Replacing Channel Scanning with Multiple Authentication for Fast Handoff in IEEE 802.11 Wireless Networks

[Extended Abstract]

Jaeouk Ok
The University of Tokyo
okjaeouk@mlab.t.u-tokyo.ac.jp

Pedro Morales
The University of Tokyo
pedro@mlab.t.u-tokyo.ac.jp

Hiroyuki Morikawa
The University of Tokyo
mori@mlab.t.u-tokyo.ac.jp

ABSTRACT

We have developed a fast handoff scheme, called AuthScan, to reduce the time-consuming channel scanning latency in IEEE 802.11 wireless networks. AuthScan comprises two steps: First, a client caches its handoff history with beacon information. Second, when in need of handoff, a client transmits *Authentication Request* frames to the selected Access Points (APs) from the cache instead of broadcasting *Probe Request* frames in active scan to discover the next AP. Our proposed method does not require any support from the infrastructure network and contributes to finish the handoff procedure with the lowest latency when compared to approaches that improve the efficiency of channel scanning. Furthermore, AuthScan requires neither hardware upgrades to the client, nor any modification to currently deployed APs. In this paper, we present the theoretical handoff latency of AuthScan and compare it to other approaches.

1. INTRODUCTION

It is important to have fast handoff for delay-sensitive applications, so that its occurrence stays unnoticed by users in IEEE 802.11 wireless networks. Our goal is to achieve fast handoff by reducing channel scanning latency, working with currently deployed clients and APs.

The necessity of channel scanning comes from a client's inability to acquire information about nearby APs on different channels while communicating with the currently associating AP. Its long latency lies on the inefficiency of the current scanning methods that mandate a client not only to unnecessarily scan through all the channels regardless of AP's existence on it, but to wait for a fixed amount of time at each channel just in case more responses might arrive. We propose a fast handoff scheme, called AuthScan, to address this inefficiency.

AuthScan is a combined approach of a handoff history cache [1] and selective unicast scan [2]. While the former enables a client to scan only the channels where nearby APs exist in routinary places, the latter enables to reduce unnecessarily long waiting time at each channel. AuthScan improves 1) AP selection propriety among a large number of cached APs by comparing quickly acquired metrics from each of them right after handoff trigger, 2) handoff latency by replacing broadcast *Probe Request* frames with unicast *Authentication Request* frames to scan target APs. Furthermore, AuthScan requires neither hardware upgrades to the client, nor any modification to currently deployed APs.

2. AUTHSCAN

Selective unicast scan requires knowledge about nearby APs. In this section we show methods for this, our particular choice, handoff procedure and latency analysis.

2.1 Target AP Cache

The knowledge about nearby APs can be obtained by various ways: cache, pre-scan, multiple interfaces, Neighbor Graph, or offline manual collection by service providers, etc. AuthScan builds a target AP list by caching previous handoff information. Caching does not require support from infrastructure network, modifications to the protocols, hardware upgrade to any devices, nor impose data communication performance degradation. All these benefits come at the cost of unimproved support for a client's unusual behavior like visiting a place for the first time. AuthScan, however, can be implemented with any other of the methods listed above.

The cache is initially populated at a stage when the handoff is achieved through conventional active or passive scan. The reason for this is that the *Authentication Response* does not contain some information found in *Probe Response* or beacon frames. Therefore, for successful completion of handoff, the cache structure includes the BSSID of posterior AP, the BSSID of prior

*CoNEXT'*07, December 10-13, 2007, New York, NY, U.S.A.

Table 1: Handoff Latency Comparison

Scheme \ Phase	Channel Scanning	Authentication	Association	Total
Passive scan	18 * $BeaconInterval$	1 * RTT	1 * RTT	1,801.2 msec
Active scan	3 * $MaxCT$ + 15 * $MinCT$	1 * RTT	1 * RTT	61.56 msec
Selective active scan	3 * $MaxCT$ + 1 * $MinCT$	1 * RTT	1 * RTT	47.224 msec
Selective unicast scan	3 * RTT + 1 * $MinCT$	1 * RTT	1 * RTT	4.024 msec
AuthScan	0	3 * RTT + 1 * $MinCT$	1 * RTT	3.424 msec

AP, channel number, PHY type, capability information, SSID, the supported rates, PHY parameter sets, and WPA parameters, etc. The recurrence of handoffs during a fixed period is used to rearrange the order of target APs in the list. The cache can be updated by an either periodic or on-demand active scan to accommodate the changes of APs in the routinary places.

2.2 Handoff Procedure

When detecting the need for link-layer handoff based on its policy (e.g. signal strength, transmission rate, etc), a client looks up its target AP cache and selects one with the highest recurrence of handoffs as the next target AP. Then it sets up its interface to the desired channel and PHY type, and transmits *Authentication Request* frame to the selected AP.

We define two algorithms: *comparative mode*, and *fast mode*. In *comparative mode*, a client checks all the target APs in the cache, before selecting the AP to handoff. This is done by sending *Authentication Request* to all the target APs, and comparing the signal strength from the received *Authentication Responses*. This is in conformation with the current standard which allows authentication with multiple APs.

In the case of *fast mode*, if the signal strength of the received *Authentication Response* is higher than a certain threshold, the client immediately moves to the association phase. If it receives *Authentication Response* whose signal strength is lower than the threshold or there is no response during *MinChannelTime*, it repeats this operation with the next target AP in the cache. In case no AP in the cache can satisfy the client's handoff policy, the client moves to the standard active scan and saves the newly found AP in the cache.

2.3 Handoff Latency

In terms of AuthScan algorithm delay, and assuming at least one of the cached APs is available and can fulfill the handoff policy, *comparative mode* takes $M * RTT + (N - M) * MinChannelTime$, where N is the number of target APs in the cache, and M is the number of *Authentication Responses* received. In the case of *fast mode*, under the best case scenario the first AP from the cache provides signal strength higher than the threshold, so the delay is $1 * RTT$. The worst case happens when the last AP from the cache provides signal strength higher than the threshold, so the delay is the same as in the case of *comparative mode.*

For example, assuming that there are four target APs under open system authentication on different channels to one another in the cache and three of them return *Authentication Response*. The highest total handoff latency will be composed of three $RTTs$ for the APs with responses, the one waiting period of *MinChannelTime* due to the AP with no response and one *RTT* for association phase. Therefore it will be $3 * RTT + 1 * MinChannelTime + 1 * RTT$. The total handoff latencies using various schemes in Japan (i.e. 18 channels) are compared in Table 1, where *RTT* is 0.6 msec, beacon interval is 100 msec, *MaxChannelTime* is 15 msec, *MinChannelTime* is 1024 μsec. From the table, we can observe that AuthScan requires the lowest handoff latency, one *RTT* less than selective unicast scan.

3. CONCLUSION AND FUTURE WORK

We have developed a fast handoff scheme, called AuthScan. The main idea of AuthScan is to replace channel scanning with multiple authentication to further improve the performance of channel scanning. AuthScan also provides a new usage of open system authentication phase that has become redundant with the advent of WPA. We are currently working on implementing AuthScan on Linux and MadWifi driver to show the effectiveness of our system through experiments.

It is clear that accurate cache management and good metrics to choose target APs in the cache are important for higher performance of AuthScan. A precisely ordered cache list can further improve the handoff latency, so effort will be oriented to the integration of movement direction information using various sensors such as accelerometers and magnetometers in a client for an accurate determination of appropriate target APs.

4. REFERENCES

[1] S. Shin, *et al.*: "Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs," MobiWac, Philadelphia, PA, 2004.

[2] H. Kim, *et al.*: "Selective Channel Scanning for Fast Handoff in Wireless LAN using Neighbor Graph," ITC-CSCC, Sendai, JAPAN, 2004.