Ph.D. Thesis Proposal

SafEdge for Residential Networks

Privacy from the bottom-up

Aldo Cassola

College of Computer and Information Science

Northeastern University

Ph.D. Committee

Advisor Guevara Noubir

Alan Mislove

David Choffnes

Ext. member Omprakash Gnawali **University of Houston**

January 2nd, 2014

Abstract

The growth of mobile devices and computing has continued in recent years to the point where mobile network providers must not only upgrade their networks to serve the new traffic-intensive content that their users demand, but to actually turn to alternative methods of delivery, namely WiFi hotspots and femtocells. This demand is driven in part by the surge in streaming services, but also by the demand for ubiquitous access to data hosted in cloud services.

The increased connectivity has changed user expectations for access to their data. Cloud service providers have seen similar increases in their user bases as clients migrate from laptops and desktop computers to tablets and smartphones. The amounts of data and computation performed in cloud services has always been of interest to eavesdroppers, and their growth can only make it more valuable to them. In such a world, a growing dependency on centralized providers makes them single points of failures for privacy threats.

With residential broadband Internet becoming more commonplace, always-connected home devices can collaborate to build cloud services closer to the network edge to mitigate the threats, creating more diffuse targets of attack. In this work we propose to leverage these networks to provide improved privacy for network access control, and edge cloud storage with little to no administrative overhead to home network users. In particular our main aim is to provide IP location privacy, anonymous access control, and efficient network performance for residential edge services. We show our prototyping work implemented over our own testbed for residential devices that we will also use for implementation and evaluation, and describe the proposed work to solve the research problems emerging in this context.

Contents

1 Introduction

The mobile arena has seen trends of growth throughout recent years. Smartphone manufacturers push their products to accommodate growing demand for always-connected wireless devices. Mobile network operators upgrade their infrastructure to support the increasing amounts of traffic, and even offload some of such traffic to WiFi hotspots and femtocells. These trends in connectivity have driven the development of cloud services, making computing resources like storage and processing power a commodity. With them, mobile users can access data stored in the Cloud around the world, and can share it with ease, often at little to no cost.

As the reliance on cloud services deepens, so do security and privacy concerns. Wireless network access offers little privacy protection. Mobile networks allow the operator full access to handset traffic as well as location data. WiFi access control can be performed in plaintext with captive portals or through standard mechanisms over encrypted channels, but both strategies are susceptible to network impersonation, and always reveal the identity of the user to the authenticator. Cloud services, on the other hand have been known to tap into user-stored information to increase their revenue, and access to their offerings can leak information about user location or data access patterns to adversaries.

While growth in the user base can push cloud providers to protect entrusted data—most services encrypt traffic between the client and the service or even offer client-side encryption for data—the privacy landscape in wireless and cloud network access seems to take privacy as an afterthought.

1.1 Motivation

Figure 1: The rise of mobile devices and the demand for cloud services have changed the landscape of network access.

1.1.1 The State and Trends of Wireless Network Access

Users increasingly rely on mobile devices for network access. As smartphones keep up with the latest generations of mobile network systems and WiFi connectivity, people expect to be online at all times, especially in urban areas. The increase in user demand has prompted providers to manage their capacity by discontinuing unlimited data transfers and imposing caps on clients—enforced by additional service fees or reduced network performance. The growth in demand also prompts providers to upgrade their systems to faster and more efficient network protocols, and increasing channel usage per cell, forcing cell size to decrease. Today, subscribers can install small femtocell stations in their vicinity to improve their network performance. In

other cases, strategically placed WiFi hotspots serve mobile subscribers, effectively offloading cellular network capacity. But bringing base stations closer to subscribers is not easy, as this means significant investment on the provider's end.

WiFi network access for WiFi hotspots is normally managed over access points operating in Open Authentication mode, serving traffic in plaintext, and authenticating users over a captive portal running on over TLS. Other network access methods exist, such as WEP and WPA variants, that authenticate users with pre-shared keys or over the IEEE 802.1x standard. Using pre-shared keys for access control is most commonly seen in the realm of home networks, where members of the household have configured their devices with the common keys. The use of 802.1x for network access is generally limited to more savvy users or professional settings, as the complexity in setup, overheads of account management, and differences in client interoperability make it impractical outside this context.

1.1.2 Advent of Free Cloud Services

Offerings such as Amazon's EC2 make large CPU and GPU processing power available to anyone with an Internet connection and a credit card. Dropbox has penetrated not only the home—for which it offers free storage—but corporate culture with their always-available storage service, reaching over 200 million users [1,2]. Even Google and Microsoft have jumped in the bandwagon by offering web-versions of their office suites and storage [3,4] platforms for free, each with 120 and 250 million users respectively [5,6].

Elastic services have contributed to the cloud service landscape. By offering computing, network and storage as a commodity, where customers only pay for actual usage, has made convenient for cloud providers to host their customer's content on these these third parties. This allows cloud providers avoid large investments on specialized hardware, in-house maintenance. In addition it is easier for cloud providers to react to spikes in service demand flexibly.

1.1.3 Security and Privacy Concerns

The architecture of mobile networks produces data that can be used to deduce user location using a variety of techniques. While its use has normally occurred during law enforcement, public concern with regards to the technology however, has shifted do to recent revelation involving mass surveillance [7].

Cloud services often make use of established security techniques, protocols and algorithms to provide authentication, authorization, data transport confidentiality, and redundancy. Individual offerings however, typically only offer a subset of the services that make business sense to the provider. For instance, free services like the ones offered by Google typically do not encrypt stored user data while their network exchanges are protected. Gmail user messages, for instance, are known to be scanned in order to serve relevant ads to the user. Redundancy on the other hand, is normally under control of the same entity offering the service. Wuala, for instance offers client-side data encryption and redundancy, but only within its own network.

Generally IP address privacy is not considered in the design of cloud systems. Clients connect through browsers or specific mobile apps, which can and do reveal information about the user to the service provider. Location of a client can be approximated with only simple IP address database lookups, or client applications can report sensor data from the user's device back to their server. Using anonymizing techniques is often not enough to protect against the above when application level data or even DNS lookups can leak IP addresses to adversaries.

Mobile network providers, on the other hand, have tried in recent years to reduce their network load by switching to more ubiquitous and faster to deploy WiFi hotspots and femtocells. The growth of the mobile handset market has been the driver of such decisions, and its upward trend continues. The cellular space offers its own challenges in privacy, for users can be easily tracked using base station location information and identity is linked to a handset from the start. As things stand, the trend to offer open WiFi access points for subscribers only adds to the existing privacy risks.

Network providers such as AT&T and Comcast have in recent years deployed WiFi access points across urban areas to shift load away from their networks while bringing subscribers closer to ubiquitous Internet access. Access is normally controlled through captive web portals to the provider's network. The absence of lower layer authentication primitives results in clients broadcasting plain text traffic, impersonation, or even

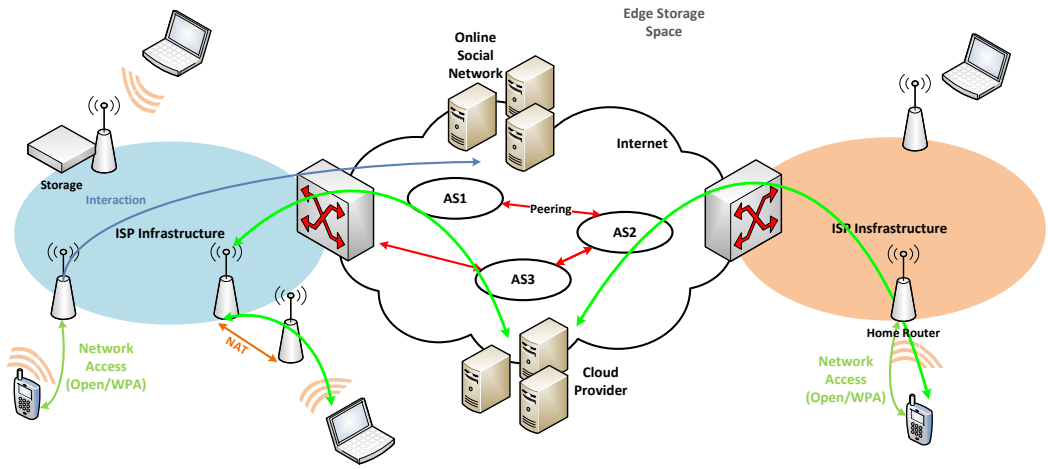


Figure 2: Network access and traffic for cloud services today does little to protect privacy.

risking connections to Evil Twins. New initiatives for hotspot secure access are being developed by the WiFi Alliance [8], which provides WPA-level protection to hotspot deployments in addition to handoff and roaming.

While technologies to counteract the risks in open WiFi networks like WPA-Personal and -Enterprise have been in use for some time, their utility is limited. WPA-Personal provides encryption keys to any client that knows the shared passphrase, making it impractical for environments where clients are added and revoked periodically. WPA-Enterprise allows user management to happen behind the scenes, as clients authenticate securely through 802.1x with a central server in the network behind the Access Point before access is allowed. However, flaws in User Interface design, outdated protocols like MSCHAP-v2, and Public Key certificate impersonation make current deployments of WPA-Enterprise vulnerable to Evil Twin attacks.

The dependency on elastic services, such as those offered by Amazon, also raises privacy concerns. If user content is hosted on third-party devices, what guarantees exist over the privacy of the content? As the trends move in this direction, it is apparent that mechanisms to protect hosted data are needed.

1.1.4 Tapping the Residential Space

As broadband access to residential areas becomes ubiquitous, the number of home Internet subscribers has kept its upward trend globally, and with it, the deployment of home routers with ever greater hardware capabilities. Such growing pool of inexpensive, always-connected devices has the potential for becoming the basis for the privacy-aware and distributed applications that we need today.

Just as in services like TOR or FON [9], where users band together for a common goal, we believe that tapping into the growing number of small residential devices to provide network access and services can provide similar gains in the privacy space. Ideally, mobile network coverage can be served by home WiFi devices whose owner has authorized use and may define payment amounts to himself without either mobile user or AP operator knowing their identities. The new class of edge cloud services would offer higher standards of protection and privacy without being tied to monolithic providers. Such services must be robust but also must operate within the constraints of limited and asymmetric network connections careful not to interfere with normal home usage. We cover our previous work on residential networks and the results of the **Open Infrastructure** testbed that confirm the feasibility of edge services on Section 2.

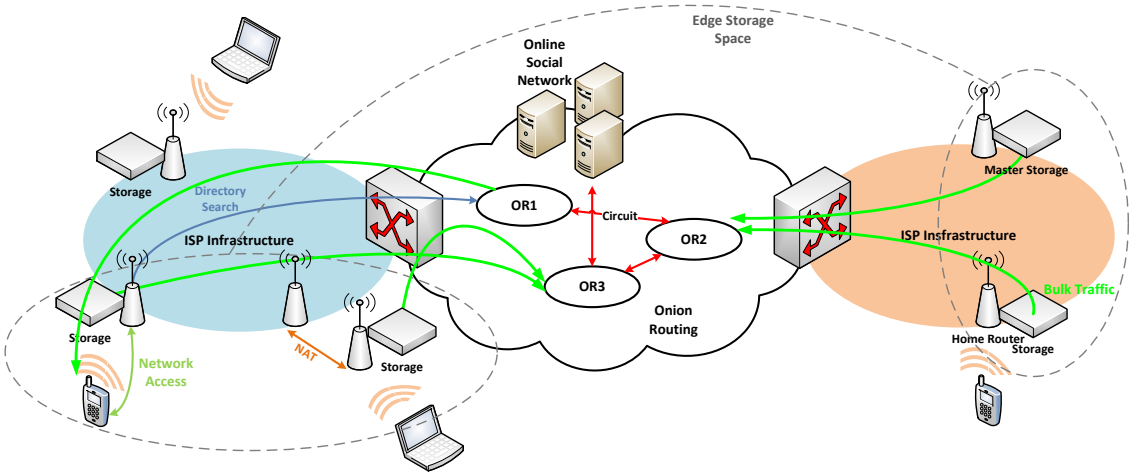


Figure 3: Using residential devices to push services to the edge allows for more robust privacy protection.

1.2 Focus of this Work

Leveraging large numbers of small residential sites to provide network services is a departure from the current privacy landscape of network and cloud access. For a privacy preserving system, infrastructure must be in place that allows usage of services with minimal leakage of user data. In the realm of network access wireless user may not want to reveal her identity to the owner of the access point, but he in turn may require payment or proof that she is authorized to access the network. Once connected, the user may request access to her documents in the cloud without revealing her identity to the provider, and protecting her data access patterns from potential eavesdroppers.

We address two aspects regarding privacy in the Edge Cloud: how to build a robust and easily-managed entry point, and implementing a well-behaved storage system. Because the potential number of services that can be offered by each component can be large, we focus in providing what we believe are a sufficient set of capabilities in each realm that can easily be generalized and extended. The following is the overview of services we aim to provide, and we define later in each section:

Identity Protection: Both clients and providers should not be able to deduce the identity of one another during operation. Needless to say, neither should potential eavesdroppers.

Traffic Data confidentiality No data should be disclosed to unauthorized parties.

Availability: For storage, data must be retrievable even in the presence of adversaries.

Impersonation protection: Clients should be able to detect provider impersonation attempts.

Minimal Invasiveness: No operations should disrupt the Access Point owner.

Ease of use: Minimal assumptions can be made on the technical capabilities of residential Access Point owners and network clients. Management overheads and administrations task must be minimal and have a flat learning curve.

Throughout this work we use simplicity as a driving principle in the design of the above services. Any use case and interaction with the system should have well-defined steps that leave the system in a consistent step, minimizing surprises. A Network Authentication method that prompts a user for a password repeatedly after the credentials had been stored can be exploited to trick the user into providing its sensitive data. In general there is evidence that the decisions taken during service and interface design have an impact in the

overall security of the systems. In the following sections we summarize both proposed frameworks, and discuss related work.

1.2.1 Residential Entry Points

Building cloud services on top of residential devices implies that residential users become service providers, and thus take on administrative roles. For instance, a user may need to decide who has access to the service he offers in her home device. This authentication/authorization problem has typically been handled by the use of secret passwords (such as Pre-Shared Key in WPA for sharing the wireless network resource) or by the use of authentication servers, as in WPA-Enterprise.

Creating a local database of users and maintaining it is a task well beyond what a non-technical user may be willing to perform to share a service. Doing so would entail a learning curve for the tools she would need to use to implement it, and the maintenance tasks that come with it are error prone. Compounding this problem to the number of potential residential users makes it clear that a naïve solution of keeping an account on every possible device is undesirable. Instead, the system should provide the capability for the owner to perform access control in the simplest manner possible, leveraging data and services that are already available.

Providing authorization and authentication for third-party services on the Internet is not a new technique. Through the use of OAuth, services like Groupon, Slideshare, and even news sites permit end-users to access protected content on their service without the need to access user credentials, often in exchange for access to the end users' social network posts and lists of friends. With the popularity of social networking sites like Facebook, their user base has made the site a global directory of billions open to be searched and crawled. Using social media services as authentication back-ends offers clear advantages over locally-maintained user tables: Setup and learning curve are virtually eliminated. Large bases of users are common in social media, and all the heavy-lifting is offloaded to the social media provider. Using a social networking site as a discovery mechanism for users seems a natural tool to use in providing authentication, the challenge is to protect user privacy and to avoid information leakage, given the issues in such networks. To do so, we design our services without placing any trust on the online-social network.

1.2.2 Storage in the Residential Cloud

By building a cloud storage service we seek to address the lack of privacy in current cloud storage offerings. The idea of distributed cloud storage is not new, as services like Wuala offered a variation of it in the past, but the goal of our work is to provide a similar system that minimizes user exposure to the service provider.

In addition, a distributed storage service can serve as a basis for Content Delivery Networks such as the ones used for video services, providing benefits to both end-users and ISPs. If data is accessible from within an ISP network users see less delay and throughput, and ISPs may see less traversal to external links to access content.

1.3 Related Work

1.3.1 Online Storage

Oblivious storage, originally coined as a technique for executable code protection from the CPU [10], has seen renewed popularity after the appearance of cloud storage services. While early schemes [11, 12] have been shown to have good asymptotic performance depending on the client storage requirements—$O(\log^2 N)$ cost with $O(1)$ client storage— empirical throughput is low (on the order of tens of Kilobytes per second). Modern work [13] can achieve hundreds of Kilobytes per second end-to-end but at the cost of tens Megabytes per second total.

Distributed Filesystems [14–21] present a filesystem abstraction view to sets of network connected storage devices. Clients view a distributed as if it were a locally mounted device, even though its servers, storage and clients are dispersed throughout the network. Filesystem design and performance vary widely, as do the guarantees in the stored data. While some filesystems may offer POSIX [22] file read and write guarantees, like Lustre [20], others may define their own semantics and optimize for a particular workload, such as the Google

Filesystem [16]. Despite their variety, distributed filesystems commonly make the assumption that network access to storage is done over high-throughput, low-latency links.

There has been effort to incorporate P2P schemes into the Cloud Storage environment. Bittorrent Inc's BTSync [23] is an experimental service that allows users to sync their files amongst their own computers with transport security. Authorization is controlled by the generation of keys, which must be shared to the devices the user wishes to keep synchronized. All transfers are performed directly and encrypted between the client's devices, with relay servers only acting to set up the flows. The service uses the UDP implementation of the Bittorrent protocol, μTP, that maximizes throughput while minimizing latency. The client software is available on a variety of operating systems for computers and mobile devices

Interest building cloud systems from groups of end-user machines has garnered some interest in recent time. WebCloud by Zhou et at. [24] proposes a system built on top of Online Social Networks that allows social-network subscribers host and distribute content from their web browsers to others in the network. Maygh by Zhang et al. [25] in turn builds on the idea and proposes a Content Delivery Network where content is served from end-user browsers, reducing traffic from static content at the original website.

1.3.2 Privacy in Network Access

Radio navigation systems form the base for handset location tracking in mobile network systems. Differences in signal time of arrival and phase offset measured from multiple known base stations have long been used to obtain cell phone location within a cell even before GPS hardware was common in mobile devices. As users move through a mobile network, a user location and habit database can be built over the long term, something that can be useful in law-enforcement scenarios.

The use of onion routing as an anonymity technique spans several decades [26], but it reached mainstream popularity with the appearance of the TOR Project [27, 28], an open-source onion routing implementation originally devised as a tool for U.S. government communications. After its release it has been used by a wide variety of people, including journalists, law enforcement, activists and end-users wishing to circumvent limitations on their privacy. TOR has sparked academic interest since its inception, and a growing body of literature studies various aspects of the TOR network including its performance, privacy protection, adversarial attacks, and improvements [29–44]. The TOR distribution package is constantly updated, and it includes a modified version of Firefox, a graphical configuration tool for setup, and a framework pluggable transports to hide TOR traffic from censors. Hardware manufacturers have also started to integrate TOR in their offerings. Pogoplug's SafePlug [45] is marketed towards end-users that wish extra protection for their networks. The device routes TCP traffic to the TOR network transparently by redirecting outbound packets to the local instance of the onion and anonymizing proxies. While this solution is easy and convenient, it does not protect against information leakage for all protocols.

WiFi networks have long been the subject of Evil Twin attacks, where rogue Access Points controlled by an attacker are placed within range of unsuspecting users, and pose as legitimate devices in an attempt to capture user traffic. A growing body of research has dealt with these types of attacks with techniques like mechanisms of trust-on-first-use [46–48], or device fingerprinting [49]. However, more sophisticated multi-layered attacks that rely on targetted jamming and weaknesses on authentication protocols and public cryptography trust mechanisms can defeat these kinds of defenses easily [50]. Mechanisms that avoid weak authentication protocols and use the structure of a Social Network to simulate a user directory [51] can protect against these kinds of attacks and provide security to the link-layer. Recently, even Facebook has recognized the the need for cleaner WiFi auth, and is working on an implementation [52].

Study of group signatures spans several decades starting with [53]. Other group signature schemes and more refined definitions and analysis of the primitives have been described in the literature over the years [54–63]. In group signature schemes, members of a group can each produce signature of a message in such a way that does not reveal which group member's key was used. Group signature has been used in industry to authenticate devices while not revealing the owners identity in Direct Anonymous Attestation by the Trusted Computing Group [64].

(a) (b)

Figure 4: Open Infrastructure testbed devices: Buffalo WZR-HP-G300NH (a) 3.5" hard drive , (b)16GB USB Flash.

1.3.3 Bandwidth Control

The goal of bandwidth control is to manage a limited outgoing network link in a manner that allows reasonable performance for all streams attempting to access the resource. In general, several queuing mechanisms are available to manage the link in IP networks, each with its own goals and parameters. This approach is useful when the routing device has complete knowledge of the packets waiting to be transmitted to the link. For instance, the Linux kernel provides a long list of QoS strategies including Hierarchical Token Bucket, pFIFO Fast, CTB, SFQ, etc, and the `tc` tool manages the queuing structure and filtering strategy for outgoing packets.

When knowledge about the capacity of a path is incomplete, estimation is the approach of choice. By probing the path being examined and measuring the properties of the traffic when arriving at the destination, an approximate value of the tight link can be obtained [65–67].

1.4 Proposal Overview

This work aims to design a network access control strategy and edge cloud storage system for residential network devices, in such a way as to protect from identity leaks to other actors in the system or to eavesdroppers. Our goals include implementing both over a real-world testbed on actual residential scenarios. To this end, we describe our testbed, our proposed work and our preliminary results in the sections below.

The rest of this document is organized as follows. Section 2 discusses the **Open Infrastructure** testbed, the residential deployment where we will implement our work. The plan for improved WiFi Access services are discussed in Section 3. Implementation of edge cloud services is addressed in Section 4. The proposed research plan is outlined in Section 5.

2 The Open Infrastructure Testbed

The **Open Infrastructure** testbed is a set of hardware and management tools designed to host new applications and experimental projects on a multitude of residential-grade WiFi Access Points (APs). The testbed's hardware deployment is comprised of off-the-shelf APs running customized firmware, network monitoring

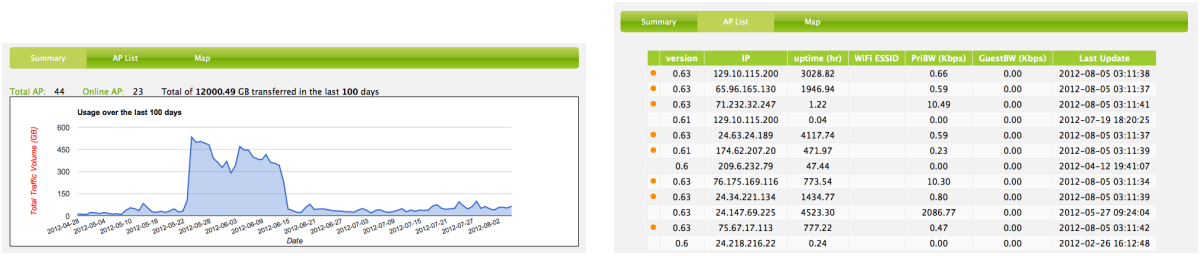


Figure 5: Web-Based Open Infrastructure AP Management Portal

and administration tools, and experiment managment scripts. We first give an account of the testbed itself, its deployment and scale, followed by our preliminary results obtained from it.

2.1 Testbed Hardware, Software, and Scope

The devices in our deployment are Buffalo WZR-HP-G300NH [68] routers with 400MHz Atheros CPU, 64MB RAM, 32MB Flash, five 1Gbit ethernet ports, one USB port, and Atheros AR9132/AR9103 WiFi Network Processor. Every device deployed has access to either a 16GB USB Flash or a 250GB hard disk, as shown in Figure 4. The devices run a modified version of the **OpenWrt** embedded Linux distribution [69] that includes a suit of management and experimental tools which we will describe below. **OpenWrt** supports a large hardware base with 27 architectures available, and over 100 well-supported router models [70].

We have deployed 30 customized APs in urban areas in Boston and Houston, serving around 100 individual users since February 2011. Our user base is comprised of mainly graduate students and young professionals between 20 and 40 years of age, and of diverse backgrounds. We have plans of expanding the scale of our testbed to 150 nodes in the next year.

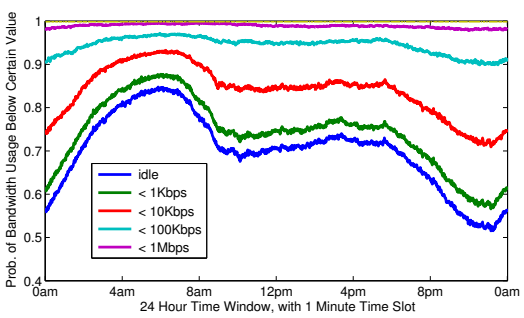
We monitor network usage through a custom heartbeat client program that aggregates data about the number of associated devices, average bandwidth grouped over different traffic types, or any configurable custom measurement. The data is aggregated over 10 second intervals and then sent over the network to our heartbeat server. All the reports are stored in our back-end MySQL server for further processing. Since the start of our deployment, we have obtained over 113 million records of data. In addition, the firmware includes a suite of SSH-based remote management tools to support remote firmware upgrades, update the AP configurations, schedule experiment tasks, etc. In order not to disturb our test users' normal network usage, any and all data stored is scheduled for upload over off-peak hours such as midnight on weekdays.

We have also developed a web-based Testbed Management Portal as a frontend for administration purposes. See Figure 5 for screenshots.

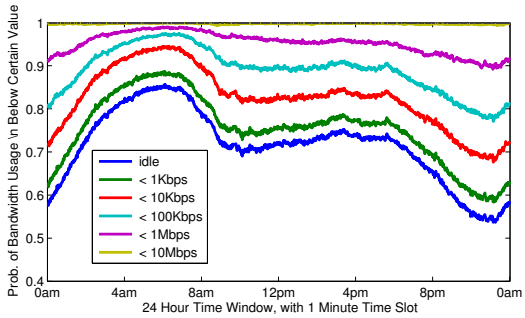
The testbed was built to provide first-hand information of urban WiFi and residential network usage patterns over extended periods of time. Because urban homes network usage differs from other network deployments, like in academic and enterprise contexts, the **Open Infrastructure** testbed provides us with real-world data that is more granular in nature than deployments spanning ISP network segments. It also provides the flexibility to measure network characteristics from the edge of several network providers, and to potentially expand monitoring over diverse geographic areas.

2.2 Preliminary Results

Feasibility in crowdsourcing network access and edge storage services is directly related to the amount of backhaul capacity each device can contribute. To understand residential bandwidth usage, we observed network usage reported by the testbed between February 2011 and May 2012. For every 1m time window in a week we calculate the probability that a traffic sample falls within a given throughput range. Figures 6a and 6b depict the results. From the results we can readily see clear differentiation between peak and non-peak

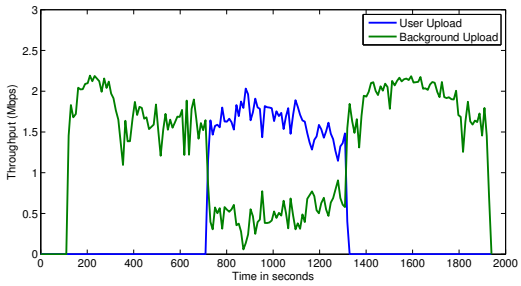


(a) Uplink usage PDF

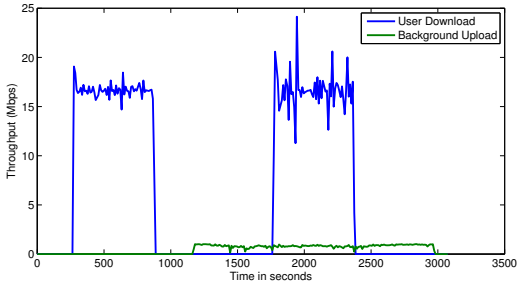


(b) Downlink usage PDF

Figure 6



(a) Uplink behavior under saturated uplink



(b) Downlink behavior under saturated uplink

Figure 7

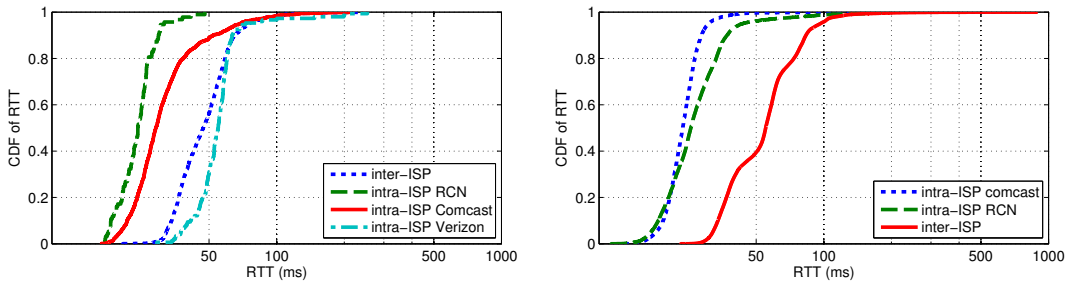
usage, and that the backhaul is mostly underutilized even during peak times for both up- and downlink . For instance note that during peak hours the probability that traffic is less than 10Kbps is greater than 65%.

We also find devices are capable of sustaining saturated uplinks without affecting the traffic of the owner, provided a sensible traffic control policy is in place. We set up deployed devices to initiate uplink UDP traffic simulating high background usage from the edge cloud. After a few seconds, a new UDP uplink transfer is started simulating traffic from the owner, such that both transfers compete for the backhaul. We then repeated a saturated uplink vs. owner upload (see Figures 7a, and 7b for typical result on 2Mbps-uplink provisioned links.)

To gain some insight into the density of home wireless access points we ran a set of wardriving experiments over four different neighborhoods in Metropolitan Boston. We collected ESSID, BSSID, GPS location, signal strength, encryption capabilities, etc of over 26 thousand urban WiFi access points. In average we observed 17 access points within range on every scan operation. After associating with an access points, we collected its signal strength. On average, successful associations see -81dBm signal power, with 8 access points having power greater than this amount.

We examine the interconnectivity between devices through round-trip time (RTT) measurements among deployed devices, and through RTT measurements during wardriving. Figure 8 summarizes our findings. Our results show that latency between network subscribers of the same provider fall between 20 and 50ms at city level, which is enough to reach the provider's uplink limit.

The density of residential networks, unused backhaul, low RTTs, and high sustainable throughput support the feasibility for coordinated residential edge devices to provide network access and well-behaved edge storage.



(a) Latency measurement, wardriving

(b) Latency measurement, **Open Infrastructure**

Figure 8

3 SafEdge Wireless Access

Protection on the wireless link layer constitutes the first line of protection against eavesdropping and impersonation. Current trends and issues in user privacy motivate us to propose improvements to WiFi access control. This section is organized as follows: we give a summary of the current issues in wireless access systems today, and our preliminary work in Section 3.1. Sections 3.2, 3.3, and 3.4 describe the proposed work.

3.1 The State of Wireless Access Control

As network demand keeps its upward trends, mobile network operators try to offload traffic on their networks whenever possible. Several mechanisms for wireless LAN offload have been proposed in the standards [71,72], and providers have implemented WiFi offload in recent years. 3G and 4G mobile networking standards also contemplate data protection mechanisms for air transmissions and end-to-end communication [73,74].

The governing standard in WiFi [75] includes mechanisms for authentication, data confidentiality and integrity. One of these mechanisms, colloquially referred to as WPA-Enterprise is the de-facto standard for medium to large network deployments requiring user authentication, and is based on the Extensible Authentication Protocol framework (EAP) defined in [76]. Even though standard WiFi security techniques are routinely applied to home devices and business deployments, mobile operators who provide WiFi hotspots do not normally implement them. Mobile users who wish to use WiFi hotspots provided by their network operator commonly interact with captive portals over an SSL-enabled website and unencrypted link layer to authenticate to the network.

While the current traffic protection standards have held up better than the previous work [77], they are still vulnerable to certain types of attacks that exploit small multi-layer flaws in the implementations. With the introduction of attacks that leverage the lack of a trust relationship between a WiFi SSID and the security certificate presented to clients [50], the need for a mechanism to provide a better WiFi access control framework becomes apparent. In particular, we propose to provide:

- Low-overhead Discovery Mechanism
- Privacy-preserving authentication
- Geographic untraceability
- Fine-grained Access Control

3.2 Goals and Services

In this work we present a flexible authorization framework for distributed services. We examine the minimal information necessary to perform authentication for the parties both in the context of the framework and of the implementation, and give a detailed account on its workings.

3.2.1 WiFi Privacy-preserving Authentication

The process of authentication usually entails establishing the identity of a client and search on an authorization matrix to determine the services the user is allowed to access. Conversely, anonymous services protect the identity of users, but offer limited authorization capabilities.

We propose the use of a privacy-preserving authentication method that does not reveal client or AP owner identity in the context of residential network access. The challenge is to create a method that protects from impersonation without identity leaks over the limited capabilities of residential network devices.

Several cryptographic schemes can be used as building blocks for anonymous authentication. With group signature schemes [56], a set of users belonging to a group can sign messages and can convince a verifier that the signature was created by a member of the group without revealing its identity. Group signatures may include the notion of a group manager capable of deanonymizing a signature if necessary. Ring signatures [78], a simpler scheme do not require a manager and forego several registration an setup procedures associated with group signatures. Both of these schemes require signatures linear of size linear in the number of member of the anonymity set.

Private Information Retrieval (PIR) [79] allows a client to retrieve bits from a database in a way that does not reveal the queried bits. A trivial PIR has the client transfer the entire database to its local storage, which then queries the database himself. However, PIR schemes exists with worst-case communication complexity $O(n^c)$ for $0 < c < 1$. A simple anonymous authentication scheme using PIR would work as follows: The AP uses key K to allow authentication to the set of users $S = \{U_1, U_2, \ldots, U_n\}$, and has access to a database of n entries $E_{Pub_{U_1}}(K)$. If a discovery mechanism (discussed in section3.2.2) exists that allows verification of identities and Public Keys, a user can request identity by sending a PIR request for the entry associated with its public key in the database. The server's reply returns the value to the user, along with a hash of K, to force the AP to commit to a value of K for all its users. Once the user decrypts K, both client and AP can perform mutual authentication.

3.2.2 Low-overhead Discovery Mechanism

Maintenance and security of user databases is a delicate and critical component in authentication systems. Administrative overhead includes taking backups, keeping it updated as users appear and leave the system. We make no assumptions on the technical capability of a residential device owner to perform these tasks, so we aim to leverage publicly available data to build a discovery mechanism.

We can use publicly available information stored in online social networks to build a discovery mechanism for users. AP owners and users may search and contact each other to agree on service provision. Clearly, an incentive mechanism for owners to share their backhaul may be needed. Designing one is out of the scope of this work, but we allow for our design to be extended to include one. A design considering monetary payment would keep user keys valid as long as service is paid. For instance, a user may have an hourly rate which he pays for when connecting at its keys remain valid for that time. Other users may prepay to have weekly or monthly access.

3.3 Architecture

3.3.1 Components

1. Home routers connected to Internet.
2. An authorization set. We define an authorization set as a group of user identifiers, and the authorization object for the identity. For instance, the /etc/passwd and /etc/shadow files on UNIX-like systems can be considered an authorization set.
3. Router owners and clients belonging to some authorization sets.
4. A service which the given home router protects. For instance, access to the residential backhaul, or to an edge cloud service (see Section 4.)
5. Client 802.1x supplicant.

6. RADIUS server.
7. WiFi Access Point Software.

3.3.2 Authentication Process

On a high level, the authentication framework operates as follows

1. Both Alice (the client) and Bob (the AP owner) commit to a security token stored on the authorization set of the other. We call this **R**egistration.
2. Alice initiates, challenging Bob to prove its membership to her authorization set.
3. Alice requests access to the service provided by Bob's router.
4. Bob challenges Alice to prove her membership to his authorization space. If required, perform exchange of currency for service as agreed.
5. Bob computes the authorization matrix for Alice and grants or denies access to the network.

3.4 Implementation and Preliminary Work

To close the gap between the TLS certificate and the host network we designed **SNEAP** [51], a flexible authentication framework that relies on the protection inherent in web browser's SSL implementation and the OAuth framework for websites.

The key insight behind **SNEAP** is the leveraging of the SSL configuration in the user's browser to establish the identity of the authenticator. Figure 9 gives an overview of **SNEAP**'s architecture and operation.

We implemented our **SNEAP** prototype under windows and Linux clients, and **Open Infrastructure** router devices running our modified supplicants and RADIUS servers, respectively. Our implementation uses Facebook as the authentication backend, but the framework can be easily extended to any other oAuth-type system. The system is an EAP (802.1x) extension for WPA supplicants, RADIUS and authenticator can prevent the Evil Twin attacks by linking the identity of the authenticating party (Facebook in our implementation) with the specific network the user tries to use. Figure 9 summarizes **SNEAP**'s architecture and operation.

SNEAP itself does not provide for anonymous authentication however, and in fact the social network identities of the access point owner and client are revealed in order to find a relationship between the two. Additionally, the very use of an online social network, seems to counter our need for a privacy-aware network access service. We propose to refine of the framework, keeping the protections of the first design, and use an improvement over the PIR scheme described in Section 3.2.1 that can protect against Sybill AP owners and evaluate its performance.

3.5 Evaluation

PIR schemes require both the database server and client to perform a series of computations to perform a query and to extract the queried value, respectively. We will examine current AP and client capabilities in performing our scheme. In addition to performance vs Database size, user load, and comparison against current WPA schemes, we will also examine whether service of ongoing transfers to the home are affected by load.

4 SafEdge Residential Storage

To reduce the dependency on centralized storage systems, the edge cloud leverages the aggregate power of smaller always-on devices. Every individual device must be capable of not only serving content efficiently, and preserving privacy, but also with minimal impact to the normal residential traffic.

Building privacy into a system is not a straightforward procedure. For instance, naïve solutions to privacy in storage would add a confidentiality layer in the form of client encryption and anonymization through the use of onion routing to communicate with the cloud provider (e.g. Dropbox + EncFS + TOR, or https:// + TOR). Such solutions do not address leakage of information to the provider inside the encryption layer. Because the

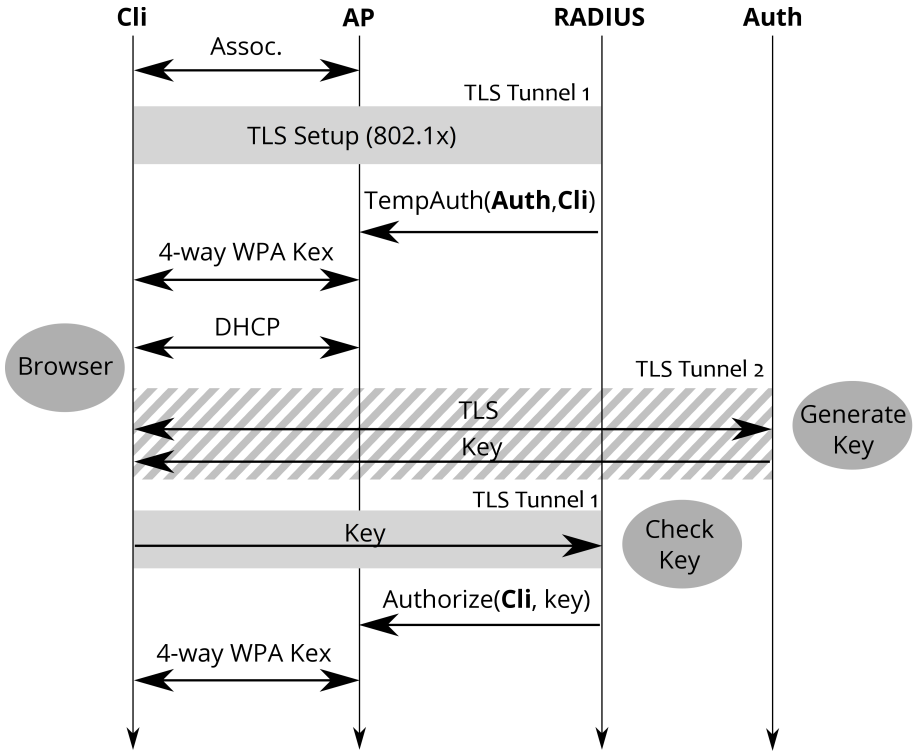


Figure 9: SNEAP overview

identity can revealed to the provider by the client software–it may include IP address or location information in the process—a tighter set of privacy guarantees need to exists to protect privacy. In addition TOR performance, although increasing over time, is limited by the number of participating nodes and available node bandwidth, adding difficulty to the design of a good performance solution.

4.1 Goals and Services

4.1.1 Content Protection

Data Confidentiality Content stored in third party storage providers must not be accessible to others than the data owner or parties authorized by him.

Data Availability Once content has been committed to storage, it should be retrievable. We consider the case of storage providers becoming adversaries after data has been committed to their space (e.g. the provider holding data hostage, forcing payment not previously agreed to, modifying the data, cheating by removing data).

Access Pattern Protection Even encrypted data can be subject to information leakage. An adversary noticing that region of the data is accessed more frequently than others may imply it is more valuable to owner. Oblivious storage techniques exist to solve this problem and their performance is evolving, but we consider it out of the scope of this work. Current best techniques [80] involve expensive mixing procedures requiring much more power than what we assume is available on residential devices. We cannot however dismiss the importance of having a system that protects access patterns, so we choose to modularize the storage strategy so **SafEdge** can be extended as better privacy mechanisms are developed.

4.1.2 Untraceability

We define traceability as the capacity of deducing either geographic location or identity of a data owner or storage provider after data exchange has occurred. While anonymity overlay networks like TOR [27] can help protect against the former, the latter depends on the application itself. To be able to provide access control without revealing the identity of either storage provider or data owner to themselves or a third party is a challenge.

4.1.3 Convenience

Ubiquity The current state and popularity of cloud storage services allow users to access and share their files no matter the network or devices used. **SafEdge** should provide at least as good access as current technologies, but because its capacity is directly related to the number of participants, special care must be taken to make it as user-friendly as possible.

High throughput, low impact traffic While we aim to provide fast transfers, we are faced with limitation of the residential uplink. A user willing to offer storage to others will be deterred from doing so if she notices participating impacts her normal browsing of video streaming.

Low overhead No additional administration tasks should be necessary from the data owner or storage provider further than what is normally required in other non-edge, centralized systems.

Incentive mechanisms User participation hinges on the perceived value of signing up to the system. Value does not need to be purely monetary; participation in FON [9] provides user the right to use other member's devices for network access. Monetary compensation may still be possible through decentralized monetary systems like Bitcoin [81], but its lack of true anonymity would mean a redesign that is out of the scope of this project.

4.2 Architecture

4.2.1 Components

Data owner A user that wishes to replicate a set of his files to **SafEdge** is called the data owner. The list of directories accessible remotely is called the **Shared Space**.

Authorized user is a user that has read or write access to a shared space. The data owner is the first authorized user of a shared space and can add other authorized users.

Client Software A device running an instance of the Client Software can present a view of the shared space to the owner or an authorized user. In particular, we assume the client software builds a copy of the Master locally, to be synced if required.

Storage Provider Software An individual willing to provide storage for data owners can become a storage provider by running this. A storage provider serves filesystem requests from client software. A data owner can recruit several storage providers for its space and may provide compensation to the providers.

Master Copy We assume at least a single copy of the original set of the owner's set of files is accessible at all times. The location of the Master Copy is called the **Home**. The Master Copy is the first storage provider and it coordinates operations amongst all other providers. The contents of the Master Copy may be encrypted, but this is not required, as we assume the user trusts her devices completely.

Storage Device A persistent-storage component such as flash, hard disk drive or tape that contains the actual stored bits.

4.2.2 Operation

1. Alice, the data owner, starts adds a directory D of her choosing to the shared space. The D is now the Master Copy of her space, and Alice is her own storage provider. She may access the master copy from anywhere with the client software. Even though Alice trusts her Master Copy completely, some degree of

identity protection is used to ensure third parties handling the traffic do not link Alice's current location with the Master Copy.

2. Alice may recruit new storage devices to serve her space. Alice can assign some level of trust to the newly recruited device. For instance, she may set her office computer or her family's device to serve data. She may be willing to trust some devices more than others, so devices shared by third-parties online can be assigned a lower trust, activating more stringent untraceability or data encryption. An service agreement between the parties (e.g. space for network access) can be offered and agreed to.
3. A client software fetch data request can be served by more than one storage providers. A client can aggregate data incoming from many links simultaneously to improve throughput. Write requests are sent to the Master Copy, and later disseminated to the rest of devices. It is the Master Copy which coordinates which providers serve a request.
4. The Master Copy checks the enlisted storage providers for the presence and correctness of the data. If a previously agreement is violated, future compensation is forfeit. Likewise, storage providers can check whether a subscriber fulfills their part and react accordingly.
5. Storage providers authenticate incoming requests, denying those from unauthorized users. Likewise, clients and Master Copy authenticate storage providers to make sure they are talking to the right one.

Typical residential broadband plans are asymmetric, with uplink being several times narrower than downlink. We contemplate two deployment scenarios:

1. A storage provider/Master Copy sits at the last mile and can determine when to back off on congestion.
2. A storage provider/Master Copy has no access to the last mile directly, and connects through a second device outside of its control. We propose a modified Available-Bandwidth detector to manage uplink traffic.

4.3 Implementation

The evidence presented in Section 2.2 supports the case for a crowdsourced edge cloud system. By leveraging the growing number of home broadband subscribers we can aggregate throughput if we achieve a critical mass. However, because uplink throughput is limited in residential networks, bandwidth must be carefully managed to not disturb network access. Our experience in the deployment of **Open Infrastructure** showed us that our users are sensitive to throughput variance and intrusive network patterns. We believe perceived performance issues alone may hinder the adoption of **SafEdge**, so special care must be taken to have a well-behaved system.

Home broadband connections are typically given a single IP address by the ISP. This address normally limited to a single device, a user device or the ISP's, depending on the provider's policies. In order to multiplex many devices to the link, users typically place a NAT routers between their devices and the ISP and configure each device to use the router. We contemplate two usage scenarios for **SafEdge**:

1. If installed on NAT router, a suitable traffic control policy, as the one tested in Section 2.2 is enough to minimize interference between the storage traffic and the user network. All storage traffic can be placed on a low priority queue that will use all available bandwidth if available, but it will immediately back off to any traffic coming from behind the address translation—i.e. the home traffic.
2. If installed as an additional device behind the NAT-router, no direct knowledge on the use of the uplink exists, and a different strategy for traffic control must be used. In particular, we must infer the available bandwidth remaining on the uplink.

Previous work on available bandwidth problem [67] focuses on finding the minimum capacity link in a path and estimating its value in a time frame of seconds to minutes. However, we believe user experience expectations, change as their connections' speed evolve, and decreasing estimates for user thresholds of delay acceptability [82] support this conclusion.

We examine the residential uplink behavior over varying loads by setting up the following test. Test host A behind a given **Open Infrastructure** node without any traffic control policy probes a well-provisioned server with large UDP-packets 1-second apart. Test host B, which shares uplink with host A generates uplink traffic, increasing monotonically over 20 second intervals to a different host. We choose this value to provide a

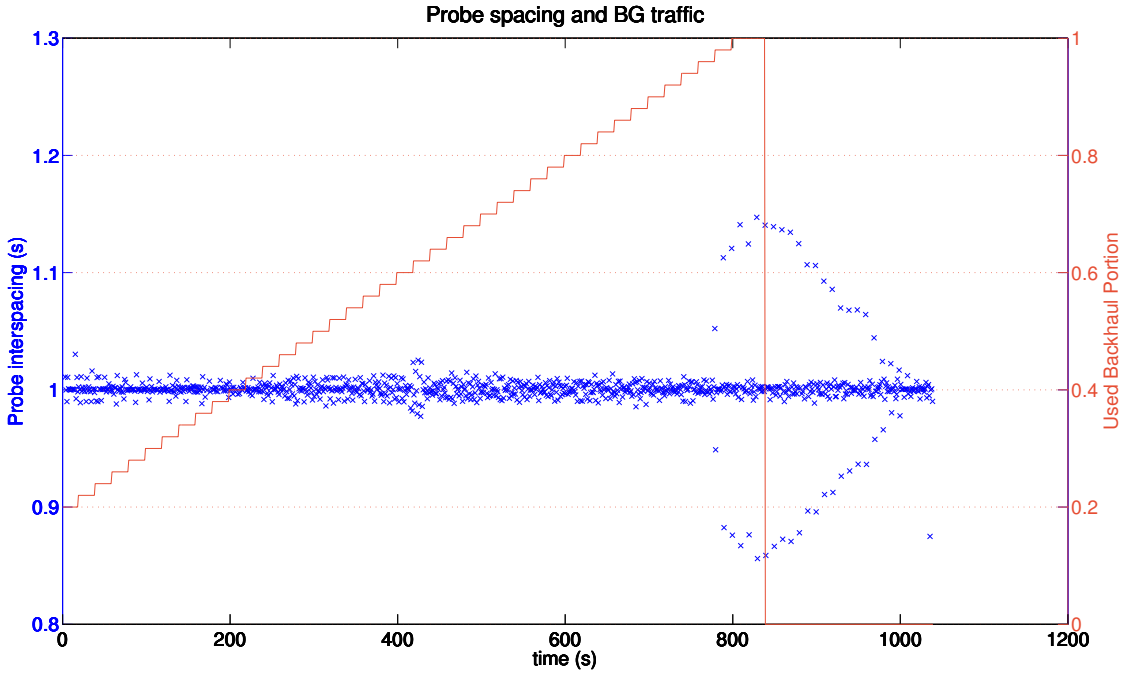


Figure 10: Typical probe interspacing over increasingly loaded uplink.

relatively long term view of the link and to bypass any possible high-burst provisioning by the ISP. Probes are maximum size UDP packets, which will be fragmented by the routing hosts on their way to the destination. The intention is two-fold: to provide a fast baseline from the fragment spacing, and to detect packet losses quickly at the probe receiver, as lost fragments result in total packet loss. Figure 10 shows the change in packet spacing observed at the probe receiver. The increased variance happens just as the traffic-generating host saturates the uplink. Fragment spacing remained constant and on the order of 1ms or less.

4.4 Evaluation

To evaluate our system, we will examine congestion control performance in each of the two possible deployment scenarios. In addition, we will measure the effect of data upload on background traffic under high load.

To characterize the edge cloud system performance, we will look at end-to-end data transfer rates as function number of users, filesystem and file sizes. As file data is stored across storage providers, we will also look at required bandwidth and performance at this end.

5 Schedule

The following table is the proposed timeline to complete the research:

To-do tasks	Completion Date (end of)
Anonymous Wi-Fi Authentication Design and Implementation	Feb 2014
Storage, Throughput Aggregation Design	March 2014
Storage and Throughput Control Impl.	April 2014
Performance Evaluation	May 2014
Dissertation Defense	June 2014

References

[1] Josh Constine. Dropbox Hits 200M Users, Unveils New "For Business" Client Combining Work And Personal Files. http://techcrunch.com/2013/11/13/dropbox-hits-200-million-users-and-announces-new-products-for-businesses/, November 2013.

[2] Dropbox Inc. Dropbox. https://www.dropbox.com, December 2013.

[3] Google. Google Drive. https://drive.google.com.

[4] Microsoft. Skydrive. skydrive.live.com, December 2013.

[5] Liz Gannes. With 120M Users, Google Drive Gets Tighter Integration With Gmail. http://allthingsd.com/20131112/with-120m-users-google-drive-gets-tighter-integration-with-gmail/, November 2013.

[6] John Callaham. Microsoft: 250 million people are now using SkyDrive. http://www.neowin.net/news/microsoft-250-million-people-are-now-using-skydrive, May 2013.

[7] Barton Gellman and Ashkan Soltani. NSA tracking cellphone locations worldwide, Snowden documents show. *The Washington Post*, December 2013.

[8] WiFi Alliance. Wi-Fi CERTIFIED Passpoint. http://www.wi-fi.org/sites/default/files/downloads-registered/wp_20120619_Wi-Fi_CERTIFIED_Passpoint.pdf, June 2012.

[9] Fon Wireless Ltd. FON. http://www.fon.com.

[10] Oded Goldreich and Rafail Ostrovsky. Software Protection and Simulation on Oblivious RAMs. *J. ACM*, 43(3):431–473, 1996.

[11] Michael T. Goodrich, Michael Mitzenmacher, Olga Ohrimenko, and Roberto Tamassia. Practical oblivious storage. In *Proceedings of the second ACM conference on Data and Application Security and Privacy*, CODASPY '12, pages 13–24, New York, NY, USA, 2012. ACM.

[12] Benny Pinkas and Tzachy Reinman. Oblivious RAM Revisited. *IACR Cryptology ePrint Archive*, 2010:366, 2010.

[13] Emil Stefanov and Elaine Shi. ObliviStore: High Performance Oblivious Cloud Storage. In *IEEE Symposium on Security and Privacy*, pages 253–267. IEEE Computer Society, 2013.

[14] Sage A. Weil, Scott A. Brandt, Ethan L. Miller, Darrell D. E. Long, and Carlos Maltzahn. Ceph: a scalable, high-performance distributed file system. In *Proceedings of the 7th symposium on Operating systems design and implementation*, OSDI '06, pages 307–320, Berkeley, CA, USA, 2006. USENIX Association.

[15] Dominik Grolimund, Luzius Meisser, Stefan Schmid, and Rogert Wattenhofer. Cryptree: A Folder Tree Structure for Cryptographic File Systems. In *Proceedings of the 25th IEEE Symposium on Reliable Distributed Systems*, SRDS '06, pages 189–198, Washington, DC, USA, 2006. IEEE Computer Society.

[16] Sanjay Ghemawat, Howard Gobioff, and Shun-Tak Leung. The Google file system. In *Proceedings of the nineteenth ACM symposium on Operating systems principles*, SOSP '03, pages 29–43, New York, NY, USA, 2003. ACM.

[17] Paolo Gasti, Giuseppe Ateniese, and Marina Blanton. Deniable cloud storage: sharing files via public-key deniability. In *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, WPES '10, pages 31–42, New York, NY, USA, 2010. ACM.

[18] Sean Rhea, Patrick Eaton, Dennis Geels, Hakim Weatherspoon, Ben Zhao, and John Kubiatowicz. Awarded Best Student Paper! - Pond: The OceanStore Prototype. In *Proceedings of the 2nd USENIX Conference on File and Storage Technologies*, FAST '03, pages 1–14, Berkeley, CA, USA, 2003. USENIX Association.

[19] John Kubiatowicz, David Bindel, Yan Chen, Steven Czerwinski, Patrick Eaton, Dennis Geels, Ramakrishan Gummadi, Sean Rhea, Hakim Weatherspoon, Westley Weimer, Chris Wells, and Ben Zhao. OceanStore: an architecture for global-scale persistent storage. *SIGPLAN Not.*, 35(11):190–201, 2000.

[20] Petros Koutoupis. The Lustre Distributed Filesystem. *Linux J.*, 2011(210), October 2011.

[21] D. Borthakur. The hadoop distributed file system: Architecture and design. *Hadoop Project Website*, 2007.

[22] IEEE Standard for Information Technology- Portable Operating System Interface (POSIX) Base Specifications, Issue 7. *IEEE Std 1003.1-2008 (Revision of IEEE Std 1003.1-2004)*, pages c1–3826, 2008.

[23] Bittorrent Inc. BTSync. `http://www.bittorrent.com/sync`.

[24] Fangfei Zhou, Liang Zhang, E. Franco, A. Mislove, R. Revis, and R. Sundaram. WebCloud: Recruiting Social Network Users to Assist in Content Distribution. In *Network Computing and Applications (NCA), 2012 11th IEEE International Symposium on*, pages 10–19, 2012.

[25] Liang Zhang, Fangfei Zhou, Alan Mislove, and Ravi Sundaram. Maygh: Building a CDN from Client Web Browsers. In *Proceedings of the 8th ACM European Conference on Computer Systems*, EuroSys '13, pages 281–294, New York, NY, USA, 2013. ACM.

[26] P.F. Syverson, D.M. Goldschlag, and M.G. Reed. Anonymous connections and onion routing. In *Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on*, pages 44–54, 1997.

[27] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. Technical report, DTIC Document, 2004.

[28] The TOR Project. TOR Project Website. `http://torproject.org`.

[29] A. Panchenko, L. Pimenidis, and J. Renner. Performance Analysis of Anonymous Communication Channels Provided by Tor. In *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, pages 221–228, 2008.

[30] R. Pries, Wei Yu, S. Graham, and Xinwen Fu. On performance bottleneck of anonymous communication networks. In *Parallel and Distributed Processing, 2008. IPDPS 2008. IEEE International Symposium on*, pages 1–11, 2008.

[31] Jörg Lenhard, Karsten Loesing, and Guido Wirtz. *Performance Measurements of Tor Hidden Services in Low-Bandwidth Access Networks*. Springer, 2009.

[32] Mashael AlSabah, Kevin Bauer, Tariq Elahi, and Ian Goldberg. *The Path Less Travelled: Overcoming Tor's Bottlenecks with Traffic Splitting*. Springer, 2013.

[33] Tao Wang, Kevin Bauer, Clara Forero, and Ian Goldberg. *Congestion-Aware Path Selection for Tor*. Springer, 2012.

[34] Mashael AlSabah, Kevin Bauer, Ian Goldberg, Dirk Grunwald, Damon McCoy, Stefan Savage, and Geoffrey M. Voelker. DefenestraTor: Throwing out Windows in Tor. In *Proceedings of the 11th International Conference on Privacy Enhancing Technologies*, PETS'11, pages 134–154, Berlin, Heidelberg, 2011. Springer-Verlag.

[35] Rob Jansen, Paul Syverson, and Nicholas Hopper. Throttling Tor Bandwidth Parasites. In *Proceedings of the 21st USENIX Conference on Security Symposium*, Security'12, pages 18–18, Berkeley, CA, USA, 2012. USENIX Association.

[36] Norman Danner, Sam DeFabbia-Kane, Danny Krizanc, and Marc Liberatore. Effectiveness and detection of denial of service attacks in Tor. pages 1–11, October 2012.

[37] Stevens Le Blond, Pere Manils, Chaabane Abdelberi, Mohamed Ali Dali Kaafar, Claude Castelluccia, Arnaud Legout, and Walid Dabbous. One Bad Apple Spoils the Bunch: Exploiting P2P Applications to Trace and Profile Tor Users. page 4th USENIX Workshop on Large, March 2011.

[38] Nicholas Hopper, Eugene Y. Vasserman, and Eric Chan-TIN. How Much Anonymity Does Network Latency Leak? *ACM Trans. Inf. Syst. Secur.*, 13(2):13:1–13:28, March 2010.

[39] Prateek Mittal, Ahmed Khurshid, Joshua Juen, Matthew Caesar, and Nikita Borisov. Stealthy Traffic Analysis of Low-latency Anonymous Communication Using Throughput Fingerprinting. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 215–226, New York, NY, USA, 2011. ACM.

[40] Kevin Bauer, Damon McCoy, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. Low-resource Routing Attacks Against Tor. In *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society*, WPES '07, pages 11–20, New York, NY, USA, 2007. ACM.

[41] Timothy G. Abbott, Katherine J. Lai, Michael R. Lieberman, and Eric C. Price. Browser-based Attacks on Tor. In *Proceedings of the 7th International Conference on Privacy Enhancing Technologies*, PET'07, pages 184–199, Berlin, Heidelberg, 2007. Springer-Verlag.

[42] Zachary Weinberg, Jeffrey Wang, Vinod Yegneswaran, Linda Briesemeister, Steven Cheung, Frank Wang, and Dan Boneh. StegoTorus: A Camouflage Proxy for the Tor Anonymity System. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 109–120, New York, NY, USA, 2012. ACM.

[43] Andriy Panchenko, Lukas Niessen, Andreas Zinnen, and Thomas Engel. Website Fingerprinting in Onion Routing Based Anonymization Networks. In *Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society*, WPES '11, pages 103–114, New York, NY, USA, 2011. ACM.

[44] Chris Wacek, Henry Tan, Kevin Bauer, and Micah Sherr. An Empirical Evaluation of Relay Selection in Tor. In *NDSS*. The Internet Society, 2013.

[45] Pogoplug. Pogoplug SafePlug. `https://pogoplug.com/safeplug`.

[46] K. Bauer, H. Gonzales, and D. McCoy. Mitigating Evil Twin Attacks in 802.11. In *Proceedings of the Performance, Computing and Communications Conference*, pages 513–516, December 2008.

[47] H. Gonzales, K. Bauer, J. Lindqvist, D. McCoy, and D. Sicker. Practical Defenses for Evil Twin Attacks in 802.11. In *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–6, December 2010.

[48] Jan Damsgaard, Mihir A. Parikh, and Bharat Rao. Wireless commons perils in the common good. *Communications of the ACM*, 49(2):104–109, February 2006.

[49] Sergey Bratus, Cory Cornelius, David Kotz, and Danie l Peebles. Active behavioral fingerprinting of wireless devices. In *Proceedings of the first ACM conference on Wireless network security*, WiSec '08, pages 56–61, New York, NY, USA, 2008. ACM.

[50] Aldo Cassola, William K. Robertson, Engin Kirda, and Guevara Noubir. A Practical, Targeted, and Stealthy Attack Against WPA Enterprise Authentication. In *NDSS*. The Internet Society, 2013.

[51] Aldo Cassola, Tao Jin, Harsh Kumar, Guevara Noubir, and Kamal Sharma. Demo: SNEAP: A Social Network-enabled EAP Method No More Open Hotspots. In *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*, MobiSys '11, pages 351–352, New York, NY, USA, 2011. ACM.

[52] Nicole Lee. Facebook's head of special projects talks wearables, WiFi and human connections. `http://www.engadget.com/2013/11/11/facebook-expand-ny/`.

[53] David Chaum, Ivan Damgård, and Jeroen van de Graaf. Multiparty Computations Ensuring Privacy of Each Party's Input and Correctness of the Result. In Carl Pomerance, editor, *CRYPTO*, volume 293 of *Lecture Notes in Computer Science*, pages 87–119. Springer, 1987.

[54] Jan Camenisch and Jens Groth. *Group Signatures: Better Efficiency and New Theoretical Aspects*. Springer, 2005.

[55] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. *Lecture Notes in Computer Science*, 1880:255–270, 2000.

[56] David Chaum and Eugène van Heyst. Group Signatures. In Donald W. Davies, editor, *EUROCRYPT*, volume 547 of *Lecture Notes in Computer Science*, pages 257–265. Springer, 1991.

[57] L. Chen and T. P. Pedersen. *New group signature schemes*. Springer, 1995.

[58] Xiangguo Cheng, Chen Yang, and Jia Yu. A New Approach to Group Signature Schemes. *JCP*, 6(4):812–817, 2011.

[59] Benoît Libert, Thomas Peters, and Moti Yung. Scalable Group Signatures with Revocation. In *Proceedings of the 31st Annual International Conference on Theory and Applications of Cryptographic Techniques*, EUROCRYPT'12, pages 609–627, Berlin, Heidelberg, 2012. Springer-Verlag.

[60] Lin Chen, Xiaoqin Huang, and Jinyuan You. Group signature schemes with forward secure properties. *Applied Mathematics and Computation*, 170(2):841–849, 2005.

[61] Yusuke Sakai, Keita Emura, Goichiro Hanaoka, Yutaka Kawai, Takahiro Matsuda, and Kazumasa Omote. Group Signatures with Message-dependent Opening. In *Proceedings of the 5th International Conference on Pairing-Based Cryptography*, Pairing'12, pages 270–294, Berlin, Heidelberg, 2013. Springer-Verlag.

[62] Ernest F. Brickell, David Chaum, Ivan Damgård, and Jeroen van de Graaf. Gradual and Verifiable Release of a Secret. In Carl Pomerance, editor, *CRYPTO*, volume 293 of *Lecture Notes in Computer Science*, pages 156–166. Springer, 1987.

[63] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In Eli Biham, editor, *EUROCRYPT*, volume 2656 of *Lecture Notes in Computer Science*, pages 614–629. Springer, 2003.

[64] Ernie Brickell, Jan Camenisch, and Liqun Chen. Direct Anonymous Attestation. *IACR Cryptology ePrint Archive*, 2004:205, 2004.

[65] Manish Jain and Constantinos Dovrolis. Ten fallacies and pitfalls on end-to-end available bandwidth estimation. In *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*, IMC '04, pages 272–277, New York, NY, USA, 2004. ACM.

[66] Manish Jain and Constantinos Dovrolis. Pathload: A Measurement Tool for End-to-End Available Bandwidth. In *In Proceedings of Passive and Active Measurements (PAM) Workshop*, pages 14–25, 2002.

[67] Manish Jain and Constantinos Dovrolis. End-to-end available bandwidth: measurement methodology, dynamics, and relation with TCP throughput. *SIGCOMM Comput. Commun. Rev.*, 32(4):295–308, August 2002.

[68] Buffalo Technology. Buffalo router model WZR-HP-G300NH. `http://www.buffalotech.com/products/wireless/single-band-wireless-routers`.

[69] The OpenWrt Distribution. OpenWRT. `http://www.openwrt.org`.

[70] The OpenWrt Distribution. Table of Hardware. `http://wiki.openwrt.org/toh/start`.

[71] 3GPP Technical Specification Group Services and System Aspects. 3GPP TS 23.261: IP Flow Mobility and seamless WLAN offload; Stage 2. Technical report, September 2012.

[72] 3GPP Technical Specification Group Services and System Aspects. 3GPP TS 23.402: architecture enhancements for non-3gpp accesses. Technical report, September 2013.

[73] 3GPP Technical Specification Group Services and System Aspects. 3G security; Security architecture. Technical report, June 2013.

[74] 3GPP Technical Specification Group Services and System Aspects. 3GPP System Architecture Evolution (SAE); Security architecture. Technical report, September 2013.

[75] IEEE. Wireless Local Area Networks (LANs). `http://standards.ieee.org/about/get/802/802.11.html`, 2012.

[76] IEEE. Standards for Wireless, Local, and Metropolitan Area Networks. `http://standards.ieee.org/findstds/standard/802.1X-2010.html`, 2012.

[77] Andrea Bittau, Mark Handley, and Joshua Lackey. The Final Nail in WEP's Coffin. *Security and Privacy, IEEE Symposium on*, 0:386–400, 2006.

[78] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to Leak a Secret. In Colin Boyd, editor, *ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer, 2001.

[79] Eyal Kushilevitz and Rafail Ostrovsky. Replication is NOT Needed: SINGLE Database, Computationally-Private Information Retrieval. In *FOCS*, pages 364–373. IEEE Computer Society, 1997.

[80] Emil Stefanov and Elaine Shi. Multi-cloud Oblivious Storage. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 247–258, New York, NY, USA, 2013. ACM.

[81] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Consulted*, 1:2012, 2008.

[82] Akamai. Akamai reveals 2 seconds as the new threshold of acceptability for ecommerce web page response times. `http://www.akamai.com/html/about/press/releases/2009/press_091409.html`, 2009.