JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 27 No. 12, pp. 131-139, December 2022
https://doi.org/10.9708/jksci.2022.27.12.131

A Study on the Authenticity Verification of UxNB Assisting Terrestrial Base Stations

Keewon Kim*, Kyungmin Park**, Jonghyun Kim**, Tae-Keun Park***

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

[Abstract]

In this paper, to verify the authenticity of UxNB that assists terrestrial base stations, the solutions for SI (System Information) security presented in 3GPP TR 33.809 are analyzed from the perspective of UxNB. According to the definition of 3GPP (Third Generation Partnership Project), UxNB is a base station mounted on a UAV (Unmanned Aerial Vehicle), is carried in the air by the UAV, and is a radio access node that provides a connection to the UE (User Equipment). Such solutions for SI security can be classified into hash based, MAC (Message Authentication Codes) based, and digital signature based, and a representative solution for each category is introduced one by one. From the perspective of verifying the authenticity of UxNB for each solution, we compare and analyze the solutions in terms of provisioning information and update, security information leakage of UxNB, and additionally required amount of computation and transmission. As a result of the analysis, the solution for verifying the authenticity of the UxNB should minimize the secret information to be stored in the UxNB, be stored in a secure place, and apply encryption when it is updated over the air. In addition, due to the properties of the low computing power of UxNB and the lack of power, it is necessary to minimize the amount of computation and transmission.

▸ **Key words**: Mobile Communication, 3GPP standard, UxNB, System Information, Authenticity

• First Author: Keewon Kim, Corresponding Author: Tae-Keun Park
*Keewon Kim (kwkim@mmu.ac.kr), Dept. of Computer Engineering, Mokpo National Maritime University
**Kyungmin Park (kmpark@etri.re.kr), Information Security Research Division, ETRI
**Jonghyun Kim (jhk@etri.re.kr), Information Security Research Division, ETRI
***Tae-Keun Park (tkpark@dankook.ac.kr), Dept. of Computer Engineering, Dankook University
• Received: 2022. 11. 04, Revised: 2022. 11. 28, Accepted: 2022. 11. 29.

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

[요 약]

본 논문에서는 지상 기지국을 보조하는 UxNB의 진본성 검증을 위해, 3GPP TR 33.809에 제시된 시스템 정보(System Information) 보안을 위한 솔루션들을 UxNB 관점에서 분석한다. 3GPP(Third Generation Partnership Project)의 정의에 따르면, UxNB는 UAV(Unmanned Aerial Vehicle)에 탑재한 기지국(Base Station)이며, UAV에 의해 공중에서 운반되며 UE(User Equipment)에게 연결을 제공하는 무선 접속 노드이다. 시스템 정보(System Information) 보안을 위한 솔루션들은 해시(Hash) 기반, MAC(Message Authentication Codes) 기반, 디지털 서명(Digital Signature) 기반으로 분류할 수 있으며, 각 범주별로 대표적인 솔루션을 하나씩 소개한다. 각 솔루션별로 UxNB의 진본성 검증 관점에서 사전 배포 정보 및 업데이트, UxNB의 보안 정보 유출, 추가적으로 요구되는 연산량 및 전송량 측면에서 해당 솔루션들을 비교 분석한다. 분석 결과, UxNB의 진본성 검증을 위한 솔루션은 UxNB에 저장될 비밀 정보가 최소화되어야 하고, 안전한 장소에 저장되어야 하고, 무선으로 업데이트되면 이를 위해서 암호화를 적용해야 한다. 또한 UxNB의 낮은 컴퓨팅 파워와 전원 부족의 특성으로 인하여 연산량 및 전송량을 최소화해야 한다.

▸ **주제어**: 이동통신, 3GPP 표준, UxNB, 시스템 정보, 진본성

I. Introduction

무인 비행체(UAV: Unmanned Aerial Vehicle)의 배치 용이성, 낮은 구매 및 유지보수 비용, 및 기동성 등의 특징과 호버링(hovering) 능력으로 인하여, 이동통신 환경에서 무인 비행체는 재난 상황 모니터링, 긴급 지원 등의 다양한 응용에서 활용도가 높다 [1].

최근에 이동통신 환경에서 무인 비행체를 다양한 응용에 적용할 경우 발생할 수 있는 다양한 문제들을 해결하기 위해 많은 연구들이 진행되었다 [2]-[6].

UAS(Unmanned Aircraft System)는 무선 통신을 사용하는 UAV(Unmanned Aerial Vehicle)와 컨트롤러로 구성되며, UAV의 원격 조종과 자율 운항을 위한 제어를 위해서는 무선 네트워크 연결이 필요하다. Abdalla와 Marojevic [2]는 무선 네트워크로 연결된 UAS의 활성화를 위해 진행 중인 3GPP(Third Generation Partnership Project) 표준화 활동을 조사하고, 이동 통신 네트워크를 통해 UAS 트래픽 관리, 다른 사용자와 통신할 UAV와 RC(Remote Controller)에 의해 제공될 요구 사항, 예상 아키텍처 및 서비스를 제시하였다.

Alfattani 등[3]은 항공 플랫폼(Aerial Platform) 환경에서 신호 반사를 활용하는 RSS(Reconfigurable Smart Surfaces) 기술과 RSS를 항공 플랫폼에서 사용하는 방법과 제어 아키텍처를 제안하였다.

3GPP 5G NR(New Radio) 네트워크를 사용하여 단일 UAV를 인증하는 경우, UAV와 5G 코어 네트워크간 인증과 UAV와 UAV 제어 스테이션 간 인증이 필요하다. 화물 배달 등과 같은 응용을 위해서 UAV 군집을 활용할 경우, 이러한 UAV 군집은 이동성이 높아서 여러 차례의 핸드오버가 필요하다. Aydin 등[4]은 AV 군집을 위한 효율적인 인증과 그룹 기반 핸드오버 방법을 제안하였다.

이동통신 표준을 주도하고 있는 3GPP는 UAV에 탑재한 기지국(BS, Base Station)을 "UE(User Equipment)에 연결을 제공하는 무선 접속 노드로 UAV에 의해 공중에서 운반되는 것"으로 약칭 UxNB로 정의하고 있다[7]. 이러한 UxNB는 경기장, 콘서트장과 같이 UE가 밀집한 장소에서 지상 기지국을 보조하여 사용할 수 있는 솔루션이다. 즉, 빠른 배치 특성을 가진 UxNB는 서비스 품질을 보장하기 위해 비지상 영역으로 이동통신망을 확장할 수 있다. Aydin 등[5]은 지상 기지국과 UxNB 간의 인증 방법과 UE들을 그룹 단위로 지상 기지국에서 UxNB로 핸드오버 수행하는 방법을 제안하였다.

Bajracharya 등[6]은 기지국, 중계기 또는 데이터 수집 및 배포에 사용할 수 있는 5G 기반 WID(Wireless Infrastructure Drone)를 제안하였다. WID는 UAV를 기반으로 하는 무선 통신 시스템으로 지상파 연결이 쉽지 않은 기기에게 공중 무선 연결을 제공한다. 고도 및 기능에 따라 세 가지 유형의 WID 플랫폼이 있다. 플랫폼의 종류는 지상 15km~25km 사이의 고고도 플랫폼(HAP), 5km~15km 사이의 중고도 플랫폼(MAP), 지면에서 5km

사이의 저고도 플랫폼(LAP)이 있다.

기지국의 커버리지 영역 내에 있는 단말의 수가 증가함에 따라 통신 서비스 품질이 저하되는 경향이 있다. UxNB의 사용을 통해 경기장과 콘서트장과 같이 일시적으로 UE가 밀집하는 장소에서 통신 서비스 품질 저하 문제 해결을 위해 사용할 수 있지만, 기지국과 코어 네트워크 사이가 무선으로 연결 되어야 하므로 새로운 보안 문제가 발생할 수 있다. 특히, UxNB와 네트워크간의 상호 인증 및 UxNB의 신뢰성 보장 등이 필요하며, UxNB 탈취에 의한 정보 유출 등의 보안 문제가 발생할 수 있다.

최근 5G 이동통신 네트워크에서의 보안 취약점에 관한 연구가 진행되었다 [8]-[13]. Hussain 등[8]은 5G 이동통신 네트워크의 RRC (Radio Resource Control) 계층과 NAS (Non-Access Stratum) 계층에 대한 정형적인 보안 검증을 위해 5GReasoner라는 프레임워크를 제안하고, 이를 활용하여 이동통신 네트워크의 보안 취약점을 식별하였다. 최근 연구 [9]-[11]에서 5GReasoner에서 제시된 공격에 대해 3GPP 표준 규격 기반으로 분석하여 공격의 일부 혹은 전체가 실현 불가능한 것임이 보였다. Zhang 등[12]은 5G Null 보안 알고리즘에 대해 IP 스푸핑 공격(IP Spoofing Attack)과 SUPI 캐칭 공격(SUPI Catching Attack)을 제시하였다. Zhang 등[12]이 제안한 공격에 대해 Park 등[13]은 3GPP 표준 규격 기반으로 분석하여 IP 스푸핑 공격이 실현 불가능한 것임을 보였다.

또 다른 보안 취약점 연구로, 5G 이동통신에서 허위 기지국(False Base Station)에 관련된 보안 이슈 및 솔루션이 3GPP TR 33.809[14]에서 제시되었다. 5G 이동통신의 보안 취약점 발생의 대표적인 원인 중 하나는 기지국이 브로드캐스트하는 SI(System Information)에 대한 보안이 보장되지 않기 때문이다. 이러한 SI 보안과 관련하여 3GPP TR 33.809[14]에서 Key Issue #2 (Security Protection of System Information)로 제시되었고, Key Issue #2를 해결하기 위한 솔루션들도 제시되었다. UE가 지상 기지국을 보조하는 UxNB의 진본성(Authenticity)을 검증을 위해, 먼저 UxNB가 브로드캐스트하는 SI의 보호가 필요하다.

본 논문에서는 먼저 3GPP TR 33.809[14]에서 Key Issue #2를 해결하기 위해 제시된 솔루션들을 분류하고 각 범주별로 대표적인 솔루션을 하나씩 간략하게 소개한다. 다음으로, 지상 기지국을 보조하는 UxNB의 진본성 검증 관점에서 사전 배포 정보 및 업데이트, UxNB의 보안 정보 유출, 추가적으로 요구되는 연산량 및 전송량 측면에서 해당 솔루션들을 비교 분석한다. 본 논문의 구성은 다음과 같다. 제 2장에서 3GPP TR 33.809[14]의 Key Issue #2와 솔루션을 소개한 뒤, 제 3장에서 지상 기지국을 보조하는 UxNB의 진본성 검증 관점에서 각 솔루션을 분석한다. 마지막으로 제 4장에서 결론을 기술한다.

II. Key Issue and Solutions in 3GPP TR 33.809

본 장에서는 SI(System Information)에 대해 간략하게 정리한 뒤, SI 보안과 관련하여 3GPP TR 33.809[14]의 Key Issue #2 (security protection of system information)와 이를 해결하기 위한 솔루션들에 대하여 소개한다.

1. Key Issue #2 Security protection of system information

5G 이동통신의 셀은 주기적으로 동기 신호와 SI를 브로드캐스트하며, 이것은 RRC 프로토콜의 기능 중 하나이다. 상태가 IDLE 또는 INACTIVE UE는 셀의 SI를 모니터링하고, 연결에 적합한 셀을 선택하여 초기 액세스를 수행한 후, 네트워크에 연결한다. SI의 구성 요소는 셀(재)선택 매개변수, 인접 셀 정보, 주파수 우선순위, 블랙리스트 셀, 공통 채널 구성 정보, NAS 공통 정보, 공공경고 시스템(Public Warning System) 메시지 등이 있다.

3GPP TR 33.809[14]에서의 Key Issue #2는 허위 SI 메시지 브로드캐스트 및 재생 공격을 수행하는 무선 공격자로부터 SI 보호에 관한 주제를 다루고 있다. 이러한 Key Issue #2를 해결하기 위한 솔루션들이 3GPP TR 33.809[14]에 제시되었다. 제시된 솔루션들은 해시(Hash) 기반 솔루션, MAC(Message Authentication Codes) 기반 솔루션, 디지털 서명(Digital Signatreu) 기반 솔루션으로 분류될 수 있다. 다음 절에서 각 범주별로 대표적인 솔루션을 하나씩 간략하게 소개한다.

2. Hash based solution

3GPP TR 33.809[14]의 해시 기반 솔루션 중에서 “Solution #14: Shared key based MIB/SIBs protection”에 대해 소개한다. 이 솔루션의 아이디어는 UE가 AS 보안 컨텍스트를 설정한 후에 네트워크 액세스를 위한 초기 단계에서 수신한 MIB(Master Information Block)/SIB(System Information Block)의 해시 값을 gNB(gNodeB)에게 보고한다. UE가 전송한 MIB/SIB의 해시 값을 gNB가 수신한 후, gNB가 해시 값의 정확성을 검

증한다. 검증에 실패하면, gNB는 불일치를 표시하고 추가적으로 MIB/SIB를 UE에게 제공한다.

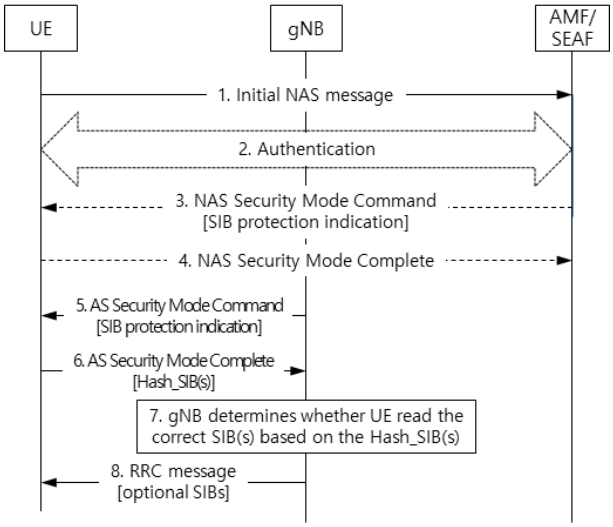

Fig. 1. System Information Protection of Solution #14 [14]

Fig. 1은 솔루션 #14의 SI 보호 절차를 나타내며, 각 단계는 다음과 같다.

1. UE는 초기 NAS 메시지를 네트워크에게 전송한다.
2. (선택적) UE는 네트워크와 Primary Authentication을 수행한다.
3. (선택적) AMF는 “NAS Security Mode Command”를 SI 보호 지원 표시와 함께 UE에게 전송한다. 만약 UE가 SI 보호 지원 표시를 수신하면, 이것을 보안 컨텍스트 일부로 저장한다.
4. (선택적) UE는 “NAS Security Mode Complete”를 AMF에게 전송한다.
5. gNB는 “AS Security Mode Command”를 SI 보호 지원 표시와 함께 UE에게 전송한다.
6. UE는 “AS Security Mode Complete”를 MIB/SIB의 해시 값과 함께 gNB에게 전송한다. 해시 값은 암호화되고 무결성이 보호된다. 또한 UE는 해시 값 계산에 사용된 SIB의 목록을 표시한다. MIB/SIB의 해시 값을 생성할 때, 셀의 PCI(Physical Cell Identity)가 추가로 포함된다. 하지만, MIB의 SFN(System Frame Number)은 포함되면 안된다.
7. gNB는 “AS Security Mode Complete”를 복호화하고 무결성을 검증한다. 만약 무결성 검증이 성공하면, gNB는 MIB/SIB의 해시 값을 검증한다.
8. gNB는 RRC 메시지를 UE에게 전송한다. Step 7에서 해시 검증이 실패한 경우, RRC 메시지에는 MIB/SIB가 포함된다.

요약하면, 솔루션 #14는 gNB가 브로드캐스트한 SI를 UE가 해시 값을 계산하여 gNB에게 전송한다. gNB는 그것을 수신한 후 정확성을 검증한다.

3. MAC based solution

3GPP TR 33.809[14]의 해시 기반 솔루션 중에서 “Solution #9: Using symmetric algorithm with assistance of USIM and home network”에 대해 소개한다. UE는 ME(Mobile Equipment)와 USIM(Universal Subscriber Identity Module)으로 구성된다. 이 솔루션의 아이디어는 서빙 네트워크(Serving Network)가 홈 네트워크(Home Network)의 도움으로 ME에게 암호화된 gNB의 키를 동적으로 제공하고, gNB는 대칭 알고리즘을 사용하여 무선 신호를 위한 32비트 MAC(Message Authentication Code)인 MAC-I를 생성하고, ME는 USIM의 도움으로 MAC-I를 검증한다.

이 솔루션의 전체 프레임워크는 네 개의 프로시저로 구성되며, 각 프로시저를 간략하게 살펴본다. 먼저 “Protection Key Agreement(PKA) procedure”와 “Protection Key Transfer(PKT) procedure”는 보호 키 CKp를 합의하고 전송한다. 여기서 CKp는 홈 네트워크와 USIM 간에 합의된 보호 키이며, 프로비저닝된 정보의 암호화에 사용되고 USIM 외부로 유출을 금지한다.

다음으로 “Protection Area Information Provisioning (PAIP) procedure”는 서빙 네트워크가 PA(Protection Area) 정보를 ME에게 제공한다. 하나의 보호 영역에 다수의 gNB가 있다. 등록 절차 또는 기타 초기 NAS 메시지 처리 중에, AMF(Access and Mobility Management Function)는 PA 정보(bsGKI 목록, 암호화된 루트 키(EK_{RBS}) 및 만료 시간 포함)를 ME에게 제공한다. 여기서 bsGKI는 각 SRKG를 식별하기 위한 식별자이고, SRKG는 루트 키 (K_{RBS})를 공유하고 있는 gNB의 그룹이고, EK_{RBS}는 CKp로 K_{RBS}를 암호한 것이다.

마지막으로 “Cell Authenticity procedure”는 gNB가 SI와 이에 대한 진본성을 위한 정보를 브로드캐스트하며, 이를 수신한 UE(ME와 USIM)는 PA 정보와 무선 시그널링을 이용하여 셀 진본성(cell authenticity)을 검증한다. 요약하면, 솔루션 #9는 gNB는 사전에 UE와 공유된 대칭키를 이용하여 SI의 MAC을 생성하여 SI와 같이 브로드캐스트하고, 이를 수신한 UE는 MAC 값 검증을 통해서 SI의 진본성을 결정한다.

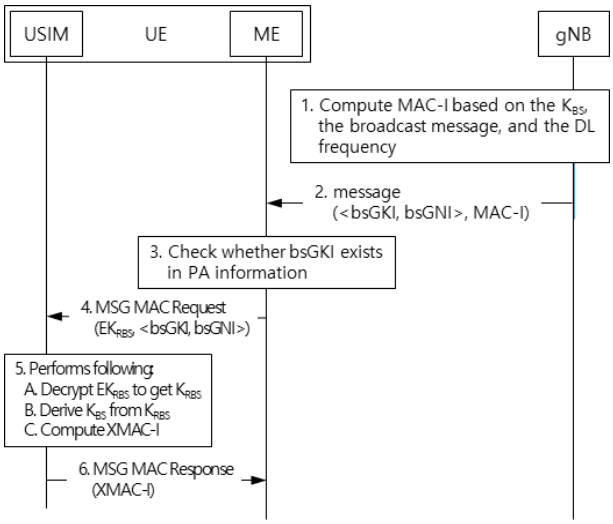

Fig. 2. System Information Protection of Solution # 9 [14]

Fig. 2는 솔루션 #9의 SI 보호 절차인 "Cell Authenticity procedure"를 나타내며, 각 단계는 다음과 같다.

1. gNB는 K_{BS}, 브로드캐스트 메시지, DL 주파수 기반으로 32비트 MAC값 MAC-I를 계산한다. 여기서, K_{BS}는 네트워크에서 K_{RBS}로부터 유도된 gNB의 키이며, 사전에 gNB에게 배포되었다.
2. gNB는 메시지 <bsGKI, bsGNI>, MAC-I를 브로드캐스트한다. 여기서, bsGKI는 각 그룹을 식별하기 위한 식별자이며, bsGNI는 이 그룹에 속한 각 gNB를 식별하기 위한 식별자이다.
3. ME는 gNB로 부터 메시지 <bsGKI, bsGNI>, MAC-I를 수신한 후, 보관하고 있는 보호 영역(PA) 정보에 bsGKI가 존재하는지 확인한다. 만약 확인이 실패하면, ME는 해당 셀을 캐시에 의심되는 셀로 표시한다. 확인이 성공하면, 다음 단계를 계속한다.
4. ME는 USIM에게 EK_{RBS}, <bsGKI, bsGNI>를 전송하고 MAC값 계산을 요청한다.
5. USIM은 저장된 CKp를 기반으로 EK_{RBS}를 복호화하여 K_{RBS}를 얻고, K_{RBS}와 <bsGKI, bsGNI>에서 K_{BS}를 유도하고, K_{BS}에 기반한 XMAC-I를 gNB가 K_{BS}를 기반으로 MAC-I를 계산하는 것과 동일 방법으로 계산한다.
6. USIM은 MAC 값 계산 요청에 대한 응답으로 XMAC-I를 ME에게 전송한다.

XMAC-I를 수신한, ME는 XMAC-I와 MAC-I를 비교한다. 만약 동일하면, ME는 브로드캐스트 메시지를 처리한다. 그렇지 않으면, ME는 해당 셀을 고위험 셀로 표시한다. 요약하면, 솔루션 #9는 사전에 gNB와 UE가 공유하는 대칭키가 있으며, gNB는 SI에 대한 MAC을 계산하여 SI와 같이 브로드캐스트하면, UE가 MAC 값을 검증하여 SI의 정확성을 검증한다.

4. Digital signature based solution

디지털 서명 기반 솔루션 중에서 "Solution #20: Digital Signing Network Function (DSnF)"에 대해 살펴본다. 이 솔루션의 아이디어는 보안 위임 개념을 사용하여, 네트워크 기능인 Digital Signing Network Function (DSnF)에서 gNB의 SI에 대해 디지털 서명을 수행한다. SI의 디지털 서명의 계산을 각 gNB 자체가 아니라, DSnF에게 SI 블록을 전송한 후, DSnF가 디지털 서명을 수행한다. 이러한 위임 서명은 지연이 발생할 수 있지만, 일반적으로 gNB는 브로드캐스트되는 SI에 대한 디지털 서명을 DSnF에게 미리 요청하여 획득할 수 있다. 이러한 디지털 서명 기반 솔루션에서는 UE에게 CA 인증서 목록을 배포해야 되며 이를 위해서, UE 제조 중에 UE에게 CA 인증서 목록을 배포하거나 기존 5G의 배포 프로세스를 재사용할 수도 있다.

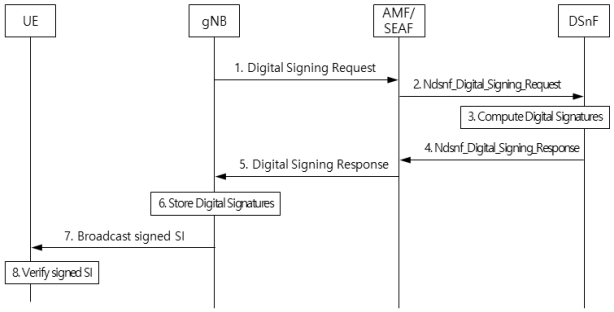

Fig. 3. System Information Protection of Solution #20

Fig. 3은 3GPP TR 33.809[14]의 솔루션 #20에 기술되어 있는 디지털 서명 요청/응답과 서명된 SI의 브로드캐스트/검증 과정을 정리하여 도식화한 그림이며, 각 단계에 대한 내용은 다음과 같다.

1. gNB는 AMF에게 SI에 대한 디지털 서명을 요청한다. 솔루션에서 제시한 디지털 서명 요청 정보의 예로는 PCI, MIB, SIB1, Time counter, Downlink frequency 등이 있다.
2. gNB의 디지털 서명 요청을 수신한 AMF는 서비스 인터페이스 Ndsnf_Digital_Signing_Request를 이용하여 DSnF에게 디지털 서명 서비스를 요청한다.
3. 디지털 서명 요청을 받은 DSnF는 보호할 정보 요소에 대해 디지털 서명을 계산한다. 솔루션에서는 사용할 디지털 서명 알고리즘을 명시적으로 제시하지는 않고 향후 연구로 남겨두었다 [14].

4. DSnF는 서비스 인터페이스 Ndsnf_Digital_Signing_Response를 이용하여 AMF에게 디지털 서명 결과와 응답을 전송한다. 디지털 서명 응답에는 디지털 서명의 검증을 용이하게 하는 다른 정보(예: 공개 키 식별자 등)가 포함될 수 있으며, 솔루션에서는 디지털 서명 응답에 대한 정확한 형식을 제시하지 않았다.
5. AMF는 DSnF로부터 수신한 디지털 서명을 해당 gNB에게 전송한다.
6. 디지털 서명을 수신한 gNB는 수신한 것을 저장한다.
7. SI와 함께 SI의 디지털 서명을 브로드캐스트 한다. 여기서 디지털 서명의 검증을 용이하게 하는 추가 정보가 브로드캐스트 메시지에 포함되며, 이러한 추가 정보의 예로는 보호되고 있는 SIB를 나타내는 정보, PCI, Downlink frequency, Time Counter 등과 같은 재생 공격 방지를 위한 정보, 키 식별자와 같은 서명 검증을 위한 공개키를 선택하기 위한 정보, 필요한 경우 인증서 체인을 구성하기 위한 정보, 다중 디지털 서명 알고리즘이 지원되는 경우 서명 알고리즘 선택을 위한 정보가 있다. 솔루션에서는 서명된 새로운 SIB에 대한 정확한 형식은 제시되지 않았다.
8. UE는 디지털 서명된 SI 메시지를 수신한 후, 획득한 SI 블록의 추가 정보 요소와 함께 보호된 SI에 대한 해시를 계산할 수 있다. 그런 다음 UE는 키 식별자를 사용하여 서명 개인키에 해당하는 공개키를 검색한다. 계산된 해시와 공개키를 사용하여 디지털 서명을 확인할 수 있다. 솔루션에서 새로운 SIB의 정확한 형식과 서명 검증 절차가 개략적으로 제시되었다.

SI는 높은 빈도로 브로드캐스트되며, 이러한 SI에 대한 서명을 실시간으로 처리하는 것보다 DSnF에게 미리 서명을 받아 저장할 수 있다. 이는 극소수의 일부 정보(예: SFN)를 제외하고 MIB 및 SIB1의 거의 모든 요소의 변경이 없다 [15]. 요약하면, 솔루션 #20은 gNB는 DSnF에게 서명을 요청하고 이를 수신하여 UE에게 SI와 디지털 서명을 함께 브로드캐스트한다. 이를 수신한 UE는 디지털 서명을 확인하여 SI의 진본성을 확인한다.

III. Comparative Analysis of the Solutions

본 장에서는 앞 장에서 소개한 3GPP TR 33.809[14]의 Key Issue #2 (security protection of system information)를 해결하기 위한 각 범주별 솔루션들을 지상 기지국을 보조하는 UxNB의 진본성 검증 관점에서 분석한다. 각 솔루션을, 첫째, UxNB에게 사전 배포되는 정보와 이를 위한 업데이트, 둘째, UxNB에 저장된 비밀 정보의 유출 영향, 셋째, 추가적으로 요구되는 연산량 및 전송량 측면에서 분석한다.

1. Provisioning information for UxNB and its update

먼저, 앞서 소개한 각 범주별 대표 솔루션들에 대하여, SI 보안을 위해서 사전에 분배가 필요한 정보들을 비교 분석한 결과의 요약은 Table 1과 같으며 상세한 내용은 다음과 같다.

Table 1. Comparison of provisioning information

Solutions	Provisioning information for UxNB
Hash based Solution #14	• None
MAC based Solution #9	• gNB's key : K_{BS} • Group Key Identifier : bsGKI • Group Node Identifier : bsGNI
Digital Signature based Solution #20	• None or • A temporarily public/private key pair and a short-live certificate

해시 기반의 솔루션 #14의 경우, SI 보안을 위해 별도의 키를 사용하지 않으므로 사전에 분배가 필요한 정보가 없다. 솔루션 #14에서 해시 값의 암호화와 무결성 보호를 위해 5G 표준의 키 계층(Key Hierarchy) [16]에서 생성된 K_{RRCint}와 K_{RRCenc}를 사용한다. 따라서 이 솔루션은 사전 분배 정보 및 업데이트가 필요 없다는 이점이 있다.

MAC 기반의 솔루션 #9의 경우, SI 보안을 위해서 UxNB내에 해당 서빙네트워크의 gNB 그룹 공유키를 사용하여 유도된 gNB의 키(K_{BS}), gNB 그룹의 식별자(bsGKI), gNB로서의 UxNB의 식별자(bsGNI)를 저장해야 한다. UxNB의 사용을 지상 기지국을 보조하여 서비스 품질 향상을 위해 사용하는 환경에 적용할 경우, 일반적으로 UxNB는 특정 지점으로 이동한 후에는 호버링 상태로 서비스를 제공할 것이다. 따라서 SI 보안을 위해서 UxNB내에 저장되는 값들은 UxNB가 실제 배포되는 위치에 따라 다르기 때문에, 현장에서 배포 전에 UxNB내의 안전한 저장소에 저장되어야 한다. 또한 현장에서 UxNB가 서비스하는 동안 그룹 식별자 또는 그룹 공유키가 변경될 경우 gNB 그룹 공유키를 사용하여 유도된 gNB의 키(K_{BS})와 gNB 그룹의 식별자(bsGKI)가 업데이트될 필요가 있다. SI 보안을 위해 UE 측면에서 저장해야 될 정보의 배포와 업

데이트 과정에 대해서는 제시하고 있지만, gNB 측면에서는 배포 과정 및 업데이트 과정을 제시하지 않고 있다. gNB가 UxNB가 될 경우에는 코어 네트워크와 UxNB 사이는 무선 구간으로 되어 있으므로 안전한 업데이트를 위해서는 암호화된 전송이 필요하다. 이를 위한 키 설정, 암호화 수행 및 전송 과정이 솔루션 #9를 위하여 명확하게 제시되어야 한다.

디지털 서명 기반의 솔루션 #20의 경우, gNB가 디저털 서명이 필요한 정보가 있으면, DSnF에게 디지털 서명을 요청하고 DSnF가 디지털 서명을 gNB에게 전송한다. 이 경우에는 gNB에게 사전 배포가 필요한 정보가 없다. 하지만 솔루션 #20에서는 SI 에서 자주 변경되는 일부 필드를 수용하기 위해서, 임시 공개키/개인키 쌍과 단기 인증서(short-live certificate) 사용 방안도 제안하였다. 단기 인증서는 DSnF 디지털 서명 인증서로 서명된 것이며 짧은 시간(예: 1시간) 동안 유효하다. 만약 단기 인증서를 사용할 경우 gNB가 직접 디지털 서명을 할 수 있으며, 이를 위해 디지털 서명을 위한 개인키를 gNB에 사전에 배포해야 한다. 이러한 정보들은 UxNB가 현장 배포 전에 UxNB내의 안전한 저장소에 저장되어야 한다. 만약 현장에서 UxNB가 서비스하는 동안 단기 인증서를 업데이트할 경우, 안전한 업데이트를 위해서는 암호화된 전송이 필요하다.

2. Secret information leakage of UxNB

일반적으로 지상 기지국은 물리적 보안을 적용할 수 있지만, UxNB의 경우 물리적 보안을 적용하기 어려운 환경이다. 무선 신호 교란(Jamming), 무선 프로토콜 상의 취약점 등을 통한 공격을 이용하여 드론을 강제 조작 및 탈취할 수 있다. 만약 이러한 보안 공격을 통해 UxNB의 보안 정보가 유출되었을 경우, 각 범주별 대표 솔루션들에서 발생 가능한 위험을 분석한다. 이를 위해서 먼저 SI 보호를 위해 UxNB에 저장되어 있는 보안 정보들을 살펴볼 필요가 있다. 솔루션별 보안 정보들을 비교 분석한 결과의 요약은 Table 2와 같으며 상세한 내용은 다음과 같다.

Table 2. Comparison of secret information

Solutions	Secret information of UxNB
Hash based Solution #14	• None
MAC based Solution #9	• Symmetric key used in MAC calculation : K_{BS}
Digital Signature based Solution #20	• None or • A temporarily private key

먼저 해시 기반 솔루션 #14의 경우, SI 보호를 위해 UxNB에 저장되는 별도의 정보는 없다. 따라서 UxNB가 강제 조작 및 탈취되어도 SI 보호 관련한 보안 정보의 유출이 발생될 수 없다.

MAC 기반 솔루션 #9의 경우, SI 보호를 위해 UxNB에 저장되는 정보는 K_{BS}라는 MAC 계산에 사용되는 대칭키가 저장된다. 만약 이러한 K_{BS} 대칭키가 유출될 경우 올바른 MAC 값의 계산이 가능하므로 실제 UxNB로 위장할 수 있을 것이다.

디지털 서명 기반 솔루션의 경우, 만약 gNB에서 디지털 서명을 수행할 경우에는 gNB에 디지털 서명을 위한 개인키가 저장되어야 한다. 만약 gNB에 저장된 서명을 위한 개인키가 유출 또는 도난당하면, 공격자가 임의의 SI에 서명할 수 있으므로 더 많은 사용자를 공격할 수 있을 것이다. 따라서 디지털 서명에 사용되는 개인키는 더욱 주의해서 보호해야 한다. 이러한 점 때문에 솔루션 #20에서는 gNB가 디지털 서명을 위해 DSnF에게 요청하는 보안 위임 방법을 사용한다. 이렇게 하면, gNB에 디지털 서명을 위한 개인키를 저장할 필요가 없다. 하지만, 이러한 위임 서명에는 전송 지연 및 대역폭 오버헤드와 같은 몇 가지 단점이 있다. 하지만, 솔루션 #20에서는 자주 변경되는 일부 필드에 대한 디지털 서명을 위해서 임시 공개키/개인키 쌍과 단기 인증서 사용도 제안하였다. 이러한 경우에 UxNB 내의 SI 보안을 위한 서명키, 즉 임시 개인키가 유출될 경우 문제가 발생할 수 있다. MAC 기반 솔루션 #9에서의 대칭키의 유출은 지역적(local)으로 영향이 있지만, 디지털 서명 기반 솔루션에서 서명키의 유출은 전역적(global)으로 영향이 있을 수 있다. 더 구체적으로 말하면, 특정 gNB에서 도난당한 대칭키는 공격자가 해당 gNB가 제공하는 사용자의 트래픽에만 액세스할 수 있도록 허용한다. 그러나 도난당한 서명키를 사용하면 공격자가 임의의 SI에 서명할 수 있으므로 더 많은 잠재적인 사용자를 공격할 수 있다. 따라서 서명키는 더욱 주의해서 보호해야 한다.

3. Additional required calculations and transmissions

각 범주별 대표 솔루션들의 SI 보호를 위해 추가적으로 필요한 연산량을 UE, gNB, 네트워크 측면에서 각각 분석하여 요약하면 Table 3과 같다. Table 3에서 Tx는 x를 수행하는데 필요한 시간을 의미한다.

Table 3. Comparison of computations

Solutions	UE	gNB	Network
Hash based Solution #14	$T_H+T_E+T_M$	$T_H+T_D+T_M$	-
MAC based Solution #9	ME : $T_H^{(*)}$ USIM : T_D+T_M	$T_H^{(*)}+T_M$	-
Digital Signature based Solution #20	T_V	-	DSnF : T_S

T_H : Time for Hash function
$T_H^{(*)}$: Time for Hash function needed if message is long
T_E : Time for Symmetric Encryption
T_D : Time for Symmetric Decryption
T_M : Time for MAC
T_V : Time for Digital Signature Verification
T_S : Time for Digital Signature Signing

SI 보안을 위해서 SI를 브로드캐스트할 때 추가적으로 전송되는 정보를 분석하여 요약하면 Table 4와 같다. Table 4에서 "A → B : X" 는 A가 B에게 정보 X를 전송한다는 것을 의미한다. Table 4에서 해시 기반 솔루션 #14는 해시 값의 전송이 필요하고, MAC 기반의 솔루션 #9는 MAC값과 기타 정보의 전송이 필요하고, 디지털 서명 기반 솔루션 #20은 디지털 서명의 전송이 필요하다. 각각 해시, MAC, 디지털 서명에 어떤 알고리즘을 사용하는가에 따라서 정확한 비트 수는 달라질 수 있다. 제한된 컴퓨팅 파워 및 전원을 가진 UxNB는 계산량과 전송량이 적을수록 서비스할 수 있는 시간 측면에서 유리할 수 있다.

Table 4. Comparison of transmission information

Solutions	Transmission information
Hash based Solution #14	• UE→gNB: MIB/SIB Hash value • gNB→UE: MIB/SIB (If the verification for the MIB/SIB sent by the UE fails)
MAC based Solution #9	• gNB→UE: <bsGKI, bsGNI>, MAC-I
Digital Signature based Solution #20	• gNB→UE: Digital Signature

IV. Conclusions

본 논문에서는 지상 기지국을 보조하는 UxNB의 진본성 검증을 위해, 3GPP TR 33.809[14]의 SI 보안을 위한 솔루션들이 사용될 수 있으며, 이러한 솔루션들을 UxNB 관점에서 분석하였다. 먼저 3GPP TR 33.809[14]에서 Key Issue #2를 해결하기 위해 제시된 솔루션들을 분류하고 각 범주별로 대표적인 솔루션을 하나씩 소개하였다. 소개한 각 솔루션별로 UxNB의 진본성 검증 관점에서 첫째, 사전 배포 정보 및 업데이트, 둘째, UxNB의 보안 정보 유출, 셋째, 추가적으로 요구되는 연산량 및 전송량 측면에서 해당 솔루션들을 비교 분석하였다. 분석 결과, UxNB의 진본성 검증을 위한 솔루션은 정보 유출의 위험성 때문에 UxNB에 저장될 비밀 정보가 없거나 최소화되어야 하고 만약 존재하면 안전한 장소에 저장될 필요가 있다. 그리고 그러한 정보가 무선으로 업데이트된다면, 해당 정보의 보호를 위해 암호화 방안을 마련해야 한다. 또한 UxNB의 낮은 컴퓨팅 파워와 전원으로 인하여 연산량 및 전송량을 최소화해야 한다. 본 연구의 분석 결과는 5G 또는 6G에서 UxNB를 도입하고자 할 때, UxNB의 진본성 검증 솔루션 개발에 유용하게 활용될 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.2021-0-00796, Research on Foundational Technologies for 6G Autonomous Security-by-Design to Guarantee Constant Quality of Security)

REFERENCES

[1] H. Lee, J.S. Bae, S.J. Bahng, and H.S. Lee, "Standardization Trends for Operation of Unmanned Aerial Vehicles based on 5G," Electronics and Telecommunications Trends, Vol. 36, No. 4, pp.13-22, Aug. 2021. DOI: 10.22648/ETRI.2021.J.360402

[2] A. S. Abdalla and V. Marojevic, "Communications Standards for Unmanned Aircraft Systems: The 3GPP Perspective and Research Drivers," IEEE Commun. Standards Mag., vol. 5, no. 1, pp. 70-77, Mar. 2021. DOI: 10.1109/MCOMSTD.001.2000032

[3] S. Alfattani et al., "Aerial platforms with reconfigurable smart surfaces for 5G and beyond", IEEE Commun. Mag., vol. 59, no. 1, pp. 96-102, Jan. 2021. DOI: 10.1109/MCOM.001.2000350

[4] Y. Aydin, G. K. Kurt, E. Ozdemir and H. Yanikomeroglu, "Authentication and Handover Challenges and Methods for Drone Swarms", IEEE Journal of Radio Frequency Identification, Vol. 6, pp. 220-228, Mar. 2022. DOI: 10.1109/JRFID.2022.3158392

[5] Y. Aydin, G. K. Kurt, E. Ozdemir and H. Yanikomeroglu, "Group handover for drone-mounted base stations", IEEE Internet of

Things Journal, vol. 8, No. 18, pp. 13876-13887, Sep. 2021. DOI: 10.1109/JIOT.2021.3068297

[6] R. Bajracharya; R. Shrestha; H. Jung, "Wireless Infrastructure Drone based on NR-U: A Perspective", 2021 International Conference on Information and Communication Technology Convergence (ICTC), Oct. 2021. DOI: 10.1109/ICTC52510.2021.9620869

[7] 3GPP. TS 22.125 v17.6.0, "Unmanned Aerial System (UAS) Support in 3GPP; Stage 1 (Rel-17)," Mar. 2022.

[8] S.R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, E. Bertino: "5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol," in Proc. 2019 ACM SIGSAC Conference on Computer and Communications Security, pp.669-684, Nov. 2019. DOI: 10.1145/3319535.3354263

[9] K. Kim, K. Park, and T.K. Park, "Analysis of Deregistration Attacks in 5G Standalone Non-Public Network," Journal of the Korea Society of Computer and Information, Vol. 26, No. 9, pp. 81-88, Sep. 2021. DOI: 10.9708/jksci.2021.26.09.081

[10] K. Kim, K. Park, and T.K. Park, "Analysis of DoS Attack against Users with Spoofed RRC Connections in 5G SNPN," Journal of KIIT, Vol. 19, No. 10, pp. 79-85, Oct. 2021. DOI: 10.14801/jkiit.2021.19.10.79

[11] K. Kim, J.G. Park, and T.K. Park, "Analysis of Incarceration Attacks with RRCReject and RRCRelease in 5G Standalone Non-Public Network," Journal of the Korea Society of Computer and Information, Vol. 26 No. 10, pp. 93-100, Oct. 2021. DOI: 10.9708/jksci.2021.26.10.093

[12] R. Zhang, W. Zhou, and H. Hu, "Towards 5G Security Analysis against Null Security Algorithms Used in Normal Communication," Hindawi Security and Communication Networks, Vol. 2021, Article ID 4498324, Oct. 2021. DOI: 10.1155/2021/4498324

[13] T.K. Park, J.G. Park, and K. Kim, "Analysis of the IP Spoofing Attack Exploiting Null Security Algorithms in 5G Networks," Journal of the Korea Society of Computer and Information, Vol. 27 No. 9, pp. 113-120, Sep.2021. DOI: 10.9708/jksci.2022.27.09.000

[14] 3GPP. TR 33.809 v0.18.0: "Study on 5G Security Enhancement against False Base Stations (FBS) (Rel-18)," Feb. 2022.

[15] H. Gao, Y. Zhang, T. Wan, J. Zhang and H. Duan, "On Evaluating Delegated Digital Signing of Broadcasting Messages in 5G," 2021 IEEE Global Communications Conference (GLOBECOM), pp. 1-7, Dec. 2021, DOI: 10.1109/GLOBECOM46510.2021.9685173

[16] 3GPP. TS 33.501 v17.5.0: "Security Architecture and Procedures for 5G System (Rel-17)," Mar. 2022.

Authors

Keewon Kim received his 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, Mokpo National Maritime University. He is interested in information security, security protocol, VLSI, and big data analysis.

Kyungmin Park received his B.S., M.S., and Ph.D. degree in Computer Engineering from Chungnam National University, Rep. of Korea, in 2010, 2013, and 2019. He joined the Electronics and Telecommunications Research Institute(ETRI), Daejeon, Rep. of Korea, in 2017, where he is currently working as a senior researcher. Currently, he is interested in mobile network security.

Jonghyun Kim received the Ph.D. degree in computer science from the University of Oklahoma, USA, in 2005. He was a researcher with the Samsung Electronics in 1995-1998. He is currently a principal researcher with the Electronics Telecommunications Research Institute, Daejeon, Korea. He is also involved in standardization activities as a vice-chair of WP1 and a rapporteur of Q.4 (cybersecurity) in ITU-T SG17. His research interests include Network Security, Cloud Security, AI-based malware detection and 5G/6G Security.

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.