Context Research

Bachelor Project 2013 by Joël Gähwiler

Introduction

My background research was more concentrated on the theory and characteristics of cloud computing. Based on the realization, that our current way of connecting to each other is dependent on companies and money, we need to create first a free way to digitally connect all people. I used the context research to find appropriate technology to accomplish such a free way of digital speaking and get closer to the actual project concept.

Since i'm still working on the project idea and concept, i postponed direct user inquiries to the next phase. I wanted to gather more information about existing technologies and possible implementation scenarios.

Nerds thinking

In the background research i criticized the missing privacy and security by using the internet today. As i searched about how real internet and computer nerds think about this topic, i realized that there is more to worry about. Caleb James Delisle gives a good overview of the technology based problems:

> The Internet is built on protocols which largely date back to the late 80's or earlier. At a time when it was a network of anarchistic academics and scholars showing the ITU that open standards matter, it was absolutely enough. Over time the network has gotten bigger and the users have found new needs.
>
> In the age when packet inspection is universal and security breaches are commonplace, cryptographic integrity and confidentiality are becoming more of a re-

quirement. The US government recognized this requirement and has been helping through IPSEC and DNSSEC efforts.

Another issue is how are we going to route packets in a world where the global routing table is simply too large for any one router to hold it all? Despite the heroic efforts of core network engineers, the growth of the global routing table seems an unstoppable march. Cisco router company has proposed a plan called Locater/Identifier Separation Protocol, or LISP which aims to solve this by re-aggregating the routing table without forcing people to change their precious IP addresses. A different view of this problem is IP address allocation, currently it is done by a central organization which assigns IP addresses in such a way as to make the routing table as small as possible. Unfortunately this creates a bar of entry to the ISP sphere because aspiring network operators must register with the central organization and apply for an allocation of IP addresses while demonstrating that they will not be wasted. It is always easier to show that you need IP addresses if you already have a network.

Denial of service, an attempt to prevent legitimate users from accessing a service, is likewise a new problem in the expanding network. To my knowledge, there is no general purpose solution to denial of service attacks. Solutions to packet flood based denial of service often revolve around hosting a service on many computers so that they can handle an enormous amount of traffic.

Finally, the existing protocols are difficult to use, we cannot reasonably assign blame to anyone for this, many of these protocols are over thirty years old and demonstrate a level of craftsmanship which I can only hope to one day achieve. However, thirty years takes its toll on the best of us and as the Internet grew and became more complex, the administration interface of the typical router has grown a thicket of knobs, buttons and switches to match the proliferation of use cases and failure modes. As a result, network operation has become a science where students receive degrees and certificates for knowing the meanings of the plethora of knobs and switches, it has also become, like the tuning of the race car, an art, passed from master to apprentice and shared on mailing lists. Suffice to say, the bar of entry into the ISP realm is too high. […] [1]

What he tries to say is basically that we anyway have to rethink the whole internet because it's based on old technology which should be replaced with new ideas.

In fact the internet isn't a free place as the most people think it is. Internet access is in the most countries expensive and only available through Internet-Service-Providers. In some countries access is also censored and regulated by the state. Because of the complexity, there is no way for the community to create an alternate access to the infrastructure.

Fundamental changes

Nerds, geeks, researchers, developers, hackers and other people thinking

1 https://github.com/cjdelisle/cjdns/blob/master/rfcs/Whitepaper.md

about the future of the internet, have one thought in common: We have to make fundamental changes to the internet. To gain privacy, security, anonymity and durability the way we connect to each other has to be changed:

1. All communication between to nodes of the internet has to be signed and encrypted all the way to eliminate manipulation and monitoring of sent and received data.
2. The infrastructure should be changed to a decentralized model, where everyone is able to connect to the network without negotiating with an central authority.
3. The network has to be permanent and durable, single point of failures are history. Also the network should be able to evolve and scale unlimited.

The MondoNet is a project, that tries to address all these problems. The basis of this project are the 10 social specifications, which an be understood like the rules of moses:

1. Decentralized
2. Universally Accessible
3. Censor-Proof
4. Surveillance-Proof
5. Secure
6. Scalable
7. Permanent
8. Fast (Enough)
9. Independent
10. Evolvable

> The purpose of this project is to study the technological, social and regulatory feasibility of developing a peer-to-peer mesh networking protocol. This would serve as the foundation of a decentralized, ad hoc wireless mesh network, which would illuminate potential technology-based solutions to censorship and surveillance on existing digital communications platforms. MondoNet provides 10 social specifications for the development of a peer-to-peer mesh networking protocol. [2]

New Technology

There are several technologies who exist or are being developed to create such a free network. Some technologies are based upon the current internet, some try to create alternative networks which can be connected to the internet. Technologies who completely abandon the internet for creating a new one, are rare. Since these technologies are still being developed,

2 http://mondonet.org/about

there aren't that many users. The most technologies getting used for illegal activities as they are stable to use. Such small networks are mostly know under darknets.

Mesh Networking

A common technology used to create decentralized networks is: Mesh Networking:

> Mesh networking (topology) is a type of networking where each node must not only capture and disseminate its own data, but also serve as a relay for other nodes, that is, it must collaborate to propagate the data in the network. [3]

In a mesh network, all peers connect to peers near by them, while these peers are connected to other near peers and so on. Like in a mesh one node can have multiple connections to another node. For creating mesh networks the biggest problem is the routing of information along the nodes to reach a specific node in the mesh. There are many implementations of routing algorithms. Basic mesh networks send request to all nodes and hope that the message gets relay until the targeted node receives the message and emits a answer. More forward algorithms calculate the route a message has to take to reach his target with a minimum of intermediary nodes. The B.A.T.M.A.N protocol is one of the famous ones:

> B.A.T.M.A.N.'s crucial point is the decentralization of the knowledge about the best route through the network — no single node has all the data. This technique eliminates the need to spread information concerning network changes to every node in the network. The individual node only saves information about the "direction" it received data from and sends its data accordingly. Hereby the data gets passed on from node to node and packets get individual, dynamically created routes. A network of collective intelligence is created. [4]

The protocol is highly used for wireless mesh networks in urban spaces, where everyone is able to connect his router to the mesh network.

Tor

> Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy. [5]

A not that fresh technology is the Tor-Network, which has been created to address censorship and anonymity issues in China and other countries. The network is based on the internet, and a client software is needed to get access to the network.

Basically people use the Tor-Network to access resources on the inter-

---

3 http://en.wikipedia.org/wiki/Mesh_networking
4 http://en.wikipedia.org/wiki/B.A.T.M.A.N.
5 https://www.torproject.org/about/overview.html.en

net in a safe and anonymous way, by route their connection over different nodes in the Tor-Network. A packet send to another server in the network gets relayed 10 till 30 times between these servers to hide the actual origin of the packet. Through this routing, a receiving sever cannot determine the sender by his IP-Address or Browser identification.

At this point the Tor-Network is only another anonymizing service as many others. But what makes the Tor-Network a darknet is that people can access web sites and services, which are only accessible over the Tor-Network through so called Onion-Links. Because the communication in the network is completely encrypted and safe, the network is highly used for illegal activities on the internet. One of the best known such place for illegal activities is the Silk Road marketplace:

> The majority of products available to purchase on Silk Road qualify as contraband in most jurisdictions. Most sellers are based in the United Kingdom and the United States, and offer products such as heroin, LSD, cannabis, and other drugs. However, the site's operators prohibit goods or services intended to harm others, such as stolen credit card numbers, counterfeit currency, firearms, personal information, assassinations, weapons of mass destruction, and materials used to make such weapons. There are also a range of other products for sale, such as art, apparel, books, jewelry, pornography, and writing services. [6]

Cjdns

Another way goes the Cjdns project by Caleb James Delisle. The program allows people to create a mesh network with friends over the internet or other infrastructure. Cjdns can be seen as a extension on top of the standard internet protocol:

> Cjdns implements an encrypted IPv6 network using public key cryptography for address allocation and a distributed hash table for routing. This provides near zero-configuration networking without many of the security and robustness issues that regular IPv4 and IPv6 networks have. [7]

Different to the Tor-Network the Cjdns mesh network mounts itself into the communication stack of the computer. By this way the most applications (which are IPv6 enabled) can communicate over the network without any changes. Another big difference is the model of joining an existing network. The person, who wants to join a certain network has to find somebody in the network to peer with. Cjdns can be seen as a friend-2-friend network, where access is granted over an invitation like system. This way of connecting to a network is needed to establish the very secure connection to the network.

The developers claim that the technology is stable but the algorithms have to be tested first. For that reason they have created the test network Hyperboria which counts between 200 and 500 connected nodes.

---

6 http://en.wikipedia.org/wiki/Silk_Road_(marketplace)
7 https://github.com/cjdelisle/cjdns

Airmesh & Raspberry PI

Airmesh is a linux distribution which combines the above technologies into an usable operating system:

> Airmesh is a collection of the best open source mesh network technologies, packaged such that they are self configuring and produce a practical, network for various uses, including learning, as well as disaster and off grid communications as well as community networks. [8]

The Raspberry PI is a small single-board [9] computer the size of a credit card. Developed for education purposes the raspberry has now a big community of developers using the pi for all kind of embed devices. The Raspberry Pi is heavily used for Internet of Things [10] projects where a mass of cheap and powerful computers is needed. In combination with the Airmesh distribution the Rasperry Pi can easily be turned into a small mesh network node.

Context Finding

At this point the project outline comes clearer. It's obvious that i will do something with mesh networks. But it's important that i will find a context to prove my concept and iterate with people over the project.

War Zones

Since the Arab Spring many countries are in rebellion. As we mostly saw in Egypt, internet plays a much grater role in modern rebellions. Rebels use the internet to organize themselves and inform the world about their doing. Interesting was that after the egyptian state shutdown the internet the rebels felt more encouraged to change something. After the egyptian shutdown, students and other computer technologists tried to get alternative access to the internet. We believe that they connected over the syrian-egyptian border to get access to the internet.

Decentralized network technologies, like mesh networking, can be very useful in such situations to deploy a alternate network very fast. With technologies, like mentioned above, it's possible to create tap-proof networks for communications in war zones. The devices to create the network can be built be rebels in a DIY manor or shipped by other countries. Some hackers from HacDC [11] created the project byzantium. The byzantium operating system turns every computer with a wireless connection into a mesh network node:

> Project Byzantium, a working group of HacDC is proud to announce the release of v0.3 alpha of Byzantium Linux, a live distribution of Linux which makes it fast and easy to construct an ad-hoc wireless mesh network which can augment

---

8 http://www.netlore.co.uk/airmesh/?page=about
9 http://en.wikipedia.org/wiki/Single-board_computer
10 http://en.wikipedia.org/wiki/Internet_of_Things
11 http://hacdc.org

or replace the existing telecommunications infrastructure in the event that it is knocked offline (for example, due to a natural disaster) or rendered untrustworthy (through widespread surveillance or disconnection by hostile entities). This release was developed in the days following Hurricane Sandy, and was perfected while the core development team was assisting with disaster relief efforts in the Red Hook neighborhood of New York City in November of 2012. [12]

Crisis Zones

Another interesting context are crisis zones. After the earthquake in Haiti the infrastructure was heavily damaged. Humanitarian organizations like the red-cross or medecin-sans-frontier, who operate in the crisis zone, need a communication network to organize the help for the people. A mesh-network could also be here an interesting model for a fast deployable network. Devices can be attached to ruins, towers and other buildings to create a network over a bigger city. With point-to-point antennas it's also possible to integrated the surrounding into the network. The following is an interesting article by Darren Quick:

> Unsurprisingly, the Australian outback doesn't exactly boast the greatest mobile phone coverage in the world. But researchers down under have managed to make mobile phone calls in this remote landscape without the use of towers or satellites. Instead of relying on expensive infrastructure, the researchers created a mesh-based phone network between Wi-Fi enabled mobile phones that allowed them to communicate with each other.
>
> The successful test was part of the Serval Project, led by Flinders University's Dr Paul Gardner-Stephen, that aims to provide fast, cheap, robust and effective telecommunications in remote areas where conventional phone infrastructure isn't cost effective or where the existing infrastructure has been damaged by natural disaster, war or terrorism. The Serval Project – named after the problem-solving African wildcat – consists of two systems. The first is a temporary, self-organizing, self-powered mobile network for disaster areas, formed with small phone towers dropped in by air.
>
> The need for a decent concentration of devices within an area to provide an extended range suggests the technology probably isn't overly useful as it stands for sparsely populated areas. But its potential in the area of disaster relief could be significant.
>
> After the Haiti earthquake Ericsson deployed a "container based mini-GSM system," which is essentially a portable mobile phone network, to enable mobile phone communications in the area. However, this took days and was expensive. The software being developed by the Flinders University researchers could do the same thing but much more quickly and much more cheaply.
>
> "With Haiti what was actually observed was that their mobile phone network and their landline phone network was essentially knocked out for the first 48 hours after the earthquake," Dr Gardner-Stephen told ABC News.

---

12 https://github.com/Byzantium/Byzantium

> "What research has actually shown is that the vast majority of the response to a disaster is actually from the local people there, so if we can provide them with ease of communications as soon as possible after the earthquake, not 48 hours, not 72 hours but potentially minutes after a disaster, then we can help them to start rescuing people from rubble and generally rebuilding, maintaining law and order. [13]

Developing Countries

Since it is really hard to get into crisis and war zones and especially talk with people who had experience with such situations, i looked for people in my circle. Patrick T. Fischer is a friend of mine who's working for different projects in Cameroon. The most of these projects are focused on the agriculture and economy of the country. His wife is from Cameroon and both have experience in agriculture.

Many farmers produce cocoa and try to sell it to merchants. Mostly this cacao gets shipped to western countries. The cacao production got imported by the french during the colonialization age. After Cameroon achieved independency in 1960 they kept the cocoa production as on of the better working economies in the country. From a western point-of view the cocoa production in Cameroon has to deal with some issues:

1. Farmers attend to slash-and-burn areas of the rainforest to get new fields for planing cocoa, manioc, nuts or bananas. Burning the forest releases phosphor into the soil and boost the fertility of the earth.

2. The farmers in the countries compete very hardly with each other and sell their goods for a too low prices, because they need the money. Missing communicating does not allow the farmers to watch the market and sell their goods at the right time.

3. Information for the most problems is available in the country. Especially in agriculture there are many experienced farmers who know to deal with certain problems. Lacking a communication system and platform to share experience the farmers rely on help by third parties.

4. Education is still a problem in these countries. Sources like wikipedia for self information are missing, and the areas mostly lack of a proper education in more difficult fields.

Concept Idea

Putting all these things together, i imagine a platform which can be used to connect certain locations or a whole area to a decentralized network. Based on that network different goals can be achieved. In detail such a system can consist of the following components:

— **Embedded System**: A small computer with am embedded system is the central unit of each component. Equipped with Wireless technology it can connect to other devices within range.

---

13 http://www.gizmag.com/serval-mobile-phone-network/15696

— **Energy Source**: Adding as example a solar panel to the component makes it independent from energy sources. It's possible to use other energy sources as they match the target locations and environment.

— **Range Extender**: The range extender module allows to extend the range of the wireless unit to communicate with more far devices. It's also possible to achieve point-to-point connections over very long distances.

— **I/O Interface**: The standard I/O interface adds communication to other devices. This enables the device to read sensors or manage actuators.

All components together build a network, which itself provides services to their users. Following services could be implanted in a basic distribution of the software:

— **Data Collection**: Components equipped with I/O interfaces can collect data from various sources. This data can be collected by a user for statistics or other further usage.

— **Information Sharing**: Through technologies like wikipedia, users can share information among themselves event if there is no connection to the real internet.

— **Communication**: People need to communicate with each other. With technologies like VoIP and Chat protocols, people can instantly communicate to each other in a decentralized fashion.

The component and its modules should by design fit into urban and natural spaces. Materials used should be eco friendly and maybe adapter to the environment. The technology should be free and accessible by all people. To bootstrap the technology and provide a reference implementation a company like Canonical should maintain the software and hardware to guarantee a safe and reliable system.

With such a system everyone is able to create a network to communicate with people and machines. Communication is necessary to achieve a level of living and progress to the world.