ACCEPTED FROM OPEN CALL

RELIABILITY EVALUATION FOR NFV DEPLOYMENT OF FUTURE MOBILE BROADBAND NETWORKS

JIAJIA LIU, ZHONGYUAN JIANG, NEI KATO, OSAMU AKASHI, AND ATSUSHI TAKAHARA

ABSTRACT

The concept of NFV appears to be a promising direction to save cellular network service providers from endlessly increasing capital investment, given the fast evolving mobile broadband communication techniques and unprecedented consumer demand for quality of service and quality of experience in mobile access. Meanwhile, given the deployment of NFV, the virtualized network functions and the physical hardware resources are still vulnerable to natural disasters and malicious attacks. We present in this article the first framework for reliability evaluation of NFV deployment and specific algorithms to efficiently determine the key set of physical or logical nodes there.

INTRODUCTION

Worldwide, cellular service providers are facing a dilemma because the unprecedented prosperity in mobile broadband communication brings great opportunities but also huge challenges. On one side, the last decade has witnessed an unprecedented increase in the number of mobile connected devices as well as consumer demand for ubiquitous and fast mobile broadband Internet access. Pushed by such tremendous broadband connectivity and mobile traffic, the Third Generation Partnership Project (3GPP) has started to develop the standards and techniques for the fifth generation (5G), which is expected to achieve a data speed of 100 to 1000 Mb/s for actual users (a 10- to 100-fold increase over the typical 4G speed of 10 Mb/s), by adopting lots of innovative communication techniques including massive multiple-input multiple-output (MIMO) [1], millimeter-wave, device-to-device communication, and so on.

On the other side, in order to keep up with the fast evolving mobile broadband communication techniques and thus provide the expected access quality of service (QoS, including download/upload throughput/delay, etc.) and quality of experience (QoE), cellular service providers have to continuously increase their financial investment in infrastructure construction, in terms of purchasing new expensive networking/computing/storage devices, upgrading existing hardware devices, deploying new base stations, and so on. Note that the infrastructure investment usually does not come alone, but together with other extra expenditures, such as the energy cost (electricity), the human resource expenditure of hiring skilled personnel for network design, construction, operation, and maintenance, especially for such extremely complicated and heterogeneous fusion of hardware devices and services from 2G, 3G, 4G, as well as the emerging 5G. Therefore, in the era of 5G, service providers have a strong desire to significantly reduce the capital expenditures (CAPEX) and operating expenditures (OPEX) so as to obtain higher capital return and broaden the profit margin.

Recently, the concept of network functions virtualization (NFV) has gained a lot of interest from cellular service providers, telecom equipment vendors, IT companies, as well as research institutes. The basic idea of NFV is to take advantage of virtualization technology to decouple various network functions (e.g., routing, switching, packet inspection) from underlying dedicated hardware devices, and to realize the network functions via software-based applications in virtual machines running on commercial off-the-shelf (COTS) equipment. After transferring the cellular network functions from expensive specialized hardware appliances to standard high-volume IT platforms, the cellular network can gradually be relieved of the current heavy reliance on underlying proprietary hardware devices. Thus, service providers can significantly reduce their CAPEX and OPEX; meanwhile, consumers can also enjoy even faster application of new communication techniques and release of new services.

For mobile broadband networks, the deployment of NFV mainly refers to virtualizing the base station (or eNodeB in Long Term Evolution, LTE) and core network. In light of the functionalities of different stack layers in an eNodeB, there have been several attempts to first implement virtualization in a higher layer, that is, from layer 3 to layer 2 to layer 1 [2]. Besides introducing an NFV framework in the virtual environment for next generation mobile networks, a criterion was proposed for bundling virtualized functions of the Evolved Packet Core in one or multiple adjacent physical devices [3].

Note that the introduction of NFV to mobile broadband networks will not only change the network stack design but also impact network

Jiajia Liu and Zhongyuan Jiang are with Xidian University.

Nei Kato is with Tohoku University.

Osamu Akashi and Atsushi Takahara are with NTT Corporation.

1536-1284/16/$25.00 © 2016 IEEE

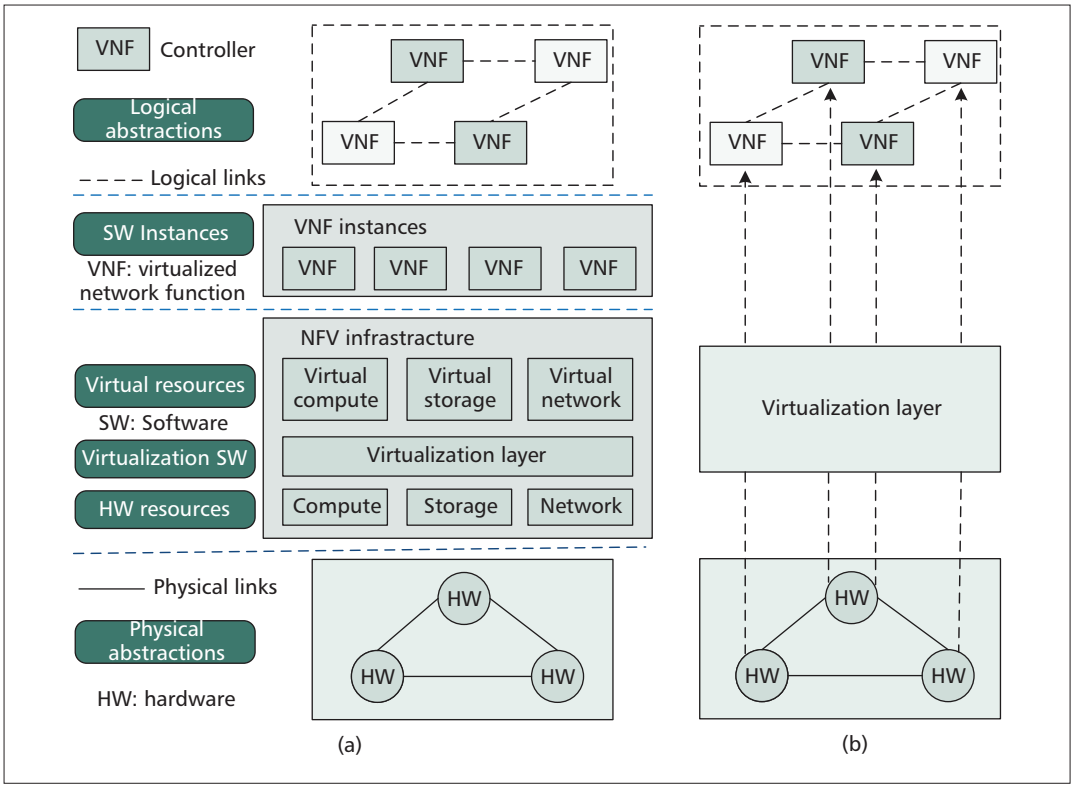

Figure 1. a) Components of NFV architecture. The underlying infrastructures are composed of hardware appliances connected with physical links. The hardware resources are virtualized into virtual resources which can be utilized by the virtualized network functions; b) an abstract illustration of the NFV architecture. The physical layer and logical layers are strongly interdependent. The NFV architecture may be vulnerable against natural disasters and security attacks.

operation and maintenance. In particular, given the deployment of NFV, the virtualized network functions (VNFs) and the physical hardware resources (for computing, network, and storage) are still vulnerable to natural disasters and malicious attacks. How much improvement in network resilience can be achieved by deploying NFV into mobile broadband networks, how to evaluate the network robustness, flexibility, and scalability, and how to optimize the virtualized network functions remain meaningful but unsolved.

Toward this end, we present in this article the first framework for reliability evaluation of NFV deployment, and then propose four algorithms to find out the minimum number of physical and logical nodes the malfunction (or removal) of which will lead to the total failure of an NFV deployment. The evaluation framework as well as the proposed algorithms can help network designers to efficiently evaluate the NFV robustness.

NFV Architecture for Reliability Evaluation

Recently, NFV technology has been proposed to build an innovative platform that transfers network functions from dedicated hardware appliances to software-based applications and decouples network functions from proprietary hardware without affecting functionality [4–8].

As shown in Fig. 1a, in the NFV architecture, the physical appliances or hardware equipment are the standard IT platforms such as high-volume servers, switches, and storage, which are managed by the software controller. The controller runs as a virtual machine monitor, manages all the hardware resources, and provides a virtual environment for the virtual appliances in the logical layer.

A *virtualized network function* is defined as an implementation of an executable software program that is responsible for handling all or a part of a specific network function (a functional building block having well defined external interfaces and functional behavior). An individual VNF can run in one or more virtual machines, and can be deployed in a chained or combined manner to deliver full-scale networking and communication services. Examples of VNFs include switching (e.g., broadband network gateway, routers), mobile network nodes (e.g., mobility management entity, serving gateway), traffic analysis (e.g., deep packet inspection, DPI), signaling (e.g., session border controller), security functions (e.g., firewalls, intrusion detection systems), network-wide functions (e.g., policy control), and application-level optimization (e.g., load balancers) [2].

In reality, physical appliances or hardware platforms must be connected and can send or receive information to or from others, thus forming a network. Accordingly, VNFs can also communicate with each other, forming a logical network. Therefore, the basic components of the NFV architecture can be abstracted into three layers and are described as in Fig. 1b, mainly including:

In reality, physical appliances or hardware platforms must be connected and can send or receive information to or from others, namely forming a network. Accordingly, VNFs can also communicate with each other, forming a logical network. Therefore, the basic components of the NFV architecture can be abstracted into three layers.

Logical links are initialized and managed independently from the physical link connections by the logical controllers for certain purpose. In the physical layer, the physical nodes are hardware appliances on which all VNFs run, and physical links are actual communication medium including wired ones and wireless ones.

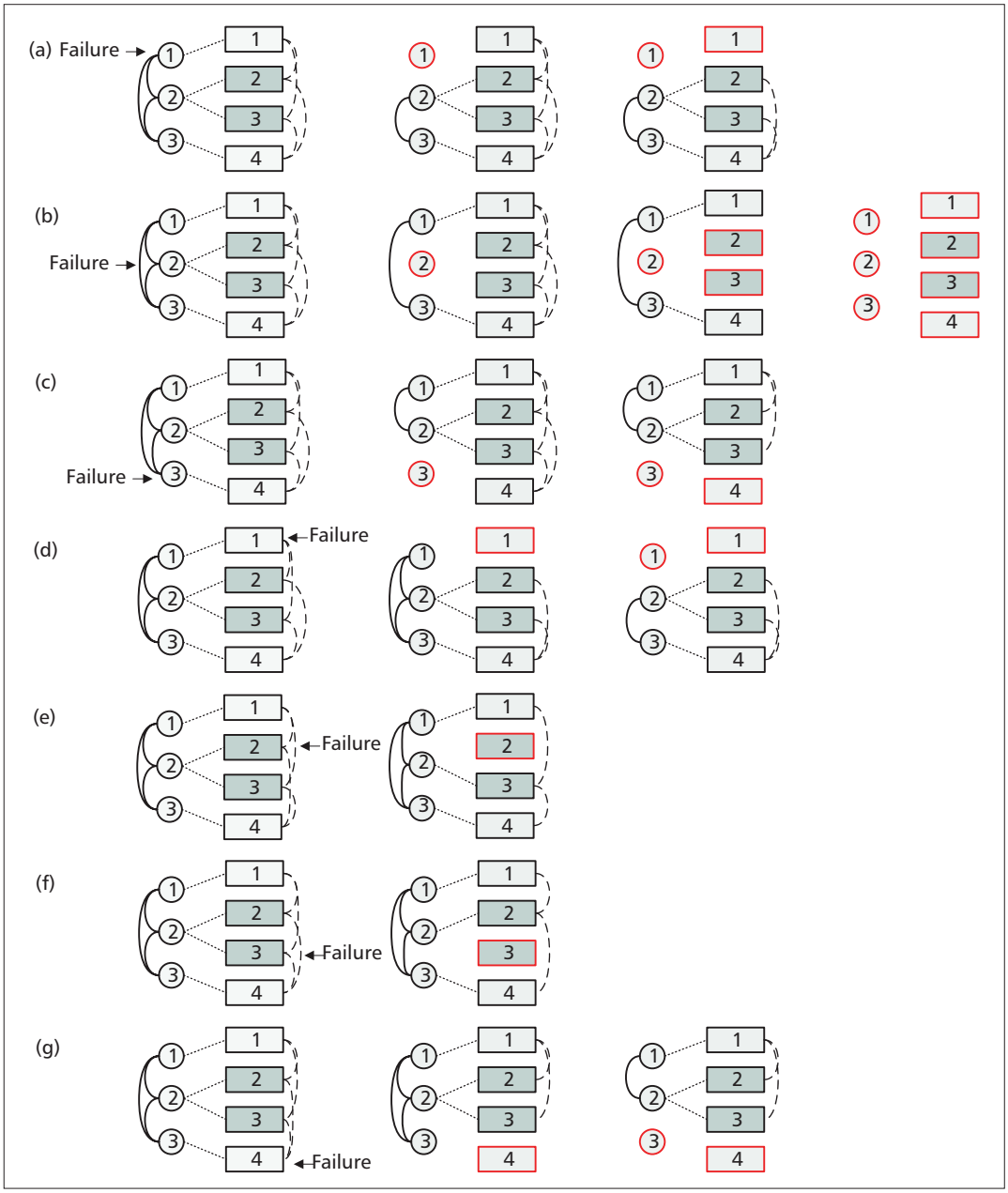

Figure 2. Illustration of cascade failure on NFV architecture, where a single node failure may result in large-scale network collapse. If we denote by P and L the set of failed nodes in the physical layer and logical layer, respectively, we have: a) for the single failure of node 1 in the physical layer, $P = \{1\}$, $L = \{1\}$; b) for the single failure of node 2 in the physical layer, $P = \{1,2,3\}$, $L = \{1,2,3,4\}$; c) for the single failure of node 3 in the physical layer, $P = \{3\}$, $L = \{4\}$; d) for the single failure of node 1 in the logical layer, $P = \{1\}$, $L = \{1\}$; e) for the single failure of node 2 in the logical layer, $P = \{\ \}$, $L = \{2\}$; f) for the single failure of node 3 in the logical layer, $P = \{\ \}$, $L = \{3\}$; g) for the single failure of node 4 in the logical layer, $P = \{3\}$, $L = \{4\}$.

- Physical layer: Composed of physical nodes or hardware infrastructures, and links between physical node
- Logical layer: Composed of virtual nodes or VNFs, and links between virtual nodes
- Virtualization layer: Composed of virtual machine monitor (or controller), providing access to VNFs and managing physical resources.

The network resources and the initialization of virtual machines are managed by the controllers through the visualization layer. Multiple controllers can/must coexist for resilient functions of the network. In the logical layer, the basic elements are VNFs, and a fraction of nodes are called controllers, as shown in Fig. 1. Logical links are initialized and managed independent of the physical link connections by the logical controllers for certain purposes. In the physical layer, the physical nodes are hardware appliances on which all VNFs run, and physical links are actual communication media, including wired and wireless ones.

The physical node on which a controller relies can forward control information to other nodes in the physical layer. We call this architecture

the *multiple controllers NFV model (MCNM)*. To ensure normal operation of MCNM, many disciplines must be obeyed:

- A logical node must be connected to and controlled by at least one controller. Otherwise, it fails.
- Similarly, nodes on the physical layer must be able to communicate with at least one controller. Otherwise, it fails.
- If no VNF runs on a physical node, the physical node shuts down. If a physical node disconnects from all controllers (i.e., is out of control of the controllers), the state of the appliance is unpredictable and cannot be employed anymore.
- Multiple virtual machines can share available resources and run simultaneously on a single physical device.
- The logical route path must rely on the physical structure. A logical link may correspond to a physical route on the physical layer.

A very important function of the virtualization layer is the mapping relations between the physical layer and the logical layer. Physical nodes provide hardware appliances for logical nodes. Resources on a physical node can serve multiple logical nodes.

It is noticed that one key feature of network systems with NFV architecture is the dependency relation among the physical nodes, virtual nodes, and controllers. Consequently, redundant topology design is desired to maintain the system robustness and reliability. In light of this point, it is of essential importance for network designers to conduct proactive evaluation for network reliability and survivability against network failures. Also, proactive reliability study can help to identify the most important set of links and physical/virtual nodes the failure of which may result in total failure of the whole network system, and accordingly to initiate proper protection activities.

Compared to traditional networks, which consist of service nodes running network functions on dedicated hardware appliances, network systems with NFV architecture, although able to reduce CAPEX and OPEX, may have much more complicated topology for connecting the physical nodes, virtual nodes, and controllers. On the other hand, traditional networks have relatively simpler topology design. Therefore, there is a clear trade-off between network cost and topology design, and network designers should determine the network architecture based on a comprehensive evaluation of network cost, topology design, as well as other issues.

Minimum Total Failure Removals Problem and Solutions for NFV Deployment

As discussed in [3], a critical security issue in NFV architecture is network reliability. A network architecture with strong robustness is always preferable. However, a lot of failure events and security attacks occur frequently in real networks. For instance, when a single node or link fails, which may be caused by random failures, intentional attacks, software malfunction, or disasters such as earthquakes, hurricanes, and volcano eruptions, it may subsequently trigger a series of network failures, which is the *cascade phenomenon* [9–11] that may bring catastrophic disasters or huge economic loss.

As shown in Fig. 1b, although the connection topology of the physical layer might be different from that of the logical layer in the NFV architecture, they are strongly interdependent on each other. Therefore, a node failure in either layer may cause substantial node failures subsequently in both layers. For each network topology in Fig. 2, the right part denotes the logical layer, which is the upper one in Fig. 1b, and the left part is the physical layer. Lines among the two parts denote the mapping relations in the virtualization layer of Fig. 1b.

We are ready to discuss the cascade phenomenon in NFV architecture. In Fig. 2, the affected scale of each single node failure is illustrated. For instance, if node 2 in the physical layer of Fig. 2b fails, all the physical links to node 2 fail. As node 2 in the physical layer is the hardware appliance for VNFs 2 and 3 in the logical layer, VNFs 2 and 3 now have no available resource to use and subsequently fail. Then VNFs 1 and 4 in the logical layer disconnect from the controllers (VNFs 2 and 3) and break down. Afterward, nodes 1 and 3 in the physical layer cannot communicate with any controller and fail as well. So far, all nodes in both layers fail, which is a complete collapse, regarded as a catastrophic disaster in real systems. We call such phenomena in which all nodes in the network cannot operate normally *total failures* [11].

Definition 1: Total Failures

As deduced by some unexpected failures or security attacks, nodes in the NFV architecture are all out of state and cannot operate normally.

Considering the catastrophic effects of total failures on NFV architecture, a very critical problem about reliability evaluation of NFV is to determine the most important set of physical/logical nodes, described as follows.

Minimum Total Failure Removal (MTFR) Problem: It is the minimum number of nodes the removal of which will lead to the total failure of an NFV architecture. The node set can be used to evaluate the robustness or reliability of NFV deployment.

Hereafter, we present four schemes to solve the MTFR problem for a given NFV deployment. In order to simplify the algorithm presentation, we denote the physical topology as G_p, logical topology as G_l, and mapping relations as G_m. These symbols are widely used in the following algorithms.

Scheme 1: Based on the given NFV structure, one can easily determine the set of failed nodes S_i deduced by initial failure of a single node i. If the union of many or all of these sets can cover all nodes in both the physical and logical layers, such sets can be employed to evaluate the MTFR. Therefore, the MTFR problem can be transferred to the *Set Cover Problem*, which is NP-Hard, and the greedy algorithm [12] can be employed to achieve a near optimal solution for the set cover problem. The details are described in Algorithm 1.

Although the connection topology of physical layer might be different from that of the logical layer in the NFV architecture, they are strongly interdependent with each other. Therefore, a node failure in either layer may cause substantial node failures subsequently in both the logical and physical layers.

Until all nodes in the network fail, the greedy search process stops. This greedy algorithm takes advantage of the dynamic information in the propagation of cascades, and can greedily select the most influential node at each step. The results will be intuitively better than that of the set cover scheme.

For Algorithm 1, the computational complexity of calculating each S_i at step 1 is $O(n)$, where n is the total number of nodes; at step 2, the computational complexity of the greedy algorithm [12] for set cover is $O(n\log n)$. Therefore, we can determine the computational complexity of Algorithm 1 as $O(n^2 + n\log n)$.

Note that the propagation of cascading failure is a dynamic process, while the above set cover scheme considers only the initial information. Thus, the output of Algorithm 1 can be regarded as a loose result for MTFR, and it is far from the optimum solution.

Scheme 2: In order to address the dynamic propagation of cascades and also to achieve less computing time, here we present a heuristic greedy algorithm, described in Algorithm 2.

As discussed above, it is of computational complexity $O(n^2)$ to calculate the failure scales of all surviving nodes at steps 1 and 2 of Algorithm 2. Note that in the worst case, it takes n iterations until total failure. Therefore, the computational complexity of Algorithm 2 is $O(n^3)$.

The above greedy algorithm finds the most influential node per step from the surviving network components after the dynamic propagation of cascades. When the subsequent failures deduced by the selected node stop, the algorithm goes on to select the next node that might deduce the maximum failure scale in the surviving network. When all nodes in the network fail, the greedy search process stops. This greedy algorithm takes advantage of the dynamic information in the propagation of cascades, and can greedily select the most influential node at each step. The results will be intuitively better than that of the set cover scheme.

Scheme 3: In order to provide a benchmark for performance comparison of the proposed schemes, we present here the optimum algorithm by adopting time-consuming exhaustive search, especially for large-scale networks.

Note that in order to find the optimum sequence with the minimum number of nodes, Algorithm 3 may enumerate all kinds of node sequences that result in total failure of the considered network. If we denote by N_c the number of controllers in the network, one can see that the optimum sequence has at most N_c nodes since the failure of all controllers can result in total failures. Considering the fact that there are $n + 1 - i$ choices for selecting the ith node in the sequence, we can determine the computational complexity of Algorithm 3 as $O(n^{N_c})$.

A common feature of Algorithms 1, 2, and 3 is that they need to consider the failure scale of all nodes, while under certain circumstances, the network structure information might not be available.

Scheme 4: For simplicity, we present a ran-

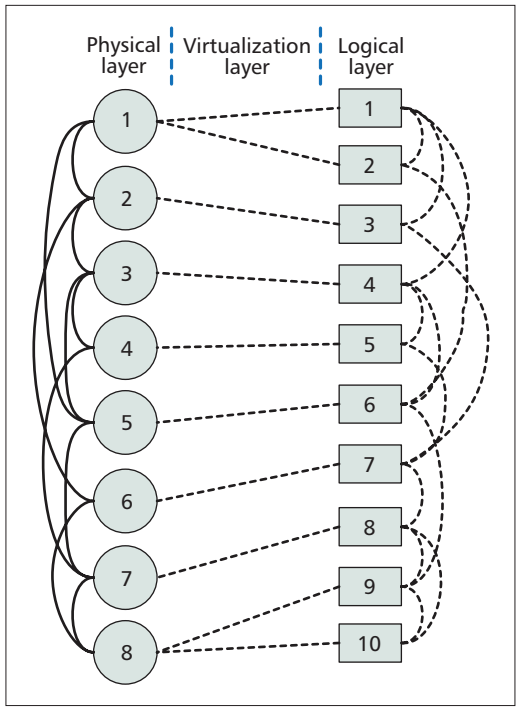

Figure 3. The network model for simulations. The physical layer is composed of 8 nodes, and the logical layer is composed of 10 logical nodes.

Input: G_p, G_l and G_m;
Output: A sequence of nodes for MTFR.
1. Calculate S_i for each node i, and construct $S = \{S_1, S_2, \ldots, S_i, \ldots\}$.
2. Employ the greedy algorithm [12] to find the set cover result for S.

Algorithm 1. Set cover algorithm.

Input: G_p, G_l and G_m;
Output: A greedy result for MTFR.
1. Calculate the set of all failed nodes S_i deduced by any single active node i in the surviving network components.
2. Choose the node with maximum failure scale S_i as the next failed node, disconnect the adjacent links, and propagate the subse quently deduced failures.
3. If all nodes in the network fail, the algorithm stops. Otherwise, go to step 1.

Algorithm 2. Heuristic greedy algorithm.

Input: G_p, G_l and G_m;
Output: Optimum result for MTFR.
1. Enumerate all possible node failure sequences which result in whole collapse of the NFV architecture.
2. Find the sequence with the minimum number of nodes.

Algorithm 3. The optimum algorithm.

Input: G_p, G_l and G_m;
Output: A random result for MTFR.
1. Randomly choose a node in the surviving components, disconnect the adjacent links, and propagate the subsequently deduced failures.
2. If all nodes in the network fail, this algorithm stops. Otherwise, go to step 1.

Algorithm 4. Random removal algorithm.

dom removal algorithm in which each node is randomly selected. Since nodes are randomly selected in the random removal algorithm, its computational complexity is $O(n)$.

Numerical Results

Without loss of generality, we consider a random network model as the basic NFV architecture for simulation study, as shown in Fig. 3. Each physical node is labeled with a number ranging from 1 to 8, and the logical layer is composed of 10 logical nodes labeled from 1 to 10. We employ one-to-one and one-to-many mapping in which a physical node maps to at least one logical node. The topology of the logical layer might be built on the physical layer according to different rules or network function requirements. The selection of logical controllers on the logical layer is random, and the number of controllers is denoted as N_c. In our simulation study, we enumerate all possible selections for each setting of N_c, and the results are averaged over all cases.

Figure 4 illustrates the relationship between MTFR and the value of N_c. One can easily observe from Fig. 4 that our heuristic greedy algorithm can achieve an MTFR very close to the optimum one. Furthermore, the simple random removal algorithm appears to be less efficient than the greedy algorithm but better than the set cover algorithm. A further careful observation of Fig. 4 shows that although the MTFR reported by each algorithm almost monotonically increases with N_c, the performance gap among them decreases as N_c increases. Therefore, we can see that the NFV architecture is more robust with more controllers at the expense of bringing complicated management issue to network service providers.

We further conducted extensive simulations to evaluate the time consumption of all proposed algorithms on a PC with double 3.20 GHZ CPUs, 4.00 GB RAM, and Windows 7 OS, and summarized the numerical results in Fig. 5. One can observe from Fig. 5 that the time consumption of the optimum algorithm increases sharply with the number of controllers N_c. Furthermore, Fig. 5 indicates that for all the proposed algorithms, the simulation results of time consumption match nicely with the analysis of computational complexity above.

Combining Figs. 4 and 5, one can see that the minimum MTFR achieved by the optimum algorithm comes at the cost of extremely long computation time; the simple random removal algorithm has the lowest computation complexity while being able to report a better MTFR than the set cover algorithm. Furthermore, the proposed greedy algorithm is able to achieve an efficient trade-off between MTFR and computation time by reporting a sub-optimal MTFR but taking much less computation time than the optimum algorithm.

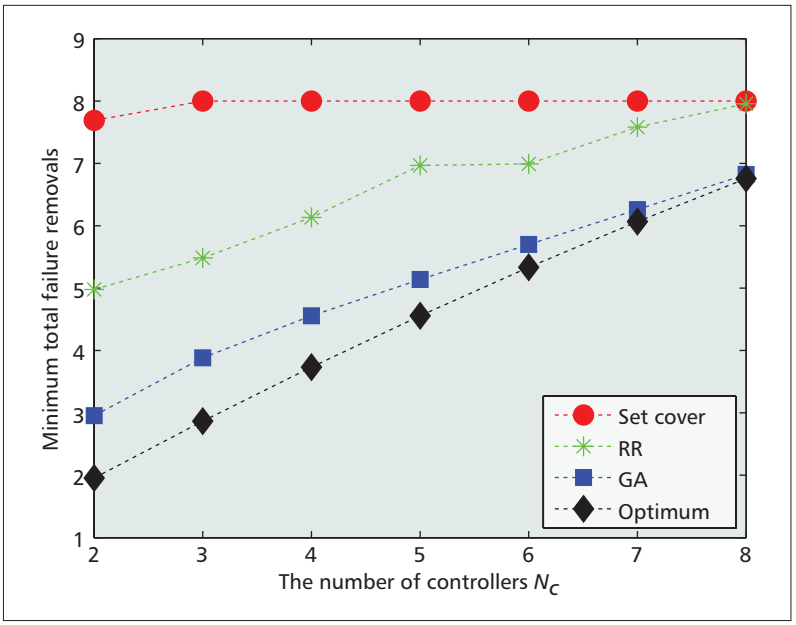

Figure 4. The simulation results of MTFR for the NFV model. Our greedy algorithm (GA) appears to be more efficient. RR: random removal.

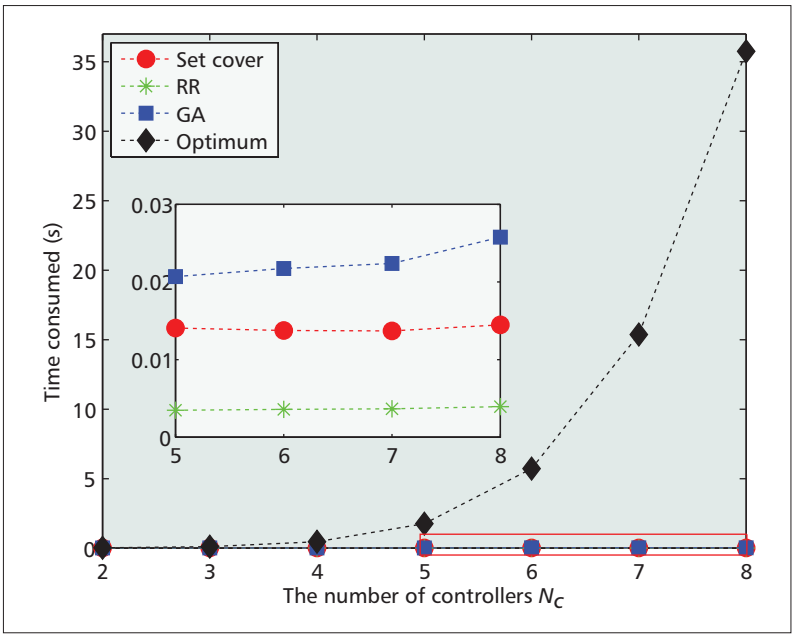

Figure 5. The simulation results of time consumption for all proposed algorithms.

Conclusions

We have presented an analytics framework for reliability evaluation of NFV deployment, as well as four algorithms to solve the important MTFR problem. As a first step, this work mainly aims to explore the NFV architecture reliability against cascading failures. Our heuristic greedy method considers the specific environment and dynamic propagation process of cascades, and gives a very good solution with low time consumption and near optimum results. The results may be useful for understanding the robustness of NFV, and inspire more research interest in NFV deployment in the future.

References

[1] S. Sun, H.-H. Chen, and W. Meng, "A Survey on Complementary-Coded MIMO CDMA Wireless Communications," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 1, 2015, pp. 52–69.

[2] ETSI, "Network Function Virtualization: Use Cases," 2013; http://www.etsi.org/deliver/etsigs/NFV/ 001099/001/01.01.0160/ gsNFV001v010101p.pdf

[3] H. Hawilo *et al*., "NFV: State of the Art, Challenges, and Implementation in Next Generation Mobile Networks (vEPC)," *IEEE Network*, vol. 28, no. 6, 2014, pp. 18–26.
[4] M. Chiosi *et al*., "Network Functions Virtualisation—Introductory White Paper," *Proc. SDN and OpenFlow World Congress*, 2012.
[5] ETSI, "Network Functions Virtualisation (NFV): Architectural Framework," 2013.
[6] J. Matias *et al*., "Toward an SDN-Enabled NFV Architecture," *IEEE Commun. Mag*., vol. 53, no. 4, 2015, pp. 187–93.
[7] P. Veitch, M. J. McGrath, and V. Bayon, "An Instrumentation and Analytics Framework for Optimal and Robust NFV Deployment," *IEEE Commun. Mag*., vol. 53, no. 2, 2015, pp. 126–33.
[8] M. Scholler *et al*., "Resilient Deployment of Virtual Network Functions," *Proc. 5th Int'l. Congress on Ultra Modern Telecommunications and Control Systems and Wksps.*, 2013, pp. 208–14.
[9] S. V. Buldyrev *et al*., "Catastrophic Cascade of Failures in Interdependent Networks," *Nature*, vol. 464, no. 7291, 2010, pp. 1025–28.
[10] C. D. Brummitt, R. M. DSouza, and E. Leicht, "Suppressing Cascades of Load in Interdependent Networks," *Proc. Nat'l. Academy of Sciences*, vol. 109, no. 12, 2012, pp. E680–89.
[11] M. Parandehgheibi and E. Modiano, "Robustness of Interdependent Networks: The Case of Communication Networks and the Power Grid," *Proc. IEEE GLOBECOM*, 2013, pp. 2164–69.
[12] V. Chvatal, "A Greedy Heuristic for the Set-Covering Problem," *Mathematics of Operations Research*, vol. 4, no. 3, 1979, pp. 23–35.

Biographies

Jiajia Liu [S'11, M'12, SM'15] is currently a full professor at the School of Cyber Engineering in Xidian University. He was a recipient of the Chinese Government Award for Outstanding Ph.D. Students Abroad in 2011, and the Tohoku University RIEC Student Award and the Tohoku University Professor Genkuro Fujino Award in 2012. He also received the Yasujiro Niwa Outstanding Paper Award in 2012, and the Best Paper Award of IEEE WCNC 2012 and 2014. He was also the awardee of the prestigious Dean Award and President Award of Tohoku University in 2013.

Zhongyuan Jiang is a lecturer in the School of Cyber Engineering at Xidian University. He got his B.S. and Ph.D. degrees from Beijing Jiaotong University in 2009 and 2013, respectively. His research interests include computer networks and complex networks.

Nei Kato [A'03, M'04, SM'05, F'13] is a professor with the Graduate School of Information Sciences, Tohoku University. He currently serves as a Member-at-Large on the Board of Governors, IEEE Communications Society, Chair of the IEEE Ad Hoc & Sensor Networks Technical Committee, Chair of the IEEE ComSoc Sendai Chapter, Editor-in-Chief of *IEEE Network*, Associate Editor-in-Chief of the *IEEE Internet of Things Journal*, and an Area Editor of *IEEE Transactions on Vehicular Technology*. He is the director of the Research Organization of Electrical Communication, Tohoku University, and strategic adviser to the President of Tohoku University. He is a Distinguished Lecturer of the IEEE Communications and Vehicular Technology Societies. He is a Fellow of IEICE.

Osamu Akashi is a senior research scientist in the Network Innovation Laboratories at NTT. He received his B.Sc. and M.Sc. degrees in information science from Tokyo Institute of Technology in 1987 and 1989, respectively. He also received his Ph.D. degree in mathematical and computing sciences from Tokyo Institute of Technology in 2001. His research interests are in distributed systems, network management, and network architecture. He is a member of ACM, IEICE, IPSJ, and JSSST.

Atsushi Takahara received his B.S., M.S., and Dr.Eng. degrees from Tokyo Institute of Technology in 1983, 1985, and 1988, respectively. He joined NTT LSI Laboratories in 1988 and has been researching formal methods of VLSI design, reconfigurable architectures, and IP processing. From 2003 to 2008, he was the director of the Service Development & Operations Department, Visual Communications Division, NTT Bizlink Inc to develop and operate an IP-based visual communication service. From 2008 to 2011, he was the executive manager of the Media Innovation Laboratory in NTT Network Innovation Laboratories. From 2011 to 2015, he was the director of NTT Network Innovation Laboratories. Since 2015, he is senior vice president, Sales and Marketing Group, NTT Electronics Corporation. His current research interests are in IP networking for real-time communication applications, IP infrastructure technologies, and optical transport technlogies. He is a member of the Association for Computing Machinery, Institute of Electronics, Information and Communication Engineers, and Information Processing Society of Japan.