Demo Proposal

The Peer-to-Peer Wireless Network Confederation Scheme: Protocol, Algorithms, and Services

Elias C. Efstathiou, 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, pfrag@aueb.gr, b.kemerlis@ccslab.aueb.gr
dcp@aueb.gr, polyzos@aueb.gr, leste@aueb.gr

1. Introduction

The *Peer-to-Peer Wireless Network Confederation* (P2PWNC) protocol is the basis of an incentive scheme that can stimulate participation in *Wireless Community Networks* (WCNs) and, therefore, help 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 wireless coverage and number of active 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 free wireless Internet access to pedestrian users through WCN-controlled wireless LAN access points (WLAN APs). If this service were to become commonplace, WCNs would complement 2G/3G cellular networks in metropolitan areas, especially now that WLAN-enabled mobile phones are available [4], [5]. Ideally, the level of WCN service could rival that of similar centrally-administered schemes such as the proposed *Wireless Philadelphia* project [6].

P2PWNC relies on *indirect reciprocity*: WCN participants provide Internet access to pedestrian users through the (Internet-connected) APs that these participants own, but only if the users can prove that they extend the same courtesy to other WCN participants. The main problem in a P2PWNC-enabled WCN (now essentially a peer-to-peer resource-sharing system) is how to discourage *free-riders* who prefer to consume service without offering anything back to the community. If we assume that all users are rational and self-interested, an incentive scheme that encourages active participation is required if a WCN is to function at all. Even though some users are altruistic (the success of WCNs so far proves this), more active participants could help WCNs rival commercial networks in terms of coverage and robustness.

2. Distinctive Characteristics and Prior Work

We have presented the P2PWNC scheme before in [7], [8], [9]. The P2PWNC website can be found at [10]. Older P2PWNC papers that present the core idea and a P2PWNC economic model include [11], [12], [13]. In [14], the full specification of the P2PWNC protocol is given, along with a performance analysis of our reference implementation, whose server-side runs on the Linux-based *Linksys WRT54GS* AP (a WLAN AP that is commonly used in WCNs).

References [7] and [8] describe a basic P2PWNC reciprocity algorithm that has the following distinctive characteristics: First, it does not rely on authorities that certify peer identities, i.e. peer pseudonyms in P2PWNC are *cheap*, and the system is open to all. (Cheap pseudonyms are an important P2PWNC characteristic that is compatible with the distinctive structure of WCNs. A WCN rarely has a powerful coordinating authority that every participant can trust; instead, WCN growth is organic and largely uncoordinated, following the growth pattern of similar decentralized systems such as the Internet and the Web, albeit at a smaller scale.) Second, the P2PWNC algorithms do not rely on tamperproof

modules and we assume that participants can reprogram the (client and server) software that implements the P2PWNC algorithms if it is in their interest.

In [9] we extend the P2PWNC algorithms of [7], [8] to cover collusion-based attacks and we also 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 underexploited WLANs in cities makes it relevant today. The idea of implementing a self-organized exchange economy within WCNs 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.

3. Scheme Overview

The P2PWNC scheme works as follows. We assume that WCN participants divide into *teams* of a few tens of *members* each. Members of the same team must know and trust each other. This is not an unreasonable assumption: WCN participants are commonly organized around smaller subgroups. Teams own and manage a number of *APs* (WLAN access points, 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 the AP of another Team B, and *contributes* when a member of a team other than Team A uses an AP of Team A. 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). Free-riding teams that contribute much less than they consume will find it hard to obtain service. And only short-term history is important: teams must contribute continuously in order to be able to consume continuously.

Members sign digital *receipts* when they consume service from another team. The receipts form a logical *receipt graph*, which is used as input to a *reciprocity algorithm* that identifies contributing teams using *network flow* techniques (more specifically, our reciprocity algorithm relies on the *maximum flow* graph algorithm, and the extended reciprocity algorithm [9] relies on a custom *generalized maximum flow* [15] algorithm). Simulations show that this algorithm can sustain reciprocal cooperation. Receipts are stored either in a *central server* or they are distributed among multiple *team servers* with the help of a *gossiping protocol.*

The receipt graph may contain fake receipts, the result of collusion among two or more teams, or of a Sybil attack [16] (the creation of multiple identities per entity). All member IDs and team IDs are unique public/private key pairs. We assume that it is computationally infeasible to break the digital signature scheme used to sign receipts and *member certificates.* We do not rely on a Public Key Infrastructure: member certificates are issued by the team itself and allow its members to consume in the name of the team; member IDs are meaningless to other teams.

4. Demo Specifics

In the proposed demo (see also figure below) we intend to show the P2PWNC protocol in operation. We will include a total of 4 Linksys WRT54GS APs. These 4 APs will play the role of two *visited* APs and two *home* APs. The visited APs, call them V1 and V2, will correspond to two different WCN locations. A mobile client will approach V1 and initiate the P2PWNC exchange of messages. These messages include the initial CONN request, followed by positive or negative CACK, and then, if the request is successful, a series of RREQ/RCPT queries for receipts and responses will follow, which correspond to WLAN session receipts being generated – see [14] for more details on the specifics of P2PWNC protocol messages. In order for V1 to decide if the mobile user is allowed to access V1 (according to the maxflow and generalized maxflow reciprocity algorithms, see [9]), V1 will consult a central receipt repository. This repository will be hosted on a standard PC. This corresponds to the centralized mode of P2PWNC operation, which is easier to demonstrate compared to decentralized mode (see [9] and [14] for details comparing the two modes of operation, as well as listing the advantages and disadvantages of each mode).

Then, we will demonstrate how the mobile client opens and maintains a secure tunnel to its home AP, call it H1, and uses this to tunnel all its Internet traffic. This way, we will demonstrate how the wireless part of the connection is secured against eavesdropping attacks and against potentially malicious visited APs that may want to eavesdrop on the traffic they relay. The disadvantage here is that this type

of tunnel that the mobile clients use causes inefficient routing. However, this represents a tradeoff between privacy and efficiency. To spare WCN users the need for a separate security server at home, acting as tunnel endpoint, we have programmed this functionality on top of the standard P2PWNC-enabled Linksys WRT54GS (here, H1). Please see [9] for more details.

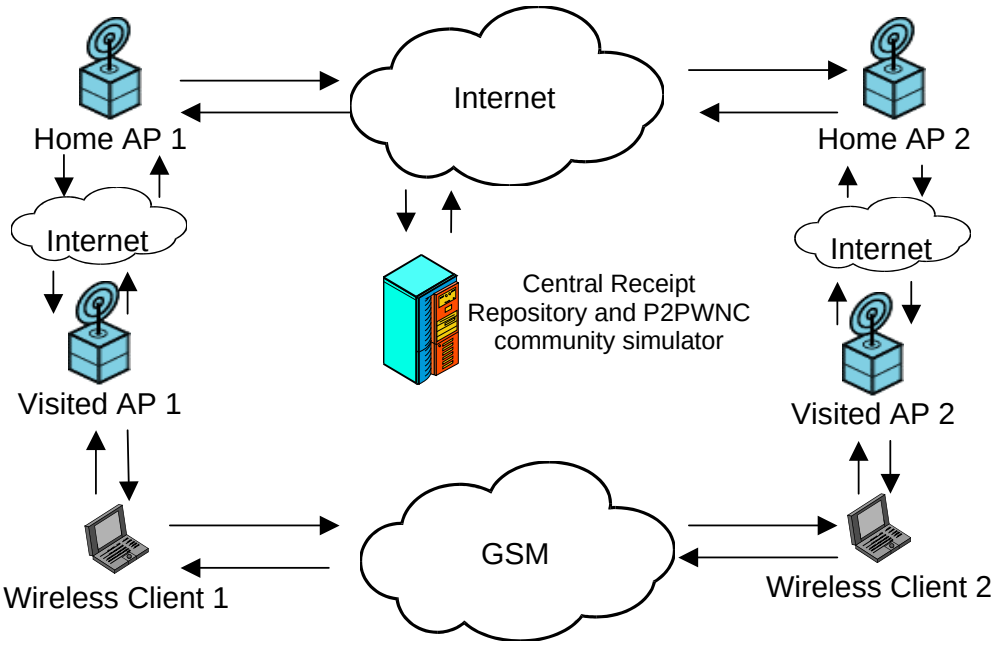
At the same time, a standard PC (the one hosting the central receipt repository) will graphically display the internal workings of the P2PWNC reciprocity algorithms whenever they are executed, alongside a view of the current state of the receipt graph. We intend to show both successful and unsuccessful login attempts by clients. In certain versions of the reciprocity algorithm, the result will not simply be a decision of whether or not V1 should provide WLAN/Internet service, but also *how much* service to provide: i.e., QoS at V1 will be enabled and a visitor will experience different WLAN/Internet speeds depending on the result of the reciprocity algorithm on the current state of the receipt graph.

The standard PC hosting the repository will also simulate a number of additional APs and mobile users (which would have been impractical to physically include in the demo) so that the receipt graph can evolve in a more-or-less realistic way. We will also have the option to manually update the receipt graph with receipts of our choosing in order to demonstrate successful and unsuccessful runs of the algorithm.

The main lesson from this demo would be to understand that the Linksys AP platform (and other similar ones) is more than adequate to host our proposed protocol and algorithms, and to handle the tunneling tasks that would make a P2PWNC/WCN-based roaming solution secure.

To complete the demonstration, one or more advanced P2PWNC services other than basic Internet access will be presented. An innovative voice-over-IP (VoIP) application that we have designed respects the decentralized organization of P2PWNC: we will show two users with WLAN-enabled smartphones that are visiting V1 and V2 respectively. In order to communicate using the WCN system they will first exchange a protocol message over standard SMS/GSM, which will notify the callee's home APs about the caller's current public IP address (which actually corresponds to the aforementioned bidirectional tunnel endpoint that is used by the mobile client). This way, a "VoIP rendezvous" can be completed without having to resort to central directories, SIP registrars, etc. The interface of the WLAN/P2PWNC-enabled smartphone (running Windows Mobile) will allow the caller to use standard telephone numbers to find the callee, but when the callee is within the range of P2PWNC WLAN (e.g. visiting V2 at the time, see figure), the P2PWNC/WCN system will be used to complete the (now VoIP) call, instead of GSM.

The demo is designed to prove that, using today's technologies, an innovative set of distributed applications can be built on top of the basic P2PWNC reciprocity platform, and that the reciprocity scheme itself (incentives for participation/cooperation/contribution of WLAN resources) in P2PWNC can be programmed to run on simple embedded systems (Linksys WRT54GS for the server side, Windows Mobile smartphones for the client side). Since all such tools are available today, a P2PWNC-enabled WCN that would also provide free Internet and VoIP services could serve as a realistic alternative to today's commercial cellular networks, complementing them in metropolitan areas where many WLANs are available.



Infrastructure requirements: From the 7 devices presented in the above figure, we will supply the 4 APs and the 2 wireless clients, as well as a laptop for playing the role of the Central Receipt Repository, and a LAN switch to connect all of them. For a satisfying presentation, we would require a connection to the Internet and at least two projectors.

5. Presenters

Elias C. Efstathiou and *Pantelis A. Frangoudis* are, respectively, 4th year and 1st year PhD students at the Athens University of Economics and Business, Mobile Multimedia Laboratory.

Vasileios P. Kemerlis will be graduating in 2006 from the Department of Computer Science, Athens University of Economics and Business.

Dimitrios C. Paraskevaidis and *Eleftherios C. Stefanis* will be graduating in 2006 from the MSc program in Computer Science at the Athens University of Economics and Business, Department of Computer Science.

George C. Polyzos is leading the Mobile Multimedia Laboratory at the Athens University of Economics and Business, where he is a Professor of Computer Science. Previously, he was Professor of Computer Science and Engineering at the University of California, San Diego, where he was co-director of the Computer Systems Laboratory, member of the Steering Committee of the UCSD Center for Wireless Communications and Senior Fellow of the San Diego Supercomputer Center. He received his Dipl. in EE from the National Technical University in Athens, Greece and his M.A.Sc. in EE and Ph.D. in Computer Science from the University of Toronto. His current research interests include mobile multimedia communications, ubiquitous computing, wireless networks, Internet protocols, distributed multimedia, and performance analysis of computer and communications systems. Prof. Polyzos is on the editorial board of Wireless Communications and Mobile Computing and has been a guest editor for: IEEE Personal Communications, ACM/Springer Mobile Networking, IEEE JSAC, and Computer Networks. He has been on the Program Committees of many conferences and workshops, as well as reviewer for NSF, the California MICRO program, the European Commission, and the Greek General Secretariat of Research and Technology and many scientific journals. He is a member of the ACM and the IEEE.

References

[1] http://www.seattlewireless.net
[2] http://www.nycwireless.net
[3] http://www.awmn.net
[4] Motorola CN620. http://www.motorola.com/wlan/solution_cn620.html
[5] Nokia 9500. http://www.nokia.com/nokia/0,,54106,00.html
[6] http://www.phila.gov/wireless/
[7] 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.
[8] E. C. Efstathiou and G. C. Polyzos, "A self-managed scheme for free citywide wi-fi," In Proc. 1st IEEE WoWMoM International Workshop on Autonomic Communications and Computing, Taormina-Giardini Naxos, Italy, June 13, 2005.
[9] E. C. Efstathiou, P. A. Frangoudis, and G. C. Polyzos, "Stimulating participation in wireless community networks," submitted work, also available as 2005-MMLAB-TR01 at http://mm.aueb.gr/technicalreports/
[10] http://mm.aueb.gr/research/P2PWNC/
[11] E. C. Efstathiou and G. C. Polyzos, "A Peer-to-Peer Approach to Wireless LAN Roaming," ACM MOBICOM Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH), San Diego, CA, Sept. 2003.
[12] P. Antoniadis, C. Courcoubetis, E. C. Efstathiou, G. C. Polyzos, and B. Strulo, "Peer-to-Peer Wireless LAN Consortia: Economic Modeling and Architecture," 3rd IEEE International Conference on Peer-to-Peer Computing, Linköping, Sweden, Sept. 2003.
[13] C. Courcoubetis and R. Weber, "Asymptotics for Provisioning Problems of Peering Wireless LANs with a Large Number of Participants," In Proc. WiOpt'04: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, University of Cambridge, UK, March, 2004.
[14] P. A. Frangoudis, "The peer-to-peer wireless network confederation protocol: design specification and performance analysis," Technical Report 2005-MMLAB-TR-02, Mobile Multimedia Laboratory, Athens University of Economics and Business, June 2005. Available at http://mm.aueb.gr/technicalreports/
[15] É. Tardos and K. D. Wayne, "Simple generalized maximum flow algorithms," In Proc. 6th International Conference on Integer Programming and Combinatorial Optimization, pp. 310-324, 1998
[16] J. Douceur, "The Sybil attack," in Electronic Proceedings 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), Cambridge, MA, March 7-8, 2002.