WSN에서 블룸필터를 이용한 분산된 시그니쳐 기반 IDS의 탐지율 향상 기법

조응준, 홍충선
경희대학교 컴퓨터공학과
ejcho@networking.khu.ac.kr, cshong@khu.ac.kr

A Mechanism for Enhancing the Detection Rate in Distributed Signatures Based IDS for Wireless Sensor Network

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

요 약

시그니쳐 기반의 IDS의 경우 탐지할 수 있는 공격의 수가 시그니쳐의 수에 따라 결정된다. 이런 특징상 시그니쳐의 크기를 획기적으로 줄이지 않는 이상 연산과 메모리 공간이 제한된 센서 네트워크에 시그니쳐 기반의 IDS를 탑재하는 것은 비효율적이다. 이런 단점을 극복하기위해 여러 연구에서 시그니쳐의 크기를 획기적으로 줄이는 방법과 분산 배치를 통한 개개의 센서 노드에 탑재되는 시그니쳐의 크기를 줄이는 방법을 제안하였다. 그러나 시그니쳐를 분산할 수록 공격 탐지율이 낮아지는 문제점이 발생한다. 본 연구에서는 시그니쳐의 출현 빈도를 사용하여 시그니쳐를 분산시킴으로서 메모리 사용대비 탐지율을 향상시키는 방법을 제안한다.

1. 서 론

무선 센서 네트워크는 자원 제한적인 작은 노드로 이루어진 네트워크이다. 이러한 제한적인 자원으로 작동하는 센서 노드에서 자원을 효율적으로 사용하는 것은 매우 중요하다. 그러나 무선 센서 네트워크가 적용가능한 곳이 광범위한 만큼 보안에서도 많은 위협이 발생할 것으로 예상되고 있다.

IDS는 실용적이면서 쉬운 네트워크 보호 기술 중 하나이다. 이런 IDS는 시그니쳐 기반의 IDS와 행위 기반의 IDS로 분류가능하다. 그러나 행위 기반의 IDS는 탐지를 위해 많은 양의 데이터 로그를 저장하고 이를 서로 비교하는 작업이 필요하기 때문에 큰 메모리 용량과 높은 연산 처리 능력이 요구된다. 이런 특징은 무선 센서 네트워크에 적합하지 않기 때문에 본 논문에서는 효율적은 시그니쳐 기반의 IDS를 개발하는 것에 목표를 둔다.

시그니쳐 기반의 IDS는 탐지할 수 있는 시그니쳐의 수가 많을수록 더 많은 공격을 탐지할 수 있다. 즉 많은 시그니쳐를 데이터베이스에 저장할 수 있어야 한다. 그러나 이런 특징은 자원 제한적인 센서 노드에 적합하지 않기 때문에 센서 노드상에 구현을 하기위해서 적절한 수정이 필요하다. 본 논문에서는 저장되는 시그니쳐를 분산시켜 센서 노드상에 저장되는 시그니쳐 데이터베이스의 크기를 줄이면서도 높은 탐지율을 유지할 수 있는 메커니즘을 제안한다.

본 연구는 지식경제부 및 한국산업평가관리원의 산업원천기술개발사업의 일환으로 수행되었음. [과제관리번호 : 2009-S-014-01, 센싱기반 감성서비스 모바일 단말 기술개발] Dr. CS Hong is corresponding author.

2. 관련 연구

2.1 블룸 필터를 사용한 IDS 메커니즘

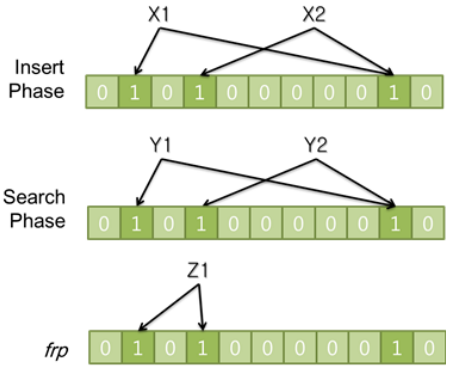

그림 1 블룸 필터의 작동 원리 및 *fpr*

[1]에서는 블룸필터를 사용하여 시그니쳐 데이터베이스의 크기를 줄이는 기법을 제안하였다. 블룸필터는 간단하고 효율적인 무작위 데이터구조[2]로 복수의 해쉬함수를 사용한다. 이런 블룸 필터는 확률적인 false positive를 가지는데 이를 fpr(false positive rate)이라 한다. 그림 1에서 볼 수 있듯이 Y1과 Y2는 입력된 X1과 X2와 일치하며 정상적으로 탐지가 되지만 Z1의 경우 입력된 데이터와 일치하지 않음에도 탐지가 되는 것을 볼 수 있다. 여기서 fpr이 일정하게 주어지고 사용되는 해쉬함수의 수가 2이고 입력되는 데이터의 수가 n일 때 필요한 최소 메모리 양 m은 다음과 같이 구할 수 있다.

$$m \geq nlog_2elog_2(1/fpr) \approx 1.44nlog_2(1/fpr)$$

[3]에서는 [1]의 연구를 바탕으로 보다 효율적으로 시그니쳐 데이터베이스를 저장하기위해 애드 혹 환경상에서 시그니쳐 데이터베이스를 분산시키는 기법을 제안하였다. [3]에서는 시그니쳐를 j개의 블룸 필터 배열에 분산시켜 필요한 최소 메모리양을 다음과 같이 구하였다.

$$m \geq 1.44(n/j)\log_2(j/fpr)$$

그리고 [3]에서는 SNORT[4]에서 정의된 시그니쳐의 우선순위에 따라 시그니쳐의 분산정도에 차이를 두어 위험한 공격의 경우 더 정확히 탐지되도록 하는 메커니즘을 제안하였다. 그러나 [3]에서 제안한 기법의 경우 하나의 센서 노드상에 탑재되는 시그니쳐의 수를 늘려 탐지율이 올라간 것이다. 물론 위험한 공격의 경우 보다 효율적으로 탐지할 수 있겠지만 이는 메모리 사용량을 희생한 대가이다. 본 논문에서는 앞서 제안된 메커니즘을 바탕으로 실제 공격 시그니쳐가 출현한 빈도를 바탕으로 시그니쳐를 분산하는 방법을 제안한다, 그리고 이를 통해 보다 메모리 사용이 효율적인 분산 IDS 메커니즘을 제안한다.

3. 출현 빈도에 바탕한 시그니쳐 분산 기법

시그니쳐 기반 IDS의 가장 큰 특징은 미탐율(true negative rate)이 0이라는 것이다. 즉 저장된 시그니쳐의 경우 100% 탐지를 보장한다. 그러나 메모리 사용량을 줄이기 위해 [1]에서 제안된 메커니즘의 경우 시그니쳐 기반의 IDS이지만 미탐율이 존재한다. 그리고 [3]에서 제안된 방안의 경우 공격의 위험성이 높을 경우 탐지율을 높일 수는 있지만 메모리 사용률이 높아지는 단점이 있다. 이런 단점을 보완하기위해 본 논문에서는 통계기반의 자료를 바탕으로 시그니쳐 데이터를 분산하는 기법을 제안한다.

[3]에서는 시그니쳐의 우선순위를 바탕으로 시그니쳐를 분산하고 있다. 본 논문에서는 시그니쳐 발생빈도를 가중치로 더하여 시그니쳐를 분산 배치하고자 한다. 우선 각 시그니쳐에 발생 빈도의 가중치를 더하기위해 해당 시그니쳐의 발생 비율을 [3]에서 제안한 우선순위 가중치 값과 곱하여 준다. 즉, 시그니쳐 우선순위로 주어진 가중치를 a, 기본 가중치를 b, 그리고 특정 시그니쳐의 발생 빈도를 c라고 하였을 때, 가중치는 모든 값을 곱하여 구할 수 있다. 이때, 기본 가중치의 크기를 조절하여 사용하는 메모리의 양을 조절할 수 있다.

4. 성능 분석 및 메모리 요구량 비교

성능 비교 및 분석을 위해 본 논문에서는 안철수 연구소[5]에서 제공하는 악성코드 대표진단명 감염보고 Top20의 자료를 참고하였다. 실제 악성코드의 수는 훨씬 많을 수 있지만 비교 및 분석을 위해 본 절에서는 20개의 악성코드의 경우만을 계산하였다. [3]과 같이 분산 배치될 배열의 수가 2, 3, 4일 경우로 하여 각각의 탐지율을 계산하였다. 비교를 위해 기존 연구의 경우 시그니쳐 빈도를 사용하지 않은 기존 메커니즘만 적용하였다. 현재 안철수 연구소에서 제공하는 악성코드 대표진단명의 경우 위험도 등급이 각각 위험, 보통, 낮음으로 구분되어 있으며 각각 9, 7, 4개씩 있는 것으로 보고되어 있다.

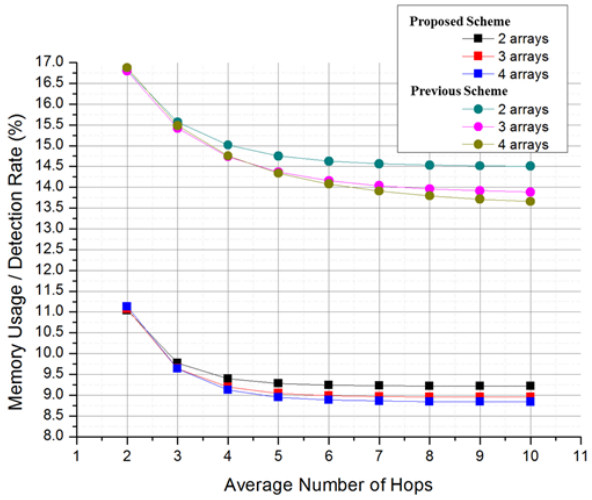

그림 2 탐지율 대비 메모리 사용량

그림 2는 제안사항과 기존 연구의 메모리 사용량 대비 탐지율을 보여준다. Y축의 값은 메모리 사용량을 탐지율로 나눈 것으로 이 값이 낮을 수록 사용하는 메모리 대비 더 많은 시그니쳐를 탐지할 수 있는 것을 나타낸다. 그림에서 알 수 있듯이 본 제안사항의 경우 기존 메커니즘보다 더 적은 메모리를 사용하면서 더 많은 공격을 탐지할 수 있는 것을 알 수 있다.

5. 결론

본 논문에서는 통계적인 자료를 사용하여 기존 메커니즘보다 효율적인 방식으로 분산 IDS에 시그니쳐 정보를 분산하는 메커니즘을 제안하였다. 본 제안사항을 활용할 경우 상대적으로 적은 메모리를 사용하면서 분산 IDS 상에서 높은 탐지율을 달성 할 수 있다.

참고문헌

[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

[3] Eung Jun Cho, Choong Seon Hong, Deokjai Choi, “Distributed IDS for Efficient Resource Management in Wireless Sensor Network”, APNOMs 2011, September 2011

[4] SNORT, http://www.snort.org/

[5] 안철수 연구소, 악성코드 통계, 2011 vol. 20, http://www.ahnlab.com/kr/site/securitycenter/asec/asecView.do?groupCode=VNI001&webNewsInfoUnionVo.seq=18399