

이벤트 발생 후 분석을 포함하는 해결책과 달리, 이 방법은 실시간 탐지를 가능하게 합니다.

테스트 IoT 네트워크 환경은 세 가지 노드 클래스로 구성됩니다: 정당한 노드(LN), 느린 간헐적인 연결을 가진 진정한 노드(SN), 그리고 느린 DoS 공격을 유발하는 악의적인 노드(MN). 실험 결과는 느린 DoS 공격 트래픽이 두 단계 IDS 전략의 일부로 의심스러운 것으로 정확히 분류될 수 있음을 뒷받침합니다. 이 전략은 MN, LN 및 SN 트래픽을 성공적으로 구분하여, 자원 제약이 있는 IoT 환경에서 공격 탐지의 신뢰성을 향상시키고, 최소한의 오버헤드를 초래합니다.

본 논문의 나머지 부분은 다음과 같이 구성됩니다

제 2장에서는 느린 DoS 공격의 성격과 특징, 그리고 현재의 탐지 방법과 IDS 전략을 검토합니다. 제 3장에서는 사용된 실험 테스트 IoT 환경을 설명하며, 제 4장에서는 새로운 느린 DoS 탐지 기술의 중요한 결과 분석을 제공합니다. 제 5장에서는 결론적 의견과 추가 작업 계획을 제공합니다.

관련 연구

느린 DoS 공격은 IoT 네트워크 보안 위협 중에서 가장 어려운 문제 중 하나로, 주요 운영 TCP 및 HTTP 매개변수의 내재된 취약점을 이용하여 인기 있는 HTTP 서버를 표적으로 삽니다. TCP의 작동은 느린 DoS 공격을 실현하는 데 중요한 역할을 합니다. TCP는 연결 지향 프로토콜로, 호스트는 성공적으로 세 가지 손잡이를 협상해야 합니다. 이 과정이 원료되면, 클라이언트와 서버는 데이터 교환을 위해 필요한 매개변수를 설정하기 위해 요청과 응답을 시작합니다. 서버는 애플리케이션이 필요한 작업을 완료하거나 TCP 연결을 닫기 전에 설정된 타임아웃 간격까지 기다립니다. 느린 DoS 공격은 특히 이 연결 지향성과 순서대로 전달되는 구조를 이용하도록 설계되었습니다. 예를 들어, 느린 DoS는 HTTP GET 요청에서 세션을 종료하는 신호를 보내는 문자열을 누락시킴으로써 서버가 클라이언트 응답을 기다리며 불필요한 자원을 소비합니다.

느린 DoS 위협

느린 DoS 공격은 많은 관심을 끌었으며, 몇 가지 완화 전략이 제안되었습니다. 그러나 반복적으로 나타나는 발견은 이러한 유형의 공격이 정확하고 신뢰성 있게 탐지하기 어렵다는 것입니다. 이는 공격이 정당한 사용자가 반복적인 대역폭이나 간헐적인 노드 간 연결을 경험하는 것으로 분류될 수 있기 때문입니다. 이로 인해 이러한 진정한 노드가 전통적인 IDS에 의해 잘못된 느린 DoS 공격자의 동기는 대상 웹 서버에 정당한 요청을 포화시키고 서버 자원을 확장하여 운영 서비스를 방해하는 것입니다. Apache HTTP 웹 서버는 크기와 설치의 용이성 때문에 가장 일반적인 인터넷 서버 중 하나로, 웹 기반 인터페이스가 필요한 IoT 장치에 이상적인 선택입니다. 이러한 웹 서버에 악의적인 공격을 가하기 위해 몇 가지 느린 DoS 변종이 등장했으며, 주요 변종은 다음과 같습니다:

- Slow Read: 이 공격은 TCP 윈도우 크기 매개변수를 활용하여, 동의된 크기와의 불일치로 인해 공격 클라이언트가 서버로부터 응답을 매우 느리게 읽어들여 성능을 저하시킵니다 [14].
- RUDY 또는 Slow HTTP Post: 이 공격은 POST 데이터를 메시지 본문으로 보내며, 이를 매우 느린 속도로 서버로 다시 전송됩니다. 이 속도는 분단 단일 바이트로 줄일 수 있습니다 [15]. RUDY는 웹 서버의 스테드 기본 기능을 표적으로 삼아 모든 사용 가능한 소켓을 차지합니다.
- 범위 공격: 이 공격은 HTTP 서버의 범위 요청 기능의 취약점을 표적으로 삽니다. 범위 값은 바이트 단위로 지정되며, 예를 들어 0-50입니다. 공격자는 긴 바이트 스트림을 요청하여 일부가 불법적으로 중첩되도록 함으로써 서버가 자원을 낭비하도록 만듭니다.
- Slowloris: 공격자는 부분적인 HTTP GET 요청을 보내고, 서버는 연결을 열지만, 공격자는 서버와 연결을 완료하기 위해 응답하지 않도록 고의로 하여 타임아웃 값이 도달할 때까지 소켓을 열어둡니다 [16].
- 여러 연결 요청이 모든 사용 가능한 웹 서버 소켓을 차지할 수 있습니다. 이 느린 DoS 변종은 LNI에 새로운 연결 또는 느린 연결을 가질 때 진정한 네트워크 활동으로 잘못 인식되기 때문에, 본 논문의 나머지 부분은 이 느린 DoS 공격에 초점을 맞추며, 현재 특정 위협 상황에서 사용되는 탐지 접근법에서 가장 흔한 공격입니다.

ML 분류기의 성능, 특히 Naive Bayes, Random Forest, Decision Tree, K Nearest Neighbour 및 Multilayer Perceptron이 DDoS 공격 탐지에 대한 분석이 [9]에서 수행되었습니다. 이 평가는 CIDS-001(Coburg Intrusion Detection)이라는 막대한 데이터 셋에서 이루어졌으며, 이는 3200만 개 이상의 네트워크 이벤트를 포함하는 종합적인 데이터셋입니다. 그러나 분석을 위해 데이터셋의 일부만(150만 개의 네트워크 이벤트)이 추출되었기 때문에, IDS 결과는 시간 IoT 환경에서 평가 목적으로 실질적으로 적용하기 어렵습니다.

[11]에서 제안된 대안적 접근법은 PCAP(패킷 캡처) 이벤트 분석을 통해 최소값의 불완전한 HTTP GET 요청을 사용하여 Slowloris 공격 탐지 경보를 생성하는 것입니다. 이 설정은 실시간 환경을 사용했지만, 시뮬레이션된 트래픽 시나리오만 고려했습니다. 패킷 분석은 또한 서명 기반 기술 [19]에서 공격 탐지를 위해 사용되었습니다.