무선 메쉬 네트워크에서 효과적인 침입탐지 시스템 배치
Effective Intrusion Detection System (IDS) Placement in Wireless Mesh Networks

김기성, 이근수, 김세헌
대전광역시 유성구 구성동 373-1 한국과학기술원 산업공학과
E-mail : {kskim, kslee}tmlab.kaist.ac.kr, shkim@kaist.ac.kr

Abstract

무선 메쉬 네트워크(Wireless Mesh Network) 기술의 급속한 발전과 함께, 안전한 무선 통신을 위한 보안 문제가 중요한 이슈로 대두되고 있다. 무선 메쉬 네트워크에서 침입탐지 시스템을 운영하기 위해서는 탐지 에이전트가 각 무선 노드에 설치되어야 한다. 무선 메쉬 네트워크를 구성하는 노드들은 유한한 배터리를 사용하므로 생존기간(Lifetime)에 제한이 있다. 침입탐지 에이전트를 노드에 설치 할 경우 이에 해당하는 배터리 소모가 발생하여 생존기간이 줄어들게 된다. 또한 침입탐지 효과의 증대를 위해서는 많은 트래픽을 감시할 수 있는 노드에 침입탐지 에이전트가 배치되어야 한다.

따라서 본 논문에서는 무선 메쉬 네트워크에서 네트워크의 생존기간을 최대로 하면서 침입탐지의 효과성을 동시에 고려한 침입탐지 에이전트 설치를 위한 방안을 제안한다. 제안하는 방식은 Set Covering Problem (SCP) 해결 방법을 응용하여, 각각의 무선 노드를 제어하는 게이트웨이가 적절한 노드를 선택하여 침입탐지 에이전트를 배치하도록 한다.

1. Introduction

침입탐지시스템(IDS)은 통신 네트워크의 트래픽을 감시하여 이상 트래픽이나 공격 트래픽이 발생 할 경우 이를 탐지하여 네트워크를 보호하는 시스템이다. IDS는 방화벽, VPN 등과 함께 유선 네트워크 보안의 핵심 기술로 사용되고 있다.

무선 통신 네트워크 기술이 발전함에 따라 WLAN, Ad-Hoc 네트워크 등 무선 네트워크 사용이 늘어났다. 안전한 무선 네트워크의 이용을 위해 무선 네트워크에 IDS 등의 보안 메커니즘을 적용하는 것이 요구된다.

무선 네트워크의 단말들은 대부분 유한한 배터리를 기반으로 동작한다. 네트워크를 감시하기 위해 트래픽을 수집하고 분석하는 부가적인 에너지가 사용된다. 침입탐지 에이전트를 노드에 설치 할 경우 이 에너지로 인해 배터리가 더 소모되어 생존기간이 줄어들게 된다. 또한 많은 트래픽에 대한 모니터링이 가능한 노드에 침입탐지 에이전트를 설치함으로써 전체 네트워크 측면에서 에너지 소모를 줄일 수 있으며 침입탐지의 효과도 향상시킬 수 있다. 따라서 무선 네트워크에서는 네트워크에 대한 침입탐지 효과를 향상시키면서 부가적으로 사용 에너지를 줄여 배터리 소모를 최소화시키는 효율적인 운영 방안이 필요하다.

DIDS는 각 노드에서 한 홉 내지 두 홉의 이웃 노드들의 연결성(connectivity)을 조사하여 가장 연결성이 우수한 노드에 IDS를 선택적으로 설치하여 침입탐지 효과를 향상시키고자 했다[1]. LES는 각 노드에서 이웃 노드들의 잔여 배터리를 기준으로 배터리가 가장 많이 남아있는 노드에 IDS를 설치하여 네트워크의 생존기간을 향상시키고자 했다[2]. 하지만 DIDS는 전체 시스템의 에너지 사용량은 적지만 연결성이 좋은 단말 노드에 IDS가 집중적으로 설치되고 가용 에너지를 조기에 소진함으

본 연구는 정보통신부 및 정보통신 연구진흥원의 대학 IT지원 연구사업의 연구결과로 수행되었음

로써 전체 네트워크의 생존기간을 줄이게 된다. 반면 LES는 잔여 배터리가 많은 노드를 선택하므로 각 개별 노드의 생존 기간을 향상시킬 수는 있지만 IDS 에이전트 설치 노드 수가 많다. 따라서 전체 네트워크 측면에서 에너지 소모량이 많기 때문에 궁극적인 네트워크 생존 기간의 최대화를 위한 최적의 알고리즘으로 볼 수 없다.

본 논문에서는 무선 메쉬 네트워크(Wireless Mesh Network, WMN)에서 네트워크의 적절한 수준의 생존기간을 보장하면서 동시에 전체 네트워크 에너지 소모량을 줄이는 방안을 제안하고자 한다.

본 논문의 구성은 Section 2 에서 대상 도메인인 WML에 대해 설명하고, Section 3에서 Formulation을 통해 문제를 정의하고, 알고리즘을 제안한다. Section 4에서 제안된 알고리즘을 실험을 통해 분석한 후, Section 5에서 결론을 맺는다.

2. System Description

WMN는 무선 상의 고정 또는 이동성 노드와 유선에 연결된 게이트웨이로 구성된다.

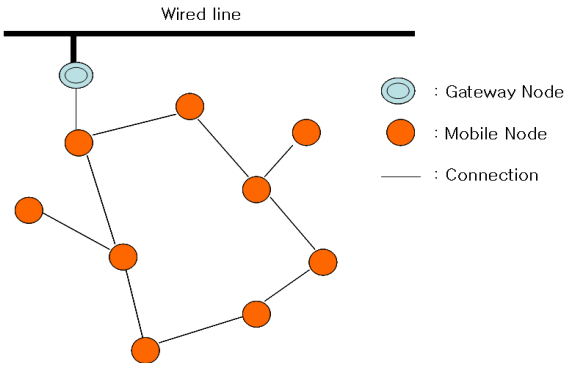

그림 1 Wireless Mesh Network의 예

각 디바이스/노드는 프로세싱 파워와 메모리를 제공하며 라우팅 정보가 공유되어 멀티 호핑(Multi-Hopping)이 가능하고 정의된 토폴로지에 의해 무선 브로드밴드(broadband) 네트워킹을 수행한다. WMN은 같은 기종의 네트워크는 물론 다른 기종의 네트워크의 연결도 가능하게 함으로 사용자가 언제든 원하는 곳에서 자유롭게 데이터에 접근가능 하도록 한다. 따라서 이는 유비쿼터스 시대의 무선 인프라 중 하나로 활용될 가능성이 높은 기술이다.

WMN에서는 각 이동 노드의 정보가 멀티 호핑을 통해 게이트웨이로 전송이 가능하다. 각 노드의 잔여 배터리량과 연결성 정보를 게이트웨이(gateway)에서 수집 할 수 있다. 본 논문에서는 이렇게 수집된 정보를 바탕으로 WMN에서의 안전한 네트워크 운영을 위한 효과적인 IDS 에이전트 배치 문제에 대해 고려하고자 한다.

3. Formulation

제안 알고리즘은 SCP를 이용한 IDS 에이전트 노드를 선택하는 단계(3.1 IDS Node Selection)와 인접해 있는 다수의 IDS노드가 특정 노드를 중복해서 감시하는 것을 방지하기 위해 선택된 각각의 IDS 노드에 감시해야 할 노드를 배분하는 단계 (3.2 Allocation Problem)로 크게 구분된다.

3.1 IDS Node Selection

본 논문에서 제시하는 IDS 에이전트 배치 문제에 대한 모형은 다음과 같다.

$$\min \quad \sum_{j=1}^{n} c_j x_j$$

$$\text{s.t} \quad \sum_{j=1}^{n} a_{ij} x_j \geq 1 \quad i = 1, \ldots, n \quad \ldots(1)$$

$$x_j \in \{0,1\} \quad j = 1, \ldots, n$$

x_j : j번 노드의 IDS 에이전트 배치 여부

c_j : j번 노드의 선택에 대한 비용

a_{ij} : i번 노드와 j번 노드의 연결 가능 여부

n : 대상 네트워크 시스템의 노드의 수

위 제안된 모형은 전형적인 Set Covering Problem(SCP)의 formulation이다. x_j는 IDS 에이전트를 j번 노드에 배치할 경우 1, 아닐 경우 0을 값으로 갖는다. c_j는 일반적으로

SCP에서 j번 노드를 선택할 때 필요한 비용이다. 문제의 목적이 네트워크의 생존 기간 향상이므로 잔여 배터리양이 적은 노드의 선택을 피하기 위해 c_j에 j번 노드의 배터리 잔여량의 역수 값을 주었다. a_{ij}는 그림 2와 같이 송신하는 i번 노드 전송범위(transmission range)안에 있는 노드 j에 대해 1, 그렇지 않을 경우 0을 갖는다.

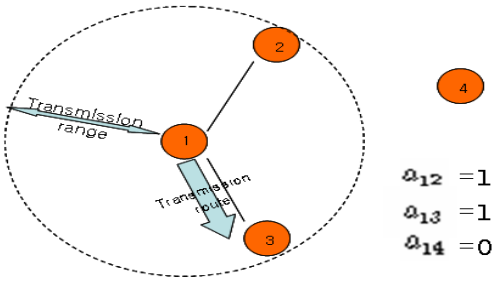

그림 2 무선 노드의 전송범위

위 모형에서 목적함수는 각 노드의 생존 기간을 고려하면서 IDS 에이전트 배치 노드수를 줄이는 것을 목표로 한다. 제약식은 IDS 에이전트 배치를 통해 전체 네트워크가 보호되어야 함을 의미한다.

3.2 Allocation Problem

IDS 에이전트 배치 노드를 선택한 후, 각 에이전트에게 어떤 노드들의 트래픽을 감시할 것인지 배분해주어야 한다. 각 에이전트에 노드를 배분하는 알고리즘은 다음과 같다.

S를 에이전트가 배치된 노드의 집합으로, L을 전체 노드의 집합이라 하자.

$S=\{i|x_i=1\}$ $L=\{1,...,n\}$

step 1. S의 원소 노드 중, 배터리 남은 양 (b_i) 이 가장 원소 k를 택한다.

$$k=\arg_i \max b_i$$

step 2. Ld를 k번 노드와 통신 가능한 노드 집합이라 하고. L에서 Ld를 뺀다.

$$L_d=\{j|a_{kj}=1 \quad \text{for all } j\}\ , \quad L=L-L_d$$

step 3. 집합 L의 원소가 남아있다면 step 2부터 반복하고 그렇지 않다면 종료한다.

$$\text{if } L=\{\ \} \text{ then } STOP \quad else \quad Goto \quad step2$$

위 알고리즘은 배치된 에이전트 중 배터리 잔여량이 큰 것 우선으로 노드를 배분한다. 이는 네트워크 생존 기간의 연장을 위해 배터리가 적은 노드에게 적은 양의 트래픽을 감시하도록 하기 위함이다.

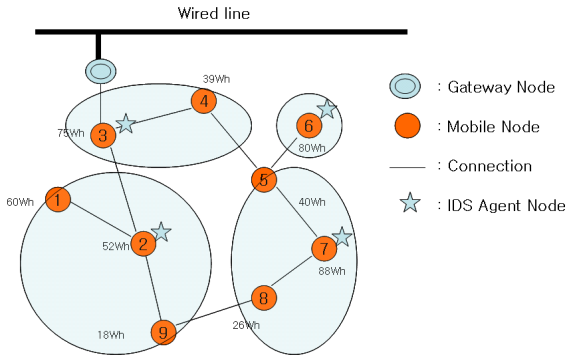

그림 3 제안된 IDS 배치 방안의 예

4. Simulation

4.1 Performance Measure

에이전트가 설치된 노드는 각 에이전트에 배분된 노드들의 패킷 트래픽을 감시하고 분석한다. 에이전트 설치 노드의 사용에너지는 다음과 같이 나타낼 수 있다.

$$E = m^t s^t + m^r s^r + m^o s^o + m^m s^m + b \quad [3]$$

s^t, s^r, s^o, s^m 는 각각 송신, 수신, 도청, 감시를 위한 패킷 크기를 나타낸다. m은 단위 데이터 양 당 소모 에너지로 ms는 패킷 크기에 따른 변동비를, b는 에이전트 노드 운영을 위한 고정비를 의미한다. 이 에너지 수치를 이용하여 시뮬레이션을 통해 제안된 배치 알고리즘을 평가한다.

시뮬레이션은 9개의 노드가 연결된 그림3의 무선 메쉬 네트워크 토폴로지를 사용했으며, 다만 각 노드의 초기 배터리량은 동일하게 부여하였다.

4.2 Simulation Result and Evaluation

그림 4와 5은 트래픽량에 따른 네트워크의 생존기간과 네트워크의 어느 한 노드가 배터리를 전부 소모했을 때의 나머지 노드들의 잔여 배터리량의 합을 보여주고 있다.

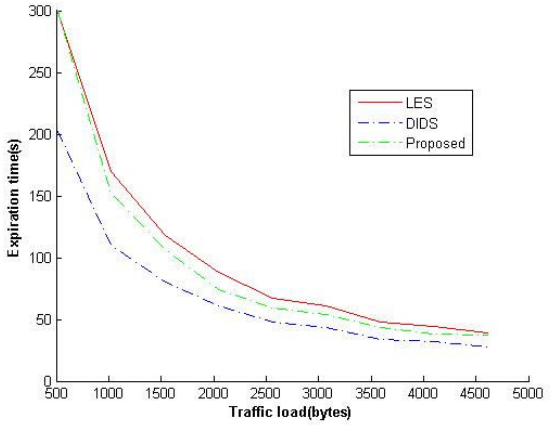

그림 4 네트워크 생존기간

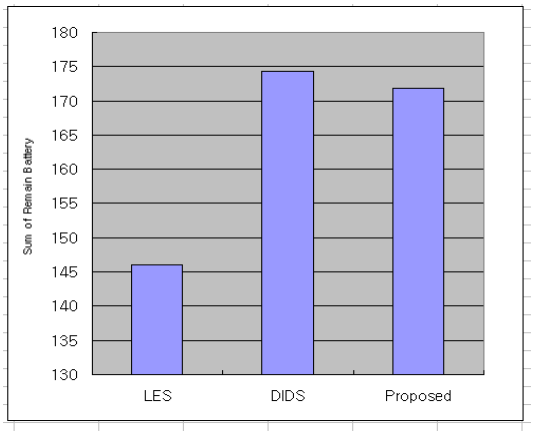

그림 5 네트워크의 배터리 잔여량

그림4에서 LES가 생존기간이 가장 길며, 제안 방안은 DIDS보다 평균 20% 정도 우수함을 보여주고 있다. 이는 DIDS의 경우 IDS 에이전트 설치를 위한 노드 선택을 전적으로 노드의 연결성을 기준으로 했기 때문에 연결성이 좋은 특정 몇몇 노드에 집중적으로 에이전트가 설치되었기 때문이다. 또한 LES는 노드의 잔여 배터리량만을 기준으로 IDS 에이전트를 설치했기 때문에 제안방안과 DIDS에 비해 우수한 생존기간을 가질 수 있지만 IDS의 효과성과 관련된 노드의 연결성은 고려하지 않음으로써 침입탐지 측면에서 효과적이지 못하다. LES는 많은 노드에 IDS 에이전트를 설치하기 때문에 전체 네트워크 측면에서 가장 많은 배터리를 소모한다. (그림5)

5. Conclusion and Future work

본 연구는 무선 메쉬 네트워크(Wireless Mesh Network)에서 효과적인 침입탐지 에이전트를 배치하는 운영 방안에 대해서 논하였다. 게이트웨이에서 노드들의 정보를 바탕으로 Set Covering Problem의 방법을 적용하여 IDS 에이전트의 배치를 계획하였다. 기존 연구결과들이(LES, DIDS) 각각 네트워크 생존 기간 증대 혹은 연결성기반 전체 에너지 소모량 최소화를 목적으로 하였다면 본 연구는 그 두 사항을 동시에 고려하는 개선된 알고리즘을 제안하였다. 실험 결과 제안 방안이 LES에 비해 생존기간이 짧지만, DIDS에 비해 평균 20% 정도 우수함을 볼 수 있었다.

차후 본 논문에서 보이지 못한 침입탐지 측면에서 추가적인 성능평가가 요구되며, 무선 메쉬 네트워크의 생존기간과 침입탐지 성능 측면에서 보다 개선된 알고리즘의 개발이 필요하다.

5. References

[1] Kachirshi O. and Guha R., "Effective Intrusion Detection using Multiple Sensors in Wireless Ad Hoc Networks," Proc. of the International Conference on System Sciences, Hawaii, 2003, pp. 57-64.

[2] Hyunwoo Kim, Dongwoo Kim, Sehun Kim, "Lifetime-enhancing Selection of Monitoring Nodes for Intrusion Detection in Mobile Ad Hoc Networks," Int. J. Electron. Common. (AEU) 60, 2006, pp. 248-250.

[3] Feeney LM, Nilsson M. "Investigating the energy consumption of a wireless network interface in an ad hoc networking environment." Proceedings of INFOCOM, Anchorage, 2001. p. 1548-.1557.

[4] Ashish Raniwala, Tzi-cker Chiueh "Architecting a HighCapacity Last-Mile Wireless Mesh Network"