第35卷 第14期 计 算 机 工 程 2009年7月
Vol.35 No.14 Computer Engineering July 2009
·网络与通信· 文章编号：1000—3428(2009)14—0135—03 文献标识码：A 中图分类号：TN925.93

基于移动终端的 WLAN 快速切换方案

徐 伟，杨 怡，陶 军
(东南大学计算机网络与信息集成教育部重点实验室，南京 210096)

摘 要：移动终端在 AP 间切换产生的时延和抖动严重影响实时业务的质量。通过分析移动终端切换的过程和现有的改进方案，提出一种基于动态域值的扫描触发机制，有效地避免移动终端在静止和 AP 信号较好条件下的 cache 更新。在 STA 上实现基于动态域值触发扫描的分片 cache 的更新算法，该算法在保证 cache 及时更新的同时降低每次更新 cache 的开销且能有效减小切换时延。

关键词：无线局域网；快速切换；分片 cache；IEEE802.11 协议

Fast Handoff Solution Based on STA for WLAN

XU Wei, YANG Yi, TAO Jun
(Key Laboratory of Computer Network & Information Integration, Ministry of Education, Southeast University, Nanjing 210096)

【Abstract】 The latency and jittering produced by handoff between Access Points(APs) has a serious and negative impact on the quality of the real-time service. Through analysis of the process of handoff and existing improvement program, this paper proposes a scanning trigger mechanism based on dynamic domain values, which effectively avoids cache updates when STA is stable and the associated AP's signal is good. This mechanism and a slice cache update algorithm are realized on the STA, which ensure timely update the cache and reduce the cost of each cache update and the handoff delay.

【Key words】 Wireless Local Area Network(WLAN); fast handoff; slice cache; IEEE802.11 protocol

1 概述

随着无线技术的快速发展，无线网络特别是基于IEEE802.11[1-2]协议标准的无线局域网(Wireless Local Area Network, WLAN)由于其部署简单、方便等特点已经被广泛地部署和应用(如学校、机场等公共场所)。基于 WLAN 的语音等实时应用也越来越受到人们的青睐，但是由于语音等实时应用对数据的延迟、抖动以及数据包的丢失要求都非常的高，因此当传输语音等实时业务的 STA 在 WLAN 中漫游时，其 AP(Access Point)之间必须进行无缝切换。在 open 和 shared key 等简单认证的条件下，不同产品的 AP 一般的切换时延为几百毫秒到几秒之间[3]。这是无法满足对于延迟和抖动极为敏感的实时应用的，VoIP 等实时应用的切换时延需要小于 50 ms[3]，因此有必要对无线局域网内的切换进行优化，减小切换时延，从而满足语音等实时业务的需要。现今对 WLAN 切换过程的优化主要集中在对扫描阶段的优化，因为当采用 open 或者 shared key 方式时扫描的时延占了 90%以上[4]，所以降低扫描的时延也就能顺利降低切换的时延。

2 802.11 WLAN 切换过程

IEEE802.11 WLAN 的切换过程可以分为扫描、认证、关联 3 个阶段，切换的时延可以分为扫描时延、认证时延和关联时延 3 个部分。当 WLAN 采用 shared key 和 open 认证方式时，扫描时延占了切换时延的 90%以上，下面重点论述切换的扫描时延。

2.1 扫描时延

扫描阶段可以分为主动扫描和被动扫描，由于被动扫描时 STA 需要被动等待 AP 周期性地发送广播帧，耗时较长，因此本文的改进是基于 STA 的主动扫描。STA 依次在每个信道上发送探询的 Probe Request 帧，然后接收该信道上 AP 的应答帧。如果 STA 在最小信道时间(*MinChannelTime*)内接收到 AP 发送的 Probe Response 帧，那么 STA 继续在该信道上等待直到最大信道时间(*MaxChannelTime*)，否则如果 STA 没有在 *MinChannelTime* 时间内接收到该信道上的任何 AP 的响应则其立即进行下一个信道的探询。在执行标准扫描的过程中扫描一个信道的最少时延为 *CS*&*T*+*MinChannelTime*；最大的时延为 *CS*&*T*+ *MaxChannelTime*。*MinChannelTime* 和 *MaxChannelTime* 分别为信道上等待的最大时延和最小时延，*CS*&*T* 则是信道切换所需的硬件时间，其与具体的硬件有关且产生的时延较短。那么扫描产生的时延 T_{scan} 为 $T_{\min} \cdot N_{ch} \le T_{scan} \le T_{\max} \cdot N_{ch}$。$N_{ch}$ 为需要扫描的信道数量(一般，802.11a 的 $N_{ch}=13$；802.11b/g 的 $N_{ch}=11$)。在 802.11 标准中定义 *MaxChannelTime* 设置为 100 ms 左右，但是根据文献[4]的研究表明该值的设置太大导致扫描一个信道的等待时延大大增加，同时切换时延也会增加到 1 s 以上，因此文献[5-7]经过大量的实验测试之后建议 *MinChannelTime* 一般设置为 1 ms~7 ms 左右，*MaxChannelTime* 则设置为 11 ms~20 ms。同时文献[4]表明信道的切换时延 *CS*&*T* 一般需要 1 ms 左右，因此扫描所产生的时延 T 在 $150\text{ ms} \le T_{scan} \le 250\text{ ms}$ 之间。虽然经过改进的扫描时延已经降低了很多，但是仍然没有满足一般实时应用要求在 50 ms 以下的需求。现今研究的

基金项目：国家自然科学基金资助项目(90604003)
作者简介：徐 伟(1983－)，男，硕士研究生，主研方向：无线局域网协议，P2P 技术；杨 怡，博士研究生；陶 军，副教授
收稿日期：2009-01-21 **E-mail：**wei_x@seu.edu.cn

改进均使得 STA 在切换之前进行定时的扫描，然后缓存下可用的 AP，使得切换时不需要进行新的扫描从而降低切换时延。

2.2 认证和关联时延

认证是 STA 在扫描到合适的 AP 之后，只有通过认证该 STA 才能通过 AP 使用 WLAN。现有的认证方式有：(1)open，即不需要认证，只要交互一个 null 帧，产生的认证时延一般为 1 ms~2 ms[6]；(2)shared key，需要一个 4 次握手的过程，产生的认证时延一般为 10 ms 左右[6]；(3)802.11i，需要到认证服务器认证，且产生的认证时延一般在 1 s 左右[7]，本文不讨论基于该认证方式的切换时延。当 STA 完成认证之后只需要发送 ReAssociation Request 帧，然后等待 ReAssociation Response 帧完成关联也就完成了整个切换的过程。一般的关联时延为 1 ms~2 ms，采用 IAPP 协议则需要更新 WLAN 域内信息，延迟会在 10 ms 左右。

3 基于 STA 的 WLAN 快速切换方案

通过对 WLAN 中切换过程的分析，本文提出了一种基于 STA 的 WLAN 快速切换解决方案。该方案通过 AP 的信号值的动态变化触发 STA 提前扫描信道来更新 cache 中的 AP，提高 cache 命中率的同时降低 STA 不必要的更新。由于 IEEE802.11b/g 协议标准的 WLAN 存在 11 个可用信道，如果一次扫描全部的信道，那么更新 cache 的时延就会影响实时通信的质量，因此本文提出了分片的 cache 更新算法，通过划分不同的信道集合来分片扫描信道更新 cache，这样既保证了 cache 的命中率，又保证了 cache 更新的时延在 50 ms 以下。

3.1 基于动态域值的扫描触发机制

当 STA 在 WLAN 内移动时，相邻 AP 的信号及强度随时变化，这导致 cache 缓存的有效性大大降低，为此现有研究方案通常采用定时维护 cache 来提高 AP 的有效性。cache 的维护必然会带来一定的开销，如果 cache 维护的频率太高则必然会降低自身的性能从而影响到通信质量；反之如果 cache 的维护频率太低则会导致 cache 失效而重启扫描过程，那样开销会大大增加。本文提出了一种基于动态域值的扫描触发机制，在保证 cache 的命中率的同时减少不必要的 cache 更新。cache 的更新必须在 STA 的切换之前，这样才能保证 cache 的命中率，因此本文采用 *RSSI* 值的变化来触发扫描更新，保证 cache 的及时更新。为了克服 *RSSI* 突发的时变，对 *RSSI* 值作了适当的改进和优化，既可以保证 STA 的平滑扫描和切换，又可以防止因为 *RSSI* 的突变而导致的频繁切换和扫描。如下所示为 $RSSI_t = \theta \cdot RSSI_{t-1} + (1-\theta) Sample_t$。$t$ 时刻的 *RSSI* 值由 t-1 时刻的 *RSSI* 值、t 时刻 *RSSI* 的抽样值、参数 θ 确定。

当 STA 关联 AP 的 *RSSI* 值低于 *Scan Threshold*1 时，STA 立即启动定时器进行 cache 的定时更新，从而在 AP 信号继续下降时能够及时更新 cache 中的候选 AP；当 AP 的信号继续下降达到 AP 的切换域值时，STA 从 cache 中取出最好的 AP 进行关联，此时调整 STA 的扫描触发域值到 *Scan Threshold*2(*Scan Threshold*1 > *Scan Threshold*2)，直到 AP 的 *RSSI* 信号大于 STA 和 AP 正常通信的 *RSSI* 值时再将定时扫描触发的 *RSSI* 域值调整到 *Scan Threshold*1。基于动态调整的域值切换机制的优点如下：(1)在 STA 静止或者关联 AP 的 *RSSI* 值较好时，可以避免无效扫描；(2)对于 PDA 等使用内置电池的手持设备而言，定时的不必要的 cache 更新会加快电池的耗尽，从而使得其待机时间变短而影响用户的使用；(3)当 STA 刚切换到新的 AP 时，新 AP 的 *RSSI* 值必然会比较低，同时 STA 的位置变化不会很快，则 cache 中的 AP 在此时也不会很快就失效，此时如果扫描的切换域值过高则会导致 STA 在这个过渡区域的无效扫描，因此采用一个较低的 *RSSI* 扫描域值既可以保证 STA 与刚切换 AP 的正常通信又能省去不必要的扫描开销。

3.2 分片信道扫描的 cache 更新算法

基于 IEEE802.11b/g 协议的无线局域网只有 11 个频段可用，如图 1 所示，在 1~11 个频段中只有 1, 6, 11 3 个频段完全不重叠，其余频段都有部分重叠，会彼此干扰，因此在 Hotspot WLAN 的部署中大多选择 1, 6, 11 3 个不交叉的信道。

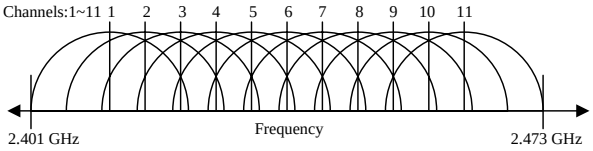

图 1 IEEE802.11b/g 使用的 11 个信道

基于动态 cache 的切换算法在切换时使用 cache 中的 AP 进行关联即可，其开销主要在于 cache 的维护。现今对动态 cache 的维护主要有 2 种方法：(1)提前扫描所有的信道，那么更新 cache 时的时延会和切换扫描的时延相当，会影响到实时通信的质量；(2)采用记录首次扫描之后存在的信道(channel mask 或者 exist channel set)加上 1, 6, 11 3 个常驻信道进行扫描更新，这样更新的时延会有所降低，但是不具有普遍意义，同时应用到不同环境时信道扫描失效的可能性大大增加。基于上述动态 cache 存在的问题和缺陷，本文提出了一种分片信道扫描更新 cache 的算法：

(1)当网卡首次启动时，执行一次全扫面，扫描所有的信道，记录存在 AP 的信道。

(2)将所有的信道划分成 3 个集合，分别为 permanent_chan_set, dynamic_chan_set, other_chan_set。其中，permanent_chan_set 为 1, 6, 11 3 个信道，保持不变；dynamic_chan_set 可以动态调整，初始值为网卡启动时执行全扫面之后除了 1, 6, 11 3 个信道之外的其余存在 AP 的信道；other_chan_set 为上一次扫描之后不存在 AP 的信道。

(3)STA 的 cache 更新首先扫描 permanent_chan_set 中的 3 个信道；其次扫描 dynamic_chan_set 中的 3 个信道，如果信道数大于 3 个则每次只扫描 3 个，依次进行更新，不足 3 个则只更新剩余的；最后如果上述 2 个 chan_set 探询到 AP 则记录一次循环扫描结束，否则标记为未结束而探询 other_chan_set，方式如上也是一次只更新 3 个信道。同时 dynamic_chan_set 和 other_chan_set 中的信道可以相互转化：当 dynamic_chan_set 中的信道不存在 AP 时，则在所有信道全部更新完之后将其移到 other_chan_set 中；反之 other_chan_set 中的信道上存在 AP 时则将该信道移到 dynamic_chan_set 中。

(4)当 STA 需要切换时则首先从 cache 缓存中选择信号最好的 AP 进行关联，如果 cache 中的 AP 全部无效则需要执行一次全扫面进行切换。

基于本文提出的 cache 更新算法既减小了 cache 更新的时延，又可以扫描所有的信道，从而避免不按常规部署的 WLAN 的信道漏选，从而具有更强的环境适应能力。

4 系统测试和分析

本文提出的算法完全在移动终端上实现，完全兼容现有无线局域网协议，具有很强的可扩展性。移动终端采用一台

Compaq nc4200 笔记本电脑，操作系统为 Linux(2.6.15)，使用 TP-Link WN310G 54 MB 和 IEEE802.11g 协议的无线网卡，原始驱动采用开源社区的 madwifi-ng，并在此驱动上实现本文提出的算法，并在实验室楼区的 Hotspot WLAN 内测试。

4.1 实验方法

为了模拟实时数据流，利用 Linux 中的 Ping 命令每隔 20 ms 向对端节点(有线网络中的一台主机)发送 ICMP 请求，接收返回的 ICMP 应答，将每个 ICMP 往返时延(Round Trip Time, RTT)记录下来。在对端节点，通过 Ethereal 获取 ICMP 数据包并进行处理，计算出每个 ICMP 请求到达的间隔(Inter-Arrival Time)。为了获得可比较的结果，STA 移动的路线和速度均相近。本实验通过和动态 cache 机制相比较，得出相应的结论。动态 cache 机制使用定时机制触发扫描，同时维护一个 cache 来缓存扫描到的 AP。

4.2 实验结果分析

如图 2 所示，当移动终端静止和小范围移动时 ICMP 包的返回时延不会有很大变化，因为本文实现了基于域值触发的扫描更新，但是 ICMP 包的返回时延仍然会有小范围的波动，这是由于 AP 信号的波动而导致 *RTT* 时延的变化。图 3 为移动中的动态 cache 更新和分片 cache 更新算法，其更新时延都在 50 ms 以下，但是明显分片 cache 更新要小于动态的 cache 更新。初始时分片 cache 更新机制在 AP 信号较好时没有进行更新，而是当 AP 信号低于扫描触发域值时才进行更新(进行更新之前 *RTT* 时延明显增加，说明 AP 信号在减弱)，这样就减少了不必要的更新，同时又能保证切换时 cache 的命中率。通过直接的切换时延测试记录动态 cache 更新和分片 cache 更新的切换时延都在 10 ms 左右，但是明显动态 cache 的更新次数要多于分片 cache 更新次数。通过对分片 cache 更新静止和运动的 2 种情况相比，动态 cache 的维护开销要明显大于本文提出的基于动态域值触发扫描的分片 cache 更新算法。

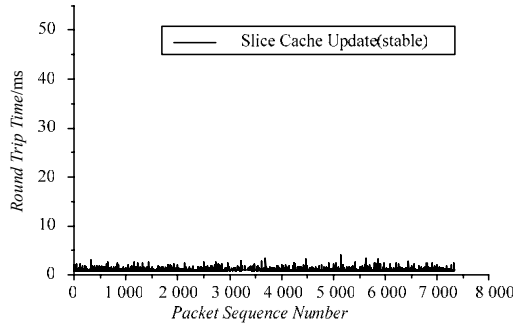

图 2　静止时 ICMP 数据包的往返时间

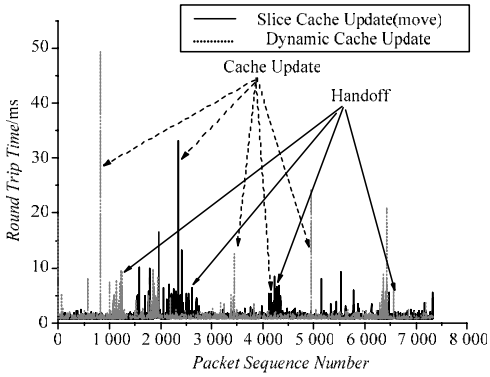

图 3　运动时 ICMP 数据包的往返时间

图 4 和图 5 为 ICMP 数据包达到通信对端的时延。移动终端在静止状态下采用分片 cache 更新算法的 ICMP 数据包的到达间隔相差不大，因为其不需要进行 cache 维护，微小的波动和 AP 的通信量大小和信号的波动有关。而在移动中的动态 cache 更新算法由于其 cache 维护的时延较分片 cache 更新算法大和频繁，因此其 ICMP 数据包的到达时延也较大、出现的波峰也较多。最后时刻动态 cache 中的峰值较多是因为此时 AP 的信号不稳定导致 ICMP 包的到达间隔变化很大而不是 cache 更新频繁所致。

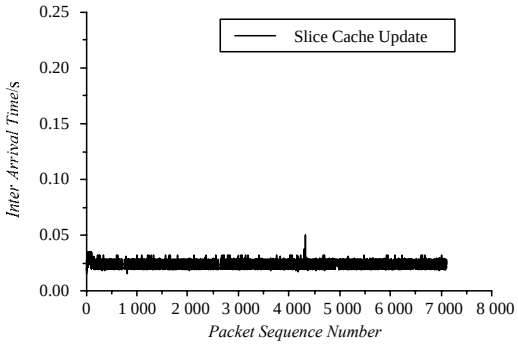

图 4　静止时 ICMP 数据包的到达间隔

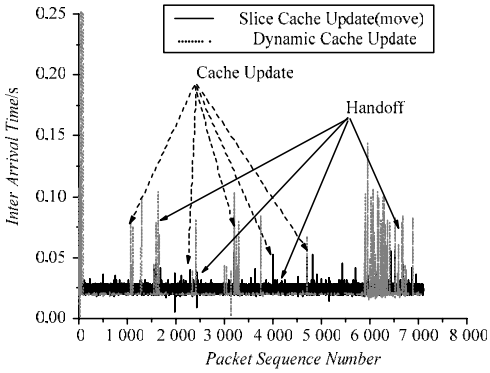

图 5　运动时 ICMP 数据包的到达间隔

5　结束语

实时应用对 WLAN 中的切换时延非常敏感，一般不能超过 50 ms，同时移动产品的电池等所具有的能量有限，能使用的时间也有限。本文提出基于动态域值的扫描触发和分片 cache 更新算法，保证了移动终端在静止或者 AP 信号强度较好的情况下，不进行 cache 更新和维护，从而节约开销，节约能量；同时分片 cache 更新算法能够在 AP 信号降低时迅速进行 cache 更新，降低了每次更新的时延，同时又保证了 cache 的命中率。

参考文献

[1] IEEE Committee. IEEE Standard 802.11-2007 Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications[S]. 2007.

[2] Gast M S. 802.11 无线网络权威指南[M]. 北京: 清华大学出版社, 2002.

[3] Wu Haitao, Tan Kun, Zhang Yongguang. Proactive Scan: Fast Handoff with Smart Triggers for 802.11 Wireless LAN[C]//Proc. of the 26th IEEE International Conference on Computer Communications. [S. l.]: IEEE Press, 2007: 749-757.

(下转第 141 页)