The Case for Liberouters

Teemu Kärkkäinen[1] Jörg Ott[2]

Abstract: In this paper we argue that a set of fundamental forces has driven modern communication services to become highly centralized. This centralization has enabled globe spanning communication infrastructure and services to be built, but has also enabled powerful actors to monitor and control communications on an unprecedented scale. As a counterbalancing force we propose a *Liberouter* network, which decentralizes both the communication infrastructure and services.

Keywords: Decentralization, centralization, Liberouter.

1 Introduction

Communications are one of a small number of fundamental functions necessary for us humans to function as a society. It is how business is done, how ideas spread, and how knowledge and information necessary for learning is transmitted. Throughout history, we have invented systems and technologies to provide increasingly effective and efficient means of communication. Starting with the invention of complex language some $100,000$ years ago and the appearance of cave paintings about $40,000$ years ago, the invention of writing systems around 4000 BCE, alphabets in 2000 BCE, the postal system in the 6th century BCE and the printing press in 1440, and culminating in modern inventions such as the telegraph and the telephone in the 19th century, radio communications in the early 20th century, and finally the invention of the Internet in the late 20th century.

Over the past few decades the Internet has become *the* communication substrate, quickly taking over other forms of communication: We use Skype instead of phone calls, Netflix instead of TV, news sites instead of newspapers, Spofity instead of the radio, email instead of letters and social media instead of meeting friends at coffee shops.

In this paper we argue that within the development of the Internet infrastructure and services we can see a strong trend towards *centralization* of technology, ownership and control. This in turn has enabled powerful actors to monitor and influence communications between people on a scale never seen before in human history. We further argue that this trend must be counterbalanced by a complementary, fully decentralized network, and show how our *Liberouter* network achieves this. The contribution of this paper is the argument *why* the Liberouter network is important in a world with ubiquitous Internet connectivity – for technical details of our system we refer the reader to our previous publications [KO14]. We present our analysis of the centralization tendencies in Section 2, and describe how our distributed system design provides a decentralized alternative in Section 3.

[1] Technical University of Munich, kaerkkae@cs.tum.edu
[2] Technical University of Munich, ott@cs.tum.edu

2 Centralization of Communications

While both the Internet and the Web are decentralized architectures, in practice both have shown a strong tendency towards centralization. This is a natural result of *technological*, *economic* and *societal* forces acting on the communication *infrastructure* and *services*. As a consequence of the centralization, powerful actors are able to apply pressure and exert control over the people's communications and the interactions on an unprecedented scale.

From the *technological* perspective, systems are typically scaled up by building hierarchical structures (e.g., trees), which results in the higher levels of the hierarchy acting as centralization points. In terms of infrastructure, last-mile ISPs are centralized points over the consumers, while their transit ISPs and peering points are centralized points over them. In addition, typical modern large scale communication services are technically distributed among many data centers, but are all under the control of a single company. This is in contrast to early Internet services and protocols, such as email (SMTP) and Usenet (NNTP), which were designed to federate independently owned and operated servers.

From the *economic* perspective, the capital requirements of building the physical infrastructure are driving centralization, as only the largest actors can raise enough capital. For example, Vodafone, a European mobile operator, spent over 32 billion euros over three years on infrastructure and spectrum rights [Vo16]. With services, the demand-side economies of scale, or "network effects," have driven centralization. Each segment is dominated by one, or a few, services; e.g., Google for search and Facebook for social networking. As a result, there is no incentive for interoperating with competitors and companies instead build closed, centralized systems. This extends to native applications through the Internet distribution channels, such as Apple's App Store, Google's Play Store, and Valve's Steam – each holding a near monopoly of control in their market segments.

From the *societal* perspective, the centralized communication systems are an effective tool for enforcing rules and regulations. Especially since much of the discourse has moved to these centralized platforms from previously decentralized mediums, e.g., from pamphleteering to blogging. The important aspect is not the content of the rules – which may be perfectly justifiable – but that the rules are decided centrally and applied to everyone. This is a dangerous power to delegate to a central authority, especially when it comes to the content of the communications, because it enables mass scale imposition of ideologies.

While the centralization has created globe spanning infrastructure and services, it has also been used to apply mass control over the users. In the crudest form of control, governments completely cut off their population from the Internet, such as the outages during the Arab Spring [De11]. More sophisticated forms of control seek to censor certain topics or information through infrastructure based filtering or direct content removal. Freedom House, a watchdog organization, found that 34% of all Internet users live in countries that have cut off communications, and 61% in countries that censor criticism of those in power [Fr16]. Finally, the large privately owned services have no free speech protections and can act as all-powerful censors either for business reasons or after being compelled by governments; e.g., Germany compelling Facebook, Google and Twitter to police "hate speech" [BB16] on their platforms.

3 Decentralization via Liberouters

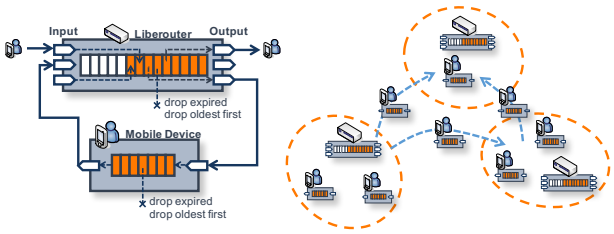

Fig. 1: The Liberouter system.

We argue that to tackle the problems caused by the centralization, a system is needed that decentralizes the communication *infrastructure* and *services* on the *technical*, *economic*, and *societal* axes. The goal is not to replace the current networks, but to augment them with a parallel, decentralized medium for communication, which can serve as a balancing force and a safety valve for the centralization.

Our solution, *Liberouters* [KO14], is a combination of opportunistic networking software with mobile phones and inexpensive embedded devices like the Raspberry Pi, as shown in Fig. 1. Left side of the figure shows the micro-level functionality of the system; a stationary Liberouter device acts as a mailbox to which mobile devices connect to pick up and drop off messages. Although each Liberouter can serve nearby mobile users independently, multiple Liberouters will cooperate to form a macro-level network as shown on the right side of the figure. Services are built as mobile applications that use the message dissemination service provided by the network to communicate directly with each other.

The design decentralizes both the infrastructure and service technologies. First, the infrastructure is made up from a dynamic set of Liberouter devices and mobile phones installed and carried by the users. The messages replicate in the network randomly through multiple paths over short lived contacts between the nodes. Second, the services running on the network are built as directly communicating mobile applications, without centrally controlled backends. Further, the messaging is open by default, i.e., the messages created by one application can by default be read by any other application.

The economic centralizing forces can be overcome by the low cost of the network components. The Liberouter devices cost about 50 euros; cheap enough to be deployed by individuals. The cost will further decline as cheaper embedded Linux platforms (e.g., Raspberry Pi Zero) come into the market. The low cost and size of the devices can enable novel infrastructure deployment models, e.g., concealing devices in public spaces where they will serve passing mobile phones. And because the services are developed as mobile apps, the service developers do not need expensive backend systems required by web services.

The design also decentralizes the system along the societal axis. An individual, or a group, deploying the Liberouter devices is in control of the rules for using and accessing the deployment. Communities can still set their own standards on what is acceptable behavior or speech, but cannot impose those standards on others against their will; neither can governments nor powerful private entities.

We believe the Liberouter network solves many of the problems created by centralization: There is no central switch to turn off the network, instead each Liberouter device would have to be found and turned off individually. The messages do not travel along centralized links where the traffic could be filtered or monitored and there are no centralized service operators that could be compelled to censor content. To monitor the communications, the attacker needs to be physically in the proximity of the devices, and even then the temporally decoupled publish/subscribe communication model does not reveal any communication relationships. To censor a message, all copies from all the devices and mobile phones would need to be deleted, otherwise the information will continue to live and replicate.

The decentralized system is an alternative set of trade-offs compared to classical Internet architectures, and as such has its own sets of limitations. For example, the asynchronous messaging model does not work for real-time applications or applications requiring low latency end-to-end interactions. And since the messages spread via human carriers, the data dissemination is likely to be geographically constrained rather than global. This is why we propose such a system as a *complement* rather than an *alternative* to the Internet.

4 Conclusion

In this paper we have made our case for a fully distributed Liberouter network, which can serve to balance the currently popular centralized networks and services, and the potential dangers created by them. We believe this balance can lead to a more sustainable and open society, as well as new innovative services and business models.

We are working to provide everything required for anyone to build their own Liberouter devices via the Liberouter website[3]. This includes system images for various embedded Linux devices with all the software required to act as a Liberouter device. We further provide various applications, including messaging, photo sharing and experience sharing that use the Liberouter network. We are also exploring various deployment opportunities where our system could provide communication services for people in situations where normal Internet access is not available.

References

[BB16] BBC News: Facebook, Google and Twitter agree German hate speech deal, http://www.bbc.com/news/world-europe-35105003, Accessed: 26.5.2016.

[De11] Dainotti, Alberto; et al.: Analysis of Country-wide Internet Outages Caused by Censorship. In: Proc. of ACM SIGCOMM IMC. 2011.

[Fr16] Freedom House: Freedom on the Net 2015. 2016.

[KO14] Kärkkäinen, Teemu; Ott, Jörg: Liberouter: Towards Autonomous Neighborhood Networking. In: Proc. of IEEE WONS. 2014.

[Vo16] Vodafone Group Plc: Annual Report 2015. 2016.

[3] http://liberouter.mobi