SELECTIVE ACTIVE SCANNING FOR FAST HANDOFF IN WLAN USING SENSOR NETWORKS

Sonia Waharte, Kevin Ritzenthaler and Raouf Boutaba
University of Waterloo, School of Computer Science
200, University Avenue West, Waterloo, ON, CA
{swaharte,kmritzen,rboutaba}@bbcr.uwaterloo.ca

Abstract

Seamless connectivity in wireless access networks is critical for time-sensitive applications requiring Quality-of-Service guarantees with bounded data transmission delay. Currently, the latency inherent in the hand-off process can preclude the successful delivery of such applications by introducing delays up to several seconds. In this paper, we address this issue by proposing an improvement of the access points discovery process at the data link layer. We present a novel WLAN architecture using an overlay sensor network as a control plane. By distributing the information on the current network status to the sensor nodes, we show that handoff latency can be significantly reduced.

1. Introduction

Wireless communications have gained over time great importance with the rapid growth in data transmission rate. Whereas cellular networks still remain constrained by low offered throughput (GPRS enables a theoretical 171.2kbps and UMTS only permits a maximum of 2Mbps for indoor or low range outdoor communications), a major breakthrough has been achieved in Internet access technologies with data rates up to 54Mbps. It is now feasible to envision supporting a wide range of QoS applications encompassing fields as diverse as video streaming or gaming. However, this is contingent on the ability to provide appropriate QoS guarantees through bounded end-to-end transmission delay. In addition, the diversity of terminal devices (laptop, personal digital assistant, etc.) renders the need for mobility support a critical feature.

Several characteristics inherent in wireless networks contribute to the increase of data transmission delays. In wireless LAN, the de facto Standard IEEE 802.11 [1] defines a fair random deferred access to the transmission medium, which introduces unbounded transmission delay due to idle time periods and retransmissions due to collision. Significant delays also occur during the handoff process. Moving from one access point to another involves time-consuming mechanisms which may be detrimental to applications requiring seamless connectivity and QoS guarantees.

In this paper, we address the problem of handoff latency at the MAC layer. As this delay mainly results from the exhaustive scan of every channel in the frequency band, we believe that improvements can be achieved by distributing the information concerning the surrounding access points (channel used, supported rate, etc.) to external agents. By consulting these agents, the mobile nodes can limit the number of scanned channels and take informed decision about the most appropriate access point to be associated with.

Based on this idea, we propose a novel architecture using an overlay sensor network on top of a WLAN. The sensor network is in charge of maintaining a knowledge base on the network status. By contacting only the surrounding sensor nodes, a mobile node can obtain precise information on the network status.

The rest of the paper is organized as follows. Section 2 describes the mechanisms involved in a handoff process in WLAN and related works. Section 3 provides a description of our architecture. Validations through simulations are presented in Section 4. Conclusion and future research directions are given in Section 5.

2. Layer 2 Handoff Process and Related Works

In WLAN, a handoff can be defined as the process of leaving the basic service set of an access point to enter a new one. A handoff is triggered by a degradation of the signal quality which falls below a predefined threshold. The handoff can be the result of either excessive noise and interference or user mobility (decrease of the signal intensity due to the increasing distance to the associated access point).

At the MAC layer, the handoff process as defined in the IEEE 802.11 Standard [1] can be decomposed into three phases: scanning, authentication and reassociation (Figure 1).

1 Scanning: In order to discover on which channel the surrounding access points are transmitting, a mobile node needs to scan all the channels. Two scanning methods are described in IEEE 802.11.

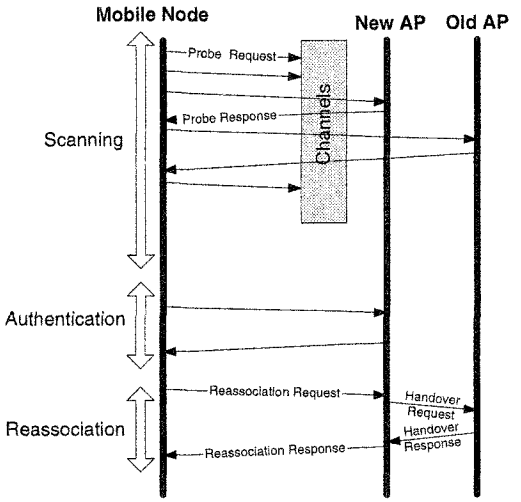

Figure 1. Handoff Process at the MAC Layer

Passive Scanning entails determining the presence of access points by successively listening to all the channels and waiting for the reception of beacon messages identifying the access point. This method, while offering the advantage of low overhead, presents the drawback of introducing a significant delay. In order to alleviate this problem, an active scanning method has been defined. The mobile node broadcasts a Probe Request on each channel and waits a minimum period MinChannelTime for any Probe Response. After the scan of all the channels and the processing of all the beacon messages or Probe Responses received (according to the implemented scanning process), the mobile node can take an informed decision on the most appropriate access point (with the best channel quality).

2 Authentication: The Authentication process involves establishing the identity of the mobile node and authorizing its access to the basic service set of the access point.

3 Reassociation: The Reassociation process consists in transferring an association between an access point and a mobile node to another access point. The operations between the old AP and the new AP are defined by the Inter-Access Point Protocol [2].

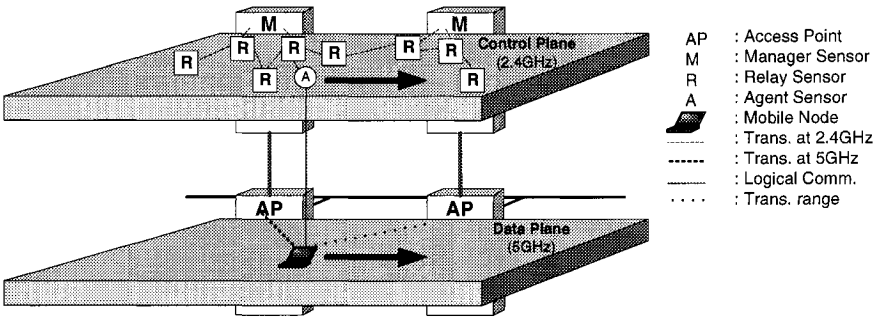

Figure 2. Overlay sensor network architecture for handoff management

The scanning process has been identified as the principal source of delay in the handoff mechanism [3] [4]. Few works have been conducted aiming at reducing the latency at the MAC Layer [3] [4] . They essentially adopt the same approach by optimizing the waiting time of the mobile node during the active scanning process. Indeed, IEEE 802.11 defines two parameters: MinChannelTime, the minimum waiting period before considering that the channel is idle; and MaxChannelTime, the maximum waiting period after a Probe Response has been successfully received. However, no exact value of these parameters has been explicitly set. The suggested optimal values deduced from previous experiments are approximately 6.5ms for MinChannelTime and 11ms for MaxChannelTime.

Thanks to their sensing, computation and transmission capabilities [5], sensor nodes can serve as an effective monitoring and data gathering technology for WLANs. Few works used sensor networks for managing wireless networks. MeshDynamics [6] uses sensor networks to manage connectivity and routing in ad hoc wireless mesh networks. AirMagnet [7] implements a distributed sensor network in WLAN for security monitoring and intrusion detection. These works demonstrate the practicality and effectiveness of sensor networks as a monitoring infrastructure for wireless networks.

3. Architecture Design

3.1 Architecture overview

Our access architecture augments the existing IEEE 802.11 access protocol (data plane at 54Mb/s) with an overlay sensor network (control plane at 2Mb/s). As the two planes use different access frequencies (5GHz and 2.4GHz), communications can occur in parallel within each respective plane (Figure 2). This characteristic allows us to lift the control overhead from the data plane.

The overlay network is composed of three types of sensor nodes: the manager, the relays, and the agents. The manager node is a sensor attached to the access point. First, it initializes the sensor relays by conveying information about the associated access point. Second, it serves as the data aggregation server where reassociation requests from mobile nodes are gathered, and reassociation responses are sent back. The relays are fixed sensors uniformly placed throughout the coverage area of an access point. Because of a sensor's short transmission range, the relays are used to route messages between the manager and the sensor agents. They are also responsible for sensing the frequency bands according to a procedure described in the following section. The agents are sensors attached to the mobile nodes. They communicate with the relay sensors upon entering the transmission area of an access point or if a handoff process is initiated due to a degradation of the signal quality.

3.2 Selective Active Scanning for Fast Handoff

In order to determine the presence of surrounding access points, the common method is to successively scan all the channels and therefore detect if a channel is busy by receiving Probe Responses or Beacons. We believe that this time-consuming method can be drastically improved by limiting the number of channels scanned to the ones in which the mobile node is interested, i.e. the access points with which it can potentially be associated. This can be achieved by maintaining a distributed database stored by the relay sensors.

The proposed handoff process is illustrated in Figure 4. The steps involved in the process are the following:

1 The mobile node broadcasts an AP_List Request on the control plane.

2 The neighboring relay nodes reply with an AP_List Response if they satisfy some criteria detailed in a subsequent section.

3 The mobile node processes all the received messages, builds a list of the neighbor access points and initiates a scanning process solely based on this list.

The remaining steps of the handoff procedure remain unmodified compared to the specifications of the standard, the only difference being that the process occurs at the control plane instead of the data plane.

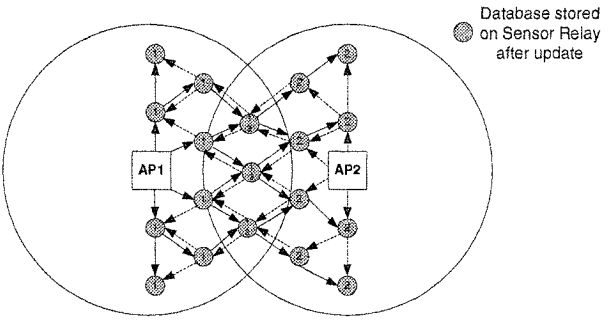

Figure 3. Example of initialization with two access points[1]

3.2.1 Sensor Network Initialization Process. Before being able to handle any handoff, the overlay sensor network needs to be initialized in order to learn about the presence of the surrounding access points. This process, initiated by the access point, occurs only once during the network lifetime. Its impact is thus minimum and does not affect the subsequent handoff mechanisms of the mobile nodes.

In the control plane, each access point sends an initialization packet containing information about itself using a flooding protocol (Figure 3). In order to avoid flooding the entire network upon addition of a new access point, the forwarding process stops two hops after the initialization packet has been forwarded by a relay node that has at least another entry (meaning that this node is in the transmission zone of another access point). The explanation for this restriction comes from the following observation: if we consider that for an access point and a relay sensor, the transmission range can not exceed 150m and 50m respectively, we are guaranteed to cover the whole transmission area of the access point within three hops. Thus, if we assume that two access points do not

[1]For clarity, not all the relay sensors and not all the messages exchanged during the initialization process are represented.

Table 1. Local Database maintained by the Relay Sensor

AP BSSID	*Channel Used*	*Supported Rate*	*Signal Strength*
xxx-xxx	34 (5170MHz)	54Mbps	65%
yyy-yyy	38 (5190MHz)	24Mbps	No signal

cover exactly the same geographical area, the aforementioned restriction of two hops is sufficient. Nonetheless, this parameter can be increased if necessary without impacting our model.

An example of the database maintained by a relay node is depicted in Table 1. This database is updated on a regular basis with information such as signal strength by only scanning the listed channels. As during the initialization process, a relay node may have received information about an out of range access point, the relay node is allowed to remove this entry if no signal is detected on the corresponding channel.

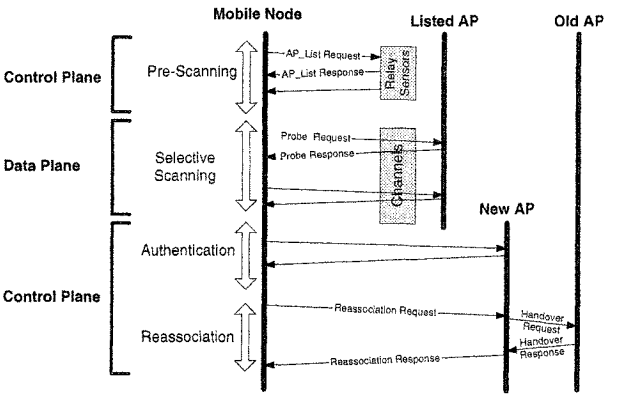

Figure 4. Proposed Handoff Process

3.2.2 Selective Scanning Method. The proposed method is illustrated in Figure 4. Compared to a traditional handoff process, we add a pre-scanning phase which proactively determines the presence of access points before a mobile node initiates a handoff. As previously mentioned, when the mobile node experiences a degradation of the received signal strength in the current associated basic service set, the mobile node initiates a handoff by first trying to discover new access points which can offer a better service quality. The mobile node then

first broadcasts an AP_List Request and waits for the surrounding relay nodes to reply with an AP_List Response. Priority is given to the closest relay sensor by defining a backoff time based on the received signal strength such that:

$$\text{backoff\_time} = (1 - \frac{P_r}{P_t})CW$$

where P_r is the received signal strength, P_t is the maximum signal strength and CW is a random congestion window size.

A relay sensor sends back an AP_List Response by following the specifications of Algorithm 1. This algorithm guarantees that only useful information is sent back to the mobile node. We consider as useful information the announcement of the presence of an access point not previously advertised by another relay sensor.

Algorithm 1: send_Probe_Response

```
1: if (backoff time = 0 and no AP_List Response received) then
2:    Send AP_List Response
3: else if (backoff time = 0 and AP_List Response received) then
4:    Compare database contained in AP_List Response with local database
5:    if (Local database contained reference to AP not in received AP_List
      Response) then
6:       Send AP_List Response to Mobile Node
7:    else
8:       Ignore Message
9:    end if
10: end if
```

If several AP_List Responses are received by the mobile node, the mobile node should process them all. It is worth noticing that the inaccuracies introduced by the difference of positions between the mobile node and the relay sensors (for instance variations in link quality) are overcome by the reception of multiple AP_List Responses. The mobile node should wait for incoming AP_List Responses for a given period of time. According to the AP_List Responses received, the mobile node initiates a traditional scanning process over the listed channels (containing only active channels) to select the most suitable access point in terms of link quality. To provide even faster handoff and to meet user expectations, it is also envisioned to allow the user to limit this scan to channels with a specific Data Rate or a minimum signal strength threshold.

To provide compatibility with existing hardware (which may not be equipped with sensor agents), a traditional handoff process can still be initiated.

3.3 Benefit of the overlay sensor network

The advantages of using sensor nodes as a control plane are two-fold:

- By monitoring the environment, the sensor nodes can obtain information on the presence of access points and the associated quality of their transmission channels. Based on this information, mobile nodes can subsequently make informed decisions about the access point they are willing to be associated with. By directly requesting this information from the nearest sensor node, significant improvement in terms of delay can be achieved. The mobile nodes thus scan only the channels of interest (i.e. the ones used by the access points the mobile node can actually be associated with).

- By transmitting control messages at the sensor plane, in parallel with data transmission at the data plane, bandwidth wastage is reduced.

The decision of using relay nodes instead of contacting directly the access points is motivated by the following factors: less interference occurs as the transmission distance is shortened, thus several mobile nodes can contact different relay nodes without interfering with each other; energy consumption at the mobile node is minimized by contacting a closer relay node; and relay nodes provide more accurate information on the surrounding access points.

It is worth mentioning that the flexibility and ease of deployment of our architecture allow further enhancements such as providing guarantees for QoS applications [8].

4. Evaluation

In order to assess the benefits of our architecture, we perform simulations in which a mobile node initiates a handoff process with either an active scanning or a selective scanning (using an Overlay Sensor Network architecture) with both standard and optimized MinChannelTime / MaxChannelTime parameters. The simulation parameters are directly taken from [3] and summarized in Table 2. The transmission models rely on IEEE 802.11a and IEEE 802.11b standards for the data plane and the control plane respectively. The relay nodes are uniformly scattered over the coverage area of the access points according to a cellular topology.

Table 2. Simulations Parameters

	Reference	*Optimized*
MinChannelTime	17ms	6.5ms
MaxChannelTime	38ms	11ms

The simulations are performed using QualNet 3.6.1 [9] and the results are averaged over 50 runs.

We consider that 8 channels can be used by the access points, with data sent at the lowest possible rate (6Mbps) on the data plane in order to maximize the transmission distance.

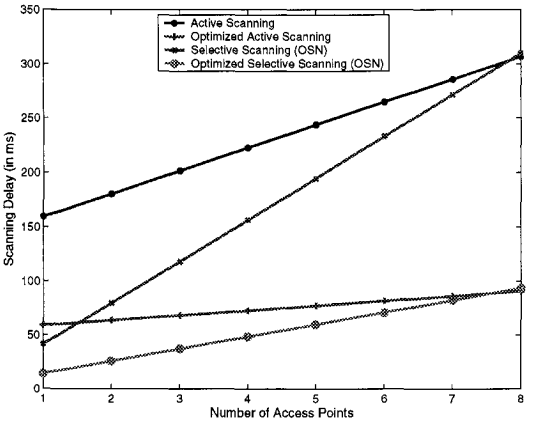

Figure 5. Scanning delay for one user with an increasing number of access points

Figure 5 shows the delay pertaining to the different scanning approaches. In the overlay sensor network architecture, the scanning also includes the pre-scanning delay. We observe that reducing the number of scanned channels brings significant improvements, especially when the number of surrounding access points is limited compared to the number of channels available.

In Figure 6, we aim at evaluating the impact of interfering transmissions on the scanning process of a mobile node. An increasing number of users, randomly placed in the BSS, generate CBR traffic to the access point at 10Mbps. We can observe that the delay introduced to access the medium is still negligible compared to the time wasted to wait for Probe Responses.

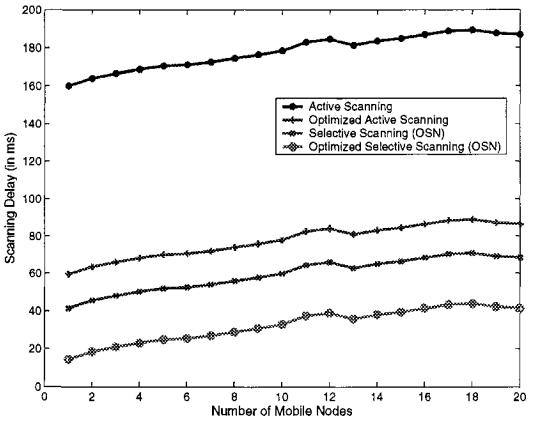

Figure 6. Scanning delay for several users with one access point

5. Conclusion

Supporting user mobility in WLAN remains a challenging task, especially with the QoS requirements of applications necessitating bounded transmission delay. The handoff process is a complex mechanism, involving significant delay, which can be detrimental to QoS guarantees.

Recent work on applying sensor networks (monitoring network connectivity [6], security, intrusion detection [7], etc.), demonstrates the practicality and effectiveness of sensor networks as a monitoring infrastructure for wireless networks.

Based on these observations, this paper aims at reducing the handoff delay in WLANs using a two-tier access architecture consisting of a sensor overlay control plane over an IEEE 802.11 data plane. Using the distributed monitoring and processing capabilities of the sensor network, we shift the burden of transmission control and coordination into the control plane, preserving the data plane solely for data transmission in parallel with the control plane. By maintaining information on the surrounding access points and by delivering this information to the mobile nodes upon request, significant improvements can be achieved.

In this paper, emphasis lies on the handoff process. However, one can envision a number of extensions for our proposed architecture. First, our architecture can be extended to support service class differentiation and QoS interworking between cellular networks and WLANs. Second, an application-adaptive scheduling algorithm can be devised to support per-traffic QoS guarantees (minimum bandwidth and maximum delay)

where each mobile node transmitting to the manager node its QoS requirements. Third, better communication techniques could also be incorporated in the sensor overlay network to improve the efficiency of control messages exchange. We believe that the application of sensor networks as a monitoring and control infrastructure for WLANs holds great promise.

References

[1] IEEE. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, 1999.

[2] IEEE. IEEE trial-use recommended practice for multi-vendor access point interoperability via an inter-access point protocol across distribution systems supporting IEEE 802.11 operation, 2003.

[3] Arunesh Mishra, Minho Shin, and William Arbaugh. An empirical analysis of the IEEE 802.11 MAC layer handoff process. SIGCOMM Comput. Commun. Rev., 33(2):93102, 2003.

[4] H. Velayos and Karlsson G. Techniques to reduce the IEEE 802.11b handoff time. In Swedish National Computer Networking Workshop, 2003.

[5] I.F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. In IEEE Communications Magazine, volume 40 of 8, pages 102114, Aug. 2002.

[6] Meshdynamics. http://www.meshdynamics.com/index.html.

[7] Airmagnet. http://www.fe-solutions.com/support/airmagnet distributed.html.

[8] S. Waharte, J. Xiao, and R. Boutaba. Overlay Wireless Sensor Networks for Application-Adaptive Scheduling in WLAN . In 7th IEEE International Conference on High Speed Networks and Multimedia Communications (To appear), 2004.

[9] Qualnet. http://www.scalable-networks.com/.