IEEE Open Journal of the Computer Society

Received 17 February 2021; accepted 3 March 2021. Date of publication 9 March 2021;
date of current version 1 April 2021. The review of this paper was arranged by Associate Editor S. Guo.

*Digital Object Identifier 10.1109/OJCS.2021.3064887*

# On Credibility-Based Service Function Chain Deployment

**WEIQI FAN [1], QIMEI CUI [1] (Senior Member, IEEE), XIANGJUN LI[1], XUEQING HUANG[2] (Member, IEEE), AND XIAOFENG TAO [1] (Senior Member, IEEE)**

[1] National Engineering Laboratory for Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] New York Institute of Technology, Old Westbury, NY 11568 USA

CORRESPONDING AUTHOR: QIMEI CUI (e-mail: cuiqimei@bupt.edu.cn)

The work was supported in part by the National Natural Science Foundation of China under Grant 61941114 and in part by National Youth Top-notch Talent Support Program.

**ABSTRACT** With the advancements of Software Defined Networking and Network Function Virtualization technologies, users can access the software-based service function chain (SFC), which is composed of multiple sequential virtual network function (VNF) nodes. Although SFC is more flexible and adaptive in terms of design and deployment, the security risks should not be underestimated. At present, there is a lack of security or risk assessment for SFC, and SFC deployments rarely take their security into account. However, vulnerabilities and risks can cause VNF node failure during operation, which can lead to issues such as disruptions in SFC service and user data leakage. This paper proposes the concept of SFC credibility, which quantifies the authenticity, availability, and reliability of the VNF nodes from both time and space dimensions. Then, a hierarchical credibility evaluation model is built such that VNF nodes can be selected for the user based on their trustworthiness. A credibility-based deployment strategy is further designed for SFC and the corresponding VNF forwarding graph. Furthermore, a comparative study with three existing deployment strategies has shown the advantages of the proposed method. The extensive experimental results demonstrate the improved trust degree and the acceptance rate of SFC with a limited budget.

**INDEX TERMS** Credibility evaluation, network function virtualization, service function chain deployment, virtual network function security.

## I. INTRODUCTION

In the era of fifth-generation (5G), Software Defined Network (SDN) and Network Function Virtualization (NFV) are becoming a research hotspot. To dynamically and centrally schedule the user traffic, SDN technology separates the control and forwarding planes of network equipment. NFV makes use of virtualization technologies to divide the functions of each network node into separated blocks. These functional blocks are carried out in software, and are no longer confined to the hardware structure [1]. As shown in the NFV network operation architecture of Fig. 1, the SDN controllers are available in all types of networks. The network functions of Metropolitan/Local Area Network (MAN/LAN) and service requests from enterprise/home users are implemented by virtualized software.

In a virtualized network, the user requests may need to go through different network functions. In general, the sequence of those network functions is specific, and the path formed by different network functions is called Service Function Chain (SFC) [2]. To provision customized and flexible services, users and operators can identify business requirements and create virtual network functions (VNFs) on the SFC with the aid of SDN and NFV. The SFC represents the type and order of VNF through which the data stream needs to pass. VNF Forwarding Graph (VNF-FG) is also a logical topology diagram used to represent the VNF connection relationship and flow direction. It can contain multiple SFC flows and provide multiple services. At present, SDN/NFV based SFC deployment has been applied in more and more scenarios, but the security risks incurred in the deployment process should not be undervalued.

As compared with the relatively reliable hardware equipment, software-level VNF is more vulnerable, which also exacerbates the reliability risk of the network [3]. Since the

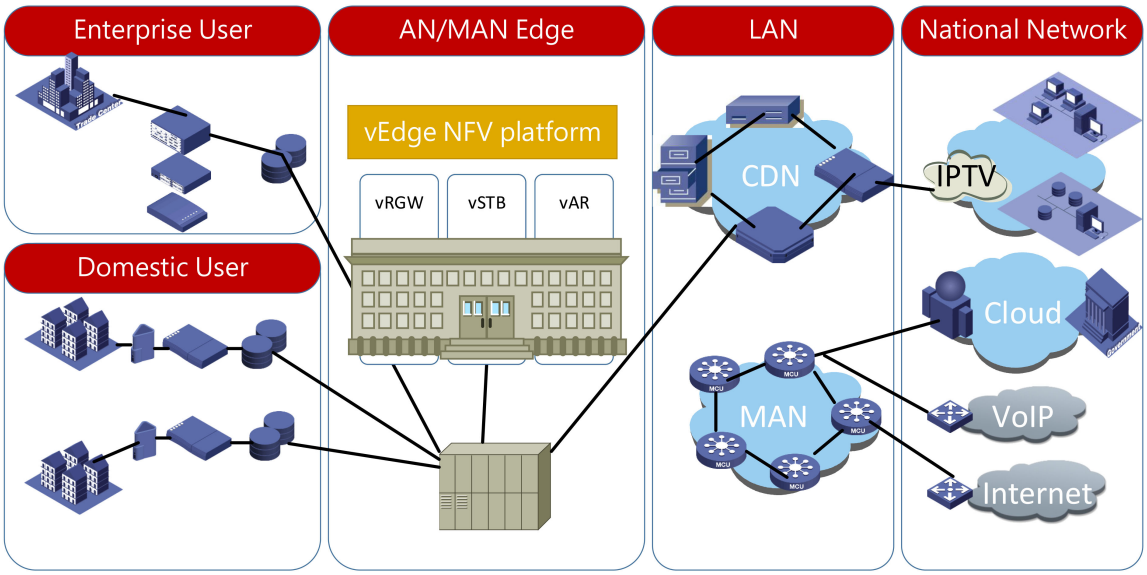


**FIGURE 1.** The NFV network Operation Diagram.

software is uploaded to the hardware node to run, the VNF failure may come from the VNF itself or the failed physical node. The resulting fuzzy VNF security boundary makes it challenging to control and eliminate the vulnerability. These uncertain threats or risks will cause VNF node failure and SFC breakage, which can further lead to service interruption, resource depletion, and user data leakage. For example, the interfaces to the virtualized network resources can be exposed when we create and manage virtual slices on top of the physical infrastructure. Moreover, the VNF equipment is also vulnerable to attacks such as Hardware Trojan Attacks, Eavesdropping Attacks, and Routing Attacks [4]. In addition, the security management in the virtualized environment is difficult, because we need to maintain end-to-end security, including end-user security, network security, and the security of the virtualized and physical resources [5].

Although the security problem has become increasingly prominent, it is rarely considered in the deployment process of SFC, and the security assessment mechanisms are also lacking. Considering various factors that impact the security and reliability of VNF and SFC, we propose a quantifiable security assessment method, and based on this method, the service function chain is further deployed. Aiming at the existing security problems in the SDN/NFV environment, we focus on improving the robustness and reliability of SFC by evolving from "passive defense" to "active security". In conclusion, the main contributions are as follows:

- The credibility of SFC is proposed as the probability that a service function chain can provide reliable services for users and keep them from being attacked. The corresponding evaluation paradigm is designed to measure credibility from three comprehensive aspects: authenticity, availability, and reliability, such that VNF with high credibility is relatively more secure.
- For the reliability aspect of SFC credibility, a unique reliability index model is constructed. By investigating the data security, defense measures, virtualization, and access control of VNF, the analytical hierarchy process can reflect the reliability of VNF more comprehensively and objectively.
- According to the evaluation paradigm of credibility, we proposed an SFC deployment strategy. Different from the current strategy, this method comprehensively considers the authenticity of nodes, the availability of resources, and the reliability of VNF. Compared with the other three strategies, our approach can effectively enhance the robustness and acceptance rate of SFC.

The rest of this article is arranged as follows: Section II introduces the related work on trust evaluation and optimization of SFC. Section III describes the credibility evaluation paradigm. Section IV introduces the reliability index model. Section V describes the credibility-based SFC deployment algorithm. Section VI presents the results of relevant simulation experiments. Finally, Section VII concludes this paper.

## II. RELATED WORK

### A. TRUST EVALUATION

Trust plays an essential role in supporting systems to overcome uncertainties and risks [6]. The trustworthiness of wireless networks involves relationships among different network entities. At present, trust evaluation has been widely adopted in various aspects of wireless networks, such as data

collection, clustering, data fusion, access control, malicious node identification, intrusion detection, and other fields [7].

1) Trust in wireless networks is a fuzzy concept and many researchers are devoted to quantifying it. The difficulty of this line of works lies in designing a reasonable method capable of proving the validity of the quantitative results. [8] designed cooperative relationship, reward system, and other calculation models, and carried out clustering by support vector machine (SVM) to improve the accuracy. [9] focused on the confidentiality of the network, and used the grey clustering method to measure the relevant indicators. The algorithm in [10] is the aggregation of qualitative evaluation and quantitative evaluation. This method quantifies the coefficients such as loss and threat value according to the attack graph, constructs the risk assessment function with the quantified results, and then divides the risk value into different security levels.

2) Since trust is mutual, many studies have focused on measuring trust relationships among nodes. In this kind of research, the emphasis is on the objectivity of trust evaluation, and the complex attributes of trust can be categorized into direct trust and indirect trust. The algorithms adopted include the entropy weight method [11] and genetic algorithm [6]. [12] proposed a distributed method which depends on the properties and recommendations of the node.

3) Beyond that, many studies focus on trust differently. [13] proposed a trust model framework based on the blockchain, [14] proposed an information theory framework based on entropy weight and probability, both of which are used for malicious node detection. With the application of machine learning more and more widely [15], many methods have been applied to security assessment. [16] studied the information model of security situation based on XML and chooses the support vector regression machine to predict the network security situation and determine the parameter values. [17] focused on the impact of time on trust evaluation and proposed a trust evaluation model based on the time frame. In addition, security and risk assessment methods are gradually applied to the cloud computing environment [18]–[20].

Although SDN and NFV bring new features to the network, and the design of SFC is free from the limitations of hardware, there is still a lack of network security or trust evaluation method and metrics. Without a specific assessment method for SFC security and reliability, there is no foundation for service function chain deployment from the security perspective. Nowadays, security in SFC has become a fuzzy concept, and it is challenging to carry out a theoretical analysis of the security level of deployed SFC.

### *B. OPTIMIZATION OF SFC*

At present, researches on the optimization of VNF/SFC can be broadly divided into three categories. 1) The first research direction focuses on improving reliability by increasing redundancy/backup [21]–[23]. Generally, the controller deploys a certain number of backup VNFs near the present VNF node. When the present VNF does not work, backup VNF nodes will be activated. However, no matter how precise the replacement algorithm is, the backup process is passive and occurs only after VNF's failure. This leads to discontinuity of services and excessive consumption of resources [24]. 2) The second direction focuses on security optimization based on the idea of mimicry defense, which can increase the difficulty of attacks and reduce the probability of a successful attack [25], [26]. However, this method can cause a big waste of communication resources, and in some cases, it may not be worthwhile to exchange communication resources for reliability. Consequently, some scholars also combined the above two methods [27], [28]. 3) The third method is based on the idea of joint optimization of various aspects of the wireless networks, including reliability, availability, communication resources, and radio resources [29]–[32]. The joint optimization of the SFC is carried out by ensuring indicators such as end-to-end QoS are satisfied. However, the reliability is measured by

$$t_{nor}/t_{en} \tag{1}$$

where $t_{nor}$ represents the uptime of VNF, and $t_{en}$ represents the entire working time of VNF. This metric is not a convincing or fundamental generalization. Because it only focuses on the results (reliable or unreliable), rather than on factors that affect reliability.

Furthermore, other authors [33] improved the reliability of SFC through various deployment algorithms. Several NFV-based use cases of ETSI records were studied in [34], and security mechanisms such as identity and access management (IAM), intrusion detection and intrusion prevention (IDS/IPS), network isolation, and data protection were considered. [35] proposed the performance metric of reliability, meta-distribution. And analyzed the reliability of heterogeneous networks based on random geometry. To sum up, most of the research works still adopt the after-action remedy, which fails to fundamentally solve the SFC optimization problem from the perspective of VNF/SFC's security mechanism.

## III. CREDIBILITY EVALUATION PARADIGM OF VNF

To quantify the trust of a VNF, **credibility** is defined as the probability that a node can provide a trusted service within a given time duration, where nodes with higher credibility are more trustworthy and secure. By considering various security-related factors, such as the type of the physical nodes and the number of resources provisioned by the VNF instance, the **credibility evaluation paradigm** consists of three metrics: authenticity, availability, and most importantly, reliability. The authenticity and availability measurement will be introduced in this section and the reliability evaluation model will be introduced with details in the next section. And Important notations in this paper are summarized in Table 1.

### *A. AUTHENTICITY EVALUATION*

From starting up to work, the security check phase of a VNF ought to encompass the following sequential steps:

- Secure boot $\alpha$: The secure boot refers to check for VNF when the VNF is starting. $\alpha \in [0, 1]$ represents the probability that a VNF is safe at startup, which depends on

**TABLE 1. System Model Parameters**

| Notation | Definition |
|---|---|
| $A$ | the authenticity evaluation of VNF |
| $V$ | the availability evaluation of VNF |
| $R$ | the reliability evaluation of VNF |
| $T$ | the credibility of VNF |
| $\theta_{SFC}$ | the credibility of SFC |
| $V_{nor}$ | the normalized $V$ |
| $V_{max}$ | the maximum $V$ |
| $V_{CPU}$ | the CPU spare space |
| $V_{MEM}$ | the remaining memory size |
| $V_{DSK}$ | the remaining hard disk capacity |
| $V_{NET}$ | the network available flow |
| $p$ | the importance of a impact factor |
| $lambda_{max}$ | the maximum eigenvalue |
| $E_\lambda$ | the eigenvector of $\lambda_{max}$ |
| $CI$ | the consistency index |
| $CR$ | the consistency ratio |
| $RI$ | the random index |
| $v$ | the evaluation level of impact factors |
| $f(v)$ | the assessment score of $v$ |
| $S$ | the judgment matrix of impact factors and basic factors |
| $W$ | the weight matrix of impact factors and basic factors |
| $G$ | the evaluation matrix of impact factors and basic factors |
| $H_i$ | the evaluation set of basic factor $i$ |
| $H$ | the evaluation set of VNF's reliability |
| $\iota$ | the division value of $v$ |
| $u_{ij}$ | the influence factor $j$ of impact factor $i$ |
| $g_{ij}$ | the evaluation set of $u_{ij}$ |
| $m$ | the number of basic factors |
| $n$ | the number of influence factors |

the certificate of faith of every software. Unless checked from the startup, we can no longer assure authenticity from the root [36]. Secure boot is the first line of protection and lays the groundwork for subsequent security assessments.

- Node authentication $\beta$: VNF is a functional block that works on the physical node. Only through the authentication of the physical node can the VNF be assured to be authentic and reliable. The authentication result can be either $\beta = 1$ (certified) or $\beta = 0$ (not certified). This step is very important because the virtual machine and user information can be loaded onto the certified node only.
- Integrity test $\gamma$: The purpose of the integrity test is to prevent a potentially malicious VNF from participating in the deployment of SFC. The result $\boldsymbol{\gamma} \in [0, 1]$ indicates the security level of the VNF, where $\boldsymbol{\gamma} = 1$ means no threat. An integrity test is divided into boundary integrity test and internal integrity test. The security boundary of a VNF can separate itself from the external environment, which could be a potential point of attack. On one side of the boundary is the attacker and on the other side is the information and data within the network. With business increases and technologies involves, the wireless networks are more heterogeneous, and the corresponding security boundaries are becoming fuzzier. A boundary integrity test can indicate whether the virtual machine's network boundary is separated from the exterior network. The internal integrity test mainly checks the presence of hazard code, vulnerabilities, injected unfamiliar information, and the presence of malware in VNF. For instance, [36] proposed an internal integrity test by monitoring whether the operating system kernel has been modified.

The above three steps will be executed in sequential order, and if one step fails, the subsequent steps will be aborted. We propose to define the **authenticity** of the NFV as a single parameter $A \in [0, 1]$, which is defined as follows:

$$A = \alpha\beta\gamma \tag{2}$$

where $A$ represents the authenticity of NFV. where A will be 0 when any step fails, and the value will be higher only when all of the three steps have high authenticity.

### B. AVAILABILITY EVALUATION

Availability refers to the probability of a trusted service being ready for use [37]. It is generally proportional to the sizes of various available resources, including CPU space, memory size, hard disk capacity, and network flow. Although there is no sequential restriction on availability between the different factors, they are Interrelated and mutually restrictive. For example, if the CPU spare space is too small, the VNF cannot be used properly even if the memory size is really large. This is shown as low availability. So, we still represent availability as a product of these factors.

$$V = V_{CPU} * V_{MEM} * V_{DSK} * V_{NET} \tag{3}$$

where $V$ represents the availability of the NFV, $V_{CPU}$ represents CPU spare space, $V_{MEM}$ is the remaining memory size, $V_{DSK}$ represents remaining hard disk capacity, $V_{NET}$ represents the available network flow.

### C. RELIABILITY EVALUATION

Reliability indicates the probability that the VNF will work normally. Traditionally, reliability is described as the ratio between the uptime to entire working time, as shown in (1). However, this definition is only one-sided and does not capture the essence of reliability. In this paper, we propose a hierarchical reliability index model detailed in Section IV.

## IV. RELIABILITY INDEX MODEL

Analytic hierarchy process (AHP) can transform complex decision problems into quantitative analysis problems through matrix operation. It is often applicable in problems with complex hierarchical structure and difficult quantitative evaluation [38]. IAF of ENISA [39] and FedRAMP [40] of USA have both studied risk control and security assessment of networks. In order to build a secure and reliable network environment, both of them also put forward the index requirements for security assessment, which is worth our reference.

In this section, according to our research experience in the field of SFC and NFV, we built the reliability index model

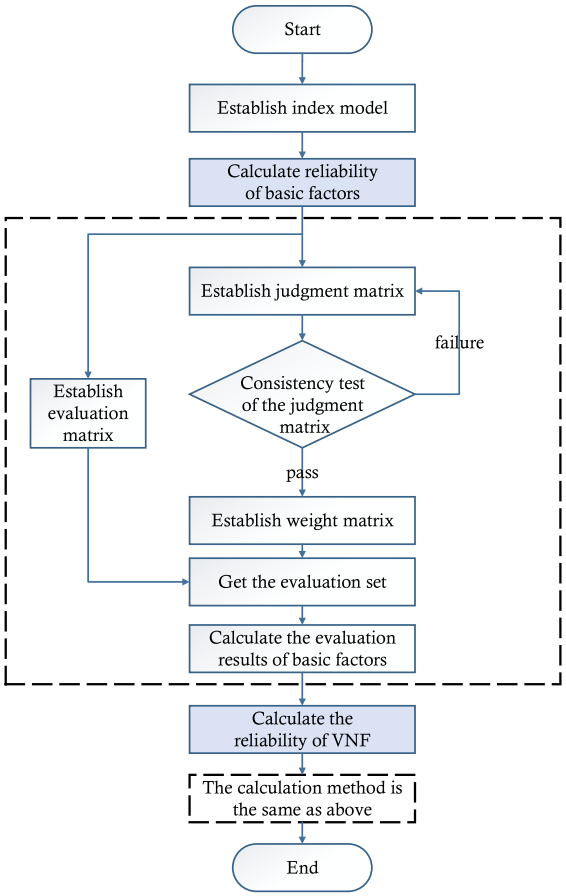


**FIGURE 2.** Flow Chart of VNF Reliability Calculation.

based on AHP by referring to the index of security assessment designed by ENISA and FedRAMP.

According to the index model, the reliability calculation process of VNF is shown in Fig. 2, which is described in detail below.

### A. ESTABLISH A INDEX MODEL

The reliability of VNF can be divided into four **basic factors**: data reliability, protection reliability, virtual reliability, and access reliability. The data reliability refers to whether the VNF can effectively protect the user's personal information and the data required by the service. Protective reliability can indicate the ability of VNF to protect against potential attacks. Virtual reliability represents the security at the software and virtualized levels. Access reliability means the access control capability of VNF. Each basic factor contains the corresponding impact factors. As shown in the following three-layer index model in Table 2, where the top layer is defined as reliability, the second layer is the basic factor, and the third layer includes various impact factors.

### B. ESTABLISH A JUDGMENT MATRIX

To quantify the reliability of an NFV node, we adopt the idea of fuzzy comprehensive evaluation method [41] to carry out

**TABLE 2.** The Reliability Index Model

| VNF Reliability | Basic Factor | Impact Factor |
|---|---|---|
| Reliability | Data reliability | Data encryption |
| | | Data integrity |
| | | Data backup |
| | | Data portability |
| | Protection reliability | Vulnerability level |
| | | Patch management |
| | | Intrusion detection |
| | | Malicious code prevention |
| | Virtual reliability | Virtual resource monitoring |
| | | Virtual resource isolation |
| | | Multi-business management |
| | | Virtual firewall |
| | Access reliability | User access control |
| | | Management platform access |
| | | Network access control |
| | | Virtual machine access |

the bottom-up multilayer calculation. After the establishment of the index model, the influence factors of the basic factors are compared in pairs and the comparative judgment matrix is constructed. The judgment matrix represents a ratio of the relative importance of the impact factors in a given basic factor.

$$S = (s_{ij})_{n*n} = \begin{pmatrix} 1 & p_1/p_2 & \cdots & p_1/p_n \\ p_2/p_1 & 1 & \cdots & p_2/p_n \\ \vdots & \vdots & \vdots & \vdots \\ p_n/p_1 & p_n/p_2 & \cdots & 1 \end{pmatrix} \quad (4)$$

where $n$ is the total number of impact factors in Table II, and $s_{ij}$ is the relative importance of impact factors $i$ and $j$. The above formula indicates $s_{i,j} = p_i/p_j$, with $p_i$ and $p_j$ being the importance of impact factors $i$ and $j$, respectively.

### C. WEIGHT ALLOCATION

Consistency test [42] is needed to determine whether the weight matrix is accurate and available. The specific calculation steps are as follows:

1) Find the Maximum Eigenvalue $\lambda_{max}$ of Matrix S and Its Corresponding Eigenvector $e_\lambda = (e_1\ e_2\ \cdots\ e_n)$;
2) Normalize $E_\lambda$;
3) Calculate Consistency Index (CI);

$$CI = (\lambda_{max} - N)/(N-1) \quad (5)$$

$N$ is the dimension of the matrix.

4) Calculate Consistency Ratio ($CR$);

Consistency ratio ($CR$) is the ratio of consistency index ($CI$) to random index (RI) for the same order matrices.

$$CR = CI/RI \quad (6)$$

Table 3 shows the random index corresponding to consistency index in this case study. The judgments are acceptable when CR is less that 0.1. In general, the consistency shows the degree of relation and relevance with respect to the main factors.

**TABLE 3.** *RI* for Different Matrix Dimensions

| $N$ | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|
| $RI$ | 0.58 | 0.90 | 1.12 | 1.24 | 1.32 | 1.41 |

**TABLE 4.** The Values of $f(v)$

| $v$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| $f(v)$ | 1.00 | 0.85 | 0.70 | 0.55 | 0.40 |

After passing the conformance test, the weight is assigned by eigenvalue method. We suppose that the maximum eigenvalue is $\lambda_{max}$ and the corresponding eigenvector is $E_\lambda = (e_1 \ e_2 \ \cdots \ e_n)$. By normalizing the element values in the eigenvectors, the final weight values of all the impact factors in the basic factors can be obtained.

$$w_i = \frac{e_i}{\sum_{i=1}^{n} e_i} \tag{7}$$

Further, we can get the weight matrix $W = (w_1 \ w_2 \ \cdots \ w_n)$.

### D. ESTABLISH EVALUATION MATRIX

After that, the specific situation of the impact factor should be evaluated. The evaluation level $v$ is divided into 5 items. Define the assessment score as $f(v)$. Table 4 shows the respective values of $f(v)$.

An impact factor $u_{ij}(i = 1, \ldots, m; \ j = 1, \ldots, n)$ belong to the basic factor $i$, where $m$ and $n$ are the numbers of basic factors and impact factor, respectively. The division value of $v_k(k = 1, \ldots, 5)$ is obtained as follows:

$$\iota_{ijk} = \frac{\xi_k}{\sum_{i=1}^{5} \xi_k} \tag{8}$$

The influence factor $u_{ij}$ needs to be graded by different experts or artificial intelligence machines. $\xi_k$ refers the time that $u_{ij}$ is graded in $v_k(k = 1, \ldots, 5)$, and $\iota_{ijk}$ refers the weight. So the evaluation set of $u_{ij}$ is

$$g_{ij} = \begin{pmatrix} \iota_{ij1} & \iota_{ij2} & \iota_{ij3} & \iota_{ij4} & \iota_{ij5} \end{pmatrix} \tag{9}$$

Further, the evaluation set of all the impact factors of the basic factor $i$ is obtained, thus we will obtain the total evaluation matrix.

$$G_i = \begin{pmatrix} g_{i1} \\ g_{i2} \\ \vdots \\ g_{i1} \end{pmatrix} = \begin{pmatrix} \iota_{i11} & \iota_{i12} & \cdots & \iota_{i15} \\ \iota_{i21} & \iota_{i22} & \cdots & \iota_{i25} \\ \vdots & \vdots & \vdots & \vdots \\ \iota_{in1} & \iota_{in2} & \cdots & \iota_{in5} \end{pmatrix}_{n \times 5} \tag{10}$$

In this paper, $n$ is 4 and $m$ is 4.

### E. CALCULATE THE EVALUATION RESULTS

It is known from step C that the weight matrix is $W = (w_1 \ w_2 \ w_3 \ w_4)$. And $W_i = (w_{i1} \ w_{i2} \ w_{i3} \ w_{i4})$ is defined as the weight vector of the basic factor $i$. Reliability evaluation set of basic factors $i$ is obtained as follows:

$$H_i = W_i \times G_i = \begin{pmatrix} \iota_{i1} & \iota_{i2} & \iota_{i3} & \iota_{i4} & \iota_{i5} \end{pmatrix} \tag{11}$$

$H_i$ is the reliability evaluation set of basic factors $i$, and $(\iota_{i1} \ \iota_{i2} \ \iota_{i3} \ \iota_{i4} \ \iota_{i5})$ correspond to the division value of evaluation level $v_k(k = 1, 2, 3, 4, 5)$ respectively.

Similarly, the above steps are carried out among the basic factors to obtain the reliability evaluation set $H$ of VNF.

$$H = W \times G = \begin{pmatrix} \iota_1 & \iota_2 & \iota_3 & \iota_4 & \iota_5 \end{pmatrix} \tag{12}$$

$G = (H_1 \ H_2 \ H_3 \ H_4)^T$, and $H_i(i = 1, 2, 3, 4)$ is the reliability evaluation set of every basic factor.

Finally, the reliability of a VNF is calculated as

$$R = \sum_{k=1}^{5} \iota_k f(v_k) \tag{13}$$

In addition, the reliability evaluation results obtained by this method are independent of the dimension of the matrix. In other words, when the factors affecting the reliability of VNF change (increase or decrease), it can also be calculated by this method.

### F. CREDIBILITY EVALUATION

With the above analysis of three aspects: authenticity ($A$), $V$ (availability), and $R$ (reliability), the complete credibility evaluation model is shown in Fig. 3. In particular, the credibility of VNF can be obtained as follows.

$$T = A \times (\omega_v V_{nor} + \omega_r R) \tag{14}$$

where the authenticity is the basis for VNF security and trust, when value of authenticity is 0, the value of credibility should be 0. With different situations (applications), the availability and reliability are assigned different weights $\omega_v$ and $\omega_r$. To make sure the values of availability and reliability are comparable, the availability of each VNF can be normalized as $V_{nor} = V/V_{max}$, where $V_{max}$ represents the maximum availability in the VNFs in the whole network.

The credibility of the deployed SFC is

$$\theta_{SFC} = \overline{E}(T) \tag{15}$$

where $\overline{E}(\cdot)$ means to take the average credibility of all VNF instances in the SFC.

## V. CREDIBILITY-BASED SFC DEPLOYMENT STRATEGY

In this section, we designed a credibility updating algorithm and an SFC deployment strategy according to the proposed credibility evaluation paradigm.

### A. CREDIBILITY UPDATING ALGORITHM

The credibility of VNF is online and dynamic, and evaluation update method is very important for the deployment of SFC. Without appropriate update mechanism, the changes of nodes and the dynamic behavior of VNF can not be detected timely. Consequently, the efficiency of SFC will decrease, and it is

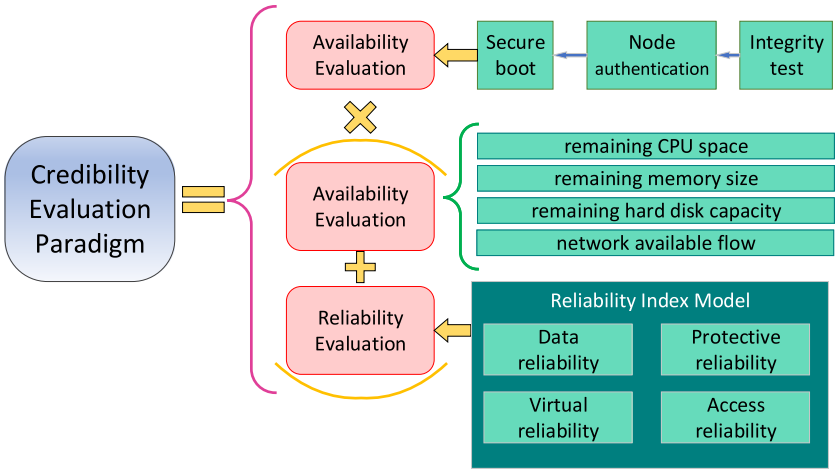


**FIGURE 3.** The Model of Credibility Evaluation Paradigm.

**TABLE 5.** The Levels of Credibility

| Credibility | [0.85, 1] | [0.7,0.85) | [0.55,0.7) | [0.4,0.55) | [0,0.4) |
|---|---|---|---|---|---|
| VNF level | 1 | 2 | 3 | 4 | 5 |

also easy to be attacked by disguised malicious VNF nodes. Different from traditional updating when VNF fails, we adopt sliding window and event triggering mechanism for the credibility updating algorithm.

**Step 1:** Every VNF is graded according to credibility evaluation paradigm. The VNF level is shown in the Table 5.

**Step 2:** The sliding window updating mechanism is adopted such that past credibility of a node can impact on the current results. For instance, with a window size of 3, the credibility $T_i$ of time $i$ is calculated as

$$T_i' = \varphi_i T_i + \varphi_{i-1} T_{i-1} + \varphi_{i-2} T_{i-2} \tag{16}$$

where $T_i'$ represents the credibility updated by sliding window algorithm, and $\varphi_i$ represents the weight of time $i$. For each timeslot, the credibility is updated once and the corresponding VNF level is changed as well.

**Step 3:** we define a trigger event called "skipping". When the level of VNF in time $i$ is different from the time $i-1$, it is in the state of "skipping". In this state, we update the credibility by

$$T_i' = T_{i-1} + (T_i - T_{i-1}) * e^{(T_{i-1} - T_i) * \alpha} \tag{17}$$

where $e$ represents exponential, and $\alpha$ represents different proportions. The slope of $f(x) = e^x$ at 0 is 1, which guarantees a fast-fall and slow-rise characteristics. We can adjust the value of $\alpha$ for better optimization when level is up or down. After a period of delay time $k$, switch back to sliding window mechanism. The reason Why we not switch to sliding window mechanism immediately is to prevent malicious nodes from posing as good nodes and then start to attack.

**Algorithm 1:** Credibility Updating Algorithm.

**Require:**
The size of window, $size$;
The current timeslot, $i$;
The level of VNF at timeslot $i$, $grade_i$
The credibility of VNF at timeslot $i$, $T_i$
The delay time, $k$

```
Calculate credibility by credibility evaluation paradigm.
if i >= size then
    for each i do
        Calculate credibility by sliding window mechanism.
        if grade_i ≠ grade_{i-1} then
            Calculate credibility by skipping mechanism.
            Initialize delay time clock.
        end if
    end for
    if clock ≥ k then
        Switch to sliding window mechanism.
    end if
end if
Update the credibility of VNFs;
return T;
```

The credibility updating algorithm is given in Algorithm 1. For each time $i$, the time complexity of our algorithm is $O(n)$ and the space complexity is $O(1)$.

### *B. CREDIBILITY-BASED DEPLOYMENT STRATEGY*

Finally, we propose a SFC deployment strategy according to the credibility evaluation paradigm. In the VNF-FG, we consider the credibility of VNF. In this way, a safe and reliable VNF can be fully selected. As shown in Fig. 4, where $SRC$ represents the source and $DST$ represents the destination. Maintains a table that records VNF credibility in the network.

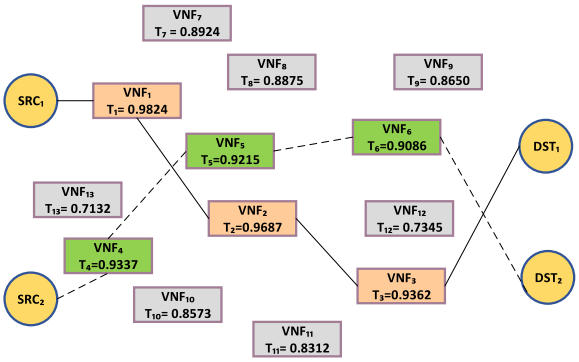


**FIGURE 4.** Deployment cost of SFC.

**Algorithm 2:** Credibility-Based Deployment Strategy.

**Require:**
The set of nodes, $Node_n$;
The matrix of bandwidth, $B_{nn}$;
The set of deployment requests for the SFC, $Re_m$;
**Ensure:**
The set of deployment instances for VNF, $In$;
The matrix of VNF's deployment location, $loc_{nn}$;
The matrix of network flow, $flow_{nn}$;

```
Initialization parameter.
for each re ∈ Re_m do
    for each v ∈ Node_n do
        Calculate the distance from the source node
        through v to the destination node.
    end for
    Sort the nodes according to the sum of their
    distance from source to destination.
    Sort the nodes according to credibility.
    for each nf ∈ In do
        for each v ∈ Node_n do
            if the same type of nf is deployed then
                break;
            else if the CPU of v > the CPU of nf then
                Register nd in In;
                the CPU of v -= the CPU of nf;
            end if
        end for
        Update B_nn, flow_nn, and loc_nn;
    end for
end for
return B_nn, In, loc_nn, flow_nn;
```

For each SFC deployment requests, select the VNF in various types with high credibility to participate in the deployment. The pseudocode for the entire selection process is given in Algorithm 2.

For each service function chain deployment request, the time complexity of our algorithm is $O(n^2)$ and the space complexity is $O(n^2)$.

**TABLE 6.** Parameters in Numerical Results

| Parameter | Value of each parameter |
|---|---|
| Number of nodes | 50 |
| Bandwidth | 500 |
| CPU | 150 |
| Authenticity | [0.7,1.0] |
| Availability | [0.4,1.0] |
| Reliability | [0.4,1.0] |
| Types of VNFs | 5 |
| Amount of VNFs in a SFC | 2,3,4 |
| Deployment cost of VNFs | 10,15,20,25,30 |
| CPU of VNFs | 25,30,35,40,45 |
| $\alpha$ in the skipping event | 3 |
| $\varphi_i$,$\varphi_{i-1}$,$\varphi_{i-2}$ | 0.8,0.1,0.1 |
| $\omega_v$,$\omega_r$ | 0.5,0.5 |

## VI. NUMERICAL SIMULATION

*Physical network:* We used a network map of 50 nodes in the simulation. Each physical node provides different resources for VNFs (such as CPU, memory, and so on). These resources have different sizes and are used to instantiate and process data. To simulate the complexity and variability of a real deployment environment, we randomly generates the values of properties related to the authenticity, availability and reliability of each node and VNF instance. Then we used above data to calculate the credibility of each VNF.

*SFC requests and VNF forwarding graph:* Because the user's services and the function of VNF instance are various, each SFC request is composed of 2-4 VNFs in series. And in the VNF-FG, five types of VNF instances are placed in the physical network to meet the requirements of different services. CPU and other resources required by each VNF are also randomly generated by MATLAB.

*Simulation and Results:* In this paper, we propose a credibility evaluation paradigm and a credibility-based deployment strategy (CBDS). Firstly, we simulate the feasibility of paradigm, and illustrate the advantages of the updating method Algorithm 1 by comparison. Then, we compare our CBDS algorithm with other three algorithms to prove its superiority. The other three algorithms are based on minimum deployment costs (MDC), TOPS algorithms proposed by [31], and random deployment strategy (RDS), respectively. TOPS algorithms minimize bandwidth resource consumption while optimizing CPU and link utilization. While MDC algorithms tends to choose the VNF with the lowest deployment costs.

In this paper, we use MATLAB and Python to simulate and analyze the result. We first use MATLAB to complete the simulation of Algorithm 1, then use Python to complete the simulation of Algorithm 2, and finally use MATLAB to analyze and compare the data. The considered parameters in numerical results are shown in the Table 6.

### A. UPDATING ALGORITHM

In this subsection, we simulate our updating algorithm, sliding window with skipping (SWWS), and compare with two other

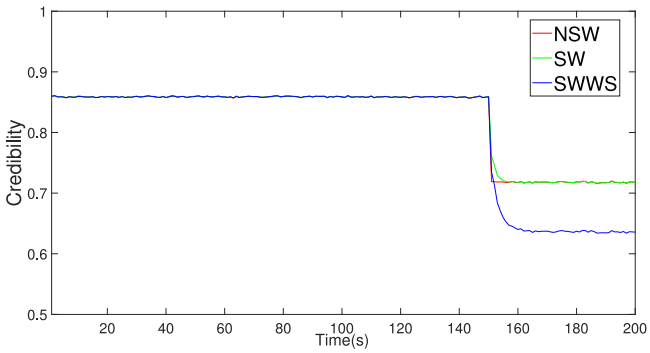


**FIGURE 5.** VNF is attacked at 150 s.

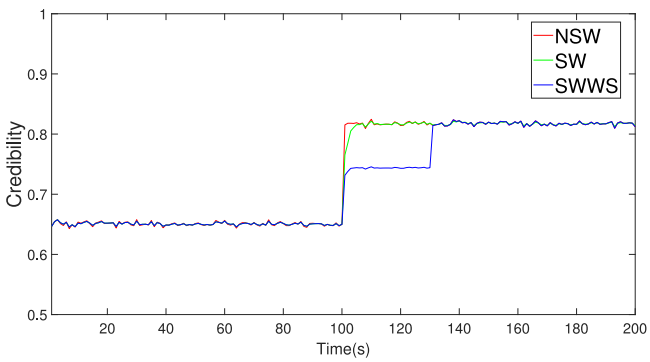


**FIGURE 6.** Credibility increases without fraud.

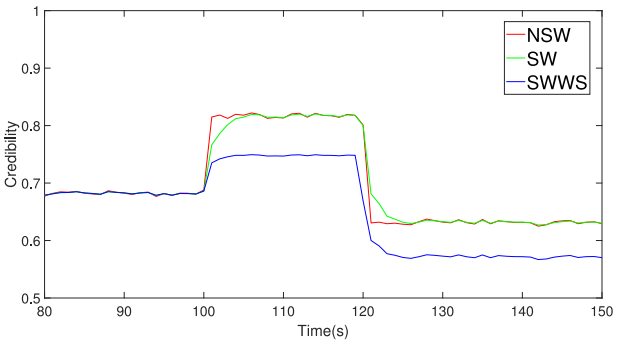


**FIGURE 7.** Credibility increases with fraud.

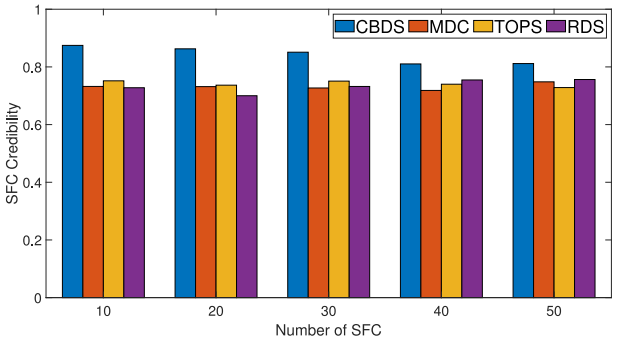


**FIGURE 8.** Credibility of SFC.

algorithm. One is No-sliding window (NSW) and anothor is sliding window (SW) method proposed by [12]. We randomly generated all the values required by credibility evaluation paradigm and simulated the attack process. And we carry out 100 simulations to get the average value.

We simulate the scenario in which a factor of VNF is attacked, as shown in Fig. 5. The simulation duration was set to 200 seconds. VNF is attacked at 150 seconds. Compared with NSW and SW, our update method would further amplify the negative impact of this attack by rapidly decreasing the credibility. When SFC is deployed, the probability of the attacked object being selected will be greatly reduced to achieve the purpose of active defense.

On the contrary, when VNF credibility is increased (this increase may be due to successful defense or malicious VNF fraud, etc.), according to our algorithm, the increase will be reduced when grade skipping occurs, and it will be restored to the sliding window algorithm after a delay time $k$. The whole process is shown in Fig. 6. The advantage of this is to prevent malicious VNF fraud. When the malicious VNF defrauds the trust of the SFC, it will participate in the deployment of the SFC. And that's when they might attack. Slowly increasing the credibility of VNF so that it will not be a priority option, and the delay time $k$ can further reduce the probability of this fraud attack. This situation is shown in Fig. 7, the malicious VNF pretends itself to be a normal VNF at 100 seconds and attacks at 120 seconds.

### B. CREDIBILITY

In order to calculate the credibility of SFC in different deployment algorithms, we deploy different numbers of SFC in turn and compare the advantages and disadvantages of them.

Fig. 8 shows that the credibility of CBDS is significantly higher than other algorithms. When deploying 10 SFCS, it increases by 18% compared with the MDC, 24% compared with the TOPS and 19% compared with the RDS. However, with the increase in the number of deployed SFC, the advantage of CBDS gradually weakens. This is because when multiple SFC are deployed at same time, the nodes with higher trust are already used or the CPU is full, so the nodes with low credibility will participate in the composition of SFC. But even with 50 SFC deployments, CBDS is still more than 10% higher.

### C. YIELD RATE

To measure the balance of credibility and VNF deployment costs, we propose to use "yield rate" to evaluate the benefit.

$$Y = \frac{\sum \theta}{\sum cost} \tag{18}$$

where, $\sum \theta$ represents the total trust gain of VNFs in a SFC, namely the total credibility of VNFs, and $\sum cost$ represents the deployment cost of VNF instances.

Fig. 9 shows that CBDS deliver trust benefit of 14% higher other algorithms averagely. This indicates that for all VNF, the trust benefit of the whole VNF instance is improved by

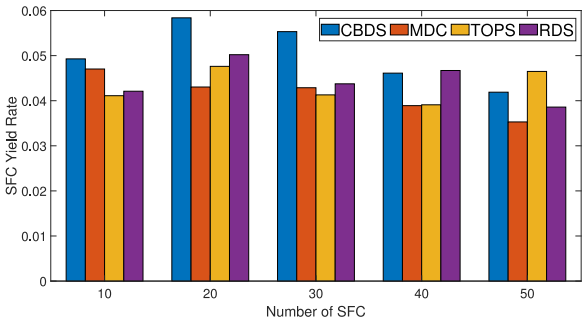


**FIGURE 9.** Yield rate of SFC.

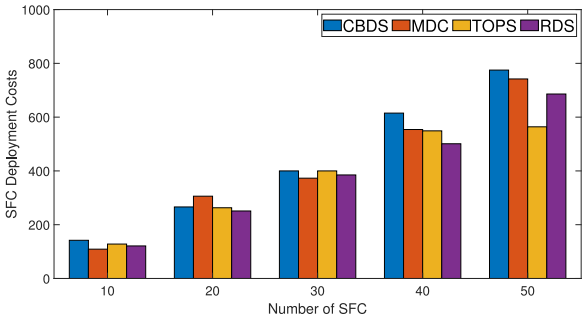


**FIGURE 10.** Deployment cost of SFC.

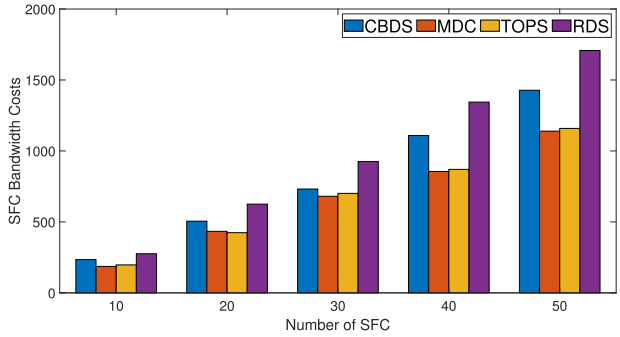


**FIGURE 11.** Bandwidth cost of SFC.

CBDS. When the number of SFC is less than 30, the yield rate of CBDS is significantly effective, while when the number of SFC is greater than 40, the effect of CBDS is not obvious.

### D. DEPLOYMENT COST

We also compare the VNF deployment cost and bandwidth cost in different quantities of SFC. In the numerical simulation, the deployment costs of different kinds of VNFs is various, and the bandwidth cost is proportional to the distance between VNF. Fig. 10 shows that when the number of SFC is beneath 40, the cost of deploying VNF instances is similar, and when the number of VNF instances increases, CBDS will increase.

The identical is authentic in bandwidth consumption. When the number of deployed SFC is beneath 30, the bandwidth consumption is the same. Fig. 11 shows that solely when the VNF instance is increased to 40 does the bandwidth cost of

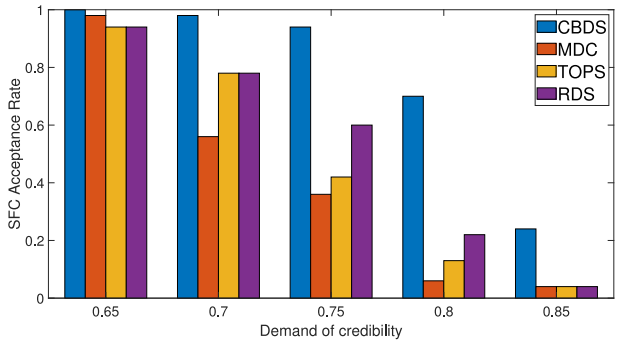


**FIGURE 12.** Acceptance rate of SFC.

CBDS increase. Both of the above display that CBDS does not cause excessive cost increases when deploying VNF instances inside an appropriate threshold. Combined with Fig. 9, this shows that while CBDS increases the cost of deployment and bandwidth to some extent, it is worth the cost for security.

This is additionally illustrated by means of the yield rate.

### E. ACCEPTANCE RATE

Different scenarios have different requirements for security and trust. In order to meet the trust requirements of different scenarios, there is usually a minimum threshold for credibility. When credibility is below this threshold, the SFC is not accepted because its credibility does not meet the trust condition of the deployment scenario, on the contrary, it is accepted when its credibility is greater than the threshold. Hereby, we compare the acceptance rate of SFC deployed by different algorithms or different credibility requirements.

Fig. 12 shows that CBDS can significantly improve the acceptance rate of SFC. CBDS preferred VNFs with high credibility to form SFC and provide services for users. According to the algorithm in this paper, credibility synthesizes the identity authentication of nodes, availability of resource and reliability of VNF, while other existing algorithms only pursue deployment overhead or available resources, so the acceptance rate of CBDS is significantly higher than that of other existing algorithms. When the credibility requirement is greater than 0.85, this advantage of CBDS is obvious and is 5 times higher than other algorithms. And with the reduction of requirements, the advantages of the trust algorithm still exist.

## VII. CONCLUSION

In this paper, we analyzed cutting-edge research on SFC security. We introduced AHP into SFC and VNF, and proposed a paradigm to quantify security and provide a new solution to security problems in the SFC and NFV. Distinct from remedial action after turning into unreliable or insecurity, it emphasizes initiative and robustness. We proposed the concept of VNF credibility, installed a hierarchical model, and quantitatively analyzed the credibility of VNF and SFC, so as to grant a foundation for the selection of VNF. Compared with the existing evaluation methods, the credibility evaluation paradigm, which depicts the degree of trust of SFC from both time and

space dimensions by various influencing factors, is more comprehensive and persuasive. We proposed a SFC deployment strategy whose VNF-FG based on credibility to ensure the SFC is composed of VNF with high reliability and availability, and provide reliable service for users. The results confirmed that the credibility-based deployment strategy enhances the security and acceptance rate of SFC without immoderate consumption cost. We additionally recognized the limitations of our research. There might also be better solutions to the credibility-based service function chain composition. In the future, we will work on greater fine-grained security quantifiable research and the optimization of the SFC deployment strategy.

## REFERENCES


[1] S. Van Rossem *et al.*, "Deploying Elastic Routing Capability in an Sdn/nfv-enabled environment," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw.*, 2015, pp. 22–24.

[2] A. M. Medhat, T. Taleb, A. Elmangoush, G. A. Carella, S. Covaci, and T. Magedanz, "Service function chaining in next generation networks: State of the art and research challenges," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 216–223, Feb. 2017.

[3] D. Cotroneo *et al.*, "Network function virtualization: Challenges and directions for reliability assurance," in *Proc. IEEE Int. Symp. Softw. Rel. Eng. Workshops*, , 2014, pp. 37–42.

[4] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging SDN and NVF security mechanisms for loT systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 812–837, Jun–Mar. 2019.

[5] M. S. Siddiqui *et al.*, "Policy based virtualised security architecture for SDN/NFV enabled 5 G access networks," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw.*, 2016, pp. 44–49.

[6] S. Ma, "Towards effective genetic trust evaluation in open network," in *Proc. IEEE 20th Int. Conf. High Perform. Comput. Commun.; IEEE 16th Int. Conf. Smart City; IEEE 4th Int. Conf. Data Sci. Syst.*. 2018, pp. 563–569.

[7] J. Jiang, X. Zhu, G. Han, M. Guizani, and L. Shu, "A dynamic trust evaluation and update mechanism based on C4. 5 decision tree in underwater wireless sensor networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9031–9040, Aug. 2020.

[8] U. Jayasinghe, G. M. Lee, T.-W. Um, and Q. Shi, "Machine learning based trust computational model for loT services," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 39–52, Jan.–Mar. 2018.

[9] Z. Lu and Y. Zhou, "The evaluation model for network security," in *Proc. 4th Int. Conf. Commun. Syst. Netw. Technol.*, pp. 690–694, 2014.

[10] H. Ge, L. Gu, Y. Yang, and K. Liu, "An attack graph based network security evaluation model for hierarchical network," in *Proc. IEEE Int. Conf. Inf. Theory Inf. Secur.*, 2010, pp. 208–211.

[11] Z.-J. Jia, X.-X. Liu, E.-F. Xu, and Y.-Y. Yang, "Study on multi-attribute dynamic trust evaluation model based on network transaction," in *Proc. Chin. Control Decis. Conf.*, 2018, pp. 6078–6082.

[12] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1228–1237, May 2015.

[13] W. She, Q. Liu, Z. Tian, J.-S. Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38947–38956, 2019.

[14] Y. L. Sun, W. Yu, Z. Han, and K. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, Feb. 2006.

[15] Q. Cui *et al.*, "Stochastic online learning for mobile edge computing: Learning from changes," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 63–69, Mar. 2019.

[16] X. Cheng and S. Lang, "Research on network security situation assessment and prediction," in *Proc. 4th Int. Conf. Comput. Inf. Sci.*, 2012, pp. 864–867.

[17] F. Wang and H. Zhou, "Dynamic trust evaluation model for online transaction based on time-frame," in *Proc. Int. Conf. Web Inf. Syst. Mining*, 2009, pp. 505–509.

[18] Z. Yu, "Research on cloud computing security evaluation model based on trust management," in *Proc. IEEE 4th Int. Conf. Comput. Commun.*, 2018, pp. 1934–1937.

[19] J. Zhang, D. Sun, and D. Zhai, "A research on the indicator system of cloud computing security risk assessment," in *Proc. Int. Conf. Qual., Rel., Risk, Maintenance, Saf. Eng.*, 2012, pp. 121–123.

[20] K. A. Saed, N. Aziz, A. W. Ramadhani, and N. H. Hassan, "Data governance cloud security assessment at data center," in *Proc. 4th Int. Conf. Comput. Inf. Sci.*, 2018, pp. 1–4.

[21] A. Engelmann and A. Jukan, "A reliability study of parallelized VNF chaining," in *Proc. IEEE Int. Conf. Commun.*, 2018, pp. 1–6.

[22] S. Aidi, M. F. Zhani, and Y. Elkhatib, "On optimizing backup sharing through efficient VNF migration," in *Proc. IEEE Conf. Netw. Softwarization*, 2019, pp. 60–65.

[23] J. Fan, M. Jiang, and C. Qiao, "Carrier-grade availability-aware mapping of service function chains with on-site backups," in *Proc. IEEE/ACM 25th Int. Symp. Qual. Serv.*, 2017, pp. 1–10.

[24] Industry Specification Group, "Network functions virtualisation (nfv); reliability; report on models and features for end-to-end reliability," *ETSI GS NFV-REL*, vol. 1, p. v 1, 2016.

[25] B. Ma and Z. Zhang, "Security research of redundancy in mimic defense system," in *Proc. 3rd IEEE Int. Conf. Comput. Commun.*, 2017, pp. 2910–2914.

[26] X. Sang and Q. Li, "Mimic defense techniques of edge-computing terminal," in *Proc. IEEE 5th Int. Conf. Big Data Comput. Serv. Appl.*, 2019, pp. 247–251.

[27] J. Xie, P. Yi, Z. Zhang, C. Zhang, and Y. Gu, "A service function chain deployment scheme based on heterogeneous backup," in *Proc. IEEE 18th Int. Conf. Commun. Technol.*, 2018, pp. 1096–1103.

[28] S. Xu, X. Ji, and W. Liu, "Enhancing the reliability of NFV with heterogeneous backup," in *Proc. IEEE 3rd Inf. Technol., Netw., Electron. Automat. Control Conf.*, 2019, pp. 923–927.

[29] J. Kang, O. Simeone, and J. Kang, "On the trade-off between computational load and reliability for network function virtualization," *IEEE Commun. Lett.*, vol. 21, no. 8, pp. 1767–1770, Aug. 2017.

[30] J. Zhang, D. Zeng, L. Gu, H. Yao, and M. Xiong, "Joint optimization of virtual function migration and rule update in software defined NFV networks," in *Proc. GLOBECOM IEEE Global Commun. Conf.*, 2017, pp. 1–5.

[31] W. Ma, O. Sandoval, J. Beltran, D. Pan, and N. Pissinou, "Traffic aware placement of interdependent NFV middleboxes," in *Proc. IEEE INFOCOM IEEE Conf. Comput. Commun.*, 2017, pp. 1–9.

[32] L. Wang, Z. Lu, X. Wen, R. Knopp, and R. Gupta, "Joint optimization of service function chaining and resource allocation in network function virtualization," *IEEE Access*, vol. 4, pp. 8084–8094, 2016.

[33] S. Herker, X. An, W. Kiess, S. Beker, and A. Kirstaedter, "Data-center architecture impacts on virtualized network functions service chain embedding with high availability requirements," in *Proc. IEEE Globecom Workshops*, 2015, pp. 1–7.

[34] M. Pattaranantakul, R. He, Q. Song, Z. Zhang, and A. Meddahi, "NFV security survey: From use case driven threat analysis to state-of-the-art countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3330–3368, Oct.–Dec. 2018.

[35] X. Yu, Q. Cui, Y. Wang, N. Li, X. Tao, and M. Valkama, "Stochastic geometry based analysis for heterogeneous networks: A perspective on meta distribution," *Sci. China Inf. Sci.*, vol. 63, no. 12, pp. 1–21, 2020.

[36] T. Sechkova, E. Barberis, and M. Paolino, "Cloud & edge trusted virtualized infrastructure manager (vim)-security and trust in openstack," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshop*, 2019, pp. 1–6.

[37] L. Bao, "QoS-based trust computing scheme for SLA guarantee in cloud computing system," in *Proc. Int. Conf. Comput. Intell. Inf. Syst.*, 2017, pp. 236–240.

[38] Y. Wang, J. Wang, Z. Xu, and H. Li, "Assessing cyber-threats situation for electric power information networks," in *Proc. IEEE 9th Int. Conf. Natural Comput.*, 2013, pp. 1557–1562.

[39] D. Catteddu *et al.*, "Cloud computing information assurance framework," *Eur. Netw. Inf. Secur. Agency*, vol. 13, no. 14, 2009.

[40] C. Council, "Proposed security assessment & authorization for us government cloud computing," *Draft Version 0.96, US CIO*, Nov., 2010.

[41] J. Chen, "A flexible fuzzy comprehensive evaluation method," in *Proc. IEEE, 3rd Int. Symp. Intell. Inf. Technol. Secur. Informat.*, 2010, pp. 502–506.

[42] T. R. Sahroni and H. Ariff, "Design of analytical hierarchy process (AHP) for teaching and learning," in *Proc. 11th Int. Conf. Knowl. Inf. Creativity Support Syst.*, 2016, pp. 1–4.

**WEIQI FAN** received the B.E. degree from HIT, in 2019. He is currently working toward the M.E. degree with the National Engineering Laboratory for Mobile Network Technology, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include wireless communications and network security.

**QIMEI CUI** (Senior Member, IEEE) received the Ph.D. degree from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2006. Since 2014, she has been a Full Professor with the School of Information and Communication Engineering, BUPT. In 2016, she was a Guest Professor with the Department of Electronic Engineering, University of Notre Dame, Notre Dame, IN, USA. Her main research interests include spectral-efficiency or energy-efficiency-based transmission theory, and networking technology for 4G or 5G broadband wireless communications and green communications.

**XIANGJUN LI** received the B.E. degree in 2019 from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, where she is currently working toward the Ph.D. degree. She is currently with the National Engineering Laboratory for Mobile Network Technology, BUPT. Her research interests include wireless communications, resource allocation, and reinforcement learning.

**XUEQING HUANG** (Member, IEEE) received the B.E. degree in communications engineering from the Hefei University of Technology, Hefei, China, the M.E. degree in information and communication engineering from the Beijing University of Posts and Telecommunications, Beijing, China, and the Ph.D. degree in electrical engineering from the New Jersey Institute of Technology, Newark, NJ, USA. He is currently an Assistant Professor of computer science with the New York Institute of Technology, Old Westbury, NY, USA. Her research interests include mobile edge computing, with current emphases on resources allocation and security schemes for IoT applications.

**XIAOFENG TAO** (Senior Member, IEEE) received the B.S. degree in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 1993, and the M.S. and Ph.D. degrees in telecommunication engineering from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 1999 and 2002, respectively. He is currently a Professor with BUPT. He has authored or coauthored more than 200 papers and three books in wireless communication areas. His research focuses on 5G or B5G. He is a Fellow of the Institution of Engineering and Technology, and a Chair of the IEEE ComSoc Beijing Chapter.