Resilient decentralized communicatidon for unstructured peer-to-peer networks

Dan Bachar
Technische Universität München
TUM Chair for Connected Mobility
Munich, Germany
dan.bachar@tum.de

Abstract

Recent events (natural disasters, war, protests) have shown that people heavily rely on online social networks and instant messaging platforms to communicate and coordinate aid efforts during cases such as disaster relief, protests, or emergency response to natural disasters. The existing internet infrastructure is distributed, but its management and ownership is heavily centralized which places power in the hands of a few individuals or companies, that are susceptible to implicit and explicit censorship, while the infrastructure itself is prone to failure in cases of disaster, leaving reliant communities in the dark. In this paper, we propose performance statistics for both simulated as well as real-life unstructured peer-to-peer social networks, as well as investigate and propose resilience metrics for such opportunistic networks.

1 Introduction

The decentralized administration of the internet is one of the basic enablers of the rapid growth of the Internet as a whole, thanks to the autonomous nature of decision making across different network systems. The core functionality of the Internet is based on a general-purpose solution developed originally by DARPA, uses IP routing using transmission control protocols to make sure a packet travelling along a network path between two distinct hosts will reach its destination reliably. Establishing, maintaining, and terminating connections between the different Internet autonomous system (ASs) is the task of the border routers between them, which are parts of the infrastructure belonging to the individual Internet Service Providers (ISPs) that together form an Autonomous System (AS). The ISPs have a central critical role in the functionality of the Internet, as they provide connection to the Internet backhaul to customer end-users. The power dynamic of this system inherently gives control over consumption patterns to the ISPs, as well as monitoring their users behaviour through traffic patterns. Consolidation of power at the hands of a few ISPs gives them the unique ability to control the flow of information in their AS territory, potentially enabling oppresive practices such as throttling, monitoring, censorship, and surveillance of their consumers. Insofar as authoritative regimes are established over a region, access to content can become severly restricted. Additionally, an imminent danger to the freedom of speech and freedom of access to information is the increasing trend of media corporations such as Meta and X to employ both explicit and implicit content moderation practices. Together, the aforementioned practices have in recent years led to a growing interest in decentralized peer-to-peer social networks and messaging platforms. Most notably, the rise of fully-decentralized networks like Mastodon, user-supported decentralized networks such as Bluesky, and end-to-end encrypted decentralized messaging platforms like Briar, Signal, and until recently Firechat, have proven that there is a growing shift in user interest patterns away from traditional Centralized Social Networks (CSNs) towards decentralized social networks of diverse approaches. Decentralized social networks can exist either as unstructured or structured peer-to-peer networks, as a democratic ability to run the entire software stack of a server individually (cf. Mastodon), or as a collection of transparent community-operated competing components belonging to the same social network, like in Bluesky. Structured peer-to-peer networks such as Chord, Kademlia, and the InterPlanetary File System (IPFS) use Distributed Hash Tables (DHTs) to store and retrieve content in a decentralized manner. On the other hand, unstructured peer-to-peer networks are more dynamic and do not use DHT to spread centralized information. Instead, unstructured peer-to-peer networks rely on flooding and gossip for content dissemination, like in Gnutella and BitTorrent. In this research paper, we focus on unstructured peer-to-peer networks, as they are more resilient to network topology changes, peers leaving and joining, and are more suitable for the dynamic nature and high churn of users in disaster-struck areas and refugee camps, as well as keeping more information decentralized and less prone to censorship.

2 Background

There is a growing architectural gap between the internet's general-purpose design and the individual implementation of ISPs in their ASes, and the increasing demand for specific functionalities (e.g. Multicast) makes it necessary to implement change when things break [1]. This is because the Internet was made with the concept of one-size-fits-all, allowing different Internet providers to implement different rules, policies, and techniques to efficitate their networks. The general-purpose design of the Internet also introduces the immutability of paths between pairs of nodes - once a path between two nodes exists, and the nodes can use it to reach each other, it is a complex process to get the nodes to communicate over new addresses, which happens when those nodes move. In the modern age nodes oftentimes exhibit movement patterns that may render their previous Internet connection point unusable, thereby forcing the nodes to search for a new attachment point - oftentimes switching from WiFi to cellular, between WiFi networks, or cellular to WiFi. In disaster zones, for example after earthquakes, fires, and other natural disasters, existing networking infrastructure is rendered useless due to destruction. In less-developed areas of the world, such infrastructure might not be available at all: the Laponia region near the Arctic Circle, homeland of the Sámi people, is characterized as a sparsely-populated region full of icy fjords, deep valleys, glaciers

and mountains. The inhabitants of this region have traditionally been reindeer-herders, and often migrate with the reindeer herds along the yearly cycle. Due to the harsh terrain, sparse level of population, and partial autonomy of the Sámi council, the Sámi people lack reliable cellular and internet infrastructure. To provide the Sámi people with modern communication options, the traditional packet-switching paradigm of communication as conceptualized by the Internet is not optimal. Instead, Lindgren et al. propose the the Store-Carry-Forward paradigm using Delay-Tolerant Networking (DTN) [2], where hosts store messages until an opportunity arises to forward them, carry them while moving until they reach a rendezvous with another node or a network attachment point, and then forward them upon contact. This paradigm enables the opportunistic usage of technologies such as Bluetooth to forward messages, which is ubiquitous to virtually all Smartphones and computers today. Insofar as the Internet is not available, DTNs using Store-Carry-Forward networking can be used as a fallback, being supplemented by traditional Internet infrastruture as it becomes available. This concept has been the guiding idea of this research paper, with the intent to investigate the reliability and performance of unstructured peer-to-peer networks and grassroots social networks built using the aforementioned paradigm.

3 Related Work

Decentralised administration is one of the basic enablers of the growth of the Internet as a whole, thanks to the autonomous

4 Setup

4.1 Hardware

Recent events (natural disasters, war, protests) have shown that people heavily rely on online social networks and instant messaging platforms to communicate and coordinate aid efforts during cases such as disaster relief, protests, or emergency response to natural disasters. The existing internet infrastructure is distributed, but its management and ownership is heavily centralized which places power in the hands of a few individuals or companies, that are susceptible to implicit and explicit censorship, while the infrastructure itself is prone to failure in cases of disaster, leaving reliant communities in the dark. In this paper, we propose performance statistics for both simulated as well as real-life unstructured peer-to-peer social networks, as well as investigate and propose resilience metrics for such opportunistic networks.

4.2 Software

Recent events (natural disasters, war, protests) have shown that people heavily rely on online social networks and instant messaging platforms to communicate and coordinate aid efforts during cases such as disaster relief, protests, or emergency response to natural disasters. The existing internet infrastructure is distributed, but its management and ownership is heavily centralized which places power in the hands of a few individuals or companies, that are susceptible to implicit and explicit censorship, while the infrastructure itself is prone to failure in cases of disaster, leaving reliant communities in the dark. In this paper, we propose performance statistics for both simulated as well as real-life unstructured peer-to-peer social networks, as well as investigate and propose resilience metrics for such opportunistic networks.

5 Methodology

Recent events (natural disasters, war, protests) have shown that people heavily rely on online social networks and instant messaging platforms to communicate and coordinate aid efforts during cases such as disaster relief, protests, or emergency response to natural disasters. The existing internet infrastructure is distributed, but its management and ownership is heavily centralized which places power in the hands of a few individuals or companies, that are susceptible to implicit and explicit censorship, while the infrastructure itself is prone to failure in cases of disaster, leaving reliant communities in the dark. In this paper, we propose performance statistics for both simulated as well as real-life unstructured peer-to-peer social networks, as well as investigate and propose resilience metrics for such opportunistic networks.

6 Results

Recent events (natural disasters, war, protests) have shown that people heavily rely on online social networks and instant messaging platforms to communicate and coordinate aid efforts during cases such as disaster relief, protests, or emergency response to natural disasters. The existing internet infrastructure is distributed, but its management and ownership is heavily centralized which places power in the hands of a few individuals or companies, that are susceptible to implicit and explicit censorship, while the infrastructure itself is prone to failure in cases of disaster, leaving reliant communities in the dark. In this paper, we propose performance statistics for both simulated as well as real-life unstructured peer-to-peer social networks, as well as investigate and propose resilience metrics for such opportunistic networks.

7 Analysis

Recent events (natural disasters, war, protests) have shown that people heavily rely on online social networks and instant messaging platforms to communicate and coordinate aid efforts during cases such as disaster relief, protests, or emergency response to natural disasters. The existing internet infrastructure is distributed, but its management and ownership is heavily centralized which places power in the hands of a few individuals or companies, that are susceptible to implicit and explicit censorship, while the infrastructure itself is prone to failure in cases of disaster, leaving reliant communities in the dark. In this paper, we propose performance statistics for both simulated as well as real-life unstructured peer-to-peer social networks, as well as investigate and propose resilience metrics for such opportunistic networks.

8 Discussion

Recent events (natural disasters, war, protests) have shown that people heavily rely on online social networks and instant messaging platforms to communicate and coordinate aid efforts during cases such as disaster relief, protests, or emergency response to natural disasters. The existing internet infrastructure is distributed, but its management and ownership is heavily centralized which places power in the hands of a few individuals or companies, that

are susceptible to implicit and explicit censorship, while the infrastructure itself is prone to failure in cases of disaster, leaving reliant communities in the dark. In this paper, we propose performance statistics for both simulated as well as real-life unstructured peer-to-peer social networks, as well as investigate and propose resilience metrics for such opportunistic networks.

References

[1] Mark Handley. 2006. Why the internet only just works. *BT Technology Journal* 24, 3 (2006), 119–129. doi:10.1007/s10550-006-0084-z

[2] Anders Lindgren and Avri Doria. 2007. Experiences from deploying a real-life DTN system. In *Proceedings of the Fourth IEEE Consumer Communications and Networking Conference*. IEEE, Las Vegas, Nevada, USA, 217–221. doi:10.1109/ccnc.2007.50