

Designing a Peer-to-Peer Wireless Network Confederation

Elias C. Efstathiou¹ and George C. Polyzos

*Mobile Multimedia Laboratory, Department of Computer Science
Athens University of Economics and Business, Athens 104 34, Greece
{efstath, polyzos}@aueb.gr*

Abstract

We present the Peer-to-Peer Wireless Network Confederation (P2PWNC), a P2P system designed to enable the sharing of WLAN bandwidth among residential hotspots. The benefits of joining the Confederation outweigh the costs, and its token-based incentive mechanism prevents free-riding.

Keywords: WLAN, Wi-Fi, incentives, roaming, P2P

1. Introduction

In WLAN roaming, wireless users can access any WLAN hotspot belonging to a roaming association as long as their home network participates in the same association. The benefits are self-apparent, but so are the costs: providing service to visitors increases hotspot traffic and adversely affects normal service provision to the Wireless ISP's subscribers. True inter-WISP roaming is in its infancy. Hotspot deployment is also slow. In the whole of the USA, there exist less than 5,000 public hotspots (6/2003, Nielsen//NetRatings) – Wi-Fi is not ubiquitous. Most hotspots require some kind of subscription but no subscription accesses all of them. On the other hand, in the USA, there are millions of broadband subscribers. Assume each one installed a WLAN access point and became part of a global confederation of micro-WISPs. Then, each one of them would also be able to access broadband Internet when roaming inside the coverage areas of the others. In this paper, we discuss a simple system designed to achieve this: the *Peer-to-Peer Wireless Network Confederation* (P2PWNC).

2. Motivation

Public hotspots are not just for business professionals anymore. The price of IEEE 802.11b chipsets is dropping below \$4 and they are being incorporated in all portable devices, including laptops, palmtops, and smart-phones.

¹ To whom correspondence should be addressed. This work is partly supported by the EU IST project "Market Management of Peer-to-Peer Services" (MMAPPS, RTD No IST-2001-34201).

802.11b's 5 Mbps of actual throughput will increase to more than 20 when 802.11g chipsets become standard. Voice-over-IP over 802.11 is a viable alternative to cellular telephony (at least in metropolitan areas). Moreover, the advantages of ubiquitous WWW, email, and other IP services are significant.

3. Requirements

The basic requirements [1] for the P2PWNC system are: (1) *Autonomy*. All participating micro-WISPs have complete control of their contribution level and participation status (they may disable their hotspot or control the rate of visitor traffic). (2) *Reciprocity*. Peers must contribute in order to consume. Contribution means running the hotspot and allowing visitors to access it. Consumption means enjoying service from other peer micro-WISPs when roaming. (3) *Simplicity*. Assuming a hotspot is already in place, joining the P2PWNC should be no more difficult than joining a P2P file-sharing network. (4) *Self-sufficiency* and *decentralization*. All the P2PWNC subsystems rely only on the peers themselves and do not require any central entities or servers external to the P2PWNC.

4. Design

The P2PWNC is a P2P network of *Domain Agents* (DAs). Nodes running the DA software are located in every independent P2PWNC hotspot. DAs automatically regulate the provisioning of wireless service to visiting users. DAs communicate among themselves and exchange unforgeable tokens every time Internet service is provided to visitors. Two entities participate in this token-exchange session: the visited DA (the "contributing" DA, which earns tokens); and the roaming user's home DA (the "consuming" DA, which spends tokens). Tokens are the incentive mechanism [2] of the P2PWNC. They are a virtual currency that represents the value that the visited DA ascribed to its consumed resources. Resources include wireless bandwidth, as well as wired bandwidth to the hotspot's ISP. The main difference between a P2P file-sharing system and the P2PWNC is that here, the shared good is *rivalrous* (bandwidth consumption can lead to congestion, whereas files can always be replicated)

and *non-fungible* (files can change locations whereas hotspots are normally associated with one location).

Each DA has a unique logical identifier, or Peer ID (e.g. `The_Smith_Family_Hotspot`). Each P2PWNC user has a user identifier of the form `user-ID@DA-ID`, where `DA-ID` is the name of the user's home DA. In addition to a standard WLAN router, a DA is composed of the following modules:

Authentication. This module maintains a database with the security credentials of all users registered with this DA. (These users would probably be the persons occupying the residence where the DA is installed.)

Name-service. This module uses a *Distributed Hash-Table* (DHT), like CAN [4], to map DA IDs to the current IP address of the DA host in a location-independent way (unlike DNS). A DHT would allow for node address changes and unpredictable failures. The P2PWNC DHT uses the DAs themselves as nodes.

Traffic-policing. This module logs and shapes local and visitor, egress and ingress Internet traffic.

Strategy. This module regulates DA contribution actions by dynamically assigning token prices for every incoming and outgoing kilobyte that visitors consume. It also regulates DA consumption by deciding to pay or not to pay for incoming requests from visited DAs on behalf of roaming users registered with this home DA. Strategy must ensure that the DA's own registered users receive the best possible treatment when roaming and that visitor traffic does not adversely affect normal local traffic.

Distributed accounting. Based on a DHT, this module maintains the current token-level of every DA in a fault-tolerant way using other DAs (because individual DAs can be hacked).

Privacy enhancement. This module is a *Chaumian mix* [3], used by other DAs, whose function is to hide visited DAs from home DAs and vice-versa. It is used for anonymity and untraceability as defined in [5].

5. Implementation Choices

(1) *Privacy.* Mix-nets are used to guard user privacy because, by definition, P2PWNC providers are independent and potentially untrustworthy. (2) *Offline DAs.* DAs that are offline cannot pay for their roaming users. Another DA may wish to do so though (assuming a DA coalition within the P2PWNC). (3) *Token generation.* A P2PWNC distributed bank can generate unforgeable tokens and transfer them to new DAs. (4) *DA administrative interface.* The DA software must be simple to configure. Required parameters may include a list of registered users and their credentials, the DA's Internet bandwidth, the average home and visitor load, and the average expected usage of the P2PWNC by roaming users registered with this DA. (Note that there is no incentive for a DA to register more users than necessary since, when these users are roaming, they cost tokens.)

6. Prototype

We have developed two DA nodes on Linux 2.4.21. Each has its own Peer ID and represents a different residential hotspot. Each node has two network interfaces and is connected to the Internet and to a Cisco Aironet 1200 series AP. (This access point also supports the IEEE 802.1X access control standard.) The DA's DHCP server allocates IP addresses to wireless clients from a private address range (`192.168.0.0/16`). Clients access the Internet via the DA, which performs Network Address Translation. Currently, the DA supports two client authentication methods: 802.1X-based (for clients that support 802.1X, which is standard in Windows XP); and a custom web-based login procedure (for all clients with a web browser). Both authentication methods are reasonably secure (using MD5-challenge) against eavesdropping. After authentication, the traffic-policing module initiates traffic logging and shaping. We use the `libpcap` library for traffic logging and the `tc` tool for traffic control. Currently, the policing module supports the shaping of both egress and ingress IP traffic using a hierarchical token-bucket queuing discipline. We rely either on the `iptables` firewall or the 802.1X access point to block traffic from unauthorized users.

The authentication database stores accounts that we use for testing. If a client's domain ID is not local, we use the JXTA P2P libraries to transfer the request to the home DA, where the credentials can be checked locally.

There is still much work needed on the strategy module: currently, it does not dynamically adjust prices, nor are the tokens cryptographically secure. A next step is to build a distributed public-key infrastructure, which is necessary to support all the P2PWNC cryptographic functions (mixes, secure name lookups, secure token exchanges, and secure token generation).

We are using this prototype in conjunction with simulations and an analytic model [2] in order to study the feasibility and overall stability of the P2PWNC.

References

- [1] P. Antoniadis, C. Courcoubetis, E. C. Efstathiou, G. C. Polyzos, and B. Strulo, "The Case for Peer-to-Peer Wireless LAN Consortia," IST Mob. & Wireless Summit, Portugal, 2003.
- [2] P. Antoniadis, C. Courcoubetis, E. C. Efstathiou, G. C. Polyzos, and B. Strulo, "Peer-to-Peer Wireless LAN Consortia: Economic Modeling and Architecture," to appear, 3rd IEEE International Conference on P2P Computing, Sweden, 2003.
- [3] D. Chaum, "Security without Identification: Transaction Systems to make Big Brother Obsolete," *Communications of the ACM*, vol. 28, no. 10, Feb. 1985, pp. 1030-1044.
- [4] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, "A Scalable Content-Addressable Network," SIGCOMM, San Diego, CA, 2001.
- [5] D. Samfat, R. Molva, and N. Asokan, "Anonymity and Untraceability in Mobile Networks," ACM International Conference on Mobile Computing and Networking, 1997.