IoT 환경에서 유무선 DDoS 공격 영향 분석

최진태, 김경백

전남대학교 전자컴퓨터공학부

jefron1100@gmail.com, kyungbaekkim@jnu.ac.kr

Analysis of wireless and wired DDoS Attack under IoT environment

Jintae Choi, Kyungbaek Kim

Dept. Electronics and Computer Engineering, Chonnam National University

요 약

최근 IoT 디바이스가 보편화 되면서 그 수가 빠르게 증가하고 있으며, 인간의 삶에 더욱 밀접한 IoT 기기들이 등장하고 있다. 이러한 IoT 디바이스들은 유선으로 네트워크에 연결되기도 하지만 대부분 무선으로 연결된다. 이에 따라 유, 무선으로 구성된 IoT 네트워크에 DDoS 공격이 가해졌을 경우, IoT 디바이스들의 통신에 미치는 영향에 대해 실험하고 분석한다. 이러한 분석을 통해, 무선 IoT 디바이스와 무선 채널에 대한 공격이 유선 IoT 디바이스보다 DDoS 공격에 더 큰 영향을 받음을 보이고, 무선 IoT 디바이스를 위해 네트워크 단에서 DDoS 공격 탐지 및 방어 대한 연구의 필요성을 제안한다.

Ⅰ. 서 론

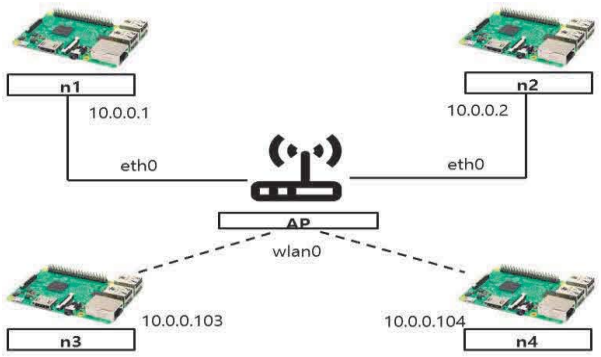
최근 IoT 디바이스가 보편화 되면서 그 수가 빠르게 증가하고 있다. IT 분야의 리서치 기업 가트너는 2014년 64억 개의 IoT 디바이스가 2020년에는 135억 개에 달할 것으로 추측한다. 더불어 2014년을 기준으로 2015년에는 IoT 디바이스의 사용률이 30% 증가했다.[2][3] IoT 디바이스의 증가와 함께 IoT 디바이스의 영역도 점차 늘어나 카메라, 난방기기, 냉장고자동차와 같이 인간의 삶에 밀접한 기기들도 IoT 디바이스의 영역에 포함 될 것이다.[4] 이러한 IoT 기기들은 주로 각 가정 및 회사, 학교, 병원 등에서 유, 무선으로 AP에 연결되어 통신하는데, IoT 환경에서는 특히 무선 환경을 사용한다. 이에 따라 한 AP와 연결된 IoT 디바이스가 DDoS공격을 받을 때 IoT 네트워크의 각 기기들이 어떤 영향을 받는지에 대한 연구가 필요하다.

Ⅱ. 본론

본 논문에서는 한 AP에 유선 또는 무선으로 연결된 IoT 디바이스에 DDoS 공격이 가해질 경우, IoT 디바이스 사이의 Ping RTT를 관찰한다. 이를 통해, DDoS 공격이 유, 무선으로 연결된 IoT기기에 미치는 영향을 분석한다. 분석을 위해 먼저 실험 환경을 구축하고, 각 공격 상황에 대한 IoT 디바이스의 Ping RTT 결과를 통해 IoT 네트워크 환경의 디바이스들이 DDoS 공격에 어떤 영향을 받는지 분석한다.

1. 유무선 IoT 게이트웨이 실험 환경 구축

DDoS 공격이 유, 무선으로 연결된 IoT 디바이스에 미치는 영향을 실험하기 위해서 그림 1과 같은 실험 환경을 구축하였다. IoT 게이트웨이 AP로는 상용으로 사용하고 있는 TP-LINK TL-WR9400N plus 모델을 사용하였고, 4개의 각 노드는 Raspberry Pi 3 Model에 Raspbian 운영체제를 설치하여 사용하였다. 노드 n1과 n2는 유선으로 AP에 연결하였고, 노드 n3, n4는 무선으로 AP에 연결하였다.



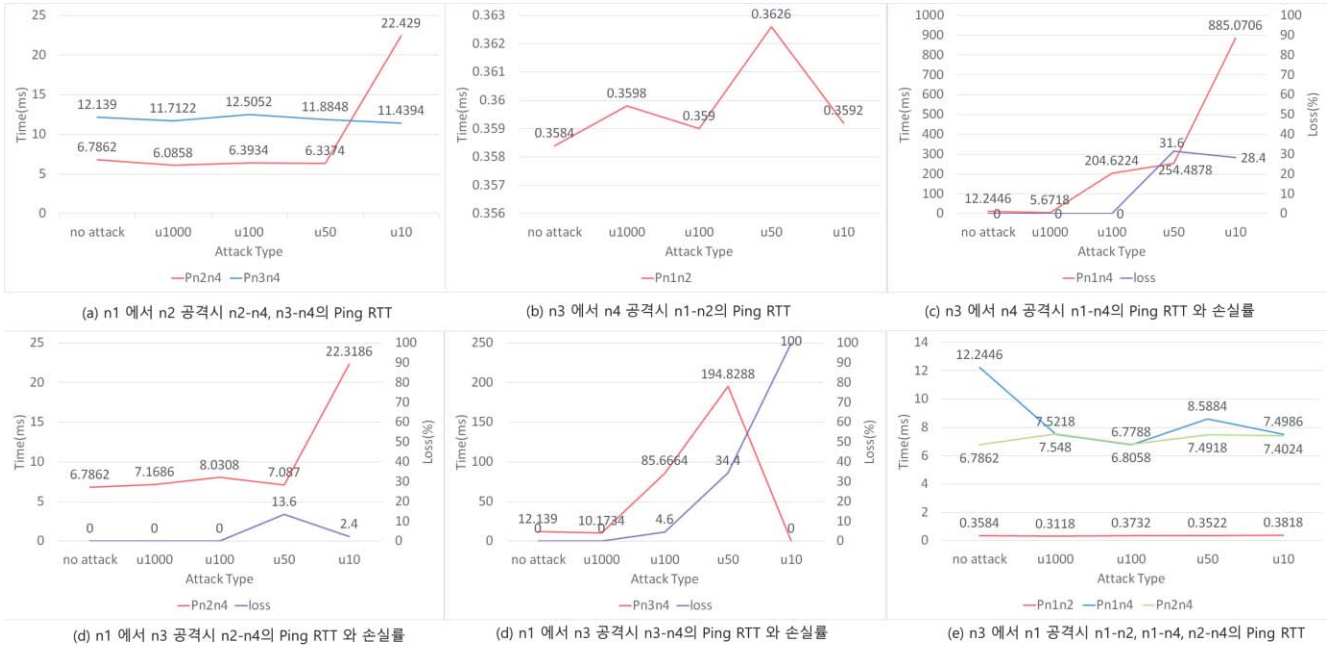
[그림 1] 유무선 IoT 게이트웨이 실험 환경

2. 실험 측정 방법

그림 1과 같은 실험환경에서 유선에서 유선 공격, 무선에서 무선 공격, 유선에서 무선 공격, 무선에서 유선 공격에 대한 각 IoT 디바이스들의 통신 상태를 비교한다. DDoS 공격은 n1과 n3에 설치된 hping3 DDoS 공격 툴을 사용한다. ICMP Flooding 공격을 수행하며, 공격속도를 u1000(100 packets for second), u100(1000 packets for second), u50(5000 packets for second), u10(10000 packets for second)으로 각각 다르게 하여 IoT기기의 통신 상태를 측정한다. IoT 기기의 통신 상태 측정은 1초당 1개의 Ping을 60번씩 보내어 주고받은 시간의 최솟값, 평균값, 최댓값과 손실률을 측정한다.

3. 유무선 IoT 게이트웨이 환경에서 DDoS 공격의 영향 분석

3.1 유선에서 유선 공격



[그림 2] 각 공격 상황의 실험 결과

그림 2의 그래프 (a) 유선에서 유선 공격은 n1에서 n2로 이루어진다. 이러한 유선에서 유선 공격 상황의 유선-무선의 통신 상태를 측정하기 위해 n2와 n4의 Ping RTT를 측정한 결과와 무선과 무선의 통신 상태를 측정하기 위해 n3와 n4의 Ping RTT를 측정한 결과를 보여준다. 유선-무선(n2-n4) Ping RTT의 경우 u50부터 영향을 받았으나 무선-무선(n3-n4)의 Ping RTT의 경우는 영향을 받지 않는 것으로 나타났다. 이를 통해 유선-유선 공격 환경에서 무선-무선 통신은 크게 영향을 받지 않는 것을 알 수 있다.

3.2 무선에서 무선 공격

그림 2의 그래프 (b)와 그래프 (c)의 무선에서 무선 공격은 n3에서 n4로 이루어진다. 그림 2의 그래프 (b)는 무선에서 무선 공격 상황에 유선과 유선의 통신 상태를 나타낸 그래프이며, 이를 측정하기 위해 n1와 n2의 Ping RTT를 측정하였다. 그림 2의 그래프 (c)는 무선에서 무선 공격 상황에 유선과 무선 간의 통신 상태를 나타낸 그래프이며, 측정을 위해 n1과 n4의 Ping RTT를 측정하였다. 측정결과 유선-유선(n1-n2)의 통신에는 영향이 없었지만, 유선-무선(n1-n4)통신에는 큰 영향을 끼쳤다. 특히, 공격 속도가 증가할수록 Ping의 응답속도가 느려지며, 손실률도 증가 하는 것으로 나타났다. 이에 따라 무선으로 연결된 디바이스가 공격을 받게 되면 무선에서 무선으로의 공격 효과가 매우 높게 나타나는 것을 알 수 있다.

3.3 유선에서 무선 공격

그림 2의 그래프 (d)와 그래프 (e)의 유선에서 무선 공격은 n1에서 n3로 이루어진다. 그림 2의 그래프 (d)는 유선에서 무선 공격 상황에서 유선과 무선의 통신을 측정하기 위해 n2와 n4의 Ping RTT를 측정한 그래프이고, 그림 2의 그래프 (e)는 유선에서 무선 공격 상황에 무선과 무선 간의 통신을 측정하기 위해 n3와 n4의 Ping RTT를 측정한 그래프이다. 그림 2의 그래프 (d)를 보면 유선에서 무선 공격 상황의 유선-무선 통신은 DDoS 공격에 큰 영향을 받는 것을 알 수 있다. Ping의 응답속도는 7ms에서 22ms로 증가 했으며 공격속도 u100부터는 손실률도 증가 하는 것을 볼 수 있다. 그림 2의 그래프 (e)를 보면 유선에서 무선 공격 상황의 무선-무선 통신에서는 DDoS 공격에 매우 큰 영향을 받는 것을 알 수 있다. u1000의 속도부터 Ping의 응답시간과 손실률이 증가하며, u10의 속도부터는 손실률이 100%로 통신이 불가능한 상태가 되었다.

3.4 무선에서 유선 공격

무선-유선의 공격상황에서는 유선-유선, 무선-유선의 모든 경우가 크게 영향을 받지 않는 것으로 나타났다.

Ⅲ. 결론

본 논문에서는 유, 무선 환경으로 AP와 연결된 IoT 디바이스에 DDoS 공격이 일어났을 때, IoT 기기들의 통신에 어떤 영향을 미치는지에 대한 분석을 하였다. 분석 결과 유선-유선 상의 공격은 공격받는 유선의 디바이스이외에 다른 디바이스들은 크게 영향을 받지 않는 것으로 나타났다. 하지만, 무선으로 연결된 디바이스로 DDoS 공격이 가해질 경우(무선에서 무선 공격, 유선에서 무선 공격)에는 모든 무선 디바이스들의 통신 속도가 느려지며 손실률도 매우 높아진다. 이러한 실험 결과와 분석을 통해 무선으로 이루어진 IoT 디바이스에 DDoS 공격이 가해질 경우, 그 IoT 네트워크의 디바이스들은 모두 불능이 될 수 있음을 알 수 있으며, DDoS 공격이 AP를 지나 무선으로 연결된 디바이스에 도착하기 전에 네트워크 단에서 DDoS 공격을 탐지 및 방어하는 기술에 대한 연구가 필요함을 제안한다.

ACKNOWLEDGMENT

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2017-2016-0-00314).

참 고 문 헌

[1] Yungee Lee, Wangkwang Lee, Giwon Shin1 and Kyungbaek Kim, Assessing the Impact of DoS Attacks on IoT Gateway, CUTE 2016

[2]http://news.grayhash.com/category/malware/%EB%AF%B8%EB%9D%BC%EC%9D%B4%20%EB%B4%87%EB%84%B7

[3] http://www.gartner.com/newsroom/id/3165317

[4] 현대경제연구원. 사물인터넷(IoT) 관련 유망산업 동향 및 시사점. 2016. 07. 11