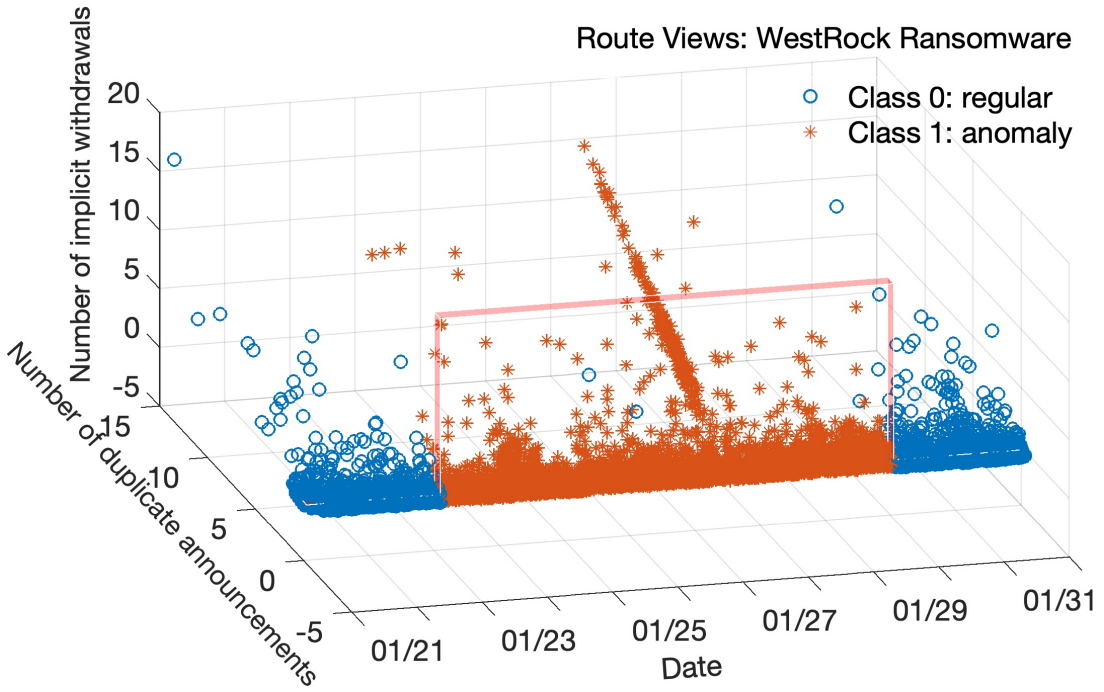




WannaCrypt datasets: 11,520 data points, attack lasted 5,760 minutes

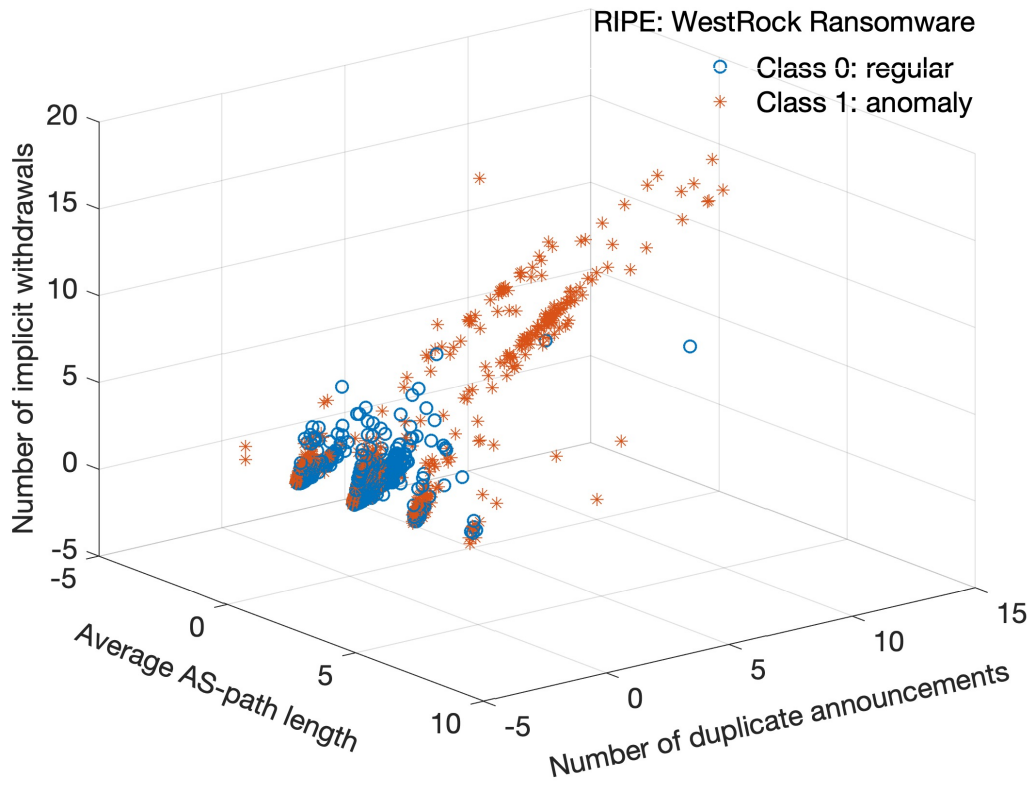
WestRock data visualization: patterns during regular and anomalous events

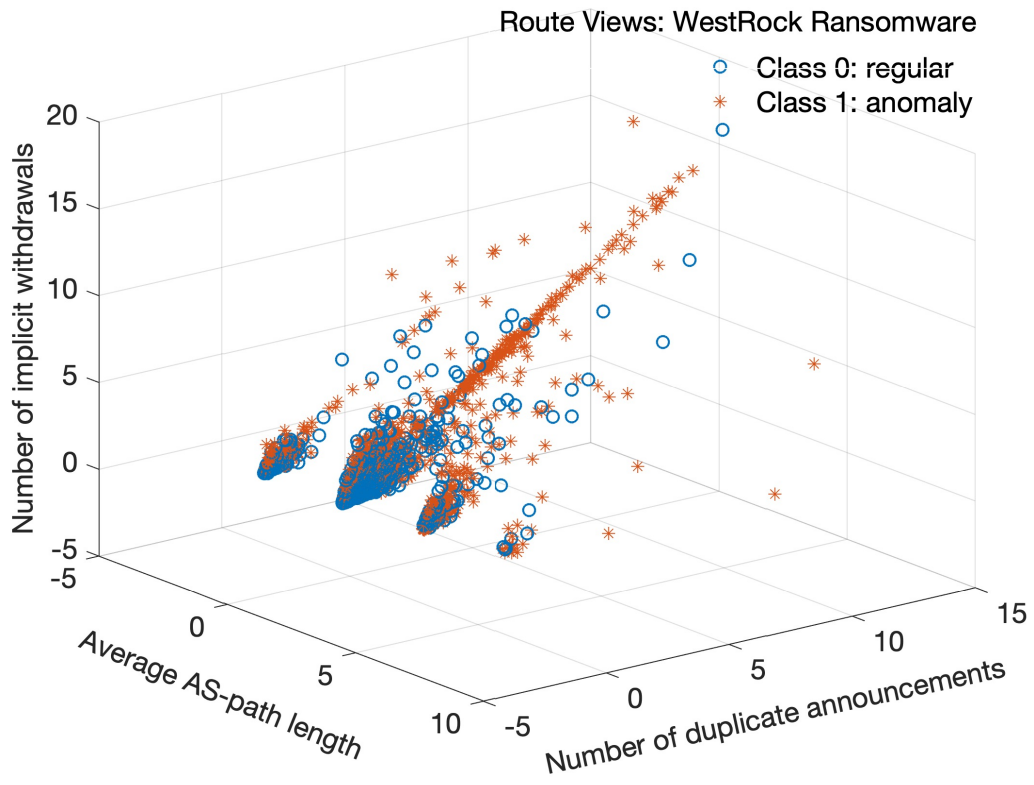




WestRock datasets: 15,840 data points, attack lasted 10,008 minutes

WestRock data visualization: spatial separation for regular and anomalous classes





WestRock datasets: 15,840 data points, attack lasted 10,008 minutes

Roadmap

- Introduction
- Border Gateway Protocol: anomalies and datasets
- Relational database for Border Gateway Protocol
- Ransomware attacks
- Supervised and semi-supervised algorithms
- Performance evaluation and experimental results
- Conclusion
- Future Work
- References and publications

Implemented machine learning algorithms

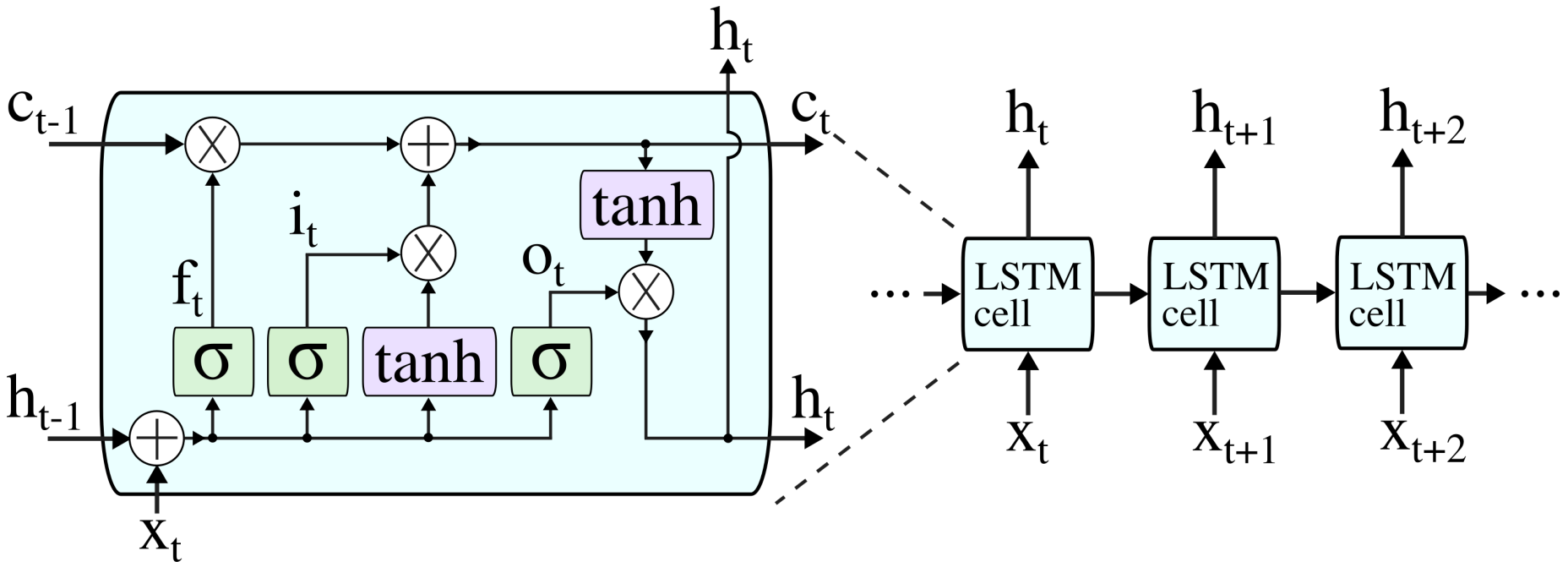
- Recurrent recurrent neural networks (RNNs):
  - LSTM, GRU
- Broad learning system (BLS) and its extensions:
  - incremental learning, RBF-BLS, CFBLS, CEBLS, CFEBLS
- Variable features broad learning system:
  - VFBLS, VCFBLS
- Extremely randomized trees (Extra-Trees)
- Gradient boosting decision trees (GBDT):
  - XGBoost, LightGBM, CatBoost
- Isolation forest (iForest) for label refinement

Recurrent neural networks: long-short term memory

- Capable of learning long-term dependencies by connecting time intervals to form a continuous memory
- Composed of:
  - forget gate f_t: discards irrelevant memories based on the cell state
  - input gate i_t: controls the information that will be updated in the LSTM cell
  - output gate o_t: functions as a filter that controls the output

Recurrent neural networks: long-short term memory

- Repeating module for the Long-Short Term Memory (LSTM) neural network:



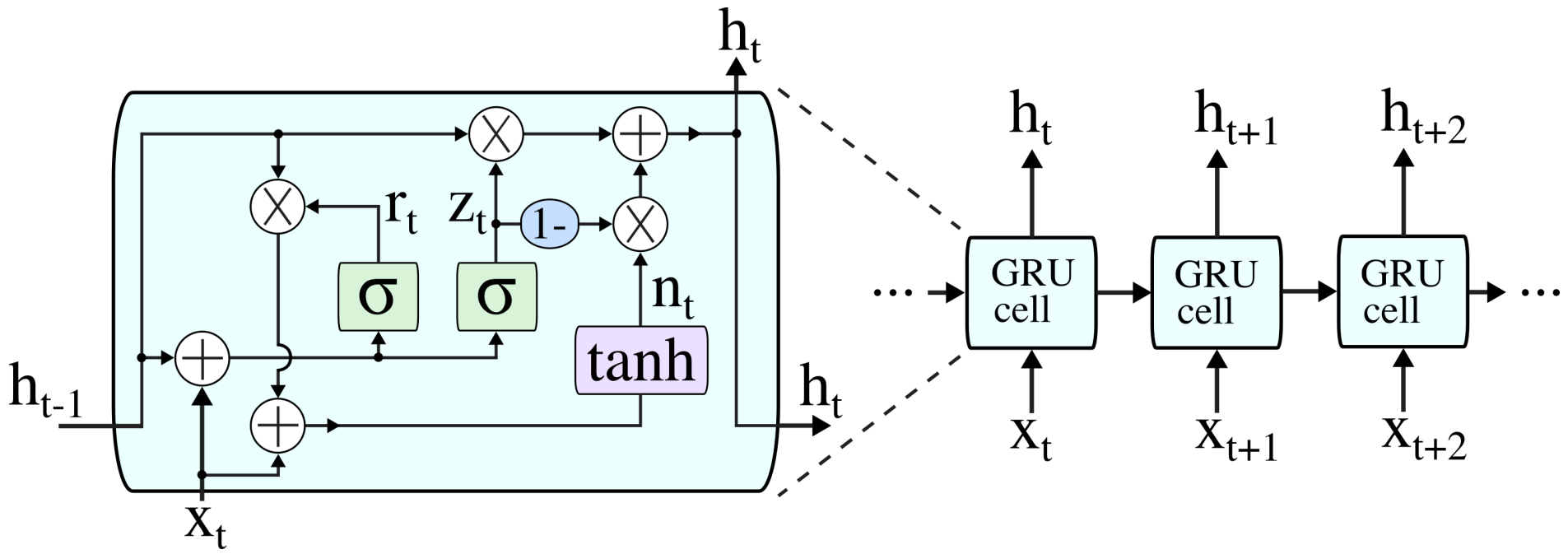
K. Greff, R. K. Srivastava, J. Koutnik, B. R. Steunebrink, and J. Schmidhuber, "LSTM: a search space odyssey," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 10, pp. 2222–2232, Oct. 2017.

Recurrent neural networks: gated recurrent unit

- Derived from LSTM with a simpler structure
- Gated mechanisms control input and memory at the current timestep
- Consists of:
  - reset gate r_t : determines the combination of new input information and previous memory content
  - update gate z_t : defines the content stored at the current timestep

Recurrent neural networks: gated recurrent unit

- Repeating module for the Gated Recurrent Unit (GRU) neural network:

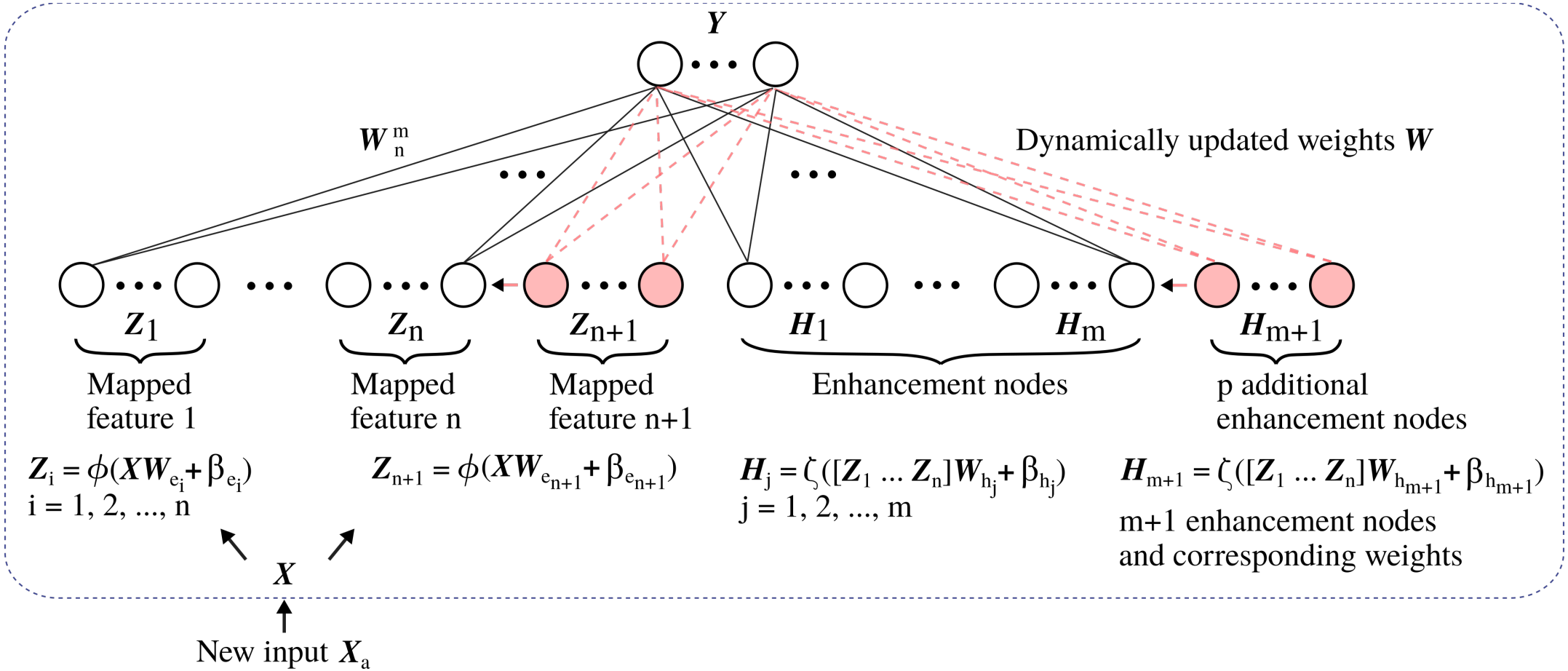


K. Cho, B. van Merriënboer, C. Gülçehre, D. Bahdanau, F. Bougares, H. Schwenk, and Y. Bengio, "Learning phrase representations using RNN encoder-decoder for statistical machine translations," in *Proc. Conf. Empirical Methods Natural Lang. Process.*, Doha, Qatar, Oct. 2014, pp. 1724–1734.

Broad learning system

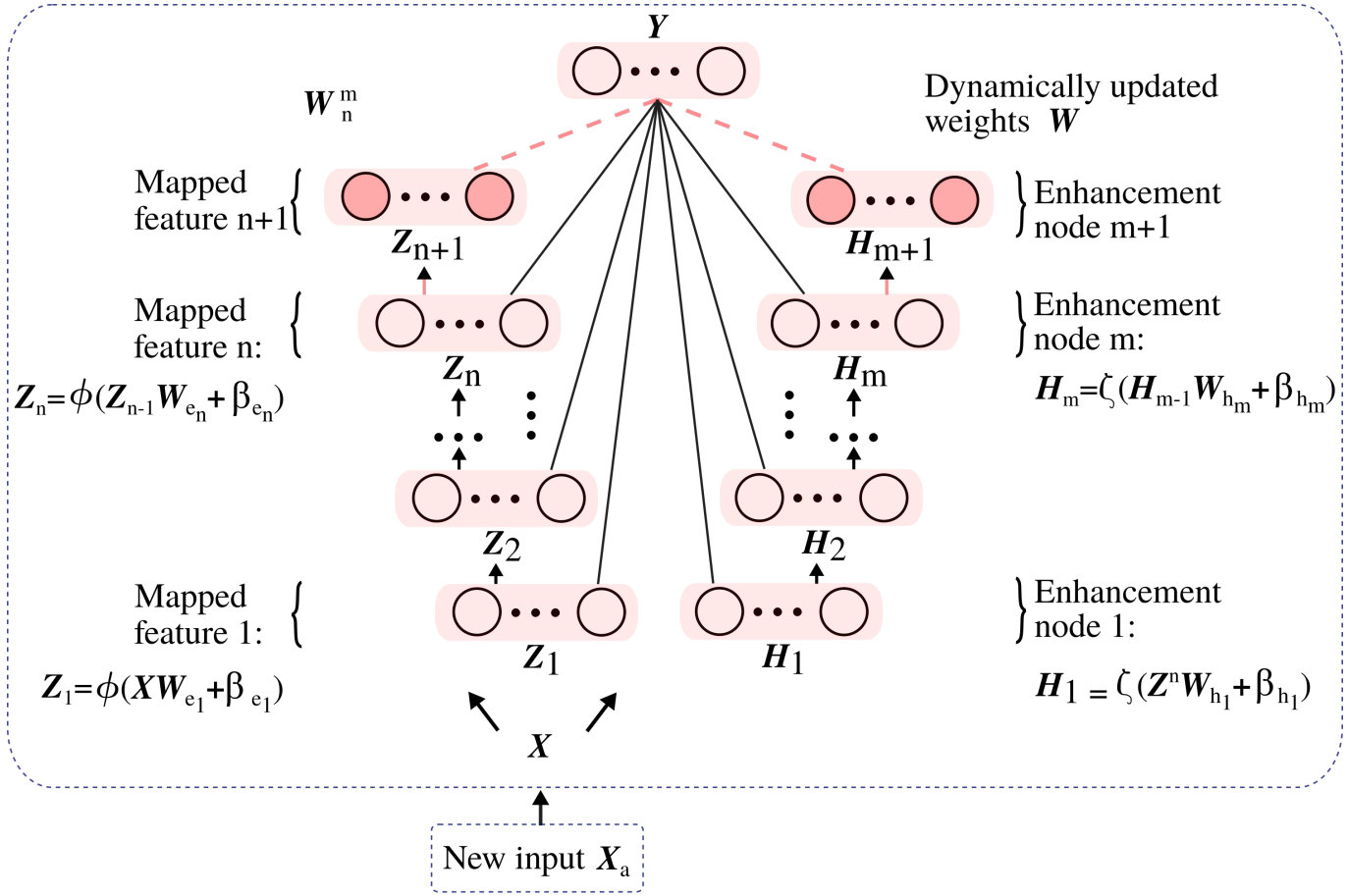
- Single layer feed-forward neural network containing sets:
  - n mapped features ($\boldsymbol{Z}^n$)
  - m enhancement nodes ($\boldsymbol{H}^m$)
- State matrix $\boldsymbol{A}_n^m$: concatenation of Z^n and H^m
- Moore-Penrose pseudo-inverse or ridge regression: invert $\boldsymbol{A}_n^m$ and calculate output weights $\boldsymbol{W}_n^m$ for given labels $\boldsymbol{Y}$
- BLS extensions:
  - incremental learning
  - radial basis function network BLS (RBF-BLS)
  - cascades of: mapped features (CFBLS), enhancement nodes (CEBLS), both mapped features and enhancement nodes (CFEBLS)

Broad learning system: BLS with increments of input data, mapped features, and enhancement nodes



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.

Broad learning system: CFEBLS with increments of input data, mapped features, and enhancement nodes



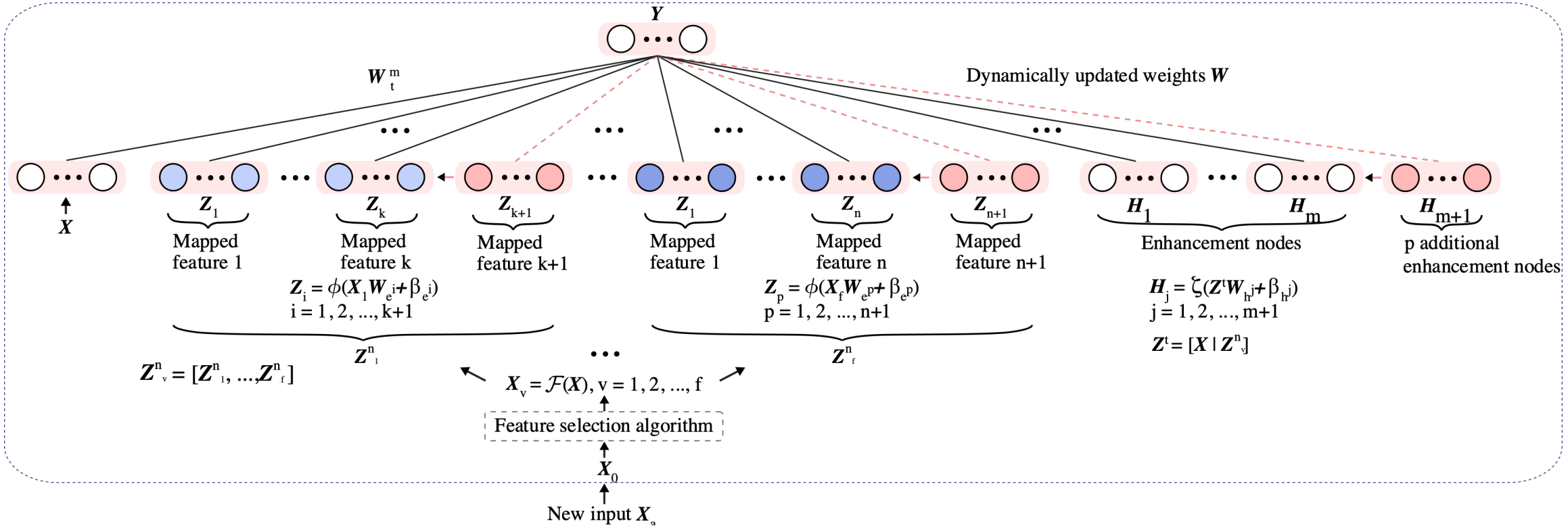
C. L. P. Chen, Z. Liu, and S. Feng, "Universal approximation capability of broad learning system and its structural variations," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 4, pp. 1191–1204, Apr. 2019.

Variable features and variable features with cascades broad learning system

- Expand the BLS network by using:
  - original input data
  - subsets of input data using feature extraction
  - variable number of mapped features
- Develop more generalized models
- Single experiment with integrated stages:
  - feature selection
  - model generation
- Incremental learning of input data: implemented to rank and select features in each incremental step

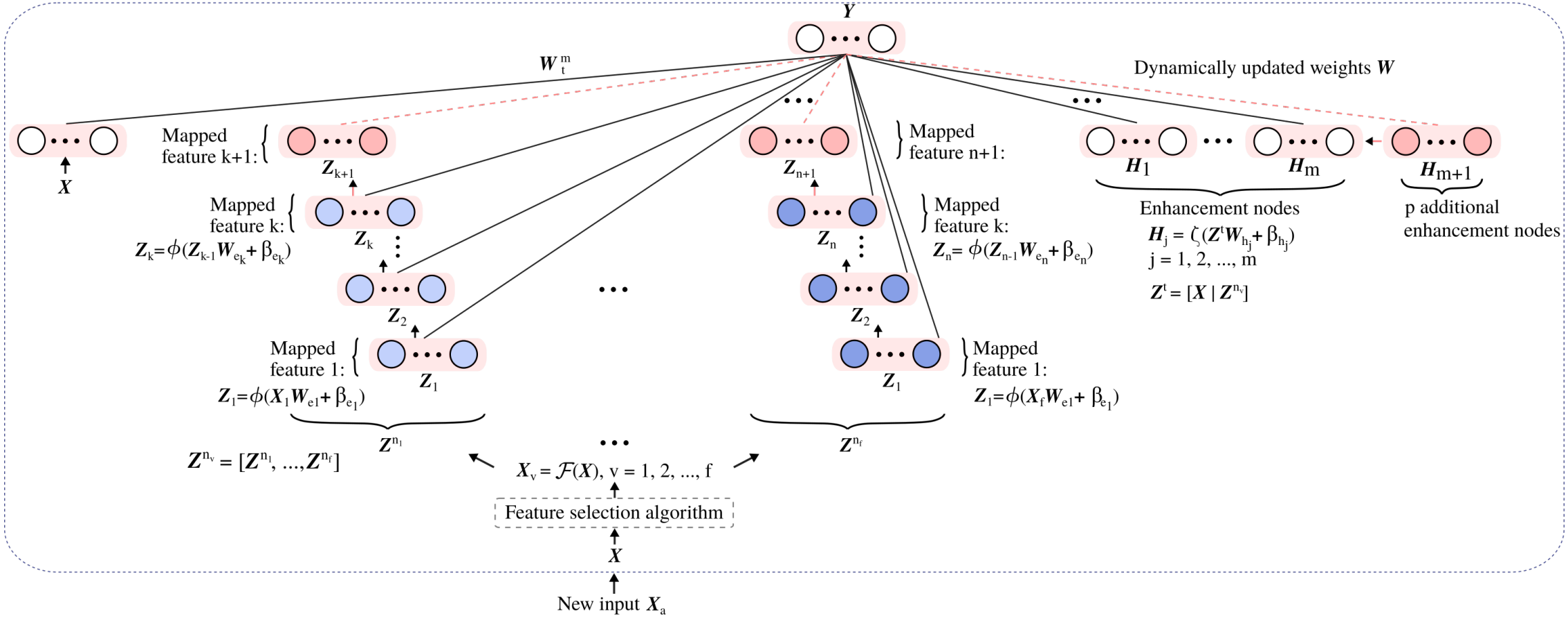
Z. Li, A. L. Gonzalez Rios, and Lj. Trajkovic, "Machine learning for detecting anomalies and intrusions in communication networks," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 7, pp. 2254–2264, July 2021.

Variable features BLS: VFBLS with increments of input data, mapped features, and enhancement nodes



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

Variable features BLS: VCFBLS with increments of input data, mapped features, and enhancement nodes



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

Extremely randomized trees

- The Gini importance is used to compute feature scores in a given dataset:

$$Importance(\boldsymbol{X}_c) = \frac{1}{N^T} \sum_T \sum_{t \in T: v(s_t) = \boldsymbol{X}_c} p(t) \Delta i(s_t, t),$$

- where:
  - $\boldsymbol{X}_c$: subset of $\boldsymbol{X}$ corresponding to one feature
  - N_T: number of trees
  - t: index of a node in a tree
  - s_t: direction of the split
  - $v(s_t)$: randomly generated threshold
  - $p(t)$: weight
  - $\Delta i(s_t, t)$: decrease of the node impurity equivalent to its importance

Gradient boosting decision trees

- Boosting algorithms:
  - class of ensemble learning
  - greedy algorithms sequentially including estimators (base learners)
  - goal: minimize the loss function by including estimators trained based on residuals
- Gradient boosting machines (GBM): boosting algorithms that employ functional gradient descent to minimize the loss function
- Gradient boosting decision trees (GBDT):
  - GBM variant employing decision trees as estimators
  - optimized GBDT algorithms: XGBoost, LightGBM, CatBoost

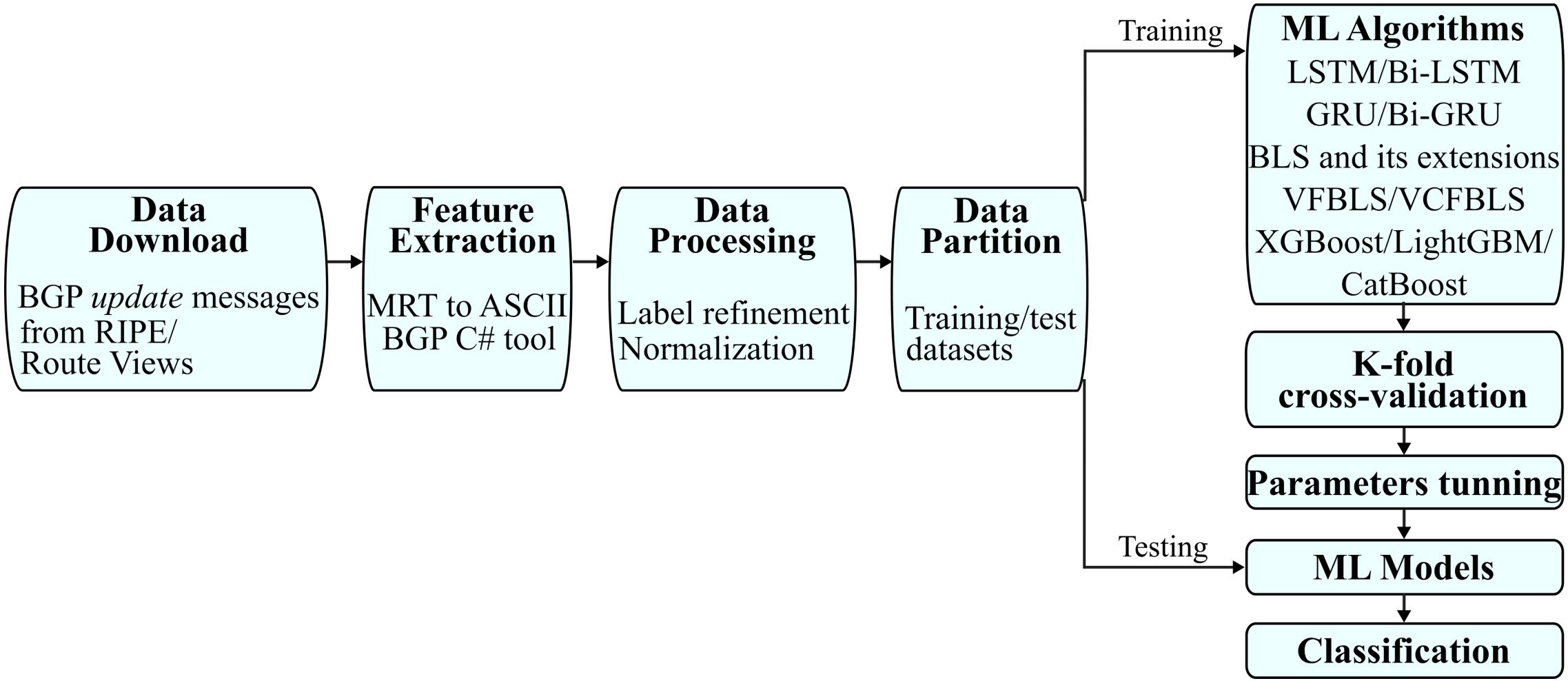
Isolation forest

- Unsupervised algorithm for anomaly detection
- Short execution time due to linear complexity
- Ensemble of binary decision trees isolation trees (iTrees):
  - split values: randomly selected for each feature based on the range of their values
  - data points: iteratively routed through the based on the defined split values until a node has only one instance or all node data have the same values
- Scores calculated based on the average path length $E(h(x))$ from root to leaf:
  - outlier: score close to 1
  - inlier: score close to 0
  - indistinct: score approximately 0.5

Roadmap

- Introduction
- Border Gateway Protocol: anomalies and datasets
- Relational database for Border Gateway Protocol
- Ransomware attacks
- Supervised and semi-supervised algorithms
- Performance evaluation and experimental results
- Conclusion
- Future Work
- References and publications

Experimental procedure



WannaCrypt: the best performance of RNN, Bi-RNN, BLS, VFBLS, VCFBLS, and GBDT models

Model	Refinement	Collection site	No. Ftr.	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)	TP	FP	TN	FN
$LSTM_3$	none	RIPE	37	12.67	65.48	63.22	60.73	65.94	1,543	998	1,862	797
GRU_3		Route Views	37	12.01	72.63	74.14	64.50	87.18	2,040	1,123	1,737	300
GRU_2	iForest	RIPE	37	17.16	67.89	63.38	65.10	61.78	1,445	776	2,085	894
$LSTM_4$		Route Views	37	22.83	76.46	76.00	70.20	82.86	1,938	823	2,038	401
$Bi\text{-}LSTM_4$	none	RIPE	37	41.85	66.96	64.30	62.58	66.11	1,547	925	1,935	793
$Bi\text{-}GRU_4$		Route Views	37	27.98	79.39	79.60	71.79	89.27	2,089	821	2,039	251
$Bi\text{-}LSTM_4$	iForest	RIPE	37	29.82	64.08	65.95	57.48	77.34	1,809	1,338	1,523	530
$Bi\text{-}GRU_4$		Route Views	37	29.10	80.79	79.70	75.97	83.79	1,960	620	2,241	379
RBF-BLS	none	RIPE	37	3.67	55.73	56.68	50.48	64.62	1,512	1,483	1,397	828
CFBLS		Route Views	37	0.62	50.67	55.21	46.55	67.82	1,587	1,822	1,058	753
RBF-BLS	iForest	RIPE	37	1.02	55.61	56.46	50.37	64.22	1,502	1,480	1,401	837
BLS		Route Views	37	19.07	50.79	52.38	46.24	60.41	1,413	1,643	1,238	926
Incr. BLS	none	RIPE	37	16.44	46.97	62.10	45.69	96.92	2,268	2,696	184	72
Incr. CEBLS		Route Views	37	16.73	56.65	63.97	50.98	85.85	2,099	1,932	948	33
Incr. CFEBLS	iForest	RIPE	37	3.36	50.96	61.73	47.46	88.29	2,065	2,286	595	274
Incr. CEBLS		Route Views	37	14.81	56.82	60.98	51.24	75.29	1,761	1,676	1,205	578
VFBLS	none	RIPE	37, 16, 8	6.49	55.06	46.07	49.85	42.82	1002	1008	1872	1338
		Route Views	37, 16, 8	5.51	48.60	53.33	44.97	65.51	1,533	1,876	1,004	807
	iForest	RIPE	37, 16, 8	6.36	55.04	46.06	49.80	42.84	1,002	1,010	1,871	1,337
		Route Views	37, 16, 8	3.50	48.14	52.88	44.60	64.94	1,519	1,887	994	820
VCFBLS	none	RIPE	37, 16, 8	3.97	54.92	46.70	49.69	44.06	1,031	1,044	1,836	1,309
		Route Views	37, 16, 8	4.92	49.18	53.17	45.29	64.36	1,506	1,819	1,061	834
	iForest	RIPE	37, 16, 8	3.98	54.92	46.73	49.66	44.12	1,032	1,046	1,835	1,307
		Route Views	37, 18, 8	3.84	50.09	53.57	45.94	64.26	1,503	1,769	1,112	836
Incr. VFBLS	none	RIPE	37, 16, 8	6.66	53.22	64.36	48.87	94.23	2,205	2,307	573	135
		Route Views	37, 16, 8	4.86	56.82	64.10	51.10	85.98	2,012	1,926	954	328
	iForest	RIPE	37, 16, 8	6.88	53.30	64.13	48.89	93.16	2,179	2,278	603	160
		Route Views	37, 16, 8	4.83	57.09	64.10	51.27	85.46	1,999	1,900	981	340
Incr. VCFBLS	none	RIPE	37, 16, 8	8.64	53.20	64.32	48.86	94.10	2,202	2,305	575	138
		Route Views	37, 16, 8	10.30	55.98	64.24	50.51	88.21	2,064	2,022	858	276
	iForest	RIPE	37, 16, 8	6.84	53.01	64.40	48.75	94.83	2,218	2,332	549	121
		Route Views	37, 16, 8	8.88	55.10	64.07	49.94	89.35	2,090	2,095	786	249
XGBoost	none	RIPE	8	0.54	59.87	61.18	54.01	70.56	1,651	1,406	1,474	689
		Route Views	16	0.87	53.05	59.56	48.51	77.14	1,805	1,916	964	535
	iForest	RIPE	8	1.31	61.19	61.69	55.31	69.73	1,631	1,318	1,563	708
		Route Views	16	1.02	52.20	59.12	47.93	77.13	1,804	1,960	921	535
LightGBM	none	RIPE	8	0.09	60.25	61.48	54.35	70.77	1,656	1,391	1,489	684
		Route Views	37	0.14	52.74	59.18	48.29	76.41	1,788	1,915	965	552
	iForest	RIPE	8	0.15	66.08	61.41	54.17	70.88	1,658	1,403	1,478	681
		Route Views	37	0.23	52.38	58.95	48.02	76.31	1,785	1,932	949	554
CatBoost	none	RIPE	8	1.09	60.31	62.04	54.30	72.35	1,693	1,425	1,455	647
		Route Views	16	0.70	52.30	59.30	48.01	77.48	1,813	1,963	917	527
	iForest	RIPE	8	0.66	60.48	61.98	54.47	71.91	1,682	1,406	1,475	657
		Route Views	16	0.70	52.32	59.30	48.01	77.51	1,813	1,963	918	526

WestRock: the best performance of RNN, Bi-RNN, BLS, VFBLS, VCFBLS, and GBDT models

Model	Refinement	Collection site	No. Ftr.	Training time (s)	Accuracy (%)	F-Score (%)	Precision (%)	Sensitivity (%)	TP	FP	TN	FN
GRU_4	none	RIPE	37	13.99	75.23	80.24	74.84	86.48	3,459	1,163	1,717	541
$LSTM_4$		Route Views	37	18.95	55.42	70.72	57.20	92.60	3,704	2,771	109	296
$LSTM_2$	iForest	RIPE	37	12.63	75.36	79.73	76.41	83.35	3,333	666	1,029	1,852
$LSTM_3$		Route Views	37	13.77	60.00	69.06	62.75	76.80	3,072	1,824	1,056	928
$Bi\text{-}GRU_4$	none	RIPE	37	20.59	78.49	81.92	80.10	83.83	3,353	833	2,047	647
$Bi\text{-}GRU_3$		Route Views	37	21.89	62.50	69.70	65.73	74.18	2,967	1,547	1,333	1,033
$Bi\text{-}GRU_4$	iForest	RIPE	37	23.73	84.27	86.90	84.23	89.75	3,589	672	2,209	410
$Bi\text{-}GRU_3$		Route Views	37	20.23	64.74	72.19	66.67	78.70	3,148	1,574	1,306	852
RBF-BLS	none	RIPE	37	3.98	55.70	70.75	57.41	92.18	3,687	2,735	145	313
		Route Views	37	2.60	54.74	69.99	56.95	90.78	3,631	2,745	135	369
	iForest	RIPE	37	2.20	55.73	70.77	57.42	92.20	3,687	2,734	147	312
		Route Views	37	3.97	54.61	69.81	56.91	90.28	3,611	2,734	146	389
Incr. RBF-BLS	none	RIPE	37	1.71	58.20	73.55	58.18	99.98	3,999	2,875	5	1
Incr. CEBLS		Route Views	37	23.33	57.89	73.31	58.05	99.48	3,979	2,876	4	21
Incr. RBF-BLS	iForest	RIPE	37	33.28	58.20	73.54	58.16	99.98	3,998	2,876	5	1
		Route Views	37	7.01	58.15	73.52	58.16	99.93	3,997	2,876	4	3
VFBLS	none	RIPE	37, 16, 8	7.31	55.15	70.18	57.19	90.80	3,632	2,718	162	368
		Route Views	37, 16, 8	7.99	54.75	69.92	56.99	90.45	3,618	2,731	149	382
	iForest	RIPE	37, 16, 8	6.18	54.74	69.81	57.00	90.05	3,601	2,716	165	398
		Route Views	37, 16, 8	5.67	54.23	69.41	56.76	89.33	3,573	2,722	158	427
VCFBLS	none	RIPE	37, 16, 8	4.14	55.33	70.31	57.30	90.95	3,638	2,711	169	362
		Route Views	37, 16, 8	4.62	54.68	69.73	56.99	89.80	3,592	2,710	170	408
	iForest	RIPE	37, 16, 8	6.56	54.72	69.86	56.98	90.27	3,610	2,726	155	389
		Route Views	37, 18, 8	4.66	54.43	69.55	56.87	89.53	3,581	2,716	164	419
Incr. VFBLS	none	RIPE	37, 16, 8	6.77	58.17	73.54	58.16	100	4,000	2,878	2	0
		Route Views	37, 16, 8	6.82	58.18	73.55	58.16	100	4,000	2,877	3	0
	iForest	RIPE	37, 16, 8	11.60	58.27	73.55	58.23	99.80	3,991	2,863	18	8
		Route Views	37, 16, 8	7.62	58.20	73.55	58.18	99.98	3,999	2,875	5	1
Incr. VCFBLS	none	RIPE	37, 16, 8	12.04	58.23	73.57	58.19	99.98	3,999	2,873	7	1
		Route Views	37, 16, 8	9.08	58.30	73.57	58.25	99.85	3,994	2,863	17	6
	iForest	RIPE	37, 16, 8	11.27	58.15	73.53	58.14	99.98	3,998	2,878	3	1
		Route Views	37, 16, 8	10.40	58.20	73.56	58.17	100	4,000	2,876	4	0
XGBoost	none	RIPE	8	0.54	60.44	73.38	60.26	93.80	3,752	2,474	406	248
		Route Views	37	0.27	55.83	70.94	57.44	92.73	3,709	2,748	132	291
	iForest	RIPE	8	0.52	59.84	73.05	59.88	93.62	3,744	2,508	373	255
		Route Views	8	0.38	55.58	70.42	57.46	90.93	3,637	2,693	187	363
LightGBM	none	RIPE	16	0.05	58.37	72.20	59.01	92.98	3,719	2,583	297	281
		Route Views	8	0.06	57.50	72.16	58.27	94.73	3,789	2,713	167	211
	iForest	RIPE	37	0.10	57.66	71.42	58.77	91.02	3,640	2,554	327	359
		Route Views	16	0.05	57.72	72.81	58.14	97.38	3,895	2,804	76	105
CatBoost	none	RIPE	8	0.33	55.60	71.36	57.09	95.15	3,806	2,861	19	194
		Route Views	8	0.31	58.17	73.53	58.16	99.95	3,998	2,876	4	2
	iForest	RIPE	16	0.32	55.58	71.34	57.07	95.12	3,804	2,861	20	195
		Route Views	8	0.48	58.24	73.53	58.22	99.78	3,991	2,864	16	9

Discussion

- Bi-GRU_4: best classification model for
  - WannaCrypt: Route Views data with label refinement
  - WestRock: RIPE data with label refinement
- LightGBM models offer the shortest training times
- Highest sensitivity: incremental VFBLS and VCFBLS
- Highest precision: RNN and Bi-RNN

Roadmap

- Introduction
- Border Gateway Protocol: anomalies and datasets
- Relational database for Border Gateway Protocol
- Ransomware attacks
- Supervised and semi-supervised algorithms
- Performance evaluation and experimental results
- Conclusion
- Future Work
- References and publications

Conclusion: relational database BGP-RDB

- Implemented a relational database: BGP-RDB
- Based on:
  - BGP messages: open, update, keepalive, notification
  - state transitions of TCP connections: idle, connect, opensent, openconfirm, active
- Raw MRT data: downloaded from RIPE and Route Views data collection sites
- Developed using sqlite3 Python module:
  - enable easy integration with Python-based anomaly detection systems

Conclusion: comparison of machine learning algorithms

- Evaluated performance:
  - RNN, Bi-RNN, BLS, VFBLS, VCFBLS, and GBDT supervised algorithms
  - WannaCrypt and WestRock datasets
- Semi-supervised machine learning:
  - Label refinement: iForest unsupervised algorithm to identify regular data points within anomalous periods and improve performance
  - Classification: based on supervised algorithms
- Performance evaluation based on:
  - training time, accuracy, F-Score, precision, sensitivity (recall), confusion matrix
- Bi-GRU_4 models generated the best classification performance

Roadmap

- Introduction
- Border Gateway Protocol: anomalies and datasets
- Relational database for Border Gateway Protocol
- Ransomware attacks
- Supervised and semi-supervised algorithms
- Performance evaluation and experimental results
- Conclusion
- Future Work
- References and publications

Future work

- Generate new features based on:
  - BGP messages
  - State transitions of a TCP connection
- Re-create current BGP datasets by querying the BGP-RDB database
- Integrate the BGP-RDB database into real-time anomaly detection systems
- Explore for label refinement:
  - other anomaly detection unsupervised algorithms
  - clustering algorithms
- Implementation of various feature selection algorithms for VFBLS and VCFBLS algorithms

Roadmap

- Introduction
- Border Gateway Protocol: anomalies and datasets
- Relational database for Border Gateway Protocol
- Ransomware attacks
- Supervised and semi-supervised algorithms
- Performance evaluation and experimental results
- Conclusion
- Future Work
- References and publications

References: Border Gateway Protocol

- RFC:
  - A Border Gateway Protocol 4 (BGP-4): https://datatracker.ietf.org/doc/html/rfc4271
- Collection sites:
  - RIPE NCC: https://www.ripe.net/analyse.
  - University of Oregon Route Views projects: http://www.routeviews.org
- Tools:
  - zebra-dump-parser: https://github.com/\rfc1036/zebra-dump-parser
  - BGP C sharp tool: https://github.com/communication-networks-laboratory/BGP_c_sharp_tool

References: anomaly detection

- Surveys:
  - 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.
  - P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly based network intrusion detection: techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1–2, pp. 18–28, Feb.–Mar. 2009.
  - A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2016.
- BGP:
  - B. Al-Musawi, P. Branch, and G. Armitage, "BGP anomaly detection techniques: a survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 377–396, 2017.

References: machine learning algorithms

- Books:
  - I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: The MIT Press, 2016.
  - K. P. Murphy, *Probabilistic Machine Learning: An introduction*. Cambridge, MA, USA: The MIT Press, 2022.
- Surveys and journals:
  - 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.
  - J. E. van Engelen and H. H. Hoos, "A survey on semi-supervised learning," *Mach. Learn.*, vol. 109, no. 2, p. 373–440, Feb. 2020.

Publications

- Journals:
  - Z. Li, A. L. Gonzalez Rios, and Lj. Trajković, "Machine learning for detecting the WestRock ransomware attack using BGP routing records," *IEEE Commun. Mag.*, submitted for publication.
  - Z. Li, A. L. Gonzalez Rios, and Lj. Trajković, "Machine learning for detecting anomalies and intrusions in communication networks," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 7, pp. 2254–2264, July 2021.
- Conferences:
  - H. K. Takhar, A. L. Gonzalez Rios, and Lj. Trajković, "Comparison of virtual network embedding algorithms for data center networks," in *Proc. IEEE Int. Symp. Circuit Syst.*, Austin, Texas, USA, May 2022, pp. 1660—1664 (virtual).
  - 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).

Publications

- A. L. Gonzalez Rios, K. Bekshentayeva, Maheeppartap Singh, Soroush Haeri, and Lj. Trajković, "Virtual network embedding for switch-centric data center networks," in *Proc. IEEE Int. Symp. Circuit Syst.*, Daegu, Korea, May 2021, pp. 1—5 (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.
- 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, PP. 1—5 (virtual).
- 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, pp. 1–5.
- A. L. Gonzalez Rios, Z. Li, G. Xu, A. Diaz Alonso, and Lj. Trajković, "Detecting network anomalies and intrusions in communication networks," in *Proc. 23rd IEEE Int. Conf. Intell. Eng. Syst. 2019*, Godollo, Hungary, April 2019, pp. 29–34.