ETRI

전자통신동향분석 제26권 제6호 2011년 12월

이동통신 네트워크 DDoS 공격 및 대응기술 동향

Technical Trends of DDoS Attacks and Defense in Cellular Network

이성원 (S.W. Yi) 인프라보호연구팀 선임연구원
김종현 (J.H. Kim) 인프라보호연구팀 선임연구원
서동일 (D.I. Seo) 인프라보호연구팀 책임연구원

목 차

최근 이동통신 네트워크 기술의 발전과 고성능 이동단말의 출현으로 인하여 다양한 서비스가 제공되고 있으며, 이로 인하여 이동통신 기술은 통신 인프라에서 생활 인프라로 진화하고 있다. 그러나 이러한 이동통신 환경의 변화는 네트워크의 안정성과 가용성을 위협하는 보안 위협도 증대시키고 있다. 본 고에서는 알려진 이동통신 네트워크에 대한 DDoS 공격기술과 그 대응기술, 그리고 현재 이동통신 보안을 위한 상용 제품들을 소개하고 향후 이동통신 네트워크 DDoS 대응기술의 발전 방향을 살펴보고자 한다.

Ⅰ. 서론

1984년 최초의 셀룰러 방식 이동전화의 국내도입 이후, 이동통신 기술은 CDMA, WCDMA를 거쳐 현재 LTE로 발전해왔다. 또한, 스마트폰의 출현으로 SNS, navigation, 위치 검색 등 다양한 서비스가 제공됨에 따라 이동통신 서비스는 더 이상 통신 인프라가 아닌 생활 인프라로 진화하고 있다.

최근 이동통신 서비스의 확대는 모바일 트래픽의 급증으로 이어지고 있으며 모바일 트래픽은 2015년까지 매년 92% 이상 증가할 것으로 예측되고 있다[1]. 따라서, 이동통신 사업자들은 3G 서비스의 한계극복과 신시장 선점을 위해 LTE 네트워크 서비스를 경쟁적으로 도입하고 있다.

향상된 네트워크 속도 및 네트워크 구조의 변화는, 대중화되는 모바일 서비스와 함께 이동통신 네트워크에 새로운 보안 위협을 가져오고 있다. 즉, 독립적으로 존재하던 이동통신 네트워크는 새로운 모바일 서비스의 도입으로 인하여 인터넷과의 직접 접속이 가능해졌으며, 모바일 단말의 All IP, always-on 서비스의 확대는 인터넷에서 사용되던 공격기술이 이동통신 네트워크를 대상으로 사용될 수 있는 기회를 제공하게 되었다.

실례로 모바일 악성코드의 경우, 안드로이드 기반 악성코드는 2010년 16개에서 2011년 7월에만 107개로 급증하는 추세를 보이고 있으며 그 성향도 PC용 악성코드와 유사한 형태가 다수 보이기 시작했다[2]. 또한 [3]은 중국에서 2010년 100만 대 이상의 휴대폰이 악성코드에 감염되었다고 보고하고 있다. 이에 따라, 휴대전화를 이용하거나 휴대전화를 대상으로 하는 공격의 사례가 국내에서도 보고되기 시작했다[4]. 여기서 휴대전화 문자폭탄 공격의 경우, 공격자는 한 사람을 대상으로 공격을 시도했으나, 복수의 공격자를 대상으로 하는 네트워크 수준의 DDoS 공격으로 손쉽게 변경될 수 있다.

이동통신 네트워크의 취약성, 공격 및 대응기술에 대한 연구는 미국을 중심으로 2000년 초부터 꾸준히 진행되어 왔다[5]-[11]. 이동통신 네트워크 DDoS 공격의 특징은 크게 2가지로 요약될 수 있다. 첫째는 대부분의 이동통신 네트워크 DDoS 공격이 이동통신 네트워크 서비스 및 운영에 필요한 특정한 리소스를 대상으로 삼는다는 것이다. 특정 서비스 또는 웹 사이트에 서비스 거부를 목표로 하는 인터넷 DDoS 공격과 달리 이동통신 네트워크 공격은 네트워크의 공통 리소스를 공격 대상으로 한다. 예를 들어, 이동통신 네트워크를 공격하기 위해 이동통신 네트워크의 특정 리소스를, 즉 paging/dedicated traffic 채널, 시그널링 메시지 등, 집중적으로 소모시켜서 전체 이동통신 네트워크 가입자에게 서비스 거부를 일으키는 것이다. 이러한 공격은 네트워크 서비스 전체가 공격의 피해를 받아서 직접 피해액만 시간당 수백억 원대에 이르는 것으로 알려져 있다.

둘째로는 대량의 트래픽을 공격도구로 사용하는 인터넷 DDoS와 달리 소량의 트래픽만으로도 효율적인 공격이 가능하다는 것이다. 따라서, 이러한 공격들은 공격의 특성이 인터넷에서는 정상 트래픽으로 보이나 이동통신 네트워크 구간에서는 특정 리소스를 공격적으로 소모시켜 전체 네트워크에 서비스 장애를 일으키게 된다. SMS 문자 메시지를 이용한 공격, paging channel 공격의 예에서와 같이 워싱턴 D.C., 맨해튼 정도 크기의 대도시를 공격하는데 적게는 수백 kbps에서 많아도 수 Gbps 정도의 공격 트래픽만을 필요로 한다[5],[6],[9].

이는 일반적으로 수백 Gbps 정도의 트래픽을 사용하는 인터넷 DDoS에 비해 2차수 이상의 차이를 보인다. 따라서, 일반적으로 인터넷에서 사용하는 DDoS

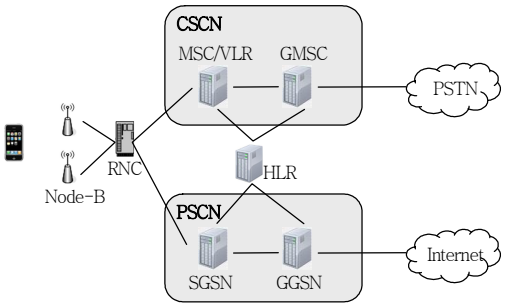
탐지 및 대응기술로는 이동통신 네트워크에 대한 DDoS 공격의 탐지가 매우 어렵다. 또한, 이동통신 네트워크에 대한 공격은 데이터 서비스(mobile apps)와 음성 서비스를 동시에 공격할 수 있어서 경제적 피해뿐 아니라 응급상황 시 인명피해를 초래할 수 있으며, 또한 군사적인 목적의 활용이 가능한 것으로 알려져 있다.

본 고에서는 현재까지 알려진 이동통신 네트워크에 대한 취약점, 공격기술들을 요약하고 그 대응기술 및 이동통신 네트워크 보안을 위한 상용 제품들을 살펴보고자 한다. 이러한 요약과 분석은 보다 강건한 이동통신 네트워크 운영정책 수립과 아직 확립되지 않은 이동통신 네트워크에 대한 보안 대응체계 수립에 활용될 것으로 기대된다.

II. 이동통신 네트워크 구조

UMTS는 3GPP에서 결정된 3세대 이동통신 기술로서 3세대 규약인 WCDMA와 2세대 규약인 GSM, EDGE를 포함한다. 이 장에서는 현재 가장 많이 사용되고 있는 3G 이동통신 기술인 WCDMA를 중심으로 이동통신 네트워크의 구조와 기능에 대해 설명한다.

WCDMA는 NTT DOCOMO에 의해 개발된 3G 무선접속 기술이며, WCDMA 네트워크는 (그림 1)에서와 같이 무선단말, 무선접속 네트워크(Node-B에서 RNC 구간), 코어 네트워크(SSGN-GGSN 구간)으로 구성된다. 무선 접속 네트워크는 무선단말을 유선 네트워크에 연결하기 위한 네트워크로 무선단말과 유선 네트워크 간의 시그널링을 위한 control 채널과 데이터 전송을 위한 traffic 채널을 포함한다. 코어 네트워크(CN)는 음성 서비스를 위한 Circuit Switched 코어 네트워크(CSCN)와 데이터 서비스를 위한 Packet Switched 코어 네트워크(PWCN)로 나뉘어 지는데,



(그림 1) 단순화된 이동통신 네트워크(WCDMA) 구조도

4세대 이동통신 시스템인 LTE에서는 하나의 통합된 코어 네트워크를 가지게 된다.

이동통신 네트워크에서의 최초의 데이터 서비스는 2G 기술이 도입된 시기에 제공된 문자 메시지(SMS) 서비스이다. 인터넷에서 이동통신 네트워크로 접속을 제공하는 문제 메시지 서비스는 데이터 서비스의 일종이나 CSCN을 통해 제공되고, 그 이후 모든 데이터 서비스는 PSCN을 통해 제공된다. 또한, 3G 기술의 출현으로 무선단말에서의 인터넷 접속도 가능해졌다. 음성 및 데이터 서비스를 위해 이동통신 네트워크의 각 엔티티들이 제공하는 주요 기능은 다음과 같다.

- Node-B: 이동단말과 이동통신 네트워크를 연결해주는 엔티티로서, 무선접속 기능을 담당하며 이외의 기능은 최소화되어 RNC에 의해 제어된다.
- RNC: UMTS 무선접속 네트워크의 핵심 엔티티로서 Node-B를 제어하고, 무선 리소스 관리, 이동성 관리 등의 기능을 제공한다. 또한, RNC는 이동단말에서 또는 이동단말로 데이터를 전송할 경우 암호화되는 포인트이다.
- SGSN: 특정 지역 내에서 패킷 데이터의 전송을 담당하는 엔티티로서 패킷 라우팅, 데이터 통신을 위한 이동성 관리, 인증 및 과금관리 등의 기능을 담당한다.
- GGSN: 이동통신 네트워크의 PSCN과 외부 패

킷 스위칭 네트워크(예: 인터넷)와의 접속을 제공한다. GGSN은 하나의 서브 네트워크에서 라우터와 같은 기능을 담당하며 이동단말의 이동성에 대한 anchor의 역할을 수행한다. 또한 이동네트워크에서 오는 GTP 패킷을 변환해 주는 기능을 담당한다.

- MSC: 음성서비스를 제공하기 위한 서버로서 통화제어, 단말기의 이동성 확보 등의 기능을 제공한다.
- HLR: 가입자 정보를 관리하는 서버이다.
- VLR: VLR 영역 내에 현재 위치한 MS로부터의 call을 처리하기 위한 정보 등을 제공한다.

이상으로 본 장에서는 이동통신 네트워크의 구조와 네트워크상의 각 엔티티들의 기능을 간략히 살펴보았다. 다음 장에서는 본 장에서 설명한 이동통신 네트워크의 구조를 바탕으로 이통통신 네트워크 DDoS 공격기술을 소개한다.

Ⅲ. 이동통신 네트워크 DDoS 공격 개요

인터넷에서의 DDoS 공격은 대부분은 애플리케이션 서버 또는 서버군에 대량의 패킷을 전송하여 일반 사용자들에게 서비스 거부를 일으키는 형태의 공격이 주류를 이룬다. DNS와 같이 네트워크 서비스를 제공하기 위한 서비스 엔티티에 대한 공격은 드물고, 그 대응에 있어서도 제한된 수의 서버만을 보호하면 되므로 전자에 비해 용이하다.

그러나, 이동통신 네트워크에 대한 DDoS 공격은 인터넷 DDoS와 달리 특정 서버를 대상으로 하는 것이 아니라 전체 네트워크 서비스를 대상으로 하여 그 공격 방법이 매우 다양하다. 또한 인터넷 DDoS의 경우 수백 Gbps의 트래픽이 사용되는데 비해, 이동통신 네트워크에 대한 DDoS 공격은 수십 kbps에 수백 Mbps 정도의 트래픽만으로도 서울과 같은 대도시에 대한 공격이 가능하다.

이동통신 네트워크에 대한 공격을 위해서는 이동단말에 접속하기 위한 접속 ID를 수집해야 한다. 이동단말에 접속하기 위한 ID로는 IP와 이동전화 번호가 사용된다. 공격자가 이동단말의 IP 주소를 수집하는 방법으로 address scanning 기술이 있다. 일반적으로 공격자는 260kbps의 트래픽만으로도 B 클래스 주소를 10초 안에 scan할 수 있는 것으로 알려져 있다[6]. 또한, [12]는 웜과 같은 악성 스캔 트래픽의 영향에 대해서도 경고하고 있다. ISP에서는 이동단말에 할당하기 위해 IP 대역을 확보하고 있고, 관리의 효율을 위해 일반적으로 이러한 IP들은 서로 인접한 블록을 형성한다. 따라서, 몇 개의 IP가 공격자에게 노출되면 전체 IP 블록을 유추하기는 어렵지 않다.

공격에 사용될 이동전화 번호 수집에 가장 일반적인 방법은 인터넷 검색을 이용하는 방법으로 [5]에 따르면, 단순 인터넷 검색만으로도 특정 지역에 거주하는 1만 4천여 개의 이동전화 번호를 수집할 수 있는 것으로 알려져 있다. 또한 최근 개인정보 유출사고가 증가하고 있는데 이러한 사고를 통한 이동전화 번호 유출은 특정 집단, 지역 등의 상세 정보를 제공함으로써 보다 정밀한 공격에 악용될 수 있다.

가장 단순한 방법으로는 자동화된 공격기술에서 많이 사용되는 샘플링 기술이 있다. 현재 국내의 이동전화 번호 체계를 보면 010-xxxx-xxxx의 형태로 약 1억 개의 번호를 가질 수 있다. 국내 이동전화 가입자를 4천만 명으로 가정했을 경우 랜덤 샘플링으로도 약 40%의 실제 가입자를 확보할 수 있다.

따라서, 공격에 사용된 사용자 ID(IP와 이동전화 번호)의 수집은 실제 공격의 전 단계로 복잡한 단계 및 기술을 필요로 하지 않으며, 특정 집단, 지역 등 공격 대상의 선택 및 특화도 어렵지 않다.

Ⅳ. 이동통신 네트워크 DDoS 공격기술

이동통신 네트워크에 대한 공격은 공격의 대상이 되는 리소스에 따라 네트워크 제어계 공격, 자원고갈형 공격, 그리고 간접 공격으로 구분할 수 있다.

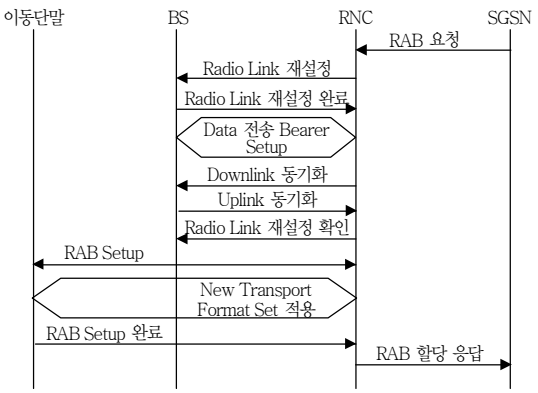
1. 네트워크 제어계 공격(Control Plane Attack)

네트워크 제어계 공격은 공격 트래픽을 이용하여 대상 호스트나 네트워크 자원을 직접 공격하기보다 네트워크 운영을 위한 오버헤드를 증가시켜 서비스 거부를 일으키는 공격기술이다.

이동통신 네트워크에서 데이터 전송을 위해서는 이동단말과 네트워크의 연결을 위해 RRC connection이 생성되어야 하고, 실제 무선 리소스의 할당을 위해서는 RAB가 생성되어야 한다. 이때, RAB는 하나의 RRC 내에서 여러 개가 생성될 수 있다. 이동단말이 일정시간 동안 데이터 전송이 없을 경우 RAB는 삭제되고 사용되던 무선 리소스는 반납된다.

(그림 2)에서와 같이 RAB의 생성과 반납에는 다수의 signaling 메시지의 송수신을 필요로 한다. 특히, RNC의 경우 RAB의 생성 시에는 약 15개, 반납 시에는 12개의 메시지를 처리해야 한다.

공격자들은 소량의 연속적인 패킷을 주기적으로 보냄으로써 RAB의 반복적인 생성과 삭제를 유발할 수 있고 이로 인해 RNC는 과도한 양의 메시지를 처리해야 한다. 따라서, 대다수의 정상적인 사용자는 서비스 거부를 경험하게 된다. [6]에 의하면 64kbps의 공격 트래픽(즉, 40 바이트 패킷을 16만 이동단말에 5초 간격으로 전송)만으로도 뉴욕과 같은 대도시의 모든 RNC를 다운시킬 수 있는 것으로 알려져 있다.



(그림 2) UMTS Radio Bearer 설정절차[6]

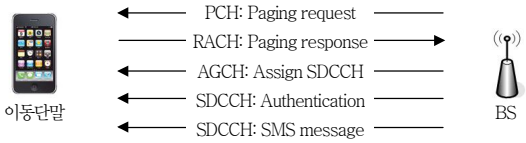
2. 자원고갈형 공격(Low-rate Flooding Attack)

가. 문자 메시지 공격

독립적으로 존재하던 이동통신 네트워크가 인터넷과 융합되면서 인터넷에서 이동통신 네트워크의 접속이 가능해졌다. 인터넷에서 이동통신 네트워크로 접속을 제공하는 대표적인 서비스가 문자 메시지(short message service) 서비스이다.

국내에서 발생한 문자 메시지 공격의 경우[4], 공격 대상이 특정인이어서 피해가 제한적이었으나, 앞에서 기술된 바와 같이 공격 대상을 확보하는 기술이 매우 간단하여 전체 이동통신 네트워크에 대한 공격으로 손쉽게 확대 및 변형이 가능하다.

문자 메시지는 이동단말 또는 웹을 통해 생성될 수 있다. 생성된 문자 메시지는 SMS 트래픽을 처리하는 서버인 SMSC로 전송된다. 문자 메시지 서비스는 데이터 서비스의 한 종류이나 CSCN을 통해 제공된다. 따라서, SMSC는 HLR의 도움으로 대상 단말의 위치를 알아내고 해당 위치의 MSC, BS 또는 Node-B를 통해 이동단말로 문자 메시지를 전송한다. BS에서 이동단말로 문자 메시지의 전송에는 다양한 control channel(PCH, RACH, AGCH, SDCCH)이 사용되며 그 상세 절차는 (그림 3)에 보여진다. CCH는 무선 채널의 사용권(AGCH), 이동단말의 호출(PCH) 등을 지원하기 위한 채널이나, 소량의 데이터 전송(SDDCH)



(그림 3) 단순화된 SMS 무선접속 절차

을 위해서도 사용된다.

공격자들은 SDDCH를 포화시키기 위해서는 초당 360개의 메시지를 수집된 피해자에게 전송함으로써 워싱턴 D.C.와 같은 대도시의 이동통신 네트워크를 십여 분간 마비시킬 수 있다[5],[9]. 이는 하나의 이동단말에 약 10초당 1개의 문자 메시지를 전송하는 정도의 공격량으로, 필요한 총 대역폭도 수 Mbps 이하이어서 인터넷을 대상으로 하는 일반적인 DDoS 기술로는 탐지가 매우 어렵다.

나. Paging 채널 공격

Paging 채널 공격은 전형적인 자원고갈형 공격의 한 예로서, 인터넷 DDoS 공격과 달리 이동통신 네트워크에서 소량의 리소스만을 가진 특정 리소스를 대상으로 하여 효율을 높인 공격 방법이다[6],[10]. CDMA 기반 이동통신 네트워크에서 이동단말은 세 가지 상태에 있을 수 있다(GPRS의 예이나 WCDMA에서도 유사함). Idle 상태는 이동단말이 네트워크에서 분리되어 있는 상태를 말한다. 이동단말이 네트워크에 접속되어 있을 경우는 standby 또는 ready 상태에 있다. Ready 상태에 있는 이동단말은 트래픽 채널을 할당받아 데이터를 즉시 송/수신할 수 있는 상태를 말하며, 이동단말이 셀(cell) 이동 시에도 실시간으로 데이터의 송/수신이 가능하다. 이를 위하여 네트워크는 이동단말의 위치를 실시간으로 관리하여야 하며 이에 많은 시그널 메시지를 필요로 한다.

한편 standby 상태의 이동단말은 몇 개의 셀로 구성된 routing area 내에서만 관리된다. 따라서, 이동단말이 routing area 내에서 cell 이동 시에는 네트워크와 시그널링을 필요로 하지 않는다. 그러나 이동단말에 전달할 데이터가 있는 경우, 이동단말의 현재 위치를 파악해야 한다. 이동단말의 위치는 해당 routing area에 속한 모든 cell에 paging 신호를 보내고 이때 사용되는 무선 채널이 PCH이다. 이동단말은 자신을 호출하는 신호를 수신하면 standby 상태에서 ready 상태로 변하며, 특정 시간(T_R) 동안 데이터를 송/수신하지 않으면 다시 standby 상태로 변하게 된다.

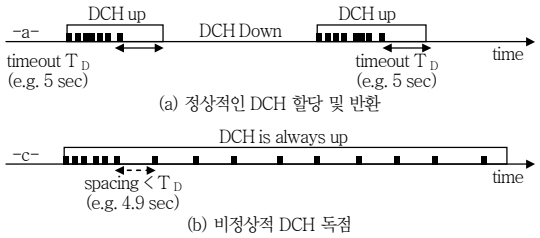
Paging 채널 공격은 이동단말이 상태를 변화시킬 때 paging 채널(PCH)을 이용하며 PCH는 타 채널에 비해 상대적으로 적은 BW를 가진다는 점을 이용한다. 공격자는 최소 크기의 UDP 패킷을 주기적으로 전송하여 paging 채널을 고갈시켜서 정상적인 사용자에게 서비스 거부를 일으킨다. 이때, 공격자는 전송 대상이 되는 이동단말에게 한 번에 데이터를 전송하는 대신 이동단말을 sub group으로 나누고 sub group별로 순차적으로 데이터를 전송할 수 있으며, 이 경우 네트워크 보안 관리자는 공격 트래픽과 flash crowd에 의한 트래픽을 구별하기 매우 어렵게 된다.

다. 데이터 채널 공격

이동통신 네트워크와 인터넷에서 네트워크 자원을 할당하는 방식에 있어서 가장 큰 차이는 인터넷은 packet switching과 같은 형태의 기술에 의존하지만 이동통신 네트워크의 자원할당에는 불가피하게 이용자에게 독점적인 방식의 자원할당을 사용한다.

UMTS 기반의 이동통신 네트워크에서 데이터의 전송에는 DCH와 FACH가 사용된다. 이동통신 네트워크의 RNC는, 이동단말이 일반적인 데이터의 전송을 할 경우 고속 전송을 지원하기 위해 해당 단말에 DCH을 할당하고, 소량의 데이터만을 전송할 경우는 FACH를 할당한다.

채널의 할당 및 전환은 이동단말의 상태와 전송 데



(그림 4) DCH/FACH 채널 할당 비교[10]

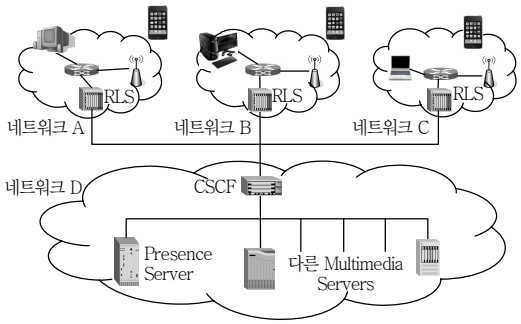
이터의 양에 따라 동적으로 결정된다. FACH에서 DCH 채널의 전환은 최소 모니터링 윈도 동안 전송되는 데이터의 양과 미리 설정된 임계값에 따라 결정된다. 반대로 DCH에서 FACH 채널로의 전환은 타임아웃 값에 따라 결정된다. 즉, 특정 시간 동안 데이터 전송이 없으면 DCH는 반환되고 FACH를 할당 받는다.

이동통신 네트워크의 공격자는 DCH를 효율적으로 고갈시키기 위해서 설정된 임계값보다 조금 큰 값의 데이터를 전송함으로써 DCH을 할당받고 DCH를 반환하기 직전에 소량의 데이터를 전송함으로써 지속적으로 채널을 사용할 수 있다((그림 4) 참조).

일반적으로 사용되는 타임아웃 값이 약 5초, 40바이트 소량 패킷을 사용하고 약 500만 명의 이동단말을 공격한다고 가정할 경우, 약 1Gbps 이하의 트래픽만으로도 서울과 같은 대도시의 공격이 가능하게 된다.

3. 간접 공격(Indirect Attack)

최근 이동통신 기술은 SNS, 영상통화, 음악, 영화 등의 다양한 multimedia 서비스를 제공하고 있으며, 이를 위하여 각 ISP는 IMS를 구축하고 있다. 이러한 서비스들은 사용자들의 상태를 실시간으로 제공하는 presence service를 기반으로 하며, IETF는 효율적으로 presence 상태를 교환하기 위한 방법으로 RLS를 제안하고 있다. IMS 서비스 사용자는 다른 사용자의 상태를 확인하기 위해 각각의 사용자와 presence



(그림 5) RLS, CSCF, Presence 서버의 연결 구조[11]

메시지를 교환하는 대신에 RLS에 접속하고 다른 사용자의 presence 정보를 한 번에 받을 수 있다. (그림 5)는 RLS와 presence 서버의 연결 구조를 나타낸다. (그림 5)에서 Call Session Control Function (CSCF)은 과금과 라우팅을 지원하기 위해 사용되며 대부분의 IMS 시스템에서 사용된다.

이동통신 네트워크 공격자는 실시간으로 서비스 사용자가 타 사용자의 상태를 파악해야 하는 요구사항과 이를 위해 필요한 인프라(RLS, CSCF 등)의 구조적인 문제를 이용한다. 예를 들어, 공격자는 수십~수백 명의 버디리스트를 가진 사용자의 컴퓨터를 공격에 이용할 수 있다. 우선, 공격자는 다수의 좀비PC를 이용해 RLS에 접속한다. 복수의 RLS는 동시에 버디리스트에 속한 이용자의 presence 서버에 해당 이용자의 상태확인 요청을 한다. 따라서 presence 서버는 폭증하는 요청 메시지로 인하여 정상적인 서비스가 어려워지고, 일반 사용자는 서비스 거부를 경험하게 된다. 2차 공격은 presence 서비스의 실시간성으로 인하여 생성된다. Presence 서버에 지연이 발생하면 대다수의 정상적인 사용자는 실시간 presence 상태확인을 위해 공격적으로 재전송 요청 메시지를 보낸다. [13]에 의하면 사용자는 응답을 받지 못할 경우, 32초 내에 약 10개 재전송 요청을 보낼 수 있다. 갑자기 증가하는 재전송요청은 CSCF에 폭주하게 되어 CSCF를 사용하는 다른 서버들의 요청

에 서비스 거부를 일으킨다[11].

이러한 공격 구조는 실제로 훨씬 더 단순하고 효율적으로 이용될 수 있다. 예를 들어, 악성 사용자는 이동통신 네트워크 공격을 위해, 현재 1000만 명 이상이 사용하고 있는 것으로 알려진 SNS 서버에 DDoS 공격을 가한다. SNS 서버가 서비스 거부를 일으키면 해당 서버를 사용하는 이동단말들은 계속해서 상태정보 재전송 요청을 보내게 되고, 이러한 재전송 요청은 이동통신 네트워크의 control 채널을 고갈시킬 수 있다. 이러한 공격의 위험성은 2011년 서버 오작동으로 인한 이동통신 네트워크 불통사태를 통해 쉽게 유추해 볼 수 있다[14].

V. 대응기술 동향

이동통신 네트워크에 대한 DDoS 공격 및 대응기술에 대한 연구는 2000년 초부터 지속적으로 이루어지고 있다. 초기에는 GSM, GPRS에 대한 연구가 주류를 이루었으나, 이후 CDMA2000, WCDMA 네트워크로 확대되었으며, 최근에는 이동통신 기술과는 독립적인 공격기술에 대한 연구로 점차 그 영역을 넓혀가고 있다.

이러한 연구들은 주로 이동통신 네트워크의 취약점, 공격기술 및 그 효과에 대한 내용을 중심으로 다루고 있으며, 그 대응도 AQM을 이용한 공격 mitigation 기술 또는 이상 트래픽 탐지 기술 등이 주를 이루고 있다. [6], [7], [9] 기반의 대응기술은 RED[15] 또는 WFQ[16] 같은 queue 관리 기술을 코어 네트워크의 라우터 또는 서비스 서버의 queue에 적용함으로써 공격 발생 시 공격의 효과를 경감시켜주는 기술이나, 오탐을 피하기 어려우며 이에 따른 packet loss rate를 증가시키는 효과가 있다[15],[17]. 국내의 경우 이동통신 네트워크 보안 관련 연구는 아직 활발히 연구되지 않아 연구 시작 단계인 것으로 알려져 있다.

이동통신 네트워크 공격 대응을 위한 상용 제품은 주로 WCDMA 네트워크에서의 무선 보안 게이트웨이 형태의 제품이 주류를 이루고 있다. Check Point의 Firewall-1 GX, Fortinet의 FCR-5001A, FCR-3810A, 그리고 Juniper Network의 Netscreen-500 GPRS, ISG 2000 GPRS 등이 대표적인 제품들이다. 이들 제품들은 주로 이동통신 네트워크에서의 스팸 탐지 및 대응, GTP 프로토콜 이상 탐지 및 트래픽 이상 탐지 등의 보안 기능을 제공한다.

GTP는 GSM, UMTS 그리고 LTE 네트워크에서 데이터 서비스(GPRS) 제공을 위해 널리 사용되는 IP 기반의 터널링 통신규약이다. 그러나 GTP는 기본적으로 보안 기능을 제공하지 않기 때문에, 대부분의 무선 보안 게이트웨이류의 보안장비에서는 GTP 트래픽의 메시지 사이즈, 버전 확인 등의 초보적인 보안 기능을 제공하고 있다. 최근 이러한 제품들은 LTE, 펨토셀 기반의 네트워크를 지원하는 제품으로 확대되는 추세이다. 현재 이동통신 네트워크를 대상으로 하는 국산 보안 제품은 알려진 바가 없다.

지금까지 살펴본 바와 같이, 대부분의 이동통신 네트워크에 대한 DDoS 탐지 및 대응기술, 그리고 침입탐지류의 기술들은 코어 네트워크(CN)에서 트래픽을 모니터링하고 이를 기반으로 이상 트래픽 또는 비정상 트래픽을 탐지하는 방식의 기술에 의존한다. 그러나 이러한 이상 또는 비정상 탐지류의 기술들은 일반적인 트래픽보다 값이 큰 트래픽의 탐지에는 많이 사용되나 소량의 트래픽을 이용한 공격에는 그 성능이 제한적일 수 있다.

이는 이동통신 네트워크에서의 이상 탐지가 이동통신 네트워크에서 리소스 사용상의 특성 및 서비스 특성을 아직 반영하지 못하고 기존의 패킷 수와 바이

트 볼륨 등에 의존한 탐지 방식을 사용하기 때문인 것으로 풀이된다.

Ⅵ. 결론

이동통신 네트워크 기술의 발전에 따라, 독립적으로 존재하던 이동통신 네트워크에 인터넷이 결합되어 SNS, 위치기반 서비스 등의 다양한 데이터 서비스가 제공되기 시작했다. 또한, 고성능 오픈 플랫폼 단말의 출시로 이동단말에서 사용자가 원하는 다양한 소프트웨어를 실행할 수 있는 환경이 제공되었다. 이러한 이동통신 네트워크 관련 기술 및 이동단말에서의 사용 환경의 변화는 새로운 다양한 서비스의 등장과 함께 네트워크 공격에 대한 위험도 증대시키고 있다.

최근 이동단말을 대상으로 하는 악성코드가 급격히 증가되고 있음은 이동통신 네트워크에서의 보안 위협 증가를 시사하는 사례라 볼 수 있다. 또한, 4G 네트워크 기술이 본격화 될 경우 always-on 서비스 지원을 통해 이동통신 네트워크에 대한 위협은 더욱 증가할 것으로 예측된다.

본 고에서는 이동통신 네트워크를 대상으로 하는 DDoS 공격기술 및 이들 공격에 대한 현재의 대응기술을 설명하였다. 이러한 공격 대응기술들은 이동통신 네트워크의 코어 네트워크에서 이상 또는 비정상 탐지를 기반으로 하고 있다. 따라서, 인터넷에서 발생하는 것과 같은 대량의 DDoS 공격에는 탐지와 대응 기능을 제공하지만 소량의 트래픽을 이용한 DDoS 공격에 대한 탐지 및 대응 성능에는 더 많은 연구를 필요로 한다.

● 용 어 해 설 ●

WCDMA: 3G 이동통신 네트워크에서 사용되는 무선접속 기술

3GPP: 이동통신 관련 단체들 간의 공동연구 프로젝트로 3G 이동통신 시스템 규격작성을 목적으로 함.

LTE(Long Term Evolution): 고속 데이터 이동통신 서비스를 위한 표준

약어 정리

3GPP	3rd Generation Partnership Project
AQM	Active Queue Management
BS	Base Station
CN	Core Network
CSCF	Call Session Control Function
CSCN	Circuit Switched Core Network
DDoS	Distributed Denial of Service
EDGE	Enhanced Data Rate for GSM Evolution
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTP	GPRS Tunneling Protocol
HLR	Home Location Register
IMS	Internet Multimedia Subsystem
LTE	Long Term Evolution
MSC	Mobile Switching Center
PWCN	Packet Switched Core Network
RAB	Radio Access Bearers
RED	Random Early Discard
RLS	Resource List Server
RNC	Radio Network Controller
RRC	Radio Resource Control
SGSN	Serving GPRS Support Node
SMSC	Short Messaging Service Center
SNS	Social Network Service
UMTS	Universal Mobile Telecommunication System
VLR	Visiting Location Register
WFQ	Weighted Fair Queuing

참 고 문 헌

[1] CISCO “CISCO Global Mobile Data Traffic Forecast 2010-2015,” Feb. 2011.

[2] "안철수연구소 보도자료," 2011. 10. 10.
[3] YTN, "중국, 휴대전화 공격 악성코드 기승," 2010. 10. 8.
[4] 서울신문, "열다섯 고교생 해커, 문자폭탄 프로그램 테러," 2010. 8. 12.
[5] W. Enck et at., "Exploiting Open Functionality in SMS-capable Cellular Networks," *Proc. ACM CCS*, Alexandria, Virginia, US, Nov. 2005.
[6] J. Serror, H. Zang, and J.C. Bolot, "Impact of Paging Channel Overloads or Attacks on a Cellular Network," *Proc. WiSe*, Los Angeles, California, US, Sept. 2006.
[7] P. Lee, T. Bu, and T. Woo, "On the Detection of Signaling DoS Attacks on 3G Wireless Networks," *J. Comput. Netw.*, vol. 53, no. 15, Oct. 2009.
[8] P. Traynor, P. McDaniel, and T.L. Porta, "On Attack Causality in Internet-connected Cellular Network," *Proc. USENIX Security Symp.*, 2007.
[9] P. Traynor et al., "Mitigating Attacks on Open Functionality in SMS-Capable Cellular Network," *Proc. ACM MobiCom*, 2006.
[10] F. Ricciato, A. Coluccia, and A. D'Alconzo, "A Review of DoS Attack Models for 3G Cellular Networks from a System-design Perspective," *J. Comput. Commun.*, vol. 33, 2010, pp. 551-558.
[11] B. Zhao et al., "A Chain Reaction DoS Attack on 3G Networks: Analysis and Defenses," *Proc. IEEE Infocom*, 2009.
[12] Fabio Ricciato, "Unwanted Traffic in 3G Networks," *ACM SIGCOMM Comput. Commun. Review*, vol. 36, no. 2, Apr. 2006.
[13] J. Rosenberg et al., "SIP: Session Initiation Protocol," RFC 3261, IETF, June 2002.
[14] "LG U+ 사상 초유 데이터 불통 사태," 매일경제 이코노미, 제1619호, 2011. 8. 17.
[15] S. Floyd and V. Jacobson, "Random Early Detection Gateway for Congestion Avoidance," *IEEE/ACM Trans. Netw.*, vol. 1, no. 4, Aug. 1993.
[16] A. Demers, S. Keshav, and S. Shenker, "Analysis and Simulation of a Fair Queueing Algorithm," *SIGCOM Symp. Proc. Commun. Architectures & Protocols*, 1989, pp. 3-12.
[17] S. Yi et al., "Proxy-RED: an AQM Scheme for Wireless Local Area Networks," *J. Wireless Commun. Mobile Comput.*, vol. 8, no. 4, 2006.