DSAP: A Protocol for Coordinated Spectrum Access

Vladimir Brik, Eric Rozner, Suman Banerjee
Department of Computer Sciences
University of Wisconsin-Madison
Madison, WI 53706, USA
{vladimir,erozner,suman}@cs.wisc.edu

Victor Bahl
Microsoft Research
One Microsoft Way
Redmond, WA 98052, USA
bahl@microsoft.com

***Abstract*— The continually increasing number of wireless devices operating in the unlicensed frequency bands makes the freely-available wireless spectrum a scarce commodity. Under such circumstances, wireless spectrum management is crucial to minimize the effects of overcrowding and maximizing quality of service. In this paper we design, implement and evaluate Dynamic Spectrum Access Protocol (DSAP), a centralized method for managing and coordinating spectrum access to arbitrary frequency bands in general, and unlicensed bands in particular, across diverse technologies.**

I. Introduction

Spectrum regulatory bodies like the Federal Communications Commission (FCC) in the US, and similar organizations across the world are recognizing the fact that the current spectrum allocation and access policy does not allow efficient use of the wireless spectrum. In a 2002 report by FCC's Spectrum Policy Task Force observed that the agency needs to modernize its nearly century-old policies on radio frequency management to match the new developments in wireless technologies, e.g., Software-Defined Radios [13], [12], and evolve towards a more flexible approach that allows greater spectral utilization [7]. One such approach is dynamic spectrum access, whereby access rights to parts of the spectrum are provided to users or entities on-demand through time-bound leases. In particular, the FCC in recent years has begun considering the feasibility of relaxing restrictions on unlicensed devices and allowing them to operate in the so-called "white spaces" in the broadcast spectrum and the spectrum of the 3.7 GHz band [15], [1]. This opens a possibility of intelligently using licensed bands for unlicensed networking.

To take advantage of such developments, in this work we propose a protocol called DSAP (Dynamic Spectrum Access Protocol) that enables lease-based dynamic spectrum access but through a coordinating central entity and allows efficient resource-sharing in these wireless environments. Analogous to DHCP that provides IP address leases to individual Internet hosts in a given network [5], DSAP is designed to provide spectrum leases to wireless devices in some geographic region, e.g., a home or an office building. While our approach is generalizable to any spectral band, in this paper we focus on the the unlicensed band and show how DSAP allows wireless devices to share spectral resources in an efficient manner.

With increasing dense deployment of wireless devices in the unlicensed bands, lack of spectrum sharing mechanisms (or spectrum etiquette) is a growing cause of concern. While some wireless access technologies, e.g., 802.11 WLANs, Bluetooth, have channel access mechanisms that allow its devices to share the channel amongst each other, none of these technologies have mechanisms that allow efficient discovery and coexistence with devices using other access technologies. Frequently such uncoordinated channel access among multiple technologies in the same part of the spectrum leads to poor performance for the competing devices [6], [4], [16]. We demonstrate this in Figure 1. Here two 802.11g nodes are involved in an ongoing UDP transfer. Nearly 30 seconds into this transfer, a neighboring pair of Bluetooth nodes begins their own transfer. As a result, the throughput of the 802.11g node pair diminishes. If, however, the 802.11g nodes are able to switch to a different frequency band, say the 5 GHz 802.11a band, the interference from the Bluetooth nodes can be avoided. In the example shown in the figure, DSAP triggers such a switch after detecting interference for 5 seconds, thereby eliminating interference between the Bluetooth and WLAN node pairs and restoring their throughputs. Clearly in absence of a protocol like DSAP performance of both node pairs would continue to suffer over the entire duration of the transfer.

The notion of spectral leases is not a new concept. In the current model of spectrum access, such leases are issued by the FCC through well-defined static licenses of exclusive use. More recently, some centralized and

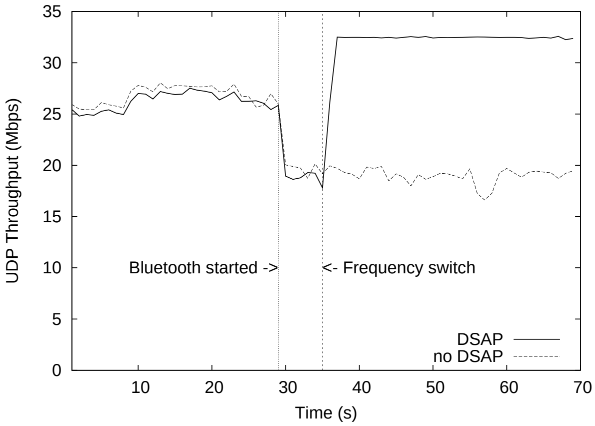

Fig. 1. Avoiding interference between Bluetooth and 802.11-based devices

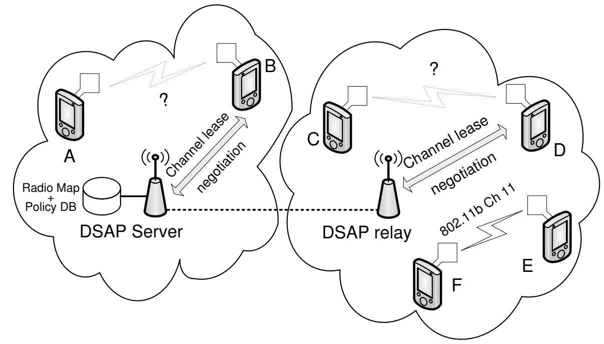

Fig. 2. Components of DSAP

distributed proposals, such as DIMSUMNet [3] and CSCC [18], respectively, have suggested dynamic leases for spectrum access.

Although a distributed approach to spectrum access control (such as CSCC) has its advantages, we believe that many practical environments, such as homes and offices, lend themselves well to a centralized design. Compared to the distributed approach, having a central spectrum access manager that possesses detailed information about the network allows for highly efficient wireless network configuration and better enforcement of a complex set of policies.

In their recent position paper, Buddhikot et.al. [3] proposed a practical dynamic alternative to FCC's current rigid spectrum licensing of radio spectrum. Their approach, called DIMSUMnet, is a centralized mechanism based on spectrum brokering that manages large portions of spectrum and assigns portions of it to individual domains or users. DIMSUMnet entails leasing parts of a Coordinated Access Band (CAB), a contiguous chunk of spectrum reserved for controlled dynamic spectrum access, to base stations or nodes equipped with special Adaptive Cognitive Radios. While the authors propose a mechanism to deal with densely populated local areas, it seems DIMSUMnet is best suited for spectrum brokering in a relatively large geographic region. In their work Buddhikot et.al. primarily examine architectural choices that allow flexible re-utilization of licensed spectral bands currently allocated to various operators, but often under-utilized. As a consequence, their suggested mechanisms need to tie closely to technologies used by such operators.

While our proposed mechanisms in DSAP align with the broad objectives of DIMSUMNet, they differ from that of the latter in multiple ways. First, DSAP, which has been implemented and evaluated, provides fine-grained, spectrum management in a relatively limited geographic area at fairly small timescales. Second, DSAP focuses only on negotiation mechanisms by which users can request and acquire communication rights to a part of the wireless spectrum. Beyond the negotiation mechanisms, DSAP does not dictate the choice of technology, protocol standards, or encoding mechanisms that users should employ for their communication. By design, DSAP is technology and protocol agnostic.

Overall, we envision DSAP and DIMSUMnet as being complementary, with DSAP acting as a spectrum broker for heavily-used, densely-populated localized areas where lease modifications and updates could occur frequently (possibly occurring several times a second) and with DIMSUMnet serving as a regional spectrum broker.

In summary, the following are the key contributions of this work:

- Detailed design of DSAP for dynamic spectrum access through centralized coordination and management, targeted to relatively localized geographic regions.
- Implementation of a DSAP prototype that allows efficient spectrum sharing for infrastructure-based as well as ad-hoc peer-to-peer style communications between users.
- Evaluation of DSAP through detailed experiments.

II. DSAP: Dynamic Spectrum Access Protocol

DSAP is a centralized protocol that provides dynamic allocation of wireless spectrum to network nodes. In brief, the goal of DSAP is to increase performance of wireless networks by intelligently distributing segments of arbitrary radio frequency spectrum to wireless nodes to avoid congestion and minimize interference, and to adjust the clients' wireless medium usage patterns to fit the administrator's needs.

In highly dynamic environments with a large number of network nodes it will be difficult for a node to maintain complete and up-to-date information about its surroundings. Without such knowledge, finding optimal wireless configuration may be impossible. A DSAP server, with the cooperation of network nodes, takes on the role of the spectrum arbitrator. The server stores information about its clients and channel conditions thoughout the network in a database that we call a *RadioMap*. Based on the issued leases, the set set of administrator-defined policies and the *RadioMap*, the DSAP server determines an "optimal" distribution of radio spectrum among the clients in the network and reconfigures the clients accordingly. We envision DSAP as a very dynamic protocol: if deemed advantageous, some configuration parameters on network nodes may be reconfigured several times a second, while others may remain unchanged for extended periods of time.

A. Protocol Entities

As part of the protocol we define three DSAP entities (see Figure 2):

DSAP client: Any wireless device that uses DSAP for coordinated spectrum access is called a DSAP client. A communicating DSAP client will not choose a wireless communication channel arbitrarily. Instead, before communicating on a channel, a DSAP client will request appropriate channel assignment from a centralized entity (DSAP server).

DSAP server: This is the centralized entity that coordinates spectrum access requests. It accepts spectrum lease requests from clients, compares such requests to ongoing communication and spectrum assignments as well as a local "policy database" populated by an administrator that guides spectrum management decisions, and responds back with an time-bound spectrum allocation.

DSAP relay: This is an entity that allows multi-hop communication between DSAP servers and clients that are not in direct range of each other. Note that a DSAP client may also serve as a DSAP relay for other clients.

B. General Concepts

At the heart of DSAP is the concept of a (channel) *lease*. A lease is a collection of configuration parameters assigned by a DSAP server to a client. Basically, a lease gives its owner the right to communicate on a certain channel, subject to some restrictions. A DSAP client may only communicate on a channel for which it has a lease, unless it is communicating with the DSAP server. Leases remain valid for a finite period of time. They may be revoked by the server, relinquished by the client or expire due to timeout.

Lease field	Example
Lease ID*	0x0001
Channel*	2.412 GHz
Duration*	10 s
Protocol	802.11b
Max Transmit Power	400 mW
APT	0.1 Mbps *or* 20 RSSI

TABLE I

SAMPLE OF DSAP LEASE OPTIONS (* – REQUIRED)

A lease may include a wide variety of information and restrictions, but only a few are required (see Table II-B for details). A minimalist lease allows a DSAP client to communicate on a specified channel for a specified amount of time after a lease has been issued.

One of the options that needs elaboration is the APT. APT stands for *acceptable performance thresholds* and consists of a set of performance metrics, such as noise level. If the lease owner's performance metrics drop below those in the APT, the client will be immediately eligible for a new lease.

One of the sources of information in which the DSAP server bases its spectrum assignments is the *RadioMap*, a database that holds information about all the clients (possibly including geographical location) and channel conditions throughout the network. The *RadioMap* is populated by periodic updates from DSAP clients who assess radio conditions in their vicinity and report these findings to the DSAP server. Based on this information the DSAP server is able to determine an optimal spectrum distribution in the network and assign leases accordingly.

The *RadioMap* alone allows the server to determine the optimal spectrum assignment under "policy-neutral" conditions. But ultimately administrator-defined policies will determine the distribution of spectrum leases. For example, a policy may ensure higher quality of service for a group of nodes, determined either by their identifiers (MAC addresses), or their geographical location.

C. DSAP Messages

At a high level DSAP and DHCP are conceptually similar protocols: DSAP is to wireless configuration as DHCP is to IP configuration. Although there are differences between the messages of the two protocols,

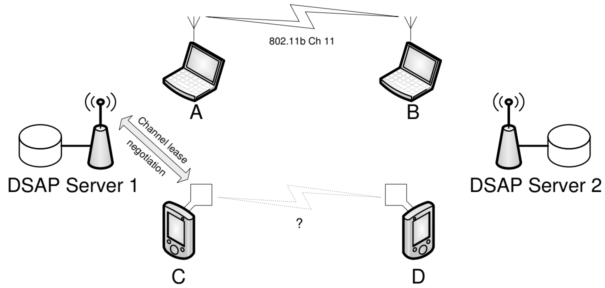

Fig. 3. A DSAP scenario

most of DSAP's messages have analogues in DHCP.

A *ChannelDiscover* message is broadcast by DSAP clients who wish to obtain a new channel lease from the server. The parameters included in this message are the client's (MAC) identifier, location if available, radio capabilities (e.g. supported wireless MAC protocols), destination's identifier and location, if available, and the desired lease options (see Figure II-B).

ChannelOffer messages are sent from a DSAP server to a client either in response to a *ChannelDiscover* or *ChannelRequest* (described below) message. This message contains the server's choice of lease for the client (see Figure II-B), which may be different from what the client requested.

ChannelRequest message is used by a DSAP client to acknowledge the terms of the server's *ChannelOffer* message. A *ChannelRequest* message can also be sent by a client who wishes to renegotiate certain aspects of a currently assigned lease.

ChannelACK is sent by the server in response to *ChannelRequest*. This message either accepts or declines the client's request for a lease.

ChannelRelease: If the client no longer requires its lease, it should use the *ChannelRelease* message to notify the server that the lease may be recycled.

ChannelReclaim is sent by a server that chooses to forcefully reassign or terminate a client's lease. A *ChannelOffer* message can be piggybacked to a *ChannelReclaim* message in order to immediately reassign a different lease to the client.

D. General Operation

We explain some typical operations and interactions of DSAP with a simple example, using nodes shown in Figure 3.

a) Acquiring a new lease: Suppose a client C, which has just entered the coverage area of the DSAP server, wants to initiate new communication with another client, D (see Figure 3). First C requests an appropriate channel from the DSAP server. C broadcasts a *ChannelDiscover* message to any DSAP server in vicinity with request for a channel *lease*. Based on prior channel/spectrum assignments and prescribed policy, the DSAP server will respond with a *ChannelOffer* message. In this message the server indicates a channel that C and D can use for their communication, as well as other parameters, as described previously.

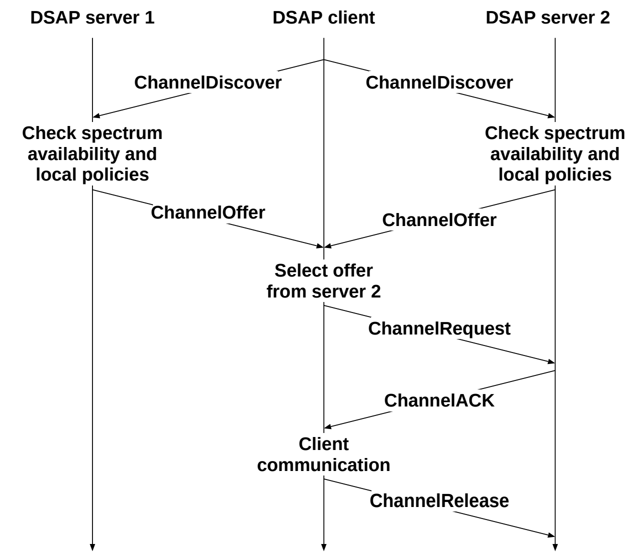

Fig. 4. Protocol interactions between the client and server in DSAP

As evidenced in Figure 4, there may be more than one DSAP server in the vicinity of a client, to increase robustness for instance. Hence, it is possible that each server makes a *ChannelOffer* to the requesting client. Therefore we require that the client pick only one of these offers for its own use through a *ChannelRequest* message (with the lease it received in *ChannelOffer*) to the appropriate server, thereby implicitly declining offers from all others. Finally the DSAP server will respond with a *ChannelACK* confirming (or denying) the channel lease request.

b) Client lease update requests: If necessary, clients currently holding a lease can request either a lease extension or, should the channel conditions unexpectedly worsen, a channel lease update using subsequent *ChannelRequest* messages. The lease update serves to modify the conditions of the current lease, such as increase in allowed transmit power, for example. The *ChannelRequest* message may include some desired parameters for the intended lease. If these parameters

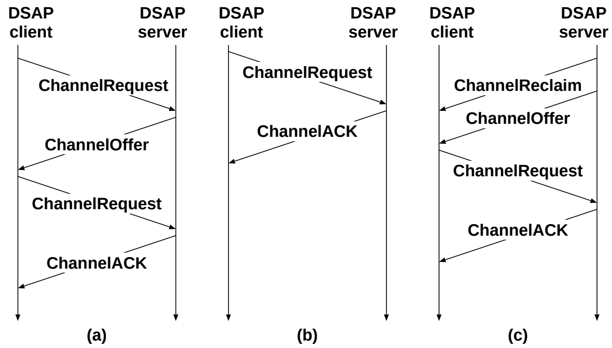

Fig. 5. (a) Client request with server offer; (b) Client request accepted; (c) Server-initiated lease update

can be met by the server, a *ChannelACK* message is sent from the server and the client updates its lease (see Figure 5 (b)). If the server cannot accommodate the parameters in the *ChannelRequest* message or if the client's *ChannelRequest* message does not contain any desired parameters, the server will reply with a *ChannelOffer*. Just as before, the client will acknowledge the offer with another *ChannelRequest* and the server will send a *ChannelACK* in response (see Figure 5 (a)). A client can also choose to relinquish its channel lease prior to its expiry by using a *ChannelRelease* message.

c) Server lease updates: Finally, the server may send a gratuitous *ChannelReclaim* message by which a server can terminate a lease prior to its pre-negotiated expiry. A server could immediately initiate a new lease by piggybacking a *ChannelOffer* to the *ChannelReclaim* message. This has the effect of modifying the client's previous lease. Modifications of a lease could limit transmission power of a node, or change the communication channel. After receiving the *ChannelOffer* message from the server, clients send a *ChannelRequest* reply to indicate the offer was acknowledged. Finally, the server sends a *ChannelACK* to the client to either finalize or cancel the transaction. See Figure 5 (c) for an example lease modification initiated by the server.

E. Handling non-compliant devices

Non-compliant devices can be divided into two categories: legacy devices and misconfigured/malicious devices. Dealing with both categories of devices is a matter of policy; here we outline some general concepts.

Under most circumstances, the DSAP server will possess more information about the state of the network than any node. Thus, clients that self-configure are likely to underperform compared to clients using server-issued configuration. Therefore, usually it will be in the node's interest to obey to the server, especially since doing otherwise may prevent it from interacting with DSAP-compliant nodes.

If a non-compliant node is behaving in a way that is detrimental to the network's efficiency, such a node could be detected by the server due to broadcast nature of the wireless medium. For example, it will be possible to determine if a node uses a frequency for which it does not have a lease. If the DSAP server finds itself in a situation where an entity cannot be brought under control either because it is misconfigured or unconfigurable, the DSAP protocol will allow the server to reconfigure compliant clients in a way that minimizes the negative effects of a non-compliant entity.

Some degree of backward compatibility may be provided by the mechanism used for communication by DSAP clients and the server. Although the way clients and servers communicate is no specified by DSAP and may vary, in practice this may be done by dedicating a single channel for the client-server messages. In this case, legacy nodes that are able to operate on this channel will be able to reach any node on the network. In some cases it will be possible to adjust the leases of DSAP-compliant nodes so that a legacy node can communicate with them.

F. DSAP Control Channel

Thus far we have assumed that DSAP clients and servers are always able to communicate with one another. Practically this could be accomplished by dedicating a certain frequency band to client-server communication. For example, the "low" portions of available bands can be used for this purpose, such as 802.11a channel 36 or the lowest 6 MHz of some more flexible wireless technologies. Nevertheless, in this work we do not explore the specifics of the control channel implementation as it is not a part of the DSAP protocol.

G. Interaction with wide-area spectrum management architectures

Most of the aspects of the DSAP protocol covered in this paper apply to geographically limited wireless environments and configuration of individual nodes. However, DSAP is capable of managing any spectrum segments and in principle can be integrated with wide-area spectrum management architectures, such as a regional spectrum broker (for an example, see DIMSUMnet [3]).

III. An Experimental Prototype

We have performed basic evaluation of the performance advantages DSAP offers. The experiments were performed on a wireless testbed of five machines running Gentoo Linux. The following chipsets were used: Broadcom BCM2033, Cambridge Silicon Radio DBT-120 (Bluetooth), Atheros AR5212 (802.11) with BlueZ [11] and MadWiFi drivers [10].

Every node in the testbed was equipped with multiple wireless network cards. To simplify the implementation, we have chosen to dedicate one wireless interface exclusively for communication with the DSAP server. Bluetooth and 802.11 channel hopping experiments were performed using the second wireless interface. An additional interface was used in 802.11 MAC protocol switching experiments to compensate for behavior of the MadWiFi drivers, where, upon switching 802.11 MAC protocols the card would engage in a lengthy (order of seconds) scan process, thereby introducing significant delay. Rather than modifying the MadWiFi drivers, we have chosen to work-around the problem by pre-configuring two cards with two different 802.11 MAC protocols and simulating protocol switch by changing the card used for communication.

The DSAP client daemon was implemented in user space. It would modify wireless settings based on the directives of the DSAP server. The DSAP client made no effort to make interface reconfiguration transparent to the client application. DSAP relays were not implemented.

We performed multiple experiments to explore DSAP's ability to achieve the following:

1) Manipulating transmit power to maintain node priority and quality of service.
2) Increasing throughput by intelligently switching channels to minimize interference.
3) Managing 802.11 and Bluetooth nodes to ensure interference-free coexistence.
4) Distance-aware wireless MAC protocol control for mobile nodes.
5) Management of mobile nodes that experience varying channel conditions.

Due to space restrictions, we will only present results for last two experiments, leaving the rest for the full version of the paper.

A. Range and interference management

In this experiment we show how a DSAP server can balance generated interference and a node's ability to communicate.

In our experimental setup it was the DSAP server's policy to minimize interference in the 2.4 GHz range, which is used by 802.11g. Since 802.11a operates in the 5.2 GHz range, the server would issue 802.11a leases

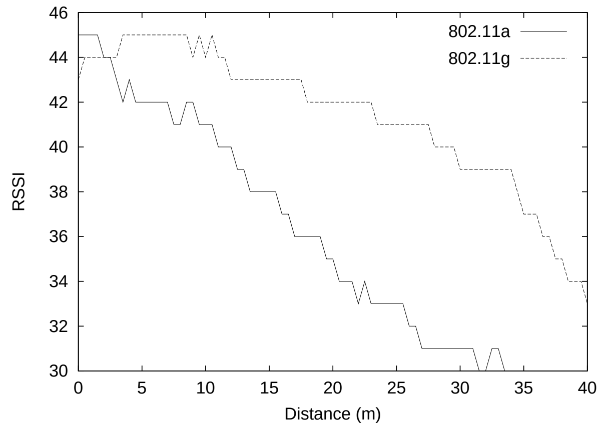

Fig. 6. Signal strength experienced by a mobile node corresponding to the data in Figure 7

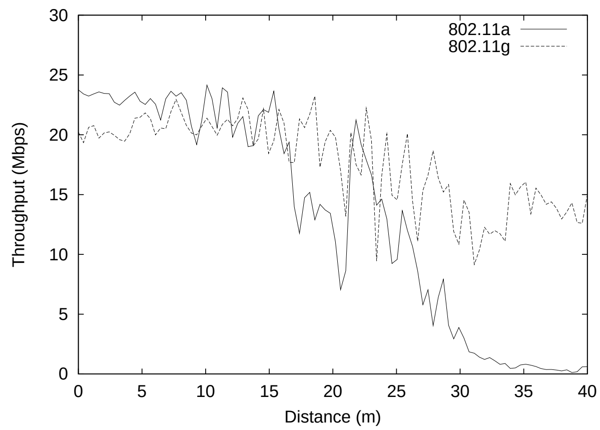

Fig. 7. Range and throughput of mobile nodes corresponding to the data in Figure 6

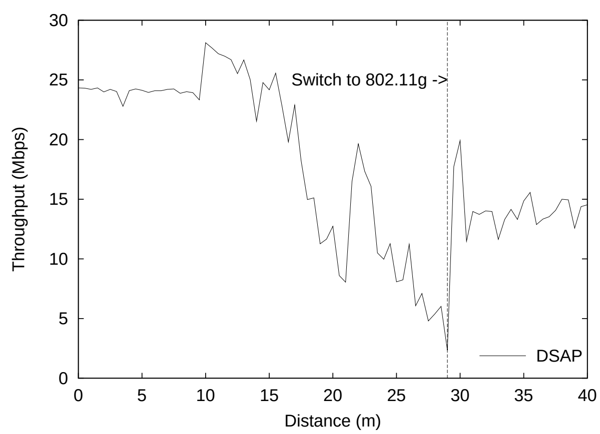

Fig. 8. Throughput experience by a DSAP client (compare with Figure 7)

whenever nodes support 802.11a and its short range is acceptable.

As mentioned earlier, leases issued by the DSAP server include metrics of "acceptable performance threshold" (APT), and should the lease holder experience lower performance than the APT, it automatically becomes eligible for a new lease.

For this experiment we have chosen to use the throughput and RSSI (Received Signal Strenth Index) as the APT metrics, since both are readily available. Exact thresholds for the experiment were determined empirically. For leases to 802.11a channels without contention we have chosen the APT to be throughput of 5 Mbps and RSSI of 32 (see Figures 7,6).

When node A requested a lease for communication with node B, the server granted an 802.11a channel 36 lease to the nodes in order avoid interference on the 2.4 GHz range. However, node A is moving away from node B at the rate of 1 meter per second (Figure 6). Performance degrades with distance, and when it drops below the APT specified by the DSAP server, node A requests a new lease. The DSAP server, being aware of the distance between A and B, issues a new lease for 802.11g channel 6, which allows A to continue communication with B at the price of increased interference in the 2.4 GHz range. The experiment was performed indoors with all nodes operating at transmit power of 32 mW (the default for our cards).

Figures 6, 7 show link quality and throughput, respectively, experienced by mobile nodes using only 802.11a and 802.11g. One can see that at distances greater than 25 meters, performance of 802.11a quickly deteriorates, while 802.11g delivers decent performance even 40 meters away.

In contrast, Figure 8 shows what happens when a DSAP server is used to manage throughput and interference. In accordance to its policy, the DSAP server initially issues an 802.11a lease to minimize usage of the 2.4 GHz band. When node A is about 30 meters away from B, its performance drops below the acceptable threshold, at which point an 802.11g lease is issued to maintain good performance at longer range. This way the DSAP server was able to keep the 2.4 GHz band unused for as long as possible while maintaining certain quality of service for the nodes.

B. Mobile Nodes

Mobile nodes may encounter interference when moving into the interference or transmission range of other nodes, which may adversely affect any on-going transmissions. With DSAP, mobile nodes can obtain new leases when entering the transmission or interference range of another node. Based on this premise, we have conducted the following experiment.

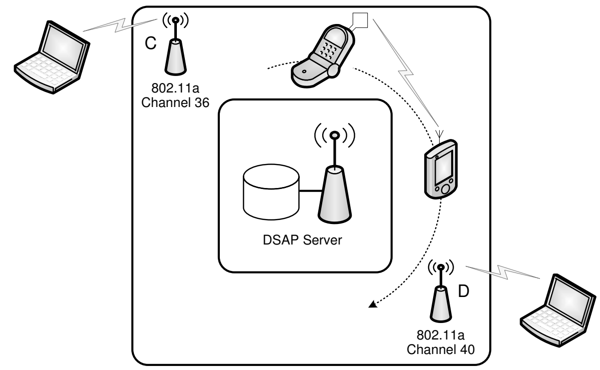

Fig. 9. Layout of experiment represented in Figure 10

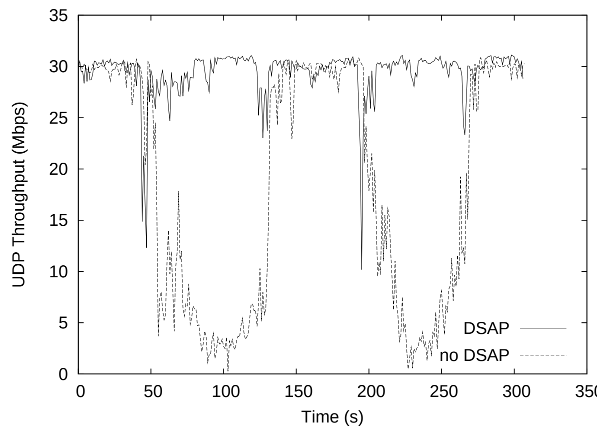

Fig. 10. Mobile nodes encountering interference from two AP's

Two mobile nodes (A and B) are engaged in a UDP transfer on 802.11a channel 40. The nodes, placed about six feet apart, continuously move around a square corridor at a rate of about 0.75 m/s. On opposite ends of the square corridor, two different nodes (C and D) are sending UDP data to some local neighbors (one local neighbor near each of C and D). Node C (and its local neighbor) is operating on 802.11a channel 36 while node D (and its local neighbor) is on 802.11a channel 40 (call it Node D). See Figure 9 for the experiment layout. Both of these nodes transmit with limited power (around 0 dBm). As the mobile nodes move around the corridor, their throughput drastically fluctuates. When in the line-of-sight of Node D, the throughput of the mobile nodes drops dramatically because Node D and the mobile nodes are sending data on the same channel. When in the line-of-sight of Node C, the throughput of the mobile nodes increases because there is no interference between 802.11a channels 40 and 36. Note that as a result of the reduced transmission power of Nodes C and D, there is little interference between the mobile nodes and an interfering node if the mobile nodes are not in the line-of-sight of the interfering node.

Figure 10 measures the throughput of the mobile nodes in this scenario. When the mobile nodes do not implement DSAP, their throughput fluctuates greatly as a result of the interference from Node D (see Figure 10, no DSAP). When the mobile nodes utilize DSAP, they are able to change channels when the interference of Node D begins to affect throughput. As a result, the mobile nodes change to channel 36 when they experience interference from Node D. However, the mobile nodes will again come into the line-of-sight of Node C and thus will have to change channels once again in order to avoid interference, this time to channel 40. In the figure, the channel changes can be witnessed at the following approximate times: 50, 125, 187 and 275 seconds. In the case of the non-DSAP enabled mobile nodes, the interference from Node D can be witnessed at the following approximate intervals: 50 to 125 seconds and 187 to 275 seconds. As the Figure 10 indicates, the DSAP-enabled clients were able to well outperform non-DSAP clients.

IV. Related Work

Owing to new developments in radio technology and consequent re-examination of spectrum allocation policies by the FCC in the US and other similar regulatory bodies worldwide, a number of researchers have been examining dynamic spectrum access and management techniques in recent literature. We have already provided detailed description of two such proposals, namely CSCC [18] and DIMSUMNet [3], in Section I. Due to space constraints, in this section we focus on only a few other such related developments.

In the context of cellular networks, Peha et al. [9] have shown Dynamic Channel Assignment (DCA) with Autonomous Reuse Partitioning (ARP) provides more capacity than standard DCA on Personal Communication Services (PCS) bands. Base stations implementing an ARP algorithm search channels in the same order and assign the first channel that meets a minimum Carrier-to-Interference Ratio [14]. Furthermore, they have indicated that multiple operators sharing spectrum through DCA use it as efficiently as a single operator would.

Bahl et al. [17] proposed a set of etiquette rules for short range wireless devices operating in unlicensed frequency bands which focus on regulating Transmit Power Control (TPC), and allocating the unlicensed band between Dynamic Frequency Selection (DFS) and Listen Before Talk with Channel Wait Time (LBT-CWT). The rules allow the co-existence devices using different MAC and PHY layer protocols. Such rules can be incorporated into DSAP.

V. Summary and Future Work

In this paper we present the design of DSAP, a centralized protocol that coordinates arbitrary wireless technologies and manages access to arbitrary radio spectra by issuing clients temporary leases for parts of radio spectrum. Using a proof-of-concept implementation we demonstrate how a DSAP server could increase performance in wireless LANs by intelligently utilizing the available spectrum.

The proof-of-concept implementation of the DSAP client made no attempt to make the wireless interface reconfiguration transparent to the applications, resulting in the possibility of packet loss. We plan to minimize or even eliminate this phenomenon by taking advantage of multiple interfaces (if available), as was done in MultiScan [2], or in the case of TCP, taking pro-active measures to maintain TCP performance as discussed in Freeze-TCP [8].

The experiments were performed on a small scale, involving no more than five nodes at a time and simple policies. DSAP's performance in large networks with complex set of policies will be evaluated using network simulators.

Security issues of the DSAP model were not addressed in the proof-of-concept implementation. Perhaps the biggest threat to a DSAP-enabled network is existence of unauthorized DSAP-servers with inappropriate set of policies. Evaluation of the security implications DSAP introduces and implementation of mechanisms to ensure secure operation is future work.

References

[1] Facilitating the provision of spectrum based services to rural areas and promoting opportunities for rural telephone companies to provide spectrum-based services. FCC Notice of Inquiry, December 2002.

[2] Vladimir Brik, Arunesh Mishra, and Suman Banerjee. Eliminating handoff latencies in 802.11 wlans using multiple radios: Applications, experience, and evaluation. http://www.cs.wisc.edu/ suman/pubs/MultiScan.pdf.

[3] Milind M. Buddhikot, Paul Kolodzy, Scott Miller, Kevin Ryan, and Jason Evans. DIMSUMNet: New directions in wireless networking using coordinated dynamic spectrum access. *IEEE WoWMoM05*, June 2005.
[4] R. Rao C.F. Chiasserini. Performance of IEEE 802.11 WLANs in a bluetooth environment. In *IEEE Wireless Communications and Networking Conference*, Chicago, IL, September 2000. WCNC 2000.
[5] R. Droms. RFC 2131, Dynamic Host Configuration Protocol, March 1997.
[6] G. Ennis. Impact of bluetooth on 802.11 direct sequence. In *IEEE P802.11 Working Group Contribution*. IEEE P802.11-98/319, September 1998.
[7] Spectrum Policy Task Force. Technology advisory council (TAC) briefing, December 2002.
[8] Tom Goff, James Moronski, and D.S. Phatack. Freeze-TCP: A true end-to-end tcp enhancement mechanism for mobile environments. In *INFOCOM 2000*.
[9] Salgado H., Sirbu M., and J.M. Peha. Spectrum sharing through dynamic channel assignment for open access to personal communications services. In *IEEE ICC 1995*, June 1995.
[10] http://sourceforge.net/projects/madwifi/. Multiband Atheros Driver for WiFi (MadWiFi).
[11] http://www.bluez.org. Bluez - official linux bluetooth protocol stack.
[12] http://www.sandbridgetech.com. Sandbridge Technologies, Inc.
[13] http://www.vanu.com. Vanu, Inc.
[14] T. Kanai. Autonomous reuse partitioning in cellular systems. In *Proc. IEEE VTC*, pages 782–785, 1992.
[15] Paul Kolodzy. Spectrum policy task force report. FCC, December 2002.
[16] A. Soltanian N. Glomie, R.E. Van Dyck. Interference of bluetooth and IEEE 802.11: Simulation modeling and performance evaluation. In *Proceedings of the Fourth ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, Rome, Italy, July 2001. MSWIM ’01.
[17] Bahl P., Hassan A., and DeVries J.P. Draft proposal for comment: Etiquette rules and procedures for unlicensed bands. http://research.microsoft.com/mesh/, January 2003.
[18] Dipankar Raychaudhuri and Xiangpeng Jing. A spectrum etiquette protocol for efficient coordination of radio devices in unlicensed bands. In *14th IEEE PIMRC2003*, September 2003.