



School of IT
Technical Report



The University of Sydney

**TITAN: A NEW PARADIGM IN WIRELESS INTERNET
ACCESS BASED ON COMMUNITY COLLABORATION
TECHNICAL REPORT 578**

BJORN LANDFELDT, JAHAN HASSAN, ALBERT ZOMAYA,
TASOS VIGLAS, SELVAKENNEDY SELVADURAI, DAVID EVERITT,
BERHARD SCHOLZ, BING BING ZHOU

DECEMBER 2005

Titan: A New Paradigm in Wireless Internet Access based on Community Collaboration

Bjorn Landfeldt, Jahan Hassan, Albert Zomaya, Tasos Viglas, Selvakennedy Selvadurai,
David Everitt, Bernhard Scholz, Bing Bing Zhou
School of Information Technologies
University of Sydney
Sydney 2006, Australia.
Email:{bjornl, jahan, zomaya, tasos, skennedy, deveritt, scholz, bbz}@it.usyd.edu.au

Abstract— This paper introduces project TITAN, which investigates an alternative construct of residential broadband access. The aim of the project is to increase the utilisation of deployed broadband capacity such as xDSL and cable modem connections. In order to achieve this, we propose a Collaborative Community Network (CCN) where residential broadband users contribute their *spare* broadband capacity to other users over a wireless medium, to form a collaborative community wireless Internet access network. Our novel design has the strength that it can provide high data-rate wireless Internet access by utilising *existing* infrastructure, while utilising the community pool of network resources to provide a distributed network management. We build an autonomous high capacity wireless access network using a combination of cognitive wireless mechanisms and a distributed processing platform to continuously optimise the configuration and utilisation of the network. A novel and interesting consequence of our architecture is a paradigm shift in terms of the boundary between service providers and consumers. In our model, consumers collaborate with the service providers to achieve the goals of high availability, high capacity wireless network access.

This paper introduces the TITAN model and functional components and discuss the main research challenges associated with the model.

Keywords- wireless networks, access network, wireless Internet, WLAN, DSL.

I. INTRODUCTION

Wireless access has proven itself a winner with consumers, providing mobility and ease of use. However, there is an inherent limitation in the capacity of wireless networks where achievable data rates are proportional to the number of terminals in each cell. As the number of terminals grows and therefore the required data rate grows, due to the finite spectrum the cell size has to shrink. Because of this constraint, it is not possible to provide more than low to moderate data rates over wide area wireless networks. High capacity wireless will only be achieved as cell sizes go towards Wireless LAN (WLAN) configurations.

WLAN technology has shown a real promise, providing wireless networking at high data-rates to a low cost. There has been tremendous success in marketing WLAN systems as evidenced by the revenue generated from selling WLAN hardware. It has been reported that the worldwide wireless LAN hardware revenue reached \$ 2.5 billion in 2003, an

increase of 56% from 2002, primarily driven by strong wireless *gateway growth* [11]. Coupled with the gateway devices, WLAN technology provides a promising platform for high data-rate wireless Internet access.

Wireless Hotspots efforts began with a great promise to offer wireless Internet access by setting up WLAN access points (AP) at popular sites, such as shopping malls, airports, etc. However, a major obstacle in deploying large scale WLAN networks is the inherent cost in maintaining a large number of sites, making the business case for such networks non-profitable. The Hotspot model was no exception and the initial business models were soon invalidated. They incurred an excess cost in infrastructure installation and maintenance, leading to a net loss. A new way of providing wireless Internet access which can circumvent these costs is therefore of prime interest.

Another current strong trend is the roll out of broadband services primarily through the reuse of existing infrastructure deployments, e.g. ADSL over copper pairs and shared access over cable networks. In addition, wireless broadband providers are deploying wide area data networks for low to medium capacity access. The fixed access networks have a significantly higher capacity in terms of aggregated data rates than the wireless networks, and are largely under-utilised resources. Typically, the deployed capacity to homes (home-Local Exchange) is not utilised more than a small fraction of the time whereas the aggregated Local Exchange-core utilisation is higher. Wide area wireless networks on the other hand are deployed at a rate where access utilisation is much higher and the network density grows with the utilisation.

In order to capitalise on the installed base of broadband Internet access in existing (residential) sites, and to provide low-cost high data-rate wireless Internet access, we propose a new architecture called Collaborative Community Network (CCN). CCN can increase the utilisation of already deployed fixed broadband access to residential sites through a novel model of collaboration between access providers and consumers. CCN aims to provide true high capacity wireless Internet access in a very cost-effective manner. This architecture provides consumers with the ability to use true broadband mobile services and the service providers with a higher return on

investment (ROI) of the last hop.

The rest of the paper is organised as follows. Section II provides an overview of the CCN architecture. A brief discussion on related architectures is provided in section III, followed by a discussion on the functional components of CCN and issues that need to be investigated in section IV. As the proposed architecture opens up private network components for public use over the wireless medium, strong security measures are required. We discuss the security requirements and challenges of CCN in section V and finally conclude the paper with a note on our current research directions.

II. OVERVIEW OF CCN

In our model, consumers (home users) contribute the sites for WLAN base stations (Access Points) to the network by purchasing a wireless subscription package consisting of Internet access via a wireless gateway (WG). Access through other base stations or WG is offered *provided* that other consumers can utilise spare capacity over each other's residential broadband connections and wireless networks. The resource sharing is completely transparent to the users and does not impose any limitations in their own experience through the use of priorities. In other words, when a consumer is not utilising resources of his/her own disposal, only then are they lent to other users. Thus, a collaborative access network is created for high-speed Internet access of wireless devices.

Such a network has some properties that need careful addressing. Since no player can be made responsible for the planing and management of equipment (as is the case with traditional public access networks), the network in itself will have to provide these functions. Issues such as load balancing, redundancy and fault tolerance will have to be implemented in the residential site equipment rather than centrally under operator management. The role of the service provider will instead be overall policy enforcement and management of the core network.

In order to provide such functions, the access network components will have to collaborate in a fully distributed fashion. All connectivity layers of the communication model will be affected and will have to be constructed in such a way to make the network collaborative. The collaborative mechanisms can be divided into two groups, the physical layer and medium access (MAC) group and network layer functions group. In this project we envisage a division of these mechanisms over two functions in a wireless residential gateway. The physical layer and MAC group mechanisms will be carried out by the AP function and the network layer functions by the border gateway function.

There are two main scenarios in which resources can be shared depending on the wireless coverage. In case the wireless APs are not overlapping, resources can be lent to visiting nodes so that spare capacity is utilised. This mode is the most fundamental and easiest to realise. However, since the occupants at the AP site should have precedence over visitors the variability of resource availability might be high. In the second scenario, if there is overlapping wireless coverage

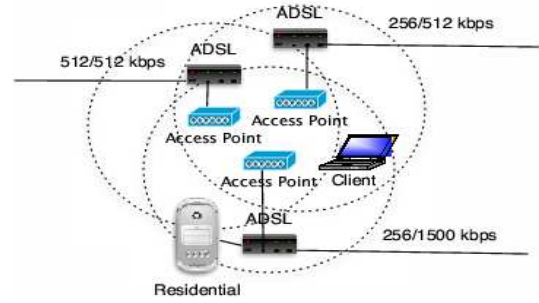


Fig. 1. Collaboration via spare capacity sharing in CCN

resources can be shared among visitors and the occupants at the AP sites. In this case, the possibilities of resource allocation become more interesting in that individual flows can be admitted over different APs in order to maximise the *aggregated* resource allocation. The cost of operating in such a mode is increased complexity in the access network.

Figure 1 sketches a simple example of the second scenario. In the scenario there are three partially overlapping APs, each connected to the Internet via ADSL links with different capacity. The laptop is a visiting mobile node at the site. Even though the highest capacity access link is the 256/1500 kbps ADSL connection, it is not selected for admitting flows from the laptop since the owner of that link is using much of its capacity. Instead one of the two other available APs will admit connection requests. It is also important to note that the owner of the 256/1500 kbps link can utilise spare capacity over the other links provided that the wireless interface can support multiple concurrent channels. We believe that this mode of operation is a likely scenario in urban areas, especially in city centres. In densely populated areas, with the current popularity of 802.11 wireless home networking APs we will soon reach a stage when numerous overlapping APs are commonplace. Current systems fail to take advantage of this situation. Instead, overlapping coverage is today thought of as competing usage of spectrum. In our model, we view the sharing as a potential and seek to exploit the overlap rather than to avoid it.

In order to make full benefit of this shared access scenario, as mentioned before we envisage that the mobile devices will have multi-channel operation capability. This opens up enormous possibilities in terms of resource utilisation and also a multitude of new research questions to answer. In this project, we focus on two main research areas within this problem space: making the access network utilise the available resources in a collaborative fashion, and making the access network autonomous and fault resilient. We will discuss these areas in section IV.

III. RELATED ARCHITECTURE

Various architectures that are designed with the goal of providing Internet access over IEEE802.11 wireless LAN infrastructure can be found in the literature. Hotspots started out with a great promise of providing such access, but only to within a limited area such as at hotels, airport lobbies, etc.

Examples of Hotspot providers include T-Mobile [13], Boingo [5], Surf and Sip [10], Air2LAN, etc. As mentioned briefly, the Hotspots model incurred quite significant infrastructure and maintenance cost leading to a non-profitable business model, following the similar downfall experienced by Metricom’s Richochet- a single-company owned wireless access infrastructure [6]. Simply stated, when there is significant cost in setting up infrastructure, it is harder for the business to thrive, especially if the cost of the equipment and infrastructure has to be born by a single company. It is worth noting that the major contributing component for providing public access over wireless networks is site costs, the cost of renting space and maintaining the facilities for the base-stations.

Shared AP hotspots, a slightly different HotSpot model is becoming more popular than the single-operator hotspot model because it enables cost sharing. In this model, various HotSpot operators come together to form a consortium, and customers of the participating operators can access any of the operator’s site from the consortium. The Airpath Provider Alliance (APA) [3] is one such consortium, providing ubiquitous Wi-Fi roaming, with over 600 providers operating over 3300 hotspots around the world.

Architectures providing multi-hop wireless access to the fixed Internet have also been proposed in the literature. Hyacinth [8] and TAP [7] are two such architectures that take advantage of 802.11’s multichannel capability. These architectures are infrastructure intensive, as the APs have to be specially installed for this purpose thus resembling the non-profitable business model of hotspots. Both architectures also require multi-hop wireless communication among APs in order to direct traffic to the fixed Internet. Our model does not only focus on providing connectivity, in addition, we aim at utilising the existing broadband connections fully. Thus, in CCN the model provides direct connectivity to the fixed infrastructure over a single wireless hop.

It is possible to extend our model with multi-hop wireless where there is a gap between broadband access links. For example, mesh networking techniques [12] can be used to extend the coverage of CCNs. However, in this case the advantages of CCN are largely lost and the network defaults to a lower capacity best effort network.

IV. OVERVIEW OF FUNCTIONAL COMPONENTS

In this section we outline the two main components in our architecture and provide an overview of the research challenges we are concentrating on. As previously mentioned and as illustrated in Figure 2, our architecture consist of a collaborative wireless access network coupled with a distributed processing platform for processing network control and maintenance algorithms. Since the network has to be autonomous it is imperative that it has the capability of configuring and maintaining itself and only relying on the operator/ISP for overall policy enforcement. A powerful platform translates to a capacity of performing complex algorithmic processing which will empower the autonomy. In the following sections, we detail the main issues within the two components.

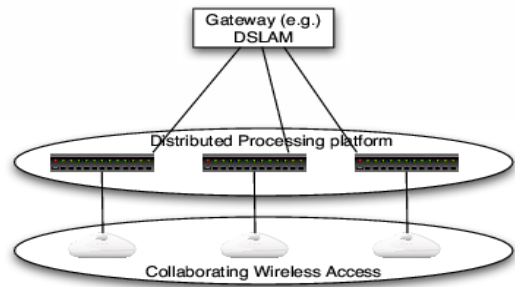


Fig. 2. Two Collaboration spaces in CCN

A. Collaborative Wireless Access Networks

As previously mentioned, we focus on an environment where wireless coverage overlap in densely populated areas. Imagine an environment with high rises of apartment blocks. Let’s assume that every apartment deploys an AP and that there are numerous high rises tightly located as is the case in many major cities. In such a scenario, each spatial location may very well be covered by tens or even hundreds of APs. Current wireless systems do not consider such a dense deployment, rather each AP administrator is assumed to actively try to avoid overlapping coverage by frequency selection. This process is flawed since a) consumers cannot be relied upon to make site surveys and select appropriate channels and b) even if they would have this capacity the number of non-overlapping channels is limited. For example, in IEEE 802.11b/g the number of non-overlapping channels is 3 and in 802.11a it is 12 where 8 are used for normal access and 4 are used for outdoors point-to-point connections. Thus, even with maximum separation it is possible that many APs would share a channel.

Sharing a channel by APs can become a critical issue depending on access technology and application type. Let’s examine IEEE 802.11. This standard uses two modes of operation for channel access depending on traffic type. The most commonly used mode is best effort data which uses the Distributed Coordination Function (DCF) mode, based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). If the data is delay sensitive, such as streaming media or interactive traffic, CSMA/CA is a poor choice. The 802.11 standard offers two alternative access methods for such traffic. First, the Enhanced Distributed Channel Access (EDCA), which is a DCF with priority scheduling. It has been shown that this scheme performs poorly when the channel becomes saturated [14]. Second, the standard offers the optional Point Coordination Function (PCF) and Hybrid Coordination Function (HCF) channel access modes which are based on a polling mechanism. The support for these classes of traffic will degrade rapidly in overlapping environments because the polling mechanism requires a deterministic behaviour from the nodes (AP is the master and computing devices are slaves). When there are competing APs this no longer holds true and the polling mechanisms can no longer control the environment.

Considering the above, there is a need to revise the way channel access mechanisms are viewed and the functions they

should provide when constructing CCNs. Since the main two aims of the project is to maximise the utilisation of the fixed access network capacity and to provide high-accessibility and high-capacity public network access, we need to revisit the very core of WLAN construction. We build our research on three assumptions: (i) wireless devices (wireless access points included) will be able to communicate with multiple APs, (ii) APs will collaborate in order to achieve the best common good, and (iii) there will be infrastructure support for computational intensive tasks.

The first assumption can easily be realised even if the different APs use different frequency bands if the hosts are multi homed. In addition, more recent radio implementations have the capability to operate in different frequency bands concurrently which makes the implementation of multi homed radio especially attractive. For example, the Super-G chipset from Atheros [4] can concurrently operate in the 2.4 GHz and the 5 GHz bands.

We look at two major research issues within the collaborative wireless access networks stream. The first research issue we address is the configuration of the wireless environment to achieve optimum utilisation of wireless resources. The second research issue we address is the load balancing of traffic over the fixed broadband links to the access points. We discuss these below.

1) *Configuration of the Wireless Environment*: The goal is to achieve optimum utilisation of wireless resources. There are a number of dimensions to this problem. First, the available frequency bands should be divided among the access points so that competition for resources is kept to a minimum. Second, radio output power can be used to limit the scope of access points so that frequency bands can be reused. Third, the admission of traffic should be distributed in such a way that saturation of individual access points is avoided. Finally, since we aim at constructing a public access network it is important that the network not only provides high capacity but also high availability. To this end, we investigate how to fail-safe the communications channels by the addition of node redundancy. In effect, if the offered traffic load allows it, nodes can be put in stand-by mode to allow fast fail-over switching should an active access point fail.

All these functions are negotiated by the wireless access points resulting in network auto-configuration. We are focussing our efforts in two areas to realise this goal. The first effort relates to the configuration itself where we use algorithmic techniques to determine the optimum division of resources and configuration of individual nodes. The second effort is related to the willingness of the access points themselves to participate in the collaboration and behave “nicely”. To this end we are investigating game theoretical approaches.

2) *Traffic Load Balancing*: The second research issue we address is the load balancing of traffic over the fixed broadband links to the access points. In this area we are focussing on two individual problems: (i) the assigning (lending) of resources to visiting nodes, and (ii) the mapping of flow characteristics to link characteristics. The first issue relates to admission control

for maximum utilisation of spare resources while protecting prioritised traffic (traffic from access point site occupiers). In this work we combine traditional admission control techniques with machine learning techniques to be able to predict an expected network behaviour after a flow has been admitted. The second issue is an effort to admit flows to broadband connections taking the symmetry of the traffic into account. Consider an ADSL link with a downlink capacity of 1.5 Mbps and an uplink capacity of 256 kbps. If highly symmetrical traffic is admitted over this link the limited uplink capacity may in effect starve the downlink. For example, if the uplink is saturated, TCP traffic will not be able to fill the downlink since the acknowledgments will have to travel over the uplink. By removing some of the symmetric traffic to another link, enough capacity can be freed for TCP to fill the remaining capacity of the downlink.

B. Distributed Processing Platform

Our model builds on the usage of spare computational capacity at residential gateways for algorithmic processing. The processing is done to make the access network autonomous as discussed earlier. In this section, we detail our specific concerns in the distributed processing part of the project.

A Collaborative Community Network (CCN) can be viewed as a large distributed computing environment. However, such environment has different constraints and requirements to those of traditional high performance computing systems. One of the major problems in a CCN environment is that of task scheduling. Since tasks are not expected to be interrelated in such an environment, the problem reduces to one of task-allocation and most of the effort will focus on load-balancing to equally spread the load on the RG processors and maximise their utilisation while minimising the total task execution time [9].

In order to achieve these goals, the load-balancing mechanism should be ‘fair’ in distributing the load across the RGs. This implies that the difference between the heaviest-loaded and the lightest-loaded nodes should be minimised. Therefore, the processor load information on each RG must be updated constantly so that the load-balancing mechanism can be more effective. Moreover, the execution of the dynamic load-balancing algorithm should not take long to arrive at a decision to make rapid task assignments [15]. In general, load-balancing algorithms can be broadly categorised as centralised or decentralised and dynamic or static.

In a centralised load-balancing algorithm, the global load information is collected at a single RG, called the central scheduler. This scheduler will make all the load-balancing decisions based on the information that is sent from other RGs. In decentralised load-balancing, each RG in the system will broadcast its load information to the rest of the RGs so that locally maintained load information tables can be updated. As every RG in the system keeps track of the global load information, load-balancing decisions can be made on any RG.

A centralised algorithm can support a larger system as it imposes fewer overheads on the system than the decentralised

(distributed) algorithm. However, a centralised algorithm has lower reliability since the failure of the central scheduler will result in the dysfunction of the load-balancing policy. Despite its inability to support larger systems, a decentralised algorithm is also easier to implement. In the case of CCN a hybrid approach, which is more fault-tolerant than a centralised algorithm, is more appropriate than a fully distributed algorithm.

Moreover, for static load-balancing problems, all information governing load-balancing decisions is known in advance. Even though they are easier to implement than dynamic load-balancing they are inappropriate for CCNs. We are therefore focussing our efforts on devising a combination of a hybrid centralised/distributed and dynamic load-balancing scheme.

V. SECURITY ISSUES

The very fundamental security requirement for making the CCN a viable architecture is to protect the infrastructure owned by individual residential users from abuse by visitors. The challenge lies in zoning of resources and properly restricting and enforcing visiting access to only the broadband access.

Having kept the home network infrastructure safe from unauthorised users so that the gateway owners will be willing to take part in forming a CCN, the security requirement will be focused on two major issues: i) network access control, and ii) data security/privacy. The recent security ratifications from IEEE task group i (TG1) [2] has defined several security remedies to be taken for WLANs. It has recommended 802.1X port-based access control which includes authentication-based key derivation [1]. An AAA server is to be used for authentication and key derivation; RADIUS is commonly used for this purpose. By using 802.11i's four-way handshake mechanism, various keying material is derived for use in the communication between an AP and a MN. The weaknesses of WEP, which was the pre-802.11i security standard of IEEE, have been addressed by 802.11i. The outstanding matter from 802.11i is the scope of pre-authentication, and access control decision, to be usable for CCN.

Pre-authentication was specified within the 802.11i specification for reducing the time required for authentication during each handoff to a new AP within the same Extended Service Set (ESS). This is because real-time applications will suffer from the long time needed for a full EAP-TLS based authentication proposed in the 802.11i ratifications. The reason for this limitation to a single ESS is because the standard stipulates the use of EAP over LAN which has a limited scope. Since in a CCN, each AP constitutes an ESS this method will fail and we are therefore investigating alternatives.

For WLANs, access control decision is taken usually by the central RADIUS server on behalf of the entire network. In the case of CCN, network access control is more complicated because each AP represents an individual WLAN, and there are many of them composing the access network. Each AP may have its own criteria for allowing access which is based on various unique contextual information. We focus on a smart

authentication solution that will be capable of the following: i) reduce the time and/or frequency for authentication ii) be applicable for stationary handoff due to load-balancing etc., and iii) be applicable in inter-domain handoffs.

VI. CONCLUSION

This paper has presented an overview of project TITAN. The paper aims at raising awareness of the potential benefits of constructing public wireless access networks using residential sites and also the problems associated with using existing wireless standards for this purpose. We have presented the unique approach of using spare capacity on residential gateways as a distributed processing platform for advanced algorithmic processing in order to make the network autonomous. This distributed platform will enable the network to perform a range of functions such as load balancing, anomaly detection and traffic scheduling without external intervention. We have also presented the main research problems we are investigating within the scope of CCNs in order to build a functioning system.

Even though this way of constructing wireless public access networks is new and exciting, there are many outstanding issues in need of addressing before such a system can be deployed. A large effort is needed in determining commercial aspects such as business models and consumer packaging. In addition, integration into existing wide area wireless and wired infrastructure needs to be investigated.

Acknowledgment- Titan is a Smart Internet Technology CRC funded project.

<http://www.smartinternet.com.au/SITWEB/index.jsp>

REFERENCES

- [1] IEEE Standard for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std. 802.1X-2001, June 2001.
- [2] IEEE 802.11i: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancement, June 2004.
- [3] Airpath wireless, inc., <http://www.airpath.com/>.
- [4] Super g maximizing wireless performance, atheros communications white paper, url: http://www.superg.com/atheros_superg_whitepaper.pdf, march 2004.
- [5] Boingo wireless, inc , <http://www.boingo.com>.
- [6] S. M. Cherry. What Went Wrong at Ricochet? *IEEE Spectrum*, 39(3):60–61, March 2002.
- [7] R. Karrer, A. Sabharwal, and E. Knightly. Enabling Large-scale Wireless Broadband: The Case for TAPs. In *Proceedings of 2nd Workshop on Hot Topics in Networks (HotNets)*, November 2003.
- [8] A. Raniwala and T c. Chiueh. Architecture and Algorithms for an IEEE 802.11-based Multi-channel Wireless Mesh Network. In *Proceedings of IEEE INFOCOM*, April 2005.
- [9] S. Salleh and A. Y. Zomaya. *Scheduling In Parallel Computing Systems: Fuzzy and Annealing Techniques*. Kluwer Academic Publishers, USA., 1999.
- [10] Surf and sip network, <http://www.surfandsip.com/>.
- [11] Cellular online, <http://www.mobileoffice.co.za/>.
- [12] IEEE 802.11s: ESS mesh networking, http://grouper.ieee.org/groups/802/11/reports/tgs_update.htm.
- [13] T-mobile hotspot provider, <http://www.t-mobile.com/hotspot/>.
- [14] W. Wang, S.C. Liew, and V.O.K Li. Solutions to Performance Problems in VoIP over a 802.11 Wireless LAN. *IEEE Transactions on Vehicular Technology*, 54(1):366–384, January 2005.
- [15] A.Y. Zomaya and Teh Y.-W. Observations on using genetic algorithms for dynamic load-balancing. *IEEE Transactions on parallel and Distributed Systems*, 12(9):899–911, 2001.

School of Information Technologies
Madsen Building F09
University of Sydney NSW 2006 AUSTRALIA
T: +61 2 9351 4917 F: +61 2 9351 3838
W: www.alumni.it.usyd.edu.au

ISBN 1 86487 794 4