Creation, Management and Migration of Virtual Access Points in Software Defined WLAN

You-En Lin* and Ting-Ming Tsai*
*Information & Communications Research Laboratories
Industrial Technology Research Institue
Hsinchu, Taiwan 103
Email: You-En.Lin@itri.org.tw

Abstract—**The demand of mobile wireless communication increases year by year. To satisfy the demand, multiple radio techniques (RATs) are suggested to be integrated in the next generation wireless communication system, i.e. 5G. Wi-Fi is one candidate RAT but the anarchy of access points of Wi-Fi degrades the network performance. Software-defined wireless local area network (WLAN) built atop virtual access points is proposed to increase the flexibility of network planning and address the poor performance of conventional WLAN. However, there is still a gap between the concept of software-defined WLAN and its implementation. In this paper, we intend to eliminate the gap and dig deeper into the implementation. A series of procedures for creation, management and migration of virtual access points is proposed. Since these procedures are for access points and follow the standard of IEEE 802.11, no modification of user equipment is required. Through case study, we show that the proposal outperforms conventional WLAN.**

I. Introduction

The demand of wireless access network massively increased in recent ten years because the popularity of personal mobile/wearable devices, and there are more and more cloud services which demands for higher throughput and lower latency [1], such as virtual reality of conferences, exhibitions and concert over wearable devices. METIS is a European project for developing the next generation of mobile and wireless communication, i.e. the 5G system [2]. A use case in METIS is that a four-day open-air music festival is held in a rural area less than one square kilometer. This event may bring at least 100,000 visitors, and most of them would desire for wireless access networks for various Internet services, such as recording high-definition video and sharing the video with friends on social networks. Furthermore, staffs of the music festival as well as security personnel, medical personnel and related equipment are dependent on wireless access networks and reliable communications.

Nevertheless, the technology of existing wireless access network is not affordable for such scenarios of high density and high demand of Internet services. In the next generation of mobile and wireless communication, it is a trend to integrate multiple radio access technologies, called Multi-RAT [3]. Wireless Local Area Network (WLAN), or say Wi-Fi, has been very popular in digital home and digital office for years. Thus, Wi-Fi is one of radio access technologies that are highly desired to be integrated into the next generation of wireless communication system. Through the integration of wireless local area network, signal-dead zones of traditional cellular mobile networks can reduce, while the flow of data packets can be dispatched to another radio band so that faster packet service become possible.

There are many challenges to integrate WLAN into the next generation of wireless communication system since the original goal and design of WLAN. As its name, WLAN is originally designed for local area usage, such as homes or small offices, and it is not for wide area deployment. Everyone can buy an access point of WLAN and set up its name, operating channel and security password. Afterword, the access point can operate on line and provide the service of network accessing. Basically, existing WLAN access points are deployed in a manner of decentralized management. Each access point requires manpower to login and change its configuration. In this way, neighboring access points are impossible to automatically coordinate with each other and change the configuration of itself to adaptive to the dynamic environment of wireless networks. Therefore, as the density of access points increase, the existing WLAN has several uncomfortable problems for users. For examples, the latency to connect with an accessible access point is too long, or even there is no connection. When users move, the connection often breaks and requires users to select another accessible access point and pass the authentication. In summary, the problems of existing WLAN are as

1) **Poor load balance**: In existing WLAN, there is no way to dispatch users among different access points in the view of the whole network. Users select an access point by its signal strength. Therefore, it is possible that many users connect with the same access power with the strongest signal strength and each user can only have low throughput or even loss the connection because of overloading.
2) **Co-channel interference**: When an access point of WLAN is deployed by a user, the operating channel is usually set by the preference of the user or randomly selected. In the view of the whole WLAN, there is no way to automatically change the operating channel and adapt to the usage of radio spectrum. Therefore, co-channel interference often occurs when neighbor access points select the same operating channel. The co-channel

978-1-4673-8350-9/15 $31.00 © 2015 IEEE
DOI 10.1109/CCBD.2015.61

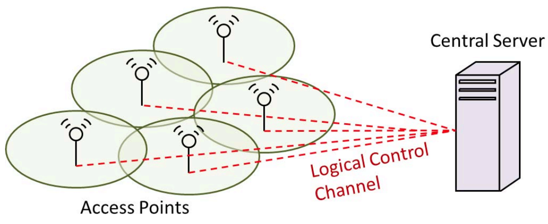

Figure 1. A central server control multiple physical access points through a logical channel.

interference reduces the signal quality and causes lower throughput.

3) **Poor mobility support**: In existing WLAN, access points work independently because of the restriction of the logical link control layer and the boundary of the physical layer. Before users connect with a new access point, user station (equipment) has to scan channel to find out available access points and then execute the procedures of authentication and association. These procedures cannot be reduced so that that is why the latency of handover of WLAN is so long to break down the connection of some cloud services.

In order to improve the performance of WLAN under high-density scenarios, as well as being the pavement of Multi-RAT technology in the next generation of wireless communication system, we extend the concept of Software-Defined Network (SDN) into the area of WLAN. As shown in Figure 1, access points in WLAN are connected to a centralized server through a logical control channel which can be implemented through any existing communication techniques, such as Ethernet or Asymmetric Digital Subscriber Line (ADSL). The server can eliminates the above issues under the high-density scenario through the creation, management and migration of virtual access points (VAPs) on physical access points in the network.

This paper is organized as the follows. Related work is surveyed in Section II. The management of user accounts and network entry is presented in Section III. Additionally, the procedure of creating virtual access points for end users is defined. In Section IV, the procedures for managing the created virtual access points are defined, including channel switching, multiplexing and migration of virtual access points. Several use cases are studied to show the benefits of the proposal in Section V. Finally, Section VI concludes the paper.

II. Related Work

There has been some work try to utilize SDN to increase the performance of routing in Wireless Mesh Networks (WMN). Authors in [4] propose to integrate SDN principles in WMN formed by OpenFlow switches. SDN is originally developed from wired networks and a centralized controller to deploy fine-grained traffic in networks. However, some properties of wireless mesh networks are different from wired networks. It is not rare that nodes in WMN may become isolated and the network is fragmented. To exploit the pros and mitigate the cons, the framework proposed in [4] uses a centralized controller of traditional OpenFlow for the routing of data. Meanwhile, there is another distributed controller for routing the control message of OpenFlow itself and data traffic in the case of central controller failure.

SDN is as a tool to optimizing data flows between routers in a centralized manner. Meanwhile, the management of wireless radio resources and infrastructure also important as well as the routing paths. Therefore, there has been some work that investigates a centralized management of infrastructure resources [5], [6]. A better deployment of access points helps mitigating co-channel interference and balancing the load between access points. Authors in [5] propose to utilize virtual access points (VAPs) to increase the flexibility of deployment of physical access points. VAP is a logical access point that is constructed by virtualization technique [7]. Physical hardware resources are divided by virtualization and shared by different virtual machines so that each VAP and independently operates and keep its own configuration for different services of wireless networks. There has been an implementation and demo of virtual access point [6]. Since the advantage of virtual machine can lively migrate between different physical resources, VAPs can lively migrate between different physical access points and that helps the flexibility of network planning [5].

Motility and handover cause disconnection in existing WLAN as aforementioned. Authors in [8], [9] propose to utilize virtual access points to improve the performance of handover in WLAN. In their scheme, access points are operating in the same channel so that mobile stations are not necessary to scan channels for discovering a new access point. Hence, the handover latency between physical access points reduces. In addition, the authors let all the complexity be pushed back inside the network so that mobile stations are not aware that they move. However, this scheme has a drawback of co-channel interference because all access points are operating in the same channel. The co-channel interference becomes serious when the density of access points increases. Latter, the authors in [10] propose an advanced version of work [8]. Access points can be deployed with multiple operating channels, and thus the problem of co-channel interference is mitigated. Nevertheless, multiple operating channels reveal new issues. Stations cannot handover to neighbor access points if they do not know the operating channel. To address this issue, the authors in [10] propose a network-assisted manner that let neighbor access points change the operating channel and pick up a mobile station from the serving access point to a target access point.

Although here has some work that integrates the concept of SDN into wireless mesh network [4] and utilizes virtual access points to increase flexibility of network planning [5], [6], [9] or mobility [8], [10], there is still a gap between the concept and the implementation, e.g. the limitation of the WLAN protocol when switching VAPs. In this paper, we want to dig deeper into the implementation about the message flows of creation, management and mobility of virtual access points basing on the WLAN protocol.

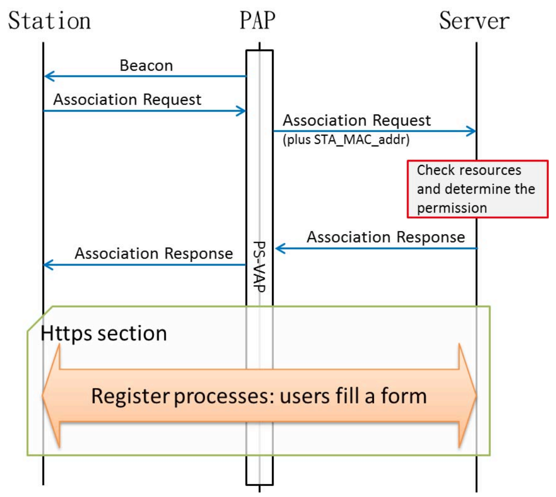

Figure 2. User association with a PS-VAP is managed by the server. User can use a PS-VAP to register with the server.

III. Network Entry and Creation of VAP

This section illustrates the management of network entry of users and the creation of corresponding virtual access points.

A. Network Scenario

A network topology is shown as Figure 1. Assume that an area has been densely covered by multiple physical access points (PAPs) of IEEE 802.11. Coverage of PAPs overlaps with each other. These PAPs are control by a central server through a logical control channel which can be implemented by a network socket.

B. Management of Network Accessing and User Account

In order to control the load balance of physical access points and the whole wireless network, network accessing permission of users is managed by the central server. We classified users into two types: unregistered users and registered users. For unregistered users, they can only access a Public and Static Virtual Access Point (PS-VAP). For registered users, the central server would construct a Dedicated and Dynamic Virtual Access Point (DD-VAP) to serve them.

The procedures of an user station entering a WLAN are roughly divided into three phases: channel scanning, authentication and association [11]. PS-VAP is without authentication password and opens for unregistered/registered users while PS-VAP is limit for network accessing. Association permission is granted by the central server instead of by access points. For the network entry of registered users, the server would create a DD-VAP for the user. The details are illustrated in Section III-D.

Since the association permission is granted by the central server, some permission rules can be implemented on the server. In one embodiment, the server finds that the resource of the network is now only allowable for N unregistered users. When an unregistered user gets association permission, the server decreases the available accounts by one until empty. Afterwards, no further unregistered users can get permission into the system.

The message flow chart of network entry through a PS-VAP is shown in the first six steps in Figure 2. When a user wants to access network through a PS-VAP, the user station sends an association request to a PS-VAP which it hears beacons from. If a PS-VAP receives an association request, the PS-VAP does not make a decision of permission by itself. The PS-VAP would relay the attempt which includes the MAC (Medium Access Control) address of the user station to the central server. The server checks the current loading of the network and determines whether the unregistered user is allowed to enter the network or not. If the user is allowed, the server would log the user and reduces the available resources by one unit. If the available resources for unregistered users run out, the server will reject new unregistered users. The PS-VAP forwards the association reply to the user when network entry is admitted. Otherwise, the PS-VAP would not reply to the user.

The procedure of user registration can be done through any communication method with the server, e.g. through wired or wireless networks. An example is shown in Figure 2. An unregistered user can become a registered user by using a PS-VAP. The procedure is as follows. An unregistered user first connects with a PS-VAP so that the user can get limited network access and creates a communication section with the central server, e.g. through https. Once the user can have a communication section with the server, the user can execute registration with the server and become a registered user.

The account and profile of a registered user is maintained by the central server. The user profile includes the SSID, the authentication method and key, QoS requirement and other preferred settings that are required for the creation of DD-VAP of the user. Hence, when a user wants to register an account, the user has to provide its equipment MAC address and a desired SSID of the DD-VAP at least. The server uses the MAC address and SSID to generate the key to access its database and also generate the Basic Service Set Identification (BSSID) of the DD-VAP of the user. In one embodiment, the generated BSSID would be the MAC address of the DD-VAP when communicating with the user.

C. Creation of Public and Static VAP

Public and static VAPs (PS-VAPs) are used for network entry of unregistered and registered users. This section presents the procedures and the timing of the creation of PS-VAPs. A program and/or firmware in a PAP are installed such that the PAP would send a request to the central server when the PAP powers on, as shown in Figure 3. The central server replies a basic configuration to the PAP, i.e. PS-VAP profile. The PS-VAP profile includes the Service Set Identifier (SSID) and the operating channel. The PAP can create a VAP based on the PS-VAP profile. The created VAP could be open access and public to any user without authentication. Since this kind of created VAPs is the first created VAP on a PAP and keeps alive

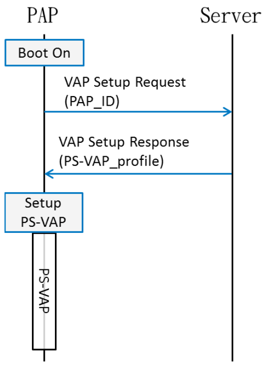

Figure 3. When a PAP boots, it sends a VAP setup request to the server and gets a profile to create a PS-VAP

until the PAP is powers off, this kind of VAPs is named Public and Static VAP (PS-VAP). The central server assigns the same SSID and operating channel for all PS-VAPs so that users at anywhere of the coverage of PAPs can directly hear one PS-VAP at least and have no necessary to scan channels for a specific SSID. The channel that PS-VAPs operate is named as the control channel latter compared to the channels used by other VAPs.

D. Creation of Dedicated and Dynamic VAP

Dedicated and dynamic VAP (DD-VAP) is a virtual access point that is created on a PAP and is dedicated to a user when the user requires. The procedure for a user to create a DD-VAP is shown as Figure 4.

When a registered user wants to access the network, it would listen on the control channel and wait for beacon of a PS-VAP. If the user hears a beacon of PS-VAP, it knows that is an available PS-VAP. The user sends a Probe Request that contains the registered SSID and its ID, for example MAC address. A PS-VAP does not determine whether to reply the Probe Request by itself. Alternatively, a PAP would forward the request to the server by sending a VAP Setup Request which contains the station ID, SSID and the PAP ID at least. The server checks whether the user is a valid registered user by using the station ID and SSID. If the user is a valid user, the server reads the user profile (QoS requirement) and check whether the current resources of the PAP is enough to support the user. If yes, the server replies a VAP Setup Response that contains the user profile to the PAP. The PS-VAP sends the Probe Reply to the user. The PAP creates the DD-VAP for the user by using the profile provided by the server. The user proceeds to authentication, association and data transmission with the created DD-VAP. During the authentication, the DD-VAP is a relay node. The real authentication processes is done with the server. In one embodiment, the private profile of the user is not clone to the DD-VAP.

Notice that DD-VAP is dynamically created and dedicated to one user. Creating VAPs on a commercial PAP is available on the existing market while the creation of VAPs is relatively

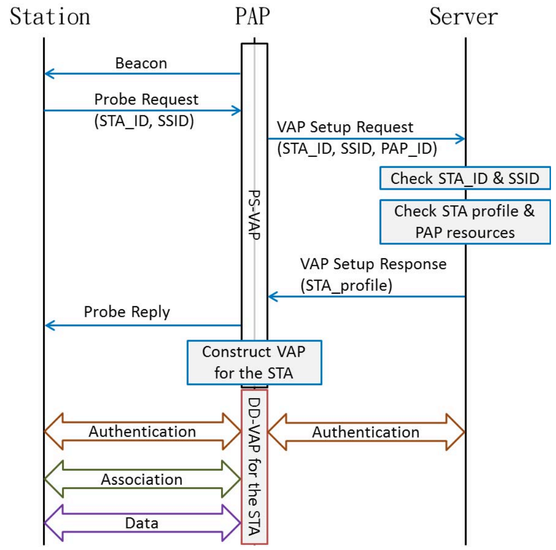

Figure 4. Creation of Dedicated and Dynamic VAP for a registered user

static and configured by manpower. Hence, these conventional VAPs are idle and waiting for serving users. That causes much overhead when the number of VAPs increases. That is why the number of VAPs supported by conventional PAPs is limited and cannot be dedicated and customized to each user's preference.

IV. Management of VAP

DD-VAPs are responsible for the main part of data transmission of a registered user. To improve the performance of the whole wireless network, the management of DD-VAP is important and essential. In this section, we define the procedures of management, including measurement, reconfiguration, channel switching and user data protection.

A. Measurement and Reconfiguration

DD-VAPs are managed by the central server. The management could be done through two kinds of commands: Measurement and Reconfiguration. The procedure of measurement is used for the server to ask DD-VAPs measure some information that the server requires for making decisions. Once decisions are made, the procedure of reconfiguration is used for the server to change the configuration of DD-VAPs.

Figure 5 shows an instance of managing a DD-VAP through Measurement and Reconfiguration commands. The server uses Status Request which contains a profile for a DD-VAP and/or the corresponding user station to measure the channel status. A measurement profile contains the channels to be measured and measurement items, such as background noise, interference and packet loss rates. If the Status Request contains the parts that require the user station to cooperate, or the DD-VAP does not have the queried data, the DD-VAP sends a Measurement Request to the user station. The format of the Measurement Request can follow the existing messages in IEEE 802.11 [11]

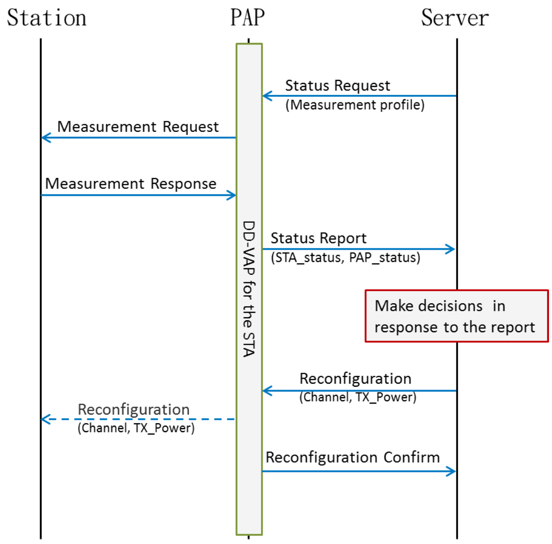

Figure 5. The server uses Measurement and Reconfiguration commands to manage DD-VAPs.

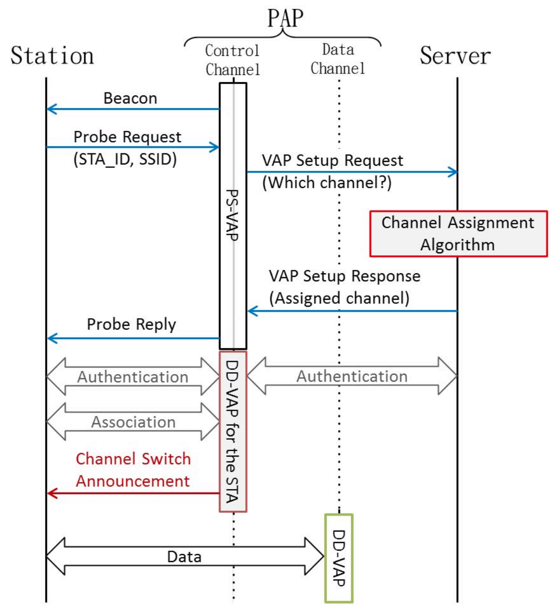

Figure 6. Switching the operating channel when the server setups a DD-VAP

so that the user station does not require any modification. The Measurement Response from the station does, too. After the DD-VAP collects the queried data, the DD-VAP sends the Status Report to the server, including the status from the user station and the PAP that the DD-VAP resides on.

The server can know the radio environment through Measurement commands and then use the information to make a proper decision. The aim is to optimize the network performance through algorithms in related work [12]. The server sends a Reconfiguration command to a DD-VAP. The Reconfiguration contains the made decision, such as changing the operating channel or adjusting transmission power. If the Reconfiguration contains the parts for the user station, the DD-VAP forwards the message to the user station. The DD-VAP replies a Reconfiguration Confirm after the new setting is executed.

B. Channel Switch

To address the issue of multiple DD-VAPs congesting on the same channel and co-channel interference to each other, the operating channel of a DD-VAP can be assigned by the server when the DD-VAP is created initially or the DD-VAP is operating.

Figure 6 shows the case when channel assignment is executed during the creation of a DD-VAP. When a DD-VAP is operating, channel switch can be done through the comments of Measurement and Reconfiguration as stated in Section IV-A and Figure 5.

In Figure 6, when a station sends a Probe Request to a PS-VAP, the PS-VAP sends a VAP Setup Request which contains a query of channel assignment. When the server receives the query of channel assignment, the server executes a channel assignment algorithm [12] that considers both the operating channel and operating timing of neighbor DD-VAPs. After an operating channel is determined, the server notifies the PS-VAP through the VAP Setup Response. Initially, the DD-VAP for the user is still created on the control channel which the PS-VAP operates. After the procedure of association is done, the DD-VAP uses the Channel Switch Announcement (CSA) in a Beacon to notify the user of the channel switch. For the case when a DD-VAP is operating, the event of channel switch is also notified through the CSA in a Beacon.

The CSA is a standard message in the IEEE 802.11 Beacon message [11]. Thus, no modification of user station is required. Notice that the CSA is a broadcast message so that all stations associated with the access point would switch the operating channel. Since a DD-VAP is dedicated to one user, the proposed system can achieve the channel switch of a specific user by switching the operating channel of its DD-VAP.

C. Multiplexing VAPs and User Protection

In a normal case, a PAP has to serve multiple users. Hence, there are multiple DD-VAPs created on one PAP. These DD-VAPs possibly operate on different channels. When a PAP plays different DD-VAPs, the PAP has to switch between channels. In other words, a user sometimes cannot physically connect with its DD-VAP. Data may be lost if a user sends data while the PAP is interleaving for playing the DD-VAP of other users. We propose the following mechanism to address this issue.

We redefine the usage of the message “CTS-to-Self” in IEEE 802.11 [11] at the side of access points. No modification is required at the user side. Before a PAP plays another DD-VAP and changes the operating channel, the PAP has to send

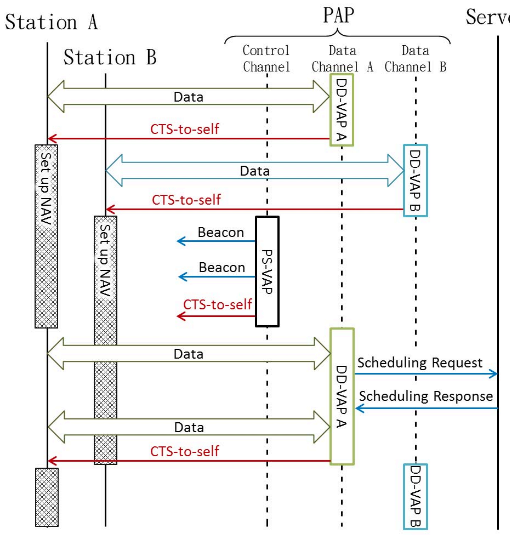

Figure 7. User protection when a PAP switches to another channel and plays another DD-VAP

out the message "CTS-to-Self". The destination of CTS-to-Self is the MAC address of the DD-VAP. The CTS-to-Self contains a NAV (Network Allocation Vector) that specifies how long the DD-VAP is busy. In other words, the NAV describes the duration that the DD-VAP is interleaving for other channels and not available for this user. When the user receives CTS-to-Self, the user sets up a timer as long as the NAV. The user keeps silent and defers transmissions until the timer expires.

Figure 7 shows an example of a PAP playing three VAPs, including a PS-VAP, a DD-VAP for Station A and a DD-VAP for Station B. A CTS-to-Self is sent by the PAP before the PAP jumps to other channels. In the view of Station A, the NAV timer is set as long as its DD-VAP leaves for other services, including playing as a PS-VAP and the DD-VAP of Station B.

The time resource of a PAP is shared by all VAPs created on the PAP. The time ratio that a VAP can use is scheduled by the central server so that channel congestion and co-channel interference between neighbor VAPs is minimized as much as possible. If a DD-VAP or the corresponding station (e.g. Station A in Figure 7) has more data to send, the DD-VAP can send a Scheduling Request to the server. In one embodiment, the Scheduling Request implies the increase/decrease of the time ratio of a VAP and asks the server to re-optimize the schedule of VAPs.

D. Migration of DD-VAP

When a user moves in a conventional WLAN, the user may experience disconnection since the user station has to scanning all possible channels for an available access point and then proceeds to authentication, association and data transmission. The latency is so long for the user station sending/receiving data again and thus it cause disconnection of applications. We address this issue by cloning and moving the DD-VAP of a user such that the user going to anywhere still connects with the same access point and could not be aware of movement and handover.

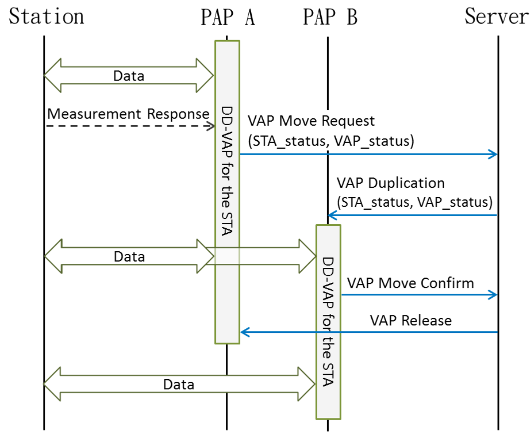

Figure 8. The server copies and moves the DD-VAP of the user when the user moves between different PAPs.

The procedure of moving a DD-VAP between different PAPs is shown as Figure 8. Assume that a station is connecting with PAP A. The DD-VAP for the station can be aware of the signal quality between itself and the station through data transmission and acknowledgment. If data transmission is not frequent, the DD-VAP can also get the channel status through Measurement commands as stated in Section IV-A.

If the DD-VAP finds that the station may leave the coverage of the PAP A, the DD-VAP sends a VAP Move Request to the server. The VAP Move Request contains the station status, VAP status and other enough information for the server to determine one or several possible target PAPs. For instance, PAP B is selected by the server as a target PAP, and the server sends a VAP Duplication message to PAP B. The VAP Duplication contains the current context of the DD-VAP on PAP A, including BSSID, the operating channel and timing, frame sequence number, acknowledgment status and others.

PAP B follows the VAP Duplication message and creates a clone DD-VAP of the station. Afterwards, there are two the same DD-VAP on the same channel at the same time. Data to/from the station are sent/received by both DD-VAPs. The upper layers (for example TCP or UDP) could discard duplicated packets for application layers. The DD-VAP on PAP B continues to monitor the status of the station either through data transmission or Measurement commands.

Once the DD-VAP on PAP B finds that the station stably move into the coverage of PAP B, the DD-VAP on PAP B sends a VAP Move Confirm to the server. The VAP Move Confirm would trigger the server to release the DD-VAP on PAP A by sending VAP Release. When PAP A receives the VAP Release, PAP A destroys the DD-VAP of the station. Afterwards, the station is served by the DD-VAP on PAP B.

Notice that the operating channel and the BSSID is the same before and after VAP migration so that the station could not

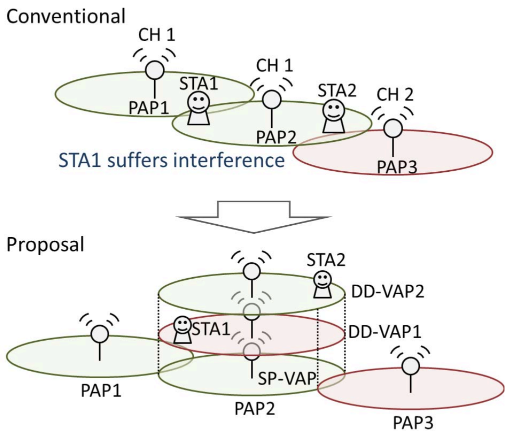

Figure 9. The proposal has finer channel assignment to eliminate the dilemma in conventional WLAN.

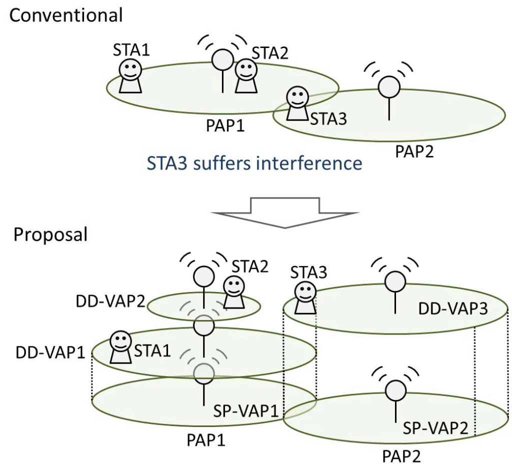

Figure 10. The proposal has better flexibility to adjust transmission power and control interference than the conventional one.

require executing channel scanning, re-authentication and re-association. The station could not be aware of the handover between different PAPs.

V. Study of Use Cases

In this section, we study three use cases as examples to highlight the benefits of the proposal. The first use case is the dilemma of channel assignment when neighbor access points interfere with each other. The second use case is about power control to deal with co-channel interference when channel switching is not allowable. Finally, the third use case is about the load balance when user stations select access points by the strongest signal strength.

A. Finer Channel Assignment

Figure 9 shows an use case of channel assignment when neighbor access points interfere with each other. In this case, assume that there are three physical access points, i.e. PAP 1 to 3, and suppose that the operating channel of PAP 1 and PAP 3 have been fixed at CH 1 and CH 2. If these two channels are only available for PAP2, the question is which channel PAP 2 should use. Additionally, there are two users, i.e. STA 1 and STA 2, which are associated with PAP 2. STA 1 is at the boundary of PAP 1 and PAP 2 while STA 2 is at the boundary of PAP 2 and PAP 3.

We first look at the conventional approach and quickly find that there is a dilemma when PAP 2 either chooses CH 1 or CH 2 as the operating channel. If PAP 2 chooses CH 1 as the operating channel to serve its stations, it is fine for STA2 but STA1 would suffer co-channel interference from PAP 1. If PAP 2 choose CH 2 as the operating channel, it is fine for STA 1 but STA 2 would suffer co-channel interference from PAP 3. Therefore, in either case, PAP 2 cannot the best channel that satisfies all stations.

The proposal can eliminate the above dilemma through creating a dedicated virtual access point for each user. On PAP 2, DD-VAP 1 is dedicatedly created for serving STA 1 and it operates at CH 2. Therefore, STA 1 is free from the interference of PAP 1. Similarly, DD-VAP 2 is dedicatedly created for STA 2 and it operates at CH 1 so that STA 2 is free from interference of PAP 3.

B. Flexible Interference Control

Figure 10 shows an use case of interference control when channel assignment is not available. Assume that there are two physical access points, i.e. PAP1 and PAP2, and they have been assigned fixedly at the same channel. Suppose that there are there stations, i.e. STA 1 to 3. STA 1 and STA 2 are associated with PAP 1, and STA 3 is associated with PAP 2. Additionally, STA 1 is settled at the boundary of PAP 1 while STA 2 is located near the center of PAP 1. STA 3 is near the boundary of PAP 1 and PAP 2, and STA 3 would suffer from co-channel interference from PAP 1.

We find that there is a dilemma to deal with the co-channel interference in conventional WLAN. STA 3 can become free from co-channel interference if PAP 1 turns down its transmission power. It is fine with STA 2 because it is near the center of PAP 1 so that it can still receive proper signal strength when PAP 1 turns down the power. However, STA 1 may suffer poor signal strength and even disconnect with PAP 1 since it is settled farther from PAP 1. On the other hand, if PAP 1 does not turn down the power, STA 3 would continuously suffer from co-channel interference.

To address the above dilemma, the proposal utilizes a dedicated VAP for each user and schedules these VAPs. On PAP 1, DD-VAP 1 is created for SAT 1, and DD-VAP 2 is for STA 2. PAP 2 creates DD-VAP 3 for STA 3. The transmission power of each VAP can be adjusted independently. To serve STA 1, DD-VAP 1 should use larger enough transmission power. On the other hand, DD-VAP 2 can use smaller enough power to serve STA 2 in order to reduce the co-channel interference to STA3. Even without proper scheduling of DD-

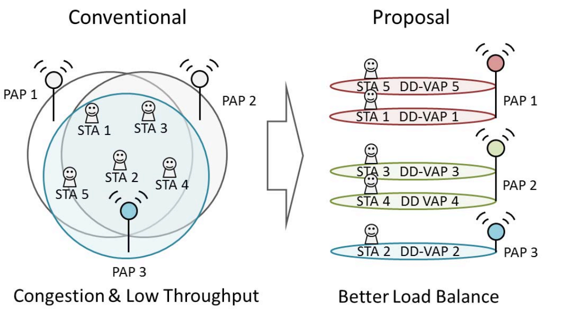

Figure 11. The proposal has better load balance through migration of DD-VAPs.

VAPs on PAPs, the co-channel interference that STA3 suffer from has reduced in average since the smaller power of DD-VAP 2. If the scheduled time of DD-VAP 3 on PAP 2 can be synchronized with the timing of DD-VAP 2 on PAP 1, the co-channel interference can be eliminated almost.

C. Better Load Balance

Figure 11 shows a use case about load balance when user stations select access points to entry the network. In this case, assume that there are tree physical access points, i.e. PAP 1 to 3, and their coverage are overlapped with each other. There are five user stations which intend to entry the network so that they select an access point to associate. Suppose that PAP 3 has the strongest signal strength for all stations.

In the conventional approach, user stations would like to select an access point with the strongest signal strength to associate. Therefore, five user stations associate with PAP 3, while PAP 1 and PAP 2 are idle. Obviously, the loading of PAPs is quite unequal. Although the signal quality of PAP3 is better, users in PAP3 may get lower throughput than expectation because more users share the resources and may cause congestion.

The proposal method can improve the load balance even if user stations prefer to select the strongest access point at network entry. The central server continuously monitors the loading of PAPs and balances the loading by migration of DD-VAPs. As stated in Section IV-D, users are not aware of changing of PAPs since they are always associated with the same DD-VAP, while the DD-VAP may migrate to different PAPs. For an instance, if PAP 3 can provide 100 Mbps and it is shared by five users, a user gets 20 Mbps in average. Contrarily, if PAP 1 can provide 80 Mbps and it is shared by two users migrated from PAP 3, a migrated user can get 40 Mbps, which is much better 20 Mbps before migration.

VI. Conclusions and Future Work

The original design of Wi-Fi is not for wide area deployment. The anarchy of access points in WLAN causes various issues and poor performance. To address these issues, a software-defined WLAN atop virtual access points is proposed. A series of procedures for creating, managing and migrating virtual access points is defined and based on the standard of IEEE 802.11 so that no modification of user equipment is necessary. A VAP is dynamically created by the demand of a user so that the overhead of VAP is minimized and the whole network can support more VAPs. A VAP is dedicated to a user so that the network can be optimized with finer granularity, i.e. per user instead of per cell. A procedure for channel switch is proposed to deal with co-channel interference. A solution is proposed to prevent user data loss when a PAP plays VAPs on different channel, Migration of VAPs is proposed to deal with the long latency of handover and as a tool for management of load balance. For the future work, we are looking for proper open-source hardware of access points so that it is free to modify the operations of access points and verify our proposal on these access points.

References

[1] Cisco, "Visual networking index: Global mobile data traffic forecast update 2012 – 2017." [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html

[2] "The METIS 2020 Project - Laying the foundation of 5G." [Online]. Available: https://www.metis2020.com/

[3] P. Demestichas, A. Georgakopoulos, D. Karvounas, K. Tsagkaris, V. Stavroulaki, J. Lu, C. Xiong, and J. Yao, "5G on the horizon: Key challenges for the radio-access network," *IEEE Vehicular Technology Magazine*, vol. 8, no. 3, pp. 47–53, 2013. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6568922

[4] A. Detti, C. Pisa, S. Salsano, and N. Blefari-Melazzi, "Wireless mesh software defined networks (wmSDN)," in *IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2013, pp. 89–95. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6673345

[5] T. Hamaguchi, T. Komata, T. Nagai, and H. Shigeno, "A framework of better deployment for WLAN access point using virtualization technique," in *IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2010, pp. 968–973. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5480932

[6] O. Braham and G. Pujolle, "Virtual access point to the cloud," in *IEEE 1st International Conference on Cloud Networking (CLOUDNET)*, 2012, pp. 206–208. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6483689

[7] F. Anhalt and P. Primet, "Analysis and evaluation of a XEN based virtual router," Research Report RR-6658, 2008. [Online]. Available: https://hal.inria.fr/inria-00320620

[8] Y. Grunenberger and F. Rousseau, "Virtual access points for transparent mobility in wireless LANs," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2010, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5506709

[9] L. Suresh, J. Schulz-Zander, R. Merz, A. Feldmann, and T. Vazao, "Towards programmable enterprise WLANS with Odin," in *Proceedings of the first workshop on Hot topics in software defined networks*. ACM, 2012, pp. 115–120.

[10] M. Berezin, F. Rousseau, and A. Duda, "Multichannel virtual access points for seamless handoffs in IEEE 802.11 Wireless networks," in *IEEE 73rd Vehicular Technology Conference (VTC Spring)*, 2011, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5956552

[11] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std., 2012. [Online]. Available: http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[12] S. Chieochan, E. Hossain, and J. Diamond, "Channel assignment schemes for infrastructure-based 802.11 WLANs: A survey," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 1, pp. 124–136, 2010. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5415868