Reducing Layer 2 Handoff Latency in WLANs using Advanced Context Distribution

Laeth A. Al-Rawi, Rosli Salleh, Ghaith A. Al-Rawi, Hassan A. Al-Rawi, H.Keshavarz

Abstract— WLANs have experienced very fast deployment in both public and private areas over recent years. They provide nontrivial replacement for the complicated and high cost wired LANs. However, the Access Points that WLANs are build from do not have very wide coverage range (usually under 100m indoors). Consequently, many handoffs occur as the mobile host moves while accessing the network resources located at the distribution system. Unfortunately, these handoffs can disturb real time applications if they take too long (more than 50ms). In order to resolve this problem, this paper introduces a new mechanism for reducing handoff delay called Advanced Context Distribution (ACD). ACD is able to reduce re-association phase delay by eliminating Inter Access Point Protocol (IAPP) excess time consumed for transferring station context information from the old access point to the new associated access point (up to 40ms delay).

Index Terms— IEEE 802.11, WLANs, IAPP, Hand-off Latency.

1 Introduction

Recently, WLANs have become very popular as they provide user mobility, high data rates (up to 54Mbps) and low cost [3]. By deploying them, users can access LAN resources without the annoying wires by using an entity called Access Point (AP) that can bridge user traffic from and to the distribution system (LAN). However, this AP does not have a very long coverage range (usually under 100m indoors) which may restrict user mobility. Consequently, many APs are needed to expand WLAN boundaries and so the user can reach longer distances and still have accessibility to the LAN (something not possible by using only one AP). Although this is a good improvement, the user still has to change association from the old AP to a new AP while moving, and the received signal from the old associated AP gets weaker (handoff). This association changing process is called a handoff, during which no data is sent or received by the user. This process can affect real time applications like voice and video over Internet Protocol (VOIP) because these applications need real-time traffic speed possibly affected by long delays (over 50ms) [6].

The rest of this paper is organized as follows. First, the basics of IEEE 802.11 handoff procedure are reviewed. Next, the IAPP is briefly explained. The last sections review one of the mechanisms for reducing re-association delay. Finally, we will conclude by explaining in detail our new mechanism (ACD) and simulation results.

2 IEEE 802.11 Handoff Procedure

The total handoff process can be divided into two logical phases, namely, Discovery phase and Re-authentication phase, in which management frames are exchanged between the Mobile station (MS) and the Access Point (AP) to move MS association from the old to the new AP [7]. This process also involves some cooperation between the APs in order to transfer MS context information from the old to the new AP (e.g. using IAPP) (Figure 1).

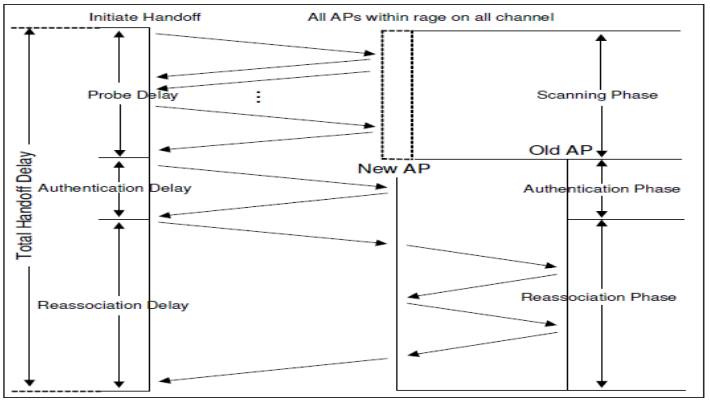

Fig. 1. IEEE 802.11 handoff procedure with IAPP [5]

2.1 The Discovery Phase

Whenever the Received Signal strength (RSS) from the associated Access Point (AP) gets weaker, the Mobile Station (MS) starts the discovery phase by switching to each channel defined by the standard used (11 channels in IEEE802.11b/g and 32 channels in IEEE802.11a) and scans for any available APs [2]. The MS does this because it does not have any information about the surrounding APs so it must discover them itself. There are two kinds of scanning defined by the IEEE802.11 standard, active and passive scanning. In active scanning, the MS scans each channel by sending probe request frames and waits for responses from all available APs on that channel. This scanning type can take a long time, up to 400ms, as the MS must wait for the MinChannelTime (minimum channel timer is used by the MS to specify the minimum time needed for receiving responses from APs) on each channel while it is being scanned [4]. On the other hand, by using passive scanning, the MS only switches on each channel and waits for beacons sent by the APs located on that channel. Although this type looks easier done by MS as it does not consume a lot of power or bandwidth, it takes longer than active scanning because MS has to wait for at least a one-beacon interval on each channel (normally 100ms) introducing

• *Corresponding author: Hassan Keshavarz is currently pursuing masters degree program in computer science in University of Mlaya, Malaysia, PH-0060172950923. E-mail: keshavarz_hassan@hotmail.com*

big delays (~1s) which are not acceptable in real time applications.

2.2 The Re-authentication phase

When the Mobile Station (MS) finishes scanning all available channels and discovers the surrounding Access Points (APs), it tries to (re)associate to the AP with the best Received Signal Strength Identifier (RSSI). However, this association or re-association process is not accepted by the new found AP without the MS being (re)authenticated (authentication phase consists of two processes: re-authentication and re-association) [7]. Consequently, the MS starts by sending an authentication request frame to that AP and waits for a response which indicates AP acceptance or rejection. After the MS is successfully (re)authenticated by the AP, it (re)associates to this AP by sending an (re)association request frame and waits for a response. Whenever the AP receives the (re)association frame, it sends its response depending on some required features like supported rates by the MS. Finally, the MS associates with the new AP and all traffic destined to the MS will be sent through that AP.

The re-association process involves cooperation between the old and new APs in order to transfer MS-related context information to the new AP. This cooperation can be done using Inter Access Point Protocol (IAPP). The IAPP can transfer MS credentials between APs from different vendors (context transferring process will be explained in the next section). This context transfer introduces extra delay to the total handoff latency because of the extra IAPP packets exchanged between the APs for the transfer of context information [1].

3 The Inter Access Point Protocol (IAPP)

In order to achieve secure context information transfer related to a Mobile Station between Access Points from different vendors, the Inter Access Point Protocol (IAPP) was developed [4]. The IAPP can also enforce a single MS association point to the wireless network by informing all APs on the multicast domain that the MS is now associated with an exact AP. This enforcing process is done with an IAPP ADD_Notify packet used whenever the MS associates to an AP, to tell all APs to remove any specific MS context information from their caches. On the other hand, an IAPP Move_Notify packet can transfer MS context information from its old associated AP directly to the caller/newly associated AP. The IAPP Move_Notify packet is sent by the new AP (when the MS re-associates to a new AP) directly to the old AP (which the MS was associated with) in order to tell the old AP to move the station context information from its cache and cut any connection with the MS. The context information is then transferred to the new AP using an IAPP Move_Response packet (IEEE802.11f). Although these IAPP packets can ensure MS credential transfer, they are not safe from attacks while traversing the LAN. Therefore, Remote Authentication Dial in USER Service (RADIUS) server is recommended to provide context information confidentiality. The RADIUS server can also perform address mapping from MAC address to IP address necessary for the APs to contact each other (at the network layer) [8]. Another issue with using IAPP is that extra delay (up to 40ms) is imposed, possibly affecting the total handoff process [4]. Thus, the next section introduces a new mechanism which eliminates this extra delay (caused by IAPP packet exchange) by shifting AP interaction to the scanning phase, something done even before the re-authentication phase.

4 Reducing Re-association Delay

A new scheme called Proactive Neighbour Caching (PNC) is proposed [8]. It uses a neighbour graph (NG) which dynamically identifies the mobility topology of a wireless network (network topology). The main idea of this scheme is to separate the context transfer process (using IAPP) from the re-association process. That means the mobile station's (STA) context information can be proactively transferred to the next potential AP before the actual handoff process takes place. Based on the network topology, the PNC scheme will choose a candidate set of next potential APs so the context information will be transmitted to a limited set of next potential APs (only AP neighbours). The PNC scheme ensures that STA's context information always remains one step ahead; therefore handoff delay is reduced because the new AP that the STA may re-associate with already has the STA's context information. Experiments show that the PNC scheme can reduce re-association delay from 40ms as reported by [4] to 1.69ms. However, since STA's context is propagated to all neighbouring APs and as long as the STA only re-associates to one neighbour AP, resources will be wasted in the APs (memory).

5 Proposed Mechanism

In this section, the Advanced Context Distribution (ACD) mechanism is presented. It aims to reduce re-association delay caused by Mobile Station (STA) context information transfer from the old AP to the new AP using the Inter Access Point Protocol (IAPP). STA context information is the STA's security information that may allow faster STA re-authentication on re-association (IEEE 802.11f, 2003). Using IAPP to transfer STA context can increase re-association delay (up to 40ms) due to its four additional messages during re-association [4, 7].

The ACD mechanism reduces re-association delay by reactively transferring the STA's context information from the old AP to only the new APs that request context transfer during the scanning phase (Figure 2). The new APs are those with a high probability that an STA may re-associate with. During the scanning phase, STA broadcasts probe request frames on each channel to find a new AP for re-association. After receiving the probe request frame from the STA, each new AP calculates the Received Signal Strength (RSS) value and can request for the transfer of STA context from the old AP only if it can satisfy the specific Context Threshold condition (i.e. only new APs with bigger RSS value than the Context Threshold value can request transfer).

The Context Threshold (CT) is a predefined and dynamically updated value (threshold) introduced in the ACD mechanism. It guarantees that only new APs with the best RSS value can request STA context transfer (not all old AP neighbours). It will be checked and updated dynamically by the STA each time it receives a new probe response frame from any new AP. The whole process is as follows:

Whenever the STA starts the scanning phase, it switches to the first channel and sends a probe request frame. As long as this is the first channel to be scanned by the STA, the probe request sent will hold the original handoff threshold by setting the CT equal to the handoff threshold (e.g. CT=HT=3dB). The probe request will also hold the Internet Protocol (IP) address of the old associated AP. The STA gets the old AP's IP address whenever it associates to that AP (the AP will send its IP address to the STA in an (re)association response frame). The old AP's IP address will be added to the probe request frame body to enable communication between the new discovered APs and old AP. Upon receiving any probe response frame on that channel, the STA calculates that response frame's RSS and compares it with the saved CT value (Figure 2). If the calculated RSS is bigger than the CT value, the STA will update the CT value by setting it equal to the new RSS (set CT= probe response calculated RSS). However, if the RSS is less than the CT value (RSS<CT), the STA will not modify the CT. Next, the STA attaches the modified CT value with each new probe request frame which it will send on the next channel and check the response. This process will be continuously repeated by the STA until the scanning phase is finished (all channel are scanned). Therefore, the existing probe request frame is modified to hold the old AP's CT value and IP address. The existing association and re-association response frames are also altered in order to add the AP's IP address field.

Whenever an Access Point (AP) receives the probe request frame from the STA, it does two main things. First, it sends a probe response back to the station. Second, it saves the old AP's IP address extracted from the probe request frame, calculates the received probe request frame's RSS value and compares it with the CT value received from the STA (in a probe request frame) to check if it satisfies the Context Threshold condition. If the RSS is less than the CT (RSS < CT), the new AP cannot request the STA context information. On the other hand, if the calculated RSS value is bigger than the CT value (RSS > CT), the new AP satisfies the transmission condition. Consequently, it can request for STA context information transfer from the old associated AP by sending an IAPP MOVE-notify packet to the old AP (using the IP address received from the STA) and waits for the response. When the Old AP receives the IAPP MOVE-notify packet, it will, unlike the conventional IAPP functionality, send back an IAPP MOVE-response packet in which the context information of the STA is held without deleting the context information from its cache until it receives an ADD_Notify packet (new modifications on the IAPP functionality is done). When the new AP receives the MOVE-response packet, it caches the STA's context information into its memory normally.

When the STA finishes the scanning phase, it sends an authentication request frame to the best AP (with the biggest RSS) and waits for the response. Upon receiving a successful status authentication response frame, the STA tries to associate with the AP by sending a re-association request frame to the new, selected AP. When it receives the re-association request frame, the new AP will send back a re-association response with its IP address. The AP also sends an IAPP ADD-notify packet to all APs within the multicast domain (using IAPP multicast address 224.0.1.178) in order for them to remove any context information, for this new associated STA, that might be sent from the old AP during the scanning process (upon AP's request). Since the STA context information has already been transferred and cached into the selected new AP's memory, the STA can re-establish its service faster than from scratch. Thus, the proposed handoff mechanism can reduce re-association delay in order to reduce overall handoff latency by transferring STA context information reactively to the selected

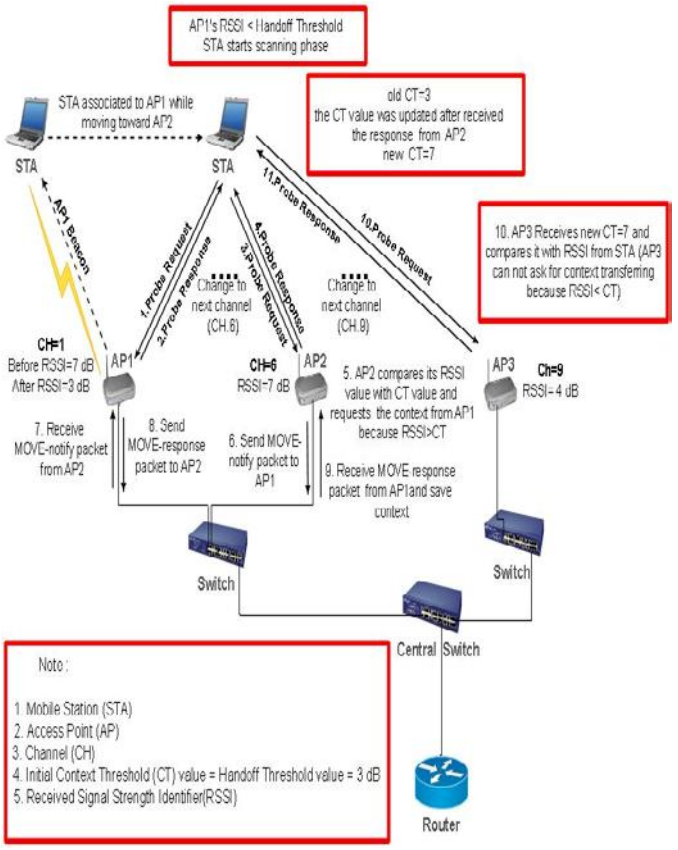

Fig. 2 Advanced Context Distribution (ACD)

By using a dynamic transferring threshold (CT), we can ensure that the context information of a specific Station (STA) is transferred only to the Access Points (AP) with the highest probability to be associated with the STA and not to all

neighbouring APs that might be discovered during the scanning phase. This prevents any extra load on APs (processing IAPP packets) and LAN by reducing the number of exchanged messages (IAPP packets) between the APs, and it also prevents resources wastage (AP memory used to save STA context information).

6 SIMULATION RESULTS

This section presents the results collected by implementing our proposed mechanism (ACD) using the OMNeT++ simulation. The results show that by using ACD, we can eliminate extra delay during the re-association phase imposed by the extra messages exchanged between the Access Points in order to transfer a station's context information. This elimination results from transferring context information before the re-association phase (during scanning phase).

6.1 Re-association delay

In our implementation, many trials were conducted and the results show that by using ACD the re-association delay is an average of 1.6ms (Figure 3). This reduction in re-association phase delay is a result of the advanced context transfer from the old associated AP to the new AP during the scanning phase. Consequently, by the time the Mobile Station (MS) identifies the best AP to re-associate itself with, that MS's context information will be saved in that AP's memory. The re-association delays of both the conventional IAPP context transferring mechanism and our new mechanism (ACD) were compared to show the new mechanism's contribution. With ACD we could reduce the re-association delay from an average of 27ms (using conventional IAPP) to an average of 1.6ms, which is an improvement of ~94% (Figure 4).

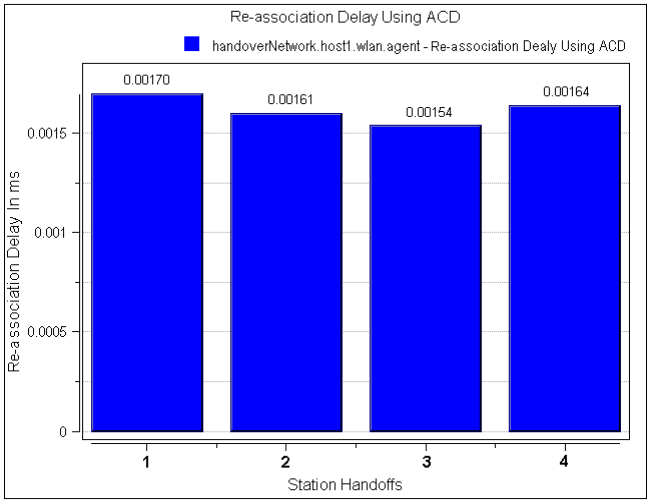

Fig . 3. Re-association Delay Using ACD

As a result of greatly reduced re-association delay, our new mechanism (ACD) can reduce total handoff delay.

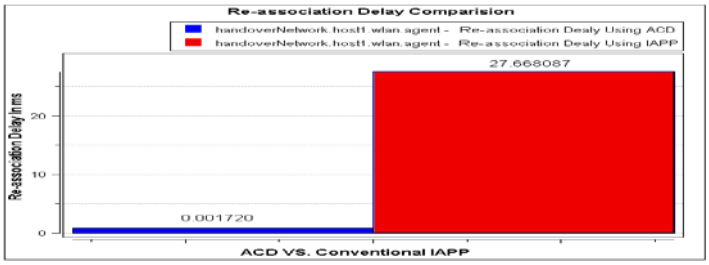

Fig. 4 Re-association Delay Comparisons

7 CONCLUSION

This paper covered the conventional handoff process by briefly explaining the phases involved. The IAPP was also reviewed in order to show its role during the handoff process. A mechanism for reducing re-association delay was also examined and its disadvantages identified. Finally, a new mechanism to reduce re-association delay was introduced in the last sections.

ACKNOWLEDGMENT

We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript. This work is supported by the Faculty of Computer Science and Information Technology, University of Malaya.

REFERENCES

[1] IEEE 802.11f 'Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation', IEEE Standard 802.1 IF, 2003.
[2] IEEE 802.11 standard 'Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications', IEEE Standard, 2007.
[3] R. Ishwar and S. Stefan 'SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks' in Proceeding of IEEE INFOCOM, vol. 1, pp: 675 – 684, 2005.
[4] H. Ping-Jung and T. Yu-Chee 'A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks', IEEE Vehicular Technology Conference (VTC), vol.2, pp: 966-970, 2006.
[5] K. Hye-Soo, P. Sang-Hee, P. Chun-Su, K. Jae-Won and K. Sung-Jea 'Fast Handoff Scheme for Seamless Multimedia Service in Wireless LAN', Lecture Notes in Computer Science, Springer Berlin / Heidelberg, vol. 3976, pp: 942-953, 2006.
[6] K. Seongkwan , C. Sunghyun , P. Se-kyu, L. Jaehwan and K. Sungmann 'An Empirical Measurements-based Analysis of Public WLAN Handoff Operations', 2008.
[7] M. Shin, A. Mishra and W. Arbaugh 'An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process', in Proc. ACM SIGCOMM Computer Communication Review (ACMCCR), vol. 33, pp: 93-102, 2002.
[8] A. Mishra, M. Shin, and W. Arbaugh, "Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network," in Proc. IEEE INFOCOM 2004, March 2004.