JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 11, pp. 105-114, November 2020
https://doi.org/10.9708/jksci.2020.25.11.105

Security Threats and Potential Security Requirements in 5G Non-Public Networks for Industrial Applications

Tae-Keun Park*, Jong-Geun Park**, Keewon Kim*

*Professor, Dept. of Computer Engineering, Dankook University, Yongin, Korea
**Principal Researcher, Information Security Research Division, ETRI, Daejeon, Korea
*Professor, Dept. of Computer Engineering, Dankook University, Yongin, Korea

[Abstract]

In this paper, we address security issues in 5G non-public networks for industrial applications. In contrast to public networks that offer mobile network services to the general public, 5G non-public networks provide 5G network services to a clearly defined user organization or groups of organizations, and they are deployed on the organization's defined premises, such as a campus or a factory. The main goal of this paper is to derive security threats and potential security requirements in the case that 5G non-public networks are built for discrete and process industries according to the four deployment models of 5G-ACIA (5G Alliance for Connected Industries and Automation). In order to clarify the scope of this paper, we express the security toolbox to be applied to 5G non-public networks in the form of the defense in depth concept. Security issues related to general 5G mobile communication services are not within the scope of this paper. We then derive the security issues to consider when applying the 5G-ACIA deployment models to the industrial domain. The security issues are divided into three categories, and they are described in the order of overview, security threats, and potential security requirements.

▸ **Key words**: 5G, Non-Public Network, Security Requirement, Industrial Domain, Deployment

[요 약]

본 논문에서는 산업 애플리케이션을 위한 5G Non-Public Network에서의 보안 이슈를 다룬다. 일반 대중에게 모바일 네트워크 서비스를 제공하는 공공 네트워크와는 달리, 5G Non-Public Network는 명확하게 정의된 사용자 조직이나 조직들의 그룹에게 5G 네트워크 서비스를 제공하며, 캠퍼스나 공장과 같이 사용자 조직이 지정한 영역 내에 구축된다. 본 논문의 주목적은 5G-ACIA (5G Alliance for Connected Industries and Automation)에서 제안한 네 가지 구축 모델에 따라 5G Non-Public Network가 이산 산업 및 공정 산업을 위하여 구축될 경우 고려되어야 할 보안 위협 및 잠재적 보안 요구사항을 도출하는 것이다. 본 논문의 범위를 명확하게 하기 위해 먼저 5G Non-Public Network에 적용할 보안 툴박스를 심층 방어 개념으로 표현한다. 일반적인 5G 이동통신 서비스와 관련된 보안 이슈는 본 논문의 범위에 포함되지 않는다. 그 다음, 산업 도메인에 5G-ACIA의 구축 모델을 적용할 때 고려해야 할 보안 이슈를 도출한다. 도출된 보안 이슈들은 세 가지 범주로 나뉘며 각각의 보안 이슈들은 개요, 보안 위협 및 잠재적 보안 요구사항의 순서로 서술된다.

▸ **주제어**: 5G, Non-Public Network, 보안 요구사항, 산업 도메인, 구축

• First Author: Tae-Keun Park, Corresponding Author: Keewon Kim
*Tae-Keun Park (tkpark@dankook.ac.kr), Dept. of Computer Engineering, Dankook University
**Jong-Geun Park (queue@etri.re.kr), Information Security Research Division, ETRI
*Keewon Kim (nirkim@dankook.ac.kr), Dept. of Computer Engineering, Dankook University
• Received: 2020. 10. 15, Revised: 2020. 11. 03, Accepted: 2020. 11. 03.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

5G (Fifth-Generation)는 다양한 경제 및 사회 분야에 디지털 기술 도입을 가능케 하는 핵심적인 요소가 되도록 설계되었기 때문에 모바일 광대역 통신 제공을 위한 4G와 확실한 차이점을 가진다 [1-3]. 이러한 5G는 4차 산업혁명의 핵심 인프라 기술로서 인공지능과 빅데이터 등 여타 핵심 기술들과 결합하여 다양한 분야에서 차세대 서비스를 제공하는데 기여할 것으로 예상되고 있다 [1-4].

다양한 경제 및 사회 분야 중에서 본 논문은 산업 도메인 (Industrial Domain)에 5G 기술을 적용하고자하는 것에 초점을 맞춘다. 산업 도메인은 자동차, 반도체 등의 이산 산업 (Discrete Industry)과 정유, 발전 등의 공정 산업 (Process Industry)을 포함한다. 이러한 산업 도메인에 5G를 적용하고자 할 때 고려될 필요가 있는 기술, 규제, 비즈니스 측면 등에 대하여 검토 및 평가를 수행하는 글로벌 포럼으로 5G-ACIA (Alliance for Connected Industries and Automation)가 있다. 5G-ACIA는 산업 도메인에 5G의 적용을 위해 네 가지 5G NPN (Non-Public Network) 구축 모델을 제시하였다 [5].

본 논문에서는 5G-ACIA가 제시한 네 가지 구축 모델 중 하나로 5G NPN을 구축할 때 고려해야 할 보안 이슈를 도출한다. 이를 위하여 먼저 5G NPN에 적용될 보안 툴박스를 심층 방어 (Defense in Depth) [6] 개념 형태로 표현한다. 다음으로, 일반적인 이동통신 서비스 제공과 관련된 5G 보안 이슈 이외에, 산업 도메인에 5G 기술을 적용할 때 추가적으로 고려해야만 하는 보안 이슈를 개요, 보안 위협, 잠재적인 보안 요구사항의 순서로 기술한다.

II. 5G NPN Deployment Models of 5G-ACIA

일반적으로 이동통신 네트워크는 일반 대중을 대상으로 서비스를 제공하지만, 5G NPN은 일종의 사설 네트워크 (Private Network)로서 명확하게 정의된 사용자 조직 또는 조직의 그룹에게 5G 서비스를 제공하는 네트워크를 의미한다 [5]. 예를 들어 5G NPN은 공장의 사용자 그룹에게 서비스를 제공하기 위하여 구내에 구축될 수 있다. 이러한 5G NPN을 구축할 경우 얻을 수 있는 이점으로, (a) 높은 QoS (Quality of Service), (b) 전용 보안 자격증명으로 충족되는 높은 보안, (c) 오동작에 대한 보호의 한 형태로서, 또는 성능, 보안, 프라이버시 및 안전 등의 이유로, 다른 네트워크와의 격리, (d) 가용성, 유지보수 및 운영 책임에 대한 쉬운 식별 등을 들 수 있다 [5].

5G-ACIA는 제조 산업 및 IIoT (Industrial Internet of Things)에 5G NPN을 활용하는 것에 대하여 집중하고 있다. 5G-ACIA의 5G NPN 구축 모델들은 큰 틀에서 두 개의 범주로 나뉜다 [5].

- 격리된 독립형 NPN
- PN (Public Network) 연계형 NPN

첫 번째 범주인 “격리된 독립형 NPN”에는 하나의 구축 모델만 포함되어 있는데 반하여, 두 번째 범주인 “PN 연계형 NPN”은 PN과 기반구조 공유 및 상호작용의 정도에 따라 세 가지 다른 형태의 구축 모델을 포함한다. 그림 1은 5G-ACIA의 네 가지 5G NPN 구축 모델을 보여준다.

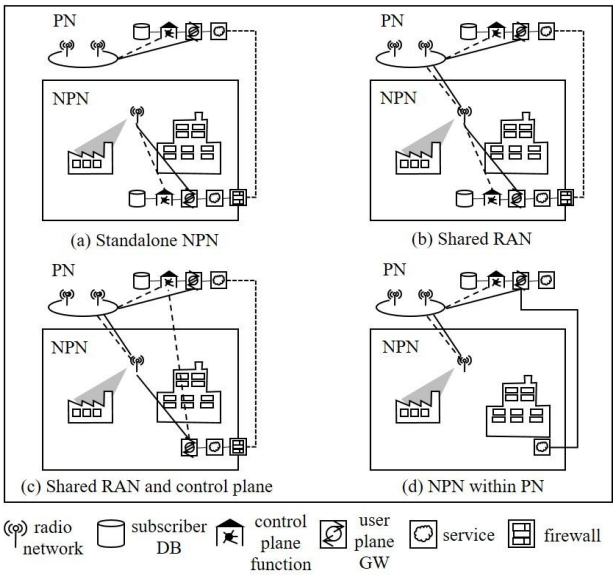

Fig. 1. 5G NPN Deployment Models of 5G-ACIA

그림 1의 (a)는 “SNPN (Standalone NPN)” 구축 모델을 보여준다. 이 구축 모델에서 모든 네트워크 기능들은 공장의 논리적 경계 내에 위치하며 NPN은 PN과 분리되어 있다. NPN과 PN 사이의 유일한 통신 경로는 방화벽을 통하는 것이다.

그림 1의 (b)는 “Shared RAN (Radio Access Network)” 구축 모델을 보여준다. 이 구축 모델에서 NPN과 PN은 RAN의 일부를 공유하지만 다른 네트워크 기능은 분리되어 있다. NPN 트래픽 부분과 관련된 모든 데이터 흐름은 공장의 논리적 경계 내에 있으며 PN 트래픽은 PN으로 전송되도록 구성되어 있다. 이러한 구성은 RAN 공유를 가능하게 하는 3GPP 표준 규격 [7]에 의해 가능해진다. 이 구축 모델에서도 방화벽을 통해 NPN과 PN 사이의 선택적 연결을 제공할 수 있다.

그림 1의 (c)는 “Shared RAN and CP (Control Plane)” 구축 모델을 보여준다. 이 구축 모델에서 NPN과 PN은 공장에서 RAN을 공유할 뿐만 아니라 CP에 속하는 모든 작업들은 PN에서 수행하도록 한다. 하지만 모든 NPN 트래픽들은 공장의 논리적인 경계 내에서만 흘러 다닌다. 이 구축 모델에서도 방화벽을 통해 NPN과 PN 사이의 선택적 연결을 제공할 수 있다.

그림 1의 (d)는 “NPN within PN” 구축 모델을 보여준다. 이 구축 모델에서 PN 트래픽과 NPN 트래픽은 모두 공장 외부에 존재하는 완전히 다른 네트워크를 통해 전달된다. 이러한 트래픽 처리는 클라우드 환경에서 네트워크 기능의 가상화를 통해 달성될 수 있다. 가상화된 네트워크 기능들은 PN과 NPN 모두를 위하여 사용될 수 있다. 방화벽을 통한 NPN과 PN 사이의 선택적 연결은 이 구축 모델에서 필요하지 않다.

III. Our Approach

심층 방어는 보안 위협으로부터 대상을 보호하기 위한 연속적인 보안 조치 계층의 결합으로 정의된다 [6]. 그림 2는 심층 방어 구조의 두 가지 예 [8]를 보여준다. 그림 2의 왼쪽에 위치한 네 개의 겹으로 이루어진 심층 방어 구조 예를 살펴보면 가장 바깥쪽에 네트워크 방어가 존재하고 그 안쪽에 호스트 방어와 애플리케이션 방어가 존재하며 가장 안쪽에 데이터 방어가 존재하는 형태의 구조를 가지고 있다. 이러한 심층 방어의 개념은 산업 자동화 및 제어 시스템의 네트워크에서도 사용되고 있다 [9].

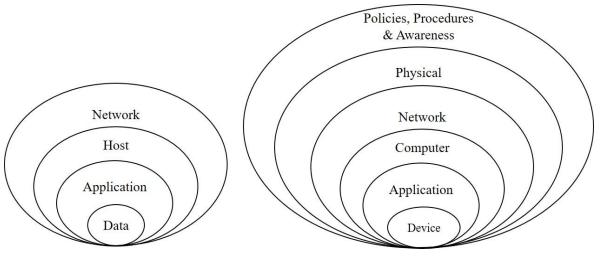

Fig. 2. Examples of Defense in Depth

산업 도메인에 5G 기술을 도입하는 것을 포함하여 산업 자동화 및 제어 시스템의 네트워크에 발전된 통신 기술을 적용하고자 하는 노력이 지속되어 왔다. 그림 3은 이러한 노력의 결과로 바뀌고 있는 산업 자동화 및 제어 시스템의 개념적인 구조를 보여준다.

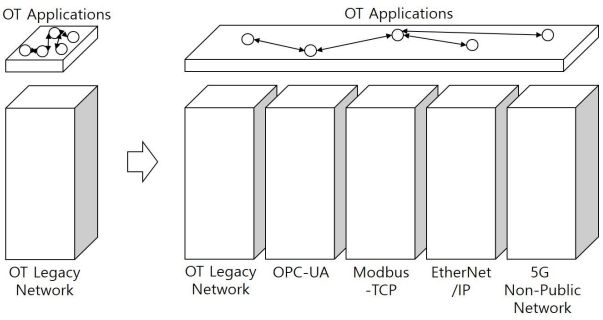

Fig. 3. Conceptual Structure Change of Industrial Automation and Control Systems

전통적인 산업 자동화 및 제어 시스템은 그림 3의 왼쪽과 같이 OT (Operational Technology) 네트워크의 통신 서비스를 사용하는 OT 애플리케이션과 전통적인 OT 네트워크로 구성된다. OT란 산업계에서 사용하는 물리적 장치와 프로세스의 운영에 대한 관리, 모니터링, 제어를 수행하는 컴퓨터 시스템과 통신 시스템의 범주를 의미한다.

산업 자동화 및 제어 시스템 네트워크에 발전된 통신 기술을 적용하고자 하는 노력의 결과물로 OT 애플리케이션에게 통신 서비스를 제공하는 발전된 네트워크인 OPC-UA, Modbus-TCP, EtherNet/IP 등이 등장하였다. 그 결과, 산업 자동화 및 제어 시스템의 개념적인 구조는 그림 3의 오른쪽과 같이 변화하게 되었다.

그림 3의 오른쪽과 같은 변화된 산업 자동화 및 제어 시스템의 개념적 구조를 기반으로 심층 방어 개념 형태의 OT 보안 툴박스를 표현해 보면 그림 4와 같다. OT 보안 툴박스는 여러 계층에서의 보안 요구사항들을 다루는 많은 기능들을 포함한다 [9]. 전통적인 OT 네트워크뿐만 아니라 OPC-UA, Modbus-TCP, EtherNet/IP, 5G NPN 위에서 OT 애플리케이션이 동작하는 환경에 사용될 OT 보안 툴박스는 그림 4와 같이 표현될 수 있다. OT 보안 툴박스의 중앙에는 OT 애플리케이션 보안 기능들이 존재하고 그 외부를 네트워크 보안 기능이 감싸고 있는 형태가 된다.

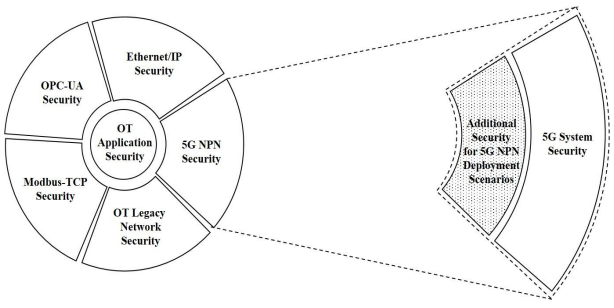

Fig. 4. OT Security Toolbox in the Form of Defense in Depth

본 논문은 산업 도메인에 5G 기술을 적용할 때 고려해야 할 보안 위협과 잠재적인 보안 요구사항을 도출하는 것을 주목적으로 하고 있기 때문에 그림 4의 “5G NPN Security” 부분을 보다 세분화할 필요가 있다.

5G 시스템을 포함하여 이동통신 시스템은 전통적으로 일반 대중에게 통신 서비스를 제공하기 위하여 개발되고 발전되어 왔다. 따라서 5G 시스템의 표준을 제정하는 3GPP는 일반적인 이동통신 서비스 제공에 필요한 보안 기능들을 표준 문서로 작성하여 제공하고 있다. 이러한 일반적인 5G 통신 서비스를 위한 보안 기능들은 그림 4의 오른쪽에 “5G System Security”로 표현되었다. 5G NPN도 기본적인 5G 통신 서비스를 활용하기 때문에 그림 4에서 “5G NPN Security”가 “5G System Security”를 포함하는 형태로 표현되었다. 그리고 산업 도메인에 5G 기술을 적용할 때 추가적으로 고려해야만 하는 보안 기능들은 그림 4에서 “Additional Security for 5G NPN Deployment Scenarios”로 표현되었다. 이상에서 서술한 본 연구의 접근방법을 도식화하면 그림 5와 같다.

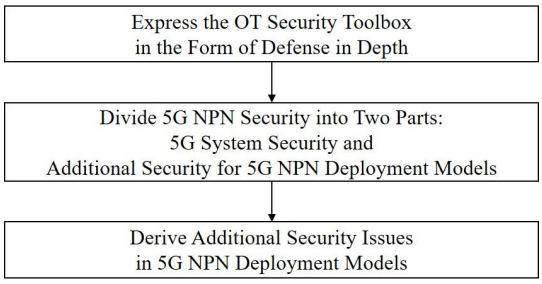

Fig. 5. Outline of Our Approach

3GPP에서도 현재 5G NPN 구축에 필요한 추가적인 보안 이슈에 대한 작업을 진행하고 있다 [10]. 따라서 본 논문에서는 IV장에서 3GPP 표준에서 다루고 있는 5G NPN 보안 이슈들에 대하여 간략히 소개한 뒤, 본 논문에서 추가적으로 도출한 5G NPN 보안 이슈들에 대하여 V장에서 개요, 보안 위협, 잠재적인 보안 요구사항의 순서로 상세히 서술한다.

IV. Security Issues in 3GPP 5G System for Vertical Services

본 장에서는 3GPP TR 33.819 [10]에서 다루고 있는 5G NPN 보안 이슈들에 대하여 간략히 소개한다. 소개할 보안 이슈들은 여섯 가지 범주로 나눌 수 있다.

1. Security for SNPNs

1.1 Completing AKA based Authentication and Calculating K_{SEAF} for SNPNs

PN에서 생성되는 키 (Key)와 SNPN에서 생성되는 키를 서로 다르게 하여 UE (User Equipment)가 접속하기 원하는 네트워크에만 연결되도록 하여야 한다는 것에 대한 이슈이다.

2. Security Aspects on Interworking between NPN and PLMN

2.1 Authentication and Authorization for Interworking, Roaming between NPN and PLMN

이 이슈는 UE가 NPN을 통해 PLMN (Public Land Mobile Network)에서 제공하는 서비스에 접근하고 사용하는 경우, 또는 그 반대의 경우, 인증 (Authentication)과 인가 (Authorization)를 위하여 무엇을 해야 하느냐에 관련된 것이다. 본 논문에서 PN과 PLMN은 동일한 네트워크이다.

2.2 Security and Privacy Aspects of Service Continuity and Session Continuity

이것은 UE가 NPN을 통해 PLMN 서비스에 접근하거나 PLMN을 통해 NPN 서비스에 접근할 때, 서비스 및 세션 연속성 (Service and Session Continuity)의 보안 측면과 관련된 이슈이다.

2.3 Independent Credentials for Authentication and Authorization with NPN and PLMN

이 이슈는 UE가 NPN을 통해 PLMN에서 제공하는 서비스에 접근하고 사용하려 할 때, 인증과 인가에 사용할 자격 증명 (Credential)의 지원 여부와 관련이 있다.

3. Security for 5GLAN services

3.1 Authentication and Authorization of UE in 5GLAN Communication

이것은 5GLAN 그룹 통신에 대한 인증 및 인가를 지원하기 위한 보다 세부적인 보안 절차가 필요하다는 것에 대한 이슈이다. 만일 그러한 보안 절차가 제공되지 않는다면, 불법적인 UE가 인증 및 인가 없이 5GLAN 유형의 서비스에 접근할 수 있게 된다.

3.2 UP Security Policy for the 5GLAN Group

이 이슈는 하나의 동일한 5GLAN 그룹에 속하는 UE가 설정한 여러 PDU 세션에 대해 5G Core Network가 UP (User Plane) 보안 정책에서 서로 다른 UP 보안 구성을 적용하는 경우, 발생할 수 있는 문제에 대한 것이다.

4. Security for TSC and 5GS interaction

4.1 Protection of Interfaces that 5G System Interacts with a TSN Network

5G 시스템은 IEEE 802.1Q가 정의한 TSN (Time Sensitive Networking)과 통합될 수 있다. 3GPP TS 23.501 [15]에 정의된 TSC (Time Sensitive Communication)는 5G 시스템이 외부 IEEE TSN 네트워크의 브리지로서 투명하게 통합될 수 있도록 한다. 이 이슈는 5G 시스템이 TSN 브리지로서 제공하는 인터페이스를 적절하게 보호해야 한다는 것과 관련이 있다.

4.2 TSC Time Synchronisation

TSC 서비스를 제공하는 5G 시스템에서 시간 동기화가 필수적이다. 이 이슈는 gPTP(Generalized Precision Time Protocol) 메시지의 전송 보호에 대한 것이다.

5. Authentication on NPNs

5.1 Key Hierarchy for NPNs

3GPP의 키 계층 구조 (Key Hierarchy)는 UE를 인증하는 것에 AKA (Authentication and Key Agreement) 방법이 사용된다고 가정한다. 그러나 이러한 가정이 NPN에서도 사실이라고 말할 수는 없다. 이 이슈는 비-AKA 방법에서의 키 생성에 대한 것이다.

5.2 Authentication and Authorization of NPN Subscribers by an AAA

SNPN은 자격증명과 인증 방법에 제한을 두지 않고 있다. 이 이슈는 NPN 운영자가 기기나 사용자 인증 및 인가를 위하여 일반적으로 사용하는 AAA (Authentication, Authorization, Accounting)와 관련된 것이다.

6. Security for PNiNPNs

6.1 (D)DoS Attack by Large Number of Registration Requests to CAG Cell

3GPP에서 PNiNPN (PN integrated NPN)은 CAG (Closed Access Group) 및/또는 네트워크 슬라이싱을 사용하는 PLMN의 지원을 받아 구축되는 NPN을 의미한다. CAG는 UE가 사용할 수 없는 NPN 전용 네트워크 슬라이스에 접근하려는 것을 막기 위하여 도입된 메커니즘이다. 이 때, 다수의 악의적인 UE가 존재한다면, 그 UE들은 CAG 셀을 통해 네트워크에 접속하려 시도할 수 있다. 이 이슈는 이상에서 언급한 방법을 통해 5G 시스템에 대하여 시도될 수 있는 DoS (Denial of Service) 또는 DDoS (Distributed DoS) 공격과 관련이 있다.

6.2 CAG ID Privacy

이것은 CAG ID가 등록 요청 메시지에 평문 (Plaintext) 형태로 포함된다는 사실과 관련된 보안 이슈이다.

6.3 DoS Attack by Unauthorized Removal of Entries from the UE's Allowed CAG ID List

이것은 등록 거절 메시지가 보호되지 않을 경우, 능동적 공격자가 적절한 코드를 가진 등록 거절 메시지를 UE에 보냄으로써 UE로 하여금 자신의 허용 CAG 목록에서 특정 CAG ID를 스스로 제거하도록 하는 것과 관련된 이슈이다.

V. Additional Security Issues in 5G NPN Deployment Models of 5G-ACIA

본 장에서는 5G NPN 구축 모델의 적합성을 평가할 때 사용되는 3GPP 정의 서비스 속성 [5] 및 5G-ACIA가 선정한 네 가지 OT 보안 속성 [9]과 관련하여 발생 가능한 보안 이슈를 도출한다. 도출된 보안 이슈들은 세 가지 범주로 나눠지며, 각각의 이슈들은 개요, 보안 위협, 잠재적인 보안 요구사항의 순서로 서술된다.

1. Device Connectivity and Isolation via Network Perimeter Protection

IoT 네트워크에서의 사이버 공격을 시연한 연구 [11]에서는 중간자 공격의 가능성을 증명하기 위하여 그림 6과 같은 플랫폼을 구성하였다.

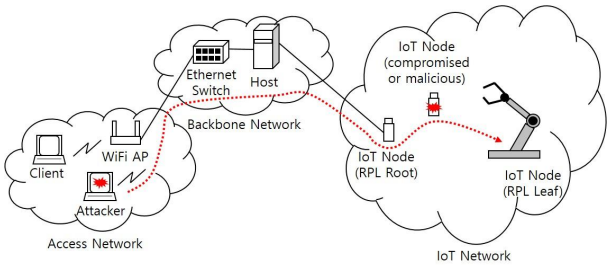

Fig. 6. A Small IoT Platform Illustrating a Man-In-The-Middle Attack

연구 [11]에서는 IoT 네트워크를 구축하는 단계에 악의적인 코드를 가지고 있는 노드가 설치되었고, 이 악의적은 노드는 외부의 공격자가 명령을 내릴 때까지 정상적인 노드인 것처럼 동작한다고 가정한다. 이 악의적인 노드는 정상적인 노드처럼 동작하는 동안, 라우팅 토폴로지에서 루트 노드에 가능한 가까운 라우터 노드로 선택되고자 노력

한다. 결과가 성공적이면 악의적인 노드는 공격자가 원하는 시점에 언제든지 중간자 공격을 시도할 수 있게 된다.

이상에서 설명한 내부자 공격은 신뢰할 수 없는 기관에 의해 제조되거나 프로그램된 장치에 의해 언제든지 발생 가능하다. 일반적으로 IoT와 같은 네트워크를 구축할 때, Closed-Source Firmware가 로딩되어 있는 노드들이 포함될 수 있기 때문에 이러한 종류의 내부자 공격은 현실적인 위협으로 인식되고 있다 [11].

그림 6과 유사하게 그림 1의 5G NPN 구축 모델에도 악의적인 노드가 존재할 수 있고, 그러한 노드는 외부의 C&C (Command and Control) 서버에 접속하여 공격 명령 수신을 시도할 수 있다.

이러한 형태의 위협은 5G NPN 구축 모델 관련 3GPP 정의 서비스 속성인 “Device Connectivity” 및 5G-ACIA가 선정한 OT 보안 속성인 “Isolation via Network Perimeter Protection”과 연관된다. 이와 관련하여 다음과 같은 세 가지 보안 이슈들을 도출하였다.

1.1 Security for UEs Authorized to Access Services External to NPN in Aspects of Global Connectivity

5G-ACIA가 선정한 OT 보안 속성인 “Isolation via Network Perimeter Protection”에 따르면 OT 네트워크는 외부와 격리되어야 한다 [9]. 그런데 5G NPN 구축 모델 관련 3GPP 정의 서비스 속성인 “Device Connectivity”에 속한 “Global Connectivity”에 따르면 NPN의 UE가 NPN 외부 서비스에 접속할 수 있다 [5].

1.1.1 Security Threats

SNPN으로 구축된다고 하더라도 [5]에 따르면 PLMN에 가입되지 않은 UE가 방화벽을 통한 외부와의 선택적인 연결을 활용할 수 있다. 즉 그림 1의 (a)에 표시된 방화벽을 통해 UE가 NPN 외부의 서비스에 접속하는 것이 가능하다.

또한 NPN과 PLMN에 모두 가입된 (즉, 이중 가입된) UE는 NPN 내부에 위치하면서 방화벽을 통한 외부와의 선택적 연결을 활용하지 않고도 NPN 외부 서비스 접속이 가능하다. 즉 PLMN을 통해 UE가 NPN 외부의 서비스에 접속하는 것이 가능하다.

이와 같이, UE가 NPN 외부의 서비스에 접속 가능하다면 NPN 내부의 악의적인 UE는 NPN 외부에 존재하는 C&C 서버나 공격자에게 접속할 수 있다.

1.1.2 Potential Security Requirements

NPN의 UE가 접속할 수 있는 NPN 외부 서비스의 종류와 범위가 명확하게 정의되고 관리되어야 한다.

NPN의 UE가 접속할 수 있는 NPN 외부 서비스는 사전 승인된 것이어야 하며, 사전 승인되지 않은 NPN 외부 서비스 접속은 NPN의 방화벽 및 PLMN에 의하여 차단되어야 한다.

NPN 외부 서비스 접속 시도가 차단된 UE들을 위한 별도의 보안 절차가 필요하다. 즉 NPN으로부터 해당 UE의 분리/제거 등에 대한 절차가 필요하다.

1.2 Security for UEs Authorized to Access NPN Services Outside NPN in Aspects of Global Connectivity

5G-ACIA가 선정한 OT 보안 속성인 “Isolation via Network Perimeter Protection”에 따르면 OT 네트워크는 외부와 격리되어야 한다 [9]. 그런데 5G NPN 구축 모델 관련 3GPP 정의 서비스 속성인 “Device Connectivity”에 따르면 NPN의 UE는 NPN 외부로 이동한 후에도 NPN 서비스를 이용할 수 있다 [5]. 이것을 로밍(Roaming)의 경우와 서비스 연속성의 경우로 나누어 생각해 볼 수 있다. 먼저 로밍의 경우를 다룬다.

1.2.1 Security Threats

그림 1의 (d)를 제외한 나머지 세 가지 구축 모델에서는 NPN 외부로 이동한 UE가 방화벽을 통한 외부와의 선택적 연결을 활용하여 PLMN으로부터 NPN 서비스에 접속할 수 있다 [5].

UE가 PLMN으로 로밍하였기 때문에 악의적인 노드인 UE는 NPN 외부에 존재하는 C&C 서버나 공격자에게 접속하고 공격 명령을 수신한 이후 NPN 서비스에 접속을 시도할 수 있다.

1.2.2 Potential Security Requirements

PLMN에 가입된 UE에 대하여 UE가 접속할 수 있는 NPN 외부 서비스의 종류와 범위가 명확하게 정의되고 관리되어야 한다.

PLMN에 가입된 UE에 대하여 UE가 접속할 수 있는 NPN 외부 서비스는 사전 승인된 것이어야 하며 사전 승인되지 않은 NPN 외부 서비스 접속은 PLMN에 의하여 차단되어야 한다.

PLMN에 위치한 (즉, NPN을 벗어난) NPN의 UE가 NPN 서비스에 접속하려 시도하기 전에 PLMN에서 접속 시도한 서비스 모두에 대한 이력 관리가 필요하다. NPN을 벗어난 이후 서비스 접속 시도가 차단된 적이 없는 UE의 NPN 서비스에 대한 접속 절차만 시작이 허용되어야 한다.

1.3 Security for UEs in Aspects of Service Continuity

1.2에서 로밍에 대하여 다루었으므로 여기에서는 NPN에서 시작된 서비스가 UE의 이동 중에도 계속 사용 가능한 것을 의미하는 서비스 연속성의 경우를 다룬다.

1.3.1 Security Threats

IV장에서 살펴본 보안 이슈 중에 "2.2 Security and Privacy Aspects of Service Continuity and Session Continuity"라는 이슈가 있었다. 이 이슈는 N3IWF (Non-3GPP InterWorking Function)를 사용하여 서비스 연속성을 제공하는 경우에 관한 것이었다.

그 이슈와 구별하여 여기에서 다루고자 하는 위협은 N3IWF를 활용하는 서비스 연속성이 보안 문제없이 안전하게 제공된다고 하더라도, 악의적인 노드인 UE는 NPN 서비스를 사용하는 동안에 여전히 NPN 외부에 존재하는 C&C 서버나 공격자에게 접속할 수 있다는 것과 관련이 있다. 참고로 NPN의 UE가 PLMN으로 이동하면서 서비스 연속성을 제공받고 있다면, 이는 NPN이 N3IWF를 통해 PLMN의 RAN과 연결되어 있는 형태가 된다. 따라서 본 이슈에서의 보안 위협은 앞서 서술한 1.1.1의 보안 위협과 유사하다.

1.3.2 Potential Security Requirements

1.1.2에 서술된 잠재적인 보안 요구사항의 내용과 동일하다.

2. Device Connectivity and Trust Domains in OT Networks

IEC 62443 표준은 산업 자동화 제어 시스템에 대하여 다루고 있으며, 이 분야에서 보안 관리에 대한 가장 중요한 표준으로 널리 받아들여지고 있다. IEC 62443 표준 시리즈는 크고 복잡한 산업 자동화 제어 시스템에 대하여 보안 구역 (Security Zone)에 대한 개념을 사용하고 있다.

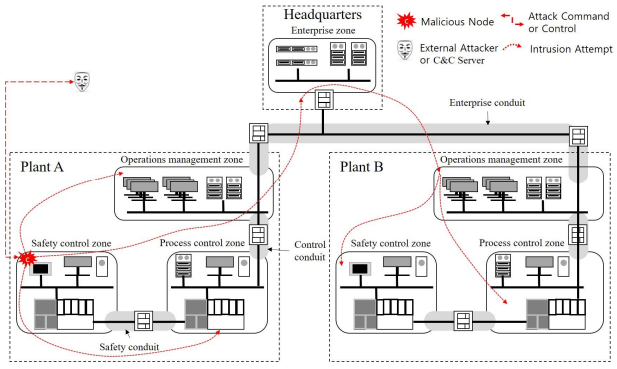

Fig. 7. Example of Zones and Conduits

그림 7은 두 개의 생산 플랜트 (Plant)가 본사에 의해 감독되는 IEC 62443 보안 설계와 퍼듀 모델 (Purdue Model)에 기초한 산업 자동화 제어 시스템의 예제 [9]에 악의적인 노드와 C&C 서버를 추가한 그림이다. 그림 7에서 공정 제어 (Process Control), 안전 제어 (Safety Control), 운영 관리 (Operation Management)를 위한 세 개의 보안 구역을 플랜트 내에 조성하였다.

보안 구역 내의 자산이 가치를 생산하려면 일반적으로 정보는 보안 구역 내에서뿐만 아니라 보안 구역 외부로도 전달되어야 한다. 이를 위해 IEC 62443 표준 시리즈는 정보 흐름의 보안 측면을 다루는 도관 (Conduit)이라는 개념을 도입하였다. 도관은 보안 구역 사이의 경계를 가로지르는 정보 흐름을 묶어 놓은 것이다. 도관은 물리적이거나 가상적일 수 있다. 또한 도관을 통해 이루어지는 통신을 검증하기 위하여 도관에 방화벽을 설치할 수도 있다 [9]. 만일 도관에 충분한 보안이 제공되지 않는다면, 그림 7에서와 같이 내부의 악의적인 노드가 다른 보안 구역으로의 침투를 시도할 수 있다.

이상의 내용은 5G-ACIA가 선정한 OT 보안 속성인 "Alignment with Trust Domains in OT Networks"와 연관된다. 이와 관련하여 다음과 같은 한 가지 보안 이슈를 도출하였다.

2.1 Security for Virtual Conduits between Security Zones

여러 개의 네트워크 슬라이스로 두 개의 플랜트를 구축한 예를 그림으로 표현하면 그림 8과 같다 [12]. 그림 8은 세 개의 전용 네트워크 슬라이스로 구축된 두 개의 플랜트가 하나의 네트워크 슬라이스를 공유하고 있는 구조를 보여준다.

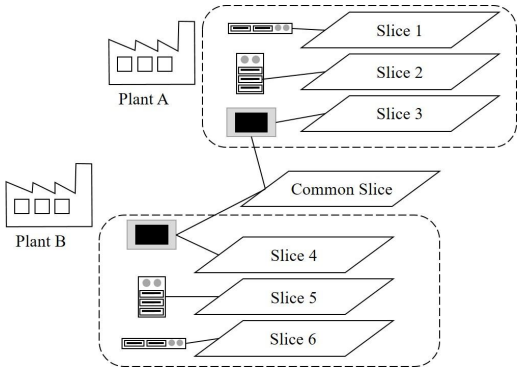

Fig. 8. Example of Sharing a Network Slice

그런데 그림 8과 같이 두 개의 다른 플랜트에 속한 장치들이 서로 통신하기 위하여 하나의 네트워크 슬라이스를

공유한다면, 공유 슬라이스에 연결된 모든 장치는 서로의 존재를 알 수 있고 접속을 시도할 수 있게 된다.

이를 막기 위해서는 여러 개의 공유 슬라이스를 만들고 서로를 발견할 필요가 없는 노드들을 격리하여야 한다. 또는 도관의 개념과 같은 보안이 제공되는 적절한 슬라이스 간 상호 연결 방법이 제공되어야 한다.

2.1.1 Security Threats

OT 네트워크에서의 신뢰 도메인 (Trust Domain) 또는 산업 자동화 제어 시스템에서의 보안 구역을 네트워크 슬라이싱 기술로 구현하고자 할 때, 도관을 구현할 적절한 방법이 필요하다.

도관을 공유 슬라이스로 구현할 경우, 하나의 공유 슬라이스로 구현한다면 서로 보이지 않아야 할 노드들이 서로를 발견할 수 있고, 여러 개의 공유 슬라이스로 구현한다면, 하나의 도관을 위해 생성해야 하는 네트워크 슬라이스의 수가 늘어나서 유지 및 관리 비용이 증가할 수 있다.

공유 슬라이스에 연결되는 장치들을 게이트웨이 (즉, 슬라이스 간 통신을 담당하는 노드)로 구성하는 경우, 충분한 보안이 제공되지 않는다면, 그림 7에서와 같이 내부의 악의적인 노드가 다른 보안 구역으로의 침투를 시도할 수 있다.

2.1.2 Potential Security Requirements

신뢰 도메인 또는 보안 구역을 연결하는 도관은 상호 통신이 허용된 노드들만 서로를 발견하고 정보를 교환하도록 허용하여야 한다.

3. QoS and Authentication

5G NPN을 구축하려는 많은 기업들이 이미 AAA 서버를 사용하고 있기 때문에 5G-ACIA의 NPN 구축 모델에서 AAA 서버에 대하여 고려할 필요가 있다.

SNPN에서 UE의 인증 절차와 관련하여 3GPP TR 33.819 [10]는 그림 9와 같이 두 가지 옵션을 제시하고 있다. 첫 번째 옵션은 “SNPN-without AAA”이고 두 번째 옵션은 “SNPN-with-AAA”이다.

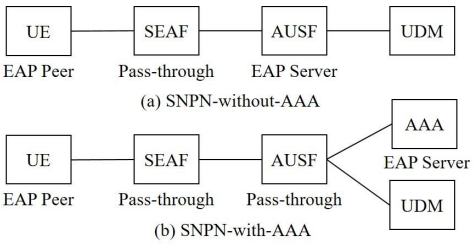

Fig. 9. Two Options of Deploying Authentication Schemes for 5G SNPN

SNPN이 인증을 위하여 AAA 서버를 사용하는 옵션에서는 AUSF (Authentication Function)의 역할이 AAA 서버와 연동되도록 설계된 방식에 따라 달라질 수 있다. AUSF는 EAP (Extensible Authentication Protocol) 서버 역할을 수행하거나, “pass-through authenticator” 역할을 수행하거나, 아무런 역할을 수행하지 않을 수 있다.

그림 9의 (a)에서, SNPN은 인증을 위하여 AAA 서버를 사용하지 않고 5G의 인증 기능을 사용한다. 이 옵션에서는 UDM (Unified Data Management)이 인증 방법을 선택할 수 있으며, 해당 인증 방법은 UE와 AUSF에서 구현된다. 그림 9의 (b)는 AUSF가 “pass-through authenticator” 역할을 수행하고, AAA가 EAP 서버 역할을 수행하는 경우를 보여준다.

이러한 구축 옵션은 5G NPN 구축 모델 관련 3GPP 정의 서비스 속성인 “QoS” 및 5G-ACIA가 선정한 OT 보안 속성인 “Authentication and Secure Storage and Processing of Credentials”와 연관된다. 이와 관련하여 다음과 같은 한 가지 보안 이슈를 도출하였다.

3.1 AAA Authentication Completion Time of NPN Subscribers Using the URLLC Service

5G-ACIA가 선정한 OT 보안 속성인 “Authentication and Secure Storage and Processing of Credentials”에 따르면 OT 네트워크의 장치들은 인증을 필요로 하며 자격 증명을 안전하게 저장하고 처리하여야 한다 [9]. 그런데 5G NPN 구축 모델 관련 3GPP 정의 서비스 속성인 “QoS”에 속한 “Latency”에 따르면 다양한 응용에서 요구하는 최대 허용 종단간 지연시간 내에 서비스를 제공하여야 한다 [5].

3.1.1 Security Threats

[14]에 따르면 URLLC (Ultra-Reliable, Low-Latency Communication)는 액세스 인증, 전송 보호 및 보안 컨텍스트에 대한 낮은 지연시간을 필요로 한다. 또한 3GPP TR 33.825 [13]는 낮은 지연시간을 위한 인증 및 키 합의 프로시저의 가속화가 필요하다고 명세하고 있다. 이상의 내용은 URLLC에서의 인증 절차와 데이터 송수신이 주어진 짧은 시간 내에 완료되어야 한다는 것을 의미한다.

“SNPN-with-AAA”에서 AAA 서버는 5G 장치뿐만 아니라 기업 내의 5G 통신을 사용하지 않는 많은 장치들의 인증도 담당할 수 있다. 5G 통신을 사용하지 않는 장치들 중에서 악의적인 노드들이 존재한다면, AAA 서버에 대하여 DoS 또는 DDoS 공격을 시도할 수 있다. 악의적인 노드가 존재하지 않더라도 많은 수의 장치들에 의하여 AAA 서버의 서비스가 지연될 수 있다.

만일 AAA 서버의 서비스가 지연되거나 제공되지 않는다면 URLLC 서비스를 사용하는 장치의 운영에 문제가 발생할 수 있고, 그 결과, 5G SNPN의 가용성에 문제가 발생할 수 있다.

3.1.2 Potential Security Requirements

"SNPN-with-AAA"에서 URLLC 서비스를 사용하는 장치의 인증을 담당하는 AAA 서버는 요구되는 시간 내에 인증 절차를 완료할 수 있어야 한다.

이러한 요구사항을 만족할 수 없다면, URLLC 서비스를 사용하는 5G 장치들에 대하여 "SNPN-without-AAA"의 사용을 우선적으로 고려하여야 한다.

VI. Conclusions

최근 4차 산업혁명이라는 개념이 구체화되면서 OT 분야에 인공지능 및 5G 이동통신 시스템과 같은 최신 IT 기술을 적용하려는 노력이 추진되고 있다. 5G 시스템은 미래 스마트 팩토리의 유연성 (Flexibility), 다양성 (Versatility), 유용성 (Usability) 및 효율성 (Efficiency)을 대폭 개선할 것으로 기대된다. 하지만 IT 환경과 OT 환경의 접점이 확대될수록 사이버 보안 위협에 대한 우려가 커질 수밖에 없다. 따라서 본 논문에서는 5G-ACIA의 구축 모델에 따라 5G NPN이 이산 및 공정 산업을 위하여 구축될 때, 고려되어야 할 보안 위협 및 잠재적 보안 요구사항을 도출하였다. 본 연구에서 도출된 결과물들이 산업 애플리케이션을 위한 5G NPN을 구축하는데 있어서 중요한 역할을 수행할 수 있을 것으로 기대한다.

ACKNOWLEDGEMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2020-0-00952, Development of 5G Edge Security Technology for Ensuring 5G+ Service Stability and Availability).

REFERENCES

[1] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J. J. Ramos-Munoz and J. M. Lopez-Soler, "A Survey on 5G Usage Scenarios and Traffic Models," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 905-929, 2020, doi: 10.1109/COMST.2020.2971781.

[2] J. Kim, S. Kim, "An Efficient Session Management Scheme for Low-latency Communications in 5G Systems," Journal of the Korea Society of Computer and Information, Vol. 25, No. 2, pp. 83-92, Feb. 2020.

[3] 3GPP TS 22.261 v16.11.0: "Service Requirements for the 5G System; Stage 1," March 2020.

[4] M. Wollschlaeger, T. Sauter and J. Jasperneite, "The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0," IEEE Industrial Electronics Magazine, vol. 11, no. 1, pp. 17-27, March 2017, doi: 10.1109/MIE.2017.2649104.

[5] 5G-ACIA White Paper: "5G Non-Public Networks for Industrial Scenarios," July 2019.

[6] N. Papakonstantinou, J. Linnosmaa, A. Z. Bashir, T. Malm and D. L. V. Bossuyt, "Early Combined Safety - Security Defense in Depth Assessment of Complex Systems," 2020 Annual Reliability and Maintainability Symposium (RAMS), Palm Springs, CA, USA, 2020, pp. 1-7, doi: 10.1109/RAMS48030.2020.9153599.

[7] 3GPP TS 23.251 v16.0.0: "Network Sharing; Architecture and Functional Description," July 2020.

[8] K. Goztepe, R. Kilic, and A. Kayaalp, "Cyber Defense in Depth: Designing Cyber Security Agency Organization for Turkey," Journal of Naval Science and Engineering, Vol. 10, No. 1, pp. 1-24, 2014.

[9] 5G-ACIA White Paper: "Security Aspects of 5G for Industrial Networks," May 2020.

[10] 3GPP TR 33.819 v16.1.0: "Study on Security Enhancements of 5G System (5GS) for Vertical and Local Area Network (LAN) Services," July 2020.

[11] R. E. Navas, H. L. Bouder, N. Cuppens, F. Cuppens, G. Z. Papadopoulos, "Demo: Do Not Trust Your Neighbors! A Small IoT Platform Illustrating a Man-in-the-Middle Attack," Proceedings of the 17th International Conference on Ad Hoc Networks and Wireless, pp. 120-125, September 2018.

[12] P. Porambage, Y. Miche, A. Kalliola, M. Liyanage and M. Ylianttila, "Secure Keying Scheme for Network Slicing in 5G Architecture," 2019 IEEE Conference on Standards for Communications and Networking (CSCN), GRANADA, Spain, 2019, pp. 1-6, doi: 10.1109/CSCN.2019.8931330.

[13] 3GPP TR 33.825 v16.0.1: "Study on the Security of Ultra-Reliable Low-Latency Communication (URLLC) for the 5G System

(5GS),” Oct. 2019.
[14] Huawei, “5G Scenarios and Security Design,” November 2016.

Authors

Tae-Keun Park received his B.S., M.S., and Ph.D. degrees in Computer Science and Engineering from POSTECH, Pohang, Korea in 1991, 1993, and 2004, respectively. He joined POSTECH PIRL in 1993 and moved to SK Telecom in 1996. From 2000 to 2001 and from 2001 to 2002, he worked for 3Com Korea and Ericsson Korea, respectively. In 2004, he joined in the department of Multimedia Engineering, Dankook University, Korea. He is currently on the faculty of the department of Computer Engineering at Dankook University. His research interests include network security, IoT, wireless/mobile communications, and distributed services.

Jong-Geun Park received his BS and MS degree in industrial engineering from SungKyunKwan University, Rep. of Korea, in 1997 and 1999, respectively, and received his PhD degree in computer engineering from Chungnam National University, Rep. of Korea, in 2013. From 1999 to 2001, he was a researcher at ADD, Daejeon, Rep. of Korea. Then, he joined ETRI, Daejeon, Rep. of Korea, in 2001, where he is currently working as a principal researcher. Currently, he is interested in mobile network security, SDN/NFV, and Cloud security.

Keewon Kim received the M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Korea, in 2001 and 2006, respectively. He is currently an assistant professor in the department of Computer Engineering, Dankook University. He is interested in information security, security protocol, VLSI, and big data analysis.