Building Secure Media Applications over Wireless Community Networks

E. C. Efstathiou, F. A. Elianos, P. A. Frangoudis, V. P. Kemerlis, D. C. Paraskevaidis, G. C. Polyzos, E. C. Stefanis
Mobile Multimedia Laboratory, Department of Computer Science
Athens University of Economics and Business
Patision 76
Athens
Greece
efstath@aueb.gr, elianos@cs.aueb.gr, pfrag@aueb.gr, vpk@cs.aueb.gr, dcp@aueb.gr, polyzos@aueb.gr, leste@aueb.gr

Abstract

We present the design and implementation of a fully decentralized P2PWNC (Peer-to-Peer Wireless Network Confederation) WLAN roaming architecture, enhancing previously published work. We present a proof-of-concept secure VoIP application that is built on top of the existing P2PWNC infrastructure and can provide a low-cost substitute to GSM service. We also augment the P2PWNC scheme with a set of locally accessible, differentially charged multimedia and location-based services, offered by WCN participants that operate P2PWNC-enabled access points (APs).

Keywords

P2PWNC, WLAN, VoIP, community networks, location-based services

1. Introduction

We propose to harness the under-utilized resources of residential Wireless LAN (WLAN) access points via an incentive-aware fully decentralized scheme. We have designed and implemented a system for bandwidth sharing based on service reciprocity – only WLAN owners that share their bandwidth with passersby may consume bandwidth when they themselves are mobile. We call the proposed scheme the *Peer-to-peer Wireless Network Confederation (P2PWNC).* At its heart lies a *reciprocity algorithm* whose input is the system's history of prior service provisions and its role is to identify *free-riders* and to exclude them from service, providing users the incentive to share their Internet connections using their home WLAN.

We target at deploying our scheme over existing Wireless Community Networks (WCNs), such as Seattle Wireless [1] or the Athens Wireless Metropolitan Network [2]. WCNs are wide-area networks whose nodes are interconnected using low-cost WLAN equipment. Usually, these networks offer citywide, but spotty, coverage, and their nodes are managed by volunteering WLAN enthusiasts. As extensive

simulations presented in [3] show, the P2PWNC scheme can stimulate participation in WCNs and sustain reciprocal cooperation between community members.

The proposed mechanism is compatible with the distinctive nature of WCNs; it does not require registration with central authorities and relies only on *uncertified*, free identities. The real world identities of the scheme's users are protected and free, anonymous WLAN roaming can be achieved.

The contributions of this paper are the following: First, we present the design and implementation of the fully decentralized P2PWNC WLAN roaming architecture, enhancing previously published work [3] to make it Quality-of-Service-aware. Our work in [3] extends the centralized design presented in [4]. Second, as a proof of concept, we present a secure VoIP application that is built on top of the existing P2PWNC infrastructure and can, under some circumstances, provide a low-cost substitute to GSM. Finally, we propose an augmented scheme, where a set of locally accessible, differentially charged multimedia-oriented and location-based services is offered by WCN participants operating P2PWNC-enabled access points (APs).

2. System Architecture

In the P2PWNC scheme, users are organized into small teams (of a few tens of members). Teams manage and operate a number of WLAN access points connected to Cable/DSL links at locations throughout the city. A team is a service provider and a consumer at the same time; it provides service via its own access points, and it consumes when its members visit foreign WCN-controlled access points.

Each team is identified by an uncertified public-secret key pair. The team founder can recruit team members by issuing a public-secret key pair and a *member certificate* for each one of them. In the proposed scheme, full distrust between peers (teams) is assumed. On the other hand, we assume that team members know and trust each other. Unlike our prior approach [4], no Trusted Central Authority (TCA) for issuing peer identities and managing the history of the system is assumed. Instead, it has been replaced by team-local modules who maintain a *private* history of the system [3].

Each time service provision takes place, a digital *receipt* is generated. The receipt is signed by the consuming roamer using his secret key and has the following format:

$$\{\text{Consumer cert., Providing team public key, Timestamp, Receipt weight}\}_{\text{consumer signature}}$$

The timestamp represents the time a session between a mobile user and an AP started, and the weight field indicates the amount of traffic forwarded by the AP on behalf of the consumer.

Receipts are the service accounting unit of the P2PWNC scheme. They represent the history of prior transactions between peers. Receipts form a directed graph, whose vertices are P2PWNC teams and whose edges represent service provision. They are directed from a consuming to a providing team and encode an 'I owe you' relationship. In the fully decentralized scenario under consideration, receipts are stored in team-local repositories.

The receipt graph formed is used as input to the *reciprocity algorithm.* The reciprocity algorithm outputs whether or not a roamer requesting service from a potentially providing team deserves to be served, according to the history of prior

transactions. It identifies contributing teams using network flow techniques [3, 4]. The objective of our reciprocity algorithm is to encourage teams to match their consumption with at least an equal amount of contribution (measured in volume of foreign traffic that APs relay).

A WLAN session between a roamer and a service providing AP is controlled by a simple ASCII-based protocol. As soon as a roamer requests access by a potential provider, the latter consults its team-local repository to judge whether access should be granted. If the reply is positive, the client is admitted. During this session, the AP periodically requests receipts so that a consumer acknowledges the service she has enjoyed thus far. As a side effect, it is ensured that the session has not been hijacked, since a receipt can be generated only using the consumer's secret key.

Since our scheme does not depend on a central receipt repository, a *gossiping* protocol [3] has been employed, to assist in receipt dissemination. Without such a protocol, each team-local repository would have a limited view of the system's history.

As an extension to the P2PWNC protocol specified in [3], an additional traffic control service module has been implemented. Its role is to perform traffic shaping and QoS operations on the P2PWNC access point. Taking the result of the reciprocity algorithm into account, the AP can instruct (via a special protocol message) the traffic control module to offer different portions of the available bandwidth to wireless users.

3. Securing Applications over the P2PWNC Infrastructure

In our extended architecture, we require that roamers tunnel all their traffic to a trusted VPN gateway located at their home network. The VPN gateway is embedded on one of the access points of the visitor's team. This way, the visitor does not have to dedicate a separate PC to act as the VPN gateway. By tunneling his traffic to his home network, a roamer is protected from eavesdropping on the wireless link on the visited network. In addition, since all traffic is encrypted, the untrusted visited access point cannot spy on the traffic that it forwards on behalf of the roamer.

In the following, we describe the operation of the VoIP application under consideration (see Figure 1). Wireless Client W1 initiates a call to Wireless Client W2, and we assume that both are currently visiting WCN-controlled P2PWNC APs. In order to access the Internet, visitors establish P2PWNC protocol sessions with the visited APs and tunnel all internet traffic to their home VPN gateways. Call initiation takes place using a GSM SMS. The caller (W1) notifies the callee (W2) of her public IP address (the public IP of W1's home VPN gateway) and the callee, being within range of a P2PWNC-enabled access point, completes the call over the Internet.

4. Extending the Scheme with Local Content Services

4.1 Content services

So far, we exclusively focused on the provision of free Internet access to mobile users through WCN-controlled WLAN APs. We now aim to enhance the P2PWNC scheme with *content services* delivered on top of the existing P2PWNC infrastructure.

We envisage an augmented wireless confederation scheme in which mobile users

will be able to choose among a set of services, locally offered by the visited WLAN operators. This set of services will be mainly multimedia-oriented and location-based and will be accessible only to roaming visitors over the local wireless link. The main purpose of these services will be to entertain and inform visitors.

For example, we expect that services such as live multimedia streaming or *podcasting* will be popular among visitors. What is more, WLANs can provide directories of nearby venues such as cinemas and restaurants to passersby.

Unlike the existing scheme, in which accounting is based solely on the amount of traffic forwarded by the visited WLAN access point on behalf of a roamer, in the augmented version of P2PWNC *content services* will also come at a price.

4.2 Accounting scheme

The P2PWNC receipt-based accounting scheme is not modified. The digital receipt format, as well as the reciprocity algorithm remain unchanged. Since the only accounting unit used in P2PWNC is the receipt, an AP will differentially price its services by requesting receipts with an increased weight compared to the weight they would have had if the receipts represented Internet bandwidth consumption or some other less expensive service. To elaborate, P2PWNC accounting is still based on the visitors' traffic, as is the case in the typical P2PWNC scenario. However, the traffic 'weight' associated with a service will be multiplied by a respective factor. This factor represents how much more (or less) expensive a service is compared to the basic P2PWNC Internet access service.

Respecting the autonomous and self-organizing spirit of WCNs, the system will leave the decision on how much each service should be charged to the WLAN access point operator.

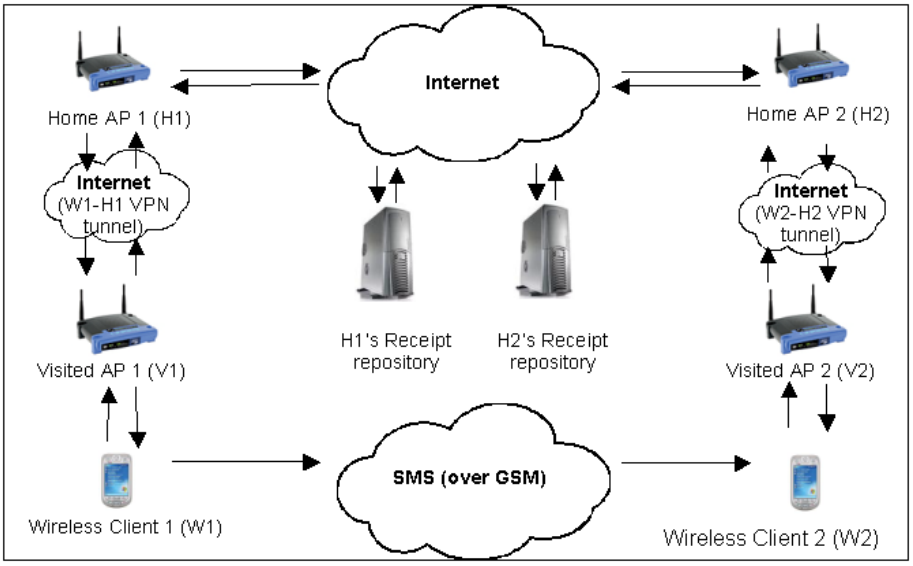

Figure 1: Setup for a P2PWNC-based VoIP call initiated by W1.

4.3 Augmented P2PWNC architecture

Since a new set of services will be offered at the edges of the P2PWNC infrastructure (i.e., over the wireless links that connect APs and roamers), additional software is required in the AP and mobile user modules. The AP needs to be equipped with a *service charging* module, which will provide service cost information. Suitable user interfaces should facilitate easy service configuration on behalf of the hotspot operator and easy subscription on behalf of the mobile user. As soon as the P2PWNC protocol handshake has been carried out successfully, the AP will inform the mobile user of the available services and their charges. After the mobile user has subscribed to a service, her request will be handled by a *content services module*. The augmented P2PWNC hotspot architecture is shown in Figure 2.

4.4 Incentives for participation

The first thing that should be noted concerning the proposed enhancements to the basic P2PWNC architecture is the fact that local content services are considered cheap in terms of WLAN resources, since they are only offered locally over the wireless link. We assume, on the other hand, that it is costly for residential WLAN owners to share their DSL/Cable bandwidth, which is the case when they offer Internet access to visitors. Thus, a contributing team has an incentive to offer content services to visitors, since, without wasting wired bandwidth, 'precious' receipts are earned, which in turn give the team's members more chances of obtaining free Internet access and content services from other teams.

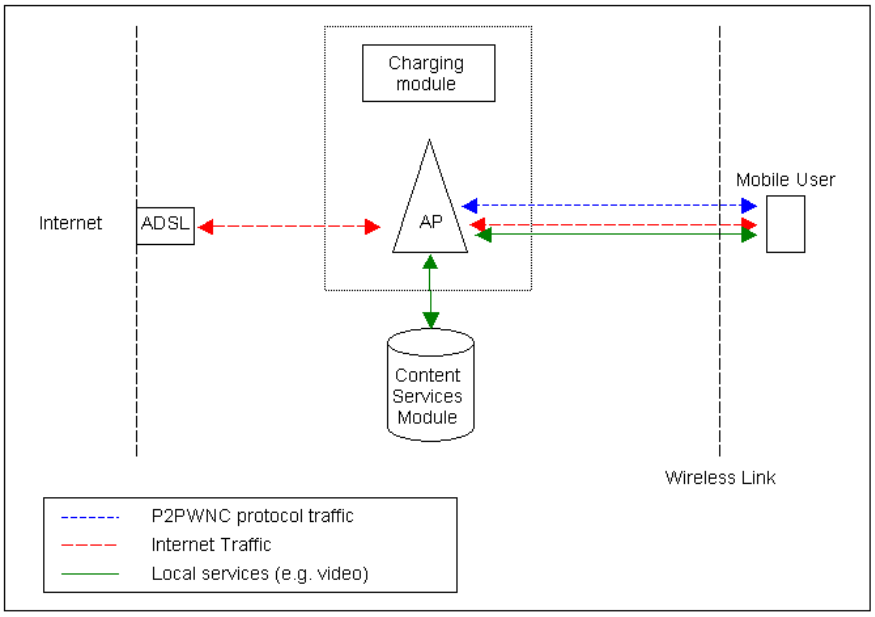

Figure 2: Augmented P2PWNC hotspot architecture.

5. Current Status

Our reference implementation of the P2PWNC protocol, on the AP side, runs on top of Linux-based embedded wireless routers (Linksys WRT54GS). On the mobile user end, there is a C implementation that runs on Linux, as well as a Windows Mobile version, targeting devices such as PDAs and smart-phones. There is also a P2PWNC Java API, which has been used in implementing the client and the receipt repository modules. We have also implemented, tested and demonstrated the novel secure VoIP application that was described in Section 3. These tests proved that cheap and constrained WLAN devices, such as embedded wireless routers can efficiently support P2PWNC protocol operations and tunneling tasks. Our software is open source and it is available for download from our project website at http://mm.aueb.gr/research/P2PWNC.

6. Related Work and Conclusion

The notion of taking advantage of residential WLAN APs is not new. Certain next generation network operators [5] propose agreements with household hotspot owners to provide WLAN access to visitors. AP owners try to make a profit by sharing their Internet connection, to compensate for maintaining their DSL/WLAN connections. The network operator mediates between visitors and hotspot owners, taking care of billing. Such centralized solutions suffer from management complexity issues and the overhead, due to legal and economic issues, may discourage residential hotspot owners. A similar approach to P2PWNC, FON [5], has recently appeared and has attracted much attention. This scheme attempts to encourage AP owners to share their connections with the promise of freely being served when they roam. Also, in a future version, they claim that they will provide the option of making a profit by sharing one's Internet connection, in a similar manner to [5]. FON is also centralized and is expected to face the same problems as [5]. What is more, it is still in the early days of its development, and it seems that little has been done as far as incentive mechanisms and cheat-proof accounting is concerned. Centralized solutions, also, by nature, lack the privacy guarantees of fully distributed schemes that support *free* user identities.

References

[1] Seattle Wireless. http://www.seattlewireless.net
[2] Athens Wireless Metropolitan Network. http://www.awmn.net
[3] E.C. Efstathiou, P.A. Frangoudis, and G. C. Polyzos, "Stimulating Participation in Wireless Community Networks," IEEE INFOCOM 2006, Barcelona, Spain, 2006.
[4] P.A. Frangoudis, E.C. Efstathiou, and G.C. Polyzos, "Reducing Management Complexity through pure Exchange Economies: A Prototype System for Next Generation Wireless/Mobile Network Operators," 12th Annual Workshop of the HP OpenView University Association (HPOVUA), Porto, Portugal, 2005.
[5] Speakeasy WiFi NetShare Service. http://www.speakeasy.net/netshare/
[6] FON. http://en.fon.com/