

Gaps and problems in current IP-Geolocation Approaches

In this digital era, IP geolocation has become a very critical component. In modern network operations and content delivery and security enforcement, and regulatory compliance. However, current approaches suffer from fundamental limitations that hinder accuracy, standardization and practical deployment. This paper identifies the gaps and the problems of existing IP Geolocation approaches.

Current IP Geolocation heavily relies on the commercial databases which suffers from several critical issues like **DHCP Lease, Granularity Limitations, Verification Challenges, Inconsistent results.**

In this paper we will discuss about these gaps briefly.

As we know that IP Address allocation changes frequently due to DHCP leases. This is a very common problem of many commercial databases. Many of the databases are still dependent on Regional Internet Registries, which gives inconsistent results due to lack of update.

Residential broadband users typically receive dynamic IP addresses that can change daily, weekly or sometimes monthly. Sometimes it is not possible to track changes in real-time, resulting in geolocation data.

Large Organizations frequently restructure their networks and reassign IP address blocks.

Most of the ip-geolocation databases failed to update this in real time.

Most Commercial Databases provide city level accuracy at its best, with some error margins but in Rural Areas the error is too high which leads an incorrect geolocation sometimes.

When precise location data is unavailable, many commercial databases provide a greater region which makes difficult to pinpoint an Ip address, leading to real world problems.

As there is no standardization mechanism for verifying the accuracy of geolocation this makes the problem too difficult to assess the reliability of different providers and different providers uses undisclosed algorithms and data sources, making it impossible to validate their algorithms and data sources. Providers combine data from different records bgp routing tables, latency measurements, reverse DNS lookups, user-submitted data, and proprietary partnerships. The relative weighting and qualities of these sources is unknown.

Modern IP geolocation data providers often validate their data against other geolocation providers, creating circular dependencies where systematic errors propagate across the industries. If multiple providers use similar flawed methodologies or share underlying data sources, their agreement provides false confidence.

Some geolocation providers allow users to report incorrect locations, but this approach suffers from selection bias, malicious reporting.

Independent Studies have shown that for the same IP address, different commercial providers can return locations separated by hundreds even thousands of kilometres.

Sometimes the commercial provider may return different locations for the same IP address over time, even when the actual assignment has not changed. This occurs due to database updates that correct previous errors, but it creates confusion for applications that cache geolocation results or perform time-series analysis.

Problems are also aroused in network complexities like **CGNAT, VPN and Proxy**.

The fundamental challenge CGNAT poses to geolocation is the many-to-one mapping, multiple geographically distributed users share a single ip address, this creates several real-life problems for modern providers like it became impossible to pinpoint location individually. When thousands of users share a single IP address and are distributed across a hundred-kilometre service area, there is no technical mechanism to determine which specific user generated a particular network flow. Any geolocation estimate for that IP address must represent an aggregate of all users, typically the geographic centroid or the location of the CGNAT gateway. The set of users behind a given CGNAT IP address changes constantly as NAT bindings are created and destroyed so it is also a problem for modern ip geo providers.

VPN providers constantly acquire new IP addresses and retire old ones so it became a major gap for ip - geolocation providers, in this case modern ip geolocation providers are facing some problems like False Positives (Legitimate users marked as VPN), False Negatives (VPN Servers marked as Legitimate)

Proxy Servers are also considered as nightmare to ip geo providers. Geolocation providers couldn't distinguish between proxy servers used for legitimate infrastructure and those used for location manipulation.

So, without fundamental changes in approach, IP geolocation faces existential crisis as CGNAT and VPN adoption continue accelerating. The technology must evolve from providing precise but increasingly inaccurate point locations toward providing probabilistic location intelligence.