6LoWPAN 상에서의 Botnet 분석 및 탐지 메커니즘

조응준*, 홍충선**
경희대학교 컴퓨터공학과
e-mail : *ejcho@networking.khu.ac.kr, **cshong@khu.ac.kr

Analysis and Detection Mechanism of Botnet on 6LoWPAN

Eung Jun Cho, Choong Seon Hong
Dept. of Computer Engineering, Kyung Hee University

요 약

최근 들어 스팸 메일, 키 로깅, DDoS와 같은 공격에 Botnet이 사용되고 있다. Botnet은 크래커에 의해 명령, 제어되는 Bot에 감염된 클라이언트로 이루어진 네트워크이다. 지금까지 유선망의 Botnet을 탐지하기 위한 많은 기법이 제안되었지만, 현재 많은 개발이 이루어지고 있는 6LoWPAN과 같은 무선 센서 네트워크상의 Botnet에 관한 연구와 그 대처방안은 전무한 상태이다. 본 논문에서는 6LoWPAN 환경에서 Botnet이 얼마나 위험할 수 있는지 살펴보고 이를 탐지하기 위한 메커니즘을 제안하고자 한다.

1. 서론

컴퓨터 기술의 발전과 함께 컴퓨터를 이용한 크래커의 공격 유형도 다양해지고 있다. 과거 사용자나 관리자에게 해를 끼치지 않는 범위의 해킹이 이루어졌다. 하지만 최근에는 사용자의 시스템에 피해를 끼치는 바이러스의 형태로 발전 하였다. 그 후 공격의 형태는 더욱 진화하여 네트워크 자체를 공격하는 웜이 등장하였다. 2003년 1월 25일, 국내에서 발생했던 슬래머 웜에 의한 공격이 그 예로, MS-SQL의 취약점을 공격, 당월26일 오전까지 우리나라의 네트워크가 마비되는 사태가 일어났었다. 그리고 최근에는 Botnet [1] 을 이용하여 인터넷 쇼핑몰이나 기타 상업 사이트를 공격하여 해당 사이트를 마비시킨 뒤 공격을 중단하는 대가로 돈을 요구하는 범죄도 발생하고 있다.

앞의 공격 패러다임의 변화를 살펴 볼 때 새로운 기술의 등장에 따라 그에 상응하는 새로운 유형의 공격들이 등장할 것이다. 본 논문에서는 현재 활발히 연구되고 개발 중인 6LoWPAN(IPv6 over Low power WPAN) [2]상에 보안 분야에서 큰 이슈가 되고 있는 Botnet이 어떻게 사용될 수 있는지 분석하고 그것을 탐지하기 위한 메커니즘을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 설명하고 3장에서는 6LoWPAN상에서 가능한 Botnet의 공격 형태를, 4장에서는 6LoWPAN 상의 Botnet 탐지 메커니즘을 제안한다. 그리고 5장에서 결론 및 앞으로 필요한 연구를 설명한다.

본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2009-(C1090-0902-0016))

2. 관련 연구

2.1 6LoWPAN

6LoWPAN은 한정된 전력과 적은 처리량이 요구되는 어플리케이션들에게 무선연결환경을 제공하는 단순하고 간단한 저가형 통신 네트워크이다. 특히 센서 네트워크에 적합하며 IEEE 802.15.4[3]를 PHY/MAC으로 하는 저전력 WPAN 상에 IPv6를 탑재하기 위한 기술이다.

2.2 Botnet

Botnet은 다수의 Zombie 클라이언트인 Bot [1]에게 크래커가 명령을 내려 특정 사이트를 공격하거나 대량의 스팸메일을 발송하는 네트워크 시스템이다. 특히 Botnet은 DDoS(Distributed Denial of Service) 공격에 적합한 형태의 네트워크로 DDoS 공격은 탐지가 되어도 차단시키는 것은 매우 어려웠다. 초기 Botnet은 C&C(Command & Control)서버로 IRC(Internet Relay Chat)를 사용하였다. 크래커가 자신의 채널을 열어 Bot이 접속을 하면 명령을 전달하는 방식이다. 그 후, Botnet은 웹 서버를 사용한 방식으로 발전하였고 최근에는 P2P [4][5]와 Hybrid P2P [6] 방식을 사용하는 Botnet도 발견되고 있다.

3. 제안하는 메커니즘

현재까지 C&C 서버 유형의 Botnet 탐지를 위한 많은 메커니즘이 제안되었다. Botnet의 집단행동을 기반으로 DNS sinkhole [7] 기법을 적용하여 Botnet을 탐지하여 제거하는 기법도 그 중의 하나이다. 그러나 이러한 탐지 메커니즘은 P2P 방식의 Botnet에 취약하다. 그리고 6LoWPAN과 같은 센서 네트워크 상에 Botnet이 형성되었을 경우에 그에 적합한 대처법의 연구는 전무한 상태이

다. 따라서 본 논문에서 6LoWPAN상의 Botnet 유형과 탐지 메커니즘을 제안하고자 한다.

3.1 6LoWPAN상에서의 Botnet 의 공격 형태

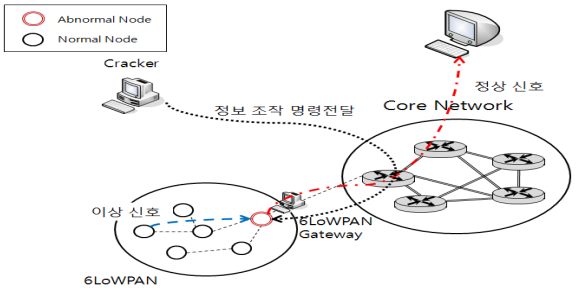
본 절에서는 6LoWPAN상에서 가능한 Botnet의 유형과 그 공격 형태를 소개한다. 6LoWPAN은 유선IP망과 다음과 같은 차이점이 있다.

첫째, 대역폭의 차이이다. 유선IP 망이 10Mbps~ 1Gbps의 대역폭을 제공하는데 반해 6LoWPAN은 단지 250Kbps의 대역폭만을 제공한다. 대역폭의 제한으로 6LoWPAN상의 Botnet은 공격 형태도 달라져야 한다.

둘째, 6LoWPAN의 가장 큰 특징 중 하나는 센서 노드 자체가 패킷을 전달하는 노드 역할을 하는 것이다. 보통 하나의 6LoWPAN은 많은 수의 센서 노드들로 구성되어 있어, 센서 노드들을 기존 IP 무선망처럼 AP 만으로 연결하는 것에는 한계가 있다. 그래서 통신 가능 지역을 늘리고 AP같은 시설 투자비용을 줄이기 위해 각각의 센서 노드는 end-point역할 뿐만 아니라 다른 센서 노드의 패킷을 목적지로 전달해주는 역할도 한다.

셋째, 센서 노드가 사용되는 장소의 차이이다. 기존 컴퓨터와는 다르게 센서 노드는 핵 누출 탐지, 기상 정보 관측, 사용자 위치 추적, 실시간 건강관리 등 그 활용분야가 무한하다고 할 수 있다. 진정한 유비쿼터스 환경 구축에 가장 적합한 기술로 인정받고 있는 것도 이러한 이유에서다.

위와 같은 특징으로 6LoWPAN의 환경에서 DDoS같이 대량의 트래픽이 필요한 공격은 적합하지가 않다. 즉, 센서 노드의 낮은 연산능력과 전송률로 인하여 DDoS 공격을 수행하기위해서는 유선망의 클라이언트보다 훨씬 더 많은 수의 센서 노드가 필요하다. 그러나 많은 수의 센서 노드를 확보 하더라도 제한된 배터리로 공격을 지속적으로 수행할 수 없다. 반면에 Bot에 감염된 센서 노드를 이용하여 특정 패킷의 정보를 조작하는 식의 공격이 가능하다.



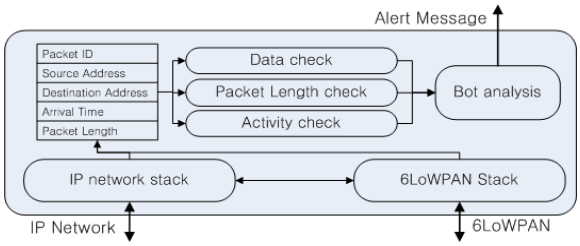
(그림 1) 6LoWPAN상의 Bot

그림 1은 6LoWPAN상의 Bot의 예로, 데이터 조작을 통해 시스템에 피해를 주는 예이다.

이런 공격 외에도 기존 무선 센서네트워크에서 존재하던 Sinkhole attack [8]과 같은 공격에 Botnet이 사용되어 크래커가 임의로 제어가 가능한 Sinkhole attack 같은 유형의 공격이 나타날 수도 있다.

3.2 6LoWPAN상의 Botnet 탐지

6LoWPAN상의 Botnet을 탐지하기 위해서 우선 6LoWPAN의 구조를 알아야 한다. 6LoWPAN은 여러 개의 센서 노드와 그 노드들을 외부로 연결 시켜 주는 6LoWPAN 게이트웨이로 구성되어 있다. 일반적으로 하나의 6LoWPAN의 센서 노드들은 같은 기능을 수행 할 가능성이 높다. 이런 특징을 바탕으로 본 논문에서는 bot이 탑재된 노드의 유무를 탐지하는 법을 제안한다. 그림 2는 게이트웨이에 탑재될 Bot 탐지 모듈이다.



(그림 2) Bot 탐지를 위한 게이트웨이의 모듈

우선 정보 분석을 위해 게이트웨이를 지나는 패킷으로부터 표 1의 정보를 별도로 저장한다.

<표 1> 트래픽 분석에 사용되는 정보

항목	설명
Packet ID	패킷 고유 번호
Address$_s$	출발지 주소와 포트 번호
Address$_d$	목적지 주소와 포트 번호
Arrival Time	패킷 도착 시간
Packet Length	패킷 길이

Data check 모듈은 패킷으로 전달되는 정보를 게이트웨이에서 해석이 가능한지 검사한다. Botnet 유지에 사용되는 데이터 패킷의 경우 게이트웨이에서 해석이 불가능한 데이터일 가능성이 높기 때문이다. 그림 3은 Data check 모듈의 동작 코드이다.

```
if(Data is not match with OPCode or data)
{    if(address_s == address of sensor node)
         address = address_s
     else if(address_d == address of sensor node)
         address = address_d
     Record( address, Arrival time, Data check
     flag) into Data analysis DB    }
```

(그림 3) Data check 모듈 동작 코드

Activity check 모듈은 노드가 스스로 얼마나 많은 통신을 시도하는지 분석한다. Bot에 감염된 노드는 Botnet 유지와 크래커와의 통신을 위해 자신의 위치와 상태를 주기적으로 보고를 해야 한다. 이런 특징을 바탕으로 다른 센서 노드보다 외부 통신을 더 빈번하게 하는 노드의 유무를 탐지한다. 그림 4는 Activity check 모듈의 동작 코드이다.

```
if(Address_s == address of sensor node && address_d != list of stored packet)
{   Record(address_s, Arrival time, Activity check flag) into Data analysis DB   }
```

(그림 4) Activity check 모듈의 동작 코드

Packet Length check 모듈은 통신 시 노드에서 보내는 데이터 길이의 평균을 분석한다. 앞에서 언급하였듯이 같은 네트워크 내의 센서 노드들은 비슷한 역할을 수행하기 때문에 주고받는 데이터의 길이도 비슷하게 된다. 그러나 Bot에 감염된 노드의 경우 센싱 정보 외에도 Botnet 유지를 위한 정보와 크래커로부터 명령을 전달 받아야 하므로 이 차이를 통해 Bot의 유무를 탐지한다. 그림 5는 Packet Length check 모듈의 동작 코드이다.

```
if(Address_s == address of sensor node )
{   Record(address_s, Arrival time, Packet length check flag) into Data analysis DB   }
```

(그림 5) Packet Length check 모듈의 동작 코드

Bot analysis모듈은 세 모듈로부터 받은 정보를 바탕으로 다른 노드들과 값이 상이하게 다른 노드의 유무를 검사한다. 검사 결과 이상이 발견되면 관리자에게 경고 메시지를 발생하여 Bot이 존재함을 알리게 된다. 그림 6은 Bot analysis 모듈의 동작 코드이다.

```
for(i=0; i<number of stored node address; i++)
{   if(node_i > average of other node + t)
    make alert signal   }//t : threshold
```

(그림 6) Bot analysis 모듈의 동작 코드

5. 평가

제안된 메커니즘은 bot의 행위를 분석하여 유무를 판단하는 기법으로 다음과 같은 장점이 있다. 첫째, 행위 기반 탐지 메커니즘으로 어떠한 유형의 bot에도 대응이 가능하다. 둘째, bot과 정상 노드의 상대적인 차이를 판별하여 탐지하기 때문에 다른 기능을 가진 여러 6LoWPAN 환경에도 같은 메커니즘을 수정 없이 사용 가능하다. 그리고 미탐 및 오탐의 경우 반복적인 실험을 통해 임계치값과 Bot analysis 모듈에서 최소한의 평균치를 구하는 시간을 조절하여 줄일 수 있을 것이다.

6. 결론 및 향후 과제

본 논문에서는 6LoWPAN에서 발생 가능한 Botnet의 유형과 그 탐지 메커니즘을 설명하고 제안하였다. 본 논문에서 제안한 Botnet 탐지 메커니즘은 Bot에 감염된 노드의 행동방식이 다른 정상 노드와 다를 것이라는 점과 같은 네트워크 내의 센서 노드들은 비슷한 작업을 할 것이라는 점을 가정하고 있다. 그러나 Bot의 숫자가 많아질 경우와 하나의 6LoWPAN이 많은 종류의 작업을 하게 될 경우를 고려할 필요성이 있다. 그리고 무엇보다 6LoWPAN 내부의 센서 노드 숫자가 천 단위 이상으로 커질 경우 게이트웨이에서 패킷을 일일이 분석하게 되면 게이트웨이의 부하가 커져 성능저하가 발생할 것이다. 따라서 6LoWPAN의 규모가 커지고 동시에 많은 종류의 서비스를 지원하며 네트워크 내에 다수의 Bot이 존재 할 경우, 이를 게이트웨이에서 어떻게 효율적으로 분석하고 탐지 할지에 대한 연구가 필요하다. 그리고 Bot analysis 모듈에서 어느 정도의 데이터를 축적시켜야 오탐율과 미탐율이 낮아지고 정확성을 높일 수 있는지, 그리고 어떠한 통계적 기법을 사용하는 것이 효율적인지 실험을 통해 검증해야 할 것이다.

참고문헌

[1] Ramneek Puri, “Bots & Botnet: An Overview”, August, 2003

[2] N. Kushalnagar, G. Montenegro, and C. Schumacher, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, IETF RFC 4919, Aug. 2007

[3] IEEE Computer Society, “IEEE Std. 802.15.4-2003,” Oct. 2003.

[4] Thorsten Holz, Moritz Steiner, Frederic Dahl, Ernst Biersack, Felix Freiling, “Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm”, April, 2008

[5] Elizabeth Van Ruitenbeek and William H. Sanders, "Modeling Peer-to-Peer Botnets", Quantitative Evaluation of Systems, 2008. QEST '08. Fifth International Conference on, Sept, 2008

[6] Ping Wang, Sherri Sparks, Cliff C. Zou, “An Advanced Hybrid Peer-to-Peer Botnet”, Dependable and Secure Computing, IEEE Transactions on, 2003

[7] Hyunsang Choi; Hanwoo Lee; Heejo Lee; Hyogon Kim "Botnet Detection by Monitoring Group Activities in DNS Traffic", Computer and Information Technology, 2007. 7th IEEE International Conference on, Oct. 2007

[8] Edith C. H. Ngai, Jiangchuan Liu, Michael R. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks", ICC 2006, Proceedings of the IEEE International Conference on Communications, 2006