The Case for Virtualized Wireless Access Networks

Frank A. Zdarsky, Ivan Martinovic, and Jens B. Schmitt

disco | Distributed Computer Systems Lab
University of Kaiserslautern, 67655 Kaiserslautern, Germany
{zdarsky,martinovic,jschmitt}@informatik.uni-kl.de

Abstract. Densely populated areas such as city centers are often sprinkled with numerous wireless access points operated for commercial or private use. Together they create what's known as *tragedy of the commons* phenomenon: without proper coordination, a significant amount of license-exempt radio frequency resources is wasted due to contention at shared medium access. In this paper we argue that both commercial and private operators would benefit if their access points were enabled to cooperate and form a single virtual access network that manages available radio resources itself in a globally optimal way. On top of this virtual network, each operator would then allocate resource shares for his own disposal. As a first step towards this vision we then present a distributed algorithm and protocol that allows previously unrelated access points to form and manage a single network in a self-organized manner and demonstrate its effectiveness.

1 Introduction and Motivation

The airspace is becoming crowded as increasingly many IEEE 802.11-based wireless access points are deployed in close proximity of each other. Many of these access points are part of small home or company networks that restrict access to few selected clients, while others belong to networks that try to reach city-wide coverage and offer Internet access to a wide audience. Such large-scale wireless access networks are often deployed for profit by wireless ISPs. However, wireless community networks (e.g. [1]), which offer free Internet access based on spare capacity donated by their members, are rapidly gaining in popularity. Furthermore, some cities are deploying so-called "municipal wi-fi" networks offering Internet access free of charge[2]. As a consequence of these parallel infrastructure deployments, "hotspot areas" may be covered by several networks at the same time. In fact, as observed in [3], areas with densities of more than 10 (and even up to 80!) overlapping access points are not uncommon in some major U.S. cities.

Considering that the number of non-overlapping channels available for IEEE 802.11 wireless LANs is very low and that this number will be reduced further by channel combining techniques intended to increase transmission speeds, it is not surprising that network performance in environments with high access point densities is severely degraded due to contention at shared medium access. As a result it becomes challenging at least to provide a certain service with a reliably high quality, which is unfortunate in particular in the light of such applications as Voice/Video over WLAN. While each provider may locally optimize his network, choosing the best installation sites and operation parameters for its access points, the lack of information about neighboring access points means that from a global perspective the available license-exempt frequency resources are not utilized to their full potential. This is especially true compared to a well-planned wireless network operating in licensed frequency bands.

Economists use the term "tragedy of the commons"[4] to denote a class of phenomena in which the use of a common good (here the license-exempt frequency resources) by utility-maximizing individuals leads to very low overall utilizations of the good. Their solution is to either restrict the use of the common good to selected individuals or to introduce binding cooperation mechanisms between individuals[5].

We contend that all operators of access points, commercial or private, would benefit from the introduction of cooperating mechanisms between their wireless LANs as well. In this paper we therefore introduce the concept of a *virtualized wireless access network*. The basic idea is to allow wireless access points from different physical networks and operators to form a single virtual access network that self-manages its available resources as efficiently as possible. Then, on top of this virtual access network, each contributor to the network may then create a logical access network that uses a share of the managed resources which is proportional to the amount of the original contribution. Logical networks should appear to wireless clients as independent physical networks and allow providers to offer the same set of services as in their own physical network and under the provider's branding.

The virtualized wireless access network has advantages for both private users as well as commercial users:

- Wireless ISPs benefit from reducing their deployment and maintenance cost and may be able to serve customers in locations where they do not have own installation sites for access points or where these sites are not profitable. Most importantly, however, they do not have to concern themselves with radio management of their access network anymore and may offer a more reliable service to their customers, as contention from other wireless LANs is reduced.
- Private users benefit from lower contention from other LANs as well, but also from the possibility of free access in other locations of the city, where participating access points are available.

In the following section we discuss related work, before giving a more in-depth overview of technical aspects regarding virtual wireless access networks in section 3. We demonstrate in section 4 that cooperation between wireless LANs leads to a significant reduction in global network contention. Following this we introduce in section 5 a distributed algorithm and protocol that allows access points to form a virtual network and manage its resources in a distributed, self-organized manner and evaluate the algorithm in section 6, before concluding the paper with a brief outlook.

2 Related Work

Our proposed concept of a virtualized wireless access network is in fact the logical extension of the concept of a *virtual access point*[6] that has recently caught on with wireless ISPs, as it allows them to share access point deployment, and maintenance cost. The difference is that we envision a single, city-scale access network to which private households may contribute (and benefit from) just the same as commercial or public ISPs. This network should be self-forming and self-managing, as the nature of this network does not lend well to a centrally managed network.

One objective of a self-managing virtual wireless access network should be to utilize available resources efficiently by minimizing contention in the network. A number of contributions in the literature have already treated the general wireless LAN planning problem. These schemes are of little use in our context, as they assume that a very regular and optimal placement of access points is possible. Nevertheless we mention them for completeness: [7] have formulated an access point placement problem with the objective of minimizing contention, [8] a channel assignment problem. Joint placement and channel assignment schemes have been proposed, where co-channel overlapping may be allowed [9] or not [10]. In contrast to these contributions on the *planning* of wireless LANs, in [11] we proposed a model for the case where access point locations are already given and the problem is to determine the configuration of transmission power, channel assignment and associations of stations to access points that minimizes contention in the given network.

Online radio resource management schemes, on the other hand, are more closely related, as they assign operating channels, control transmit power, and perform load balancing of stations over access points online. Both centralized and decentralized schemes have been proposed in the literature (e.g. [12] and [13], respectively) and are used in existing products (e.g. [14] and [15], respectively). Their focus lies on controlling contention inside a single, closed, well-planned network domain, though. The problem of actively controlling inter-domain contention has received little attention in the literature. [16] suggest the use of a radio resource broker that tries to control contention between different wireless LANs by assigning to each LAN the set of channels and transmission powers that it may use. This centralized approach seems to be most appropriate for a small number of networks whose operators have reached agreements concerning the use of such a broker. Finally, [3] suggest algorithms that allow access points to adjust transmission power levels and rates automatically and independently from other access points.

3 Virtualized Wireless Access Networks

A *virtualized wireless access network* (VWAN), as used in this paper, is characterized by the fact that it consists of a set of wireless access points (APs) from different physical access networks (usually belonging to different administrative domains). These APs manage available resources themselves rather than requiring central management. They manage resources in a way that maximizes the *global* utilization of the network, and they allow logical subnetworks to be formed on top of the VWAN. In this section we describe the operation of a VWAN and discuss the most important design issues, some of which are still open at this point.

Creation and Maintenance of a Virtualized Wireless Access Network. Adding an access point to an existing VWAN should be an automatic process and should not require manual intervention of an operator. Therefore, an AP should on power-up perform a passive or active scan of the wireless medium for other APs that are already part of the VWAN. This is recognized by the presence of a specific Information Element (IE) contained in the periodically broadcasted beacon management frames of member access points. This IE also indicates the IP address at which the AP sending the beacon may be contacted by the new member. All further communication between the new AP and the old members is then sent via the wired backbone. During the life-time of the VWAN, APs are constantly monitoring whether a reconfiguration of the network with respect to channel assignment, transmit power settings, association of stations to access points, etc. would lead to a higher utilization of network resources. If so, this reconfiguration is performed automatically, without requiring intervention by the owners of the APs. In section 5 we propose an algorithm and protocol that enables such self-management of access points.

Creation of Logical Subnetworks. Every operator of an AP that is part of the VWAN may monitor the current state of the whole network, e.g. querying information about the number, locations and utilizations of other APs in the network. To create his own (logical) wireless access network, the operator may then select a subset of available physical APs and assign a resource share of each AP to the logical access network. This allows operators to serve customers in areas where they do not have infrastructure of their own. The amount of resources that an operator may reserve for his logical network should be a function of what he has contributed to the VWAN. How exactly the "exchange rate" is determined is still an open issue. However, it might be reasonable for operators to earn more credit for establishing access points in areas where only few access points already exist, spend more on resources of popular access points, and have a discount on using resources on own access points.

Sharing of Access Points. The sharing of a physical AP between different operators is enabled by a concept called *virtual access point* (VAP)[6]. A VAP is a logical entity that exists within a physical AP. When a single physical AP supports multiple VAPs, each VAP appears to stations to be an independent physical AP. A VAP is an emulation of a physical AP at the MAC layer. This has the advantage that no additional radio hardware is needed to implement VAPs. On the other hand this means that all VAPs of a single physical AP operate on the same channel, which is not a real restriction in this context, though.

The most common way of implementing VAPs is to assign each VAP its own BSSID (the IEEE 802 48-bit MAC address of the AP) and to let each VAP broadcast its own beacon frames. As beacons contain the SSID (the 32 byte network identifier string) and the capability information for each network, it is possible for providers to use their own branding for their VAPs and offer different authentication mechanisms, transmission rates, etc., despite sharing a single physical AP. A disadvantage of sending one beacon frame per VAP is the increased bandwidth overhead, which means that this approach does not scale abritrarily well. However, as nicely argued in [6], other approaches of using only a single BSSID and single or multiple SSIDs per beacon do not offer the same functionality or are not compatible with legacy stations. Furthermore, the same scalability issues would arise when using different physical APs. A solution may be to aggregate some logical wireless access networks under the same VAP, which should at least be possible for those operators that are not commercial ISPs, but maybe members of a wireless community network.

Sharing of Internet Uplinks. As argued in the introduction, we see benefits in allowing home users to participate in the VWAN as well. This raises questions on whether their uplink to the Internet is sufficient for this type of application. However, this problem is analogous to that in wireless community networks. Some of the more sophisticated open-source AP firmwares that specialize on wireless community networks (e.g. DD-WRT [17]) are already using techniques which may to some extent also be applied in this context.

A first issue is the available bandwidth in the wired uplink to the Internet. Using QoS mechanisms it is not difficult to isolate the traffic of different VAPs and assign them the share of resources that the VAP's operator has paid for. But is the capacity of the Internet uplink sufficient to make it worthwhile for a commercial wireless ISP (WISP) to use APs of home users? At the moment, many households have Internet uplinks that are much slower than an IEEE802.11a wireless access link. However, considering the increasing availability of high-speed Internet access, such as ADSL2+, in private households, due to the convergence of Internet, Television, and Telephony (so-called "triple-play"), the gap between wireless and wired link capacities in home networks may become much narrower in the future. Furthermore, in wireless community networks using mesh-routing, but also in so-called mushroom networks[18], it is not uncommon to route traffic to the Internet via wireless links to multiple wired uplinks, thereby increasing the available uplink capacity.

Secondly, there is the problem that home users are usually assigned a single IP address by their ISP, which is furthermore often only dynamically assigned. Again, wireless community networks show that with NAT and port forwarding this need not be an issue. When IPv6, and in particular MobileIPv6, continue to gather momentum, this problem may also be mitigated.

Until then our approach is to set up static tunnels from each VAP in a foreign network to the respective provider's home network and use GRE to tunnel data between the two. This has the advantage that to both provider and its customers this process is transparent: they will not notice that they are in a different network, other than an increase in round-trip-time.

Security Issues. There are several security issues that have to be solved to make VWANs fully usable. For example, can a WISP trust a home user (and vice versa) not to tamper with the wireless AP in order to eavesdrop on connections or tamper with accounting? How can it be monitored that a VAP actually provides the assured bandwidth share? We cannot yet offer satisfactory solutions to these problems and leave them for future work.

4 Effect of Cooperation on Contention

In this section we describe an experiment that exemplifies the significant reductions in network contention that may be gained through cooperation between operators of wireless LANs for different access point densities. This evaluation is based on the mathematical optimization framework that we proposed in [11]. It allows to determine the channel assignment, transmit power setting and station association that minimizes the contention level in a network. The contention level counts how many nodes actually interfere with a given node's transmission, summed over all nodes. We refer the reader to our previous work for further details.

Our reference scenario contains 25 access points (APs) arranged on a 5x5 grid. The distance between grid lines is chosen as twice an AP's transmission range, in other words the distance at which a node can just receive the AP's signal at its minimum required power level. We then generate two stations per AP, one located somewhere at the maximum transmission range, the other located between the AP and the maximum transmission range, with uniform distribution.

Path losses between each pair of nodes are calculated based on the empirical indoor propagation loss model recommended in ITU-R P.1238-2 [19]. The maximum transmission power of each node is assumed to be 20dBm (or 100mW), which is the maximum power allowed for IEEE 802.11b wireless LANs in Europe. We assume that a node detects a busy medium when interfering signals are stronger than -84dBm and that it requires a minimum signal strength of -82dBm to successfully decode a signal. These are typical values for an Orinoco Gold IEEE 802.11b adapter. The number of non-overlapping channels is assumed to be 3.

The APs of the reference scenario described above are then squeezed towards the center or stretched away from it to yield new scenarios of different AP densities. This technique is analogous to the one used in [3]. We create scenarios with stretch factors between 0.0 and 1.5, where a stretch factor of 1.0 denotes the reference scenario, and a stretch factor of 0.0 the situation where all APs are squeezed together at the center.

For all scenarios we use our optimization framework to determine the minimal possible contention level that may be achieved by standard non-cooperating wireless LANs and compare them to those that may be achieved by wireless LANs which cooperate in reducing contention. In the non-cooperative case, access points select their operating channel independently from their neighbors by scanning for free channels and then choosing a free channel or, if no free channel is available, one of the busy channels randomly. The results are shown in Fig.1, which for reference also includes a theoretical lower bound (TLB) that denotes the lowest contention level for any set of networks with the given number of access points and stations.

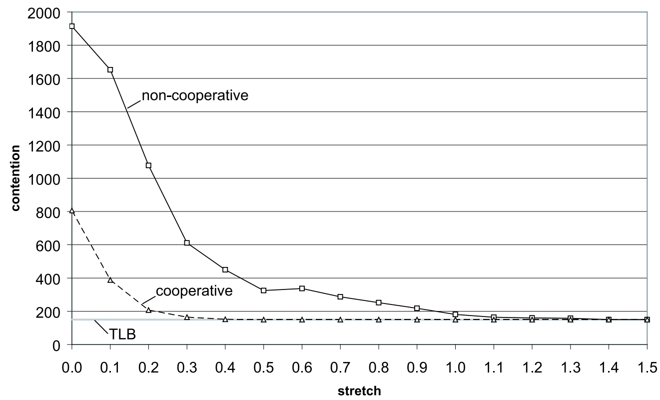

Fig. 1. Contention levels with and without cooperation for varying access point densities.

The results show that in very sparse wireless LAN scenarios, non-cooperative wireless LANs achieve the same or only slightly worse contention values than cooperative LANs. As the density increases (that is the stretch factor decreases), contention in the non-cooperative approach increases rapidly, as more and more co-channel overlapping occurs. The slight decrease at a stretch of 0.5 can be explained by the fact that starting from this stretch APs are in direct transmission range of each other and therefore try to change to a free channel if possible. In contrast, cooperation between wireless LANs, that is coordinating the use of operating channels and station associations, reduces contention significantly (for example already by a factor of 2 at stretch 0.5) even when AP densities are high.

Note that contention occurring at stretch factors >1.0 is due to the fact that while nodes at this distance are outside their transmission range as specified above, the strength of the received signal may still be greater than the signal strength at which the Clear Channel Assessment function of a node reports a busy channel.

5 Distributed Coordination Algorithm

In this section we propose a distributed algorithm that allows neighboring access points to cooperatively reduce contention, based solely on joint knowledge about their vicinity. It consists of five modular building blocks:

- *Data dissemination*, in which an access point (AP) discovers other APs within its horizon and collects information about the stations (STAs) that each of these APs is aware of and is able to cover at the required signal strength.
- *Local negotiation*, in which an AP suggests a local reconfiguration of the network to all APs within its horizon, waits for their feedback on how this reconfiguration would affect network performance in their vicinity and then decides either to commit or abandon this reconfiguration.
- A *fitness function* with which to evaluate the current state of the network within an APs horizon and the effect of a proposed reconfiguration.
- A *local reconfiguration algorithm* that is used to find better local reconfigurations.
- A *coordination mechanism* to determine, which APs are allowed to propose local reconfigurations and when.

An AP's *horizon* defines which other APs and STAs in its geographical vicinity it knows and cooperates with in finding improvements. When choosing the extent of the horizon, one has to make the typical trade-off between the chances for finding the globally optimal configuration and the computational effort and signaling overhead. In our experiments we have defined the horizon of an AP i as the set of all APs whose transmissions AP i can receive directly or can infer from listening to stations from other APs in range.

5.1 Data Dissemination

APs initially find out about their neighbors by scanning for periodic beacon signals on all available channels. Upon receiving a beacon from a previously unknown neighbor, the AP sends out a WELCOME message to its new neighbor, both on the wireless link and on the wired backbone network. This assumes that the IP address of the new neighbor is known. The most simple solution is to let each AP include its IP address as an additional Management Frame Information Element in its broadcasted beacons.

Both the WELCOME message and the reply to it (WELCOME_ACK) contain information about the sending AP as well as about all STAs which the sending AP is currently aware of and whose minimum signal strength requirements it can meet. By sending these messages over both the wireless link and the backbone, we can further gain information about whether the wireless link is asymmetric or not, that is if one access point is able to hear the other but not vice versa.

Furthermore, all active APs periodically send UPDATE messages to all APs within their horizon containing their current STA information list. This information has an explicit expiration time, so if an AP does not receive UPDATE messages from a neighbor for a certain duration, it assumes the neighbor has deactivated without signing off. UPDATE messages are always sent via the wired backbone, so that this soft-state approach does not consume valuable wireless resources.

We also consider the case that two APs that cannot hear each other directly nevertheless produce contention in each other's BSS. This may happen when an STA is located in between the AP it is associated to and another AP that is within contention range. The STA may then notify its own AP of the contending AP's presence so that both APs may contact each other using the mechanism described above.

5.2 Local Negotiation

Based on its knowledge about APs and STAs within its horizon, an AP may run a local optimization algorithm to search for better configurations for itself and its neighboring APs. If an AP finds a configuration that improves contention within its own horizon, it suggests the new configuration to its neighbors by sending them an OFFER message with the new configuration.

Upon receiving an OFFER, every neighbor determines the effect of the configuration change on their part of the network. Note that the sets of nodes within the horizons of the APs sending the OFFER and receiving the OFFER is usually not identical, although the intersection should usually be large. All receivers of an OFFER then answer with an OFFER_REPLY message containing the predicted change in contention that would result from actually committing the configuration change. If the net effect of the reconfiguration proposal is positive, the initiating AP sends a COMMIT message to all neighbors, who then update the local knowledge about their neighborhood and possibly change the radio channel they operate on or instruct individual STAs to reassociate with a different AP.

There are three cases in which the initiating AP sends a WITHDRAW message to its neighbors in order to cancel a reconfiguration attempt. The first case is that the initiator calculates a negative or zero net effect of the reconfiguration proposal. Secondly, it may happen that one of the receivers of an OFFER message is already processing a reconfiguration proposal by a different AP which has not been committed or rejected yet. It then refuses the new OFFER by answering with a BUSY message. Finally, if at least one of the neighbors does not respond to the OFFER within a certain time interval, the initiator assumes the message was lost or the receiver has deactivated.

5.3 Reconfiguration Algorithms

In order to find a reconfiguration that yields a lower amount of contention, an AP applies an optimization algorithm to the set of APs and STAs within its horizon, including itself. We have experimented with two optimization algorithms: a problem-specific genetic algorithm[11] and with a greedy heuristic which we termed "balance or conquer".

This heuristic is inspired from previous findings that balancing of STAs between APs, where possible, leads to low contention values if there is no contention between different BSSes. In the presence of inter-domain contention, however, load balancing may actually be detrimental to reducing contention.

The "balance or conquer" heuristic owes its name to its repertoire of four strategies for improving contention:

1. Try to transfer STAs to (from) other APs such that the number of STAs per channel (not per AP!) is roughly the same within the horizon (= balance). Change your own channel, if necessary.
2. Find another AP whose stations you can cover completely and take them all (= conquer), effectively switching the other AP off.
3. Try transferring all stations to other APs, balancing the number of STAs per channel, effectively switching yourself off.
4. If currently switched off, try to incrementally take over STAs (starting with the nearest one) from other APs, as long as this does not increase contention. Change your channel, if necessary.

During a single run of the heuristic, an AP instantiates the optimization model with the knowledge it has collected. It then computes the change in contention that would result from applying each of the four strategies and then greedily picks the one with the highest presumed benefit.

5.4 Coordination of Reconfigurations

The last building block of our algorithm is concerned with the question *when* APs attempt to find and propose an improved configuration. We have used both an uncoordinated approach, in which each AP performs reconfiguration attempts as a Poisson process. Furthermore, we have used two token-passing algorithms, where an AP currently holding a token waits for a random time interval before attempting to propose a reconfiguration. Whether this proposition was successful or not, it then passes the token on to a randomly chosen neighboring AP. The two token-based approaches differ in that the first approach starts with a single token that circulates the network, while in the second all APs initially hold a token. When an AP receives a new token from a neighbor while already holding one, the new token is destroyed, so that eventually only one token remains in the network. Lost or destroyed tokens could be replaced by letting each AP generate a new token at a very small rate, which could vary with the amount of contention—and therefore the necessity for a new token—within an AP's horizon.

The rationale behind experimenting with different reconfiguration coordination approaches is that one can expect the global level of contention in the system to decrease more rapidly when a high number of access points concurrently tries to find and propose reconfigurations, as is the case with the uncoordinated approach. On the other hand, when reconfigurations are made at different locations of the network at the same time, there is a chance that the effect of one reconfiguration is counterproductive with respect to another reconfiguration in the long run.

6 Experiments and Results

6.1 Performance of the Distributed Algorithm

In this section we conduct simulations to study how our distributed algorithm compares both to standard WLAN and the optimal solution in a cooperative scenario.

We use 10 different scenarios, each with 50 APs and 100 STAs within a 1km by 1km simulation area. A scenario is generated as follows: In a first step, 16 of the APs are placed to regularly cover the simulation area. Afterwards, the remaining APs are placed uniformly over the simulation area. The location of each STA is chosen by picking an AP randomly and then placing the STA within a distance of 10% to 90% of the transmission range of the AP, drawn from a uniform distribution. Node transmission and reception powers as well as the path losses are chosen as in the previous section.

As reference solution for each scenario we use the behavior of typical wireless LAN, but under the cooperation assumption. That is, STAs associate with the AP from which they receive the strongest signal, irrespective of the administrative domain the AP belongs to. Furthermore, all APs choose an unused channel or pick one randomly if all channels are already occupied. This reference solution also serves as the starting point for our distributed algorithm. To estimate the optimal configuration, we use a run over 100,000 iterations of our genetic algorithm, equivalent to roughly an hour's worth of computation on a standard PC.

We perform simulations both using the genetic algorithm (GA) and the balance-or-conquer (B|C) as local reconfiguration heuristics. In order to study the effect of concurrent reconfigurations versus sequential reconfigurations, we further use three different reconfiguration coordination approaches with both algorithms: Uncoordinated reconfiguration (0 tokens), token-passing with 1 token and N initial tokens, where N=50 (the number of access points). If no tokens are passed in the network, the generation of reconfiguration attempts per AP is a Poisson process with rate 1/s. If one or more tokens are present, the holding time of a token is exponentially distributed with mean 1s. Each simulation instance runs for one hour of simulation time and is repeated for each of the ten scenarios.

The resulting average contention values (both absolute and relative decrease compared to WLAN) and their standard errors are shown in Table 1.

Table 1. Comparison of contention levels achieved by the distributed algorithm using GA and B|C.

	WLAN	GA	Local GA			Local B|C		
initial tokens			0	1	N	0	1	N
mean	512.5 (0.0%)	374.5 (-26.4%)	409.8 (-19.8%)	411.5 (-19.3%)	413.5 (-18.9%)	454.0 (-11.1%)	416.8 (-18.2%)	425.3 (-16.6%)
std. error	18.8	7.2	13.6	11.9	10.9	15.9	10.6	11.6

Figure 2 additionally shows the development of the contention level over time for one of the simulated scenarios. As the global GA is only (albeit a very good) heuristic, it does not necessarily find the global minimum. As the optimization problem is far too complex to exactly determine the true minimum, we have additionally included the theoretical lower bound (TLB) which we derived in [11].

In our simulations, the GA version of our distributed algorithm manages to realize on average 65.5% of the improvement potential compared to WLAN, the B|C version 61.8%, both for the 1 token case. This corresponds to a decrease in network-wide contention by 19.3% and 18.2%, respectively. We note that both versions switch off a significant number of APs to achieve this result (12.2% and 13.6%, respectively), rather than balancing STAs across available APs.

Although both versions achieve comparable results, this does not mean that both versions are equally suitable for real-world application. The computational effort per search for a better local reconfiguration is on the order of two magnitudes higher for the genetic algorithm than for B|C, while only achieving slightly better results. Furthermore, the stability of the contention levels is not the same between the two versions as can be directly seen from Fig.2 as well.

We also observe that the choice of the reconfiguration coordination mechanism has a strong effect on the speed of the improvements in contention, but also on the quality of the attained contention level. Using no coordination between reconfiguration attempts of different APs leads to very quick improvements compared to the 1 token approach. Interestingly, though, in almost all cases the B|C heuristic is able to converge to lower contention levels the slower the rate of reconfigurations. The N token case is usually somewhere in between, reacting as the uncoordinated case when a large number of tokens is still present. Over time it converges to the behavior of the 1 token case, as more and more tokens are destroyed. Figure 3 shows the channel changes per second (as a total over the whole network) for the local GA algorithm and the 0, 1, and N token cases, which again supports the aforementioned observations.

6.2 Importance of Coordination

Finally, we would like to find out how important the local negotiation part is for our distributed algorithm. We therefore conduct a set of experiments in which we remove the negotiation process, so that an AP finding a better configuration

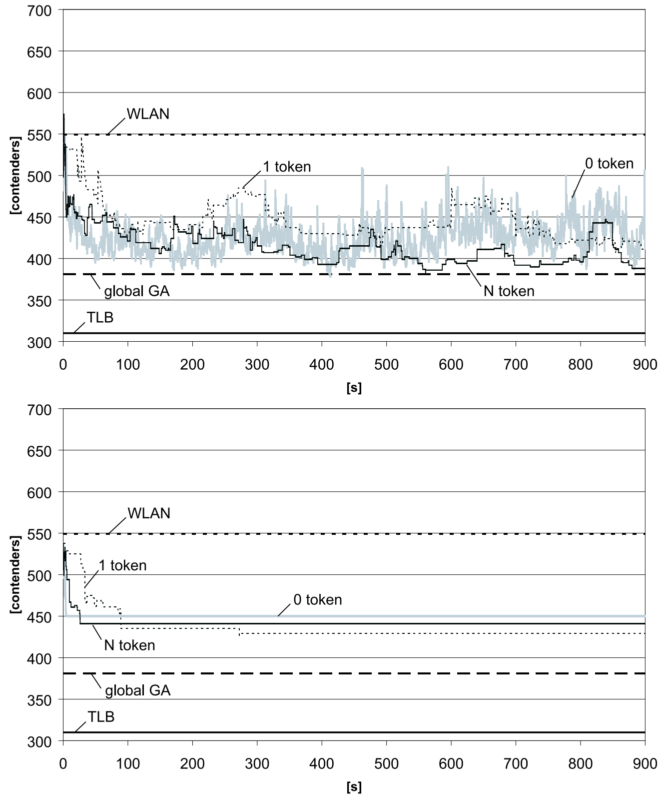

Fig. 2. Performance of GA (top) and B|C (bottom) as local reconfiguration algorithms compared to global minimum and WLAN.

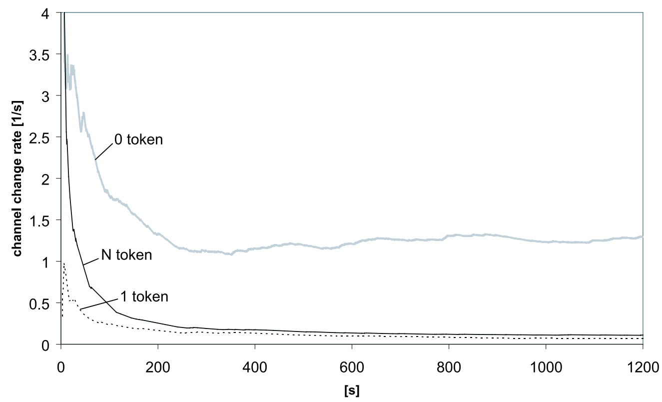

Fig. 3. Channel change rate of GA as local reconfiguration algorithm.

immediately commits the necessary changes instead of sending offers to all other APs within its horizon asking for feedback. The results of one of the scenarios are shown in Fig.4. Indeed, when an AP does not ask its neighbors for potential negative effects of a configuration change, it frequently happens that this AP reconfigures to gain a small improvement, but that this reconfiguration has strong negative effects on the network just outside its horizon. Affected APs may in turn attempt to improve their situation, possibly undoing the original changes. As a consequence, contention levels fluctuate heavily and may on the average even be higher than with plain WLAN.

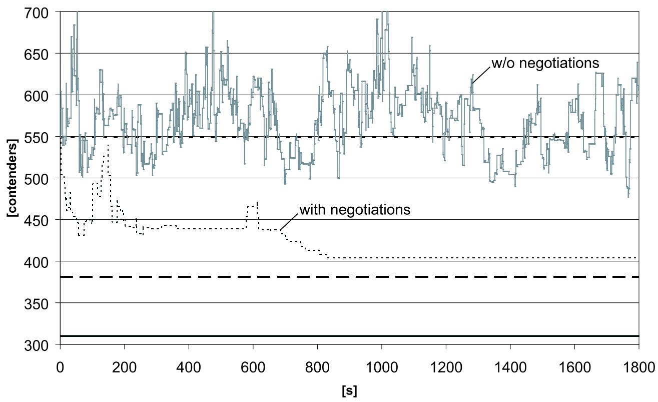

Fig. 4. Comparison of algorithm performance with and without negotiations.

7 Conclusions

In this paper we have introduced the concept of a virtualized wireless access network, which consists of wireless access points from many different operators, including those of both commercial WISPs and private households. Virtual wireless access networks are self-forming and self-managing, with the objective of minimizing contention between the participating access points and stations and of using the scarce license-exempt frequency resources as efficiently as possible. On top of this resource-efficient network, its various contributors may then create logical networks on which they may offer services under their own brand. We have argued why participation in a virtualized wireless access network may be beneficial for both commercial and private contributors. Furthermore, we have proposed a distributed algorithm and protocol allowing access points to cooperatively manage radio resources and have shown its effectiveness.

Currently we are working on a proof-of-concept based on a set of set of LinkSys WRT54G routers and the DD-WRT open source embedded Linux system, which already contains many of the required features.

References

1. NYCwireless (2006) http://www.nycwireless.net.
2. Singer, M.: 'Wireless Philadelphia' Sparks Concern (2004) http://www.internetnews.com/wireless/article.php/3442851 (last access: 2006-02-01).
3. Akella, A., Judd, G., Seshan, S., Steenkiste, P.: Self-Management in Chaotic Wireless Deployments. In: 11th International Conference on Mobile Computing and Networking (MOBICOM '05), Cologne, Germany (2005)
4. Hardin, G.: The Tragedy of the Commons. Science **162**(3859) (1968) 1243–1248
5. Ostrom, E.: Coping with Tragedies of the Commons. Annual Review of Political Science **2** (1999) 493–535
6. Aboba, B.: Virtual Access Points. 802.11 wg document, IEEE (2003) http://www.drizzle.com/\~aboba/IEEE/11-03-154r1-I-Virtual-Access-Points.doc (last access: 2006-02-01).
7. Amaldi, E., Capone, A., Cesana, M., Malucelli, F.: Optimizing WLAN Radio Coverage. In: IEEE International Conference on Communications (ICC 2004), Paris, France (2004) 180–184
8. Leung, K., Kim, B.J.: Frequency Assignment for IEEE 802.11 Wireless Networks. In: 58th IEEE Vehicular Technology Conference (VTC 2003 Fall), IEEE (2003) 1422–1426
9. Ling, X., Yeung, K.: Joint Access Point Placement and Channel Assignment for 802.11 Wireless LANs. In: IEEE Wireless Communications and Networking Conference (WCNC 2005). (2005)
10. Lee, Y., Kim, K., Choi, Y.: Optimization of AP Placement and Channel Assignment in Wireless LANs. In: IEEE Conference on Local Computer Networks (LCN 2002). (2002)
11. Zdarsky, F.A., Martinovic, I., Schmitt, J.B.: On Lower Bounds for MAC Layer Contention in CSMA/CA-Based Wireless Networks. In: 3rd ACM/SIGMOBILE International Workshop on Foundations of Mobile Computing (DIALM-POMC'05), Cologne, Germany (2005) 8–16
12. Hills, A., Friday, B.: Radio Resource Management in Wireless LANs. IEEE Communications Magazine **42**(10) (2004) 9–14
13. Wang, Y., Cuthbert, L., Bigham, J.: Intelligent Radio Resource Management for IEEE 802.11 WLAN. In: IEEE Wireless Communications and Networking Conference (WCNC 2004), Atlanta, Gergia USA (2004) 1365–1370
14. WS5100 Wireless Switch Reviewer's Guide. Product brochure, Symbol Technologies (2005) ftp://symstore.longisland.com/Symstore/pdf/wireless/WS5100ReviewersGuide.pdf (last access: 2006-02-01).
15. AutoCell—The Self-Organizing WLAN. White paper, Propagate Networks (2003) http://www.propagatenet.com/resources/docs/whitepaper_autocell.pdf (last access: 2006-02-01).
16. Matsunaga, Y., Katz, R.: Inter-Domain Radio Resource Management for Wireless LANs. In: IEEE Wireless Communications and Networking Conference (WCNC 2004), Atlanta, Georgia, USA (2004) 2183–2188
17. DD-WRT (2006) http://www.dd-wrt.org.
18. Mushroom Networks (2006) http://www.mushroomnetworks.com.
19. ITU-R P.1238-2: Propagation data and prediction methods for the planning of radio communication systems and radio local area networks in the frequency range of 900 MHz to 100 GHz (2001)