Layer-2 Mobility Management in Hybrid Wired/Wireless Systems

Jidong Wang and Lichun Bao *

Abstract

In hybrid wired and wireless systems, mobile hosts constantly changes points of attachment to the wired networks, causing frequent disruptions to the ongoing network traffic. An infrastructure supported approach is required to meet the stringent delay and jitter requirements in non-disrupted services. We propose a mobility management scheme, called Personal AP, to support seamless roaming. In Personal AP systems, the network attachment information, i.e., the association states, of a mobile station is extracted, and handed off from one physical access point to another along with the mobile station, thus eliminating the mobile station from re-associating with new access points. Simulation results show that Personal AP can greatly reduce the handoff latencies, and is suitable to support delay-sensitive multimedia applications.

1. Introduction

Mobility management issues have been extensively studied in cellular networks [6], where handoff are categorized into three types: network controlled handoff, network controlled and mobile station assisted handoff, mobile station controlled handoff [5]. Especially, the mobility management in the integrated data packet and cellular networks, namely the 4th generation (4G) system, was mostly based on network controlled Mobile IP approach [4] [7] [8] [13] [11]. Recently, a lot of research interests have been devoted to provide multi-hop WLAN architecture with robust mobility support [3] [15] [16].

In accordance to the on-going efforts standardizing the architectural taxonomy for control and provisioning of wireless access points by the IETF [17], we differentiate wireless terminal point (WTP) and access point (AP). WTP is the physical entity terminating wireless connections, while AP is the logical entity encapsulating data, control and management planes in the networking architecture. Especially, the data plane consists of the physical and the data link layer protocols. With regards to the architectural arrangements of the AP functionalities, AP can be organized by the autonomous, centralized or distributed architecture.

There are concrete implementations for each of the architectures. IEEE 802.11 standards inherently provide mobile station controlled mobility management at the data link layer [1]. IEEE802.11f added the network controlled handoff component, called IAPP, for the inter-operations of access points [2]. Both IEEE 802.11 and IEEE 802.11f depends on the mobile stations sending out association or re-association requests to APs before handoff happens. Therefore, they are representatives of the autonomous architecture, and stand in most current deployments. The advantage of the autonomous architecture is that it is cheap and easy to deploy.

The centralized architecture has the most varieties in real-world implementations. In addition to WTP and AP, it defines another concept – "access controller" (AC) that works as the central controller of the system-wide functionalities. The central architecture can have one of three functional separations, a) *Local MAC*, where the majority of AP is implemented on the WTP, b) *Split MAC*, where only delay-sensitive functions are implemented on WTP, and c) *Remote MAC*, where the entire AP functions are implemented at the AC (access controller).

Most of the aforementioned architectures are based on the framework specified in IEEE 802.11 [1], in which the handoff latencies are incurred by probing, authentication and association activities. There are a lot of efforts devoted to reducing the handoff latencies. IEEE 802.11f provided pre-caching optimizations during the association procedures [2]. However, 802.11f depends on the re-association frame in order to identify the old AP for mobility management purposes.

We propose a *Personal AP* mobility management mechanism based on the autonomous AP architecture, where the WTP (wireless terminal point) implements all of the AP functionalities. Therefore, we use AP and WTP interchangeably in this paper. In Personal AP systems, APs constantly send out traffic reports about individual mobile stations for handoff decisions. Once a handoff decision is made regarding a mobile station, the complete context of the mobile station is transferred from the old AP to the new AP, and the new AP operates just like the old AP with all the related association states. Because the APs as a whole appear as if person-

*Bren School of Information and Computer Sciences, University of California, Irvine, CA 92697. Email: {jidongw, lbao}@ics.uci.edu

alized for mobile stations, we call our system "Personal AP". The context information regarding a mobile station at an access point is includes association states, timestamp, sequence number, BSSID, capability, related security information etc. [2] [10].

Personal AP system is an extension of other mobility management schemes in that it is for maintaining constant connections for *on-going* data transfers. If a mobile station falls into sleep or does not have continuous and intensive traffic, the mobility support mechanism can fall back to other handoff mechanisms, such as the regular IEEE 802.11 or Mobile IP.

The paper is organized as follows. Section 2 analyzes the handoff procedure in large-scale IEEE 802.11 system deployments. Section 3 introduces both the centralized and distributed WLAN system management framework. Section 4 describes the Personal AP mechanisms in support of seamless mobility management in IEEE 802.11 systems. Section 5 evaluates the performance of Personal AP system in comparison with the regular IEEE 802.11 mobility management. Section 6 concludes the paper.

For simplicity, we use these acronyms because of their frequent appearances: STA - station, MS – mobile STA, AP – access point.

2. Mobility Management in 802.11 Systems

In general, there are three steps in IEEE 802.11 handoff procedures: channel scanning, authentication and re-association, as illustrated in Fig. 1. Accordingly, the handoff latency is broken down into three parts: the probing delay, the authentication delay and the re-association delay.

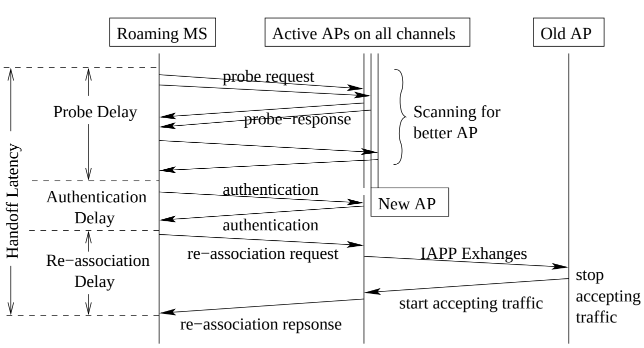


Figure 1. Illustration of Handoff Delay

The probing delay is due to the channel scanning by the mobile station of all the APs across all supported channels. The channel scanning scheme can be either passive or active. For applications requiring fast handoffs between access points, active channel scanning is preferred because of the lower latency in discovering potential access points to associate to [12]. Probing delay contributes the majority (about 90%) of the handoff latency [9].

The handoff latency can be reduced at any of the three steps of the procedure. Different mobility management schemes have aimed at saving time spent at various steps of the handoff process.

3. Personal AP Architectures

3.1. Assumptions

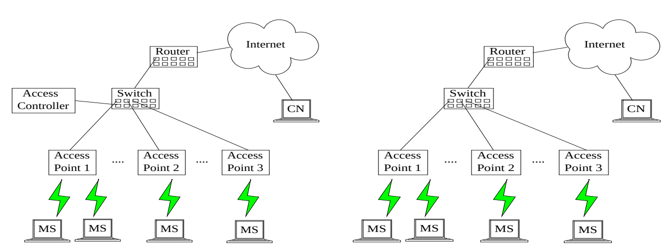
In IEEE 802.11, the Basic Service Set (BSS) is the building block of the wireless system, and consists of a single AP and a number of MSs associated with the AP in a typical deployment. Multiple BSSs are interconnected with each other through a distribution system and form an Extended Service Set (ESS). The associated MSs communicate with each other or with Internet hosts through APs. The IEEE 802.11 standard [1] specifies two WLAN architectures, *infrastructure mode* and *ad-hoc mode*.

In Personal AP systems, We assume that APs are densely deployed so as to provide continuous coverage at the deployment site. This is a reasonable assumption in either enterprise or campus deployment because of the dropping hardware costs, and the desired continuous connectivity. Under the dense AP deployment assumption, multiple APs with similar capabilities and different BSSIDs operate in the same frequency channel. Stations changing from one frequency band to another require additional mechanisms other than what we describe in this paper for Personal AP system.

Personal AP system enforces the requirement of IEEE 802.11 that an STA may have only one association with the infrastructure at any given time.

3.2. Architectural Options

The coordination between APs for mobility management can be implemented in either a centralized architecture or a distributed architecture.



(a) Centralized (b) Distributed

Figure 2. Personal AP Architectures

Fig. 2 (a) shows our centralized WLAN architecture that adds in a access controller in the distribution system of an IEEE 802.11 deployment. The access controller monitors MS's activities, and determines when and where to make handoff decisions.

In large Personal AP system deployment, there could be multiple access controllers, and the global user database needs to be maintained to enable seamless roaming between different access controller clusters.

Personal AP system can also be implemented on a distributed architecture where all the functionalities of the access controller are delegated to the APs, as shown in Fig. 2 (b), in which the APs are connected by a high-speed switched network, and coordinate with each other to maintain the best connection for the MS.

The deployment of the Personal AP system is self-adaptive. In the centralized architecture, the access controller advertises its existence by periodically broadcasting advertisement packets. If the Personal APs receive the advertisement packet, they adapt to centralized mode by registering itself with the access controller, and rely on to the access controller for handoff decisions and coordination. If the APs do not receive the advertisement packet, they will adapt to distributed mode by default.

Because the centralized architecture does not require layer-2 broadcast to exchange MS information, it is more efficient in terms of the control overhead, thus is more preferable than the distributed architecture.

4. Personal AP Protocol

Except for the handoff operations, most of the following descriptions about Personal AP protocol are suitable for both centralized and distributed mobility management architectures, unless otherwise indicated.

4.1. Handoff Decisions

Handoff decisions in a WLAN system depend on many factors from both users and service providers. The goal of Personal AP system is for the service providers to offer the best and non-disrupted network connectivities to the on-going user traffic. Therefore, the key factors that determine a handoff decision are:

1. Signal quality of the on-going connection. Usually, the received signal strength index (RSSI) value is the best indicator of the MS to AP connections. In order to provide the best connectivity for the user applications, the MS to AP connection with the highest RSSI value should be taken.

2. Traffic characteristics of the user applications. User applications inherently have different data rates, burstiness, duration characteristics. And the expected behavior of the applications are also different. For instances, remote login `SSH` and web browsing `HTTP` applications presents irregular and bursty traffic patterns with short response time, while `FTP` for file transfer and `RTP` for multimedia streaming are usually allowed to have long response time with high average volume. Therefore, mobility support protocols can take advantage such facts to allow STA-initiated handoff in the former two applications, and require the Personal AP protocol to help fast handoff in the latter two applications.

In order to get timely MS-AP network connection information, the APs in the Personal AP system collect the RSSI information of the overheard data frames from all possible MSs.

For simplicity, the indicator of the connection quality is based on an exponential moving average (EMA) of the RSSI values of the MS-AP connections. An EMA smooths out sudden changes in the signal strength in MS's irrational movements, and avoid unnecessary handoffs. A RSSI moving average $\overline{RSSI}$ is computed according to

$$\overline{RSSI}_{new}^{MS} = \alpha \cdot RSSI_{new}^{MS} + (1-\alpha) \cdot \overline{RSSI}_{old}^{MS}$$

where $RSSI_{new}^{MS}$ reflects the newly acquired signal quality information. The α value is an empirical value, and our implementation chooses $\alpha = 0.9$ for fast MS tracking.

In the centralized Personal AP architecture, the signal quality data is sent to the access controller, which summarize a characteristic indicator of the MS-AP connections, and may decide to handoff to the AP that reports the best connection.

In the distributed architecture, the APs summarize the connection quality instead. In order to optimize the control overhead, the frequency of the RSSI reports is adapted to the rate of RSSI changes. When the MS moves in a high speed, its RSSI changes faster, and the RSSI reports are sent more frequently for better accuracy. If the MS moves slow, the RSSI reports are sent less frequent. In addition, not all APs need to report the summarized RSSI values regarding a particular MS-AP connection. Only those APs that are either associated with the MS, or have better summarized RSSI values than that of the current MS-AP connection may broadcast their observations of the connection quality. Because the connection quality information is exchanged periodically and proactively, an AP with the current association with the MS evaluates the benefits of potential handoff decision. For simplicity, a handoff decision is made by an AP if another AP reports the best connection quality among all the APs in the distributed Personal AP architecture.

4.2. Handoff Operations

Once a handoff decision is made for an MS to connect with a new AP, Personal AP protocol transfers the context information from the old AP to the new AP. Because Personal AP system has similar context transfer operations as IAPP, we follow a similar style describing Personal AP as in IAPP, and try to provide non-conflicting names for control messages between the APs, and the access controller in the centralized architecture. For traffic monitoring purposes, WATCH messages carry the RSSI reports from APs. To tell new APs to act as the associated AP for an MS, START message is used. Messages related with handoff transfer operations are prefixed with HO_.

IAPP Ver.	Command	Identifier	Length	Data
1B	1B	2B	2B	0~n B

Figure 3. IAPP and Personal AP Packet Format

Fig. 3 shows the general IAPP packet defined in IEEE 802.11f. The IAPP packet is carried in either TCP or UDP protocols over IP. The command field specifies the command type like WATCH, HO_INFORM, the identifier field is used to match request and response by sharing the same value of identifier field. Data field has variable length depending upon the command type. For example, for HO_START message sending from access controller to old AP, the data field includes information like new AP's BSSID, while for Context transfer message, the data field contains the context information regarding an MS-AP connection, including information elements such as the MS's MAC address, association ID (AID), data frame sequence number, and the old AP MAC address (equivalent to the BSSID), data frame sequence number as well as the buffered dataframes for MS.

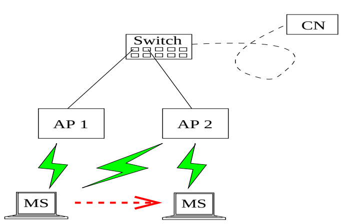


Figure 4. A Simple Mobility Scenario in Personal AP system

For clarity, we run through the handoff operations by looking at one MS's movement through a Personal AP system with two overlapping APs, interconnected by an Ethernet switch, as shown in Fig. 4. For generality in both centralized and distributed architectures, other relevant components, such as the access controller, the Internet and the correspondent node (CN), are omitted from the figure.

At the beginning, the MS joins the WLAN using the standard 802.11 association process by performing the probing, authentication and association processes. In Fig. 4, the STA is associated with AP1, which is regarded as the STA's primary and personal AP. After the initial association, APs operate differently in centralized architecture and distributed architecture.

4.2.1 Centralized Coordination

In the centralized architecture, AP1 informs the access controller about the association, and the access controller in turn creates and maintains an MS specific entry mapping the MS to AP1. Suppose that the MS carries out an active connection with its correspondent node, while moving from AP1 to AP2. Because both AP1 and AP2 periodically report the MS RSSI values to the access controller, when the MS-AP2 connection indicates a better choice than the current MS-AP1 connection, a network-initiated handoff will be triggered by the access controller.

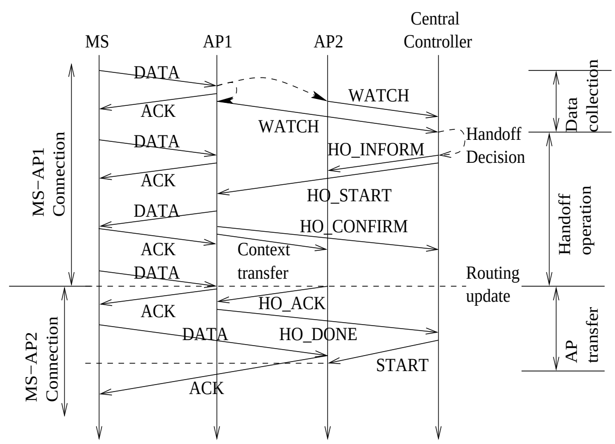


Figure 5. Handoff Control Flow in Centralized Personal AP System

As shown in Fig. 5, the handoff operations start off by APs reporting the MS-AP channel quality and traffic information to the access controller using WATCH messages. When the access controller makes handoff decision, the access controller sends an HO_INFORM message to the new AP (AP2), asking AP2 to accept the MS. At the same time, the access controller sends an HO_START message to the old AP (AP1), requesting transfer the MS context to AP2. Once AP1 gets the handoff complete message HO_ACK from AP2, AP1 sends out an HO_DONE message to the access controller, telling the completion of the handoff operations. The access controller in turn tells AP2 to function as the associated AP with the transferred context by sending a START message.

4.2.2 Distributed Coordination

In the distributed architecture, while the MS roams, AP1 periodically broadcasts the RSSI values in WATCH messages to other APs in the layer-2 network. When the RSSI values at AP2 are better than that at AP1, AP2 starts to broadcast the RSSI regarding MS-AP2 connection. After certain backoff latency, the AP reporting the best RSSI values wins, and a handoff operation is initiated by the currently associated AP. In this case, AP2 wins, and AP1 arrives at a handoff decision,

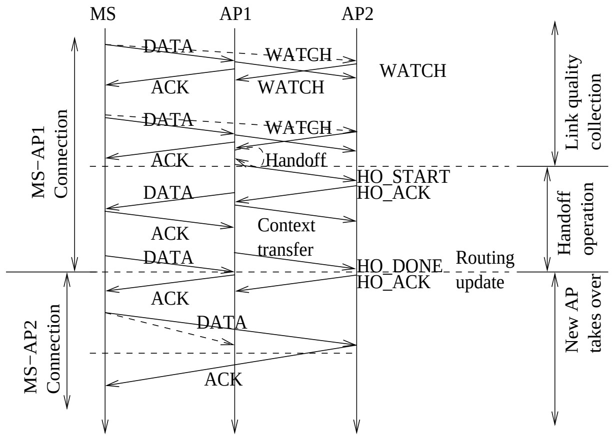


Figure 6. Handoff Control Flow in Distributed Personal AP System

and initiates the handoff operation by sending a HO_START message to the old AP (AP2) to transfer the MS context to AP2.

While the context information is being transferred, AP1 may keep receiving incoming data packets from the correspondent node. In such cases, AP1 forwards the data packets to the new AP. The MS may also send data frames to the old AP, in which case AP1 simply acknowledges the data frames and forwards them to the correspondent node.

After the context information is transferred, AP2 acknowledges the receipt of the transfer by sending HO_ACK to AP1. From this point on, further data packets from the CN will directly get to AP2, and future data frame from the MS will be acknowledged by AP2.

4.3. Data Plane Operations

Because the handoff operations transfer the complete context information regarding the MS-AP association to the new AP, the new AP is able to pretend to be the old AP, and carry out the same data plane communication as the old AP. Virtually, it is similar to the fact that the old AP has “followed” and “moved” with the MS like a “ghost” in the Personal AP system. Therefore, the handoff operations have no effects to the MS’s perception of the WLAN system. The same MS-AP information is carried in data frames.

4.4. Routing Control

The layer-2 routing in Personal AP systems consist of two part: layer-2 and layer-3 routing update when the MS moves between APs.

The layer-2 route update happens when the MS moves between APs that are located within the same subnet, which is exactly the example given in Fig. 4. In this case, an a layer-2 broadcast route update is sent by the new AP with the MS’s MAC address as the source address. This broadcast message updates the intermediate switches’ learning table for layer-2 routing purposes. Such route update procedure happens once the new AP receives the HO_DONE message, and does not interfere with the other parts of the handoff process.

The layer-3 route update happens when the MS moves between APs that are located in different subnets, and the subnet IP address spaces take separate entries in the routing table of upstream routers for the correspondent node. In this case, Personal AP systems depend on the layer-3 (IP layer) route updates to the MS, but still carries out the layer-2 route update procedure at the new AP, because layer-2 and layer-3 operations at the APs are separate, therefore saving the association and re-association process in 802.11. Nonetheless, the layer-3 route update can be triggered by the APs in the Personal AP system so that the MS starts DHCP IP address renewal or search for Mobile IP agents for packet routing purposes.

In any case, the Personal AP context transferal takes place as usual because the context information is only related with layer-2 MS-AP context.

4.5. Network Management

Because Personal APs now appear to be ubiquitous, and the context information follow assigned MSs, it may cause some disruptions to the regular network management functionalities, such as beacon transmissions, and power-save mode scheduling. However, MSs only need to receive them at the initial stage when the MSs join the Personal AP network. Once the MSs start intensive communication, network connectivity and capability are provided at the best efforts by the Personal APs. Therefore, there is no need to periodically receive beacons for these MSs.

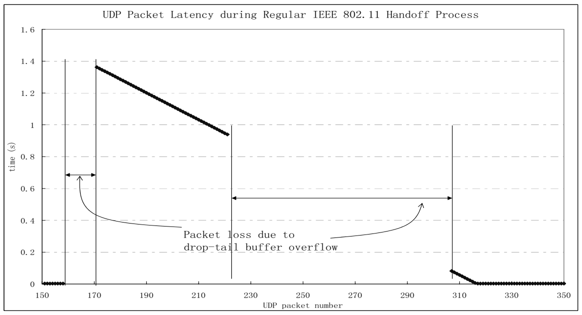
Because the mechanism to determine when to roam is not defined by the IEEE 802.11, and is left to vendors to implement, the handoff decision may not only be decided by APs, but also involve the decision by the MSs. If an MS roaming decision is based on the beacon receptions, Personal AP system still transfers the MS-AP context information between APs, but the context will be discarded when the new MS-AP association is established.

For those MSs in power-save mode, Personal AP system does not provide additional mechanisms to handle their data frames because their traffic is not delay-sensitive.

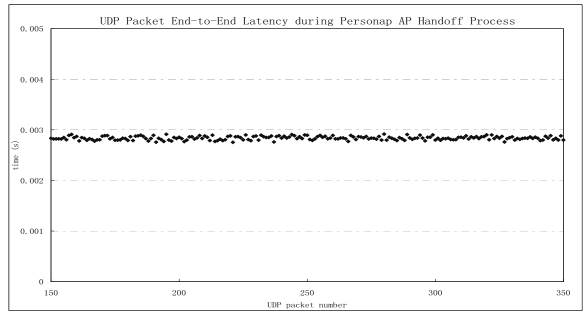
5. Performance Evaluations Of Personal AP

5.1. Comparisons with IAPP

Comparing with IAPP proactive caching approach, the advantages of using the Personal AP system are the fast speed of handoff, and the relieved MS’s roles in the mobility management. First, the Personal AP scheme does not need to maintain the neighbor graph for each AP. Secondly, in IAPP,



(a) UDP Delay in 802.11 System



(b) UDP Delay in Personal AP System

Figure 7. Delay in CBR Traffic

multiple copies of pre-authentication context are distributed to neighbor APs, while Personal AP only forwards one copy of context block to the designated new AP. Third, an MS is unaware of the Personal AP mobility management operations, and there is no association or re-association process for the MS. Therefore, Personal AP saves the handoff latency and is more efficient in handling mobility than IAPP.

One drawback of IAPP is that it relies on an STA making use of the 802.11 `re-association` request when roaming from one AP to another. If an STA uses the 802.11 `association` request, there could be multiple concurrent associations between the STA and the WLAN distribution system.

5.2. Simulation Results

We compare our Personal AP mobility management approach with the regular 802.11 handoff mechanisms. A simulation study is conducted using simulator NCTUns 2.0 [14] [1] to evaluate the handoff latency and traffic delays on TCP and UDP flows. Because we assume sufficient bandwidth on the wired infrastructure, whether to use the centralized or distributed Personal AP architecture does not make any difference to the traffic characteristics. Therefore, the following results apply to both the centralized and the distributed Personal AP architectures.

The first set of simulations run over a network topology containing two APs, one MS and one correspondent node (CN) as shown in Fig. 4. A CBR traffic using UDP and an FTP traffic using TCP connection are setup respectively from the MS to the CN for the duration of our simulations. The CBR traffic consists of UDP packets of 1024 bytes at a constant rate of 100 packets/second.

During the simulation, the MS moves from one AP1 to AP2 and triggers handoff in both Personal AP and normal IEEE 802.11 setups. The handoff latency is collected as the performance metric to compare our Personal AP with the standard 802.11 handoff as shown in Fig. 7 and Fig. 8.

Under the standard IEEE 802.11 handoff, the STA performs full channel scanning through all eleven channels. The latency is measured from the time instant that the MS sends out `probe` request to the time that the STA receives `re-association` reply. For simplicity, the re-authentication process is not counted because it does not contribute much to the total latency.

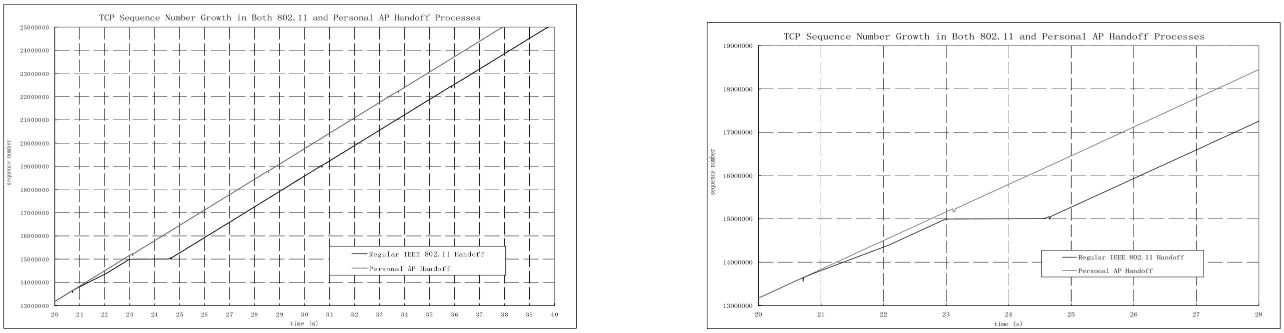
Under the Personal AP system, the delay is tracked from the moment when the access controller triggers a handoff decision to the moment when the new AP acknowledges its full association with the MS.

In Fig. 7 (a) and (b), the horizontal axis is the packet sequence number, the vertical axis is the UDP end-to-end delay in seconds. During the regular 802.11 handoff, end-to-end latency increases significantly before handoff completes. Some packet losses also happened due to buffer overflow and packet drops. In Fig. 7(a), a total of 109 UDP packets are lost during the handoff in the regular 802.11 system. Comparatively, Personal AP system completes handoff within milliseconds, which are trivial compared to 10 ms packet interval and 2.7 ms average transmission delay.

Fig. 8 (a) and (b) in shows the TCP performance differences between regular 802.11 and Personal AP. As we can see, the TCP connection using the regular 802.11 handoff scheme was disrupted for 1.5748 seconds from 42.1280 to 43.7028 second, of which the 802.11 re-association process incurred a latency of around 650 ms. Such delay is significant for multimedia or real time applications that are sensitive to delays. In the Personal AP system, the handoff process took 0.985 ms from 23.0002923 to 23.0012773 second to complete, which barely affects the TCP stream.

One notable phenomenon in the simulations is that the

[1] NCTUns 2.0 is by far the best network simulator we could find for our purposes.



(a) TCP Delays in 802.11 and Personal AP Systems

(b) Closeup Look at TCP Delay in 802.11 and Personal AP Systems

Figure 8. Sequence Number Growth of TCP Flows

handoff starts at different time instants in Personal AP and regular 802.11 systems. The regular 802.11 handoff mechanisms provided by NCTUns adopted a "lazy" scheme in which the MS does not initiate the handoff process until the RSSI is below a certain low threshold, even if there are APs that has better RSSI with that MS. In the Personal AP system, the handoff begins when the central switch receives a better RSSI report from a new AP about the MS than the currently associated AP. Therefore, the regular 802.11 system started handoff at 42.1280 second, while the Personal AP system started handoff at time 23.0003 second.

In particular, a second set of simulations were carried out to investigate the performance of Personal AP systems under heavy traffic load by assume a finite 10Mbps wired bandwidth. The end-to-end delay is measured in scenarios where all MSs send UDP traffic to a single host at a constant 100 packet/second rate. The delay versus the different numbers of MSs is shown in Fig. 9.

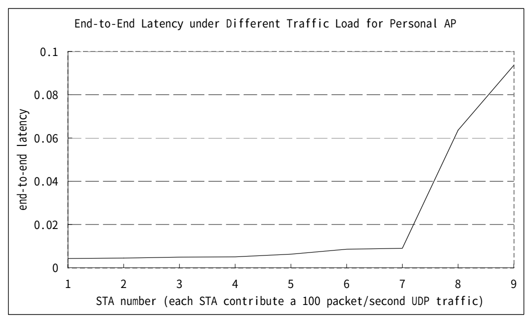


Figure 9. End-to-End Delay in Personal AP Systems

As indicated by Fig. 9, the end-to-end delay increases more significantly as the aggregated traffic gets closer to the 10Mbps total bandwidth of the wired network.

In addition, the control overhead of the distributed Personal AP architecture is also measured to see the scalability of Personal AP systems. The centralized architecture does not rely on layer-2 broadcast for inter-AP coordination, therefore has less control overhead. The overhead is measured by the average bandwidth consumption by each AP for individual MSs, including the RSSI reports and handoff control messages.

Fig. 10 shows the average bandwidth consumption for one MS during the simulation where handoff happens four times. As we can see, the bandwidth consumption increases as the moving speed of MSs increases. However, it is within several hundreds of bits per second even when the MS is moving at a fairly high speed, and is less than 0.002 percent of the available 10Mbps bandwidth for one STA. Moreover, the bandwidth consumption increases approximately linearly with number of STAs. Under such generic statistics, Personal AP systems scale well for a large number of STAs.

6. Conclusion

We have presented a novel handoff approach that is based on Personal AP concept for mobility management, and implemented it under both centralized and distributed architectures. The goal is to reduce or eliminate disruptions to ongoing traffic carried out by mobile stations. It is achieved by coordinating mobile station traffic and connectivity information between APs, and transferring the MS-AP context to the best connected AP to the mobile station, therefore, keeping the MS-AP association states intact at different APs, and avoiding the mobile station to re-attach itself to the wired

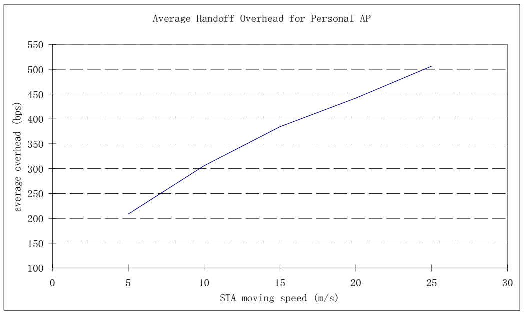


Figure 10. Overhead in Personal AP System

network. Simulation results show that Personal AP system introduces very little handoff latencies, and has very little control overhead. Such characteristic makes Personal AP systems attractive for supporting VoIP and multimedia applications.

References

[1] IEEE Std 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Technical report, IEEE, Jul. 1997.

[2] IEEE Std 802.11f. IEEE Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation. Technical report, IEEE, Jul. 2003.

[3] A. Acharya, A. Misra, and S. Bansal. High-performance architectures for IP-based multihop 802.11 networks. In *IEEE Wireless Communications, Vol. 10*, pages 22–28, Oct. 2003.

[4] K. Ahmavaara, H. Haverinen, and R. Pichna. Interworking architecture between 3GPP and WLAN systems. In *IEEE Communications Magazine, Vol. 41*, pages 74–81, Nov. 2003.

[5] I.F. Akyildiz, J. McNair, J.S.M Ho, H. Uzunalioglu, and W. Wang. Mobility management in next-generation wireless systems. In *Proceedings of the IEEE, Vol. 87*, pages 1347–1384, Aug. 1999.

[6] I.F. Akyildiz, J. Xie, and S. Mohanty. A survey of mobility management in next-generation all-IP-based wireless systems. In *Wireless Communications, IEEE (See also IEEE Personal Communications)*, pages 16–28, Aug. 2004.

[7] M.M. Buddhikot, G. Chandranmenon, S. Han, Y. W. Lee, S. Miller, and L. Salgarelli. Design and implementation of a WLAN/cdma2000 interworking architecture. In *IEEE Communications Magazine, Vol. 41*, Nov. 2003.

[8] M.M. Buddhikot, G. Chandranmenon, S. Han, Y.W. Lee, S. Miller, and L. Salgarelli. Integration of 802.11 and third-generation wireless data networks. In *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, pages 503–512, 2003.

[9] A. Mishra, M. Shin, and W. Arbaugh. An empirical analysis of the IEEE 802.11 MAC layer handoff process. In *Computer Communication Review*, pages 93–102, 2003.

[10] A. Mishra, M. Shin, and W.A. Arbaugh. Context caching using neighbor graphs for fast handoffs in a wireless network. In *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, pages 351–361, Mar. 2004.

[11] C. Perkins. RFC2002 - IP Mobility Support. Technical report, Internet Engineering Task Force (IETF), IBM, Oct. 1996.

[12] I. Ramani and S. Savage. SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks. In *Proceedings of the IEEE Infocom Conference*, Miami, FL, Mar. 2005.

[13] A. Saleh. Mobile IP performance and interworking architecture in 802.11 WLAN/CDMA2000 networks. In *Proceedings of Second Annual Conference on Communication Networks and Services Research*, pages 75–79, May 2004.

[14] S.Y. Wang, C.L. Chou, C.H. Huang, C.C. Hwang, Z.M. Yang, C.C. Chiou, and C.C. Lin. The Design and Implementation of the NCTUns 1.0 Network Simulator. *Computer Networks*, 42(2):175–197, Jun. 2003.

[15] H. Wei and R.D. Gitlin. WWAN/WLAN two-hop-relay architecture for capacity enhancement. In *IEEE Wireless Communications and Networking Conference (WCNC) 2004*, pages 225–230, Mar. 2004.

[16] S. Xu, S. Papavassiliou, and S. Narayanan. Layer-2 multi-hop IEEE 802.11 architecture: design and performance analysis. In *IEE Proceedings of Communications, Vol. 151*, pages 460–466, Oct. 2004.

[17] L. Yang, P. Zerfos, and E. Sadot. Architecture Taxonomy for Control and Provisioning of Wireless Access Points(CAPWAP). Technical report, IETF CAPWAP Working Group, Nov. 16 2004. draft-ietf-capwap-arch-06.