Holden Rohrer, Holden Watson, and Nithya Jayakumar
2019 Oct 21
Applied Combinatorics–Math 3012
Livshyts

Part 2: Progress Report

Topic: Distributed Systems Integrity and Correctness

1 Global Consensus

There's a famous problem in computer science called the Two Generals' Problem. It follows two Roman camps on opposite sides of a valley, claimed by enemies. Each can send a scout to the other to decide when to attack—which is necessary because if either attacks alone he is guaranteed to lose—but there is no guarantee the scout will arrive. Clearly, one message cannot guarantee consensus between the two. But neither can thirty—or a billion.

This is an attempt at global consensus in a distributed system, and is still an unsolved problem so far as such a problem can be "solved." However, algorithmic approaches are rapidly becoming more important as global consensus is intimately intertwined with novel technologies. These start with the internet and routing paths (even though they're both about 60 years old), torrent software, the TOR network, server redundancy in commercial applications, and the holy grail of distributed computing: cryptocurrency.

We want to review existing literature on the topic as well as practical applications of those principles (e.g. Bitcoin's consensus algorithm and its failures),[1] so we will use a variety of sources, primarily academic in nature, as well as use computing tools and/or combinatoric algorithms to understand how effective (or ineffective) certain systems are at achieving different tasks, like the several routing algorithms available to ISPs and different cryptocurrencies' consensus and hash algorithms (like between Monero and Bitcoin).

2 RSA Algorithm

Perhaps the most famous public-key cryptosystems algorithm is the RSA algorithm. This algorithm makes use of the difficulty to determine the prime factorization of large numbers, the infinite number of primes in existence, Eulers theorem, and the Euclidean Algorithm to encrypt communication. The RSA algorithm is an asymmetric (two keys) cryptographic algorithm, and can also be classified as public-key cryptography, as it involves the general knowledge of one of the keys.

As computer power and shortcuts to factorize large numbers become more efficient as we progress through the 21st century, the rapid increase of the magnitude of the large primes is necessary to keep encryptions secure. Decryption on the receiving end of the encrypted message uses a variety of techniques to decrypt the message efficiently, including the Chinese Remainder Theorem.

3 Network Robustness

Network connectivity is usually an issue on a local scale: one router or modem or device has a broken component—usually software that needs to be reset in one way or another. However, it rears its head on a very large scale as well: routing connections, as mentioned earlier, relies on the ability to communicate with at least one "neighbor" on the network, which is fine unless that neighbor goes down for whatever reason. And in non-decentralized systems, such as modern ISPs, that's exactly what happens: a software bug or power outage or any sort of problem tanks an entire area's coverage for hours to days.

3.1 Combinatorics Applications

Graphs, as noted in the textbook, describe similar situations very well: a member of the internet could draw out every other user and their connections as a graph, and that graph has measurable robustness. For a given service like Amazon AWS or Microsoft Azure, the service's connection to the rest of the web relies on hundreds of smaller connections in a distributed network across the nation.

We want to, using graph theory, study the reliability of those services in terms of bridges or k-connectivity, as well as how that could be improved (especially for the consumer market).

[1] *https://bitcointalk.org/index.php?topic=702755.0*