5G 네트워크기반 허위재난문자 메시지 판별방식에 관한 연구

이지환, 임민중
동국대학교

nanwonhae1@dgu.ac.kr, minjoong@dongguk.edu

A study on 5G network-based false disaster text message identification

Jihwan Lee, Minjoong Rim
Dongguk University

요 약

본 논문에서는 우리나라에서 서비스되고 있는 긴급재난문자 시스템(CBS)에서 허위기지국의 등장으로 나타날 수 있는 허위재난문자 전달에서 발생할 문제점에 대해 알아보고, 사용자가 수신한 재난문자의 진위여부를 식별할 수 있는 시스템을 제시하고자 한다.

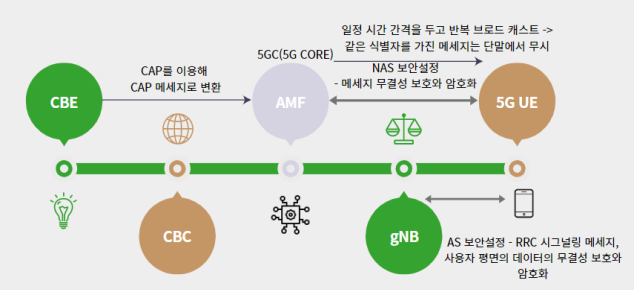
Ⅰ. 서론

우리나라는 재난발생 시 안전을 도모하기 위해 CBS (Cell Broadcasting System)을 이용하여 재난문자를 전송하고 있다. 재난상황 발생 시, 행정안전부에서 지정한 기관에서 재난문자 내용을 담아 보내고자 하는 네트워크 셀의 기지국에 전달하고 기지국에 전달된 재난문자는 CBS 기능이 가능한 사용자 단말에 이를 전달한다. 그러나 허위기지국이 이 방식을 악용하여 사용자 단말에 허위 재난문자를 전송하여 국민들에게 혼란을 주거나 대피장소에 집중 공격을 하는 등의 문제를 일으킬 수 있다. 허위기지국은 정상적인 연결을 제공하는 기지국을 모방하여 허위신호 생성 및 커버리지 내 단말에 공격을 시도하는 기지국을 의미한다. 본 논문에서는 5G네트워크 상에서 허위기지국 공격에 대응하기 위한 방식을 제안한다.

Ⅱ. 본론

긴급재난문자는 5G 네트워크내에서 적용하면 그림 1과 같이 나타낼 수 있다. CBE(Cell Broadcast Entity)는 CBS에서 전송하는 메시지를 정의하고 제어를 허용하는 핵심기관이다. 이는 우리나라에서 행정안전부장관이 지정·해제할 수 있으며, 현재 보건복지부·환경부·기상청 등 행정기관과 공항·철도공사 등 공공기관이 해당된다. CBC(Cell Broadcast Centre)는 메시지를 수신할 특정 영역, 메시지 방송 기간 및 메시지 반복 빈도를 결정하는 기관이다. CBE에서 최초 생성된 메시지는 CAP(Common Alerting Protocol)을 통해 CAP 메시지로 변환되어 CBC에 전달한다. CAP는 재난경보시스템에서 정보전달을 위해 사용되는 공통 경보 프로토콜이다. CBC에서 이를 다시 5G CORE로도 불리는 AMF(Access & Mobility Management Function) 및 기지국(gNB, gNodeB))를 거쳐 사용자 단말 (UE, User Equipment)에게 전달된다. AMF에서 수신한 CAP 메시지는 UE에 일정 시간 간격을 두고 브로드캐스트하게되는데 이때 같은 식별자를 가진 메시지는 단말에서 무시한다.

허위기지국은 RAN(Radio Access Network)를 통해 사용자에게 수동적 또는 능동적으로 공격하며 무선 액세스 네트워크의 보안 취약점과 UE가 더 강한 무선 신호에 연결하려는 특성을 악용한다.[1] 사용자 단말이 이에 연결하는 경우 허위재난문자를 수신하게 되어 직접적인 피해를 받을 수 있다. 허위기지국에서 악용하는 메시지는 RRC(Radio Resource Control) 시그널링 메시지를 보호하기 위한 AS (Access Stratum) 보안설정이 완료되기 전에 전송되는 일부 유니캐스트 메시지와 gNB에서 브로드캐스트되는 시스템 정보와 같은 메시지 또는 보안설정 이후에도 보호되지 않는 메시지가 있다. 이에 허위재난문자 수신방지를 위한 두가지 방식을 제안한다.



[그림 1. 5G 네트워크 기반 긴급재난문자 송출체계도]

1. 재난문자 암호화

재난문자 암호화는 기존 CBS방식에 비대칭 공개키 방식인 DSA(Digital Signature Algorithm)를 적용한다. DSA는 미국 국립표준기술연구소(NIST)가 개발한 디지털 서명을 위한 알고리즘으로 비대칭 공개키 방식이다. 도메인 파라미터(p, q, g)와 공개키, 개인키를 모두 이용하여 디지털 서명을 생성하고 공개키를 사용하여 그 서명을 검증한다. 도메인 파라미터와 공개키만 기본적으로 공개되고 개인키는 공개되지 않으며 $g^a \pmod p \equiv b$ 이산로그문제에 기반하여 g, b가 주어졌을 때 a를 구하는 과정을 이용한다. g^a은 쉽게 구할 수 있지만 $\log_g b \pmod p$를 계산해서 a를 구하는 것은 매우 어렵다. DSA를 5G 네트워크상에 적용하면 CBE 즉, 행정안전부에서 지정한 기관에서 재난문자를 송신하는 과정에서 암호화를 거쳐 최종적으로 사용자 단말에서 재난문자를 수신하였을 때 복호를 진행함으로써 재난문자의 진위를 판별할 수 있다. 사용자

단말에서 빠른 복호를 할 수 있으므로 재난문자의 특성 중 하나인 신속성을 만족하며, 비대칭 키 방식을 이용하여 송신자 측에서는 신뢰할 수 있는 기관임을 증명하고, 수신자 측에서는 메시지를 보낸 측의 신뢰도 확인한다.

구분	RSA	DSA
암호화 원리	소인수분해	디지털 서명방식
Key 생성속도	느림	빠름
암호화 속도	빠름	느림
복호화 속도	느림	빠름

[표 1. RSA, DSA 특성 비교]

2. NR(New Radio) 이중 연결(Next Generation RAN E-UTRA New Radio Dual Connectivity, NGEN-DC) 응용

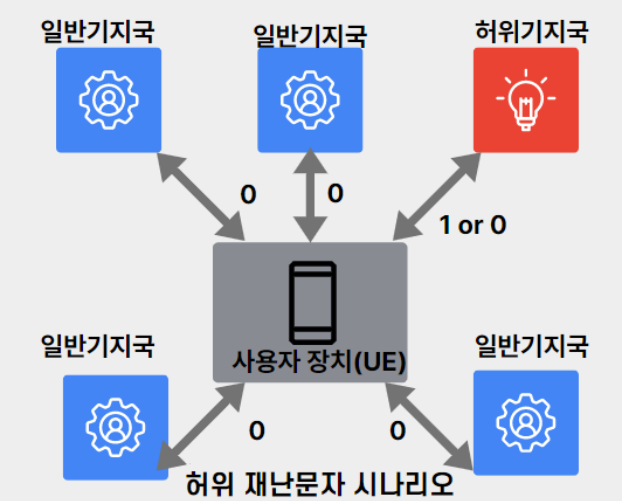
NR 이중 연결(NGEN-DC)은 이동 통신망에서 하나의 단말이 LTE와 5G 기지국에 동시에 연결되어 각각의 기지국과 데이터를 동시에 송수신하는 기술을 말한다. 이 기술은 단말의 마스터 기지국이 LTE 기지국에 연결되고, 2차 기지국은 5G 기지국에 연결되어 고속 데이터 전송을 추가로 이용할 수 있도록 동시 연결을 지원한다.

이를 응용하여 사용자 단말이 재난문자를 수신한 경우 2차 기지국 연결을 끊고 동일한 셀에 위치한 다른 5G 기지국에 연결한다. 만약 공습경보 등에 해당되는 위급재난문자인 경우 다른 셀에있는 기지국까지도 연결한다. 사용자 단말이 다른 기지국에 연결했다면 단말이 수신한 재난문자를 기지국에 재전송하여 상위기관인 CBE로부터 이를 수신하였다면 1(True)를 받아오고, 그렇지 않은 경우에는 0(False)를 받아온다. 사용자 단말은 주변의 여러 기지국들로부터 수신한 값 중 더 많은 값을 토대로 수신한 재난문자의 진위여부를 판단한다.

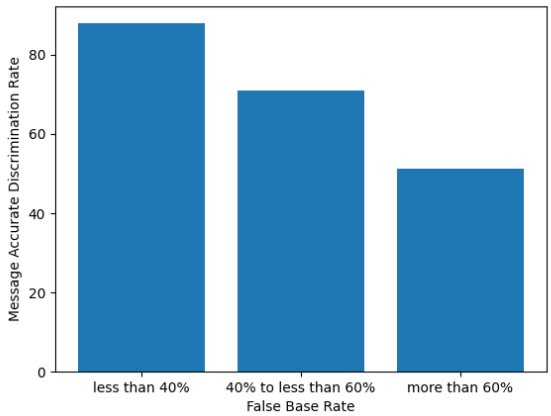
이 방식은 5G 핵심망인 5GC가 재난상황시 사용자들의 통신량 증가에 대비하여 안정되게 대처할 수 있고 NR 이중 연결(NGEN-DC)이 안정적으로 적용되어 단말이 각각 LTE, 5G 기지국에 연결된 상황을 가정한다. 또한, 각 gNB가 CBE로부터 수신한 재난문자를 일정시간동안 저장해두는 상황을 가정한다.

또한, 일반적인 상황에서 사용자 단말의 재난문자 수신 속도가 빨라야 하므로 '선 수신-후 판단' 방식을 이용한다. 이는 사용자 단말이 기지국으로부터 메시지를 수신하면 사용자에게 이를 나타냄과 동시에 재난문자 암호화방식이나 NR 이중연결 응용방식을 이용하여 재난문자의 출처 및 진위확인을 통해 정확한 정보를 선별한다.

NR 이중 연결(NGEN-DC) 응용 과정 중 사용자 단말이 5G 기지국에 연결되었을 때 다른 기지국에 연결하는 과정을 실험하였다. 셀내 기지국을 5*5 크기의 2차원 배열로 표현하여 초기 정상기지국은 1의 값을 가진다. 셀내 허위기지국은 무작위로 등장하여 값이 0으로 바뀐다. 사용자 단말은 셀에 속한 기지국 5곳에 무작위로 전달하여 1(True)이나 0(False)를 받아왔으며, 가장 많이 받아온 값으로 수신한 재난문자의 진위여부를 판단하였다. 정상 메시지를 사용자 단말이 전달하여 주변 기지국에 전달한 경우, 허위기지국은 0또는 1을 사용자 단말에 전달하고 정상기지국은 1을 전달한다. 반대로 허위메시지를 전달한 경우 허위기지국은 1을 전달하고 정상기지국은 0을 전달한다. 허위기지국이 차지하는 비율에 따라 사용자 단말의 메시지 정확 구분율을 평균을 구해 y축에 나타냈고 x축에 전체 기지국 중 허위기지국의 비율을 나타냈다. 허위기지국의 비율이 40% 미만인 상황에서 약 87%의 일치율을 보였고, 40%이상 60%미만의 상황에서 약 71%의 일치율을 보였으며 60%이상의 경우 51%의 일치율을 보였다. 이렇듯 전체 기지국에서 허위기지국의 점유율이 절반 이상을 차지하여도 사용자 단말은 재난문자의 진위여부를 높은 확률로 정확히 파악할 수 있었다.



[그림 2. 허위 재난문자 알고리즘 적용 시나리오]



[그림 3. NR 이중 연결(NGEN-DC) 응용 실험결과]

III. 결론

본 논문에서는 CBS를 이용한 재난문자 전달과정에서 등장하는 허위기지국의 문제점에 대해 알아보았다. NR 이중연결 기반의 허위재난문자 판별시스템과 DSA 암호화 과정을 추가한 시스템을 통해 사용자 단말이 수신한 재난문자의 진위여부를 확인하도록 제안하였다. 향후 연구에서는 실제 재난문자 전송시스템을 물리적으로 구성한 후, 재난문자 3가지 종류인 위급재난문자, 긴급재난문자, 안전안내문자의 특성에 맞게 증가하는 통신량을 고려하여 재난상황별 시스템의 성능도를 고려할 예정이다.

ACKNOWLEDGMENT

본 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2022R1F1A1062987).

참 고 문 헌

[1] 박훈용, 박종근, 김보남, 유일선. (2020). 5G 보안에서의 허위 기지국 대응에 대한 주요 이슈 분석. 정보보호학회지, 30(6), 23-30.

[2] 박종근, 김종현, 김익균, 진승헌. (2019). 초연결 지능화 인프라 보안기술 동향 - 5G 시대의 이동통신 보안 중심. [ETRI] 전자통신동향분석, 34(1), 0-0.

[3] 이태겸, 오승희, 조오현. (2022). 5G 기반 긴급재난문자 서비스 요구사항 및 시나리오 연구. 한국통신학회논문지, 47(7), 996-1003.