IEEE P802.11
Wireless LANs

|  |
| --- |
| Annex for Determination of Bloom Filter Size and PADP Usage Guidelines  |
| Date: 2015-01-11 |
| Author(s): |
| Name | Company | Address | Phone | email |
| SK Yong | Apple | 3 Infinte Loop, Cupertino, CA |  | skyong [at] apple.com |
| Chris Hartman | Apple |  |  |  |
| Yong Liu | Apple |  |  |  |
| Eric Wong | Apple |  |  |  |
| Guoqing Li | Apple |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This document describes the Determination of Bloom Filter Size and PADP Usage Guidelines

**Annex A**

**(Informative)**

**A.1: Determination of Bloom Filter Size, *m***

A Bloom filter is a space-efficient probabilistic data structure used to test if an element (i.e. service) is a member of a set. A Bloom filter is an array of *m* bits, representing a set S={x1, x2, …, x*n*} of *n* services. These *m*-bits are initiatlly set to all zero. A service x is mapped to a random number uniformly between 1, …, *m* by using *k* hash functions, *hi*(*k*), for 1≤ *i* ≤ *k*.

A service y is reported as a member of S, if the bits *hi*(*y*) are set to all one, and is guaranteed not to be a member of S if any bit *hi*(*y*) is set to zero. *p* is the probability of false positive (lower bound) event which occurs when y is actually not a member of S but reported as being in the set.

The variables *p*, *n*, *m* and *k* are related to each other with the following approaximation [1]

 (1)

The optimal value of *k* is given by

 (2)

Substituing (2) in (1) and reording terms, the value of *m* rounded to the neasrest multiple of 8 is given as

 (3)

For example, for *n*=25 services and *p*=0.01, the size of the Bloom fitler *m* is 240 bits and the required number of hash function is 7.

**A.2: PADP Usage Guidelines**

PADP is a flexible protocol that allows different usages depending on the deployment scenario. In this section, two usage scenarios are described.

**A.2.1: Background Search**

Applications that run in the background (e.g. automatically receiving sales coupons that a user has previously signed up for) may not require immediate discovery results to be presented to the user. It may be appropriate to prevent non-AP STAs with such background applications from performing Solicited PAD. Futhermore, Solicted PAD in a dense wireless LAN environment can cause network congestion. In such a scenario, it is more effective to perform Unsolicited PAD, whereby an AP advertises multiple services it offers, while non-AP STAs need respond only if there is a matched service.

The AP may select to advertise several typical services using Service Hash (SH) element, and advertise the remaining services using Service Hint Information (SHI) element, in the Beacon frames[[1]](#footnote-1). Upon receiving the Beacon frame, a non-AP STA processes the SH and SHI elements to verify if there are any potential matching services. Figure W and X show two cases where there is a matching SHI.

If the probabalility of false positives in the SHI element is relatively high (see Figure W), the non-AP STA may send a Probe Request with the Service Hash to confirm the service is indeed offered by the AP. The AP then responds with a Probe Response with SAI element that containing the corresponding Service Name. The non-AP STA may then send a PAD Service Information Request containing the Service Name and specific Service Information Query Request to obtain more information about the service from the AP. The AP responds to the PAD Service Information Request with the PAD Service Information Response containing the Service Name and specific Service Infromation Query Response. After the PAD Service Information Request and Respsone exchange, the non-AP STA should be able to make an informed decision about choosing to associate to the AP.



Figure W: Example of a message exchange for background search with high probability of false positive.

If the probabalility of false positive is relatively low (see Figure X), the non-AP STA may directly send a PAD Service Information Request frame containing the Service Name and specific Service Information Query Request to obtain more information about the service from the AP.



Figure X: Example of a message exchange for background search with low probability of false positive.

In a scenario where there is a matching SH element, the non-AP STA may directly send a PAD Service Information Request frame containing the Service Name and specific Service Information Query Request to obtain more information about the service from the AP as shown in Figure Y. Alternatively, the non-AP STA may choose to associate based on the matching SH element.



Figure Y: Example of message exchanges for background search with matching Service Hash element.

**A.2.2: Immediate Search**

Applications that are initiated by users (e.g. a user is looking for a fast movie download service) require immediate discovery results to be presented to the user. In this scenario, a non-AP STA should perform a Solicited PAD, whereby the non-AP STA sends Probe Request frames to query specific services immediately after user initiation of the service/application, and the AP responds with a Probe Response frame accordingly, if there is a matched service (see Figure Z). The Probe Request frame contains the SH element of the search service. The AP responds with a Probe Response frame with an SAI element containing the corresponding Service Name. The non-AP STA then may perform a PAD Service Information Request and Resposne exchange with the AP as shown in Figure Z, to obtain more information about the service.



Figure Y: Example of a message exchange for immediate search.

References:

[1] S. Tarkoma, C. E. Rothenberg, and E. Lagerspetz, “Theory and Practice of Bloom Filters for Distributed Systems,” *IEEE Communications Surveys and Tutorials,* vol. 14, no. 1, pp. 131-155, Feb 2011

1. Alternatively, the AP may elect to advertise all of the services using either the SH or SHI elment in the Beacon frames [↑](#footnote-ref-1)