LENV: A New Light-weighted Edge Network Virtualization Framework in Software-defined Wireless Networks

Tingting Hu, Kaiping Xue*, Wenjia Wei, Wei Jiang
Department of EEIS, University of Science and Technology of China, Hefei, China, 230027
kpxue@ustc.edu.cn

***Abstract*—With the proliferation of mobility demands and network services, network operators in enterprise Wireless Local Area Network (WLAN) must implement a flexible and centralized network management to keep pace with this trend. Unfortunately, due to the inflexible network architecture and closed network equipments, the traditional network faces a series of challenges, like network expansibility and mobility issues. In this paper, we propose a new architecture named Light-weighted Edge Network Virtualization (LENV), which achieves edge network functions virtualization by leveraging the Software Defined Networking (SDN) approach in enterprise WLAN. LENV virtualizes edge network functions towards a centralized logical module which hosts in the wireless access point (AP) for each client under the controller's strategies. Therefore, network functions can be deployed more flexibly based on client's requirements and network status. In addition, combined management schemes consisting of association control, access control and mobility management have been considered and studied in LENV, which ensure enterprise WLAN extensible and stable. In the end, our further simulation shows that LENV can significantly benefit mobility and security in enterprise WLAN.**

I. Introduction

With the expansion of the enterprise and rapid development of mobile devices, enterprise WLAN has to manage more wireless APs to serve a large number of clients. To achieve the stability and flexibility, network functions consisting of interference management, mobility management, access control and load balancing should be realized by administrator on top of the network [1], [2]. It will increase new challenges in wireless network management, especially for the edge network. Many research projects have concerned about how to manage these network functions with both low latency and high network performance [3], [4].

Edge network functions include NAT, DHCP, firewall, associating and authenticating clients who attempt to access the network, authorizing clients into different partitions, etc. [5]. In the traditional network, these network functions disperse on different entities like middle-boxes so that mobile network is usually solidified in the hardware of net devices [6]. Coupling with specific hardware tightly and the lack of centralized management can hardly provide a flexible and extensible network.

Recently, centralized control and virtualization technologies have gained growing interest in network management such as Odin [7] and CloudMac [8]. SDN decouples the control plane and the data plane of networks, which can be used to virtualize configuration and control of network elements in the control plane through protocols such as OpenFlow [9]. SDN can also be viewed in a wider context that many networking-related functions migrate from firmwares in dedicated network equipments into focused and effective software controllers. It simplifies network devices and makes them programmable. Meanwhile, a flexible and effective control strategy in the control plane is useful to accomplish the network virtualization [10], which can generate policies and enforce several flowtable entries on one network device to implement different functions.

In this paper, we propose a framework named Light-weighted Edge Network Virtualization (LENV) in software-defined WLAN to provide a scalable and agile management for enterprise network. Based on SDN strategies, LENV virtualizes and integrates edge network functions into an abstract and logical module named Virtual Wireless Access Device (VWAD), which is issued to the AP by the control plane. Each VWAD corresponds to a client who can access to the network, which can be seem as a virtual AP to guide the physical entity to provide network functions based on client's requirement. LENV also supports the virtualization of edge network nodes to various logically isolated virtual nodes for achieving network slicing, so one network device may maintain several VWADs belong to different virtual networks. In general, LENV makes network functions centralized and takes advantage of VWAD to facilitate the realization of network functions.

Further, LENV can be extensible to support various management schemes. With the aid of VWADs, we propose feasible and effective mechanisms. Our fine-gained access control scheme achieves a feasible joint design between the authentication process and access authority management according to clients' identifies. While for mobility management, we consider not only the specific mobility handover scheme, but also the handover policies based on reversed signal strength measurement (it's usually denoted as *Reversed-Measurement* for convenience).

The contributions of this paper are summarized as follows:

- We propose LENV, a new architecture for the edge network virtualization in SDN WLAN. It integrates network functions into the logical module VWAD for each client based on SDN technology to implement the centralized and flexible function management.
- In LENV, we develop an integrated management scheme which considers both security and mobility factors. Fur-

978-1-4673-7687-7/15/$31.00 ©2015 IEEE

thermore, this scheme can be achieved without any modifications to the 802.11 client.

- We build a system simulation platform to validate the performance of our proposed schemes such as seamless mobility and security aspects in enterprise WLAN.

The rest of this paper is structured as follows. Section II gives a brief introduction to the related works. In Section III, we mainly explain the architecture of LENV and describe the details of schemes in LENV. Section IV focuses on the evaluation. Finally, a summary concludes this paper with an outlook of future works in Section V.

II. Related Works

In recent years, many schemes about enterprise WLAN architecture are proposed. The OpenRoads [11] is the first work in software-defined WLAN, which creates different wireless network slices by using different SSIDs. The OpenRadio project [12] proposes a SDN architecture to make the wireless data plane programmable, which implements the PHY and MAC layers of different wireless protocol stacks. In the DenseAP [14], channel re-assignment and re-association related decisions are triggered by *disconnection* message which tells the client to scan the WIFI channel and need associate with a new AP. The CENTAUR [13] can provide network services and support seamless mobility by centralized management.

With our proposed LENV, the PHY is not programmable but a native component by comparing to the OpenRoads. The DenseAP can hardly achieve seamless mobility, because the client should reconnect with the network when it changes the association relationship. Although the CENTAUR can support seamless mobility, it requires special software or hardware modification on clients. In contrast, LENV is able to implement seamless mobility without any modification on clients, which can avoid the cost of transforming devices' hardware and improve the performance of networks.

The framework named Odin [7] can achieve seamless mobility without any modification on clients, but it is limited by the memory space of data storage and cost of transmission. In Odin, clients' association states are recorded in Odin Agents which host in physical APs and the mobility scheme is implemented by moving clients' association states between APs. However, the Odin Agent might not have enough memory space and computing power of the AP is limited with the large scale of clients. In our LENV, we record all the state messages in the control plane. When the moving event is triggered, we just need update the database and flowtable entries, because our scheme is based on SDN strategies and VWAD can be implemented by flowtable entries operation. Moreover, our LENV considers schemes about security and handover policies of mobility which are not considered in Odin.

III. LENV Framework Based on SDN Technology

In this section, we propose a new network architecture named LENV to provide a flexible and centralized network management based on SDN technology in enterprise WLAN. We will focus on the basic principle of the framework firstly, and then describe specific schemes of network components functional virtualization in detail.

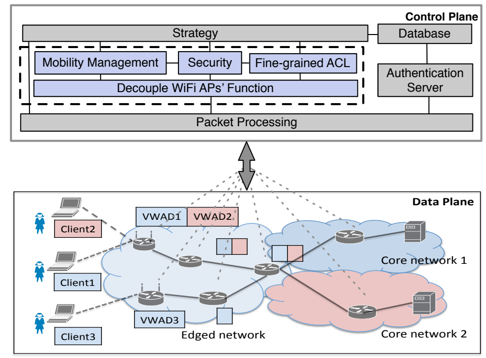

Fig. 1: High-level overview of LENV architecture

A. Overview

Fig.1 indicates the conceptual framework of the proposed design. As it shows, LENV's architecture comprises a logically centralized control plane and physical infrastructure in line with SDN technology. The data plane splits into two types of networks: edge network and core network. In enterprise WLAN, different clients usually meet various businesses and have different access rights to network services [5]. The core network in our design is separated to several different service networks: *Core network1* and *Core network2*, which present network services of different access permissions.

Next, we will focus on how to eliminate entities of edge network functions and integrate these functions within the controller. As shown in Fig.1, the control plane consists of an authentication server, OpenFlow function modules and a database which records message-pairs <*username, authentication code, Group ID*> (Group ID: the ID of a group in which clients have the same access authority to network services). The control plane is responsible for collecting and recording the current status of each entity, and generates a set of policies to implement network functions and achieve management schemes. So LENV can virtualize edge network functions consisting of clients' association and authentication control, fine-grained control and mobility management into an abstract module named Virtual Wireless Access Device (VWAD) for each client based on SDN strategies. As Fig.1 shows, the control plane assigns *VWAD1* which servers *Client1*, *VWAD2* which serves *Client2* to *AP1* and assigns *VWAD3* which serves *Client3* to *AP2*. It can be thought that the client associates with the logical VWAD via physical resources of the physical AP which can host many VWADs. Moreover, the Group ID of *Client1* and *Client3* are the same, so they have the same access permissions to the network.

In LENV, we also present a *Reversed-Measurement* scheme to select the AP of the strongest WIFI signal strength (RSSI) for the client, and the mobility management method is implemented by handovering the client's corresponding VWAD to a new physical AP. Therefore, clients need not request the same network service like the association one more time during the mobility process, which achieves the seamless mobility. As a whole, LENV can improve the network performance and the quality of experience for clients.

B. Decouple Access Point's Functions from Infrastructure

To effectively implement centralized management and edge network virtualization in enterprise WLAN, the basic design goal of LENV is decoupling network functions from entities (eg.wireless APs) in the edge network. In traditional 802.11 wireless network, APs responding with request messages of the client are candidate APs for the client. Then the client chooses an AP with the strongest RSSI of respond messages. Since the respond message contains a *BSSID* message which can be considered to the mac address of the AP, the client can communicate with the AP directly. On the one hand, this traditional 802.11 association scheme depends on selection of clients, so it usually causes low QoE of the client, which is always associated with an AP even if its RSSI is weaker and weaker when the client moves far away from the AP. On the other hand, the client's association state is fixed in a physical AP, which can not support seamless mobility in the muti-APs environment.

The schematic diagram of decoupling AP's functions from its original infrastructure in LENV is shown in Fig.2. AP's functions consisting of association and authentication are all integrated in the control plane and association states are also recorded in it. Moreover, in order to support seamless mobility, the association is controlled by the control plane based on the *Reversed-Measurement*. The specific component functions of the innovative AP in LENV are as follow:

1) Pre-Processing Module: The innovative AP implements 802.11 mac-layer split, which is an OpenFlow wireless switch (it can be realized by combining physical slim AP, Click Router with Open vSwitch) communicates with the SDN controller via the OpenFlow interface. However, the OpenFlow protocol can not support processing 802.11 mac-layer's messages, which can be solved in the *Pre-Processing* module in our design. This module is used to reconstruct packets that contains mac-layer's messages by adding mac-layer's messages to fields like tags and trailers of packets, and then forward packets to the controller. We can also solve this issue via defining an extend OpenFlow protocol.

2) Reversed-Meansurement Module: The *WIFIPhy* module is responsible for handling WIFI channel management, listening and forwarding WIFI signal. In order to implement the *Reversed-Measurement*, we get RSSI of the up-stream which is received by the AP via adding radio-tap header into the packet in the *WIFIPhy* module, and use it to estimate RSSI of the client. Because the channel attenuation of up-streams and down-streams for a pair of AP and client are nearly the same in 802.11 wireless network. The *MACLow* module is used to generate ACK frame, beacon frame and other mac frames.

3) VWAD Module: The *VWAD* module is a logical module which is generated by the controller. As Fig.2 shows, each client connected with the network is corresponding to a unique *VWAD*. For example, if a client tries to join the network, the controller will select an AP based on the *Reversed-Measurement* to assign a VWAD to provide edge access services. The other edge network functions which are requested by the client will be added into the *VWAD* latter with the controller guiding.

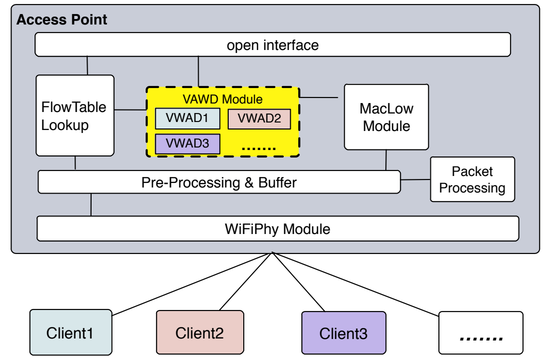

Fig. 2: Schematic diagram of AP in LENV

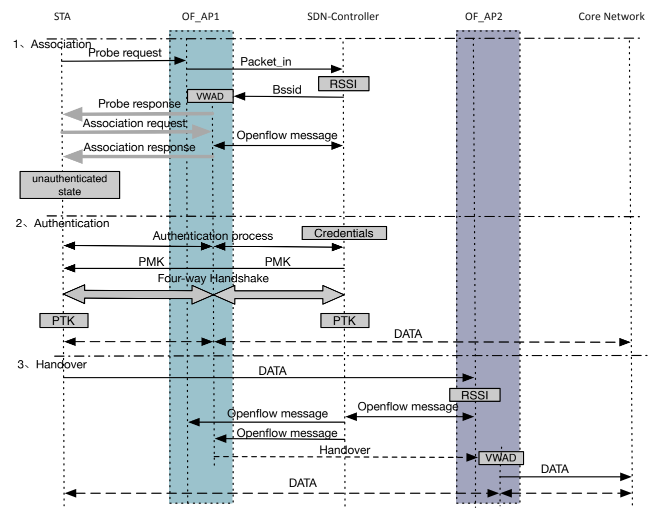

Fig. 3: Ladder diagram of the interactive process in LENV

The details of a new-joined AP's association process in LENV is shown in the first stage of Fig.3. At first, the client initiates broadcasting the *probe request* message, APs which receive this request message are candidate APs for the client. Then, candidate APs forward request messages to the controller. The controller looks up *Packet-in* messages to find out the client's current status, the client's mac address and RSSI of each candidate AP. With these messages, it generates strategies which are assigning a unique VWAD to the AP whose RSSI is strongest and mapping a unique BSSID value to the VWAD. The message-pair $<$*mac address,* $VWAD_{\mathrm{ID}}$*, BSSID,* $AP_{\mathrm{ID}}>$ will stored in the database. After that, the AP which receives VWAD provides association services for the client. However, the other candidate APs will drop all packets of this client according to flowtable entries (shown in Table.I). At last, the client gets the BSSID value from the *probe response* message and can unicast transmit with the AP in which its VWAD hosts.

TABLE I: Rules for clientA's dataflow

Entity	VWAD	Actions
The associated AP for clientA	$VWAD_a(BSSID_a)$	*Ack and Forward*
Other candidate APs	*no* $VWAD_a$	*Drop*

C. Fine-grained Access Control Based On Client's Identity

In LENV, we propose a fine-grained access control scheme, which not only prevents the intrusion from rogue clients, but also enables granular control of legal clients. As shown in Fig.4, the database in the control plane maintains message-pairs *<username, authentication code, Group ID>*. If only the client authenticates successfully with the legal username and correct authentication code, it can be permitted to access the network. To achieve fine-grained access control, LENV divides legal clients to different groups which have a different set of access permissions. Therefore, a sophisticated access control such as guest/staff separation can be realized based on clients' Group ID and via virtual paths in the edge network.

1) Authentication Process: We will first discuss the authentication process in detail, which is shown in the second stage of Fig.3. We assume that the enterprise network scenario is based on IEEE 802.1X and WPA2. The unauthenticated client will send its identity message to the AP which owns its VWAD after the association process, and then the identity message will be authenticated with the authentication server in the control plane. If the identity is legal, the controller will assign a pairwise-master key (PMK) to the client and its VWAD. After that, the client and the controller will perform Four-way Handshake via the AP to negotiate a Pairwise Transient Key (PTK) which is used to be the session key for the later communication. Finally, the controller adds PTK to the client's message-pair in the database and installs the PTK in the VWAD by issuing flowtable entries. If only the AP owns the session key, it can successfully encrypt and decrypt packets in the WPA2 enterprise network session. Specifically, PTK is controlled by the controller centrally, and it is only visible to the controller but transparent to the AP via hiding it in the VWAD. Therefore, our mechanism can protect the key from malicious steal and leakage, which provides effective guarantee for the security of enterprise WLAN.

2) Fine-grained Access Control Scheme: Fine-grained access control for legal clients is illustrated in Fig.4. For each authenticated client, the controller will get the client's Group ID information from the database according to the client's identity. Then it issues flowtable entries to add Group ID to the client's VWAD. As a result, the AP will add Group ID to the packet by using the VLAN tag field in the edge of network. Entry nodes into the core network can check the VLAN tag value to judge the forwarding port. By combining the authentication scheme and Group ID assignment, we are able to achieve the fine-grained control for legal clients to access network services.

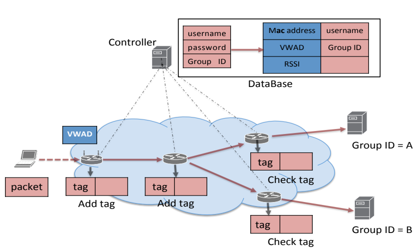

Fig. 4: Example fine-grained access control scenario

D. Mobility Management

In an enterprise WLAN, there are hundreds of APs to support a wide WIFI coverage area and clients meet exploded mobility demands, so supporting seamless mobility and minimizing mobility delay in wireless network is well studied problems. LENV not only provides a seamless mobility mechanism to show how to achieve the movement, but also considers different handover policies to solve when and where of movement. It's important to note that we consider that all APs work in the same channel in this paper.

1) Seamless Mobility Mechanism: The third stage of Fig.3 shows the specific process of seamless handover between APs. When the client is moving to the WIFI coverage range of *AP2*, *AP2* can listen to packets sent by the client. The first packet together with the RSSI and mac address of the client are forwarded to the controller due to the lack of corresponding flowtable entries in *AP2*. If the controller decides that the handover is required, the controller will issue flowtable entries according to the policy which is moving the client's VWAD from the initial associated AP to *AP2* and update the client's message-pair in the database. Because the client's BSSID, PTK and Group ID are stored in the VWAD, the client can connect with *AP2* without re-association and re-authentication process when the VWAD moves from *AP1* to *AP2* successfully. The main feature of the seamless mobility is that the procedure is transparent to the client which never participates in the process.

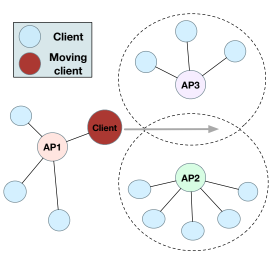

Fig. 5: Example ping-pong effect scenario

2) Seamless Mobility Policies: We will discuss several seamless handover policies in LENV. As we mentioned in *Subsection A*, the controller can choose an AP with strongest RSSI for the client based on the *Reversed-Measurement*. We consider a basic RSSI policy which is that the handover event triggers when the requirement (*RSSI of competed AP>RSSI of current associated AP*) is satisfied. Although this policy guarantees that the client always connect with the maximum RSSI's AP, it may not adapt to the situation in Fig.5. We assume that the client moves from the WIFI coverage range of *AP1* to the overlapping area of *AP2* and *AP3*, and the RSSI of the packet received by *AP2* is very close to *AP3* when the client is in the overlapping area. The VWAD may handover between these two APs constantly like the ping-pong effect, which will result in network performance sliding down significantly.

Hence, we propose a handover policy which is shown at *Algorithm*1 to avoid the ping-pong effect and association control. The details as follows: We consider using a *smoothness* value $RSSI_s$ as a balanced value to avoid the ping-pong effect which is caused by slight difference between the strongest RSSI of candidate APs and the RSSI of current associated AP. Only when the difference value is higher than $RSSI_s$, the handover event may triggers. We also consider that if the RSSI of the current associated AP is strong, it is no need to trigger handover event even though existing candidate APs. So we define a *threshold* value $RSSI_h$, only when *RSSI of the current associated AP*$<RSSI_h$, the handover process can be triggered. The rest of the algorithm is designed to solve the problem about handovering the VWAD to which candidate AP. Because RSSIs of our candidate APs are all strong, so our Aiming is to choose the candidate AP whose load balance is lowest. We calculate the number of *VWAD*s which is hosted in AP as N_c for each candidate AP, and then we handover VWAD from associated AP_a to AP with minimal N_c.

Algorithm 1 VWAD Handover Algorithm

Require:
The set of APs : V;
The number of stations associated to AP j : L_j;
RSSI value of the client i received by AP j : S_{ij};
Ensure:
STA u is associated with AP of id a ;
if $S_{ua} < \max_{j \in V \& j \neq 0} S_{uj} - RSSI_s$ **then**
  Get the set of APs : C;
  if $S_{ua} < RSSI_h$ **then**
    if $the\ size\ of\ C = 1$ **then**
      Handover $vwad_u$ from associated AP_a to candidate AP_c;
    else
      Caculate the load balance N_c for each candidate AP:
      Handover $vwad_u$ from AP_a to AP with minimal N_c;
    end if
  end if
else
  No Handover
end if

IV. Performance Analysis

In this section, we perform a simulation to evaluate the performance of management schemes that we proposed in LENV. The simulation is supported by OpenNet [15] which is a simulator for software-defined WLAN. The topology of simulation we adopte is as Fig.6 shown.

A. Performance Profiling of Seamless Mobility Mechanism

With the topology in Fig.6, the client *m1* is initially associated with *AP2* and then moves to the WIFI coverage of *AP3* at a constant speed. Along the simulation progress, *m1* sends UDP traffic at 5.7Mbps to the server *H1* using Iperf. Fig.7 shows the comparison result between traditional 802.11 mobility scheme and our proposed scheme.

We can clearly see that UDP throughput drops to zero from 31s to 34s for re-association and re-authentication process in traditional 802.11 network. While using seamless mobility scheme, UDP throughput decreases a little during the handover process of VWAD without disconnection. As a result, we achieve the seamless mobility without re-association and re-authentication when the client moves between APs. Because seamless mobility scheme is based on the *Reversed-Measurement*, the time of handovering is earlier than traditional 802.11 scheme, which can benefit the network performance because the client can always associate with an AP of strong RSSI. By the way, in our LENV architecture, there is an overall reduction of UDP throughput as opposed to traditional 802.11 network due to APs should interact with the SDN controller.

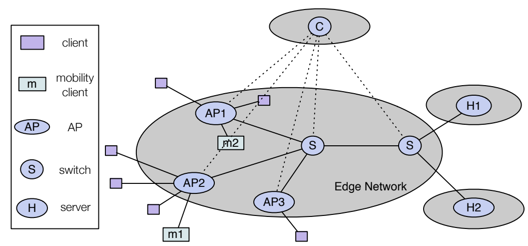

Fig. 6: Architecture of simulation topology

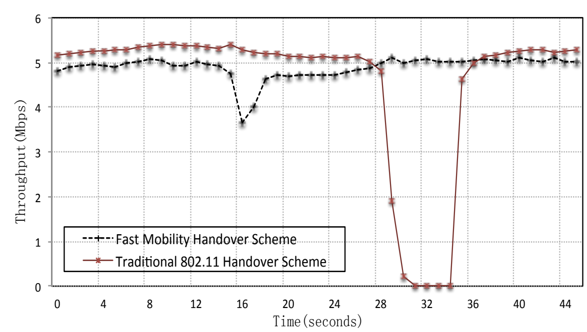

Fig. 7: Network throughput of moving client with respect to traditional 802.11 network and LENV network

B. Simulation and Evaluation Analysis of Security Scheme

In LENV, the fine-grained access control consists of the authentication and Group ID assignment. In our simulation topology, we separate network services providers to two levels and assign moving clients to two corresponding groups of different access permissions. Group ID of *m1* and *m2* is *1* and *2* respectively. In the case, we test the connectivity by using *Ping*, the result is that *m1* can communicate with *H1* suceessfully but fail to communicate with *H2*.

Meanwhile, Fig.8 shows the impact of our authentication scheme, from which we can see that UDP throughput with our authentication scheme decreases a little about 1Mbps at 16s when performing a VWAD migration. However, UDP throughput curve with other researches' scheme like Odin which not considers authentication handover scheme is interrupted about 2 seconds. Because the scheme without authentication handovering should process re-authentication after association handover process. As a consequence, our proposed security scheme brings a better performance in comparison with the other handover scheme without authentication handover scheme and achieves the fine-grained access control based on clients' access permission.

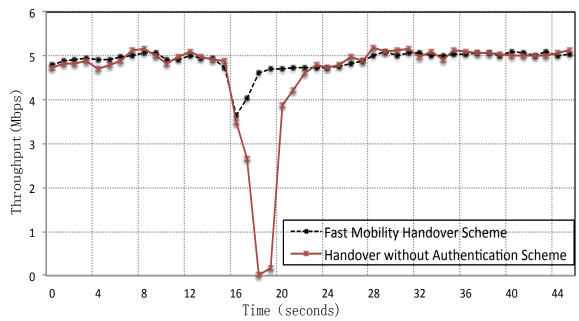

Fig. 8: Network throughput of moving client with respect to authentication handover scheme and handover scheme without authentication handover

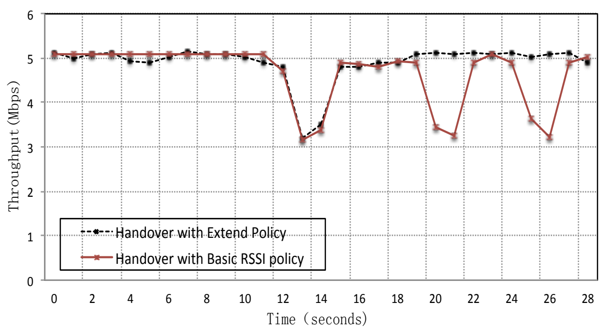

Fig. 9: Network throughput of moving client with respect to basic RSSI handover policy and extend handover policy

C. Reliability Analysis of Seamless Mobility Policies

Main point in this simulation is to show that how different handover policies influence the performance of network throughput. As we mentioned in mobility management, the improper handover policy may incur the ping-pong effect, so we will show the reliability of our extend handover policy to avoid it.

In this simulation, *AP2* associates with three clients and *AP3* associates with one client, the client *m2* moves from the WIFI coverage of *AP1* to the overlapping area of *AP2* and *AP3*. From Fig.9, we can clearly see that if the policy is based on the *Reversed-Measurement*, *m2* will handover between the two APs frequently, which results in the network throughput fluctuating upward and downward. In the case of using the extend handover policy, the throughput just drops a little one time while the VWAD is handovering. It avoid the ping-pong effect and the controller chooses the AP which can make the maximum average RSSI of the whole network.

V. Conclusion and Future Work

In this paper, we have shown the flexibility and stability of our proposed architecture. It decouples network functions from net devices and logically centralizes network functions to the abstract module through communicating and cooperating with the control plane. Moreover, we provide management schemes consist of association control, security and mobility for LENV in enterprise WLAN. These schemes our proposed enhance the fine-grained controllability, efficient programmability and reduce the cost of network performance overhead, the simulation results also verify it.

Furthermore, we will build the experiment platform and test our architecture with it. Moreover, we will extend our strategy to APs which working on different channels and propose a more sophisticated algorithm to solve the load balance problem deeply to enhance our existing results.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grant No.61379129, No.61390513 and the National High-Tech Research and Development Plan of China (863 Program) under Grant. No.2014AA01A706.

References

[1] M. E. Berezin, F. Rousseau, A. Duda, "Multichannel virtual access points for seamless handoffs in ieee 802.11 wireless networks.". in *Vehicular Technology Conference*, May. 2011, pp. 1-5.

[2] I. Papanikos, M. Logothetis, "A study on dynamic load balance for IEEE 802.11b wireless LAN". in *Proc. COMCON'01*, Jun. 2001.

[3] S. H. Yeganeh, A. Tootoonchian, Y. Ganjali, "On scalability of software-defined networking". *IEEE Commun. Magazine*, vol. 51, no. 2, pp. 136-141, 2013.

[4] R. Murty, J. Padhye, R. Chandra, A. Wolman, B. Zill, "Designing high performance enterprise Wi-Fi networks". *NSDI* Vol. 8, pp. 73-88, Apr. 2008.

[5] T. Koponen, M. Casado, et. al. "Network virtualization: Technologies, perspectives, and frontiers". *Journal of Lightwave Technology* Vol. 31, No. 4, pp. 523-537, 2013.

[6] A. Tootoonchian, Y. Ganjali, "Software-Defined and virtualized future mobile and wireless networks: A Survey". *Mobile Networks and Applications*, Springer, 2014, pp. 1-15.

[7] L. Suresh, J. Schulz-Zander, R. Merz, A. Feldmann, T. Vazao, "Towards programmable enterprise wlans with odin", in *Proc. ACM HotSDN'12*, New York, USA, Aug. 2012, pp. 115-120

[8] M. C. Chan, C. Chen, J. X. Huang, T. Kuo, L. H. Yen, C. C. Tseng, "CloudMAC: An OpenFlow-based architecture for 802.11 MAC Layer processing in the cloud". *Proc. BWAWS'12*, 2012.

[9] A. Lara, A. Kolasani, B. Ramamurthy, " Network innovation using openflow: a survey". *IEEE Commun Surv Tutor* Vol. 16, No. 1, pp. 493-512, 2014.

[10] R. Jain, S. Paul, " Network virtualization and software defined networking for cloud computing: a survey'. *IEEE Commun Mag*, Vol. 51, No. 11, pp. 24-31, 2013.

[11] K. K. Yap, M. Kobayashi, R. Sherwood, T. Y. Huang, M. Chan, N. Handigol, N. McKeown, "Openroads: empowering research in mobile networks". *SIGCOMM Comput. Commun. Rev.* Vol. 40, No. 1, pp. 125-126. 2010.

[12] M. Bansal, J. Mehlman, S. Katti, P. Levis, "Openradio: a programmable wireless dataplane", in *Proc. ACM HotSDN'12*, New York, USA, Aug. 2012, pp. 109-114.

[13] V. Shrivastava, N. Ahmed, S. Rayanchu, S. Banerjee, S. Keshav, K. Papagiannaki, A. Mishra, "CENTAUR: realizing the full potential of centralized wlans through a hybrid data path". *Proc. MobiCom'09*, Sep. 2009, pp. 297-308.

[14] R. Murty, J. Padhye, A. Wolman, M. Welsh, "Dyson: an architecture for extensible wireless LANs.". in *Proc. USENIXATC'10*, Berkeley, CA, USA, Jun. 2010, pp. 1515.

[15] M. C. Chan, C. Chen, J. X. Huang, T. Kuo, L. H. Yen, C. C. Tseng, "OpenNet: A Simulator for Software-Defined Wireless Local Area Network". *Proc. IEEE WCNC'14*, Apr. 2014, pp. 3332-3336