Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EVALUATION OF IEEE 802.11 MAC LAYER HANDOFF PROCESS IN CAPWAP CENTRALIZED WLAN

[1*]MOHAMMED BALFAQIH, [2*]ROSDIADEE NORDIN, [3#]ZAIN BALFAQIH, [4ǂ]SHARIQ HASEEB, [5*]AISHA HASHIM

[*]Department of Electrical, Electronic and System Engineering, Faculty of Engineering, UKM, Malaysia

[#]Department of Information System, Faculty of Engineering, Effat University, Saudi Arabia

[ǂ]Wireless Communication Cluster, MIMOS Berhad, Malaysia

[*]Department of Electrical and Computer engineering, Faculty of Engineering, IIUM, Malaysia

E-mail: [1]m_balfageh@hotmail.com, [2]adee@eng.ukm.my, [3]zbalfagih@effatuniversity.edu.sa, [4]shariq.haseeb@mimos.my, [5]aisha@iium.edu.my

ABSTRACT

The growing demand to provide secure wireless connectivity, especially in hot spot areas such as conference halls and events, motivated the development of Control and Provisioning of Wireless Access Point (CAPWAP) centralized Wireless Local Area Network (WLAN). The centralized WLAN utilizes an Access Controller (AC) to simplify configuration, management, and control of Wireless Termination Points (WTPs) in large scale deployment of a wireless network. In order for the clients to associate and re-associate to WTPs, scanning and authentication phases are performed. The contributed latency during scanning and authentication phases, in the MAC layer handoff process, makes it difficult to support real-time applications that are sensitive to network latencies. This work simulates the effect of using different scanning and authentication methods in CAPWAP centralized WLAN during MAC layer handoff process. This can be considered as a significant contribution since no prior work has been done, to our knowledge, to simulate the handoff latency components in centralized networks. This work also studies the effect of varied propagation environments including isolation, and indoor and outdoor environments on handoff process. Moreover, the effects of employed WTP type and the client movement speed on the handoff process latency have been analyzed.

Keywords: *Handoff, CAPWAP, Scanning, Authentication, Centralized Network.*

1. INTRODUCTION

Nowadays, there is a growing need for a high data transmission rate with easy deployment as is required of many electronic devices, including laptop computers, PDAs and smart phones. Therefore, deployment of IEEE 802.11 WLAN is the most widely accepted broadband wireless network technology. However, the high numbers of Access Points (APs) - called WTPs in centralized networks - in a large scale network have introduced several burdens in terms of control, management and monitoring. Distributing and maintaining a consistent configuration while considering security issues present even more challenges in large deployments and new architectures. To solve these problems, centralized WLAN has been proposed.

In centralized WLAN, ACs centrally manage the WTPs and provide compatibility between different vendors in a large scale environment. An AC is a network entity that provides WTP access to the network infrastructure, where WTP exchanges station traffic with it. The core network hosts an Authentication, Association and Accounting (AAA) server and an AC for providing QoS, network management and bandwidth control. Centralized networks can be deployed in shopping centers, campuses, enterprises and even small villages or towns. Recently, in order to establish communication between AC and WTP, the Internet Engineering Task Force (IETF) working group had defined a standard protocol, known as CAPWAP protocol [1]. The overview and functions of CAPWAP, as well as the WTP types supported by CAPWAP, are discussed in Section 3.

Since WTPs have a limited transmission range and clients are able to roam freely, usually, the client handoffs among the WTPs. The handoff

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

process is initiated in the same manner as in the first time association with scanning phase, where the client scans the nearby WTPs and selects the appropriate one. Then, the client will authenticate the selected WTP to get access to the network based on the employed authentication method. However, in order to seamlessly provide real time application such as gaming, audio, and VOIP, handoff latency must be limited to be within 150 ms [2, 3]. Thus, handoff process evaluation work is needed in CAPWAP centralized network to check the ability of seamless handoff in such a network, as well as the demand of the fast handoff method.

This paper simulates the latency of different scanning and authentication methods during the handoff process in CAPWAP centralized network, using the centralized WLAN simulator that we developed. Since no work has been done to simulate the handoff latency components in CAPWAP centralized WLAN, this can be considered as a significant contribution in the field. The effect of the employed WTP type and the client movement speed are also studied. Moreover, to check the effect of different propagation environments on the handoff latency, the handoff process has been tested within isolation, and indoor and outdoor environments.

The following section studies the related works and their limitation. It is followed by a brief description of the CAPWAP centralized WLAN architecture and CAPWAP protocol, in Section 3. Section 4 explores the handoff components in CAPWAP centralized WLAN including IEEE 802.11 scanning methods and IEEE 802.11 authentication. In Section 5, the simulation setup, including the simulation configuration parameters and performance metrics, is provided. Then, discussion and analysis of the findings is presented. Finally, a conclusion of this work is provided in Section 6.

2. RELATED WORK

There are some works [4, 5, 6] that have been done to evaluate the handoff process latency theoretically and experimentally in centralized WLAN. In [4], the authors studied the secure handover in enterprise WLANs through three different standard protocols that support fast handoff, namely CAPWAP, Handover Keying protocol (HOKEY) and IEE802.11r. Theoretically, they obtained that handoff latency in CAPWAP centralized network can be represented by the following equation:

$$4(T_w + T_c) + T_c \quad (1)$$

where T_w is the transmission latency between the client and WTP, and T_c is the communication latency between WTP and AC. From [7], the assumed values were 15 ms and 5 ms for T_w and T_c, respectively.

The measurement covers the four-way handshake between the client and the AC, and key distribution to the WTP. However, the measurements did not include the scanning phase latency. The handoff latency in CAPWAP and IEEE802.11r was about 85 ms, which is lesser than 360 ms, and 45 ms in IEEE802.11i and HOKEY respectively. The presented results are theoretical and do not match the simulation and experimental results. The measurement of the handoff latency for Layer 2 and Layer 3 was performed in [5]. The setup of the Layer 2 and Layer 3 roaming is described as follows. In Layer 2 roaming (Intra-domain) setup, the IEEE 802.11i standard was used, which includes pre-authentication feature. By listening to beacon messages, the client identifies the candidate the WTP can associate with. When the client decides to roam, it sends Extensible Authentication Protocol (EAP) messages to the candidate WTP. The receiving WTP stores this pre-authentication information using Pairwise Master Key (PMK) caching, enabling the station and the WTP to establish all required encryption keys. Thus, the client can complete its authentication before it initiates the roaming. In Layer 3 roaming (Inter-domain), the client requires a new IP address. ACs are configured to be peers of each other and they share information using a Generic Routing Encapsulation (GRE) tunnel. Therefore, ACs can share the WTP and the client's information, which allows forwarding the switching table. When the client moves to another WTP, the AC detects the home VLAN and tunnels traffic to the home AC that allows handoff in a new network. However, the implementation setup does not follow the roaming in CAPWAP protocol. The results obtained were that the average handoff latency was 316 ms and 386 ms for real-time video streaming in layer 2 and layer 3, respectively.

In [6], the authors experimentally had evaluated the latencies of different types of authentication methods during first time association in a centralized network, under non-erroneous and erroneous conditions. The testbed evaluated the open-system, WPA2-personal, and WPA2-enterprise authentication methods. The results showed that under non-erroneous conditions, the average latency of the open-system authentication

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

latency is 37.85 ms while the WPA2-personal authentication takes almost 63.93 ms. The higher latency is contributed during WPA2-enterprise authentication with approximately 173.53 ms. On the other hand, under erroneous conditions, the average latency of open-system authentication is around 214.8 ms. The WPA2-personal and the WPA2-enterprise consumed around 129.39 ms and 2987.66 ms, respectively. However, the main limitation of this work is the limited scale of the employed testbed. Moreover, the effect of the employed WTP type on the latency of the authentication phase was not considered.

3. CAPWAP CENTRALIZED WLAN ARCHITECTURE

The centralized architecture is a hierarchical architecture involving AC and several controlled WTPs as shown in Fig. 1. The purpose of this architecture is to simplify configuration, management and control of WTPs in large scale deployment of wireless networks.

AC is a control node that provides access to central management of some functionalities such as radio frequency (RF) configuration and monitoring, WTP configuration, and firmware downloading [8]. On the other hand, WTP is the network entity that contains an RF antenna and 802.11 PHY to transmit and receive user traffic for the IEEE 802.11 WLAN access networks [8]. The WTP term is used instead of AP since the AP term may also refer to the logical entity which implements 802.11 services. In order to establish communication between AC and WTP, IETF Working group had defined a standard protocol named CAPWAP protocol.

CAPWAP is an interoperable protocol that is concerned with management and configuration of the WTP devices, configuration and control of the radio resource, and security regarding the registration of the WTP to an AC. According to the centralization level of the control operations, CAPWAP supports two different operational architectures [8, 10]: Local, and Split Medium Access Control (MAC). The naming reflects how the 802.11 MAC functions are distributed between AC and WTP. In both architectures, CAPWAP functions entirely left to the AC while the WTP is responsible for physical functions.

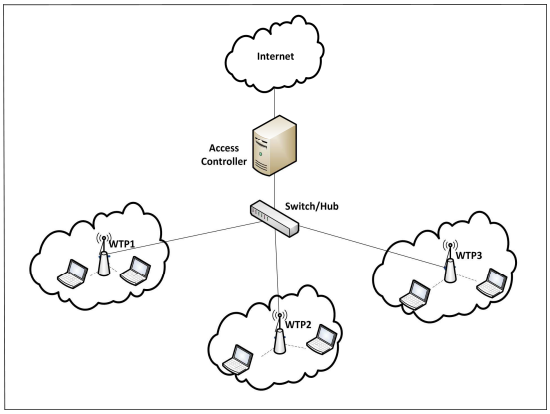

Figure 1: Centralized WLAN Architecture.

In Local MAC Architecture, the whole MAC functionalities, including control and management frames, reside on the WTPs. Consequently, integration and distribution services are implemented by the WTPs or are bridged to the AC. The integration service enables delivery of the MSDUs between 802.11 and 802.3. The distribution service enables MAC layer to deliver MSDUs within the Distribution System (DS).

The downside of such architecture is the extra loading over the WTPs. Local MAC architecture is less centralized because the station's state information remains at the WTP and is processed locally. However, in some cases it is forwarded to the AC. This causes some difficulties to manage a growing network of many WTP devices. When compared to split MAC WTP, local MAC WTP is more expensive and less secure.

On the other hand, in Split MAC WTP architecture, in order to allow AC to scale a large number of WTP devices, non-realtime MAC functions are handled by the AC while the WTP terminates realtime MAC functions. Here, due to the fact that the AC is responsible for control frames, the distribution and integration services reside on the AC. The CAPWAP protocol encapsulates and exchanges all Layer 2 wireless data and management frames between AC and the WTP. However, split MAC has some delay from splitting MAC functions and is dependent on the AC where it forwards all information to the AC. The two architectural variants may be appropriate for certain deployment scenarios [11].

The Authentication, Authorization and Accounting (AAA) server in both architectures resides on the AC. This implies that the IEEE 802.1X, Extensible Authentication Protocol (EAP) and IEEE Robust Security Network Association

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(RSNA) key management functions are also located on the AC. This will be reflected in the handoff process as shown in the Discussion and Analysis section of this paper. Fig. 2a and Fig. 2b show the message flow of handoff process in Local MAC WTP and Split MAC WTP, respectively. The main phases during the 802.11 MAC layer handoff process in Local and Split MAC WTP architectures are detailed in next section.

4. MAC LAYER HANDOFF PROCESS COMPONENTS IN CAPWAP CENTRALIZED WLAN

In centralized architecture, the MAC layer handover is the roaming of the client from a WTP to another that is connected to the same AC [9, 5]. The WTPs are in the same broadcast domain and configured with the same SSID. This requires exchanging the MAC address between client and new WTP. The MAC layer handoff process in CAPWAP protocol differs in local MAC and split MAC WTPs according to the differences in MAC function mapping. When the client roams from a WTP to another, it will create new PMK with the new WTP from previous PMK as follows [12]:

$$PMK_n = TLS - (MK, PMK_{n-1} | AP_{MAC} | STA_{MAC}) \quad (2)$$

As we can note from Fig. 2a and Fig. 2b, since 802.1X authentication and key management are performed at the AC, the AC has the PMK of the previous session. Thus, there is no need to process full 802.1X re-authentication or transfer the AAA context to derive a new PMK. This reduces the re-authentication latency during handoff process. However, the scanning phase in both architectures is following the standard scanning methods with either passive or active method. This in turn will cost the client considerable latency during the handoff process [13].

4.1 IEEE 802.11 Scanning Methods

In WLANs, including centralized WLAN, in order for the client to find a nearby AP, the scanning phase must be initiated. There are two scanning methods that can be used i.e. passive scan and active scan methods. In passive scan mode, the client listens to the wireless medium for beacon frames from all WTPs, on a specific channel, for 100 ms intervals [14, 15]. Then, the client will switch to another channel and select the WTP with the best Received Signal Strength Indicator (RSSI). In contrast, in the active scan mode, the client broadcasts a probe request frame to determine which WTPs are within range. Then, the recipient WTP will reply with a probe response message and from which the client will select the WTPs to join. The client waits for *MinChannelTime*, per channel, if no response is received. Otherwise, it would wait *MaxChannelTime* to stop accepting the probe response frames. According to [7], the *MinChannelTime* is around 33 ms and *MaxChannelTime* is around 55 ms. As compared to passive scan mode, active scan mode has a lower latency of about 35 ms per channel [7] and it is more suitable for real-time application. However, two parameters affect the probing latency in active mode, i.e. the number of scanned channels and the waiting time per channel.

The probe response and beacon messages frame format contains capability information supported data rate, among others. In secured networks, the Robust Security Network (RSN) information element to identify supported authentication and cipher suites are also included, e.g. 802.1X authentication, Pre-Shared Key (PSK) authentication, and Temporal Key Integrity Protocol (TKIP) [16]. Upon selecting the next WTP, the client will proceed with the authentication phase. The authentication methods are detailed in the following section.

4.2 IEEE 802.11 Authentication Methods

The two traditional authentication methods in 802.11 are open-system authentication and shared key authentication [12]. The open-system authentication is the default authentication method. Upon selecting the AP, the client will send an authentication request message containing the identity of the client. The AP will reply with an authentication response message indicating acceptance or rejection. The client, after receiving the acceptance, will convey its information, such as supported data rate and SSID, through an association request and waits for an association response. This four signaling messages are called authentication and association messages. However, the open-system authentication is considered as null authentication since there is no identity verification required [12].

The Shared key authentication method uses the static Wired Equivalent Privacy (WEP) security algorithm where the AP sends a challenge to the client and requests the client to encrypt and send it back. The AP will decrypt and encrypt the challenge response of the client. If the challenge matches the response, the AP will grant the connection to the client. For encryption purposes,

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

after successful association, the static WEP key that is used during the authentication process will be used to encrypt the 802.11 data frames.

However, due to the weakness and ease of hackability in open-system and shared key authentication methods, there are many other secure authentication methods that have been defined in 802.11. These methods include Wi-Fi Protected Setup (WPS), Wi-Fi Protected Access (WPA) and WPA2. These algorithms use different authentication and encryption methods.

The authors in [12] have defined what is known as RSN Associations (RSNAs). In order to establish connections in a RSNA, authentication and creation of a dynamic encryption key, through the four way handshake protocol, are required. Based on alliance certification, RSNAs are classified into two categories namely personal (WPA2-personal) and enterprise (WPA2-enterprise). In both methods, the employed encryption method could be either AES-Counter Mode CBC-MAC Protocol (AES-CCMP) or Temporal Key Integrity Protocol (TKIP).

The WPA2-personal, also known as WPA2-PSK, combines the PSK authentication method and key management protocol to establish connection. The WPA2-PSK is designed for small networks such as home and small buildings because of their ease of deployment [17]. On the other hand, the WPA2-Enterprise, also known as WPA2-802.1X or WPA2-EAP, provides more secure authentication as compared to WPA2-personal. However, it requires a more complicated configuration setup [18]. The WPA2-Enterprise combines 802.1X authentication and the key management protocol to provide stronger secure authentication and data privacy.

5. RESULTS

In order to evaluate the performance of the handoff process in CAPWAP centralized WLAN, the CAPWAP centralized WLAN simulator was developed by Visual Basic.NET (VB.NET).

This is because there is no available simulator that evaluates the CAPWAP protocol and the mobility within it. Moreover, there is not much work done on the CAPWAP protocol, even though it had been defined since 2009. According to [19] the reason is that the vendors still use their proprietary solutions, as they try to stand out amongst others by promoting their own protocols.

The employed performance metric is the handoff latency. This represents the MAC layer handoff latency which is the amount of time that the mobile client takes to roam to a new WTP that has the same broadcast domain and is configured with the same SSID. The handoff latency is an important performance criterion in delay-sensitive applications.

5.1 Simulation Setup

The MAC layer handoff latency was explored using different types of WTPs (local MAC WTP and split MAC WTP) in different propagation environments, by employing different scanning and authentication methods. The considered propagation environments were isolation environment, the indoor environment and the outdoor environment based on [20]. The simulation configuration parameters are shown in Table 1.

Table 1: Simulation Configuration Parameters.

Parameters	Value
Environment Dimensions	1000*1000
Simulation Time	1000 seconds
Physical Characteristics	802.11n
Bandwidth	20MHz - 40MHz
Frequency	2.4 - 2.5 GHz
Transmit Power	13 dBm
Data Rate	144 – 300 Mbps
Modulation	64-QAM
Code Rate	5/6
Receiver Sensitivity	-90 / -9
Operator Channels	1-6-11
No. of AC	1
No. of WTP	16
No. of Client	50 (performing handoff)
WTP Bandwidth	20 MHz – 40 MHz
WTP Type	Local MAC WTP / Split MAC WTP
Authentication Method	Open-system / WPA2-Personal / WPA2-Enterprise
Scanning Method	Active / Passive
MinChannelTime	33 ms
MaxChannelTime	55 ms
Beacon Interval	100 ms
Handoff Threshold	- 73.8 dBm
Environment	Isolation / Indoor / Outdoor
Mobile Client Speed	Human Walking/Human Running

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

All simulation scenarios were configured to run over an area of 1000m x 1000m. The AC was connected directly to the WTP using a LAN connection while the clients were connected to the WTPs using WLAN. The simulated scenarios were configured with 50 clients (performing handoff), 16 WTPs and 1 AC. The simulation time was 1000 seconds in each experiment. In addition to that, to evaluate the client speed effect, the moving speed of the client was set to either human walking speed (1.3 m/s) or human running speed (3.3 m/s) [21]. The moving path of the mobile client was unchanged in each experiment. The physical characteristics of WLAN followed the 802.11n standards with 2.4 – 2.5 GHz frequency, 13 dBm transmitted power, 64-QAM modulation and 5/6 code rate. All WTPs were configured with one of the non-overlapped channels which are channels 1, 6 and 11. The IEEE 802.11n supports 20 MHz and 40 MHz bandwidth. To evaluate the bandwidth effect in handoff latency, 20 MHz and 40 MHz bandwidths were used in different sub-scenarios. The *MinChannelTime* and *MaxChannelTime* were set to 33 ms and 55 ms, respectively [7]. The beacon interval in passive scan was set to 100 ms [14].

5.2 Discussion and Analysis

In order to facilitate presentation and discussion of the simulation results, our results will be categorized into two main scenarios i.e. IEEE 802.11 MAC layer handoff latency in local MAC WTP, and IEEE 802.11 MAC layer handoff latency in split MAC WTP.

5.2.1 IEEE 802.11 MAC layer handoff latency in local MAC WTP

In this scenario, a local MAC WTP is used to provide a connection to the mobile client. Fig. 3 shows the handoff latency values obtained in different environments, using 20 MHz bandwidth and human walking speed as the moving speed.

The results show that the main effect of the environment in the handoff process is on the frequent handoff events, when considering the same mobility path and simulation time. This is due to the fact that the mobile client initiates the handoff process when the RSSI reaches the defined handoff threshold which occurs frequently in some environments that have a high path loss. The high path loss degrades the signal strength and shrinks the coverage area of the WTP. The numbers of handoff events in the outdoor environment (between buildings) are 257 events while in the outdoor (free space), the number decreases to 164 events. In isolation and indoor environments, the numbers of handoff events are 58 and 182, respectively. The small coverage size increases the possibility of the Ping-pong Effect which in turn will decrease the network performance by causing an interruption of the service. Hence, determining a handoff threshold is a critical issue in the handoff process [22]. In addition to that, figure 3 shows that the active scan latency with an open-system authentication in all environments represents around 94% of the total handoff latency with average 282 ms. The open-system authentication and CAPWAP control messages represent 3.2% and 2.1%, respectively, of the total handoff latency. With WPA2/personal and WPA2/enterprise authentication, the active scan latency represents around 87.1% of total handoff latency. Since the AC keeps the PMK key, the AC proceeds directly with four way handshake after open-system authentication in both authentication methods. The WPA2/personal and WPA2/enterprise authentication represent around 10.8%, while CAPWAP control messages represent 2.1% of the total handoff latency. On the other hand, passive scan represents around 98% of total handoff latency using open-system authentication and around 96% using WPA2/personal or WPA2/enterprise authentication methods. The average passive scan latency is about 993 ms.

In Fig. 3, the results show that the active scan latency is about 280 ms using the different authentication methods. The open-system authentication method latency is about 11 ms, while the latency for the personal and enterprise authentication method is around 35.5 ms. On the other hand, the passive scan method produces about 110 ms regardless of the authentication method employed. The personal and enterprise authentication methods latency is almost 35.5 ms, while the latency using the open-system authentication is around 11 ms.

Table 2 shows the average handoff latency values using different scanning and authentication method represented in Fig. 3. The results show that the environment does not have much effect on handoff latency. This is because there is no traffic load in the simulated scenario showing the throughput effect in both bandwidths. However, the environment resulting in the poorest results is the outdoor environment (between buildings). The passive scan latency is affected by the beacon interval and listening to beacon messages; thus the passive scan latency increases based on listening-consumed time per channel.

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In Table 3, the average handoff latency is calculated for a mobile client with human walking speed and local MAC WTP, with 40MHz bandwidth, and using different scanning and authentication methods. The number of handoff events in all environments is equal to the previous scenario since the mobile clients have same moving speed and mobility path. The average handoff latency values are lesser than when using local MAC WTP with 20 MHz bandwidth. However, there is no significant difference since there is no traffic load during the handoff process which will show the difference of the throughput in both bandwidths. The WTP working in 20 MHz bandwidth will reach to an unacceptable traffic value before the 40 MHz WTP, causing high queuing delay that increases the handoff latency before the WTP with 40 MHz [22].

Table 4 shows the handoff latency of a mobile client in different environments using 20 MHz bandwidth and human running speed as the moving speed. The number of handoff events in all environments increases since the moving speed was increased. In the outdoor environment (between buildings), the number of handoff events is 691 events while in the outdoor environment (free space) it is 389 events. In isolation and indoor environments, the number of handoff events is 131 and 453, respectively. As shown by the results, the handoff latency of the mobile client with 20 MHz bandwidth and human running speed has a higher latency when compared to the mobile client with human walking speed and the same bandwidth. Table 5 shows the average handoff latency of a mobile client with 40 MHz bandwidth and running moving speed. Compared to the mobile client with 20 MHz bandwidth, the mobile client has a lesser handoff latency. Moreover, the handoff latency is higher than the mobile client with the same bandwidth and human walking speed.

5.2.2 IEEE 802.11 MAC layer handoff latency in split MAC WTP

In this scenario, the handoff latency is measured for a mobile client connected to a split MAC WTP by considering the same scenarios as in the previous sub-section. Fig. 4 shows the handoff latency of a mobile client connected to split MAC WTP with 20MHz bandwidth. The moving speed of the client is that of human walking speed. The results show that the handoff latency in all environments has almost the same percentage with the mobility in local MAC WTP. The authentication latency in split MAC WTP is higher than using local MAC WTP in most of the cases. The values of the average handoff latency in Fig. 4 are illustrated in Table 6.

The results show that the active scan latency is about 282 ms while the passive scan method produces about 110 ms regardless of the authentication method employed. The open-system authentication method latency is about 9.6 ms while the personal and the enterprise authentication method latency is around 35.7 ms. Similar to the local MAC WTP, the handoff process is evaluated with different moving speeds and different bandwidth usage but they are not presented here due to the lack of space.

Table 7 represents a summary of the handoff latency evaluation in CAPWAP centralized WLAN. It shows the different parameters that are considered and their effect on the handoff latency, the handoff events number and the signaling cost.

6. CONCLUSION AND FUTURE WORK

In this paper, the handoff latency components using different scanning and authentication methods in CAPWAP centralized WLAN have been intensively investigated. The impact of propagation environment and on the handover performance has been considered and analyzed. Moreover, the effect of the employed WTP type and the mobility speed of the mobile client are also investigated.

The main conclusion of this paper is that the scanning latency is the main contributor to the handoff latency. The scanning latency represents approximately 87.1%, in active scan mode, and approximately 96% in passive scan mode, of the total handoff latency. In addition, the outdoor environment (between buildings) gave the highest latency among the simulated environment. From the results, split MAC WTP causes more handoff latency comparing to local MAC WTP. In addition, increasing the movement speed raises the handoff latency. Since there is no traffic load during our evaluation, there is no much difference between employing 20 or 40 MHz bandwidth.

Our future work is to present a fast handoff scheme to reduce the MAC layer handoff latency in CAPWAP centralized WLAN. As the results showed that the scan phase is the main component of the handoff latency, the proposed scheme will therefore focus on reducing scanning phase latency.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ACKNOWLEDGEMENT

The authors would like to acknowledge Universiti Kebangsaan Malaysia, under Grant Ref. No. GUP-2014-005 for the financial assistance in this work

REFRENCES:

[1] B. O'Hara, P. Calhoun, J. Kempf, "Configuration and Provisioning for Wireless Access Points (CAPWAP) Problem Statement", Internet Engineering Task Force, RFC 3990, 2005.

[2] ITU, International telephone connections and circuits – General Recommendations on the transmission quality for an entire international telephone connection, One-way transmission time, ITU-TG.114, 2003.

[3] N. Seitz, "ITU-T QoS Standards for IP-Based Networks", IEEE Communication Magazines, 2003, pp. 82-89.

[4] T. C. Clancy, "Secure Handover in Enterprise WLANS: CAPWAP, HOKEY, and IEEE 802.11R", IEEE Wireless Communications, Vol. 15, Issue 5, 2008, pp. 80-85.

[5] M. A. Amin, K. Abu Bakar, A. Abdullah, R. H. Khokhar, "Handover Latency Measurement using Variant of CAPWAP Protocol", Network Protocols and Algorithms, Vol. 3, No. 2, 2011, pp. 67-101.

[6] M. H. Mazlan, S. H. Syed Ariffin, M. Balfaqih, S. N. M. Hasnan, S. Haseeb, "Latency Evaluation of Authentication Protocols in Centralized 802.11 Architecture", IET International Conference on Wireless Communications and Applications (ICWCA), 2012, pp.1-6.

[7] A. Mishra, M. Shin, W. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process", ACM SIGCOMM Computer Communication Review (ACMCCR), Vol. 33, Issue 2, 2003, pp. 93-102.

[8] L. Yang, P. Zerfos, E. Sadot, "Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)", Internet Engineering Task Force, RFC 4118, 2005.

[9] T. Sridhar, "Wireless LAN Switches; Functions and Deployment", The Internet Protocol Journal, Vol. 9, No. 3, 2006.

[10] G. Conradi, "Current Status and Overview of the CAPWAP Protocol", http://www1.cse .wustl.edu/~jain/cse574-10/ftp/capwap/index.html, 2010.

[11] P. Calhoun, M. Montemurro, D. Stanley, "CAPWAP Protocol Binding for IEEE 802.11" Internet Engineering Task Force, RFC 5416, 2009.

[12] IEEE Std. 802.11i, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications Amendment 6, Medium Access Control (MAC) security enhancements", IEEE Standard, 2004.

[13] S. Behcet, X. Zheng, "CAPWAP Handover Protocol", IEEE International Conference on Communications ICC '06, 2006, pp. 1933 – 1938.

[14] H. Velayos, G. Karlsson, "Techniques to Reduce IEEE 802.11b MAC Layer Handover Time", In Proceedings of IEEE ICC, vol. 7, 2004, pp. 3844-3848.

[15] S. Pack, J. Choi, T. Kwon, Y. Choi, "Fast Handoff Support in IEEE 802.11 Wireless Networks" IEEE Communications Surveys & Tutorials, Vol. 9, No. 1, pp. 2-12, 1st Quarter 2007.

[16] IEEE Std. 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. IEEE standard", 2012.

[17] F. C. Kuo, F. Meyer, H. Tschofenig, X. Fu, "Comparison Studies between Pre-Shared and Public Key Exchange Mechanisms for Transport Layer Security", 25th IEEE International Conference on INFOCOM, 2006, pp. 1-6.

[18] A. Chiornita, D. Rosner, L. Gheorghe, "A Practical Analysis of EAP Authentication Methods", 9th Roedunet International Conference (RoEduNet), 2010, pp. 31-35.

[19] X. Cheng, "High Density Multi-cell Wireless Networks", Bachelor Thesis Eng. Leiden Institute of Advanced Computer Science (LIACS), 2011.

[20] M. Hidayab, A. H. Ali, K. B. A. Azmi, "Wifi signal propagation at 2.4 GHz", Microwave Conference, APMC 2009. Asia Pacific, 2009, pp.528-531.

[21] S. Park, H. Kim, S. Park, Park C., Kim J., Ko S., "Selective Channel Scanning for Fast Handoff in Wireless LAN using Neighbor Graph", Personal Wireless Communications Lecture Notes in Computer Science, Vol. 3260, 2004, pp. 194-203.

[22] F. Li, M. Li, R. Lu, H. Wu, M. Claypool, R. Kinicki, "Measuring Queue Capacities of IEEE 802.11 Wireless Access Points", In Proceedings of the Fourth IEEE International conference on Broadband Communications, Networks and Systems (BROADNETS), 2007, pp. 846-853.

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

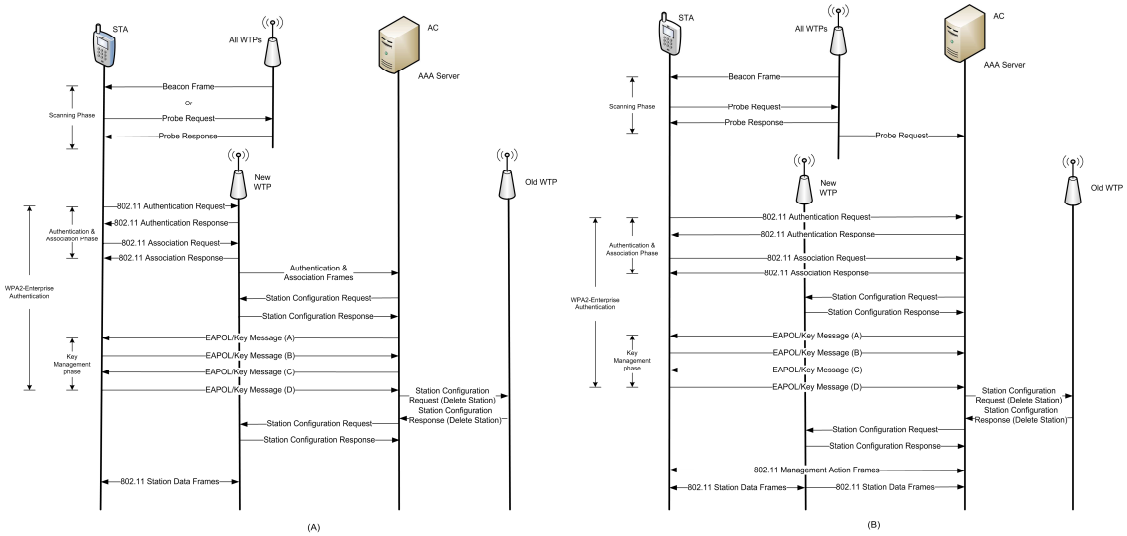

Figure 2: (A) Message Flow of Client Handoff Process in Local MAC WTP (B) Message Flow of Handoff Process in Split MAC WTP [11].

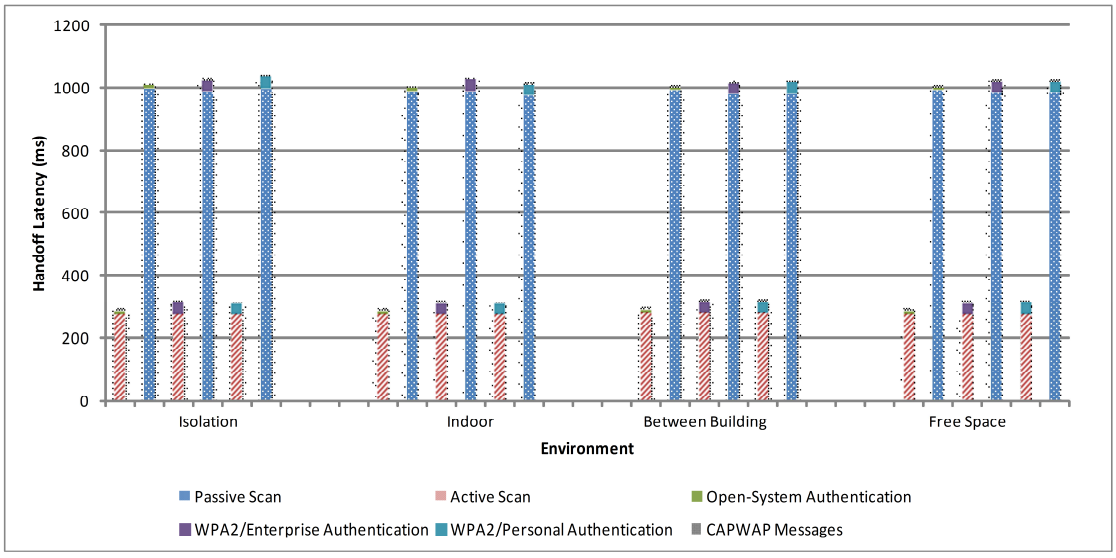

Figure 3: The Average Handoff Latency of a Mobile Client with Human Walking Speed and Local MAC WTP with 20MHz Bandwidth Using Different Scanning and Authentication Methods.

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: The Average Handoff Latency of a Mobile Client with Human Walking Speed and Local MAC WTP with 20MHz Bandwidth Using Different Scanning and Authentication Methods.

Authentication / Scanning	Open-System Authentication	WPA2/Personal Authentication	WPA2/Enterprise Authentication	
Passive Scan	1016.42 ms	1032.55 ms	1042.83 ms	Isolation
Active Scan	296.46 ms	322.63 ms	320.09 ms	
Passive Scan	1007.72 ms	1034.03 ms	1019.25 ms	Indoor
Active Scan	296.38 ms	320.99 ms	320.19 ms	
Passive Scan	1009.74 ms	1022.22 ms	1025.65 ms	Between Building
Active Scan	325.44 ms	325.55 ms	325.44 ms	
Passive Scan	1011.55 ms	1028.26 ms	1027.14 ms	Free Space
Active Scan	295.13 ms	321.33 ms	323.02 ms	

Table 3: The Average Handoff Latency of a Mobile Client with Human Walking Speed and Local MAC WTP with 40MHz Bandwidth Using Different Scanning and Authentication Methods.

Authentication / Scanning	Open-System Authentication	WPA2/Personal Authentication	WPA2/Enterprise Authentication	
Passive Scan	991.99 ms	1035.15 ms	1023.38 ms	Isolation
Active Scan	293.48 ms	320.58 ms	320.33 ms	
Passive Scan	1004.05 ms	1020.68 ms	1027.30 ms	Indoor
Active Scan	293.62 ms	318.42 ms	320.61 ms	
Passive Scan	1006.97 ms	1023.24 ms	1028.61 ms	Between Building
Active Scan	298.57 ms	323.53 ms	324.12 ms	
Passive Scan	1014.78 ms	1031.99 ms	1036.13 ms	Free Space
Active Scan	293.58 ms	319.42 ms	318.29 ms	

Table 4: The Average Handoff Latency of a Mobile Client with Human Running Speed and Local MAC WTP with 20MHz Bandwidth Using Different Scanning and Authentication Methods.

Authentication / Scanning	Open-System Authentication	WPA2/Personal Authentication	WPA2/Enterprise Authentication	
Passive Scan	1005.36 ms	1034.01 ms	1036.96 ms	Isolation
Active Scan	296.23 ms	322.54 ms	320.33 ms	
Passive Scan	1006.86 ms	1025.74 ms	1035.44 ms	Indoor
Active Scan	293.62 ms	318.42 ms	320.61 ms	
Passive Scan	1005.27 ms	1032.6 ms	1031.16 ms	Between Building
Active Scan	298.57 ms	323.53 ms	324.12 ms	
Passive Scan	1012.93 ms	1033.88 ms	1030.02 ms	Free Space
Active Scan	293.58 ms	319.42 ms	318.29 ms	

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 5: The Average Handoff Latency of a Mobile Client with Human Running Speed and Local MAC WTP with 40MHz Bandwidth Using Different Scanning and Authentication Methods.

Authentication / Scanning	Open-System Authentication	WPA2/Personal Authentication	WPA2/Enterprise Authentication	
Passive Scan	1013.99 ms	1019.15 ms	1020.56 ms	Isolation
Active Scan	296.35 ms	321.94 ms	320.71 ms	
Passive Scan	1005.18 ms	1028.35 ms	1028 ms	Indoor
Active Scan	294.28 ms	319.26 ms	320.45 ms	
Passive Scan	1000.16 ms	1031.04 ms	1027.15 ms	Between Building
Active Scan	299.39 ms	324.18 ms	324.65 ms	
Passive Scan	1003.26 ms	1026.03 ms	1029.31 ms	Free Space
Active Scan	294.44 ms	319.94 ms	319.77 ms	

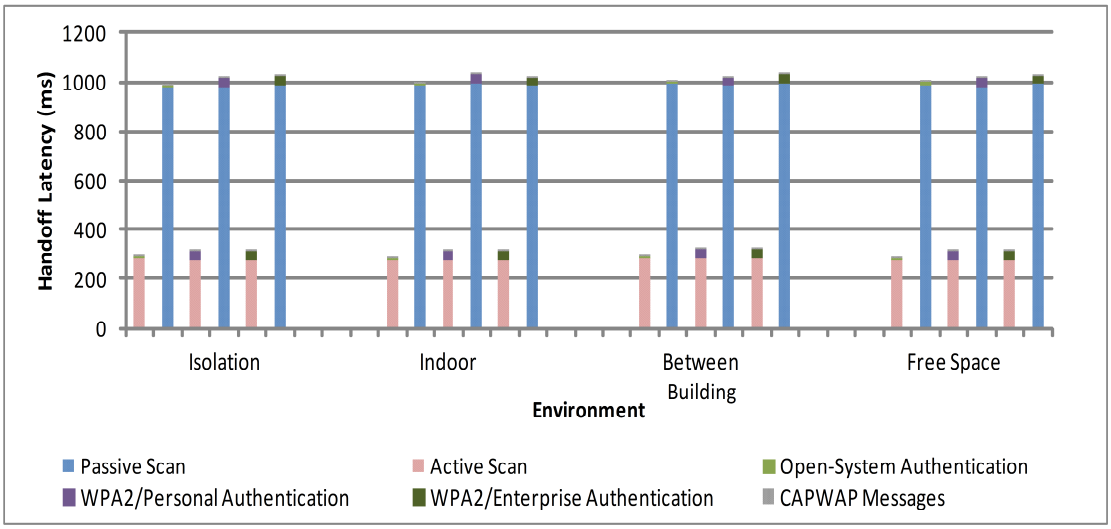

Figure 4: The Average Handoff Latency of a Mobile Client with Human Walking Speed and Split MAC WTP with 20MHz Bandwidth Using Different Scanning and Authentication Methods.

Table 6: The Average Handoff Latency of a Mobile Client with Human Walking Speed and Split MAC WTP with 20MHz Bandwidth Using Different Scanning and Authentication Methods.

Authentication / Scanning	Open-System Authentication	WPA2/Personal Authentication	WPA2/Enterprise Authentication	
Passive Scan	996.03 ms	1024.27 ms	1030.84 ms	Isolation
Active Scan	297.66 ms	321.18 ms	321.60 ms	
Passive Scan	1001.05 ms	1036.35 ms	1026.58 ms	Indoor
Active Scan	294.89 ms	321.48 ms	322.77 ms	
Passive Scan	1008.22 ms	1027.09 ms	1035.21 ms	Between Building
Active Scan	298.98 ms	325.98 ms	325.89 ms	
Passive Scan	1004.77 ms	1024.44 ms	1034.32ms	Free Space
Active Scan	294.31 ms	321.36 ms	322.69 ms	

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 7: Summary of the Handoff Latency Evaluation in CAPWAP Centralized WLAN.

Consideration	Scanning method	Authentication method	Bandwidth	Environment	Moving Speed
The handoff latency	✓	✓	✓	✓	✓
The handoff events number	✗	✗	✓	✓	✓
The signaling cost	✓	✓	✗	✗	✗