Security-SLA-Guaranteed Service Function Chaining Deployment in Cloud-Fog Computing Networks

Dongcheng Zhao, Gang Sun, Long Luo, Hongfang Yu, Victor Chang, and Rajkumar Buyya

Abstract—Network Function Virtualization (NFV) has gained prominence in next-generation cloud computing, such as the fog-based radio access network, due to their ability to support better QoS in network resource allocation. However, most of the current SFC deployment works do not consider the Security-Service-Level-Agreement (SSLA) in the deployment solution. Therefore, in this work, we propose the SSLA of the placement of Service Function Chains (SFCs) to defend against attacks. Firstly, we formulate linear programming to guarantee the SSLA in the deployment solution. Then, we propose the Maximal-Security SFCs deploying algorithm (MS), to maximize the security of the SFC deployment. However, the MS algorithm will cause a higher deployment cost. To reduce the deployment cost, we propose the Minimal-Cost and SSLA-Guaranteed SFCs deploying algorithm (MCSG), to minimize the placement cost and guarantee the SSLA. In order to reduce the blocking ratio caused by MCSG, the Minimal-Cost and SSLA-Guaranteed SFCs deploying algorithm with Feedback Adjustment (MCSG-FA) is proposed. Finally, we evaluate our proposed algorithms, and the simulations prove which the blocking ratio and the deployment cost are better than that of the compared algorithm when meeting the SSLA requirements.

Index Terms— Service Function Chaining; Network Function Virtualization; Deployment; Security; Fog-Cloud Computing

I. INTRODUCTION

Virtualization technology is a key technology to improve network flexibility [1-3]. As the development of the network, the author has presented Network Function Virtualization (NFV) [4] technology to transfer the traditional network function to the Virtual Network Function (VNF), to improve the network flexibility. Multiple VNFs consist of Service Function Chains (SFCs) [5] to guarantee the user’s service strategy, and the SFC requests are deployed into the cloud network to provide services [5, 6].

With more and more users in the cloud network, the network delay and congestion are becoming more and more serious in the centralized cloud computing. Additionally, the security of service is also being challenged. In order to solve these challenges, the distributed fog computing [7] is proposed to extend and supplement cloud computing. The fog-based radio access network has become a new study direction [8]. In Fog Radio Access Network (FRAN), there are some nodes with fog computing, similar to cloud nodes, these fog nodes can provide services for users can be virtualized, thereby improving the flexibility of the networks [9], but the service resource capacity of the fog node is usually less than that of the cloud node. Thus, joint use of cloud-fog computing can decrease network congestion and delay and provide more secure services for mobile users.

Currently, there are many research focus on SFC deployment in cloud computing. For example, in [10], the authors studied the SFC deployment issue for traffic-aware and energy-efficient and proposed a SAMA algorithm to place SFCs into the cloud network for minimizing the deployment cost. But the authors did not research fog computing. Joint use of cloud-fog computing can decrease network latency and congestion and provide more secure services for mobile users [11, 12]. In [13], Ricard Villalta et al. conducted an SDN/NFV deployment experiment for 5G services based on cloud-fog computing, optimized VNF deployment with constraints (e.g., latency) satisfied.

With the increase of SFC requests, how to ensure the Security-Service-Level-Agreement (SSLA) of services has become an enormous challenge. In order to guarantee the SSLA of services when the services are attacked, there are some studies on the security of NFV. For example, Mahdi Daghmehchi Firoozjai et al. [14] classified security threats and proposed some possible solutions from the architectural layer. These studies proposed some security architectures of NFV to ensure the SSLA of the service from the architectural layer but still cannot defend against all attacks. However, it did not consider utilizing the federated environment of the cloud-fog network to provide more secure services for mobile users. In [15], the authors proposed the security-on-demand services for ATM Networks, i.e., different user requests have different SSLA requirements. Then, the user request is deployed according to the user’s SSLA requirement. Besides, in [16, 17], the authors discussed how to manage and meet user’s SSLA requirement. In business, some companies (e.g., Huawei) provide servers with different security levels to users to deploy service requests with different SSLA requirements, and the higher security level of the server, the higher charge.

To solve the challenge management SSLA in SFCs, in this paper, we consider that each service node and each physical
link has a security possibility that can defend against attacks. Therefore, in this paper, we investigate the SFC placement problem in the federated environment of the cloud-fog network to meet the SSLA requirements of users when the security of each service node and each physical link is aware. The main contributions of the paper are as follows.

1. To resolve the SFC deployment problem with the SSLA requirements and guarantee the SSLA of the deployment solution, we first formulate the SFC deployment problem with the SSLA requirements as linear programming with SSLA-guaranteed.
2. To maximize the security of the SFC deployment, when the security of each service node and each physical link is aware, we propose the Maximal-Security SFCs deploying algorithm, (MS). The MS algorithm can maximize the security of SFC deployment, but the total deployment cost is high.
3. To decrease the high total placement cost of the MS algorithm, we present the Minimal-Cost and SSLA-Guaranteed SFCs deploying algorithm, (MSCG), for reducing the total placement cost when the SSLA requirement is satisfied. Although, the MCSG algorithm can decrease the total placement cost, but will cause an increase in the blocking ratio.
4. To decrease the total deployment cost and the blocking ratio at the same time, we propose the Minimal-Cost and SSLA-Guaranteed SFCs deploying algorithm with Feedback Adjustment, (MSCG-FA).

The rest of this paper is arranged as follows. Section II introduces related works. Section III models the SFC deployment problem with the SSLA requirement. Section IV presents the three SFC deployment algorithms. We evaluate our proposed algorithms in section V. Finally, section VI concludes this work.

II. RELATED WORK

A. NFV Deployment in Cloud Computing

NFV has become a key technology for improving the network flexibility, which is proposed to move the traditional network functions to the VNFs. Multiple VNFs consist of SFC in a specific order, and these SFCs are deployed into the cloud network for providing services for users. SFC deployment in cloud computing is the current research focus [18-23].

In [18], the author researched the shared pipeline problem in the environment of NFV. The study transmitted a plurality of data packets by utilizing the shared pipeline, reducing the core computing resources requirement, but increasing the length of the pipeline. In order to solve the problem, the authors presented two heuristic algorithms to balance between the core computing resources requirement and the pipeline length, to reduce network delay and resource consumption. To decrease the total VNF delay (including the processing delay and the transmission delay), Long Qu et al. [19] studied the optimal scheduling problem of VNFs. They proposed a heuristic algorithm for optimizing the scheduling of VNF based on the genetic algorithm can decrease the total scheduling time by about 20%.

The authors in [20] studied the significant performance overhead problem caused by virtual network functions, and proposed a high-performance framework based on the programmable software and hardware to obtain the flexibility and the high performance of NFV, and presented a performance-aware VNF deployment algorithm to satisfy the performance requirement of the VNF. To ensure the QoS and decrease the energy consumption of servers, in [21], the authors studied the VNF migration to adjust the load of the server dynamically and presented corresponding heuristic algorithms to reduce the total cost.

In [22], Marcelo Caggiani Luizelli et al. researched the efficient deployment problem of large-scale VNFs and links, and presented the heuristic algorithm to solve this problem to optimize the virtual network function deployment and reduce resource costs, while meeting the network traffic demand. To minimize the placement cost, the authors in [23] researched the optimal placement of the service function chain and put forward a graph algorithm based on a matrix and multi-stage optimization to optimize the deployment of the service function chain, to achieve the goal of reducing costs.

These researches [18-23] studied the deployment problem of SFC in cloud computing, but they did not consider the NFV security and utilization of the federated environment of the cloud-fog network to provide better services, it is an aspect that can be improved.

B. NFV and Fog Computing

With the increase of users in the cloud network, centralized cloud computing was facing an enormous challenge. Therefore, the distributed fog computing [24-27] is proposed to extend and supplement the centralized cloud computing to solve these challenges. There are some studies on fog computing [28-34].

In [28], the researches presented fog computing into the Internet of Things. They put forward a face identification model based on fog computing to solve the face identification problem, thereby improving the processing efficiency and reducing the network delay. Kai Liang et al. [29] introduced fog computing into the radio access networks, combining virtualization and SDN to slice the resources of the radio access networks to improve the flexibility of radio access networks. In [30], the authors studied a fog computing-based model of Internet access networks by utilizing virtual machines to host the business of fog network for reducing network latency and improving user experience.

The authors in [31] studied fog computing access control and proposed channel encryption and decryption model to improve the security of fog computing to defend network attacks. In [32], Seongjin Park et al. studied the vehicular network's connection problem by utilizing fog computing. This research utilizes fog node to collect information on the mobile vehicle and realizes the corresponding vehicle service
to achieve quick connection recovery when a failure occurs, and reduce the vehicle communication delay and the control cost. The authors in [33] take into account the problem that fog computing resources can not satisfy the requirements of vehicle users in the peak hour of vehicles. The fog vehicular computing concept is proposed to balance the needs of vehicle users and achieve the effective utilization of fog computing resources.

In [9], the authors discussed the fusion problem of 5G, cloud-fog computing, and NFV, and put forward a fusion and open architecture to provide the continuous management from cloud computing to fog computing. To meet the performance requirements of 5G services, Ricard Vilalta et al. [34] put forward the SDN/NFV architecture based on the federated environment of the cloud-fog network multi-dimensional network resources to provide performance assurance for 5G services.

In [28-33], fog computing was widely applied to the Internet of Things, radio access network and vehicular network and provided similar services to users, but these studies did not research NFV. These research projects [9, 13, 34] studied the NFV problem by utilizing the advantages of fog computing. They only proposed the NFV architecture of the fog computing environment, but the NFV deployment algorithm is not proposed, so deploying NFV in the fog network needs to be studied.

C. NFV SSLA in Cloud/Fog Computing

With the explosive growth of service requests and virus attacks are more frequent, ensuring the SSLA of services has become a heavy challenge. Therefore, there is some research on the SSLA of NFV [14, 35-38].

In NFV, due to the sharing of underlying resources and the live migration of VNF, VNF is vulnerable to the shared resource misuse attack and the side-channel attack. In order to solve these security threats, the authors in [14] first classified the attacks and then proposed corresponding and possible solutions. Because the SSLA of NFV is very important, the authors discussed the security of NFV architecture, and the influence of the outsider attack, the insider attacks, and between VNFs attacks on the security of NFV [35]. However, this work did not have a corresponding solution to defense these attacks. Due to network function virtualization brings more network attacks to businesses, it is necessary to provide higher security. Therefore, research [36] proposed a security framework to ensure SFC security.

In recent years, DDoS attacks continue to increase. At the same time, the traditional defense methods are not ideal, to solve this problem, in [37], Bahman Rashidi et al. presented the DDoS defense mechanism to achieve a collaboration network based on "domain-helps-domain" to deal with a lot of DDoS attacks. Although the DDoS defense mechanism can effectively handle many DDoS attacks, it may not be able to deal with other attacks effectively.

In order to decrease the impact of server failures on the business, the authors [38] studied the high availability deployment problem of the service function chain. They presented an SFC deployment algorithm based on service backup. The SFC deployment algorithm can improve the survivability of the business, but it cannot guarantee the SSLA of the service.

These studies [14, 35-38] only proposed some security architectures of NFV to guarantee the security of the service from the architecture layer, or cannot defend against all attacks, and did not consider utilizing the federated environment of the cloud-fog network to provide more secure services for users. In [39-41], the authors researched the security of fog computing and proposed some architectures and defense mechanisms to guarantee fog computing security. Additionally, the fog radio access network has smaller coverage than the cloud network, which helps deploy defense hardware to defend against attacks. Therefore, the fog radio access network can provide higher security than the cloud network does. Therefore, the security deployment problem of SFC is worth further research for providing more secure services for users. The authors [42] studied the security-aware virtual network mapping problem in the cloud environment, and it did not research fog computing. It is not appropriate to take the security value of the link with the least security as the security value of the whole embedding path when the authors computed the security of the embedding path.

III. PROBLEM DESCRIPTION AND MODEL

A. Problem Description

In the research, we give the physical network and SFC deployment requests of mobile users with SSLA requirements. We consider each physical node and each physical link to have a security possibility that can defend against attacks [42]. Under the premise of the security possibility of each physical node and link are aware, we design the SFC deployment algorithms for reducing the blocking ratio and the deployment cost while meeting the SSLA of mobile users.

B. Physical Network

In this work, the physical network includes two parts: the centralized cloud network and multiple distributed FRANs. An instance of the physical network is shown in Fig.1. We indicate the physical network as $G_p = (N_p, E_p)$. Wherein, $N_p = \{n_1, n_2, \ldots, n_{|N|}\}$ indicates the set of the physical nodes in the physical network, $|N|$ indicates the number of the physical nodes. $E_p = \{l_1, l_2, \ldots, l_{|E|}\}$ shows the set of the physical links, $|E|$ indicates the number of the links.

Resource constraints of the physical network: we define the physical network resource constraints as $RC = (C_{NP}, C_{EP}, S_{NP}, S_{EP}, L_{NP})$.

Resource attributes of the physical node: we use $C_{NP}$ to represent the resource attributes set of the physical nodes, which consist of the unit cost of the resource of the physical node $p(n_i)$ and the capacity of the computing resource of the physical node $\epsilon(n_i)$.
Resource attributes of the physical link: \( C_{EP} \) is denoted as the resource attributes set of the physical links, which consists of the unit cost of the resource of the physical link \( p(l) \) and the resource capacity of the physical link \( b(l) \).

Security possibility of the physical node: denotes the numerical concept of the security level of the physical node [42], we use \( S_{NP} = \{s(n_1), s(n_2), ..., s(n|NP|)\} \) to denote the security possibility set of the physical nodes.

Security possibility of the physical link: denotes the numerical concept of the security level of the physical link [42], \( S_{EP} = \{s(l_1), s(l_2), ..., s(l|EP|)\} \) is denoted as the security possibility set of the physical link. While maintaining the security of the physical node/link may need to purchase the specialized hardware or invest in human resources to maintain, so the higher the security possibility, the higher the unit cost of the physical node/link.

Locations of the physical nodes: \( L_{NP} = \{L(n_1), L(n_2), ..., L(n|NP|)\} \) shows the set of the locations of all physical nodes.

Deployment constraints: we define the deployment constraints of the SFC deployment request as \( DC = (C_{NP}, C_{EF}, SR, L_{NP}, L_{F}, L_{U}) \).

Resource constraints of VNFs: we define \( C_{NP} = \{\phi(v_f), \phi(v_{f_2}), ..., \phi(v_{f_{|NP|}})\} \) as the computing resource constraints set of all VNFs.

Resource constraints of SFC links: \( C_{EF} = \{\phi(e_1), \phi(e_2), ..., \phi(e_{|EF|})\} \) represents the bandwidth resource constraints set of the SFC links.

SSLA requirement of the SFC deployment request: we define \( SR \) as the overall SSLA constraint of the SFC deployment request.

Location constraints of VNFs, service terminal and mobile user: \( L_{NP}=\{L(v_{f_1}), L(v_{f_2}), ..., L(v_{f_{|NP|}})\} \) describes the set of the location constraints of all VNFs. VNFs of the cloud network can only be deployed into the cloud network, and VNFs of the fog radio access network can only be mapped into the FRAN in which the mobile user is located. \( L_T \) represents the location of the service terminal. \( L_U \) depicts the location of the mobile user.

D. Networking Model for Placing SFC

In deploying the SFC placement request, we are devoted to effectively deploying the VNFs and links. And the deployment of the VNFs can be formulated as:

\[
DS: (N_F, C_{NP}) \xrightarrow{DS} (N_{p_1}, C_{NP_1}),
\]

\[
DS(v_{f_i}) \in N_{p_1}, \forall v_{f_i} \in F_F,
\]

\[
A(DS(v_{f_i})) \geq \phi(v_{f_i}), \forall v_{f_i} \in F_F,
\]

\[
Z(LC(v_{f_i}), q) \in [0,1], \forall v_{f_i} \in F_F, \forall q \in \{0,1,...,Q\},
\]

\[
L(DS(v_{f_i})) \in [0,1,2,...,Y], \forall v_{f_i} \in F_F,
\]

\[
Z(LC(v_{f_i}), L(DS(v_{f_i}))) = 1, \forall v_{f_i} \in F_F,
\]

wherein \( DS = (DS_N, DS_E) \) denotes the deployment solution of the SFC deployment request, where \( DS_N = \{DS(v_{f_1}), DS(v_{f_2}), ..., DS(v_{f_{|NP|}})\} \) shows the set of the placement solution of all VNFs, \( DS_E = \{DS(e_1), DS(e_2), ..., DS(e_{|EF|})\} \) shows the set of the placement solution of all SFC links. \( N_{p_1} \subseteq N_F \) indicates a subset of the physical nodes for hosting the VNFs, \( C_{NP_1} \subseteq C_{NP} \) describes the node resources allocated to the SFC placement request. \( DS(v_{f_i}) \) denotes a physical node for hosting the \( i-th \) VNF \( v_{f_i} \). \( A(DS(v_{f_i})) \) describes available node resources of the physical node \( DS(v_{f_i}) \). \( q \in \{0,1,...,Q\} \) describes the number of the network area, \( Z(LC(v_{f_i}), q) \in \{0,1\} \) indicates a binary variable, if \( Z(LC(v_{f_i}), q) = 1 \) describes which the VNF \( v_{f_i} \) can be deployed into the network area, otherwise \( Z(LC(v_{f_i}), q) = 0 \). \( L(DS(v_{f_i})) \) describes the number of the network area of the physical node \( DS(v_{f_i}) \). \( Z(LC(v_{f_i}), L(DS(v_{f_i}))) = 1 \) describes which the physical node \( DS(v_{f_i}) \) satisfies the location constraint of the VNF \( v_{f_i} \), otherwise \( Z(LC(v_{f_i}), L(DS(v_{f_i}))) = 0 \).

In this work, we deploy the SFC links when we deploy the VNFs, and we describe the deployment of the SFC links as:
DS : (E_F, C_EF) → DS(PL, C_EF),

DS(e_i) = p_{e_i}, \ ∀ e_i \in E_F, \exists p_{e_i} \in P_1,

B(p_{e_i}) = \min_{l_j = p_{e_i}} \{ b(l_j) \} ≥ e(e_i), \ ∀ p_{e_i} \in P_1,

wherein P_1 indicates a subset of the physical paths. C_EF denotes the resources of physical links allocated for the SFC request. P_{e_i} and DS(e_i) also show a physical path for hosting the SFC link e_i. B(p_{e_i}) depicts the available bandwidth resource of the physical path p_{e_i}.

We first assume the security of the SFC deployment DS as in Equation (1).

TSecurity(DS)

= \left\{ \left| \sum_{i=1}^{[fr]} VNFSecurity(\text{DS}(\text{vf}_i)) \right| \left| \sum_{i=1}^{[P]} PathSecurity(\text{DS}(\text{e}_i)) \right| \right\} (1)

= \left\{ \left| \sum_{i=1}^{[fr]} s(\text{DS}(\text{vf}_i)) \right| \left| \sum_{i=1}^{[P]} l_{j_i = \text{DS}(\text{e}_i)} s(l_j) \right| \right\}

To satisfy the SSLA requirements of the SFC deployment request, we first consider maximizing the security of the SFC deployment and model the maximal-security deployment as the linear programming (2).

\max \left( \sum_{i=1}^{[fr]} S(\text{DS}(\text{vf}_i)) \right) \left( \sum_{i=1}^{[P]} l_{j_i = \text{DS}(\text{e}_i)} s(l_j) \right)

s.t.

A(DS(\text{vf}_i)) ≥ e(\text{vf}_i), \forall \text{vf}_i \in N_F

Z(LC(\text{vf}_i), q) \in \{0,1\}, \forall \text{vf}_i \in N_F, \forall q \in \{0,1,...,Q\}

L(DS(\text{vf}_i)) \in \{0,1,2,...,Q\}, \forall \text{vf}_i \in N_F

Z(LC(\text{vf}_i), L(DS(\text{vf}_i))) \in \{0,1\}, \forall \text{vf}_i \in N_F

DS(e_i) = p_{e_i}, \ ∀ e_i \in E_F, \exists p_{e_i} \in P_1

B(p_{e_i}) = \min_{l_j = p_{e_i}} \{ b(l_j) \} ≥ e(e_i), \ ∀ p_{e_i} \in P_1

min( \sum_{\text{vf}_i \in N_F} P(\text{DS}(\text{vf}_i)) e(\text{vf}_i) + \sum_{e_i \in E_F} \sum_{l_j = p_{e_i}} P(l_j) e(e_i))

s.t.

\left\{ \left| \sum_{i=1}^{[fr]} S(\text{DS}(\text{vf}_i)) \right| \left| \sum_{i=1}^{[P]} l_{j_i = \text{DS}(\text{e}_i)} s(l_j) \right| \right\} ≥ SR

A(DS(\text{vf}_i)) ≥ e(\text{vf}_i), \forall \text{vf}_i \in N_F

Z(LC(\text{vf}_i), q) \in \{0,1\}, \forall \text{vf}_i \in N_F, \forall q \in \{0,1,...,Q\}

L(DS(\text{vf}_i)) \in \{0,1,2,...,Q\}, \forall \text{vf}_i \in N_F

Z(LC(\text{vf}_i), L(DS(\text{vf}_i))) \in \{0,1\}, \forall \text{vf}_i \in N_F

DS(e_i) = p_{e_i}, \ ∀ e_i \in E_F, \exists p_{e_i} \in P_1

B(p_{e_i}) = \min_{l_j = p_{e_i}} \{ b(l_j) \} ≥ e(e_i), \ ∀ p_{e_i} \in P_1

Suppose the security of the SFC deployment solved by the linear programming (2) still does not meet the SSLA requirement of the SFC deployment request. In that case, the SFC deployment request will be rejected because the current network cannot provide a more secure deployment. Since the security possibility is the higher, the unit cost of the physical node/link is the higher, and the maximal-security implementation may lead to the higher deployment cost. To minimize the total deployment cost when the SSLA requirements of the SFC deployment request is guaranteed, we model the minimal-cost and SSLA-guaranteed SFCs deployment as the linear programming (3).

IV. ALGORITHM DESIGN

Due to the SFC deployment with the SSLA requirement is an NP-hard problem, the linear programming cannot gain a deployment solution DS in an effective time. To solve this problem, we put forward the Security-Aware SFCs Deploying algorithm, SASFCD. The SASFCD algorithm can satisfy three different scenarios by calling three sub-algorithms: the MS algorithm, the MCSG algorithm and the MCSG-FA algorithm. In general, we assume which the SFC deployment requests follow the Poisson process to arrive dynamically. First, all arrival SFC deployment requests are stored in the queue ArrivalSFC. These finished SFC requests are stored in the set FinishedSFC. Each SFC deployment request in the queue ArrivalSFC is deployed one by one. We use SFC_{blo} to indicate the set of blocked SFC deployment requests owing to falling short of resources. Algorithm 1 shows the SASFCD algorithm.

Algorithm 1: The Security-Aware SFCs Deploying algorithm (SASFCD)

\textbf{Input:} 1. Physical network G_P = (N_P, E_P) and resource constraints RC = (C_EF, C_NP, S_{NP}, S_{EP}, LC_{NP})

2. SFC deployment request queue ArrivalSFC.

\textbf{Output:} Total deployment cost TCost and the blocked SFCs, SFC_{blo}.

1: Initialization: set TCost = 0 and SFC_{blo} = 0;
2: \textbf{while} ArrivalSFC ≠ ∅, \textbf{do}
3: Updating resources according to the set FinishedSFC;
4: Call MS or MCSG or MCSG-FA algorithm for deploying the first SFC deployment request SFC_1 in ArrivalSFC;
5: \textbf{if} the deployment solution DS for SFC_1, DS ≠ ∅, \textbf{then}
6: updating TCost and the physical network;
7: \textbf{else}
8: SFC_{blo} = SFC_{blo} ∪ \{SFC_1\};
9: \textbf{end if}
10: ArrivalSFC = ArrivalSFC \{SFC_1\};
11: \textbf{end while}
12: \textbf{return} TCost and SFC_{blo}.

The Maximal-Security SFCs deploying algorithm, MS, is used to maximize the security of the SFC deployment solution. In the MS algorithm, we use the maximal-security strategy as a guide strategy for deploying VNF into the most secure physical node and finding the most secure path to
maximize the security of the placement solution of SFC, finally get the most secure deployment solution. When we deploy each VNF \(v_f\) into the physical node \(n_p\), and find the most secure path \(p_{ei}\), we will find the most secure path \(p^{ei} (n_p, L_U)\) from the current physical node \(n_p\) to the user. The aim is to optimize the deployment solution and improve the blocking ratio to ensure the security of the final deployment solution. If the security of the SFC deployment solved by the MS algorithm cannot meet the SSLA requirement of the SFC deployment request, the SFC deployment request will be rejected. The MS algorithm is as shown in Algorithm 2.

The security of each VNF \(v_f\) deployed into the physical node \(n_p\), \(VNF\text{Security}(v_f\rightarrow n_p)\), that is defined as in Equation (4).

\[
VNF\text{Security}(v_f\rightarrow n_p) = s(n_p)
\]

(4)

The deployment cost of each VNF \(v_f\) deployed into the physical node \(n_p\), \(VNFCost (v_f\rightarrow n_p)\), that is defined as in Equation (5).

\[
VNFCost (v_f\rightarrow n_p) = \epsilon(v_f) p(n_p)
\]

(5)

The security of the physical path \(p_{ei}\) hosting each SFC link \(e_i\), \(Path\text{Security}(p_{ei})\), is denoted as in Equation (6).

\[
Path\text{Security}(p_{ei}) = \prod_{l_i \in p_{ei}} s(l_i)
\]

(6)

The security of the physical path \(p^{ei} (n_p, L_U)\) hosting each link \((n_p, L_U)\), \(Path\text{Security}(p^{ei} (n_p, L_U))\), is denoted as follows. The physical path \(p^{ei} (n_p, L_U)\) must meet the link resource requirements of the SFC link \(e_i\).

\[
Path\text{Security}(p^{ei} (n_p, L_U)) = \prod_{l_i \in p^{ei} (n_p, L_U)} s(l_i)
\]

(7)

The deployment cost of the physical path \(p_{ei}\) hosting each SFC link \(e_i\), \(Path\text{Cost}(p_{ei})\), can be described in Equation (8).

\[
Path\text{Cost}(p_{ei}) = \sum_{l_i \in p_{ei}} p(l_i) \epsilon(e_i)
\]

(8)

The total security of each VNF \(v_f\) deployed into the physical node \(n_p\), \(TSecurity(v_f\rightarrow n_p)\), that is represented as in Equation (9).

\[
TSecurity(v_f\rightarrow n_p) = VNF\text{Security}(v_f\rightarrow n_p) \times Path\text{Security}(p_{ei})
\]

(9)

\[
TSecurity(v_f\rightarrow n_p) = \{\sum_{l_i \in p_{ei}} s(l_i)\} \prod_{l_i \in p^{ei} (n_p, L_U)} s(l_i)
\]

The total deployment cost of each VNF \(v_f\) deployed into the physical node \(n_p\), \(TCost(v_f\rightarrow n_p)\), that is denoted as follows.

\[
TCost(v_f\rightarrow n_p) = VNFCost (v_f\rightarrow n_p) + Path\text{Cost}(p_{ei})
\]

\[
= \epsilon(v_f) p(n_p) + \sum_{l_i \in p_{ei}} (p(l_i) \epsilon(e_i))
\]

(10)

The total security of the current deployment solution \(DS\) in the MS algorithm, \(TSecurity(DS)\), is represented as in Equation (11).

\[
TSecurity(DS) = Path\text{Security}(p^{ei} (n_p, L_U)) \times \prod_{i=1}^{N_F} \{VNFCost (v_f) \times Path\text{Cost}(DS(e_i))\}
\]

(11)

The total deployment cost of the current deployment solution \(DS\), \(TCost(DS)\), can be defined as follows.

\[
TCost(DS) = \sum_{i=1}^{N_F} VNFCost (v_f) + \sum_{i=1}^{E_P} Path\text{Cost}(DS(e_i))
\]

(12)

**Algorithm 2: The Maximal-Security SFCs deploying algorithm (MS)**

**Input:** 1. Physical network \(G_P = (N_P, E_P)\) and resource constraints \(RC = (C_{SF}, C_{EP}, S_{SF}, S_{EP}, L_{NSP})\); 2. The SFC request \(G_S = (N_S, E_S)\) and deployment constraints \(DC = (C_{NSP}, C_{EQ}, SR, L_{CS}, L_T, L_U)\).

**Output:** Deployment solution \(DS\) and total deployment cost \(TCost(DS)\).

1: for each VNF \(v_f\), \(i=1,2,…, |N_F|\), \(v_f\in N_P\), do 2: for each physical node \(n_p\in N_P\), do 3: if the node \(n_p\) meets the location constraint of \(v_f\), then 4: Try to deploy \(v_f\) into the physical node \(n_p\), calculate the security of the deployment solution of \(v_f\) \(VNF\text{Security}(v_f\rightarrow n_p)\) and the deployment cost \(VNFCost(v_f\rightarrow n_p)\) according to Equation (4), (5); 5: Find most secure paths \(p_{ei}\) and \(p^{ei} (n_p, L_U)\), calculate the security of the path \(p_{ei}\) \(Path\text{Security}(p_{ei})\), the security of the path \(p^{ei} (n_p, L_U)\) \(Path\text{Security}(p^{ei} (n_p, L_U))\) and the deployment cost \(Path\text{Cost}(p_{ei})\) according to Equation (6), (7) and (8); calculate the total security \(TSecurity(v_f\rightarrow n_p)\) and the total deployment cost \(TCost(v_f\rightarrow n_p)\) according to Equation (9) and (10); 6: end if 7: end for 8: Find the deployment solution of the VNF \(v_f\) with the maximal total security \(TSecurity(v_f\rightarrow n_p)\), and store the deployment solutions of \(v_f\) and \(e_i\) in \(DS\); 9: if don’t find the deployment solution, then 10: Clear \(DS\) and \(TCost(DS)=0\); 11: return \(DS\) and \(TCost(DS)\); 12: end if 13: calculate the total security \(TSecurity(DS)\)’ according to Equation (11);
14: if \( \text{TSecurity}(DS) \leq \text{SR} \), then
15: Clear \( DS \) and \( \text{TCost}(DS)=0 \);
16: return \( DS \) and \( \text{TCost}(DS) \);
17: end if
18: end for
19: Find the most secure path \( p_{e[E]} \) and store it in \( DS \), calculate the total deployment cost \( \text{TCost}(DS) \) according to Equation (12);
20: return \( DS \) and \( \text{TCost}(DS) \).

The higher security of the deployment solution will lead to a higher total deployment cost to minimize the total deployment cost. While satisfying the SSLA requirement of the SFC deployment request, we put forward the Minimal-Cost and SSLA-Guaranteed SFCs deploying algorithm, MCSG. In the MCSG algorithm, we use the minimal-cost and SSLA-guaranteed strategy as a guide strategy for deploying VNF for minimizing the total deployment cost of the deployment solution of SFC. In contrast, the security of the deployment solution meets the SSLA requirement of the SFC deployment request. In the MCSG algorithm, similar to the MS algorithm, we will find the most secure path \( p_{i+1}(n_j, L_U) \) from the current physical node \( n_j \) to user, to reduce the total cost. The MCSG algorithm is as shown in Algorithm 3.

\[ \text{MaxSecurity}(p_{i+1}(n_j, L_U)) = \prod_{k=1}^{[\text{NF}]} \max \{s(n_k), \forall n_k \in p_{i+1}(n_j, L_U)\} \] (13)

The deployment cost of the physical path \( p_{i+1}(n_j, L_U) \) hosting each link \( (n_j, L_U) \), \( \text{PathCost}(p_{i+1}(n_j, L_U)) \), can be described as in Equation (14).

\[ \text{PathCost}(p_{i+1}(n_j, L_U)) = \sum_{l \in p_{i+1}(n_j, L_U)} p(l_i) e(e_{i+1}) \] (14)

The total security of the current deployment solution \( DS \) in the MCSG algorithm, \( \text{TSecurity}(DS)^\prime \), is denoted as in Equation (15).

\[ \text{TSecurity}(DS)^\prime = \text{MaxSecurity}(p_{i+1}(n_j, L_U)) \times \prod_{k=1}^{[\text{NF}]} \left( \text{VNFSecurity}(DS(vf_i)) \times \text{PathSecurity}(DS(e_i)) \right) \] (15)

\[ \leq \prod_{k=1}^{[\text{NF}]} \max \{s(n_k), \forall n_k \in p_{i+1}(n_j, L_U)\} \times \prod_{k=1}^{[\text{NF}]} s(DS(vf_i)) \prod_{l \in DS(e_i)} s(l_i) \]

The total deployment cost of each VNF \( vf \), deployed into the physical node \( n_j \) in the MCSG or MCSG-FA algorithm, \( \text{TCost}(vf_i \rightarrow n_j)^\prime \), that is denoted as in Equation (16).

\[ \text{TCost}(vf_i \rightarrow n_j)^\prime = \text{VNFCost}(vf_i \rightarrow n_j) + \text{PathCost}(p_{e[E]}) + \text{PathCost}(p_{i+1}(n_j, L_U)) \] (16)

Algorithm 3: The Minimal-Cost and SSLA-Guaranteed SFCs deploying algorithm (MCSG)

Input: 1. Physical network \( G_P = (N_P, E_P) \) and resource constraints \( RC = (C_{NF}, C_{E_P}, S_{NF}, S_{E_P}, L_{NP}) \);
2. The SFC request \( G_F = (N_F, E_F) \) and deployment constraints \( DC = (C_{NF}, C_{E_P}, SR, SL_{NF}, LT, L_U) \).

Output: Deployment solution \( DS \) and total deployment cost \( \text{TCost}(DS) \).

1: for each VNF \( vf_i \), \( i = 1, 2, \ldots, [\text{NF}] \), \( vf_i \in N_{NF} \) do
2: for each physical node \( n_j \in N_P \), do
3: if the node \( n_j \) meets the location constraint of \( vf_i \), then
4: Try to deploy \( vf_i \) into the physical node \( n_j \), calculate the security of the deployment solution of \( vf_i \), \( \text{VNFSecurity}(vf_i \rightarrow n_j) \), and the deployment cost \( \text{VNFCost}(vf_i \rightarrow n_j) \) according to Equation (4) and (5);
5: Find most secure paths \( p_{e[E]} \) and \( p_{i+1}(n_j, L_U) \), calculate the security of the path \( p_{e[E]} \), \( \text{PathSecurity}(p_{e[E]}) \), the security of the path \( p_{i+1}(n_j, L_U) \), \( \text{PathSecurity}(p_{i+1}(n_j, L_U)) \), the maximal security of the pre-deployment of the rest of VNFs \( \text{MaxSecurity}(p_{i+1}(n_j, L_U)) \), the deployment cost \( \text{PathCost}(p_{e[E]}) \) and the deployment cost \( \text{PathCost}(p_{i+1}(n_j, L_U)) \) according to Equation (6), (7), (13), (8) and (14); calculate the total security \( \text{TSecurity}(DS)^\prime \) and the total deployment cost \( \text{TCost}(vf_i \rightarrow n_j)^\prime \) according to Equation (15) and (16);
6: end if
7: end for
8: Find the deployment solution of the VNF \( vf_i \) with the minimal deployment cost \( \text{TCost}(vf_i \rightarrow n_j)^\prime \) and the total security \( \text{TSecurity}(DS)^\prime \geq SR \), and store the deployment solutions of \( vf_i \) and \( e_i \) in \( DS \);
9: if don’t find the deployment solution, then
10: Clear \( DS \) and \( \text{TCost}(DS)=0 \);
11: return \( DS \) and \( \text{TCost}(DS) \);
12: end if
13: end for
14: Find the most secure path \( p_{e[E]} \) and store it in \( DS \), calculate the total deployment cost \( \text{TCost}(DS) \) according to Equation (12);
15: return \( DS \) and \( \text{TCost}(DS) \).

The MCSG algorithm uses the minimal-cost and SSLA-guaranteed strategy as a guide strategy for deploying
VNF for minimizing the total placement cost. However, the MCGS algorithm can decrease the total placement cost by using the security-guaranteed strategy as a guide strategy that will cause an increase in the blocking ratio. Therefore, we propose the MCGS-FA algorithm to improve the blocking ratio. In the MCGS-FA algorithm, we first call the MS algorithm to get an initial deployment solution with maximal security. We try to find a deployment solution with a minimal total deployment cost. If we find a new deployment solution, and the security of the new deployment solution meets the SSLA requirement of the SFC requests. The total placement cost of the new placement solution is less than that of the initial deployment solution, and we use the new placement solution to replace the initial deployment solution. The MCGS-FA algorithm can improve the total deployment cost and the blocking ratio through the processing of the feedback adjustment. The MCGS-FA algorithm is as shown in Algorithm 4.

The total security of the current deployment solution $D'$ in the MCGS-FA algorithm, $TSecurity(D')$, is denoted as in Equation (17).

$$TSecurity(D') = \prod_{i=1}^{i} (VNFSecurity(D'(vf_i)) \times PathSecurity(D'(e_i))) \quad (17)$$

The total deployment cost of the current deployment solution $D'$ in the MCGS-FA algorithm, $TCost(D')$, can be defined as follows.

$$TCost(D') = \sum_{i=1}^{\[N\]} VNFCost(D'(vf_i)) + \sum_{i=1}^{[E]} PathCost(D'(e_i)) \quad (18)$$

Algorithm 4: The Minimal-Cost and SSLA-Guaranteed SFCs deploying algorithm with Feedback Adjustment (MCGS-FA)

**Input:** 1. Physical network $G_P = (N_P, E_P)$ and resource constraints $RC = (C_{NP}, C_{EP}, S_{NP}, S_{EP}, L_{NP})$;
2. The SFC request $G_F = (N_F, E_F)$ and deployment constraints $DC = (C_{NF}, C_{EF}, SR, L_{NF}, L_{EF}, L_{U})$.

**Output:** Deployment solution $DS$ and total deployment cost $TCost(DS)$.

1. Call the MS algorithm to achieve $DS$ and $TCost(DS)$;
2. if $DS \neq \emptyset$, then
3. for each VNF $vf_i$, $i=1,2,..., [N_F], vf_i \in N_P$, do
4. for each physical node $n_j \in N_P$, do
5. if the node $n_j$ meets the location constraint of $vf_i$, then
6. Try to deploy $vf_i$ into the physical node $n_j$, calculate the security of the deployment solution of $vf_i$ $VNFSecurity(vf_i \rightarrow n_j)$ and the deployment cost $VNFCost(vf_i \rightarrow n_j)$ according to Equation (4), (5);
7. Find minimal cost paths $p_{n_i}$, $p_{n_i}^*(n_j, L_{U})$, calculate the security $PathSecurity(p_{n_i}^*)$, the deployment costs $PathCost(p_{n_i})$ and $PathCost(p_{n_i}^*(n_j, L_{U}))$, and the total deployment cost $TCost(vf_i \rightarrow n_j)$ according to Equation (6), (8), (14) and (16);
8. end if
9. end for
10. Find the deployment solution of the VNF $vf_i$ with the minimal deployment cost $TCost(vf_i \rightarrow n_j)$, and store the deployment solutions of $vf_i$ and $e_i$ in $DS'$;
11. if don’t find the deployment solution, then
12. Clear $DS'$ and $TCost(DS') = 0$;
13. return $DS$ and $TCost(DS)$;
14. end if
15. Calculate the total security $TSecurity(DS')$ according to Equation (17);
16. if $TSecurity(DS') < SR$, then
17. Clear $DS'$ and $TCost(DS') = 0$;
18. return $DS$ and $TCost(DS)$;
19. end if
20. end for
21. Find the minimal-cost path $p_{v|f|e}$ and store it in $DS'$, calculate the total security $TSecurity(DS')$ according to Equation (17), calculate the total deployment cost $TCost(DS')$ according to Equation (18);
22. end if
23. if find a complete solution $DS'$ and $TSecurity(DS') \geq SR$ and $TCost(DS') < TCost(DS)$, then
24. let $DS = DS'$, $TCost(DS) = TCost(DS')$;
25. end if
26. return $DS$ and $TCost(DS)$.

V. PERFORMANCE EVALUATION

A. Simulation Environment

In this work, to improve the security of the deployment solution and provide services for more mobile users, we consider utilizing the federated environment of the cloud-fog network to provide more secure services for more mobile users. So the physical network is comprised of cloud network (the USANET network, as shown in Fig.3) and multiple FRANs. The FRAN is as shown in Fig.4. In our simulations, there are 15 FRANs that connect to the black nodes in the USANET network.

In general, in this work, we presume which the unit cost of the node resource of each physical node in the physical network is log(1/(1-s(n_j))) unit, the unit cost of the resource of each physical link in the physical network is log(1/(1-s(l_i))) unit. In our simulations, when we evaluate the total deployment costs and the running time of our proposed algorithms, we assume which the resource capacity
constraints of the physical node follow a uniform distribution \(U(50, 80)\) unit. The resource capacity constraints of the physical link follow a uniform distribution \(U(30, 50)\) unit. When we evaluate the blocking ratios of all algorithms, we assume which the resource capacity of the physical network is unlimited.

Fig.3 The USANET network

Fig.4 The topology of a FRAN

In general, in this simulation, we presume which 10000 SFC deployment requests arrive dynamically by following the Poisson process. The length of the SFC deployment request (i.e., \(n\)) varies among 5, 6, 7 and 8, the resource requirements of the VNF and the SFC link obey a uniform distribution \(U(5, 10)\) unit. We suppose that the location of the service terminal randomly distributed in a physical network node in the cloud network, and the location of the mobile user randomly distributed in a physical network node in the FRAN. The SSLA requirement of the SFC deployment request is set as follows. We first find a most secure path \(p (L_T, L_U)\) from the service terminal to the mobile user. Where, \(n \in p (L_T, L_U)\) denotes the physical node on the physical path \(p (L_T, L_U)\). Then, we set the SSLA requirement of the SFC deployment request according to Equation (19).

In our simulations, we will contrast our three algorithms with the traffic-aware and energy-efficient SFC deployment algorithm, SAMA, which is presented in [10] for minimizing the total placement cost. The SAMA algorithm is presented for the cloud network. In order to suit the federated environment of the cloud-fog network, we develop the SAMA algorithm so that it can place the SFC in the cloud-fog network.

\[
SR = \text{PathSecurity}(p(L_T, L_U)) \\
\times \prod_{i=1}^{n_{\text{VNF}}} \left\{ \frac{\text{Average}\{s(n_i), \forall n_i \in p(L_T, L_U)\} \times 2/3}{\min\{s(n_i), \forall n_i \in p(L_T, L_U)\} / 3} \right\} \\
= \prod_{i \in p(L_T, L_U)} s(l_i) \times \prod_{i=1}^{n_{\text{VNF}}} \left\{ \frac{\text{Average}\{s(n_i), \forall n_i \in p(L_T, L_U)\} \times 2/3}{\min\{s(n_i), \forall n_i \in p(L_T, L_U)\} / 3} \right\} \\
\text{Equation (19)}
\]

B. Simulation Results and Analysis

Fig.5 represents the blocking ratios of the MS, the MCG, the MCG-FA and the SAMA algorithms, wherein the length of the SFC deployment request (i.e., \(n\)) is changed among 5, 6, 7 and 8. From the results, it can be seen that the blocking ratios of our three algorithms are better than the blocking ratio of the SAMA algorithm. The SAMA algorithm is proposed to minimize the total deployment cost, when it was looking for a
solution, do not consider the SCLA requirement of the SFC deployment request. Thus, the blocking ratio of the SAMA algorithm is high. Besides, in our three algorithms, when we deploy each VNF $v_i$, we find the most secure path $p_{si}$ in the physical node $n_i$ and find the most secure path $p^{M}(n_i, L_U)$ from the current physical node $n_i$ to the user, to improve the blocking ratio. The MS algorithm uses the maximal-security strategy as a guide strategy for deploying VNF into the most secure physical node and finding the most reliable paths to maximize the security of the placement solution of SFC. It can maximize the security of the deployment of SFC and guarantee the success ratio. The MCSG algorithm uses the minimal-cost and SCLA-guaranteed strategy as a guide strategy for deploying VNF to minimize the total placement cost, but lead an increase in the blocking ratio. So, the blocking ratio of the MCSG algorithm is higher than the blocking ratio of the MS algorithm. The MCSG-FA algorithm first calls the MS algorithm to get an initial deployment solution, so that the MCSG-FA algorithm has a similar success ratio to the MS algorithm. Then it tries to find a deployment solution with the minimal total deployment cost to replace the initial deployment solution. This can reduce the consumption of key resources to improve the blocking ratio further. Hence, the MCSG-FA algorithm has a lower blocking ratio than the MCSG algorithm does.

We contrast the total links deployment costs of the MS, the MCSG, the MCSG-FA, and the SAMA algorithms in Fig.6, and compare the total VNFs deployment costs of the SAMA algorithm and our three algorithms in Fig.7, and compare the total SFCs deployment costs of four algorithms in Fig.8. From the results, we can see that the total links deployment cost of the MS algorithm is higher than the total links deployment cost of the SAMA algorithm because the MS algorithm pursues the maximal security of the deployment of SFC without regard to the deployment cost, and the SAMA algorithm is used for minimizing the total placement cost. Hence, the total links deployment cost, the total VNFs deployment cost and the total SFCs deployment cost of the SAMA algorithm are lower than that of the MS algorithm.

Because the MCSG algorithm uses the minimal-cost and SCLA-guaranteed strategy as a guide strategy for deploying VNF, it can effectively decrease the total links deployment cost, the total VNFs deployment cost and the total SFCs deployment cost compared to the MS algorithm. The MCSG-FA algorithm first calls the MS algorithm to get an initial deployment solution and then tries to calculate a deployment solution with the minimal total deployment cost to replace the initial deployment solution. It also can decrease the total links deployment cost, the total VNFs deployment cost and the total SFCs deployment cost compared to the MS algorithm.

Moreover, in the MCSG algorithm and the MCSG-FA algorithm, when we deploy each VNF $v_i$, we will find the most secure or minimal-cost $p^{M}(n_i, L_U)$ to reduce the hop of the entire deployment path. Therefore, the MCSG and MCSG-FA algorithms can obtain lower total link deployment costs than the SAMA algorithm. We find the path $p^{M}(n_i, L_U)$ and use the minimal-cost strategy, and it can deploy VNF into the entire deployment path based on a lower cost compared to the SAMA algorithm. Hence, the MCSG and MCSG-FA algorithm can get the lower total VNFs deployment cost than the SAMA algorithm does. So, the total SFCs deployment costs of the MS and the MCSG-FA algorithms are lower than that of the SAMA algorithm.

Fig.6 The total links deployment cost
VI. CONCLUSION

In the paper, we investigated the SFC placement problem with the SSLA requirement in the federated environment of the cloud-fog network. To guarantee the security of the deployment solution when the security of each physical node and link was aware, firstly, we formulated the linear programming with SSLA-guaranteed. Then, we presented an algorithm, MS, to maximize the security of the deployment of SFC. The MS algorithm could maximize the security of SFC deployment, but the total deployment cost was high. To reduce the deployment cost, we propose an algorithm, MCSG, to minimize the deployment cost and guarantee the SSLA of the deployment. Although the MCSG algorithm could reduce the total deployment cost, it would increase the blocking ratio. To improve the blocking ratio and the total deployment cost simultaneously, we presented an algorithm, MCSG-FA. Finally, we validated our proposed algorithms in the cloud-fog network. The results reveal that our proposed algorithms had better performance than the compared algorithm in the blocking ratio and the deployment cost. Our future work will include the integration between the...
cloud-fog network and AI-based intelligent systems to make our services more robust, secure and efficient.

ACKNOWLEDGEMENT

This research was partially supported by the National Key Research and Development Program of China (2019YFB1802800), PCL Future Greater-Bay Area Network Facilities for Large-scale Experiments and Applications (PCL2018KP001) and VC Research (VCR 0000086) of Prof. Victor Chang.

REFERENCES


