Introducing Network Situation Awareness into Software Defined Wireless Networks

Xing Zhao[1*], Tao Lei[2], Zhaoming Lu[2], Xiangming Wen[2] and Shan Jiang[2]
[1]China Academy of Information and Communications Technology
[2]Beijing Key Laboratory of Network System Architecture and Convergence
[2]School of Information and Communication Engineering
[2]Beijing University of Posts and Telecommunications, Beijing, P.R. China
[e-mail: zhaoxing@caict.ac.cn]
*Corresponding author: Xing Zhao

Received April 5, 2017; revised July 31, 2017; accepted October 21, 2017; published March 31, 2018

Abstract

The concept of SDN (Software Defined Networking) endows the network with programmability and significantly improves the flexibility and extensibility of networks. Currently a plenty of research works on introducing SDN into wireless networks. Most of them focus on the innovation of the SDN based architectures but few consider how to realize the global perception of the network through the controller. In order to address this problem, a software defined carrier grade Wi-Fi framework called SWAN, is proposed firstly. Then based on the proposed SWAN architecture, a blueprint of introducing the traditional NSA (Network Situation Awareness) into SWAN is proposed and described in detail. Through perceiving various network data by a decentralized architecture and making comprehension and prediction on the perceived data, the proposed blueprint endows the controllers with the capability to aware of the current network situation and predict the near future situation. Meanwhile, the extensibility of the proposed blueprint makes it a universal solution for **software defined wireless networks** SDWNs rather than just for one case. Then we further research one typical use case of proposed NSA blueprint: network performance awareness (NPA). The subsequent comparison with other methods and result analysis not only well prove the effectiveness of proposed NPA but further provide a strong proof of the feasibility of proposed NSA blueprint.

Keywords: Software defined network (SDN), Software defined wireless network (SDWN), network situation awareness (NSA), network performance awareness

1. Introduction

The increasing numbers of wireless terminals and wireless applications have brought increasing requirements for wireless data services [1]. A variety of wireless access technologies have emerged to fulfill these traffic demands. Traditionally, the physical equipment couples with concrete protocols in wireless network architectures. Therefore, the upgrade and evolution of protocols often mean the replacement and reconfiguration of underlying physical devices, which will bring enormous manpower and material costs for network operators. Aiming at this issue, software defined networking (SDN) is proposed by the Clean Slate project team in 2008 [2]. In 2011, the Open Networking Foundation (ONF) was established to further promote the development of SDN. As defined by ONF, SDN decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services [3].

With these advantages, SDN can be applied to multiple areas. For example, the authors in [27] proposed an SDN-enabled big data platform for social TV analytics. The proposed SDN-enabled big data processing system integrates SDN and Hadoop, and exploits the SDN benefit to transfer intermediate data between different processing units to accelerate the data processing rate. In this paper, we focus on introducing SDN into wireless networks to address the problems mentioned above. In fact, many researchers have worked on innovating new wireless network architectures based on the concept of SDN. Ref. [4] introduces SDN into wireless network mainly studying the convergence and centralized control of heterogeneous wireless networks. Researchers from Stanford University propose the OpenRadio wireless network architecture and further implement it in Stanford campus network. It focuses on destructing a programmable wireless data plane and providing programmatic interfaces to the monitor to program the wireless networks [5].

In the typical SDN architecture given by ONF, network intelligence is (logically) centralized in software-based SDN controllers, which maintain a global view of the network. As a result, the network appears to be the applications and policy engine as a single, logical switch. The open APIs between the SDN control and applications layers allow network applications to operate on an abstraction of the network, leveraging network services and capabilities based on the information collected by the SDN controller. Hence, the degree of precision and integrity of the information perceived by the SDN controller directly determines how accurate the upper network managements will be.

Almost all the existing research on software defined wireless networks (hereinafter referred to as “SDWN”) inherits this centralized control logic. This means that the SDN controller needs a precise perception of the global network states, including underlying physical devices information, network behaviors, and user behaviors, etc. However, most previous research focuses on the innovation of SDWN architecture and virtualization of the data plane, lacking consideration for how to ensure the high perception ability of controllers, which makes the SDWN like a supercomputer without a matching CPU with inferior performance in practical applications. Therefore, it is crucial to further study the perception of SDN controllers.

Since Tim Bass brought forward the concept of network situation awareness (NSA) [6], it has been widely used in various areas. NSA is about to perceive the network state and quantify the network situation by using appropriate assessment algorithms, and then predict the future network state based on the perceived information, and finally present the results to network

operators in a friendly way. Therefore, introducing NSA into SDWN is well advised and meaningful to ensure the SDN controller's global awareness of the whole SDN network.

However, a review of numerous works on NSA reveals the lack of application in communication areas. Most applications are used in military domains [7] and the network security area [8-10]. Only a few are involved in wireless networks [11], such as wireless mesh networks [12], cognitive radio networks [13], etc. To date, there have not been many influential studies about introducing NSA into SDWN.

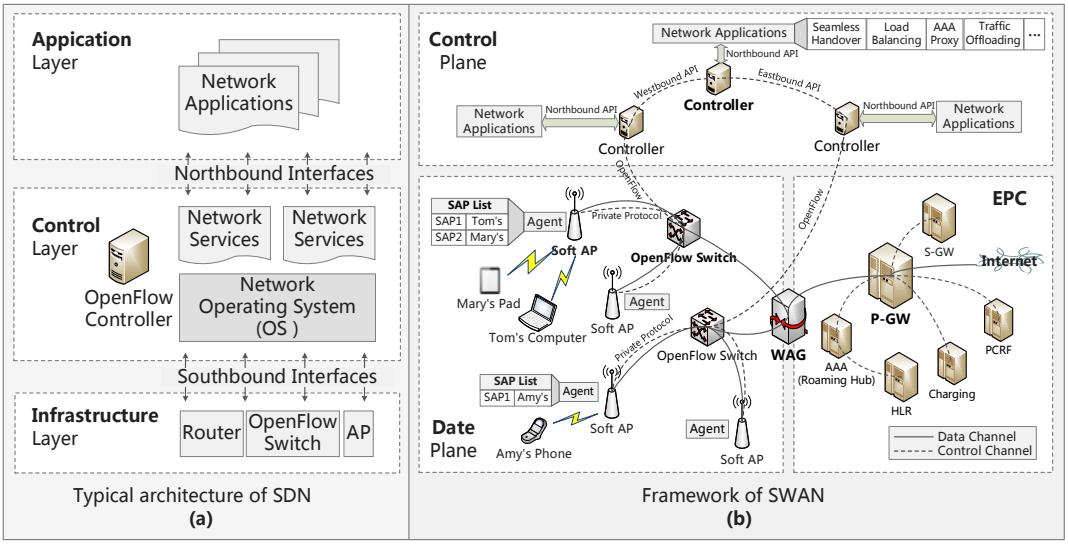


Fig. 1. (a) Typical architecture of software defined network; (b) the framework of SWAN

The main contributions of this paper can be summarized as follows.

(1) We present a software defined carrier grade Wi-Fi framework called SWAN, which is a special SDWN framework. SWAN framework mainly consists of control plane and data plane, and SAP abstraction is the key technology in SWAN.

(2) We introduce the NSA into the proposed SWAN framework to endow the control plane with global network awareness capability. We introduce the blueprint of NSA architecture for SDWN in the case of SWAN in detailed.

(3) We introduce a typical use case of proposed blueprint that is service-oriented network performance awareness (NPA). The subsequent comparison with other methods and result analysis not only well prove the effectiveness of proposed NPA but further provide a strong proof of the feasibility of proposed NSA blueprint.

This paper is structured as follows. We first investigate the typical SDN architecture and propose a framework of software defined carrier grade Wi-Fi network which is called SWAN in Section 2. Then the concepts and procedures of NSA will be introduced briefly in Section 3. Then further work on introducing the traditional NSA into the proposed SWAN framework which leads into proposing a blueprint of NSA architecture for SWAN networks is in the same section. Subsequently in Section 4 we introduce a service-oriented NPA method to enhance the controller's perception of network performance. Finally, Section 5 provides a conclusion of this paper.

2. Software defined wireless networks

2.1. Logical view of the SDN architecture

Most recent SDWN research maintains the same logic with the typical architecture of SDN defined by ONF, which consists of three layers as depicted in **Fig. 1** (a) [6]:

- ***Infrastructure layer:*** This refers to the underlying network forwarding devices, which mainly consist of OpenFlow protocol enabled SDN switches (hereinafter referred to as "OpenFlow Switch") and the abstraction of forwarding plane. It's worth noting that we list OpenFlow here because it's one of the most common southbound SDN interfaces, but there can be various alternative protocols.
- ***Control layer:*** This takes charge of maintaining the network state centrally and mainly consists of OpenFlow controllers and network operating system (NOS). The controller interacts with SDN switches through southbound interface (e.g., OpenFlow) to acquire the underlying infrastructure information; at the same time, the extendable northbound interfaces are provided by the controller to interact with upper application layer.
- ***Application layer:*** This is made up of various network applications which are implemented by programs. They can achieve multiple network managements by invoking the northbound interfaces and issuing the control commands to physical devices through the control layer.

With this software-defined model, SDN gives network managers the flexibility to configure, manage, secure, and optimize network resources via dynamic, automated SDN programs. Thereby, network operators or administrators can programmatically configure this simplified network abstraction rather than having to hand-code tens of thousands of lines of configuration scattered among thousands of devices [6].

2.2. SWAN: a framework for software defined carrier grade Wi-Fi networks

Based on the typical SDN architecture, we try to introduce its idea into wireless networks, and propose our novel framework for software defined carrier grade Wi-Fi networks, which is called "SWAN". As depicted in **Fig. 1** (b), the framework mainly consists of the control plane, and Wi-Fi access networks which are also known as the data plane.

2.2.1. SAP abstraction

SAP is constructed to abstract the connection between UE (User Equipment) and AP (Access Point). The SAP contains the status information of Layer 2 and Layer 3 which is needed to establish a connection between UE and AP. Each UE has a unique SAP to connect to. From the UE's perspective, an SAP is a general 802.11 AP that handles the regular 802.11 association handshakes with the UE. Each physical AP can host multiple SAPs, so each physical AP can support multiple users to access. In order to distinguish different SAP, each SAP has a unique BSSID (Basic Service Set Identifier). The concept of SAP abstracts the connection status between UE and AP, thus giving the controller the ability to control their connection status according to corresponding network management demands.

2.2.2. Data plane

The data plane is composed of physical APs with SWAN agents running on it, OpenFlow switches, and Wireless Access Gateway (WAG).

The physical APs in SWAN are fit APs. Only the lower MAC control frames which have real-time constraints are generated by the physical APs. Management frames are generated by the SWAN agents. The physical AP with agent on it is called a soft AP which denotes "software defined AP".

The purpose of constructing SWAN agent is to reduce the controller's processing pressure. SWAN agents run on the top of physical APs and can handle some local control logical. Each agent carries the corresponding SAPs of UEs that are connecting with this physical AP.

OpenFlow switch in the data plane is a switch supporting OpenFlow protocol. It contains flow tables which specify the routing policy. Since we have added agents on the physical APs, we formulate a private protocol for the OpenFlow switches to interact with the APs. The agents on the physical APs can obtain all frames that the physical APs receive, including both management and data frames. Thus, the agents can collect radio specific information of each frame such as per-frame received signal strength (RSSI), bit-rate and information about the noise. They can submit this statistical information to the OpenFlow switches via the private protocol, and then the OpenFlow switches forward this information to the controller through the OpenFlow protocol. This means that the controller can obtain various information from the underlying devices actively in SWAN.

WAG is a gateway between Wi-Fi networks and LTE EPC. It is connected directly with the Packet Gateway (P-GW) through a secure tunnel, which forwards data packets from the Wi-Fi access networks to the external Internet.

2.2.3. Control plane

The control plane is comprised of SWAN controllers and network management applications. The SWAN controller is a SDN controller which has additional function modules for supporting 802.11 MAC layer processing. One SWAN controller controls one network domain. Interfaces between controllers are called eastbound and westbound APIs, and are used for extending the network and sharing information between different domains. The SWAN controller has a global view of the whole network. It uses OpenFlow protocol to interact with the OpenFlow switches. After acquiring the network status and statistics information from the agents on the AP, the controller can bind this information with operations into the northbound API for upper layer applications [14].

Network applications running on top of the SWAN controller execute as threads on the controller, which are easy to design and modify. They can use publish-subscribe mechanism to acquire needed information from the northbound API, which is called passive mode. Thereby they can realize varieties of user-level or network-level managements (e.g. load balancing, seamless handover, etc.) through the comprehension of those information as illustrated in **Fig. 1** (b).

3. Introducing network situation awareness into SWAN

After the introduction of SWAN in Section 2, we can see that the SWAN controller is the core unit of the whole SWAN framework. The upper applications need to acquire necessary information through the controller so as to realize varieties of network management functions. The accuracy and integrity of the information collected by the controller will directly determine whether the network management is effective. Therefore in this section, we will try

to introduce the traditional NSA into the proposed SWAN framework to endow the control plane with global network awareness capability.

3.1. Overview of network situation awareness

NSA is about to perceive the network state and quantify the network situation by using appropriate assessment algorithms, then predict the future network state based on the perceived information, and finally present the results to network operators in a friendly way. Generally, as shown in **Fig. 2**, NSA can be divided into three levels: (1) perception, (2) comprehension, and (3) projection [15]. In conducting NSA in SWAN, the meanings of each level can be summarized as below.

Perception: The goal of this level is to acquire the information related to the operation of a SWAN network, which mainly consists of three kinds: (1) underlying physical devices information, including each AP's hosted SAPs, location, signal strength, load condition, etc. (2) user behaviors, such as access request, association request, UE's identification and real-time location, etc. (3) network behaviors, such as handoff managements (e.g., handoff decision, handoff initiation and handoff execution), the construction of SAP for each UE, the distribution of various control decisions and so on.

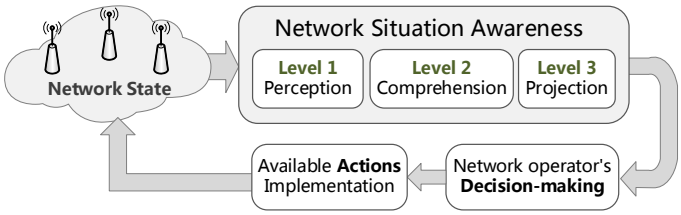


Fig. 2. The process of network situation awareness

Comprehension: After deriving the information, we need to understand what the perceived data means to the network operator's goals and objectives. The comprehension is based on the synthesis of disjointed Level 1 elements [16]. Previous research on this layer mainly focuses on knowledge representation and network situation assessment. The former is the representation of uncertain information and network components, the latter denotes using some mathematical models to make reasonable explanations of the network's current state based on the information perceived in Level 1.

Projection: As the highest level of NSA, this level is to predict the future behavior (or state) of SWAN components based on their current state derived in Level 2 and historical data collected in Level 1. For example, the controller should be able to predict the load condition of the near future based on the current load and perceived historical information such as the number of connected users, etc.

3.2. Blueprint of NSA architecture for software defined wireless networks in the case of SWAN

Previous research on NSA mostly focus on certain aspects of one network (e.g. security) and lack the overall situation awareness from underlying physical devices to upper network services and behaviors. So in this paper, based on the three-layer NSA model presented previously, we combine situation awareness with the network elements of SWAN and propose

a blueprint of NSA architecture for SWAN as shown in **Fig. 3**. In order to satisfy the awareness of the whole SWAN network, an effective NSA architecture for SWAN must fulfill the following properties:

Full network coverage: The system should have the capability to cover all the underlying physical devices in this network as well as the various network and user behaviors.

Real-time: The architecture should be able to acquire the network data in real time and ensure the time-effectiveness of the assessment or prediction results.

Simplicity: Simple modules, procedures and low computation complexity algorithms should be used as far as possible to ensure the efficiency of the whole architecture.

Effectiveness: The system must be able to assess the current network state and detect all the typical abnormal states, such as unauthorized access, underlying physical devices behaving in a faulty way, etc.

Accuracy: High accuracy often means more sophisticated mechanisms and more detailed processing steps, which will cause heavy workload and reduce the response rate of the system. So the architecture needs to address the tradeoffs between simplify and accuracy.

Extensibility: Assessment or prediction models should be convenient to add or modify, as also should the new function models be.

For the *full network coverage* demand, since one network is composed of numerous wireless APs, any AP can be a possible point of emergency. Therefore, a decentralized architecture must be used [16]. So in the proposed architecture, as shown in **Fig. 3**, perception tasks of level 1 are in the charges of agents located in each AP to ensure full network coverage.

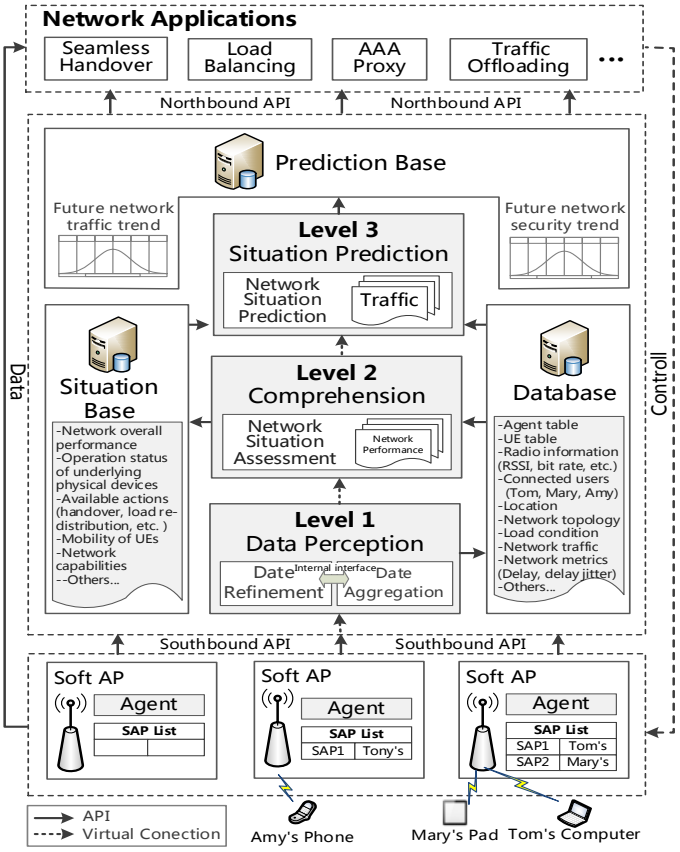


Fig. 3. Blueprint of the NSA architecture for SWAN

In addition, the data will be refreshed periodically for assuring *real-time* need. Information processing tasks are performed in the controller which has higher performance to ensure the required *accuracy*. In order to conduct a sufficient NSA of the SWAN networks, the controller contains three main parts （Level 1~Level 3） corresponding to the three levels mentioned in Section 3.1. Level 1~Level 3 covers the perception of various information and the following comprehension and projection based on those data, which can provide a more *efficient* NSA for SWAN networks.

Regarding the *extensibility* demand, as shown in **Fig. 3**, each level is further composed of several small function units and corresponding database. Those software defined function units take charge of independent functions and interact with each other through external interfaces. The databases are used for sharing information between different levels. Under this hierarchical structure logic, different units won't interfere with each other. At the same time, the programmability of those units makes adding or removing certain units simple and easy to implement. Therefore, we can directly modify or add certain function units by programming. Then we only need to provide necessary information to the neighbor units through the interfaces but no longer need to do additional work to the neighbor units, which makes it particularly easy to extend.

It is important to note that NOS is essentially responsible for logical control in the controller [17]. These function units in the same level actually are not physically independent. They are all running upon the controller (NOS) as integrated software, which can be understood as the inherent function entities existing in NOS. Just like a computer Operating System (OS) such as

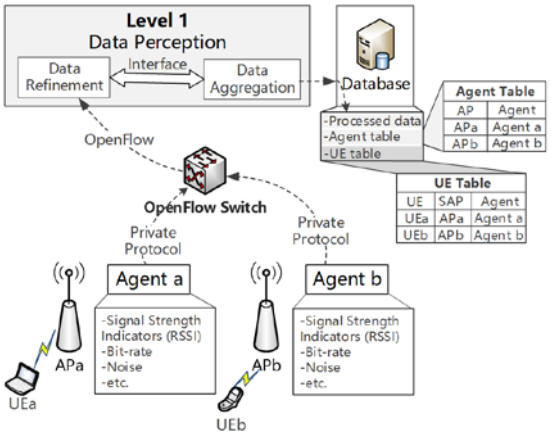


Fig. 4. Level 1: Data Perception

Windows naturally has the ability to manage the peripherals, the NSA units endow NOS with the inherent capability to perceive the various information of a SWAN network as well as give reasonable situation assessment and prediction based on it. The specific work done in each layer is elaborated deeply as below. **Table 1** lists the information required in each level to achieve a sufficient NSA in SWAN.

3.2.1. Level 1: Data perception

The first step is the acquisition of useful network information. The controller can derive much information from agents on the Aps as shown in **Fig. 4**. Since the agents can obtain all frames that the physical AP receives, including both management and data frames as elaborated in Section 2.2.2, the agents can collect radio specific information of each frame such as

per-frame's RSSI, bit-rate, noise and submit this statistical information to the controller through the OpenFlow switch actively. Agents use private protocol to interact with OpenFlow switches and OpenFlow switches use OpenFlow protocol to submit the information to the controller. Except for radio information, other underlying physical information can be derived from the agents too, such as AP's physical location, load condition, etc. The data will be updated at some regular interval to ensure the currency, therefore assuring the NSA results are always in *real time*.

After receiving all these original information from agents, the controller will conduct data refinement and aggregation to remove the possible redundancy that exists in the original data. The preprocessed data will be stored in the database and can be shared by subsequent processing procedures.

In addition, as shown in **Fig. 4**, the database also holds two configuration tables. One is the agent table which records all the agents in the network. The other one is UE table. It contains the UEs' SAP and some related information such as the particular agent hosting the SAP. The contents of the two tables will also be updated periodically by certain detection mechanisms.

As for the signaling overhead created in the process of Level 1 NSA, we take the following

Table 1. Required information for sufficient NSA in proposed blueprint

Perception	Comprehension	Projection
- Agent table - UE table - SAP's BSSID - Connected users (Tom, Mary, Amy) - Network parameters (Delay, delay jitter, packet loss rate, etc.) - Radio specific information of each frame (RSSI, bit-rate, noise, etc.) - Location information - Network topology - Load condition - Others…	- Network overall performance - Mobility of UEs - Network capabilities - Available actions (Handover, Load balancing, etc.) - Operation status of underlying physical devices - Others...	- Future network state - Future network security - Future network performance - Future network traffic flow - Others…

measures to avoid interfering the normal data transmission: (1) *all the needed information are collected at a certain time period.* Thus the perception task won't occupy the system resources all the time so that it will have relatively low impact on the system. Furthermore, the time period can be adjusted dynamically according to the traffic amount. When the traffic is busy, we can make the period longer to further reduce the influence on the system efficiency; and instead, lower it; (2) *agents submit the information to the controller through the management frames, which are transmitted separately from the ordinary data frames.* So we can set aside a special channel for the management frames and don't need to waste the bandwidth resources for data transmission. In addition, we calculate the transmission cost roughly. For example, if we collect 100 kinds of information (e.g. RSSI, BSSID, etc.) in total, and since most of the information are numeral, then for each kind of information, 16 bits are enough to present. Then the total number of bytes required in one time of perception will be 100*16/8=200 bytes, which can be counted as negligible compared to the data amount of the traffic flow.

3.2.2. Level 2: Comprehension

After data perception in Level 1, the controller needs to comprehend these data and turn these "information" into "knowledge". Comprehension level mainly refers to network situation assessment (hereinafter referred to as "NSAT"), which means analyzing the current network information and quantifying the valid operating states and abnormal states of the network through using some assessment algorithms, and then storing these situation assessment results in the situation base.

Through network situation assessment, the controller (1) *can understand the operating status of underlying physical devices*. For example, the SWAN controller keeps touch with the AP by sending some management frames periodically, so if the controller doesn't receive the default response from one AP, then this AP will be identified as "behaving in a faulty or malicious way". Then the controller can keep a table which labels each AP with "normal" or "faulty" in the situation base; (2) *can detect the mobility of UEs*. In SWAN, a UE will broadcast to all the agents. Through Level 1 data perception, the controller can acquire all the RSSI values that agents receive from the same UE. Then the situation assessment component can compare those RSSIs received at all agents which can hear the broadcast with a configured threshold. If there is a RSSI greater than the threshold and the corresponding agent is not the one which the UE is connecting to, then it means the UE has moved a lot so that it needs to be handed off to the agent with the greatest RSSI. In this way, the controller can detect the mobility of all UEs and keep track of them in the situation base as well; (3) *can perceive the available network actions such as handover, load balancing, etc.* For example, through detecting the mobility of each UE, the controller can realize if it's necessary to invoke a handover for it; through analyzing the real-time load condition per agent derived in level 1, if there are phenomena that certain APs have heavy loads while their neighboring APs have relatively quite low load, the load balancing application can be activated as available action; (4) *can aware the current network-level operating status of the network, such as network performance, network security, etc.* For example, through using certain evaluation method to aggregate the network parameters (e.g. delay, packet lose rate, etc.) information, the current performance of this network can be derived, which we'll further research and implement in Section 4.

Besides, as a super complex and large system, one network contains numerous nodes and UEs. Therefore the situation of one network is composed by the running status of various network equipment, network behaviors and user behaviors, and is manifested by the various network key factors, such as *cyber-attack information* (e.g. nodes attacking, UDP flood, IP spoofing, etc.), *traffic information* (e.g. bit rates, traffic amount, etc.), *network parameters*, etc. NSAT should be able to assess certain aspect of one network, such as network security, network performance, but should not be limited to this narrow definition. If we want to get an understanding of the overall network situation, we need to further synthesize the assessment results of all the key factors through a reasonable approach.

3.2.3. Level 3: Situation prediction

The situation prediction level takes charge of predicting the near future state of one SWAN network through using some prediction technologies based on the "knowledge" stored in the situation base and the "information" stored in the database. As mentioned previously, the comprehensive situation of one network is composed of multiple network factors. Consequently, the future network situation is the synthesis of the future status of those factors.

Currently little research considers the comprehensive situation prediction mechanisms, while much more focuses on network traffic prediction [18], which refers to using various theories and technologies to form appropriate prediction models and then make reasonable predictions on the future network traffic. Through network traffic prediction, the trend of the near future traffic can be derived, which is instructive to the design of more reasonable dynamic bandwidth allocation methods and more efficient congestion control schemes.

Fig. 5 summarizes the universal traffic prediction process based on previous research [19-21]. First, network traffic prediction unit derives necessary historical data about network traffic and chooses an appropriate prediction model according to the features of current traffic (e.g. abruptness, long range dependence, periodicity, chaos, etc.). Next some

pre-processing of the data are needed. Then we can obtain the future network traffic prediction results through substituting the processed data into chosen prediction model. The prediction results are shown in the form of a flow trend graph and stored in the prediction base to facilitate being invoked by upper network applications.

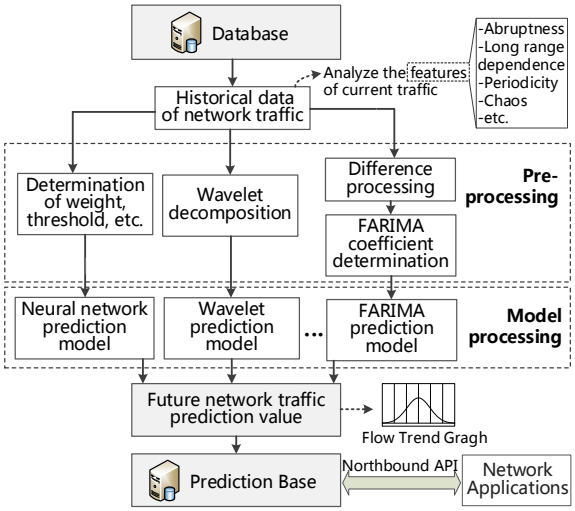


Fig. 5. The procedure of network traffic prediction

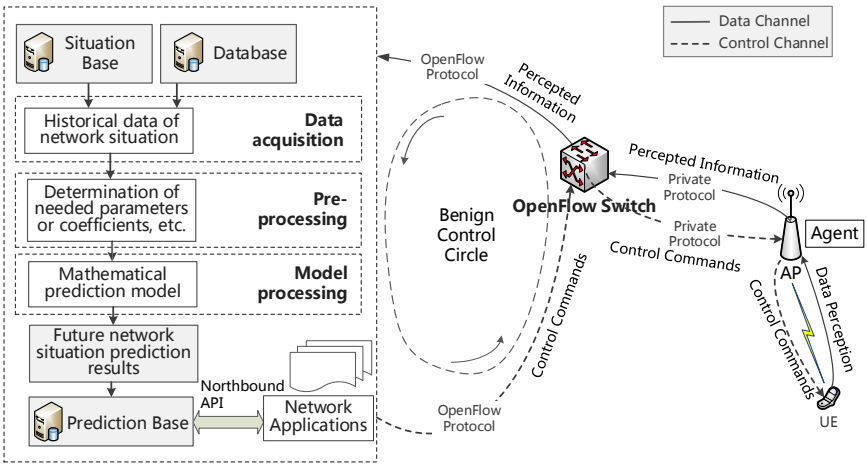


Fig. 6. Level 3: network situation prediction

Inspired from traffic prediction, situation prediction can be implemented in the same way as shown in **Fig. 6**, which is also made up of three steps: (1) *Data acquisition* (derive the current situation data from the situation base); (2) *Pre-processing* (calculate the needed parameters or determine some coefficients according to the type of the chosen prediction model); (3) *Model processing* (obtain the final network situation prediction results by using the mathematical prediction model), the results of which will also be stored in prediction base for later use.

The comprehension and projection results are supposed to be provided to upper network applications through the northbound APIs. Benefiting from the proposed NSA mechanism, the upper applications on the controller can make more appropriate management strategies according to the data perceived in Level 1 and issue those control commands to the underlying physical devices, which contributes to the optimization of network performance and prevention of abnormal conditions (e.g., AP or switch breaking down, network congestion, load imbalance); in return, the reduce of occurrence of abnormal network states also makes the perceived data more credible and instructive to the decision of network management strategies. In this way, the proposed blueprint forms a *benign control circle* as shown in **Fig. 6**.

Meanwhile, we also pay attention to the costs involved in the integration of three levels (perception, comprehension and projection). Since the three levels are separated in the proposed blueprint, each level is working independently. The controller "integrates" the three levels through sharing information between the corresponding databases. Hence the physical structures of the NSA components as shown in **Fig. 7** is advised to adopt, which distribute the function units of each level to separate servers to reduce the computational load of the main controller, and build corresponding databases in separate database servers. The servers are physically connected with cables. Each level can manipulate its corresponding database. Different servers interact with each other through software interfaces. Therefore, during the processing and integration of these three levels, the only costs involved in the main controller are from reading data from the databases. The main controller no longer needs to be involved in the complex processing work, so that it can concentrate more on managing the network based on the NSA results returned. In fact, all the physically distributed servers logically are all parts of the controller, which means they are united in logic.

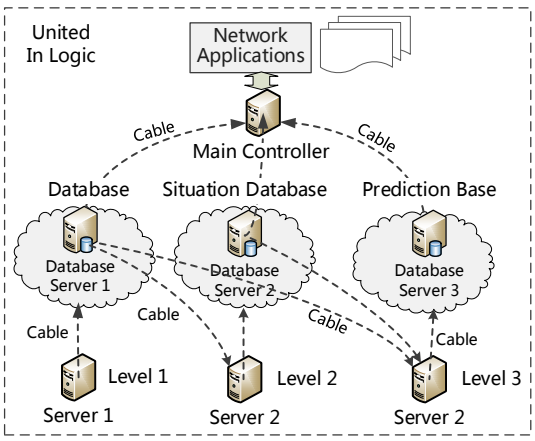


Fig. 7. Physical distribution of NSA components

In order to fulfill the *simplicity* and *effectiveness* criteria, all the assessment methods adopted in proposed NSA architecture must keep the optimal balance between computation complexity and accuracy to further reduce the costs involved as much as possible.

In addition, it's important to note that the proposed NSA blueprint is designed on the basis of the SWAN framework, but it's not limited just to be applied in SWAN. On the contrary, since the proposed blueprint actually doesn't depend too much on the specific structure of SWAN, it has the potential to be extended to other SDWN scenarios. Namely, the proposed NSA blueprint is a universal method for SDWNs rather than only applicable for one case.

4. Typical use case: service-oriented network performance awareness

After the detailed theoretical introductions of proposed NSA blueprint, in this section we'll focus on implementing one typical use case of proposed blueprint to further verify the efficiency of it. For network operators and users, network performance is one of their greatest concerns: on one hand, network performance is directly related to the operation condition and service quality of a network; on the other hand, the current performance of a network has a direct impact on a series of network behaviors such as routing, network selection, flow distribution, etc. Hence it's necessary as well meaningful to get accurate awareness of network performance.

Therefore, in this section we'll try to realize the network performance awareness (NPA) based on the proposed NSA blueprint. Here we refer to NPA as "evaluating the performance of one network in real time and presenting the evaluation results in the form of rating". Assuming that we set the standards of a "full mark" network in advance, then through the NPA progress, we're able to know the performance score of a network indicating whether this network is in a good condition. Because we implement the NPA function based on the proposed NSA blueprint, through verifying the efficiency of NPA results, the feasibility of proposed NSA blueprint can be validated too.

4.1. Implementation of service-oriented NPA

Different characteristics of various network services determine that their requirements for one network are also disparate, therefore the performance of one network varies according to the services running on it. A network may be bad when running a real-time video service but may be counted as good when browsing a web page (Best effort service). So the performance of a network shouldn't be judged sweepingly but should be evaluated combining with the type of services currently running on it. But most previous research [22-24] conducts NPAs only based on the network parameters (e.g., delay, packet loss rate, etc.), without considering from the perspective of services running on the network.

Among the various assessment methods, FAHP (Fuzzy Analytical Hierarchy Process) introduces a fuzzy consistent matrix to address the fuzziness of complex judgment, which is especially suitable for multi-attribute decision-making problems with fuzziness as NPA issues in this paper. But previous FAHP usually needs to conduct consistency checks after constructing the fuzzy comparison matrices. If the CR (Consistency Radio) [25] is not of acceptable value, the matrices must be modified by the assessors until CR is under the threshold, which not only increases the time complexity but also brings lots of additional work to the assessors. Thereby in our implementation, we introduce low-computation FAHP (L-FAHP) improved on the basis of Chang's classic FAHP [26] as our evaluation algorithm,

which has a relatively low computation complexity through omitting the consistency check that exists previously.

So aiming at the issues mentioned above, a novel service-oriented NPA is implemented based on the proposed NSA blueprint as shown in **Fig. 8**, which mainly consists of three parts. The core awareness parts are located in Level 2 NSA. Data needed during NPA are derived through Level 1 NSA.

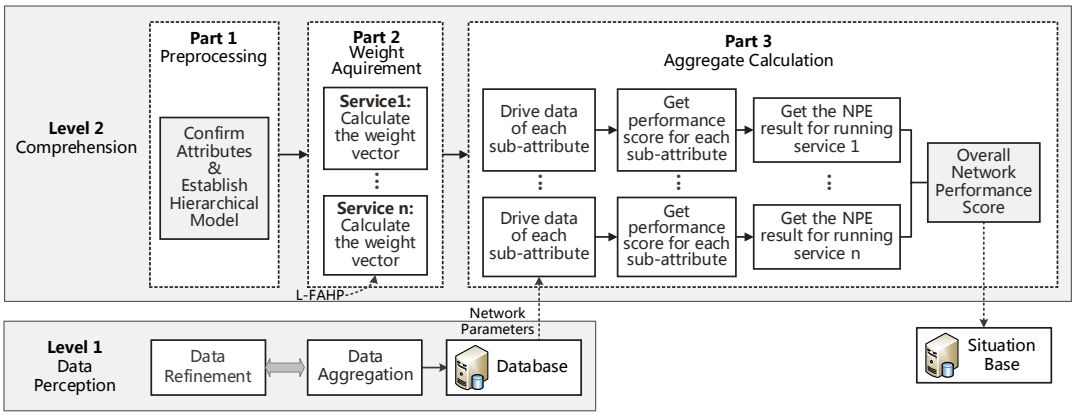


Fig. 8. The service-oriented NPA framework based on proposed NSA blueprint

Preprocessing: The primary objective in this part is to confirm appropriate evaluation attributes and establish the analytical hierarchical model. With the overall network performance as a goal, we treat each type of service as a main-attribute and network parameters as sub-attributes. Each main-attribute has a corresponding set of sub-attributes. Then the analytical hierarchical model can be established as shown in **Fig. 9**.

Weight acquirement: As the core part, the objective of this part is to derive the weight of each main-attribute and sub-attribute by using proposed L-FAHP method, which omits the consistency check that exists in previous research by introducing an experts-construct-directly algorithm, thereby significantly reducing the computation complexity and fulfill the *simplicity* demand listed in Section 3.

Aggregative calculation: After deriving the weight of each attribute, the overall NPA result can be calculated through aggregation. Firstly, original data of network parameters can be derived from data perception in Level 1 NSA. Next, based on the grading rules set in advance, we can get the score of each sub-attribute. It's worth noting that we also modify the grading rules in accordance with each service to further distinguish the influence degree of one same network parameter on different services. Through combining the weight and score of each sub-attribute obtained earlier using the following formula, the respective NPA result of each service R can be derived.

$$R = \sum_{i=1}^{n} (W_i \times S_i) \tag{1}$$

Where R represents the NPA result of each single service, n stands for the number of sub-attributes of each service, W_i represents the weight of sub-attribute i, S_i represents the score of sub-attribute i.

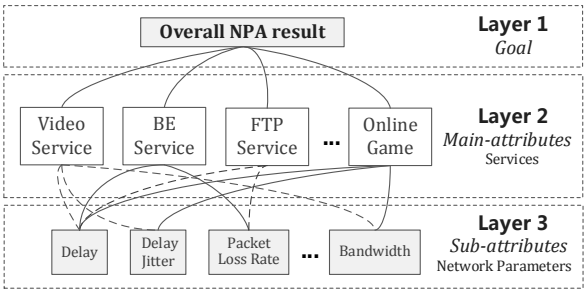


Fig. 9. The hierarchy evaluation model.

Then we can acquire the overall NPA result by combining the weight and score of each single service in the same way and complete the integrated NPA process. By analyzing the NPA result of single service, we can understand what the network performance will be when adding this type of service into existing traffic, which is conducive to distribute traffic flow and select appropriate network to access more properly based on the service type. Through analyzing the overall NPA result, we can have a more accurate cognition of current network state, which is the foundation of afterwards network managements such as routing and network selection.

4.2. Results and discussion

Due to space limitations, the specific algorithms and calculation of proposed service-oriented NPA method are no longer elaborated here. We will focus on the simulation results and provide detailed result analysis to verify the effectiveness and simplicity of it. According to the data released by Cisco [1], the proportions of video service and best effort (BE) service in global consumer internet traffic of 2013 are 60.04% and 39.87% respectively and the sum of them is 99.91%, which means the current network traffic is mainly consisted of these two services and the performance of one network is mainly determined by them too. Therefore we take those two services into consideration in the simulation, and choose three network parameters: delay, delay jitter, and packet lose rate for each service during evaluation.

Table 2. Evaluation scores

Delay (ms)	Delay Jitter (ms)	Packet Loss Rate (%)	NPA Score		
			Video Service	BE service	Overall score
65.506	1.649	0	0.8982	0.9846	0.9368
65.483	1.679	0	0.8981	0.9846	0.9368
65.625	1.865	0	0.8976	0.9845	0.9365
65.668	2.790	0	0.8960	0.9843	0.9355
65.646	2.003	0	0.8973	0.9845	0.9363
65.764	3.879	0	0.8940	0.9841	0.9343
66.084	5.085	0	0.8914	0.9836	0.9327
66.614	6.591	0	0.8880	0.9829	0.9305
72.721	14.862	3.731	0.7246	0.7331	0.7284
74.368	15.066	41.199	0.4864	0.5754	0.5262
76.668	11.714	60.606	0.4886	0.5767	0.5280
77.252	12.498	57.471	0.4864	0.5759	0.5264
77.784	11.760	85.603	0.4868	0.5761	0.5268
77.882	12.032	120.301	0.4862	0.5758	0.5263

After confirming the evaluation objects and attributes, the original network parameters data are needed for later processing. In practice, those data are derived from Level 1 perception. Here in order to facilitate comparing with other algorithms, we take data from literature [24] as sample data of network parameters. **Table 2** gives the calculated NPA scores based on the sample data. The range of scores is (0~1), in which "1" means the network is in a perfect state and "0" means the network is intolerably bad. Then we compare the NPA results with other three NPA methods [22-24] as presented in **Fig. 10**. Horizontal axes of **Fig. 10** (a~c) show the time period ranges and vertical axes show the evaluation values ranging from 0 to 1. "NPA" stands for the comprehensive NPA results of proposed framework. "NPA-V" means the NPA value of video service, "NPA-B" means BE service. "EVSSM" indicates NPA method based on entropy of vague sets and similarity measure [22]. "CRITIC" is for criteria importance through inter-criteria correlation [23]. "IEM" is for improved entropy method [24].

4.2.1. Results analysis

It can be seen from **Fig. 10** (a~c) that the trends of NPA's curves well coincide with others, which means the evaluation results obtained by proposed method are reasonable. Since video service has significant temporal continuity, it requires the network to keep in a good state during a period of time. On the contrary, BE service has high burstiness and low temporal continuity, which has relatively lower requirements for network performance. The figures show that NPA-B is higher than all the others in periods 1~8 and NPA-V is lower than NPA, CRITIC and IEM all the time, that is to say that the score of video service is lower than that of BE service in the same network condition, which is totally consistent with afore theoretical analysis.

Meanwhile, it can be observed from **Table 2** that in the time intervals 8~10, the network becomes worse sharply. So we compare the decrease rates of all the evaluation scores in **Fig. 10** (d). As shown in **Fig. 10** (d), in period 8~9, the decrease rates of NPA, NPA-V, NPA-B are apparently greater than others. In period 9~10, the decrease rate of NPA is still larger than CRITIC and is up to 70.8% higher than IEM, which indicates that the proposed NPA method as well has good sensitivity to the variety of network states.

In the traditional construction of comparison matrix, experts need to give $n(n+1)/2$ times of judgments. While by using proposed L-FAHP, a consistent fuzzy matrix can be destructed only in need of $(n-1)$ times of assessments, which reduces $(n-1)(n-2)/2$ times of assessments for the experts. When the value of n gets large, the times of judgments saved will be very considerable. Thereby it reduces the time complexity as well as the workload of experts substantially.

Furthermore, through the introduction in Section 4.1, we can see that the NPA results are directly determined by the original data of network parameters, which are usually derived through some detection means in previous NPA methods. But those detections are usually conducted in a certain point of one network, so that the accuracy and comprehensiveness of derived data cannot be guaranteed. While benefiting from proposed NSA blueprint, the

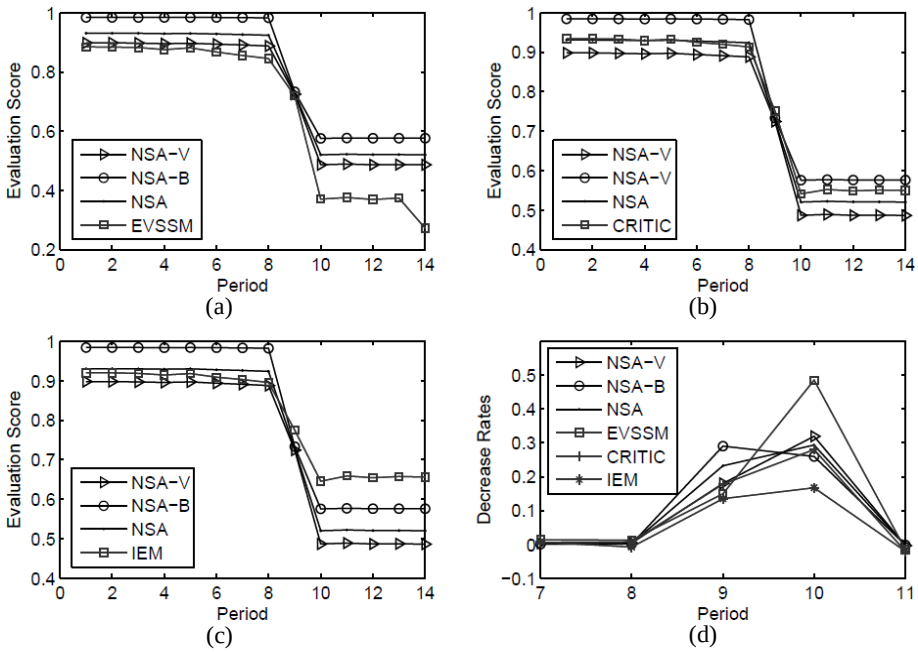


Fig. 10. The evaluation score comparison of proposed method with (a) EVSSM (b) CRITIC and (c) IEM. (d) The comparisons of the decrease rates during period 7~11.

service-oriented NPA method can acquire the original data through Level 1 data perception. Since the Level 1 NSA can collect accurate full-scale and real-time network parameters information through the agents located in each physical AP, which ensures that we can get more accurate and comprehensive original data than ever, so we can obtain more accurate NPA results than before too. That is to say, because of the advantages of proposed NSA blueprint, when it comes to practical application, the proposed NPA method can have an even better theoretical performance than previous NPA research.

In fact, the proposed NSA blueprint provides an abstract frame to do multi-level and comprehensive network awareness, the proposed NPA is the concrete instance of this frame. The efficiency of proposed NPA method exactly well proves the feasibility of proposed NSA blueprint. Furthermore, if we want to implement other use cases, we just need to fill corresponding algorithms into the NSA frame as we did in the NPA progress. Currently because of the limited time, we only implement the NPA involving Level 1 and Level 2 NSA. But we'll continue working on the construction of our integrated NSA platform, and present more use cases and experimental verifications in the future.

5. Conclusion

Since SDN was proposed, many researchers have tried to introduce it into wireless networks to address the increasing traffic demand and QoE requirements. But most of them focus on the innovation of SDWN architectures but rarely consider how to ensure the perception ability owned by the controllers. Aiming at this issue, in this paper, we firstly investigate the necessity of introducing NSA into SDWN. Then on the basis of typical SDN framework, we propose a framework for software defined carrier grade Wi-Fi networks which is called SWAN and briefly present its architecture. Then more research focus on introducing the concept of NSA

into proposed SWAN framework and creating a universal NSA blueprint for SDWN architectures. In this blueprint, data perception tasks are distributed to the agent in each AP. Comprehension and prediction tasks are taken charge by the controller. The cooperation of agents and controllers endows SDN controllers with the capability to aware the current and near future situation of one SWAN network, thereby essentially improving SWAN controller's perception of the network. Then aiming at a typical application scenario of this blueprint: network performance awareness, we further implement a novel service-oriented NPA function based on this blueprint, which evaluates the network performance from the perspective of services running on this network. The results analysis not only verifies the effectiveness of proposed NPA method, but also validates the proposed NSA blueprint is feasible in practical application.

Acknowledgments

This research is supported by the WLAN achievement transformation based on SDN of Beijing Municipal Commission of Education, the grant number is 201501001.

References

[1] Cisco VNI, "Cisco Visual Networking Index: Global Mobile data Traffic Forecast Update 2013-2018," *Cisco Public Information*, 2014.

[2] N. McKeown, S. Shenker, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, J. Turner, "OpenFlow: Enabling Innovation in Campus Networks," *Acm Sigcomm Computer Communication Review*, vol. 38, p. 69-74, 2008. Article (CrossRef Link)

[3] ONF White Paper, "Software-defined networking: The new norm for networks," 2012.

[4] S. Costanzo, L. Galluccio, G. Morabito, S. Palazzo, "Software Defined Wireless Networks: Unbridling SDNs," in *Proc. of European Workshop on Software Defined Networking, IEEE*, pp. 1-6, 2012. Article (CrossRef Link)

[5] M. Bansal, J. Mehlman, S. Katti, P. Levis, "Openradio: a programmable wireless dataplane," in *Proc. of* the ACM first workshop on Hot topics in software defined networks, pp. 109-114, 2012. Article (CrossRef Link)

[6] T. Bass, "Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems," in *Proc. of Proceedings of the Iris National Symposium on Sensor & Data Fusion*, p. 24-27, 1999.

[7] X. Yang, W. Shan, L. Jia, "Technology of Situation Awareness Based on Radar Network in Cyberspace," in *Proc. of IEEE International Conference on Green Computing and Communications, IEEE and Internet of Things. IEEE*, pp. 1505 - 1508, 2013. Article (CrossRef Link)

[8] R. Xi, S. Jin, X. Yun, Y. Zhang, "CNSSA: A Comprehensive Network Security Situation Awareness System," in *Proc. of 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE*, pp. 482-487, 2011. Article (CrossRef Link)

[9] J. Lai, H. Wang, L. Zhu, "Study of network security situation awareness model based on simple additive weight and grey theory," in *Proc. of International Conference on Computational Intelligence and Security, IEEE*, vol. 2, 1545-1548, 2006.

[10] S. Lu, X. Wang, L. Mao, "Network security situation awareness based on network simulation," in *Proc. of Workshop on Electronics, Computer and Applications, IEEE*, pp. 512-517, 2014. Article (CrossRef Link)

[11] S. Sharma, A. R. Nix, S. Olafsson, "Situation-aware wireless networks," *IEEE Commun. Mag.*, vol. 41, no. 7, pp. 44-50, 2003. Article (CrossRef Link)

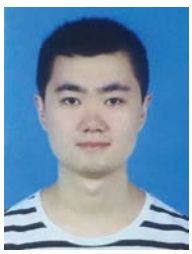
[12] G. Liao, C. Chen, S. Hsu S, T. Wu, H. Chao, "Adaptive situation-aware load balance scheme for mobile wireless mesh networks," in *Proc. of Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE*, pp. 391-396, 2011.Article (CrossRef Link)
[13] S. Krishnamurthy, S. Venkatesan, R. Prakash, "Control channel based MAC-layer configuration, routing and situation awareness for cognitive radio networks," in *Proc. of Military Communications Conference, MILCOM, IEEE*, pp. 455-460, 2005.
Article (CrossRef Link)
[14] H. Kim, N. Feamster, "Improving network management with software defined networking," *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 114-119, 2013. Article (CrossRef Link)
[15] M.R. Endsley, E.S. Connors, "Situation awareness: State of the art," in *Proc. of Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, IEEE*, pp. 1-4, 2008.Article (CrossRef Link)
[16] M. Panteli, P.A. Crossley, D.S. Kirschen, D.J. Sobajic, "Assessing the impact of insufficient situation awareness on power system operation," *IEEE Trans. on Power Systems*, vol. 28, no. 3, pp. 2967-2977, 2013. Article (CrossRef Link)
[17] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, "NOX: towards an operating system for networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 3, pp. 105-110, 2008. Article (CrossRef Link)
[18] R. Li, Z. Zhao, X. Zhou, J. Palicot, H. Zhang, "The prediction analysis of cellular radio access network traffic: From entropy theory to networking practice," *IEEE Commun. Mag.*, vol. 52, no. 6, pp. 234-240, 2014. Article (CrossRef Link)
[19] L. Xiang, X. Ge, C. Liu, L. Shu, C.X. Wang, "A new hybrid network traffic prediction method," in *Proc. of IEEE Global Telecommunications Conference (GLOBECOM 2010)*, pp. 1-5, 2010. Article (CrossRef Link)
[20] V. Alarcon-Aquino, J.A. Barria, "Multiresolution FIR neural-network-based learning algorithm applied to network traffic prediction," *IEEE Trans. on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 36, no. 2, pp. 208-220, 2006.
Article (CrossRef Link)
[21] T. Hongjian, Y. Yahui, "Network traffic prediction based on multi-scale wavelet transform and mixed time series model," in *Proc. of 9th International Conference on Computer Science & Education (ICCSE) IEEE*, pp. 696-699, 2014. Article (CrossRef Link)
[22] Y. Qian, Y. Guo, J. Song, K. Fu, "Network performance comprehensive evaluation based on entropy of vague set and similarity measure," in *Proc. of IEEE 14th International Conference on Communication Technology (ICCT)*, pp. 555-559, 2012.Article (CrossRef Link)
[23] F. Xu, "New method for similarity measures between vague sets," *Computer Engineering and Applications*, vol. 22, pp. 33-34, 2011.
[24] Y. Luo, J. Xia, T. Chen, "Comparison of objective weight determination methods in network performance evaluation," *Journal of Computer Applications*, vol. 29, no. 10, pp. 2624-262, 2009.
[25] T.L. Saaty, "A scaling method for priorities in hierarchical structures," *Journal of mathematical psychology*, vol. 15, no. 3, pp. 234-281, 1977.
[26] D. Chang, "Applications of the extent analysis method on fuzzy AHP," *European journal of operational research*, vol. 95, no. 3, 649-655, 1996. Article (CrossRef Link)
[27] Hu H, Wen Y, Gao Y, et al, "Toward an SDN-enabled big data platform for social TV analytics[J]," *IEEE network*, vol. 29, no. 5, pp. 43-49, 2015. Article (CrossRef Link)

Zhao Xing received her M.S. degree in Communication Engineering from Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2016. She is now a junior engineer of China Institute of information and communication. Her current research interests include software defined wireless networks, network performance evaluation and network situation awareness.

Lei Tao received the B.E. degree in Electronic and Information Engineering from China University of Geosciences, Beijing, China. He is currently a Ph.D. candidate student in Communications Engineering at Beijing University of Posts and Telecommunications (BUPT). His current research interests include next generation wireless network and software defined wireless local access network, WLAN management technologies. The corresponding author, email: leitao3120@bupt.edu.cn.

Wen Xiangming is the director of Beijing Key Laboratory of Network System Architecture and Convergence, where he has managed several projects related to open wireless networking. He is also the vice president of Beijing University of Posts and Telecommunications (BUPT). He received both his M.Sc. and Ph.D. in information and communication engineering from Beijing University of Posts and Telecommunications. His current research interests focus on radio resource management, software defined wireless networks, and QoE management in wireless networks.

Lu Zhaoming received the Ph.D. in Beijing University of Posts and Telecommunications (BUPT) in 2012. He joined the School of Information and Communication Engineering in Beijing University of Posts and Telecommunications (BUPT) in 2012. His research includes Open Wireless Networks, software defined wireless networks, cross-layer design for mobile video applications and so on.



Jiang Shan received the B.E. degree in Communication Engineering from Jilin University, Jilin, Changchun. He is currently pursuing his M.S. degree in Electronics and Communication Engineering at BUPT. His current research interests include soft-defined networks architecture, network performance analysis.