RFID MDS 시스템의 DDoS 공격 가능성 분석과 방어책에 관한 연구

남동일, 최병진, 유승화

A Study of optimized MDS defense against DDoS attack on RFID network

Dong Il Nam, B. J. Choi, S. W. Yoo

Abstract

Radio Frequency Identification (RFID) is a technology used to identify the physical objects and get information about the object on which the tag attaches from network. It is expected that RFID will lead IT market from human-oriented to object-oriented. Therefore, RFID technology and services will become wide-spread. But the system of RFID naming service is quite similar to the existing DNS facilities. So it has many weak points against to DDos attack. Furthermore if the MDS server is under attack, there might be trouble of total RFID networks.In this paper, we propose a new detecting model to find attack traffic at local routers by using Management Information Base (MIB) which is optimized for RFID MDS server.

Key Words : RFID Security, DDOS attack, MDS

* 아주대학교

1. 서론

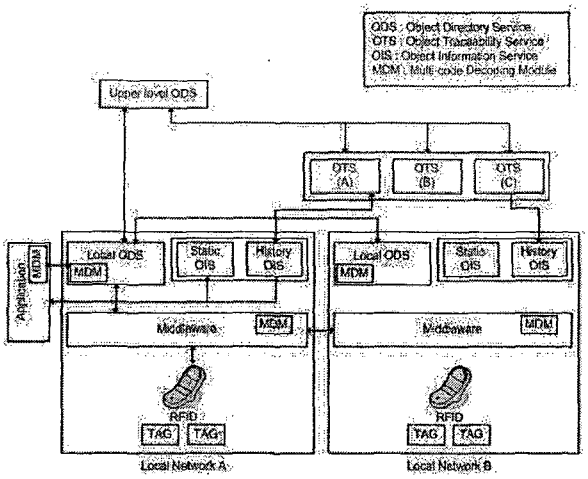
RFID(Radio Frequency Identification)기술은 사물 각각에 작은 식별정보인 RFID 태그(Tag)를 저장하고 사물 및 주변 환경정보를 안테나와 리더(Reader)를 통해 무선주파수로 네트워크에 전송하여 처리하는 비 접촉형 자동식별 기술로 궁극적으로 모든 사물에 컴퓨팅 및 통신 기능을 부여해서 유비쿼터스 네트워크로 발전시키는 것을 목표로 한다. RFID 기술은 여러 분야에 쉽게 적용할 수 있는 범용성과, 기존 산업의 인프라에 큰 수정을 가하지 않고도 특별한 충돌 없이 자연스럽게 적용시킬 수 있는 장점을 가지고 있다. [1]

그러나 RFID 네트워크의 많은 부분은 기존 인터넷 인프라 구조의 특징을 그대로 지니고 있다. 따라서 유선 인터넷 인프라가 가지고 있는 취약점에 많은 부분이 노출되어있다. 특히 RFID 의 핵심부분이라 할 수 있는 MDS 서버의 경우 기존 DNS 서버와 운용방식이 거의 비슷하며 DDoS 공격에 쉽게 노출되어 있다. 또한 최근DDoS 의 변형공격인 DRDoS 공격방법이 등장하면서 이러한 약점에 대한 방어책은 더욱 절실하게 요구되고 있는 실정이다. [4]

본문에서는 이러한 DDoS 및 DRDoS 공격으로부터 RFID 의 MDS 서버를 효율적으로 방어하는 방법에 대해 제안한다. 제안된 방법에서는 첫번째로 RFID MDS 시스템에 대하여 소개한다. 또한 이번에 제안하는 방법의 구현에 중요한 역할을 하는 카운팅 블룸 필터를 소개한다. 그 후에 기존 Friendly Server List Filtering 방법에 대하 소개하고 이를 개선하여 로컬라우터 상에서 공격 트래픽을 감지하여 MDS 서버를 방어할 수 있는 L-카운팅 블룸필터를 제시한다. 4장에서는 실험결과를 제시한 후 5장에서 결론을 도출한다.

2. RFID 네트워크 구조와 카운팅 블룸 필터

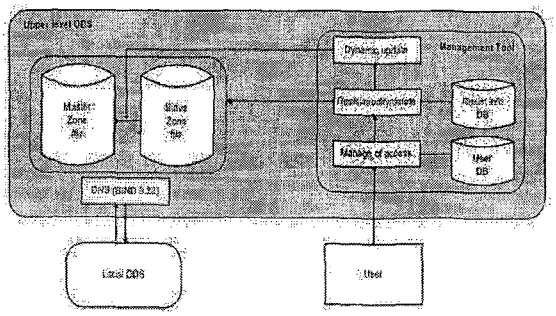
2.1 RFID MDS Network 구조



(그림 1) RFID MDS 네트워크 구성도

(그림 1)은MDS 를 도식화한 것이다. MDS 네트워크의 주요 구성 요소로는 객체 검색 서비스를 제공하는 Upper Level ODS (Object Directory Service) 와 Local ODS, 이력 정보에 대한 서비스를 담당하는 OTS (Object Traceability Service), 객체에 대한 정보를 보유한 OIS (Object Information Service) 등이 있다. Upper Level ODS 는 각 기관의 Local ODS의 위치에 대한 정보 파일을 관리하고 이에 대한 서비스를 제공하는 역할을 한다. Upper Level ODS 는 Local ODS의 위치 정보를 DNS 형태로 서비스한다. 이것은 BIND를 통해서 구현되는데, BIND의 검색을 위한

정보들이 저장되는 파일로는 마스터존(Master Zone) 파일과 슬래이브존(Slave Zone) 파일이 있다. (그림 2)은 Upper Level ODS 의 구성도를 보여준다.

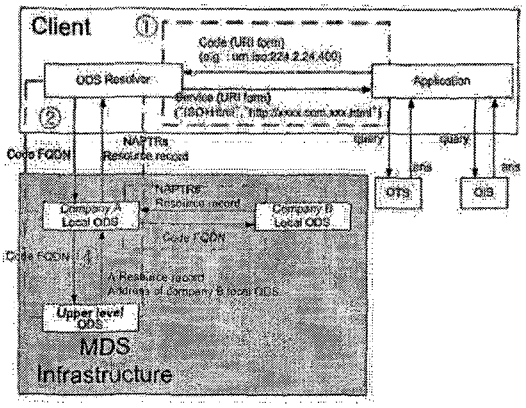


(그림 2) Upper Level ODS 구성도

2.2 RFID MDS 의 동작구조

(그림 3)은 MDS의 동작 구조를 보여준다. 객체의 RFID 코드를 읽어들인 사용자는 ODS에 접속하기 위해서 해당 코드를 미들웨어에게 전송한다. 미들웨어는 MDM을 이용해서 RFID 코드가 어떤 체계로 이루어졌는 지 식별하고 이에 알맞은 URI 형태로 변환한다.

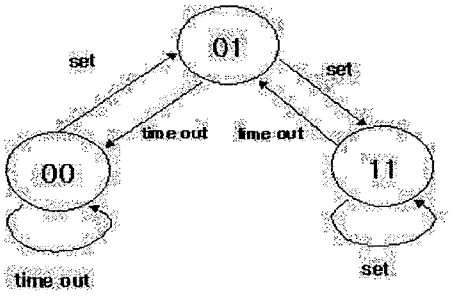
변환된 URI 형태의 코드를 기관의 ODS 리졸버 (Resolver)에게 질의한다. 이 때 질의 패킷은 DNS 질의 형태를 이용하기 때문에, 변환된 URI는 ODS 리졸버에 의해서 다시 FQDN (Fully Qualified Domain Name)의 형식으로 고쳐진다.



(그림 3) MDS 동작 구조

(그림 3)에서 질의를 수신한 A 기관의 Local ODS는 요청받은 코드의 정보가 자신이 속해있는 기관의 OIS에 존재하지 않는 경우, National ODS에게 질의한다. 이 때에도 전과 동일하게 DNS 질의 형태를 이용한다. National ODS는 이 코드에 대한 정보가 B 기관의 Local ODS에 있다는 사실을 검색하고, A 기관의 Local ODS에게 B 기관 Local ODS의 주소를 A 타입의 RR 레코드 형식으로 알려준다.

2.3 카운팅 블룸 필터



(그림 4) 카운팅 블룸필터의 상태흐름도

카운팅 블룸필터는 입력되는 하나의 엔트리에 대해서 서로다른 k개의 해쉬함수와 두개의 비트 백터를 이용하여 집합 A = {a1, a2, ...

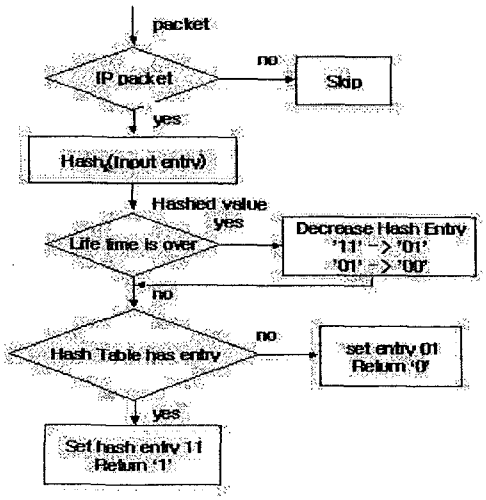
an)에 존재하는지를 표현하는 방법으로서 DDoS 공격을 백본링크상에서 막는데 이용된다. 통과하는 트래픽의 각 패킷을 체크하여 SIP, DIP(Destination IP address), D_Port(Destination Port) 이 세가지 엔트리를 이용하여 (Ks, Kd, Kp)의 튜플을 구성한다.

각각의 엔트리는 생명주기를 가지고 있으며 생명주기내에 패킷이 일정개수이상 들어오면 DDoS 공격이라고 판단하며, 생명주기가 지나면 두개의 비트로 이루어진 백터값이 하나씩 떨어진다. (그림 4)는 카운팅 블룸필터의 해쉬 엔트리에 관한 상태흐름도이다. 카운팅 블룸필터는 적은 시스템 리소스 소비와 빠른 실행속도를 가지고 있어 백본 링크상에서 대규모의 데이터를 필터링 하기에 적합하다. [2][3].

3. 카운팅 블룸필터 알고리즘

앞에서 언급했던 상위 ODS를 DDoS 공격으로부터 보호하기 위해 인증된 서버 리스트를 만들고 리스트에 있는 Local ODS 로 부터 들어온 쿼리에 한하여 ODS 서비스를 제공해 주는 방법은 인증된 서버 리스트 정보가 누출되는 경우, 혹은 인증된 Local ODS 서버의 관리자 권한이 침입자에게 장악되어 DDoS 공격 쿼리를 보내 공격하는 경우에는 방어책이 될 수 없을 뿐만 아니라 최신 DDoS 공격 기법인 DRDOS 공격에 역시 약하다는 단점을 가지고 있다. 이를 보완하기 위해 본문에서는 기존의 방법에 카운팅 블룸필터를 로컬 방화벽에 적용시킬 수 있게 변형한 Local Counting Bloom Filter 탑재를 제안한다.

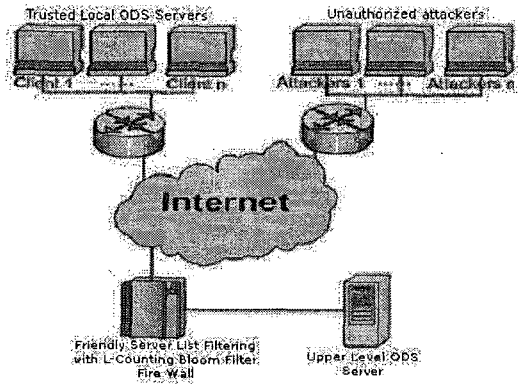
로컬 방화벽에 도착한 inbound 패킷들의 목적지 주소와 목적지 포트번호는 대부분 비슷하지만 발신지 주소는 사전에 인증된 서버마다 다르기 때문에 SIP 를 해쉬값으로 이용하면 DDoS 공격 혹은 DRDoS 공격에 대한 필터링이 가능하다. 특정 SIP 값을 가진 ODS 질의 패킷이 들어오면 L-카운팅 블룸필터는 해당 SIP의 해쉬값에 대응하는 비트벡터 값을 00에서 01로 증가 시킨다. 일정 단위시간 이내에 같은SIP 값을 지닌 DNS 질의 패킷이 또 들어오게 될 경우 01에서 11로 비트벡터 값을 증가시킨다. 그로부터 일정 시간 이내에 다시 또 같은 SIP 을 가진 질의 패킷이 들어오게 되면 이때는 DDoS 공격으로 판정하고 해당 SIP 를 가진 패킷은 모두 버리게 된다. 만일 일정시간 내에 같은 SIP 를 가진 질의 패킷이 들어오지 않을 경우 해당 SIP의 해쉬값에 대응하는 비트벡터 값은 감소한다. 이러한 방법을 이용하면 인증된 Local ODS 리스트 정보가 누출되어 공격자가 인증된 서버에서 보낸 쿼리인 것처럼 패킷을 조작하여 상위 ODS에 보낸다고 해도 필터링 할 수 있으며 블룸필터의 특징인 적은 오버헤드와 빠른 처리 속도를 감안하면 여러 대의 서버로부터 한꺼번에 공격 받는 DRDoS 공격에 좋은 성능을 발휘할 것이란 것을 쉽게 예상할 수 있다.



(그림 5) L-카운팅 필터의 플로우차트

4. 시뮬레이션

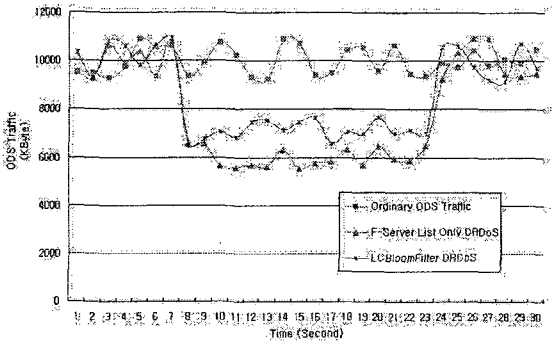
4.1 시뮬레이션 환경



(그림 6) 시뮬레이션 환경 구축도

(그림 6) 에서와 같이 시스템을 구축하였다. L-카운팅 블룸필터 라우터에는 L-카운팅 블룸필터와 Friendly Server List Filtering 에 기반한 방화벽이 포함되어 있다. 각각의 필터는 독립적으로, 혹은 동시에 같이 작용할 수 있으며 제안된 방법은 두 개의 필터가 동시에 작동하는 경우이다.

4.2 시뮬레이션 결과



(그림 7) DRDoS 플러딩 공격의 실험결과

(그림 7)은 최근 등장한 DDoS 변종 공격 패턴 중 하나인 DRDoS 공격에 대한 실험 결과이다. DRDoS 공격에 본문에서 제안된 방법이 역시 좀 더 나은 성능을 보였다. 이는 제안된 방법이 적은 오버헤드와 빠른 처리속도를 가지고 있는 카운팅 블룸 필터에 기반을 둔 것에 기인한다고 할 수 있다.

DRDoS 등 대규모의 DDoS 공격을 방어하는데 있어서 가장 중요한 요소 중 하나는 패킷을 필터링 하는데 있어 소요되는 CPU의 자원이다. 방화벽이 필터링을 처리하는 과정에 있어 Overhead가 커질수록 필터링 처리시간은 늦어지고 이로인해 정상적으로 필터링 되지 못하거나 Time Out 등으로 Drop 되는 패킷의 숫자는 증가하게 된다.

5. 결론 및 향후 연구계획

본문에서는 MDS 서버를 방어하기위해 고안된 L-카운팅 블룸필터를 제안하였다. 본 문에서는 기존의 알고리즘에 대한 취약점을 분

석한 뒤 그러한 점을 보완할 수 있는 로컬 카운팅 블룸필터를 기존의 방화벽에 추가로 탑재하였다. 이에 따라 적은 시스템 자원과 빠른 속도로 의심스러운 공격 패킷들을 쉽게 필터링 할 수 있었으며 최근 들어 부각되고 있는 DRDoS 공격을 막아내는데 있어서도 탁월한 성능을 발휘함을 보여주었다. 그러나 DDoS 공격은 날이 갈수록 지능화, 고도화 되고 있는만큼 로컬라우터에서 막는 방법과 백본링크 및 미들급 라우터에서 방어방법이 병행되어야 보다 효율적으로 공격을 차단할 수 있다. 즉 인터넷 전반에 걸친 총괄적인 방어방법이 요구된다고 할 수 있다.

참고문헌

[1] E.J. Park "Code Filtering Algorithm for multi-code directory service in global RFID net-work." Ajou Univ, February 2005.

[2] EPC global, "EPCTM Tag data standards version 1.1 Rev.1.24," Standard Specification, April, 2004.

[3]http://www.sns.ias.edu/~jns/security/iptables/ , "Overview about iptables firewall"

[4] Steve Gibson, "DRDoS (Distributed Reflection Denial of Service)" February 2002.

[5] I.R Choi, "Detection of DDoS Attacks and Port Scanning Using Counting Bloom Filter On The Internet Backbone Links" Ajou Univ, August 2004.

[6] E.S. Jeong "Effective detecting DoS attack and scanning at Internet backbone using Bloom Filter" Ajou Univ, February 2004.