CoAP을 위한 프로토콜 제안 시 DDoS 보안 고려사항

조서연, 공성현, 석병진, 이창훈†
서울과학기술대학교 컴퓨터공학과
e-mail : {joseoyeon, gongsh, sbj7534, chlee}@seoultech.ac.kr

DDoS Security Considerations When proposing a protocol for CoAP

Seoyeon Jo, Seonghyeon Gong, Byoung-jin Seok, Changhoon Lee†
Dept. of Computer Science Engineering, Seoul National University of Science and Technology

요 약

DDoS(Distributed Denial of Service) 공격은 네트워크상에서 다수의 시스템 협업으로 하나의 표적 시스템을 공격하여 서비스의 가용성을 침해하는 공격이다. 이는 점차 지능적인 방법으로 진화하고 있으며 특히 IoT를 대상으로 한 DDoS 공격이 증가하고 있다. 이기종의 기기들이 연결된 IoT는 기존 IT디바이스와 비교하여 제한된 자원을 가지고 있어 IoT 네트워크 특성을 고려한 DDoS 보안 기법이 요구된다. 국제 인터넷 표준화 기구 IETF에서 IoT를 지원하기 위해 제정한 CoAP(Constrained Application Protocol)은 기존 IT 네트워크와 호환성을 가진 응용 계층 프로토콜이다. 본 논문은 CoAP의 DDoS 공격 취약점과 대응 방안을 정리하고 새로운 프로토콜을 추가할 시 고려해야 할 사항을 제시한다.

1. 서론

사물 인터넷(IoT: Internet of Things)은 분산된 사물들이 인터넷에 연결되어 지능적인 관계를 형성하는 인프라다[1]. IoT 네트워크는 이기종 장치 네트워크가 연결되는 초연결성을 가진다[2]. LLN(Low power and Lossy Network) 환경에서 기존의 IT 보안 기술이 적용되지 않는 사물 인터넷이 IT 네트워크에 연결되면서 DDoS 공격 위협이 증가하고 있다[3].

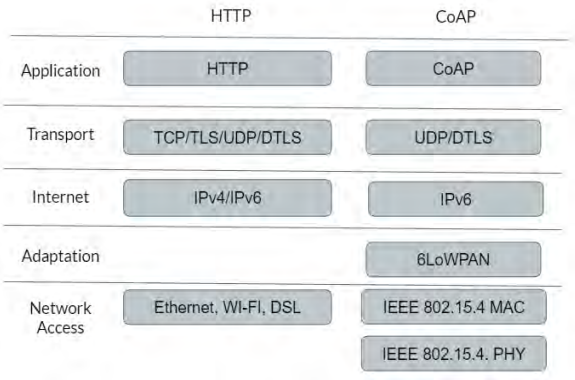
Gartner[4]는 2020년에 인터넷에 연결되는 사물 수를 250억 개로 예상한다. IoT 기기의 과잉 연결은 네트워크 트래픽의 병목 현상을 유발하기 쉬워 DDoS 공격의 주요 대상이 된다. 실제로 CoAP을 활용한 DDoS 공격 트래픽이 평균적으로 55Gbps에 달하며, 58만개의 CoAP 장치 중 33만개가 증폭 공격에 취약하다[5]. 특히 IoT 기기 중 자원이 제한된(Resource-constrained) 경량 디바이스들은 DDoS 공격에 매우 취약하며, 이를 대상으로 한 공격이 빈번히 발생하고 있다. 이에 대응하기 위해서는 자원이 제한된 운영환경과 사용되는 프로토콜을 고려한 솔루션이 필요하다. 본 논문에서는 IoT 통신을 위한 경량 프로토콜 CoAP에 대한 DDoS 공격 위협을 정리하고 CoAP의 네트워크 계층을 기준으로 DDoS 공격 위협과 보안 요구사항을 분류한다. 또한, 이를 기반으로 IoT 네트워크 프로토콜 설계 시 DDoS 공격 대응을 위한 고려사항을 제시한다.

본 논문의 2장에서는 CoAP 네트워크 계층을 기준으로 각 계층별 프로토콜 구조를 설명하고 DDoS 위협과 보안 방법의 한계를 정리한다. 또한, 3장에서는 IoT 네트워크상의 새로운 프로토콜 설계 시 DDoS 공격에 대한 저항성을 갖기 위한 고려사항을 제시한다. 마지막으로 4장에서 결론을 통해 마무리하고자 한다.

2. CoAP의 DDoS 공격과 보안

2.1 CoAP 네트워크 구조

이 장에서는 CoAP 네트워크에서 계층 간 프로토콜과 그에 따른 특징을 다룬다. CoAP은 저전력, 제한된 메모리를 가진 네트워크 및 기기를 위해 설계된 웹 전송 프로토콜이다. RFC 7252[6] 문서에는 CoAP 메시지 교환 방식이 정의되어 있다. 이에 따른 CoAP의 계층별 프로토콜 구조는 (그림 1)과 같으며 CoAP의 특징은 다음과 같다.



(그림 1) HTTP와 CoAP 프로토콜 비교[7]

† 교신저자, chlee@seoultech.ac.kr(Corresponding author)

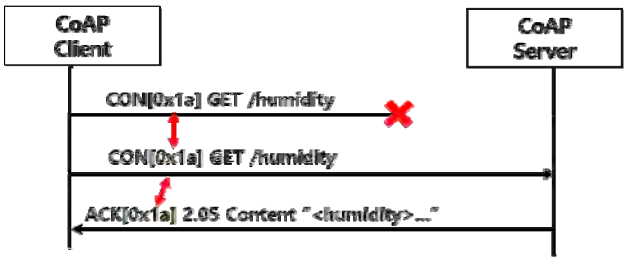
- 프록시를 통해 HTTP와 상호호환성을 가지고 요청-응답 상호작용 모델을 제공한다.
- 종단 노드는 적은 용량의 ROM, RAM이 내장된 8/16 비트 마이크로컨트롤러를 사용한다.
- HTTP와 같이 GET, PUT, POST, DELETE 메소드를 활용할 수 있으며 RESTful 상호작용이 가능하다[3].
- HTTP와 달리 UDP (Port:5683)를 사용하며 바이너리로 인코딩된다.

IEEE 802.15.4 - LLN(Low Power and Lossy Network) 환경에서 무선 개인 통신망을 위한 물리계층 표준이다. 10 미터 내의 기기들을 지원하며 CSMA/CA를 사용한다. 이 표준을 사용하는 프로토콜들은 Zigbee, NFC, Z-wave(ITU-T G.9959)가 있다[8].

IPv6 - 기기간의 직접적인 통신을 요구하는 IoT 기기에 IP를 부여하기 위해 채택되었다. IPv4 주소체계를 확장해 주소 크기를 128bit로 늘린다. 또한 IPv4 주소 체계와의 호환성을 위해 RPL(IPv6 Routing Protocol for Low-power Lossy Networks)이 사용된다[9][10].

6LoWPAN(IPv6 over Low power WPAN)[11] - 물리계층이 IEEE 802.15.4로 정의된 WPAN(Wireless Personal Area Networks) 상에 IPv6를 탑재하기 위한 프로토콜이다. IEEE 802.15.4의 MTU(Maximum Transmission Unit)는 127 Byte지만 IPv6의 MTU는 1280 Byte이다. 6LoWPAN은 이 두 프로토콜의 패킷 길이를 조절하기 위해 단편화 및 재조립 기능을 지원한다[8][11].

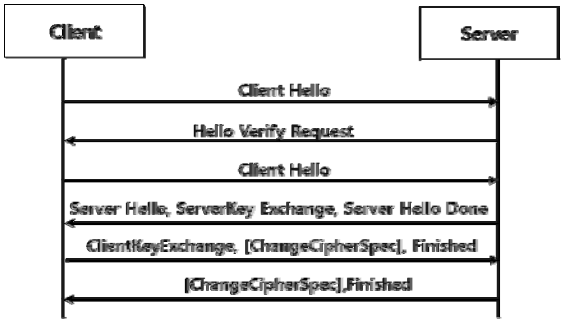
UDP - 비동기식으로 데이터그램을 전송한다. (그림 2) 와 같이 CoAP UDP는 패킷 손실 처리를 위해 CON/ACK 메시지를 이용하여 일정시간 동안 요청에 대한 응답이 없다면 요청을 재전송한다. 또한 수신측에서 중복된 데이터 인자를 구분할 수 있도록 토큰을 사용한다[12]. 만약 수신 측에서 바로 응답을 할 수 없는 경우에는 ACK 패킷만을 먼저 보낸다.



(그림 2) CoAP UDP의 패킷 손실 처리 [6]

DTLS(Datagram Transport Layer Security) - UDP를 사용하는 프로토콜의 암호화 및 전송 신뢰성을 보장하기 위해 사용한다. 만약, 패킷 암호화가 적용되지 않은 경우, 공격자는 IP주소를 위조하여 명령 패킷을 획득하고 명령 방식을 알 수 있다. 안전한 보안이 형성되기 전 수행되는 핸드쉐이크 과정은 인증에 취약하며[12] (그림 3)과 같이 UDP의 핸드쉐이크 과정은 6단계이다.

CoAP - UDP 기반 센서 디바이스 통신으로 저전력, 저대역폭, 경량 기기와 같은 제한된 환경을 위해 설계되었다. HTTP와 같은 요청-응답 모델이며 HTTP-CoAP 프록시로 호환성을 가질 수 있다[8][9].



(그림 3) DTLS Process of Handshake [13]

2.2 CoAP 네트워크 계층별 프로토콜의 DDoS 취약점

이 장은 CoAP 네트워크 프로토콜 간 DDoS 취약점을 다룬다. IoT 네트워크는 기존의 IT 네트워크의 프로토콜이 적용되어 기존 IT 네트워크 보안 위협들은 IoT 네트워크에 적용가능하다. 반면에 IT 네트워크 보안 기술의 IoT 네트워크에 대한 적용은 제한된 자원에 기인해 많은 어려움을 겪고 있다. <표 1>은 Manisha Malik 외 3명이 논문[7]에서 제시한 IoT 네트워크 계층 프로토콜 취약점 분석 결과와 Krushang Sonar등 2명이 제시한 논문[10]에서 제시한 IoT에서의 DDoS 공격 위협을 정리한 기반으로 작성하였다. CoAP 네트워크 프로토콜의 DDoS 취약점이다.

<표 1> CoAP 네트워크 계층간 프로토콜 DDoS 취약점

프로토콜	DDos 공격 유형	공격 동향
CoAP	Get flooding, DRDDoS[14]	Avaliable attack in HTTP, BoTnet base DRDoS
DTLS	DTLS Handshaking attack	DDoS used Handshaking
UDP	UDP flooding, ICMP/ping flood [10]	block packet ingestion consumes network bandwidth
IPv6	Selective forwarding[7], Sinkhole[7], IP Spoofing [10], Land Attack	Routing disturbance by IP address change
6LoWPAN	Packet fragmentation[12]	Amplification by Packet Fragmentation
804.15.4 MAC	Jamming Attacks [7]	Noise or interference propagation signal reflection
804.15.4 PHY		

CoAP - Netscout[14]는 CoAP이 HTTP와 같이 URI 요청 GET 메소드를 활용한 GET flooding 취약점이 존재한다는 것을 밝혔다. DRDoS(Distributed Reflection Denial of Service)는 IP Spoofing과 반사체를 이용한 증폭 공격이다. 반사체는 요청과 응답 패킷 길이가 비대칭성을 가진 응답 서버이며 증폭 계수란 요청 패킷 길이에 따른 응답 패킷 길이다. 증폭 계수가 클수록 DRDoS의 공격효율이 높다. [14]은 CoAP을 이용한 증폭 계수가 34로 평균 수준의 증폭 효율을 가지고 있지만 지속적으로 CoAP을 이용한 DRDoS 공격이 나타나는 것을 보인다.

DTLS - 노드가 네트워크에 참여할 때 보내는 초기

메시지를 이용한 DDoS 공격 취약점이 있다. DTLS 6 핸드쉐이크를 사용하여 소량의 메시지를 보내도 인증을 위한 교환 패킷 양이 많아 증폭 공격 위협이 크다.

UDP - UDP Flooding 공격은 희생자 호스트의 임의 포트에 출발지 IP를 위조한 패킷을 대량으로 보내 네트워크 대역폭을 소모하여 가용성을 해치는 것을 목적으로 한다. 수백 대의 좀비 호스트를 이용하는 공격으로 패킷 자체에는 특이점이 없어 차단하기 어렵다.

IPv6 - 이 프로토콜은 IP 주소 변조에 의한 라우팅 교란으로 서버 자원 소모를 통해 서비스의 가용성과 IP 주소의 무결성을 훼손하기 위한 공격이 주를 이룬다. Selective forwarding은 특정 메시지에 대한 전달을 거부하는 공격이다. Sinkhole은 라우팅 정보를 변경하여 공격자의 노드로 모든 패킷이 지나가게 한다[7]. Land Attack은 출발지와 목적지 IP 주소를 동일하게 변조하여 요청자에게 응답 패킷이 돌아온다. IP Spoofing 공격은 패킷의 변조된 Source IP로 응답코드를 전송하는 공격이다. IP 주소가 위조되었기 때문에 실제 공격자의 위치를 찾아내기 어렵다.

6LoWPAN - 재조합 및 단편화를 통해 IPv6와 IEEE 804.15.4 사이의 패킷 길이를 조절해주는 역할을 한다. 1280Byte를 보내면 6LoWPAN에서 단편화하여 약 10개로 나눠진 패킷을 만든다. 공격자가 소량의 긴 패킷을 작은 패킷으로 나누어 대량 트래픽을 생성할 수 있는 패킷 단편화[12] 취약점이 존재한다. 현재 6LoWPAN을 위한 보안 방식 표준은 확립되지 않았다[7][12].

물리계층 - 대역폭 소진 공격(Jamming Attacks)은 전파 방해 잡음이나 간섭 전파 신호를 방사하여 통신의 가용성을 해친다[7].

2.3 기존 DDoS 보안 솔루션

본 장에서는 각 네트워크 프로토콜에서의 DDoS 공격을 방지하기 위한 기법을 정리한다. IoT 또한 IT와 같이 3가지 기본 요구사항[3]을 가진다.

- 기밀성: 데이터는 인가된 주체만 확인가능하다.
- 무결성: 데이터 변조되지 않았음을 보장한다.
- 가용성: 언제, 어디서나 필요시 데이터에 접근하여 사용할 수 있다.

DDoS 공격은 주로 시스템의 가용성을 해치는 형태로 나타난다. <표 2>는 앞장에서 분류한 네트워크 프로토콜 간 DDoS 동향에 따른 방어기법을 정리한다.

CoAP - 최현상 외 3명이 제시한 [15]은 IoT 기기들을 이용한 DRDoS 증폭 공격에 대한 방어기법으로 무결성을 검증하기 위한 사전 인증을 통해 IP주소 변조를 막는 안티 스푸핑, 프로토콜 패치 기법, 네트워크 모니터링을 통해 일정 시간 트래픽이 비정상적으로 들어오는 경우 출발지 IP 스푸핑 패킷을 차단한 방어기법을 제안한다.

DTLS - UDP를 사용하는 통신에서 데이터의 무결성을 확보하기 위해 DTLS 암호화 통신이 권고되지만 초소형 장치들의 RAM과 ROM은 DTLS에서 사용되는 보안 알고리즘 연산 실현성이 없다[12]. 무결성이 확보되면 IP

<표 2> CoAP 네트워크 계층간 프로토콜 DDoS 보안 방법

프로토콜	DDoS 동향	DDoS 방어
CoAP	Available attack in HTTP, BoTnet base DRDoS	Anti-spoofing, Protocol Patch, network monitoring[15]
DTLS	DDoS used Handshaking	Streamlined Handshaking,DTLS Lightweight encryption algorithm [16]
UDP	block packet ingestion consumes network bandwidth	ICMP inflow restriction [7], Packet Filtering[17]
IPv6	Routing disturbance by IP address change	HCF(Hop Count Filtering)[18]
6LoWPAN	Amplification by Packet Fragmentation	Header compression
804.15.4 MAC 804.15.4 PHY	Noise or interference propagation signal reflection	Cooperative Jamming[19]

spoofing을 방지할 수 있다. 안수현 외 2명이 제안한 [16]은 저전력 환경에서 사용할 수 있는 경량 암호화 알고리즘인 Prince와 Quantum Resistance를 갖춘 DTLS+를 제안한다. DTLS는 핸드쉐이킹 교환 패킷이 많아 저전력 기기에 적합하지 않으며, 이를 이용한 DDoS 공격 위협이 존재한다. 따라서 DTLS의 핸드쉐이크를 간소화해야 한다.

UDP - 전준하 외 2명이 제안한[17]는 DDoS 공격을 사전에 차단하기 위해 ORACLE Solaris의 IP 필터의 패킷 필터링 규칙에 더하여 내부에서 외부로 나가는 트래픽 제어를 위한 역 방화벽 규칙을 제안한다. 하지만 헤더를 참조하여 패킷을 구별하기 때문에 데이터 신뢰성은 보장하지 않는다.

IPv6 - IP spoofing에 대응 방식인 Packet Filtering은 정의된 보안정책에 따라 패킷의 헤더를 분석하여 패킷의 허용/거부를 결정한다. 서정우 외 2명이 제시한 [18]은 IP Spoofing 방지를 위해 라우터를 거칠 때 변하는 TTL(Time to Live)을 이용해 Hop count 평균을 정리한 참조 테이블을 설계하고 위조탐지를 실험한다.

6LoWPAN - 이 프로토콜에는 패킷 단편화에 의한 증폭 공격이 많이 나타난다. 상위계층인 IPv6에서는 40byte의 헤더를 가진다[7]. 패킷 단편화에 의한 DDoS 공격 효율을 줄이기 위해 헤더 압축이 필요하다.

물리계층 - 이 계층의 대역폭 소진 공격(Jamming Attacks) 및 전파 신호 반사 공격은 Cooperative Jamming[19] 기법으로 가용성을 위해 간섭 신호에 대하여 도청자만 영향을 받도록 수신기의 전력 제한 조건에서 보안 채널 용량을 극대화하거나 전력 사용량을 최소화하는 설정을 통해 방지한다.

3. IoT 프로토콜 설계 시 DDoS 대응 방안 제안

IoT와 같이 자원이 제한된 네트워크에서 IT 네트워크와 호환성을 위해 6LoWPAN, IPv6 프로토콜이 도입되었다. 하지만 IT 네트워크에서 사용하지 않았던 프로토콜이 도입되면서 DDoS 공격 효율을 증가 시키는 두 가지 요인이 추가되었다. 첫번째는 6LoWPAN의 패킷 단편화와 DT

LS의 핸드쉐이크다. 이런 프로토콜의 도입은 패킷 증폭 공격 위험성을 높인다. 두 번째는 IoT기기의 경량 프로세서 연산능력 한계다. 경량 프로세서의 기밀성을 위해 DTLS가 권고되지만 IoT의 프로세서의 연산능력 한계 때문에 현실적으로 실현 불가능하며, 도입되어도 핸드쉐이크를 이용한 DDoS 공격 위협이 존재한다. 따라서 IoT를 위한 프로토콜 설계 시 해당 프로토콜이 DDoS 공격에 대한 안전성 및 네트워크 가용성에 대한 검증이 필요하다. 본 논문에서 제시하는 고려해야 할 검증 사항은 다음과 같다.

1. 네트워크 프로토콜 간 호환성을 위해 패킷 단편화를 지원하는 프로토콜 도입 시 증폭 계수를 고려한다. 요청 패킷과 응답 패킷의 길이 비대칭성이 크고 단편화되는 패킷의 수가 증가하면 증폭 계수가 높아진다. 이를 개선하기 위해서는 헤더를 압축하여 패킷 길이를 조절하거나 핸드쉐이크 과정을 간소화하여 증폭 계수를 줄이는 방안이 고려되어야 한다.

2. DTLS와 같이 일정 수준의 연산능력과 자원을 요하는 프로토콜 설계 시 IoT 환경 안에서 가용성에 대한 검증을 수행해야 한다. <표 3>은 센서 자원에 따른 분류표로, 이를 기반으로 각 Class가 지원하는 Code size와 Data size에 맞춘 경량 암호 알고리즘이 필요하다.

<표 3> 센서 자원에 따른 분류[12]

Name	Data size (e.g, RAM)	Code size (e,g. Flash)
Class 0	<< 10 KiB	<< 100 KiB
Class 1	~ 10 KiB	~ 100 KiB
Class 2	~ 50 KiB	~ 250 KiB

4. 결론

IoT는 다양한 산업 분야에 응용되면서 IoT 보안의 중요성은 증가하고 있다. IoT 네트워크에는 기존 IT 네트워크의 공격 기법들이 적용 가능하다. 반면에 기존 IT 네트워크의 보안 기술은 IoT 기기의 제한된 자원으로 인해 적용이 어려운 실정이다. 이를 개선하기 위해서는 IoT 네트워크를 고려한 보안 기술 개발이 필요하다.

본 논문에서는 IoT 네트워크에 대한 DDoS 공격에 대응하기 위한 프로토콜 설계 고려사항을 제시한다. 이를 위해 기존 CoAP의 DDoS 보안 위협, 보안 방법과 한계를 네트워크 프로토콜을 기준으로 정리했다. 또한, IoT 환경을 위해 도입된 6LoWPAN, IPv6이 DDoS 공격에 취약할 수 있음을 보였다. 이를 기반으로 본 논문에서는 IoT 네트워크를 위한 프로토콜 설계 시, 해당 프로토콜의 DDoS에 대한 안전성 검증을 위해 프로토콜의 가용성 및 증폭 계수 관점에서 두 가지의 보안 고려사항을 제안했으며, 이를 준수할 경우 DDoS 공격 대한 안전성과 가용성을 보장할 수 있을 것으로 기대된다. 추후에는 센서 디바이스에 대한 연산능력을 고려한 경량 프로토콜 연구를 수행하고자 한다.

참고문헌

[1] 정보통신기술진흥센터, IoT 현황 및 주요 이슈, (2015)
[2] 권혁찬, 사물 인터넷 네트워크 보안, 사물인터넷 포럼 (2016)
[3] Li, Shancang, and Li Da Xu. Securing the internet of things. Syngress, 2017.
[4] Gartner, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, (2017)
[5] https://www.zdnet.com/article/the-coap-protocol-is-the-next-big-thing-for-ddos-attacks/
[6] Z. Shelby, The Constrained Application Protocol (CoAP), IETF, RFC 7252 (2014)
[7] Manisha Malik, Kamaldeep and Maitreyee Dutta, Defending DDoS in the Insecure Internet of Things: A Survey. Artificial Intelligence and Evolutionary Computations in Engineering Systems,pp. 223-233. (2018)
[8] Jorge Granjal, Edmundo Monteiro, Jorge Sa Silva, Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues, IEEE, (2015)
[9] 오하영, 사물 인터넷 기반 기기간 통신 무선 환경에서 향상된 RPL 기반 경량화 라우팅 프로토콜(2014)
[10] Krushang Sonar, Hardik Upadhyay, "A Survey: DDoS Attack on Internet of Things", International Journal of Engineering Research and Development, (2014)
[11] 김은숙, 김용운 6LoWPAN 기반의 IP-USN 기술 표준화 동향, 전자통신동향분석 제 22권 제 6호, (2007)
[12] 강남희. "사물인터넷 보안을 위한 표준기술 동향." 한국통신학회지(정보와통신), 31.9 (2014.08): 40-45.
[13] 권혁진, 강남희. 사물인터넷에서 경량화 장치 간 DTLS 세션 설정 시 에너지 소비량 분석. 한국통신학회논문지, (2015)
[14] Matthew Bing, "COAP ATTACKS IN THE WILD", netscout (2019) https://www.netscout.com/blog/asert/coap-attacks-wild
[15] 최현상, 박현도, 이희조, 증폭 DRDoS 공격 및 방어에 관한 연구, 한국정보전자통신기술학회논문지, 8권 제5호. pp.429~437 (2015)
[16] 안수현 김광조, IoT 환경에 적합한 경량 DTLS 프로토콜 구성 방법, (2017)
[17] 전준하, 이기영, "DDoS 공격 방지를 위한 역 방화벽(Reverse Firewall)에 관한 연구", 한국통신학회 하계종합학술발표회, (2017)
[18] 서정우, 이상진, IP 스푸핑을 통한 DDoS 공격 탐지 방안에 대한 연구, Journal of The Korea Institute of Information Security & Cryptology (2015)
[19] 한국 방송 통신 전파 진흥원, 물리계층 보안 기술 동향, 방송통신 기술 이슈&전망 제 21호 (2013)