Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 42, S. 134-139, Ekim 2022
© Telif hakkı EJOSAT'a aittir
Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue. 42, pp. 134-139, October 2022
Copyright © 2022 EJOSAT
Research Article

BGP Anomaly Detection Using Association Rule Mining Algorithm

Mubarak Altamimi[1*], Zafer Albayrak[2], Muhammet Çakmak[3], Ahmet Nusret Özalp[4]

[1*]Karabuk University, Faculty of Engineering, Department of Computer Engineering, Karabuk, Turkey, (ORCID: 0000-0003-0304-4028), 1928126570@ogrenci.karabuk.edu.tr

[2] Sakarya University, Faculty of Engineering, Department of Computer Engineering, Sakarya, Turkey, (ORCID: 0000-0001-8358-3835), zaferalbayrak@subu.edu.tr

[3] Karabuk University, Faculty of Engineering, Department of Electric-Electronics Engineering, Karabuk, Turkey, (ORCID: 0000-0002-3752-6642), muhammetcakmak@karabuk.edu.tr

[4] Karabuk University, Faculty of Engineering, Department of Computer Engineering, Karabuk, Turkey, (ORCID: 0000-0003-4882-9216), ahmetnusretozalp@karabuk.edu.tr

(2nd International Conference on Engineering and Applied Natural Sciences ICEANS 2022, October 15 - 18, 2022)

(**DOI:** 10.31590/ejosat.1186700)

ATIF/REFERENCE: Altamimi, M., Albayrak, Z., Çakmak, M. & Özalp, A. N. (2022). BGP Anomaly Detection Using Association Rule Mining Algorithm. *European Journal of Science and Technology*, (42), 134-139.

Abstract

An anomaly is the occurrence of an exception that affects network security. The requirement for abnormality detection in a network is Anomaly detection, which detects and removes anomalous flow from the network. The Border Gateway Protocol (BGP) is the most common external Gateway Protocol used to communicate with autonomous systems to share routing and reachability information. This protocol's abnormal behavior may be caused by a variety of factors, including inadequate provisioning, malicious attacks, traffic or equipment issues, and network operator mistakes. BGP was built on the assumption of trust, and as a result, it has been hacked numerous times over the years. Code Red I is one well-known assault that targets BGP networking and produce abnormalities in its operation. These attacks were utilized as the dataset for training the model using network traffic data. The goal of this study is to detect the events that triggered an anomaly in the BGP during a time, as well as to detect an anomaly from the BGP throughout that time interval using the training dataset model. We present real association rule mining for BGP anomaly detection in the Intrusion Detection System (IDS).

Keywords: BGP Anomalies Detection, Datamining, Association Rules, Dataset, Code Red I, Apriori Algorithm.

İlişkilendirme Kuralı Madenciliği Algoritmasını Kullanarak BGP Anomali Tespiti

Öz

Anomali, ağ güvenliğini etkileyen olağan dışı durumun ortaya çıkmasıdır. Bir ağdaki olağandışı durumun algılanması gereksinimi, ağdan anormal akışı algılayan ve kaldıran Anomali tespitidir. Sınır Ağ Geçidi Protokolü (BGP), yönlendirme ve erişilebilirlik bilgilerini paylaşmak için otonom sistemlerle iletişim kurmak için kullanılan en yaygın harici Ağ Geçidi Protokolüdür. Bu protokolün anormal davranışı, yetersiz tedarik, kötü niyetli saldırılar, trafik veya ekipman sorunları ve ağ operatörü hataları gibi çeşitli faktörlerden kaynaklanabilir. BGP güven varsayımı üzerine inşa edilmiştir ve sonuç olarak yıllar içinde birçok kez saldırıya uğramıştır. Code Red I, BGP ağını hedef alan ve işleyişinde anormallikler üreten iyi bilinen bir saldırı tespitinde kullanılan verisetidir. Veriseti içindeki saldırılar türleri, ağ trafiği verilerini kullanarak modelin eğitimi için veri kümesi olarak kullanılmıştır. Bu çalışmanın amacı, bir süre boyunca BGP'de bir anormalliği tetikleyen olayları tespit etmek ve aynı zamanda eğitim veri seti modelini kullanarak bu zaman aralığı boyunca BGP'den bir anormalliği tespit etmektir. İzinsiz Giriş Tespit Sisteminde (IDS) BGP anomali tespiti için gerçek birliktelik kuralı madenciliği sunuyoruz.

Anahtar Kelimeler: BGP Anormali Tespiti, Veri madenciliği, Birliktelik Kuralları, Veri kümesi, Code Red I, Apriori Algoritması.

Corresponding Author: ahmetnusretozalp@karabuk.edu.tr

1. Introduction

The Internet is a decentralized network that spans the whole globe and is composed of tens of thousands of autonomous systems (ASs). An AS is a group of routers that work together under the same technical management. They connect to each other with an Interior Gateway Protocol (IGP) like Open Shortest Path First (OSPF) and to other ASs with an Exterior Gateway Protocol (EGP) like Border Gateway Protocol (Hoarau, Tournoux,& Razafindralambo, 2021). Both the declaration of a new route for a prefix and the withdrawal of an existing route may be sent by a router in the same packet. Because routers only send updates when anything has changed. It is possible that the internet may one day reach a "steady state" in which receiving fresh update notifications is unnecessary. The Internet's BGP routing, on the other hand, seems far from stable (Zhao, Band, Elnaffar, Sookhak, Mosavi, & Salwana, 2021). Changes in BGP routing can occur for a variety of reasons.

An active BGP session between two routers is required for the exchange of update messages. Each router uses local policies to determine which route is the "best" for each prefix and whether or not to broadcast it to the neighbor. Alterations to the BGP routing might potentially result in performance issues. A single event, such as a failed connection, might trigger a series of changes as routers seek other routes. During this phase of convergence, packets destined for the target prefix may become stuck in forwarding loops (Garcia-Luna-Aceves, 2022 ; Griffin, & Wilfong, 2019). Internet Service Providers (ISP) execute their relationships via routing policies. ISP may employ traffic engineering to regulate traffic direction and routing protocols through route prepending. Based on their algorithms, routing protocols are divided into three categories: link-state, such as OSPF (Alotaibi, H. S., Gregory, & Li, 2022).

Distance vector (i.e. Routing Information Protocol (RIP)) and PATH vector (i.e. BGP) are two types of vectors. By sending path-vector signals, Autonomous System Boundary Routers (ASBR) use BGP to let people know which networks can be reached (Edwards, Cheng, & Kadam, 2019). When a path vector message is received, each router must check the advertised path against its policy. If the message conforms to the routers policy, it is updated in both the routing table and the message itself before being sent to the next neighbor (Szymoniak, Siedlecka-Lamch, Zbrzezny, Zbrzezny, & Kurkowski, 2021). It makes the necessary changes to the routing table in order to maintain a track of the autonomous systems that are required to be traversed on the way to the target system. It adds its AS number to the message and replaces the following router item with its identity. BGP is divided into two types: Internal Border Gateway Protocol (IBGP), which connects BGP routers inside an AS to External Border Gateway Protocol (EBGP), which runs between BGP routers across ASs. On the other hand, are connected by a dedicated link between peers or a third party like the Internet Exchange Point (IXP). Over the years, BGP has experienced multiple revisions and modifications. Version 4 of BGP is now in use. as documented in RFC4271(Deshpande, Thottan, & Sikdar, 2019).

When we talk about attacks, we are talking about cyberattacks that cover all areas of technology, including network protocols even extending to the Internet of Things(IoT) devices, increasingly, IoT devices are becoming areas where cyberattacks are common, Networks in internal networks also threaten BGP backbones as layers (Özalp, Albayrak, Çakmak & Özdoğan, 2022). This protocol's abnormal behavior may be caused by a variety of factors, including malicious attacks, traffic or equipment issues. In our study, we contributed to the literature in terms of (Kong, Jong, & Ryang, 2019) where author used a novel practical association rule mining approach for anomaly detection in the Intrusion Detection System (IDS). Moreover, the study followed to improve the association rule mining approach, He proposed a realistic technique for mining uncommon association rules from the network packet database, and showed the benefits, but it did not cover the scientific need because the fragility of the rules did not resulted in the detection of anomalies (Safara, Souri, & Serrizadeh, 2020). There are also fundamental differences between the studies (Badhon, Kabir,& Kabir, 2021 ; Telikani, Gandomi, & Shahbahrami, 2020). and the current study, which is different from the previous studies, and those differences lie in the idealism of the proadcast that was followed to contribute to accurate scientific results. our study is to detect the events that triggered an anomaly in the BGP during a time, as well as to detect an anomaly from the BGP throughout that time interval using the training dataset model, and appriori frequent pattern algorithm. moreover, we use additional optimizing tools to verify and visualized the rules that resulted.

2. Material and Method

Today, there are models and methodologies in studies to detect anomalies in BGP protocol. As in current attack detection studies, in addition to anomalies, frequently seen types of attacks are also investigated (Özalp, & Albayrak,2022). Also As we have seen today, the methods of hybrid models are gaining importance in the detection of BGP anomalies (Uluer, Albayrak, Özalp, Çakmak & Altunay, 2022).

2.1. Anomaly Detection

Anomaly detection is a method of processing data that does include an Unsupervision data process that may be used to identify anomalies in a dataset, where are outlier data points in a dataset that contradict the data's typical trend. These data points or data deviate from the typical activity patterns of the dataset In real-world datasets, anomalies and outliers are frequent. They may be caused by data corruption, failed experiments, or human error. Because the existence of anomalies might affect the models performance, the dataset should be devoid of an anomaly in order to train a robust data science model (Alazizi, Habrard, Jacquenet, He-Guelton, & Siblini, 2019).

A methodology that had been used in this study to detect the anomaly of the BGP is using the technique of association rule mining algorithm, where Apriori algorithm used to detect Anomalies, rules based on anomalies value of the attributes on the dataset of BGP, and compare that results and take the best of them. The Fig. 1 shows a flowchart of the methodology that had been used in.

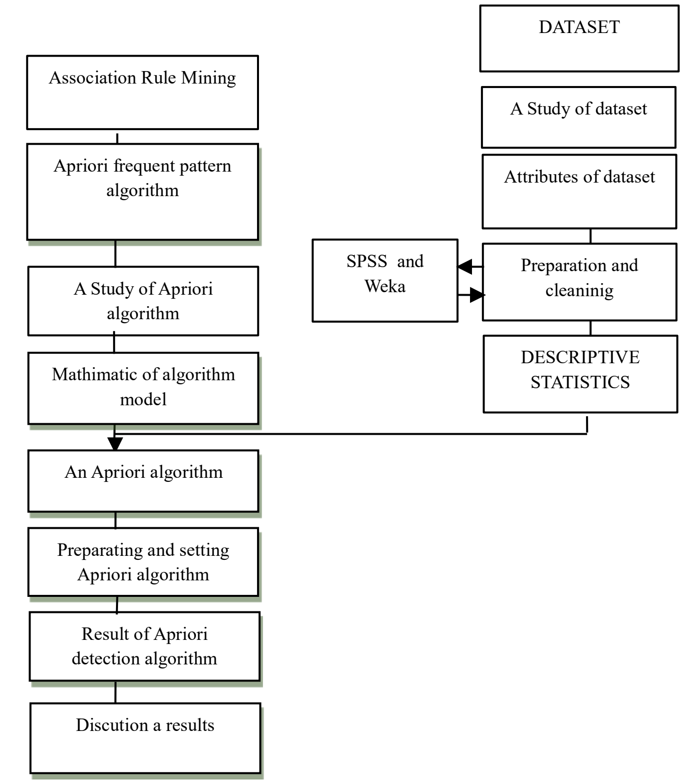

DATASET
Association Rule Mining
A Study of dataset
Apriori frequent pattern algorithm
Attributes of dataset
SPSS and Weka
Preparation and cleaninig
A Study of Apriori algorithm
DESCRIPTIVE STATISTICS
Mathimatic of algorithm model
An Apriori algorithm
Preparating and setting Apriori algorithm
Result of Apriori detection algorithm
Discution a results

Figure 1: A Methodology of BGP anomaly detection

2.1.1. Dataset

Code Red I, is the most well-known attacks. These attacks served as the training data for the model. Code Red I was used as a test dataset. Based on their Pearson's correlation coefficient value, a few selected features and the Top 5 features were chosen to be able to distinguish between anomaly and non-anomaly BGP update signals. The dataset for this study was downloaded from a website in "CSV" format and was ready to use Kaggle2020 (Moore, Shannon, & Claffy, 2020). Several announcements, average AS- PATH length, and maximum edit-distance are all included in this dataset. Code Red I was one well-known Border Gateway Anomalies that happened in January 2003, September 2001, and July 2000. BGP update messages from the Reseaux IP Europeans' are accessible to the public via the Network Coordination Centre (NCC) and include Code Red I. At the model preparation stage, data is collected, data is integrated, outliers and extreme values are removed(Chandola,Banerjee, & Kumar, 2021)

Data is converted into data mining language, and data is reduced by removing superfluous variables from the model. The dataset was reviewed to improve data quality and discover missing or noise, as well as whether there is a deviation or anomalous value in the study data. It is required to eliminate variables that will not be used in the analysis to prepare the dataset. The dataset was evaluated using Weka preprocessing and SPSS statistics (Awadlesh, 2019).

2.1.2. Association rule algorithm for anomaly detection

The Apriori algorithm, which is one of the top ten data mining methods, is a similar technique to mining association rules. The basic idea is to mine repeated element groups in two stages: first, create a candidate group and then build a descending closed list. There is a wide variety of applications for Apriori algorithms, such as in the business world and the protection of computer networks(Verma, Malhotra, & Singh, 2020).

```
Input: dataset D, Minimum Support $\epsilon$, Minimum Confidence $\varepsilon$
Output: Rt All association rules
Method:
    L1 = large 1-itemsets;
    for($k=2$; $L_{k-1} \neq \emptyset$; $k++$) do begin
        Ck =apriori-gen($L_{k-1}$); //generate new candidates from $L_{k-1}$
        for all transactions $T \in D$ do begin
            Ct=subset($C_k$,T); //candidates contained in T.
            for all candidates $C \in C_t$ do
                Count(C)=Count(C)+1; // increase support count of C by 1
            End
        $L_k=\{C \in C_t \mid Count(C) \geq \epsilon \times |D|\}$
    End
    $L_f = \cup_k L_k$
    $R_t$=GenerateRules($L_f$ , $\varepsilon$)
```

associations between entities. It is an important subject of study in data mining and a long-standing issue. The mining of recurrent element sets is divided into two stages: the formation of the item set and the drawing of a decreasing closed list. We use the Apriori algorithm in the Weka application to determine the rang association rule based on minimum support and minimum metric that called confidence.We can distinguish between correlation rules and the best rules that result from Apriori algorithm implementation and focusing on the correlation ratio through the value of confidence, support and left(Naresh, P& Suguna, 2019).

Table 1. Type of relation and association model of apriori algorithm

Scheme	Relation	Instances	Attributes	Top rules	Associator model
weka.associations.APRIORI -P 2 -I -1 -N 10 -T 0 -C 0.9 -D 0.05 -U 1.0 -M 0.1	Code_Red_I-weka.filters.unsupervised.attribute. NumericTo Nominal-R first-last	7199	42	5	(full training set)

When experimenting, the improved Apriori algorithm was used by applying Weka(Zhang, Yang, & Zhao, 2021) and tuning its properties to implement the process of detecting anomalies value from the BGP Anomaly Detection dataset Code Rede I where the minimum support value was set to 0.95 and set the confidence to be 0.9 and number of cycles performed=1 and the result of the total Frequent Item Set was 39 as summarized in Table 2.

Table 2. Support and confidence of Apriori Algorithm

Criteria	**value**
Minimum support	0.95
Minimum metric<confidence>	0.9
Number of cycles performed	1
Size of the set of large itemsets L(1)	8
Size of the set of large itemsets L(2)	18
Size of the set of large itemsets L(3)	11
Size of the set of large itemsets L(4)	2

3. Research Results and Discussion

After adjusting the Num Rules property in the Apriori algorithm to the value of 5 and setting the value of the Minimum Support to the value of 0.95 and the Confidence at the value of 0.9 and converting the data type in the Dataset to Numeric to Nominal, we noticed the emergence of the best five anomalous association rules based on the frequency of the occurrence of anomalous values of the associated attributes in them. As the anomalous association rule is 1, it is the result of the recurrence of the anomalous value of a Maximum AS- PATH length15 correlates with the appearance of the anomalous value of a maximum correlation rule 2 is the result of the recurrence of edit distance 12 at Instance 6898, and anomalous the anomalous value of the attribute maximum edit distance 12 correlates with the appearance of the anomalous value of a maximum AS-PATH length15 at Instance 6898. The anomalous association rule 3 is the result of the repetition of the anomalous values of each of the attributaries, maximum edit distance16 maximum AS- PATH length 15 and correlates together with the appearance of the anomalous value of the attributes maximum edit distance 1 at instance 6859, and the anomalous correlation rule 4 is the result of the repeated occurrence of the outliers for each of the attributes maximum edit distance 12 and maximum edit distance16 maximum edit distance15 and maximum AS-PATH length 15 outliers are correlated together with the appearance of the outliers' maximum edit distance 12 and maximum AS- PATH length 15 at instance 6859, and the anomalous correlation rule 5 is the result of the repeated outliers. The best five abnormal association rules resulting from the experiment are explained as follows:

1. Maximum AS-PATH length15 6898 ==> Maximum edit distance12 6898 <conf:(1)> lift:(1.04) lev:(0.04) [288] conv:(288.41).
2. Maximum edit distance12 6898 ==> Maximum AS-PATH length15 6898 <conf:(1)> lift:(1.04) lev:(0.04) [288] conv:(288.41).
3. Maximum edit distance16 Maximum AS- PATH length15 6859 ==> Maximum edit distance12 6859 <conf:(1)> lift:(1.04) lev:(0.04) [286] conv:(286.78).
4. Maximum edit distance12 Maximum edit distance16 6859 ==> Maximum AS- PATH length15 6859 <conf:(1)> lift:(1.04) lev:(0.04) [286] conv:(286.78).
5. Maximum edit distance15 Maximum AS- PATH length15 6839 ==> Maximum edit distance12 6839 <conf:(1)> lift:(1.04) lev:(0.04) [285] conv:(285.95).

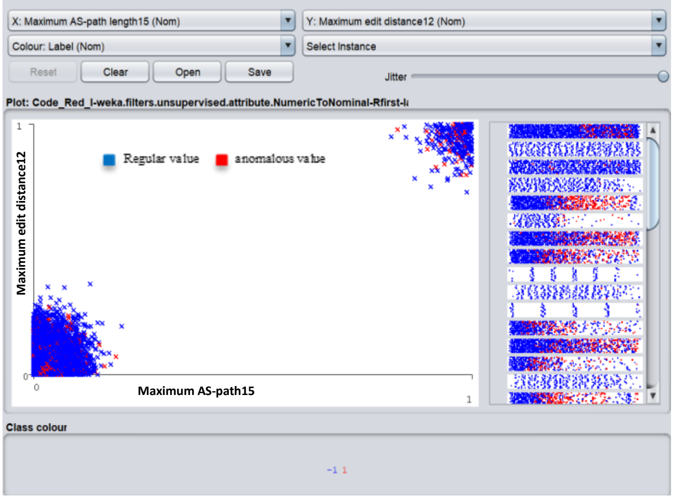
Table 3. shows the values of the attributes that appeared in the results of the experiment and the associated rules, so that the minimum support was set at a value of 0.95 and the confidence at a value of 0.9, as well as showing the value of the instance and its corresponding order for each attribute [24]. Depending on the algorithm showing the anomalous association rules and the values of the instance and according to the order specified in the dataset and the assignment of the instance label, the value of 1 was determined for the label instance if there is an anomaly in any attributes in the dataset. The value of -1 for label instance if there is no anomalous value for any attributes in the dataset. Furthermore, the RNN algorithm in which the dataset is configured does not recognize the value -1 and it is denoted by the value 0. Based on the foregoing, the result of the visualization process for the attributes dataset values by using the Weka framework is shown in the figures below. As can be seen in the next figures, and based on the anomalous values and rules resulting from the visualization of the Apriori algorithm experiment, assigning the value -1 to the regular value, represented by the blue color, and the value 1 to the anomalous values, represented by the red color for the label attribute in the class colour visualization process, it appears as follows**:**

Table 3. Type of relation and association model of Apriori algorithm algorithm

List of Attributes	**Minimum**	**Confidence**	**Result of Rules**	**Instance**
Maximum AS-PATH length15	0.95	0.9	Maximum AS-PATH length 15 ==> Maximum edit distance 12	6898
Maximum edit distance12			Maximum edit distance 12 ==> Maximum AS-PATH length 15	6898
Maximum edit distance16			Maximum edit distance 16, Maximum AS-PATH length 15 ==> Maximum edit distance 12	6859
Maximum edit distance12			Maximum edit distance 12, Maximum edit distance 16 ==> Maximum AS-PATH length 15	6859
Maximum edit distance15			Maximum edit distance 15, Maximum AS-PATH length 15==> Maximum edit distance 12	6839

In Fig. 3 anomalies appear for each of the attributes maximum AS-PATH length 15 and maximum edit distance 12 that represent the x-axis and the y-axis in red at the point (0,0), as well as they appear more intensely at the point (1,1).

In Fig. 4 anomalies appear for each of the attributes maximum edit distance12 and Maximum AS-PATH length15 that represent the x-axis and the y-axis in red at the point (0,0), as well as they, appear more intensely at the point (1,1).



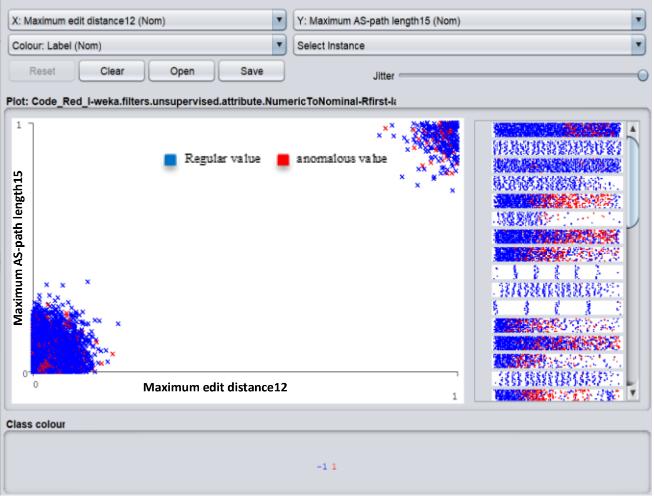
X: Maximum AS-path length15 (Nom)

Y: Maximum edit distance12 (Nom)

Colour: Label (Nom)

Plot: Code_Red_I-weka.filters.unsupervised.attribute.NumericToNominal-Rfirst-l

Figure 3: Visualization of the first anomalous rule



X: Maximum edit distance12 (Nom)

Y: Maximum AS-path length15 (Nom)

Colour: Label (Nom)

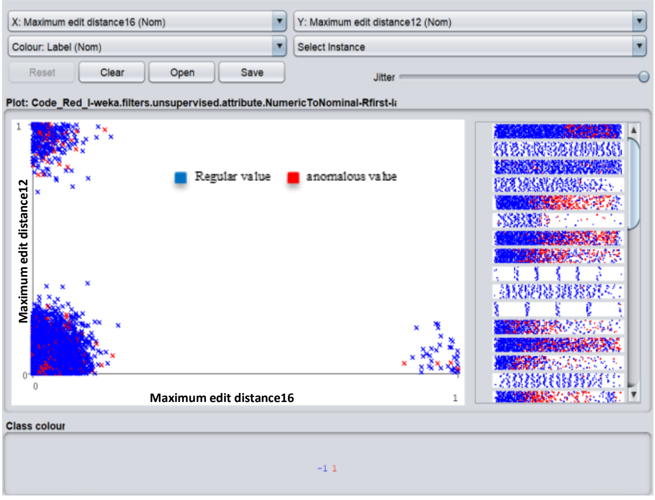
Plot: Code_Red_I-weka.filters.unsupervised.attribute.NumericToNominal-Rfirst-l

Figure 4: Visualization of the second anomalous rule

In Fig. 5 anomalies appear for each of the attributes maximum AS-PATH length15 and maximum edit distance12 that represent the x-axis and the y-axis in red at the point (0,0), as well as they appear more intensely at the point (1,1).

In Fig. 6 anomalies appear for each of attributes maximum edit distance16 and maximum AS-PATH length15 that represent the x-axis and the y-axis in red at the point (0,0), as well as they appear more intensely at the point (1,1).

In Fig. 7 anomalies appear for each of the attributes maximum AS-PATH length15 and maximum edit distance12 that represent the x-axis and the y-axis in red at the point (0,0), as well as they appear more intensely at the point (1,1)



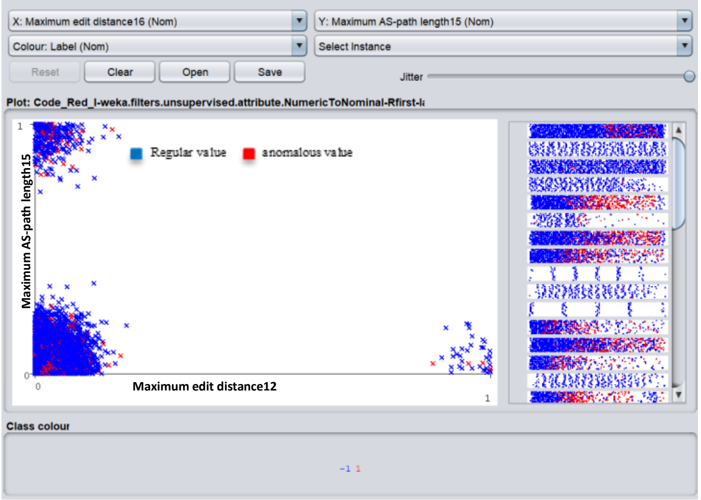
X: Maximum edit distance16 (Nom)

Y: Maximum edit distance12 (Nom)

Colour: Label (Nom)

Plot: Code_Red_I-weka.filters.unsupervised.attribute.NumericToNominal-Rfirst-l

Figure 5: Visualization of the third anomalous rule



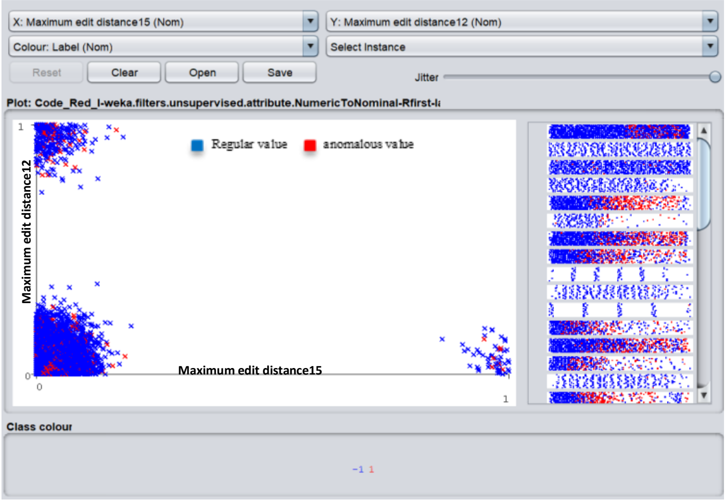
X: Maximum edit distance16 (Nom)

Y: Maximum AS-path length15 (Nom)

Colour: Label (Nom)

Plot: Code_Red_I-weka.filters.unsupervised.attribute.NumericToNominal-Rfirst-l

Figure 6: Visualization of the fourth anomalous rule



X: Maximum edit distance15 (Nom)

Y: Maximum edit distance12 (Nom)

Colour: Label (Nom)

Plot: Code_Red_I-weka.filters.unsupervised.attribute.NumericToNominal-Rfirst-l

Figure 7: Visualization of the fifth anomalous rule

4. Conclusion and Future Studies

Attacks, configuration errors, and power outages are examples of abnormal BGP events that should be caught early on, because they might lead to anomalous or pathological routing behavior at the global or prefix level. Association rule mining is a key research area in data mining. Whereas Apriori association rule mining uses as a collection of rules that are based on hashing method among infrequent item sets to detect BGP anomalous. We provide a framework to systematically evaluate BGP routing data discovering rules of anomalous BGP events.

The framework is specifically trained to learn the rules of aberrant BGP events using data mining techniques. Worm event rules were deduced from BGP data that collected during the Code Red I. This method is effective in locating the flow linked with the unusual events. Thus, Apriori association rule mining algorithm enables network managers and the BGP anomaly detector to make more informed decisions.

References

Hoarau, K., Tournoux, P. U., & Razafindralambo, T. (2021, October). Suitability of graph representation for bgp anomaly detection. In 2021 IEEE 46th Conference on Local Computer Networks (LCN) (pp. 305-310). IEEE.

Zhao, X., Band, S. S., Elnaffar, S., Sookhak, M., Mosavi, A., & Salwana, E. (2021). The implementation of border gateway protocol using software-defined networks: A systematic literature review. IEEE Access.

Garcia-Luna-Aceves, J. J. (2022, August). Attaining stable and loop-free inter-domain routing without path vectors. In Proceedings of the ACM SIGCOMM Workshop on Future of Internet Routing & Addressing (pp. 58-65).

Griffin, T. G., & Wilfong, G. (2019). An analysis of BGP convergence properties. ACM SIGCOMM Computer Communication Review, 29(4), 277-288.

Alotaibi, H. S., Gregory, M. A., & Li, S. (2022). Multidomain SDN-Based Gateways and Border Gateway Protocol. Journal of Computer Networks and Communications, 2022.

Edwards, P., Cheng, L., & Kadam, G. (2019). Border gateway protocol anomaly detection using machine learning techniques. SMU Data Science Review, 2(1), 5.

Szymoniak, S., Siedlecka-Lamch, O., Zbrzezny, A. M., Zbrzezny, A., & Kurkowski, M. (2021). SAT and SMT-Based Verification of Security Protocols Including Time Aspects. Sensors, 21(9), 3055.

Deshpande, S., Thottan, M., Ho, T. K., & Sikdar, B. (2019). An online mechanism for BGP instability detection and analysis. IEEE transactions on Computers, 58(11), 1470-1484.

Kong, H., Jong, C., & Ryang, U. (2019). Rare association rule mining for network intrusion detection. arXiv preprint arXiv:1610.04306.

Safara, F., Souri, A., & Serrizadeh, M. (2020). Improved intrusion detection method for communication networks using association rule mining and artificial neural networks. IET Communications, 14(7), 1192-1197.

Badhon, B., Kabir, M. M. J., Xu, S., & Kabir, M. (2021). A survey on association rule mining based on evolutionary algorithms. International Journal of Computers and Applications, 43(8), 775-785.

Telikani, A., Gandomi, A. H., & Shahbahrami, A. (2020). A survey of evolutionary computation for association rule mining. Information Sciences, 524, 318-352.

Yulanda, R. D., Wahyuningsih, S., & Amijaya, F. D. T. (2019, July). Association rules with apriori algorithm and hash-based algorithm. In Journal of Physics: Conference Series (Vol. 1277, No. 1, p. 012048). IOP Publishing.

Khafaji, H. K. (2021, February). A New Algorithm for Extracting Textual Maximal Frequent Itemsets from Arabic Documents. In Journal of Physics: Conference Series (Vol. 1773, No. 1, p. 012012). IOP Publishing.

Sarno, R., Sinaga, F., & Sungkono, K. R. (2020). Anomaly detection in business processes using process mining and fuzzy association rule learning. Journal of Big Data, 7(1), 1-19.

Moore, D., Shannon, C., & Claffy, K. (2020, November). Code-Red: a case study on the spread and victims of an Internet worm. In Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment (pp. 273-284).

Luo, X., & Li, Y. (2019). Security enhancement mechanism of modbus TCP protocol. DEStech Transactions on Computer Science and Engineering, 10.

Chandola, V., Banerjee, A., & Kumar, V. (2021). Anomaly detection Algorithms every Data Scientist should know. ACM computing surveys (CSUR), 41(3), 1-58.

Awadlesh, I. (2019). Weka: IT For Business Intelligence: Classification and Clustering Analysis. Term Paper, April, 19.

Verma, N., Malhotra, D., & Singh, J. (2020). Big data analytics for retail industry using MapReduce-Apriori framework. Journal of Management Analytics, 7(3), 424-442.

Naresh, P., & Suguna, R. (2019, May). Association rule mining algorithms on large and small datasets: A comparative study. In 2019 International Conference on Intelligent Computing and Control Systems (ICCS) (pp. 587-592). IEEE.

Yi, F., Zhang, L., Yang, S., & Zhao, D. (2021, October). A Security-Enhanced Modbus TCP Protocol and Authorized Access Mechanism. In 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC) (pp. 61-67). IEEE.

Özalp, A. N., & Albayrak, Z. (2022). Detecting Cyber Attacks with High-Frequency Features using Machine Learning Algorithms. Acta Polytechnica Hungarica, 19(7).

A. F. Uluer, Z. Albayrak, A. N. Özalp, M. Çakmak and H. C. Altunay, "BGP Anomali Tespitinde Hibrit Model Yaklaşımı," 2022 30th Signal Processing and Communications Applications Conference (SIU), 2022, pp. 1-4, doi: 10.1109/SIU55565.2022.9864921.

A. N. ÖZALP, Z. ALBAYRAK, M. ÇAKMAK and E. ÖZDOĞAN, "Layer-based examination of cyber-attacks in IoT," 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2022, pp. 1-10, doi: 10.1109/HORA55278.2022.9800047.

Alazizi, A., Habrard, A., Jacquenet, F., He-Guelton, L., Oblé, F., & Siblini, W. (2019, November). Anomaly detection, consider your dataset first an illustration on fraud detection. In 2019 IEEE 31st international conference on tools with artificial intelligence (ICTAI) (pp. 1351-1355). IEEE.