무선 센서 네트워크를 위한 자원 효율적인 분산 IDS 프레임워크

조응준 O, 홍충선

경희대학교 컴퓨터공학과

ejcho@networking.khu.ac.kr, cshong@khu.ac.kr

요 약

Signature 에 기반한 IDS(Intrusion Detection System)는 그 특성상 signature 의 수에 따라 그 성능이 크게 좌우된다. 따라서 많은 signature 를 확보할수록 더 높은 많은 공격을 탐지할 수 있다. 그러나 자원 제약적인 센서 노드상에 많은 signature 를 저장하는 것은 효율적이지 못하다. 본 논문에서는 센서 노드의 메모리 사용량을 줄이면서도 오버헤드가 낮은 분산 IDS 메커니즘을 제안하고 제안 방법의 성능을 수학적으로 분석하여 그 성능이 우수함을 입증하였다.

1. 서론

무선 센서 네트워크는 Internet of Things 나 사물망 통신과 같은 기술이 주목 받으면서 더욱 활발하게 연구되고 있는 기술 중 하나이다. IEEE 802.15.4 를 기반으로 하는 IPv6 over LoW Power wireless Area Network (6LoWPAN)은 센서 노드상에 IPv6 를 할당하여 사용할 수 있는 기술로, 이로 인해 무선 센서 네트워크는 더욱 다양한 분야에 활용될 것으로 전망되고 있다. 따라서 이처럼 다양한 분야에 사용되는 무선 센서 네트워크의 보안도 크게 주목을 받고 있다.

Intrusion Detection System (IDS)는 공격탐지 시스템으로 네트워크를 보호하기 위한 기초적이면서도 중요한 시스템이다. IDS 는 탐지 기법에 따라 signature 를 기반으로 탐지하는 것과 행위기반으로 탐지하는 것으로 분류된다. 이 중 signature 를 기반으로 탐지하는 기법은 탐지할 수 있는 signature 의 수에 따라 그 성능이 좌우된다. 즉 IDS 에서 탐지를 하기 위해 샘플로 보유하고 있는 signature 의 수가 많을수록 더 많은 공격을 탐지 할 수 있다. [1]은 자원 제약적인 센서 네트워크에서 자원의 효율성을 높이기 위해 Bloom filter[2]를 이용하여 signature 의 크기를 획기적으로 감소시키고 작은 저장공간만을 활용하여 효율적으로 센서 네트워크 상에서 IDS 를 운영할 수 있는 메커니즘을 제안하였다. 본 논문에서는 [1]에서 제안된 메커니즘에서 발생할 수 있는 문제점을 살펴보고 이를 해결하기 위해 분산 IDS 메커니즘을 제안한다.

2. Bloom filter 기반의 IDS

[1]에서는 Bloom filter 를 활용하여 센서 네트워크에 적합한 IDS 를 소개하고 있다. Bloom filter 는 rm 특성상 False Positive 이 존재하는데 사용되는 해쉬 함수의 수를 k, 입력 데이터의 개수를 n, 그리고 Bloom fliter 에 사용되는 배열의 크기를 m 이라고 하였을 때 false positive rate (이하 fpr)은 (1)과 같이 구할 수 있다[2].

$$fpr = \left(1 - \left(1 - \frac{1}{m}\right)^{kn}\right)^{k} \approx \left(1 - e^{-kn/m}\right)^{k} \quad (1)$$

(1)을 $k=2$ 일 때 m 에 대하여 정리하면 (2)와 같이 정리된다.

$$m \geq n \log_2 e \log_2 \left(1/fpr\right) \approx 1.44n \log_2 \left(1/fpr\right) \quad (2)$$

즉 fpr 값이 주어지고 입력데이터의 수가 정해지면 특정 fpr 을 만족하기 위한 최소한의 m 값을 구할 수 있다. [1]에서는 이런 특성을 고려하여 signature 기반의 IDS 를 설계할 때 Bloom filter 를 적용하여 메모리 사용을 최소화 시키고 있다.

수신한 패킷이 공격 패턴으로 판단될 경우 이에 따르는 대응이 필요하다. 그러나 Bloom filter 를 사용할 경우 별도의 데이터베이스가 없는 한 입력된 데이터가 정확히 어떤 유형의 공격인지 알 수 없다. 이를 위해 [1]에서는 그림 1 에서 나타난 것처럼 signature-code 의 정보와 공격 패턴의 정보, 그리고 대응 방식의 데이터베이스를 가진 sink 에게 공격을 탐지한 노드가 signature-code 를 전송하여 어떤 종류의 공격인지를 판단하고 이에 대응하는 방법을 실행하는 방식을 사용하고 있다.

그러나 이 방식의 경우 모든 Bloom filter 가 fpr 을 가지고 있기 때문에 공격자가 이를 악용하여 signature-code 를 계속 발생시키도록 공격을 실행 할 수 있다. 이는 sink 에서 signature-code 분석을 위한 부하뿐만이 아니라 센서 노드의 에너지 소모도 일으키는 문제점이 있다.

본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2010-(C1090-1031-0005)) Dr. CS Hong is corresponding author.

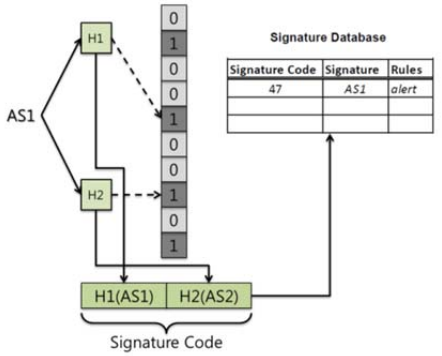

그림 1 Bloom filter 를 이용한 IDS 의 동작 예시

3. 제안사항

본 논문에서는 다중 Bloom filter 배열을 활용한 분산 IDS 메커니즘을 제안한다. 그리고 제안을 위해 무선 센서 네트워크는 ad hoc 상태로 작동을 하고 분산 Bloom filter 배열은 임의로 배치되는 것으로 가정한다.

센서 네트워크의 경우 그 특성 상 기반시설 없이 통신을 하기 위해 ad hoc 형태로 데이터를 전송하는 경우가 많다. 이 경우 다수의 센서 노드가 다른 노드의 데이터를 목적지까지 전달하는 전달(relay) 노드로 참여한다. 이러한 통신 구조에서는 데이터를 수신하는 수신자 노드 외에도 전달 노드가 IDS 의 일부로 시스템에 참여하는 것이 가능하다. 즉 센서 노드에 Bloom filter 배열을 분산 배치 하는 것으로 각각의 노드에 설치되는 배열의 크기는 줄이면서도 성능을 유지하는 것이 가능하다. 그림 2 는 중간자 노드가 어떻게 IDS 동작에 참여하는지를 나타내는 예시이다.

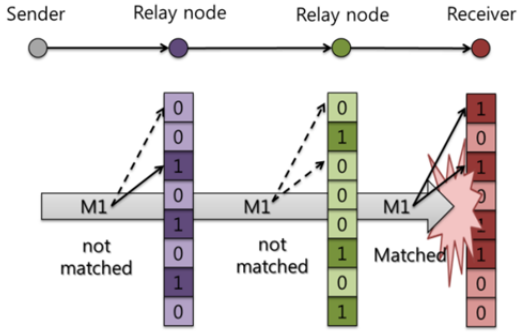

그림 2 분산 IDS 의 기본 작동 원리

(2)에서 볼 수 있는 것처럼 배열의 크기 m 과 입력데이터 수 n 은 정비례관계에 있는 것을 알 수 있다. 따라서 이런 Bloom filter 의 배열의 수를 여러 개로 분산시킬 경우 각 배열에서 탐지해야 하는 signature 의 수를 분산 시킬 수 있기 때문에 그만큼 목표로 하는 fpr 을 달성하기 위한 최소한의 배열의 크기가 작아지게 된다. 그러나 이때 고려할 점이 각 Bloom filter 의 fpr 은 모두 독립적으로 발생하기 때문에 Bloom filter 배열의 수가 증가한다면 fpr 도 증가 하게 된다. 이러한 특성을 반영하여 최소 배열 공간의 크기를 구하기 위한 식을 (2)로부터 유도하면 (3)과 같다.

$$m \geq 1.44 \frac{n}{j} log_2 \left(\frac{j}{fpr} \right) \qquad (3)$$

여기서 j 는 Bloom filter 배열이 분산되는 숫자를 의미한다. (3)에서 볼 수 있듯이 m 의 값은 $\frac{\log_2 j}{j}$에 비례하는 것으로 나타나는데 $j > log_2 j$ 이기 때문에 m 은 j 의 값에 반비례하는 것을 알 수 있다.

[1]의 연구 중 단점으로 지적된 데이터베이스에 signature-code 를 보내는 부분을 본 논문에서는 센서 노드에 각각 포함시키는 것으로 한다. Bloom filter 가 분할되는 만큼 센서 노드상에 필요한 signature-code 데이터 베이스의 크기도 작아진다.

4. 성능분석 및 결론

j 값과 센서 네트워크의 평균적인 통신 거리에 따른 탐지율을 계산해보면 h 가 센서 네트워크의 평균적인 통신 거리(홉 수)라고 할 때 (4)와 같이 나타낼 수 있다.

$$D = \sum_{z=0}^{h-1} \left(1 - \frac{1}{j}\right)^z \frac{1}{j} \qquad (4)$$

위 식을 기반으로 하여 h 와 j 값에 따른 탐지율 D 를 그래프를 나타내면 그림 3 과 같다.

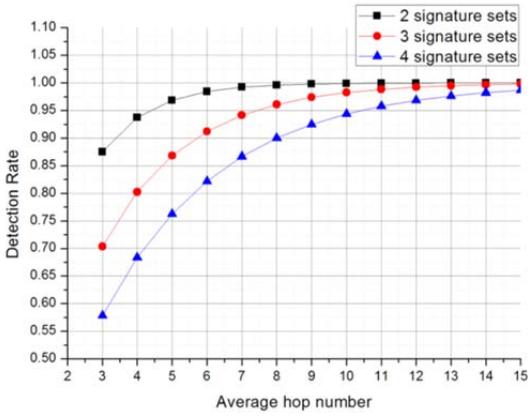

그림 3 Bloom filter 배열과 평균 홉 수에 따른 탐지율의 변화

이상의 결과에서 볼 수 있듯이 본 논문에서는 [1]보다 자원 효율적이며 성능도 근접하고 [2]에서 발생 가능한 문제점을 해결한 분산 IDS 를 제안하였다.

6. 참고 문헌

[1] Syed OBAID AMIN, Muhammad SHOAIB SIDDIQUI, Choong SEON HONG and Sungwon LEE, "Implementing Signature Based IDS in IP-Based Sensor Networks with the Help of Signature-Codes", IEICE Transactions on Communications, Vol.E93-B, No.02, pp.389-391, February 2010

[2] A.Broder and M. Mizenmacher, “Network applications of bloom filters: A survey”, Internet Mathematics, vol.1, no.4, pp.485-509, 2004