The Peer-to-Peer Wireless Network Confederation Scheme

Elias C. Efstathiou, Fotios A. Elianos, Pantelis A. Frangoudis, Vasileios P. Kemerlis
Dimitrios C. Paraskevaidis, George C. Polyzos, Eleftherios C. Stefanis

Mobile Multimedia Laboratory
Department of Computer Science
Athens University of Economics and Business
Athens 104 34, 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*—In metropolitan areas, public infrastructures for high-speed wireless networking can be built through the private contributions of individual "micro-operators" who use their Internet-connected Wireless LANs (WLANs) to forward foreign traffic from and to nearby low-mobility clients. We have designed a practical WLAN aggregation scheme that (1) assumes that micro-operators are selfish and do not trust each other and uses a secure incentive technique to encourage their contribution; (2) protects the real-world identities of micro-operators and clients by relying only on disposable opaque identifiers (public keys); (3) is fully distributed, open to all, and does not rely on any authority to resolve disputes or to control membership; (4) is automated, using standard hardware and software we developed for some of the main available platforms (Linux-based WLAN access points and Windows Mobile-based cell phones).**

I. Introduction

The *Peer-to-Peer Wireless Network Confederation* (P2PWNC) protocol is the basis of an incentive technique that can stimulate participation in Wireless Community Networks (WCNs) and increase the wireless coverage that these networks offer. WCNs are citywide wireless networks whose nodes are owned and managed by volunteers. Successful WCNs in terms of coverage area and number of participants include *Seattle Wireless* [1], *NYCwireless* [2], and the *Athens Wireless Metropolitan Network* [3].

The main WCN service of interest to us is the provision of wireless Internet access to pedestrian users through WCN-controlled WLAN access points (APs). If such a service were commonplace, WCNs could complement cellular networks in metropolitan areas. This is important because WLAN-enabled cell phones are now available [4]. WCNs could also rival in coverage similar centrally managed WLAN schemes, such as *Wireless Philadelphia* [5].

II. Distinctive Characteristics and Prior Work

We presented the design of P2PWNC before in [6], [7]. Our first implementation results appear in the INFOCOM 2006 paper [8]. The P2PWNC website is at [9]. In [10], we give the full specification of the P2PWNC protocol, along with performance measurements of our implementation, whose AP-side runs on the Linux-based Linksys WRT54G AP [11] (an AP that is commonly used in WCNs).

References [6], [7] describe a basic reciprocity algorithm that encourages cooperation among selfish micro-operators by tying consumption to contribution. The algorithm has the following distinctive characteristics. First, it does not rely on authorities that certify identities, that is, identities in P2PWNC are free and the system is open to all. Free identities are an important characteristic that is compatible with the distinctive structure of WCNs. A WCN rarely relies on an authority that all participants can trust; instead, WCNs grow organically and largely uncoordinated. Second, the reciprocity algorithm does not rely on tamperproof modules, and we assume that participants can reprogram the software that implements the algorithm if it is in their interest. In [8] we also extend the algorithm of [6], [7] to cover collusion-based attacks, and we present a centralized version of P2PWNC (with minimal demands on the center) that could be practical for certain WCNs.

The P2PWNC protocol is simple to implement and the growth of underutilized WLANs in urban areas makes it relevant. The idea of organizing WCNs as peer-to-peer exchange economies is novel. We believe P2PWNC can achieve its basic goal, which is to stimulate participation in WCNs while respecting their open and self-organized nature.

III. Scheme Overview

The P2PWNC scheme works as follows. We assume that WCN participants divide into *teams* of a few *members* each. Members of the same team must know and trust each other.

Teams own and manage a number of *APs*, which we assume are connected to Cable/DSL links, at locations throughout the city. We say that Team A *consumes* when a member of Team A accesses the Internet through an AP of another Team B, and *contributes* when a member of another team uses an AP of Team A. Our reciprocity algorithm encourages teams to match their consumption with approximately an equal amount of contribution (measured in volume of foreign traffic that APs relay). Teams that contribute less than they consume will find it hard to obtain service. And only short-term history counts: teams must contribute continuously in order to consume continuously.

Members sign digital *receipts* when they consume service. The receipts form a logical *receipt graph*, which is used as input to a *reciprocity algorithm* that identifies contributing teams using *network flow* techniques. Our reciprocity algorithm computes *maximum flows* on the graph, and our extended reciprocity algorithm [8] computes *generalized maximum flows*. Simulations show that our algorithm can sustain reciprocal cooperation. P2PWNC receipts are stored either in a *central receipt repository* or they are distributed among multiple *team servers* with the help of a *gossiping protocol*.

All member and team IDs are unique public/private key pairs. We do not rely on PKI (Public Key Infrastructure) and *member certificates* are issued by the team itself. These certificates allow team members to consume in the name of their team; member IDs are meaningless to other teams.

IV. Demo Specifics

In the demo (see also Fig. 1 below) we show the P2PWNC protocol in operation. We include a total of 4 Linux WLAN APs. These 4 APs play the role of 2 *visited* APs and 2 *home* APs. The visited APs, V1 and V2, correspond to two different WCN locations. A WLAN-enabled cell phone (the QTEK 9100), W1, is in the area covered by V1 and initiates the P2PWNC message exchange with V1. These messages include a *CONN* request, followed by a positive or negative *CACK*. Then, assuming the connection request succeeds (this depends on the outcome of the reciprocity algorithm), a series of *RREQ* requests from V1 start, followed by *RCPT* responses from W1. These correspond to receipts being generated (see [10] for details). In order for V1 to decide if W1 is allowed to access V1, V1 consults a central receipt repository hosted on a standard PC. This corresponds to the *centralized mode* [8] of P2PWNC operation.

Then, W1 opens a VPN tunnel to its home AP, H1, and uses it to tunnel all its Internet traffic. This way, the wireless part of the connection is secured against eavesdropping attacks and W1's traffic is secured against the untrusted visited AP V1 that may want to eavesdrop on the foreign traffic it relays. To spare users the need for a separate VPN gateway at home, we have included this functionality on the Linux AP that the user is already supposed to own to participate in P2PWNC (here, H1).

The PC hosting the central receipt repository also visualizes the internal workings of the graph-based reciprocity algorithm. Moreover, depending on the outcome of the algorithm, and because we also support QoS control at V1, W1 will be allocated an amount of WLAN/Internet bandwidth that depends on its team's contribution. We can emulate additional APs and clients and we can change the receipt graph at will to better present our demo scenarios.

Finally, an advanced service is presented. We have implemented an innovative VoIP application that is compatible with the decentralized nature of WCNs: we will show two cell phone users, W1 and W2, with WLAN-enabled phones, visiting V1 and V2 respectively. In order to communicate, the caller, W1, sends an SMS message over GSM that notifies the callee of the caller's current public IP address (which corresponds to the remote side of the aforementioned bi-directional tunnel that connects W1 to H1). This way, a VoIP call is established without relying on SIP/H.323 registrars or other VoIP directories. We simply assume that the caller knows the callee's phone number.

V. Conclusion

Today's WLAN-enabled cell phones and low-cost APs can: (1) support our P2PWNC reciprocity protocol; (2) be used to establish secure VPN tunnels; and (3) provide a low-cost and secure substitute to 2G and 3G cellular services. P2PWNC is designed to provide cooperation incentives to participating micro-operators, and also uses QoS levels as an additional incentive. Because the necessary hardware and software is available today, Wireless Community Networks—enhanced with P2PWNC incentive techniques—can provide reliable low-cost Internet and VoIP services, complementing cellular networks in urban areas where many private WLANs are already operational.

References

[1] http://www.seattlewireless.net
[2] http://www.nycwireless.net
[3] http://www.awmn.net
[4] QTEK 9100 Pocket PC Phone Edition, WLAN-enabled. http://www.qtek.nu/europe/products/9100.aspx
[5] http://www.phila.gov/wireless
[6] E. C. Efstathiou and G. C. Polyzos, "Self-Organized Peering of Wireless LAN Hotspots," *European Transactions on Telecommunications*, vol. 16, no. 5 (special issue on Self-Organization in Mobile Networking), Sept./Oct. 2005.
[7] E. C. Efstathiou and G. C. Polyzos, "A Self-Managed Scheme for Free Citywide Wi-Fi," IEEE WoWMoM international workshop on Autonomic Communications and Computing, Giardini Naxos, Italy, June 13, 2005.
[8] E. C. Efstathiou, P. A. Frangoudis, and G. C. Polyzos, "Stimulating Participation in Wireless Community Networks," IEEE INFOCOM 2006, Barcelona, Spain, April 23-29, 2006, in press. Preliminary version available at [9].
[9] http://mm.aueb.gr/research/P2PWNC
[10] P. A. Frangoudis, "The Peer-to-Peer Wireless Network Confederation Protocol: Design Specification and Performance Analysis," Technical Report 2005-MMLAB-TR-02, Mobile Multimedia Lab, at: http://mm.aueb.gr/technicalreports
[11] http://en.wikipedia.org/wiki/WRT54G

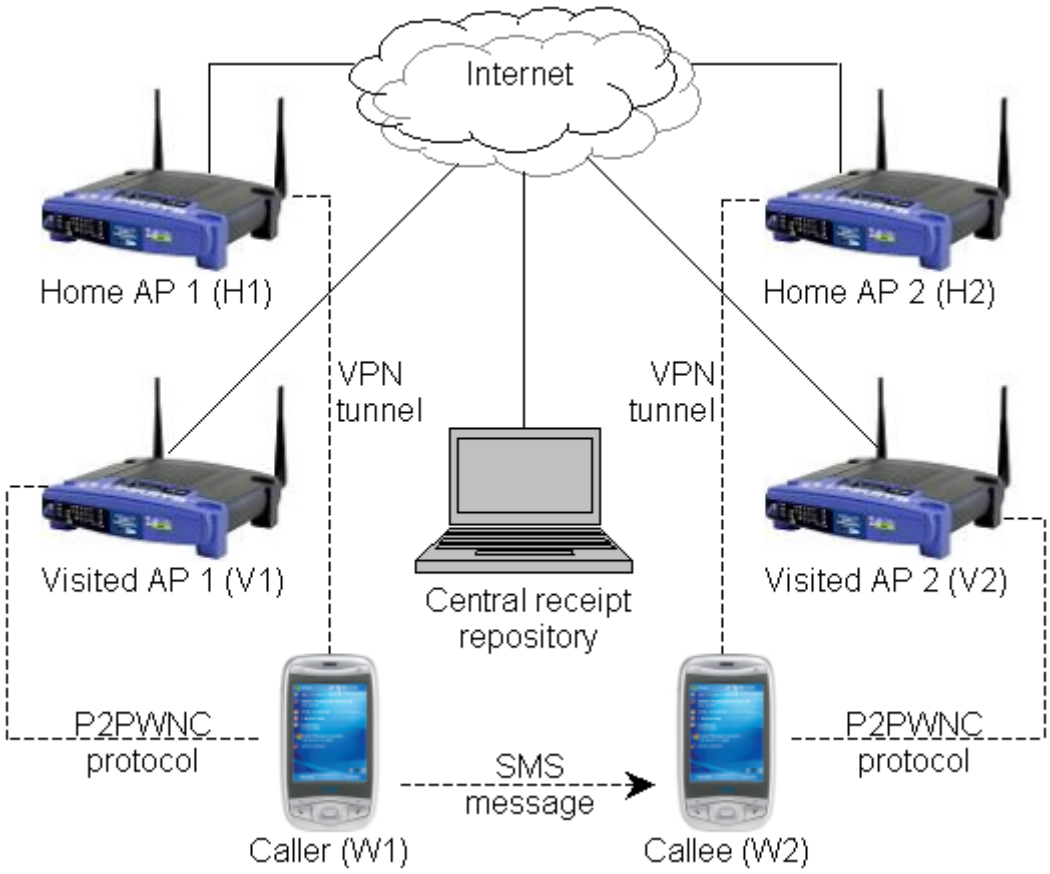

Fig. 1. Setup for a P2PWNC-based VoIP call initiated by W1.