World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:6, No:8, 2012

CAPWAP Status and Design Considerations for Seamless Roaming Support

M. Balfaqih, S. Haseeb, M. H. Mazlan, S. N. Hasnan, O. Mahmoud and A. Hashim

***Abstract*—**Wireless LAN technologies have picked up momentum in the recent years due to their ease of deployment, cost and availability. The era of wireless LAN has also given rise to unique applications like VOIP, IPTV and unified messaging. However, these real-time applications are very sensitive to network and handoff latencies. To successfully support these applications, seamless roaming during the movement of mobile station has become crucial. Nowadays, centralized architecture models support roaming in WLANs. They have the ability to manage, control and troubleshoot large scale WLAN deployments. This model is managed by Control and Provision of Wireless Access Point protocol (CAPWAP). This paper covers the CAPWAP architectural solution along with its proposals that have emerged. Based on the literature survey conducted in this paper, we found that the proposed algorithms to reduce roaming latency in CAPWAP architecture do not support seamless roaming. Additionally, they are not sufficient during the initial period of the network. This paper also suggests important design consideration for mobility support in future centralized IEEE 802.11 networks.

***Keywords*—**802.11, centralized Architecture, CAPWAP, Roaming.

I. Introduction

IEEE 802.11 technology primarily was designed for indoor environments with limited data rates - only 1 and 2 Mbps -. The success of IEEE 802.11 to increase the available data rate, remove significant factor holding back adoption of IEEE 802.11 in large-scale deployments. However, the high number of Access Points (APs) in a large-scale network has introduced several burdens such as control, management and monitoring. Distributing and maintaining a consistent configuration with considering security issues present even more challenges in large deployments and new architectures. These issues forced many network vendors to offer proprietary centralized solutions. The common characteristic of the proposed solutions is a splitting functionality of APs and add more centralized operation functions for configuring, managing and monitoring purposes. Because that proposed solutions do not provide any form of interoperability, Control and Provisioning of Wireless Access Point (CAPWAP) Working Group have defined standard interoperable protocol to address the aforementioned problems [1]. The CAPWAP is a standard protocol between Wireless Termination Points (WTPs) and Access Controllers (ACs) to centrally manage WTPs and provide compatibility between different vendors in large-scale environment.

AC is a network entity that provides WTP access to the network infrastructure where WTP exchanges station traffic with it. By using some station traffic information, mobile station can roam seamlessly from one WTP to another. The handoff process occurred in three phases: scanning, re-authentication/re-association and 802.11i re-authentication. Empirical analysis of the handoff process found that the handoff delay takes hundreds of milliseconds [2], while the requirement for real-time applications is less than 50 ms.

Based on Autonomous Architecture perspective, reducing handoff delay was widely discussed in the literature. Generally, the proposed schemes adopted four methods: reducing the number of scanned channels [3, 4, 5, 6], shortening waiting time in each scanned channel [7, 8, 9] using dual-radio where one antenna searches new AP and another one continues data transmission [10, 11, 12] and reducing re-authentication/re-association delay [13, 14, 15]. On the other hand, based on CAPWAP centralized architecture, CAPWAP Handover Protocol (CAPWAPHP) was designed [16] to centrally manage station handoff where the protocol reduces the authentication delay by proactively transferring AAA context to neighboring WTPs. In addition, the measurement of handoff latency was provided in [17].

This paper presents an overview of centralized CAPWAP architecture as well as covers CAPWAP protocol and past works related to. It also details the handoff procedure in CAPWAP and suggests important design consideration for mobility support in future IEEE 802.11 networks. The rest of the paper is organized as follows. In section II, we review CAPWAP centralized architecture. CAPWAP protocol overview is presented in section III. The published works within CAPWAP protocol are explored in section IV. Section VI details handoff procedure. Perspective on seamless roaming is given in section V. Finally, section VII concludes this paper.

II. CAPWAP centralized architecture

CAPWAP architecture consists of WTPs communicating to AC via CAPWAP protocol (see Fig. 1). According to the centralization level of the control operations, CAPWAP supports two different operational architectures [18]: Local and Split Medium Access Control (MAC). The naming reflects how the 802.11 MAC functions are distributed between AC and WTP (see Fig. 2).

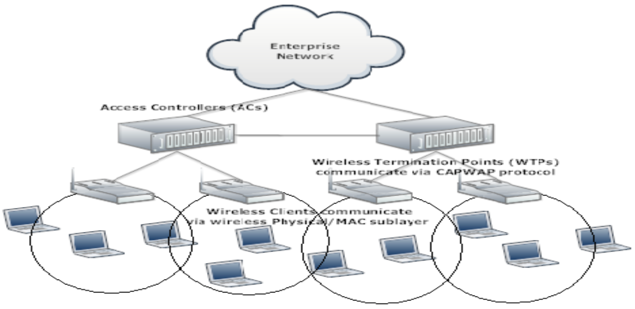
Enterprise Network
Access Controllers (ACs)
Wireless Termination Points (WTPs) communicate via CAPWAP protocol
Wireless Clients communicate via wireless Physical/MAC sublayer

Fig. 1 CAPWAP Centralized Architecture

M. Balfaqih is with Mobile Platform Department, MIMOS Berhad Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia and International Islamic University Malaysia (IIUM), Gomback, 50728 Kuala Lumpur, Malaysia (phone: 0172154199; e-mail: m_balfageh@ hotmail.com).

S. Haseeb, M. H. Mazlan and S. N. Hasnan, are with Mobile Platform Department, MIMOS Berhad Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia. (e-mail: shariq.haseeb@mimos.my hasbullah.mazlan@mimos.my and haizum.hasnan@mimos.my).

O. Mahmoud and A. Hashim are with International Islamic University Malaysia (IIUM) Gomback, 50728 Kuala Lumpur, Malaysia (e-mail: omer@iium.edu.my, aisha@iium.edu.my).

In both architectures, CAPWAP functions entirely left to the AC while the WTP is responsible for physical functions.

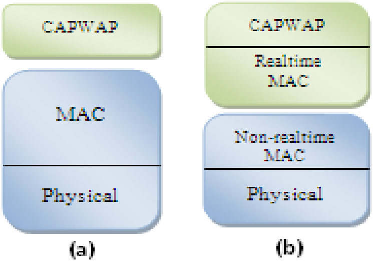

Fig. 2 802.11 MAC functions mapping between ◆ AC and ◆ WTP in (a) Local MAC (b) Split MAC

A. Local MAC Architecture

In this architecture, the whole MAC functionalities including control and management frames reside on WTPs. Consequently, Integration and Distribution services are implemented by WTP or are bridged to AC. The Integration service enables delivery of MAC service data units (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 WTP. Local MAC Architecture is less centralized because that station's state information remains at WTP and is processed locally but, in some cases, is forwarded to AC. This causes some difficulties to manage a growing network of many WTP devices. Comparing to Split MAC WTP, Local MAC WTP is more expensive and lesser secured.

B. Split MAC Architecture

In order to allow AC to scale to a large number of WTP devices, non-realtime MAC functions are handled by AC while WTP terminates realtime MAC functions. The realtime functions are time-sensitive functions such as beacon generation, probe response and processing of control frames. Due to that AC is responsible for control frames, the distribution and integration services reside on the AC. CAPWAP protocol encapsulates and exchanges all layer 2 wireless data and management frames between AC and WTP.

However, Split MAC has some delay from splitting MAC functions and the dependency on AC where it forwards all information to AC. The two architectural variants may be appropriate for certain deployment scenario.

III. CAPWAP Protocol

There are several connectivity options between ACs and collection of WTPs including direct connection, layer 2 switched connection and layer 3 routed connection. The CAPWAP protocol is defined to be layer 2 technology where the goals of CAPWAP as stated in [19] are: First, centralize authentication and policy enforcement functions for a wireless network. Second, enable shifting time critical processing from the WTP. Third, provide extensibility via a generic encapsulation and transport mechanism. CAPWAP functions are 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.

The CAPWAP transport layer carries CAPWAP data messages and control messages, which are sent over separate User Datagram Protocol (UDP) ports. Datagram Transport Layer Security (DTLS) is used to secure CAPWAP control messages and optionally CAPWAP data messages. When WTP is turned on, CAPWAP enters a discovery phase to automatic associate WTP with AC [18]. In this phase, the WTP sends Discovery Request messages, and ACs respond with Discovery Response message. Then, the WTP selects AC to connect and establishes DTLS session. Subsequently, at configuration phase, the WTP and the AC exchange their configuration and capabilities. Finally, normal state of operation which is Run phase is started where the WTP and the AC ready to exchange CAPWAP messages.

IV. Works in CAPWAP Protocol

A number of algorithms have been proposed within CAPWAP protocol to improve its reliability and performance. Previous works purpose to reduce roaming latency, optimize the wireless network resources and automate frequency planning. We classified the past works based on the main scope to three groups: Open Source CAPWAP implementation, frequency planning and roaming.

A. Open Source CAPWAP Implementation

First open source CAPWAP implementation was proposed in [20]. The authors presented some experimental tests to measure the performance of their CAPWAP implementation. They performed three sets of measurement of the time elapsed since WTP requests the association until the AC responses. These measurements include; the delay for the sender and the receiver to generate request and compute the answer, the delay for the configuration of IEEE 802.11e QoS MAC parameters on the WTP and the delay of echo request from the WTP to the AC. The results show that the association delay was 86.51 ms with 90% confidence interval of 4.81 ms. However, the presented open source does not implement the whole CAPWAP states. In addition, it does not support the Split MAC Architecture.

M. Bernaschi et al. in [21] provided a simple management architecture to solve some configuration problems. In particular, frequency planning problem, load balancing problem and automatic adoption of Wireless Multimedia (WMM) parameters. To solve the frequency planning problem, sub-optimal solution was proposed called Closest configuration. Each WTP in Random configuration randomly uses a channel of the set of allowed configuration channels while in Closet configuration the AC identifies the channel to use based on the power of beacons from WTPs. The evaluation proved that Closest configuration reduces the interference by almost 50% compared to Random configuration. On the other hand, Cell Breathing [22] was adopted to address load balancing problem. Cell Breathing idea is based on that stations chose to associate with WTP with highest power. Therefore, Cell Breathing algorithm increase the power of beacons sent by low loaded WTPs and decrease the power of beacons sent by high loaded WTPs. The evaluation result showed that Cell Breathing algorithm improves the load balancing by almost 20% comparing to fixed configuration.

The major drawback of using Cell Breathing is the possibility of coverage holes when a station becomes outside the beacon transmission range of all APs.

For automatic adoption of WMM parameters, the authors adapted the method presented in [23]. WTP sends periodically to the AC statistics about the length of sending queues for WMM. The WTP statistics are integrated with the throughput information available at the AC to control real-time traffic and set 802.11e MAC parameters in order to realize QoS goals. However, this method does not support streaming traffic account and IEEE 802.11b/g. Moreover, the algorithm needs about 50s to start Best Effort (BE) traffic which reduces the efficiency.

M. Bernaschi et al. in [24] developed their initial implementation of Open CAPWAP by extending its possibilities. Here, they added a mechanism to support generic external applications which are needed for CAPWAP protocol functionalities. This mechanism is based on adding an application management server to the Open CAPWAP AC daemon. In addition, the authors proposed and tested frequency planning solution called (*i*FP) for the Provincia di Roma network of WiFi Hot-Spot. The network interference metric corresponding to a channel assignment C is:

$$N_C(V) = \sum_{i=1}^{n} I_C\ (a_i)$$

I$_C$(*a*i) is the WTP interference metric corresponding to a channel assignment c where:

$$I_C(a_i) = \sum_{a_j \in v(a_i)}^{n} w_c(\ a_i\ , a_j)$$

w$_c$*(ai,aj)* is the weight metric where:

$$w_c\left(a_i, a_j\right) = \ s_i I\left(C(a_i), C\left(a_j\right)\right) P(a_i, a_j)$$

S*i* is the active mobile station number associated to WTP*ai*; *I(c(a*$_i$*),c(a*$_j$*))* is the interference factor between channel *c(a*$_i$*)* and *c(a*$_j$*)* and P(*a*$_i$,*a*$_j$) is the spatial WTPs distribution. The proposed frequency planning aims to minimize the network interference metric *Nc*. First, the WTPs are divided into different clusters corresponding to the neighborhood relationship. Then, each cluster optimizes its interference locally by finding for each managed WTP the channel assignment that minimizes the I$_C$(*a*i) value.

Finally, the best channel for a WTP is found which fixes the configuration of all other WTPs in the Hot-Spots network. The evaluation result showed that the average throughput is around 4.2 Mbps which is low.

B. Frequency Planning

A. Levanti et al. in [25] proposed automatic frequency planning to avoid transient channel adjustments and blocked cell phenomena problem. The blocked cell is interfered cell with two orthogonal cells that do not listen to each other where the throughput of interfered cell will reduce to zero. To address these problems, each WTP scans all channels periodically to identify all potential interference and sends a report to the AC. There were two ways to scan the channels. The first way is forwarding a specific field in the CAPWAP header contains beacon frames heard by the overlapping WTP/APs to AC.

The second way is encapsulating some message elements in a standard CAPWAP control frame to simultaneously signal all the interference heard from the WTP/APs. The interference metric that is used to define the overall interference is:

$$\sum_{i=1}^{N}\sum_{j=1}^{M}\left(N_{APi} + N_{APj}\right) I\left(ch_{APi}, ch_{APj}\right). P_{APi<-APj}$$

In the metric, N is the number of WTPs connected to the AC; M is the total number of WTPs and interfering APs in other network; N_{AP} is the number of contending stations in the WTP cell; ch_{APi} is the operative channel of the *i*-th AP/WTP; and $P_{APi<-APj}$ is the power received by the *i*-th WTP. The AC computes the interference metric for every frequency planning. The minimization heuristic solution was used to minimize the interference metric where different solutions can be found by changing the initial conditions. Each WTP channel is sequentially moved to the channel that minimizes the interference metric and all other APs stay on the current assignments. A planning cycle is concluded when the channels of all the WTPs in the network are updated. Finally, the AC selects minimum stable solution and sends the new operation channels to all WTPs through IEEE 802.11 Direct Sequence Control messages. Interfering matrix was used to determine the blocked cell position in order to move it to new channel. The evaluation result showed that throughputs for blind metric minimization and blocked cell in worst cases are 18.49 and 18.73 Mbps respectively. Despite that the throughput of the algorithms is high, other planning solutions have higher throughput in the range (40, 60) Mbps.

In [26], A. Levanti et al. used the algorithm in [27] to minimize other proposed interference metrics for frequency planning. Interfering matrix was defined where the network WTPs are the number of rows and number of columns represent the total number of interfering WTP/APs. Each element of the matrix is represented as:

$$A(l, m) = \ I(ch_l\ , ch_m). P_{ch_m}\ a(r_l, m)$$

Where, $A(l, m)$ is the interference among the *l*-th node and *m*-th source of interference. I(ch*l* , ch*m*) is the interference factor between channels *l* and *m*. P_{ch_m} is the power transmitted by the *m*-th interfering WTP/AP on channel $ch_m$and $a(r_l, m)$ is the power attenuation due to the distance between the *m*-th transmitter and the *l*-th receiver tuned on the same channel. The proposed interference metrics are total interference metric and maximum interference metric:

$$I_{TOT} = \sum_{l=1}^{N}\sum_{m=1}^{M} I(ch_l, ch_m). P_{ch_m}\ a(r_l, m)$$

$$I_{MAX} = \sum_{l=1}^{N} \begin{matrix} max \\ m = 1,2,..M \end{matrix} \quad I(ch_l, ch_m). P_{ch_m}\ a(r_l, m)$$

Here, N is the number of WTPs managed by the AC; M is the total number of WTPs and interfering APs in other networks; ch*l* is the operative channel of the *l*-th AP/WTP an ch*m* is the interfering channel of the *m*-th AP/WTP. The average throughput of the algorithm is 50 Mbps as appear in the simulation result. This algorithm is not aware of blocked cell problem where the throughput will be zero in such cell.

C. Roaming

In the roaming scope, B. Sariaya et al. in [16] presented CAPWAP handover protocol (CAPWAPHP) to reduce the authentication delay. For this purpose, the AC proactively transfers Authentication, Authorization and Accounting (AAA) context to neighboring WTPs to accelerate the MS roaming. Neighbor Graph (NG) was centrally kept at AC to identify the candidate WTPs which a roaming MS could tolerably reassociate to. Initially, the NG is an empty graph and is generated by observing the actual movement of the MS. The AAA server in IEEE802.11i was used as Authentication Server (AS). The AAA context contains pair-wise master key (PMK), User Name, filter id and login IP host. In first authentication process, PMK is generated at AS which is then transported to the WTP and the MS. When the MS moves to another WTP, another PMK should be derived from the previous WTP, e.g. original PMK taking into account MAC addresses of the MS and the new WTP. The operation of CAPWAPHP was presented via four scenarios; first-time association and re-association in Local MAC, and first-time association and re-association in Split MAC. In Local MAC, the first-time association starts when MS sends an 802.11 Association Request (ARq) to a desirable WTP to establish a layer 2connection which is forwarded to AC through Associate Mobile Request (ASRq). The AC responds with an Associate Mobile Replay (ASR) which is UDP packet contains all header and frame format fields. The WTP sends an Associate Response (AR) to the MS in order to execute 802.11i authentication phase. Sequentially, the AC sends AAA context to all neighbored WTPs of current WTP through Context Transfer Data (CTD) message, and sends Hoff-Notify (H-notify) message to non-neighbored WTPs to remove any stale association with MS. The second scenario is re-association of the MS when it moves out of current WTP. If the new WTP has the AAA context, it will authenticate itself to the MS. otherwise, the new WTP will send Handoff-Init (H-I) message to the AC to check the availability of any cached context. The AC gets the context from the previous WTP and its neighbors and sends it to the new WTP through Handoff-Init-Response (H-I-R) message. After the authentication is completed, the AC updates the WTPs by Context Transfer Clear (CTC) and CTD messages. For Split MAC, after the first time association the AC keeps the AAA context. So, the new WTP in re-association needs only to take the AAA context from AC and update the neighbored WTPs. The resulting authentication delay in local MAC and Split MAC was almost 26 ms comparing to 800 ms without context transfer. However, CAPWAPHP does not support seamless roaming where the minimum handoff delay was 59 ms. The NG also is not efficient during the initial NG building phase. Moreover, multiple AC will increase fault tolerance and reliability of the system. The measurement of the handoff latency for layer 2 and layer 3 was performed by [17]. In layer 2 roaming (Intra-domain) setup, the IEEE 802.11i standard was used which include pre-authentication feature. By listening to beacon messages, a Mobile Station (MS) identifies about the candidate WTP that can associate with. When the MS decides to roam, it sends Extensible Authentication Protocol (EAP) messages to the candidate WTP.

The receiving WTP stores this pre-authentication information using Pair-wise Master Key (PMK) Caching, enabling the station and the WTP to establish all required encryption keys. So, the MS can complete its authentication before it initiates the roam. In layer 3 roaming (Inter-domain), the MS requires a new IP address. ACs are configured to be peer of each other and they share information using A Generic Routing Encapsulation Tunnel (GRE). Therefore, ACs can share the WTP and MS information, which allow forwarding of the switching table. When the MS moves to another WTP, the AC detects the home VLAN and tunnels traffic to the home AC that allows seamless handover in a new network. The result appeared that the average handoff latency for real-time video streaming in layer 2 and layer 3 was 316 ms and 386 ms respectively. To achieve seamless roaming for real time application, the handoff latency must be less than 50 ms. Therefore, a new seamless roaming protocol must be proposed. Table1 summarized the works in CAPWAP protocol.

TABLE I
SUMMARY OF WORKS IN CAPWAP PROTOCOL

Ref.	Scope	Contribution	Limitation
20	Open Source CAPWAP protocol implementation	First open source CAPWAP implementation	Does not implement the whole CAPWAP states, Does not support the Split MAC Architecture
21	Open Source CAPWAP implementation , Frequency planning, Load balancing, and QoS	Reduces the interference, Improves the load balancing, Realize QoS goals	Low throughput, Possibility of coverage holes, Does not support streaming traffic account
24	improve open source CAPWAP, Frequency planning	Support generic external applications	low throughput
25	Frequency planning	High throughput	Blocked cell problem
26	Frequency planning,	Addresses blocked cell problem	Low throughput
16	Roaming	Reduces Reauthentication latency	Does not support seamless roaming, Not efficient during the initial NG building phase
17	Roaming	Evaluation for layer2 and layer3 handover	Not open-source

V. LAYER 2 ROAMING PROCEDURES IN CAPWAP ARCHITECTURE

IEEE 802.11 based on WLAN is the most popular technology for wireless connection. However, due to a short transmission range of WTP, roaming frequently occurs to MS to change WTP. This section explores the roaming procedures in Local MAC and Split MAC.

The roaming process is divided into three phases: Scanning, Re-authentication/Re-association and 802.11i Re-authentication. The main components of roaming latency are Scanning and 802.11i Re-authentication phases [2].

A. Scanning Phase

When the Received Signal Strength (RSS) of the current WTP degraded below the threshold, the MS needs to find the candidate WTPs to associate with. This is completed by MAC layer via scanning function. There are two kinds of scanning process: active and passive. The active scan is based on sending probe request frames by the MS. WTP processes the received probe request message and replies with a probe response message. The MS collects WTPs' information and selects the next WTP to associate with. In the passive scan, MS listens to beacon frames which are periodically sent by WTPs. The MS then chooses the next WTP by using the information obtained by the beacon frames. The Scanning phase in both Local and split MAC architectures resides on WTP. WTP generates the beacon frames and responds to Probe Request frame with a corresponding Probe Response frame. The difference between the two architectures is that the probe request in Split MAC is forwarded to the AC for optional processing.

B. Re-authentication/Re-association Phase

The Re-authentication phase is a transfer of MS's credentials from the old WTP to new WTP which may accept or reject the identity of the MS. After successful authentication the MS sends a re-association request frame to the new WTP.

In Local MAC, when the MS sends authentication request, the WTP accepts or rejects the MS through authentication response frame. Then, The WTP responds with association response frame and forwards the authentication and association frames to the AC. In split MAC, due to that the AC is responsible for responding to the MS, the WTP forward the authentication and association frames to the AC.

C. 802.11i Re-authentication Phase

The standard IEEE802.11i can be used to improve the access control security. Once the association is completed, 802.11i authenticates MS by 802.1x and EAP-TLS. In both Split and Local MAC, the AC transmits a station configuration request message involving add station with the flag field 'A' bit set. Then, the WTP forwards the all IEEE 802.1x and IEEE 802.11 key exchange messages to the AC for processing.

The MS secure roaming example was provided in [28] with considering that crypto service is provided by the WTP.

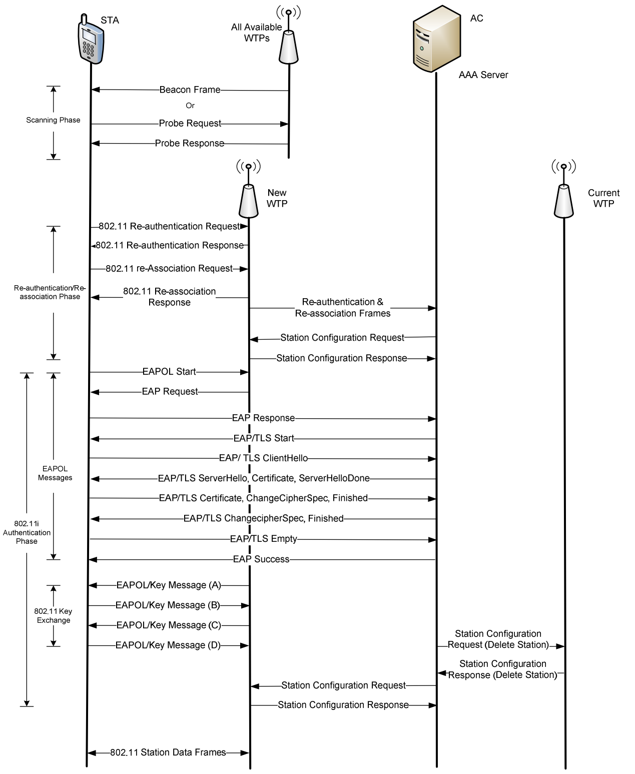
STA
All Available WTPs
AC
AAA Server
Scanning Phase
Beacon Frame
Or
Probe Request
Probe Response
New WTP
Current WTP
Re-authentication/Re-association Phase
802.11 Re-authentication Request
802.11 Re-authentication Response
802.11 re-Association Request
802.11 Re-association Response
Re-authentication & Re-association Frames
Station Configuration Request
Station Configuration Response
EAPOL Messages
802.11i Authentication Phase
EAPOL Start
EAP Request
EAP Response
EAP/TLS Start
EAP/ TLS ClientHello
EAP/TLS ServerHello, Certificate, ServerHelloDone
EAP/TLS Certificate, ChangeCipherSpec, Finished
EAP/TLS ChangecipherSpec, Finished
EAP/TLS Empty
EAP Success
802.11 Key Exchange
EAPOL/Key Message (A)
EAPOL/Key Message (B)
EAPOL/Key Message (C)
EAPOL/Key Message (D)
Station Configuration Request (Delete Station)
Station Configuration Response (Delete Station)
Station Configuration Request
Station Configuration Response
802.11 Station Data Frames

Fig. 3 MS roaming example in CAPWAP Centralized Architecture

VI. PERSPECTIVE ON SEAMLESS MOBILITY SUPPORT IN FUTURE CAPWAP ARCHITECTURE

The seamless mobility is one of the most critical issues in wireless network, including CAPWAP architecture. Recently, running realtime applications on top WLAN is widely grown. This presses vendors to support the seamless roaming. However, the aforementioned works on roaming have not realized the seamless mobility. In this section, we present important considerations for layer 2 seamless roaming supporting in CAPWAP architecture. These considerations will reduce the main roaming delay components – scanning and authentication – and improve the roaming efficiency.

A. Predictive Scheme

Next WTP prediction is the best way to skip or at least reduce the handoff delay components. In CAPWAP Architecture, this may be done if the AC could estimate and pre-authenticate the potential WTPs before triggering the handoff process. In fact, CAPWAP binding includes IEEE 802.11 info message [28], which is optional header encapsulated with data messages, contains radio and PHY-specific information. These information are Received Signal Strength Indication (RSSI), Signal to Noise Ratio (SNR) and Data Rate. Such information can be used to decide the handoff process start and the candidate WTP in order to override scan latency.

In addition, employing AAA server in IEEE802.11i to pre-authenticate the candidate WTPs will reduce the Re-authentication latency.

B. Intelligent Decision

The intelligent decision is based on considering additional parameters to detect next WTP such as congestion status, channels quality and traffic flows. The CAPWAP protocol was proposed for monitoring purposes, and such information is available in IEEE 802.11 statistics message element [28]. Therefore, the AC could request this statistics message in order to make centralized intelligent roaming decision.

C. Multi-ACs Roaming Support

In order to increase roaming reliability and its fault tolerance, the multi-ACs roaming must be supported. As mentioned in [17] the ACs can exchange their messages through Generic Routing Encapsulation (GRE) tunnel. This will give the ability for multi-ACs roaming.

D. Independence

Any modification in AC to support seamless roaming must not require modification in WTP and vice versa. This is to ensure that the modification does not hamper the CAPWAP operation. In other words, seamless roaming scheme should not affect the independence of device modification.

E. Flexibility

Roaming scheme must be compatible with both local and split MAC WTPs. This is to ensure that AC has sufficient flexibility in selecting next WTP.

VII. Conclusion and Future Work

In this paper, we presented an overview of centralized CAPWAP architectural and CAPWAP protocol along with its proposals that have emerged. Last section suggested important design considerations for mobility support in future IEEE 802.11 networks. The previous works in roaming do not achieve the realtime applications' condition. Additionally, they are not sufficient during the initial period of the network. Therefore, a new scheme must be proposed to support CAPWAP seamless roaming. In our future work, we will present CAPWAP predictive centralized scheme to enable seamless roaming in a secured network.

References

[1] B. O'Hara al, P. Calhoun and PJ. Kempf, RFC 3990,"Configuration and Provisioning for Wireless Access Points (CAPWAP), Problem Statement", IETF, February 2005.

[2] W. A. Arunesh Mishra and Minho Shin, "An empirical analysis of the ieee 802.11 mac layer handoff process," ACM SIGCOMM Computer Communication Review, vol. 33, no. 2, pp. 93–102, April 2003.

[3] M. Shin, A. Mishra and W. A. Arbaugh, "Improving the latency of 802.11 Hand-offs using Neighbor Graph," In Proceedings of the 2nd international conference on Mobile systems, applications, and services, pp. 70-83. ACM, New York, USA, 2004.

[4] L. Ravindranath, F. Prashanth, L. Prasath, P. Durairaj and A. Siromoney: "Improving the Latency of 802.11 Handoffs using Sentinel based Architecture," In Proceedings of HiPC 2005 (Posters), Goa, India, December 2005.

[5] R. Khan, S. Aissa and C. Despins, "MAC layer handoff algorithm for IEEE 802.11 wireless networks," Computers and Communications, 2009. ISCC 2009. IEEE Symposium on Advanced Communication Technology, vol., no., pp.687-692, 5-8 July 2009

[6] C. Lee, S. Seo and J. Song, "An Indoor Tracking-based Handoff Mechanism for VoIP Applications in IEEE 802.11 WLANs," Information and Automation for Sustainability, 2008. ICIAFS 2008. 4th International Conference on , vol., no., pp.324-329, 12-14 Dec. 2008

[7] V. M. Chintala and Qing-An Zeng, "Novel MAC Layer Handoff Schemes for IEEE 802.11 Wireless LANs," Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE, vol., no., pp.4435-4440, 11-15 March 2007.

[8] K. Kwon and C. Lee, "A fast handoff algorithm using intelligent channel scan for IEEE 802.11 WLANs," Advanced Communication Technology, 2004. The 6th International Conference on Advanced Communication Technology, vol.1, no., pp. 46- 50, 2004.

[9] H. Velayos and G. Karlsson, "Techniques to reduce the IEEE 802.11b handoff time," Communications, 2004 IEEE International Conference on Advanced Communication Technology, vol.7, no., pp. 3844- 3848 Vol.7, 20-24 June 2004.

[10] K. Ramachandran, S. Rangarajan and J.C. Lin, "Make-Before-Break MAC Layer Handoff in 802.11 Wireless Networks," Communications, 2006. ICC '06. IEEE International Conference on, vol.10, no., pp.4818-4823, June 2006.

[11] Q. Hong-yan, C. Bing and Q. Xiao-lin, "A Dual-Soft-Handoff Scheme for Fast Seamless Roaming in WLAN," Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on , vol.2, no., pp.97-100, 24-25 April 2010

[12] V. Brik, A. Mishra and S. Banerjee, "Eliminating handoff latencies in 802.11 WLANs using Multiple Radios: Applications, Experience, and Evaluation," In proceeding IMC '05 Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement, USA, 2005.

[13] A. Mishra, M. Shin and W.A. Arbaush, "Context caching using neighbor graphs for fast handoffs in a wireless network," INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies , vol.1, no., pp. 4 vol. (xxxv+2866), 7-11 March 2004.

[14] A. Mishra, M. Shin and N.L. Petroni, Arbaugh, "Proactive key distribution using neighbor graphs," Wireless Communications, IEEE , vol.11, no.1, pp. 26- 36, Feb 2004.

[15] S. Pack and Y. Choi, "Fast handoff scheme based on mobility prediction in public wireless LAN systems," Communications, IEE Proceedings- , vol.151, no.5, pp. 489- 495, 24 Oct. 2004.

[16] B. Sarikaya and Xiao Zheng, "CAPWAP Handover Protocol," Communications, 2006. ICC '06. IEEE International Conference on , vol.4, no., pp.1933-1938, June 2006.

[17] M. A. Amin, K. Abu Bakar, A. Abdullah and R. H. Khokhar, "Handover Latency Measurement using Variant of Capwap Protocol" , Network Protocols and Algorithms ISSN 1943-3581 , Vol. 3, No. 2, 2011.

[18] L. Yang, P. Zerfos and E. Sadot, RFC4118, "Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)", IETF, June 2005.

[19] P. Calhoun, M. Montemurro and D. Stanley,RFC 5415, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", IETF, March 2009.

[20] M. Bernaschi, F. Cacace, G. Iannello, M. Vellucci and L. Vollero, "OpenCAPWAP: an open-source CAPWAP implementation for management and QoS support," Telecommunication Networking Workshop on QoS in Multiservice IP Networks, 2008. IT-NEWS 2008. 4th International, vol., no., pp.72-77, 13-15 Feb. 2008.

[21] M. Bernaschi, F. Cacace, G. Iannello, M. Vellucci and L. Vollero, "OpenCAPWAP: An open source CAPWAP implementation for the management and configuration of WiFi hot-spots", presented at Computer Networks, 2009, pp.217-230.

[22] Y. Bejeranoa and S.-J. Han, "Cell breathing techniques for balancing the access point load in wireless LANs," in: Proceedings of Infocom, 2006.

[23] F. Cacace, G. Iannello, M. Vellucci and L. Vollero, "A reactive approach to QoS Provisioning in IEEE 802.11e WLANs", in: Proceedings of 4th EURO-NGI Conference on Next Generation Internet Networks, Krakow, Poland, April 2008.

[24] M. Bernaschi, F. Cacace, A. Davoli, D. Guerri, M. Latini and L. Vollero, "A CAPWAP-based solution for frequency planning in large scale networks of WiFi Hot-Spots", Computer Communications, Volume 34, Issue 11, 15 July 2011, Pages 1283-1293.

[25] A. Levanti, F. Giordano and I. Tinnirello, "A CAPWAP Architecture for Automatic Frequency Planning in WLAN," Computers and Communications, 2007. ISCC 2007. 12th IEEE Symposium on , vol., no., pp.MW-51-MW-56, 1-4 July 2007.

[26] A. Levanti, F. Giordano and I. Tinnirello, "A CAPWAP-Compliant Solution for Radio Resource Management in Large-Scale 802.11

WLAN," Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE, vol., no., pp.3645-3650, 26-30 Nov. 2007.

[27] A. Mishra, S. Banerjee, and W. Arbaugh, "Using Partially Overlapped Channels in Wireless Meshes", in IEEE Infocom, 2005.

[28] P. Calhoun, M. Montemurro and D. Stanley, RFC 5416 , "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11" , 2009.