http://dx.doi.org/10.14400/JDPM.2014.12.1.423

DDoS 공격에 대한 분석 및 대응방안

홍성혁*
백석대학교, 정보통신학부

Analysis of DDoS Attack and Countermeasure: Survey

Sunghyuck Hong*
Baekseok University, Division of Information and Communication

요 약 DDoS 공격은 DoS 공격의 업그레이드 된 공격방법으로 수많은 DoS 공격이 한 사람의 공격자에 의해 동시에 일어나게 하는 것이다. 초기에는 공격자가 공격 대상을 마비시킬 정도로 수많은 공격 PC를 소유할 수 없기 때문에 이론적인 공격기법이 불과 몇 년 사이에 IT환경이 빠른 속도로 성장하고 악성코드를 이용하여 많은 사용자의 개인 PC를 Botnet화 할 수 있는 방법 등이 발견되면서 사용자들에게 엄청난 손실을 가져올 수 있는 최악의 공격기법이 되었다. 또한 DDoS 공격은 공격의 원인을 찾는 발생지를 찾기 힘들기 때문에 그에 대한 이후 처리에도 문제가 사회적으로 파장이 심각하여 본 연구에서는 DDoS 공격에 대한 분석과 대응책을 제시한다.

주제어 : 패킷공격탐지, 라우터보안, 분산서비스거부, DDoS탐지알고리즘, 네트워크

Abstract DDoS attacks is upgrade of DoS attacks. Botnet is being used by DDoS attack, so it is able to attack a millions of PCs at one time. DDoS attacks find the root the cause of the attack because it is hard to find sources for it, even after the treatment wavelength serious social problem in this study, the analysis and countermeasures for DDoS attack is presented.

Key Words : Packet attack detection, route security, Distributed denial of service, DDoS detection algorithm, Network

1. 서론

DDoS 공격은 인터넷을 통하여 분포하는 대규모의 호스트들이 서로 협력하여 비정상적인패킷을 대량으로 발생시키는 형태이다. 이러한 공격 형태는 사용 가능한 망 자원 또는 공격대상의 시스템 자원을 소비하여 합법적인 사용자들이 시스템이나 망에 접근하여 서비스를 이용하는 것을 방해한다. 따라서 합법적인 사용자들의 서비스 보장과 망의 효율적인 관리를 위해 DDos 공격에 대한 믿을 수 있는 실제적인 방어 기법이 요구되고 있다.[1] DDoS 공격은 정상적인 request 패킷을 과다하게 보내기 때문에, 대응이 사실상 어려워, DDoS 공격에 대한 연구가 많이 진행되고 있다. 본 연구에서는 네트워크 보안 장비별 공격자 식별을 행동 패턴을 분석하여 새로운 DDoS 방어 대응책을 제시 하였다.

2. 패킷공격 탐지와 공격자의 식별

Received 15 October 2013, Revised 17 December 2013
Accepted 20 January 2014
Corresponding Author: Sunghyuck Hong(Baekseok University)
Email: shong@bu.ac.kr

ISSN: 1738-1916

2.1 라우터의 보안

네트워크의 급속한 발전과 함께 현대인들에게 인터넷은 이제 빠질 수 없는 존재가 되었다. 업무를 함에 있어서나 개인생활을 하는데 있어서 인터넷이란 존재가 많은 비중을 차지한다는 말에 이의를 달 사람은 많지 않을 것이다. 이러한 인터넷을 사용할 수 있게 된 이유는 바로 라우터의 등장이라고 할 수 있다. 보안을 고려한 관점에서 라우터의 보안이 그 어떠한 네트워크 보안 중에 가장 중요 할 수 있다. 그런 중요성을 가지고 있는 라우터를 운영함에 있어 고려해야 할 필수적인 보안요소를 알아보겠다.[2]

2.1.1 Default password 보안

원격에서 라우터를 관리할 때 사용할 패스워드를 장비의 초기 설정 그대로 사용할 경우 누구라도 라우터에 접근할 수 있을 것이다. 그래서 기본 패스워드는 인터넷에서 검색을 통해서 쉽게 알려질 수 있으므로 이러한 방법을 감안해서 패스워드는 반드시 변경한 후에 사용해야 합니다. 그리고 Cisco IOS의 enable secret와 같은 기술인 MD5 해싱 기능을 사용하여 보다 강력한 암호와 알고리즘을 사용하는 것이 바람직하다. 또 Service password-encryption같은 기능을 사용함으로 암호 자체도 판독이 불가능하도록 할 수 있다.

2.1.2 SNMP community string 보안

해당 관리자는 네트워크의 트래픽 분석과 장비의 상태를 파악하기 위해서는 MRTG, ESM 또는 RRD과 같은 도구를 사용할 수 있다. 이러한 기능은 일반적으로 snmp protocol을 사용한다. 기본설정으로 이용할 시에 해당 장비(라우터, 스위치, 방화벽 등)의 중요한 정보(Routing, Table, MAC address 등)을 외부로 노출시킬 가능성이 높아진다. 그러므로 SNMP를 사용할 경우에는 반드시 Community strings를 변경한 후에 사용해야 한다. 또한 쓰기 권한 설정 시에 라우터 정보를 변경 할 수 있기 때문에 사용자는 각별히 주의해야 한다.

2.1.3 AAA서버(TACACS/RADIUS)를 통한 사용자 기반의 인증

인증을 위해서 사용되는 AAA(Authentication Authorization Account)서버를 활용함으로써 사용자기반의 인증을 좀 더 강화 할 수 있다. 로컬인증이 아닌 별도의 인증 서버를 사용함으로써 사용자 기반의 인증을 좀 더 체계적으로 할 수 있다. OS에서 사용되고 있는 인증제도와 비슷하게 인증 및 권한 설정까지 가능하기 때문에 인증서버 자체에 대한 보안을 다시 고려해야 한다는 점은 관리자에게 또 다른 문제가 될 수도 있다.

2.1.4 SSH를 통한 보안

라우터 및 기타 네트워크 장비를 접속할 때 SSH를 사용함으로서 Sniffing으로 인한 정보 유출을 방지할 수 있다. 사용의 단순함 때문에 많이 사용되었던 텔넷은 접근 ID와 Password 및 실행한 내용까지 모두 Sniffing이 되더라도 해독하는데 어려움을 줄 수 있다. 또한 배너 문구를 사용하여 접속자에게 경각심을 일깨우는 방법을 통해 사용자에게 손쉽게 알려주는 좋은 방법이다.

2.1.5 SNMP, TELNET, SSH, HTTP의 접근제어

SNMP 및 TELNET, SSH, HTTP의 접근 설정 시에 해당 장비에 접근을 허용할 호스트 IP를 지정함으로써 다른 IP에서의 접근 시도를 사전에 방지할 수 있습니다. 이렇게 계정 정보가 유출되더라도 부적절한 접근을 사전에 막을 수 있다.

2.1.6 Logging 설정을 통한 보안

로그는 라우터만 아니라 모든 네트워크 서버 및 장비에서 침입 및 서버를 분석하는 가장 기본적인 방법이다. 로그서버를 유지하면서 해당 라우터로 이벤트 발생 및 접근시도 등에 대해서 분석시에 유용하게 사용 될 수 있다. 또한 NTP 서버를 사용함으로써 해당 장비와 로그서버 사이의 시간을 동기화 시키는 부분도 중요하기 때문에 장비들의 조금씩 다른 시간 설정이 정확한 분석을 어렵게 만들 수 있다.

2.2 라우터의 보안 기능

2.2.1 IP spoofing 방지

URPF(Unicast Reverse Path Forwarding)을 사용함으로서 변조 된 Source IP를 가지고 접근하는 것을 차단할 수 있다. 이 기능을 설정 시 Cisco의 경우 CEF(Cisco

Express Forwarding)의 FIB table(Forwarding Information Base)을 이용하여 Table에 없는 source IP가 유입 시에 차단이 된다. 또한 ACL(Access Control List)를 사용해서도 IP spoofing을 방지 할 수 있다.

2.2.2 IP spoofing 필터링

ACL을 사용함으로써 사설 대역이나 Broadcast Address를 필터링 할 수 있습니다. 또한 BGP를 구성시에 Prefix List 구성을 통해서 외부로부터의 불적절한 IP가 유입되는 것을 억제할 수 있다.

2.2.3 Secure Routing

암호화를 지원하고 있는 라우팅 프로토콜(BGP, IS-IS, OSPF, PIPv2, EIGRP)를 사용함으로서 인증된 라우터 간에만 라우팅 테이블에 업데이트가 가능하기 때문에 이 기능을 사용함으로서 라우팅 테이블이 유출되거나 조작되는 것을 막을 수 있다.

2.3 트래픽 모니터링

2.3.1 네트워크 트래픽 분석

DDoS 공격의 대표적인 특징은 바로 IP-Spoofing이다. 대부분 공격 메카니즘이 공격자는 정체를 숨기고 사용자가 방어를 어렵게 하기 위해 공격패킷의 SIP(Source IP address) 부분을 각 패킷마다 랜덤하게 생성하고 허위로 채워 넣어버리는 IP-Spoofing 기법을 사용한다. IP-Spoofing기법을 사용하지 않는 DDoS 공격에 대처하는 방법은 생각만큼 어렵지 않을 뿐만 아니라 많은 방어 방법들이 이미 제안되어 있다. 그러나 대부분의 DDoS 공격방법들은 공격패킷의 여러 필드를 임의로 변경하는 방법들을 공격패킷의 여러 필드를 임의로 변경하는 방법을 사용한다. 로컬라우터 상에서 평상시의 트래픽과 DDoS 공격트래픽의 차이점을 분석함으로서 DDoS 공격을 효율적으로 찾아내고 방어할 수 있다. 바꿔 말하면 방어하고자 하는 시스템의 트래픽의 특징을 분석하지 않고 DDoS 공격을 효과적으로 방어한다는 것은 불가능하다.

2.3.2 Router resource 점검

라우터 내부의 CPU를 주기적으로 점검함으로서, 장비의 현재 상태를 파악하는 것을 장애 대처에 앞서 매우 중요하다. 또한, Router와 외부구간 또한 내부구간의 사용률을 점검함으로써 DoS 공격이나 Spoofing공격을 예측 할 수도 있다.

2.4 DDoS 공격의 특징

DDoS 공격은 공격자가 일반 사용자들의 PC에 악성코드를 심어 감염시킨 후 감염 된 PC를 이용하여 특정 웹 사이트나 서버에 대량의 트래픽을 송신하는 공격방법으로서 공격자가 감염자의 PC를 이용하기 때문에 공격자 스스로가 외부에 노출되지 않으면서도 대량의 데이터를 보낼 수 있다는 특징이 있다. 현재에 들어서는 C&C(Command and Control)서버 등을 이용하여 손쉽게 공격대상을 변경 가능하고 공격 방식 또한 여러 가지 형태로 바꾸는 현태로 계속적으로 진화해 나가고 있다.

- DDoS 공격 시간의 다변화
- 공격 시작 시간은 알 수 있고 종료 시간이 없음
- 공격 타겟들의 조정이 발생
- 악성코드 제작자의 전략 변화 및 기능 강화
- DDoS 악성코드 파일들이 더욱 유기적이면서 독립적인 면을 함께 갖춤

2.4.1 UDP/ICMP Flood 공격

UDP/ICMP Flooding형태의 공격기법이 있는데, UDP Flood, ICMP Flood 공격과 같은 경우 두 가지 방법으로 나누어 정상적인 방식과 비정상적인 방식의 트래픽 간 차이를 분석하여 적절한 대응을 하는 것이 DDoS를 방어하는 주요점이 된다.[4][6]

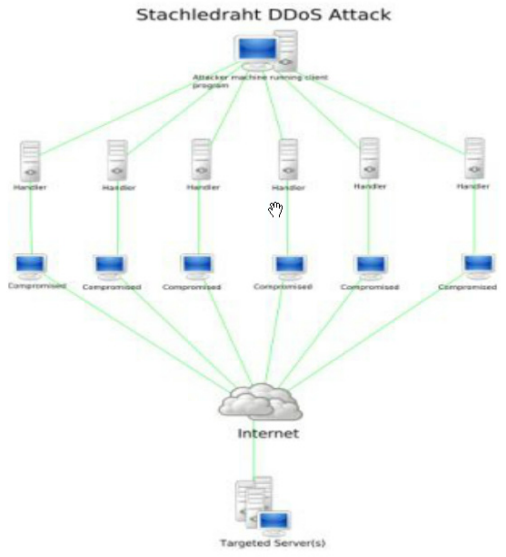
〈Table 1〉 Attack Pattern with ICMP

Field / Attack Tools	Type	Code	ID	DATA
TFN	0	0	456	
TFN	0	0	666	
stachledraht	0	0	667	ficken
stachledraht	0	0	1000	gesundheit
stachledraht	0	0	666	skillz
stachledraht	0	0	9015	niggahbitch
stachledraht	0	0	6666	skillz
stachledraht	0	0	6667	ficken

〈Table 2〉 Attack Pattern with UDP

Field / Attack Tools	Departure Port	Destination Port	DATA
trin00	-	31335	144
trin00	-	31335	Hello
mstream	-	27444	144adsl
mstream	-	6838	newserver
mstream	-	10498	stream
mstream	-	10498	ping
mstream	-	10498	pong
stachledraht	0	0	6667

위 표와 같이 일반적으로 UDP Flood, ICMP Flood공격을 수행할 때, 단일 좀비 PC에서 발생시키는 패킷은 그 크기가 다양하며 전송 간격 또한 다양화 하게 된다. 하지만 Firewall로 모든 패킷이 집중되어 단일 시간에 대량의 패킷이 모이게 될 수 없다. 이때 네트워크의 구조에 따라 어떠한 위치의 Firewall의 임계치를 설정할 것인가가 중요한 쟁점으로 대두됩니다. 망 외부에서 발생하는 DDoS의 경우 보통 기관 또는 기업 전체의 최상의 라우터의 Firewall에서 임계치를 설정하는 경우가 많은데, 이때 모든 네트워크의 Bandwidht가 DDoS로 인하여 소모되는 경우가 발생할 수 도 있다. 이를 막기 위해서 보호해야 하는 장비의 첫 번째 라우터에 연결된 Firewall의 임계치 기능을 설정해야 한다. 이럴 경우 DDoS로 인하여 해당 네트워크 전체의 Bandwidth가 소모되는 것을 막고 위급한 경우 해당 망을 다른 경로로 우회하여 보호할 수 있게 된다.



[Fig. 1] DDoS attack flows

또한 위 그림과 같이 특정 Firewall에서 대량의 이벤트 및 임계치 항목이 증가할 경우 타겟이 되는 서버에 대한 빠른 확인이 가능하며 순간적으로 대량의 공격이 발생하기 때문에 실제 보안관제시 빈도분석 기법을 통하여 보다 효율적인 관제가 가능하다.

2.4.2 Cache-Control Attack

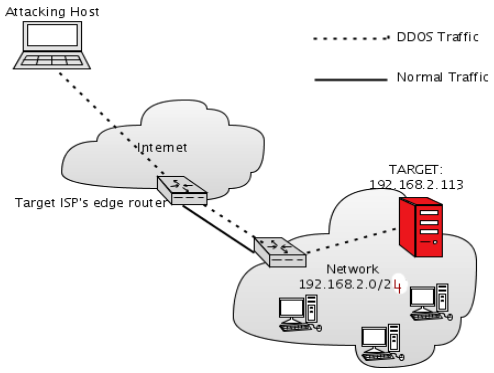
CC(Cache-Control Attack)은 HTTP User-Agent 헤더에 불필요한 값을 추가하여 웹서버의 오동작을 발생시킵니다. 수백에서 수천 개의 좀비 PC가 1분에 300~400 개의 Syn패킷을 보내며, 일정 시간을 공격하다가 쉬고 다시 공격하는 양상을 보이게 된다. 이때 보안장비를 통하여 실시간 방어하지 않는다면 짧은 시간 안에 웹서버의 자원이 소모되어 서비스가 중단되는 사태가 발생할 수 있습니다. 이를 방어하기 위해서는 Firewall등 낮은 Layer의 장비에서는 차단이 불가능하며 Application Layer의 장비가 필요하게 되며, 보통 IDS/IPS의 Signature Pattern에 특정 조건을 추가함으로서 모니터링 및 방어가 가능하다. 이때 오탐 가능성을 염두에 두고 모니터링 시에 건수 등 빈도 분석기법을 사용하여 정확도를 높이고 일반적인 상황에서의 오탐을 배재하도록 하여야한다 [7].

2.5 DDoS의 효과적인 관제 및 대응방안

DDoS 공격은 대부분 특정한 타겟을 정하고 이에 대해 집중적인 공격을 가하게 된다. 이를 효과적으로 방어하기 위해서는 기관이나 기업담당자 뿐만이 아니라 네트워크 단에서의 상호 협조가 필요하다. 또한 공격을 방어하는 것이 아닌 공격이 시작되기 전에 좀비 PC가 되는 것을 방지하는 것 또한 DDoS에 대한 효율적인 관제 및 방어 방법이 될 수 있다 [3].

2.5.1 DNS-Sinkhole

대부분의 좀비 PC가 C&C서버로부터 공격에 대한 지령을 받는다는 점에 착안하여 C&C와의 접속을 DNS단에서 가로채어 공격 지령이나 추가 악성코드 다운로드



[Fig. 2] DNS-Sinkhole Structure

등 2차 피해를 막아주는 역할을 한다. DNS-Sinkhole은 좀비 PC가 도메인을 통하여 C&C서버로 접속하려고 시도 할 때, DNS단에서 DNS-Query를 변경하여 정상적인 C&C서버 IP가 아닌 DNS-Sinkhole서버 IP를 알려주어 좀비 PC가 C&C서버로 접속하는 것을 차단한다. 기존의 라우터 기반 Sinkhole과는 달리 지속적으로 IP가 변하는 도메인 C&C에 대해 매우 효과적인 방법으로 DNS단에서 단지 특정 IP로 응답하는 것이기 때문에 DNS단에서의 부하도 적고 또한 모니터링이 매우 쉽다 특정 Sinkhole 서버로 유입되는 모든 트래픽은 악성트래픽으로 접속하는 모든 IP는 좀비 PC로 판단되기 때문이다.

또한 위 그림과 같이 Sinkhole서버는 고정되어 있기 때문에 해당 서버에 대한 모니터링 및 관리가 쉽다는 장점이 있으며 DNS단에서 악성도메인 리스트를 보유하고 질의 변경만 해주면 되기 때문에 DNS를 사용하는 모든 PC가 이러한 기능들을 사용할 수 있기 때문에 적은 비용으로도 비싼 DDoS 방어 장비를 사용하지 않아도 원천적으로 DDoS 공격 자체를 차단 할 수 있다. [3][5]

2.6 매칭기법을 적용한 DDoS 효과적인 탐지 방법

DDoS 탐지 방법은 기존에는 공격을 탐지하기 위해 일정 기간의 트래픽을 수집하여 평균을 내어 평균값을 기준으로 임계값을 설정한다. 이로 인해 임계값에 도달하기 전의 트래픽에 대해서는 공격이어도 정상으로 판정하거나 혹은 임계값을 넘었을 때 공격과 유사한 정상 트래픽도 공격으로 간주하는 오탐율이 많이 존재한다. 탐지 방법은 임계값을 고려하는 통계적인 방법과 공격 트래픽의 특성을 패턴으로 가지고 있어 두 조건의 관계를 이용하여 공격 및 정상으로 판정하는 방법이다.[1]

3. 제안하는 DDoS 탐지 알고리즘

DDoS 공격에 대한 분석을 토대로 본 연구에서는 이중 탐지 기법을 이용한 DDoS 공격탐지의 전반적인 흐름은 먼저 트래픽 수집 시에 모든 트래픽을 수집하지 않고 동일한 트래픽이 반복적으로 유입되는 DDoS의 특성을 고려하여 시간딜레이를 두고 트래픽을 샘플링하는 방법을 제안한다. 샘플링 된 데이터들 중 필요한 감사 자료만을 추출하여 이중 링크 리스트구조에 저장하고 저장된 데이터는 지속적으로 통계 값을 산출하며 적용하게 된다. 그리고 저장된 데이터를 기준으로 하여 통계적 기법과 패턴 매칭 기법을 적용하게 된다. 통계적인 기법은 네트워크에서 수집된 트래픽에 평균과 표준 편차를 산출하여 임계값을 구하여 탐지에 적용하는 방법을 말하고 패턴 매칭 기법은 DDoS 공격을 탐지할 때 가장 큰 관건이 오탐율을 줄이는 것 이다 [8,9]. 본 연구에는 패턴을 분석함으로써 DDoS 공격과 정상적인 접근을 구분하였다.

Fig. 3은 제안하는 DDoS 알고리즘의 pseudo code로 정상적인 패턴과 비정상적인 패턴을 분석하여 DDoS 공격시와 정상적인 접근을 분리하여 다루었다.

```
If network (bandwidth>normal bandwidth)
  consumption is more
  DDOS attack happens -> goto 1:
Else
  No DDOS attack -> allow access to server or
internal network
1:Then check for packet Time to Live parameters
  Set A [] as attack packets (IP)
  Set L [] as legitimate packets (IP)

  If there are different values for an IP
  {
    add that IP to A[]
  }
  if the no. of packets in a given time interval is more
  for an IP
  {
    add that IP to A[]
  }
  if there are varying port numbers for an IP
  {
    add that IP to A[]
  }
```

[Fig. 3] Proposed DDoS Pseudocode

제안하는 DDoS 알고리즘은 기존의 시그니처와 달리 패턴을 분석하여 차단하는 방식은 Fig. 3에서와 같이 정상적인 밴드윗보다 더 트래픽 양이 증가하면, 자동으로 DDoS 공격으로 보고 판단하는 프로세스가 진행된다. 갑자기 트래픽이 증가하면, 특정IP로부터 들어온 패킷을 A라는 임시 저장소에 보관하고, 정상적인 패킷은 L이라는 저장소를 통해서 내부 네트워크로 접근 가능하도록 허가한다. TTL(Time To Live)값을 분석하여 정상적인 값과 상이한 패킷과, 일정시간 동안 과도한 packet 수가 감지되었을때의 패킷, 그리고 마지막으로 상이한 port number를 이용하는 패킷들은 모두 DDoS 공격으로 보고 attack 저장소인 A에 저장하여 내부로의 접근을 막으므로써 DDoS 공격을 차단할 수 있다.

4. 결론

인터넷의 빠른 발전으로 인하여 해킹 툴이 고도화되어 쉽게 전파되고, 시스템의 보안 취약점이 인터넷으로 빠르게 공개되고 있으며, 다양한 기능의 악성코드가 유포되는 시간의 짧아지고 있다. 이러한 빠른 변화는 공격자의 침해 발생 후에 대응하는 서비스만으로는 침해사고의 영향을 최소화하는데 어려움을 가지고 있으며, 사전 침해 사고 활동의 중요성을 부각시키기고 있다. 국내에서는 시그니처 기반의 악성코드 경유/유포지 탐지기술이 개발되었으나 대량의 신종 악성코드 탐지 어려움에 있어, 최근 악성코드는 분석도구 회피, 실행정보 은닉 등 다양한 지능화된 기능이 적용됨에 따라, 행위기반 동적 분석 기술이 필요하며 융복합 단말에서 개인정보 유출 방지 등 일부 보안 기술이 개발되었고 있다. 최근 등장한 FMC 서비스에서의 보안기술이 발전하고 사이버 공격기술이 다양화 및 급 발전 되어가고 있을 뿐만 아니라, 일부 국가에서는 적대국가의 국가 기밀 절취나 사회적 교란을 목적으로 국가적인 차원에서 조직적으로 사이버 공격을 감행하는 정보전의 양상을 띠고 있어 국가정보통신망에 대한 보호대책이 그 어느 때 보다도 중요성을 더하게 되었다. 현재 보유한 보안 시스템만으로 DDoS 공격을 효율적이고 빠른 대응이 가능하도록 하기 위해서는 공격 패턴을 분석하여 특정 패턴이 탐색될 때마다 특정 지역과 특정 시간대를 분석하여 IP 별로 차단하는 것이 가장 효과적일 것으로 판단한다. 따라서 단순히 트래픽이 가중된다고 차단하는 것이 아니라 행동을 분석하여 이상징후를 등록하여 패턴 매치가 완전히 일어 날 때 방화벽에서 접근 통제를 하면 지능화되고 있는 DDoS 공격을 막을 수 있을 것으로 기대하며, 앞으로 DDoS 공격 방ㅇ어 알고리즘을 지속적으로 개발하여 서로의 결과 값을 비교 분석은 향후에 진행할 예정이다.

REFERENCES

[1] Michael O'neil, "Unix System in a Large Enterprise Environment-Axent Esm", SANS Institute Information Security Reading Room, June 22, 2001.

[2] Mara C. FERNANDEZ, Ernestina MENASALVAS, Oscar MARBAN, Jose MM PENA, Socorro MILLAN, "MINIMAL DECISION RULES BASED ON THE APRIORI ALGORITHM", Int. J. Appl. Math Computer. Sci Vol.11, No.3, pp. 681-704, 2001.

[3] W.ahn, "EAR: An Energy-Aware Block Reallocation Framework for Energy Efficiency", Proc. of ICCS - LNCS 4490, pp. 941-948, 2007.

[4] R. Chandramouli, S. Bapatla, and K. Subbalakshmi, "Battery Power-Aware Encryption", ACM Tr. Info and System Security, Vol 9 No. 2 pp. 162-180, 2006.

[5] P. Prasithsanaree and P. Krishnamurthy, "on a Framework for Energy-Efficient Security Protocols in Wireless Networks", Computer Communcations, Vol. 27, pp. 1716-1729, 2004.

[6] W. Zeng, H. Yu, and C. Lin, Multimedia Security Technologies for Digital Rights Management, Academic Press, 2006.

[7] T. Maples and G. Spanos, "Performance Study of Selective Encryption Scheme for the Security of Networked Real-Time Video", Proc. of ICCCN, pp. 2-10, 1995.

[8] F. Liu and H. Koenig. "A Novel Encryption Algorithm for High Resolution Video", Proc. of NOSSDAV, pp. 69-74, 2005.

[9] B. Bhargava, C. Shi, and S. Wang, "MPEG Video Encryption Algorithms", Multimedia Tools and Applications, Vol. 24, pp. 57-79, 2004.

홍 성 혁 (Hong, Sunghyuck)

・1995년 2월 : 명지대학교 컴퓨터공학과 (공학사)
・2007년 8월 : Texas Tech University, Computer Science (공학박사)
・2012년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
・관심분야 : 네트워크 보안, 해킹, 센서네트워크 보안
・E-Mail : shong@bu.ac.kr