IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 13, 2016; accepted January 6, 2017, date of publication January 17, 2017, date of current version March 13, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2653244

A Novel Multipath-Transmission Supported Software Defined Wireless Network Architecture

CHUAN XU[1], (Member, IEEE), WENQIANG JIN[1], GUOFENG ZHAO[1], HUAGLORY TIANFIELD[2], (Member, IEEE), SHUI YU[3], (Senior Member, IEEE), AND YOUYANG QU[3]

[1]School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[2]Department of Computer, Communications and Interactive Systems, Glasgow Caledonian University, Glasgow G40BA, U.K
[3]School of Information Technology, Deakin University, Burwood, VIC 3125, Australia

Corresponding author: G. Zhao (zhaogf@cqupt.edu.cn)

This work was supported in part by the National Science Foundation of China under Grant 61402065, in part by the China Scholarship Council under Grant 201507845020, and in part by the Young Backbone Academics Funding Program of Chongqing Municipal Education Commission.

ABSTRACT The inflexible management and operation of today's wireless access networks cannot meet the increasingly growing specific requirements, such as high mobility and throughput, service differentiation, and high-level programmability. In this paper, we put forward a novel multipath-transmission supported software-defined wireless network architecture (MP-SDWN), with the aim of achieving seamless handover, throughput enhancement, and flow-level wireless transmission control as well as programmable interfaces. In particular, this research addresses the following issues: 1) for high mobility and throughput, multi-connection virtual access point is proposed to enable multiple transmission paths simultaneously over a set of access points for users and 2) wireless flow transmission rules and programmable interfaces are implemented into mac80211 subsystem to enable service differentiation and flow-level wireless transmission control. Moreover, the efficiency and flexibility of MP-SDWN are demonstrated in the performance evaluations conducted on a 802.11 based-testbed, and the experimental results show that compared to regular WiFi, our proposed MP-SDWN architecture achieves seamless handover and multifold throughput improvement, and supports flow-level wireless transmission control for different applications.

INDEX TERMS Software-defined networking, network function virtualization, multipath transmission, handover, virtual access point.

I. INTRODUCTION

The exponential growth of wireless data services towards the fifth generation (5G) has triggered the huge number of low power nodes such as WiFi and small cells [1], widely deployed in enterprise and other public places to provide ubiquitous access for mobile users with simultaneous active connections to more than one base station or access point [2], [3], which is explored to support high throughput and seamless mobility in 5G networks.

Contrasting to the increasing new requirements from users for WiFi networks, e.g., mobility, high bandwidth and customized service support, the management and operation of today's local wireless access networks is often very inflexible, and ignores the specific demands from numerous applications. Moreover, WiFi and other wireless access networks are often deployed in their own infrastructures and organized uncoordinated, neighboring access points cannot be leveraged to reduce transmission delays and improve user mobility, not to mention exploiting the power of multiple access points to improve network throughput.

Based on the concept of virtualization technology [17], [18], the provisioning of multiple virtualized interfaces on mobile device utilized to improve throughput on mobile device. Link layer virtualization of mobile device, such as Virtual WiFi [4], FatVAP [5] and Juggler [6], leverage the virtualized technology to simultaneously associate with multiple access points and schedule multiple channels over them, to aggregate data transmission at the user. Unfortunately, they perform poorly due to mobility nature and actual high cost of access point re-connection in a mobile environment. In WiSwitcher [7] and Spider [8], the wireless driver is modified to employ MAC layer virtualization to create multiple virtual network interfaces on users, and connections to each access point on a single channel are maintained and scheduled between the channels based on their history records. However, the wireless device driver or protocol stack has to be modified to provide virtualized interfaces at link or mac layer, which makes it hard to be implemented on commodity mobile devices.

Multipath technologies are emerging as a new trend in networking of future Internet and 5G [9]. The multipath transport protocols (MPTCP) was proposed by IETF [10], to support concurrent transmissions. MPTCP supervises two or more standard TCP sessions, which makes it possible to use multiple paths for data transmission under the same TCP connection to support smooth handover between heterogeneous networks. However, MPTCP works on the prerequisite that at least one of two devices has multiple logical interfaces, and it can't guarantee high transmission rate when the difference of characteristics (such as bandwidth and RTT) between the two interfaces (e.g., 3G or 4G, and WLAN) is large in real world [11] and underperform for short flows [12]. Moreover, in some network conditions, a single path may have better performance than multiple paths. Consequently, Nam et al. [13] proposed to dynamically add or remove MPTCP paths based on SDN, according to the available capacity of connected paths.

Software-defined network (SDN) [14]–[16] is an interesting innovative paradigm for programmable network by decoupling the control plane and data plane of networks. This dramatically simplifies network control and enables innovation and evolution by abstracting the control functions of the network into a logically centralized control plane. Moreover, the concept of network function virtualization (NFV) [17], [18] effectively separates the abstraction of functionalities from the network hardware and substrate. By extending SDN to mobile and wireless networks, it leads to a new trend, i.e, software-defined wireless network (SDWN). With the functionality abstraction from hardware and the logically centralized control, SDWN can address the challenges of wireless network, and improve the efficiency on multiple wireless access networks. Recently, the SDWN concept is realized in wireless access networks and cellular networks through different approaches [19]- [30]. To separate the network service from the underlying physical infrastructure and allow rapid innovation of WLAN services, several architectures have been proposed, such as OpenRoads [19], OpenRadio [20], OpenRF [21], CloudMac [22], and Odin [23], which provide seamless mobility and good scalability.

In this paper, we propose a novel multipath-transmission supported Software-Defined Wireless Network architecture (MP-SDWN)[1] for WLAN systems. Multiple physical access points are utilized to provide multiple transmission paths for single mobile user to improve the network performance on mobile device. We present the details of system architecture and design, and give the typical use cases with MP-SDWN. Moreover, we extend Odin to implement MP-SDWN architecture, and evaluate our system on a real testbed. The experimental results show that compared to regular WiFi, MP-SDWN achieves seamless handover and several fold throughput improvement, especially in the case of insufficient bandwidth allowed on a single AP, and supports differentiated wireless transmission control at flow-level for different applications from the same user. We make contributions in the following three aspects.

- Firstly, a unified and extended SDN and NFV abstraction, namely, multi-connection virtual access point (MVAP), is put forward to simplify the complexity of IEEE 802.11 protocol stack and to move the operation of protocol stack into application layer, and facilitate easy handling and migration of per-user state cross different physical access points. Different from the existed virtual access point abstraction, MVAP maintains a same virtual access point for each user on a set of adjacent physical access points simultaneously, to support multiple connections over the set of physical access points when user migrates or stays in the wireless signal overlap area. Moreover, MVAP adds a collaborative hierarchical flow table distributed on all access points for each user, to forward flows from the user in parallel to improve user's throughput.
- Secondly, a wireless flow transmission rule table (WFTR) is introduced into mac80211 subsystem to achieve wireless transmission control at flow-level, similar to the packet forwarding control in wired network, which allows administrators to differentiate flow priorities of diverse applications. WFTR contains control parameters including transmission power, transmission rate and priorities. By use of WFTR, MP-SDWN can provide flow-level QoS control to satisfy the needs from various applications.
- Thirdly, an admin proxy is devised which allows ISPs to share the network control, e.g., load balancing, QoS policy, troubleshooting. Moreover, the interface supports injecting customized routing or scheduling algorithm into core module to simulate the effect. We set three typical applications on top of MP-SDWN including load balancing, wireless transmission control and energy efficiency.

The remainder of the paper is arranged as follows. Section II presents a literature review. Section III puts forward a novel multipath-transmission supported Software-Defined Wireless Network architecture and presents architecture and mechanism of MP-SDWN. Section IV presents the detailed implementation of MP-SDWN. Section V discusses typical use cases and network services based on MP-SDWN. Section VI evaluates the performance of MP-SDWN by conducting a number of typical WiFi application experiments on our testbed. Section VII draws conclusions.

II. LITERATURE REVIEW

The key concept of SDN and NFV is to separate the network service from the underlying physical infrastructure and allow rapid innovation of wireless network services.

[1] github.com/FNRC/MP-SDWN

This is very important in the context of 5G wireless technologies. Software-defined wireless network (SDWN) concept has been studied as follows.

OpenRoads [19] is the first work to move the wireless network forward on a path to greater openness. It uses OpenFlow to separate control from the data path through an open API, and FlowVisor to create network slices and ensure isolation among them. The prototype of OpenRoads was deployed as a backward compatible wireless network infrastructure for WiMAX service on campus. OpenRadio [20] proposes a programmable wireless data plane to provide modular programming capability for the entire wireless stack, while utilizing multi-core DSP architecture to achieve NFV. OpenRadio introduces a software abstraction layer to decouple wireless protocol definition from the hardware, and exposes a modular and declarative interface to program wireless protocols. OpenRF [21] is a software defined cross-layer architecture for managing MIMO signal processing with commodity Wi-Fi cards. OpenRF adopts the SDN idea and enables access points to control MIMO signal processing at physical layer, such as interference nulling, coherent beam forming and interference alignment. Through converting high-level QoS requirements of downlink flows to low-level physical layer techniques, OpenRF controller makes cross-layer decision to guarantee the transmission rate and control the interference across access points.

CloudMAC [22] is a network architecture that is aimed at having a programmable MAC layer without resorting to software radios. CloudMAC is a distributed architecture, which consists of virtual access points, wireless termination points and an OpenFlow switch. Furthermore, the 802.11 WLAN MAC processing is partially performed in virtual machines connected by an OpenFlow controlled network. Odin [23] is an SDN framework that is proposed to simplify the implementation of high level enterprise WLAN services, by introducing light virtual access point (LVAP), which is similar to the virtual access points used in CloudMAC. The decision module in Odin is an application on top of the OpenFlow controller, and a TCP connection is used between the agent and the controller to invoke commands on the agents and collect statistics from them. OpenSDWN leverages and extends the LVAP abstraction of Odin [24] to a set of programming abstractions to model the operational functions of a wireless network, namely state management, resource provisioning, network monitoring, and network reconfiguration. OpenTDMF [25] introduces TDMA to control all the stations for channel access. Similar to SDN, it adopts centralized coordination to solve channel selection and time synchronization problems.

To sum up, these SDWN solutions mainly focus on abstracting the underlying wireless physical technologies and moving as much intelligence as possible to the center of the network. However, the additional processing tasks required of the powerless access point devices and centralized controller of SDN might slow down the response to PHY or MAC layer incidents and increase the packet delay [27].

SDN and NFV are also introduced for implementation of the programmable 5G networks [28]. SoftRAN [26] redesigns the control plane functionalities cooperatively between the controller and the radio elements by introducing a virtual big-base station, to achieve the tradeoff between the optimal centralized control and the sensitive transimission delay. OpenRAN [29] is a software defined radio access network including wireless spectrum resource pool, cloud resource pool and a SDN controller. CellSDN and Softcell [30] study the software-defined core network in the LTE network. CellSDN deploys a network operating system to abstract the control functions from both accessing and forwarding devices. SoftCell is the follow-up research of CellSDN, which simplifies the operation of cellular networks and supports high-level service policies to direct traffic through sequences of middleboxes. In [31], multi-dimensional resources integration (MDRI) for service provisioning in cloud radio over fiber network (C-RoFN) was studied, and a resources integrated provisioning scheme using an auxiliary graph was introduced. In [32], an efficient cooperative scheme, namely, partial-sequence cooperative communication (PS-CC) scheme was proposed for the DCSK-CC system. In [33], multi-stratum resource optimization (MSRO) for C-RoFN was proposed to globally optimize radio frequency, optical spectrum, and baseband unit (BBU) processing resources effectively to maximize radio coverage and meet the QoS requirement.

III. MP-SDWN

Based on SDN and NFV, our proposed MP-SDWN is constructed on the open-source network devices. In this section, we give an overview of the MP-SDWN architecture, and discuss the network functions enabled by MP-SDWN.

A. MP-SDWN ARCHITECTURE

As shown in Fig. 1, our proposed MP-SDWN comprises a logically centralized Controller and distributed AP Daemons that reside on physical AP devices for virtualizing and programming the wireless components. The Controller and the AP Daemons are connected through OpenFlow switches. The entities are described as follows.

1) CONTROLLER

As an SDN controller, the Controller enables applications to orchestrate the underlying physical wireless network entities. The Controller provides a set of interfaces (the northbound interface) to the applications and translates their requests into a set of commands (the southbound interface) to the network executing devices. It maintains a view of the network components including users, access points, applications and OpenFlow switches, and performs the centralized functions including user authentication; creating, migrating and releasing of MVAP (*multi-connection virtual access point, which forms the same virtual access point over different physical access points.*) for per-user; user and network-slice management; network performance monitoring and resources scheduling; etc.

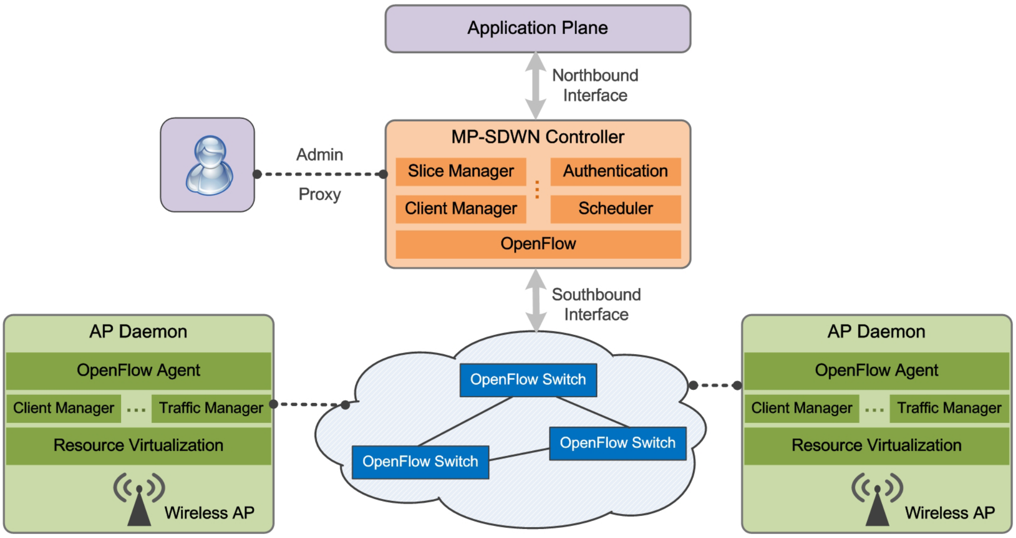


FIGURE 1. System architecture of the proposed MP-SDWN.

2) AP DAEMON

An AP Daemon runs on the physical access points, and executes the command from the Controller to orchestrate the wireless network, measures and reports the MVAP performance of users on access points. Firstly, it takes over the WiFi devices and virtualizes high-level wireless functions of 802.11 MAC protocol for different network slices. Secondly, it maintains MVAP and wireless flow transmission rules (WFTR) for each user, dispatching and forwarding his/her traffic flow according to flow-tables in MVAP, and differentiating flow priorities among diverse applications according to the rules in WFTR. Thirdly, as the status of user changes frequently, it sniffers the wireless frames in real time for monitoring the performance of MVAPs, to support a publish-subscribe information system when a certain frame event is triggered. Moreover, applications can access the statistics at different granularity including frame, flow, MVAP, user, OpenFlow and network slice.

3) ADMIN PROXY

The admin proxy provides a set of open programmable interfaces for system administrators, who thus can create multiple independent network slices, and inject their own routing or scheduling algorithms into network slices. The admin proxy allows administrator to exert the network control, e.g., load balancing, troubleshooting, and supports test run evaluation from injecting customized routing, flow assignment or migration algorithm into MP-SDWN core module. In addition, the performance of customized algorithm can be observed through the performance monitoring module.

B. NETWORK SLICING AND ISOLATION WITH MVAP

The proposed MP-SDWN provides network slicing to support multiple virtual WLAN running on top of the same physical infrastructure with different policies and control applications. In WLAN systems, a virtual network with a specific set of service set identifiers (SSIDs), which are independent of physical devices and can be deployed on one or more access points as needed. Fig. 2 (a) illustrates how virtual networks are slicing on top of MVAPs. A virtual network is defined as a set of physical resources and logical policies. The former includes a set of physical access points (or a set of resource requirements, such as SSIDs, throughput, etc.), users and a number of virtual switches to construct the virtual network. The latter contains how to manage and control the virtual network (network application provided by the Controller, such as mobility management, load balance, flow control, etc.) to serve the users, which are implemented through the admin proxy interface.

Furthermore, the corresponding network slice to the virtual network is maintained on the AP Daemon with a set of MVAPs, which are isolated through various independent groupings. When a user tries to join a particular SSID, the Controller chooses the best from the access point resource of the virtual network to serve the user according to its signal strength captured on multiple physical access points, and the user is automatically allocated with MVAP resource and assigned to the slice which the SSID belongs to. Network applications of this slice can only manage the users in their own virtual network through the isolation provided both on the Controller and its corresponding slice running in the AP Daemons. As network applications do not have visibility of MVAPs outside their slice, we thus achieve control logic isolation between virtual networks.

C. USER ASSOCIATION TO MULTIPLE APs WITH MVAP

In traditional WLAN systems, users need to be associated with a physical access point before transmitting data frames. The first step of the association is the discovery process, that is, a user actively sends probe request to scan for access

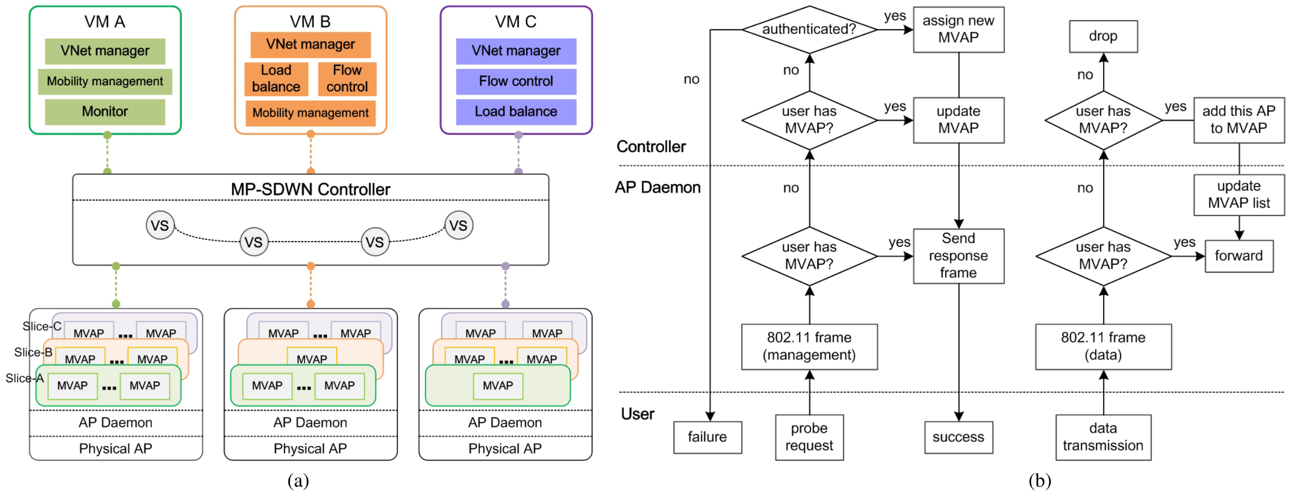


FIGURE 2. **Multi-connection virtual access point (MVAP). (a) Network slicing and isolation for virtual WLAN with MVAP. (b) Wireless frame processing with MVAP.**

points, or passively learns the beacon frames generated from access points. After getting the probe response messages, the user then decides which access point to associate with. When the user has made the choice, the association is established between the user's MAC address and the Basic Service Set ID (BSSID) of the access point. The BSSID of an access point is a MAC address of the access point's wireless interface and is different from the service set ID (SSID) of the network. However, in MP-SDWN system, each user can receive a unique BSSID to connect to, essentially making them user-specific access points and the user performs migration without need of re-association in our system. Fig. 2 (b) illustrates the process of handling a user's association using MVAP.

When a probe request is captured on an access point, AP Daemon checks whether the MVAP of this user is running on this access point; if true, the association is successful; if not, an association event is triggered and sent to the Controller. When receiving the association event, the Controller checks whether the user has the information of MVAP again. If not, it means that the user is a new one, the authentication is triggered for the user, once the user is validated, the Controller will create a new MVAP for the user and return a label to the relevant physical access points. If true, it means that the user has already accessed. Then, for new user, the Controller updates the status of MVAP and sends it back to the user with a probe response as instructed by AP Daemon, and afterwards the user completes the association handshake with its MVAP. At the same time, the Controller selects a set of access points which can serve for this user to construct the access point cluster, and keeps the MVAP running on all of them. As a result, a set of selected physical access points host a unique MVAP for this connected user, and the BSSID of the MVAP is computed from the user's MAC address and a hash value from the authentication. At last, the Controller assigns an IP address to the user, and adds it to the ISP's network slice.

D. MULTIPATH TRANSMISSION SUPPORTED WITH MVAP

To maximize the power of multiple paths, flows from a user are transmitted distributed on multipath over a set of physical access points simultaneously, which is shown in Fig. 3.

1) UPLINK WORKFLOW

The uplink workflow of multipath transmission is illustrated in Fig. 3 (a). Since AP1, AP2 and AP3 are working on the same channel, the wireless frames of the eight flows sent from the user to two servers can be received on all of them. To improve the transmission efficiency, we maintain MVAP with flow table running on each access point to control the flow forwarding. Based on the flow matching according to the flow table, the eight flows can be assigned to and transmitted through different APs (flow1 and flow4 are transmitted by AP1, flow2, flow3, flow7 and flow8 by AP2, and flow5 and flow6 by AP3), therefore, the three transmission paths are employed to accelerate user data transmission dramatically.

2) DOWNLINK WORKFLOW

The downlink workflow of multipath transmission is illustrated in Fig. 3 (b). When packets of the flows are sending back from the two servers, we use Openflow switch to forward the packets distributed to the three APs. Based on the flow matching, the eight flows can be assigned and transmitted to the right APs (flow1 and flow4 are forwarded by AP1, flow2, flow3, flow7 and flow8 by AP2, and flow5 and flow6 by AP3). In addition, according to the STA_INFO maintained on these APs, APs transform the corresponding packets of flows to wireless frames and send them to the user independently.

Moreover, based on the centralized architecture, both the flow tables running on APs and Openflow switch are controlled and updated by the Controller to ensure the coherence of flow transmission in our system.

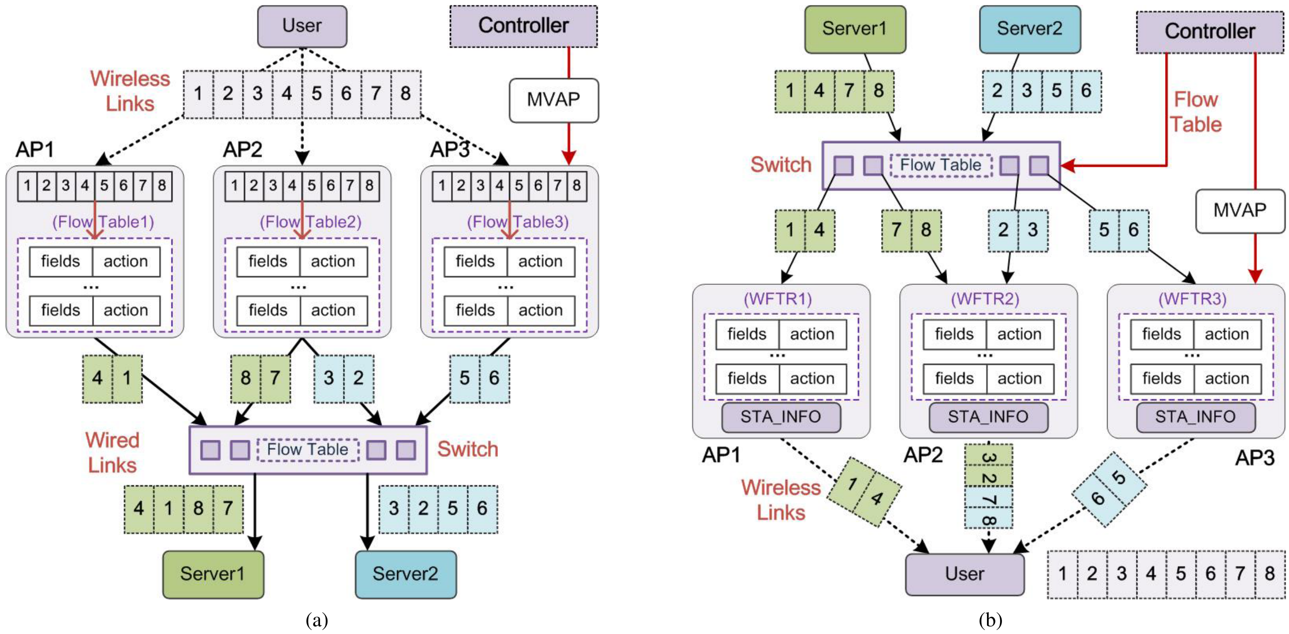


FIGURE 3. **The principle of multipath transmission for user. (a) The uplink workflow of multipath transmission. (b) The downlink workflow of multipath transmission.**

E. SECURITY WITH MVAP

For safeguarding the large number of users accessing in MP-SDWN system, we provide two security mechanisms based on MVAP to protect the users.

1) AUTHENTICATION

WPA2 is the standard for authentication in WiFi networks (defined by IEEE 802.11i). The WPA2 Enterprise is designed for enterprise networks and requires a radius authentication server and more complicated setup, but provides additional security (e.g., protection against dictionary attacks on short passwords). For a user, the Controller acts as an authentication proxy to negotiate a session key with authentication server and to add it to the user's MVAP to maintain the state. The popular web authentication type is also supported, and AP Daemon controls the request redirection from a new user; after the authentication, the session state of the user is also stored in MVAP to maintain the connection.

2) DETECTION AND CONTROL

Based on the network slicing and isolation, users from different virtual networks are restricted in their own slices, which may be useful to regular users. However for sophisticated attackers, they may imitate legal user's MAC address to trick the system to unauthorized access to the virtual resource or attack some target not belonging to their own virtual networks. An effective way is to verify the user's device information against its MAC address, so a HTTP protocol analysis method is employed in MVAP to detect the flows which are originated from the cheater, and to update the rules of the flow table in MVAP to block the cheater as quickly as possible. Furthermore, an optional way is installing an app or plugin in mobile device to generate the encrypted heartbeat message periodically to verify the MVAP of this user, but this may not be feasible to be implemented in all mobile devices.

IV. IMPLEMENTATION

A. CONTROLLER

The Controller is implemented as an extension to Floodlight OpenFlow controller, which allows us to use OpenFlow for specific functionality. The high-level architecture of the Controller is depicted in Fig. 4. The Controller is consisted of four modules and three databases. The core module is the *management module*, which controls the system components to provide services and interfaces for both users and manager, including resource allocation, MVAP control, monitoring, etc. *Configuration module* provides the interface to set up the virtual network, user service QoE and access point device for different managers. *Event module* and *message module* undertake communications with distributed AP Daemons in MP-SDWN. *Event module* is used to receive requests, status reports and monitoring data from AP Daemons while the *message module* is to dispatch the command, configuration and services to AP Daemons. The *database modules* are used to store the configuration parameters, different grained resources and monitoring data separately.

The Controller performs three main roles, that is, to set up and configure the virtual network resources from the users to the access point devices, to host wired and wireless infrastructure for network resource allocation and management and to provide programmable interfaces to reconstruct the virtual network and redefine its core functions.

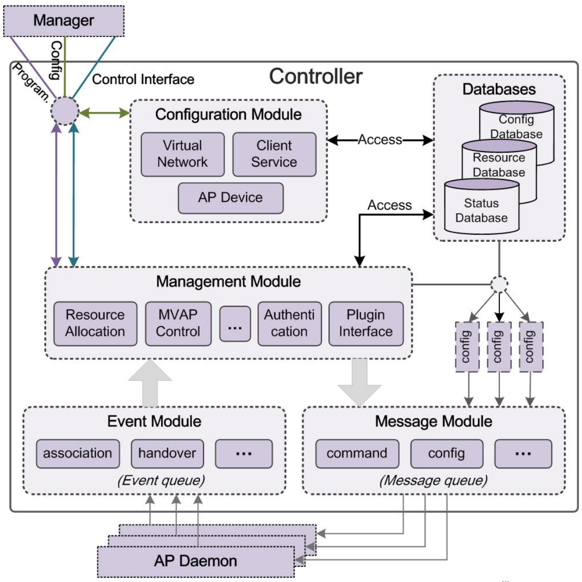


FIGURE 4. Schematic of Controller.

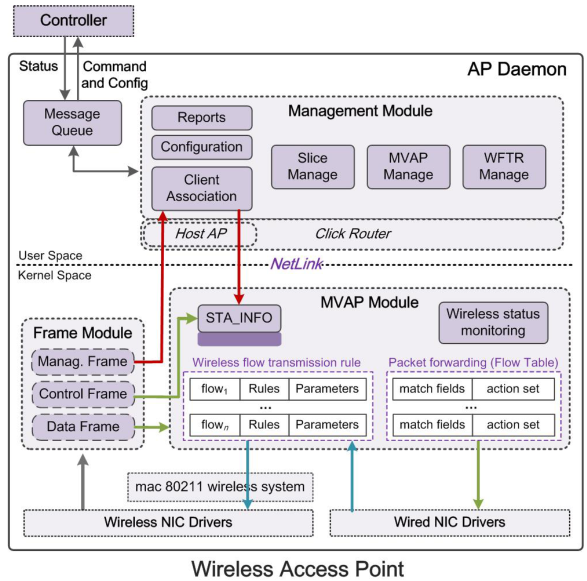


FIGURE 5. Schematic of AP Daemon.

1) CONFIGURATION

The *configuration module* handles the configure requests from the manager to set up both the physical and virtual resources, including virtual network (SSID, network scale, policy, MVAP, etc.), user service (MVAP, flow transmission rule for applications, and QoS such as throughput, latency, etc.), access point device (channel, power, policy, slicing, etc.). Two persistent databases are used to maintain record of the status, attributes, capabilities and configuration of both physical and virtual resources. The resource database is a Mysql database which contains all the resource attributes (virtual network, access point, user, etc.) in MP-SDWN and relationships between resources. The configuration database stores full slicing configuration for each manager to manage its virtual network. Finally, all the configurations are packaged and dispatched to the corresponding AP Daemons by the *message module*.

2) NETWORK MANAGEMENT

The *management module* is to perform various wireless network management functionalities, including, e.g., user access, authentication, dynamic resource allocation, MVAP control, system monitoring, mobility management, dynamic reconfiguration of the virtualized network and customized plugin management. Through the *event module*, the running status on AP Daemons and changes of users can be reported to the Controller immediately, and these running status data are stored in *status database* for decision-making and performance analysis. At the same time, if the running process needs to be controlled, the command or the response message will be triggered and dispatched to the corresponding AP Daemons by the *message module*.

3) NETWORK PROGRAMMABILITIES

The admin proxy is implemented as a set of programmable interfaces exposed to network manager or network applications, and both synchronous and asynchronous communication types are supported by the Controller. Based on the plugin management function, the customized routing or scheduling algorithms from network manager can be inserted and run within its virtual slice, while executed, send the request message to the Controller and get the corresponding action performed immediately. The network applications can share network control, such as load balancing, troubleshooting and handover through asynchronous communication API which is written as a publish-subscribe model. The publisher is taken by the Controller, whereas the application acts as the subscriber. The Controller offers a set of events and parameters to which the application can register. When an event takes place, the message will be triggered and reported to the application through the hook function.

B. AP DAEMON

AP Daemon is the local virtualization agent residing on the physical resource, which takes over both the wired and wireless network devices on the physical access point devices and virtualizes high-level wireless functions of 802.11 MAC protocol for different network slices. On AP Daemons, OpenvSwitch is employed to manage the flow table to control the wired backhaul and Click modular router to process the wireless management frames, while the data-path is preserved in the kernel space. The implementation of AP Daemon is depicted in Fig. 5. AP Daemon is developed in C and consisted of three modules running across in Linux user and kernel spaces in OpenWRT system. *Frame module* and *MVAP module* are running in the kernel space. *Frame module* identifies the wireless frames and forwards them to different processing module, e.g., management frame is sent to user association module for verification and association, control and data frames are sent to *MVAP module* for transmission. *MVAP module* controls the MVAP and schedules the resources for users with wired and wireless transmissions. *Management module* works in the user space for verifying new user requirement, controlling network slice and MVAP, executing the command from Controller and reporting the network status.

AP Daemon performs three main roles, that is, to verify and maintain the user, to control and dispatch flows from a user onto multipath and to provide flow-level wireless transmission control for user's different applications.

1) USER ASSOCIATION

To process the user request more efficiently, we keep the management frame forwarding from kernel space to user space through *netlink* interface, and transplant the function of *hostapd* into *click* to deal with user request. If it's a new user, the information is sent to the Controller to verify access authentication, otherwise, the request is to be dropped. After that, the response message can be returned quickly; if the user is accepted, *MVAP module* allocates the virtual resources to this user, including MVAP, flow table, and STA_INFO. To guarantee the wireless rate for each user, we employ the same STA_INFO structure as in mac80211 subsystem, and update the transmission rate from the control frame by the minstrel algorithm [34]. To maintain the user's connection, each MVAP needs to unicast beacon frame to its corresponding user periodically. However, since the MVAP is running on multiple AP Daemons for supporting multipath transmission, only the main access point selected by Controller can unicast beacon frame to the user. Furthermore, to reduce the overhead of per-user beacon generation, we increase the beacon interval.

2) MULTIPATH TRANSMISSION

To speed up the packet forwarding, we execute the data frame processing in the kernel space. Based on the flow table of MVAP implemented in multiple AP Daemons, the flows from a user can be assigned to and transmitted over multiple access points simultaneously. After flow matching with the packet forwarding table, the flows are submitted to *dev_queue_xmit()* function to be sent to the wired network NIC driver directly. The flow table is controlled and updated by the Controller. When the status changes, such as delete event, shift event and migration event, etc., the Controller will be triggered to recalculate and populate new configuration. Despite different applications in different conditions, the performance of multiple path transmission must depend on the efficiency of the flow assignment algorithm. Through the data frames from a user are received over multiple access points, only the main AP Daemon is permitted to generate ACKs to meet the IEEE 802.11 requirement. ACK frame generation is handled in hardware by the WiFi device due to their strict timing constraint. Based on the custom BSSID mask mechanism which is supported by Atheros WiFi driver, we implement a BSSID mask to get the common bits of all the BSSIDs being hosted in this access point device.

3) WIRELESS TRANSMISSION CONTROL IN FLOW-LEVEL

The fine-grained wireless service differentiation and transmission control are achieved by matching rules with wireless flow transmission rules (WFTR) within the wireless access points, which produce relevant actions, e.g., assigning fixed or packet transmission settings. When the 802.3 frames are captured from *__netif_receive_skb()* function, the wireless transmission parameters are set according to the rules in WFTR table, including transmission rate, power, retransmission and RTC/CTS strategy, and written into STA_INFO structure for each flow to support flow-level wireless transmission control for different applications from the same user.

V. USE CASES AND NETWORK SERVICES

MVAP simplifies the complexity of IEEE 802.11 stack by moving the operation of protocol stack into application layer, facilitates easy handling and migration of per-user state cross different physical access points, and provides unified slicing of both the wired and wireless portions of network, which allows network manager to meet the specific requirements of wireless networks. In this section, we present the typical use cases and discuss the realization of major useful network services enabled by MP-SDWN architecture.

A. USE CASES

MP-SDWN is designed to provide seamless access, high performance and differentiated network services for each user in the dense deployment scenarios.

1) MOBILITY AND MIGRATION

Based on the virtualization of 802.11 MAC protocol, MP-SDWN supports seamless mobility and dynamic resource management for each user. As illustrated in Fig. 6 (a), when more connections are maintained simultaneously for a user over a set of physical access points, the multipath can be applied to improve the stability and effectiveness of the user's migration. During the handover, the changes in wireless signal strength on nearby access points are captured, then a migration event will be triggered by access points, and finally, the controller will update user's flow assignment on the associated access points, according to the status of mobility and performance demand from the user.

2) MULTIPATH TRANSMISSION

Based on the multiple connections established over a set of selected access points, MP-SDWN provides multipath transmission to improve the network performance for each user. As illustrated in Fig. 6 (b), when a user roams around the wireless signal overlap area under a set of adjacent physical access points, MP-SDWN creates a MVAP for the user, to establish the multiple connections on a set of adjacent physical access points simultaneously. Based on the MVAP mechanism, all the traffic from the user can be assigned and transmitted simultaneously over the multiple paths at flow-level, which can improve the throughput obviously.

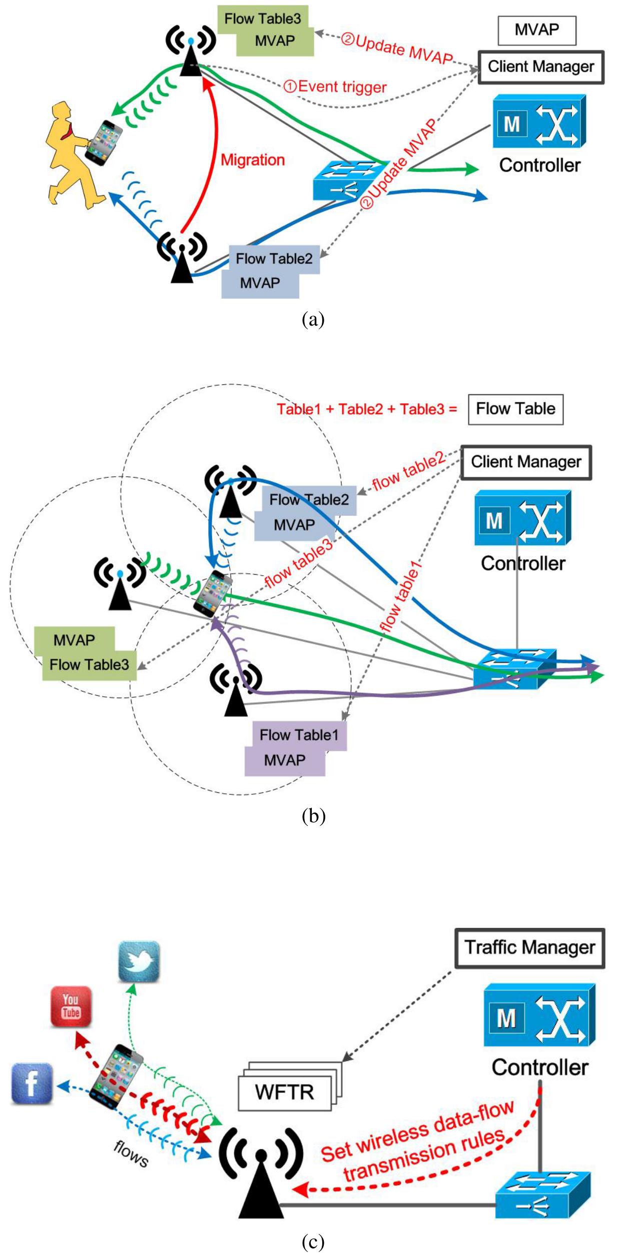


FIGURE 6. **The typical use cases based on MP-SDWN. (a) Mobility and migration. A user can be migrated seamlessly as the MVAP works on the two APs simultaneously during the handover. (b) Multipath transmission. When a user stays in the wireless signals overlap area under a set of APs, multiple transmission paths are supported based on the multiple connections that are established on the set of physical APs. (c) Flow-level transmission control. Manager can set specific wireless transmission rules for per-flow to each user through the Controller.**

3) FLOW-LEVEL TRANSMISSION CONTROL

Through maintaining the WFTR table in the mac80211 subsystem, MP-SDWN supports flow-level wireless transmission control for different applications from the same user. As illustrated in Fig. 6 (c), with the aid of the admin proxy, network administrator can use the WFTR table to set the wireless transmission parameters, such as transmission rate, power, retransmission and RTC/CTS (Request to Send / Clear to Send) strategy, to per-packet for different flows.

B. NETWORK SERVICES

Based on the programmable interfaces of the admin proxy in the proposed MP-SDWN architecture, managers can realize applications corresponding to the use cases. We have realized three typical network services as follows.

1) LOAD BALANCE

The implementation of load-balancing in a WLAN will benefit the throughput improvement for users in term of two criteria of resource scheduling. One is the airtime unfairness. Consider the scenario where multiple users are connected to one access point and share the same channel. If only one of the users is uploading traffic while other users are all downloading data, since the uplink time almost equals to the downlink time and the download throughput is shared by multiple users, this results in the airtime unfairness among the users. The other criterion is the effectiveness of bandwidth. Consider the scenario where there are a large number of users and a set of adjacent APs, and most of the users are connected to one access point with high signal strength while the other two access points serve very fewer users. Since all traffic is transmitted by the access point with high signal strength, more users have to share bandwidth with competitors than those connected to other access points. This leads to the ineffective of access point's bandwidth. The load balancing application queries the system about the resource usage periodically, including running status of users, the connection between users and access points with their corresponding RSSI (received signal strength indicator) values, and the access point load.

2) FLOW-LEVEL WIRELESS TRANSMISSION CONTROL

By applying the flow rules to packet forwarding, the differentiated services of different applications from a user can be supported in middleboxes. However, in the centralized flow control model it is difficult to achieve fine-grained control due to the formidable burden of packet matching. By taking the advantage of the WFTR's running on distributed AP Daemons, the wireless transmission rate of flows can be set to different values for different applications. For delay-sensitive applications, such as voice call and online game, setting high transmission rate can perserve high quality service for users; on the other hand, for delay tolerant applications, such as file download, the transmission rate can be reduced. This use case scheme can provide differentiated services at flow level for different applications.

3) ENERGY EFFICIENCY

A large number of WLANs have been deployed in enterprises, campuses and public areas to provide high-speed Internet connectivity. These WLANs typically consist of dense access points to assure enough capacity to meet users demand during the peak period. Meanwhile, it incurs severe energy wastage during low-utilization periods. To improve energy efficiency of dense WLANs, the most effective method is

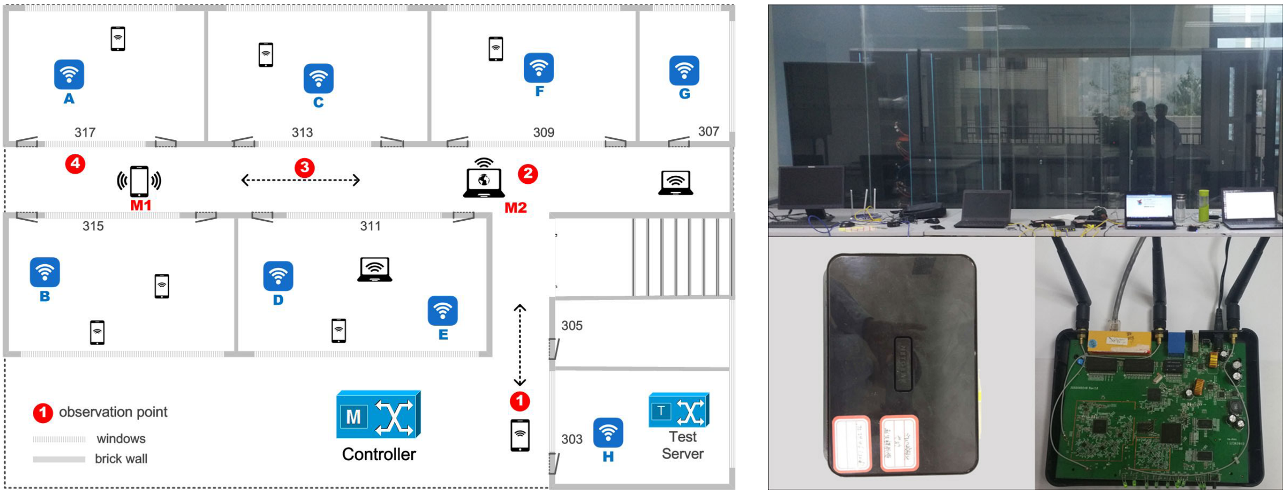


FIGURE 7. **The testbed of MP-SDWN system.**

to turn off/on the access points according to the changes of capacity requirements from users. However, the effectiveness of these methods heavily depends on the real-time status between users and access points and the resource scheduling strategy. To implement the energy efficiency application, we have realized the Controller to provide real-time data from status database to establish a comprehensive relation matrix between users and access points (including signal strength, throughput and load of access points). Then, while network coverage and user QoE are guaranteed, the low-load access points are selected to sleep. Lastly, the Controller offloads users to other access points, and turns off the selected access points to save energy.

VI. PERFORMANCE EVALUATION

The main benefit of MP-SDWN is its flexibility and the potential performance improvement with MVAP. In this section, we implement the MP-SDWN on a testbed extended from Odin[2] to evaluate the performance improvement of our MP-SDWN system against standard WiFi and other SDWN systems. First we demonstrate the performance improvement in handover, then, we quantify benchmark efficiency of the multipath transmission concept, and lastly, we show the effect of wireless transmission control at flow-level for different applications.

A. TESTBED

MP-SDWN has been implemented in a real network testbed deployed on the third floor of YiFu building on campus. As depicted in Fig. 7, the testbed consists of 20 IEEE 802.11n enabled access points, distributed in each office room across this floor, connected with OpenFlow switches to the Controller. Furthermore, all access points are restricted to same channel on 2.4GHz band. We have also deployed two mobile devices, one is an android mobile phone (M2, Huawei P8), and another is a notebook (M1, Lenovo E450); a server (located in room 301) and a number of random mobile devices. We have set up four observation points (OPs) to collect the data from the Controller when the devices move about. Moreover, we use *Iperf* toolkit in the mobile devices to generate TCP/UDP flows and capture them on the server.

AP Daemon is deployed on two types of Netgear devices, WNDR3800 and WNDR4300, and runs OpenWRT release 14.07 with the ath9k Linux driver, the embeded linux version is 3.10.49, user-level click modular router 2.0.1, and OpenvSwitch (OvS) version 2.3.90 supporting OpenFlow (OF) version 1.3. MP-SDWN controller runs Ubuntukylin-14.04 with floodlight version 1.2 on dual 4-cores CPU and 16G RAM Dell Server supported.

B. HANDOVER PERFORMANCE

With the logically centralized architecture, MP-SDWN can schedule MVAP resources seamlessly for user migration. To evaluate the effectiveness of handover performance, we consider a regular WiFi as the baseline scenario. We deploy MP-SDWN and regular WiFi systems on AP_{C-F}, and choose OP_1 to OP_2 to perform the evaluation, where the handover will take place when the user is making a round trip. In a regular WiFi network, handover is triggered by mobile device when its RSSI decreases to a threshold and the network cannot manage the mobility of users.

We generate a number of TCP or UDP flows at the user side through *Iperf*, and each TCP or UDP flow is limited to a fixed speed. Fig. 8 shows the distribution of throughput at the receiver's side when the user is performing a round trip handover. When the handover is triggered, both the TCP throughput and the UDP throughput in regular WiFi suffer a significant degradation periodically, and the user would take 2-4 seconds to re-establish the association with a new access point, which can effectively lead to the throughput degradation. As UDP protocol is a connectionless protocol, the UDP

[2]github.com/lalithsuresh/odin

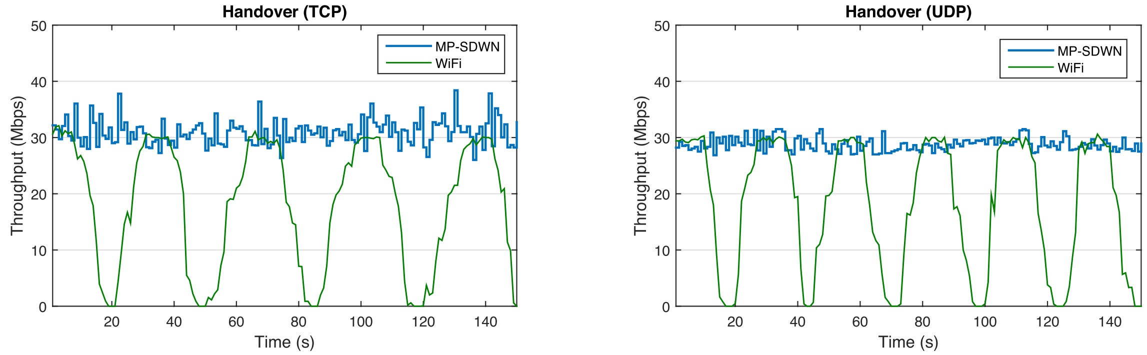


FIGURE 8. Throughput at the receiver side when the user is performing a round trip handover.

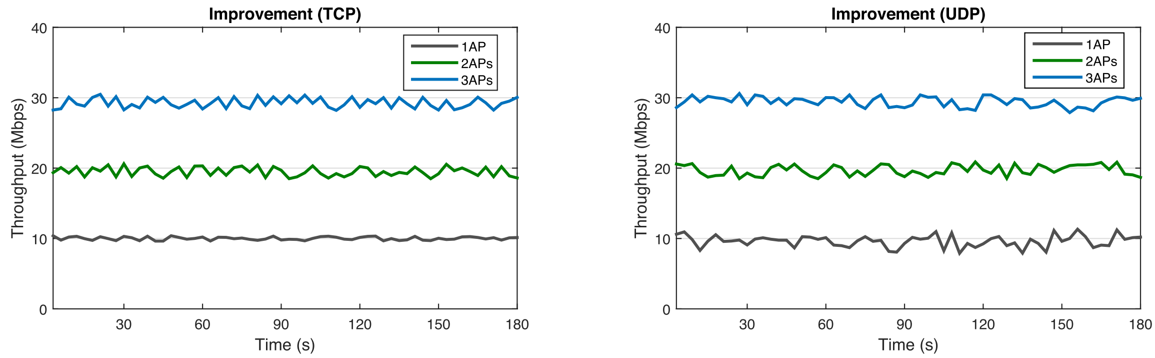


FIGURE 9. Throughput improvement with multiple APs.

throughput recovers more quickly than the TCP throughput. Furthermore, as the signal strength varies while the user moving, the TCP and UDP throughputs in regular WiFi undergo cyclical variations. In contrast, since MVAP perfectly supports seamless handovers, the TCP or UDP throughputs is very stable, and remains at about 30Mbps.

C. THROUGHPUT IMPROVEMENT WITH MULTIPATH

Since MVAP provides multiple paths to transmit the traffic from a user, it will improve the throughput of the user significantly, especially when a single access point cannot provide enough bandwidth to meet the requirement from the user. To validate the throughput improvement in the MP-SDWN system meaningfully, we restrict the bandwidth of each access point to 10Mbps, and use *Iperf* at user side to generate multiple different TCP and UDP flows. When the user slowly moves from observation point OP_1 to OP_4, we obtain the throughput changes of the user.

As clearly shown in Fig. 9, as more transmission paths are introduced to transmit the traffic from the user when the number of access points increases, both the TCP and the UDP throughputs have increased obviously. When only one access point serves for the user, due to the bandwidth being restricted on each access point, the TCP throughput fluctuates around 10Mbps. Afterwards, when more access points are employed to transmit the traffic from the user, the TCP throughput increases obviously, which reaches around 20Mbps with two access points and around 30Mbps with three access points supported. The same phenomenon appears in UDP throughput, which reaches around 20Mbps with two access points and around 30Mbps with three access points. Since the wireless environment is unstable when the user moves about, the throughput increases with some fluctuations. Furthermore, as the mobile device is not powerful enough, the increasing traffic will have to introduce more packet loss to slow down the TCP and UDP throughputs.

D. IMPACT OF THE NUMBER OF FLOWS ON USER's THROUGHPUT

As discussed above, multiple transmission paths supported on multiple access points improve user's throughput significantly. But when the number of transmission paths are fixed, is it possible to obtain more throughput with more flows for the user? To this end, we conduct experiments to analyze the impact of the number of flows on throughput.

To simulate the real network scenario, we have deployed a number of users to generate background traffic to increase load on access points, which makes each access point provide limited bandwidth available for the user. We deploy the MP-SDWN and regular WiFi systems on AP_{A-C}, and use *Iperf* to generate multiple independent TCP or UDP flows on the user at OP_4 and observe the throughput variation on the user at server side.

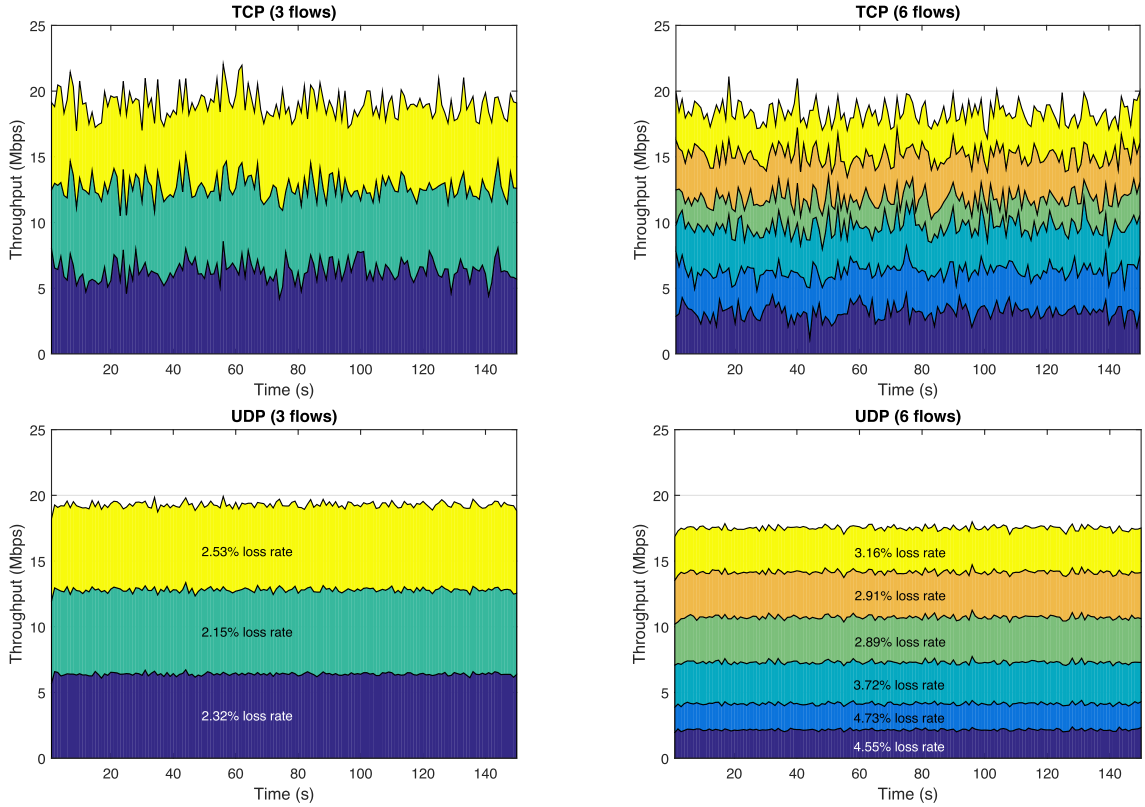
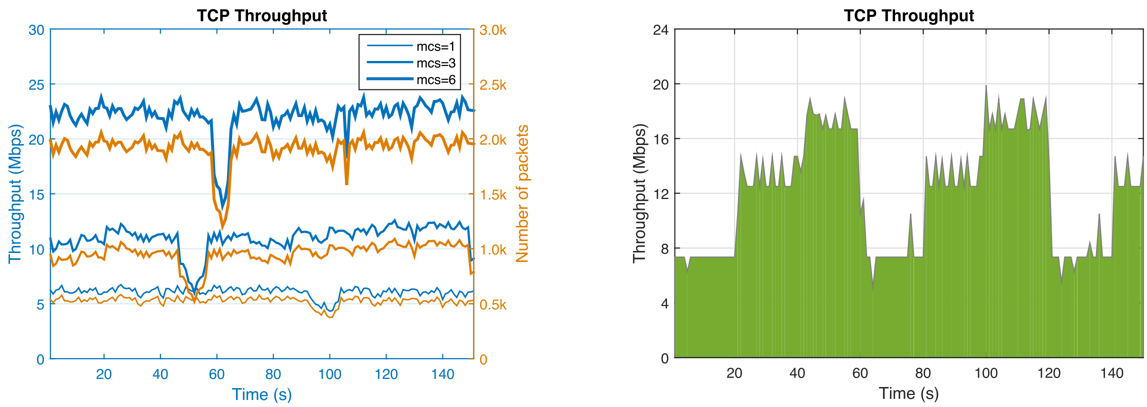


FIGURE 10. **Impact of the number of flow on user's TCP and UDP throughputs.**



(a) (b)

FIGURE 11. **Wireless transmission control at flow-level. (a) TCP throughput of flows on user device with different wireless settings. (b) TCP throughput changes with wireless flow periodical re-setting (MCS = 1, 3, 6 every 20 seconds).**

We employ three/six TCP and UDP flows, respectively, to testify the impact on throughput, as shown in Fig. 10. It can be seen that dispatching more flows onto the three access points does not necessarily obtain higher throughput on user. Interestingly, when the number of flows increases from 3 to 6, the total TCP throughput decreases nearly 1Mbps, and the throughput of each flow become uneven, for example, the throughput of one flow is obviously smaller than others. What is more, the total UDP throughput drops even more and the average loss rate is from 2.26% to 3.57%, while the throughput and loss rate of two flows are obviously lower than others. The reason is that, in our case, there are only three physical access points selected to serve the user, when more flows dispatched onto one access point, wireless bandwidth competitions among those flows would cause intense conflict, worsen packet loss and lower throughput of flows. That means we should refine the control strategy to dispatch flows on multiple access points.

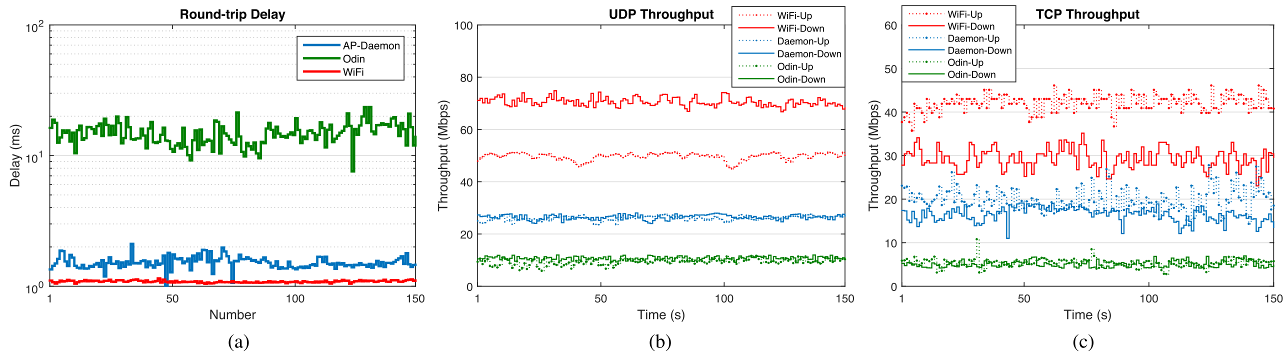


FIGURE 12. **The transmission performance comparison among AP Daemon, regular WiFi and Odin. (a) RTT between Client and Controller. (b) UDP throughput with less than 2% loss rate. (c) TCP throughput.**

E. FLOW-LEVEL WIRELESS TRANSMISSION CONTROL

Based on WFTR tables running on distributed AP Daemons, flow-level wireless transmission control is enabled in MP-SDWN for different applications from the same user. To validate the effectiveness of WFTR, we generate three independent TCP flows on user mobile device through Iperf, and configure them with different wireless transmission rules to control the wireless frames transmission speed. Moreover, we adjust the wireless transmission rate periodically and observe its effect on TCP throughput.

As shown in Fig. 11 (a), since the Modulation and Coding Scheme (MCS) of different flows are set to different values (1, 3 and 6), the wireless frames transmission rates are restricted to different levels, which directly influences the TCP throughput of flows. When the value of MCS is set to 1, the wireless frame transmission rate of the flow is quite stable, only with a small dip occurs at 100s. However, the wireless frame transmission rate fluctuates obviously following MCS increasing. When the value of MCS increases to 6, the wireless frame transmission rate becomes very unstable and suddenly drops at 62s and 108s. The reason may be that as the fixed MCS setting removes the ability of adaptive rate adjustment from flows, the frame drops would lead to sudden TCP throughput burst. As shown in Fig. 11(b), when periodically (every 20 seconds) re-setting the values of MCS (1, 3 and 6), the TCP throughput changes immediately without any delay. Although setting high MCS value increases the TCP throughput, it also brings about obvious fluctuation.

F. BENCHMARK PERFORMANCE OF AP DAEMON

To compare the data transmission performance on a single AP using AP-Daemon, regular WiFi and Odin, respectively we have deployed them in each case, it connects only one client.

The RTTs between client and Controller are shown in Fig. 12 (a). The RTT produced using regular WiFi is very stable at 1ms, and the RTT by AP Daemon is slightly larger and stable between 1ms and 2ms. However, the RTT by Odin increases sharply and fluctuates between 10ms and 20ms. To test the UDP throughput, we adjust UDP transmission speeds to keep the loss rate below 2%. As shown in Fig. 12 (b), the UDP throughput by regular WiFi is much bigger than by others, with nearly 50Mbps uplink and 70Mbps downlink; the throughput by AP-Daemon is relatively stable at 25Mbps in both directions; but by Odin it is only about 10Mbps in two ways. As shown in Fig. 12 (c), similar phenomenon is observed in TCP throughput. The uplink and downlink throughputs by regular WiFi fluctuate at 40Mbps and 30Mbps, the values of AP Daemon fluctuate at 20Mbps and 17Mbps, and the throughputs by Odin are smaller but stable at 5Mbps. Obviously, since wireless network virtualization and transmission control would bring additional frame processing tasks on to AP device, the performance of AP Daemon is not as good as that of regular WiFi. Moreover, in the test, the AP only is connected with one client, the performance degradation manifests the overhead incurred by virtualization. However, compared to Odin, as we execute the data frame processing in kernel space to reduce switching overhead between user space and kernel space, the performance of AP Daemon is far better than that of Odin, which means that our implementation of virtualization is far more efficient than that of Odin.

VII. CONCLUSIONS

With the aim of improving the performance and enhancing the management of wireless networks, we have put forward a novel Multipath-transmission Supported Software Defined Wireless Network (MP-SDWN) for WLAN systems to meet fast increasing needs from numerous applications. The eminent advantages as follows.

For high mobility and throughput, we have proposed the concept of multi-connection virtual access point (MVAP), to simplify the complexity of IEEE 802.11 protocol stack and to move the operation of protocol stack into application layer. For each user, MVAP maintains multiple connections over a set of adjacent access points simultaneously, which can provide multiple transmission paths to forward all flows from the user in parallel to enhance user's mobility and throughput.

For service differentiation, we have introduced a wireless flow transmission rule table (WFTR) into mac80211 subsystem to achieve wireless transmission control at flow-level. Cooperation with Openflow, WFTR provides flow-level wireless transmission control to meet the QoS needs for different applications on the same user.

For customized network service and management, we have devised an admin proxy in MP-SDWN that contains a set of programmable interfaces exposed for network administrator to exert the network control, e.g., load balancing, QoS policy, troubleshooting. We have prototyped three typical network services, namely, load balancing, wireless transmission control and energy efficiency.

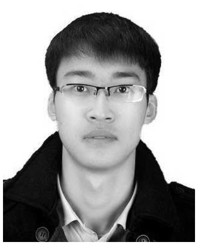
We have built up a real 802.11 protocol based testbed to evaluate the proposed system, the experimentally results show that compared to regular WiFi, MP-SDWN system achieves seamless handover and remarkable throughput improvement, and supports differentiated wireless transmission control at flow-level for different applications from the same user.

Although our work is focused mainly on WLAN systems due to fact that the proof-of-concept testbed currently only supports this technology, we believe that our proposed MP-SDWN architecture can also be useful for 5G technologies.

REFERENCES

[1] Cisco, "Cisco service provider Wi-Fi: A platform for business innovation and revenue generation," Solution Overview, 2012, pp. 1–12.
[2] E. Hossain and M. Hasan, "5G cellular: Key enabling technologies and research challenges," *IEEE Instrum. Meas. Mag.*, vol. 18, no. 3, pp. 11–21, Jun. 2015.
[3] N. Bhushan *et al.*, "Network densification: The dominant theme for wireless evolution into 5G," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 82–89, Feb. 2014.
[4] R. Chandra and P. Bahl, "Multinet: Connecting to multiple IEEE 802.11 networks using a single wireless card," in *Proc. 23rd AnnualJoint Conf. IEEE Comput. Commun. Soc. (INFOCOM)*, vol. 2. Mar. 2004, pp. 882–893.
[5] S. Kandula, K. C.-J. Lin, T. Badirkhanli, and D. Katabi, "FatVAP: Aggregating ap backhaul capacity to maximize throughput.," in *Proc. NSDI*, vol. 8. 2008, pp. 89–104.
[6] A. J. Nicholson, S. Wolchok, and B. D. Noble, "Juggler: Virtual networks for fun and profit," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 31–43, Jan. 2010.
[7] D. Giustiniano, E. Goma, A. Lopez, and P. Rodriguez, "Wiswitcher: An efficient client for managing multiple aps," in *Proc. 2nd ACM SIGCOMM Workshop Program. Routers Extensible Services Tomorrow*, 2009, pp. 43–48.
[8] H. Soroush, P. Gilbert, N. Banerjee, B. N. Levine, M. Corner, and L. Cox, "Concurrent Wi-Fi for mobile users: Analysis and measurements," in *Proc. 7th Conf. Emerging Netw. Experim. Technol.*, Dec. 2011, Art. no. 4.
[9] J. Qadir, A. Ali, K.-L. A. Yau, A. Sathiaseelan, and J. Crowcroft, "Exploiting the power of multiplicity: A holistic survey of network-layer multipath," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2176–2213, 4th. Quart., 2015.
[10] A. Ford, C. Raiciu, M. Handley, and O. Bonaventure, "TCP extensions for multipath operation with multiple addresses," document RFC 6824, IETF, 2013. [Online]. Available: http://www.ietf.org/rfc/rfc6824.txt
[11] S. Ferlin, T. Dreibholz, and Ö. Alay, "Multi-path transport over heterogeneous wireless networks: Does it really pay off?" in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 4807–4813.
[12] S. Deng, R. Netravali, A. Sivaraman, and H. Balakrishnan, "WiFi, LTE, or Both: Measuring multi-homed wireless Internet performance," in *Proc. 2014 Conf. Internet Meas. Conf.*, 2014, pp. 181–194.
[13] H. Nam, D. Calin, and H. Schulzrinne, "Towards dynamic MPTCP path control using SDN," in *Proc. IEEE NetSoft Conf. Workshops (NetSoft)*, Jun. 2016, pp. 286–294.
[14] N. McKeown *et al.*, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Apr. 2008.
[15] M. Yu, J. Rexford, M. J. Freedman, and J. Wang, "Scalable flow-based networking with DIFANE," *SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 4, pp. 351–362, Oct. 2010.
[16] K. Sood, S. Yu, and Y. Xiang, "Software-defined wireless networking opportunities and challenges for internet-of-things: A review," *IEEE Internet Things J.*, vol. 3, no. 4, pp. 453–463, Aug. 2016.
[17] N. M. M. K. Chowdhury and R. Boutaba, "Network virtualization: State of the art and research challenges," *IEEE Commun. Mag.*, vol. 47, no. 7, pp. 20–26, Jul. 2009.
[18] M. Yang, Y. Li, D. Jin, L. Zeng, X. Wu, and A. V. Vasilakos, "Software-defined and virtualized future mobile and wireless networks: A survey," *Mobile Netw. Appl.*, vol. 20, no. 1, pp. 4–18, 2015.
[19] K.-K. Yap *et al.*, "Openroads: Empowering research in mobile networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 1, pp. 125–126, 2010.
[20] M. Bansal, J. Mehlman, S. Katti, and P. Levis, "Openradio: A programmable wireless dataplane," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw.*, 2012, pp. 109–114.
[21] S. Kumar, D. Cifuentes, S. Gollakota, and D. Katabi, "Bringing cross-layer mimo to today's wireless LANs," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 387–398, 2013.
[22] P. Dely, J. Vestin, A. Kassler, N. Bayer, H. Einsiedler, and C. Peylo, "CloudMAC—An OpenFlow based architecture for 802.11 MAC layer processing in the cloud," in *Proc. IEEE Globecom Workshops*, Dec. 2012, pp. 186–191.
[23] L. Suresh, J. Schulz-Zander, R. Merz, A. Feldmann, and T. Vazao, "Towards programmable enterprise WLANs with Odin," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw.*, 2012, pp. 115–120.
[24] R. Riggio, M. K. Marina, J. Schulz-Zander, S. Kuklinski, and T. Rasheed, "Programming abstractions for software-defined wireless networks," *IEEE Trans. Netw. Service Manage.*, vol. 12, no. 2, pp. 146–162, Feb. 2015.
[25] Z. Yang, J. Zhang, K. Tan, Q. Zhang, and Y. Zhang, "Enabling TDMA for today's wireless LANs," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr./May 2015, pp. 1436–1444.
[26] A. Gudipati, D. Perry, L. E. Li, and S. Katti, "Softran: Software defined radio access network," in *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw.*, 2013, pp. 25–30.
[27] K. Sood, S. Yu, and Y. Xiang, "Performance analysis of software-defined network switch using m/geo/1 model," *IEEE Commun. Lett.*, vol. 20, no. 12, pp. 2522–2525, Dec. 2016.
[28] M. Qian, Y. Wang, Y. Zhou, L. Tian, and J. Shi, "A super base station based centralized network architecture for 5g mobile communication systems," *Digit. Commun. Netw.*, vol. 1, no. 2, pp. 152–159, 2015.
[29] M. Yang, Y. Li, D. Jin, L. Su, S. Ma, and L. Zeng, "OpenRAN: A software-defined ran architecture via virtualization," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 549–550, 2013.
[30] X. Jin, L. E. Li, L. Vanbever, and J. Rexford, "Softcell: Scalable and flexible cellular core network architecture," in *Proc. 9th ACM Conf. Emerg. Netw. Experim. Technol.*, 2013, pp. 163–174.
[31] H. Yang, J. Zhang, Y. Ji, Y. He, and Y. Lee, "Experimental demonstration of multi-dimensional resources integration for service provisioning in cloud radio over fiber network," *Sci. Rep.*, vol. 6, 2016, Art. no. 30678.
[32] P. Chen, Y. Fang, G. Han, and G. Chen, "An efficient transmission scheme for DCSK cooperative communication over multipath fading channels," *IEEE Access*, vol. 4, pp. 6364–6373, 2016.
[33] H. Yang, J. Zhang, Y. Ji, and Y. Lee, "C-RoFN: Multi-stratum resources optimization for cloud-based radio over optical fiber networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 118–125, Aug. 2016.
[34] (2009). *Minstrel Rate Adaptation Algorithm*. [Online]. Available: https://sourceforge.net/p/madwifi/svn/HEAD/tree/madwifi/trunk/ath_rate/minstrel/minstrel.txt

CHUAN XU (M'16) received the Ph.D. degree in control theory and engineering from Chongqing University, China, in 2012. He is currently an Associate Professor with the Chongqing University of Posts and Telecommunications, China. His research interests include analysis in mobile networks, software defined wireless networking, and network management. He was/is involved in several Chinese Government Projects including 973 projects and NSFC projects. He has several granted patents and authored over 30 articles in internationally major journals and conferences.



WENQIANG JIN is currently a Junior Researcher Staff Member with the Future Networks Research Institute, Chongqing University of Posts and Telecommunications, China. His research interests include software-defined wireless network and NFV.

GUOFENG ZHAO is currently a Full Professor with the School of Communication and Information Engineering in Chongqing University of Posts and Telecommunications. His main research activities concern software defined networking, network management, and modeling of wired and wireless networks. He has also worked on a number of the national and international projects. He is currently serving as a TPC Member for international conferences and journals.

HUAGLORY TIANFIELD (M'03) received the B.Eng. degree (Hons) and the M.Eng. (Research) and Ph.D.Eng. degrees in China in 1986, 1989, and 1992, respectively, all in electronic engineering (industrial automation). He held research and academic positions in China, Germany, France, and England, U.K. He has been extensively involved in professional activities. He is currently a Professor of Computing with Glasgow Caledonian University, Glasgow, U.K., since 2001. He is also the Director of Cloud and Data Research Laboratory. His research areas include cloud computing, cyber security, and big data applications. He has authored and co-authored over 180 research articles published in refereed journals and conferences, and is a frequent invited speaker at events and institutions worldwide. He is currently the Chair of the IEEE Systems, Man, and Cybernetics Society's Technical Committee on Cyber-Physical Cloud Systems, the Editor-in-Chief of the *Multiagent and Grid Systems–An International Journal*, and an Associate Editor of the IEEE Transactions on Systems, Man, and Cybernetics-Systems.

SHUI YU (SM'12) is currently a Senior Lecturer with the School of Information Technology, Deakin University. He is a member of the Deakin University Academic Board (2015–2016), a member of the AAAS and the ACM, the Vice-Chair of the Technical Subcommittee on Big Data Processing, Analytics, and Networking of the IEEE Communication Society, and a member of the IEEE Big Data Standardization Committee.

His research interest includes security and privacy in networking, big data, and cyberspace, and mathematical modeling. He has authored two monographs and edited two books, over 150 technical papers, including top journals and top conferences, such as the IEEE TPDS, the IEEE TC, the IEEE TIFS, the IEEE TMC, the IEEE TKDE, the IEEE TETC, and the IEEE INFOCOM. He initiated the research field of networking for big data in 2013. His h-index is 21.

Dr Yu actively serves his research communities in various roles. He is currently serving the Editorial Boards of the IEEE Communications Surveys and Tutorials, IEEE Access, the IEEE *Internet of Things Journal*, and a number of other international journals. He has served over 50 international conferences as a member of organizing committee, such as the Publication Chair for the IEEE Globecom 2015 and the IEEE INFOCOM 2016, the TPC Co-Chair for the IEEE Big Data Service 2015, and the IEEE ATNAC 2014 and 2015.

YOUYANG QU received the B.S. and M.S. degrees from the Beijing Institute of Technology, in 2012 and 2015, respectively. He is currently pursuing the Ph.D. degree with the School of Information Technology, Deakin University, Australia. His research interests focus on dealing with security and privacy issues in cloud computing, Internet of Things, and big data.