(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2019 년 7 월 4 일 (04.07.2019)

WIPO | PCT

(10) 국제공개번호
WO 2019/132270 A1

(51) 국제특허분류:
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
H04L 9/08 (2006.01)

(21) 국제출원번호: PCT/KR2018/014994

(22) 국제출원일: 2018 년 11 월 29 일 (29.11.2018)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2017-0181217 2017 년 12 월 27 일 (27.12.2017) KR

(71) 출원인: 충남대학교산학협력단 (**THE INDUSTRY & ACADEMIC COOPERATION IN CHUNGNAM NATIONAL UNIVERSITY**) [KR/KR]; 34134 대전시 유성구 대학로 99, Daejeon (KR).

(72) 발명자: 류재철 (**RYOU, Jae Cheol**); 34140 대전시 유성구 어은로 57, 132동 801호, Daejeon (KR). 김현진 (**KIM, Hyun Jin**); 34185 대전시 유성구 온천북로 7, 102동 1092호, Daejeon (KR).

(74) 대리인: 심경식 등 (**SHIM, Kyoung-Shik** et al.); 06227 서울시 강남구 역삼로 212, 동아빌딩 6층, Seoul (KR).

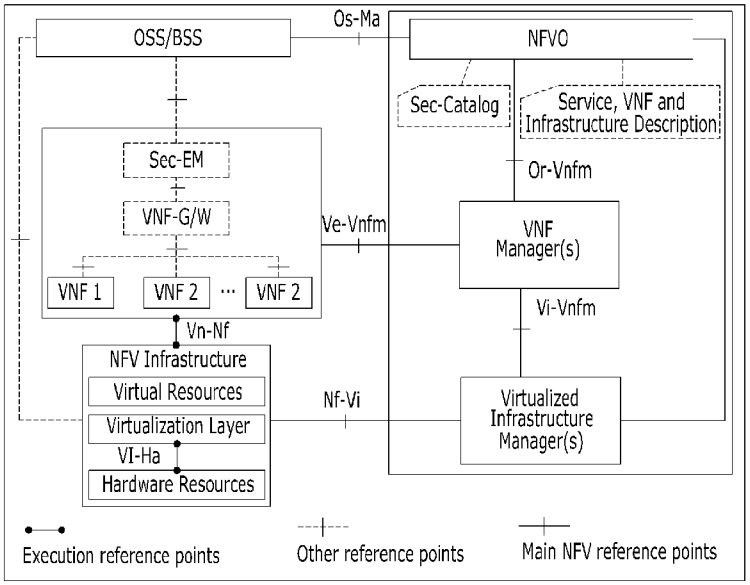
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE,

(54) **Title:** SECURE COMMUNICATION METHOD IN NFV ENVIRONMENT AND SYSTEM THEREFOR

(54) **발명의 명칭:** NFV 환경에서 보안 통신 방법 및 그 시스템

[도1]



(57) **Abstract:** Disclosed are a secure communication method in a network function virtualization (NFV) environment and a system therefor. A secure communication method in an NFV environment, according to one embodiment of the present invention, is a secure communication method between virtualized network functions (VNF) in an NFV environment, and comprises: a step in which an element manager performs authentication between a first VNF and a second VNF by using a hash chain; a step in which each of the first VNF and the second VNF that have been authenticated generates a secret key on the basis of the hash chain thereof; and a step in which the first VNF and the second VNF perform communication by using the secret keys thereof.

WO 2019/132270 A1

[다음 쪽 계속]

LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

(57) 요약서: 본 발명은 NFV 환경에서 보안 통신 방법 및 그 시스템이 개시된다. 본 발명의 일 실시예에 따른 NFV 환경에서 보안 통신 방법은 NFV(network function virtualization) 환경에서 VNF(virtualized network function) 간 보안 통신 방법에 있어서, 요소 관리자는 해시체인을 이용하여 제1 VNF 와 제2 VNF 간 인증을 수행하는 단계, 상기 인증 완료된 제1 VNF 와 제2 VNF 는 자신의 해시체인을 기반으로 비밀키를 각각 생성하는 단계, 상기 제1 VNF 와 제2 VNF 는 자신의 비밀키를 이용하여 통신을 수행하는 단계를 포함한다.

명세서

발명의 명칭: NFV 환경에서 보안 통신 방법 및 그 시스템

기술분야

[1] 본 발명은 NFV 환경에서 보안 통신 방법 및 그 시스템에 관한 것으로, 특히 NFV 환경에서 테넌트 내 VNF 간의 인증을 수행하고, 트래픽을 제어하여 VNF 간 안전한 통신을 보장하는 NFV 환경에서 보안 통신 방법 및 그 시스템에 관한 것이다.

배경기술

[2] 최근 세계 네트워크 동향은 하드웨어에 의존하지 않고, 자원을 보다 효율적으로 활용하기 위해서 가상화 기술을 도입하고 있다. 조직 및 기업이 가상화 기술을 도입함으로써, 효율적인 자원 활용과 인프라의 구축 및 관리의 간소화에 따라서 비용 절감 효과를 얻을 수 있기 때문이다.

[3] NFV(Network Functional Virtualization) 기술은 이러한 요구를 반영하기 위한 차세대 네트워크 가상화 기술이다. NFV는 네트워크 장비 내 여러 기능을 분리시켜, 소프트웨어적으로 제어 및 관리가 가능한 가상 시스템인 VNF(virtual network function)를 서버의 운영체제에 업로드시켜 활용한다. 물리적인 네트워크 장비의 기능을 가상화하여 가상 머신 서버 혹은 범용 프로세서를 탑재한 하드웨어에서 실행하는 방식을 사용한다. NFV 기술을 이용하면 논리적으로 네트워크를 구축할 수 있기 때문에 기존의 네트워크 변화에 유연하게 대응하는 것이 가능하다.

[4] 하지만 가상화된 기기의 수가 증가함에 따라서, NFV내 테넌트(Tenant)의 구성 및 설정이 변경될 때마다 각각의 가상화된 VNF의 설정 정보들을 관리자가 EM(Element Manager)을 이용하여 직접 관리하는 것은 인력과 CAPEX(capital expenditure) 및 OPEX(operating expense) 등의 소요 비용이 크다.

[5] 또한, 테넌트에 로드되는 VNF는 별도의 인증 과정을 거치지 않기 때문에 악의적인 목적을 가진 사용자가 악성 VNF를 로드시켜 전체 테넌트를 오염시킬 수 있다.

[6] 이에, 네트워크 변경에 따라 VNF 설정을 자동으로 관리해주고, 동적으로 구성된 테넌트 내 VNF 간의 인증을 수행하고 VNF 간 트래픽을 제어할 수 있는 기술 개발이 요구되고 있다.

[7] 이와 관련하여, 한국 공개특허공보 제10-2012-0065347호가 존재한다.

발명의 상세한 설명

기술적 과제

[8] 본 발명이 해결하고자 하는 기술적 과제는 테넌트 내 VNF 간의 인증을 수행하고, VNF 간 트래픽을 제어할 수 있는 NFV 환경에서 보안 통신 방법 및 그 시스템을 제공하는 것이다.

[9] 본 발명이 해결하고자 하는 다른 기술적 과제는 VNF 간의 안전한 통신을 보장할 수 있는 NFV 환경에서 보안 통신 방법 및 그 시스템을 제공하는 것이다.

[10] 본 발명이 해결하고자 하는 과제는 이상에서 언급한 과제(들)로 제한되지 않으며, 언급되지 않은 또 다른 과제(들)은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제 해결 수단

[11] 상기한 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 NFV 환경에서 보안 통신 방법은 NFV(network function virtualization) 환경에서 VNF(virtualized network function)간 보안 통신 방법에 있어서, 요소 관리자는 해시체인을 이용하여 제1 VNF와 제2 VNF간 인증을 수행하는 단계, 상기 인증 완료된 제1 VNF와 제2 VNF는 자신의 해시체인을 기반으로 비밀키를 각각 생성하는 단계, 상기 제1 VNF와 제2 VNF는 자신의 비밀키를 이용하여 통신을 수행하는 단계를 포함하는 NFV 환경에서 보안 통신 방법이 제공된다.

[12] 바람직하게는, 상기 인증을 수행하는 단계 이전에, VIM(Virtualized Infrastructure Manager)은 테넌트(Tenant)내의 VNF가 인스턴화될 때 VNF 이미지의 해시체인을 생성하여 상기 요소 관리자와 공유하는 단계를 더 포함할 수 있다.

[13] 바람직하게는, 상기 공유하는 단계는, 테넌트 식별정보, VNF 식별정보, 인스턴스 식별정보 중 적어도 하나를 조합하여 상기 테넌트내 VNF 식별정보(VNF_{ID})를 계산하는 단계, 상기 계산된 테넌트내 VNF 식별정보(VNF_{ID})를 해시함수에 적용하여 해시체인을 계산하고, 상기 계산된 해시체인을 상기 요소 관리자와 공유하는 단계, 상기 계산된 해시체인이 업데이트된 경우, 상기 업데이트된 해시체인을 상기 요소 관리자와 공유하는 단계를 포함할 수 있다.

[14] 바람직하게는, 상기 업데이트된 해시체인을 상기 요소 관리자와 공유하는 단계는, 해당 VNF 이미지가 수정/변경되거나 또는 주기적으로 이전 해시체인에 해시함수를 적용하여 해시체인을 업데이트하는 단계, 상기 업데이트된 해시체인을 상기 요소 관리자로 전송하는 단계를 포함할 수 있다.

[15] 바람직하게는, 상기 업데이트된 해시체인을 상기 요소 관리자로 전송하는 단계는, 상기 업데이트된 해시채널을 이전 해시체인을 암호화 키로 사용하는 대칭 암호화 알고리즘으로 암호화하여 상기 요소 관리자로 전송하는 것을 특징으로 할 수 있다.

[16] 바람직하게는, 상기 인증을 수행하는 단계는, 상기 제1 VNF로부터 초기(Initi) 메시지 수신 시, 상기 제2 VNF에 해시체인을 요청하여 수신하는 단계, 상기 수신된 제2 VNF의 해시체인을 기 저장된 제2 VNF 해시체인과 비교하여 상기 제2 VNF를 인증하는 단계, 상기 제2 VNF의 인증 완료시 상기 제1 VNF에 해시체인을 요청하여 수신하는 단계, 상기 수신된 제1 VNF의 해시체인을 기 저장된 제1 VNF 해시체인과 비교하여 상기 제1 VNF를 인증하는 단계, 상기 제1

VNF와 제2 VNF의 인증결과를 상기 제1VNF로 전송하는 단계를 포함할 수 있다.

[17] 바람직하게는, 상기 제2 VNF의 해시체인이, 상기 제2 VNF가 가장 최근 자신에게 할당된 해시체인을 암호화키로 사용하여 현재 자신에게 할당된 해시체인을 암호화한 해시체인인 경우, 상기 제2 VNF를 인증하는 단계는, 기 저장된 제2 VNF의 가장 최근 해시체인을 이용하여 상기 제2 VNF의 암호화된 해시체인을 복호화하고, 상기 복호화된 해시체인을 기 저장된 제2 VNF 해시체인과 비교하여 제2 VNF를 인증하고,

[18] 상기 제1 VNF의 해시체인이, 상기 제1 VNF가 가장 최근 자신에게 할당된 해시체인을 암호화키로 사용하여 현재 자신에게 할당된 해시체인을 암호화한 해시체인인 경우, 상기 제1 VNF를 인증하는 단계는, 기 저장된 제1 VNF의 가장 최근 해시체인을 이용하여 상기 제1 VNF의 암호화된 해시체인을 복호화하고, 상기 복호화된 해시체인을 기 저장된 제1 VNF 해시체인과 비교하여 제1 VNF를 인증할 수 있다.

[19] 바람직하게는, 상기 비밀키는, 해시체인을 기반으로 디피-헬만(Diffie-Hellman(D-H)) 알고리즘을 이용하여 생성될 수 있다.

[20] 바람직하게는, 상기 비밀키를 각각 생성하는 단계는, 상기 제1 VNF 및 제2 VNF는 각각 요소 관리자로부터 제1 정수(p) 및 제2 정수(q)를 수신하는 단계, 상기 제1 VNF 및 제2 VNF는 상기 수신된 제1 정수(p), 제2 정수(q) 및 자신의 해시체인을 이용하여 제1 공개키 및 제2 공개키를 생성하는 단계, 상기 제1 VNF는 제1 공개키를 상기 제2 VNF로 전달하고, 상기 제2 VNF는 제2 공개키를 상기 제1 VNF로 전달하는 단계, 상기 제1 VNF는 자신의 해시체인과 제2 공개키를 이용하여 제1 비밀키를 생성하고, 상기 제2 VNF는 자신의 해시체인과 제1 공개키를 이용하여 제2 비밀키를 생성하는 단계를 포함하되, 상기 해시체인이 개인키일 수 있다.

[21] 바람직하게는, 상기 통신을 수행하는 단계는, 상기 제1 VNF는 상기 제1 비밀키를 이용하여 메시지를 암호화하고, 상기 암호화된 메시지를 VNF-게이트웨이로 전송하는 단계, 상기 VNF-게이트웨이는 상기 메시지에 대한 설정정보를 획득하고, 상기 획득된 설정정보를 기 저장된 보안정책정보와 비교하여 두 정보가 일치하는 경우 상기 암호화된 메시지를 상기 제2 VNF로 전송하는 단계; 및

[22] 상기 제2 VNF는 상기 제2 비밀키를 이용하여 상기 암호화된 메시지를 복호화하는 단계를 포함할 수 있다.

[23] 바람직하게는, 상기 VNF-게이트웨이는 두 정보가 일치하지 않은 경우, 상기 암호화된 메시지를 차단할 수 있다.

[24] 상기한 기술적 과제를 해결하기 위하여, 본 발명의 다른 실시예에 따른 NFV 환경에서 보안 통신 시스템은, NFV(network function virtualization) 환경에서 복수의 VNF를 포함하는 테넌트(Tenant)내의 VNF 간 보안 통신을 위한 시스템에서 있어서, 상기 복수의 VNF에 각각 할당된 해시체인을 관리하며,

통신을 원하는 VNF들의 해시체인을 이용하여 해당 VNF들을 인증하는 요소 관리자, 상기 테넌트내 복수의 VNF 사이에 위치하고, VNF 트래픽에 대한 보안정책정보가 설정된 Sec-catalog를 설정하여 VNF 간의 트래픽을 제어하는 VFN 게이트웨이를 포함하며, 상기 요소 관리자에서 인증 완료된 VNF는 자신의 해시체인을 기반으로 비밀키를 생성하고, 상기 생성된 비밀키로 메시지를 암호화하여 상기 VNF 게이트웨이로 전송하며, 상기 VNF 게이트웨이로부터 암호화된 메시지 수신 시, 상기 비밀키를 이용하여 상기 암호화된 메시지를 복호화하고, 상기 VNF-게이트웨이는 상기 메시지에 대한 설정정보를 획득하고, 상기 획득된 설정정보를 상기 보안정책정보와 비교하여 두 정보가 일치하는 경우 상기 암호화된 메시지를 상대 VNF로 전송하는 것을 특징으로 한다.

[25] 바람직하게는, 상기 테넌트(Tenant)내의 VNF가 인스턴화될 때 VNF 이미지의 해시체인을 생성하여 상기 요소 관리자와 공유하는 VIM을 더 포함할 수 있다.

[26] 바람직하게는, 상기 VIM은, 상기 VNF 이미지가 수정/변경되거나 또는 주기적으로 이전 해시체인에 해시함수를 적용하여 해시체인을 업데이트하고, 상기 업데이트된 해시체인을 상기 요소 관리자와 공유할 수 있다.

발명의 효과

[27] 본 발명에 따르면, 테넌트내 VNF들이 통신을 수행하기 전에 해시체인을 이용하여 VNF간을 인증함으로써, 인증되지 않은 VNF를 식별할 수 있고, 이로 인해 테넌트가 오염되는 것을 막을 수 있다.

[28] 또한, 본 발명에 따르면, VPN 게이트웨이가 Sec-catalog의 보안정책정보를 이용하여 VNF간 트래픽을 제어함으로써, VNF간 악성 트래픽 전파 문제를 해결할 수 있으므로, 안전한 NFV 환경을 보장할 수 있다.

[29] 본 발명의 효과들은 이상에서 언급한 효과들로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[30] 도 1은 본 발명의 일 실시예에 따른 NFV 환경에서 보안 통신을 위한 시스템을 설명하기 위한 도면이다.

[31] 도 2는 본 발명의 일 실시예에 따른 VNF 게이트웨이의 위치를 설명하기 위한 도면이다.

[32] 도 3은 본 발명의 일 실시예에 따른 NFV 환경에서 보안 통신 방법을 설명하기 위한 도면이다.

[33] 도 4는 본 발명의 일 실시예에 따른 VIM이 해시체인을 생성 및 공유하는 방법을 나타낸 도면이다.

[34] 도 5는 본 발명의 일 실시예에 따른 VNF간 인증 방법을 설명하기 위한 도면이다.

[35] 도 6은 본 발명의 일 실시예에 따른 비밀키 생성 방법을 설명하기 위한

도면이다.

[36] 도 7은 본 발명의 일 실시예에 따른 VNF 게이트웨이의 트래픽 제어 방법을 설명하기 위한 도면이다.

[37] 도 8은 본 발명의 일 실시예에 따른 패킷 전송에 따른 CPU 사용률의 비교 그래프이다.

[38] 도 9는 본 발명의 일 실시예에 따른 VNF간 패킷 전송률을 비교한 그래프이다.

[39] 도 10은 본 발명의 일 실시예에 따른 TCP 패킷 flooding에 대한 VNF-게이트웨이의 shaping 시험 결과를 나타낸 그래프이다.

발명의 실시를 위한 형태

[40] 이하, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 정도로 상세히 설명하기 위하여, 본 발명의 가장 바람직한 실시예를 첨부 도면을 참조하여 설명하기로 한다. 우선 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[41] 이하에서는 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[42] 도 1은 본 발명의 일 실시예에 따른 NFV 환경에서 보안 통신을 위한 시스템을 설명하기 위한 도면, 도 2는 본 발명의 일 실시예에 따른 VNF 게이트웨이의 위치를 설명하기 위한 도면이다.

[43] 도 1을 참조하면, 본 발명의 일 실시예에 따른 NFV 환경에서 보안 통신을 위한 시스템은 테넌트 내 VNF 간의 인증과 VNF간 트래픽 제어를 통해 보안 통신을 가능하게 하는 시스템으로, OSS(Operation Service Systems)/BSS(Business Service Systems), Sec-EM(Element Manager), 적어도 하나 이상의 VNF(Virtual Network Function)를 포함하는 적어도 하나 이상의 테넌트(Tenant), NFVI(Network Function Virtualization Infrastructure) 및 NFV MANO(Management & Orchestration)를 포함한다.

[44] VNF는 서버 상의 가상 머신(VM)에서 동작하는 애플리케이션(들) 등에 대응하며, 네트워크 기능을 소프트웨어적으로 실현한다. VNF로서, 예를 들면 LTE(Long Term Evolution) 네트워크의 코어 망인 EPC(Evolved Packet Core)에 있어서의 MME(Mobility Management Entity)나 S-GW(Serving Gateway), P-GW(PDN Gateway) 등을 소프트웨어(가상 머신)로 실현하도록 해도 된다.

[45] OSS(Operation Service Systems)는, 예를 들면 통신사업자(캐리어)가 서비스를 구축하고, 운영해 가기 위해서 필요한 시스템(기기나 소프트웨어, 구조 등)을 총칭한 것이다. BSS(Business Service Systems)는, 예를 들면

통신사업자(캐리어)가 이용료 등의 과금, 청구, 고객 대응 등을 위해 사용하는 정보 시스템(기기나 소프트웨어, 구조 등)의 총칭이다.

[46] Sec-EM은 테넌트에 포함된 VNF들을 관리한다.

[47] 구체적으로, Sec-EM은 VNF 이미지의 해시체인(Hash-Chain)을 사용하여 테넌트 내 VNF간의 인증을 수행하여 악성 VNF를 식별한다. 즉, Sec-EM은 테넌트에 포함된 VNF들의 해시체인을 VIM으로부터 수신하여 저장하고 있으므로, 통신을 원하는 제1 VNF와 제2 VNF의 해시체인을 이용하여 제1 VNF와 제2 VNF를 인증한다.

[48] 이처럼 Sec-EM은 VNF 통신 수행 전에 해시체인의 보관 여부를 통해서 통신을 수행하는 각 VNF가 악성 VNF인지 식별한다.

[49] 인증완료된 VNF는 자신의 해시체인을 기반으로 비밀키를 생성하고, 그 비밀키를 이용하여 메시지를 암호화하여 VNF간 통신을 수행한다. 이때, VNF는 VNF 게이트웨이를 통해 통신을 수행하는데, VNF 게이트웨이는 기 저장된 보안정책정보를 이용하여 VNF간의 트래픽을 제어한다.

[50] VNF 게이트웨이(VNF-G/W)는 도 2에 도시된 바와 같이 각 테넌트 내의 VNF 사이에 위치하고, VNF 트래픽에 대한 보안 정책이 설정된 Sec-catalog를 설정하여 VNF 간의 악성 트래픽을 이용한 DDoS 공격을 화이트리스트 기반으로 탐지 및 예방한다.

[51] VNF-게이트웨이는 Sec-catalog에서 트래픽 정보를 수신하고 VNF간에 전송되는 트래픽을 제어한다. Sec-catalog가 VNF-게이트웨이에 반영될 때, Sec-catalog에 설정된 보안정책정보와 다른 트래픽은 공격으로 간주될 수 있고 QoS(Quality of Service) 레벨은 낮아질 수 있으며, 전송 대역폭 트래픽을 줄일 수 있다. 따라서, VNF-게이트웨이의 보안정책을 이용한 트래픽 제어 기술을 이용함으로써, VNF간의 비정상적인 트래픽 패턴을 탐지하고 정보 유출 사고를 예방할 수 있다. 예를들어 공격자가 제1 VNF에서 제2 VNF로 많은 양의 트래픽을 전송하여 플러딩 공격으로 제2 VNF에서 실행중인 서버를 중단시키면, VNF-게이트웨이가 트래픽을 제어함으로써 사고를 예방할 수 있다. 또한 개인 ID 또는 주소 등 중요한 정보가 VNF를 사용하는 서버에 저장된 경우, VNF 게이트웨이는 해당 VNF로부터 외부로 많은 양의 트래픽 흐름을 감지하고, 새벽에 데이터를 전송하는 것과 같은 비정상적인 패턴을 분석함으로써, 정보 유출을 방지할 수 있다.

[52] NFVI(Network Function Virtualization Infrastructure)는 VNF의 실행 인프라스트럭처로, 컴퓨팅, 스토리지, 네트워크 기능 등, 물리 머신(서버)의 하드웨어 자원을 하이퍼바이저 등의 가상화 레이어로 가상화한 가상화 컴퓨팅, 가상화 스토리지, 가상화 네트워크 등의 가상화 하드웨어 자원으로서 유연하게 취급할 수 있도록 한 인프라스트럭처이다.

[53] NFV-MANO는 NFVI를 관리하고 VNF 인스턴스에 대한 자원들의 할당을 편성하도록 기능을 수행한다. 이러한 NFV MANO(Management &

Orchestration)는 NFVO(NFV-Orchestrator), VNFM(VNF-Manager), VIM(Virtualized Infrastructure Manager)을 포함한다.

[54] NFVO(NFV-Orchestrator)는 NFVI 리소스의 오케스트레이션, 및 NS(Network Service)의 라이프 사이클 관리(NS 인스턴스의 인스턴시에이션, 스케일링, 종료, 갱신 등)을 행한다. 또한, NFVO는 VNF 카탈로그와 Sec-카탈로그의 관리를 행한다.

[55] VNF 카탈로그(VNF catalog)는 VNF 패키지의 리포지토리를 나타내는 것으로, VNFD(VNF Descriptor), 소프트웨어 이미지, 매니페스트 파일 등의 VNF 패키지의 생성과 관리의 지원을 행한다. Sec-catalog에는 인스턴스화된(또는 등록된) VNF의 프로토콜, 포트 번호, Ingress Policing rate, Ingress Policing Burst 등의 정보가 저장된다.

[56] NFVO는 VNF 인스턴스화 프로세스 중에 VNFD(VNF Descriptor)를 VNF 카탈로그에 등록하고, VNFD가 VNF 카탈로그에 등록되면 Sec-카탈로그를 등록한다. 이때 등록된 VNF 카탈로그와 Sec-카탈로그의 설정정보는 VNF 게이트웨이에 적용된다.

[57] VNFM(VNF-Manager)은 VNF의 라이프 사이클 관리(인스턴시에이션, 갱신, 검색, 스케일링, 종료, (어시스티드/오토) 힐링 등) 및 이벤트 통지를 행한다.

[58] VIM(Virtualized Infrastructure Manager)은 가상화 레이어를 통해, NFVI를 제어한다(컴퓨팅, 스토리지, 네트워크의 리소스 관리, NFV의 실행 인프라스트럭쳐인 NFVI의 장해 감시, 리소스 정보의 감시 등).

[59] VIM는 테넌트 내의 각 VNF가 인스턴스화될 때, VNF 이미지의 해시체인을 생성한다. 또한, VIM은 VNF의 해시체인을 주기적으로 업데이트하거나, 해당 VNF가 수정/변경될 때 업데이트한다. 이때, VIM은 바로 직전(최신)에 생성된 해시체인에 해시함수를 적용하여 해시체인을 업데이트할 수 있다. VIM은 생성 또는 업데이트된 VNF의 해시체인을 Sec-EM과 공유한다.

[60] 참조 포인트 Os-Ma는 OSS(Operation Service Systems)/BSS(Business Service Systems)와 NFVO간의 참조 포인트이며, 네트워크 서비스의 라이프 사이클 관리 요구, VNF 라이프 사이클 관리 요구, NFV 관련 상태 정보의 전송, 폴리시 관리 정보의 교환 등에 이용된다.

[61] 참조 포인트 Vi-Vnfm는 VNFM으로부터의 리소스 할당 요구, 가상화 리소스의 구성과 상태 정보의 교환에 이용된다.

[62] 참조 포인트 Ve-Vnfm은 EM과 VNFM간에서의 VNF 인스턴시에이션, VNF 인스턴스 검색, 갱신, 종료, 스케일 아웃/인, 스케일 업/다운, EM으로부터 VNFM에의 구성, 이벤트의 전송, VNFM으로부터 VNF에의 VNF의 구성, 이벤트의 통지 등에 이용된다.

[63] 참조 포인트 Nf-Vi는 컴퓨팅, 스토리지, 네트워크 리소스 관리의 지시와 함께 VM의 할당, VM 리소스 할당의 갱신, VM 마이그레이션, VM 종료, VM간의 접속의 생성·제거 등, 리소스 할당 요구에 대한 가상화 리소스의 할당, 가상화

리소스의 상태 정보의 전송, 하드웨어 자원의 구성과 상태 정보의 교환 등에 이용된다.

[64] 참조 포인트 Or-Vnfm은 VNFM(VNF-Manager)에 의한 리소스 관련 요구(인증, 예약, 할당 등), VNFM에의 구성 정보의 전송, VNF의 상태 정보의 수집에 이용된다.

[65] 이하, 상기와 같이 구성된 시스템에서 VNF를 등록하는 과정에 대해 설명하기로 한다.

[66] NFVO는 송신자 인증 및/또는 인스턴스화 파라미터를 점검함으로써 요청을 유효화하고, 실행가능성 점검을 실행할 수 있다. 요청이 성공적으로 유효화되면, NFVO는 VNF를 인스턴스화하기 위해 VNFM을 호출한다. VNFM는 요청을 유효화하고 인스턴스화 파라미터를 프로세싱한다. VNFM은 이어서 리소스 할당을 위한 요청을 NFVO에 송신한다. NFVO는 임의의 요구된 리소스 사전할당을 실행하고, 이어서 리소스 할당을 위해 VIM에 요청을 송신한다. 예를 들어, 프로세서 사용량 카운터가 사전결정된 임계치를 초과하면, VIM은 더 많은 컴퓨팅 및 저장 리소스를 할당한다.

[67] 리소스 할당을 위한 요청에 응답하여, VIM은 요청된 컴퓨팅, 저장 및/또는 네트워킹 리소스를 할당하고, 확인응답(acknowledgement)을 NFVO에 송신한다. NFVO는 리소스 할당의 완료를 지시하기 위해 VNFM에 확인응답을 송신한다. VNFM은 이어서 VNF를 인스턴스화하고, 임의의 VNF 특정 수명주기 파라미터를 갖는 VNF를 구성한다. VNFM은 새로운 VNF를 Sec-EM에 통지한다. Sec-EM은 이어서 해당 VM 동작을 위해 요구된 정보를 갖는 VNF를 구성한다. VNFM은 NFV로의 새로운 VNF 인스턴스의 성공적인 추가를 보고한다. NFVO는 새로운 인스턴스 기술자로 VNF 카탈로그와 Sec-카탈로그를 업데이트한다. Sec-EM은 새로운 VNF를 OSS/BSS에 통지한다. OSS/BSS는 새로운 VNF의 성공적인 인스턴스화를 확인응답한다.

[68] 한편, VIM는 테넌트 내의 각 VNF가 인스턴스화될 때, VNF 이미지의 해시체인을 생성하고, 생성된 해시체인을 Sec-EM 또는 해당 VFM과 공유한다.

[69] 본 발명은 상기와 같이 등록된 VNF가 해당 테넌트 내의 다른 VNF와 통신을 수행하고자 하는 경우 VNF 간의 인증을 수행하고, 보안통신을 가능하게 한다.

[70] 이하, 테넌트내 제1 VNF가 제2 VNF와 통신을 원한다고 가정하여 VNF 간 보안 통신 방법에 대해 설명하기로 한다.

[71] 도 3은 본 발명의 일 실시예에 따른 NFV 환경에서 보안 통신 방법을 설명하기 위한 도면이다.

[72] 도 3을 참조하면, 제1 VNF는 제2 VNF와 통신을 수행하기 전에 Sec-EM을 통해 제1 VNF와 제2 VNF간 인증을 수행한다(S310). 즉, VIM은 테넌트 내의 각 VNF가 인스턴화될 때 VNF 이미지의 해시체인을 생성하여 Sec-EM와 공유한다. 그러면, Sec-EM은 테넌트에 포함된 VNF들의 해시체인을 VIM으로부터 수신하여 저장하고 있으므로, 통신을 원하는 제1 VNF와 제2 VNF의 해시체인을 이용하여

테넌트의 제1 VNF와 제2 VNF간 인증을 수행하여 악성 VNF를 식별할 수 있다.

[73] VIM이 해시체인을 생성하여 Sec-EM과 공유하는 방법에 대한 상세한 설명은 도 4를 참조하기로 하고, Sec-EM이 제1 VNF와 제2 VNF간 인증하는 방법에 대한 상세한 설명은 도 5를 참조하기로 한다.

[74] 단계 S310이 수행되면, 제1 VNF는 자신의 해시체인을 기반으로 비밀키를 생성하고(S320), 그 비밀키를 이용하여 메시지를 암호화하며(S330), 암호화된 메시지를 VNF-게이트웨이로 전송한다(S340). 이때, 제1 VNF는 해시체인을 기반으로 비밀키 암호화 알고리즘을 이용하여 비밀키를 생성할 수 있고, 비밀키 암호화 알고리즘은 예컨대, 디피-헬만 알고리즘(Diffie-Hellman Algorithm)일 수 있다. 디피-헬만 알고리즘은 두 VNF가 사전에 어떠한 비밀 교환 없이도 공중 통신망 환경에서 공통키를 교환하게 해주는 알고리즘으로, 공개키(Public Key)와 개인키(Private Key)를 이용하여 비밀키(Secret Key)를 생성한다. 공개키(Public Key)는 외부로 공개되는 키이고, 개인키(Private Key)는 개인이 소유하고 외부로는 알리지 않는 키로, 자신의 해시체인일 수 있다. 비밀키(Secret Key)는 실제 암호화에 사용하는 키로, 두 VNF는 동일한 비밀키를 이용하여 특정 데이터를 암호화하여 서로 송수신할 수 있다.

[75] 제1 VNF가 비밀키를 생성할 때 제2 VNF도 자신의 해시체인을 기반으로 비밀키를 생성한다. VNF가 해시체인을 기반으로 비밀키를 생성하는 방법에 대한 상세한 설명은 도 6을 참조하기로 한다.

[76] 단계 S340이 수행되면, VNF-게이트웨이는 암호화된 메시지의 설정정보를 획득하고(S350), 획득된 설정정보를 기 저장된 보안정책정보와 비교하여(S360), 두 정보의 동일 여부를 판단한다(S370). 이때, VNF-게이트웨이는 제1 VNF에 대한 보안정책이 설정된 Sec-catalog로부터 보안정책정보를 수신하고, 그 보안정책정보를 메시지의 설정정보와 비교할 수 있다.

[77] 단계 S370의 판단결과 두 정보가 동일한 경우 VNF-게이트웨이는 암호화된 메시지를 제2 VNF로 전송한다(S380). 그러면, 제2 VNF는 제1 VNF가 비밀키를 생성할 때 함께 생성한 비밀키를 이용하여 암호화된 메시지를 복호화한다(S390).

[78] 만약, 단계 S370의 판단결과 두 정보가 동일하지 않으면, VNF-게이트웨이는 암호화된 메시지를 차단한다(S385). 이처럼 VNF-게이트웨이는 두 설정정보가 일치하는 트래픽은 허용하고, 일치하지 않은 트래픽은 제어한다. VNF 게이트웨이가 보안정책정보에 따라 트래픽을 제어하는 방법에 대한 상세한 설명은 도 7을 참조하기로 한다.

[79] 상술한 과정을 통해, 인증되지 않은 VNF를 식별할 수 있고, VNF간 악성 트래픽 전파 문제를 해결할 수 있으므로, 안전한 NFV 환경을 보장할 수 있다.

[80] 도 4는 본 발명의 일 실시예에 따른 VIM이 해시체인을 생성 및 공유하는 방법을 나타낸 도면이다.

[81] 도 4를 참조하면, VIM은 VNF 식별을 위해 테넌트내 VNF 식별정보(VNF_{ID})를

계산한다(S410). 이때, VIM은 해당 VNF가 포함된 테넌트 식별정보(Tenant_ID), VNF 식별정보(VNF ID), 인스턴스 식별정보(Instance_ID) 등을 조합하여 해당 테넌트내 VNF 식별정보(VNF_{ID})를 계산한다.

[82] 그런 후, VIM은 테넌트내 VNF 식별정보(VNF_{ID})를 이용하여 VNF 이미지의 해시값을 계산한다(S420). 즉, VIM은 테넌트내 VNF 식별정보(VNF_{ID})를 해시함수에 적용하여 VNF 이미지의 해시값을 계산할 수 있다. 해시값은 바로 직전(가장 최신)의 해시값을 이용하여 업데이트되므로, 해시값은 해시체인과 동일한 의미일 수 있다.

[83] 해시함수는 임의 길이의 데이터를 고정 길이의 데이터에 매핑하는 것이고, 하나의 함수가 아니기 때문에, 작업을 되돌릴 수 없다. 따라서 해시값을 알고있는 사람일지라도 해시함수의 입력을 찾을 수 없다. 또한 동일한 해시값을 가진 경우라도 동일한 입력값이라고 보증할 수 없다. 원 입력의 한 비트만 변경되더라도 해시값은 해시함수로 인해 크게 달라지게 된다. 이러한 해시함수에는 예컨대, MD5, CRC32, SHA-type 등 다양할 수 있다.

[84] 해시체인(Hash-Chain)은 클라이언트가 설정한 임의의 값인 'seed'를 연속적으로 사용하여 해시값을 계산하는 방식이다. 즉, 길이 n을 갖는 해시체인을 생성하기 위해, x(시드)는 해시함수 h(x)의 입력으로 사용된다. 이 프로세스를 반복적으로 사용하여 루트 값 $h^{n+1}(x)$를 계산할 수 있다. 따라서 해시체인으로 패스워드를 생성하는 프로그램이 해시체인을 서버에 송신하면, 공격자는 전송 프로세스를 도청하여 $h^{n}(x)$을 알고 있더라도 $h^{n-1}(x)$을 계산할 수 없다. 이러한 해시의 보안 특성을 사용하면 클라이언트-서버 인증 과정에서 One-Time Password의 해시체인이 생성된다.

[85] 단계 S420의 수행 후, 해시체인이 업데이트되면(S430), VIM은 업데이트된 해시체인을 Sec-EM와 공유한다(S440). VIM은 해당 VNF 이미지가 수정/변경될 때 해시체인을 업데이트한다. 즉, VIM은 초기에 VNF_{ID}를 이용하여 해쉬값($Hash(VNF_{ID})$)를 생성한 후, VM의 정지/중지 등이 발생하게 되면, VNF 이미지를 다시 등록해야 하고, VNF 이미지를 다시 등록해야 하는 상황은 VNF 이미지가 수정/변경된 경우라 할수 있다. 따라서, VIM은 VNF 이미지가 수정/변경되면, 아래 수학식 1과 같이 이전(최신)의 해시체인($Hash(VNF_{ID})$)에 해시함수를 적용하여 해시체인을 업데이트한다.

[86] [수학식 1]

[87] $$Hash^{2}(VNF_{ID})=Hash(Hash(VNF_{ID}))$$

[88] 이처럼, VIM은 이전에 계산된 해시체인을 해시함수에 적용하여 해시체인을 업데이트할 수 있다. 이는 아래 수학식 2과 같이 표현할 수 있다.

[89] [수학식 2]

[90] $$Hash^{n}(VNF_{ID})=Hash(Hash^{n-1}(VNF_{ID}))$$

[91] 여기서, n은 0보다 큰 정수일 수 있다. 수학식 2를 보면, n번째 해시체인을

생성하기 위해서는 n-1번째 해시체인이 있어야 한다.

[92] 살핀바와 같이 VIM은 VNF 이미지의 해시체인을 생성하고, VIM과 Sec-EM은 VNF 이미지 등록(on-boarding) 및 인스턴스화 후 VNF의 해시값을 공유한다.

[93] 또한, VNF가 실행 중일 때 VNF 이미지의 해시값은 변경된다. 따라서 VIM은 아래 수학식 3과 같이 VNF의 해시체인을 주기적으로 업데이트한다.

[94] [수학식 3]

[95] $E_{Hash^{n-1}(VNF)}\{Hash^{n}(VNF_{ID})\}$

[96] 업데이트된 해시체인을 Sec-EM과 공유하기 위해 업데이트된 해시체인은 이전 해시체인을 암호화 키로 사용하는 대칭 암호화 알고리즘(symmetric encipherment algorithm)을 사용하여 공유된다. 대칭 암호화 알고리즘은 암호화와 복호화에 동일한 키를 사용하는 암호 알고리즘으로, 비밀키(이전 해시체인)를 모르면 암호화된 데이터를 복호화하는 것이 계산적으로 불가능하다.

[97] 또한, VNF 이미지는 VIM로부터 VNFM를 통해 업데이트된 해시체인을 공유하게 된다.

[98] 살핀바와 같이 VIM은 VNF 이미지가 수정/변경되거나 또는 주기적으로 VNF의 해시채널을 업데이트하고, 업데이트된 해시채널을 이전 해시체인을 암호화 키로 사용하는 대칭 암호화 알고리즘을 사용하여 Sec-EM과 공유한다. 이처럼, 대칭 암호화 알고리즘을 사용하여 해시체인을 공유함으로써, 이전 해쉬체인을 알지 못하면 업데이트된 해시체인을 복호화할수 없다.

[99] 도 5는 본 발명의 일 실시예에 따른 VNF간 인증 방법을 설명하기 위한 도면이다.

[100] 도 5를 참조하면, 제1 VNF가 제2 VNF와 통신을 원한 경우 제1 VNF는 초기(Initi) 메시지를 Sec-EM으로 전송한다(S510). 즉, 제1 VNF는 통신을 수행하기 전에 제1 VNF와 제2 VNF가 악성 VNF인지 판단하기 위해 Sec-EM으로 초기 메시지를 전송한다. 이때, 초기 메시지는 자신의 ID(ID_{VNF1}), 제2 VNF의 식별정보(ID_{VNF2}), 인증에 필요한 챌린지값(CH) 등을 포함할 수 있다.

[101] 단계 S510이 수행되면, Sec-EM은 제2 VNF 해시체인 요청 메시지를 제2 VNF로 전송하고(S520), 제2 VNF는 제2 VNF 해시체인을 Sec-EM로 전송한다(S530). 여기서, 제2 VNF 해시체인 요청 메시지는 제2 VNF 식별정보(ID_{VNF2}), 챌린지(CH) 등을 포함한다. 제2 VNF는 업데이트된 해시체인을 보관하고 있으므로, 자신의 해시체인인 $E_{Hashn-1}\{Hash^{n}(VNF_2)\}$를 Sec-EM으로 전송할 수 있다. 이때, $E_{Hashn-1}\{Hash^{n}(VNF_2)\}$는 가장 최근에 업데이트되어 VIM으로부터 공유된 해시체인일 수 있다.

[102] 단계 S530이 수행되면, Sec-EM은 수신된 제2 VNF의 해시체인을 기 저장된 제2 VNF 해시체인과 비교하여 제2 VNF를 인증한다(S540). 즉, Sec-EM은 수신된 제2 VNF의 해시체인이 기 저장된 제2 VNF 해시체인과 동일한 경우 인증된 VNF로 식별하고, 동일하지 않은 경우 악성 VNF로 식별할 수 있다. 제2 VNF의 n번째 해시체인은 n-1번째 해시체인으로 암호화되므로, 해시체인이 주기적으로

업데이트되지 않으면 n번째 해시체인을 복호화할 수 없다.

[103] 제2 VNF의 인증이 완료되면, Sec-EM은 제1 VNF 해시체인 요청 메시지를 제1 VNF로 전송하고(S550), 제1 VNF는 제1 VNF 해시체인을 Sec-EM으로 전송한다(S560). 여기서, 제1 VNF 해시체인 요청 메시지는 제1 VNF 식별정보(ID_{VNF1}), 챌린지(CH) 등을 포함한다. 제1 VNF는 업데이트된 해시체인을 보관하고 있으므로, 자신의 해시체인인 $E_{Hashn-1}\{Hash^n(VNF_1)\}$를 Sec-EM으로 전송할 수 있다. 이때, $E_{Hashn-1}\{Hash^n(VNF_1)\}$는 가장 최근에 업데이트되어 VIM으로부터 공유된 해시체인일 수 있다.

[104] 단계 S560이 수행되면, Sec-EM은 수신된 제1 VNF의 해시체인을 기 저장된 제1 VNF 해시체인과 비교하여 제1 VNF를 인증한다(S570). 즉, Sec-EM은 수신된 제1 VNF의 해쉬체인이 기 저장된 제1 VNF 해쉬체인과 동일한 경우 인증된 VNF로 식별하고, 동일하지 않은 경우 악성 VNF로 식별할 수 있다. 제1 VNF의 n번째 해시체인은 n-1번째 해시체인으로 암호화되므로, 해시체인이 주기적으로 업데이트되지 않으면 n번째 해시체인을 복호화할 수 없다.

[105] 단계 S570이 수행되면, Sec-EM은 인증 결과를 제1 VNF로 전송한다(S580). 여기서, 인증 결과는 제1 VNF의 악성 여부, 제2 VNF의 악성 여부 등을 포함할 수 있다. 따라서, 제1 VNF는 제1 VNF와 제2 VNF가 모두 인증된 VNF인 경우 제2 VNF와 통신을 수행하고, 제1 VNF와 제2 VNF 중 하나라도 악성 VNF로 식별된 경우 제2 VNF와 통신을 수행할 수 없다.

[106] 한편, 제1 VNF와 제2 VNF는 이전 해시체인을 암호화키로 사용하여 현재 자신의 해시체인을 암호화하여 Sec-EM으로 전송할 수 있고, Sec-EM은 이전 해시체인을 이용하여 암호화된 해시체인을 복호화할 수 있다. 따라서, 해시체인이 주기적으로 업데이트되지 않으면 현재의 해시체인을 복호화할 수 없다.

[107] 상술한 과정을 통해 Sec-EM과 VNF사이 뿐만아니라 VNF 사이에서도 인증을 수행할 수 있다.

[108] 도 6은 본 발명의 일 실시예에 따른 비밀키 생성 방법을 설명하기 위한 도면이다. 여기서는 디피-헬만(D-H) 알고리즘을 이용하여 비밀키를 생성하는 경우에 대해 설명하기로 한다.

[109] 도 6을 참조하면, 제1 및 제2 VNF는 각각 Sec-EM으로부터 임의의 제1 정수(p) 및 제2 정수(q)를 수신한다(S610). 여기서, p는 D-H 연산에 사용되는 소수로, 300보다 큰 정수 일 수 있고, q는 D-H 연산에 사용되는 기본값을 나타내는 특별한 수로, 1과 (p-1) 사이의 정수일 수 있다.

[110] 단계 S610이 수행되면, 제1 및 제2 VNF는 각각 자신의 해시체인을 이용하여 공개키를 생성한다(S620). 디피-헬만 알고리즘에서 공개키는 p, q 및 개인키를 이용하여 생성된 것이고, VNF의 개인키는 해시체인일 수 있다. 즉, 제1 VNF의 개인키는 자신의 해시체인이고, 제2 VNF의 개인키는 자신의 해시체인일 수 있다. 제1 및 제2 VNF의 해시체인은 100디지트 보다 더 큰 정수일 수 있다.

[111] 따라서, 제1 VNF는 p 및 q, 자신의 해쉬체인을 이용하여 제1 공개키(R_i)을 생성하고, 제2 VNF는 p 및 q, 자신의 해쉬체인을 이용하여 제2 공개키(R_j)를 생성한다. 여기서, i와 j는 VNF를 식별하는 번호이나, 이하에서는 설명의 편의를 위해 i는 제1 VNF, j는 제2 VNF로 칭하여 설명하기로 한다.

[112] 제1 VNF는 아래 수학식 4를 이용하여 제1 공개키(R_i)를 생성하고, 제2 VNF는 아래 수학식 5를 이용하여 제2 공개키(R_j)를 생성한다.

[113] [수학식 4]

[114] $$R_i = q^{Hash^n(VNF_i)} \bmod p$$

[115] 여기서, $Hash^n(VNF_i)$는 제1 VNF의 해쉬체인을 의미한다.

[116] [수학식 5]

[117] $$R_j = q^{Hash^n(VNF_j)} \bmod p$$

[118] 여기서, $Hash^n(VNF_j)$는 제2 VNF의 해쉬체인을 의미한다.

[119] 단계 S620이 수행되면, 제1 및 제2 VNF는 각각 자신의 공개키를 공유한다(S630). 즉, 제1 VNF는 제1 공개키를 제2 VNF에 전달하고, 제2 VNF는 제2 공개키를 제1 VNF에 전달한다.

[120] 단계 S630이 수행되면, 제1 및 제2 VNF는 각각 전달받은 상대 공개키와 자신의 해시체인(개인키)를 이용하여 비밀키를 생성한다(S640). 즉, 제1 VNF는 제2 VNF로부터 전달받은 제2 공개키와 자신의 해쉬체인을 이용하여 제1 비밀키를 생성하고, 제2 VNF는 제1 VNF로부터 전달받은 제1 공개키와 자신의 해쉬체인을 이용하여 제2 비밀키를 생성한다.

[121] 제1 VNF는 아래 수학식 6을 이용하여 제1 비밀키($K_{VNF_{ij}}$)를 생성하고, 제2 VNF는 아래 수학식 7을 이용하여 제2 비밀키($K_{VNF_{ij}}$)를 생성한다.

[122] [수학식 6]

[123] $$K_{VNF_{ij}} = R_i^{Hash^n(VNF_j)} \bmod p = \{ q^{HashN(VNF_i)} \}^{Hash^n(VNF_j)} \bmod p$$

[124] [수학식 7]

[125] $$K_{VNF_{ij}} = R_j^{Hash^n(VNF_i)} \bmod p = \{ q^{HashN(VNF_j)} \}^{Hash^n(VNF_i)} \bmod p$$

[126] 수학식 6과 수학식 7을 살펴보면, 두 수학식이 동일하다. 이를 통해 제1 비밀키와 제2 비밀키는 동일하다는 것을 알 수 있다. 따라서, 제1 VNF가 제1 비밀키를 이용하여 메시지를 암호화하여 제2 VNF로 전송하면, 제2 VNF는 제2 비밀키를 이용하여 암호화된 메시지를 복호화할 수 있다.

[127] 한편, p가 충분히 크기 때문에, 공격자가 암호화된 메시지를 복호화하기 위한 키를 찾으려는 경우 제1 공개키($q^{Hash^n(VNF_i)}$) 또는 제2 공개키($q^{Hash^n(VNF_j)}$)를

통해 비밀키를 찾을 수 없다. 따라서, 이러한 제1 VNF와 제2 VNF는 비밀키(K_{VNF_ij})를 사용하여 보안 통신을 보장할 수 있다. 결론적으로, 제1 VNF와 제2 VNF가 D-H 알고리즘으로 생성한 비밀키는 동일하기 때문에 이를 암호화에 사용할 수 있다.

[128] 도 7은 본 발명의 일 실시예에 따른 VNF 게이트웨이의 트래픽 제어 방법을 설명하기 위한 도면이다.

[129] 도 7을 참조하면, VNF 게이트웨이는 제1 VNF로부터 암호화된 메시지가 수신되면(S710), 그 메시지에 대한 설정정보를 획득한다(S720). 이때, VNF 게이트웨이는 기 설정된 보안정책정보에 해당하는 설정정보를 획득한다. 보안정책정보는 Sec-카달로그에 설정된 정보로, 예컨대, 프로토콜, 포트번호, Ingress Ploicing Rate 등을 포함할 수 있다.

[130] 단계 S720이 수행되면, VNF 게이트웨이는 획득된 포트 번호가 Sec-카달로그내의 포트번호와 동일한지를 판단한다(S730).

[131] 단계 S730의 판단결과 포트번호가 동일하면, VNF 게이트웨이는 획득된 프로토콜이 Sec-카달로그내의 프로토콜과 동일한지를 판단한다(S740).

[132] 단계 S740의 판단결과 프로토콜이 동일하면, VNF 게이트웨이는 획득된 Ingress Policing Rate이 Sec-카달로그내의 Ingress Policing Rate와 동일한지를 판단한다(S750).

[133] 단계 S750의 판단결과 두 Ingress Policing Rate가 동일하면, VNF 게이트웨이는 암호화된 메시지를 제2 VNF로 전송한다(S760).

[134] 만약, 단계 S730의 판단결과 포트번호가 동일하지 않으면, VNF 게이트웨이는 암호화된 메시지를 제2 VNF로 전송하지 않는다(S770). 즉, 포트번호가 동일하지 않으면, VNF 게이트웨이는 그 메시지를 악성 트래픽으로 판단하여 제어할 수 있다.

[135] 단계 S740의 판단결과 프로토콜이 동일하지 않으면, VNF 게이트웨이는 암호화된 메시지를 제2 VNF로 전송하지 않는다(S770). 즉, 프로토콜이 동일하지 않으면, VNF 게이트웨이는 그 메시지를 악성 트래픽으로 판단하여 제어할 수 있다.

[136] 단계 S750의 판단결과 두 Ingress Policing Rate가 동일하지 않으면, VNF 게이트웨이는 암호화된 메시지를 제2 VNF로 전송하지 않는다(S770). 즉, 두 Ingress Policing Rate이 동일하지 않으면, VNF 게이트웨이는 그 메시지를 악성 트래픽으로 판단하여 제어할 수 있다.

[137] 상술한 바와 같이 VNF-게이트웨이는 Sec-catalog에서 보안정책정보를 수신하고 VNF간에 전송되는 트래픽을 제어할 수 있다. Sec-catalog가 VNF-게이트웨이에 반영될 때, Sec-catalog에 설정된 보안정책정보와 다른 트래픽은 공격으로 간주될 수 있고 QoS(Quality of Service) 레벨은 낮아질 수 있으며, 전송 대역폭 트래픽을 줄일 수 있다. 따라서, VNF-게이트웨이의 보안 정책을 이용한 트래픽 제어 기술을 이용함으로써, VNF간의 비정상적인 트래픽

패턴을 탐지하고 정보 유출 사고를 예방할 수 있다. 예를들어 공격자가 제1 VNF에서 제2 VNF로 많은 양의 트래픽을 전송하여 플러딩 공격으로 제2 VNF에서 실행중인 서버를 중단시키면, VNF-게이트웨이가 트래픽을 제어함으로써 사고를 예방할 수 있다. 또한 개인 ID 또는 주소 등 중요한 정보가 VNF를 사용하는 서버에 저장된 경우, VNF 게이트웨이는 해당 VNF로부터 외부로 많은 양의 트래픽 흐름을 감지하고, 새벽에 데이터를 전송하는 것과 같은 사용자의 비정상적인 패턴을 분석함으로써, 정보 유출을 방지할 수 있다.

[138] 이하, 본 발명에 따른 시스템 성능에 대해 실험 결과를 이용하여 설명하기로 한다. 본 발명의 시스템(이하 ASMN라 칭함)의 성능 평가를 위해 하나의 테넌트에 VNF-게이트웨이 및 VNF 클라이언트, VNF 서버를 구성하였다.

[139] 도 8은 본 발명의 일 실시예에 따른 패킷 전송에 따른 CPU 사용률의 비교 그래프이다. 도 8은 ICMP, TCP 및 UDP 프로토콜에서 25초동안 패킷을 전송하여 CPU 사용률을 체크한 것이다. 도 8을 참조하면, ICMP, TCP, UDP의 경우 ASMN의 총 CPU 사용률이 일반적인 NFV 환경에서의 CPU 사용률보다 대략 1 % 미만으로 증가하였음을 확인할 수 있다. 따라서 VNF에서 VNF로의 통신은 마이크로 초 내에 성능 저하가 없음을 확인할 수 있다.

[140] 도 9는 본 발명의 일 실시예에 따른 VNF간 패킷 전송률을 비교한 그래프이다.

[141] 이때, 테스트 데이트는 표 1과 같다.

[142] [표1]

ASMN Traffic Input Rate		
ICMP traffic	**TCP traffic**	**UCP traffic**
64byte4096byte	64byte4096byte	64byte4096byte

[143] 클라이언트는 ICMP 프로토콜에 대해 64바이트와 4,096바이트의 임의 패킷을 생성하고, ASMN을 사용하는 동일 테넌트의 VNF 사이의 RTT(왕복 시간)를 측정하기 위해 서버로 패킷을 전송한 것이다.

[144] 도 9를 참조하면, RTT 증가는 5m/s보다 더 작은 것을 확인할 수 있다. 이를 통해 본 발명의 시스템은 성능의 저하 없이 서비스를 제공할 수 있음을 확인할 수 있다.

[145] 도 10은 본 발명의 일 실시예에 따른 TCP 패킷 flooding에 대한 VNF-게이트웨이의 shaping 시험 결과를 나타낸 그래프이다.

[146] ASMN에는 VNF의 악성 트래픽에 대한 방어 메커니즘이 포함된다. VNF의 트래픽을 사용하는 일반적인 악성 공격은 플러딩 공격이다. 방어 테스트의 데이터는 아패 표 2와 같다.

[147] [표2]

ASMN Traffic Input Rate
TCP SYN traffic
5 Mbyte

[148] VNF 서버에 대한 TCP SYN 플러딩 공격을 100초동안 시도하였다. 그런 다음 공격 시작 11초 후 VNF-게이트웨이에 10Mbit/s의 트래픽 쉐이핑 룰을 포함하는 Sec-catalog를 적용하였다.

[149] 도 10에서 280Mbit/s의 트래픽을 VNF 서버에 전송하였다. Sec-catalog을 적용한 후, 트래픽은 룰 적용 후 1초 이내에 9.76Mbit/s로 제한되었음을 알 수 있다. 즉, 들어오는 트래픽 제어를 통해 플러딩 공격을 예방할 수 있음을 확인할 있다.

[150] 이상에서 본 발명에 따른 바람직한 실시예에 대해 설명하였으나, 다양한 형태로 변형이 가능하며, 본 기술분야에서 통상의 지식을 가진 자라면 본 발명의 특허청구범위를 벗어남이 없이 다양한 변형예 및 수정예를 실시할 수 있을 것으로 이해된다.

[151]

청구범위

[청구항 1] NFV(network function virtualization) 환경에서 VNF(virtualized network function)간 보안 통신 방법에 있어서,
요소 관리자는 해시체인을 이용하여 제1 VNF와 제2 VNF간 인증을 수행하는 단계;
상기 인증 완료된 제1 VNF와 제2 VNF는 자신의 해시체인을 기반으로 비밀키를 각각 생성하는 단계; 및
상기 제1 VNF와 제2 VNF는 자신의 비밀키를 이용하여 통신을 수행하는 단계
를 포함하는 NFV 환경에서 보안 통신 방법.

[청구항 2] 제1항에 있어서,
상기 인증을 수행하는 단계 이전에,
VIM(Virtualized Infrastructure Manager)은 테넌트(Tenant)내의 VNF가 인스턴화될 때 VNF 이미지의 해시체인을 생성하여 상기 요소 관리자와 공유하는 단계를 더 포함하는 NFV 환경에서 보안 통신 방법.

[청구항 3] 제2항에 있어서,
상기 공유하는 단계는,
테넌트 식별정보, VNF 식별정보, 인스턴스 식별정보 중 적어도 하나를 조합하여 상기 테넌트내 VNF 식별정보(VNF_{ID})를 계산하는 단계;
상기 계산된 테넌트내 VNF 식별정보(VNF_{ID})를 해시함수에 적용하여 해시체인을 계산하고, 상기 계산된 해시체인을 상기 요소 관리자와 공유하는 단계; 및
상기 계산된 해시체인이 업데이트된 경우, 상기 업데이트된 해시체인을 상기 요소 관리자와 공유하는 단계를 포함하는 것을 특징으로 하는 NFV 환경에서 보안 통신 방법.

[청구항 4] 제3항에 있어서,
상기 업데이트된 해시체인을 상기 요소 관리자와 공유하는 단계는,
해당 VNF 이미지가 수정/변경되거나 또는 주기적으로 이전 해시체인에 해시함수를 적용하여 해시체인을 업데이트하는 단계; 및
상기 업데이트된 해시체인을 상기 요소 관리자로 전송하는 단계를 포함하는 것을 특징으로 하는 NFV 환경에서 보안 통신 방법.

[청구항 5] 제4항에 있어서,
상기 업데이트된 해시체인을 상기 요소 관리자로 전송하는 단계는,
상기 업데이트된 해시채널을 이전 해시체인을 암호화 키로 사용하는 대칭 암호화 알고리즘으로 암호화하여 상기 요소 관리자로 전송하는 것을 특징으로 하는 NFV 환경에서 보안 통신 방법.

[청구항 6] 제1항에 있어서,

상기 인증을 수행하는 단계는,
상기 제1 VNF로부터 초기(Initi) 메시지 수신 시, 상기 제2 VNF에 해시체인을 요청하여 수신하는 단계;
상기 수신된 제2 VNF의 해시체인을 기 저장된 제2 VNF 해시체인과 비교하여 상기 제2 VNF를 인증하는 단계;
상기 제2 VNF의 인증 완료시 상기 제1 VNF에 해시체인을 요청하여 수신하는 단계;
상기 수신된 제1 VNF의 해시체인을 기 저장된 제1 VNF 해시체인과 비교하여 상기 제1 VNF를 인증하는 단계; 및
상기 제1 VNF와 제2 VNF의 인증결과를 상기 제1VNF로 전송하는 단계를 포함하는 것을 특징으로 하는 NFV 환경에서 보안 통신 방법.

[청구항 7] 제6항에 있어서,
상기 제2 VNF의 해시체인이, 상기 제2 VNF가 가장 최근 자신에게 할당된 해시체인을 암호화키로 사용하여 현재 자신에게 할당된 해시체인을 암호화한 해시체인인 경우,
상기 제2 VNF를 인증하는 단계는,
기 저장된 제2 VNF의 가장 최근 해시체인을 이용하여 상기 제2 VNF의 암호화된 해시체인을 복호화하고, 상기 복호화된 해시체인을 기 저장된 제2 VNF 해시체인과 비교하여 제2 VNF를 인증하고,
상기 제1 VNF의 해시체인이, 상기 제1 VNF가 가장 최근 자신에게 할당된 해시체인을 암호화키로 사용하여 현재 자신에게 할당된 해시체인을 암호화한 해시체인인 경우,
상기 제1 VNF를 인증하는 단계는,
기 저장된 제1 VNF의 가장 최근 해시체인을 이용하여 상기 제1 VNF의 암호화된 해시체인을 복호화하고, 상기 복호화된 해시체인을 기 저장된 제1 VNF 해시체인과 비교하여 제1 VNF를 인증하는 것을 특징으로 하는 NFV 환경에서 보안 통신 방법.

[청구항 8] 제1항에 있어서,
상기 비밀키는,
해시체인을 기반으로 디피-헬만(Diffie-Hellman(D-H)) 알고리즘을 이용하여 생성되는 것을 특징으로 하는 NFV 환경에서 보안 통신 방법.

[청구항 9] 제8항에 있어서,
상기 비밀키를 각각 생성하는 단계는,
상기 제1 VNF 및 제2 VNF는 각각 요소 관리자로부터 제1 정수(p) 및 제2 정수(q)를 수신하는 단계;
상기 제1 VNF 및 제2 VNF는 상기 수신된 제1 정수(p), 제2 정수(q) 및 자신의 해시체인을 이용하여 제1 공개키 및 제2 공개키를 생성하는 단계;
상기 제1 VNF는 제1 공개키를 상기 제2 VNF로 전달하고, 상기 제2

VNF는 제2 공개키를 상기 제1 VNF로 전달하는 단계;
상기 제1 VNF는 자신의 해시체인과 제2 공개키를 이용하여 제1 비밀키를 생성하고, 상기 제2 VNF는 자신의 해시체인과 제1 공개키를 이용하여 제2 비밀키를 생성하는 단계를 포함하되,
상기 해시체인이 개인키인 것을 특징으로 하는 것을 특징으로 하는 NFV 환경에서 보안 통신 방법.

[청구항 10] 제9항에 있어서,
상기 통신을 수행하는 단계는,
상기 제1 VNF는 상기 제1 비밀키를 이용하여 메시지를 암호화하고, 상기 암호화된 메시지를 VNF-게이트웨이로 전송하는 단계;
상기 VNF-게이트웨이는 상기 메시지에 대한 설정정보를 획득하고, 상기 획득된 설정정보를 기 저장된 보안정책정보와 비교하여 두 정보가 일치하는 경우 상기 암호화된 메시지를 상기 제2 VNF로 전송하는 단계; 및
상기 제2 VNF는 상기 제2 비밀키를 이용하여 상기 암호화된 메시지를 복호화하는 단계를 포함하는 것을 특징으로 하는 NFV 환경에서 보안 통신 방법.

[청구항 11] 제10항에 있어서,
상기 VNF-게이트웨이는 두 정보가 일치하지 않은 경우, 상기 암호화된 메시지를 차단하는 것을 특징으로 하는 NFV 환경에서 보안 통신 방법.

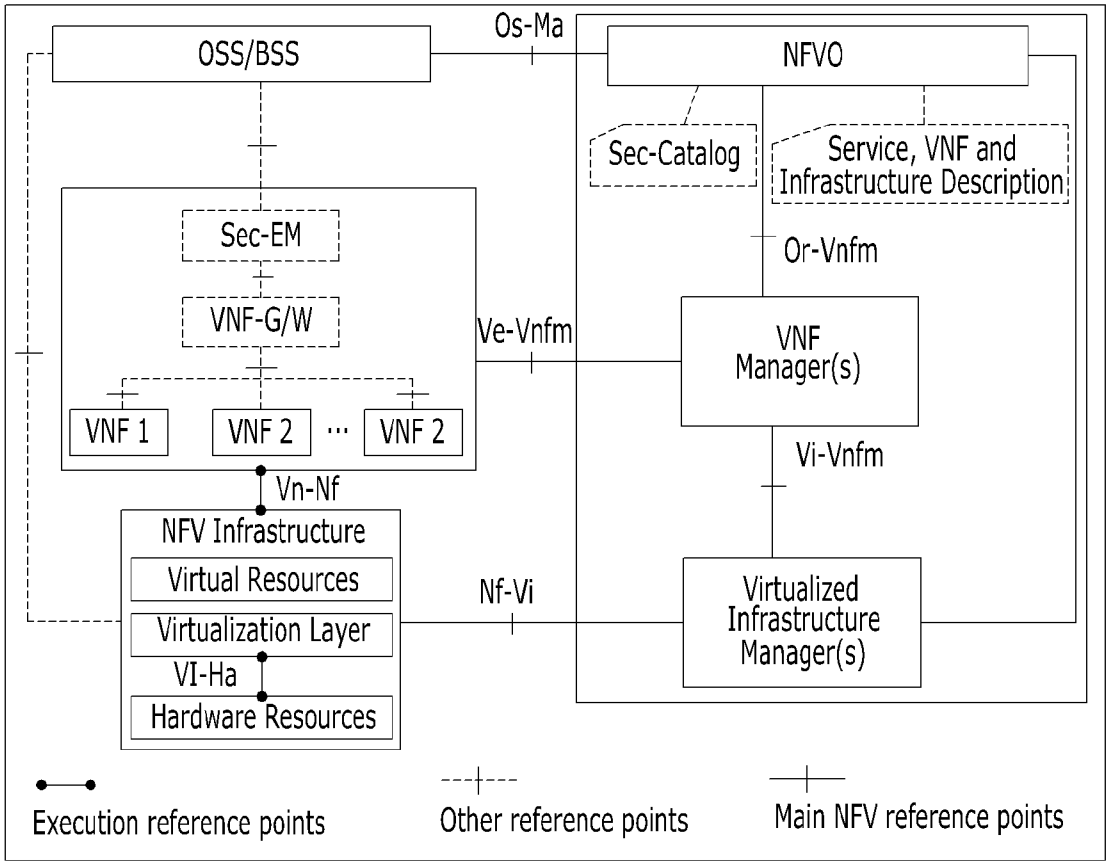
[청구항 12] NFV(network function virtualization) 환경에서 복수의 VNF를 포함하는 테넌트(Tenant)내의 VNF 간 보안 통신을 위한 시스템에서 있어서,
상기 복수의 VNF에 각각 할당된 해시체인을 관리하며, 통신을 원하는 VNF들의 해시체인을 이용하여 해당 VNF들을 인증하는 요소 관리자; 및
상기 테넌트내 복수의 VNF 사이에 위치하고, VNF 트래픽에 대한 보안정책정보가 설정된 Sec-catalog를 설정하여 VNF 간의 트래픽을 제어하는 VFN 게이트웨이를 포함하며,
상기 요소 관리자에서 인증 완료된 VNF는 자신의 해시체인을 기반으로 비밀키를 생성하고, 상기 생성된 비밀키로 메시지를 암호화하여 상기 VNF 게이트웨이로 전송하며, 상기 VNF 게이트웨이로부터 암호화된 메시지 수신 시, 상기 비밀키를 이용하여 상기 암호화된 메시지를 복호화하고,
상기 VNF-게이트웨이는 상기 메시지에 대한 설정정보를 획득하고, 상기 획득된 설정정보를 상기 보안정책정보와 비교하여 두 정보가 일치하는 경우 상기 암호화된 메시지를 상대 VNF로 전송하는 것을 특징으로 하는 NFV 환경에서 보안 통신 시스템.

[청구항 13] 제12항에 있어서,
상기 테넌트(Tenant)내의 VNF가 인스턴화될 때 VNF 이미지의

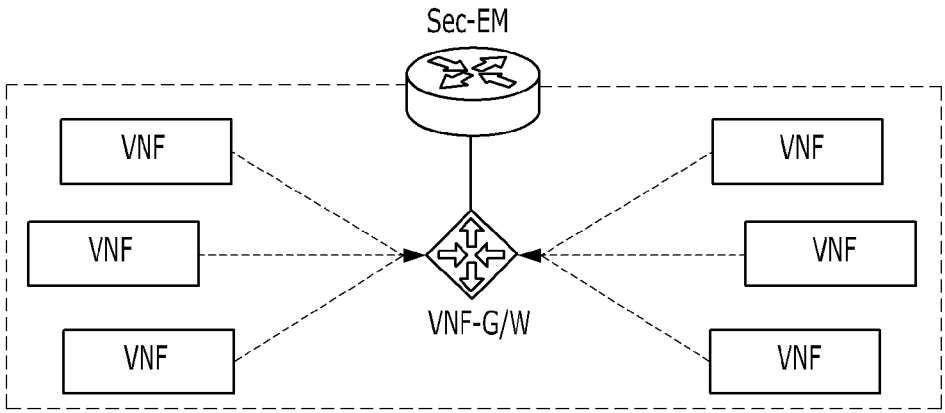
해시체인을 생성하여 상기 요소 관리자와 공유하는 VIM을 더 포함하는 단계를 더 포함하는 NFV 환경에서 보안 통신 시스템.

[청구항 14] 제13항에 있어서,
상기 VIM은,
상기 VNF 이미지가 수정/변경되거나 또는 주기적으로 이전 해시체인에 해시함수를 적용하여 해시체인을 업데이트하고, 상기 업데이트된 해시체인을 상기 요소 관리자와 공유하는 것을 특징으로 하는 NFV 환경에서 보안 통신 시스템.

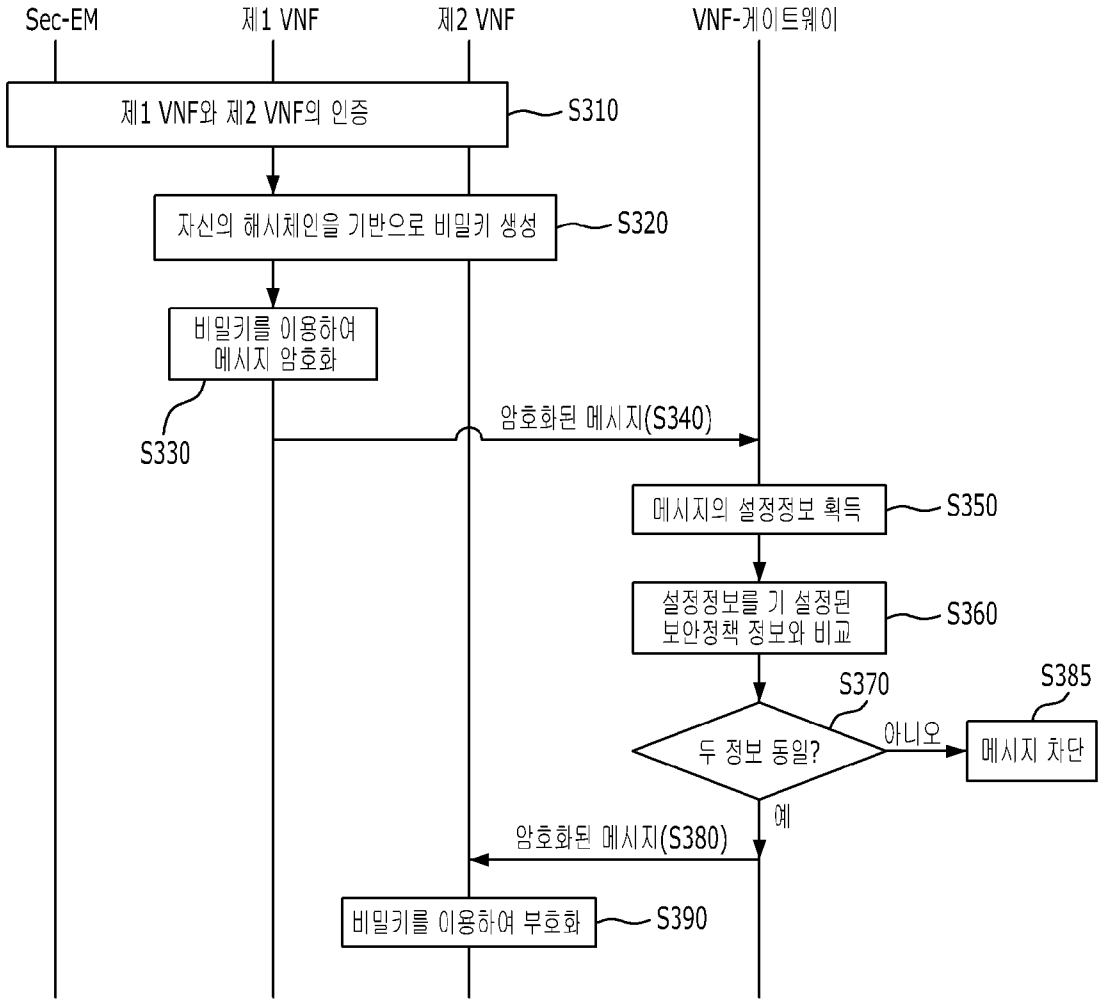
[도1]


OSS/BSS
Os-Ma
NFVO
Sec-Catalog
Service, VNF and Infrastructure Description
Sec-EM
VNF-G/W
Or-Vnfm
Ve-Vnfm
VNF Manager(s)
VNF 1
VNF 2
VNF 2
Vi-Vnfm
Vn-Nf
NFV Infrastructure
Virtual Resources
Virtualization Layer
VI-Ha
Hardware Resources
Nf-Vi
Virtualized Infrastructure Manager(s)
Execution reference points
Other reference points
Main NFV reference points

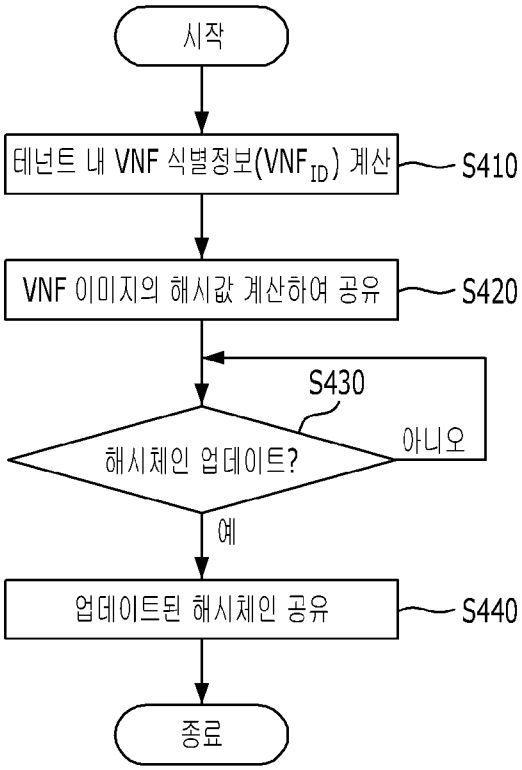
[도2]


Sec-EM
VNF
VNF
VNF
VNF
VNF
VNF
VNF-G/W

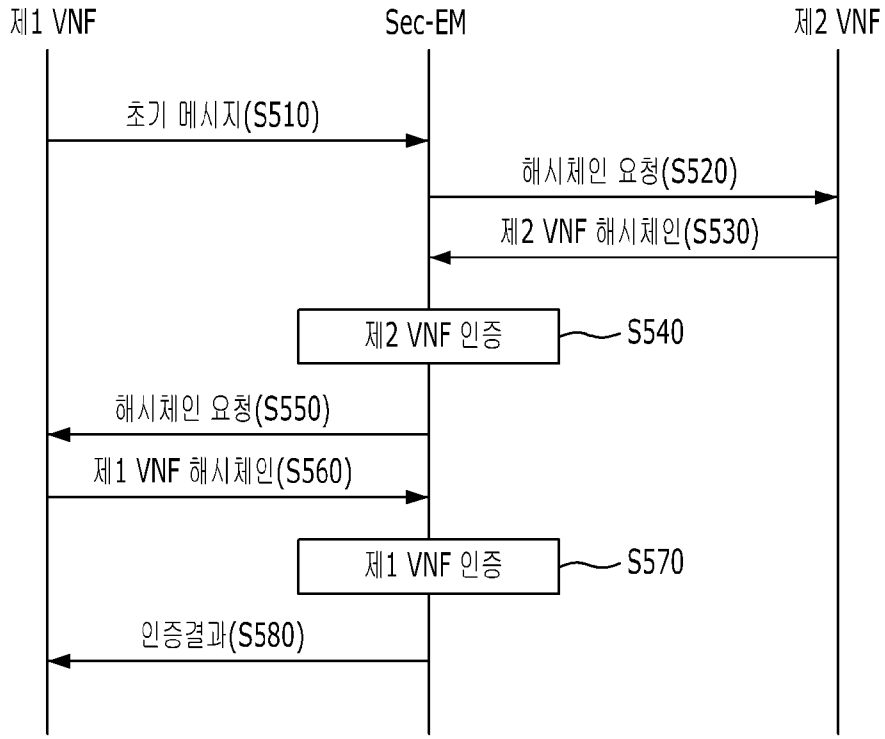
[도3]


Sec-EM
제1 VNF
제2 VNF
VNF-게이트웨이
제1 VNF와 제2 VNF의 인증
S310
자신의 해시체인을 기반으로 비밀키 생성
S320
비밀키를 이용하여 메시지 암호화
S330
암호화된 메시지(S340)
메시지의 설정정보 획득
S350
설정정보를 기 설정된 보안정책 정보와 비교
S360
S370
두 정보 동일?
아니오
S385
메시지 차단
예
암호화된 메시지(S380)
비밀키를 이용하여 부호화
S390

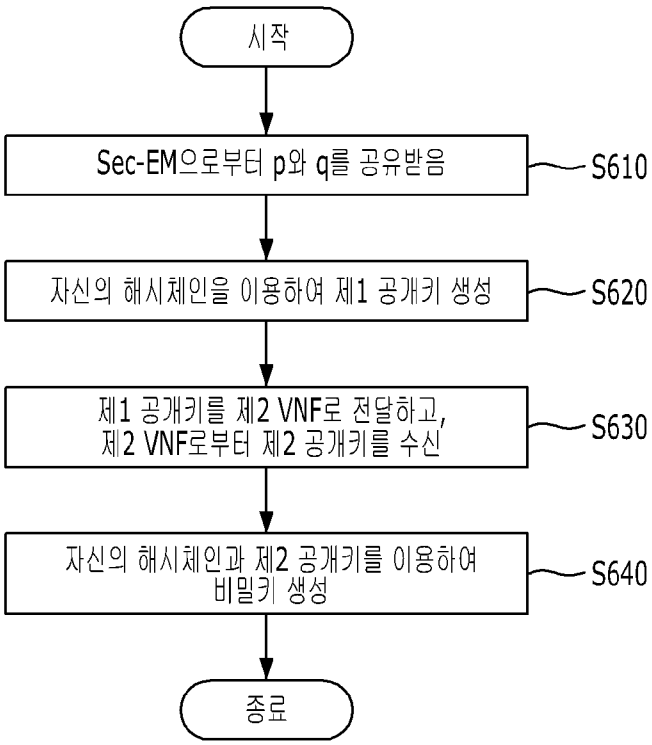
[도4]


시작
테넌트 내 VNF 식별정보(VNF_ID) 계산
S410
VNF 이미지의 해시값 계산하여 공유
S420
S430
해시체인 업데이트?
아니오
예
업데이트된 해시체인 공유
S440
종료

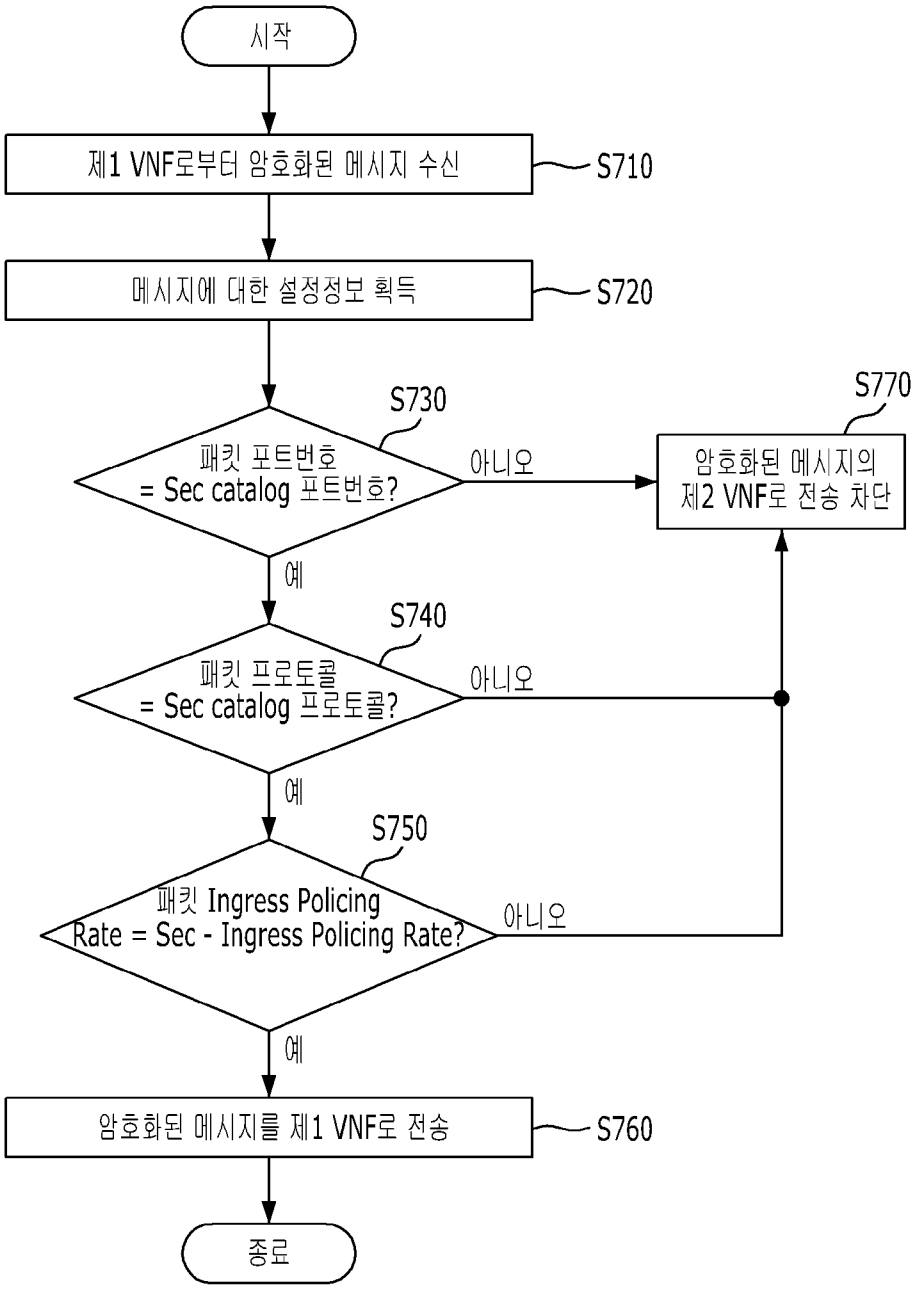
[도5]


제1 VNF
Sec-EM
제2 VNF
초기 메시지(S510)
해시체인 요청(S520)
제2 VNF 해시체인(S530)
제2 VNF 인증
S540
해시체인 요청(S550)
제1 VNF 해시체인(S560)
제1 VNF 인증
S570
인증결과(S580)

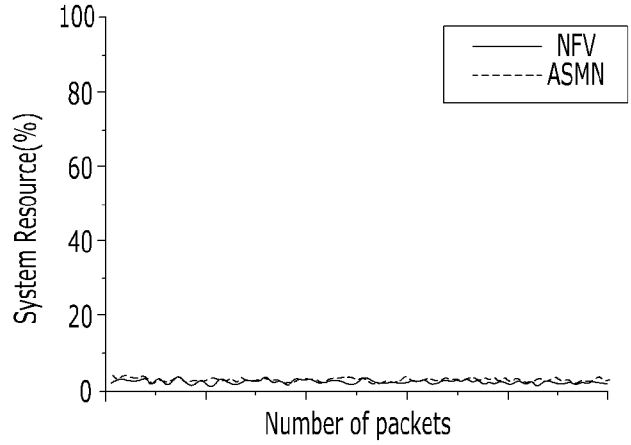
[도6]


시작
Sec-EM으로부터 p와 q를 공유받음
S610
자신의 해시체인을 이용하여 제1 공개키 생성
S620
제1 공개키를 제2 VNF로 전달하고,
제2 VNF로부터 제2 공개키를 수신
S630
자신의 해시체인과 제2 공개키를 이용하여
비밀키 생성
S640
종료

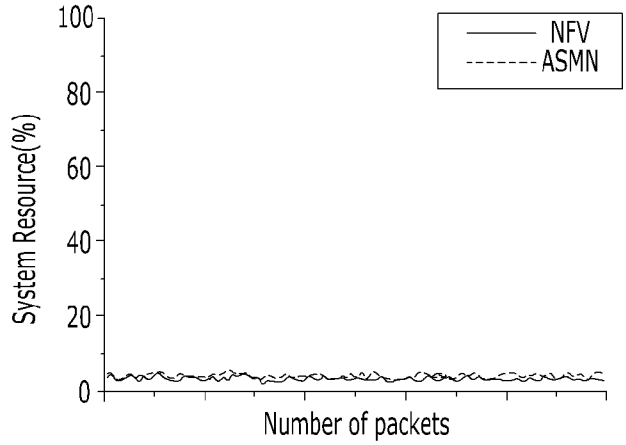
[도7]


시작
제1 VNF로부터 암호화된 메시지 수신
S710
메시지에 대한 설정정보 획득
S720
S730
패킷 포트번호
= Sec catalog 포트번호?
아니오
S770
암호화된 메시지의
제2 VNF로 전송 차단
예
S740
패킷 프로토콜
= Sec catalog 프로토콜?
아니오
예
S750
패킷 Ingress Policing
Rate = Sec - Ingress Policing Rate?
아니오
예
암호화된 메시지를 제1 VNF로 전송
S760
종료

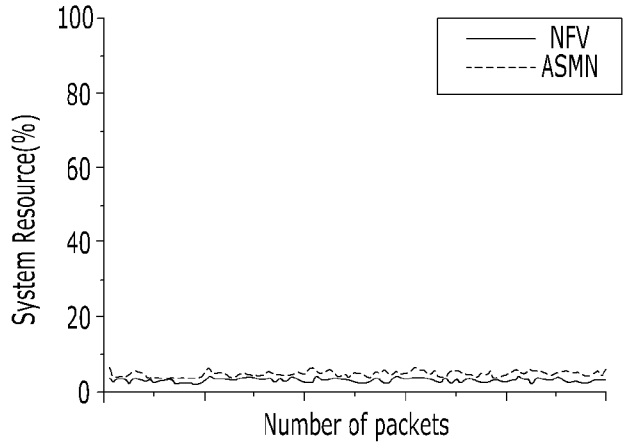
[도8]



(1) ICMP 패킷 전송에 따른 CPU 사용률

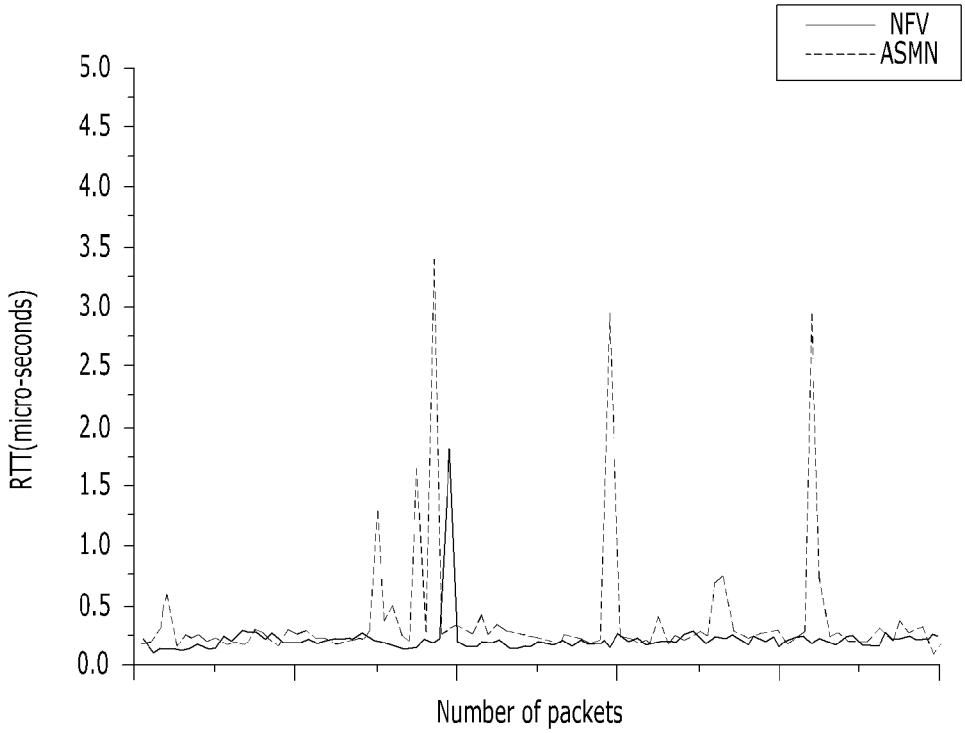


(2) TCP 패킷 전송에 따른 CPU 사용률

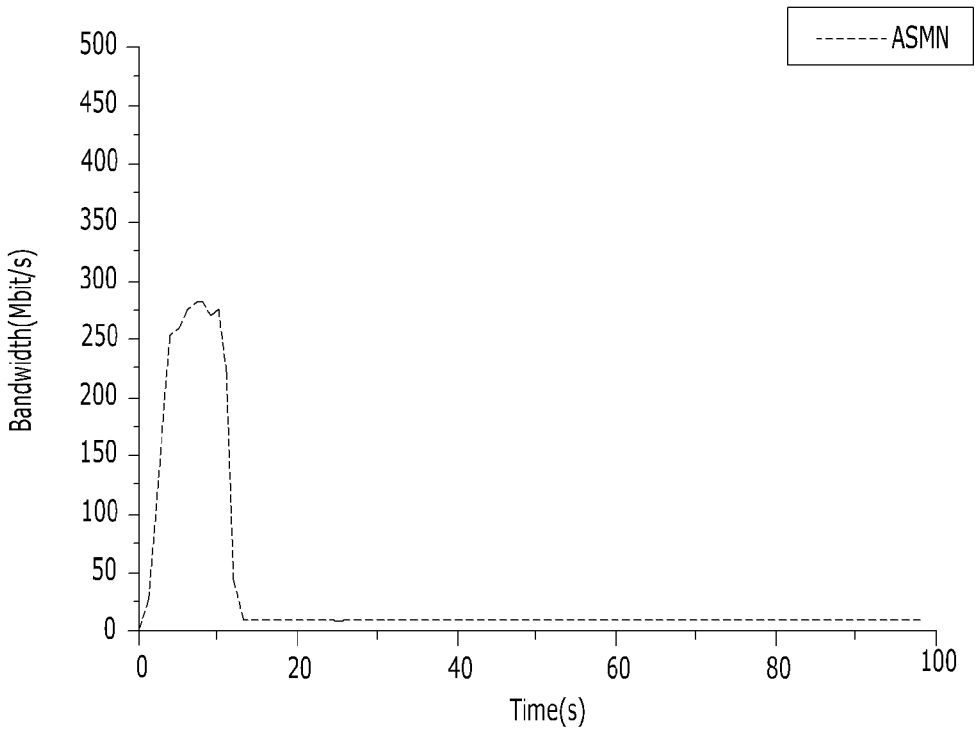


(3) UDP 패킷 전송에 따른 CPU 사용률

[도9]


NFV
ASMN
RTT(micro-seconds)
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
Number of packets

[도10]


ASMN
Bandwidth(Mbit/s)
500
450
400
350
300
250
200
150
100
50
0
0
20
40
60
80
100
Time(s)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2018/014994

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i, H04L 9/08(2006.01)i, H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/32; H04L 29/06; H04L 9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: NFV(network function virtualization), VNF(virtualized network function), secure communications, authentication, hash chain

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	OLIVER, Ian et al., "Experiences in Trusted Cloud Computing", Springer International Publishing AG., 2017, July 2017 See pages 22-23, 25-27.	1-14
Y	PAWAR, Ranjeet et al., "MKAuth: Multikey Authentication For Multicast MANET", International Journal of Modern Trends in Engineering and Research (IJMTER), Vol. 2, No. 4, April 2015 See page 106 and figure 2.	1-14
Y	ETSI GS NFV-SEC 013 V3.1.1, "Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring Specification", 28 February 2017 See sections 6.4.2, 7.6.4.	3-5,10-14
Y	MOKHTARNAMEH, Razieh et al., "A Comparison Study on Key Exchange-Authentication Protocol", International Journal of Computer Applications (0975-8887), Vol. 7, No. 5, September 2010 See page 5 and figures 1-2.	8-11

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 MARCH 2019 (05.03.2019)	**05 MARCH 2019 (05.03.2019)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex Daejeon Building 4, 189, Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea Facsimile No. +82-42-481-8578	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2018/014994

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KIM, Hyunjin et al., "Trust Mechanism in NFV Using Hash-chain", KSII The 12th Asia Pacific International Conference on Information Science and Technology(APIC-IST) 2017, 25-28 June 2017 See pages 1-3. ※ The above document(KIM, Hyunjin et al.) is a document declaring exceptions to lack of novelty when an applicant files an earlier application whose priority is claimed.	1-14
A	US 2017-0302646 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 19 October 2017 See paragraphs [0088]-[0089], [0105], [0110]-[0125], claim 1 and figure 1.	1-14

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2018/014994

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2017-0302646 A1	19/10/2017	CN 104580208 A	29/04/2015
		CN 104580208 B	30/11/2018
		EP 3232634 A1	18/10/2017
		EP 3232634 A4	20/12/2017
		WO 2016-107203 A1	07/07/2016

국 제 조 사 보 고 서

국제출원번호
PCT/KR2018/014994

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/32(2006.01)i, H04L 9/08(2006.01)i, H04L 29/06(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04L 9/32; H04L 29/06; H04L 9/08

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: NFV(network function virtualization), VNF(virtualized network function), 보안 통신, 인증, 해시체인

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	IAN OLIVER 등, `Experiences in Trusted Cloud Computing`, Springer International Publishing AG 2017, 2017.07 페이지 22-23, 25-27 참조.	1-14
Y	RANJEET PAWAR 등, `MKAuth: Multikey Authentication For Multicast MANET`, International Journal of Modern Trends in Engineering and Research (IJMTER), Vol. 2, No. 4, 2015.04 페이지 106 및 도면 2 참조.	1-14
Y	ETSI GS NFV-SEC 013 V3.1.1, `Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification`, 2017.02.28 섹션 6.4.2, 7.6.4 참조.	3-5,10-14
Y	RAZIEH MOKHTARNAMEH 등, `A Comparison Study on Key Exchange-Authentication protocol`, International Journal of Computer Applications (0975 - 8887), Vol. 7, No. 5, 2010.09 페이지 5 및 도면 1-2 참조.	8-11

☒ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2019년 03월 05일 (05.03.2019)	2019년 03월 05일 (05.03.2019)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
김성우
전화번호 +82-42-481-3348

국제조사보고서

국제출원번호
PCT/KR2018/014994

C(계속). 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	HYUNJIN KIM 등, `Trust Mechanism in NFV using Hash-chain`, KSII The 12th Asia Pacific International Conference on Information Science and Technology (APIC-IST) 2017, 2017.06.25-28 페이지 1-3 참조. ※ 위 문헌(HYUNJIN KIM 등)은 출원인이 우선권 주장의 기초가 된 선출원 출원시 신규성 상실의 예외로 선언한 공지문헌임.	1-14
A	US 2017-0302646 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 2017.10.19 단락 [0088]-[0089], [0105], [0110]-[0125], 청구항 1 및 도면 1 참조.	1-14

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2018/014994

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2017-0302646 A1	2017/10/19	CN 104580208 A	2015/04/29
		CN 104580208 B	2018/11/30
		EP 3232634 A1	2017/10/18
		EP 3232634 A4	2017/12/20
		WO 2016-107203 A1	2016/07/07