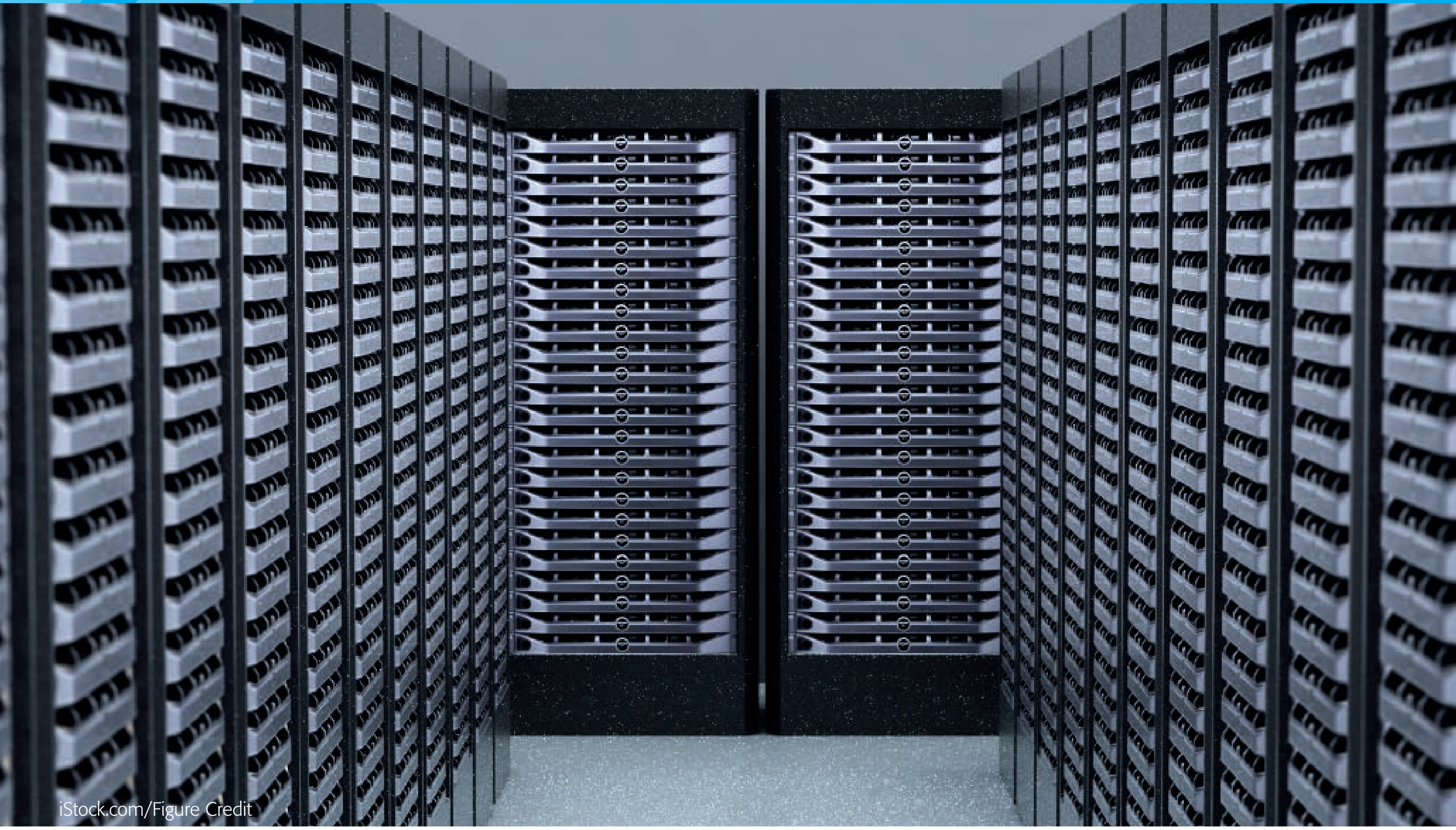
01 May 2016

A Brief Review of Security in Emerging Programmable Computer Networking Technologies

Egemen K. Çetinkaya
Missouri University of Science and Technology, cetinkayae@mst.edu

Recommended Citation

E. K. Çetinkaya, "A Brief Review of Security in Emerging Programmable Computer Networking Technologies," *IEEE Eta Kappa Nu The Bridge Magazine*, vol. 112, no. 2, pp. 27-34, Institute of Electrical and Electronics Engineers (IEEE), May 2016.



iStock.com/Figure Credit

A Brief Review of Security in Emerging Programmable Computer Networking Technologies

Egemen K. Çetinkaya
IEEE Senior Member

Abstract

Recent programmable networking paradigms, such as cloud computing, fog computing, software-defined networks, and network function virtualization gain significant traction in industry and academia. While these newly developed networking technologies open a pathway to new architectures and enable a faster innovation cycle, there exist many problems in this area. In this article, we provide a review of these programmable networking architectures for comparison. Second, we provide a survey of security attacks and defense mechanisms in these emerging programmable networking technologies.

Keywords—Cloud Computing, Fog Computing, Software-Defined Network, SDN, Network Function Virtualization, NFV, Virtualization, Security, Resilience

I. Introduction and Motivation

Communication networks in general, and the Internet in particular, have become an essential part of society. The evolution of networks continues as the technologies progress; on the other hand, the complexity of operations, protocols, and interdependencies makes our understanding of networks formidable. While the open nature of the Internet enables its growth and innovation, this openness also has become an obstacle for its flexibility and management. In the past two decades, research efforts have aimed to design and develop *programmable networks* to overcome this *ossification* in network management. Programmable networks allow customization of networks thus leading to faster service creation and granular network management.

In recent years, we have seen an explosion in network technology (however, we note that the fundamentals of these technological progresses can be rooted back to 1960s [1]–[3]). Notable networking technology progress has been in Cloud Computing (CC), Fog Computing (FC), Software-Defined Networks (SDNs), and Network Function Virtualization (NFV). These emerging network paradigms are becoming more widespread. For example, cloud-based applications such as Google Docs, Apple iCloud, Amazon Cloud Drive, Microsoft OneDrive, and Dropbox are becoming pervasive in our daily lives. Moreover, among the many emerging paradigms that use these new networking technologies are: Internet of Things (IoT) [4], big data analytics [5], connected vehicles [6], and intelligent environments such as smart city [7] and smart grid [8]. Additionally, these emerging networking concepts (in particular OpenFlow-enabled SDNs) are widely accepted by major service providers, data center networks, and network equipment vendors [1], [9]–[11]. It is noted that in 2016, the SDN market will worth $3.7 billion and will reach $15.6 billion in 2018 [10]. The North American SDN market is projected to increase with a Compound Annual Growth Rate of 25% between 2014 and 2019 [12].

As communication networks became a critical infrastructure and ubiquitous utility offering a variety of services and applications, communication networks also become an obvious target for intelligent adversaries with economical, political, or recreational objectives. Resilience, which is defined as providing an acceptable level of service in the face of attacks and challenges [13], has become an important objective to achieve for all players including: end users, equipment providers, service providers, governments, and researchers. The two main resilience disciplines include *trustworthiness,* which specifies measurable properties of network resilience and *challenge tolerance,* which addresses varying classes of challenges to the network [13]. Security is also a resilience discipline, and it is an important attribute of the emerging programmable networking technologies such as CC, FC, SDN, and NFV.

In this brief survey paper we have two modest objectives: i) to provide a brief overview of the emerging programmable networking architectures; ii) to briefly survey of security attacks and defense mechanisms in cloud computing, fog computing, SDN, and NFV. We note that there are extensive surveys of cloud security [14], [15] and SDN security [9], [11]. We did not find comprehensive surveys relating to fog computing and NFV security since they are relatively recent topics being investigated. We also keep our presentation to the work published within the last five years and include related industry - organization publications in addition to the academic papers in our survey.

II. Overview of Emerging Technologies

Virtualization is the core of the emerging programmable network technologies, which aims for efficient utilization of shared physical resources. The history of virtualization goes back to early 1960s with the IBM time-sharing machines (i.e., virtual operating systems). While the virtual memory concept was developed in the 1970s, VLAN (Virtual Local Area Network) development was in the 1980s. While these new programmable network paradigms, CC, FC, SDN, NFV, relate to each other, they do not depend on each other but rather complement one another [1], [2]. These emerging technologies are summarized in Table I and explained in the rest of this section.

A. Cloud Computing Architecture

Cloud computing has a service-oriented architecture, as shown in Figure 1. In this architecture, the resources (i.e., processing, storage, bandwidth, infrastructure) are controlled to offer different services to customers [2], [16]–[18]. The services can be IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service), SaaS (Software-as-a-Service), DaaS (Data-as-a-Service), SecaaS (Security-as-a-Service), XaaS (Anything-as-a-Service), etc. The control functions include cloud operating system, orchestration, and optimization.

TABLE I. Summary of Emerging Technologies

Technology	Acronym	Important feature
Cloud Computing	CC	Service-oriented architecture at the core
Fog Computing	FC	Computing at the edge
Software-Defined Networking	SDN	Separates data and control planes
Network Function Virtualization	NFV	Utilizes COTS hardware to implement network functions

B. Fog Computing Architecture

Fog computing (named to mean that resources are closer to end users (ground)), is a virtualized platform and an extension of cloud computing for applications such as IoT, data analytics, Smart X, connected vehicles [19]. Some of the main characteristics of location-aware fog platforms are low latency and mobility support for applications and services. The new fog computing paradigm has an hierarchical architecture (shown in Figure 2) in which at the bottom are end users, at the edge are the fog devices, and at the core is the cloud [20], [21]. This hierarchical model is similar to the Internet's hierarchical model in which at the top is the core layer, in the middle is the distribution layer, and at the bottom is the access layer.

C. SDN Architecture

The concept of programmable networks is not new, but recent efforts have focused on Software-Defined Networks (SDNs), a concept that evolved from early ideas of programmable networks [1], [3]. The simplified architecture of the SDN (Software-Defined Network) is shown in Figure 3. The two main ideas of SDNs are: 1) to decouple the control and data planes, 2) to consolidate the control plane (i.e., logically) such that it controls multiple data-plane elements. Decoupling of control and data planes can be accomplished via an API (Application Programming Interface) such as OpenFlow [1]. A northbound API such as OpenDaylight provides the interface between control and application planes. An example of a joint SDN and cloud network operation is

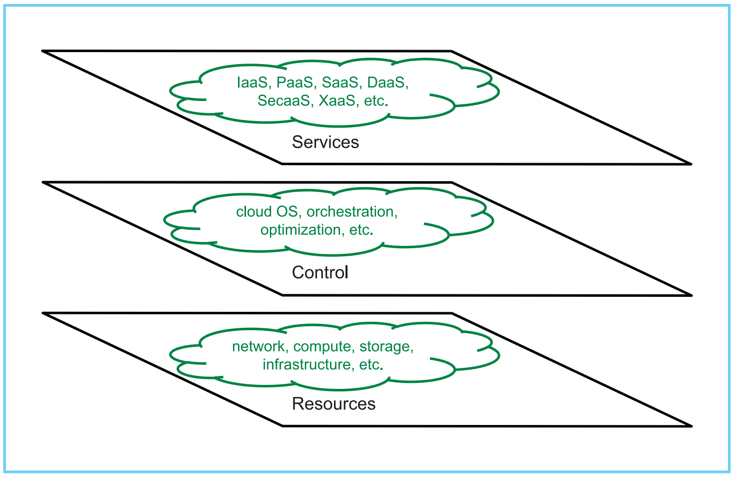


Fig. 1. Cloud computing architecture

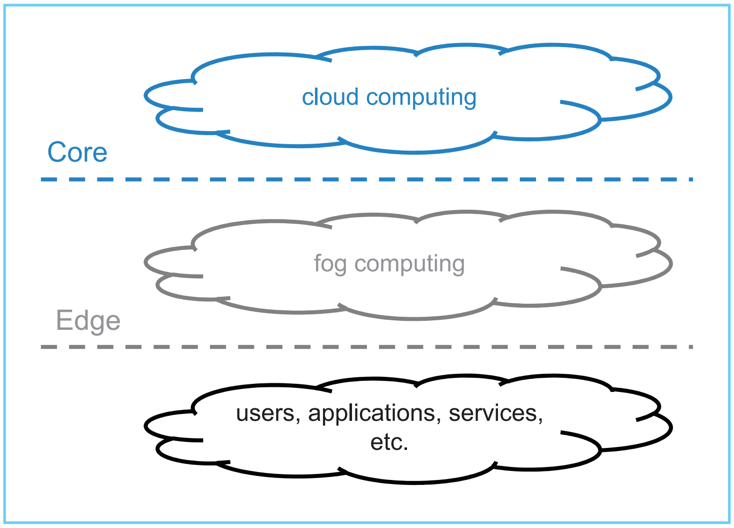


Fig. 2. Fog computing architecture

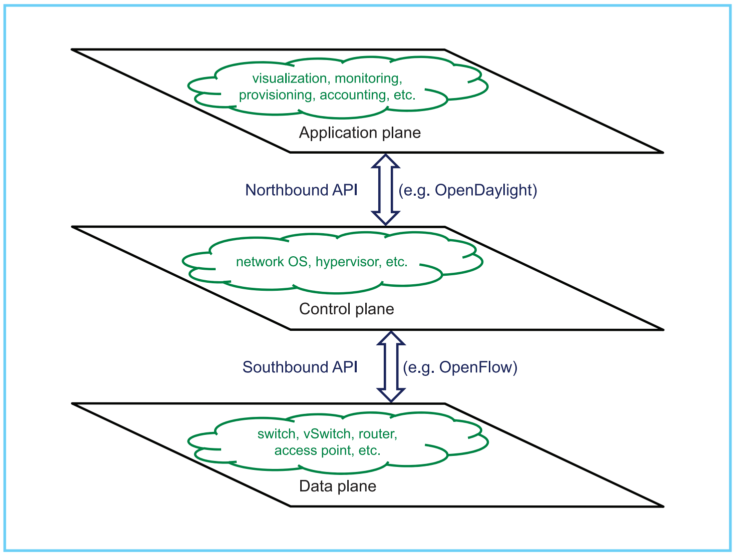


Fig. 3. SDN architecture

using SDN to traffic engineer an application hosted on the cloud network [18].

D. NFV Architecture

NFV (Network Function Virtualization) aims to virtualize network functions necessary for serving customers using shared physical resources that are implemented on COTS (commercial off-the-shelf) hardware. With the current trends, i.e., reduced ARPU (Average Revenue Per User), increased CAPEX (Capital Expenditures), and OPEX (Operational Expenditures), service providers cannot keep up with a silo of network infrastructure that does not provide new service to their customer. Instead, a better alternative would be to provide new (or existing) services using COTS (commercial off-the-shelf) hardware. Moreover, by off-loading functions of ASICs and FPGA hardware to software, this opens a path for development of new business models to the market in a fast and cost-efficient fashion. Consequently, NFV aims to virtualize network functions necessary for serving customers using shared physical resources that are implemented on COTS hardware.

ETSI (European Telecommunications Standards Institute) Network Functions Virtualisation Industry Specification Group (NFV ISG) leads the development and architecting the NFV - related technologies [22]. It is foreseen that NFV will reduce the cost of operating networks as the infrastructure transitions from custom-built hardware to using commercial hardware for compute, storage, and network resources [23]. Moreover, the passage of network functions from hardware to software will open the pathway to new business models and innovation. However, there are some realistic risks to be considered:

1. There are potential risks associated with increased OPEX [23].
2. The performance of shared virtualized network functions will not be same as the dedicated physical resources [24].
3. The value added by transitioning functions from hardware implementations to softwarization in certain application domains (e.g. home network vs. access network) will not be as high [24].

The architectural framework (shown in Figure 4) and design philosophy of virtualized network functions is described by ETSI [25]. In this architecture, the NFV infrastructure layer consists of physical and virtual resources, as well as a virtualization layer that provides partitioning of hardware resources and providing virtual resources to the VNF (Virtual Network Function) layer. The virtualization layer function is similar to a hypervisor or a virtual machine (VM). Example VNFs include network functionalities such as IDS (Intrusion Detection System), IPS (Intrusion Prevention System), FW (Firewall), and load balancer. Orthogonal to the NFV Infrastructure and VNF layers, the management and orchestration layer provides the control and monitoring of the overall VNF lifecycle.

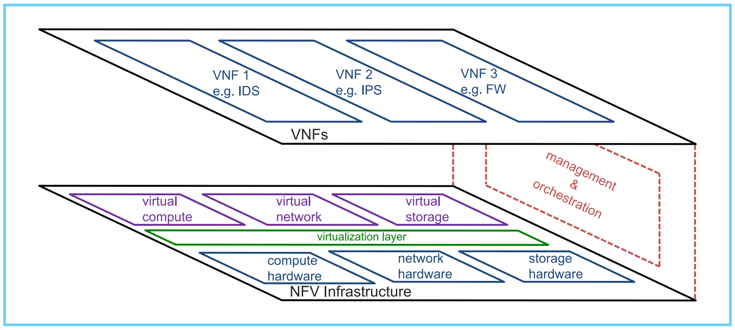


Fig. 4. NFV architecture

III. Network Security

We present security issues and solutions in the cloud computing, fog computing, SDN, and NFV in this section. Virtualization is a fundamental technology that enables existence of these emergent networking technologies. We will not present virtualization security here, but we point the reader to extensive literature surveys [26]–[28].

A. Cloud Computing Security

The Cloud Security Alliance (CSA) guidance document summarizes the best practices for secure cloud operation and governance [29]. It recommends evaluation of the assets (i.e., data or application/function/process) on the different cloud deployment models (i.e., public, private, community, hybrid) under different hosting scenarios (i.e., internal, external, combined). Aside from industry recommendation, there have been extensive surveys of the cloud security in the literature [14], [15], [30]–[32].

Security issues related to three cloud service delivery models (SaaS, PaaS, IaaS) are discussed [30]. Cloud threats, vulnerabilities, and attacks are extensively categorized according to cloud deployment and service delivery models [14], [15]. User-level threats at physical, virtualization, and application layers are detailed alongside security requirements for cloud computing [31]. Authors argue that a combination of PKI (Public Key Infrastructure), SSO (Single Sign-On), and LDAP

(Lightweight Directory Access Protocol) mechanisms can address horizontal security requirements in the cloud computing [31]. Software patching, data isolation across logical resources sharing same physical substrates, SSO for authentication across multiple clouds are additional considerations to secure the cloud computing infrastructure [32]. Furthermore, infrastructure- and process-level diversity is promoted as defensive mechanisms against the attacks due to monoculture (e.g., hardware monoculture, software monoculture) [33].

B. Fog Computing Security

A man-in-the-middle (MiM) attack on a gateway fog device is performed and shown that the MiM attack can be stealthy based on CPU utilization and memory consumption. Further, an authentication scheme is proposed to overcome such MiM attacks, in particular when the connection between fog and cloud is not stable [20]. Several security and privacy issues such as intrusion detection, access control, secure data storage and computation are discussed within the context of fog computing [21].

C. SDN Security

There have been extensive surveys of SDN security published in the recent past [9]–[11], [34], [35]. It is a consensus that there are two ideas in regards to SDN security: 1) there are those who conduct research aiming to secure the programmable network and 2) those who conduct research aiming to provide security as a service [9], [10]. Moreover, an extensive survey of resilience research (i.e., survivability, dependability, disruption tolerance, performability, traffic tolerance, security) in SDNs is presented [34]. Authors conclude based on their survey that security is built in SDNs via (i) as an addition or (ii) as an embedded property in the architecture [34]. Regardless of the school of thought, next, we summarize SDN security research.

In extensive surveys of the SDN security [11], [35], authors present a review of the literature on the past SDN security efforts. Security challenges and solutions in each of the application, control, and data planes of the SDNs are presented in detail. Some of the attacks in each layer include: application plane attacks (e.g., access control for third party applications), control plane attacks (e.g., fraudulent flow rules insertion, DoS attacks, and unauthorized access to the controller), and data plane attacks such as flooding the SDN switch and router components. Authors argue that while SDNs ease the global visibility of network states against challenges and attacks, the logically centralized control plane has also become an attractive target for the attackers [11], [35]. Other surveys review SDN security from a STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of Privilege) perspective [9], [36]. Additionally, a brief survey of wireless SDN and SDN experimentation literature is presented [36]. Recently, we conducted security experiments on the GENI testbed performing DDoS attacks (ICMP echo flood and TCP SYN flood) [37].

Some of the secure mechanisms against attacks in the SDN domain can be listed as: access control providing authorization and authentication, attack detection and filtering, flow aggregation to prevent information disclosure, and rate limiting at the control plane to thwart DDoS attacks [9]. It was noted that most of these defense mechanisms are not implemented. In addition to the defense mechanisms [9], federation of heterogeneous network applications (e.g. IoT, SmartX, connected vehicles) and defining security policies across different domains using SDN will be a future research direction [10].

D. NFV Security

ETSI Network Functions Virtualisation Industry Specification Group (ISG) has published several specifications in regards to NFV security [38]–[42]. Potential threats and players in the security domain are explained in the ETSI Security Problem Statement specification [38]. NFV poses threats due to network protocol vulnerabilities (e.g., flooding attack, routing insecurity), which are not related with virtualization, and due to virtualization (e.g., memory leaks and interrupt isolation) [38]. Furthermore, virtualization can, while mitigating some, incur new security threats [38]. Other specifications discuss OpenStack security [39], trust and its domains [40], lawful intercept points [41], and host application and platform security [42] as they relate to NFV.

In addition to the ETSI ISG specifications, other papers are available in the literature that we summarize next. A DDoS attack mitigation strategy using NFV technology is discussed [43]. In another paper, authors propose an architecture for trust monitoring in SDN and NFV [44]. In this architecture, an out-of-band SDN verifier component is added to SDN architecture to attest the network configuration, hardware identity check, and software trust measurement. They also investigate potential architectures to build the attestation mechanism in virtual hosts executing critical network functions [44]. An extended SDN architecture to prevent intrusions via addition of virtualized packet inspection function is presented [45]. The simulation result of such a virtualized DPI function can improve the network performance (e.g., throughput, overhead) significantly compared to stand-alone OpenFlow-based SDN architecture [45]. An anti-virus (AV) solution was proposed and tested as a virtual network function [46]. It was shown that this AV-NFV solution did not require a proxy compared to the traditional AV solutions and its performance and memory usage was better. A virtual firewall leveraging both SDN and NFV techniques is presented that adapts to changing virtual network characteristics [47]. Intrusion detection is experimented on a testbed as a virtualized network function [48] and further the intrusion detection function is incorporated into service chaining [49]. Some security-related use cases for the NFV environments is presented [50]. In addition to the security aspects of the NFV, placement of network security functions (e.g., packet inspection, firewalls) in the topology is also an active area of research [47], [51].

IV. Conclusions

We are in an exciting era in new networking technology progression. Programmable networks, which provide greater control and management functionality, as well as enabling the pathway to greater innovation lifecycle, are being developed and deployed. Of these recently networking technologies, we observe cloud computing, fog computing, software-defined networks, and network function virtualization are becoming more pervasive for applications. We described the architecture of these different network technologies. We observe that different network architectures show similarities. At the bottom layer is some infrastructure (physical and/or virtual), in the middle is control and management of these infrastructures, and on the top is the delivery of some services/functions/applications. Another common important feature of these networking technologies is that they rely heavily on *virtualization*. Next, we present a survey of the security issues in CC, FC, SDN, and NFV. We observe that while cloud and SDN security literature is becoming rich, fog computing and NFV security is in its infancy. We believe that, regardless of the technologies, all these different emergent programmable networks pave the road to the Future Internet Architectures.

Acknowledgment

We would like to acknowledge members of the CoNetS group for discussions on this work. We thank anonymous reviewers for feedback on an early draft of this paper.

References

[1] N. Feamster, J. Rexford, and E. Zegura, “The Road to SDN: An Intellectual History of Programmable Networks,” *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 2, pp. 87–98, 2014.

[2] R. Jain and S. Paul, “Network Virtualization and Software Defined Networking for Cloud Computing: A Survey,” *IEEE Communications Magazine*, vol. 51, pp. 24–31, November 2013.

[3] D. Medhi, B. Ramamurthy, C. Scoglio, J. P. Rohrer, E. K. Çetinkaya, R. Cherukuri, X. Liu, P. Angu, A. Bavier, C. Buffington, and J. P. Sterbenz, “The GpENI Testbed: Network Infrastructure, Implementation Experience, and Experimentation,” *Computer Networks*, vol. 61, pp. 51–74, March 2014.

[4] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” *Computer Networks*, vol. 76, pp. 146–164, January 2015.

[5] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan, “The rise of ‘big data’ on cloud computing: Review and open research issues,” *Information Systems*, vol. 47, pp. 98–115, January 2015.

[6] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, “A survey on vehicular cloud computing,” *Journal of Network and Computer Applications*, vol. 40, pp. 325–344, April 2014.

[7] H. Schaffers, N. Komninos, M. Pallot, B. Trousse, M. Nilsson, and A. Oliveira, “Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation,” in *The Future Internet*, vol. 6656 of *Lecture Notes in Computer Science*, pp. 431–446, Springer Berlin Heidelberg, 2011.

[8] S. Bera, S. Misra, and J. J. Rodrigues, “Cloud Computing Applications for Smart Grid: A Survey,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1477–1494, 2015.

[9] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-Defined Networking: A Comprehensive Survey,” *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.

[10] S. T. Ali, V. Sivaraman, A. Radford, and S. Jha, “A Survey of Securing Networks Using Software Defined Networking,” *IEEE Transactions on Reliability*, vol. 64, no. 3, pp. 1086–1097, 2015.

[11] S. Scott-Hayward, S. Natarajan, and S. Sezer, “A Survey of Security in Software Defined Networks,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 623–654, 2016.

[12] "North America Software Defined Networking Market, by Solution (SDN Switching, SDN Controllers, Virtual Cloud Application), by End User (Enterprise, Telecommunication Service Providers, Cloud Service Providers), by Geography - Analysis & Forecast to 2019." http://www.micromarketmonitor.com/market/north-america-software-defined-network-sdn-9065162554.html, July 2015.

[13] J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in com- munication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[14] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey," *International Journal of Information Security*, vol. 13, no. 2, pp. 113– 170, 2014.

[15] C. A. Ardagna, R. Asal, E. Damiani, and Q. H. Vu, "From Security to Assurance in the Cloud: A Survey," *ACM Computing Surveys*, vol. 48, no. 1, pp. 2:1–2:50, 2015.

[16] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "NIST Cloud Computing Reference Architecture," (special publication 500-292), National Insitute of Standards and Technology (NIST), Gaithersburg, MD, September 2011.

[17] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50– 58, 2010.

[18] N. Bitar, S. Gringeri, and T. J. Xia, "Technologies and Protocols for Data Center and Cloud Networking," *IEEE Communications Magazine*, vol. 51, no. 9, pp. 24–31, 2013.

[19] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog Computing and Its Role in the Internet of Things," in *Proceedings of the ACM SIGCOMM Mobile Cloud Computing Workshop (MCC)*, (Helsinki), pp. 13–16, August 2012.

[20] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of Fog computing and its security issues," *Concurrency and Computation: Practice and Experience*, 2015.

[21] S. Yi, Z. Qin, and Q. Li, "Security and Privacy Issues of Fog Computing: A Survey," in *Proceedings of the 10th International Conference on Wireless Algorithms, Systems, and Applications (WASA)*, (Qufu, China), pp. 685–695, August 2015.

[22] "ETSI Network Functions Virtualisation Industry Specification Group, NFV ISG." http://www.etsi.org/technologies-clusters/technologies/nfv, 2016.

[23] E. Hernandez-Valencia, S. Izzo, and B. Polonsky, "How Will NFV/SDN Transform Service Provider OpEx?," *IEEE Network Magazine*, vol. 29, no. 3, pp. 60–67, 2015.

[24] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network Function Virtualization: Challenges and Opportunities for Innovations," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 90–97, 2015.

[25] ETSI, "ETSI GS NFV 002: Network Functions Virtualisation (NFV); Architectural Framework," Specification RGS/NFV-002, ETSI, Decem- ber 2014.

[26] M. Pearce, S. Zeadally, and R. Hunt, "Virtualization: Issues, secu- rity threats, and solutions," *ACM Computing Surveys*, vol. 45, no. 2, pp. 17:1–17:39, 2013.

[27] D. Sgandurra and E. Lupu, "Evolution of Attacks, Threat Models, and Solutions for Virtualized Systems," *ACM Computing Surveys*, vol. 48, no. 3, pp. 46:1–46:38, 2016.

[28] G. Pék, L. Buttyán, and B. Bencsáth, "A Survey of Security Issues in Hardware Virtualization," *ACM Computing Surveys*, vol. 45, no. 3, pp. 40:1–40:34, 2013.

[29] P. Simmonds, C. Rezek, and A. Reed, "Security Guidance for Critical Areas of Focus in Cloud Computing," tech. rep., Cloud Security Alliance (CSA), 2011.

[30] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.

[31] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.

[32] J. Moura and D. Hutchison, "Review and analysis of networking challenges in cloud computing," *Journal of Network and Computer Applications*, vol. 60, pp. 113–129, January 2016.

[33] J. P. Sterbenz and P. Kulkarni, "Diverse Infrastructure and Architecture for Datacenter and Cloud Resilience," in *Proceedings of the IEEE International Conference on Computer Communications and Networks (ICCCN)*, (Nassau, Bahamas), pp. 1–7, August 2013. (invited paper).

[34] A. S. da Silva, P. Smith, A. Mauthe, and A. Schaeffer-Filho, "Resilience support in software-defined networking: A survey," *Computer Networks*, vol. 92, Part 1, pp. 189–207, December 2015.

[35] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in Software Defined Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2317–2346, 2015.

[36] I. Alsmadi and D. Xu, "Security of Software Defined Networks: A survey," *Computers & Security*, vol. 53, pp. 79–108, September 2015.

[37] M. C. Gorla, V. M. Kamaraju, and E. K. Çetinkaya, "Network Attack Experimentation using OpenFlow-enabled GENI Testbed (poster)," in *23rd GENI Engineering Conference (GEC 23) Demo and Poster Session*, (Champaign, IL), June 2015.

[38] ETSI, "ETSI GS NFV-SEC 001: Network Functions Virtualisation (NFV); NFV Security; Problem Statement," Specification DGS/NFV- SEC001, ETSI, October 2014.

[39] ETSI, "ETSI GS NFV-SEC 002: Network Functions Virtualisation (NFV); NFV Security; Cataloguing security features in management software," Specification DGS/NFV-SEC002, ETSI, August 2015.

[40] ETSI, “ETSI GS NFV-SEC 003: Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance,” Specification DGS/NFV-SEC003, ETSI, December 2014.

[41] ETSI, “ETSI GS NFV-SEC 004: Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implications,” Specification DGS/NFV-SEC004, ETSI, September 2015.

[42] ETSI, “ETSI GS NFV-SEC 009: Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration,” Specification DGS/NFV-SEC009, ETSI, December 2015.

[43] R. Krishnan, D. Krishnaswamy, and D. McDysan, “Behavioral Security Threat Detection Strategies for Data Center Switches and Routers,” in *Proceedings of the 34th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW)*, (Madrid), pp. 82–87, June 2014.

[44] L. Jacquin, A. Lioy, D. Lopez, A. Shaw, and T. Su, “The Trust Problem in Modern Network Infrastructures,” in *Cyber Security and Privacy* (F. Cleary and M. Felici, eds.), vol. 530 of *Communications in Computer and Information Science*, pp. 116–127, Springer International Publishing, 2015.

[45] Y.-D. Lin, P.-C. Lin, C.-H. Yeh, Y.-C. Wang, and Y.-C. Lai, “An Extended SDN Architecture for Network Function Virtualization with a Case Study on Intrusion Prevention,” *IEEE Network Magazine*, vol. 29, no. 3, pp. 48–53, 2015.

[46] C.-N. Kao, S. SI, N.-F. Huang, I.-J. Liao, R.-T. Liu, and H.-W. Hung, “Fast Proxyless Stream-Based Anti-Virus for Network Function Virtualization,” in *Proceedings of the 1st IEEE Conference on Network Softwarization (NetSoft)*, (London), pp. 1–5, April 2015.

[47] J. Deng, H. Hu, H. Li, Z. Pan, K.-C. Wang, G.-J. Ahn, J. Bi, and Y. Park, “VNGuard: An NFV/SDN Combination Framework for Provisioning and Managing Virtual Firewalls,” in *Proceedings of the IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN)*, (San Francisco, CA), pp. 107–114, November 2015.

[48] P. Yasrebi, S. Monfared, H. Bannazadeh, and A. Leon-Garcia, “Security function virtualization in software defined infrastructure,” in *Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management (IM)*, (Ottawa, ON), pp. 778–781, May 2015.

[49] P. Yasrebi, S. Bemby, H. Bannazadeh, and A. Leon-Garcia, “VNF Service Chaining on SAVI SDI,” in Proceedings of the First EAI International Conference on Future Access Enablers for Ubiquitous and Intelligent Infrastructures (FABULOUS), (Ohrid, Republic of Macedonia), pp. 11–17, September 2015.

[50] H. Jang, J. Jeong, H. Kim, and J.-S. Park, “A Survey on Interfaces to Network Security Functions in Network Virtualization,” in *Proceedings of the 29th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, (Gwangiu, Korea), pp. 160–163, March 2015.

[51] M. Bouet, J. Leguay, T. Combe, and V. Conan, “Cost-based placement of vDPI functions in NFV infrastructures,” *International Journal of Network Management*, vol. 25, no. 6, pp. 490–506, 2015.

Biography

Egemen K. Çetinkaya is an Assistant Professor of Electrical & Computer Engineering at Missouri University of Science and Technology (formerly known as University of Missouri-Rolla). He received his Ph.D. in Electrical Engineering from the University of Kansas in 2013. He received his B.S. degree in Electronics Engineering from Uludağ University (Bursa, Turkey) in 1999 and the M.S. degree in Electrical Engineering from the University of Missouri- Rolla in 2001. He held various positions at Sprint as a support, system, and design engineer from 2001 until 2008. His research interests are in resilient networks. He is a senior member of the IEEE, Communications Society, HKN, a member of ACM SIGCOMM, and Sigma Xi.