Wireless Community Networks: An Alternative Approach for Nomadic Broadband Network Access

Pantelis A. Frangoudis and George C. Polyzos, Athens University of Economics and Business
Vasileios P. Kemerlis, Columbia University

ABSTRACT

Low-cost wireless LAN equipment operating in unlicensed spectrum has revolutionized local area communications, introducing novel schemes for open wireless connectivity and even new business models. The ease of deployment of Wi-Fi has made it ubiquitous in densely populated urban areas, and it was just a matter of time before *wireless communities* emerged. Using inexpensive wireless technology to communicate, autonomous wireless internetworks have been built, offering a variety of broadband services. Based on our own experience participating in one of the largest wireless communities worldwide, the Athens Wireless Metropolitan Network, we attempt to explain their structure and mechanisms, study the reasons for their emergence and growth, and predict their future evolution. We expect that future wireless communities will be oriented toward providing broadband access to nomadic users. To this end, we have proposed that wireless network access be shared in a peer-to-peer, reciprocal manner. Thus, ubiquitous broadband Internet access can be achieved at a low cost, at least in metropolitan areas where there is abundant wireless coverage, providing an inexpensive alternative to broadband cellular services.

INTRODUCTION

For wireless local area network communications, Wi-Fi emergence was a true revolution. Driven by their low cost and ease of deployment, IEEE 802.11-enabled devices became standard equipment for laptops and handheld devices and appeared as the predominant technology for local wireless connectivity. Operation in unlicensed spectrum facilitated Wi-Fi deployment, since it was straightforward for commercial operators, academic institutions, or even plain radio communications enthusiasts and tech-savvy users to build wireless service architectures on top of it, without the need for acquiring a license. In modern densely populated urban areas, the coverage that WLANs offer is ever-growing. Per-

forming a scan for wireless network presence in such a setting reveals so high a number of wireless access points (APs) in the neighborhood that we should be more concerned about interference than coverage. AP density in metropolitan areas has made it possible to build a business based just on their existence and not their communication capabilities [1].

Wireless Community Networks (WCNs) have been developed as grassroots movements of WLAN enthusiasts, who use inexpensive networking equipment for free interconnection, thus creating all-wireless autonomous networks. Reasons for their emergence can be found in the above discussion. However, their success also depends on local factors (e.g. degree of penetration of fixed broadband access services in the area). Based on the offered wireless connectivity, such networks aim at providing a variety of services, with free community-wide VoIP and file sharing topping the list of the most frequently accessed services.

Increased Wi-Fi coverage and the emergence of WCNs raise the question of whether low-cost alternatives to traditional mobile services offered by 2.5G and 3G systems can be achieved. We focus on *nomadic* users, i.e. roaming users accessing broadband services from multiple fixed locations and without necessarily sustaining uninterrupted connectivity while moving. In selected urban areas the answer is clearly yes, and the trend is in the direction of adequate coverage in all urban areas [2]. Before this idealistic environment is a reality, though, issues such as the incentives of private WLAN owners to permit public access to their APs and relevant security concerns need to be resolved. As to WCNs, they are mainly exclusive; offering services to (potentially mobile) nonmembers occurs today only due to the altruism of some of their participants. The architecture of such networked communities and incentives that keep them operating with robustness are worth studying.

In the remainder of this article, we first classify public wireless access schemes and report on some of the most significant WCNs worldwide.
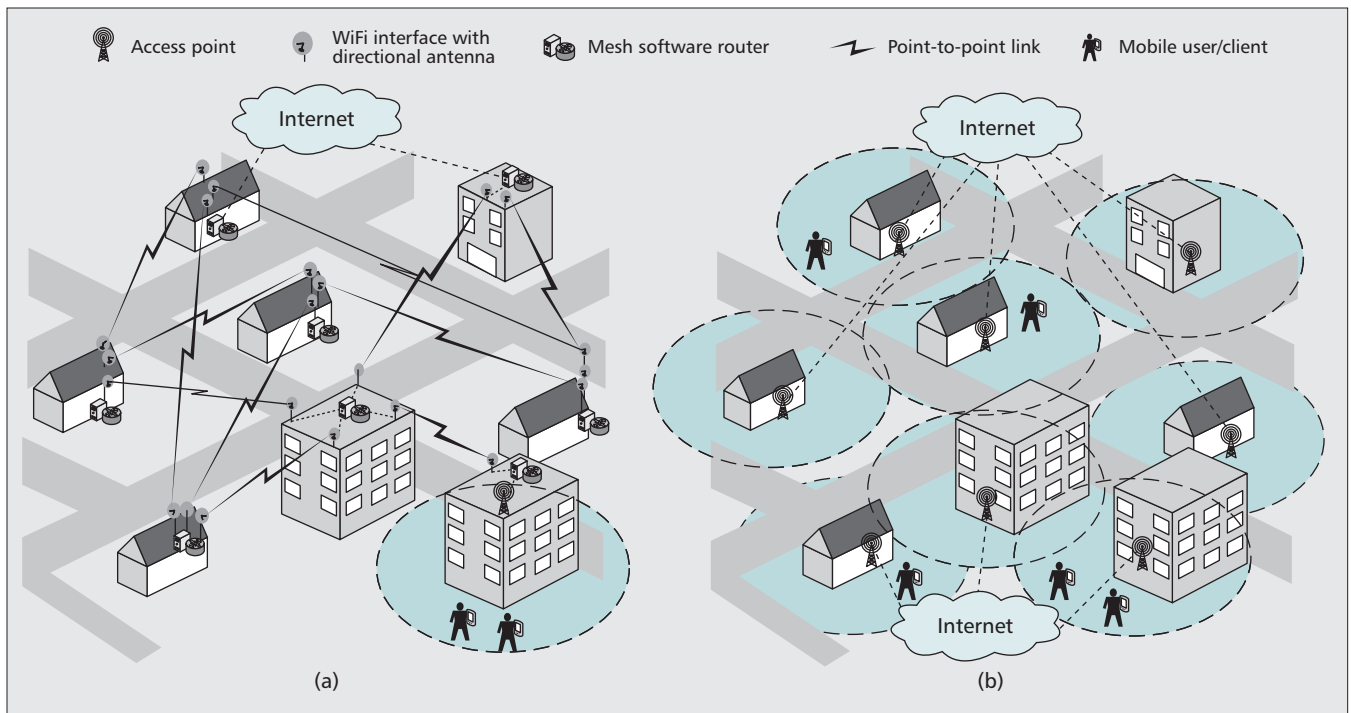
Figure 1. *Architectural alternatives for Wireless Community Networks. A wireless mesh architecture is shown in (a), while the hotspot-based alternative is shown in (b).*

We describe the architecture of community wireless mesh networks. Then we discuss the circumstances under which WCNs emerged and evolved, respectively. We present the incentive mechanisms that regulate their operation and study their future. We discuss our views and proposal for WLAN hotspot sharing and conclude the article.

A CLASSIFICATION OF PUBLIC WIRELESS ACCESS SCHEMES

Here we characterize WCNs based on the initiative behind their emergence and their architecture.

INITIATIVES

Community Initiative — A major focus of this work is on wireless communities that are the result of collective efforts of individual volunteers and function on a not-for-profit basis. Successful communities have emerged, members of which use IEEE 802.11/Wi-Fi technologies to set up a wireless backhaul to connect to one-another, enjoying a variety of broadband services, such as VoIP, online games, FTP, or Web access [3]–[7]. Sometimes community members operate public hotspots to offer wireless access to passers-by, attaching them to the community network, or even offering Internet access through community-owned Internet gateways.

In a similar fashion, an individual WLAN owner may open his private hotspot for public access without anticipating monetary compensation. Instead, he is either driven by pure altruism, or expects that his offering will be reciprocated by other community members when he is roaming near foreign hotspots [8].

Commercial Initiative — Following the above trend, commercial players have entered the scene, offering mediation services for the development of wireless communities. FON [9], for instance, has proposed a private hotspot sharing scheme, where WLAN owners can either share their WLANs for a small monetary compensation or in exchange for similar service when they are away from their own WLAN. FON takes care of user registration and authentication and withholds a fraction of the money paid to the hotspot micro-operator for the provided service.

Notably, British Telecom has recently partnered[1] with FON so that hundreds of thousands of BT's subscribers share their home broadband lines over Wi-Fi with other community members.

Municipal Initiative — Municipalities often set up APs in public spaces, offering inexpensive Internet access to citizens. To achieve this, they may get into agreements with private companies, permitting them to deploy their wireless solutions. Authentication with the operator of the network, as well as a fee for the service, may be required. This model has been adopted by the municipality of Philadelphia [10], as well as the City of London, which has set up a deal with *The Cloud*, a European Wi-Fi hotspot aggregator.

DESIGN ALTERNATIVES

Wireless Mesh — WCNs that have sprung from private initiatives often have this structure. Multi-interface nodes set up a wireless mesh. Some also act as gateways to the public Internet and can be reached over the wireless backbone. We offer a more in-depth discussion of this architecture in Fig. 1a.

---

[1] http://www.bt.com/btfon

Network	Location	Founded	Size	Architecture	Initiative
SeattleWireless	Seattle, WA, USA	2000	~80 nodes	Mesh	Community
AWMN	Athens, Greece	2002	2473 nodes	Mesh	Community
CUWiN	Urbana, IL, USA	2002	48 nodes	Mesh	Community
Berlin's Freifunk	Berlin, Germany	2002	316 nodes[a]	Mesh	Community
Wireless Leiden	Leiden, Netherlands	2002	73 nodes	Mesh	Community
NetEquality Roofnet	Portland, OR, USA	2007	126 nodes	Mesh	Community
NYCwireless	New York City, USA	2001	145 nodes	Hotspot-based	Community
Wireless Philadelphia	Philadelphia, PA, USA	2007	15 $miles^2$	Hotspot-based	Municipal
FON	Worldwide	2006	~700,000 hotspots[b]	Hotspot-based	Commercial

[a] Circa 2007 [6]
[b] Based on information available from http://www.fon.com, as of September 2009.

Table 1. *Wireless communities around the world (as of September 2009).*

Hotspot-based Architecture — Hotspot-based WCNs typically target nomadic users who use wireless hotspots to access the Internet (Fig. 1b). Here, deploying a wireless backhaul is not the norm. Municipality-initiated WCNs usually have this structure. Sometimes, hotspot-based WCNs are built relying on the private contributions of individual WLAN owners, who share their fixed broadband lines over Wi-Fi. We have witnessed both commercially initiated [9] and not-for-profit [8] such attempts.

WIRELESS COMMUNITIES AROUND THE WORLD

Here we report on some of the most significant WCNs worldwide and categorize them as described earlier. Our findings are summarized in Table 1. The reported network dimensions are based on data found on publicly available node maps and measurement studies [6].

We have chosen representative WCNs and tried to include the most well-known and influential ones. SeattleWireless [3], for instance, has been at the forefront of the WCN movement since the early 2000s.

Also, NYCwireless [11] and the CUWiN Foundation [5] are active in advocating the use of open wireless technologies, fostering the growth of WCNs and developing software for community wireless projects. They are operated by nonprofit organizations, whose interest has recently been drawn to developing free wireless access solutions for under-served communities, both in the US and in other countries.

The Athens Wireless Metropolitan Network (AWMN) [4] is one of the largest community mesh networks in the world. Currently it has more than 9000 registered nodes, with more than 2400 of them being active. Wireless Leiden [7] is a similar effort in the Netherlands. Its aim is to provide a free citywide all-wireless network in the city of Leiden and offer free broadband Internet access to nearby villages, where no fast Internet alternatives exist.

Recently, the Freifunk community has gained much popularity. Freifunk mesh networks have sprung up in various German cities, as well as in cities in Austria and Switzerland. In Berlin, Freifunk counted 316 concurrent participating nodes on average, according to a 2007 study [6].

The MIT Roofnet [12] mesh network started as a research project focusing on wireless multi-hop routing and IEEE 802.11 protocol performance, while offering Internet access to nearby residents. It is now less vibrant (approximately 20 active nodes), but its technology is used from other wireless community projects.

ARCHITECTURE OF A COMMUNITY WIRELESS MESH

NODE TYPES

There are two types of nodes. *Backbone nodes* are those that the backhaul of the network is built upon. They typically have more than two network interfaces and run routing software. Some backbone nodes operate omni-directional antennas and function also as APs. *Client nodes* can then attach to these APs and use the network's infrastructure. *Clients* can be considered the "leaves" of the network.

Typically, WCN participants discouraged new users from operating client nodes, since clients usually do not contribute to the network's operation and coverage. In practice, being a client is usually the first step a user takes when joining such a community.

LINKS

The backbone of the network is based on directional point-to-point links. Although IEEE
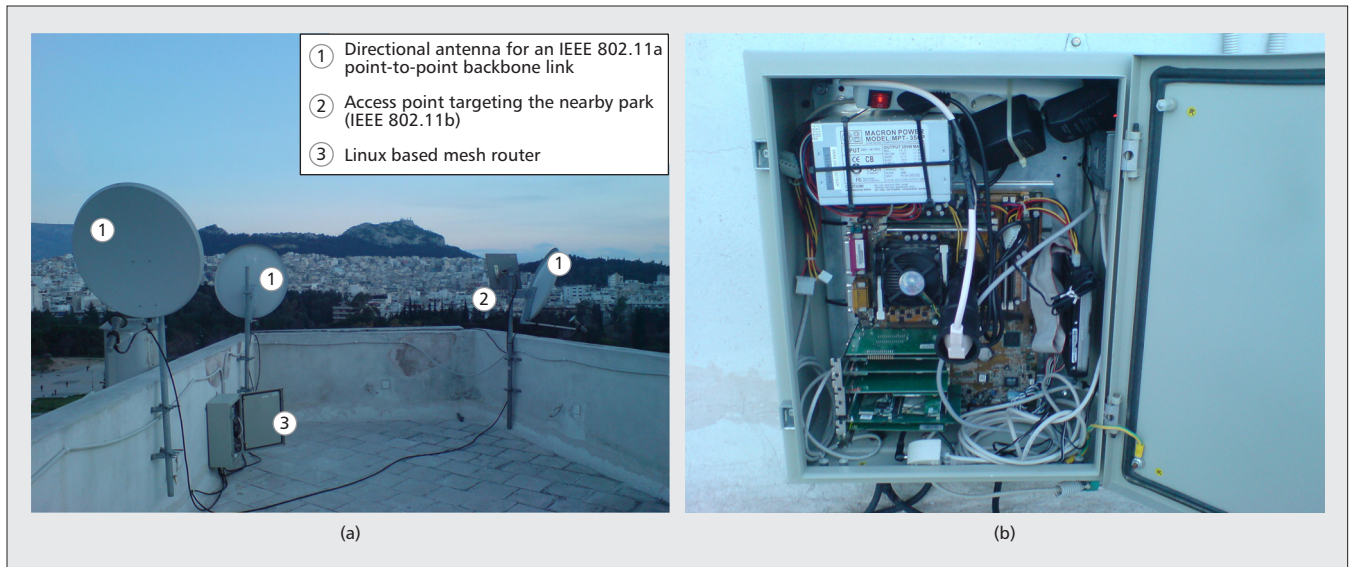
Figure 2. *Pictures from MMlab's AWMN node. Three of our backbone links, as well as our AP, are visible in (a). IEEE 802.11 wireless interfaces are attached to hand-made antennas. In (b), the Linux-powered rooftop PC, which hosts our wireless interfaces and performs routing, is shown.*

802.11 was designed as a broadcast protocol for local communication, it is widely used for setting up long-distance links, assisted by directional antennas. In the beginning, 802.11b was the protocol of choice, but with the advent of 802.11a, it was replaced in the backbone in order to minimize contention and interference from clients and APs. IEEE 802.11b is still used by APs.

A recent study [13] of the evolution of AWMN revealed that many backbone nodes maintain up to six backbone links. The more links per node, the higher path redundancy is achieved.

ADDRESSING AND ROUTING

Mesh-based WCNs have the same functionality, underlying mechanisms and applications as the public Internet. They are based on an IP layer and follow a private addressing scheme. In most of them (e.g., AWMN), a central authority tackles addressing issues. Each newly-registered node is assigned a private IP address range. Every community follows its own routing scheme, often involving BGP, much like the Internet itself. From the BGP viewpoint, each WCN node can be considered a single *autonomous system*. In some cases, experimentation with routing protocols suited for wireless ad hoc networks, such as OLSR, is carried out.

UNDERLYING TECHNOLOGIES

Open source software and often hand-crafted hardware are used for interconnection. Linux-powered embedded rooftop equipment is used for controlling the operation of each node, while much experimentation involves the design and construction of low-cost custom-made antennas. Figure 2 depicts part of the infrastructure of the AWMN node that we have set up on the rooftop of one of AUEB's buildings.

SERVICES AND APPLICATIONS

The most prevalent services are file sharing and community-wide VoIP. Also, on some occasions, members share their fixed broadband connections with the community, so that Internet access is achieved through WCN-to-Internet proxies. For other services see [13].

THE BIRTH OF WIRELESS COMMUNITIES

The appearance of WCNs dates back to the late 1990s-early 2000s, when IEEE 802.11 was introduced. Radio technology enthusiasts were the first to embrace the new technology and experiment with it for long distance interconnection. Thus, communities of interconnected peers emerged in a period when fixed wireline infrastructure could not always support them. One can consider the first wireless community networks as the evolution of amateur radio.

As wireless technology matured and gained popularity and as more advanced WLAN standards emerged, WCNs started to grow. However, one of the major factors that contributed to their growth was the low penetration of broadband access technologies in some countries.

In addition, some wireless communities [12] have been developed as experimental testbeds for wireless research. In these cases, free wireless Internet connectivity is a side effect, while the main goal of such WCNs is to test novel wireless technologies and evaluate current WLAN standards.

GROWTH

One of the reasons AWMN has grown to be one of the largest such networks worldwide was the fact that, in Greece, DSL penetration used to be one of the lowest in the European Union before 2005. Actually, back in 2002, when the first AWMN node was set up, there was a single operator offering DSL to corporate clients, with download speeds of at most 128Kbps and a very

high price. Setting up long-distance wireless links using IEEE 802.11 to achieve cheap citywide broadband connectivity seemed to be a one-way street for tech-savvy users. At the time, the most successful applications were fast file sharing and online gaming, as well as Internet connectivity through AWMN-to-Internet gateways (when some participants shared their fixed broadband Internet lines with the community).

The network evolved and gained publicity through word-of-mouth and dissemination activities of its members, which included demonstrations at technology expos and universities and participation in festivals and other public venues, where free wireless connectivity was offered through the AWMN infrastructure.

A key technological shift was the adoption of the new IEEE 802.11a variant for setting up point-to-point backbone links. Moving from 2.4GHz to the less congested 5GHz band, interference was limited. Nodes with multiple collocated interfaces had more non-overlapping channels to choose from for each of their radio interfaces, while links of higher throughput could be achieved. Backbone nodes could sustain more links, which offered path redundancy and resilience. Citywide VoIP and video conferencing within the community, as well as file sharing, have thrived since. Increased capacity, better quality of service, and the fact that backbone nodes could now sustain more links caused a population boom in the WCN. A direct consequence was the expansion of its coverage to most of the suburbs of Athens.

INCENTIVES FOR SUSTAINABLE WIRELESS COMMUNITIES

INCENTIVES FOR PARTICIPATION

Why would one participate in a WCN? Usually it is the enthusiasm stemming from experimentation with new technologies or the joy of creation offered by building one's own equipment and configuring one's node. Also, the services provided by the community are tempting, especially when the respective services over commercial (fixed) broadband infrastructure are of worse quality, or even non-existent.

Those who believe that broadband connectivity should be unleashed and the barriers imposed by the oligopoly of ISPs be removed and that broadband access should be a public good usually are the first to join WCNs. Under this perspective, WCNs can be considered a modern technological "movement." Operation in unlicensed spectrum facilitates their growth and, coupled with the extensive use of open source software, shapes their free and self-organizing character. It is atypical of their participants to think of community-initiated WCNs as the vehicle to make profit or develop a new business.

CONFORMANCE AND CONTRIBUTION

As far as WCNs such as AWMN are concerned, contribution to the community and abiding with the explicit or implicit participation rules is enforced in a tit-for-tat manner. Users that do not conform to such rules can be effectively excluded from the community.

Most WCNs are open for participation, but have some structure and their deployment is not completely anarchic. In order for the system to operate without disruptions, nodes should follow some rules, especially concerning addressing and routing. Also, they should not behave selfishly, since that could potentially cause congestion to the backbone links, as well as saturation of some services. In case a user does not behave, there is high probability that he will eventually be excluded from the network. At a technical level, nonconformant behavior can be easily detected from one's neighbors and reported to the community.

Exclusion can also easily be implemented; neighboring users can simply shut down the links they share with the user that causes anomalies to the WCN's operation. Thus, the latter will be disconnected and isolated from the community. In fact, we have witnessed similar incidents within AWMN.

Incentives for the maintenance of the first two links of a backbone node are quite straightforward WCN participation. Additional links add redundancy, network bandwidth, and reputation in the community. There is expressed mutual interest for the two link endpoints to set one up. As soon as one of the two nodes defects, the link becomes inoperative.

The case is different for client-to-AP links. There is no direct and measurable gain for an AP to offer connectivity to clients. However, in the long run, there is a potential gain for the community as a whole, since clients are anticipated to bring more content and are expected to gradually upgrade their nodes to backbone ones. Thus, serving clients is considered a means of attracting attention to the community and gradually recruiting more resources.

BUILDING REPUTATION

Interestingly, senior WCN members and members who own *powerful*[2] nodes are highly esteemed in the community. Because their nodes are important for the operation of the network, their decisions may affect many users.

Building up reputation within a WCN can easily be explained. In such communities, participation anonymity is not easy (or even possible) to achieve, nor is it desirable. Recruiting new members is an incremental process, where older members introduce new ones to the community, offering them connectivity.

The infrastructure-based nature of the network is such that long-term relationships among members are built; nodes are fixed and links are typically permanent. Most of the time, owners of nodes that share a link know each other personally, while the community encourages socialization among its members. Contribution to the community is directly attributed to its initiators, while unacceptable behavior is detected, reported and, potentially, punished, as described earlier.

A LOOK TO THE FUTURE OF WCNS

To gain insight into how WCNs will evolve, one has to reconsider the factors that led to their emergence and booming growth.

First, low-cost broadband services, once one

of the highlights of WCNs, have now become a commodity in most modern metropolitan areas. No more is joining a WCN the only way to enjoy high-quality multimedia services or fast file sharing.

On the positive side, though, promising new wireless technologies, such as the IEEE 802.11n standard, are about to be integrated. These may revitalize interest in WCNs and cause a new wave of development in the area. On the other hand, an issue that is generally still unresolved is how such broadband services will be offered for mobile users at low cost. 3G-based solutions are still considered expensive by many users and their adoption is relatively low. Basing our arguments on the increased wireless coverage in modern metropolitan areas, we believe that open wireless access schemes can become a viable alternative for the provision of nomadic broadband network access. To support this action, traditional WCNs may need to become less exclusive so that they are accessible not only strictly to their participants, but also to roaming non-members.

To this end, opportunistic WLAN access based on the private contributions of individual WLAN owners will likely attract more attention as a vehicle to make inexpensive ubiquitous broadband Internet a reality. WLAN owners can become micro-operators that trade bandwidth for payment in kind or even money. In the following section we present our architecture toward this vision.

WLAN Sharing

Fundamental Challenges

Sharing one's Internet connection with roaming individuals incurs direct and indirect costs or may be forbidden by the ISP. Users may have to put up with the managerial overhead of configuring their WLAN for shared access. Also, admitting more users to one's private network can result in reduced service level for its owner. Sometimes, WLANs are attached to metered broadband lines. Sharing such a WLAN means that its operator pays for every single byte uploaded or downloaded by visitors. Security concerns also make individuals reluctant to open their WLANs for public access. The challenge for the system designer is to minimize the incurred costs, while revealing the benefits for users to join and contribute their resources.

Joining the system should be possible with minimal installation cost, both financially and effort-wise. User registration should be fast and decentralized, to facilitate the system's organic growth and scaling. From the nomadic user's perspective, wireless access should have low cost compared to its cellular alternatives. Also, roaming privacy is a desirable feature; a user may wish to access foreign APs without disclosing personal information to the service provider or his network point of attachment to his communicating endpoints.

Note that our focus is on low-mobility, *nomadic* users and our emphasis is on access issues rather that true mobility support. Handing-off efficiently between foreign visited WLANs is a significant challenge.

Peer-to-Peer Hotspot Sharing

We have proposed [8] that wireless Internet bandwidth be exchanged in a reciprocal manner; one shares his Internet connection with anonymous passers-by over Wi-Fi with the anticipation that he will enjoy the same benefit from another peer when mobile. That is, our approach to the problem is based on the peer-to-peer paradigm. Private WLAN owners have an incentive to contribute Internet bandwidth, given that they place high value on the mobile network access they will enjoy as good contributors. We call our scheme the Peer-to-Peer Wireless Network Confederation (P2PWNC).

To lower the entry barrier to the system, no registration with central authorities is required, nor any strong user identification scheme. Participants are identified by self-issued, uncertified public-secret key pairs. To join P2PWNC, users simply configure their APs for open access and install the necessary software.

Accounting is based on digital proofs of service (*receipts*) that mobile users provide to visited APs. Receipts are stored in repositories distributed across the system; each peer maintains his own repository, which represents his (partial) view of the system's history of service provisions.

Receipt repositories (RR) are the input to the *reciprocity algorithm*, which identifies good contributors and detects *free riders*, i.e. those who consume resources without contributing to the community. Each time a mobile user requests service, the reciprocity algorithm is executed by the visited peer to decide whether the visitor is a good contributor and deserves to be reciprocated.

P2PWNC is decentralized and no registration is mandated. Other similar schemes, such as FON [9], do not have these properties. Also, P2PWNC has some inherent privacy enhancements. The non-persistence of user identifiers, as well as the fact that the disclosure of real-world user identities is not needed, assist in WLAN roaming anonymity. We have also shown that a decentralized architecture for secure and private voice and multimedia communications can be built on top of our scheme [14].

Mechanisms and Protocols

Here we present an overview of the P2PWNC operations, also depicted in Fig. 3.

Receipts, Receipt Repositories and the Reciprocity Algorithm — The P2PWNC accounting unit is a receipt, a document digitally signed by a service consumer (mobile user) using his private key. It contains the provider and consumer identities, a timestamp, and information on the amount of traffic forwarded by an AP on behalf of the signer during a P2PWNC session. Receipts represent "debt" among peers, which we assume to be transitive; if peer A has provided service to peer B and the latter has served peer C, then C indirectly "owes" some service to A. A's contribution can be reciprocated when he visits one of B's or C's APs. With each receipt encoding an "I-owe-you" relationship, a RR can be viewed as a logical directed graph, whose ver-
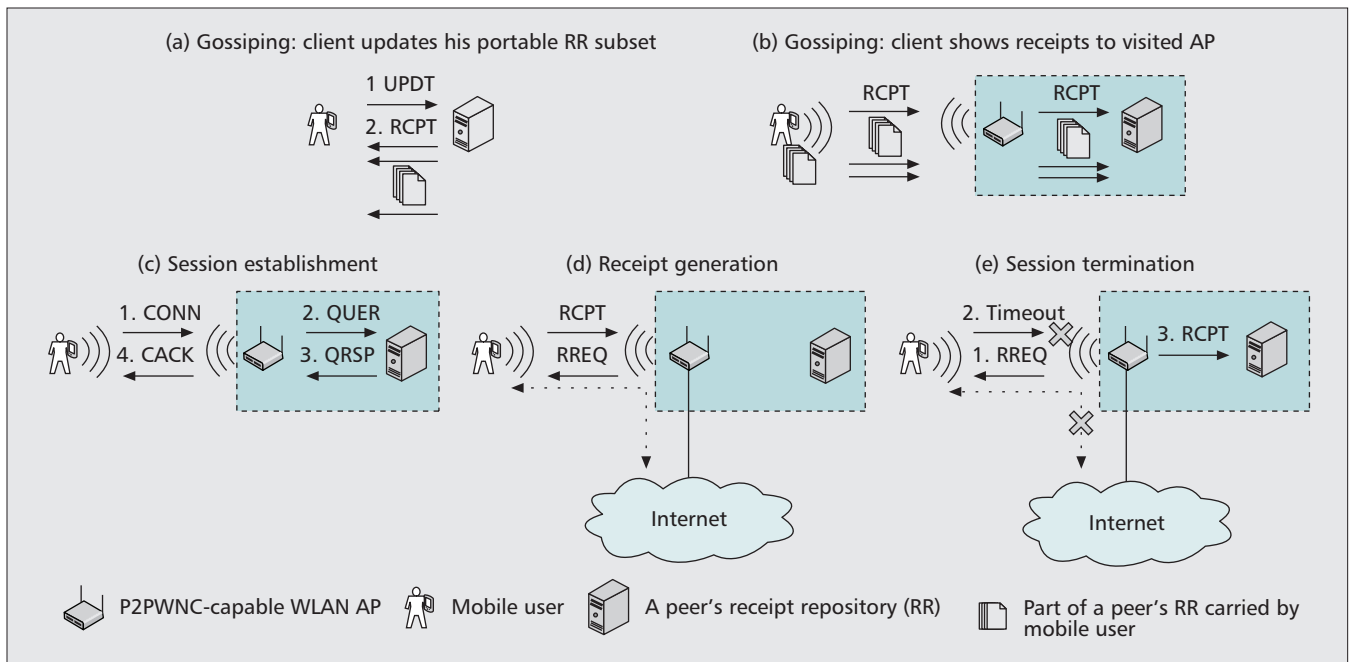
Figure 3. *P2PWNC operations. a) First, a user communicates with his home RR and updates the RR subset that he carries with him. b) Then, before requesting service from a visited AP, he presents it with the receipts he carries with him. c) Following, he issues a connection request, upon which the AP consults his own RR, where the reciprocity algorithm is invoked, and decides to accept the user or not. d) In the first case, Internet access is granted and a receipt request-response cycle begins. e) When a client fails to deliver a receipt on time, the session terminates and the AP forwards the last receipt to his RR. The messages exchanged during the above processes are summarized in Table 2.*

tices correspond to peers and its edges represent receipts and point from a service consumer to a service provider.

Such a graph is the input to the reciprocity algorithm, which is invoked each time a user requests to be served. Its output is a value expressing a user's "reputation" in the eyes of a prospective service provider. Given that accounting is decentralized and user identities are self-issued, the reciprocity algorithm should be intelligent enough to detect free riders and prevent from attacks to the accounting mechanism [8].

Session Initiation and Receipt Generation — Receipts are generated on a per-session basis. A prospective service consumer requests access to a P2PWNC-controlled Wi-Fi AP by presenting his identity. Following, the AP invokes the reciprocity algorithm and the RR responds whether the client should be admitted to the visited WLAN. If so, a receipt request-response cycle begins; the AP periodically requests an acknowledgement for the volume of Internet traffic forwarded on behalf of the visitor thus far, and the latter responds with a cumulative "fresh" receipt. After a receipt request has timed out (e.g., when the visitor leaves) or upon receiving a malformed receipt (that is, one that the AP is incapable of cryptographically verifying), the session terminates and the AP forwards the last receipt to his RR. This last receipt contains information about the session's aggregate amount of traffic. Notice that the receipt generation protocol ensures that a visitor's session has not been *hijacked* by an unauthorized party. In order to sign a receipt and maintain the session, the hijacker would need access to the visitor's private key.

Receipt Dissemination — A visited peer uses only his own view of the system's history of transactions as input to the reciprocity algorithm. To assist in giving potential service providers a better view of their overall contribution and have better chances of getting access, visitors can also supply parts of their own RRs via a *gossiping protocol*. *Gossiping* takes place at the beginning of a session; the visitor presents the AP with a subset of his own RR carried in his mobile device. These receipts are then merged with the visited peer's RR and reveal service directly or indirectly owed to the visitor. Note that because the receipts are cryptographically signed, invalid receipts do not help the presenting party. A peer regularly queries his RR for updates to his portable RR subset, since RR contents change frequently.

Implementation Issues — P2PWNC entities communicate using a simple ASCII-based protocol running over TCP/IP. Together with the reciprocity algorithm, they have been designed and implemented with resource-constrained devices in mind, such as off-the-shelf wireless routers and PDAs. P2PWNC typically runs in the firmware of such devices. The protocol messages exchanged among the various entities are summarized in Table 2.

CONCLUSION

WCNs have emerged as a means for inexpensive broadband connectivity in metropolitan areas. In this article, we discussed the reasons for their emergence and evolution and described their architecture and the incentives

relevant to their operation. With the abundance of wireline broadband connections, future WCNs may evolve toward offering connectivity to nomadic users. Based on the increased wireless coverage in metropolitan areas today, decentralized schemes such as P2PWNC can make WCN-based Internet access a viable low-cost alternative to the more expensive cellular services.

REFERENCES

[1] Skyhook Wireless, available: http://www.skyhookwireless.com.
[2] G. C. Polyzos, "A Peer-to-Peer Approach to Cellular Communications," *Proc. 9th ACM Int'l. Symp. Modeling Analysis and Simulation of Wireless and Mobile Systems (MSWiM'06)*, Torremolinos, Spain, 2006.
[3] Seattle Wireless, Available: http://www.seattlewireless.net.
[4] Athens Wireless Metropolitan Network, available: http://www.awmn.net.
[5] Cuwin — Community Wireless, available: http://www.cuwireless.net
[6] B. Milic and M. Malek, "Analyzing Large Scale Real-World Wireless Multihop Network," *IEEE Commun. Letters*, vol. 11, no. 7, July 2007, pp. 580–82.
[7] R. J. Kramer, A. Lopez, and A. J. Koonen, "Municipal Broadband Access Networks in the Netherlands — Three Successful Cases, and How New Europe May Benefit," *Proc. AccessNets '06*, Athens, Greece, Sept. 2006.
[8] E. C. Efstathiou, P. A. Frangoudis, and G. C. Polyzos, "Stimulating Participation in Wireless Community Networks," *Proc. IEEE INFOCOM*, Barcelona, Spain, Apr. 2006.
[9] Fon, available: http://www.fon.com
[10] Wireless Philadelphia Executive Committee, available: http://www.phila.gov/wireless.
[11] NYCwireless, available: http://www.nycwireless.net.
[12] J. Bicket *et al.*, "Architecture and Evaluation of An Unplanned 802.11b Mesh Network," *Proc. 11th ACM Annual Int'l. Conf. Mobile Computing and Networking (Mobicom'05)*, Cologne, Germany, 2005.
[13] F. Elianos *et al.*, "Structure and Evolution of A Large-Scale Wireless Community Network," *Proc. 10th IEEE Int'l. Symp. World of Wireless, Mobile and Multimedia Networks (WoWMoM 2009)*, Kos, Greece, 2009.
[14] E. C. Efstathiou, P. A. Frangoudis, and G. C. Polyzos, "Controlled Wi-Fi Sharing in Cities: A Decentralized Approach Relying on Indirect Reciprocity," *IEEE Trans. Mobile Comp.*, vol. 9, no. 8, Aug. 2010, pp. 1147–60.

Message	Description	Direction
CONN	P2PWNC session initiation request	Client → AP
CACK	P2PWNC session initiation response	AP → Client
RREQ	Receipt request	AP → Client
RCPT	Receipt	Client → AP AP → RR RR → Client
QUER	Query the RR (invoke the reciprocity algorithm)	AP → RR
QRSP	Query response	RR → AP
UPDT	Client (portable) RR update request	Client → RR

Table 2. *P2PWNC protocol messages.*

BIOGRAPHIES

PANTELIS A. FRANGOUDIS (pfrag@aueb.gr) is a Ph.D. candidate at the Department of Informatics, Athens University of Economics and Business and member of the Mobile Multimedia Laboratory. He holds a B.Sc. (2003) and an M.Sc. (2005) in Computer Science from the same department. His current research interests include wireless networks, Internet multimedia and network security.

VASILEIOS P. KEMERLIS (vpk@cs.columbia.edu) is a Ph.D. candidate in the Department of Computer Science at Columbia University, where he is also a member of the Network Security Laboratory. He holds a B.Sc. with honors (2006) from the Athens University of Economics and Business, Greece and an M.Sc. (2010) from Columbia University, NY, USA, all in Computer Science. His research interests include systems and network security, distributed systems, and performance analysis.

GEORGE C. POLYZOS (polyzos@aueb.gr) is a professor of Computer Science at AUEB since 1999, has founded and is leading the Mobile Multimedia Laboratory. 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 has 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 wireless networks, mobile multimedia communications, ubiquitous computing, Internet protocols and architecture, security, and system performance evaluation.