CLOSTRA

NewNode: a Technical Introduction

The new content delivery technology resilient to censorship, spying, and shutdowns.

Executive Summary

To make a functional website and share content such as videos, images, and text, web publishers rely on content delivery networks (CDNs). CDNs are paid services that use data servers around the world to store and deliver content from publishers to end users. However, CDNs can be expensive, vulnerable to censorship and outages, and prone to slowdowns when bandwidth is overwhelmed.

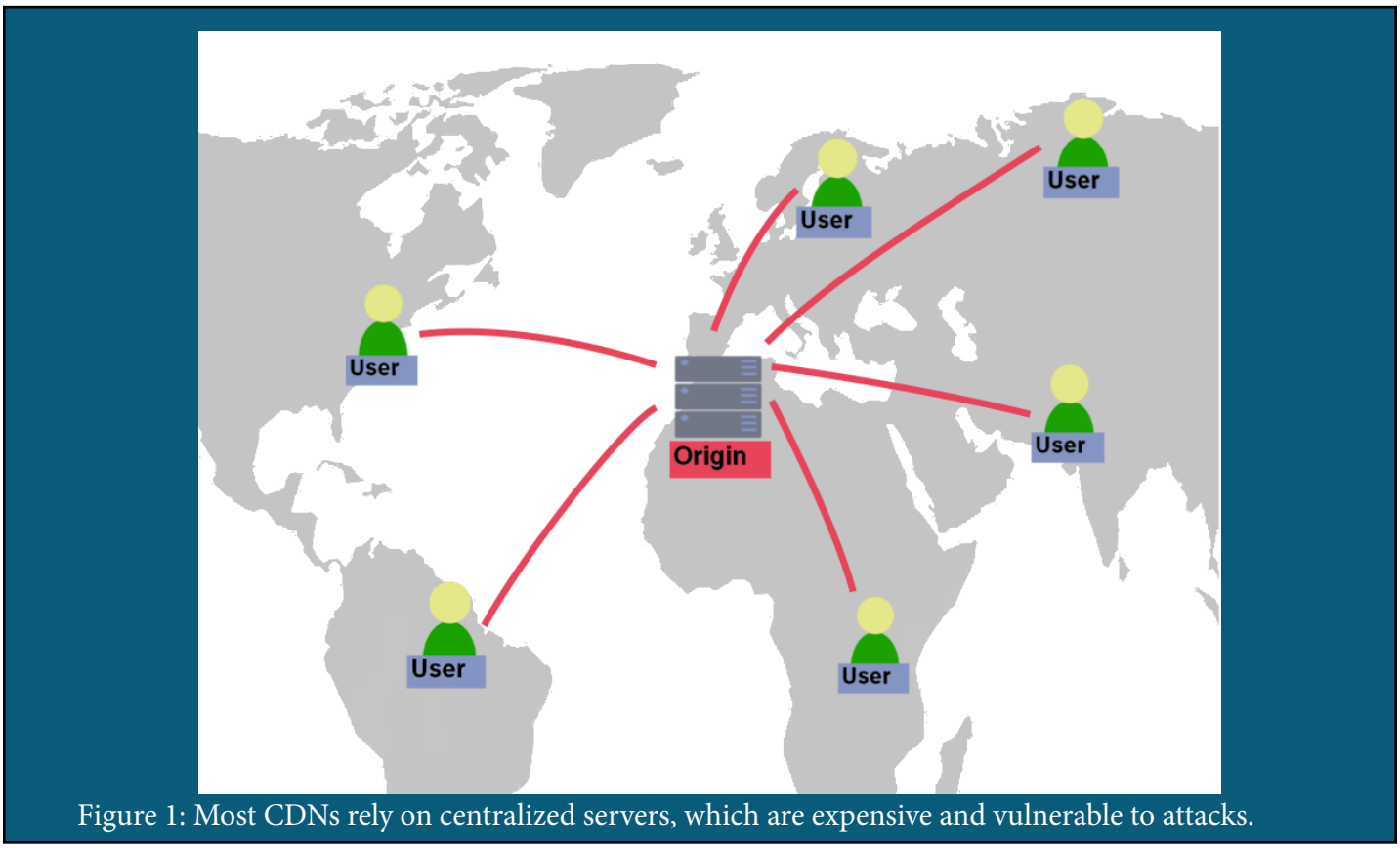


Figure 1: Most CDNs rely on centralized servers, which are expensive and vulnerable to attacks.

To avoid these issues, NewNode uses a decentralized network of devices, bringing content storage directly to the user. NewNode turns each device into a miniature server, creating a network that is totally free of the central servers typical of CDNs. This system benefits users, who have access to a large, decentralized network through which they can access content. At the same time, users benefit the system, allowing their devices to store and transport content for the entire network. This symbiotic relationship between users and network storage significantly improves the content delivery experience for web publishers in a number of ways.

NewNode avoids the slowdowns commonly caused by many devices attempting to access the same content once. Rather than causing slowdowns, increased content demand actually speeds up the delivery of that content, which now has many more nodes through which to travel.

Because information is stored and sent through a network of devices, the expenses associated with large content storage computers (typical of most CDNs) disappear. With traditional CDNs, bandwidth fees escalate as the user base grows, and when users request large files such as images and videos. Bandwidth fees of $10 per terabyte are common, which is equivalent to 100 users downloading 30 minutes of video content. These fees make traditional CDNs a major expense for content publishers. Rather than charging more for increased bandwidth usage, NewNode charges at a constant rate, since increased user activity also increases available storage space.

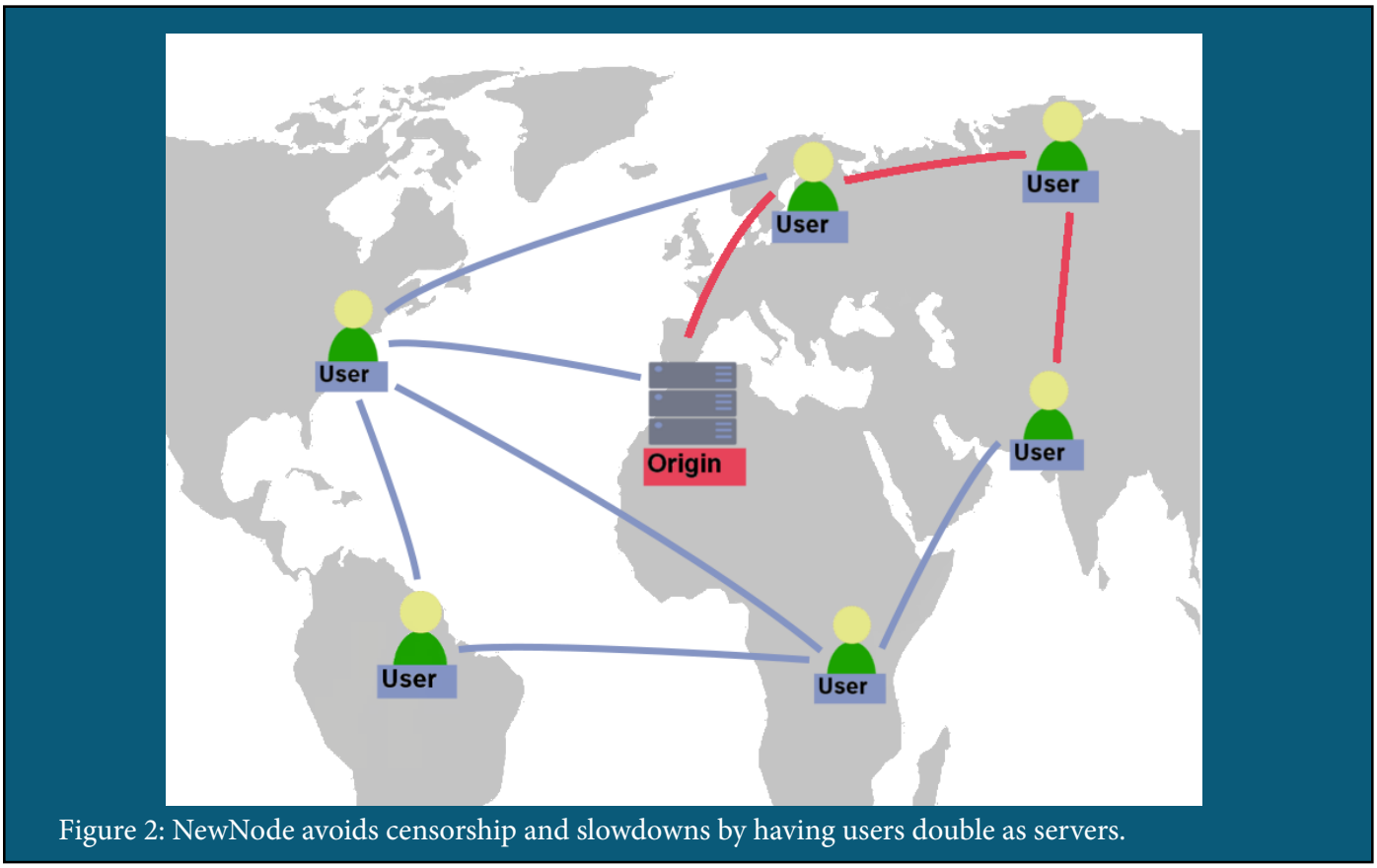


Figure 2: NewNode avoids censorship and slowdowns by having users double as servers.

Censorship also becomes incredibly difficult when information is passed through user devices - there is no clear, central information storage location for censors to target. Deep Packet Inspection (DPI) attacks and Distributed Denial of Service (DDOS) attacks are especially ineffective against NewNode, since NewNode distributes information through an encrypted grassroots user network.

Aside from censorship, content may become inaccessible because users are located in remote areas of the world, far away from traditional CDN servers. Content is often needed in countries and networks where the CDN has limited presence and limited spare capacity. With NewNode, content storage follows the user. No matter how obscure the location, wherever there is demand, there is supply.

Technical description

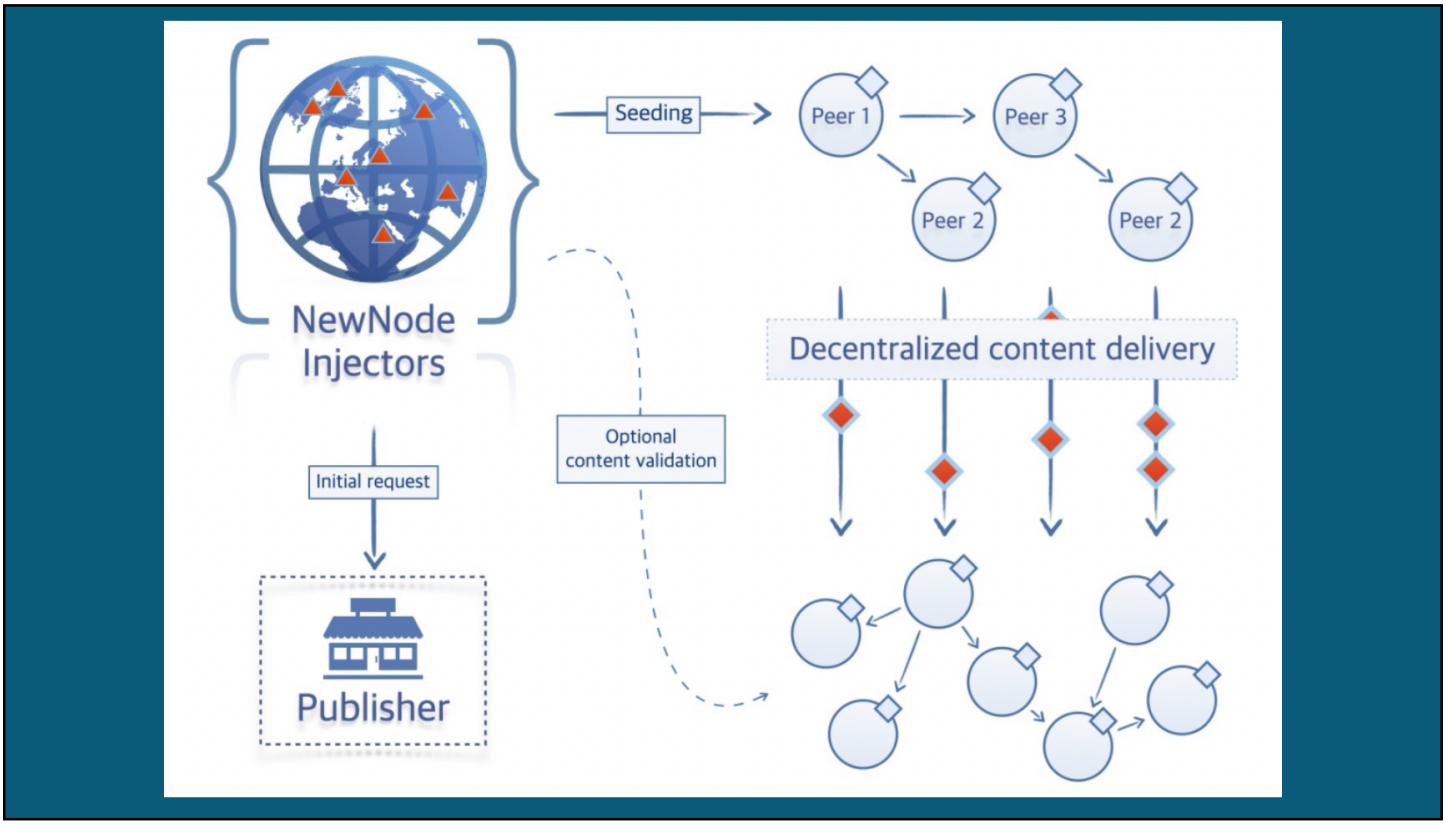
What are the key elements that make NewNode work?

Peers. Peers are nodes that function in the network. All NewNode user devices are peers.

Injectors. Injectors are cloud-based proxies that retrieve content from the original web location and present it to the peer network. They also ensure content accuracy. When content is requested, it is broken up into many tiny pieces, sent through multiple devices, and reassembled at the device that requested the content. Sometimes, censors will attempt to ruin content by presenting fake pieces to a peer, resulting in completed content that is garbled or inaccurate. To avoid this problem, injectors use a Distributed Hash Table (DHT), a database full of unique keys for every piece of content. Injectors can compare the values in the DHT to the hashes presented by the peers, and can then assure a peer that the content it has received is accurate. If the user tries to access content that the DHT has never encountered before, the peer retrieves it directly from the source, then reports it to the DHT, which then stores it for future use. Injectors run in the cloud. If they are unavailable due to lack of access, content can still be delivered - it just won't be signed (i.e. validated) by the injector.

Distributed Hash Table (DHT). As was mentioned earlier, the DHT is a database that allows the injector to confirm the accuracy of a peer's content. Unlike most hash tables, a distributed hash table like the one used by NewNode spreads information storage among many peers, rather than relying on a central storage location. Like many aspects of NewNode, this distribution prevents adversarial actors from accessing and deleting key information. Even if they find and manipulate content stored on one device, many other devices will be able to take over and continue to distribute uncensored content. NewNode uses the same DHT utilized by BitTorrent, a popular communication protocol that also relies on decentralized content distribution. BitTorrent's DHT is estimated to have more than twenty-five million nodes across the world, and a large presence in restricted jurisdictions like China. NewNode takes advantage of those nodes, adding them to its already significant peer network to increase availability, resiliency, and speed.

LEDBAT. Potential NewNode users often worry that their device will be slowed down if it has to transport other people's content. Low Extra Delay Background Transport (LEDBAT) is an algorithm that transfers data without clogging the network. Invented by Clostra CEO Stanislav Shalunov and now used by Apple and Microsoft, LEDBAT only directs traffic through your device if it senses that the device has available bandwidth - for example, if it is the middle of the night and no one is using the device. Thanks to LEDBAT, NewNode only uses available network space and does not impact the device's functionality.



Secure, reliable peer protocol. NewNode's protocol is made up of HTTP over LEDBAT, with some additional features. The protocol is enhanced and protected in several ways. First, the HTTP exchange (the request and response that takes place when accessing content through the web) is protected by a layer of transport encryption, to make surveillance and blocking harder. Next, range requests are used to access information. Range requests split the content up into several parts before sending them to the user. This allows large files to be split between several peers, rather than placing a heavy load on one peer, and helps speed up the downloading process for large files. Finally, content is authenticated using a Merkle tree. This is a security tool ensuring that data blocks passed between peers are whole, undamaged, and unaltered. When range requests split content into smaller parts, the Merkle tree verifies that every subset of content is accurate.

High Resilience

NewNode is designed to provide exceptional resilience across a broad range of disruptions.

Distributed Denial of Service Attacks (DDOS). A DDOS attack interferes with network functionality by sending a large number of requests to a server. This overloads the system and keeps legitimate requests from being fulfilled. Because the attack is distributed, it overwhelms the system from many different sources and makes it impossible to stop the attack by blocking a single source. NewNode avoids DDOS attacks because it, too, is distributed among many different peers. DDOS attacks, which latch on to one server, cannot gain footing in a system that is split between hundreds of thousands of miniature servers.

Deep Packet Inspection (DPI). Packets are small segments of data sent through the internet, which are combined in a user's device to form a complete piece of content. Censors use DPI to inspect these packets for undesirable content. They can then block packets containing information that they want to keep from users. NewNode avoids DPI attacks by encrypting the contents of its packets, which prevents censors from accessing packet content. NewNode's proprietary protocol is difficult to distinguish from other encrypted content, so DPI attackers will not recognize and target NewNode-encrypted packets. Finally, the network of injectors validates content, ensuring that DPI attacks have not cut out essential data.

Shutdowns and network outages. Sometimes governments will avoid censorship methods by simply shutting down a country's internet. Network outages can also occur by accident. Whether a shutdown is malicious or not, NewNode mitigates the effects and allows users to communicate even when connectivity is lacking. Devices plugged into the NewNode network communicate with one another through any available channel - even local connections such as WiFi Direct and Bluetooth Low Energy (BTLE). As users walk around and go about their daily lives, their devices reach out to other nearby devices to acquire and pass on messages, enabling essential communication. If even one device in the NewNode network briefly accesses the internet (for example, if one user manages to leave the country), all of the messages can be sent to recipients around the globe. Even if none of the devices can access the internet, they can still communicate across comparatively short distances, enabling organization on a city-wide or even country-wide level.

Case studies

NewNode enables web publishers to reach their audiences in censored locations around the world. Current NewNode clients include Voices of America, U.S. Agency for Global Media (USAGM), Middle East Broadcasting Network, and more. As of August 2021, NewNode has about 127k unique users across all apps.

TUT.BY is the leading independent media source in Belarus, and its Android and iOS apps have collectively more than 1 million installations. The site has been sporadically disrupted by state agencies, often during protests just when demand for TUT.BY spikes. After enabling NewNode in its mobile app, TUT.BY has been able to use its app to distribute content despite widespread internet shutdowns and the blocking of its website. As a result, the app's install base quadrupled from 250,000 to over 1 million users.

Radio Free Europe is a U.S. government-funded organization that broadcasts news and information to countries facing censorship in Eastern Europe, Central Asia, Caucasus, and the Middle East. RFE achieved a nearly 20% increase in their traffic in censored areas as a result of adopting NewNode technology.

Conclusion

NewNode is a revolutionary tool that provides significant gains in content delivery, including lower costs, higher resilience to censorship, and broader reach in areas with low connectivity. NewNode has helped hundreds of thousands of users access content around the world, and continues to make strides and improve its functionality.

Learn more:

Read about our success in Belarus:
https://www.coindesk.com/belarus-de-centralized-tech-resist-censorship

Visit our website: www.clostra.com

Contact us:
Email: contact@clostra.com
Phone: (415) 489-0510
Address: 1221 Brickell Ave., Suite 900
Miami, FL 33131