Journal of The Korea Society of Computer and Information
Vol. 21 No. 1, pp. 73-78, January 2016
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2016.21.1.073

Selection of Monitoring Nodes to Maximize Sensing Area in Behavior-based Attack Detection

Kyun-Rak Chong*

Abstract

In wireless sensor networks, sensors have capabilities of sensing and wireless communication, computing power and collect data such as sound, movement, vibration. Sensors need to communicate wirelessly to send their sensing data to other sensors or the base station and so they are vulnerable to many attacks like garbage packet injection that cannot be prevented by using traditional cryptographic mechanisms. To defend against such attacks, a behavior-based attack detection is used in which some specialized monitoring nodes overhear the communications of their neighbors(normal nodes) to detect illegitimate behaviors. It is desirable that the total sensing area of normal nodes covered by monitoring nodes is as large as possible. The previous researches have focused on selecting the monitoring nodes so as to maximize the number of normal nodes(node coverage), which does not guarantee that the area sensed by the selected normal nodes is maximized. In this study, we have developed an algorithm for selecting the monitoring nodes needed to cover the maximum sensing area. We also have compared experimentally the covered sensing areas computed by our algorithm and the node coverage algorithm.

▸ Keyword : Behavior-based attack detection, Wireless sensor network, Sensing area, Node coverage

I. Introduction

무선 센서 네트워크는 배터리를 사용해서 동작하는 작은 센싱 디바이스들로 이루어져있다. 이러한 센서들은 감지 기능과 무선 통신 기능, 컴퓨팅 파워 등을 가지고 있으며 특정 지역에서 소리, 움직임, 진동 같은 다양한 데이터를 수집해서 다른 센서 노드나 기지국으로 보낸다. 센서들은 수집 정보를 전달하기 위해 서로 무선 통신을 해야 하므로 공격에 취약한데 가비지 패킷 주입(garbage packet insertion) 같은 공격은 기존의 인증이나 암호화 같은 방식을 사용해서는 퇴치하기 어렵다[1, 2]. 이러한 공격을 막기 위해 최근에 행위 기반 공격 탐지가 제안되었는데 특정한 감시 노드(monitoring node)들이 전송되는 패킷을 스니핑(sniffing)하고 분석하는 공격 탐지 시스템 모듈을 실행시켜 이웃한 일반 노드(normal nodes)들의 행위가 합법적인지를 감시한다. 이러한 일반 노드는 그 감시 노드에 의해 커버(cover)된다고 하고, 감시 노드는 모니터링 기능을 수행하며, 일반 노드는 감지(sensing) 기능을 담당한다. 행위 기반 공격 탐지와 보고(behavior-based attack detection and reporting) 문제는 [3]에서 처음 정의 되었는데, 감시 노드에 의해 커버되는 일반 노드의 수(노드 커버리지)가 최대가 되게 관리 노드를 포함해서 K개의 연결된 감시 노드를 선택하는 문제로 NP-하드임을 증명하였고 이 문제를 위한 휴리스틱 알고리즘을 제안하였다.

무선 센서 네트워크에서 감지 효율성을 증가시키려면 감시 노드를 선택할 때 감시 노드에 의해 커버되는 일반 노드들이 감지할 수 있는 전체 영역의 면적이 커야 한다. 행위 기반 공격 탐지와 보고 문제와 관련된 기존의 연구[3-7]들은 노드 커버리지가 최대가 되도록 감시 노드들을 선택하고 있다. 그러나 이러한 방식의 감시노드 선택은 일반 노드가 감지할 수 있는 전체 영역이 최대가 되는 것을 보장하지 못한다. 그 이유는 감시 노드에 의해 커버되는 일반 노드들이 밀집되어 있으면 그 일반 노드들의 감지 영역이

• First Author: Kyun-Rak Chong, Corresponding Author: Kyun-Rak Chong
*Kyun-Rak Chong (chong@cs.hongik.ac.kr), Dept. of Computer Engineering, Hongik University
• Received: 2015. 07. 17, Revised: 2015. 10. 20, Accepted: 2015. 12. 30.
• This work was supported by 2014 Hongik University Research Fund.

중첩되기 때문에 전체 감지 영역의 면적이 작아지게 된다.

본 연구에서는 일반 노드들이 감지할 수 있는 영역의 면적이 최대가 되도록 정해진 수의 감시 노드를 선택하는 알고리즘을 개발하고, [3]에서 제안된 노드 커버리지가 최대가 되도록 감시 노드를 선택하는 그리디(greedy) 노드 커버리지 알고리즘과 감지 면적이 어떻게 차이가 나는지 실험을 통해 비교하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대해 살펴보고, 3장에서는 감지 면적이 최대가 되도록 감시 노드를 선택하는 행위 기반 공격 탐지 문제를 정의하고 제안된 알고리즘에 대해 기술한다. 4장에서는 실험 결과에 대해 분석하고, 5장에서 결론을 맺는다.

II. Related Works

행위 기반 탐지는 비정상적이거나 예상되는 행위로부터 벗어나는 경우를 관측하여 침입을 탐지하는 방법으로 여러 네트워크에서 사용되고 있다. 무선 센서 네트워크가 효과적으로 동작하기 위해서는 배치된 일반 노드(센서)들이 감지하는 전체 영역의 면적이 클수록 바람직한데, 기존의 연구[3-5]들은 행위 기반 공격 탐지에서 감시 노드를 선택할 때 노드 커버리지를 최대로 하는 방법들만 제안하고 있고 감지 영역은 고려하지 않고 있다. 최근에 센서들이 일반 노드로만 이루어져 있을 때 감지 영역이 최대가 되게 센서들을 선택하는 방법이 [8]에서 제안되었다.

무선 센서 네트워크에서 행위 기반 공격 탐지와 보고 문제는 [3]에서 연구되었는데, 이웃 노드의 행위가 합법적인지를 판단하기 위해 감시 노드들이 이웃 노드의 통신을 감청하게 된다. 이 연구에서는 정해진 K개의 감시 노드들을 사용해서 모든 일반 노드들을 커버하는 문제가 NP-하드임을 증명하였고, 일반 노드의 커버리지가 최대가 되게 K개의 연결된 감시 노드를 선택하는 그리디 휴리스틱 알고리즘과 최단 경로 트리를 사용하는 휴리스틱 알고리즘을 제안하고 있다. Dijkstra의 최단 경로 알고리즘을 사용하기 위해서는 가중 그래프를 생성해야하는데 [4]에서는 인접한 노드들이 중복되지 않게 간선에 비용을 할당하는 방법을 제안하였고, 어떤 최단 경로가 선택되면 새로 커버되는 노드의 수를 다시 계산하는 동적인 알고리즘을 제안하고 있다.

행위 기반 탐지가 성공적으로 동작하기 위해서는 수집된 정보들이 관심 지역에 배치된 다수의 감시 노드들로 이루어진 경로를 따라 관리 노드까지 전달이 가능하여야 한다. 그러므로 원하는 감시 노드의 연결 비율이 주어졌을 때 이를 달성하기 위해서 실제적으로 어느 정도의 감시 노드를 관심 지역에 배치해야 하는 지가 필요하게 된다. [5]에서는 [3]에서 정의된 행위 기반 공격 탐지 및 보고 문제를 확장하여 서로 다른 종류의 감시 노드와 일반 노드가 배치되었을 때 커버되는 일반 노드의 수가 최대가 되도록 주어진 수의 감시 노드를 선택하는 알고리즘을 개발하고, 감시 노드의 수와 전송 범위가 감시 노드의 연결 비율과 일반 노드의 커버리지에 어떤 영향을 미치는 지 실험을 통해 비교하였다.

무선 센서 네트워크에서 커버되는 감지 영역의 면적이 최대가 되게 센서들을 선택하는 방법이 [8]에서 제안되었는데, 이 연구에서는 센서들이 모두 일반 노드만으로 이루어져 있다고 가정하였다.

애드 혹 네트워크와 무선 메쉬 네트워크에서 행위 기반 탐지를 위해 감시 노드를 선택하는 알고리즘은 [2, 6, 7]에서 연구되었다.

애드 혹 네트워크에서 침입 탐지를 위한 시스템 구조가 [2]에서 제안되었는데 시스템 태스크를 수행하는 인사이더 노드와 통신만을 하는 아웃사이더 노드가 있다. 인사이더 노드는 침입 탐지 시스템(IDS) 실행이 가능한 노드(감시 노드)와 그렇지 않은 노드(일반 노드)가 있다. 실행 가능한 노드 중에서 IDS 실행을 하도록 선택되면 이 노드를 IDS 액티브라고 한다. 이 연구에서는 리소스의 제한이 주어졌을 때 인사이더 노드들이 최대한 커버되도록 IDS 실행가능 노드들 중에서 IDS 액티브 노드들을 선택하는 문제가 NP-하드임을 보이고, 이 문제가 정수 선형 계획법을 사용해서 해결 될 수 있음을 보였다. 또 이 문제를 해결하기 위한 근사 알고리즘과 인사이더가 고정되어 있지 않고 움직일 때 IDS 액티브 인사이더를 선택하는 휴리스틱을 제안하고 있다.

[6]에서는 [2]의 연구를 확장하여 인사이더 노드들이 작동 하지 않거나 악의적인 공격 등에 의해 동작이 정지될 때, 침입 탐지를 위한 방법을 제안하였다. 또 수학적 모델링을 통해 리소스 사용과 탐지 비율에 대한 정량적 분석을 하였고, 정수 선형 계획법을 사용하는 최적 알고리즘과 근사해 구하는 분산 알고리즘을 제안하고 있다.

무선 메쉬 네트워크에서 행위 기반 탐지는 [7]에서 연구되었다. 일반 노드와 감시 노드가 전송 범위 안에 위치하고 무선 주파수가 같은 채널에 맞추어져 있으면 서로 통신이 가능하게 되고, 일반 노드는 그 감시 노드에 의해 커버된다고 한다. 이 연구에서는 다채널에서 최대 커버리지 문제가 NP-하드임을 증명하였고, 정수 선형 계획법을 사용하는 최적 알고리즘을 제안하였다. 또 근사해를 구하기 위한 휴리스틱 알고리즘으로 선형 계획 라운딩을 기반으로 하는 확률적 라운딩과 결정적 라운딩 방법을 제안하고 있다.

유사한 연구로 무선 센서 네트워크에서 백본(backbone)을 구성하는 연구가 십여 년 전부터 수행되었는데 [9]에서는 그 동안 발표된 연구들을 그리드 기반, 클러스터 기반, CDS (Connected Dominating Set) 기반 등으로 분류하여 정리하였다.

III. Proposed Method

1. Problem Definition

무선 센서 네트워크는 그래프 G = (V, E)로 표현할 수 있는데 여기서 V는 센서 노드들의 집합이고 E는 통신 링크들의 집합이다. 배치된 두 센서의 거리가 전송 범위 안에 있으면 대응되는 두 센서 노드는 그래프 상에서 간선으로 연결된다. V 안에 있는 노드 중 일부 노드는 감시 노드로 사용되고 나머지는

일반 노드로 사용된다. 또 감시 노드 중에는 공격에 대한 정보를 수집하는 특별한 싱크 노드 s가 있으며 이 노드를 관리 노드라고 한다. 일반 노드는 수집한 정보를 감시 노드로 전송하고 이 정보는 감시 노드만으로 이루어진 경로를 따라 관리 노드에 전달된다.

임의의 노드 u에 대해 A(u)를 u와 인접한 노드들의 집합이라 한다. X를 노드들의 집합이라 할 때 X와 인접한 노드들의 집합 $A(X) = \bigcup_{u \in X} A(u)$이다. 임의의 노드 u에 대해 u가 감지할 수 있는 영역은 노드 u를 중심으로 반지름 r인 원으로 정의하며 R(u)로 표시한다. 여기서 r을 감지 범위(sensing range)라 한다. 노드 u, v가 있을 때 R(u)-R(v)는 노드 u의 감지 영역에서 노드 v의 감지 영역을 제외한 영역을 나타낸다. 노드의 집합 X가 있을 때 X에 의해 감지되는 영역은 X에 포함된 각 노드가 감지하는 영역의 합으로 $R(X) = \bigcup_{u \in X} R(u)$이다. 노드의 집합 X와 Y가 있을 때 R(X)-R(Y)는 X에 의해 감지되는 영역에서 Y에 의해 감지되는 영역을 제외한 영역이다.

감시 노드의 집합 X가 있을 때 X에 의해 커버되는 일반 노드들의 집합 C(X)는 $C(X) = \{ u \mid u \in A(X) \text{ and } u \notin X \} = A(X) - X$로 정의되고, X에 의해 커버되는 감지 영역은 R(C(X))로 표시한다. 또 감지 영역 R이 주어졌을 때 R의 면적은 area(R)로 표시한다.

행위 기반 공격 탐지에서 감지 영역을 최대로 하는 감시 노드 선택 문제는 최대 감시 노드의 수 K가 주어졌을 때,

$$\text{maximize } area(R(C(M)))$$

즉, 감시 노드의 집합 M에 의해 커버되는 일반 노드들이 감지할 수 있는 영역의 면적을 최대로 하는 $M \subseteq V$을 찾는 문제이다. 이 때 M에 의해 유도되는 서브그래프는 연결되어 있고, 관리 노드 s를 포함하며, $|M| \leq K$이다.

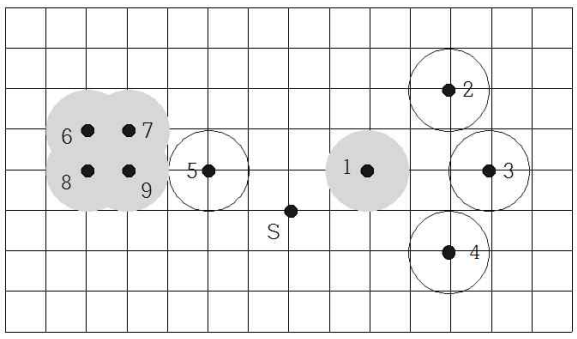


Fig. 1. An Example of Monitoring Nodes Selection

그림 1에 감지 영역의 면적이 최대가 되게 감시 노드를 선택하는 예가 나타나 있다. 이 예에서 각 그리드의 길이는 1, 전송 범위는 4, 감지 범위는 1이라고 가정한다. 검은 점들은 센서 노드이고 센서 노드 주위의 반지름 1인 원들이 각 센서 노드의 감지 영역이다. K = 2라고 가정하면 기존의 최대 노드 커버리지 알고리즘은 감시 노드로 {s, 5}를 선택하게 되고, 이 경우 커버되는 일반 노드는 {1, 6, 7, 8, 9}로 5개가 되지만, 이 노드들이 커버하는 감지 영역의 면적(회색으로 칠해진 원들의 면적의 합)은 4π보다 작게 된다. 제안된 알고리즘은 감시 노드로 {s, 1}를 선택하는데, 커버되는 일반 노드는 {2, 3, 4, 5}로 4개지만, 이 노드들이 커버하는 감지 영역의 면적은 4π가 된다.

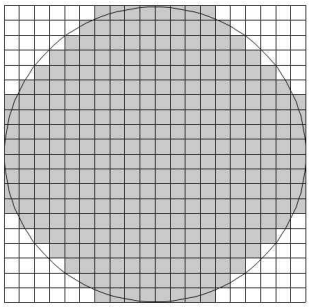


Fig. 2. An Approximation of Circle Area

각 센서들이 감지할 수 있는 영역은 원이 되는데, 여러 개의 원들이 겹쳐있을 때 이 원들의 겹쳐진 면적을 수학적으로 구하는 것은 어렵기 때문에 본 연구에서는 원의 면적을 원을 그리드 상에 투사한 근사값을 사용한다. 반지름이 10인 원의 면적은 약 314인데 근사값은 그림 2에서 회색으로 표시된 그리드의 면적의 합으로 316을 사용한다. 그림 2에서 각 그리드의 가로와 세로의 길이는 1이고 따라서 면적도 1이다.

2. Proposed Algorithm

제안 알고리즘은 일반 노드에 의해 감지되는 영역의 면적을 최대로 하기 위해 감시 노드를 선택할 때 새로 늘어나는 감지 면적이 가장 큰 노드부터 순차적으로 선택한다. 제안 알고리즘의 개요를 보면 다음과 같다. 감시 노드의 집합을 M이라 하면 초기에는 관리 노드 s만 M에 포함되어 있다. s를 제외한 나머지 노드는 모두 일반 노드가 되고 이 중 감시 노드로 선택된 노드는 순서대로 M으로 이동된다. 모든 감시 노드들은 그래프 상에서 연결 가능하여야 하므로 다음에 선택될 감시 노드는 이미 선택된 감시 노드들과 연결된 일반 노드 중에서 선택되어야 한다.

선택된 감시 노드들과 연결된 일반 노드의 집합을 N이라 하자. 초기에 N은 s에 연결된 일반 노드들로 구성되어 있다. N에 속한 노드 중에서 새로 커버되는 감지 영역이 최대가 되는 노드를 찾아 감시 노드로 사용한다. 즉 이 노드를 M에 추가하고 이 노드와 연결된 일반 노드들을 N에 추가 한다. 이 과정을 M의 크기가 K가 될 때까지 또는 더 이상 감지 영역을 새로 커버하는 노드가 없을 때까지 반복한다.

새로 커버되는 감지 영역은 다음과 같이 구한다. 노드 v가

감시 노드로 선택되면 A(v)에는 세 종류의 노드가 포함되어 있다.

(1) 감시 노드
(2) 이미 선택된 감시 노드(M)에 의해 커버된 일반 노드
(3) 노드 v에 의해 새로 커버되는 일반 노드

```
Maximal Sensing Area Algorithm
{
    M = {s};
    N = A(s);
    while (|M| < K)  {
        max = 0;
        for (each v in N-M) {
            if (area(R(A(v)-M)-R(C(M)))>max) {
                u = v;
                max = area(R(A(v)-M)-R(C(M)));
            }
        if (max) {
            M = M ∪ {u};
            N = N ∪ A(u);
        }
        else break;
    }
    return M, area(R(C(M)));
}
```

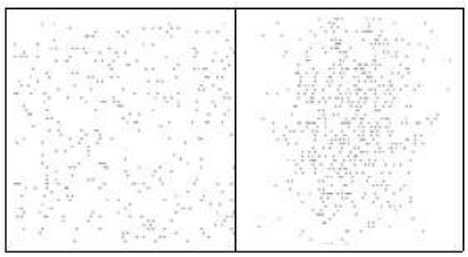
Fig. 3. The Maximal Sensing Area Algorithm

먼저 (1)의 감시 노드들은 감시 기능만을 수행하기 때문에 감지 영역의 계산에서는 제외시킨다. (3)의 일반 노드 중에는 자신의 감지 영역 전체가 새로 추가되는 경우와 자신의 감지 영역의 일부가 (2)의 일반 노드의 감지 영역과 중첩되는 경우가 있다. 후자의 경우에는 중첩되는 감지 영역의 면적만큼을 제외시켜야 한다. 그러므로 노드 v에 의해 새로 커버되는 감지 영역은 v에 인접한 노드 중에서 감시 노드들을 뺀 영역에서 (2)의 일반 노드와 중첩된 감지 영역을 제외시키면 된다. 즉, R(A(v)-M)-R(C(M))이 된다.

그림 3에 제안된 알고리즘이 나타나 있다. 관리 노드 s를 포함해서 K 개의 감시 노드(M)을 다음과 같이 순차적으로 선택한다. 현재 M에 있는 감시 노드들과 연결된 일반 노드(N-M)들 중에서 감시 노드로 선택되었을 때, 이 감시 노드와 연결된 일반 노드들이 감지하는 영역(R(A(v)-M))에서 이미 M에 의해 커버된 다른 일반 노드들이 감지하고 있는 영역(R(C(M)))을 제외한, 즉 새로 늘어나는 감지 영역이 가장 큰 일반 노드부터 선택해서 M에 추가한다. 다음 M에 연결된 노드들을 N에 추가하고 이 과정을 반복한다.

IV. Performance Evaluation

성능 평가는 본 연구에서 제안된 알고리즘이 그리디 스타일이므로, [3]에서 제안된 그리디 노드 커버리지 알고리즘이 구한 일반노드들의 감지 면적의 합과 본 연구에서 제안된 알고리즘이 구한 일반 노드들의 감지 면적의 합을 임의로 생성된 다양한 데이터를 가지고 비교하였다. 실험을 위해 두 알고리즘은 C 언어를 사용해서 Intel(R) Core(TM) 2 CPU를 가진 PC에서 구현되었다. 성능 비교를 위한 실험 데이터는 다음과 같이 임의로 생성하였다. 처음에 1000개의 센서를 1000 x 1000 정방형 필드에 배치하였고, 노드의 전송 범위(t)는 50을 사용하였다. 다양한 실험을 위해 감시 노드의 수 K는 50, 100, 200을 사용하였고, 일반 노드의 감지 범위(r)는 30, 40, 50, 60, 70을 사용하였다. 무선 센서 네트워크에서 센서의 배치 분포로 포아송 분포와 가우스 분포가 주로 사용되고 있는데, 포아송 분포는 센서가 영역 전체에 걸쳐 배치되는 특성을 가지고 있고, 가우스 분포는 영역의 중심 부근에 많이 분포되는 특성을 가지고 있다 [10, 11]. 그림 4에 두 분포의 예가 나타나 있다. 본 연구에서도 실험을 위해 두 분포를 사용하였다. 포아송 분포에서는 배치 영역의 넓이가 A이고 센서의 수가 N이라고 하면 밀도 $\lambda = N/A$인 포아송 분포를 따른다 [10]. 그러므로 실험에서는 1000 X 1000 영역에 1000개의 센서를 임의 배치하였으므로 $\lambda = 1/1000$이 된다. 가우스 분포에서는 평균 u = 500, 표준편차 $\sigma = u/3$을 사용하여 센서들을 임의 배치하였다.



(a) Poisson (b) Gauss
Fig. 4. An Example of Sensor Deployment under Poisson Distribution and Gauss Distribution

1. Poisson Distribution

센서들이 포아송 분포를 따라 배치되었을 때의 결과를 보면, 그림 5에 그리디 노드 커버리지 알고리즘[3]이 커버한 전체 영역의 면적을 1이라고 했을 때 제안한 알고리즘이 커버한 전체 면적의 상대 비율이 그래프로 나타나 있다. 모든 K 값과 감지 범위에 대해 제안한 알고리즘이 커버한 감지 영역의 면적이 더 큼을 알 수 있다.

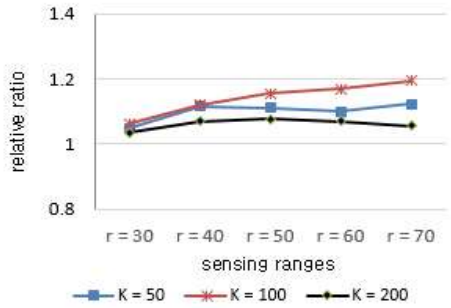


Fig. 5. The relative result comparison of the proposed algorithm and the maximal node coverage algorithm under the Poisson distribution

감지 면적의 상대 비율을 보면 제안 알고리즘이 K=50일 때 평균 10.2% 우수하였고, K=100일 때 평균 14.6%, K=200일 때 평균 6.2% 우수하였다. 그러므로 K 값 전체에 대한 평균 증가 비율은 10.3%이었고, 최대 증가 비율은 K=100, r=70일 때로 19.5% 증가하였다.

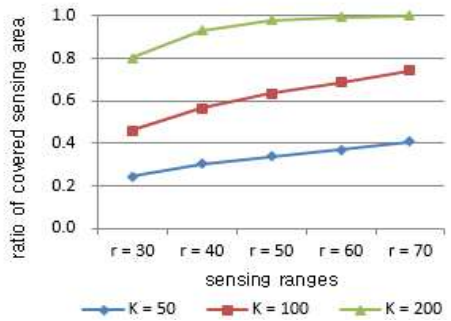


Fig. 6. The ratio of covered sensing area computed by the proposed algorithm under the Poisson distribution

그림 6에 각 K 값과 r에 대해 본 논문에서 제안된 알고리즘이 센서들이 배치된 1000x1000 필드 중에서 커버한 감지 면적의 비율이 나타나 있다. K 값에 관계없이 센서의 감지 범위가 증가함에 따라 커버한 영역의 면적도 증가함을 보이고 있다. K=50일 때는 평균적으로 전체 면적의 33.3%를 커버하였고, K=100일 때는 61.8%, K=200일 때는 94.1%를 커버하였다. 실험 결과를 보면 커버되는 영역의 면적이 감시 노드의 수에 거의 선형으로 비례함을 알 수 있다. 또 감지 범위가 클수록 커버되는 감지 영역이 넓어짐을 보여주고 있다.

2. Gauss Distribution

센서들이 가우스 분포를 따라 배치되었을 때의 결과를 보면, 그림 7에 그리디 노드 커버리지 알고리즘[3]이 커버한 감지 영역의 면적을 1이라고 했을 때 제안한 알고리즘이 커버한 감지 면적의 상대 비율이 그래프로 나타나 있다. K 값이 50과 100일 때는 모든 감지 범위에 대해 제안한 알고리즘이 커버한 감지 영역의 면적이 더 큼을 알 수 있다. K 값이 200일 때는 두 알고리즘이 커버한 감지 영역의 면적에 별 차이가 없었다.

감지 면적의 상대 비율을 보면 제안 알고리즘이 K=50일 때 평균 21.7% 우수하였고, K=100일 때 평균 12.4% 우수하였다. 그러므로 K 값 전체에 대한 평균 증가 비율은 11.3%이었고, 최대 증가 비율은 K=50, r=70일 때로 27.1% 증가하였다. 포아송 분포에서는 제안 알고리즘의 결과가 K=100일 때 가장 우수하였는데, 가우스 분포에서는 K=50일 때 가장 우수하였다.

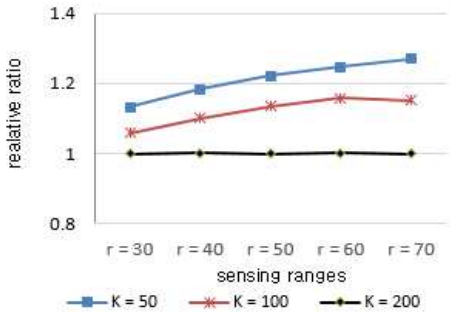


Fig. 7. The relative result comparison of the proposed algorithm and the maximal node coverage algorithm under the Gauss distribution

그림 8에 각 K 값과 r에 대해 본 논문에서 제안된 알고리즘이 센서들이 배치된 1000x1000 필드 중에서 커버한 감지 면적의 비율이 나타나 있다. 포아송 분포와 마찬가지로 K 값에 관계없이 감지 범위가 증가함에 따라 커버한 영역의 면적도 증가함을 보이고 있다. K=50일 때는 평균적으로 전체 면적의 38.8%를 커버하였고, K=100일 때는 55.0%, K=200일 때는 55.8%를 커버하였다. 실험 결과를 보면 K 값을 100에서 200으로 증가시켜도 커버되는 영역은 별로 늘어나지 않음을 보이고 있다. 그 이유는 가우스 분포에서는 영역의 중앙을 중심으로 센서들이 배치되기 때문에 감시 노드의 수를 증가시켜도 새로 늘어나는 영역은 제한적이기 때문이다.

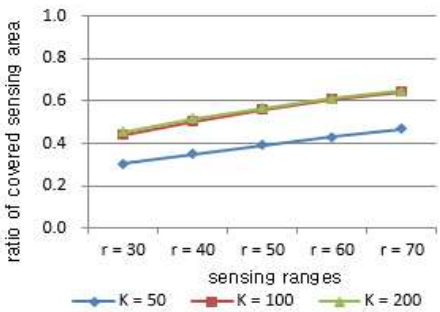


Fig. 8. The ratio of covered sensing area computed by the proposed algorithm under the Gauss distribution

V. Conclusion

무선 센서 네트워크에서 센서들은 다양한 환경적 물리적 데이터를 수집한 후 무선 통신을 사용해서 관리 노드로 보내기 때문에 네트워크 공격에 취약한데 이런 공격을 막기 위해서 보통 사용하는 기법이 행위 기반 공격 탐지이다. 행위 기반 공격 탐지에서는 일반 노드들 중에서 이웃의 불법 행위를 탐지하는 감시 노드들을 선택하는데 기존의 방법들은 커버되는 일반 노드들의 수가 최대가 되게 선택하고 있고 일반 노드들이 감지할 수 있는 전체 영역의 면적은 고려하지 않고 있다 .

본 연구에서는 전체 감지 영역의 면적이 최대가 되게 감시 노드를 선택하는 알고리즘을 개발하였고, 노드 커버리지 알고리즘과 실험을 통해 커버되는 전체 감지 면적의 크기를 비교하였다. 실험 결과를 보면 제안 알고리즘이 커버하는 전체 감지 영역의 면적이 기존 알고리즘에 비해 더 넓은 것으로 나타났고, 제안된 알고리즘은 행위 기반 탐지에서 감지 효율성을 향상시킬 것으로 기대된다. 향후 센서들의 에너지 소모와 네트워크 커버리지를 고려하는 연구가 진행될 예정이다.

REFERENCES

[1] A. Stetsko, L. Folkman and V. Matyas, “Neighbor-based Intrusion Detection for Wireless Sensor Networks,” Proceedings of 6th International Conference on Wiress and mobile Communications, pp.420-425, 2010

[2] D. Subhadrabandhu, S. Sarkar, and F. Anjum,“A framework for misuse detection in adhoc networks-part I,” IEEE Journal on Selected Areas in Communications, Special Issue on Security in Wireless Ad Hoc Networks, Vol.24, No.2, pp.274-289, 2006

[3] Y. Liu and K. Han, “Behavior-based Attack Detection and Reporting in Wireless Sensor Networks,” Proceedings of the third International Symposiums on Electronic Commerce and Security, pp. 209-212, 2010

[4] K. Chong, “An Improved Algorithm using Shortest Path Tree for Behavior-based Attack Detection and Reporting Problem in Wireless Sensor Networks,” Journal of KIISE : Information Networking, vol. 39, no. 4, pp.365-370, August 2012

[5] K. Chong, “Analysis of the Connectivity of Monitoring Nodes annd the Coverage of Normal Nodes for Behavior-based Attack Detection in Wireless Sensor Networks,” Journal of KSCI, vol. 18, no.12, pp. 27-34, 2013

[6] D. Subhadrabandhu, S. Sarkar, and F. Anjum,“A framework for misuse detection in adhoc networks-part II,” IEEE Journal on Selected Areas in Communications, Special Issue on Security in Wireles Ad Hoc Networks, Vol.24, No.2, pp.290-304, 2006

[7] D.-H. Shin and S. Bagchi, “Optimal monitoring in multi-channel multi-radio wireless mesh network,” Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing(Mobihoc), pp. 229-238, 2009

[8] V. Gupta, K. Kapoor and D. S. Renuga, “Wireless Sensor Node Selection Strategies for Effective Surveillance,” IEEE International Advanced Computing Conference, pp. 924-929, 2015

[9] R. Asgarnezhad and J. A. Torkestani, “A Survey on Backbone Formation Algorithms for Wireless Sensor Networks,” Australian Telecommunication Network and Applications pp. 1-4, 2011

[10] U. Wang, M. Wilkerson, and X. Yu, “Hybrid Sensor Deployment for Surveillance and Target Detection in Wireless Sensor Networks,” IEEE , 2011

[11] Y. Wang and Z lun, “Impact of Deployment Point Arrangement on Intrusion Detection in Wireless Sensor Networks,” 18th Annual IEEE/ACM Intl. Symp. on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, pp. 421-423, 2010

Authors

Kyun Rak Chong received the B.S. degree in computer science and statistics from Seoul national university, Korea, in 1978, the M. S. degree in computer science from Korea advanced institute and technology, Korea, in 1980, and the Ph.D. degree in computer science from the university of Minnesota, Minneapolis, in 1991. He is currently a professor in the department of computer engineering, Hongik University. In 1998 and 2006, he visited the department of computer information science and engineering, university of Florida, Gainesville. His research interests include network algorithms, wireless sensor networks, public-shared networks, and parallel machine scheduling.