

# Personal AP Protocol for Mobility Management in IEEE 802.11 Systems

Lei Zan, Jidong Wang and Lichun Bao  
 Bren School of Information and Computer Sciences  
 University of California, Irvine, CA 92697  
 Email: {lzan, jidongw, lbao}@ics.uci.edu

**Abstract**—In mobile wireless systems, the quest to support delay-stringent multimedia applications challenges most existing solutions to the mobility support and traffic management problems. An infrastructure supported approach is required to provide non-disrupted services with seamless roaming capabilities. We propose a mobility management scheme, called *Personal AP*, to support station mobility efficiently. In Personal AP mobility support system, the mobility context of each mobile station is defined by the relevant state information at the currently associated access point, including the MAC layer association states at the access point. When the mobile station roams, the access point context follows the mobile station from one physical access point to another, thus creating the “ghost” access point following the mobile station and eliminating the mobile station from re-associating with new access points. Personal AP system improve the seamless roaming support by avoid the lengthy re-association process commonly seen in regular IEEE 802.11 systems. The essential idea of Personal AP is applicable in other wireless systems as well.

**Keywords**—IEEE 802.11, Wireless LAN (WLAN), mobility, handoff, seamless roaming.

## I. INTRODUCTION

Wireless network deployments, especially those based on IEEE 802.11 suite, are gaining great momentum in enterprise, campus and home environments. In large-scale WLAN deployments, supporting user and device mobilities is a critical issue because continuous network connectivity is highly desirable for most applications. A fast handoff mechanism is particularly necessary for VoIP (voice over IP) and streaming video/audio applications because the total latency they can tolerate cannot exceed  $50ms$  (milliseconds) and  $150ms$ , respectively, for best user perceptions.

Mobility management issues have been extensively studied in cellular networks [8], where handoff are categorized into three types: network controlled handoff, network controlled and mobile station assisted handoff, mobile station controlled handoff [7]. 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 [6] [10] [11] [16] [17].

Recently, a lot of research interests have been devoted to provide multi-hop WLAN architecture with robust mobility support [5] [19] [20]. In accordance to the on-going efforts standardizing the architectural taxonomy for control and provisioning of wireless access points by the IETF [21], we differentiate wireless terminal point (WTP) and access point (AP). WTP is the physical entity terminating wire-

less 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. However, Without additional mechanisms that accelerate the re-association and handoff operations, the plain handoff approach in IEEE 802.11 commonly introduces hundreds of milliseconds latency and possible packet loss, which are fatal to multimedia applications.

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, such as our Personal AP system, b) *Split MAC*, where only delay-sensitive functions are implemented on WTP, such as Meru Networks Systems [13], and c) *Remote MAC*, where the entire AP functions are implemented at the AC (access controller), such as the Aruba Networks Systems [12].

The third architecture is the distributed one, where ad hoc networks and mesh networks fall in.

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, where each of the aforementioned architectures proposed characteristic solutions. 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 new mobility management mechanism, called *Personal AP*, based on the centralized architecture where one or multiple access controllers control the handoff operations. For simplicity, we describe the Personal AP system using only one access controller. Because most of the AP functionalities are implemented on the WTP, we use AP and WTP interchangeably in this paper. In addition, we define the station information regarding a mobile station at the access point as the context of the mobile station, which includes association states, timestamp, sequence number, BSSID, capability, security information [2] [15].

In Personal AP systems, APs constantly send traffic reports about individual mobile stations to the access controller to monitor mobile station connections with the APs. If it is better to handoff a mobile station to a new AP, the complete context of the mobile station at the old AP is transferred to the new AP, and the new AP operates just like the old AP with the same BSSID etc. Therefore, the associated AP appears to be a “ghost” following the mobile station wherever it moves, and offers the best network connectivity to the mobile station. Because now APs appear as if personalized for mobile stations, we call our system as Personal AP.

However, the context information maintenance in Personal AP systems is only necessary to provide 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. Personal AP protocol is a natural extension of IEEE 802.11f under the new “ghost” AP concept, and has a lot of common information shared with IEEE 802.11f.

The paper is organized as follows. Section II analyzes the handoff procedure in large-scale IEEE 802.11 system deployments. Section III introduces our centralized WLAN system management framework. Section IV describes the Personal AP mechanisms in support of seamless mobility management in IEEE 802.11 systems. Section V evaluates the performance of Personal AP system in comparison with the regular IEEE 802.11 mobility management. Section VI concludes the paper.

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

## II. MOBILITY MANAGEMENT IN 802.11 SYSTEMS

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

The probe 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

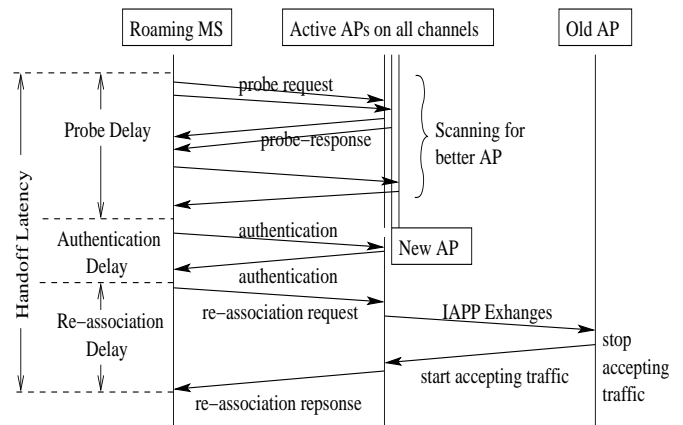


Fig. 1. Illustration of Handoff Delay

or active. In the *active* scanning scheme, an 802.11 device broadcasts an 802.11 probe request on the channel it is scanning on using a zero-length broadcast SSID (Service Set Identification). Afterward, the device will add any received 802.11 beacons or probe responses to its cached BSSID scan list. In the *passive* scanning scheme, the 802.11 device does not send an 802.11 probe request. Instead, it dwells on a channel for a period of time and adds any received 802.11 beacons or probe responses to its cached BSSID (Basic Service Set ID) scan list. 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. Probe delay contributes the majority (about 90%) of the handoff latency [14].

The authentication delay is introduced during the exchange of authentication information between a mobile STA and an AP. Depending on the security requirements of the WLAN systems, different amounts of delay are incurred during the authentication processes. In IEEE 802.11 Open System scheme, the delay is nothing. In the shared-key authentication schemes, dynamic encryption key generation requires additional message exchanges to complete.

The re-association delay is due to the exchange of **re-association** request/response frames and some context information about the mobile STA. Additional delay can be introduced by IAPP messages if IAPP is implemented [2].

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.

## III. PERSONAL ACCESS POINT ARCHITECTURE

### A. Assumptions

The IEEE 802.11 standard [1] specifies two WLAN architectures, *infrastructure mode* and *ad-hoc mode*. We are interested in large-scale WLAN system deployments under the infrastructure mode.

In Personal AP systems, we assume APs are densely deployed. This is a reasonable assumption in either enter-

prise or campus deployment because the cost of APs has been dropping greatly recently, and continuous coverage and connectivity is desired. Under the dense AP deployment assumption, multiple APs with similar capabilities and different BSSIDs operate in the same frequency channel in the adjacent area.

The requirement of IEEE 802.11 that an STA may have only a single association is enforced at any given time.

### B. Centralized Architecture

In IEEE 802.11, the Basic Service Set (BSS) is the basic building block in the architecture, and the members of a BSS communicate with each other or with the Internet hosts through APs. Multiple BSSs can interconnect with each other through a distribution system and form an Extended Service Set (ESS). Depending on the capabilities of the APs, the distribution system can be layer-two or layer-three backbone network. Fig. 2 illustrates the basic WLAN architecture defined in the IEEE 802.11 standard [1].

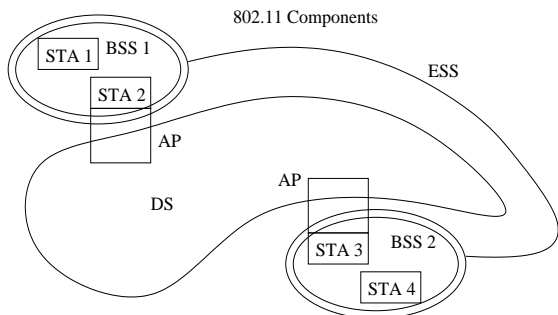


Fig. 2. WLAN architecture defined in IEEE 802.11

The biggest challenges of this conventional architecture for enterprise deployments are AP management and network maintenance issues. For cost-effective considerations, the commercial WLAN systems start out with stand-alone devices that are connected to the distribution system through Ethernet and IP. As the number of APs increases, the management and maintenance of APs, such as the radio configurations (frequency/channel usage, power selection), software upgrades, become increasingly difficult. Therefore, a unified and self-adaptive centralized architecture is desirable. Our Personal AP system is based on such centralized WLAN architecture to handle STA mobility and manage AP contexts effectively and efficiently.

Fig. 3 shows our centralized WLAN architecture. The access controller is the handoff controller of the Personal AP system. The advantages of using the centralized controller are:

1. The fast speed of handoff. 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, IAPP may not be able to find out the old AP to which the STA was associated, resulting in maintaining multiple concurrent associations between the STA and the WLAN distribution system.

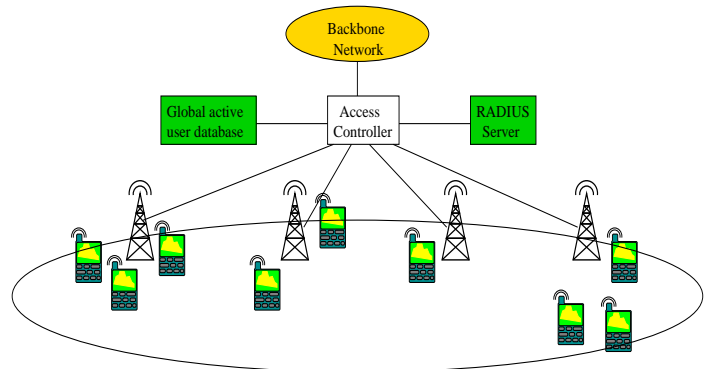


Fig. 3. Centralized WLAN Architecture

2. Relieved mobile STA roles in the mobility management. With an access controller, the mobile STAs no longer need to constantly search for best APs to connect to. Instead, the connections are monitored by the access controller for the mobile STA, and the best connection is maintained for the mobile STA using Personal AP protocols.

In large Personal AP system deployment, there could be multiple access controllers, and the Global User Database stores updated active user connectivity states helping to enable seamless roaming between different access controller clusters.

Similar to IAPP's reliance on RADIUS to implement access point and security management functionalities, Personal AP system may use RADIUS for the identity-based authentication in wireless access networks. In WLAN environment, users will undergo 802.1x authentication check before they are allowed to send traffic [4]. Although RADIUS support is optional within IEEE 802.1x-2001, it is expected that most IEEE standard 802.1x authenticators will function as RADIUS clients.

However, the capabilities of the RADIUS platform needs to be improved for handoff management between APs because RADIUS requires a fixed client IP, and fixed shared secret, which is a problem if IEEE 802.1x APs auto-configure through IP addresses obtained by DHCP, and when shared secrets are difficult to manage.

## IV. PERSONAL AP PROTOCOL

### A. Handoff Decisions

Handoff decisions in a WLAN system is dependent on many factors, such as the requirements of end-user applications, and the promises of the WLAN system. The goal of our Personal AP mobility management is to provide non-disrupted and the best network connectivities to the on-going user applications. 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 mobile STA 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 provide timely mobile STA-AP network connection information to the access controller, the APs in the Personal AP system collect the RSSI information from all overheard mobile STA data frames, and summarize a characteristic indicator of the mobile STA-APs connections. For simplicity, an exponential moving average of the RSSI values of the mobile STA-AP connections are maintained at the APs. A moving average smooths out sudden changes in the signal strength in irrational movements, and avoid unnecessary handoffs.

At each AP, a simplified RSSI moving average  $\overline{RSSI}^{MS}$  is computed from the RSSI values of mobile STA's data frames according to

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

The  $\alpha$  value is an empirical value, and our implementation chooses  $\alpha = 0.9$  for fast mobile STA tracking.

On the other hand, Personal AP allows mobile STA initiated handoff if the traffic characteristics exhibit intermittent long silent period even though the STA association and re-association process would normally involve 30ms-400ms delay. However, the exact traffic characteristics that can trigger mobile-assisted handoff are worthy of a separate study, and are not further specified in this paper.

### B. Handoff Operations

Once a handoff decision is made for an STA to connect with a new AP, Personal AP protocol transfers the context information from the old AP to the new AP.

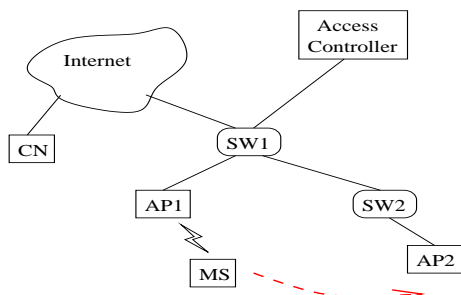


Fig. 4. A Simple Mobility Scenario in Personal AP system

We run through the handoff operations by looking at one STA's movement through an Personal AP system with one

access controller and two overlapping APs, as shown in Fig. 4. Other relevant components include Ethernet switches, wireline connections, Internet and the correspondent node (CN).

At the beginning, the mobile STA joins the WLAN networks using the standard 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. Then AP1 informs the access controller about the association, and the access controller in turn creates an STA-specific entry mapping the STA to AP1.

Suppose that the STA has an active application-layer connection with the correspondent node (CN), and communicates while moving from AP1 to AP2. Both AP1 and AP2 periodically report the STA RSSI values to the access controller. When the RSSI values at AP2 are better than that at AP1, a network-initiated handoff will be triggered by the access controller.

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. For traffic monitoring purposes, WATCH messages carry the RSSI reports from APs to the access controller. To tell new APs to act as the associated AP for a mobile STA, 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

Fig. 5. IAPP and Personal AP Packet Format

Fig. 5 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 old AP's BSSID, sequence number etc.

The process for handoff control and context transfer is illustrated in Fig. 6, which shows the control message exchanges and timing relationship between the messages.

The handoff operations start off by APs reporting the mobile STA channel quality and traffic characteristic information to the access controller using WATCH messages, when access controller makes handoff decision accordingly. After the handoff decision is made, the access controller sends a HO\_INFORM message to the new AP (AP2) to ask AP2 to accept the mobile STA. At the same time, the access controller sends a HO\_START message to the old AP (AP1) to request transfer the mobile STA context to AP2.

As AP1 confirms the handoff request using HO\_CONFIRM, AP1 also start to send the context information about the

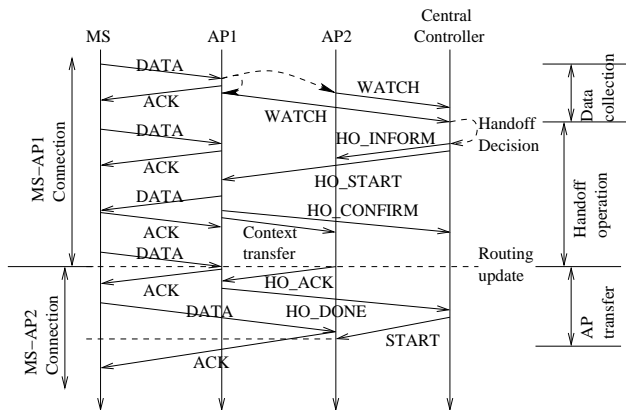


Fig. 6. Handoff Control Flow in Personal AP System

mobile STA-AP1 connection to AP2 using IAPP messages. The context information regarding a mobile STA-AP connection includes information elements such as:

1. Mobile STA MAC address.
2. Mobile STA association ID (AID).
3. AP1 MAC address (equivalent to the BSSID).
4. Mobile STA data frame sequence number.
5. AP1 data frame sequence number.
6. Buffered data frame for mobile STA.

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

After the context information is transferred, AP2 acknowledges the receipt of the transfer by sending `HO_ACK` to AP1, and also updates link layer routing table at the switches by broadcasting a route update message for the mobile STA. From this point on, further data packets from the CN will directly get to AP2, and future data frame from the mobile STA will be acknowledged by AP2.

Once AP1 gets the handoff complete message `HO_ACK`, AP1 sends out a `HO_DONE` message to the access controller, telling the completion of the handoff operations. In the Personal AP handoff process, the `HO_ACK` is the cutting line between the new and old mobile STA-AP connections.

Comparing with IAPP proactive caching approach, first, the Personal AP scheme does not need to maintain the neighbor graph for each AP. Secondly, in IAPP, 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, a mobile STA is unaware of the Personal AP mobility management operations, and there is no association or re-association process for the mobile STA. Therefore, Personal AP saves the handoff latency and is more efficient in handling mobility than IAPP.

### C. Security Context Transfer

If 802.11i [3] and 802.1x [4] are deployed in the 802.11 WLAN systems, AP advertises its security capabilities in its **beacon**, **probe** frames. The Robust Security Network (RSN) information elements of those frames include information regarding all enabled authentication suites, unicast cipher suites and multicast cipher suite. Mobile STAs select the authentication and unicast cipher suite in **association** request and AP acknowledge it by sending back **association** reply to complete security capability discovery. At the end of security capability discovery, the STA knows the SSID of the networks, the authentication and cipher suites of the network. The AP knows the authentication and cipher suites the STA chooses. In addition, the STA and AP have established an 802.11 channel and are ready to authenticate.

For either TKIP or AES-based encryption scheme, the pair-wise master key (PMK) is used to derive the other operational keys like pairwise transient key (PTK), group temporal key (GTK). Therefore, PMK is an essential security context information needed to be transferred from current AP to new AP whenever handoff is necessary. With 802.1x-based authentication process, the RADIUS server distributes the PMK to the access controller, and access controller adds it in the STA-specific cache entry and then pass to the right AP. Using PMK and 4-way handshakes, PTK is derived (not transported) and bound between STA and AP. The required information for both STA and AP to derive PTK includes PMK, ANonce (AP nonce), SNonce (STA nonce), AP's MAC address and STA's MAC address, STA's RSN Information Element (IE) and AP's RSN IE. All those information are bound to the pair of STA and AP and needs to be transferred from current AP to new AP in our personal AP scheme to enable seamless handoff.

That is, the following security information regarding a mobile STA-AP connection need to be transferred in the context information:

1. AP nonce (ANonce) of AP1.
2. STA nonce (SNonce) of the mobile STA.
3. RSN information element (IE) of AP1.
4. RSN information element (IE) of the mobile STA.
5. Pair-wise master key (PMK).

### D. Data Plane Operations

Because the handoff operations transfer the complete context information regarding the mobile STA-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 mobile STA like a "ghost" in the Personal AP system. Therefore, the handoff operations have no effects to the mobile station's perception of the WLAN system. The same mobile STA-AP information is carried in data frames.

Especially, the use of MAC and IP addresses is depicted in Fig. 7, where the superscripts 's' and 'd' indicate the source and destination of the data packet, and the the subscripts indicate the end-systems sending or receiving the

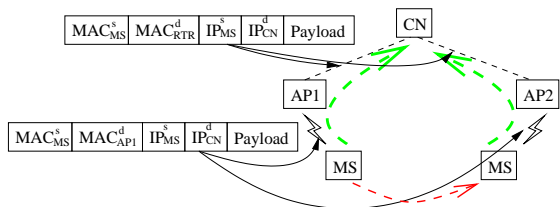


Fig. 7. Data Frame Contents Unchanged After Handoff in Personal AP system

packets. As we can see, nothing needs to change as of the data frame format.

### E. Routing Control

The routing control mechanisms in Personal AP systems consist of two part: layer-two and layer-three routing update when the mobile STA moves between APs.

The layer-two route update happens when the mobile STA 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-two broadcast route update is to send out by the new AP with the mobile STA's MAC address as the source address. This broadcast message updates the intermediate switches' learning table for layer-two routing purposes. Such route update procedure happens once the new AP receives the HO\_INFORM message, and does not interfere with the other parts of the handoff process.

The layer-three route update happens when the mobile STA 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 delegates the layer-three (IP layer) route update responsibility to the mobile STA, but still carries out the layer-two route update procedure at the new AP, therefore saving the association and re-association process in 802.11. In addition, the layer-three route update is triggered by the access controller in the Personal AP architecture so that the mobile STA 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-two mobile STA-AP context.

### F. 802.11 Network Management

Because Personal APs now appear to be ubiquitous, and the context information follow assigned mobile STAs, it may cause some disruptions to the regular network management functionalities, such as beacon transmissions, and power-save mode scheduling. However, mobile STAs only need to receive them at the initial stage when the mobile STAs join the Personal AP network. Once the mobile STAs 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 mobile STAs.

Nonetheless, 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 the responsibility of access points, but involve the decision by the mobile STAs. If a mobile STA roaming decision is based on the beacon receptions, Personal AP system still transfers the mobile STA-AP context information between APs, but the context will be discarded when the new mobile STA-AP association is established.

For those mobile STAs in power-save mode, Personal AP system does not provide additional mechanisms to handle their data frames because their traffic is not delay-sensitive in most cases. Instead, the mobile STAs are free to associate with new APs for communications.

## V. PERFORMANCE EVALUATIONS OF PERSONAL AP

We compare our Personal AP mobility management approach in the centralized architecture with the regular 802.11 handoff mechanisms. A simulation study is conducted using simulator NCTUns 2.0 [18] to exhibit performance with regard to handoff latency and traffic delays on TCP and UDP flows. NCTUns 2.0 is both a network simulator and an network emulator, and is by far the best network simulator we could find for our purposes.

In our simulations, the parameters for network configuration follow the specifications in IEEE 802.11 standard and are shown in Table I.

TABLE I  
SIMULATION PARAMETERS

Parameters	Values
MinChannelTime	3ms
MaxChannelTime	30ms
CWmin	31
CWmax	1023
SIFS	10 $\mu$ s
Slot-time	20 $\mu$ s
DIFS	50 $\mu$ s
Basic Rate for management frames	1Mbps

The simulations run over a network topology containing two APs, one mobile STA, one access controller and one correspondent node (CN) as shown in Fig. 4. Respectively, a CBR traffic using UDP and an FTP traffic using TCP connection is setup from the mobile STA 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 mobile STA moves from one AP to another and triggers handoff in both Personal AP and normal IEEE 802.11 mobility handling schemes. The handoff latency is collected as the performance metric to compare our Personal AP with the standard 802.11 handoff.

Under the standard IEEE 802.11 handoff, the STA performs a full channel scanning through all the 11 channels. The latency is measured from the time instant that the mobile STA sends out probe request to the time that the STA receives re-association reply. For simplicity, the

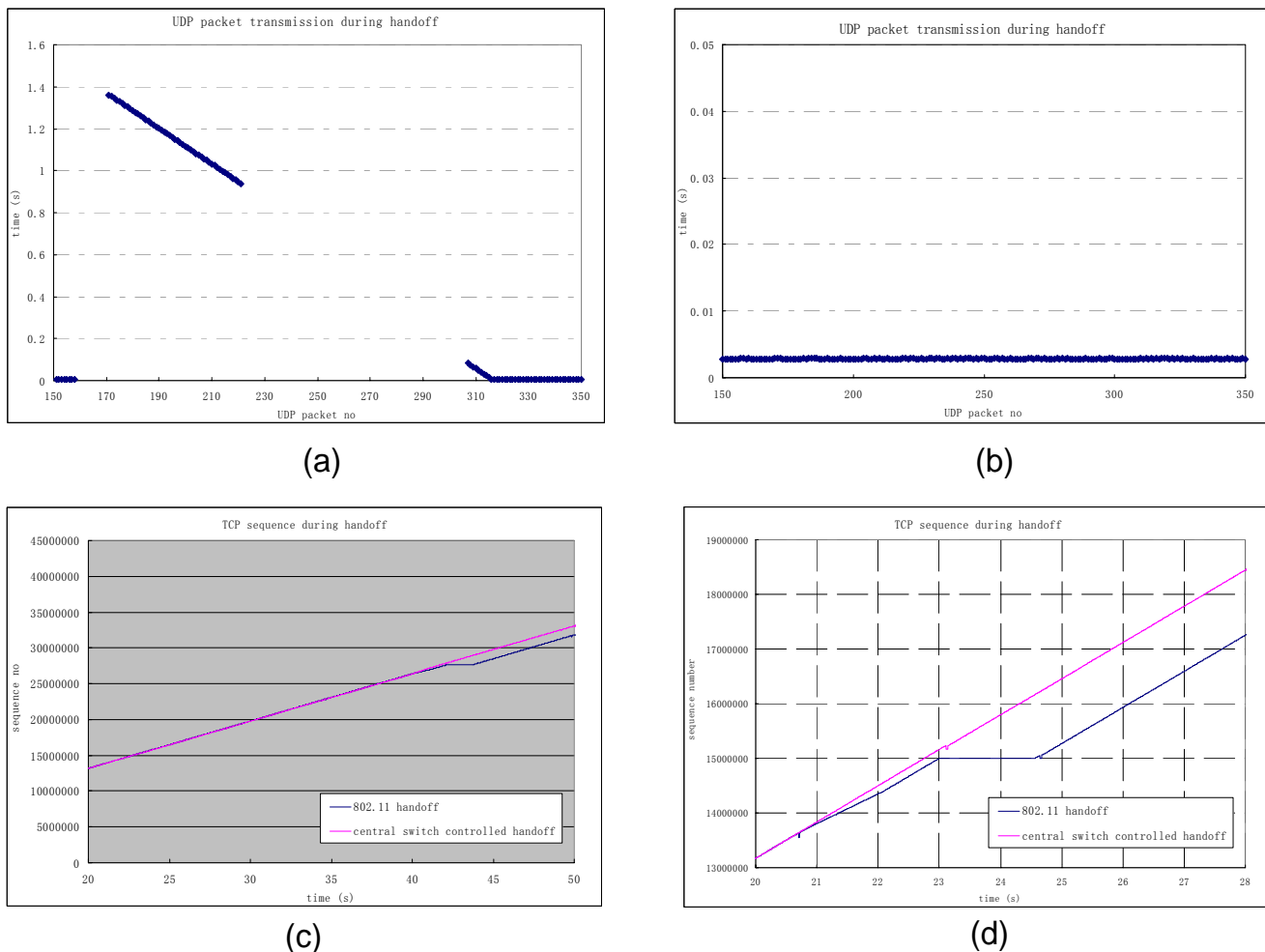


Fig. 8. The Handoff Latencies in UDP/TCP Flows: (a) UDP Delay in 802.11 System (b) UDP Delay in Personal AP System (c) TCP Delays in 802.11 and Personal AP Systems (d) Magnified TCP Delay in 802.11 and Personal AP Systems

re-authentication process is not counted since 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 mobile STA.

Fig. 8 shows the UDP and TCP performance in both regular 802.11 system, and our centralized Personal AP system. In plots (a) and (b), the horizontal axis is the packet sequence number, the vertical axis is the UDP end-to-end delay in seconds. In the regular 802.11 handoff situation, we can see a significant increase of end-to-end latency before handoff completes as well as packet loss due to buffer overflow and packet drops. In our simulation, a total of 109 UDP packets are lost during the handoff in the regular 802.11 system. Comparatively, the centrally controlled Personal AP system completes handoff within milliseconds, which are trivial compared to 10 ms packet interval and 2.7 ms average transmission delay.

Plots (c) and (d) in Fig. 8 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 handoff starts at different 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 mobile STA does not initiate the handoff process until the RSSI is below a certain low threshold, even if there are APs that have better RSSI with that mobile STA. In the Personal AP system, the handoff begins when the central switch receives a better RSSI report from a new AP about the mobile STA 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. The proactive involve-

ment of Personal AP protocol in the mobility management of mobile stations is desirable in providing the best wireless connections to the mobile STA in the world of multimedia in the next generation wireless networks [9].

## VI. CONCLUSION

We have proposed a centralized WLAN architecture for fast and efficient mobility management. A novel handoff approach that is based on Personal AP concept is presented under the centralized architecture. The goal is to reduce traffic disruptions in the regular 802.11 mobility management schemes. It is achieved by the access controller monitoring mobile STA traffic activities and roaming behaviors, and transferring the mobile STA-AP context to the best connected AP around the vicinity of the mobile STA, therefore, creating a “ghost” AP that follows the mobile STA in the Personal AP system. Simulation results show that Personal AP system introduces very little handoff latencies, comparing with the traditional IEEE 802.11 systems. This characteristic makes it attractive for supporting VoIP and streaming 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] IEEE Std 802.11i/D3.0. Specification for Enhanced Security. Technical report, IEEE, Nov. 2002.
- [4] IEEE Std 802.1x. Port Based Network Access Control. Technical report, IEEE, Jun. 2001.
- [5] 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.
- [6] 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.
- [7] I.F. Akyildiz, J. McNair, J.S.M Ho, H. Uzunaloglu, and W. Wang. Mobility management in next-generation wireless systems. In *Proceedings of the IEEE, Vol. 87*, pages 1347–1384, Aug. 1999.
- [8] 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.
- [9] *Proceedings Of Wireless, Mobile And Always Best Connected, 1st International ANWIRE Workshop*, Glasgow, UK, Apr. 22 2003.
- [10] 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.
- [11] 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.
- [12] Aruba Networks Inc. <http://www.arubanetworks.com>, 2004.
- [13] Meru Networks Inc. <http://www.merunetworks.com>, 2004.
- [14] 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.
- [15] 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.
- [16] C. Perkins. RFC2002 - IP Mobility Support. Technical report, Internet Engineering Task Force (IETF), IBM, Oct. 1996.
- [17] 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.
- [18] 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.
- [19] 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.
- [20] S. Xu, S. Papavassiliou, and S. Narayanan. Layer-2 multi-hop IEEE 802.11 architecture: design and performance analysis. In *IEEE Proceedings of Communications, Vol. 151*, pages 460–466, Oct. 2004.
- [21] 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.