Classifying Anomalous Events in BGP Datasets

Marijana Ćosović, Slobodan Obradović, and Ljiljana Trajković
University of East Sarajevo, East Sarajevo, Bosnia and Herzegovina; Simon Fraser University, Vancouver, British Columbia, Canada

Border Gateway Protocol

- Border Gateway Protocol (BGP) is an interdomain routing protocol used in networks consisting of a large number of Autonomous Systems (ASs).
- Propagation of the BGP routing information is susceptible to misconfigurations, power outages, malicious attacks, and worms.
- Determining the anomalies and their causes is useful for assessing loss of data and connectivity.
- BGP anomaly detection system design relies on machine learning techniques.
- We use well-known classifiers and exploit their ability to reliably detect network anomalies in BGP datasets.

BGP Datasets

- The BGP update messages are acquired from two projects that provide valuable information to networking research:
  - Routing Information Service (RIS) project initiated in 2001 by the Réseaux IP Européens (RIPE) Network Coordination Centre (NCC)
  - RouteViews project at the University of Oregon, USA.
- These projects collect and store routing data that provide a unique view of the Internet topology.
- Anomalous events considered in this project:

Event	Date	RRC	Peers
Moscow Power Blackout	May 2005	RIS 05	AS1853, AS12793, AS13237
AS9121 Routing Table Leak	Dec. 2004	RIS 05	AS1853, AS12793, AS13237
Panix Domain Hijack	Jan. 2006	Route Views	AS12956, AS6762, AS6939, AS3549
AS Path Error	Oct. 2001	RIS 03	AS3257, AS3333, AS6762, AS9057

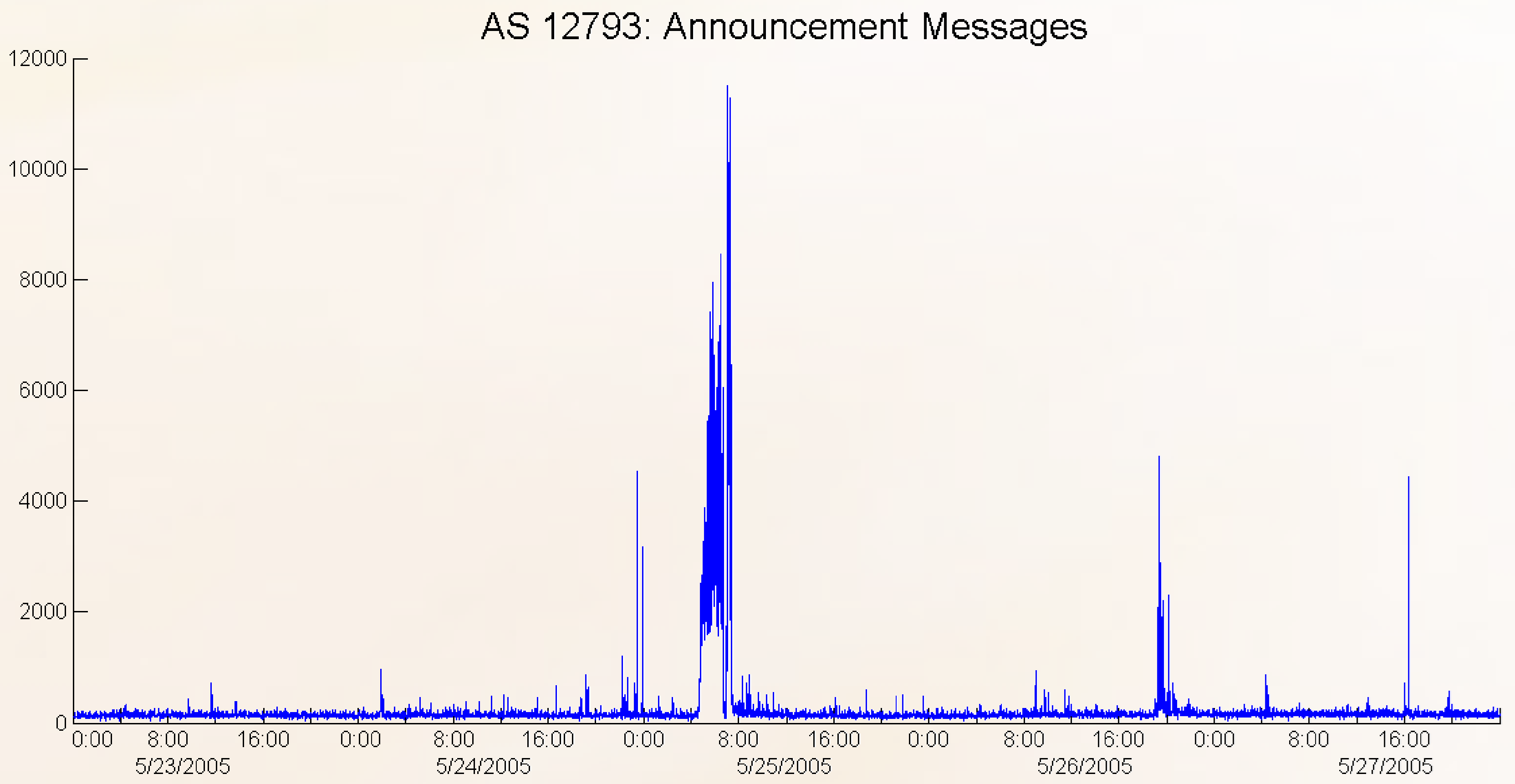
Performance Measures

- F-measure: $2 \times \dfrac{\text{recall} \times \text{precision}}{\text{recall} + \text{precision}}$
  - Recall: ratio of identified anomalies (TP) and all labeled anomalies (true)
  - Precision: ratio of identified anomalies (TP) and all data points identified as anomalous.
- MCC: $\dfrac{TP \times TN - FP \times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}}$
  - TP: number of anomalous training data points classified as anomaly
  - FP: number of regular training data points classified as anomaly
  - FN: number of anomalous training data points classified as regular
  - TN: number of regular training data points classified as regular.
- Receiver operating characteristics (ROCs)
- Precision-Recall (PR) curves.

Performance Comparison

Data set	Model	F-measure	MCC	ROC	PR
Moscow Power Blackout	NB-1	0.848	0.846	0.971	0.912
	NB-2	0.877	0.874	0.971	0.903
	NB-3	0.877	0.874	0.969	0.842
	NB-4	0.848	0.846	0.971	0.912
	NB-5	0.900	0.898	0.971	0.911
	NB-6	0.892	0.890	0.982	0.907
	J48-1	0.894	0.893	0.896	0.795
	J48-2	0.796	0.804	0.903	0.800
	J48-3	0.876	0.874	0.926	0.808
	J48-4	0.905	0.903	0.931	0.849
	J48-5	0.902	0.901	0.934	0.829
	J48-6	0.896	0.894	0.941	0.835
AS 9121 Routing Table Leak	NB-1	0.901	0.902	0.999	0.961
	NB-2	0.899	0.898	0.999	0.949
	NB-3	0.888	0.888	0.998	0.888
	NB-4	0.901	0.902	0.999	0.961
	NB-5	0.950	0.950	0.993	0.950
	NB-6	0.956	0.956	0.992	0.962
	J48-1	0.906	0.905	0.958	0.847
	J48-2	0.672	0.694	0.958	0.846
	J48-3	0.930	0.929	0.934	0.844
	J48-4	0.955	0.955	0.955	0.898
	J48-5	0.938	0.938	0.967	0.873
	J48-6	0.944	0.944	0.967	0.893
Panix Hijack Event	NB-1	0.706	0.721	0.999	0.918
	NB-2	0.820	0.821	0.999	0.911
	NB-3	0.800	0.804	0.998	0.874
	NB-4	0.706	0.721	0.999	0.918
	NB-5	0.848	0.848	0.998	0.905
	NB-6	0.794	0.793	0.994	0.865
	J48-1	0.946	0.946	0.992	0.945
	J48-2	0.864	0.870	0.992	0.944
	J48-3	0.877	0.876	0.970	0.874
	J48-4	0.962	0.962	0.977	0.888
	J48-5	0.855	0.854	0.938	0.739
	J48-6	0.947	0.946	0.988	0.919
AS PATH Error	NB-1	0.875	0.877	0.999	0.969
	NB-2	0.938	0.936	0.999	0.955
	NB-3	0.865	0.868	0.999	0.933
	NB-4	0.875	0.877	0.999	0.963
	NB-5	0.907	0.905	0.997	0.900
	NB-6	0.921	0.920	0.999	0.957
	J48-1	0.913	0.911	0.976	0.855
	J48-2	0.910	0.907	0.976	0.854
	J48-3	0.910	0.908	0.960	0.858
	J48-4	0.922	0.920	0.974	0.864
	J48-5	0.921	0.920	0.982	0.846
	J48-6	0.916	0.914	0.980	0.907

Performance of Naïve Bayes (NB) and Decision Tree (J48) classifiers



Number of announcement messages exchanged by BGP routers that are caused by an anomalous event

Classification Models

- NB-1 and J48-1: classifiers trained on discretized datasets
- NB-2 and J48-2: classifiers trained on datasets with the optimized F-measure
- NB-3, NB-4, J48-3, and J48-4: filter methods using Naïve Bayes (NB) and Decision Tree (J48) classifiers
- NB-5, NB-6, J48-5, and J48-6: wrapper methods using Naïve Bayes (NB) and Decision Tree (J48) classifiers

Conclusion

- We evaluated performance of BGP detection models based on Naïve Bayes and Decision Tree J48 classifiers.
- The Moscow Power Blackout, AS 9121 Routing Table Leak, Panix Hijack, and AS Path Error datasets are examples of known anomalies that have been tested for developing anomaly detection algorithms.
- Performance of the classifiers is influenced by the employed datasets.
- In most cases, filter and wrapper methods based on Decision Tree models have outperformed other models.

References

- N. Al-Rousan and Lj. Trajković, "Machine learning models for classification of BGP anomalies," in *Proc. 13th IEEE Int. Conf. High Performance Switching and Routing*, Belgrade, Serbia, June 2012, pp. 103–108.
- N. Al-Rousan, S. Haeri, and Lj. Trajković, "Feature selection for classification of BGP anomalies using Bayes models," in *Proc. Int. Conf. Mach. Learning Cybern.*, Xi'an, China, July 2012, pp. 140–147.
- M. Ćosović, S. Obradović, and Lj. Trajković, "Performance evaluation of BGP anomaly classifiers," in *Proc. Int. Conf. on Digital Inform., Networking and Wireless Commun.*, Moscow, Russia, Feb. 2015, pp. 115–120.
- Y. Li, H. J. Xing, Q. Hua, X.-Z. Wang, P. Batta, S. Haeri, and Lj. Trajković, "Classification of BGP anomalies using decision trees and fuzzy rough sets," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, San Diego, CA, USA, Oct. 2014, pp. 1331–1336.

CCECE 2016
The 29th Annual IEEE Canadian Conference on Electrical and Computer Engineering
15–18 May 2016, Vancouver, British Columbia, Canada