SDN-Based Network Security Functions for VoIP and VoLTE Services

Daeyoung Hyun*, Jinyoug Kim†, Jaehoon (Paul) Jeong‡, Hyoungshick Kim*, Jungsoo Park§, and Taejin Ahn¶
* Department of Software, Sungkyunkwan University, Republic of Korea
† Department of Computer Science & Engineering, Sungkyunkwan University, Republic of Korea
‡ Department of Interaction Science, Sungkyunkwan University, Republic of Korea
§ Electronics and Telecommunications Research Institute, Republic of Korea
¶ Korea Telecom, Republic of Korea
Email: {dyhyun,wlsdyd0930,pauljeong,hyoung}@skku.edu,
pjs@etri.re.kr, taejin.ahn@kt.com

***Abstract*—This paper proposes a framework for security services for Voice over IP (VoIP) and Voice over LTE (VoLTE) in commercial networks using Software-Defined Networking (SDN) and Network Functions Virtualization (NFV). The VoIP/VoLTE services are exposed to several security threats such as Denial-of-Service (DoS) attack, network sniffing, unauthorized services access, and VoIP spam. The conventional security services for VoIP/VoLTE suffer from the lack of flexible security rule installation and dynamic security rule update. The security service framework for VoIP/VoLTE based on SDN and NSF in this paper suggests an advanced way to deal with the security threats. For different security threats, the framework can flexibly install new rules and dynamically update these rules. Based on a YANG data model for remote networked-device configuration, we implemented basic configuration functions of the security service framework for VoIP/VoLTE. In order to show the feasibility of the proposed framework, we used OpenDaylight for our implementation that can provide VoIP/VoLTE service providers with effective security services.**

I. Introduction

Recently, Software-Defined Networking (SDN) technology [1] has attracted a great deal of attention in the field of network community from network research and development community. This is because it can modify a network dynamically through an independent control plan to deploy new configurations and mechanisms, and test their performance [2]. Also, Network Functions Virtualization (NFV) [3] has been considered as a promising technology for cloud-based network services. This because it allows network administrators to dynamically manage network resources such as firewall, intrusion detection system, network address translator, and mobile network gateways [4].

Internet Engineering Task Force (IETF), which is an international Internet standardization organization, has launched Interface to Network Security Functions (I2NSF) Working Group for standardizing interfaces for network security services in NFV environments [5]. This standardization is trying to define the standard interfaces for network security services through Network Security Functions (NSFs) based on SDN and NFV.

We proposed security services (e.g., firewall and web filter) through I2NSF along with SDN before [6]. In this paper, we describe the importance of a security system using network virtualization with a new target security domain, such as Voice over IP (VoIP) and Voice over LTE (VoLTE).

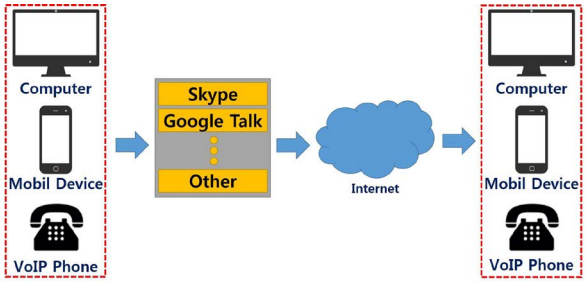


Fig. 1. Voice Call Services of VoIP and VoLTE

VoIP uses the Internet to provide video and voice call services to users. It enables the integration of additional services (e.g., simple messaging service). It outperforms the traditional voice service based on Public Switched Telephone Network (PSTN) in terms of Capital expenditure (CAPEX) and Operational expenditure (OPEX). Because of these advantages, it has been widely deployed in various applications and services [7]. However, the VoIP/VoLTE services are exposed to various security attacks. First, Denial of Service (DoS) attack can cause the lack of system resources for the service or paralyze network connection by generating massive malicious packets. Second, hackers can intercept or manipulate the packets of users by sniffing packets for malicious purposes. Third, the manipulation of user profiles can lead to the unauthorized access to services. Finally, VoIP spam can be sent to the users through the Internet.

In order to mitigate the risk of such security attacks, this paper proposes an SDN-based network security service system for VoIP/VoLTE using I2NSF. Based on a YANG data model, we implemented basic security functions to demonstrate the feasibility of our proposed security services. We also describe several important further research issues.

The remaining structure of this paper is as follows. Section II describes an architecture of VoIP/VoLTE security service. Section III explains security threat analysis for VoIP/VoLTE. Section IV proposes a YANG data model for VoIP/VoLTE security services. Section V describes our

implementation of VoIP/VoLTE security services. Section VI discusses research issues for VoIP/VoLTE security services. In Section VII, we conclude this paper along with future work.

II. Architecture

This section describes a framework for SDN-based security services using I2NSF, such as a centralized VoIP/VoLTE security system. Figure 2 shows the framework of I2NSF which has three main interfacesm such as Client Facing Interface, NSF Facing Interface, and Registration Interface [6], [8].

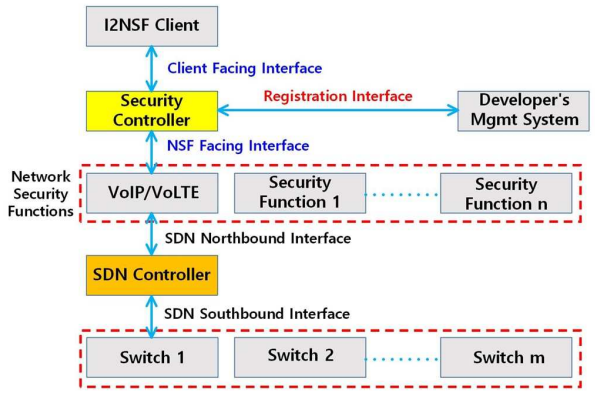


Fig. 2. Proposed Architecture using SDN

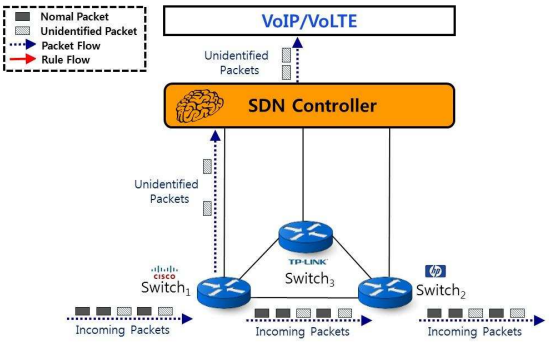
Developer's Management System (denoted as Developer's Mgmt System), which is used by a service provider, installs a security service package which will perform low-level security functions for security controller via registration interface (also called vendor facing interface). The following shows the procedure showing how a high-level security policy is enforced into low-level security policies that will be executed in the network security functions and SDN network switches.

1) Using Client Facing Interface, I2NSF Client (used by a network administrator) sends a high-level security policy to Security Controller.
2) Security Controller interprets the received high-level policy into low-level security function(s) and then sends those network configuration commands to the relevant Network Security Function(s).
3) The Network Security Function delivers network configuration to SDN Controller via SDN Northbound Interface.
4) SDN Controller sends the flow table configuration to the relevant switches via SDN Southbound Interface.

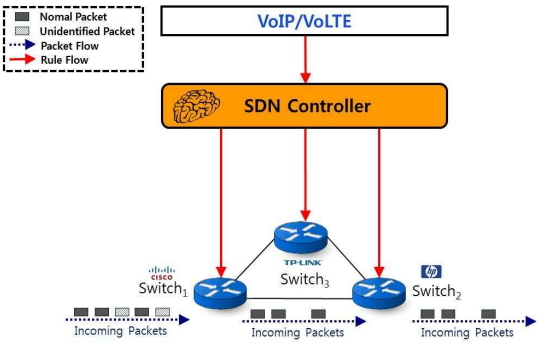
III. Case Studies

In this section, we propose a variety of attacks and especially how to respond to VoIP/VoLTE. We consider four cases of security threats.

Case 1. Malicious packets (e.g., bot command and malware payload)



(a) Mirroring of Packets of VoIP/VoLTE



(b) Blocking of Packets of VoIP/VoLTE

Fig. 3. Handling of Packets of VoIP and VoLTE Services

Fig. 3 shows the situation where an unidentified packet arrives at a switch in an SDN network.

Problem

1) $Switch_1$ needs to determine whether to mirror an unknown flow's packet or even a matched SIP packet an NSF for VoIP/VoLTE NSF via SDN Controller (i.e., SDN controller).

Mirroring of Packets of VoIP/VoLTE

1) Normal packets and unidentified packets arrive at a switch.
2) The unidentified packets are mirrored by SDN Controller and delivered to VoIP/VoLTE Intrusion Prevention System (IPS) denoted as VoIP-VoLTE IPS.
3) VoIP-VoLTE IPS analyzes the header and contents of the unidentified packets.

Blocking of Packets of VoIP/VoLTE

1) If the unidentified packets are regarded as malicious packets, a new rule for the flow for the packets is sent to SDN Controller.
2) SDN Controller configures the flow (i.e., drop) related to the new rule to block malicious packets at the switches.

3) After this flow configuration, the malicious packets are dropped at the switches.

Case 2. Sniffing Threat

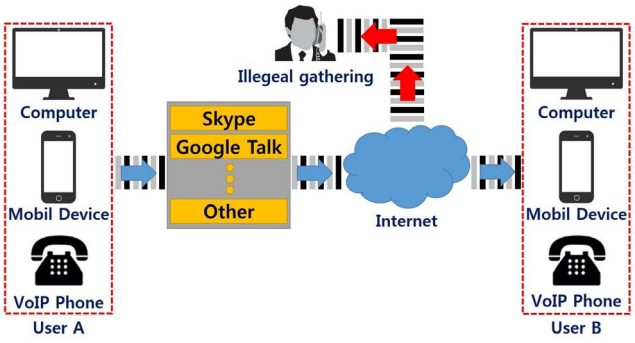


Fig. 4. Network Packet Sniffing in VoIP/VoLTE Services

Fig. 4 shows a Sniffing threat that collects audio/video data packets for VoIP/VoLTE sessions. The procedure is as follows:

Problem

1) Users A and B try to communicate with each other by a voice call service based on VoIP/VoLTE.
2) A hacker as a sniffer intercepts packets belonging to their connection in the middle.

Solution Plan

1) VoIP-VoLTE IPS checks whether the packets belonging to the current voice call connection are forwarded to a suspicious host of the sniffer.
2) If a sniffing is identified, the switches in the SDN network are configured by SDN controller through the interaction with VoIP-VoLTE IPS so that the packets toward the sniffer can be discarded by the switches.

Case 3. Launching DoS attacks to degrade the quality of services

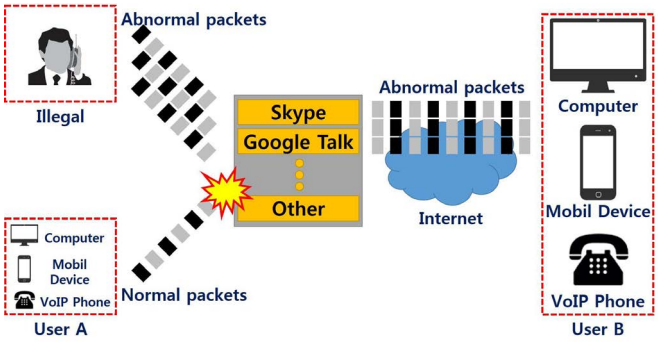


Fig. 5. The Transmission of Many Abnormal Packets of VoIP/VoLTE

Fig. 5 shows an attack that interferes with the VoIP/VoLTE connection by DoS attack, which sends dummy packets to the parties for the connection. The procedure is as follows:

Problem

1) Users A and B try to communicate with each other through a voice call based on VoIP/VoLTE.
2) The data packets are carrying voice data.
3) However, a malicious user sends many dummy packets through the server to user B, which interfere with the connection between users A and B.

Solution Plan

1) Our VoIP-VoLTE IPS checks the forwarding path of packets to determine whether the packets comes from a malicious host, not from the parties for the VoIP/VoLTE connection.
2) If a DoS attack is identified, the switches in the SDN network are configured by SDN controller through the interaction with VoIP-VoLTE IPS so that the packets from the DoS attacker can be discarded by the switches.

Case 4. Malicious Voice Calls for Unintended Charging

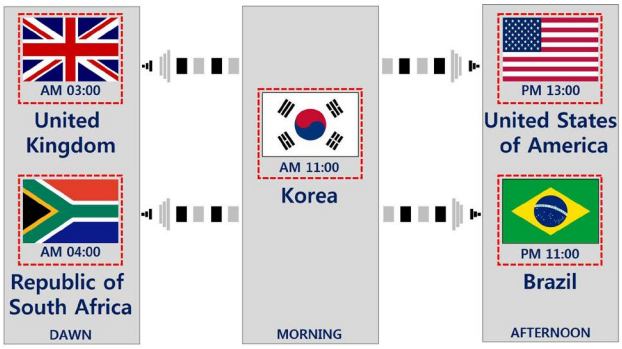


Fig. 6. Malicious Voice Calls for Unidented Charging involving Different Countries as Call Destinations

Fig. 6 shows the packets originating from Korea toward other countries with different time zones. The invalid voice calls can be detected as follows:

Problem

1) Considering South Korea as a source location of voice call packets, other countries are used as packet destinations.
2) Unidentified packets for a VoIP/VoLTE call are sent toward the unexpected countries.

Solution Plan

1) The unidentified packets are mirrored to VoIP-VoLTE IPS to find out its destination location.
2) If the packets are sent toward an unexpected country on the basis of the user's call history, the packets are regared as a malicious call for illegal bomb charging to the voice call service provider.
3) A drop rule is set up at the switches to drop the flow corresponding to the packets.

IV. YANG Data Model of VoIP/VoLTE

This section is intended to present the YANG data model to implement the security service of VoIP/VoLTE presented earlier.

```
+--: (voip-volte)
  +--rw voip-volte-rule                    *[voip-volte-rule-id]
     +--rw voip-volte-rule-id              uint 8
     +--rw event
     |  +--rw called-voip                  boolean
     |  +--rw called-volte                 boolean
     +--rw condition
     |  +--rw sip-header?                  *[sip-header-uri]
     |  |  +--rw sip-header-uri            string
     |  |  +--rw sip-header-method         string
     |  |  +--rw expire-time yang:date-and-time
     |  |  +--rw sip-header-user-agent     uint 32
     |  +--rw sip-header?                  *[sip-header-uri]
     |     +--rw cell-id-region            uint 32
     +--rw action
        +--rw (action-type)?
           +--: (ingress-action)
           |  +--rw (ingress-action-type)?
           |     +--: (permit)
           |     |  +--: rw permit         boolean
           |     +--: (deny)
           |     |  +--: rw deny           boolean
           |     +--: (mirror)
           |     |  +--: rw mirror         boolean
           +--: (egress-action)
              +--rw (egress-action-type)?
                 +--: (redirection)
                    +--: rw redirection?  boolean
```

Fig. 7. Data Model of VoIP/VoLTE

Fig. 7 presents a data model for VoIP/VoLTE, which follows of RFC 6020 [9]. Each rule for VoIP/VoLTE is saved as a list, and rule-id is given to each. VoIP/VoLTE has event, condition, and action (ECA) structure, classifying each event, checking each condition of a packet, and taking ingress-action or egress-action for each corresponding packet. The ingress-action then responds to incoming packets to permit, deny, or mirror. The egress-action responds to incoming packets to the redirection or tunneling. The permit is an action that allows incoming packets, the deny is an action to block an incoming packets, the mirror is an action to copy an incoming packets, and so forward the orignal packet according to the forwarding path and forward the packet copy to the NSF for security service. The redirection is an action to change the packet forwarding next-hop switch and the tunneling is an action to encapsulate the packet with an additional packet header [10].

V. Implementation of VoIP/VoLTE

This section explains the implementation of VoIP/VoLTE security service. The security service is based on a black list of illegal IP addresses used by hackers. The implementation is based on Mininet and OpenDaylight. It demonstrates the blocking of packets of illegal VoIP/VoLTE packets.

Fig. 8 is an architecture which provides VoIP/VoLTE security service based on SDN and I2NSF. In the figure, I2NSF

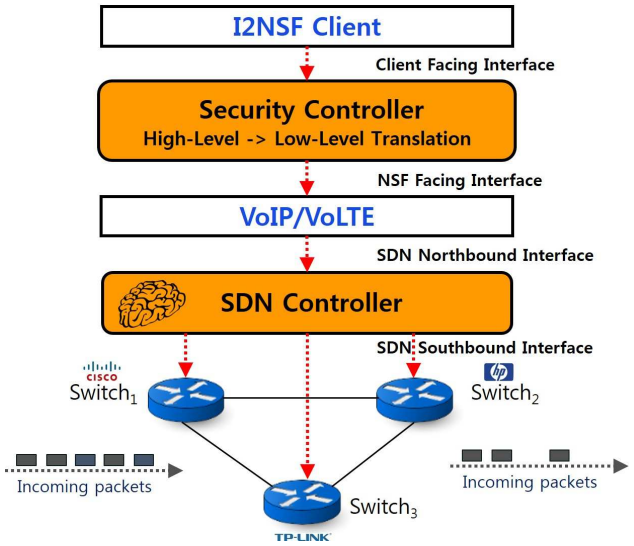


Fig. 8. An Architecutre of VoIP/VoLTE Security Services

client sends Security Controller a high-level security policy for VoIP/VoLTE security service via Client Facing Interface. Security Controller translates the high-level security policy into low-level security policies. Security Controller sends the low-level policies to VoIP-VoLTE IPS via NSF facing Interface. VoIP-VoLTE IPS sends ingress rules to Switch Controller via SDN Northbound Interface. Switch Controller sends such ingress rules for VoIP/VoLTE security services to its governed switches via SDN Southbound Interface. Refer to the detailed operations in our IETF Internet Draft in [8].

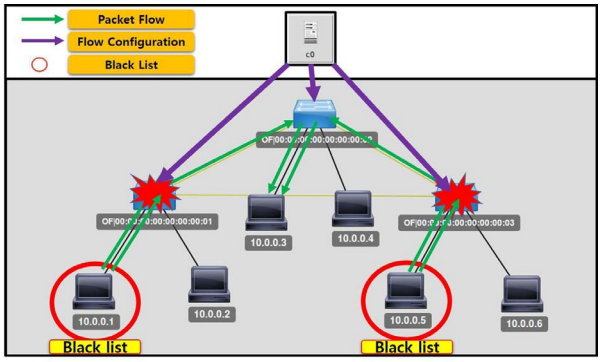


Fig. 9. Implementation of VoIP/VoLTE in OpenDaylight

Fig. 9 represents the result of packet filtering according to flow table configuration. Fig. 10 shows a snapshot where the switches drop packets from the registered IP addresses in the blacklist. A blacklist is set up in Mininet. Assume that IP addresses of 10.0.0.1 and 10.0.0.5 are registered in the blacklist, and packets are sent from 10.0.0.5 to 10.0.0.1 or from 10.0.0.3 to 10.0.0.1, respectively. On the other hand, packets sent from 10.0.0.3 to 10.0.0.2 are forwarded without dropping. The snapshot of this experiment is shown on Fig. 9.

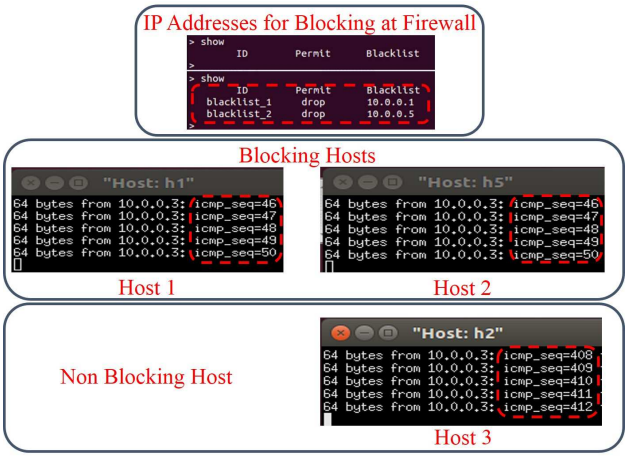


Fig. 10. Implementation of VoIP/VoLTE in Mininet

VI. Research Issues

We consider the following research problems.

1) Adoption of a VoIP/VoLTE module of Korea Telecom, which provides actual voice call services.
2) Usage of Service Function Chaining (SFC) to provision flexible network security services according to context information related to a packet along with the header and payload of the packet [11], [12].
3) Development of VoIP/VoLTE security services for the four cases to prevent security vulnerability.
4) Improvement to a YANG data model for VoIP/VoLTE.
5) Packet analysis through the mirroring and enhanced performance of packet blocking.

VII. Conclusion

We studied a variety of security threats in VoIP/VoLTE services. In particular, we proposed an architecture for VoIP/VoLTE security services. This paper showed the feasibility of our architecture by implementing a filtering for VoIP/VoLTE. Also, we proposed a YANG data model. As future work, we will enhance our YANG data model and develop an SFC-enabled I2NSF security service system to support flexible network security services.

VIII. Acknowledgment

The VoIP/VoLTE security use cases and the YANG data model presented in the paper were provided by the research and implementation of KT Infra R&D Lab. This work was supported by ICT R&D program of MSIP/IITP [R0166-15-1041, Standard Development of Network Security based SDN]. This work was supported in part by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2014006438). Note that Jaehoon (Paul) Jeong is the corresponding author.

References

[1] ONF, "Software-Defined Networking: The New Norm for Networks," *ONF White Paper*, 2012.
[2] F. Hu, Q. Hao, and K. Bao, "A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 4, pp. 2181–2206, 2014.
[3] M. Chiosi, "Network Functions Virtualisation Introductory White Paper," *Technical Report, SDN and OpenFlow World Congress*, pp. 1–16, 2012.
[4] A. Reid, "Network Functions Virtualisation (NFV); Infrastructure Overview," ETSI SG NFV-INF 001 V1.1.1, Tech. Rep. 001, Jan. 2015.
[5] IETF I2NSF Working Group, "Interface to Network Security Functions (I2NSF)," https://datatracker.ietf.org/wg/i2nsf/charter/.
[6] K. Jinyoung, M. D. Firoozjaei, J. P. Jeong, H. Kim, and J.-S. Park, "SDN-based Security Services using Interface to Network Security Functions," *Proceedings of the 7th International Conference on ICT Convergence (ICTC)*, pp. 526–529, Oct. 2015.
[7] R. Sunghun and S. Hyunsik, "Analysis of Key Technologies related to VoIP Security," *The Korea Institute of Electronic Communication Sciences*, pp. 385–390, Aug. 2010.
[8] J. Jeong, H. Kim, J. Park, T. Ahn, and S. Lee, "Software-Defined Networking Based Security Services using Interface to Network Security Functions," *IETF Internet-Draft draft-jeong-i2nsf-sdn-security-services*, Jul. 2016.
[9] M. Bjorklund, "YANG - A Data Modeling Language for the NEtwork Configuration Protocol (NETCONF)," *IETF RFC 6020*, Oct. 2010.
[10] J. Jeong, J. Kim, D. Hyun, J. Park, , and T. Ahn, "YANG Data Model of Interface to Network Security Functions Capability Interface," *IETF Internet-Draft draft-jeong-i2nsf-capability-interface-yang*, Jul. 2016.
[11] J. Halpern and C. Pignataro, "Service Function Chaining (SFC) Architecture," *IETF RFC 7665*, Oct. 2015.
[12] S. Hyun, S. Woo, Y. Yeo, J. Jeong, and J. Park, "Service Function Chaining-Enabled I2NSF Architecture," *IETF Internet-Draft draft-hyun-i2nsf-sfc-enabled-i2nsf*, Jul. 2016.