Network Slicing Deployment Strategies Based on Security and Trust: Postprint

Authors: Niu Ben, You Wei, Tang Hongbo

Date: 2018-05-20T00:00:00+00:00

Abstract

Under 5G mobile network virtualization scenarios, secure deployment of network slices is a prerequisite for future large-scale commercial deployment of 5G. To address the security of 5G network slice deployment, this paper proposes a network slice deployment strategy based on security trust. This strategy introduces the concept of security trust value to effectively quantify and analyze the security of VNFs and network resources. Based on this, a mathematical model for network slice deployment is constructed using 0-1 integer linear programming and solved with heuristic algorithms to find the deployment scheme with minimum cost. Simulation results show that the proposed strategy reduces deployment cost while ensuring security, and achieves better security benefits and deployment yield rates.

Full Text

Preamble

Title: Research on Network Slicing Deployment Strategy Based on Security Trust

Authors: Niu Ben, You Wei, Tang Hongbo (National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China)

Abstract: In the 5G mobile communication network virtualization scenario, secure deployment of network slices is a prerequisite for future large-scale commercial deployment. Addressing the security challenges of 5G network slice deployment, this paper proposes a network slicing deployment strategy based on security trust. The strategy introduces the concept of security trust value to effectively quantify and analyze the security of VNFs and network resources. Building upon this foundation, it constructs a mathematical model for network slice deployment using 0-1 integer linear programming and employs heuristic algorithms to find deployment solutions with minimal cost. Simulation results

demonstrate that the proposed strategy reduces deployment costs while achieving better security revenue and deployment return rates under the premise of ensuring deployment security.

Keywords: 5G; network slicing; security trust; deployment

0 Introduction

With the rise of the Internet of Things, vehicle networking, industrial control, and vertical industries, fifth-generation mobile communication (5G) technology will meet customized mobile service requirements across multiple domains and scenarios, realizing the vision of "everything connected" [1]. As a key technology in 5G networks, network slicing builds upon virtualization to dynamically tailor, orchestrate, and deploy multiple virtual network functions (VNFs), forming independent virtual networks that can provide customized network services according to user requirements [2]. Under the 5G architecture, network slice deployment can effectively enhance network flexibility and elasticity, promote efficient utilization of infrastructure resources, significantly reduce capital and operational expenditures, and satisfy users' customized security and service demands, thereby enabling on-demand networking.

Future 5G networks will adopt Software Defined Networking (SDN) and Network Function Virtualization (NFV) technologies, which introduce security challenges to network slice deployment due to virtualization. When deploying network slices on underlying resources, various security issues may arise: attacks on the underlying network threatening virtual networks (e.g., sniffing attacks, malicious modification of virtual machine information), compromised virtual machines affecting normal VNF operation (e.g., DoS attacks), mutual attacks between virtual networks due to shared underlying resources (e.g., cross-VM side-channel attacks, side-channel attacks), or security threats resulting from vulnerabilities in VNF software [3,4]. These security issues prevent network slices from functioning properly, compromising their confidentiality and integrity. Moreover, the difficulty in meeting user security requirements hinders large-scale deployment and commercialization of 5G network slices. Therefore, new security mechanisms and deployment methods are urgently needed to satisfy network slice deployment security requirements.

The primary challenge in network slice deployment lies in deploying VNFs within slices. Existing literature on VNF deployment primarily focuses on Internet or Evolved Packet Core (EPC) network scenarios and architectures, designing VNF deployment strategies based on different optimization objectives. For example, some studies deploy pooled virtual network functions in vEPC networks through traffic-aware and node splitting algorithms to effectively reduce virtual network resource overhead and improve network acceptance rates [5]; others deploy network element functions and optimize network topology for service function chains (SFCs) formed by mobile core network elements (PGW, SGW,

MME, etc.) [6]; some utilize genetic algorithms for dynamic VNF deployment to address the mismatch between static VNF deployment and dynamic requests or request changes [7]; others design multiple genetic algorithms to optimize maximum link utilization and bandwidth consumption [8]; some employ approximation optimization algorithms for VNF deployment [9]; and others use integer linear programming and heuristic algorithms for SFC deployment [10]. Additionally, some establish deployment models for SFC deployment and evaluation [11], while others combine variable neighborhood search with metaheuristic algorithms to find feasible design solutions for large-scale SFC deployment problems [12], and some design elastic VNF deployment strategies for operational cost optimization [13]. In summary, current VNF deployment strategies primarily aim to reduce VNF deployment costs, improve resource utilization, and balance network topology loads. However, few references and methods address VNF security, particularly VNF deployment security under the 5G network architecture. Therefore, this paper proposes a network slice security deployment algorithm to address security requirements during network slice deployment.

To overcome the limitations of existing network slice security deployment methods, this paper employs 0-1 integer linear programming to establish a mathematical model with minimum deployment cost as the objective, proposing a security trust-based network slice deployment strategy. The strategy utilizes security trust values to effectively quantify and analyze VNF and network resource security, and prioritizes the deployment and protection of high-security-level VNFs by ranking their security levels. Simulation experiments demonstrate that by considering global resource and security attributes, the proposed deployment strategy achieves good performance in deployment cost, security revenue, and deployment return rate while ensuring security.

1.1 Security Deployment Problem Description

Based on SDN/NFV technologies, 5G networks differentiate network functions from traditional EPC architecture network elements, enabling fine-grained network functions and improving network flexibility. Meanwhile, expensive dedicated hardware devices are migrated to general-purpose servers in software form, significantly reducing operational and maintenance costs. After unified orchestration by the SDN controller, deployed network slices can form a complete virtual network to provide service for users [14,15]. When deploying network slices, VNFs and requested links are deployed on underlying general-purpose resources to achieve the network services required by users [16]. Figure 1 [Figure 1: see original paper] illustrates the network slice deployment model. Under non-general premises and to simplify solution complexity while effectively shielding complex physical underlying details, this paper abstracts general physical hardware device resources and general distributed cloud platform virtual network resources in actual deployment into the network resource model shown in Figure 1 [Figure 1: see original paper].

To ensure VNF deployment security, the following security constraints should be satisfied during deployment:

a) The security trust value of network resource nodes must not be lower than the security trust value requirements of VNFs deployed on them, preventing VNF deployment on less secure resource nodes;

b) The security trust value of a VNF itself must not be lower than the security trust requirement of the network resource node on which it is deployed, preventing security vulnerabilities that the VNF may carry from affecting network resource security;

c) When deploying new VNFs on network resource nodes that already have deployed VNFs, the security trust value of the new VNF must not be lower than that of the already deployed VNFs, preventing insecure VNFs from attacking other VNFs through shared network resources;

d) VNFs with the highest security level should be deployed first and should not share underlying network resource nodes.

Security constraints a)~c) ensure that VNFs are securely deployed on underlying network resource nodes, while constraint d) ensures that high-security-level VNFs are not affected by co-residence attacks, reduces security risks, and achieves focused protection for high-security-level VNFs.

1.2 Mathematical Model

The network resources are represented as an undirected graph (Pp, PG, NE), where Pp and PG represent the sets of network resource nodes and links, respectively. For a network resource node $n \in N$, C_n, M_n, R_n, and S_n represent the CPU resource capacity, storage capacity, security trust requirement, and security trust value of the underlying resource node n, respectively. $P_{ij}^{e}(i, j \in N)$ represents the network resource link between nodes i and j, S_{ij}^{P} represents the security of the network resource link, determined by the minimum security trust value of nodes traversed from node i to node j, and B_{ij}^{P} represents the bandwidth resources of the network resource link.

The network slice deployment request topology is represented by an undirected graph (V_f, V_Q, F_E), where V_f is the set of VNFs to be deployed and V_Q is the set of request links. For a VNF $i \in V_f$, $(C_i^V, M_i^V, R_i^V, S_i^V)$ represents the CPU resource demand, storage resource demand, security trust requirement for network resources, and the VNF' s own security trust value, respectively. For a virtual network request link $e_{st}^{V} \in V_Q$ in the topology graph, (B_{st}^{V}, R_{st}^{V}) represents the bandwidth resource demand and required security trust value of link e_{st}^{V}, respectively. $\rho_{i,n}^{V,P} = 1$ indicates that VNF i is deployed on underlying network resource node n, and $\rho_{st,lv}^{V,P} = 1$ indicates that request link e_{st}^{V} is deployed on underlying network resource link e_{lv}^{P}.

2 VNF Security Level Research

During network slice deployment, VNFs within the slice should have different security levels based on different application scenarios, user requirements, business scopes, and risk factors. Focused protection of high-security-level VNFs can effectively improve the overall security of network slices. Conversely, attackers targeting high-security-level VNFs can achieve maximum impact with minimal effort, highlighting the vulnerability and susceptibility of high-security-level VNFs. Therefore, research on VNF security levels plays an important role in improving the security of entire network slice deployment. This section proposes multiple security level evaluation metrics and uses TOPSIS analysis to rank VNF security levels reasonably.

2.1 Security Level Evaluation Metrics

Metric 1: Based on VNF Type. Figure 3 [Figure 3: see original paper] shows the service-based 5G network architecture proposed by 3GPP, which separates control and bearer planes through SDN technology. VNFs forming network slices can be divided into control plane VNFs and user plane VNFs. Control plane VNFs are responsible for session management, mobility management, authentication and authorization, protocol management, and other control functions, while user plane VNFs (UPF represents the user plane function set) handle relatively simple routing and forwarding functions. For this evaluation metric, control plane VNFs are assigned a security level metric value of 1, and user plane VNFs are assigned 0.

Metric 2: Based on Traffic Volume of All Adjacent Links Connected to VNF. Let T_i represent the traffic flow through VNF i, as shown in Equation (1). The traffic metric T_i is determined by the incoming and outgoing traffic of VNF i.

$$T_i = T_i^{in} + T_i^{out}$$

Different network slices in various scenarios and services have different VNF traffic volume requirements. For example, in mMTC scenarios with massive IoT device access, VNFs with authentication functions have larger communication volume demands; in eMBB scenarios, VNFs with transmission functions have larger data communication volume demands. Due to the open nature of 5G, VNFs with frequent information flow interactions are vulnerable to harmful flow threats and attacks.

Metric 3: Based on VNF Degree Centrality. VNF degree centrality refers to the number of direct connections between a VNF and other VNFs in the network topology. In (V_f, V_Q, F_E), assuming there are g VNFs, the degree centrality $C_D(i)$ of VNF i is calculated as:

$$C_D(i) = \sum_{j=1}^{g} x_{ij}, \quad i \neq j$$

where x_{ij} represents the connection between VNF i and other g VNFs [19]. Different network slice templates for different user business requirements result in different connection relationships among VNFs within network slices. VNF degree centrality directly reflects these connection relationships. In terms of the degree of harm to the entire network after an attack and the difficulty of recovery after an attack, VNFs with higher degree centrality have greater impact when attacked and are more difficult and complex to recover.

Metric 4: Based on VNF Resource Requirements. The resource requirement R_i^V of VNF i is expressed as:

$$R_i^V = \alpha \cdot C_i^V + \beta \cdot M_i^V, \quad \alpha, \beta \in (0, 1], \alpha + \beta = 1$$

VNF resource requirements are its own capability factors, and higher resource demands make deployment more difficult. Therefore, VNFs with high resource requirements are more important and need to be assigned higher security levels for priority deployment.

Metric 5: Based on VNF Security Requirements. Higher VNF security requirements indicate higher security trust value requirements for network resource nodes hosting the VNF. Such VNFs should be considered for priority deployment to prevent potential co-residence attacks that may result from sharing nodes with less secure VNFs.

2.2 Security Level Ranking

When analyzing and ranking VNF security levels in network slices, relying on a single calculation metric is too one-sided. Considering multiple metrics may lead to inconsistent results since the five security level calculation metrics above are computed from different perspectives. To integrate multiple metrics, this paper uses TOPSIS analysis to convert multiple VNF security level calculation metrics into a multi-attribute decision ranking.

TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) is a ranking method that approximates the ideal solution. TOPSIS ranks alternatives based on their proximity to the ideal solution and negative-ideal solution in multi-attribute problems. The TOPSIS ranking procedure is as follows:

Step 1: Establish the security level decision matrix $X_{n\times m}$, as shown in Equation (4). Assuming there are n VNFs in the network slice and each VNF has m security level evaluation metrics, x_{ij} represents the j-th security level evaluation metric of the i-th VNF.

$$X_{n\times m} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nm} \end{bmatrix}$$

Step 2: To eliminate non-comparability caused by different dimensions and units, normalize the decision matrix to obtain the normalized matrix $Z = \{z_{ij}\}$, where $z_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{n} x_{ij}^2}}$. Simultaneously, set the weight matrix $\omega = (\omega_1, \omega_2, \ldots, \omega_m)^T$ with $\sum_{j=1}^{m} \omega_j = 1$ to obtain the weighted normalized matrix $Y = \{y_{ij}\}$, where $y_{ij} = z_{ij} \cdot \omega_j$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$.

Step 3: Determine the ideal solution y^* and negative-ideal solution y^o for the weighted normalized matrix. For the j-th attribute, the ideal solution is $y_j^* = \max\{y_{ij} | i = 1, 2, \ldots, n\}$ and the negative-ideal solution is $y_j^o = \min\{y_{ij} | i = 1, 2, \ldots, n\}$.

Step 4: Calculate the Euclidean distances between each security level evaluation metric and the ideal solution and negative-ideal solution. For the i-th VNF, the Euclidean distance to the ideal solution is:

$$d_i^* = \sqrt{\sum_{j=1}^{m} (y_{ij} - y_j^*)^2}, \quad i = 1, 2, \ldots, n$$

The Euclidean distance to the negative-ideal solution is:

$$d_i^o = \sqrt{\sum_{j=1}^{m} (y_{ij} - y_j^o)^2}, \quad i = 1, 2, \ldots, n$$

Step 5: Calculate the comprehensive evaluation index C_i^* for each VNF. The comprehensive evaluation index for the i-th VNF is:

$$C_i^* = \frac{d_i^o}{d_i^* + d_i^o}, \quad i = 1, 2, \ldots, n$$

Step 6: Rank the VNFs according to the comprehensive evaluation index C_i^*. A larger C_i^* indicates a higher security level of the VNF.

3.1 Network Slice Deployment Mathematical Model

When analyzing and evaluating VNF deployment schemes, the primary metrics are deployment cost, security revenue, and deployment profit rate.

a) Deployment Cost: For a network slice deployment request Q, its deployment cost is defined as:

$$Cost(Q) = \sum_{i \in V_f} \sum_{n \in N} \rho_{i,n}^{V,P} \cdot (C_i^V + M_i^V) \cdot S_n^P + \sum_{(s,t) \in V_Q} \sum_{(l,v) \in P_E} \rho_{st,lv}^{V,P} \cdot B_{st}^V \cdot S_{lv}^P \cdot Hop(e_{lv}^P)$$

where the binary value $\rho \in \{0, 1\}$ serves as a decision variable describing the deployment relationship between VNFs/virtual links and underlying network resources, with $\rho = 1$ indicating successful deployment and $\rho = 0$ indicating deployment failure. The first term in Equation (8) represents VNF deployment cost: the more CPU and storage resources a VNF requires and the higher the security trust value of the deployed network resource node, the higher the VNF deployment cost. The second term represents request link deployment cost: the more bandwidth resources a request link requires, the higher the security trust value of the deployed underlying link, and the more hops, the higher the request link deployment cost.

b) Security Revenue: For a network slice deployment request Q, its security revenue is defined as:

$$Revenue(Q) = \sum_{i \in V_f} \sum_{n \in N} \rho_{i,n}^{V,P} \cdot S_{i,n}^{V,P} + \sum_{(s,t) \in V_Q} \sum_{(l,v) \in P_E} \rho_{st,lv}^{V,P} \cdot B_{st}^V \cdot S_{lv}^P$$

Security revenue is determined by the occupied resources and overall security. Equation (9) shows that during network slice deployment, the more underlying network resources are used and the higher the overall security of the network slice, the greater the security revenue. The first term represents VNF security deployment revenue, where $S_{i,n}^{V,P}$ represents the comprehensive security of network resource node n hosting VNF i, consisting of both VNF security and underlying network resource security. If only one VNF is deployed on n, $S_{i,n}^{V,P} = S_i^V + S_n^P$; if r VNFs are deployed on n, $S_{i,n}^{V,P} = S_i^V + \frac{1}{\min\{S_1^V, \ldots, S_r^V\}}$, because multiple VNFs deployed on one node multiply the security risk of mutual VNF attacks. The second term represents request link deployment security revenue, which is related to the security trust value of the deployed underlying link and the required link bandwidth.

c) Deployment Profit Rate: For a network slice deployment request Q, its deployment profit rate is defined as:

$$\lambda = \frac{Revenue(Q)}{Cost(Q)}$$

The deployment profit rate estimates and balances deployment cost input and security revenue output, composed of deployment revenue and deployment cost.

As shown in Equations (8) and (9), increasing deployment revenue simultaneously increases deployment cost. During deployment, to maximize deployment utility, deployment cost should be controlled while increasing deployment revenue. A higher deployment profit rate indicates a better deployment scheme.

3.2 Optimization Objectives and Constraints

Optimization Objective:

$$\min \left(\sum_{i \in V_f} \sum_{n \in N} \rho_{i,n}^{V,P} \cdot (C_i^V + M_i^V) \cdot S_n^P + \sum_{(s,t) \in V_Q} \sum_{(l,v) \in P_E} \rho_{st,lv}^{V,P} \cdot B_{st}^V \cdot S_{lv}^P \cdot Hop(e_{lv}^P) \right)$$

Constraints:

$$\rho_{i,n}^{V,P} \in \{0,1\}, \quad \forall i \in V_f, \forall n \in N \tag{1}$$

$$\rho_{st,lv}^{V,P} \in \{0,1\}, \quad \forall (s,t) \in V_Q, \forall (l,v) \in P_E \tag{2}$$

$$S_n^P \geq R_i^V \cdot \rho_{i,n}^{V,P}, \quad \forall i \in V_f, \forall n \in N \tag{3}$$

$$S_i^V \geq R_n^P \cdot \rho_{i,n}^{V,P}, \quad \forall i \in V_f, \forall n \in N \tag{4}$$

$$S_i^V \geq S_k^V \cdot \rho_{i,n}^{V,P} \cdot \rho_{k,n}^{V,P}, \quad \forall i,k \in V_f, \forall n \in N, i \neq k \tag{5}$$

$$\sum_{n \in N} \rho_{i,n}^{V,P} = 1, \quad \forall i \in V_f \tag{6}$$

$$\sum_{i \in V_f} C_i^V \cdot \rho_{i,n}^{V,P} \leq C_n^P, \quad \forall n \in N \tag{7}$$

$$\sum_{i \in V_f} M_i^V \cdot \rho_{i,n}^{V,P} \leq M_n^P, \quad \forall n \in N \tag{8}$$

$$\sum_{(s,t) \in V_Q} B_{st}^V \cdot \rho_{st,lv}^{V,P} \leq B_{lv}^P, \quad \forall (l,v) \in P_E \tag{9}$$

Equations (12) represent security constraints a)~c) for VNF deployment proposed above, while Equation (13) represents link deployment security constraints. Equations (14)~(16) are constraints on underlying network resources during deployment. When deploying network slices, Equations (14) and (15) indicate that the sum of CPU and storage resource demands of VNFs deployed on the same underlying network resource node cannot exceed the resource capacity provided by that node. Equation (16) indicates that the sum of bandwidth demands of multiple request links deployed on the same underlying network resource link cannot exceed the underlying network

bandwidth capacity. Equation (17) indicates that a VNF can only be deployed on one underlying network resource node and cannot be split.

3.3 Algorithm Description

This paper proposes a heuristic security deployment algorithm named NS-SD (Network Slice Security Deployment). The algorithm consists of two phases: Phase 1 calculates security level evaluation metrics for each VNF in the deployment request and ranks their security levels using TOPSIS analysis; Phase 2 solves the optimization objective to obtain a secure deployment solution. Since the network slice deployment strategy model is an NP-hard problem, an implicit enumeration algorithm is run on the underlying network resource undirected graph to obtain the secure deployment solution [20~22].

NS-SD Algorithm Description:

Input: Network slice deployment request undirected graph V_Q; underlying network resource undirected graph P_G.

Output: Network slice security deployment scheme sd_{NS}

1. For each VNF $i \in V_f$, calculate the security level evaluation metrics of i.
2. For n VNFs, establish the security level decision matrix $X_{5\times n}$ and use TOPSIS analysis to rank VNF security levels, storing the ranking results in linked list $SPList$.
3. For each VNF and request link in $SPList$, construct candidate deployment sets.
4. If VNF i is not occupied and no other VNFs will be deployed on node n, deploy i on n and add the deployment result to sd_{NS}; otherwise, reject.
5. Use implicit enumeration algorithm.
6. If the algorithm executes successfully, update underlying network resources and add deployment results to sd_{NS}; otherwise, reject.

Steps (1)~(4) constitute Phase 1 of the algorithm, ranking the security levels of VNFs in V_f. Steps (5)~(7) are deployment preparation, generating node and link sets. Steps (8)~(20) constitute Phase 2, where (8)~(13) prioritize the deployment of the highest security level VNFs without sharing underlying nodes, and (14)~(20) deploy other nodes and links using integer linear programming. If the algorithm executes successfully, it outputs the deployment scheme sd_{NS}; otherwise, it rejects the deployment.

---

4 Simulation Experiments and Analysis

To evaluate the feasibility of the deployment model and the effectiveness of the NS-SD algorithm, this paper conducts simulation experiments based on

deployment cost, security revenue, and cost-profit rate, comparing the results with other algorithms.

4.1 Experimental Environment

For the underlying network resource topology graph, to ensure randomness and generality, this paper uses the K-means clustering algorithm from machine learning to generate an undirected graph P_G with 80 resource nodes and related links [23], as shown in Figure 4 [Figure 4: see original paper]. For each node in the generated network resource undirected graph, CPU capacity $C_n^P \in [5, 30]$, storage capacity $M_n^P \in [10, 100]$, security trust value requirement $R_n^P \in (0, 1]$, and its own security trust value $S_n^P \in (0, 1]$ are set. Each link is assigned a bandwidth capacity attribute $B_{lv}^P \in [1, 20]$.

Based on the 5G network architecture proposed in 3GPP' s latest technical specification TS23.501 [24], a network slice deployment request topology graph containing 15 VNFs is designed and generated, as shown in Figure 5 [Figure 5: see original paper]. In the generated topology, each VNF randomly sets CPU demand $C_i^V \in [5, 10]$, storage demand $M_i^V \in [10, 30]$, security trust value requirement $R_i^V \in (0, 1]$, and its own security trust value $S_i^V \in (0, 1]$. Each link sets a bandwidth demand attribute $B_{st}^V \in [1, 10]$. Among them, 9 control plane VNFs and 6 user plane VNFs are randomly set. Each VNF is also randomly assigned a traffic metric T_i, and the weighted matrix elements in TOPSIS analysis are all set to 0.2.

In the experiments, the NS-SD algorithm is compared with three other algorithms: Greedy algorithm, which adopts a greedy deployment strategy based on VNF and request link resource demands during slice deployment [25]; MST algorithm, which adopts a deployment strategy based on minimum spanning tree algorithm considering link bandwidth resource demands and minimum weight paths [26]; and NNS-SD algorithm, which is a simplified version of NS-SD with steps (8)~(13) omitted for comparison of deployment scheme revenue and cost without considering some security constraints. For fair comparison, Greedy and MST algorithms incorporate new security deployment constraints. To avoid randomness effects, each experiment is run 50 times with results averaged.

4.2 Experimental Results

The experiments evaluate algorithm performance using deployment cost, revenue, and profit rate as metrics.

1) Network Slice Deployment Cost

Figure 6 [Figure 6: see original paper] shows the variation in network slice deployment cost. The Greedy algorithm initially achieves minimum VNF deployment cost by selecting optimal underlying network resource nodes, but the chosen node locations result in excessive link hops, increasing link deployment cost. The MST algorithm ensures minimum link deployment cost, but VNF

deployment cost increases due to selecting underlying network resource nodes with excessively high security. The NS-SD algorithm initially shows rapid cost growth because it prioritizes high-security-level VNFs and links, but the implicit enumeration algorithm considers both link hops and globally searches for appropriate network resource nodes and links (with moderate security trust values). As VNF and request link deployments increase, the total deployment cost becomes lower. The NNS-SD algorithm has lower deployment cost than NS-SD because it omits some security constraints, allowing some VNFs to share underlying resources with the highest-security-level VNFs, thereby reducing some link deployment costs. However, this increases security risks for high-security-level VNFs from co-residence attacks. The experiments demonstrate that the NS-SD algorithm effectively reduces network slice deployment cost while improving overall deployment security.

2) Network Slice Deployment Revenue

Figure 7 [Figure 7: see original paper] shows the variation in network slice deployment revenue. The NS-SD algorithm achieves the highest total deployment revenue by considering global topology attributes of nodes and links and selecting the most reasonable nodes and links globally under security constraints. The Greedy algorithm deploys based on resource demands with local consideration of underlying network resource node security and poor coordination between deployed nodes and links, resulting in lower deployment revenue. The MST algorithm initially deploys VNFs on different network resource nodes to minimize VNF sharing and improve deployment revenue, but its local consideration leads to lower overall revenue. The NNS-SD algorithm shows lower security deployment revenue for some VNFs compared to NS-SD due to reduced security constraints allowing some VNF resource sharing. The experiments show that NS-SD effectively improves network slice deployment revenue while considering security constraints.

3) Network Slice Deployment Cost-Profit Rate

Figure 8 [Figure 8: see original paper] shows the variation in network slice deployment cost-profit rate. NS-SD and NNS-SD algorithms initially have lower cost-profit rates due to prioritizing high-security-level VNFs and request links, but they achieve better final cost-profit rates by considering global security and resource attributes and coordinating node and link deployment throughout the process. Greedy and MST algorithms have poor node and link coordination and local deployment considerations. Although they can achieve good cost-profit rates initially, the overall deployment scheme's cost-profit rate decreases as VNF and request link deployments increase. The experiments demonstrate that the NS-SD algorithm achieves a deployment scheme that, while ensuring security, effectively improves overall cost-profit rate by analyzing global attributes of underlying network resources and coordinating node and link deployment.

---

5 Conclusion

5G network slicing introduces new security issues due to virtualization technology. This paper studies network slice deployment problems in virtualized environments and proposes a security trust-based network slice deployment strategy to address the shortcomings of existing methods and the high security requirements of network slices. Simulation experiments verify the feasibility of the deployment model and the effectiveness of the algorithm. The method quantifies the security of VNFs and network resources and ranks VNF security levels to achieve focused protection of high-security-level VNFs in network slices. Simulation results show that the proposed deployment strategy can select appropriate nodes and links for network slice deployment while ensuring security, effectively reducing deployment cost and achieving better security revenue and deployment profit rate. Future research will investigate security issues that may arise during commercial operation of network slices to ensure high security requirements for network slices.

References

[1] China Mobile Communications Corporation. 5G service-guaranteed network slicing new white paper [EB/OL]. (2017-03-01) [2017-05-20]. http://www.huawei.com/ch-en/news/ch/2016/5G.

[2] Chen Shan-zhi. Analysis and suggestions on developing 5G [J]. Telecommunications Science, 2016, 32(7): 1-10.

[3] Fischer A, De Meer H. Position paper: secure virtual network embedding [J]. Praxis der Informationsverarbeitung und Kommunikation, 2011, 34(4): 191-195.

[4] Aljuhani A, Alharbi T. Virtualized network functions security attacks and vulnerabilities [C]// Proc of the 7th Annual Computing and Communication Workshop and Conference. 2017: 1-4.

[5] Tang Hong-bo, Yuan Quan, Lu Gan-qiang, et al. A vEPC virtual network function deployment model supporting node splitting [J]. Journal of Electronics & Information Technology, 2017, 39(3): 546-553.

[6] Baumgartner A, Reddy V S, Bauschert T. Mobile core network virtualization: a model for combined virtual core network function placement and topology optimization [C]// Proc of IEEE Network Softwarization. 2015: 1-9.

[7] Otokura M, Leibnitz K, Koizumi Y, et al. Application of evolutionary mechanism to dynamic Virtual Network Function Placement [C]// Proc of IEEE Workshop Coolsdn. 2016: 1-6.

[8] Cao J, Zhang Y, Wei A, et al. VNF-FG design and VNF placement for 5G mobile networks [J]. Science China Information Sciences, 2017, 60(4): 1-14.

[9] Cohen R, Lewin-Eytan L, Naor J S, et al. Near optimal placement of virtual network functions [C]// Proc of IEEE Computer Communications, 2015: 1-9.

[10] Luizelli M C, Bays L R, Buriol L S, et al. Piecing together the NFV provisioning puzzle: efficient placement and chaining of virtual network functions [C]// Proc of IFIP//IEEE International Symposium on Integrated Network Management. 2015: 98-106.

[11] Moens H, Turck F D. VNF-P: a model for efficient placement of virtualized network functions [C]// Proc of IEEE International Conference on Network and Service Management. 2014: 418-423.

[12] Luizelli M C, Cordeiro W L D C, Buriol L S, et al. A fix-and-optimize approach for efficient and large scale virtual network function placement and chaining [J]. Computer Communications, 2016, 10(2): 67-77.

[13] Ghaznavi M, Khan A, Shahriar N, et al. Elastic virtual network function placement [C]// Proc of the 4th International Conference on Cloud Networking. 2015: 255-260.

[14] Ravindran R, Chakraborti A, Amin S O, et al. 5G-ICN: delivering ICN services over 5G using network slicing [J]. IEEE Communications Magazine, 2017, 55(5): 101-107.

[15] Zhou X, Li R, Chen T, et al. Network slicing as a service: enabling enterprises' own software-defined cellular networks [J]. IEEE Communications Magazine, 2016, 54(7): 146-153.

[16] Nikaein N, Schiller E, Favraud R, et al. Network store: exploring slicing in future 5G networks [C]// Proc of International Workshop on Mobility in the Evolving Internet Architecture. 2015: 8-13.

[17] Wang Jing-pei, Sun Bin, Niu Xin-xin, et al. Trust model evaluation algorithm based on trusted modeling process [J]. Journal of Tsinghua University: Natural Science Edition, 2013, 53(12): 1699-1707.

[18] Meng Shun-mei. Research on trusted service composition and its key technologies in cloud computing environment [D]. Nanjing: Nanjing University, 2016.

[19] Stanley W, Katherine F. Social network analysis: methods and applications [M]. Beijing: China People' s University Press, 2012: 42-64.

[20] Shao W, Hu W, Huang X. A new implicit enumeration method for linear 0-1 programming [C]// Proc of IEEE International Workshop on Modelling, Simulation and Optimization. 2008: 298-301.

[21] Geoffrion A M. An improved implicit enumeration approach for integer programming [J]. Operations Research, 1969, 17(3): 437-454.

[22] Wang Jun, Li Duan. A new implicit enumeration method for polynomial 0-1 programming and applications [J]. System Engineering Theory and Practice,

2007, 27(3): 21-27.

[23] Harrington P. Machine learning in action [M]. Beijing: The People' s Posts and Telecommunications Press, 2013: 15-31.

[24] 3GPP. TR23.501, 3rd generation partnership project; technical specification group services and system aspects; procedures for the 5G system; rel. 15 [EB/OL]. (2017-04) [2017-05-20]. http://www.3gpp.org/ftp/Specs/latest-drafts/.

[25] Yu M, Yi Y, Rexford J, et al. Rethinking virtual network embedding: substrate support for path splitting and migration [J]. ACM Sigcomm Computer Communication Review, 2008, 38(2): 17-29.

[26] Peng Li-min. Cross-domain virtual network mapping algorithm based on minimum cost [J]. Journal of South China University of Technology: Natural Science Edition, 2015, 43(9): 67-73.

Note: Figure translations are in progress. See original paper for figures.