Embedding Security Awareness for Virtual Resource Allocation in 5G HetNets using Reinforcement Learning

Haotong Cao*†, *Student Member, IEEE,* Gagangeet Singh Aujla‡, *Senior Member, IEEE,* Sahil Garg§, *Member, IEEE*, Georges Kaddoum§, *Member, IEEE*, and Longxiang Yang¶†
* Department of Computing, The Hong Kong Polytechnic University, Hong Kong SAR, China
† Jiangsu Key Laboratory of Wireless Communications, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
‡ Department of Computer Science, Durham University, Durham, United Kingdom
§ Ecole de Technologie Superieure, Universite du Quebec, Montreal, Canada
(E-mail: haotong.cao@polyu.edu.hk, gagi_aujla82@yahoo.com, sahil.garg@ieee.org, georges.kaddoum@etsmtl.ca and yanglx@njupt.edu.cn)

Abstract

In the 5G era, heterogeneous networks (HetNets) are designed for achieving data rates and customized service demands. To realize this, virtualization technologies are widely accepted as enablers for implementing 5G HetNets, aiming at managing and scheduling virtualized physical resources in a flexible manner. However, the major focus of the existing research lies on the effective allocation of virtual resources and maximizing the number of implemented network services, ignoring the virtual resource security issues. However, the security threats and vulnerabilities due to the complexity of virtualization can lead to major performance outbreaks and information leakage. Therefore, this article attempts to tackle the security issues in 5G HetNets virtual resource allocation. The article starts from modeling the major security attacks for virtual resource allocation, through comprehensive discussion on the typical types of security attacks. Following the attack model, a novel secure framework (VRA-RL-SecAwa) based on emerging reinforcement learning approach, is presented. The proposed VRA-RL-SecAwa framework works in different phases, 1) Reinforcement learning based preliminary security preparation, 2) Greedy approach based secure virtual node resource allocation embedding, 3) Secure and shortest path virtual link resource allocation scheme, and 4) Network reconfiguration and updation. The proposed VRA-RL-SecAwa framework is evaluated through extensive simulations in order to demonstrate its efficiency and effectiveness. The results obtained validate the superiority of the proposed framework in contrast to existing variants of its category.

Index Terms

5G HetNets; Reinforcement Learning; Attack Model; Security Awareness; Virtualization Technologies; Virtual Resource Allocation.

1 Introduction

It is known to all that 5G heterogeneous networks (HetNets)[1] are designed for meeting the data rates and customized service demands. Virtualization technologies (network virtualization [2], network function virtualization, [3]) are regarded as the enabling technologies towards 5G HetNets. By running virtualization technologies, physical resources (e.g. CPUs, storages) can be flexibly abstracted, managed and scheduled by telecommunication service providers (TSPs). Therefore, more and more novel services and applications, equipped with customized resource demands (e.g. CPU, bandwidth), can be developed [4]. Fig. 1 highlights the key issue related to the association of 5G HetNets and virtual resource allocation technologies while accommodating more and more services.

In order to accommodate more services to coexist on the same underlying 5G HetNets, it is vital for the TSP to allocate virtual resources (e.g. virtualized CPUs, storages, bandwidths) efficiently (Fig. 1). As a consequence, it is important to explore the research possibilities and solutions related to the virtual resource allocation. Related publications, involving algorithms, currently exist [5-7]. In the literature, this kind of algorithms are named as virtual network embedding (VNE) solutions. However, a key problem is ignored in the virtualization research. The problem is that the complexity of virtualization can expose additional security threats and vulnerabilities. The malicious attackers can utilize these threats and vulnerabilities. These illegal behaviors will incur the network performance degradation [7]. Not to mention the further scarce information leakage. Therefore, the security of virtual resource allocation for 5G [6] networks cannot be ignored.

Though some attempts (e.g. [8-13]) have been made in the literature, they are one-sided and not comprehensive. Hence, these attempts are not applicable for implementing 5G HetNets. For instance, though Fischer *et al.*[8] discussed

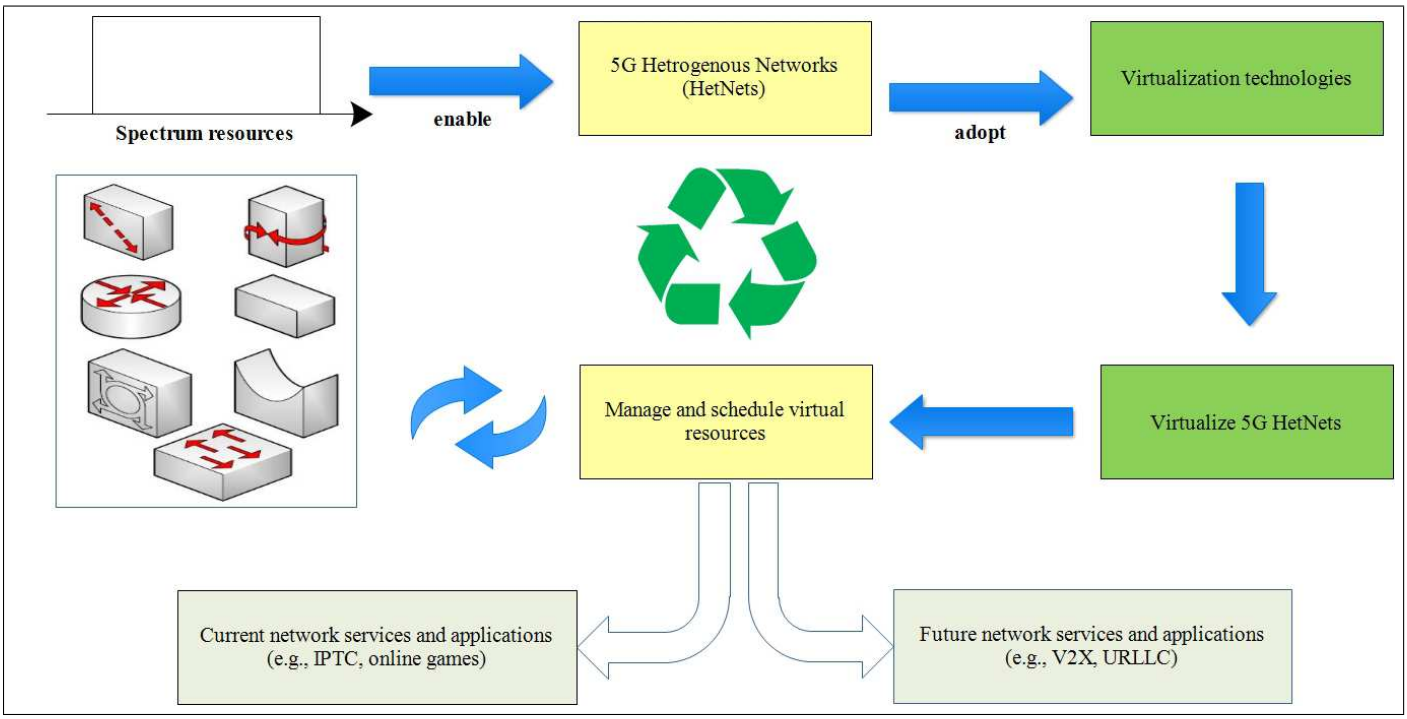


Fig. 1: Workflow of Virtualized Resource Allocation in 5G HetNets

three traditional types of attacks for 5G networks, nothing was related to the virtual resource allocation. Discussed attacks strictly belong to the node attack category. Link category was not considered in [8], either. With respect to [9] and [10], they just talked about the security mechanism in underlying network. What will happen if the potential risk of virtual nodes share the same underlying network element. In addition, Hou *et al.*[11] researched the secure issue in virtualized optical data center networks. The proposed secure model was limited in the optical networks. Hence, it cannot be promoted to universal network virtualization research. With respect to [12], Wang *et al.* talked about covert channel attacks. Wang *et al.* considered securing multiple nodes occupying the same physical device. However, the proposed mechanism for selecting secure physical nodes was ignored in [12]. While in [13], Besiltas *et al.* tried to fulfill virtual resources per virtual network within its allocated sub-physical network. Besiltas *et al.* divided the shared underlying network so as to achieve the secure virtual resource allocation. However, no security model was constructed in [13]. Besiltas *et al.* did not consider about the security threats and vulnerabilities of physical and virtual nodes.

1.1 Contributions of this Article

Based on these backgrounds, the virtual resource allocation with security awareness for 5G HetNets is investigated in this article. The major contributions of this article are highlighted as below:

- By talking about typical security attacks, the security attacks for virtual resource allocation are modeled and categorized. The secure virtual resource allocation model is presented, too. For clarity, radio and power resources are omitted in this article. The secure CPU, storage and communication bandwidth resource allocation are mainly considered.
- A novel virtual resource allocation framework with security awareness, based on reinforcement learning (RL) approach, is presented and labeled as *VRA-RL-SecAwa*. RL approach is currently an emerging technique to deal with network problems in machine learning and deep learning areas [14]. The proposed *VRA-RL-SecAwa* framework not only selects secure physical nodes, but also solves the potential covert channel attacks among virtual nodes, by isolating occupied physical elements (nodes and links).
- In order to demonstrate the efficiency and effectiveness of *VRA-RL-SecAwa*, simulations are performed. Secure virtual resource allocation strategies in [9] and [10] are selected for comparison.

1.2 Organization

The rest of this paper is organized as follows: Research background and model description are presented in Section 2. In Section 3, the novel virtual resource allocation framework with security awareness, based on RL approach, is presented. Simulation results are discussed in Section 4. In the end, conclusion and future directions are presented.

2 Background and Problem Description

This section is divided into tow parts, 1) the first part presents the comprehensive details about the research background and different types of security attacks in context with the virtual resource allocation, 2) the second part provides the insights related to the problem description for secure virtual resource allocation.

TABLE 1: Four Types of Security Attacks in 5G HetNets Virtualization

Item	Attack Type Name	Attacking Example	Primary Security Hazard and Potential Result
1	***Physical Element Attacking Virtual Element Type***	*Sniffing Attack*	Degrade the virtual network service quality
2	***Virtual Element Attacking Physical Element Type***	*Denial of Service*	Lead to the supporting physical node paralysis
3	***Attacks Among Virtual Elements Type***	*Covert Channel Attacks*	Mess up all virtual network services
4	***Attacks in the Physical Links Type***	*Replay Attacks*	Unavailability of physical links and connected nodes

2.1 Research Background and Types of Security Attack

Though virtualization technology brings flexible resource allocation for meeting various demands of 5G HetNets, it is a two-edged sword in terms of security [5]. As the virtualization technology introduces an additional layer between the architecture and the end of systems, more complexity is involved. Generally speaking, the security issue in virtual resource allocation for 5G HetNets can be classified into four types of security attacks: Physical Element Attacking Virtual Element, Virtual Element Attacking Physical Element, Attacks Among Virtual Elements, Attacks in the Physical Elements Type, which are illustrated in Table I. These four types of security attacks are described as below.

- ***Physical Element Attacking Virtual Element***: In this type, the physical element usually refers to the physical node. As known to all, the underlying nodes of physical network are are responsible for the management of virtual nodes. Following the contracted SLA and regulations, the accepted node will assign the virtualized resources (e.g. CPU, storage) to the virtual node. The virtual element can deploy its softwares on the physical node. However, if the physical element is seized control by an attacker, he can edit and cheat the virtual element information. Usually, an attack will be done on the virtual element, such as the sniffing attack (Table I).
- ***Virtual Element Attacking Physical Element***: Similar to the above type, the deployed virtual node may conduct the attack to the embedded physical node. Since the virtualization process of the physical node has vulnerabilities, the attacking virtual node will seize. In many cases, the attacking virtual node is not satisfied with achieving administration privileges, it will try to launch the denial of service (DoS) (Table I) attack [11] so as to inject redundant information. If this done, this will lead to the physical node overloaded. None virtual service cannot be deployed in this physical node any more.
- ***Attacks Among Virtual Elements***: In 5G HetNets resource allocation, different virtual network servicesare allowed to share one physical network. That means virtual nodes may share the same physical element, including its hardware and software resources can exist. In this case, there usually exists one covert channel. By the channel, these virtual nodes can exchange their own information. In some cases,certain virtual node will seize the side-channel attacks [12]. Therefore, the security issue of side-channel attacks emerges.
- ***Attacks in the Physical Links***: The last security type is the Attacks in the Physical Links Type [13], cannot be ignored, either. For instance, if certain physical device is placed on a substrate link, not managed by the TSP, the physical device may be attacked by certain attacker. That attacker can perform multiple attacks on the substrate link, such as man-in-the-middle at tacks and so on (Table. I). Hence, this type of security issue cannot be ignored. While allocating and mapping virtual links to physical paths, the physical paths, having equal or higher security level than the mapped virtual links, ought to be selected in priority.

With introducing the above four types of security attacks and listing out main security results (Table. I) [6][8], it is vital to research and propose a novel virtualization resource allocation framework with security awareness, which acts as an enabler to tackle these security attacks.

2.2 Problem Description

After introducing the security types, it is necessary to model these security types and virtual resource allocation for 5G networks formally. For a better understanding of the problem modeling and description for secure virtual resource allocation, the Fig. 2 has been presented. With respect to the model of security, the abstraction method so as to model the security constraints is adopted. The security model consists of two parts: *security level* and *security demand*. The security level part is not limited in a scalar. It ought to be expressed by a vector parameter. This formulation method aims at capturing the security guarantees for network elements [6][8]. Within the security level variance, two main insights are responsible: one is the heterogeneous customer needs, the other is the different upgrading physical network elements. That is to say, the underlying physical network consists of different generations of physical nodes and virtualization softwares. Especially to the virtualization softwares, they can offer different security guarantees. Hence, the security level modeling method is sufficient to abstract the security difference from the theoretical aspect.

With respect to the security demand part, it is formulated by security levels. The security demand can be fulfilled by the substrate node enabling to provide equal or higher level. This modeling method contributes to embracing many distinct forms of security demands. In Fig. 2, the $(L3, D2)$ in the virtual service request indicates that the virtual node requires the assigned physical node to have the security level of 3 and a security demand of no less than 2. The

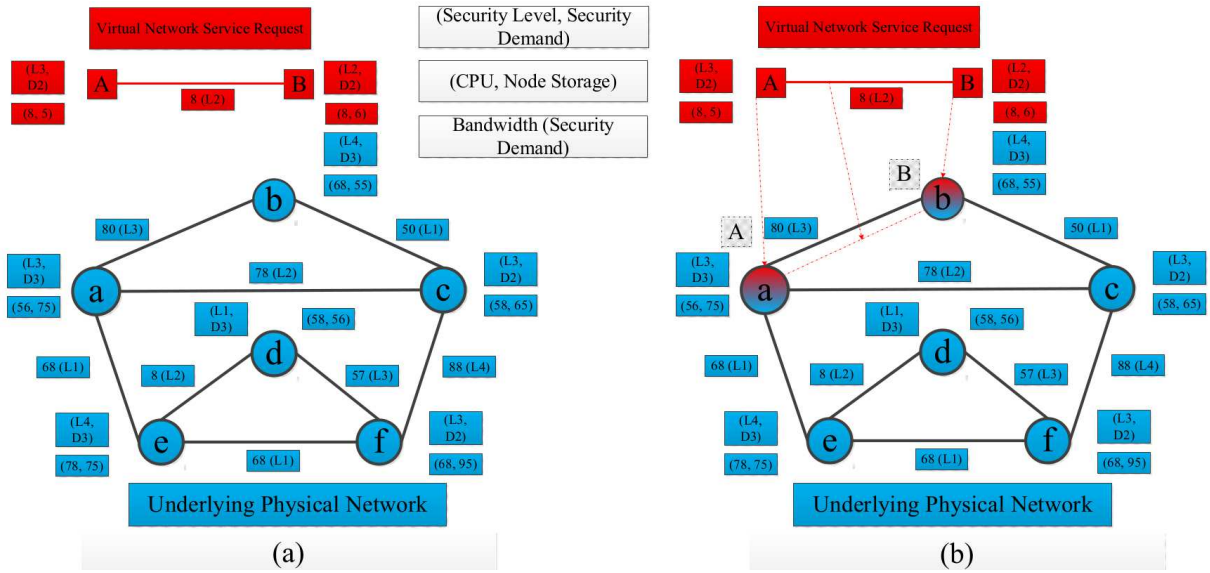


Fig. 2: Example of Secure Virtual Resource Allocation in 5G HetNets

8 $(L2)$ in the same virtual request represents the virtual link has a demand of 8 bandwidths and a security level demand of no less than 2. The virtual resource allocation for 5G networks is composed of two sub-models: for the whole underlying physical network and for the virtual service. The whole substrate network is usually modeled as an undirected graph, consisting of multiple substrate nodes and links. To the whole substrate nodes, they are the abstractions of hosts, switches, routers, phones. These abstracted nodes have similar resources, such as CPUs, storages, placed locations and so on. In this article, CPU, storage and placed location are selected as virtualized node resources, aiming at being allocated to virtual network services. With respect to the virtual links, they are adopted to connect virtual nodes. Optical fiber and twisted pairs are abstracted into virtual links. Virtualized link resources are communication bandwidths in this article. Virtualized substrate (node and link) resources are plotted and labeled in Fig. 2.

With respect to the other sub-model, it is the virtual network service request. Same to the physical network, it is abstracted into an undirected graph. It can be seen as a combination of virtual node and link resources. The virtual network service request is shown in Fig. 2 (a). Demanded node and link resources and securities are labeled out. In addition, the allocation and mapping results are shown in Fig. 2 (b): virtual node A is assigned to substrate node a while B is mapped onto b. Virtual link AB is accommodated by physical path ab. Meanwhile, all resource and security demands are fulfilled. We highlight the consumed physical elements in light red. Take note that security demand of the virtual network must be satisfied.

3 VRA-RL-SecAwa: Virtual Resource Allocation With Security Awareness

The different phases of *VRA-RL-SecAwa* framework are described in the subsequent sections.

3.1 Workflow of *VRA-RL-SecAwa*

The proposed framework is labeled as *VRA-RL-SecAwa* in this paper. In this sub-section, the workflow of *VRA-RL-SecAwa* (Fig. 3 (a)) is plotted so as to assist readers to easily understand the procedures of the *VRA-RL-SecAwa* allocating and mapping virtual resources to each demanded virtual network service.

3.2 Secure Virtual Resource Allocation Framework

Along with the Fig. 3 (a), the virtual resource allocation of certain virtual network service, VN^v, is described as an example. For allocating virtual resources of physical network (PN) to VN^v, *VRA-RL-SecAwa* has the following four key procedures:

3.2.1 RL-Based Preliminary Security Preparation

According to previous proposals [5][6][7], it is proved that quantified node values, no matter substrate or virtual, are the basis and have an influence on the quality of virtual resource allocation. Hence, it is important to adopt an efficient calculation method so as to ensure the quality of virtual resource allocation. As presented in the existing proposal [15], node values are calculated by incorporating multiple topology attributes and global resources. By providing proof and conducting simulation, the existing node ranking approach has been proved efficient, comparing with existing publications [5][6]. Based on the gained research results [15], the security level and security demand are incorporated into the product of calculating resource block. With respect to remaining procedures, they are same to what are presented in [15]. Finally, one kind of stable node values can be calculated: for all virtual nodes of the VN^v. The number of virtual node value is equal to $||VN^v||$.

With respect to the physical node values of the underlying PN, the emerging RL approach [14] is adopted, aiming at achieving a thorough knowledge of PN. In this article, four different attributes (Topology, Resource, Security, and Demand) per physical node are firstly extracted. Then,

these extracted attributes are normalized and concatenated into the feature vector. In total, $|PN|$ vectors form up an extracted matrix, acting as the input of RL agent, which is called as the policy network in AI area. See Fig. 3 (b). Then, the input matrix will go through three phases. With respect to detailed procedures of these three phrases, they are same to [14]. Comparing with the universal procedures of policy network in [14], the main difference and highlight is that Topology, Security and Demand attributes are incorporated as input, not just the Resource attribute. Within the policy network (Fig. 3(b)), the universal policy gradient method is adopted to train and testing the whole PN. In the end, candidate physical nodes, having high probability values, are selected.

3.2.2 Greedy Approach for Secure Virtual Node Resource Allocation Embedding

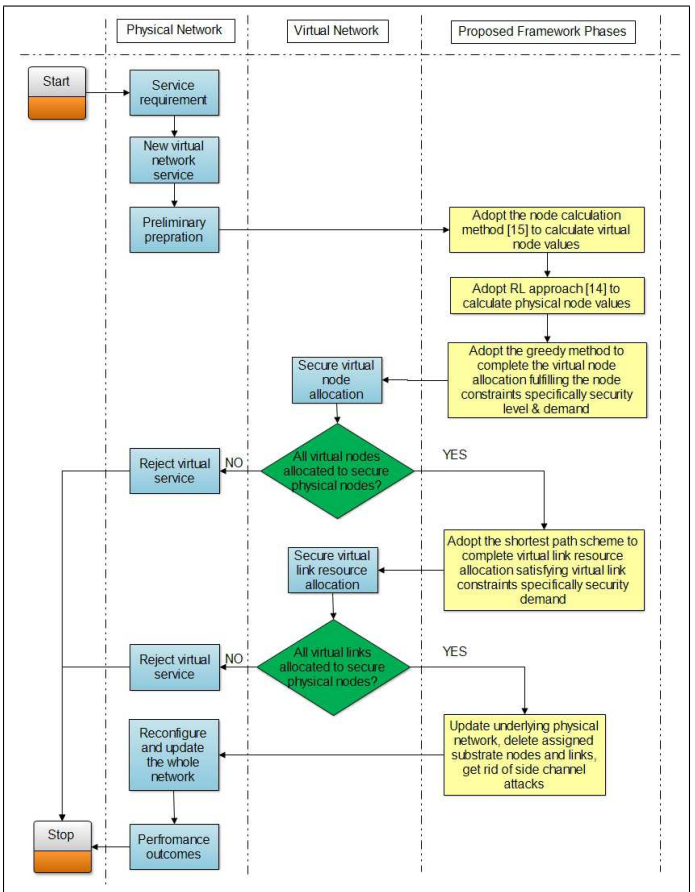
After completing the preparation, our *VRA-RL-SecAwa* starts to do the secure virtual resource allocation for VN^v. The secure allocation for VN^v consists of two parts: secure greedy node allocation and secure link resource allocation. We firstly talk about the secure greedy node allocation. The virtual node having highest value is processed in priority. We will select the RL-based physical node having highest value in priority. If the resources (CPU, storage), security level and demand of the physical node fulfill the highest virtual node. The first virtual node embedding is done. Remaining virtual nodes will be processed, following the strategy. Hence, the secure virtual node resource allocation is guaranteed.

3.2.3 Secure and Shortest Path Virtual Link Resource Allocation Scheme

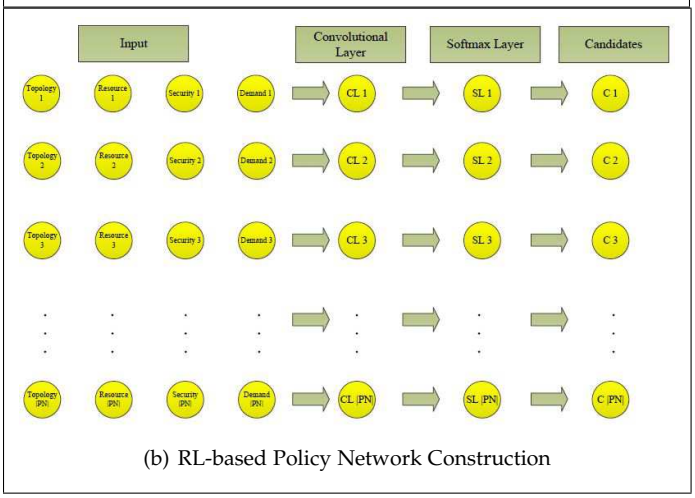
With all nodes in VN^v are embedded and corresponding resource demands are fulfilled, we will continue the secure virtual links embedding. Meanwhile, security and resource demands per virtual link must be guaranteed. We select one virtual link as the example. Two end nodes of the virtual link are done in the previous procedure. We need to select the most suitable physical path from the path set of two end nodes. Take note that three extra requirements must be fulfilled. At first, the selected physical path must have the lowest number of intermediate nodes among all physical links. Then, the security of the selected path must be larger or equal to the virtual link. Thirdly, it must reserve enough bandwidth for the virtual link. This link mapping strategy is accepted as the upgraded version [6]. Follow this scheme to embed remaining virtual links. When all virtual links are done, the link security and resource allocation are done.

3.2.4 Network Reconfiguration and Updation

With allocating virtual node and link resource of the virtual network service VN^v successfully, the resource information of the underlying network is updated. In addition, the underlying network is reconfigured. The reason of reconfiguration is that the third type of attack may influence the virtualization quality. In above three procedures, type one, two and four are considered. With respect to the third type of attack, it must be dealt with before new virtual network service is allocated. Within this procedure, all assigned



(a) Workflow of VRA-RL-SecAwa



(b) RL-based Policy Network Construction

Fig. 3: Proposed Framework

substrate nodes and substrate paths are deleted. Here, the aim is to isolate different virtual networks from each other. In this case, the side-channel attacks in the same substrate node does not exist any more. When certain virtual network expires, the allocated resources are released. Consequently, deleted substrate elements are added to the underlying substrate again. Since the underlying network scale is great and scale of virtual network service is much smaller than the substrate network, the situation where no enough substrate elements are reserved for accommodating following virtual network services is not of much importance.

3.3 Discussion of *VRA-RL-SecAwa* Complexity

This sub-section is about the time complexity of *VRA-RL-SecAwa* framework, consisting of four procedures. The first procedure is about the preliminary security preparation. It can be completed no more than $O((|N^P|) \cdot log(1/\delta))$ [15]. $|N^P|$ records the number of total physical nodes. The physical network scale is usually larger than the virtual network scale. δ represents the small positive number, indicating the learning rate. With respect to the second (greedy node allocation) and third (shortest path allocation) procedures, they are both polynomial-time procedures [7]. The fourth procedure is completed less than $O(|N^P| + |L^P|)$ [7], where $|L^P|$ refers to total physical links. Therefore, the *VRA-RL-SecAwa* framework is able to complete any virtual network service allocation and mapping within polynomial time.

TABLE 2: Simulation Parameter Setting

Parameter	Value description
Substrate node amount	100
Substrate link amount	600
Substrate CPU, storage and link bandwidth	Real number, Uniformly distributed [50,100]
Security level of substrate node	Integer number, Uniformly distributed [1,5]
Security demand of substrate node and link	Integer number, Uniformly distributed [1,5]
Virtual node amount	Integer number, Uniformly distributed [2,10]
Connectivity possibility per virtual node	0.5
Virtual CPU, node storage and link bandwidth demand	Real number, Uniformly distributed [0,10]
Security level of virtual node	Integer number, Uniformly distributed [1,5]
Security demand of virtual node and link	Integer number, Uniformly distributed [1,5]

4 Simulation Evaluation

The proposed framework has been evaluated in a simulated environment for validating its effectiveness in 5G HetNets. The simulation settings, results obtained and associated discussion are presented in the subsequent sections.

4.1 Simulation Environment

Since virtualization technology in 5G networks is still in its infancy, the proposed *VRA-RL-SecAwa* has been evaluated through extensive simulations. The underlying physical network and all virtual network service requests are modeled by GT-ITM software. The parameter settings of (substrate and virtual) networks are listed in Table. II. Here, the virtual network services are requested following the Poisson process. The arrival rate is set 5 per 100 time units. 1 time unit represents 1 minute in the simulation part. The simulations are set 10000 time units. Regarding parameters of policy network (Fig. 3 (b)), training process, and testing process, they are same to what are detailed in [14].

4.2 Results and Discussion

In this subsection, we record and plot main simulation results in Fig. 4. Then, we discuss the simulation results. Selected virtual allocation strategies (*cSAv* [9], *Sec-bd* [10]) are modified so as to make them be mostly closely related to the proposed *VRA-RL-SecAwa*.

1) *Virtual Network Service Acceptance Ratio*: Serving as the leading metric in virtual resource allocation research, we firstly plot the acceptance ratio results of all selected framework and strategies. Obviously, we can easily find that all framework and strategies undergo the decrease of service acceptance ratio. The reason for acceptance ratio decreasing is the limited physical resources. When the simulation work starts, there exist abundant physical resources. Thus, new requested virtual network services can be deployed. Virtual resource and security demands are fulfilled. The acceptance ratio will remain in a high level. However, the physical resources are limited. Thus cannot keeping acceptance ratio high.

In addition, our *VRA-RL-SecAwa* achieves higher acceptance ratio than the remaining two strategies. The second best behaved strategy is *Sec-bd* throughout the whole simulation. For example, since 1000 time point, the acceptance ratio of *VRA-RL-SecAwa* is higher than that of *Sec-bd*. Throughout the whole evaluation, the gap is firstly becoming small then return to large statue. The causes of our *VRA-RL-SecAwa* highest acceptance ratio are its extracted topology attributes, node value method, and RL-based approach. The efficiency of topology attributes and node value method was discussed in previous publication [15]. We do not repeat in this paper again. With respect to the efficient RL-based approach, it enables to achieve the node potential. Therefore, the physical nodes, having enough resources and security demands, are usually highlighted to be selected. Consequently, they are adopted to allocate virtual resources and achieve secure goals.

2) *Long-term TSP Revenue and Long-term TSP Revenue to Cost Ratio*: It is not wise to talk the TSP revenue and revenue to cost ratio separately. Thus, we decide to discuss both kinds of simulation results together. Apparently, our proposed *VRA-RL-SecAwa* achieves the highest revenue and revenue to cost among three framework/strategies. The reason for the advantage behaviors is discussed for the acceptance ratio. By extracting and quantifying proper attributes and RL approach, the most suitable physical nodes and paths will be selected out. Therefore, more physical resources can be reserved for more virtual services. When accepting more service, the revenue will be maximized. At the same time, the whole physical network will be utilized to its capacity. Therefore, the long-term revenue to cost ratio will be maximized, too.

5 Conclusions and Open Directions

Since secure network connectivity and resource allocation are important for 5G HetNets, we research the secure issue in this article. In particular, formal model for secure virtual resource allocation is constructed. A novel framework (*VRA-RL-SecAwa*) with security awareness, based on reinforcement learning approach, is proposed. To validate

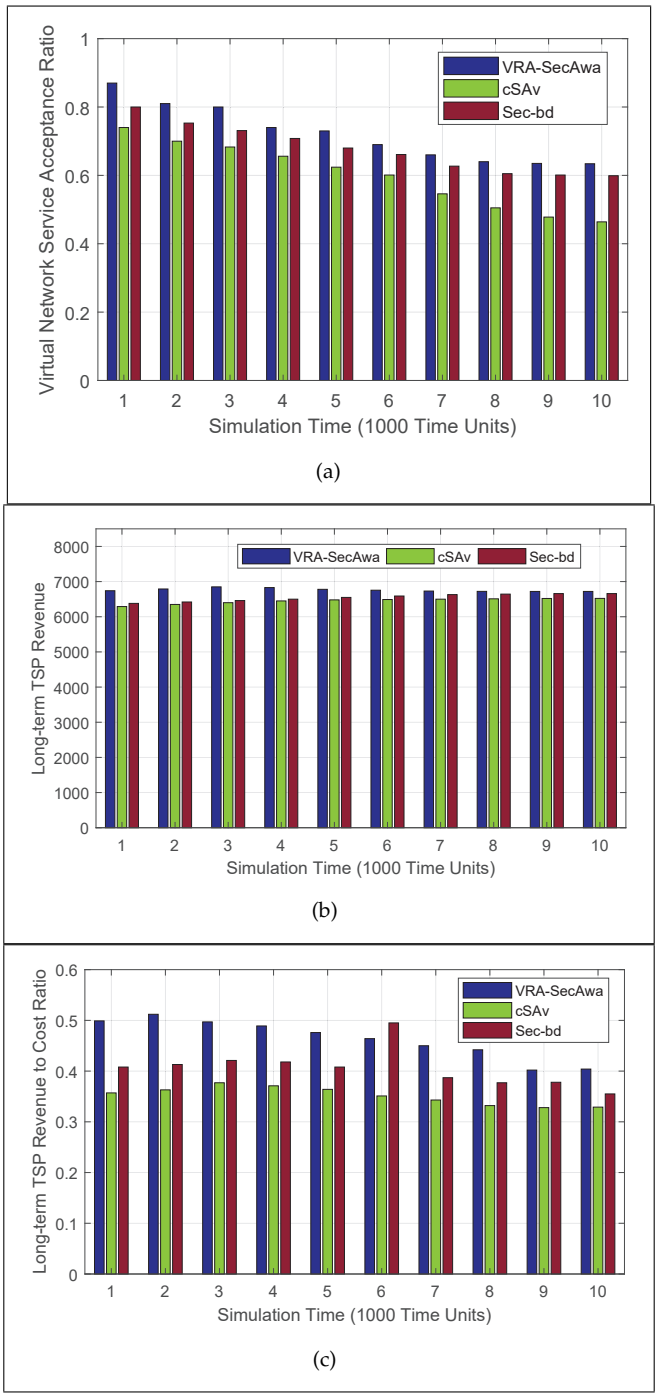


Fig. 4: Simulation Evaluation Results

the *VRA-RL-SecAwa* efficiency and effectiveness, the simulation experiments are performed and described. Since the secure issue for 5G HetNets is still in its infancy, we present some future directions below:

5.1 Future Directions and Open Issues

1) *Incorporate Historical Security Data*: One possible direction of the secure virtual resource allocation in 5G HetNets is to perfect the constructed security model. In real networking environment, incorporating historical security data [9] to model the security probability is very important. With adding historical security data, the security model can be perfected, further revealing the characteristics of network element threats and vulnerabilities [6]. If that, the perfected security model will be more convincing.

2) *Propose Other Efficient Frameworks and Allocation Algorithms*: Though the proposed *VRA-RL-SecAwa* framework is proved efficient by simulation, there exists space proposing other efficient frameworks and virtual resource allocation algorithms. For instance, following researchers can quantify other security-related attributes [8] in the preliminary preparation procedure so as to highlight and select the secure nodes.

3) *Develop Emerging Meta-Heuristic Frameworks and Algorithms*: Another possible direction is to develop more emerging meta-heuristic algorithms. Existing metaheuristics such as ant colony optimization [6] can be adopted to find efficient HetNet allocation solutions by succeeding in improving certain one solution, according to the given measuring method.

4) *Expand Experiment Network Scale*: The scale of substrate network in this article is limited within 100 nodes, accepted as the medium scale in network research [3]. If the network scale expands, can our *VRA-RL-SecAwa* framework work and converged within allowed time? The research of its convergence requires extra attention.

5) *Other Network Application Scenarios*: In this article, the *VRA-RL-SecAwa* framework is simply evaluated in the 5G HetNets scenario. With respect to other network scenarios, such as the Data Center (DC) Networks, pure computer networks, and cellular networks, the *VRA-RL-SecAwa* should be adopted to deal with the virtual resource allocation.

Acknowledgments

This article is supported by National Natural Science Foundation of China under Grant 62071246, 61427801 and 61372124, National Key Research and Development Program of China under Grant 2018YFC1314903. This work is partially funded by the Durham University Fund.

References

[1] X. You, C. Wang, J. Huang, et al, "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," Sci. China Inf. Sci., vol. 64, no. 1, 110301, 2021.

[2] X. Li, H. Mengyan, Y. Liu, V. G. Menon, A. Paul and Z. Ding, "I/Q imbalance aware nonlinear wireless-powered relaying of B5G networks: Security and reliability analysis," IEEE Trans. Netw. Sci. Engi., vol. pp, no. 99, pp. 1-1, 2020.

[3] A. Jindal, G. S. Aujla, N. Kumar, R. Chaudhary, M. S. Obaidat, and I. You, "SeDaTiVe: SDN-enabled deep learning architecture for network traffic control in vehicular cyber-physical systems," IEEE Net., vol. 32, no. 6, pp. 66-73, Dec. 2018.

[4] S. Jacob, V. G. Menon, P. G. Shynu, S. K. S. Fathima, B. Mahapatra and S. Joseph, "Bidirectional multi-tier cognitive swarm drone 5G network," in Proc. of 2020 INFOCOM WKSHPS, pp. 1219-122, Jul. 2020.

[5] H. Cao, S. Wu, Y. Hu, Y. Li, and L. Yang, "A survey of embedding algorithms for virtual network embedding," China Commun., vol. 16, no. 12, pp. 1-33, Dec. 2019.

[6] H. Cao, H. Hu, Z. Qu and L. Yang, "Heuristic solution of virtual network embedding: A survey," China Commun., vol. 15, no. 3, pp. 186-219, Mar. 2018.

[7] H. Cao, L. Yang, Z. Liu, and M. Wu, "Exact solutions of VNE: A survey," China Commun., vol. 13, no. 6, pp. 48-62, Jun. 2016.

[8] A. Fisher, H. Meer, et al, "Secure virtual network embedding," Informationsverarbeitung und Kommunikation, vol. 34, no. 4, pp. 190-193, Apr. 2011.

[9] S. Liu, Z. Cai, H. Xu and M. Xu, "Towards security-aware virual network embedding," Computer Networks, vol. 91, no. 11, pp. 151-163, Nov. 2015.
[10] L. Bays, R. Oliverira, L. Buriollos, and L. Gaspary, "Security-aware optimal resource allocation for virtual network embedding," in Proceeding of CNSM, IEEE, pp. 378-384, 2012.
[11] W. Hou, Z. Ning, L. Guo, Z. Chen and M. Obaidat, "Novel framework of risk-aware virtual network embedding in optical data center networks," IEEE Systems Journal, vol. 12, no. 3, pp.2473-2482, Mar. 2018.
[12] Z. Wang, J. Wu, Z. Guo, G. Cheng, and H. Hu, "Secure virtual network embedding to mitigate the risk of covert channel attacks," in 2016 IEEE INFOCOM WKSHPS, pp. 1-2, 2016.
[13] C. Besiktas, D. Gozupek, A. Ulas and E. Lokman, "Secure virtual network embedding with flexible bandwidth-based revenue maximization," Computer Networks, vol. 93, no. 1, pp. 89-98, Jan. 2017.
[14] H. Yao, X. Chen, M. Li, P. Zhang and L. Wang, "A novel reinforcement learning algorithm for virtual network embedding," Neurocomputing, vol. 284, pp. 1-9, 2018.
[15] H. Cao, S. Hu, and L. Yang, "New functions added to ALEVIN for evaluating virtual network embedding," in Proc. 2nd IEEE Int. Conf. Comput. Commun., Oct. 2016, pp. 2411–2414.

Haotong Cao (S'17-M'20) received the Ph.D. Degree from Nanjing University of Posts and Telecommunications (NJUPT). He is currently the PostDoc Researcher in the Hong Kong Polytechnic University. He has published multiple IEEE Trans./Journal/Magazine papers. His research interests include wireless communication theory, convex optimization, network and physical layer security, and network architecture for 6G.

Gagangeet Singh Aujla (S'15-M'18-SM'20) is an Assistant Professor of Computer Science at Durham University. Before this, he worked as a post-doctoral research associate at Newcastle University, a research associate at Thapar University (India), a visiting researcher at University of Klagenfurt (Austria) and on various academic positions for more than a decade. He received my PhD degree from the Thapar University (India), my Master and Bachelor degrees from the Punjab Technical University (India). For my contributions to the area of scalable and sustainable computing, I was awarded the 2018 IEEE TCSC Outstanding PhD Dissertation Award of Excellence. He is an Area Editor of Ad hoc Networks and Topic Editor of Sensor Journal.

Sahil Garg (S'15-M'18) received his Ph.D. degree from Thapar Institute of Engineering and Technology, Patiala, India, in 2018. He is currently working as a postdoctoral research fellow at École de Technologie Supérieure, Université du Québec, Montréal, Canada. He has many research contributions in the area of machine learning, big data analytics, cloud computing, and vehicular ad hoc networks. He also received the IEEE ICC Best Paper Award in 2018 and IEEE TCSC Early Career Research Award 2020.

Georges Kaddoum (M'11) received the bachelor degree in electrical engineering from the École Nationale Supérieure de Techniques Avancées (ENSTA Bretagne), Brest, France, the M.S. degree in telecommunications and signal processing (circuits, systems, and signal processing) from the Université de Bretagne Occidentale and Telecom Bretagne, Brest, in 2005, and the Ph.D. degree (Hons.) degree in signal processing and telecommunications from the National Institute of Applied Sciences (INSA), University of Toulouse, Toulouse, France, in 2009. Since 2013, he has been an Assistant Professor of Electrical Engineering with the École de Technologie Supérieure (ETS), University of Québec, Montréal, QC, Canada.

Longxiang Yang is a Full Professor and Doctoral Supervisor of NJUPT. He was the head of College of Telecommunications and Information Engineering, NJUPT. He has fulfilled multiple National Natural Science Foundation projects of China. He has authored and co-authored over 200 technical papers published in various journals and conferences. His research interests include cooperative communication, network coding, wireless communication theory, 6G mobile communication systems, ubiquitous networks and Internet of things.