지연접속 제어를 통한 모바일 PSCN 환경의 PT-DoS 공격에 대한 방어 기법

주은영*
*고려대학교 컴퓨터.정보통신공학과
e-mail : expect@korea.ac.kr

Defense Techniques of PT-DoS Attacks By Delay Access Control on Mobile PSCN Environment

Eun-Young Joo*
*Dept. of Information and Communication Engineering, Korea University

요 약

통신기술의 발달과 스마트 폰의 급격한 보급으로 인하여 모바일 환경은 음성 데이터 기반의 환경에서 인터넷 데이터 기반의 환경으로 급격히 변화되었다. 이로 인하여 음성 서비스 처리 위주의 음성 데이터 기반 모바일 환경은 대용량 동영상 서비스, 인터넷, 메신저 등의 유선 네트워크 환경과 같은 다양한 서비스가 요구되는 환경으로 변화되었다. 이러한 환경 변화로 인하여 모바일 네트워크는 무선 네트워크상의 취약점 뿐 만 아니라 유선환경의 네트워크 취약점을 동시에 지니는 환경으로 변화되었고, 이로 인한 다양한 새로운 취약점들이 부각되기 시작하였다. 본 논문에서는 이와 같이 새롭게 부각되고 있는 모바일 Packet Switched Core Network(PSCN) 환경에서 Service Provider(SP)의 Service Recover로 인해 유발되는 Paging Table Denial of Service(PT-DoS)를 효율적으로 제어하기 위한 Delay Access Control(DAC) 기반의 QoS를 이용한 방법을 설계/구현하였다. 그리고 실험을 통해, PT-DoS를 차단하여 PSCN 공격을 미연에 방지하는 효과를 확인하였다.

1. 서론

모바일 네트워크 환경이 기존의 음성 데이터 기반의 환경에서 인터넷 데이터 기반의 환경으로의 변화함에 따라, 여러 가지 보안상 취약점들에 노출되고 있다[1-3]. 이러한 모바일 네트워크 환경은 크게,단말기[4], Radio Network Controller(RNC), Circuit Switched Core Network(CSCN), 그리고 PSCN 환경과 같이 4가지 환경으로 구분되며, 환경에 따른 각각의 취약점들을 가지고 있다[6-8]. 모바일 환경의 변화 이전의 공격 방어 방법들은 대부분은 RNC 환경에서의 방어 기법에 대하여 다루고 있다[6-8].

본 논문에서는 모바일 네트워크의 환경 변화에 따른, PSCN 환경의 새로운 보안 취약점에 대하여 살펴보고자 한다. PSCN 환경은 SGSN(Serving GPRS Support Network)과 GGSN (Gateway GPRS Support Network)으로 구성된다[5]. PSCN 환경의 특징은 무선 사용자가 세션을 유지하기 위해서 유선 SGSN과 GGSN의 페이지 테이블의 모바일 사용자 세션을 재 활성화하여 사용하게 된다[5]. 이 방법은 모바일 장치의 무선 세션을 유지하여 원활한 서비스를 제공하기 위해서 유선망의 SGSN과 GGSN 사이를 대신 처리하기 위함이다. 본 논문에서는 PSCN 환경의 세션 처리 특징을 이용한 PT-DoS 공격을 다루고자 한다.

PT-DoS의 공격 특징은 Service Provider(SP)에서 제공되는 특정 서비스가 불안하여, 서비스가 재 기동 하는 순간 발생한다는 점이다. SP의 서비스 재 기동은 서비스에서 모바일 사용자에게 다시 서비스를 제공하기 위해서 네트워크 패킷이 DoS 형태로 PSCN망을 지나가게 되고, 이로 인해서 PSCN망의 페이지 테이블이 활성화된다. 이 때, PSCN망의 페이지 테이블 활성화로 인하여 PSCN망의 SGSN과 GGSN에 과부하가 발생하게 되어, 이로 인한 네트워크 환경에 장애를 야기한다.

이러한 문제를 해결하기 위한 대표적 연구로는 PSCN망의 DoS 취약점을 제어하기 위한 Packet Base QoS 기법[10]과 IP Base QoS[11] 기법이 있다. Packet Base QoS는 전체 패킷을 제어하는 방법이기 때문에 모든 모바일 사용자에 악 영향을 준다는 문제점을 가지고 있으며, IP Base QoS는 정상 사용자가 폭주 하는 상황에 대한 제어를 할 수 없다는 문제점을 가지고 있다.

본 논문에서는 이러한 문제점을 해결하기 위하여 DAC(Delay Access Control) 기반의 QoS 방법을 제안한다. 그리고 본 논문에서 제안하는 방법이 PSCN 망의 PT-DoS를 효율적으로 제어함을 실험을 통해 확인하고자 한다.

2. 관련 연구

PSCN망의 PT-DOS 공격의 제어하기 위한 연구로는 Packet Base QoS와 IP Base QoS 방법이 대표적이다.

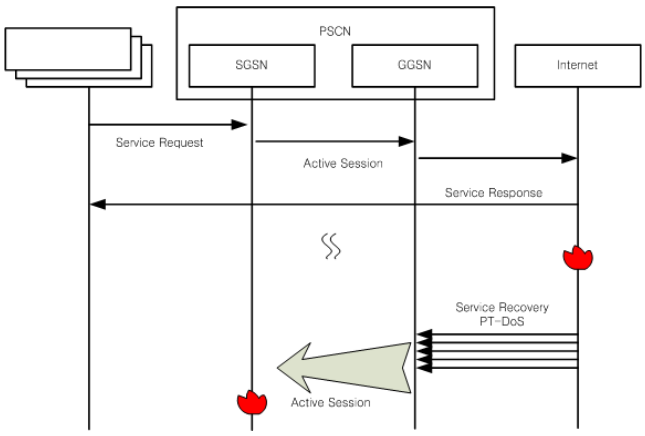
Packet Base QoS는 PSCN망에 지나다니는 패킷(packet)의 양을 제어 하는 방법이다. 이 방법은 전체 PSCN망의 전체 네트워크 대역폭(Network bandwidth)을 보호하는 방법이다[10]. 이 방법은 전체 대역폭을 제어할 수는 있으나, 정상 모바일 사용자까지 인터넷 서비스 지연 및 서비스가 안 되는 현상이 발생하는 문제점이 있다.

IP base QoS는 모바일 사용자 IP별 트래픽 양을 제어하는 방법이다. IP Base QoS는 사용자 IP별 트래픽양이 증폭되거나, DoS형태의 공격을 제어하는 효과를 가진다[11]. 하지만, 본 논문에서 다루고 있는 PSCN망에서의 PT-DoS와 같이, 전체 대역폭의 사용량은 증가 하지만 IP별 트래픽 사용량이 증가 하지 않는 경우에는 제어 할 수 없다는 문제점이 있다.

본 논문에서는 이 두 가지 제어 방법이 가지고 있는 정상 사용자 서비스 제어 및 전체 대역폭에 대한 서비스를 제어하는데 있어서의 문제점을 해결하고자, DAC QoS 기법을 제안한다.

3. DAC QoS의 설계 및 구현

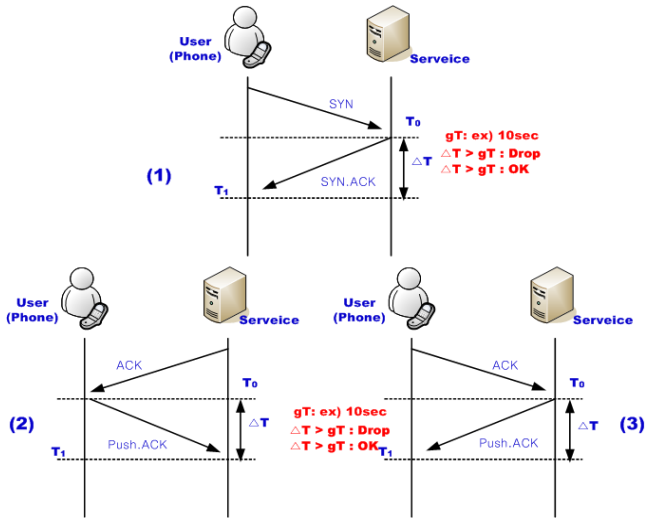
본 논문에서는 그림 1에서와 같이 SP에서 제공되는 서비스가 재시작 되면서 모바일 사용자에게 서비스가 제공되게 될 때, PT-DoS가 발생하는 공격을 보다 효율적으로 제어 하고자 한다. PT-DoS는 서비스가 재시작하는 경우, 패킷(트래픽)의 지연 접속이 발생한다는 특성에 착안하여, 이 트래픽을 제어 할 수 있도록 설계하였다. 이러한 PT-DoS는 SP의 서비스가 재시작 될 때도 발생하지만, 많은 사용자가 이용하는 SP의 서비스가 종료 되었을 때, 모바일 사용자가 SP 서비스를 찾기 위해서 다량의 트래픽을 발생하는 조건에도 발생 할 수 있다.



(그림 1) PT-DoS로 인한 PSCN망 장애 현상

본 논문에서는 SP에서 제공되는 서비스의 재시작 때 발생하는 PT-DoS 뿐만 아니라, 사용자 단말기에서 사용자 접속시도의 트래픽이 서비스 지연 상황을 발생시킨다는 가정 하에서 PT-DOS 제어를 하였다.

PSCN망에서는 모바일 사용자의 서비스 사용 세션을 유지함으로써 모바일 서비스를 원활하게 하기 위해서 세션의 유지 시간을 설정하여 관리 한다. 이 최소 세션 유지 시간을 gT라고 정의한다. 그림 2의 (1)에서와 같이 모바일 사용자와 SP 서비스 간의 이전 마지막 패킷과 현재 도달한 패킷의 시간차를 ΔT라 정의 한다. 본 논문에서는 최소 세션 유지 시간 gT기준으로 하고, 패킷의 시간차 ΔT의 차이로 지연시간이 발생했는지를 판단하게 된다. 그림 2의 (2)는 모바일 사용자의 응답이 지연된 경우를 표현한 것이며, 그림 2의 (3)은 SP의 서비스에서 지연이 발생한 경우를 표현한 것이다.



(그림 2) PSCN망의 지연현상

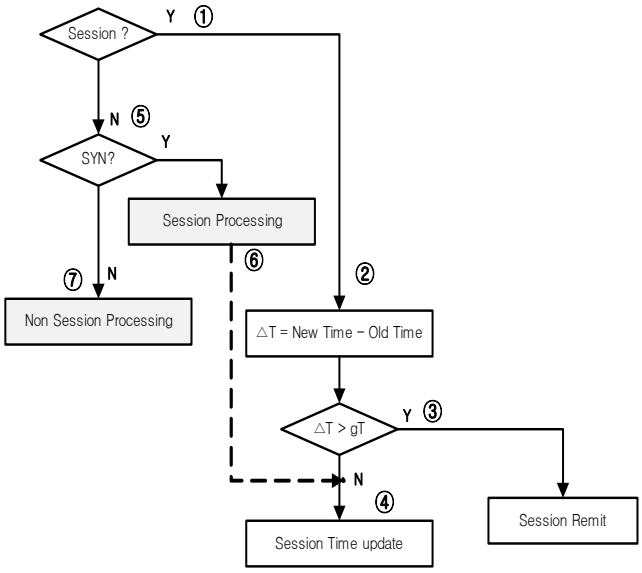
본 논문의 QoS 조건중 하나인 지연현상 제어를 하기 위해서 그림 2와 같이 ΔT가 gT보다 클 경우와 작을 경우를 나눠서 처리하였다. 간략한 지연시간 측정은 다음과 같다.

- ΔT > gT(세션 유지시간) 일 경우 Drop (QoS)
- ΔT <= gT(세션 유지시간) 일 경우 OK

본 연구에서는 이러한 지연 현상을 해결하기 위한 기존 연구를 응용하여, 3-way handshake 연결된 상태에서, 세션이 정상적일 때는 매 패킷 최소 세션 유지시간 gT 안에 트래픽이 도달 할 경우에는 정상사용자로 인증한다. 또한 지연발생이 있는 경우에는 비정상 세션으로 관리하여 네트워크 대역폭을 QoS하여 보호할 수 있도록 구현 하였다. 그림 2와 같이 패킷의 시간차 ΔT가 gT보다 클 경우에는 PT-DoS로 판단하여 QoS 기능을 활성화하게 되고, IP 별 허용 QoS 임계치 이상일 경우에는 패킷 양을 제어할 수 있도록 구현하였다.

이러한 제어 방법은 정상 세션의 경우에는 넓은 대역폭

구간을 사용하고, 비정상 세션의 경우에는 제한 된 대역폭 구간을 사용하도록 한다. 이 특징은 “분산서비스거부공격 차단장치 및 그 방법”[6]을 응용하였으며, 그림 3과 같은 처리 프로세스 과정을 추가하여 DAC 기반의 QoS 엔진을 구현하였다.



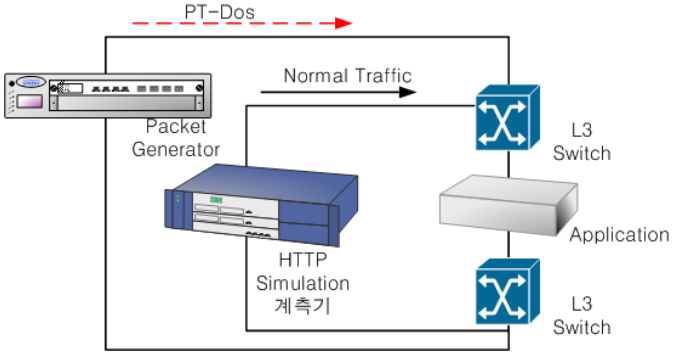
(그림 3) 세션 관리 QoS 흐름도

DAC QoS는 모바일 사용자가 서비스를 사용할 때, 이전 세션 사용자인지 검사하고(그림 3의 ①), 이전 세션일 경우에는 마지막 패킷과 현재 패킷의 시간 차이인 △T 값을 계산한다(그림 3의 ②). △T차이가 PSCN망의 세션 허용시간 gT보다 클 경우에는(지연 되었을 경우), PT-DOS으로 판단하여 해당 세션을 비정상 세션으로 제어 엔진으로 넘겨서, QoS 되도록(그림 3의 ③) 설계/구현 하였다.

4. PT-DoS 위협 제어 구현 및 실험

본 논문에서 제안하고 있는 DAC QoS 기법을 대표적인 PSCN망의 PT-DOS 공격 제어 방법인 Packet Base QoS와 IP Base QoS 기법과 비교실험을 전개하여 그 효율성을 확인하고자 하였다. 그림4의 실험환경은 그림 1과 같이 PSCN망에서 PT-DoS가 공격 되었을 경우를 가상환경으로 구현하였으며, 공격이 발생하였을 때 페이지 테이블이 활성화 된다고 가정하였다. 그림4의 HTTP Simulation 계측기로 정상 트래픽(Normal Traffic)을 생성하였고, Packet Generator로, PT-DoS의 지연접속 패킷을 생성하였다. 그리고 평상시 PSCN망 허용 범위는 20만 pps, 허용 IP의 범위는 20만 IP로 제한된 환경을 가정하고 실험을 진행하였다. 실험 조건은 표 1과 같다.

표 1의 조건#1, 조건#2의 정상 사용자는 10만개 IP로 사용자는 1pps 조건으로 통신을 하도록 설정하였다. 공격트래픽은 조건#1에서 PT-DoS 공격 IP를 10만개의 IP가 9pps 조건으로 공격이 발생하는 조건이다. 조건#2는 PT-DoS IP 90만개가 1pps 트래픽 조건으로 공격을 발생시키는 조건을 나타낸다. 조건#1은 공격에 의한 PT-DoS 조건으로, 조건#2는 대규모 사용자 지연접속 조건을 가정하였다.



(그림 4) 시뮬레이션 테스트 환경

<표 1> 실험 조건

	트래픽 생성 조건	차단조건
조건 #1	Normal IP : 10만 IP, 1 pps PT-DoS IP :10만 IP, 9 pps total : 100만 pps	Packet OoS : 20만 pps IP QoS : IP 별 1 pps DAC QpS : IP별 1pps (지연접속 : 전체 차단)
조건 #2	Normal IP : 10만 IP, 1 pps PT-DoS IP :90만 IP, 1 pps total : 100만 pps	Packet OoS : 20만 pps IP QoS : IP 별 1 pps DAC QpS : IP별 1pps (지연접속 : 전체 차단)
- PSCN망 허용 범위 20만 pps. - PSCN망 허용 범위 20만 IP.		

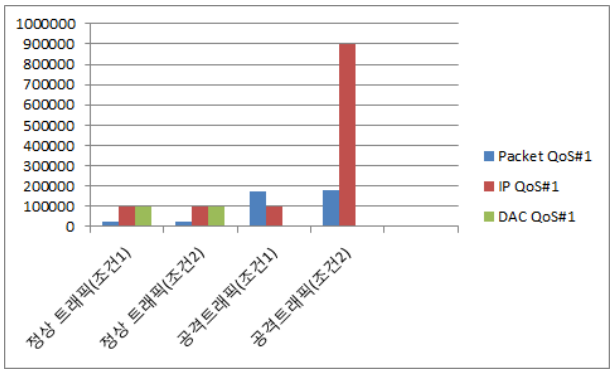
그림5의 실험결과는 각 QoS별 표1 조건#1과 조건#2의 패킷 통과량을 표시하였다. 정상트래픽 패킷 통과량은 정상트래픽이 차단되지 않았는지를 표시하고, 공격트래픽 패킷 통과량은 공격패킷 통과량을 표시한다.

Packet Base QoS의 조건#1 상황의 실험결과를 살펴보면는 정상사용자 패킷이 25,000 pps 정도 통과 하였고, 공격트래픽이 175,000 pp정도 통과 하였다. 즉, 공격 차단률은 80% 정도 이고,정상 트래픽도 75%정도 실패 한 것을 확인 할 수 있었다. 조건#2에서도 비슷한 결과를 확인 할 수 있었다. PSCN망의 허용범위 20만 pps는 수용하지만, 정상사용자 IP도 차단이 되는 것을 확인하였다.

IP Base QoS는 조건#1에서 정상사용자 패킷은 10만 pps와 공격트래픽도 10만 pps 로, PSCN 허용 범위 20만 pps를 수용하였다. 조건#2의 조건에서는 정상사용자 10만 pps, 공격트래픽 90만 pps로 공격트래픽 차단률이 0%로, PSCN망 장애 가능성을 발생 시킬 수 있는 것을 확인할 수 있었다.

DAC QoS는 조건#1과 조건#2의 정상사용자의 10만 pps, 공격 트래픽 0pps 통과율을 확인 할 수 있었다. PSCN 허용 범위 20만 pps를 충족시키면서, 정상 사용자에 피해를 주지 않는 것을 테스트 결과 확인 할 수 있었다. 이를 통

해서 본 논문에서 제시하고 있는 DAC QoS가 Packet Base QoS와 IP Base QoS 기법에 비해 조건#1(공격 상황)과 조건#2(대규모 사용자 접속) 상황 모두에서 보다 효율적으로 PT-DoS에 대한 위협 제어가 가능함을 확인할 수 있었다.



(그림 5) 테스트 실험 결과

5. 결론

본 연구에서는 PSCN 망에서 PT-DoS와 같은 모바일 네트워크 환경의 위협요소를 효율적으로 제어 할 수 있는 방안으로 DAC QoS방법을 제시하였다. 그리고 실험을 통해서 현재 DAC QoS의 오차 범위 3%에서 세션의 패킷을 제어 할 수 있는 것을 확인 하였다.

본 논문에서는 PT-DoS의 PSCN망의 세션 활성화 공격에 대한 제어에 방법을 제시하였지만 지연 접속 공격(PT-DoS)이 발생할 경우, PSCN망의 세션 페이지 테이블이 활성화 현상으로 인한 네트워크 지연이 발생하는 문제는 해결하지 못하였다. 때문에 향후에는 이러한 문제를 해결하기 위한 지연접속의 발생과 PSCN망의 페이지 테이블을 효율적으로 제어 관리하기 위한 방안에 대한 연구를 수행할 예정이다.

참고문헌

[1] 김영세, 이정우, 한진희, 신진아, 전성익, “무선 네트워크 연동 보안 기술 동향” 전자통신동향분석 제20권 제 1호, pp.100-111, 2006년 2월.

[2] 조병호, “스마트폰 정보보안 기술 통향”, 주간 기술 동향, pp.17-23, 2011년 9월.

[3] 정수환, “모바일 네트워크 보안 기술 동향”, 정보와 통신, pp.18-23, 2010 6월.

[4] 강동호, 김정녀, 조현숙 “모바일 보안 위협 및 보안 서비스 기술 동향”, 정보학회지, pp.51-56, 2010 6월.

[5] 이상원, 김종현, 서동일, “이동 통신 네트워크 DDoS공격 및 대응 기술 동향”, 전자통신동향 분석 제 26권 제6호, pp.154-163, 2011년 1월.

[6] (특허출원 제10-0858271, 1998) 조학수(1997). “분산서비스거부공격 차단장치 및 그 방법”

[7] Bahareh Sadeghi, and Edward W. Knightly, “Architecture and Algorithms for Scalable Mobile QoS”, Wireless Networks Vol.9, pp.7-20, 2003.

[8] Mathieu Demars, Benoît Fourestié, Julien Mourlon, Jean-Marc Picard, and Sylvain Renou, “3G Network QoS Estimation in a Multi Service Context”, IEEE/VTC 61st ,Vol.3, pp.1821-1824, 2005.

[9] Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta “Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks”, Networking, IEEE/ACM Transactions on Networking, Vol.17(1), pp.40-53, 2009.

[10] Rajeev Koodli, and Mikko Puuskari, ″Supporting Packet-Data QoS in Next-Generation Cellular Networks″, IEEE Communications Magazine, pp.180-188, 2001.

[11] Victor Marques, “An IP-Based QoS Architecture for 4G operator scenarios”, IEEE Wireless Communications, pp.54-62, 2003.