Border Gateway Protocol

Tier Prediction and Loss of Latency

Marti Zentmaier and Harmeet Singh

CS142 Network Science, Tufts University

4/24/25

1. Introduction

1.1 Background

The Border Gateway Protocol (BGP) is the main routing protocol of the Internet. It's responsible for exchanging reachability information between Autonomous Systems (ASes), which are independent networks managed by organizations such as universities, corporations, and Internet service providers. BGP lets ASes form a decentralized but globally connected network, where each AS advertises the IP prefixes it owns and the paths it can use to reach other prefixes. Routers use these advertisements to build AS Paths, which form the foundation for packet forwarding across the Internet.

Although BGP appears to be a protocol focused on efficiency, it's largely affected by the economic relationships between ASes. These relationships fall into two main categories: customer-provider and peer-to-peer. A customer pays a provider to carry its traffic, while peers exchange traffic without payment, usually between networks of similar size. These roles affect routing decisions. For example, an AS might route traffic through a paying customer, even if the path is longer, because it generates revenue. As a result, BGP routing isn't always about finding the shortest or fastest path; it's about enforcing business policies. These relationships form a hierarchy among ASes, referred to as tiers. Tier-1 ASes sit at the top; they don't pay anyone for transit and can reach every other network through peering agreements. Tier-2 ASes pay Tier-1 providers but may still peer with others, and Tier-3 ASes typically depend entirely on upstream providers to reach the rest of the Internet. This tier structure plays an important role in how internet traffic flows, but it isn't always visible, and many ASes don't openly advertise their position. Because of this, we explore the two questions defined below.

1.2 Research Question

First, can we estimate how much latency is added due to how the Border Gateway Protocol routes traffic, and why that happens? It's well known that network traffic tends to follow paths that lead to profit for some companies, but is this the only reason and can we explore why this is the case? Our second question is, can we predict the tier of any given Autonomous System using only BGP data? The purpose of this question is to find out information about systems that don't openly share their tier or role in the network. We aim to find patterns that can help classify ASes using machine learning on features derived from BGP announcements.

2. Data

Originally we started with only one dataset but over the course of working on these questions we added in two more datasets to support broader testing and validation. Our data comes from RIPE NCC, a nonprofit organization that collects and registers routing data in different regions and globally. It does so through the use of multiple route collectors. We used data provided from route collector 11 (rrc11) and route collector 21 (rrc21). These are based in New York, United States and Paris, France respectively. We took two datasets from route collector 11, one from March 1, 2025 and one from April 1, 2025 to test our methods across some period of time. We only took one dataset from route collector 21 since we only wanted to verify findings at another location. That data is collected from April 29 2025.

3. Method

3.1 Data Preparation

The format of all three datasets is consistent. They are provided as a bgpdump, which is raw data that RIPE's route collector stores and is not human-readable. To make this data usable, we downloaded a tool named "bgpdump" on a linux machine and then used the tool on the raw data. This converted it such that each line became one of the entries made by network traffic.

Each line is called an announcement. An announcement is the way a given Autonomous System (AS) declares to all that can hear it, "Hey, I have access to these IP prefixes, and I heard this from so and so!" IP prefixes are the networks that the AS can reach, and each announcement also includes an AS Path, which shows the ASes from which the information was learned. If the AS Path contains just one ASN, it means the announcement is originating from that AS. If it contains multiple ASNs, you can trace it back to the original source. Below is the template of an announcement:

DumpType | Timestamp | EntryType | Peer IP | Peer ASN | IP Prefix | AS Path | Route Protocol | Peer IP | Metric | LocalPreference | BGP Communities | AggregationStatus

We only cared about the Peer ASN and AS Path, as those two fields contained all the information needed to create our graph network. We built this network by creating a directed edge from each ASN in the AS Path to the next. Once we constructed the graph, we obtained the following graph attributes:

March 1, 2025 RRC11*: 84009 Nodes | 168808 Edges*

April 1, 2025 RRC11*: 38020 Nodes | 75464 Edges*

April 29, 2025 RRC21*: 38169 Nodes | 93379 Edges*

3.2 Distance-Based Latency Approach

We wanted to determine how much latency was added as a result of the way the Border Gateway Protocol routes traffic. First, what is latency? Latency is the time it takes for network packets to travel from one network to another. Two main factors contribute to latency: transmission delay and propagation delay. Transmission delay is the time it takes to push all the bits of a packet onto the network link, and it depends on the size of the packet and the available bandwidth. Propagation delay refers to how far the packet must travel—the greater the distance, the longer the delay. Latency combines both of these delays to represent the total time it takes for a packet to reach its destination. With this understanding, we then moved on to estimating the latency in our dataset.

To do this, we needed all the ASNs that appeared in the network—which we had access to—but we also needed a way to send pings between any two ASNs that shared an edge. At first, this seemed straightforward, but the tools available quickly revealed limitations. Many tools restrict how many ping requests can be sent, and given the size of our networks, this meant we couldn't feasibly compute latencies for all edges. While we could have tried working with a subset, doing so risked omitting important parts of the network and losing crucial structural information. Even if we had access to tools that allowed unlimited pinging, we would still face another issue: not all ASes allow ICMP (ping) traffic. This is often intentional where many companies block ping requests to avoid unnecessary incoming traffic. The same is true for individual users and customers, many of whom have pinging disabled by default.

Our new approach was to focus on what makes up latency and simply remove transmission delay from the equation. The reason for this is that we had access to the physical locations of most networks, and because propagation delay is proportional to distance, we could get a reasonable estimate of how long it would take for data to travel between two points. While this gave us a useful approximation, it wasn't fully accurate, since we excluded transmission delay, our latency estimates only reflect the distance-based component of the total delay.

With our new approach, we used an ASN lookup to find the latitude and longitude of each ASN. However, some ASNs could not be located this way. We assumed that these missing entries were not Tier 1 or Tier 2 networks, since those are large, publicly known companies—even if they try to hide their behavior, their existence is documented. This meant that any ASN missing from the lookup was likely a customer, so we assigned it a constant value based on the average of all known distances. Because customer ASNs tend to be leaf nodes in the network, this approximation doesn't significantly affect the results. Still, in the rare case that a customer has multiple edges or if a higher-tier network is misclassified as private, assigning an average distance helps prevent skewing shortest path calculations.

Now that we had access to most latitude and longitude coordinates, we calculated the edge weights using the Haversine formula. This formula calculates the straight-line distance between two points on Earth ignoring any obstacles using latitude and longitude coordinates. We chose this approach because we assumed that networks are designed with near-optimal wiring layouts to deliver the best possible performance. While this may not reflect every real-world routing scenario,

it provides a consistent baseline for estimating geographic distance. Below is the Haversine formula:

$$x_1 = point\ 1\ latitude,\ y_1 = point\ 1\ longitude,\ x_2 = point\ 2\ latitude,\ y_2 = point\ 2\ longitude$$

$$a = sin^2(\frac{x_2 - x_1}{2}) + cos(x_1) * cos(x_2) * sin^2(\frac{y_2 - y_1}{2})$$

$$c = 2 * arctan\,2(\sqrt{a}, \sqrt{1 - a})$$

$$d = 6371km * c$$

Once we applied distances to all relevant edges in the graph, we could begin making comparisons. Our method was to take each AS Path observed in the bgpdump and compare it to the shortest possible path in our constructed network graph, using standard shortest path calculations. This allowed us to estimate how much longer real-world BGP paths were compared to the most direct geographic routes. See Section 4.1 for the final results.

3.3 Machine Learning Techniques

To predict the tier of an Autonomous System, we used supervised machine learning models trained on features derived from the BGP announcement data. We treated each AS as a node in a graph, where edges represent observed AS paths. From this graph structure, we calculated structural features for each node, including in-degree, out-degree, in-degree centrality, out-degree centrality, and closeness centrality. These features serve as input to our machine learning models. We chose this input because BGP announcements are collected from publicly available route collectors, so if the predictions prove successful, we can label private companies with tiers—even if they don't disclose this information—since their routing activity would still be visible to route collectors. We used these particular features because they show how central or well-connected an AS is within the routing network, which we expect to correlate with tier. For example, Tier-1 ASes are likely to have high centrality and large degree values due to their role in providing global transit, while Tier-3 ASes tend to have fewer connections and lower centrality.

We labeled 70% of the ASes in our dataset using publicly available tier information (Tier 1, Tier 2, or Tier 3) from CAIDA's AS Rank API and reserved the remaining 30% for testing. We trained three classification models – Random Forest, XGBoost, and LightGBM – to predict the tier of a given AS. Each model was tuned using a grid search over relevant hyperparameters. For the Random Forest model, we tuned the number of trees, the maximum depth of each tree, the minimum number of samples required to split a node, and whether to apply class balancing. For XGBoost, we tuned the number of trees, tree depth, learning rate, the fraction of features to sample for each tree, and the fraction of training data to use per iteration. For LightGBM, we tuned the number of trees, tree depth, learning rate, and class weight settings. These hyperparameters were chosen to control model complexity, improve generalization, and handle class imbalance in the training data, since Tier 1 ASes are far less common than those in Tier 2 or 3.

After training, we applied the models to predict the tiers of ASes without known labels. We verified the validity of some predictions using external tier information from CAIDA's AS Rank API, which provides data on AS relationships and tier classifications. To assess generalizability, we tested model performance on a new dataset collected from a different BGP monitor—RRC21, located in France—using data from April 29, 2025. This allowed us to evaluate how well the models performed on unseen ASes from a different region of the Internet.

4. Results

4.1 Distance-Based Method Results and Conclusion

The distance-based findings were particularly interesting. After comparing the actual AS Paths from the bgpdump data to the shortest possible geographic paths in our constructed network, we observed the following results for each dataset:

Dataset	***Shorter Alternative***	***Cheaper & Shorter***	***More Expensive & Shorter***
RRC11 – March 1, 2025	*~33%*	*~19%*	*~14%*
RRC11 – April 1, 2025	*~31%*	*~19%*	*~12%*
RRC21 – April 29, 2025	*~39%*	*~24%*	*~15%*

Table 1: Distance Findings

Each metric examines every given AS Path and attempts to find how many of them have an alternative path that fits one of the following criteria. "Shorter Alternative" identifies the percentage of AS Paths that have another path with fewer hops, regardless of whether the alternative is more or less expensive in terms of geographic distance. "Cheaper & Shorter" and "More Expensive & Shorter" account for distance cost as well, effectively splitting the first metric into two more detailed categories. These provide additional information into whether shorter paths are also geographically cheaper or more costly.

The findings we observed were fairly consistent across both regions and all three time snapshots. This suggests that there is clear room for improvement in how the Border Gateway Protocol decides to route traffic. Based on the table, one might estimate that around a 20% improvement in latency could be possible. However, this is not entirely accurate, as several factors and metrics remain inaccessible or hidden from us at this time. Below is an example of a shorter

and cheaper path that illustrates this point:.

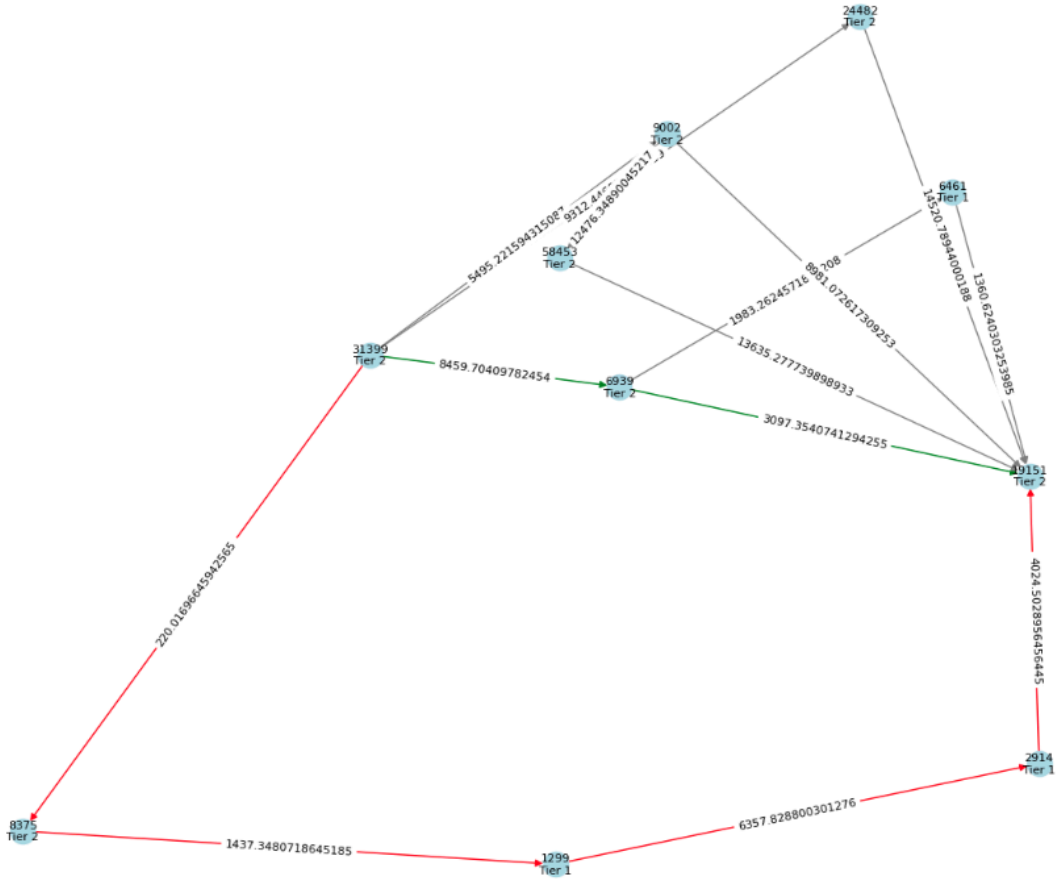

Figure 1: Cheaper Shorter Alternative Route

From Figure 1, we can gain some insight into what might be missing from our analysis. Clearly, ASN 31399 should be taking the green path, as it is cheaper both in terms of hop count and geographic distance. However, for some reason, it instead follows the red path. This unexpected behavior could be due to a number of factors.

Firstly, we do not have an accurate measurement of total latency. We cannot say for certain whether the red path is actually more expensive than the green path. As noted in Section 3.2, we removed transmission delay from our latency estimates. It's entirely possible that including transmission delay could shift the results and change our understanding of which paths are truly shorter. With full latency data, we might find that what appears to be the better path based on distance alone isn't actually optimal in practice.

The other missing metrics are less technical and more hidden from the public eye. These involve the social and economic aspects of network behavior—such as contracts between companies that dictate how data is sent and received. In some cases, routing decisions may also be influenced by concerns around data privacy or trust, where an AS may deliberately avoid sending

traffic through certain networks. These factors are difficult to measure but likely play a significant role in why seemingly less efficient paths are chosen

What comes next for latency measurements is expanding our analysis to include more regions, and eventually a global network, to see how our values hold up at a larger scale with more diverse connections. An important goal is to find a way to obtain true latency values, including both transmission and propagation delays, so we don't overlook important details. In addition, future work could explore the underlying social and economic relationships between the companies that own these networks. Understanding those dynamics may help identify opportunities to improve routing decisions and ultimately provide everyday consumers with a faster and more efficient Internet experience.

4.2 Machine Learning Results and Conclusion

All three models performed well on the held-out test set, with XGBoost and LightGBM slightly outperforming Random Forest. XGBoost and LightGBM both achieved an accuracy of 0.91, a macro-averaged F1-score of 0.71, and a weighted F1-score of 0.90. Random Forest performed slightly worse, with an accuracy of 0.89, macro F1-score of 0.69, and weighted F1-score of 0.88. The macro F1-scores show how well the models handled each tier class individually, while the weighted F1-scores account for the class imbalance. We can see that Tier 1 ASes had the lowest precision and recall across all models, which shows the challenge of learning from sparse examples. These results are summarized in the confusion matrices and performance tables included in our figures, which show that XGBoost and LightGBM produced more consistent predictions across all three tiers.

We also tested the trained models on new data collected from the RRC21 monitor in France. This dataset gave us an opportunity to evaluate model generalization to a new geographic and topological context. On this test set, XGBoost again outperformed the other models, achieving an accuracy of 0.89 and maintaining strong class-level performance. Random Forest and LightGBM achieved similar accuracy (0.83 and 0.82, respectively), but showed a sharper drop in F1-score for Tier 1 predictions. Overall, the results demonstrate that tree-based models—especially gradient boosting methods—can show meaningful patterns in BGP-derived features and generalize reasonably well across monitors. The included performance charts and classification reports visualize how each model handled class imbalance and minority class detection in both the original and external datasets.

Model	***Accuracy***	***Macro F1***	***Weighted F1***
Random Forest	*.89*	*.69*	*.88*
XGBoost	*.91*	*.71*	*.90*

LightGBM	*.91*	*.71*	*.90*

Table 2: Classification Metric on Held-Out Test Set (RRC11 March 1st New York)

Model	***Accuracy***	***Macro F1***	***Weighted F1***
Random Forest	*.83*	*.65*	*.84*
XGBoost	*.89*	*.77*	*.89*
LightGBM	*.82*	*.64*	*.83*

Table 3: Performance on New Dataset (RRC21 April 29th France)

Our machine learning models demonstrate that it is possible to infer the economic role of an Autonomous System, specifically its tier, directly from publicly observable BGP announcement data. This method gives immediate insight into network structure without relying on manually looking up sources like PeeringDB or BGPView. By analyzing structural features such as degree and centrality, we can detect consistent patterns that differentiate Tier 1, 2, and 3 networks. This not only offers a scalable alternative to manual lookup but also helps reveal the positions of ASes that intentionally hide their role. Even when an AS does not publish its tier or business relationships, its behavior in the global routing graph gives enough information for a trained model to make a reliable prediction. This work shows the potential of combining graph-based features with machine learning to bring more transparency to Internet infrastructure.

5. Sources

RIPE Network Coordination Centre. (2025, March). Routing Information Service – RRC11 (March 2025 data). RIPE NCC.
https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/rrc11

RIPE Network Coordination Centre. (2025, April). Routing Information Service – RRC11 (April 2025 data). RIPE NCC.
https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/rrc11

RIPE Network Coordination Centre. (2025, April). Routing Information Service – RRC21 (April 2025 data). RIPE NCC.
https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/rrc21

RIPE Network Coordination Centre. (n.d.). bgpdump. GitHub.
https://github.com/RIPE-NCC/bgpdump

RIPE Network Coordination Centre. (n.d.). MRT file format: Naming and location. RIPE NCC.
https://ris.ripe.net/docs/mrt/#name-and-location

RIPE Network Coordination Centre. (n.d.). Route Collectors: BGP timer settings. RIPE NCC.
https://ris.ripe.net/docs/route-collectors/#bgp-timer-settings

Wikipedia contributors. (2024, March 30). *Haversine formula*. Wikipedia.
https://en.wikipedia.org/wiki/Haversine_formula

Cloudflare. (n.d.). *What is an autonomous system?* Cloudflare.
https://www.cloudflare.com/learning/network-layer/what-is-an-autonomous-system/

Inter.link. (n.d.). *The difference between Tier 1 and Tier 2 ISPs*.
https://inter.link/the-difference-between-tier-1-and-tier-2-isps/