Machine Learning Techniques for Detecting BGP Anomalies

ENSC 499: B.A.Sc. (Honours) Thesis Defense

Hardeep Kaur Takhar
School of Engineering Science
Simon Fraser University

Roadmap

- **Motivation and Introduction**
- **Overview of Related Work**
- **BGP Data and Machine Learning Algorithms**
- **Evaluation Procedure**
- **Conclusion and References**

Roadmap

- **Motivation and Introduction**
- Overview of Related Work
- BGP Data and Machine Learning Algorithms
- Evaluation Procedure
- Conclusion and References

Motivation

- **Internet:**
  - Designed as a transparent communication network
  - Prone to malicious activities:
    - increase in cyber attacks and crime
- Deployment of IoT, e-commerce, and social networks, has led to numerous devices connected to the Internet
- Anomaly detection in communication networks using machine learning techniques is an important topic in cybersecurity
- Machine learning techniques have been widely advocated to enhance anomaly detection

Source: J. Kurose and K. Ross, "Computer networks and the Internet," in Computer Networking: A Top-Down Approach, 6th ed., New Jersey, U.S.A: Pearson, 2013, pp. 1-80.

Introduction

- **Anomalies:**
  - Non conforming patterns in data
  - Caused due to faulty equipment, hackers, or intruders
  - Malicious intents of intruders and hackers may be stopped from reoccurring by learning the nature of anomalies from past events
  - Severe economic consequences for both individuals and corporations due to cyber attacks
- **Border Gateway Protocol (BGP):**
  - Routing protocol for establishing connections between Autonomous Systems (ASes) using TCP (port 179)
  - Routes data between ASes using an optimal path

Introduction

- **Autonomous Systems (ASes):**
  - Groups of BGP routers (peers) managed by a single administrative domain
  - The Internet is a network of interconnected ASes
  - Responsible for packet delivery and connectivity

Source: (2020, Dec.) What is an autonomous system? | What are ASNs?. [Online]. Available: https://www.cloudflare.com/learning/network-layer/what-is-an-autonomous-system/ .

Roadmap

- Motivation and Introduction
- **Overview of Related Work**
- BGP Data and Machine Learning Algorithms
- Evaluation Procedure
- Conclusion and References

Related Work

- **Supervised Machine Learning**
  - Data labels are used for anomaly and regular classes to train the classifier
  - Algorithms:
    - Support Vector Machine: SVM
    - Hidden Markov Models
    - Naïve Bayes: NB
    - Long Short-Term Memory: LSTM
    - Gated Recurrent Unit: GRU
  - SVM: not widely used for anomaly detection in large datasets due to speed
  - LSTM: widely used for sequential data

Related Work

- **Semi-Supervised Machine Learning**
  - Data labels are used for regular class only to train the classifier
  - Models:
    - generation-based
    - graph-based
    - discriminant-based
    - difference-based

Related Work

- **Unsupervised Machine Learning**
  - No data labels are used to train the model
  - Algorithms:
    - OneClass Support Vector Machine: OCSVM
    - Local Outlier Factor: LOF
    - Isolation Forest: IF
    - Elliptic Envelope: EE
  - Isolation Forest is known to outperform other unsupervised learning algorithm

Source: Y. Yasami and S. P. Mozaffari, “A novel unsupervised classification approach for net-work anomaly detection by k-means clustering and ID3 decision tree learning methods,” J. Supercomput., vol. 53, no. 1, pp. 231–245, Oct. 2010.

Roadmap

- Motivation and Introduction
- Overview of Related Work
- **BGP Data and Machine Learning Algorithms**
  - **Border Gateway Protocol (BGP) Messages**
  - **Data**
  - **BGP Update Message**
    - **BGP Features**
  - **Machine Learning Algorithms**
    - **Long-Short Term Memory: LSTM**
    - **Broad Learning System: BLS**
- Evaluation Procedure
- Conclusion and References

Border Gateway Protocol (BGP) Messages

- **BGP Messages:**
  - **Open**
  - **Update**
    - BGP update message contains protocol status and configurations
    - Its fields may be extracted to obtain critical information about the network connectivity
  - **Keepalive**
  - **Notification**
- **Examples of BGP Anomalies:**
  - Worms: Slammer, Nimda, Code Red I
  - Ransomware: WannaCrypt
  - Link failures: Moscow blackout

Data

- **Dataset:**
  - **Moscow Power Blackout:**
    - May 24, 2005, at 20:57 (MSK) to May 26, 2005, at 16:00 (MSK)
    - Complete shutdown of the Chagino substation (part of the Moscow energy ring) and subsequent failure of Moscow Internet exchange
    - Caused by a transformer failure at the substation

Data

- **BGP Update Messages Collection Sites :**
  - **Réseaux IP Européens (RIPE):**
    - Routing Information Service (RIS) project initiated by RIPE Network Coordination Centre (NCC)
    - Collectors:
      - rrc04: CIXP, Geneva
      - rrc05: VIX, Vienna
  - **Route Views:**
    - Project at the University of Oregon

Sources:
(2020, Dec.) RIPE Network Coordination Centre: About us. [Online]. Available: https://www.ripe.net/about-us/.
(2020, Dec.) RIPE NCC. [Online]. Available: https://www.ripe.net .
(2020, Dec.) University of Oregon Route Views project. [Online]. Available: http://www.routeviews.org .

BGP Update Message

- **Example of a BGP update message**

Field	Value
Time	2003 1 24 00:39:53
Type	BGP4MP/BGP4MP_MESSAGE AFI_IP
From	192.65.184.3
To	193.0.4.28
BGP packet type	Update
Origin	IGP
AS-path	513 3320 7176 15570 7246 7246 7246 7246 7246 7246 7246 7246 7246
Next-hop	192.65.184.3
Announced NLRI prefix	198.155.189.0/24
Announced NLRI prefix	198.155.241.0/24

Source: (2020, Dec.) Border Gateway Protocol (BGP) datasets with routing records collected from Reseaux IP Europeens (RIPE) and BCNET. [Online]. Available: http://www.sfu.ca/~ljilja/cnl/projects/BGP_datasets/index.html .

BGP Features

- **Features:**
  - (37 features)
  - **Categories:** Volume and AS-path

Feature type	Name
Volume	Packet size (B), Number of incomplete packets, Number of Exterior Gateway Protocol (EGP) packets, Number of Interior Gateway Protocol (IGP) packets, Inter-arrival time, Number of announcements, Number of withdrawals, Number of announced NLRI prefixes, Number of withdrawn NLRI prefixes, Number of duplicate announcements, Number of duplicate withdrawals, Number of implicit withdrawals
AS-Path	Maximum AS-path length = n: where n = (7, ..., 15), Maximum edit distance = n: where n = (7, ..., 17), Maximum edit distance, Average edit distance, Average AS-path length, Maximum AS-path length, Average unique AS-path length

Source: (2020, Dec.) Border Gateway Protocol (BGP) datasets with routing records collected from Reseaux IP Europeens (RIPE) and BCNET. [Online]. Available: http://www.sfu.ca/~ljilja/cnl/projects/BGP_datasets/index.html .

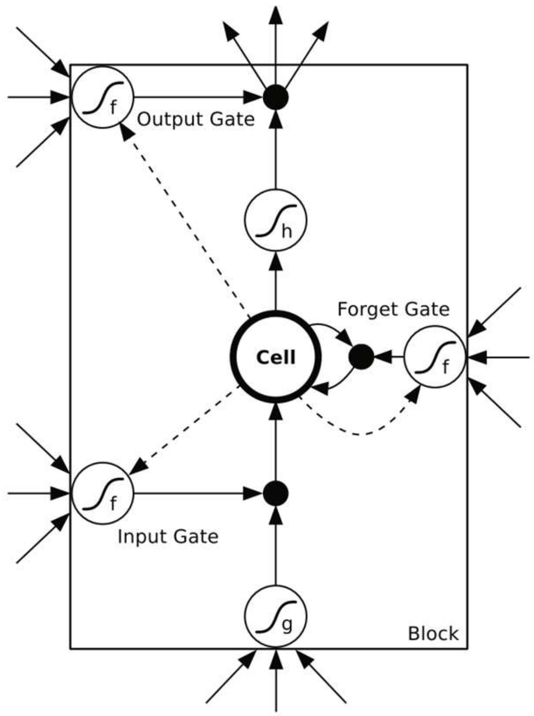
Machine Learning Algorithms

- **Machine Learning and Algorithms:**

- Supervised machine learning
  - Support Vector Machine (SVM)
  - Long-short term memory (LSTM)
  - Broad Learning System (BLS)
- Semi-Supervised learning
  - Generation based models
  - Graph based models
  - Difference or discriminant based models
- Unsupervised learning
  - Isolation Forest (IF)
  - One-class support vector machine (OCSVM)
  - Elliptic envelope (EE)

Long-Short Term Memory: LSTM

- **LSTM:**
  - a recurrent neural network
- **Benefits:**
  - does not suffer from vanishing gradient problem
  - effectively learns time sequences

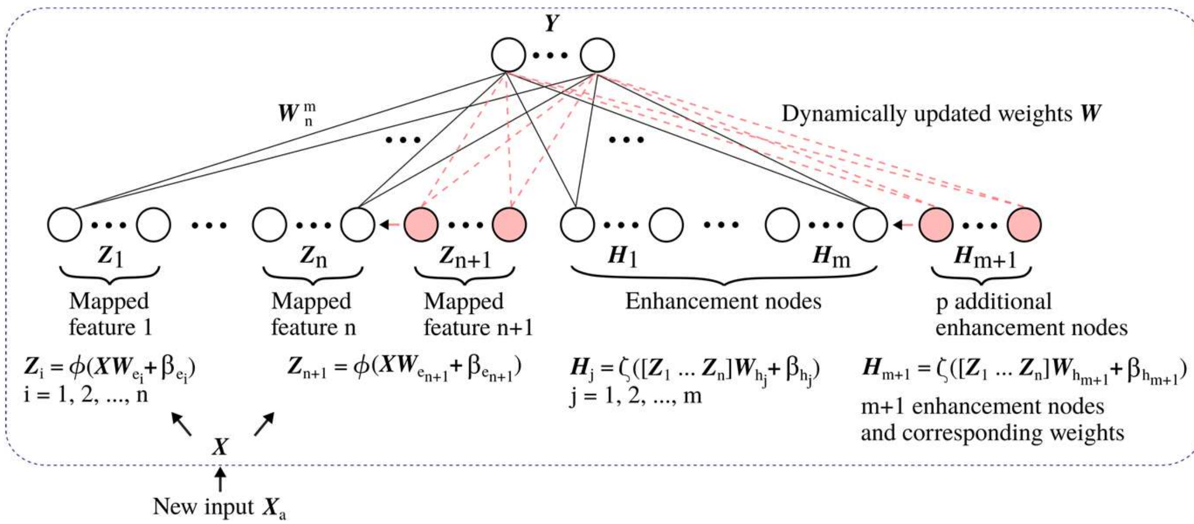


LSTM memory block with one cell

Source: A. Graves, "Supervised sequence labelling with recurrent neural networks," in *Studies in Computational Intelligence*, vol. 385, J. Kacprzyk, Ed., Berlin; Heidelberg; Verlag, Springer, 2012.

Broad Learning System: BLS

- **Architecture:**
  - mapped features
  - groups of mapped features
  - enhancement nodes



Source: 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: BLS

- **Advantages:**
  - Single layer architecture
  - Short training time
  - Model does not need retraining if additional input data are available
  - Pseudoinverse:
    - used to obtain output weights
    - faster generation of output weights

Roadmap

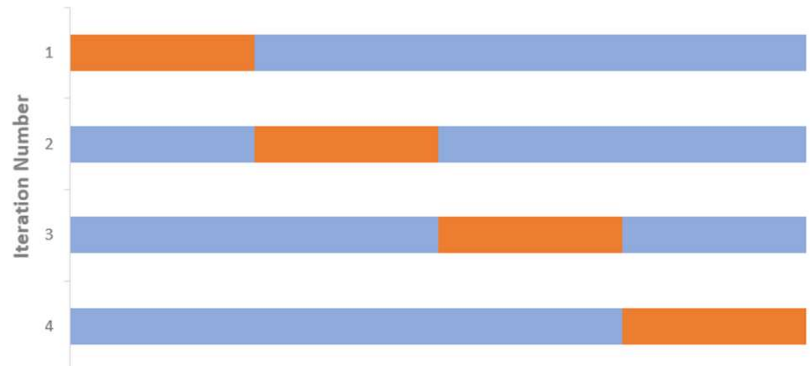
Data Labeling

- **Anomalous data:** duration of the blackout
- **Regular data:** two days prior and two days after the attack
- **Training and test datasets :**
  - **RIPE:**
    - Training dataset: 75%
    - Test dataset: 25%
  - **Route Views:**
    - Training dataset: 65%
    - Test dataset: 35%
  - Percentages refer to anomalous data points

Source: (2020, Dec.) Border Gateway Protocol (BGP) datasets with routing records collected from Reseaux IP Europeens (RIPE) and BCNET. [Online]. Available: http://www.sfu.ca/~ljilja/cnl/projects/BGP_datasets/index.html .

k-Fold Cross-Validation

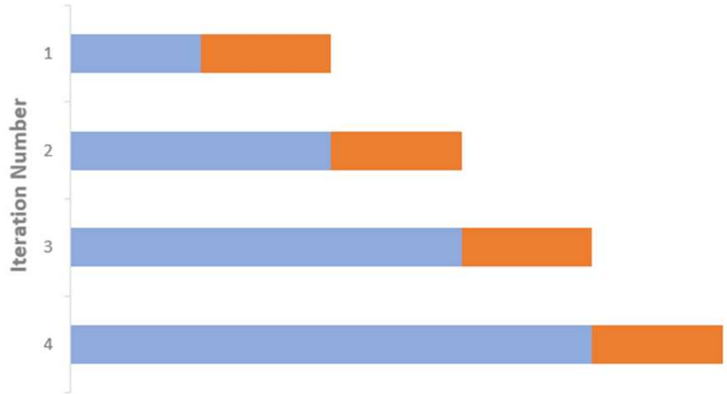
- **Cross-Validation (CV):**
  - Statistical procedure performed to generate a generalized classifier model
  - k-Fold CV is the most popular form of CV (k=10)
  - Example of four-fold CV:



Source: (2020, Dec.) Cross-validation: evaluating estimator performance [Online]. Available: https://scikit-learn.org/stable/modules/cross_validation.html .

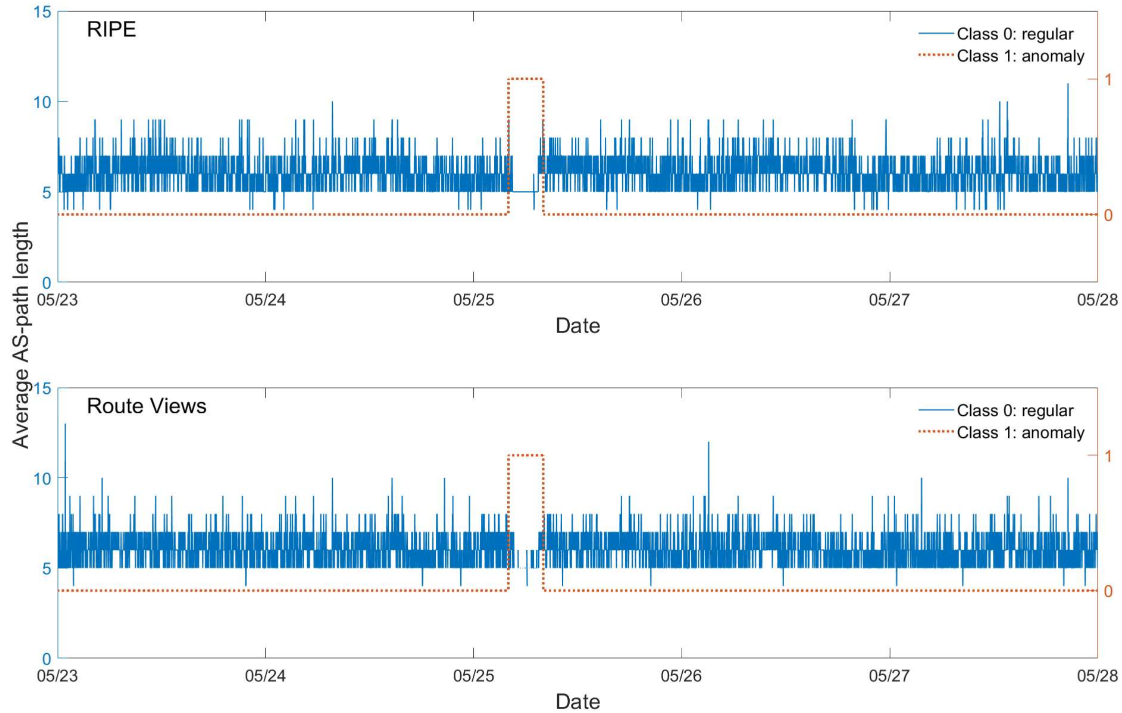
k-Fold Cross-Validation

- **Time Series Split:**
  - Variation of k-Fold cross validation
  - Training dataset (blue) and test dataset (orange)
  - Successive training datasets are concatenated over time
  - Maintains time sequence of sequential data:



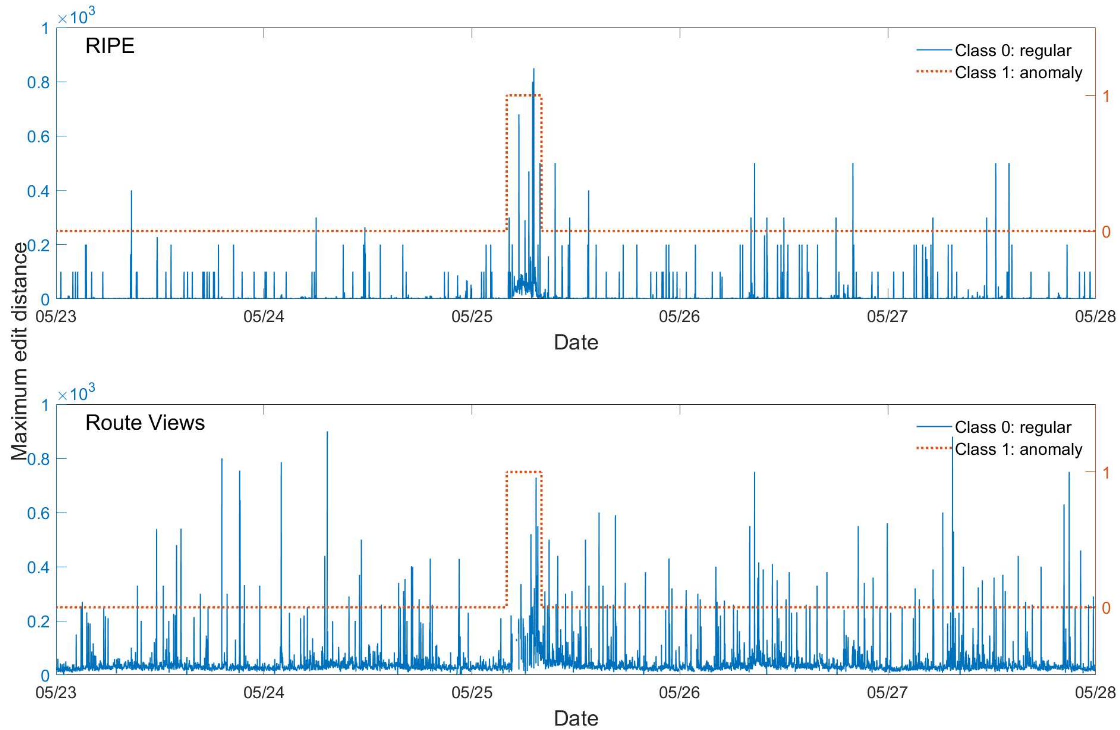
Source: (2020, Dec.) Cross-validation: evaluating estimator performance [Online]. Available: https://scikit-learn.org/stable/modules/cross_validation.html.

Moscow Blackout Data: Features



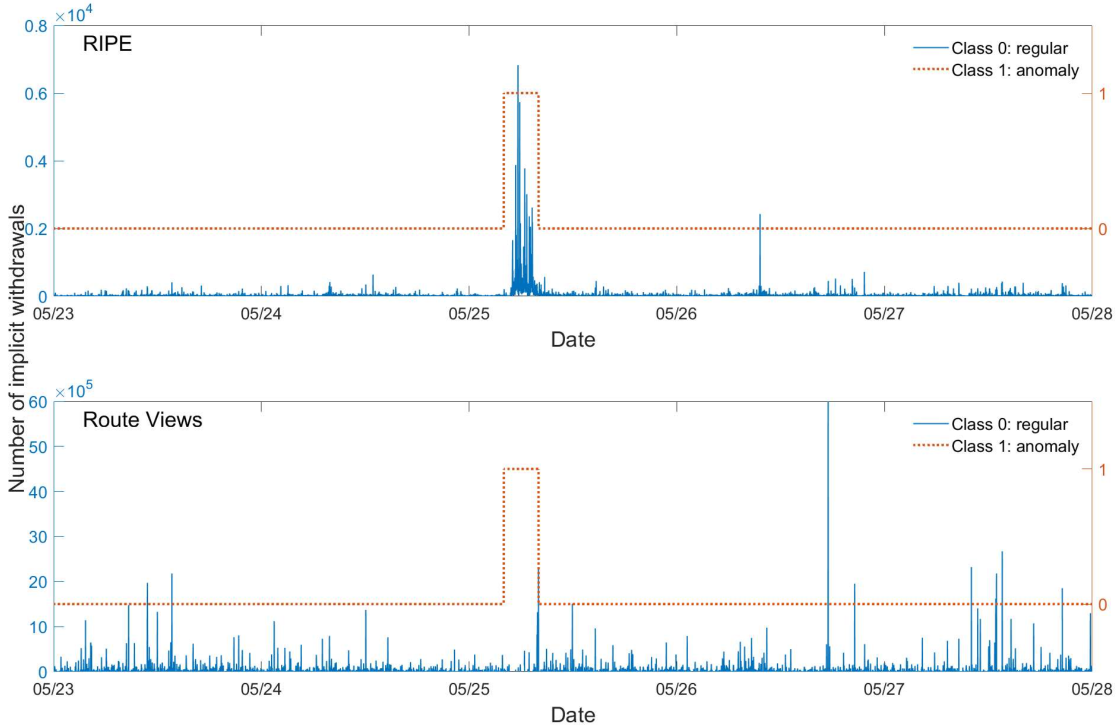
- RIPE (rrc04) and Route Views: limited samples

Moscow Blackout Data: Features



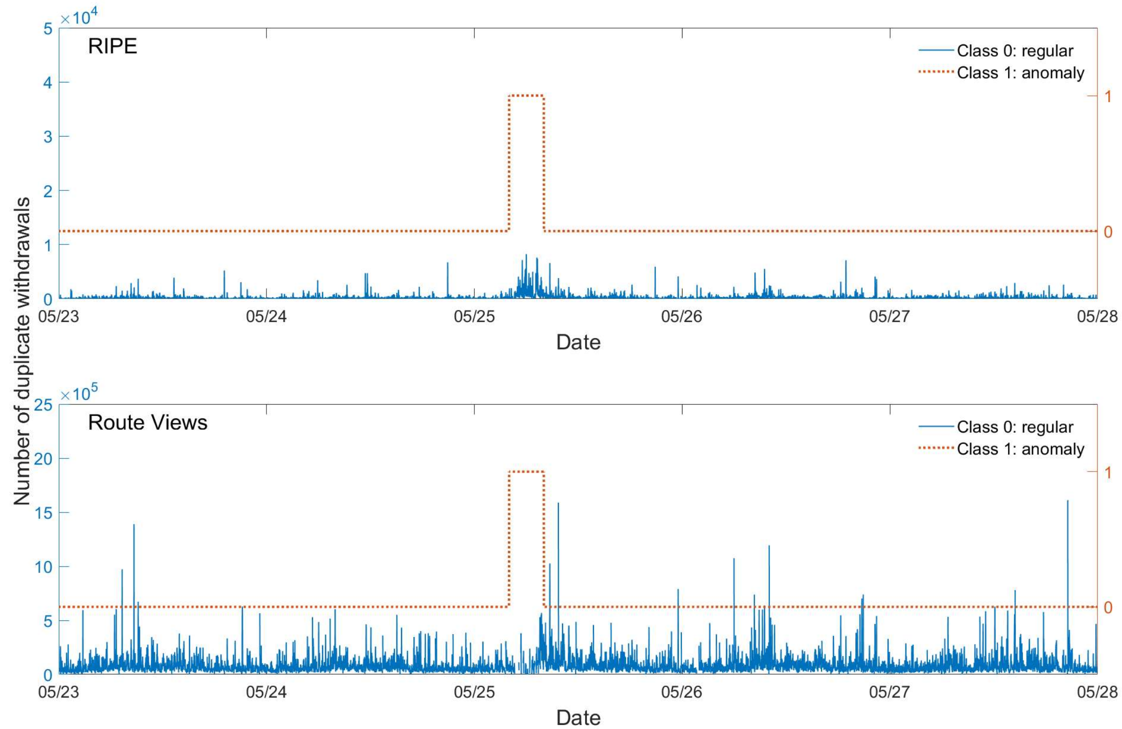
- RIPE (rrc04): increased maximum edit distance

Moscow Blackout Data: Features



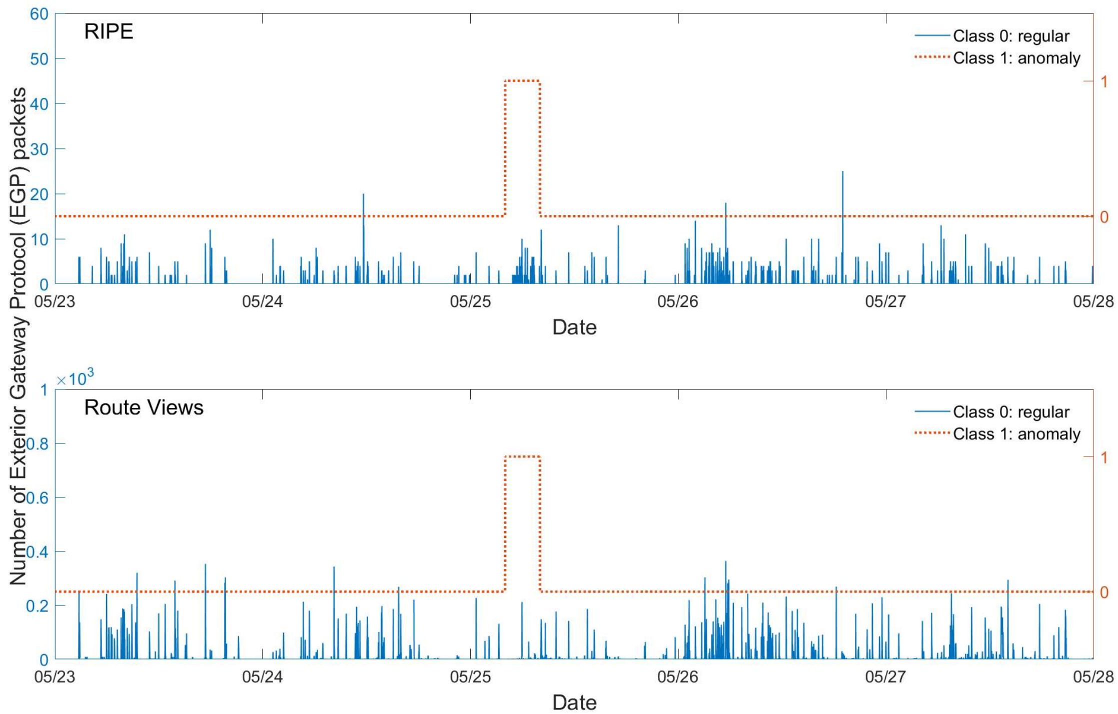
- RIPE (rrc04): high number of implicit withdrawals

Moscow Blackout Data: Features



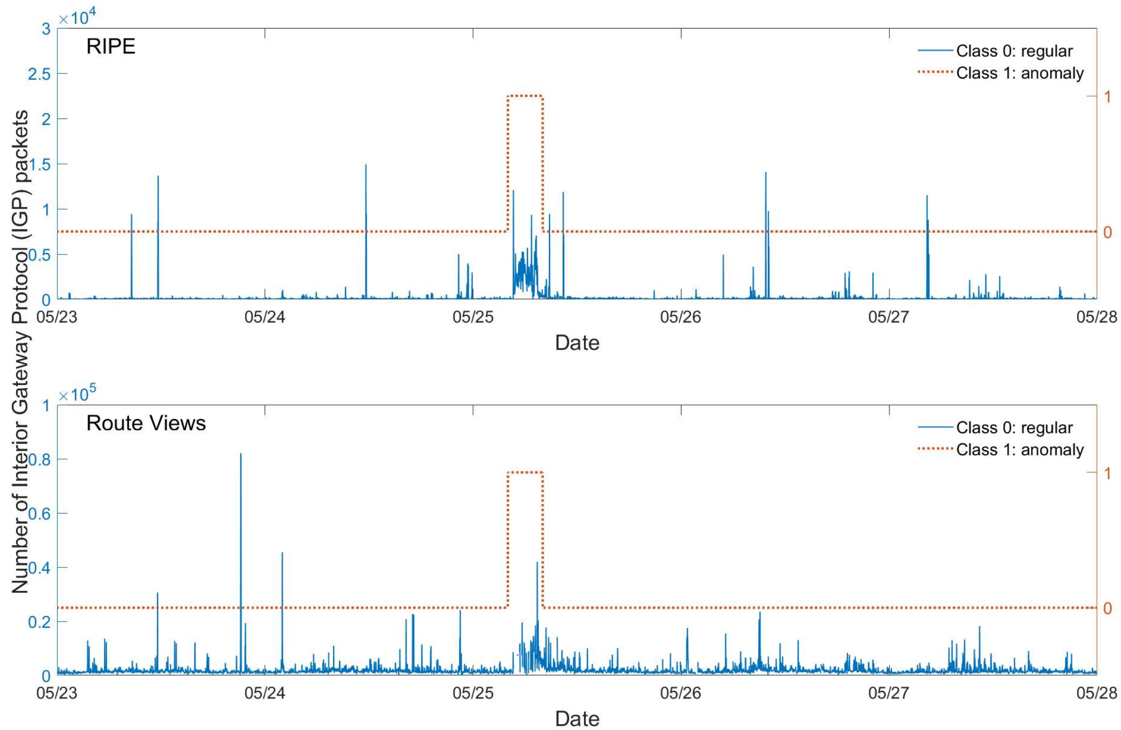
- RIPE (rrc04): high number of duplicate withdrawals

Moscow Blackout Data: Features



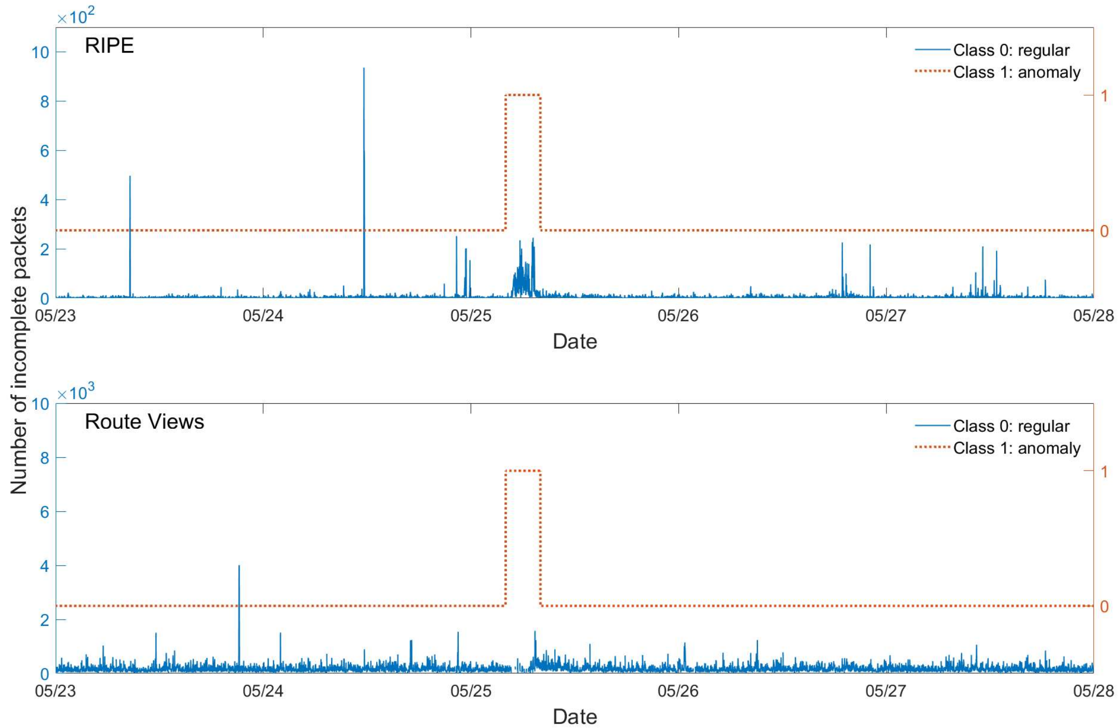
- RIPE (rrc04): increased number of EGP packets

Moscow Blackout Data: Features



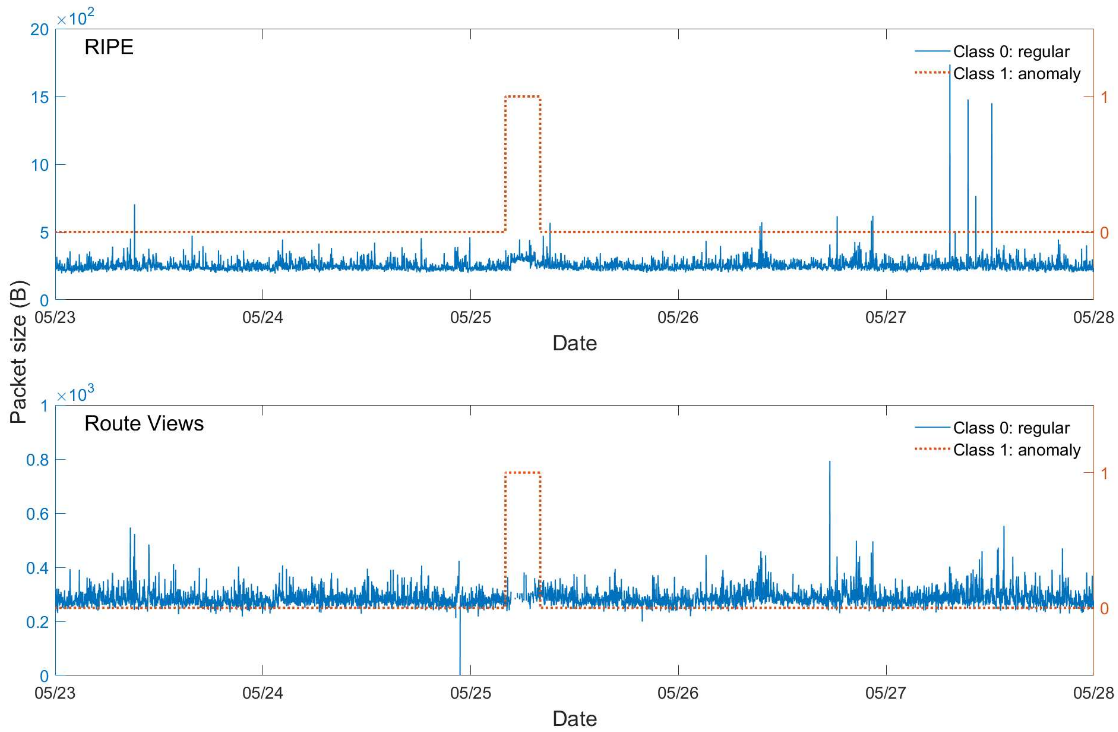
- RIPE (rrc04) and Route Views: increased number of IGP packets

Moscow Blackout Data: Features



- RIPE (rrc04): increased number of incomplete packets

Moscow Blackout Data: Features



- RIPE (rrc04): reduced packet size

Performance Metrics

- **Experiment:**
  - **Supervised machine learning:**
    - labels are required to train the classifier
    - binary classification
  - **Classification labels:**
    - **regular:** negative event
    - **anomaly:** positive event

Performance Metrics

- **Confusion matrix:**
  - **True Positive (TP):** anomalous data point classified as an anomaly
  - **False Positive (FP):** regular data point classified as an anomaly
  - **True Negative (TN):** regular data point classified as regular
  - **False Negative (FN):** anomalous data point classified as regular

		Predicted Class	
Actual Class		Regular	Anomaly
	Regular	TN	FP
	Anomaly	FN	TP

Performance Metrics

- **Precision:**
  - measures the correctly identified positive cases from all predicted positive cases
  - $\frac{TP}{TP+FP}$
  - useful when the costs of false positives is high
- **Sensitivity (recall):**
  - measures the correctly identified positive cases from all actual positive cases
  - $\frac{TP}{TP+}$
  - useful when the cost of false negatives is high

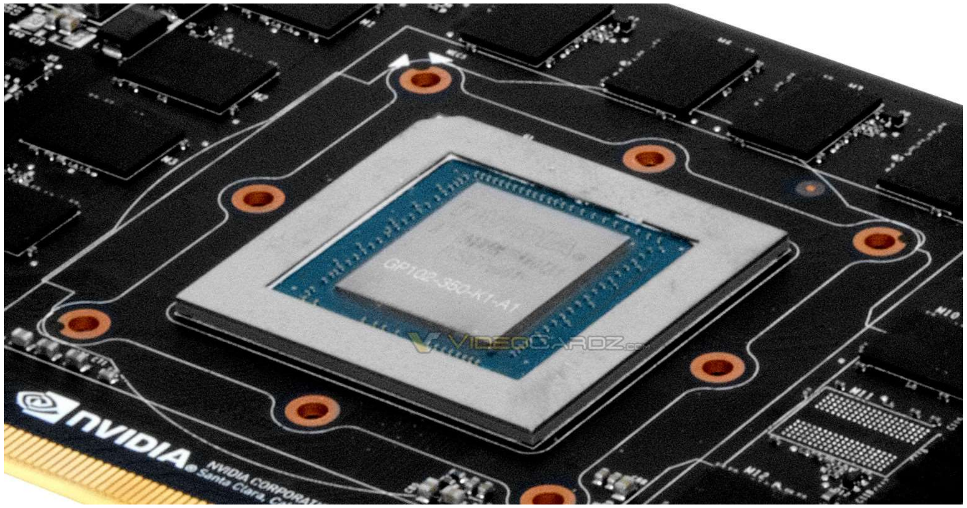
Source: (2020, Dec.) Accuracy vs. F1-Score. [Online]. Available: https://medium.com/analytics-vidhya/accuracy-vs-f1-score-6258237beca2 .

Performance Metrics

- **F-Score:**
  - harmonic mean of precision and sensitivity
  - $2 \times \frac{Precision \times Sensitivity}{Precision + Sensitivity}$
  - better for unbalanced datasets
  - better measure of incorrectly classified cases than accuracy
- **Accuracy:**
  - measure of all the correctly identified cases
  - $\frac{TP+TN}{TP+TN+FP+FN}$
  - used when all classes are equally important

Hardware Platform

- Dell Alienware Aurora with 32 GB memory and Intel Core i7 7700K processor
- Results were obtained using Python 3.6 running on Ubuntu 16.04



BLS: Performance

	Mapped features	Groups of mapped features	Enhancement nodes
Number of nodes RIPE (rrc04)	300	30	600
Number of nodes RIPE (rrc05)	400	30	300
Number of nodes (Route Views)	300	30	600

	Precision (%)	Sensitivity (recall) (%)	F-Score (%)	Accuracy (%)
RIPE (rrc04)	14.51	26.11	18.65	97.54
RIPE (rrc05)	19.58	31.11	24.03	90.64
Route Views	17.95	19.58	18.73	95.79

Source: (2020, Dec.) Broad Learning System for Classifying Network Intrusions. [Online]. Available: http://www.sfu.ca/~ljilja/cnl/projects/BLS_intrusion_detection/index.html .

BLS: Performance

Dataset	Sparse Regularization Parameter
RIPE (rrc04)	2^{-21}
RIPE (rrc05)	2^{-16}
Route Views	2^{-13}

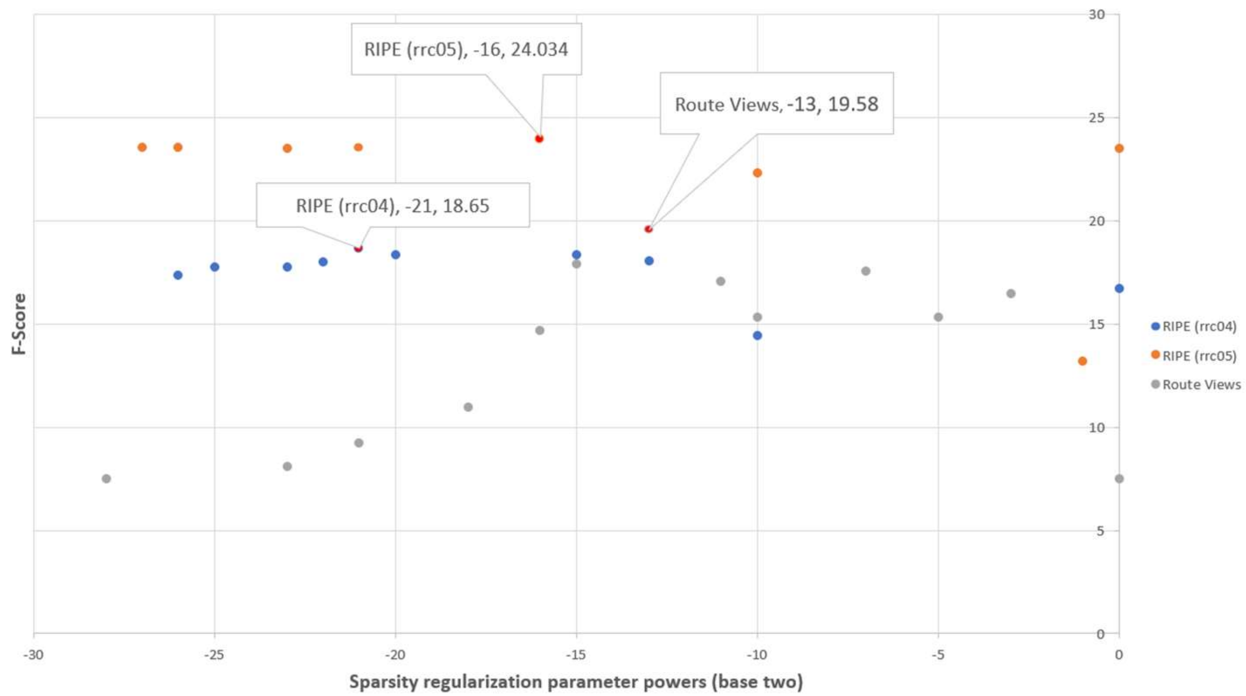
Dataset	True Positive (TP)	True Negative (TN)	False Positive (FP)	False Negative (FN)
RIPE (rrc04)	47	3,323	277	133
RIPE (rrc05)	56	3,370	230	124
Route Views	28	3,424	128	115

Source: (2020, Dec.) Broad Learning System for Classifying Network Intrusions. [Online]. Available: http://www.sfu.ca/~ljilja/cnl/projects/BLS_intrusion_detection/index.html .

F-Score: Regularization Coefficient

- **Regularization Coefficient:**
  - Used to avoid overfitting
  - Helps reduce the error of output weights
  - Improves computation of weights
- **Evaluated the effect of the coefficient on the F-Score using Moscow Blackout data**

Effect of Regularization Coefficient



- Nonlinear impact of regularization coefficient
- Highlighted are the best F-Scores

Source: (2020, Dec.) Broad Learning System for Classifying Network Intrusions. [Online]. Available: http://www.sfu.ca/~ljilja/cnl/projects/BLS_intrusion_detection .

BLS: Performance

- **Discussion:**
  - RIPE (rrc05) data: highest F-Score (24.034%)
  - Route Views and rrc04 data: Similar F-Score and accuracy
  - RIPE (rrc04) data: highest number of false positives and false negatives
  - The regularization coefficient was varied to achieve the best performance
  - BLS: did not perform well for the Moscow blackout data
  - LSTM and GRU: performed with higher accuracy due to their ability to better learn temporal dependencies in the Moscow blackout data

Sources: Z. Li, A. L. Gonzalez Rios, and L. Trajković, "Detecting Internet worms, ransomware, and blackouts using recurrent neural networks," in *Proc. IEEE Syst., Man, Cybern.*, Toronto, Canada, Oct. 2020, pp. 2165-2172.

Improving Performance

- Spatial separation of features is critical for classification:
  - better observed for RIPE datasets
- Feature selection helps improve accuracy of classifiers and reduces misclassification
- Sources of misclassification:
  - noise and redundancies in training data
  - missing data points in Route Views dataset
- Use feature selection algorithms to eliminate redundant features
- Partitioning training and test datasets:
  - training dataset: 60% to 80%
  - test dataset: 20% to 40%

Sources: Z. Li, A. L. Gonzalez Rios, and L. Trajković, "Detecting Internet worms, ransomware, and blackouts using recurrent neural networks," in *Proc. IEEE Syst., Man, Cybern.*, Toronto, Canada, Oct. 2020, pp. 2165-2172.

Roadmap

- Motivation and Introduction
- Overview of Related Work
- BGP Data and Machine Learning Algorithms
- Evaluation Procedure
- **Conclusion and References**

Conclusion

- **Blackout, a different phenomenon:**
  - Difficult to establish the window of the anomaly
  - Traffic might have been rerouted via other ASes
- **Varying windows for observing the blackout:**
  - Moscow is geographically closer to the RIPE collection sites
  - Route Views: larger number of ASes

Sources:
- Z. Li, A. L. Gonzalez Rios, and L. Trajković, "Detecting Internet worms, ransomware, and blackouts using recurrent neural networks," in *Proc. IEEE Syst., Man, Cybern.*, Toronto, Canada, Oct. 2020, pp. 2165-2172.
- A. L. Gonzalez Rios, Z. Li, G. Xu, A. Diaz Alonso, and Lj. Trajkovic, "Detecting network anomalies and intrusions in communication networks," in Proc. 23rd IEEE International Conference on Intelligent Engineering Systems 2019, Gödöllő, Hungary, April 2019, pp. 29-34.

Conclusion

- **Best Performance:**
  - **Accuracy:** RIPE
    - rrc04: **97.54%**
  - **F-Score:** RIPE
    - rrc05: **24.034%**
    - high number of false positives
- **BLS** underperformed for classifying Moscow blackout anomalies:
  - achieved better performance when classifying worm attacks

Sources:
- Z. Li, A. L. Gonzalez Rios, and L. Trajković, “Detecting Internet worms, ransomware, and blackouts using recurrent neural networks,” in *Proc. IEEE Syst., Man, Cybern.*, Toronto, Canada, Oct. 2020, pp. 2165-2172.
- A. L. Gonzalez Rios, Z. Li, G. Xu, A. Diaz Alonso, and Lj. Trajkovic, "Detecting network anomalies and intrusions in communication networks," in Proc. 23rd IEEE International Conference on Intelligent Engineering Systems 2019, Gödöllő, Hungary, April 2019, pp. 29-34.

References

[1] J. Kurose and K. Ross, "*Computer Networking: A Top-Down Approach*", 6th ed., New Jersey, U.S.A: Pearson, 2013, Chapter:1, pp. 1-80.

[2] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput*., vol. 9, no. 8, pp. 1735–1780, Oct. 1997.

[3] A. Graves, "Long short-term memory," in *Supervised Sequence Labelling with Recurrent Neural Networks*, Berlin, Heidelberg: Springer, 2012, pp. 37–45.

[4] 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.

[5] Z. Li, A. L. Gonzalez Rios, and L. Trajković, "Detecting Internet worms, ransomware, and blackouts using recurrent neural networks," in *Proc. IEEE Syst., Man, Cybern*., Toronto, Canada, Oct. 2020, pp. 2165-2172.

[6] Z. Li and A. L. Gonzalez Rios, *Private communications*, Dec. 2020.

References

[7] (2020, Dec.) RIPE NCC. [Online]. Available: https://www.ripe.net .

[8] (2020, Dec.) University of Oregon Route Views project. [Online]. Available: http://www.routeviews.org .

[9] (2020, Dec.) Border Gateway Protocol (BGP) datasets with routing records collected from Reseaux IP Europeens (RIPE) and BCNET. [Online]. Available: http://www.sfu.ca/~ljilja/cnl/projects/BGP_datasets/index.html .

[10] (2020, Dec.) Z. Li, A. L. Gonzalez Rios, and L. Trajković, Border Gateway Proto-col routing records from Reseaux IP Europeens (RIPE) and BCNET. [Online]. Avail-able: https://ieee-dataport.org/open-access/border-gateway-protocol-routing-records-reseaux-ip-europeens-ripe-and-bcnet .

[11] (2020, Dec.) Broad Learning System for Classifying Network Intrusions. [Online]. Available: http://www.sfu.ca/~ljilja/cnl/projects/BLS_intrusion_detection/index.html .

References

[12] (2020, Dec.) What is an autonomous system? | What are ASNs?. [Online]. Available: https://www.cloudflare.com/learning/network-layer/what-is-an-autonomous-system/ .

[13] 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 International Conference on Intelligent Engineering Systems* 2019, Gödöllő, Hungary, April 2019, pp. 29-34.

[14] Y. Yasami and S. P. Mozaffari, "A novel unsupervised classification approach for net-work anomaly detection by k-means clustering and ID3 decision tree learning methods," J. Supercomput., vol. 53, no. 1, pp. 231–245, Oct. 2010.


thank
you