A Peer-to-Peer Approach to Wireless LAN Roaming

Elias C. Efstathiou
Mobile Multimedia Laboratory
Department of Computer Science
Athens University of Economics and Business
Athens 104 34, Greece
+30 210 8203 693
efstath@aueb.gr

George C. Polyzos
Mobile Multimedia Laboratory
Department of Computer Science
Athens University of Economics and Business
Athens 104 34, Greece
+30 210 8203 650
polyzos@aueb.gr

ABSTRACT

We make the case for a Global Confederation of Peer-to-Peer (P2P) Wireless Local Area Networks. A P2P Wireless Network Confederation (P2PWNC) is a community of administrative domains that offer wireless Internet access to each other's registered users. The ubiquitous Internet access that the roaming users of these domains could enjoy compensates for their home domain's cost of providing access to visitors. Existing roaming schemes utilize central authorities or bilateral contracts to control access to resources. In contrast, a P2PWNC forms a pure P2P community in which participating domains are autonomous entities. Domains make independent decisions concerning the amount of bandwidth they contribute. As a result, similarly to existing P2P systems, a P2PWNC will suffer from "free-riding" if no incentive mechanisms exist to ensure that domains offer the amount of resources that is economically justified. Flexible rules on reciprocity can be set to delimit domain actions and encourage domains to provide in order to consume. In this paper, we present several aspects of the P2PWNC requirements and design. We outline several P2PWNC implementation issues relating to user privacy and the confederation's real-world deployment. We also describe the P2PWNC prototype that we developed.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design – *distributed networks, network communications, packet-switching networks, wireless communication.*

General Terms

Design, Economics, Security, Legal Aspects.

Keywords

WLAN, Wi-Fi, WISP, P2P, roaming, incentives, privacy, mixes

1. INTRODUCTION

Ubiquitous access to the Internet is becoming a necessity. However, the required infrastructure is not yet in place. Wireless Internet Service Providers (WISPs) that rely on the cheaper IEEE 802.11 set of technologies are facing difficulties that limit their coverage to selected hotspots. At the same time, 802.11 wireless LANs are being deployed in households, school campuses, airports, and many other public and private venues.

In this paper, we present a simple framework designed to unite all these wireless networks in one global group. We call this union a *Peer-to-Peer Wireless Network Confederation* (P2PWNC). The P2PWNC is based on the Peer-to-Peer (P2P) paradigm and technology. WLAN providers that participate in the P2PWNC offer network access to each other's users. The key entities in the P2PWNC are the *Domain Agents* (DAs). Simply put, the P2PWNC is a P2P network of DAs. Each DA is a physical computing node that represents one independent administrative domain. The P2PWNC domains may range in size from a residential hotspot with just one access point, to an international WISP that controls numerous access points in several locations. P2PWNC DAs regulate the acts of wireless service provision and consumption for their respective domains. The purpose of DAs is to eliminate the administrative overhead of roaming agreements. In their place, the DA P2P network uses a simple accounting mechanism based on *token-exchange*: when a user from one P2PWNC domain is roaming within another P2PWNC domain, the user's home DA transfers tokens to the visited DA in compensation for the resources of the visited domain that the user consumed.

A distinctive characteristic of the P2PWNC is that each DA makes independent decisions concerning the amount of resources it provides to visitors. The P2PWNC is therefore designed around complete domain autonomy. This is a key difference from existing roaming schemes. A central P2PWNC design goal is building into the system incentive mechanisms for *reciprocal behavior*: domains must provide resources to visitors in order for their own roaming users to be able to consume similar resources elsewhere within the P2PWNC.

No external entity controls the P2PWNC or the interactions of its participants. By eliminating administrative overhead, the P2PWNC makes it easier for domains that wish to join it to actually do so. There is no direct cost for becoming a member domain of the P2PWNC and, from the perspective of a WLAN administrator, joining the P2PWNC is almost as easy as joining a file-sharing network. For these reasons, the P2PWNC may be more socially acceptable. The thesis of this paper is that the

WMASH'03, September 19, 2003, San Diego, California, USA.
Copyright 2003 ACM 1-58113-768-0/03/0009… $5.00.

P2PWNC is a suitable vehicle for achieving the goal of ubiquitous access to the Internet.

An important characteristic of P2P systems is that they allow designers to place components on several peer nodes within the P2P network without having to rely on external servers. Three basic P2PWNC subsystems are designed around its P2P nature. These are: (1) the P2PWNC distributed accounting subsystem, which relies on the DAs themselves (and not some external entity) to store P2PWNC accounting history in a fault-tolerant way; (2) the P2PWNC privacy subsystem, which provides identity privacy (anonymity) and location privacy (untraceability) to users by relying on intermediate traffic *mixes*; and (3) the distributed hash-table, which is the underlying data structure that is used by both the accounting subsystem and the P2PWNC *name-service*.

In the P2PWNC, roaming agreement complexity is taken away from human administrators and entrusted to DAs. A DA must ensure that it has enough tokens to cover the needs of its domain users that are roaming within the P2PWNC. DAs must also regulate resource contribution to visitors so that the visitor traffic does not adversely affect normal domain usage. Because DAs consist of software modules, we cannot assume that they will not be hacked by malicious domain administrators. The P2PWNC design therefore assumes that any participating DA may deviate from its standard protocols.

The rest of this paper is organized as follows. In Section 2, we give some background information regarding the P2P paradigm and the state of current WLAN roaming schemes. Section 3 presents the principles that guide the P2PWNC design decisions. Section 4 presents P2PWNC architectural elements. Section 5 presents two issues that affect the implementation of the P2PWNC: security and economic modeling. Section 6 presents potential P2PWNC deployment issues. In Section 7, we present our implementation of a prototype P2PWNC domain agent. Section 8 concludes the paper.

2. BACKGROUND

2.1 The Peer-to-Peer Paradigm

The Peer-to-Peer (P2P) paradigm is usually referred to as the "opposite" of the client-server model. In this section, we list those aspects of the P2P interaction model that make it unique and which are also generic enough to encompass most P2P systems, both computer-based and non computer-based, including, of course, the P2PWNC.

Shared goods. All P2P systems involve the sharing of goods. Examples of shared goods may include lower-level resources, such as storage, processing, or bandwidth; and higher-level assets such as content, expert opinions, or news items. These resources can be *rivalrous*, meaning that consumption by one peer excludes others from consuming the same resource, or *non-rivalrous*, where the previous restriction does not apply. Storage space is an example of a rivalrous good and digital content is an example of a non-rivalrous good, since several peers can consume the same digital content simply by replicating it.

Peers as economic agents. In a P2P system, peers can be thought of as economic agents [3] that both provide and consume goods. The *value* of a P2P system is usually linked to the number of providing agents. However, this is an oversimplification as there are usually numerous ways to measure value that are hard to define analytically (and which are also system-dependent). Furthermore, a small number of peers may contribute a lot more resources than others, making the total number of minor providers in the system less significant. In a *homogeneous* P2P system, all peers are both providers and consumers and each peer contributes a fair share of the total value. However, most P2P systems (including the P2PWNC) are not homogeneous.

Peer autonomous behavior. P2P systems are designed around peer independence. Peers may join and leave the system at any time. In addition, peers that are part of the system may dynamically tune their rates of contribution and consumption. System functionality does not rely on any specific peer and the P2P system as a whole adapts to this dynamic behavior of its components. For this reason, computer-based P2P systems may perform very well even in cases of random network outages or accidental node malfunctions.

Free-riding, altruism and rules. *Free-riding* is a phenomenon most P2P systems have to deal with [1]: peers tend not to contribute resources in order to minimize their own costs. At the same time they may benefit from other peers. *Altruism* (contributing while disregarding one's cost) is the opposite force that tends to balance P2P systems. However, for a P2P system to operate more closely to an optimal point, fair-share *rules* need to be introduced. Rules are system parameters that regulate peer actions. As in real life, such rules may be difficult to enforce, especially when peers wish to remain autonomous (i.e., obey or disobey at will). One example rule that peers may borrow from real life is to assign prices to the goods they share (in some virtual or real currency). Such a general rule can create a free-market economy within the system and limit peer free-riding. However, when such a rule is introduced, the system faces the possibility of *strategic manipulation* or downright *hacking*.

Incentive mechanisms. Many P2P systems need to induce peers to: (1) participate in the system; (2) provide more goods; (3) provide goods of higher quality; or (4) consume less system resources. Rules must be designed in such a way so that the P2P community benefits as a whole. General incentive mechanisms employed by P2P systems to encourage contribution include peer *ratings*; *token-based accounting of actions; regular audits of accounting history*; or combinations thereof. These mechanisms usually rely on a peer *naming-scheme*, which must also encourage peers not to change their system names often (otherwise, accounting history could become meaningless).

We can now give a *definition of P2P systems*:

P2P systems are communities of economic agents cooperating for mutual benefit without centralized control. Their basic principle is to preserve agent autonomy while maintaining system scalability and reliability. P2P systems make use of otherwise under-exploited resources, a fact which gives designers of computer-based P2P systems the freedom to "put anything, anywhere" (term borrowed from [5]) i.e. place system components on several different peer nodes, ensuring system fault-tolerance and scalability.

2.2 Current State of WLAN Roaming

Today, WLAN roaming (sometimes also referred to as WISP roaming) is practically non-existent [6]. One reason for this is the general uncertainty about the Mobile Internet market as whole and this is one of the main obstacles to the development of a viable multilateral roaming platform. A business model related to WLAN roaming, called *hotspot aggregation*, does not constitute roaming according to the cellular telephony definition of roaming, since the roaming users are essentially customers of the one aggregator. In the USA, there are numerous young companies that attempt to get a share of the WLAN market and this has resulted in a fragmented landscape. In addition, many of these companies are poorly funded. On the other hand, in Europe, hotspot deployment has not advanced as much, mainly because of the fact that, in Europe, it is assumed that the well-known and established European cellular operators will control the majority of future WLAN hotspots.

A WISP association, called *Pass-One* [12], is considered a pioneer in the administrative side of roaming. However, the roaming model proposed by Pass-One is very elaborate and it generally assumes that participating WISPs will be business entities that will have responsibilities sometimes comparable to those of an average 2G mobile operator. For example, in one of their roaming guidelines, Pass-One suggests that the networks that participate in the association should employ multi-language technical assistance for roaming visitors coming from other networks, in case they need it. This excerpt below, taken from Pass-One's web site, summarizes the association's objectives: "Pass-One's main task will be specifying the rules for authentication, authorization and profile transfer, access management, accounting and billing, tariff planning, settlement and overall service delivery." These objectives could very well apply to a GSM, not a WLAN, roaming association.

On the technical side of roaming, the *Wi-Fi Alliance* recently released a draft entitled "Best current practices for WISP roaming" [2]. This draft deals primarily with the concept of a unified client experience (for example, consistent login screens and procedures across WLAN providers). Additional technical issues that currently are of interest to the roaming enablers of the Wi-Fi Alliance include how to standardize on a protocol for the back-end AAA-to-AAA (Authentication, Authorization and Accounting) communication; whether the WISPs should support the use of SIM-card authentication for their networks; and others. On the overall design front, a very recent report [6] defines the following three layers for a proposed multilateral roaming platform: (1) the signaling layer between WISPs, (2) the clearing layer, and (3) the settlement layer. Again, the proposed architecture is heavily influenced by the cellular practices.

It was our general intention with this section to show that existing WISP roaming frameworks have a tendency to imitate the complexity of 2G roaming, which may not be necessary in the Internet world, as we shall present below.

3. PRINCIPLES

3.1 Limitations of Existing Roaming Schemes

WLAN service providers enter into roaming agreements with competitors because it is prohibitively expensive to achieve a large-enough coverage footprint without help from others. Nevertheless, even the combined coverage of these WISP associations still leaves WLAN coverage being far from ubiquitous. We do not doubt that this situation will eventually change. However, there exist several limitations in the current roaming frameworks, which we list below that make this transition harder and slower than it should be.

The *service mark* logic. There are many successful service marks that guarantee quality (e.g. VISA). The service mark logic that certain WISP associations [12] attempt to replicate in the context of providing Internet services may be flawed. Internet access has become a commodity and in the mind of end-users it will be a "best-effort" service for a long time to come. We do not suggest that users do not ever expect "99.99%" reliability and quality-of-service. What is important is that users know now that when their connection goes awry, the fault may be difficult to trace. With WLANs, the problems become even harder since they operate at unlicensed frequency bands. WLAN associations that promise a "complete user experience" attempt to sell something that they cannot possibly deliver, not unless they control every link and every server on the Internet, not to mention the unregulated wireless spectrum. On the other hand, the WLAN devices themselves today are quite reliable and will soon be even more reliable. Setting up the wireless part of the user experience is relatively easy to get right, assuming all one wants to do is build a "best-effort" hotspot. Since the complete experience cannot be controlled, the overhead and costs involved with becoming part of a service mark may be too much for small networks that wish to become micro-WISPs.

WISP short-term profit goals. WISPs and hotspot aggregators currently charge too much for too little (spotty coverage). The wired Internet took decades before becoming commercial. The wireless Internet should be allowed to follow a similar (albeit faster) path and be given an opportunity to grow and reach maturity. Although this is difficult to achieve in the current economic climate, it would be unfortunate to allow the cheaper and simpler WLAN technology to follow the difficult path of 3G. The P2PWNC is designed around organic growth and it can mimic the evolutionary steps of the original Internet.

Insufficient privacy. Current roaming models expose too much information to both the visited and the home network. There is no fundamental reason for the visited network to know either the user identifier or the home network that the roaming user originates from. In addition, the home network itself does not need to know the user's current location. Previous research has shown this to be possible and there exist Internet-based techniques to hide this information and still account for usage (see section 5.1).

Insufficient autonomy. WISP roaming is fundamentally different from 2G-style roaming because the Internet model is fundamentally different from the 2G model. 2G evolved from the PSTN model: it assumes relatively dumb terminals, centralized control, strict network hierarchies, and a circuit-switched basic service. The Internet model assumes powerful terminals, end-to-end service deployment, a relatively simple core network, and a basic, best-effort packet-forwarding service. Moreover, the Internet notion of a network is very accommodating, exemplified by the flexibility provided by IP subnet hierarchies and NAT (Network Address Translation) islands. As a result, inflexible 2G-style roaming agreements where each partner must provide "circuits" to *all* requesting members of another partner (which can create imbalance if the roaming traffic is not symmetric) can be defined more flexibly in the Internet world. In the P2PWNC, the "terms of use" are a lot less strict.

Administrative overhead. Current WISP roaming frameworks still incur serious administrative overhead when candidate WISPs decide to join a roaming association. In our proposal and from the perspective of a WLAN administrator, joining the P2PWNC is almost as easy as joining a P2P file-sharing network.

3.2 The P2PWNC as a P2P System

Studying the P2PWNC as a P2P system is relatively straightforward. It is apparent that a WLAN roaming framework is different from a P2P file-sharing system but this is the case mainly because the goods shared in file-sharing systems are *fungible* (i.e. moveable) and non-rivalrous (files can be replicated). All the fundamental aspects of the P2P paradigm presented in section 2.1 also apply to the P2PWNC. Here, we concentrate on the four general aspects that were mentioned in the definition of a P2P system. We study a more specific mapping in the next section.

Under-exploited resources. Today, almost anyone with a broadband Internet connection could set up a WLAN hotspot. Most households and organizations that do so can easily cover an area extending beyond the limits of their residence or office. With appropriate tweaking, coverage areas can extend even further. This bandwidth resource exists today and it is not being exploited to its full potential. For example, a residential hotspot would operate, on average, only at a small percentage of its maximum throughput. There is practically nothing related to the core WLAN service that a commercial hotspot offers, which a residential hotspot cannot provide. We can therefore observe that all these would-be micro-WISPs can assist in achieving the ubiquitous wireless coverage goal. However, these latent resources need to be shared.

Cost-sharing. We mentioned in the previous section that the small radius of a WLAN cell necessitates many cells in order to build a large-enough coverage footprint. When a single provider attempts to cover large areas, provisioning costs may rise quickly. These costs include initial equipment installation costs as well as Operation, Administration and Maintenance (OA&M) costs. Most importantly, WISPs may face their greatest cost when building their back-end database infrastructure and customer relationships [7]. Cooperation for mutual benefit involves the distribution of these costs among multiple collaborating providers. However, appropriate incentive mechanisms need to be in place in order for diverse networks to cooperate. In WISP roaming, the obvious incentive for potential providers is the direct benefit their customers would enjoy by accessing foreign hotspots.

"Put anything, anywhere." Many additional network nodes are required outside of the local hotpots themselves should the WISP or the WISP association decide to use advanced network services. For example, to support SIP-type (Session Initiation Protocol) presence and mobility services, SIP proxies need to be present at both the visited and the home domains. Also, in section 5.1, we will present one way to enhance privacy through the use of intermediate traffic mixes, which are also valuable external servers. In section 5.2, we also discuss the issue of keeping reliable accounting records in a distributed manner by using multiple distributed account holders. In general, by being able to follow the "put anything, anywhere" guideline, one node of each of the types we mentioned can be placed inside every participating P2PWNC DA, thereby eliminating reliance on external servers and keeping all the functionality within the P2PWNC system.

Agent autonomy. In the context of the P2PWNC, autonomy means that every participating WLAN may dynamically adjust its provisioning rates, or may even shut down for unpredictable periods of time.

We will not attempt to prove formally that the overall system will be stable. For now, we limit ourselves to comparing the P2PWNC to another Internet system with autonomous agents: the World-Wide Web. The WWW enabled completely decentralized information sharing through the use of multiple independent servers that were not centrally controlled by any one administration. Today, the Web works fine and no central authority has to manage it. The P2PWNC could become just as stable.

3.3 Bandwidth: the P2PWNC Good

In the previous section, we noted one difference between the P2PWNC and a P2P file-sharing system: the latter trades in fungible, non-rivalrous goods. In this section, we describe the actual P2PWNC good in more detail.

The term *bandwidth* describes pretty accurately the good shared in the P2PWNC. Bandwidth is a non-fungible (i.e. associated with a specific location), rivalrous good (i.e. consumption of local bandwidth by one agent excludes others from consuming the same bandwidth). This consumption model is simplified and does not go into details such as possible multiple-access schemes that may be employed at the physical layer or the link layer (such as CDMA or CSMA/CA, respectively). Here, we shall use the term bandwidth as a shortcut for *ingress and egress Internet traffic throughput*.

The bandwidth of a hotspot cell is shared among Internet users of that cell. The users' aggregate bandwidth cannot exceed a certain limit, hence the rivalry. (We do not examine here the special cases of multicast and broadcast traffic.) To better study this bandwidth, we split it into its three components of interest: (1) wireless hotspot bandwidth, (2) wired bandwidth to and from the hotspot's upstream ISP, and (3) incoming and outgoing packet buffers maintained at local switching equipment (such as the hotspot's firewall/router).

Usable wireless hotspot bandwidth in IEEE 802.11b cells is around 5 Mbps. Wired bandwidth to and from the hotspot's upstream ISP can vary, from a 128/384 kbps (uplink/downlink) ADSL line, to a leased T1 or T3 line. Packet buffers can be maintained either at PCs that run simple Internet connection-sharing software, or at sophisticated wireless routers. The hotspot users have to share all these different resources.

Beyond the hotspot's default ISP gateway, aggregate user traffic probably splits into more than one route. We define the P2PWNC good using only the three components listed above since they represent the *domain of rivalry* that a hotspot can observe. One of these three resources will be the *bottleneck* that will define the hotspot's aggregate Internet throughput.

Because "not all bits are created equal," higher-level digital goods are normally assembled out of this simple packet service. These goods include web objects, streaming and interactive multimedia, and other types of information that the hotspot can differentiate and market according to more elaborate sharing rules. However, these rules are based on a different way of looking at the sole underlying good, which is always a transported digital stream of ones and zeros.

4. ARCHITECTURAL ELEMENTS

4.1 Overview

The P2PWNC is a P2P network of *Domain Agents* (DAs). In the P2PWNC model, each independent administrative domain that participates in the P2PWNC maintains exactly one DA. Each DA has a unique logical name within the P2PWNC system. These names may be identical to their DNS domain names, but this is not a requirement. For example, the Athens University of Economics and Business (AUEB), being an independent administrative domain, may name its DA `aueb.gr`, thus reusing its DNS name. A residential hotspot that participates in the P2PWNC may use the name `The_San_Diego_Smiths` for their DA. Established WISPs may reuse their DNS names for their respective DAs (e.g. `boingo.com` or `cometa.net`). Examples of additional types of administrative domains that can participate in the P2PWNC include private companies that provide WLAN access to employees, or mobile operators that partner with venue owners and provide hotspot services. Because exactly one DA represents each one domain, there is no fundamental difference between a small residential hotspot and nationwide WISP as far as the P2PWNC P2P network is concerned. However, it is obvious that the P2PWNC is not a homogeneous P2P system.

In every domain, there is an associated group of *registered users*. For AUEB, this group includes the university's students and faculty; for a residential hotspot, this group would be the persons living in the household, which probably bought and maintain the WLAN and the broadband connection; for a private company, the registered users would be all of the company's employees; and for a WISP or mobile operator, their registered users would be all of their subscribers. The specifics of the relationship between user and domain are irrelevant. Whether it is a personal or a business relationship and whether it is based on subscription fees or it comes for free is not relevant: each DA should simply keep a list of its own registered users. (These varying user populations are another reason why the P2PWNC is not a homogeneous P2P system.)

The combination of: (1) the actions of bandwidth consumption performed by the domain's roaming registered users, and (2) the actions of bandwidth provisioning performed by the domain itself, represents the totality of actions performed by the domain's DA, acting as an economic agent within the P2PWNC. This means that in the P2PWNC model, the usual peer roles of provider and consumer are well separated: roaming users can only consume, while a domain (through its WLAN infrastructure) can only provide. This distributed nature of a P2PWNC peer makes a potential system implementation more complex (see section 5.2) but it does not affect the peer's nature or the P2PWNC P2P model in a fundamental way. In addition, we note here that only service provisioning to visitors is a P2PWNC action. Normal provisioning of WLAN service to a domain's registered users is not. However, the two types of provisioning may affect one another due to local bandwidth sharing (and this is one of the indirect costs of providing access to visitors as we mentioned previously).

4.2 DA Modules

A P2PWNC DA is designed as a collection of functional components, called *modules*, which are listed here:

Name-service module. The function of the name-service module is to map P2PWNC system names to DA Internet addresses. Unlike DNS names, P2PWNC domain names are logical and do not form name hierarchies. Again, unlike the DNS, they are also completely decoupled from network location. The ability to choose a peer name autonomously is important in all P2P systems and is characteristic of the peer's independence. Implementing a purely logical naming scheme today is possible through the use of *Distributed Hash-Table* (DHT) technology, which can be used to look-up all sorts of information. A DHT module is an important component of every DA as we shall show below.

Authentication module. The authentication module maintains a database of registered users along with the users' security credentials (passwords, in the simplest case). This module's role is to respond to authentication requests for users that are registered with the module's domain. These requests may come from the local *WLAN module* (in the case of requests coming from registered users who are using the service locally) or from another P2PWNC DA (when requests come from registered users who are roaming).

Traffic-policing module. This module is responsible for all traffic logging and shaping activities. At its most basic, this module is a dynamic firewall that only allows authorized users to consume domain bandwidth. However, by cooperating with the *provider-strategy module* (see below) it can become a powerful service differentiator that can allocate specific amounts of bandwidth to both local visitors and registered users according to the DA's current resource-management strategy.

WLAN module. This module encapsulates the basics of WLAN service provisioning, which usually includes a DHCP server, a DNS server, a NAT/NAPT router, a WLAN access point controller, and other service-specific components. Additional higher-layer components, such as a SIP proxy (for application-layer mobility), or a caching web proxy may also exist.

Distributed accounting module. Accounting of all P2PWNC actions is done using a DHT-based distributed accounting subsystem. Each DA stores part of the total P2PWNC accounting information in its distributed accounting module. By exploiting characteristics of DHTs, this accounting subsystem can be both scalable and fault-tolerant. It is important that malicious DAs cannot undetectably forge part of the P2PWNC action history because DAs rely on this information to devise their current and future strategies. At its most basic, the distributed accounting system could maintain the current number of "spending tokens" that each DA owns.

Consumer-strategy module. When a roaming user requests WLAN service, the visited DA will inform the user's home DA of this fact. The home DA's consumer-strategy module is then responsible for paying the required amount of tokens to the visited DA's provider-strategy module (see below). Depending on what the visited DA is asking for and, in conjunction with local (home) DA strategy, the consumer-strategy module may not allow the transaction to continue. Depending on the corresponding provider strategy of the visited DA, the roaming user may be denied service completely or may be offered service of lower quality.

Provider-strategy module. The provider-strategy module, in the most general sense, decides current service "prices." Based on the information it receives from the distributed accounting subsystem concerning its own token level as well as the token levels of the DAs it interacts with, this module decides on a pricing *granularity* and builds a tariff table. Example tariffs include "2 tokens for every outgoing and incoming kilobyte", or "30 tokens for one hour's worth of connection time with guaranteed ingress and egress throughput of 200 kbps", or "50 tokens for one hour of unlimited access." The provider strategy module communicates with other DAs' consumer-strategy modules and can potentially bargain with them. In so doing, it may end up charging *personalized* prices [8]. In addition, the module can base tariffs on current demand ("a token *now* buys you 10 minutes of Internet access"). Finally, assuming the traffic-logger module can identify higher-level services (such as emails being exchanged, interactive multimedia sessions, or web browsing), the provider may also differentiate prices on the basis of application-layer information.

Privacy-enhancement module. In section 5.1 we classify a roaming user's privacy needs and present the P2PWNC *mix network*, whose function is to hide the visited DA from the home DA and vice versa. The privacy-enhancement modules in DAs are *traffic mixes* based on Chaum's principles [9], which, together with other DA privacy-enhancement modules, form the backbone of the P2PWNC mix network.

DHT module. The DA DHT module is the low-level component that implements the distributed hash-table functionality required by the name-service module and the distributed accounting module. It can be based on existing DHTs, like Chord [15], or CAN [13].

4.3 User Identifiers

We now turn our attention to the P2PWNC users. We do not assume that each user is registered with only one domain. However, we do assume that each P2PWNC user has a (globally unique) *user identifier* of the form `user_name@domain_name` for each P2PWNC account, where `domain_name` is the domain's P2PWNC system name that we mentioned in section 4.1. Also, as we shall see in section 5.1, in order to address the need for identity privacy, a user may maintain one or more *pseudonyms* for each account, some of which may be dynamically generated with the cooperation of the respective home DA. In order to use P2PWNC services, users input their user identifiers and associated security credentials to *user agents*, which carry out the authentication procedure with the cooperation of the local DA WLAN module. Users may use different identifiers to ensure privacy, or to choose among multiple roles, or perhaps to receive additional P2PWNC privileges assuming that, for example, one of their home DAs currently has "better-standing" (i.e., higher token-level) within the P2PWNC.

5. DESIGN ISSUES

5.1 Security and Privacy

The P2PWNC security and privacy issues form a superset of the general WLAN security and privacy issues. There is much ongoing research on the latter, which we will not present here. We will, however, explore the additional security and privacy implications that arise due to the nature of the P2PWNC system. *Security processes* in the context of the P2PWNC are all login transactions, distributed accounting sessions, and DHT searches that are suspect due to the following basic characteristic of the P2PWNC system: the P2PWNC is a community of diverse, independent providers, most of which may be unknown and untrustworthy. When roaming users interact with these providers, there are many additional concerns that arise both for the roaming user and for the visited provider. We present four of these issues below, along with our ideas on how to address them. In addition, we support that the incentive mechanisms of the P2PWNC can make some types of malicious behavior rare, through longer-term reciprocal "punishments" that rely on current DA strategies and the P2PWNC's global accounting history.

Traffic logging by untrustworthy providers. After a successful user-agent login, the user would access the Internet as usual. Under normal circumstances, user traffic is completely visible to the default gateway, which, in this case, is the visited DA. Simple encryption techniques hide neither the identities of the remote parties the user is communicating with, nor the timing details of their communication. All this *metadata* can be valuable to hostile traffic loggers. A simple solution for users would be to *tunnel* (i.e. encrypt and route) all communication through the home domain or some other trustworthy domain. This way, the visited DA only sees packets coming and going to the same destination. The required tunneling agents can be standard modules in all P2PWNC DAs.

Abuse by untrustworthy users. Altruistic providers that offer free access may fall victims to abusive user behavior. Authenticated users may generate increased traffic loads, which may congest the local WLAN as well as the link to the provider's upstream ISP. This can be avoided if the DA's traffic-policing module continues to observe every active user session, even if P2PWNC accounting is not taking place. Unfortunately, even if the domain stops routing packets for the attacker, physical-layer Denial-of-Service (DoS) attacks can always cause disruption. (Fortunately, there is much ongoing research in DoS prevention at all layers.)

Identity privacy: pseudonyms. Pseydonyms, or *aliases*, are a powerful and simple way to hide the user's real identity from visited domains. Of course, long-term usage of an alias may provide enough information for adversaries to associate the alias with the real user. Also, aliases may not be enough when the name of the home domain used in them is the real one: if adversaries know for a fact that only one person from a specified domain is in the area, they can associate the alias with that one person [14]. Because the home-domain name is important for P2PWNC authentication, more powerful techniques are required to hide it (see below). However, standard aliases are good enough for most purposes, assuming that users can always use new aliases. To achieve this, the home DA must maintain in its authentication database a list of all aliases for every registered user. Another option would be to use an algorithm (that is known to both the user and the home DA), which can generate fresh aliases [14].

Identity and location privacy: the P2PWNC mix network. In order to hide: (1) the username and home domain from the visited domain (anonymity), and (2) the current location from the home domain (untraceability), the P2PWNC uses a *mix network* based on Chaumian mixes. (Details concerning the exact strengths and weaknesses of Chaumian mixes can be found in [11] and we will not present them here.)

Assume a user with identifier `A@C` is visiting domain *P* (*C* short for *consumer*, *P* for *provider*). User *A* wishes to access the P2PWNC but also wishes to hide: (1) the real identifier and home domain from domain *P*, and (2) the current location, *P*, from the home domain *C*. In order to achieve this and still allow P2PWNC accounting to proceed, the user can do the following: instead of using A@C as the login identifier for accessing domain *P*, *A* uses instead alias_A@M1, where *M1* (short for *Mix* 1) is a P2PWNC domain with an active privacy-enhancement module. So far, domain *P* only knows that a user called alias_A from domain *M1* requests service. The security credentials that accompany the user request contain enough information for *M1* to understand that it is being used as a mix. Within these credentials, *A* has hidden the real identity as well as a chain of mixes to be used. *M1* sees that the next mix in the chain is *M2*, so it proxies the request to it. The last mix in this chain is not really a mix but it is the home domain agent. Because the chain is encrypted by *A* using nested public key encryptions, no intermediate mix really knows whether the next one shall be the last [11].

Let us assume that there are only two intermediate mixes in the chain, *M1* and *M2*. (Remember that M1 and M2 could just as easily have been called X and Y - there is nothing to distinguish them from a usual P2PWNC domain, and, in fact, they will probably be just that.) When *M2* proxies the request to *C*, *C* has enough information within the request to know that alias_A is really user *A*. However, *C* cannot know with certainty where *A* is, because the only entity that contacted *C* was *M2*. P2PWNC transactions and accounting sessions proceed normally among domain pairs (P, M1), (M1, M2) and (M2, C). If mixes were not being used, in a session marked (P, C), tokens would flow from *C* to *P*. When the two mixes are introduced, tokens first flow from *C* to *M2*. *M2* knows that it is participating in a mix session so it spends all the newly earned tokens paying *M1*, since *M2* believes *M1* to be the provider. *M1*, on the other hand, knows that it is not the provider and that it is really participating in a mix session. So, *M1*'s newly earned tokens are, in turn, spent paying *P*, which *M1* believes (correctly in this case) to be the provider. Visited domain *P* knows with certainty that it *is* the provider and keeps the tokens. However, *P* thinks that *M1* paid for the service and it is infeasible for *P* to trace the tokens back to *C*.

5.2 Economics

In this section, we present a number of open design issues, regarding the economic nature of the P2PWNC:

Optimal system parameters. The P2PWNC is designed as a playing field for various types of players including strategic and non-strategic agents, free-riders and altruists, even the random hacker. The core principle behind its design is to protect the peers' right to remain autonomous while achieving system stability. System parameters should enable the P2PWNC to operate near its maximum potential. Defining and calculating these types of parameters (see [4]) is an open research question.

A secure distributed accounting subsystem. The P2PWNC accounting subsystem is of extreme importance. P2PWNC DAs base most of their decisions on information obtained by this subsystem. The main function of the accounting subsystem is to monitor all peer contribution and consumption acts and keep a record of the associated flow of tokens from consumers to providers. Its purpose is to make sure that both agents participating in a transaction uphold their end of the agreement. Possible breaches should also be recorded.

The P2PWNC accounting subsystem can be build using the P2PWNC DAs themselves, with each DA storing information for multiple accounts in a way that is both fault-tolerant and secure. Thus, no external third party would be required since every peer, in effect, would hold partial information regarding the accounts of one or more other peers. To prevent unauthorized tampering, cryptographically secure (i.e. unforgeable) tokens can be used.

Domain strategies. Token spending may have several levels of granularity and we already mentioned some example tariffs in section 4.2. A DA may charge by the kilobyte or by the hour; it may charge according to current congestion levels or according to the identity of the consumer. Moreover, a DA may be altruistic and not charge anything. These decisions depend on current DA strategies. Although the normal goal of a DA would be to ensure the best possible level of service for their own roaming users, the DA will have to earn tokens in order to do this, which means that the DA must also provide service to visitors, a fact that can adversely affect the local service provided to the domain's registered users. DAs must find a way to balance these two conflicting requirements.

"Offline" domains. A fundamental assumption of the P2PWNC's design is that each DA can control the aggregate rate at which its registered users can consume the resources of other DAs. This is a function of the DA consumer-strategy module. As soon as a roaming user requests service from a visited DA, a trigger message is sent from the visited (providing) DA to the home (consuming) DA. The home DA is then responsible for making the official consumption request on behalf of its roaming user. If the consumer-strategy module of the home DA decides otherwise, the visited DA has no reason to allow the user request to proceed.

An interesting issue here is what should happen if a home DA is offline. Assuming that the visited DA has a provisioning strategy that allows these types of requests, there may be two ways for the visited DA to receive the tokens that it is entitled to. One would be for the user-agent to pay without the intervention of the home DA. This is possible only if: (1) the relevant DA consumer-strategy module is also part of the user-agent; and (2) the home DA has at some point in the past distributed token "allowances" to each one of the user-agents under its control. Yet another solution would be for the payment to be made by a different P2PWNC domain, which could "speak on behalf" of the home domain that is currently offline.

Token generation. In the discussion so far we assumed the existence of cryptographically secure, unforgeable tokens. An important issue is how the domain agents first acquire some of these tokens when joining the P2PWNC for the first time. One promising solution here includes a (P2PWNC internal) distributed bank that can generate P2PWNC tokens and distribute them to new entrants. Schemes such as threshold cryptography [10] and standard public key encryptions can be used to ensure that no unauthorized tokens ever appear inside the system.

Domain heterogeneity. A final issue relating to the economics of the P2PWNC is how to effectively handle domain heterogeneity. We envisage domains with coverage areas diverse in size and location, as well as domains with completely uneven user populations. Small domains that receive few requests are valuable because they contribute towards the "ubiquitous access" target of the P2PWNC. However, if they only receive few requests there may be no way to reward them. Their respective DA could, of course, set token prices that are high and hope that consuming DAs would agree to pay. This is, however, part of the more general issue of how to design the P2PWNC system in such a way so that a few domains do not monopolize all the tokens.

6 DEPLOYMENT ISSUES

6.1 DA Administrative Interface

There are many parameters affecting the operation of the P2PWNC. The administrative interface for DAs must hide these details from domain administrators. DA configuration and maintenance has to be kept as simple as possible. We present here a hypothetical example of a university that provides WLAN access across campus, which decides to join the P2PWNC. By doing so, the university's students and faculty would be eligible to request service from all the other P2PWNC domains (with a certain probability that their request would be granted). Having already set up campus-wide WLAN cells, the university would have to accommodate a P2PWNC DA and allow it to assume the burden of traffic policing. We propose that a minimal number of parameters should be required to set up this DA. These parameters may include:

1. A list of registered users and their security credentials
2. The domain's aggregate egress and ingress throughput to and from its upstream ISP
3. Infrastructure details, such as the number of WLAN cells and potential local traffic bottlenecks
4. The average expected load from locally registered users and visitors
5. The average expected usage of the P2PWNC by roaming users of the domain.

Devising methods to measure some of the parameter values above is non-trivial. On the other hand, the objective is to allow a DA's administrator to make educated guesses for some parameters. Afterwards, it will be the DA's responsibility to: (1) constantly regulate local prices, (2) ensure visitor traffic does not adversely affect traffic from local registered users, and (3) ensure the best possible treatment for the DA's own registered users that are roaming.

6.2 P2PWNC Business Models

Although the P2PWNC is designed around reciprocal behavior and does not assume a more specific business model, we list here our ideas on various profit opportunities that are designed around the basic P2PWNC philosophy (which is the independent behavior of domains). In a P2PWNC-based wireless Internet, the following players have reasonable chances of making a profit:

Vendors of P2PWNC domain agents. Assuming the P2PWNC DA interfaces are open and extensible, there is an opportunity for different vendors to introduce their own version of the DA software that is, for example, better at ensuring high DA ratings within the P2PWNC. Designers would achieve this by improving the algorithms used by the DA consumer- and provider-strategy modules.

Vendors of P2PWNC support modules. These modules would include hotspot-indexing engines, software that would tune various domain agent parameters (see section 6.1), and numerous security and privacy enhancements.

Upstream ISPs that enable P2PWNC micro-WISPs. Currently, broadband ISPs have not decided on a general course of action regarding their private customers that build hotspots on top of their broadband connections. If the P2PWNC scheme becomes popular, ISPs that assist their customers with setting up P2PWNC DAs may be valued more by customers.

P2PWNC domain aggregators. Similar to web hosting companies, P2PWNC domain aggregators would host DAs for multiple micro-WISPs. Also, they would pool WISP resources together, assuming they could devise suitable algorithms to ensure better average treatment for the registered users of all aggregated micro-WISPs. However, lower-level WLAN equipment management is more difficult to outsource and perform remotely.

"Pay-as-you-go" domains. By interpreting the notion of *registered* users differently, we envisage vendors that would sell pre-paid cards, containing valid user identifiers and security credentials for anyone to use. The domain part of these identifiers could be a real P2PWNC domain with existing WLAN infrastructure, or a "virtual" P2PWNC domain, which although has no way to earn P2PWNC tokens to support this scheme (since it has no real WLAN infrastructure), it may have dealings with P2PWNC domains outside the normal P2PWNC interaction model that ensure a flow of tokens to the virtual domain's DA.

6.3 Operational Issues

More economic analysis and simulations are needed before we can appreciate how the P2PWNC and its token-based incentive technique would operate in the real world. It is likely that analysis will never be able to compute some ideal operational parameters for the P2PWNC. (See [4] for additional information.) It is more probable that, like the Internet itself, the P2PWNC might just work in an ad hoc fashion, ensuring, however, good chances for roaming users to find a P2PWNC hotspot and to be allowed to access the Internet. A real-world concern here is that policies enforced by regulatory bodies and broadband ISPs (e.g. concerning the use of the ISM band or the sharing of broadband connections) may throttle the P2PWNC's growth opportunities.

7. PROTOTYPE

In order to test the feasibility of creating a software-based DA, we programmed a prototype (using C, Java and Python) and built two DAs running on standard PCs with Linux 2.4.21. The WLAN, Authentication and Traffic-control modules are almost complete. Each of the DAs has two Ethernet cards, one of which is connected to the Internet and the other to a Cisco Aironet 1200-series WLAN AP. (This type of access point also supports the IEEE 802.1X port-based network access control standard.) A DHCP server allocates addresses to wireless clients from the private address range `192.168.0.0/16`. In order for the clients to access the Internet, the WLAN module performs Network Address and Port Translation (NAPT). A local caching-only DNS server also exists. Currently, the WLAN module supports two client authentication methods: (1) IEEE 802.1X-based, assuming the client also supports IEEE 802.1X supplicant functionality (which comes standard with Microsoft Windows XP); and (2) a custom web-based login procedure. Both authentication procedures rely on simple username-password pairs for security credentials. After the authentication module authenticates the clients, the traffic-policing module initiates traffic logging and shaping. We rely on the `libpcap` library (`www.tcpdump.org`) for packet capturing and logging and on the Linux `tc` tool (`www.lartc.org`) for traffic shaping. Currently, the traffic-policing module supports the shaping of both egress and ingress TCP/UDP traffic, based on a hierarchical token-bucket queuing discipline. Unauthenticated wireless users cannot access the Internet. For the web-based authentication method we use the Linux standard `iptables` firewall (`www.netfilter.org`) to block traffic. With 802.1X, the access point blocks the unauthorized users itself.

The authentication database stores several accounts we use for testing. If the domain part is not recognized as local, we use the JXTA P2P libraries (`www.jxta.org`) to transfer the request to the other DA (currently only two domains exist), where the credentials are checked against that authentication database. Our provider-strategy module is not complete. Currently, it allocates different rates to different users using static rules that only check which domain the user comes from (local or not-local). Token exchanges between the consumer-strategy and the provider-strategy modules are done based on a simple static algorithm ("one token for every successful visitor WLAN login"). There is still much work needed on the two strategy agents. Currently, the strategy agents do not set prices dynamically and the tokens they exchange are not cryptographically secure. The privacy modules are also missing. A lot of analytic work is also needed on the algorithm that the strategy agents will follow. In addition, our DAs currently support domains with only one WLAN access point. We soon plan to extend the DA password-based authentication, with certificate-based authentication. Then we will begin to build the P2PWNC public-key infrastructure that is necessary to support all the P2PWNC cryptographically secure functionality (mixes, DHT searches, secure token exchanges, secure token generation and tunneled communications).

8. CONCLUSION

We have introduced the concept of a Peer-to-Peer Wireless Network Confederation (P2PWNC). The P2PWNC can be seen as a simple substitute for existing WLAN roaming schemes. It is based on the Peer-to-Peer paradigm of autonomous agents that provide and consume resources. We have motivated the existence of the P2PWNC, described its high-level design, and provided guidelines for its implementation. We discussed a number of issues relating to security, privacy, economics, and business realities that need to be investigated and resolved in order to design a practical and efficient confederation. Finally, we presented our DA prototype implementation.

9. ACKNOWLEDGEMENTS

This work is partly supported by the EU research project "Market Management of Peer-to-Peer Services" (MMAPPS, RTD No IST-2001-34201). The authors gratefully acknowledge ongoing discussions with their MMAPPS partners, particularly Costas Courcoubetis, Panos Antoniadis, and Ben Strulo. Also, a sincere thanks to Dimitris Mistriotis and Dimitris Paraskevaidis, final-year AUEB-CS students, who provided invaluable help with our Linux-based prototype.

10. REFERENCES

[1] Adar, E., and Huberman, B.A. Free Riding on Gnutella, First Monday, vol. 5, no. 10, 2000.

[2] Anton, B., Bullock, B., and Short, J. Best Current Practices for Wireless Internet Service Provider Roaming, Wi-Fi Alliance Public Document, Feb. 2003. http://www.wi-fi.org.

[3] Antoniadis, P., and Courcoubetis, C. Market Models for P2P Content Distribution, AP2PC'02, Bologna, Italy, July 2002.

[4] Antoniadis, P., Courcoubetis, C., Efstathiou, E.C., Polyzos, G.C., and Strulo, B. Peer-to-Peer Wireless LAN Consortia: Economic Modeling and Architecture, to appear, 3rd IEEE International Conference on P2P Computing, Sweden, 2003.

[5] Braynard, R., Kostic, D., Rodriguez, A., Chase, J., and Vahdat, A. Opus: an Overlay Peer Utility Service, Proc. 5th OPENARCH, June 2002.

[6] BWCS Report. WISP Roaming – Single Subscription, Global Reach, May 2003.

[7] Camponovo, G., Heitmann, M., Stanoevska-Slabeva, K., and Pigneur, Y. Exploring the WISP Industry: Swiss Case Study, 16th Electronic Commerce Conference, Bled, Slovenia, 2003.

[8] Courcoubetis, C., and Weber, R. Pricing Communications Networks: Economics, Technology and Modelling, Wiley, Interscience Series in Systems and Optimization, 2003, 139-140.

[9] Chaum, D. Security without Identification: Transaction Systems to make Big Brother Obsolete, Communications of the ACM, vol. 28, no. 10, Feb. 1985, 1030-1044.

[10] Desmedt, Y. Threshold Cryptography, European Transactions on Telecommunications, vol. 5, no. 4, 1994, 449-457.

[11] Lopatic, T., Eckert, C., and Baumgarten, U. MMIP – Mixed Mobile Internet Protocol, CMS'97, Sept. 1997, 77-88.

[12] Pass-One - WISP association. Mission statement. http://www.pass-one.com.

[13] Ranasamy, S., Francis, P., Handley, M., Karp, R., and Shenker, S. A Scalable Content-Addressable Network, Proc. ACM SIGCOMM, San Diego, CA, 2001, 161-172.

[14] Samfat, D., Molva, R., and Asokan, N. Anonymity and Untraceability in Mobile Networks, ACM International Conference on Mobile Computing and Networking, Nov. 1995.

[15] Stoica, I., Morris, R., Liben-Nowell, D., Karger, D.R., Kaashock, M.F., Dabek, F., and Balakrishnan, H. Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications, IEEE/ACM Transactions on Networking, vol. 11, Feb. 2003.