Netsukuku

Close the world, ʇxǝu ǝɥʇ uǝdO

http://netsukuku.freaknet.org

January 15, 2008

Abstract

Netsukuku is a P2P network system designed to handle massive numbers of nodes with minimal consumption of CPU and memory resources. It can be used to build a world-wide distributed, fault-tolerant, anonymous, and censorship-immune network, fully independent from the Internet. Netsukuku does not rely upon any form of backbone router, internet service provider network, or any centralized system, although it may take advantage of existing systems of this nature to augment unity and connectivity of the existing Netsukuku network.

In this document, we will give a plain-english description of the theory behind the Netsukuku system, with a focus upon core concepts and capabilities.

1 The old wired

The Internet is a hierarchical network maintained, operated, and controlled by large corporations and governments. Each and every packet of data must traverse countless backbone routers via unending lengths of fiber, all under corporate or government ownership, and subject to their exclusive control.

The Internet Service Providers provide connectivity to the lowest rank of this hierarchical pyramid, the end user. This is far removed from the ideal of a global user-based and decentralized network, depending upon the ISPs, both putting them in a position of power over the data received by the end users, and making them a single point of failure for those who they provide service to. The people can join the net only in accordance with the restrictive conditions and terms imposed by the ISPs, and subject to the filters and restrictions placed upon them, often even without their knowledge.

Today, the Internet represents the ultimate means of access to information, knowledge and communication. More than 1 billion people[8] can connect to this massive and immensely valuable, yet fundamentally proprietary and controlled, network. As impressive a statistic as this may be, the remaining 5 billion, lacking the economic resources necessary to assemble the necessary infrastructure or subscribe to what services are already available, are still waiting for the multinationals to supply a service within their reach. In this modern day, their lack of connectivity is more than an inconvenience; without this tool available to them, they are at a massive economic and educational disadvantage

to those of us who possess it.

The Internet was designed to be a secure, distributed, and failure-resistant communications of such quality that it would be appropriate for military usage, but now, paradoxically, as even the rigidly controlled military system proposed held distribution and redundancy in high regard, ISPs has the power to completely cut off even entire nations by simply refusing to provide their services any further, granting them an obscene amount of power, which is already commonly taken advantage of in no small way for profit. This prolific centralization also enables more sinister abuses of power, such as we see in China's censorship of all dissident thought[9]. This becomes even more worrying in light of the fact that any corporation who owns a single backbone router may view and modify a massive amount of the total data flowing through the Internet, even when it begins and ends at points outside of their control. Additionally, authorities with access to ISP data may use and have used the system as a means to identify and persecute locals who voice dissent[10]. This results from the non anonymous nature of the Internet: the ISP can easily trace all traffic going through their servers back to its point of origin.

Throughout the history of the Internet, its centralised and hierarchical structure has been the model for many subsidiary systems, such as the Domain Name System. DNS servers are managed by many of the same organizations responsible for providing Internet service (beyond simple consumer ISPs), with registration of a domain upon these servers a privilege provided by InterNIC, a United States controlled company, who grants registrars the right to sell single domain names to end users. This system is subject to all of the same issues as the Internet itself, if not more, resulting from its even greater centralization, and the reliance upon it for locating servers by almost all users of the Internet.

In China, all Internet traffic is constantly watched by several servers filtering the Internet traffic: a Chinese citizen must go to extreme and illegal measures to even become aware of a site which so much as mentions certain keywords, such as "democracy[9]." Disturbingly, even the risk of discovery of his circumventing the censors pales in comparison to that imposed by attempting to express his own political opinion online. Should it differ significantly from that supported by his government, his own life might even be at stake. This state of affairs is widely known, but few realise how close to home this practice truly is. Internet traffic is already routinely sniffed by countless national governments, and there even exists a small industry producing hardware and software to process the massive streams of data captured.

Efforts have been made to create systems offering additional levels of security and anonymity atop the existing Internet, but all have met with only limited success, if any, and none are totally free of vulnerabilities to the unavoidably well positioned administrators of the network. Even were one of these systems to prove technologically sufficient, its widespread adoption would be made impossible by the common tendency to adhere to the status quo, reinforced by the efforts of those who benefit from the current system to retain their power. As long as these efforts to bring more freedom, privacy, and accessibility to the Internet face resistance by governments and other organizations fearful of the risk imposed by true common freedom of expression, it will remain impossible to make the necessary changes by building upon the existing system. The only

remaining option is to rebuild from the ground up with a truly distributed, self-sufficient and fault-tolerant network, requiring support from none but those that use it. Such a system is inherently censorship-immune, as without any form of centralized backbone, any given node is unable to have any sort of widespread effect upon data originating elsewhere, or even form a clear idea of the content of data not sent to it. Netsukuku is just such a system.

2 The Netsukuku wired

The Netsukuku network is composed of nearby computers directly linked each other, and thus has no dependence upon the Internet, or indeed any existing network. The system augments level 3 of the OSI model with its own true distributed routing protocol. Netsukuku's distributed nature is emulated by the core services that are built upon it to replace those with similar centralization problems to the Internet, such as the previously discussed DNS, which is replaced by the introspectively-named Abnormal Netsukuku Domain Name Anarchy (ANDNA)[4].

2.1 Gandhi

The most notable characteristic of Netsukuku is its fully distributed self-management. The network dynamically configures itself without any external interventions, or any form of central organizing authority, something commonly believed to be infeasible, if not outright impossible. All nodes share the same privileges, each making a contribution to sustain and expand Netsukuku. Of particular interest is Netsukuku's increase in efficiency proportional to the number of well-connected nodes in the network, meaning that more users will typically lead to even lower latencies and greater bandwidth available to all. This is the exact opposite of the current system, where more users simply add stress to the system, leading to long response times and slow data transfers. This makes the network almost self-improving, as each user of the network has incentive to improve the network's quality. Even he who consumes massive amounts of bandwidth stands only to benefit from adding more interconnections of greater quality to more nearby nodes, substantially improving the network for all.

This total decentralisation and distribution allows Netsukuku to be neither controlled nor destroyed: the only way to manipulate or demolish it is to knock physically down each single node composing the network, making any form of attack or takeover attempt completely infeasible; if a hostile party had the resources to do such a thing, they would invariably find it easier to simply take what they had hoped to gain through control of information by force.

2.2 No name, no identity

Netsukuku allows anyone, in any place, at any moment, to connect directly to the network without need for paperwork or subscriptions. All the elements of the net are highly dynamic; nodes can come and go at will, needing to retain no inherent identifying characteristics, making identity and even route immensely malleable concepts. The IP address identifying a computer is chosen randomly, making it impossible to associate it with a particular location. Furthermore,

because the routes are composed by a huge number of nodes, it becomes a wholly infeasible task to trace a specific node by its traffic. Finally, traffic is protected by a strong cryptographic layer[5], which guarantees unparalleled security and anonymity for any connection.

2.3 So, what is it?

Netsukuku is a peer to peer or mesh network built on top of it's own dynamic routing protocol. While currently there are many dynamic routing protocols, most are, unlike Netsukuku, incapable of managing networks of significant size. To continue comparison, Internet backbone routers are managed by another set of functionally similar protocols, including OSPF, RIP, and BGP. They use classical graph algorithms designed to find out the best path to reach a node in a given net-graph, making for reasonably efficient routing. Unfortunately, all of these protocols must consume massive amounts of computational resources to function on a network of the scale of the Internet, and must exist on special dedicated machines. So great are the physical requirements of these unique (usually even purpose-built) machines, that decentralization is not only politically infeasible, but also economically impossible. Additionally, they depend upon a certain amount of hierarchy to function at all, and are thus easily disqualified from candidacy for mesh networking.

The Netsukuku protocol structures the topology of the network in different layers that resemble a fractal[3]. The Quantum Shortest Path Netsukuku (QSPN)[2] algorithm, designed for this specific situation, is then used to determine routes. Since the topology is characterized by an high degree of self-similarity, only the basic pattern must be stored. This massive compression level grants the ability to store the entire network map in just a few kilobytes. On the other hand, the QSPN algorithm must be executed by not any central routers, but instead the network itself. The component nodes perform this duty simply by generating, propagating, and parsing Tracer Packets (TPs), an activity that consumes very few computational resources.
For more information, please refer to the technical documentation: [3], [2].

2.4 The wireless

The cheapest and most convenient medium to establish physical connections between typical urban nodes is radio, incarnate as WiFi and similar technologies. In a scenario of widespread adoption, a new Netsukuku user need do little more than install a transceiver within range of other local nodes, linking themselves into the network, and configure their computer to take advantage of it. Today there exist a wide variety of WiFi technologies and similar which allows wireless connectivity between nodes even several kilometers distant. Even with common consumer technologies, an entire city can be easily covered by placing a single node in each neighbourhood.

Unfortunately, there will inevitably remain cases where geography or distance prevent a direct radio link. In these situations, or even in many cases where a long range radio link is feasible, a high-bandwidth low-latency connection more along the lines of a fiber bundle can be highly desirable, perhaps for connecting distant cities. However, such a solution is extremely costly, and is out of reach of a typical grassroots effort. If and when Netsukuku becomes

widely prolific, such projects might be sponsored by cities or governments, but in the meantime, we are unlikely to see much of that. Therefore, as a stopgap measure, it is possible to replace missing physical links by tunneling over the Internet[6], a practice that should be discouraged in the long term, but which makes a global Netsukuku network vastly more feasible in the immediate future.

References

[1] Netsukuku website: http://netsukuku.freaknet.org/

[2] QSPN document: http://netsukuku.freaknet.org/doc/main_doc/qspn.pdf

[3] Netsukuku topology document: http://netsukuku.freaknet.org/doc/main_doc/topology.pdf

[4] ANDNA document: http://netsukuku.freaknet.org/doc/main_doc/andna.pdf

[5] Carciofo NTK_RFC: http://lab.dyne.org/Ntk_carciofo

[6] Internet and Netsukuku: http://netsukuku.freaknet.org/doc/main_doc/inetntk.pdf

[7] CNET article on the legality of Comcast's filtering: http://www.cnet.com/8301-13739$_1$ − 9769645 − 46.*html*

[8] Miniwatts Marketing Group Internet Statistics: http://www.internetworldstats.com/stats.htm

[9] CBS on China's Internet Censorship: http://www.cbsnews.com/stories/2002/12/03/tech/main531567.sh

[10] Second Indymedia Server Seized in UK Within a Year: http://yro.slashdot.org/article.pl?sid=05/06/28/0113237tid=153tid=158tid=149tid=17

^_^