Mobile Context Handoff in Distributed IEEE 802.11 Systems

Jidong Wang and Lichun Bao

Abstract—**The mobility management is one of the most critical issues in mobile wireless systems. The quest to support delay-stringent multimedia applications challenges most existing solutions to the mobility management problem. We propose a mobility management scheme, called *Mobile AP*, to support station mobility efficiently. In Mobile AP mobility support system, the context of each mobile station is defined by the association states between the mobile station and the wireless communication infrastructure. When the mobile station roams in Mobile AP systems, the context of the association follows the mobile station from one physical access point to another, thus eliminating the need for the mobile station to re-associate with new access points. We implement Mobile AP system in IEEE 802.11 systems, and the essential idea is applicable in other wireless systems.**

I. 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] [8] [9] [15] [14].

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. Recently, a lot of research interests have been devoted to provide multi-hop WLAN architecture with robust mobility support [3] [17] [18].

According to the on-going standardization efforts in the IETF to classify different functional entities [19], wireless terminal point (WTP) and access point (AP) are two concepts in the WLAN architectural taxonomy. WTP is the physical entity terminating wireless connections, whereas AP is the logical entity encapsulating data, control and management planes in the networking architecture. Specifically, the data plane consists of the physical and the data link layer protocols.

By arranging The architecture of the AP functionalities in various places, 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. Especially, IEEE 802.11f provides pre-caching optimizations during the association procedures [2].

The centralized architecture has the many varieties in real-world implementations. In addition to WTP and AP, it defines another concept – “access controller” (AC) that works as the central intelligence for the system-wide operations. The central architecture can have one of three functional separations, a) *Local MAC*, where the majority of AP functionalities is implemented on the WTP, such as the Mobile AP system proposed in [20], b) *Split MAC*, where only delay-sensitive functions are implemented on WTP, such as Meru Networks Systems [11], and c) *Remote MAC*, where the entire AP functions are implemented at the AC (access controller), such as the Aruba Networks Systems [10].

The distributed architecture delegates all the decisions on mobility management to the access points, such as ad hoc networks and mesh networks.

No matter which architecture to choose in an IEEE 802.11 system, existing approaches have tried to shorten the handoff latencies incurred by probing, authentication and association activities during the layer-2 handoff process. We propose completely different approach in the same architectural considerations by eliminating the layer-2 handoff process from the air-interface transactions. Instead of establishing a new wireless association with a new WTP (wireless terminal point), we transfer the old association states between the mobile station and the old WTP to the new WTP, therefore allowing a new WTP to pretend as the old WTP for the mobile station. In addition, such concealment of mobile context transfer from the mobile stations saves the precious wireless channel bandwidth, therefore improving network throughput considerably. We call such a mobility management protocol as *Mobile AP*. Our Mobile AP protocol works in the aforementioned autonomous AP architecture, where the AP functionalities are completely implemented on each of the WTPs, and inter-AP coordinations are carried out over a switch network, which we specify in the paper.

In this paper, we define the context of the mobile station as the states maintained at the APs, which includes association states, timestamp, sequence number, BSSID, capability, security information [2] [13]. However, Mobile AP is supplementary to existing handoff solutions in that it can 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 IEEE 802.11f. In fact, Mobile AP has a lot of information shared with IEEE 802.11f.

A critical requirement of IEEE 802.11 that any STA may have only a single association with the WLAN system at any given time. Mobile AP strictly enforces such requirement.

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

The paper is organized as follows. Section II analyzes the handoff procedure in large-scale IEEE 802.11 system deployments. Section III introduces our assumptions for implementing Mobile AP in WLAN systems. Section IV describes the Mobile AP protocol for seamless mobility management in IEEE 802.11 systems. Section V evaluates the performance of Mobile AP system in comparisons with the regular IEEE 802.11 mobility management. Section VI concludes the paper.

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 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. 1 illustrates the basic WLAN architecture defined in the IEEE 802.11 standard [1].

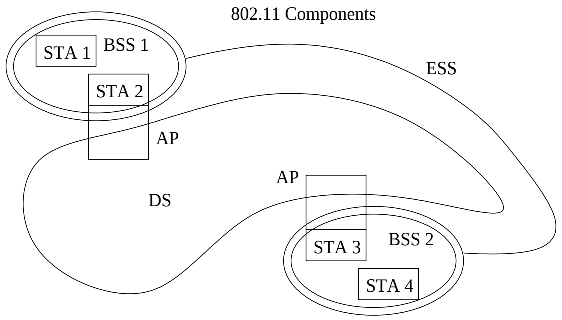


Fig. 1. WLAN architecture defined in IEEE 802.11

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. 2. Accordingly, the handoff latency is broken down into three parts: the probe delay, the authentication delay and the re-association delay.

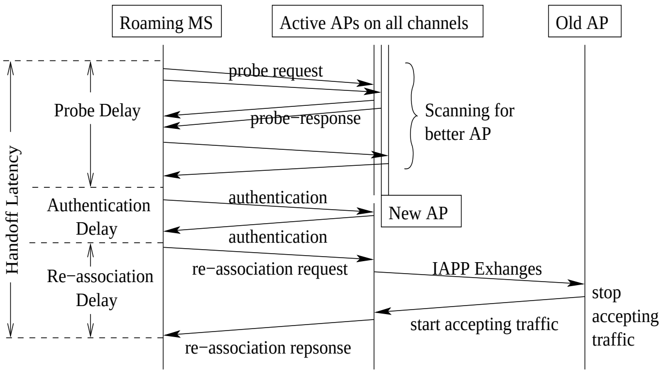


Fig. 2. Illustration of Handoff Delay

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 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 [12].

The authentication delay is introduced during the exchange of authentication information between an MS 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 MS. 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, which are the focuses of different mobility management schemes.

III. MOBILE AP ASSUMPTIONS

In Mobile AP systems, we assume that there is APs connected with each other through a high-speed switched network, so that efficient broadcast or multicast communications is available in the layer two (Data Link Layer in ISO/OSI networking architecture) for Mobile AP coordination purposes. In addition, we assume that APs are densely deployed so that we have continuous wireless coverage over the areas visited by the mobile stations. This is a reasonable assumption in either enterprise or campus deployment where continuous coverage and connectivity is highly desirable and affordable due to the dropping cost of APs. Under the dense AP deployment assumption, multiple APs with similar capabilities and different BSSIDs operate in the same frequency channel in the adjacent area.

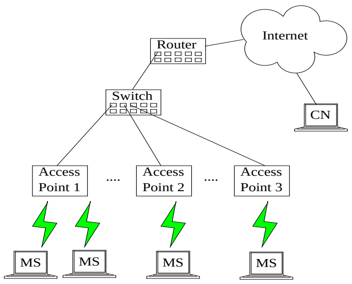


Fig. 3. Mobile AP Deployment Scenario

Fig. 3 illustrates the WLAN infrastructure required for Mobile AP implementations. As we can see, Mobile AP architecture requires nothing more than what is needed in IEEE 802.11 WLAN systems with the autonomous APs. Although it is not strictly required for the best performance of Mobile AP systems, we assume that a dedicated switch is installed for prompt and efficient communications between Mobile APs. Much bigger WLAN system can be built over layer-2 switching networks by connecting the layer-2 switches. In order to efficiently coordinate the MSs associated under each switch, some additional control logics are necessary. However, we focus on a WLAN system connected by a single switch in this paper because a WLAN system with a proper switch can already support dozens of APs under very low cost.

IV. MOBILE AP PROTOCOL

A. *Handoff Decisions*

Handoff decisions in a WLAN system is dependent on many factors, such as the requirements of end-user applications as well as the optimality of the WLAN system performance including network throughput, quality of MS-AP links. In this paper, the goal of the Mobile AP protocol for 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 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 when the traffic characteristics exhibit intermittent long silent period, and require the Mobile AP protocol to help fast handoff in the latter two applications where the traffic is constantly heavy.

In order to timely collect MS-AP network connection quality information in the distributed and autonomous AP architecture, each AP reports the RSSI information from all overheard MS data frames, and summarize indicators of the MS-AP connections. For simplicity, an exponential moving average of the RSSI values of the MS-AP connections are maintained at each AP. A moving average smooths out sudden changes in the signal strength due to abnormal movements, and avoid unnecessary handoffs.

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

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

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

After collecting the MS-AP connection quality information, each AP selectively broadcasts its local MS-AP connection and link quality information. Specifically, an AP periodically sends the summarized RSSI values of the MS-AP links with the associated MSs. An AP may also proactively report dramatic MS-AP link quality changes for faster handoff decisions.

On the other hand, an AP also broadcasts link quality information of the MSs that are not associated with the AP, but have better link quality than the current associated AP. If APs other than the currently associated AP can hear the MS, but cannot provide better link quality, they do not report any link quality information to the network.

Because the link quality information is exchanged periodically and proactively, an AP can evaluate the benefits of potential handoff decisions. Usually, a handoff decision is made by an AP if another AP reports the best link quality among all the APs. For example, suppose AP_1 is currently associated with an MS, then AP_1 decides to initiate a handoff operation if AP_2 has the highest RSSI value regarding the MS, and that

$$\beta \cdot \overline{RSSI}^{MS}_{AP_1} < \overline{RSSI}^{MS}_{AP_2},\ \beta > 1.$$

B. *Handoff Operations*

Once an old AP decides to handoff an associated STA to a new AP, the old AP transfers the MS-AP context information to the new AP using Mobile AP protocol.

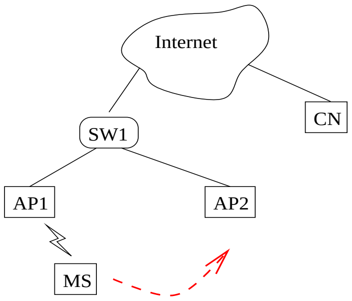


Fig. 4. A Simple Mobility Scenario in Mobile AP system

We run through the handoff operations by looking at one STA's movement through an Mobile AP system with 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 MS joins the WLAN networks using the normal association process by performing the probing, authentication and association processes. In Fig. 4, the STA is associated with AP1.

Now, suppose that the STA has an active application-layer connection with the correspondent node (CN), and communicates while moving from AP1 to AP2. While the STA roams, both AP1 and AP2 periodically report the STA RSSI values by broadcasting in the layer-2 network. When the RSSI values at AP2 are better than that at AP1, AP1 will trigger a handoff decision as specified in the last section.

Because Mobile AP system has similar context transfer operations as IAPP, we follow a similar data frame formats in Mobile AP as in IAPP, and try to provide non-conflicting names for control messages. For instances, in order to exchange MS-AP link quality information, the `WATCH` message is defined to carry the RSSI reports from APs. Messages related with handoff transfer operations are prefixed with `HO_`. Overall, only three handoff messages are used in Mobile AP protocol: `HO_START`, `HO_ACK`, `HO_DONE`.

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

Fig. 5. IAPP and Mobile 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_START`, 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 the `Context transfer` message, the data field contains old AP's BSSID, sequence number etc.

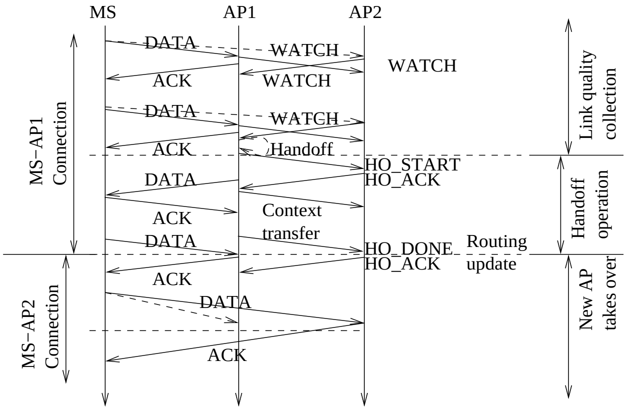


Fig. 6. Handoff Control Flow in Mobile AP System

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 broadcasting the MS channel quality information using `WATCH` messages. When AP2 reports better link quality with the MS, AP1 makes the handoff decisions, and initiates the handoff operation by sending `HO_START` message to AP2 to accept the MS. After AP2 confirms the reception of the handoff message using `HO_ACK`, AP1 starts to send the context information about the MS-AP1 association to AP2 using IAPP context transfer messages. The context information regarding an MS-AP connection includes information elements such as:

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

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 MS may also keep sending 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. Subsequently, AP2 also updates link layer routing table at the switch by broadcasting a route update message for the MS. 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.

In IEEE 802.11f, IAPP includes a performance enhancing mechanism using proactive caching approach [2]. Proactive caching pre-authenticates MSs at potential new APs in the neighbor graph for the MSs, therefore saving some of the steps for new associations. Mobile AP is different from IAPP in that, first, the Mobile 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 Mobile AP only forwards one copy of context block to the designated new AP. Third, an MS is unaware of the Mobile AP mobility management operations, and there is no association or re-association process for the mobile STA. Therefore, Mobile AP efficiently reduces the handoff latency and is more effective in handling mobility than IAPP.

C. 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 Mobile AP system. Therefore, the handoff operations have no effects to the mobile station's perception of the WLAN system. The same MS-AP information is carried in data frames.

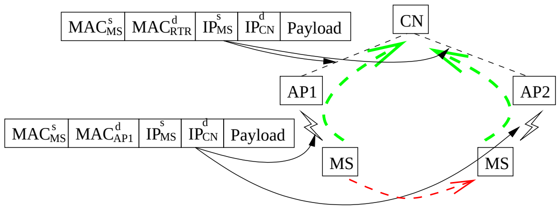


Fig. 7. Data Frame Contents Unchanged After Handoff in Mobile AP system

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

D. Routing Control

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

The layer-two 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-two broadcast route update is to send out 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-two 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-three route update happens when the MS moves between APs that are located in different subnets. In this case, the MS is responsible for the layer-three (IP layer) route updates. However, Mobile AP is still applicable in such scenario by eliminating the MS-AP association process. The handoff coordination across different subnets is outside our scope.

E. Beacon Management

Because Mobile 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 Mobile AP network. Once the MSs start intensive communication, network connectivity and capability are provided at the best efforts by the Mobile APs. Therefore, there is no need to periodically receive beacons for these MSs.

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 be outside the control of the APs, and involve the decisions by the MSs. If an MS roaming decision is based on the beacon receptions, Mobile 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, Mobile AP system does not provide additional mechanisms to handle their data frames because their traffic is not delay-sensitive in most cases. Instead, the MSs are free to associate with new APs for communications.

V. PERFORMANCE EVALUATIONS OF MOBILE AP

We compare our Mobile AP with the regular 802.11 handoff mechanisms. A simulation study is conducted using NCTUns 2.0 [16] to demonstrate the performance differences 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 by far the best network simulator we could find for our purposes.

In our simulations, the parameters for network configuration adopt the specifications in IEEE 802.11 standard:

- `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 containing two APs, one MS, one switch and one correspondent node (CN) as shown in Fig. 4. Respectively, a CBR traffic using UDP and an FTP traffic using TCP connection are setup from the MS to the CN for the duration of the simulations. The CBR traffic consists of 1024-byte UDP packets at a constant rate of 100 packets/second.

During the simulation, the MS moves from one AP to another and triggers handoff in both Mobile AP and normal IEEE 802.11 mobility handling schemes. The handoff latency is collected as the performance metric to compare our Mobile 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 MS sends out `probe` request to the time that the STA receives `re-association` reply. For simplicity, the re-authentication process is not counted since it does not contribute much to the total latency.

Under the Mobile 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.

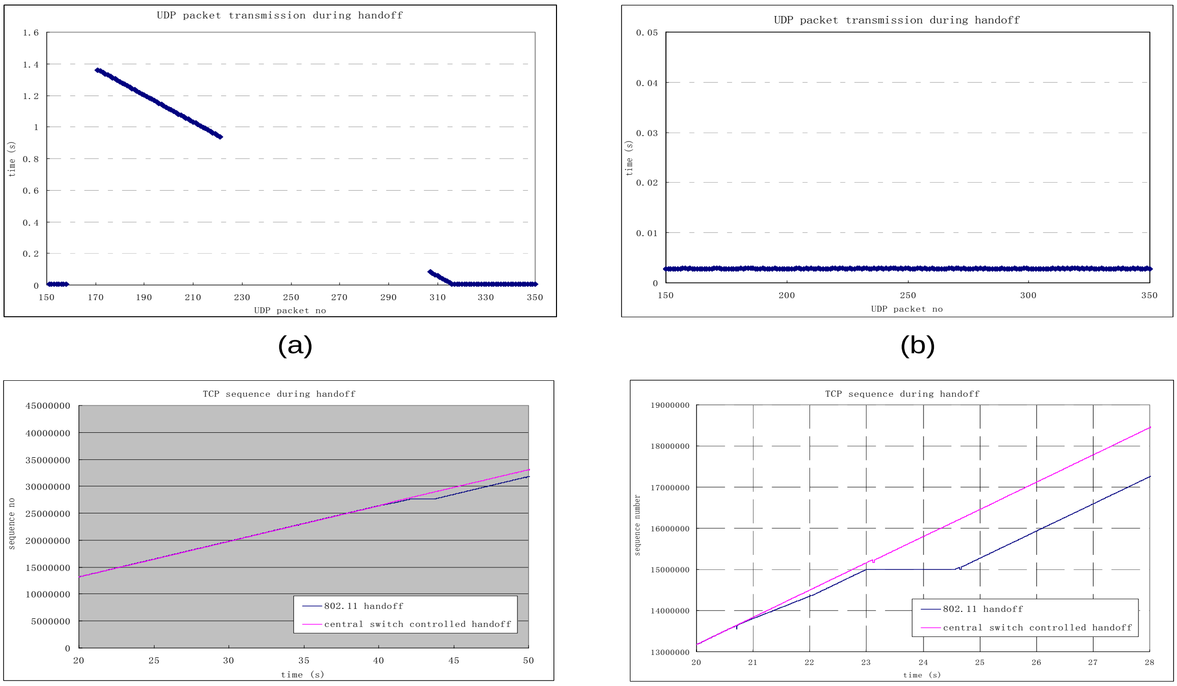
Fig. 8 shows the UDP and TCP performance in both regular 802.11 system, and our centralized Mobile AP system. In plots (a) and (b), the horizontal axis is the packet sequence number, the vertical axis is the UDP end-to-end delay in seconds. In the regular 802.11 handoff situation, we can see a significant 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 Mobile 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 in regular 802.11 and Mobile 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 Mobile 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 time instants in Mobile 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 Mobile 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 Mobile AP system started handoff at time 23.0003 second. Such phenomenon is proved desirable in providing the best wireless connections to the MS in the world of multimedia in the next generation wireless networks [7].

VI. CONCLUSION

We have proposed a distributed WLAN architecture with autonomous Mobile APs for fast and efficient mobility management. A novel mobility management approach based on the Mobile AP concept is presented under the architecture. Mobile AP reduce traffic disruptions experienced in the regular 802.11 mobility management schemes by exchanging mobile station – AP



(a) (b)

(c) (d)

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

link quality information between APs, therefore allowing APs to determine the next best AP for the roaming MS. Mobile AP achieves seamless roaming by transferring the MS-AP context to the best connected AP around the vicinity of the MS, therefore eliminating the needs for mobile stations to re-associate with other APs. Simulation results show that Mobile AP system introduces negligible handoff latencies.

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] *Proceedings Of Wireless, Mobile And Always Best Connected, 1st International ANWIRE Workshop*, Glasgow, UK, Apr. 22 2003.

[8] 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.

[9] 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.

[10] Aruba Networks Inc. http://www.arubanetworks.com, 2004.

[11] Meru Networks Inc. http://www.merunetworks.com, 2004.

[12] 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.

[13] 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.

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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] L. Zan, J. Wang, and L. Bao. Personal AP Protocol for Mobility Management in IEEE 802.11 Systems. In *The 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MOBIQUITOUS)*, San Diego, CA, Jul. 17-21 2005.