The Case for Peer-to-Peer Wireless LAN Consortia*

Panayotis Antoniadis[1], Costas Courcoubetis[1], Elias C. Efstathiou[1], George C. Polyzos[1],
and Ben Strulo[2]

[1]Mobile Multimedia Laboratory
Department of Informatics
Athens University of Economics and Business
Athens 104 34, Greece
{antoniad, courcou, efstath, polyzos}@aueb.gr

[2] BTexact Technologies
Adastral Park
Martlesham Heath
Ipswich, IP5 3RE, UK
ben.strulo@bt.com

ABSTRACT

We make the case for Consortia of Peer-to-Peer (P2P) Wireless Local Area Networks (WLAN). A P2P WLAN Consortium (PWC) is a community of WLAN Administrative Domains (ADs) that offer network access to each other's registered users. The ubiquitous network access that these roaming members of an AD enjoy can compensate for their AD's cost of providing access to visitors. Existing WLAN roaming schemes utilize central authorities or bilateral contracts to control access to resources. In contrast, a PWC forms a P2P community in which participating ADs are autonomous entities. ADs make independent decisions concerning the amount of resources (e.g. access bandwidth) they contribute. As a result, similarly to existing P2P systems, a PWC will suffer from abusive behavior (free riding) if no incentive mechanisms exist to ensure that ADs offer the amount of resources that is economically justified. Flexible rules on reciprocity can be set to delimit domain policies in order to bring the system to a near-optimum equilibrium, by forcing peers to contribute in order to consume. In addition to making the case for PWC, in this paper we discuss a number of technologies and issues related to the implementation of PWC such as rule design, security and differentiated QoS in such a distributed environment.

I. INTRODUCTION

Internet services such as e-mail and the Web are, for many, more valuable than the telephone. However, Internet access is still nowhere near as ubiquitous as access to the telephone network. On the other hand many portable devices, such as smart-phones, palmtops, and tablet computers are becoming perfectly capable of handling end-to-end Internet protocols and applications. The users of these portable devices would greatly benefit from Internet access that is wireless, always on, ubiquitous, high-speed and cost-effective. However, deploying infrastructure with wide coverage to support this is a non-trivial task.

Wireless Local Area Networks (WLANs) are an important component of this infrastructure in the making. Specifically, the IEEE 802.11 WLAN standard [1] has grown steadily in popularity since its inception and is now well positioned to complement much more complex and costly technologies such as 3G (at least in metropolitan areas). This is already happening. WLAN signals already pervade many cities and WLAN cells frequently cover greater areas than was intended with their installation.

This fact, combined with how easy it is to gain access to a WLAN has drawn much attention from security experts and network administrators [2]. Successful WLAN vendors now proudly advertise the fact that their equipment can deny access to unauthorized users. However, artificially limiting network coverage or broadly denying network access is not helping to create a ubiquitous communications environment.

What we propose is an access network infrastructure that can incorporate existing and future WLANs and whose main function is to allow flexible access without compromising security. We name this infrastructure a *Peer-to-Peer WLAN Consortium* (PWC). Simply put, a PWC is a community of peer WLAN Administrative Domains (ADs) that offer network access to each other's registered users. Users roaming to other ADs within the Consortium can enjoy various services such as Internet access, intranet services and other higher-level services, thus benefiting from the community formed and, hopefully, compensating for their AD's cost of providing similar access and services to visiting members of other domains.

Existing alternative schemes like Wireless ISP (WISP) associations, e.g. *Pass-One* [3], or large WISPs, such as *Cometa Networks* [4], have similar goals with the PWC. WISP associations attempt to standardize technologies, protocols and behavior among existing WISPs in order to make WLAN roaming as seamless as possible. Cometa and other large WISPs attempt to set up new WLAN APs in areas where demand is expected to be high (hotspots) and create their own standards, usually by investing a substantial amount of capital in the process.

A distinctive characteristic of the PWC is that it allows the ADs to make independent decisions concerning the amount of resources (e.g. access bandwidth) they contribute. In that sense, PWC is a ‘pure’ P2P system, similar in principle to existing P2P file sharing applications such as Gnutella, Kazaa, etc. No central entity controls the

* This work is partly supported by EU's Fifth Framework project "Market Management of Peer-to-Peer Services" - MMAPPS (RTD No IST-2001-34201)

interaction between the peers (the ADs), which dynamically enter and leave the system having full control of their participation level in the community.

This characteristic of the PWC enables a more scalable, flexible, low-cost and economically efficient solution for global broadband wireless coverage than existing schemes. In a PWC, however, without the appropriate incentives, actions are taken by individual ADs without taking into account the costs and benefits to other ADs in the system. The result of this is, in general, inefficient usage of the system. In the most simple and extreme case, free riding is complete and each AD offers no resources (in order to minimize its cost - a decrease in the quality of the service provided to its own local customers) while consuming as much as possible of other ADs' resources. Altruism (i.e., non-self-interested behavior) can go some way to correcting this inefficiency; this may be (part of) the explanation of why existing P2P systems (such as Gnutella) operate with some degree of success even if relevant studies [5,6] indicate that the majority of participating peers in such systems are free riders. It is unlikely, however, that altruism will be sufficient to correct all of the inefficiency present in a P2P system.

So what are the appropriate mechanisms that are needed in order to give peers the correct incentives to contribute to the P2P system? In standard markets, prices provide the appropriate incentives. However in P2P systems where no global information is available (peers acquire information only by communicating with other peers), freely determined (unregulated) prices would not lead to efficient behavior. Moreover, the complexity of implementing price mechanisms involving real money in a highly distributed P2P system, in which there is no central controlling entity, motivates the search for simpler to implement incentive mechanisms. In P2P, there may be no explicit prices, but implicit ways to account for production and consumption of resources by individual peers. Specific system rules, implemented as part of the P2P software running on each agent, could be used to restrict the behavior of the peers and influence their decisions in order to achieve more efficient usage of the system.

Our approach is to use rules for influencing the behavior of the peers instead of prices. One may think of these rules as being designed and enforced by a regulator whose goal is to improve the economic efficiency of the overall system by avoiding free riding. Existing P2P file sharing applications have recently started to incorporate system-specific rules into their applications. In most cases these rules are very simple and compensating in nature. In Kazaa [7] for example, the contribution of each peer is computed and, according to its level, peers have the corresponding priority in case of congestion. We intend to extend the notion of system rules to include enforceable rules that actually constrain peers' behavior. We will experiment with different types of such rules and evaluate the corresponding equilibria of the system, as well as the possible trade-offs, using suitable economic models and simulations.

The remainder of this paper is organized as follows. In sections II and III, we motivate the PWC system and present its key design principles and high-level architecture. In section IV we discuss the implementation issues. Section V concludes the paper.

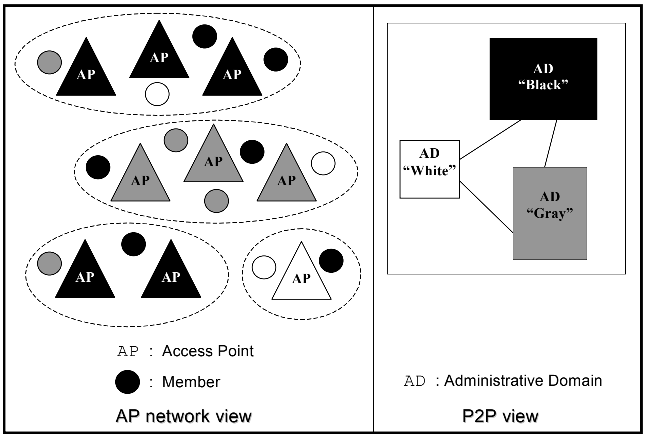

Fig. 1. A P2P WLAN Consortium consisting of three peers (ADs)*, their AP networks and their Members (indicated with the corresponding color).*

II. DEFINITIONS AND HIGH-LEVEL ARCHITECTURE

A. Definitions

A brief description of the main PWC entities follows.

WLAN Administrative Domains (ADs): WLAN ADs constitute the peers in the PWC (see fig. 1). We will use the terms 'Peer' and 'AD' interchangeably. We envisage ADs covering the full range of possible sizes. From a private residence with a home WLAN kit to a university campus with an internal network of WLAN cells and a company that offers WLAN access to employees, or even a WISP with a nationwide network.

WLAN Access Points (APs): The physical devices that offer local wireless coverage, which an AD deploys in order to cover specific geographical locations. The cells that APs form may or may not overlap.

AD Members (Users): The users interact with the PWC and consume network resources. These users should not be confused with the user-centered P2P notion of 'Peers'. A PWC peer is both a provider and a consumer of resources but these two functions are well separated, with the AD providing resources to visiting users, while its own roaming members consume the resources provided by other ADs. There is a number of ways a user can be associated with an AD: it could take place through a paying relationship (WISP case), a real-life family relationship (home WLAN), or some other arrangement (e.g. students being registered with their University's AD).

User-Agents (UAs): The client devices and associated software components that users employ to consume AD resources. These devices would probably be portable and support standard Internet protocols and applications.

B. High-Level Architecture

Figure 2 shows two administrative domains (AD1, AD2) of a PWC. In white, we represent the support modules that would exist in any typical WLAN AD, even if it wasn't participating in a PWC. These modules include the *WLAN Control module*, which manages the AP network and shapes traffic coming from, or destined to, APs (and, ultimately, UAs); and the *User Authentication module*, which checks UA credentials (certificates or username-password pairs) and then decides what services the UA is authorized to access.

In addition to WLAN-specific network services, each AD may offer other local services, represented by the *Local AD Services module*, shown here in black, as well as Internet connectivity. Examples of local services include PSTN VoIP gateways; web caches; and advanced location based services (LBS).

The PWC specific modules include the *PWC Management module*, which handles the P2P communication between ADs. This module, in our high-level architecture, implements all the P2P functionality of the system (group management, distributed accounting, rules enforcement, etc.).

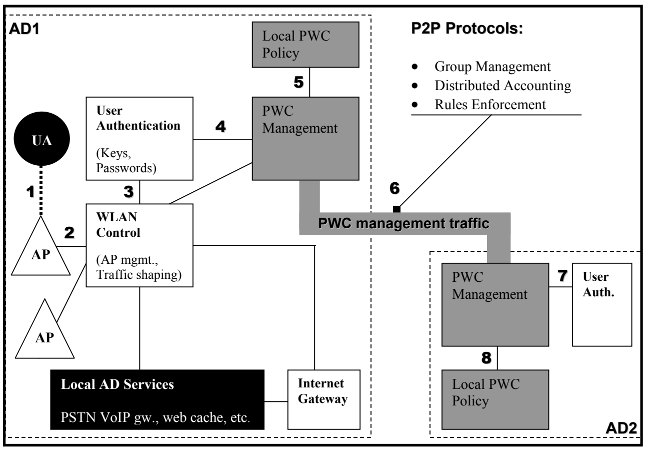

Fig. 2. P2P WLAN Consortium High-Level Architecture

The *Local PWC Policy module* encapsulates the strategy of an AD as a participant in a PWC (the amount of resources offered to visitors, the request rate allowed for its own members, etc.).

In order to demonstrate the functionality of these modules we outline the sequence of actions that will take place when a roaming member of AD2 requests Internet access from AD1. First, the member's UA sends an authentication request with the appropriate security credentials (step 1). The message is forwarded from the associated AP to the User Authentication module (steps 2, 3), where it is established that the roaming user's home domain is AD2.

After AD1 recognizes the visiting user as a member of the PWC (step 4), it checks if according to its local policy this (preliminary) request should be satisfied (step 5) and initiates a P2P transaction with the home domain (AD2) forwarding the credentials of the visiting user that requests service (step 6). Upon arrival of the message from AD1, the PWC management module in AD2 checks with its User Authentication Module (step 7) to verify membership of the roaming user and decides based on its Local PWC Policy module (step 8) whether it allows its member to consume resources in the visited AD (AD1).

If the answer is positive, AD2 will issue the 'official' P2P resource request in its member's behalf. In addition, all necessary messages that implement the P2P functionality of the system will be exchanged. Finally, distributed accounting records will be updated upon service completion.

III. THE CASE FOR P2P WLAN CONSORTIA

A. Motivation

The main novelty of the PWC is its P2P nature. We claim that when coupled with a flexible set of system rules regarding reciprocity, a PWC would be a more efficient solution than others because of:

1. *Scalability*: a PWC can achieve wide coverage, as opposed to hotspot-only coverage that WISPs offer today, since global infrastructure costs can be effectively shared among (potentially millions of) ADs and the system can be build over time, with independent and small investment decisions.

2. *Decentralization*: the PWC is designed around complete AD autonomy and AD independence from central authorities, a fact that can make the PWC more socially acceptable and economically efficient.

3. *Flexibility and low complexity*: the PWC replaces Telecom-style (or ISP) peering agreements (roaming contracts) among providing peers with more flexible arrangements. In traditional peering agreements, peers accept to serve all of each other's roaming customers, creating unbalanced situations when the roaming traffic is not symmetric. In our proposal, peers have control over the amount of resources they release to roaming customers as a result of the peering agreement. This 'managed' peering with its extra flexibility allows peers to benefit more and hence creates more motivation for participation.

4. *Economic efficiency*: the PWC would work as a regulated market (e.g., the regulator could specify the rules) instead of a free market, where certain operators might acquire strong market power (and for example raise prices for services above the socially optimal because of their strong market position). The problem of tuning the appropriate parameters faced by the regulator becomes simpler as the number of peers grows and peers belong to a small number of types.

B. Incentives for Participation

As already mentioned, the vision for the PWC is to offer ubiquitous wireless access by effectively distributing the cost amongst the large number of participating ADs. Hence, suitable incentives should be provided to peers to join the PWC, since its economic value highly depends on the number of the peers in the Consortium. The decision of joining a PWC would clearly be determined by the benefit an AD will acquire from participating and its corresponding costs for sharing resources.

In general, a peer's benefit relates to the services its members enjoy as visitors to foreign ADs and the corresponding quality of service. Quality of service is related to the probability that a visitor member's request is refused by an AD, the available access bandwidth, delay, etc.

The costs from resource sharing could be both direct and indirect. Direct are the costs that the AD itself incurs, such as a possible usage-fee to its ISP, or resources offered for higher-level services. Indirect costs are related to the impact of foreign traffic to the performance of the local traffic due to congestion.

In our system, peers are free to choose the amounts of resources offered and consumed as long as these satisfy certain constraints, dictated by the *rules* of the P2P system. By rules we mean P2P community-wide constraints on peer behavior that may replace price mechanisms or supplement them. For instance, rules may express constraints on the relation between the rate of resource availability and resource requests made by a peer, or constrain the behavior of peers who wish to join a particular group, or constrain prices that can be charged. Peers are then allowed to choose their optimal operating mode, which maximizes the net benefit they gain by participating in the Consortium. Traditional peering approaches do not offer such flexibility and reduce participation gains, resulting in limited peering. In that respect, rule design is critical for the efficient operation of the system.

IV. IMPLEMENTATION ISSUES

A. Rule Design Issues

It is important to specify an analytic model, which will lead to the determination of the range of the coefficients for the rules governing the PWC. Then, using simulation at this more abstract level, we can study the effect of the rules on the economic efficiency of the system, together with sensitivity and stability issues (note that decisions about resource provisioning and consumption are made asynchronously by each AD, and roaming traffic is random). As a next step, we can study, using a more detailed simulation, the behavior of a real PWC with a large number of ADs using rules with parameters and decision functions obtained by the analysis of the more abstract model.

The analytic model will include appropriately chosen cost and benefit functions for the ADs. These functions should take into account a number of features that characterize and differentiate ADs. Some of these features may be objective. In the case of the PWC, there are two objective differentiating characteristics of peers: (1) their *capacity* (the wireless access bandwidth or bandwidth to the Internet, depending on which is the bottleneck) and (2) their '*footprint*'. Peers with high capacity can serve a large number of customers with lower cost and better QoS. The number and geographical location of the access points that an AD shares in a PWC (the AD's footprint), affects the demand that this AD faces, and as a result the value it generates to the system. Peers that offer WLAN connectivity in remote areas offer a small amount of their resources compared to other peers, since they serve fewer requests. Nevertheless, they generate greater (per request) value and they contribute significantly to the 'ubiquitous access' target of the system.

More generally, the design of appropriate and robust rules that are easily and provably enforceable is a key open issue. These rules represent a fundamental statement of the nature of the P2P community. They must be made explicit to the peers and we expect different communities to adopt different structures of rules to attract peers. To enable this competitive playing field, we aim to provide developers with a framework in which it is easier to create the software that instantiates these rules. That support comprises three elements of functionality, a *generic service provision middleware*, a *system of local policy implementation*, and a *distributed rule enforcement system*.

B. Decision Support System for ADs

The question of whether it is (economically) beneficial for an AD to join a PWC, and, more importantly, the levels of resources that the AD should make available to the PWC might be a very complex one. Also, such issues should be answered frequently due to changing load conditions (both of local and roaming traffic). A *Decision Support System* would be beneficial here. One could imagine that such a system could be incorporated into the peer software, permitting automatic operation. Many components of this system will implement parts of the analytic model validated by simulation, as discussed earlier.

C. 'Disconnected' Operation

It is highly desirable for the scheme to be operational even when no communication is possible between the PWC management module at the AD a roaming user is visiting and that user's home AD. This would be possible if the User Agent (UA) of the member of an AD who visits another AD could 'carry' with it all the required credentials and could adequately prove its AD's identity and its good standing in the PWC (e.g. reputation, ability to 'pay', etc.).

D. Wireless Access Policy

The PWC must address the security concerns related to wireless access in order to become a realistic alternative to other WLAN schemes. A general overview of current best-practice techniques for WLAN security shows that: (1) The wireless part of the network is separated from the wired part via a firewall (see WLAN control module in fig. 2), with the wireless side considered inherently insecure. (2) Wireless stations are assigned IP addresses from a private IP range and use NAT to access the Internet and the local intranet. (3) To protect against eavesdropping, encryption is used, usually at the MAC-layer. Higher-layer encryption such as IPSEC or application-oriented TLS/SSL can also be used. (4) To be authenticated, the UA is usually required to present its credentials before or right after IP address assignment. These credentials may need to be resent at regular intervals.

The *IEEE 802.1X access control standard* [8] is most applicable in the context of WLAN and the PWC. In the IEEE 802.1X scenario, the AP acts as an authenticator, passing UA credentials to an Authentication Server (such as IETF RADIUS or DIAMETER – see User Authentication module in fig. 2), which then instructs the AP to either start or stop accepting generic layer-2 traffic from the specific UA. As an added bonus, layer-2 session encryption keys are exchanged during the authentication procedure.

For the purposes of the PWC we can assume that the visiting users will present as credentials either a username-password pair that is applicable to their AD, or a digital certificate signed by their AD (in keeping with the P2P philosophy of the PWC, we should avoid external or centralized certificate authorities).

Assuming a basic level of trust within the P2P network, server-to-server communication can happen securely as part of the PWC management exchanges (see fig. 2). The two authentication servers will recognize each other as part of the same Consortium. If the visitors are successfully authenticated by their home AD, it will communicate this information back to the visited AD. The visited AD, having all the information it requires, can decide (based on local policy, previous interactions with the home AD, token exchanges etc.) whether or not to grant access to the visitors.

E. Differentiated QoS

Using a simplified model of a PWC AD, the three basic resources an AD offers are: (1) wireless connectivity, (2) access to the wired network, and (3) access to local AD services. All these resources have their own notion of quality. For certain resources, control over offered quality levels is relatively straightforward. For others (wireless bandwidth), it is impossible to achieve with today's standard components.

Although various approaches to service differentiation could be very dissimilar, the PWC P2P software could theoretically offer a generic-enough abstraction of offered QoS, which could map to an application specific mechanism that would eventually be called whenever the AD decides to discriminate between visiting users.

For example, a very basic mechanism (potentially of limited effectiveness) for an AD to control the resources it makes available to the PWC would be to do admission control at the level of visiting members of foreign ADs. However, a finer, probably more effective and certainly more economically efficient solution would be to offer full *DiffServ* based service with appropriate parameters. By utilizing the upcoming IEEE 802.11e standard, wireless QoS will also be achievable.

F. Prototype Implementation

Our prototype implementation is based on reusing and extending parts of the 802.1X standard for port-based network access control, the IETF DIAMETER standard for authentication, and the Sun JXTA project for P2P protocols. We are currently focusing on ADs with only one AP. We have built a prototype PWC peer based on Linux that: (1) acts as a 802.1X port-based access controller for client devices in the wireless part of the network, (2) communicates with a co-located authentication server for checking user credentials and (3) connects to a P2P network consisting of other PWC peers in order to exchange PWC information and dynamically tune its local access policy. Currently, visiting members prove their identity using stored digital certificates signed by their home AD. We assume basic trust for identification purposes within the P2P network so that each AD can accept another AD's certificate as valid. These initial decisions should be investigated, evaluated and extended in future work.

V. CONCLUSION

We have introduced the concept of a Peer-to-Peer Wireless LAN Consortium. We motivated its existence and described its high-level architecture. We also discussed a number of important implementation issues that need to be investigated and resolved in order to design practical and efficient consortia.

REFERENCES

[1] IEEE Std 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications", ISO/IEC 8802-11:1999(E), 1999.

[2] S. Fluhrer, I. Martin, and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", in Proceedings of the 8th Annual Workshop on Selected Areas in Cryptography, 2001.

[3] Pass-One. http://www.pass-one.com.

[4] Cometa Networks. http://www.cometanetworks.com.

[5] E. Adar and B.A. Huberman, "Free Riding on Gnutella", First Monday, 5(10), 2000.

[6] S. Saroiu, P.K. Gummadi, and S.D. Gribble, "A Measurement Study of P2P File Sharing Systems", in Proceedings of Multimedia Conferencing and Networking, San Jose, 2002.

[7] Kazaa. http://www.kazaa.com.

[8] IEEE Std 802.1X, "Port-Based Network Access Control", PDF: ISBN 0-7381-2927-5, 2001.