

BGPFlow: Flow-based Feature Extraction for BGP Anomaly Detection

Yanxu Fu¹, Pei Zhang¹, Han Zhang^{2,3}, Xiaohong Huang¹, Yan Ma¹
Kun Xie¹, Dandan Li¹

¹School of Computer Science (National Pilot Software Engineering School), Beijing University of Posts and Telecommunications, Beijing, China

²Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing, China

³Zhongguancun Laboratory, Beijing, China

{fuyanxu,zhangpei,huangxh,mayan,pat,dandl}@bupt.edu.cn,zhhan@tsinghua.edu.cn

ABSTRACT

The Border Gateway Protocol (BGP) plays a pivotal role in inter-domain routing, but its decentralized nature and lack of inherent security make it vulnerable to various anomalies. Efficient detection of these anomalies relies on appropriate aggregation methods that extract both quantitative and topological features from routing updates. However, due to the immense scale and complexity of the Internet, inappropriate feature aggregation methods may introduce data noise, thereby increasing detection latency and degrading the overall accuracy of the system. In this paper, we propose BGPFlow, a flexible and scalable feature extraction framework that supports multiple levels of aggregation and integrates both quantitative and graph-based features. We organize the BGP feature flows using the Original Autonomous System (Original AS) as the key and performs aggregation at the country level. To reduce the computational complexity of graph-based features, we apply a graph clustering method based on Graph Autoencoder (GAE) to compress country-level BGP topologies, preserving structural semantics while enhancing the detection of both large-scale and smaller anomalies. Through case studies involving routing anomalies of various scales, we demonstrate the efficiency of BGPFlow in detecting real-world network incidents.

CCS CONCEPTS

• **Networks** → **Network monitoring**;

KEYWORDS

BGP, BGP Anomaly, BGP Features, BGP Observability

ACM Reference Format:

Yanxu Fu¹, Pei Zhang¹, Han Zhang^{2,3}, Xiaohong Huang¹, Yan Ma¹, Kun Xie¹, Dandan Li¹. 2025. BGPFlow: Flow-based Feature Extraction for BGP Anomaly Detection. In *1st Workshop on Next-Generation Network Observability (NGNO '25)*, September 8–11, 2025, Coimbra, Portugal. ACM, New York, NY, USA, 8 pages. <https://doi.org/10.1145/3748496.3748993>

1 INTRODUCTION

As the de facto inter-domain routing protocol of the Internet, the Border Gateway Protocol (BGP) plays an important role in ensuring global network connectivity. Misconfigurations or malicious network attacks can result in the propagation of erroneous routing information across the Internet, leading to BGP routing anomalies that undermine the stability and reliability of the global Internet infrastructure. For example, a configuration error in the BGP settings of CenturyLink, an international backbone transit provider, resulted in a 3.5% reduction in global Internet traffic[5]. Similarly, a failure of the BGP backbone routers of KT Corporation, South Korea's major ISP, caused nationwide service disruptions[7]. In another incident, Facebook experienced a seven-hour service outage due to the withdrawal of routing prefixes for its authoritative DNS servers[16], resulting in economic losses ranging from billions of dollars. The increasing occurrence of BGP anomalies and vulnerabilities on the Internet highlights the critical need for efficient detection mechanisms.

In recent years, machine learning has emerged as a highly effective method for the detection of BGP anomalies[4, 11]. Typically, BGP updates are transformed into quantitative and topological features, which are then fed into models such as support vector machines (SVM), hidden Markov models

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org. NGNO '25, September 8–11, 2025, Coimbra, Portugal

© 2025 Copyright held by the owner/author(s). Publication rights licensed to the Association for Computing Machinery.
ACM ISBN 979-8-4007-2087-1/25/09...\$15.00
<https://doi.org/10.1145/3748496.3748993>

(HMM)[18], Principal Component Analysis (PCA) [25], and deep learning methods[9]. Despite the growing number of BGP feature extraction methods and tools proposed in recent years[1, 14], several limitations remain in their practical implementation. Firstly, many existing approaches perform feature aggregation from the observation perspectives of BGP collector or vantage points (VPs). Although such aggregation strategies are effective in detecting large-scale anomalous events, they often introduce data noise that may obscure or dilute the signals of smaller-scale anomalies. Secondly, as the number of globally routable ASes has grown to approximately 80,000, graph-based feature extraction methods face increasing challenges in terms of computational complexity and processing latency. These limitations undermine their performance in real-time anomaly detection scenarios.

In this paper, we propose BGPFlow, a flexible and scalable feature extraction framework that supports multiple levels of aggregation and integrates both quantitative and graph-based features. We organize the BGP feature flows using the original AS as the key and perform aggregation at the country level. Original AS refers to the autonomous system that originates its own routes. Leveraging the Original AS as the primary key in BGP feature aggregation enables network operators to monitor routing dynamics of their own networks from a first-hand perspective. Aggregating features at the country level offers two key benefits. Firstly, it simplifies the structure of large-scale Internet topology by partitioning it into smaller country subgraphs, thereby reducing computational complexity and isolating noise. This partitioning also facilitates anomaly detection and root cause localization within each country subgraph. Secondly, countries are natural administrative entities within the network ecosystem. Just as network operators primarily focus on managing their own infrastructures, national authorities are responsible for safeguarding the overall security and stability of their country's networks. In the event of large-scale anomalies, national authorities are also well-positioned to coordinate multiple resources to effectively respond to and mitigate such incidents in a timely manner. Thus, BGPFlow provides comprehensive observability views for understanding Internet routing behavior at multiple granularities.

To further reduce the computational complexity of feature extraction from large-scale national network topologies, we introduce a graph clustering method based on Graph Autoencoder (GAE)[15] to compress national-level BGP topologies. This approach preserves structural semantics while enhancing the detection capability for both global and localized anomalies. Through case studies involving routing anomalies of various scales, we demonstrate the effectiveness and efficiency of BGPFlow in detecting real-world network incidents.

The remainder of this paper is organized as follows. Section II presents background and related works. Section III introduces the proposed BGPFlow framework in detail. In Section IV, we performed a study of use cases with BGPFlow. Finally, Section V concludes the paper and outlines directions for future work.

2 BACKGROUND AND RELATED WORKS

2.1 The BGP Dataset Collection

The BGP RIB and update messages carry rich path attributes and routing state information. This information can be used to construct a global network topology, enable real-time monitoring of route dynamics, and serve as a critical data foundation for the detection and analysis of routing anomalies. Among the most representative BGP data collection projects are RouteViews[22] and RIPE RIS[21]. These projects deploy multiple route collectors. Each collector runs a process that emulates a standard BGP router and connects to one or more real routers, known as vantage points (VPs). Each VP sends incremental update messages to the collector whenever changes occur in its Adj-RIB-Out table, reflecting updates to its local routing information base (Loc-RIB). Periodically, the collector generates a comprehensive snapshot of the current Adj-RIB-Out tables of each VP, along with all update messages received since the previous dump, allowing retrospective analysis of BGP routing dynamics. A RIB dump provides a view of the reachable paths from VPs to all globally routable IP prefixes at a specific point in time. The typical RIB dump interval ranges from 2 to 8 hours. However, the update dump records the changes of the routing prefixes in each VP, including events such as route announcements, withdrawals, path changes, and policy modifications. These updates are dumped at a higher frequency, with a typical dumping interval of 5 minutes. It should be noted that a single AS may have multiple VPs that establish BGP session connections with the BGP collector. To avoid redundancy and ensure consistency in feature extraction, we retain only one VP per AS in our analysis. Fig.1 presents an example of the collection of the BGP dataset.

2.2 BGP Feature Engineering

The main role of BGP is to exchange network reachability information with other BGP systems. Routes are announced and withdrawn constantly from various parts of the world[3]. Under normal circumstances, the number of announcement and withdrawal messages remains at a relatively low level. However, when the network encounters sudden anomalous events, BGP may trigger a cascading path exploration process to identify the most recent and optimal routes. This can result in a sharp surge in the number of announcement and

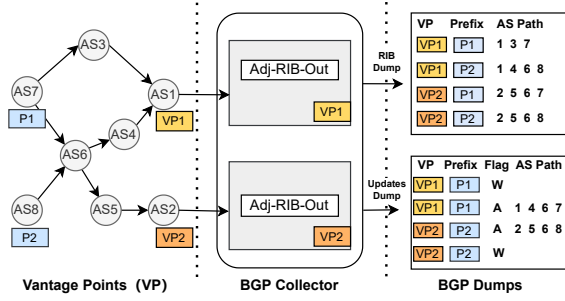


Figure 1: Example of BGP Dataset Collection

withdrawal messages, potentially leading to instability in the global routing system.

Labovitz et al.[6] first identified unexpected trends in Internet routing instability and further classified BGP update patterns such as WADiff, AADiff, WADup, AADup, and WWDup, offering a detailed taxonomy for analyzing routing behavior. Li et al.[13] revisited BGP routing dynamics and confirmed ongoing high-frequency routing updates but also noting increased stability. Bahaa et al.[2] classified BGP update messages into volume features and AS path features. Fonseca et al.[19] introduced methods for BGP dataset generation and feature extraction aimed at detecting routing anomalies based on these classifications. Xu et al.[24] were the first to introduce and explore the perspective of analyzing routing behaviors from the viewpoint of the origin AS. They used PCA to exploit the temporal correlations in the update streams to extract clusters of origin ASes whose prefixes are likely affected by the same events. Xu and Li[17] proposed an approach for BGP anomaly detection utilizing automatic feature extraction via neural networks. They developed a system capable of identifying and classifying various BGP anomalies by learning from extensive datasets. Hoarau et al. introduced BML[14], a BGP dataset generation tool that extracts most of the known features from the literature and the Internet topology, and allows users to build custom features from the BGP data.

3 OUR APPROACH

In this section, we describe the BGPFlow workflow. Initially, we construct a prefix reachability table, a prefix-to-source-AS mapping table, and a country-level topology based on routing snapshots. We organize the BGP feature flows using the original AS as the key and perform aggregation at the country level. To reduce the computational complexity of graph-based features, we apply a graph clustering method based on Graph Auto Encoder to compress country-level BGP topologies, preserving structural semantics while enhancing

the detection of both large-scale and smaller anomalies. Fig.2 presents the workflow of BGPFlow.

3.1 Constructing the Prefix Reachability Table

We utilize a RIB dump to construct an initial prefix reachability table. Formally, let R_0 denote the initial routing snapshot collected at time t_0 from a specific routing collector, and $\{r_1, r_2, \dots, r_n\}$ are records of R_0 . The records record the reachable paths from VPs to all global routing prefixes. We traverse each record and use a two-dimensional data dictionary T_p to store real-time prefix reachability information, where each entry $T_p[p][v]$ represents the AS path from VP $v \in V$ to the original AS of prefix $p \in P$. The two-dimensional dictionary can be implemented as a nested hash table or using tuple keys in standard hash maps. It allows for fast lookups and insertions when update the prefix reachability information table.

Simultaneously, for the AS path in each record, we first extract the original AS for the routing prefix and maintain a prefix-to-original AS mapping table, $M_{P \rightarrow A}$, where $M_{P \rightarrow A}[p]$ denotes the original AS for the prefix p . Then, we extract all AS pairs from the path. For each pair, we retrieve the country of each AS. If both ASes belong to the same country, the pair is added as an edge to the node-edge collection of that country, thereby constructing a country-specific AS graph $G_C = (V_C, E_C)$.

The tables mentioned above are updated via subsequent BGP update messages. Integration of these tables with the country-level topology enables the effective derivation of subsequent routing features. In addition, the country-level topology also offers significant support in pinpointing the origins of BGP anomalies.

3.2 Original-AS Level Feature Extraction

Leveraging Original AS as the key in BGP feature aggregation enables network operators to monitor routing dynamics of their own networks from a first-hand perspective. These features capture the routing behavior between the VPs and the original AS. When certain routers or BGP sessions along the path toward the original AS, or the original AS itself, encounter sudden anomalous events, it can lead to a sharp increase in the number of announcement and withdrawal messages associated with that original AS. This provides network operators with an observable view to assess the status of the affected original AS.

We define F_{prefix_i} represents m -dimension features of $prefix_i$ in the t time interval given as $F_{prefix_i} = (f_1, f_2, \dots, f_m)_t$, f_i can be volume feature or AS-PATH feature related to the $prefix_i$, which is described in[2]. Let $U = \{u_1, u_2, \dots, u_n\}$ be the sequence of routing update messages observed after t_0 ,

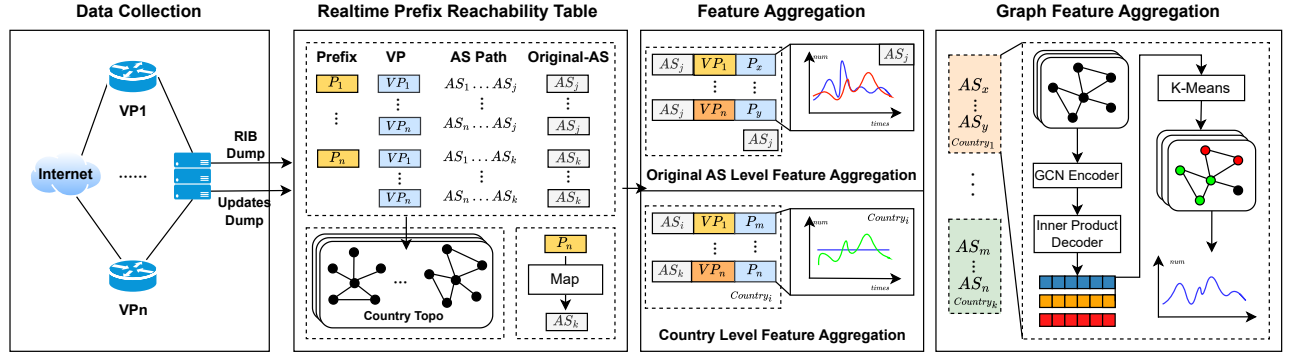


Figure 2: The Workflow of BGPFlow

ordered by their timestamps. For each subsequent update $u_i \in U$, we apply the following operations:

- If u_i is a withdrawal message for prefix p from VP v , we delete $T_p[p][v]$, and update $M_{p \rightarrow A}[p]$ accordingly.
- If u_i is an announcement message for prefix p from v with AS path $path_i$, we insert or update $T_p[p][v] = path_i$, and record the original AS in $M_{p \rightarrow A}[p]$.

During this update process, we update both the prefix reachability table and prefix-to-original AS mapping table, and compute features associated with each prefix. Meanwhile, based on the mapping relationship between prefixes and original AS, we aggregate the prefix-level features to original AS level. Let $M_{p \rightarrow A}[p] = a$ map prefix p to its current original AS a . For each AS a , we define its feature vector F_{origin_a} as the aggregation (e.g., average, sum, or max) of all prefix-level features associated with it:

$$F_{origin_a} = \text{AGGREGATE}(\{F_{prefix_p} \mid M_{p \rightarrow A}[p] = a\})$$

The features extracted by BGPFlow effectively capture the routing instability of the original AS. However, there may be certain limitations in detecting original AS hijacking scenarios. Specifically, when a large AS hijacks the prefix of a smaller AS, the BGP announcements and withdrawals from the victim (smaller) AS often remain unchanged. Meanwhile, the announcement/withdrawal patterns of the hijacker (larger) AS may exhibit minimal variation. In such cases, aggregating by the original AS may fail to reflect the anomaly. To address this limitation in detecting original AS Hijacking, we maintain a feature called `moas_num`, which records the number of MOAS for each original AS within a given time interval. Since we maintain an in-memory prefix reachability table, we can detect new MOAS occurrences for any given prefix, excluding stable MOAS entries already present in the RIB, and quantify the number of Moas. Furthermore, by aggregating prefix-level MOAS counts (while eliminating duplicate MOAS instances), we can track the MOAS number for

each original AS over different time intervals. This approach enables the identification of potentially suspicious original AS Hijacking events, which can then be further validated through active probing or filtered using external knowledge bases[20, 23].

3.3 Country Level Feature Aggregation

At the end of each time interval T , we aggregate volume and path features based on the country affiliation of original ASes, forming routing features at the country level. We then compute graph-based features to characterize the country-level routing topology. Let $M_{A \rightarrow C}[a] = c$ map AS a to its country c . For each Country c , we define its feature vector $F_{country_c}$ as the aggregation (e.g., average, sum, or max) of all Original AS level features associated with it:

$$F_{country_c} = \text{AGGREGATE}(\{F_{origin_a} \mid M_{A \rightarrow C}[a] = c\})$$

During the aggregation process, a notable issue arises from the fact that some ASes are registered in one country—based on assignments by a Regional Internet Registry—while their actual operations may occur in a different country. This discrepancy has the potential to introduce noise or misattribution in the aggregation, thereby affecting the accuracy of country-level analysis. To minimize their impact on aggregated country-level statistical and topological features, we use several IP-to-country geolocation databases to perform geolocation mapping of original AS, including DB-IP[8], MaxMind GeoIP2[10], and IP2Location[12]. These databases claim to achieve up to high accuracy at the country level. We collect the announced prefixes for each AS registered under a given country and divide them into /24 subnets. Three IP addresses are randomly selected from each subnet to query the geolocation databases. We then compute the union of all returned country labels to form its geolocation mapping country set. An AS is excluded from the country AS set only if there is no intersection between its registered country and

Algorithm 1: Graph Compression with Graph Auto Encoder**Input:** AS-level graph $G = (V, E)$, number of clusters k **Output:** Compressed graph $G' = (V', E')$ Construct adjacency matrix A and feature matrix X ;

Train Graph Auto Encoder (GAE):

- Encode: $Z \leftarrow \text{GCN}(X, A)$
- Decode: $\hat{A} \leftarrow \sigma(ZZ^\top)$
- Optimize: $\mathcal{L} = \|A - \hat{A}\|^2 + \lambda\|Z\|^2$

Cluster latent embeddings Z using K-Means into k groups;For each cluster, define a supernode in G' ; aggregate inter-cluster edges;**return** Compressed graph $G' = (V', E')$;

its geolocation mapping country set. Although the heuristic algorithm is relatively strict, inaccuracies in IP geolocation databases can still lead to misclassifications. Therefore, additional verification is performed using WHOIS records and information about the associated organizations to further refine the filtering process.

Partitioning the Internet into country-level subgraphs helps reduce computational complexity and isolate noise. However, countries such as the United States still encompass more than 18,000 advertised ASes, resulting in significant computational overhead. To reduce this complexity, we apply a GAE to compress and cluster the country-level routing topology, preserving its key structural features while significantly reducing its size.

(1) Graph Auto Encoder Architecture. The GAE consists of two main components:

- **Encoder:** A two-layer Graph Convolutional Network (GCN) that encodes the local topology and node features into a latent embedding $Z \in \mathbb{R}^{n \times d}$, where n is the number of AS nodes and $d \ll n$.
- **Decoder:** An inner-product decoder that reconstructs the adjacency matrix A from the learned embeddings via $\hat{A} = \sigma(ZZ^\top)$, where σ is a sigmoid activation function.

The model is trained to minimize the reconstruction error $\mathcal{L} \leftarrow \|A - \hat{A}\|_F^2 + \lambda\|Z\|_2^2$, where the second term serves as a regularizer.

(2) Clustering in Latent Space. After training, the learned embeddings Z capture topological roles and similarity patterns among ASes. We apply a K-Means clustering algorithm on Z to partition ASes into k structurally similar groups. These clusters are then interpreted as supernodes, forming the basis of a compressed graph $G' = (V', E')$, where each node in V' represents a cluster of ASes and edges reflect

inter-cluster connectivity derived from the original graph. Using G' , we can efficiently compute graph features.

4 USE CASE STUDY

For the implementation of BGPFlow, we recommend using a single collector as the basic unit for the extraction of features and the detection of anomalies, and then performing a comprehensive evaluation of the results of the detection from different collectors.

We apply BGPFlow to the analysis of routing anomalies of varying scales, including the Facebook outage (organization-level), the KT outage in South Korea (country-level), and the CenturyLink event (global-level). In our experiments, we use the RIPE RIS collector RRC00, located in Amsterdam and maintains a set of VPs that span various regions and ASes. The results demonstrate that BGPFlow can effectively reduce data noise, improve timeliness and aid in the rapid localization of the source of the event.

On October 4, 2021, Facebook suffered a seven-hour service outage caused by a BGP configuration error that withdrew the route prefixes of its DNS authoritative servers. The incident disrupted access to major platforms including Instagram, Messenger, and WhatsApp for hundreds of millions of U.S. users, resulting in billions of dollars in economic losses. Fig.3(a) illustrates the results of feature aggregation at collector level, while Fig.3(b) shows the aggregation at original AS level (AS32934, Facebook's core AS). It can be observed that aggregating features by original AS significantly reduces noise and enables anomaly detection approximately 20 minutes earlier. This is primarily because route propagation from multiple ASes to the collector involves extensive path exploration, introducing significant irrelevant noise and delays.

On 25 October 2021, KT Corporation, one of South Korea's major ISP, experienced a failure in its BGP backbone router, which led to the withdrawal of numerous routes and consequently caused extensive network outages nationwide. Fig.4(a) presents the results of aggregation at collector level, whereas Fig.4(b) shows the aggregation at the country level. These figures illustrate that aggregating features at the national level significantly reduces data noise. By using the prefix reachability table, we reconstructed the national topology before the event. We were able to pinpoint KT Corporation's network as the root cause of the routing anomaly incident.

On August 31, 2020, CenturyLink's BGP configuration error led to a 3.5% drop in global Internet traffic. CenturyLink is a global Tier 1 backbone carrier in the United States (renamed Lumen Technologies in 2020). We construct a graph representing the US AS-level topology and compute topological features both before and after clustering, as illustrated in

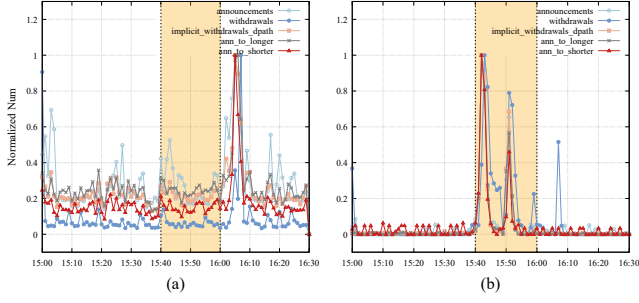


Figure 3: Comparison of Collector Level Feature Aggregation (a) and Original-AS Level Feature Aggregation (b) for Facebook Outage event

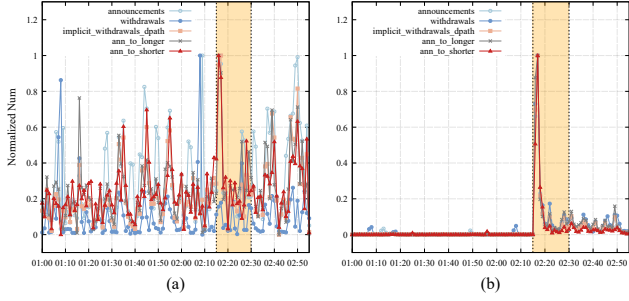


Figure 4: Comparison of Collector Level Feature Aggregation (a) and Country Level Feature Aggregation (b) for KT Outage event

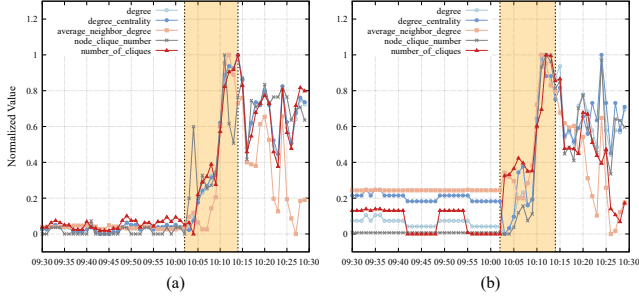


Figure 5: Comparison of Original Graph Feature Aggregation (a) and Clustered Graph Feature Aggregation (b) for CenturyLink Outage event

Fig.5. Fig.5(a) presents raw topological features directly extracted from the full AS-level graph, while the Fig.5(b) shows the same features computed over the cluster-compressed graph, where structurally similar ASes are grouped based on our graph autoencoder model. Despite structural compression, the temporal trends of most features remain consistent before and after clustering, suggesting that our method preserves the essential dynamics of topological signals. Metrics

such as percolation limit, eigenvector, assortativity and triangles exhibit synchronized peaks and inflection points across both representations. This visual consistency shows that graph clustering does not distort the semantic evolution of features.

As shown in Table I, we present the Pearson Correlation Coefficient (PCC), feature computation time and embedding&cluster time under different clustering granularities (varying values of K), alongside the computation time required for extracting features from the original US uncompressed topology. The results demonstrate that even with relatively high PCC values (indicating strong temporal consistency with the original features), the clustering-based approach significantly reduces computation time—often by one to two orders of magnitude. This confirms that our clustering strategy achieves a favorable trade-off between representational fidelity and computational efficiency, making it practical for large-scale or real-time BGP anomaly detection tasks. However, it is worth noting that some features (e.g., number of cliques, average neighbor degree) are highly sensitive to local connectivity patterns, resulting in lower PCC values at smaller K values. These patterns are often abstracted or lost during node merging in the clustering process. In particular, smaller values of K —which correspond to coarser clustering granularity—tend to exacerbate this effect, leading to decreased correlation with their original counterparts. Addressing the loss of fine-grained topological information remains an important direction for future refinement of our clustering framework.

5 CONCLUSION

In this paper, we propose BGPFlow, a flexible and scalable feature extraction framework that supports multiple levels of aggregation and integrates both quantitative and graph-based features. Unlike existing tools, BGPFlow introduces a feature stream organized by the original AS as the key, and performs aggregation at the country level. To reduce the computational complexity of graph-based features, we applied a GAE-based graph clustering method to compress national-level BGP topologies, preserving structural semantics while enhancing the detection of global and local anomalies. Through case studies involving routing anomalies on various scales, we demonstrate the effectiveness and efficiency of BGPFlow in detecting real-world network incidents. In our future work, we will integrate BGPFlow with machine learning models to achieve end-to-end BGP anomaly detection and root cause analysis. Furthermore, leveraging BGPFlow as a foundational data platform, we plan to explore the application of LLMs and agents in this domain.

Table 1: Graph Features Comparison

Graph Features	k = node num * 3/40		k = node num * 4/40		k = node num * 5/40		Original Topo Calc Time(s)
	PCC	Calc Time(s)	PCC	Calc Time(s)	PCC	Calc Time(s)	
degree	0.931	0.059	0.979	0.057	0.976	0.076	0.542
degree centrality	0.570	0.032	0.910	0.045	0.933	0.058	0.452
average neighbor degree	0.808	0.212	0.660	0.274	0.908	0.327	2.293
node clique number	0.747	4.443	0.922	5.041	0.895	5.423	13.102
number of cliques	0.095	3.425	0.871	5.762	0.799	5.029	13.278
eigenvector	0.140	4.179	0.845	5.207	0.904	6.865	148.26
pagerank	1.000	0.859	1.000	1.012	1.000	1.775	8.961
clustering	0.021	8.132	0.753	10.416	0.832	13.364	185.072
triangles	0.783	8.135	0.958	10.428	0.892	13.376	185.235
assortativity	0.963	1.284	0.969	1.586	0.975	1.876	10.677
percolation limit	0.954	0.039	0.970	0.052	0.974	0.065	0.547
embedding&cluster time	-	7.996	-	9.999	-	12.287	-
total calculation time	-	38.795	-	49.879	-	60.521	568.419

6 ACKNOWLEDGMENT

This work was supported in part by the Fundamental Research Funds for Central Universities under Grant(2024ZCJH12).

REFERENCES

- [1] Thomas Alfroy, Thomas Holterbach, Thomas Krenc, K. C. Claffy, and Cristel Pelsser. 2024. The next generation of BGP data collection platforms. In *Proceedings of the ACM SIGCOMM 2024 Conference (ACM SIGCOMM '24)*. Association for Computing Machinery, New York, NY, USA, 794–812. <https://doi.org/10.1145/3651890.3672251>
- [2] Bahaa Al-Musawi, Philip Branch, and Grenville Armitage. 2017. BGP Anomaly Detection Techniques: A Survey. 19, 1 (2017), 377–396. <https://doi.org/10.1109/COMST.2016.2622240>
- [3] catchpoint. 2022. *The Comprehensive Guide to BGP*. Technical Report. Catchpoint Systems. <https://resources.catchpoint.com/hubfs/eBooks/TheComprehensiveGuidetoBGP.pdf>
- [4] Yihao Chen, Qilei Yin, Qi Li, Zhuotao Liu, Ke Xu, Yi Xu, Mingwei Xu, Ziqian Liu, and Jianping Wu. 2024. Learning with semantics: Towards a semantics-aware routing anomaly detection system. 5143–5160. <https://www.usenix.org/conference/usenixsecurity24/presentation/chen-yihao>
- [5] Catalin Cimpanu. 2020. CenturyLink outage led to a 3.5% drop in global web traffic. (2020). <https://www.zdnet.com/home-and-office/networking/centurylink-outage-led-to-a-3-5-drop-in-global-web-traffic/>
- [6] Craig Labovitz, G. Robert Malan, and Farnam Jahanian. 1997. Internet routing instability. 27, 4 (1997), 115–126. <https://doi.org/10.1145/263109.263151>
- [7] Kim Da-sol. 2021. KT suffers major network outage nationwide. (Oct. 2021). <https://www.koreaherald.com/article/2713348> Section: The Korea Herald.
- [8] DB-IP. [n. d.]. IP geolocation API & free address database | DB-IP. ([n. d.]). <https://db-ip.com/>
- [9] Yutao Dong, Qing Li, Richard O. Sinnott, Yong Jiang, and Shutao Xia. 2021. ISP self-operated BGP anomaly detection based on weakly supervised learning. In *2021 IEEE 29th International Conference on Network Protocols (ICNP)*. <https://doi.org/10.1109/ICNP52444.2021.9651957>
- [10] MaxMind GeoIP. [n. d.]. MaxMind GeoIP® databases | MaxMind. ([n. d.]). <https://www.maxmind.com/en/geoip-databases>
- [11] Thomas Holterbach, Thomas Alfroy, Amreesh Phokeer, Alberto Dainotti, and Cristel Pelsser. 2024. A system to detect forged-origin BGP hijacks. In *Proceedings of the 21st USENIX Symposium on Networked Systems Design and Implementation (NSDI'24)*. 1751–1770. <https://www.usenix.org/conference/nsdi24/presentation/holterbach>
- [12] IP2Location. [n. d.]. Free IP geolocation database. ([n. d.]). <https://lite.ip2location.com/>
- [13] Jun Li, Michael Guidero, Zhen Wu, Eric Purpus, and Toby Ehrenkrantz. 2007. BGP routing dynamics revisited. *ACM SIGCOMM Computer Communication Review* 37, 2 (March 2007).
- [14] Kevin Hoarau, Pierre Ugo Tournoux, and Tahiry Razafindralambo. 2021. BML: An Efficient and Versatile Tool for BGP Dataset Collection. In *2021 IEEE International Conference on Communications Workshops (ICC Workshops) (2021-06)*. 1–6.
- [15] Thomas N. Kipf and Max Welling. 2016. Variational Graph Auto-Encoders. (2016). [arXiv:stat.ML/1611.07308](https://arxiv.org/abs/1611.07308) <https://arxiv.org/abs/1611.07308>
- [16] Angélique Medina. 2021. Facebook outage analysis | ThousandEyes. (2021). <https://www.thousandeyes.com/blog/facebook-outage-analysis>
- [17] Mengying Xu and Xing Li. 2020. BGP Anomaly Detection Based on Automatic Feature Extraction by Neural Network. In *2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)*. <https://doi.org/10.1109/ITOEC49072.2020.9141762>
- [18] Nabil M. Al-Rousan and Ljiljana Trajković. 2012. Machine learning models for classification of BGP anomalies. In *2012 IEEE 13th International Conference on High Performance Switching and Routing*. <https://doi.org/10.1109/HPSR.2012.6260835>
- [19] Paulo Fonseca, Edjard S. Mota, Ricardo Bennessy, and Alexandre Pasito. 2019. BGP Dataset Generation and Feature Extraction for Anomaly Detection. In *2019 IEEE Symposium on Computers and Communications (ISCC) (2019-06)*. 1–6. <https://doi.org/10.1109/ISCC47284.2019.8969619>
- [20] Lancheng Qin, Dan Li, Ruifeng Li, and Kang Wang. 2022. Themis: Accelerating the Detection of Route Origin Hijacking by Distinguishing Legitimate and Illegitimate MOAS. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 4509–4524.

- [21] RIPE. [n. d.]. Welcome to RIPE and the RIPE NCC. ([n. d.]). <https://www.ripe.net/>
- [22] RouteViews. [n. d.]. RouteViews - University of Oregon RouteViews Project. ([n. d.]). <https://www.routeviews.org/routeviews/>
- [23] Xingang Shi, Yang Xiang, Zhiliang Wang, Xia Yin, and Jianping Wu. 2012. Detecting prefix hijackings in the internet with argus. In *Proceedings of the 2012 Internet Measurement Conference (IMC '12)*. Association for Computing Machinery, New York, NY, USA, 15–28. <https://doi.org/10.1145/2398776.2398779>
- [24] Kuai Xu, Jaideep Chandrashekar, and Zhi-Li Zhang. 2010. Principal component analysis of BGP update streams. *Journal of Communications and Networks* 12, 2 (2010), 191–197. <https://doi.org/10.1109/JCN.2010.6391376>
- [25] Yujing Liu, Xiapu Luo, Rocky K. C. Chang, and Jinshu Su. 2013. Characterizing Inter-Domain Rerouting by Betweenness Centrality after Disruptive Events. *IEEE Journal on Selected Areas in Communications* 31, 6 (June 2013). <https://doi.org/10.1109/JSAC.2013.130616>