J Inf Process Syst, Vol.17, No.4, pp.801~817, August 2021
https://doi.org/10.3745/JIPS.04.0220

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Security in Network Virtualization: A Survey

Seung Hun Jee*, Ji Su Park**, and Jin Gon Shon*

Abstract

Network virtualization technologies have played efficient roles in deploying cloud, Internet of Things (IoT), big data, and 5G network. We have conducted a survey on network virtualization technologies, such as software-defined networking (SDN), network functions virtualization (NFV), and network virtualization overlay (NVO). For each of technologies, we have explained the comprehensive architectures, applied technologies, and the advantages and disadvantages. Furthermore, this paper has provided a summarized view of the latest research works on challenges and solutions of security issues mainly focused on DDoS attack and encryption.

Keywords

Cloud, Network Virtualization, NFV, NVO, SDN, Security

1. Introduction

In the era of the 4th industrial revolution, virtualization technologies play a big role in the acceleration of cloud, Internet of Things (IoT), big data, and 5G network. Virtualization is a new process of creating a virtual instance of a computing system in the abstraction layer over the infrastructure layer. Virtualization can increase agility, scalability, flexibility, and mobility. On the other hand, virtualization can also decrease capital expenditure, operating expense, and complexity. Virtualization is classified into server, storage, and network virtualization. Among these, this paper has focused on network virtualization.

Traditional network device consists of a management plane for monitoring and management, a control plane for configuration and control, and a data plane for forwarding and port. These planes are tightly coupled and integrated into the device. Traditional network architecture is designed as a vertical 3-tier structure, consisting of a core, a distribution, and an access layer. Major traffics such as e-mail and multimedia service flow in the north-south direction, from silo-based servers to the external customers.

The network device has been changed into a loosely coupled structure. A management plane, a control plane, and a data plane are physically separated and communicate through separate interfaces. Each plane becomes virtualized, programmable, and centralized controllable. Network architecture also has been changed into a horizontal 2-tier structure, consisting of a spine and a leaf layer. Major traffics flow in the east-west direction to transport server-to-server traffic for distributed computing and big data.

IoT, cloud, big data, and 5G environments are because of technical advances in the virtualization

Manuscript received January 20, 2020; first revision March 23, 2020; second revision May 12, 2020; accepted July 12, 2020.

Corresponding Author: Jin Gon Shon (jgshon@knou.ac.kr)
* Dept. of Computer Science, Korea National Open University, Seoul, Korea (mayets@knou.ac.kr, jgshon@knou.ac.kr)
** Dept. of Computer Science and Engineering, Jeonju University, Jeonju, Korea (jisupark@jj.ac.kr)

technologies. Network virtualization is the youngest but the most influential technology than others. In this paper, we have provided the comprehensive architectures, applied technologies, security challenges and solutions against DDoS attack, which is mainly focused on software-defined networking (SDN), network functions virtualization (NFV), and network virtualization overlay (NVO). We expect this paper can show you how your network can be deployed to use network virtualization technologies.

2. Network Virtualization

2.1 Quick Review of Networks

Network elements are composed of a set of nodes and links as shown in Fig. 1(a). Network node can be a physical or virtual node as shown in Fig. 1(b), and network link can also be a physical or virtual link as shown in Fig. 1(c). Virtual node is not a physical hardware, but a logical software over the abstraction layer. Virtual link can provide direct connection among nodes that are not physically connected.

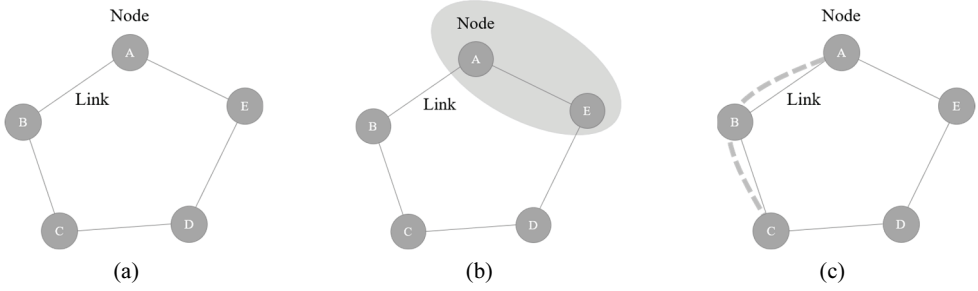

Fig. 1. Network elements (physical nodes and links) and their virtual usages: (a) nodes and links, (b) virtual node (shaded part), and (c) virtual link (dotted line).

Network topology provides a roadmap for one node to know the way to the other node through the link. There are many methods to design network topologies. Here are two famous methods to design network topologies, fat-tree topology and Clos topology. Fat-tree topology is a tree-like, 3-tier's architecture as shown in Fig. 2(a), which is generally used in the traditional network architectures. Clos topology is a 2-tier's architecture as shown in Fig. 2(b), which is widely used in the virtualized or cloud network architectures. In the fat-tree topology described in Fig. 2(a), the hop count from node A to node B is 4, but in the Clos topology described in Fig. 2(b), the hop count from node C to node D is just 2. That is why recent network architectures prefer Clos topology to fat-tree topology [1].

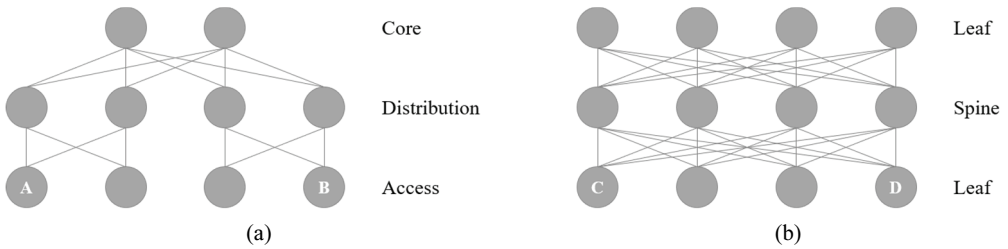

Fig. 2. Fat-tree topology (a) and Clos topology (b).

2.2 Classifications of Network Virtualization

Network virtualization can be classified by network elements into node virtualization and link virtualization. Node virtualization is the separation of software from hardware. Link virtualization is logical extension without physical extension. In this classification, SDN and NFV belong to node virtualization. SDN is mainly to virtualize the control plane, and NFV is mainly to virtualize the data plane. In the meantime, NVO belongs to link virtualization to connect direct network without a physical cable. Table 1 shows a summarization of what we explained above.

Table 1. Classification of network virtualization by network elements

Technology	Network node		Network link	
	Control plane	Data plane	LAN	WAN
SDN	Yes	Yes or No	No	No
NFV	Yes or No	Yes	No	No
NVO	No	No	Yes	Yes

2.3 Summary of Surveys on Network Virtualization

There have been many surveys on network virtualization. Table 2 summarizes research surveys and compares ours with them [2-15]. In the column of "Contributions," we mark some of surveys as (highly) historical when they explain how network virtualization was born, raised and developed from the past. Recent and informational surveys are marked as (highly) recommended when they provide information for the readers to understand the definition, categories, applied technologies, and security issues of network virtualization.

Table 2. Comparison of our survey and the major surveys

Survey	Year	SDN	NFV	NVO	Security	Contributions
Bari et al. [2]	2012	O	X	X	O	Historical, early SDN surveyed
Jain and Paul [3]	2013	O	O	O	△	Highly historical, widely surveyed
Scott-Hayward et al. [4]	2013	O	△	X	O	Highly historical, SDN security focused
Schehlmann et al. [5]	2014	O	X	X	O	Recommended, SDN security focused
Xia et al. [6]	2014	O	△	X	△	Historical, SDN surveyed
Ahmad et al. [7]	2015	O	△	X	O	Highly recommended, SDN security focused
Kreutz et al. [8]	2015	O	O	O	O	Highly recommended, widely surveyed
Yao and Yan [9]	2016	O	X	X	O	Recommended, SDN security focused
Nadeem and Karamat [10]	2016	X	X	O	X	Recommended, recent NVO surveyed
Abdou et al. [11]	2018	O	X	X	O	Recommended, SDN security focused
Yi et al. [12]	2018	△	O	X	O	Highly recommended, NFV security focused
Pattaranantakul et al. [13]	2018	△	O	△	O	Highly recommended, widely surveyed
Alwakeel et al. [14]	2018	△	O	X	O	Recommended, recent NFV security focused
Liu et al. [15]	2019	O	X	X	O	Highly recommended recent SDN security focused
Our survey	2020	O	O	O	O	Probably recommended widely surveyed

3. Software-Defined Networking

In this section, the comprehensive architecture, technologies of SDN, security threats, and research works on SDN security have been explained.

3.1 Architecture of SDN

SDN is a technology to separate control plane and data plane. As shown in Fig. 3, traditional network architecture consists of management plane, control plane, and data plane in one-box hardware. SDN architecture consists of management plane, control plane, and data plane. The separated planes communicate each other through northbound and southbound interface in SDN [16].

SANE architecture [17] proposed in 2006 and Ethane architecture [18] proposed in 2007 are the beginning of SDN history. Ethane controls the network into two components; a centralized controller responsible for enforcing global policy, and ethane switches to simply forward packets based on rules in a flow table. SDN, with its characteristics of separation of control plane from data plane, offers a greater advantage such as automation, centralized management, and network programming. Centralized control plane provides a global network visibility and management of entire network flows.

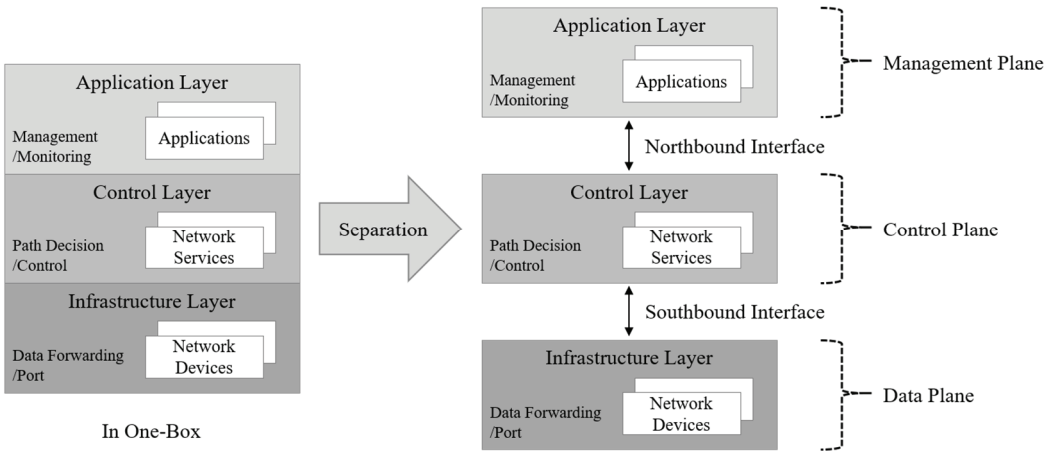

Fig. 3. Traditional network architecture vs. SDN architecture.

3.2 Technologies

Three layers are SDN application in the application layer, SDN controller in the control layer, and SDN switch in the infrastructure layer. Two interfaces of SDN are southbound and northbound interface. Southbound interface (SBI) provides an interface between control and data plane. Northbound interface (NBI) provides an interface between control and management plane.

SDN application is a management plane to communicate network requirement toward a control plane via NBI. *SDN controller* is a control plane to translate SDN application's requirement and execute the exclusive control of data plane via SBI. *SDN switch* is a data plane to consist of network elements and execute the packet forwarding.

Open vSwitch is an open source multi-layer virtual switch that is widely used in SDN. It supports

traditional network service such as VLAN, sFlow, and SPAN. It also supports new network service such as OpenFlow and network programming [19].

Mininet is a network emulator to create a virtual SDN network. It can make virtual hosts, switches, routers, links, and controllers on your laptop computer. The advantages of Mininet are fast, easy, programmable, and free [20].

OpenFlow is a southbound interface technology between SDN controller and switch. Main feature of OpenFlow is a packet processing operation called action and instruction [21]. OpenFlow is proposed by McKeown et al. [22] to enable easy network experiments in a campus network. OpenFlow Switch consists of a flow table, a group table, and OpenFlow channel. SDN controller can control SDN switches (e.g., add, update, and delete flow entries in flow tables). Each flow entries consist of match fields, counters, and instructions.

Network Configuration Protocol (NETCONF) provides mechanism to install, manipulate, and delete the configuration of network devices. It uses an XML-based data encoding for the configuration data as well as the protocol messages [23]. *YANG* [24] is a data modeling language used to model configuration and state data manipulated by the NETCONF. NETCONF/YANG is a technology of southbound interface to configure and monitor the SDN network.

Representational State Transfer (REST) is an architectural style for distributed hypermedia systems, describing the software engineering principles [25]. The application programming interface (API) is an interface between different parts of a computer program. REST API use the HTTP/HTTPS protocol to execute a command represented by uniform resource identifier (URI) strings. REST API is used a northbound interface to communicate between the SDN application and controller [26].

Chef [27], *Puppet* [28], and *Ansible* [29] are DevOps tools to configure servers and networks. They are widely used as infrastructure as code (IaC) for management and orchestration. In SDN environment, they can be used as northbound interfaces to communicate between SDN application and controller.

3.3 Security Threats of SDN

SDN gives rise to a new challenge of security threats such as software vulnerability, single point of failure (SPOF) of SDN controller, and DDoS attack. Programmability of SDN can increase software vulnerability if there are security holes in source codes. When SDN controller is broken in SPOF, Entire network will be out of service. DDoS attack against SDN is a critical security threat. If DDoS attack is targeted at SDN application, controller, and switch, the availability of SDN is seriously threatened.

3.4 Research Works on SDN Security

In this section, we have reviewed several research works of SDN security mainly focused on DDoS attack as follow.

(1) Security enhancement using SDN against DDoS attack

To use the architectural advantages; centralized network control and visibility of total network, SDN has been enhanced network security from the malicious DDoS attack. To use the technical advantages; network programming, SDN also has been delivered various security code to protect DDoS attack. Various research works include these as follows.

SDN-based MAC address hiding method has been proposed to protect IP spoofing attack from acquiring MAC address [30]. Attack detection technology has been proposed using SDN controller to overcome DDoS attack in IoT environment [31]. ArOMA, an autonomic DDoS defense framework has been proposed to leverage the programmability and centralized manageability features [32].

(2) Security challenges and solutions in SDN against DDoS attack

Despite of the architectural and technical advantages of SDN, the three-layer and two-interface architecture results in new security issues. The SDN controller can be especially vulnerable to DDoS attack. The SDN switch is also a weak point to fail the connection among hosts due to DDoS attack. To solve this security issues, various research works include these as follows.

FleXam has proposed a flexible per-flow sampling extension to enable the controller to access packet-level information to detect DDoS attack more precisely [33]. FuzzyGuard has proposed, a DDoS attack prevention extension. In it, a control network with both the protection of data flow and the convergence of attack flow is constructed in the data plane by using the idea of independent routing control flow [34]. Moving window principal components analysis is proposed to be based anomaly detection and mitigation approach to map data onto a low-dimensional subspace and keep monitoring the network state in real-time in SDN network [35]. Dynamic DDoS defense approach has been proposed to improve the defect of static DDoS defense mechanism [36].

An approach to detect large flows in real-time has been proposed to mitigate DDoS attack, when the large flows hit over the static configured thresholds [37]. A technique to defend the DDoS SYN Flooding attack to monitor backlog queue of server has been proposed [38]. TCP SYN flood attack detection and mitigation method has been proposed to use OpenFlow and sFlow to improve performance of detecting from only one router to many routers [39].

AVANT-GUARD has been proposed to a framework to advance the security of the architectural extension of OpenFlow data plane. To detect TCP session information, AVANT-GUARD filters the malicious flow request information, and sends the legitimate flow request information to the SDN controller [40]. LineSwitch has been proposed to provide a solution based on probability and blacklisting to detect and mitigate DDoS attack [41]. SLICOTS has been also proposed to mitigate TCP SYN flooding attack by monitoring TCP requests. When the number of half-open state of TCP connection hit over the thresholds, SLICOTS issues a flow rule to block that malicious flow [42]. SHDA has been proposed to a mitigation method from Slow HTTP DDoS attack. SHDA monitors HTTP incomplete requests from web server, the number of requests exceeds a predefined threshold, and then block the malicious packet [43].

(3) Security challenges and solutions in SDN against other security threats

To overcome single point of failure caused by single SDN controller, many researchers have proposed a multi-controllers deployment scheme to distribute service traffic and implement redundancy [15]. Mathematical implementation of common vulnerability scoring system (CVSS) and Bayesian network methodology in SDN has been proposed to identify the status of different entities while mutual exploitations take place against SDN security [44]. Table 3 summarizes the related work on the solution and implementation against the security issues that can happen in SDN application, controller, and switch.

Table 3. Summary of security proposals of SDN

Layer	Research work	Solution	Implementation
SDN application	Yoon et al. [30]	MAC address hiding	To protect acquiring MAC address
	Sahay et al. [32]	ArOMA	To mitigate DDoS attack automatically
	Shirali-Shahreza and Ganjali [33]	FleXam	Per-flow sampling to inspect packet
	Wang et al. [35]	Anomaly detection	Moving window principal-based analysis
SDN controller	Hong et al. [43]	SHDA	To monitor incomplete HTTP requests
	Shin et al. [40]	AVANT-GUARD	Connection migration mechanism
	Won et al. [31]	Attack detection method	To identify normal or abnormal traffic
	Afaq et al. [37]	Real-time detection of flow	To detect of mitigate the large flows
	Bang et al. [38]	Flow-based detection	To detect DDoS attack based on sFlow
	Nugraha et al. [39]	Flow-based mitigation	To mitigate it using OpenFlow
	Mohammadi et al. [42]	SLICOTS	To monitor TCP connection
	Huang and Yu [34]	FuzzyGuard	To mitigate DDoS using fuzzy inference
	Wei et al. [36]	SDN-based proxy switch	To defense dynamic DDoS attack
	Ambrosin et al. [41]	LineSwitch	Proxy-based mitigation of attack

4. Network Functions Virtualization

In this section, the comprehensive architecture, technologies of NFV, security threats, and research works on NFV security have been explained.

4.1 Architecture of NFV

NFV is a technology to decouple network software from network hardware to virtualize network functions. As shown in Fig. 4, Traditional network architecture such as switch, router, and firewall consists of software and hardware. NFV architecture is decoupled into virtual network functions (VNFs), NFV infrastructure over virtualization layer, physical hardware in ×86 hardware server, and NFV management and orchestration [45].

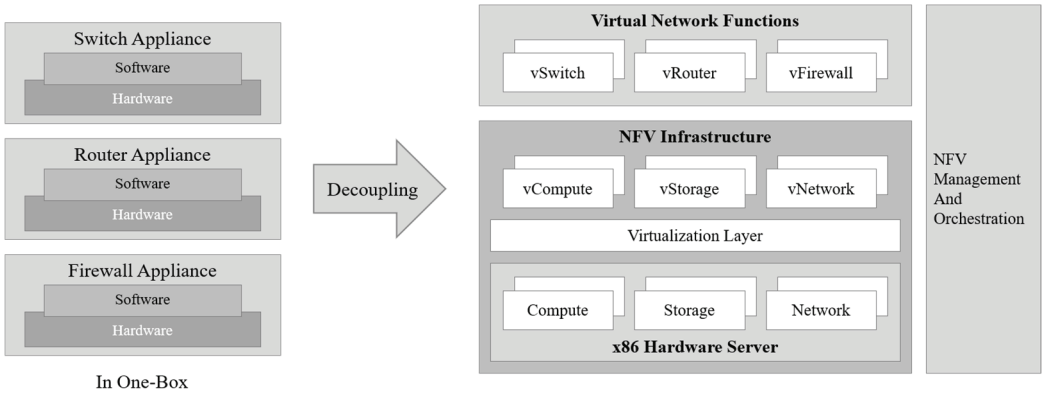

Fig. 4. Traditional network architecture vs. NFV architecture.

ETSI ISG NFV released a paper to define NFV architecture in 2014. OPNFV has been working on the open standards for NFV-based VNFs [46]. NFV can reduce capital expenditures and operating expenses, save power consumption of hardware, and increase time to market deployment by minimizing the typical engineering job [47]. SDN and NFV are high complementary but dependent to each other. They can be sometimes combined and made more valuable technology.

4.2 Technologies

In ETSI NFV model, NFV consists of three main components: NFV infrastructure (NFVI), VNFs, and NFV management and orchestration (NFV MANO) [48].

NFVI consists of the infrastructure components (e.g., compute, storage, and network) on a platform to support a hypervisor software (e.g., KVM) needed to run network apps. Hypervisor acts as an abstract or virtualization layer, which can be installed and operated on the commercial off-the-shelf (COTS) hardware like commodity x86 servers. VNFs are software applications that deliver network functions such as virtual switch, virtual router, and virtual firewall. The main purpose of using NFV is to deploy VNFs-based various network services that can be launched quickly, just by installing software without installing hardware. Many groups such as OPNFV take efforts to develop open-source methods to make VNFs cloud native. NFV MANO provides a dashboard service to manage NFV infrastructure and orchestrate VNFs. NFV MANO consists of three functional blocks in detail; NFV Orchestrator is used to manage network services in VNFs. VNF manager is used to manage VNFs in NFVI. Virtualization infrastructure manager (VIM) is used to control NFVI compute, storage, and network resources.

OPNFV is a project that facilitates a common NFVI, continuous integration (CI) with upstream projects, stand-alone testing toolsets, and a compliance and verification program for industry-wide testing and integration to accelerate the transformation of enterprise and service provider networks. As a common NFVI platform, OPNFV brings together upstream components across compute, storage, and network virtualization to create an end-to-end platform such as Hunter and Arno [49].

4.3 Security Threats of NFV

NFV gives rise to a new challenge of security threats such as VNF vulnerability, insecure interfaces, and DDoS attack [14]. VNF can increase software vulnerability if there are security holes in VNF codes. Insecure interfaces can also be a security threat. If the packet between VNF and NFV interface is unencrypted and eavesdropping by a malicious attacker, it can be a serious security threat. Most of all, DDoS attack against NFV is a critical security threat. If DDoS attack is targeted at NFV environment, the availability of NFV is seriously threatened.

4.4 Research Works on NFV Security

In this section, we have reviewed several research works of NFV security mainly focused on DDoS attack as follow.

(1) Security enhancement using NFV

To use the architectural and technical advantages with the decoupling of software and hardware, NFV has enhanced network security and mitigates the risks of malicious cyberattack. Traditional firewalls and

IDS/IPS are dependent on the performance of the hardware. More performance is required, more resource is allocated to scale up with hardware change. In NFV, more performance is required, more resource is allocated to scale out without hardware change. A quality of security has been proposed to provide adaptive security services using NFV [50].

(2) Security challenges and solutions in NFV against DDoS attack

Despite of the architectural and technical advantages of NFV, the physically or logically separated and distributed architecture of NFV is exposed new security threats that were not considered before. Especially DDoS attack is very critical threats to NFV environment targeting NFVI, VNFs, and NFV MANO. To solve this security issues, Research works include these as follows.

The security risks and targets of NFV is analyzed, and best practices of NFV are proposed. One of security risks is a DDoS attack to target VNFs, which a best practice to delay DDoS attack is a flexible VNF deployment [51]. Moving target defense (MTD) based mechanism has been proposed to detect and mitigate DDoS attack [52]. SDN, NFV, and AI are collaborated to detect and mitigate DDoS attack. A virtual public key infrastructure (vPKI) mechanism has been proposed to detect a fake VNFs [53]. VNF-based DPI engine has been proposed to be integrated with Open vSwitch in hypervisor and is working as VNF component in virtual machine [54].

(3) Security challenges and solutions in NFV against other security threats

SecMANO has been proposed a design to provide NFV based security management and orchestration. It aims to deploy and manage security functions on the demands of users and customers dynamically and adaptively [55]. Interface to network security functions (I2NSF) made by the Electronics and Telecommunications Research Institute (ETRI) in Korea has been proposed by the Internet Engineering Task Force (IETF) to network-based security services in NFV environments, such as firewall, IDS/IPS, DPI. I2NSF defines a framework and interfaces to interact with network security functions (NSFs) [56].

Compared to SDN, NFV requires more standardization and is necessary to research security issues and solution to deliver safe and secure network functions. Table 4 summarizes the related work on the solution and implementation against the security issues that can happen in NFVI, VNFs, and NFV MANO.

Table 4. Summary of security proposals of NFV

Layer	Research work	Solution	Implementation
NFVI	Jeong et al. [56]	I2NSF	A framework and for NSF
VNFs	Lal et al. [51]	Flexible VNF	Hide the DDoS attack targeting
	Liu et al. [52]	Moving Target	MTD-based DDoS detection
	Kim et al. [53]	vPKI mechanism	To detect a fake VNFs using AI
	Kim et al. [54]	VNF-based DPI engine	To detect rate of ICMP flooding
NFV MANO	Park et al. [50]	QoSE	To provide adaptive security services
	Pattaranantakul et al. [55]	SecMANO	NFV framework for secured MANO

5. Network Virtualization Overlay

In this section, the comprehensive architecture, technologies of NVO, security threats, and research works on NVO security have been explained.

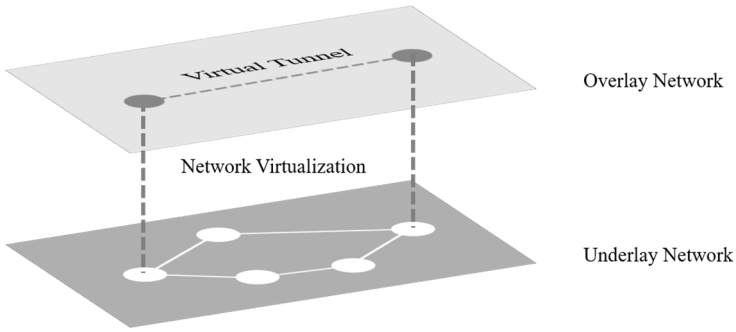

Fig. 5. Architecture of NVO composed of underlay and overlay network.

5.1 Architecture of NVO

NVO is a technology to create a virtual overlay network on top of the physical underlay network. As shown in Fig. 5, underlay network consists of physical nodes and links, which determines next-hop routing path based on various traditional routing protocol such as static, OSPF, BGP, and so on. Overlay network consists of virtual nodes and links, which determines next-hop routing path based on various overlay protocol such as VLAN, GRE, VXLAN, and so on [57].

5.2 Technologies

Virtual local area network (*VLAN*) is a traditional technology to slice a single physical link into multiple virtual links and the maximum number of VLANs is 4,096. When data center and cloud network need to expand, the number of VLANs can be exceeded over 4,096. *Generic routing encapsulation* (*GRE*) is also a traditional technology to make an overlay virtual link over underlay physical links. Only L3 network can be virtually extended in GRE [58].

Network virtualization using GRE (*NVGRE*) is a L2 frame over IP and GRE overlay proposed by Microsoft. NVGRE encapsulation is based on GRE, which mandates the inclusion of the optional GRE key field and carries virtual subnet identifier (VSID) [59]. *Stateless transport tunneling* (*STT*) is a L2 frame over IP and TCP overlay proposed by Nicira. STT can be applied in a software switch. But STT is now historically interesting and is a base work on GENEVE [60]. *Virtual extensible LAN* (*VXLAN*) is a L2 frame over IP and UDP overlay proposed by VMware. VXLAN encapsulation is based on UDP and provides a 24-bit VXLAN network identifier (VNI), which typically provides a one-to-one mapping to the tenant VID [61]. *Generic network virtualization encapsulation* (*GENEVE*) is a L2 frame over IP and UDP overlay proposed by VMware. GENEVE tunnel options are encoded in a type length value (TLV), which will be useful to new feature functionality, scalability, and security [62].

5.3 Security Threats of NVO

NVO uses an encapsulation that overwrites the new packet header over the original header. It has a technical advantage of hiding the original packet information under the encapsulation. However, there is a vulnerability if the packet is not encrypted but plaintext, the data can be leaked from packet sniffing. Secured tunneling and encryption mechanisms (e.g., IPsec) can be applied on NVO technology to increase security.

5.4 Research Works on NVO Security

In this section, we have reviewed several research works of NVO security mainly focused on packet encryption as follow.

(1) IPsec encryption

A multi-tunneling (e.g., GRE/TLS, GRE/IPsec) has been proposed to make IP packet to be encapsulated and encrypted with GRE and TLS, or GRE and IPsec [63]. But the overhead of doubled encapsulated packet causes a traffic and performance delay.

The layer-2 Ethernet extension across the data center has been proposed to increase the scope against IP spoofing attack. The authentication and encryption using IPsec or other IP-based mechanism can be used to mitigate IP spoofing attack [60].

The mechanism like IPsec has proposed to authenticate and optionally encrypt VXLAN traffic, which the tunneled traffic over the IP network can be secured. This needs to be coupled with an authentication infrastructure for authorized end points to obtain and distribute credentials [61].

IPsec is proposed to provide authentication and encryption of the IP packets formed as part of GENEVE encapsulation, because GENEVE does not have any inherent security mechanisms within an encapsulated UDP/IP packet [62].

In addition, VXLAN over IPsec like GRE over IPsec [64] is proposed to provide traffic encapsulation and encryption of VXLAN and GRE with IPsec VPN [65]. IPsec over GENEVE is proposed to provide IP encapsulating security payload (ESP) encryption to secure a layer-3 IP network [66].

(2) MACsec Encryption

Media access control security (MACsec) has been proposed to provide a secure connection of layer-2 Ethernet interface. MACsec encrypts every ethernet frame using the symmetric key cryptography to enhance confidentiality, integrity, and authentication of network frame. MACsec key agreement protocol (MKA) is used to discover an authenticated MACsec peers, and symmetric secure association keys (SAKs) are used to encrypt ethernet frame [67].

Table 5 summarizes the related works on the solution and implementation against security issues of NVO to secure a layer-3 IP packet and layer-2 Ethernet frame.

Table 5. Summary of security proposals of NVO

Layer	Research work	Solution	Implementation
Layer-3	Jung et al. [63]	Multi-tunneling	To be encapsulated and encrypted
	Garg and Wang [59]	IPsec in NVGRE	IPsec-based encryption in NVGRE
	Mahalingam et al. [61]	IPsec in VXLAN	IPsec-based encryption in VXLAN
	Gross et al. [62]	IPsec in GENEVE	IPsec-based encryption in GENEVE
Layer-2	IEEE [67]	MACsec	To secure an Ethernet Link

6. Open Issues and Challenges

Here are two open issues and challenges of SDN and NFV. First one still lacks a fine way to protect DDoS attack. Centralized architecture of SDN/NFV controller is a delicious target, and distributed

architecture of SDN/NFV switch is also a weak point of malicious attacker. That is why many researches and developments are needed to find a way to detect and mitigate DDoS attack in SDN/NFV environment. Second one is that open and vendor-neutral SDN/NFV solutions are losing power and commercial SDN/NFV solutions are developing into their closed and vendor-specific architectures. To implement software-defined, agile, and centrally managed SDN/NFV environment successfully, SDN/NFV needs to be open standards-based and vendor-neutral.

Here are also two open issues and challenges of NVO. First one is a lack of interoperability among different NVO technologies and standardization is still on going. This issue makes network infrastructure more difficult to manage and operate, especially to do some different kinds of troubleshooting in NVO environment. Second one is a lack of packet encryption technology of overlay tunnel interface. Encapsulation is not enough to protect your data. Encapsulation and encryption need to be combined to protect your data more safely from malicious attacker.

7. Conclusion

In this paper, we have explained a survey of network virtualization technologies. SDN is a new network architecture that separates hardware and software from the network device. The virtualization of SDN is mainly focused on control plane. We have explained the three tiers and two interfaces architecture, and the applied technologies of SDN. To take advantages of the architecture and technology of SDN, it can provide you a centralized and programmable security method to detect and mitigate malicious attack such as DDoS attack. NFV is a new network architecture that decouples network software from network hardware, network function from network device, and three separated components are integrated. The virtualization of NFV is mainly focused on data plane. To take advantages of the architecture and technology of NFV, it can provide you a virtualized and function-based security method to detect and mitigate malicious attack such as DDoS attack. NVO is a new network overlay architecture that addresses the requirements of multi-tenant office or data center network, especially with the mobility of user's device or the migration of VMs or virtual workloads. The virtualization of NVO is mainly focused on LAN or WAN. To take advantages of the architecture and technology of NVO, it can provide you a virtual overlay network with the encapsulation packets. As of security challenges, SDN, NFV, and NVO are continuously to be researched, developed, and deployed in your network to enhance your network environment.

Table 6 summarizes network virtualization mainly focused on the architecture, applied service, and the security strength and weak point of SDN, NFV, and NVO technologies in our paper.

Table 6. Summary of network virtualization technologies

Topic	SDN	NFV	NVO
Virtualization	Control plane	Data plane	LAN/WAN
Architecture	Three tiers and Two interfaces	Three components	Overlay network
Applied service	Office, Data center and Cloud	Telco, 5G, IoT	L2 and L3 extension
Contribution	Programmable network	Functional network	Encapsulation
Open challenge	Centralized controller	Distributed components	Encryption

Network virtualization technologies are the key paradigm that can improve the limitations of traditional network as we have seen a lot of research works are being done. A variety of research and technology adoption are being carried out to address potential security vulnerabilities and threats that have exploited them. Research on continuous security technologies will be needed in the future. We expect you to learn various network virtualization technologies, and apply your data center network, IoT network, and 5G mobile network for your convenience. Future research topic will focus on the detection and mitigation from DDoS attack in SDN.

References

[1] C. Clos, "A study of non-blocking switching networks," *Bell System Technical Journal*, vol. 32, no. 2, pp. 406-424, 1953.

[2] M. F. Bari, R. Boutaba, R. Esteves, L. Z. Granville, M. Podlesny, M. G. Rabbani, Q. Zhang, and M. F. Zhani, "Data center network virtualization: a survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 909-928, 2012.

[3] R. Jain and S. Paul, "Network virtualization and software defined networking for cloud computing: a survey," *IEEE Communications Magazine*, vol. 51, no. 11, pp. 24-31, 2013.

[4] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: a survey," in *Proceedings of 2013 IEEE SDN for Future Networks and Services (SDN4FNS)*, Trento, Italy, 2013, pp. 1-7.

[5] L. Schehlmann, S. Abt, and H. Baier, "Blessing or curse? Revisiting security aspects of software-defined networking," in *Proceedings of the 10th International Conference on Network and Service Management (CNSM) and Workshop*, Rio de Janeiro, Brazil, 2014, pp. 382-387.

[6] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on software-defined networking," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 27-51, 2014.

[7] 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.

[8] D. Kreutz, F. M. 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.

[9] Z. Yao and Z. Yan, "Security in software-defined-networking: a survey," in *Security, Privacy and Anonymity in Computation, Communication and Storage*. Cham, Switzerland: Springer, 2016, pp. 319-332.

[10] M. A. Nadeem and T. Karamat, "A survey of cloud network overlay protocols," in *Proceedings of 2016 6th International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, Konya, Turkey, 2016, pp. 177-182.

[11] A. Abdou, P. C. Van Oorschot, and T. Wan, "Comparative analysis of control plane security of SDN and conventional networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3542-3559, 2018.

[12] B. Yi, X. Wang, K. Li, and M. Huang, "A comprehensive survey of network function virtualization," *Computer Networks*, vol. 133, pp. 212-262, 2018.

[13] M. Pattaranantakul, R. He, Q. Song, Z. Zhang, and A. Meddahi, "NFV security survey: from use case driven threat analysis to state-of-the-art countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3330-3368, 2018.

[14] A. M. Alwakeel, A. K. Alnaim, and E. B. Fernandez, "A survey of network function virtualization security," in *Proceedings of the IEEE SoutheastCon*, St. Petersburg, FL, 2018, pp. 1-8.

[15] Y. Liu, B. Zhao, P. Zhao, P. Fan, and H. Liu, "A survey: typical security issues of software-defined networking," *China Communications*, vol. 16, no. 7, pp. 13-31, 2019.

[16] Open Networking Foundation, "Software-Defined Networking (SDN) Definition," 2021 [Online]. Available: https://www.opennetworking.org/sdn-definition.

[17] M. Casado, T. Garfinkel, A. Akella, M. J. Freedman, D. Boneh, N. McKeown, and S. Shenker, "SANE: a protection architecture for enterprise networks," in *Proceedings of the 15th USENIX Security Symposium*, Vancouver, Canada, 2006.

[18] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, "Ethane: taking control of the enterprise," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 4, pp. 1-12, 2007.

[19] Linux Foundation, "What is Open vSwitch," 2016 [Online]. Available: https://docs.openvswitch.org/en/latest/intro/what-is-ovs.

[20] B. Lantz, B. Heller, and N. McKeown, "A network in a laptop: rapid prototyping for software-defined networks," in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, Monterey, CA, 2010, pp. 1-6.

[21] Open Networking Foundation, "OpenFlow Switch Specification version 1.5.1," 2015 [Online]. Available: https://opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf.

[22] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69-74, 2008.

[23] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, "Network configuration protocol (NETCONF)," Internet Engineering Task Force, RFC6241, 2011.

[24] M. Bjorklund, "YANG: a data modeling language for the network configuration protocol (NETCONF)," Internet Engineering Task Force, RFC6020, 2010.

[25] R. T. Fielding, "Architectural styles and the design of network-based software architectures," Ph.D. dissertation, University of California, Irvine, CA, 2000.

[26] W. Zhou, L. Li, M. Luo, and W. Chou, "Requirements and Design Patterns for REST Northbound API in SDN," Internet Engineering Task Force, Internet Draft, 2016.

[27] Chef [Online]. Available: https://www.chef.io.

[28] Puppet [Online]. Available: https://puppet.com.

[29] Ansible [Online]. Available: https://www.ansible.com.

[30] S. Yoon, T. Ha, S. Kim, Y. Kim, and H. Lim, "Hiding MAC addresses for cyber security on software-defined networks," in *Proceedings of Symposium of the Korean Institute of Communications and Information Sciences (KICS)*, 2018, pp. 1452-1452.

[31] J. H. Won, J. W. Hong, and Y. Y. You, "A study on the improvement of security threat analysis and response technology by IoT layer," *Journal of Convergence for Information Technology*, vol. 8, no. 6, pp. 149-157, 2018.

[32] R. Sahay, G. Blanc, Z. Zhang, and H. Debar, "ArOMA: an SDN based autonomic DDoS mitigation framework," *Computers & Security*, vol. 70, pp. 482-499, 2017.

[33] S. Shirali-Shahreza and Y. Ganjali, "Efficient implementation of security applications in OpenFlow controller with FleXam," in *Proceedings of 2013 IEEE 21st Annual Symposium on High-Performance Interconnects*, San Jose, CA, 2013, pp. 49-54.

[34] M. Huang and B. Yu, "FuzzyGuard: a DDoS attack prevention extension in software-defined wireless sensor networks," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 13, no. 7, pp. 3671-3689, 2019.

[35] M. Wang, H. Zhou, and J. Chen, "A moving window principal components analysis based anomaly detection and mitigation approach in SDN network," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 12, no. 8, pp. 3946-3965, 2018.

[36] Q. Wei, Z. Wu, K. Ren, and Q. Wang, "An OpenFlow user-switch remapping approach for DDoS defense," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 10, no. 9, pp. 4529-4548, 2016.

[37] M. Afaq, S. Rehman, and W. C. Song, "Large flows detection, marking, and mitigation based on sFlow standard in SDN," *Journal of Korea Multimedia Society*, vol. 18, no. 2, pp. 189-198, 2015.

[38] G. Bang, D. Choi, and S. Bang, "A protection method using destination address packet sampling for SYN flooding attack in SDN environments," Journal of Korea Multimedia Society, vol. 18, no. 1, pp. 35-41, 2015.

[39] M. Nugraha, I. Paramita, A. Musa, D. Choi, and B. Cho, "Utilizing OpenFlow and sFlow to detect and mitigate SYN flooding attack," *Journal of Korea Multimedia Society*, vol. 17, no. 8, pp. 988-994, 2014.

[40] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "Avant-guard: scalable and vigilant switch flow management in software-defined networks," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, Berlin, Germany, 2013, pp. 413-424.

[41] M. Ambrosin, M. Conti, F. De Gaspari, and R. Poovendran, "LineSwitch: tackling control plane saturation attacks in software-defined networking," *IEEE/ACM Transactions on Networking*, vol. 25, no. 2, pp. 1206-1219, 2016.

[42] R. Mohammadi, R. Javidan, and M. Conti, "SLICOTS: an SDN-based lightweight countermeasure for TCP SYN flooding attacks," *IEEE Transactions on Network and Service Management*, vol. 14, no. 2, pp. 487-497, 2017.

[43] K. Hong, Y. Kim, H. Choi, and J. Park, "SDN-assisted slow HTTP DDoS attack defense method," *IEEE Communications Letters*, vol. 22, no. 4, pp. 688-691, 2017.

[44] R. Deb and S. Roy, "Dynamic vulnerability assessments of software-defined networks," *Innovations in Systems and Software Engineering*, vol. 16, no. 1, pp. 45-51, 2020.

[45] European Telecommunications Standards Institute (ETSI), "Network Functions Virtualisation (NFV)," 2021 [Online]. Available: https://www.etsi.org/technologies/nfv.

[46] sdxcentral, "What are virtual network functions or VNFs?," 2014 [Online]. Available: https://www.sdxcentral.com/networking/nfv/definitions/virtual-network-function.

[47] European Telecommunications Standards Institute (ETSI), "Network Functions Virtualisation - Introductory White Paper," 2012 [Online]. Available: https://portal.etsi.org/NFV/NFV_White_Paper.pdf.

[48] European Telecommunications Standards Institute (ETSI), "Network Functions Virtualisation (NFV); Architectural Framework," 2014 [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf.

[49] OPNFV, "Open Platform for NFV (OPNFV) - technical overview," [Online]. Available: https://www.opnfv.org/software/technical-overview.

[50] T. Park, Y. Kim, J. Park, H. Suh, B. Hong, and S. Shin, "QoSE: quality of security a network security framework with distributed NFV," in *Proceedings of 2016 IEEE International Conference on Communications (ICC)*, Kuala Lumpur, Malaysia, 2016, pp. 1-6.

[51] S. Lal, T. Taleb, and A. Dutta, "NFV: Security threats and best practices," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 211-217, 2017.

[52] C. C. Liu, B. S. Huang, C. W. Tseng, Y. T. Yang, and L. D. Chou, "SDN/NFV-based moving target DDoS defense mechanism," in *Recent Trends in Data Science and Soft Computing*. Cham, Switzerland: Springer, 2019, pp. 548-556.

[53] H. Kim, S. Park, and J. Ryou, "Research on DDoS Detection using AI in NFV," *Journal of Digital Contents Society*, vol. 19, no. 4, pp. 837-844, 2018.

[54] J. T. Kim, J. H. Kim, and I. K. Kim, "Analysis on the VNF-DPI for the cloud security," in *Proceedings of Symposium of the Korean Institute of Communications and Information Sciences (KICS)*, 2018, pp. 811-812.

[55] M. Pattaranantakul, R. He, A. Meddahi, and Z. Zhang, "SecMANO: towards network functions virtualization (NFV) based security management and orchestration," in *Proceedings of 2016 IEEE Trustcom/BigDataSE/ISPA*, Tianjin, China, 2016, pp. 598-605.

[56] J. Jeong, S. Hyun, T. Ahn, S. Hares, and D. R. Lopez, "Applicability of interfaces to network security functions to network-based security services," Internet Engineering Task Force, Fremont, CA, draft-ietf-i2nsf-applicability-10, 2019.

[57] J. Hyun and W. Hong, "Technical research trends of network virtualization technologies," in *Proceedings of the Committee on Korean Network Operations and Management (KNOM) Conference*, Chooncheon, Korea, 2016.

[58] T. Narten, E. Gray, D. Black, L. Fang, L. Kreeger, and N. Napierala, "Problem statement: Overlays for network virtualization," Internet Engineering Task Force, Fremont, CA, RFC 7364, 2013.

[59] P. Garg and Y. Wang, "NVGRE: network virtualization using generic routing encapsulation," Internet Engineering Task Force, Fremont, CA, RFC 7637, 2015.

[60] B. Davie and J. Gross, "A stateless transport tunneling protocol for network virtualization (STT)," Internet Engineering Task Force, Fremont, CA, draft-davie-stt-06, 2016.

[61] M. Mahalingam, D. G. Dutt, K. Duda, K. Agarwal, L. Kreeger, T. Sridhar, M. Bursell, and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): a framework for overlaying virtualized layer 2 networks over layer 3 networks," Internet Engineering Task Force, Fremont, CA, RFC 7348, 2014.

[62] J. Gross, I. Ganga, and T. Sridhar, "GENEVE: generic network virtualization encapsulation," Internet Engineering Task Force, Fremont, CA, RFC 8926, 2020.

[63] B. G. Jung, H. G. Lee, H. S. Park, and J. D. Park, "Hyper-connected trust network technology," *Electronics and Telecommunications Trends*, vol. 32, no. 1, pp. 35-45, 2017.

[64] Y. Andamasov, "GRE over IPsec for secure tunneling," 2021 [Online]. Available: https://support.vyos.io/en/kb/articles/gre-over-ipsec-for-secure-tunneling-2.

[65] Fortinet, "FortiOS 6.2.3 (VXLAN over IPsec tunnel)," 2020 [Online]. Available: https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/821119/vxlan-over-ipsec-tunnel.

[66] S. Boutros, C. Qian, and D. Wing, "IPsec over Geneve Encapsulation," Internet Engineering Task Force, Fremont, CA, draft-boutros-nvo3-ipsec-over-geneve-01, 2018.

[67] IEEE Standard for Local and metropolitan area networks – Media Access Control (MAC) security (IEEE Std 802.1AE), 2018 [Online]. Available: https://1.ieee802.org/security/802-1ae/.

Seung Hun Jee **https://orcid.org/0000-0002-2183-0172**

He received B.S. in the Department of French Language and Literature from Seoul National University in 2002, and in the Department of Computer Science from Korea National Open University in 2015. Since March 2015, he has been with the Department of Computer Science from Korea National Open University as a M.S. candidate. He has been working as a network engineer in SK since 2005.

Ji Su Park **https://orcid.org/0000-0001-9003-1131**

He received his B.S., M.S. degrees in Computer Science from Korea National Open University, Korea, in 2003, 2005, respectively and Ph.D. degrees in Computer Science Education from Korea University, 2013. He is currently a Professor in Department of Computer Science and Engineering from Jeonju University in Korea. His research interests are in grid computing, mobile cloud computing, cloud computing, distributed system, computer education, and AIoT. He is employed as associate editor of *Human-centric Computing and Information Sciences* (HCIS) by Springer, *The Journal of Information Processing Systems* (JIPS) by KIPS. He has also served as the chair, program committee chair or organizing committee chair at international conferences and workshops. He has received "best paper" awards from the CSA2018 conferences and "outstanding service" awards from CUTE2019 and BIC2020.

Jin Gon Shon **https://orcid.org/0000-0002-0540-4640**

He received the B.Sc. degree in Mathematics and the M.S. and Ph.D. degrees in Computer Science from Korea University, Seoul, Korea. Since 1991, he has been working for Department of Computer Science, Korea National Open University. His research interests consist of two groups; computer science and e-learning fields. They include computer networks, distributed computing, wireless sensor networks, big data processing, and educational technologies such as mobile technologies and universal design for e-learning.