Journal of The Korea Society of Computer and Information
Vol. 18, No. 12, December 2013
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2013.18.12.027

무선 센서 네트워크에서 행위 기반 공격 탐지를 위한 감시 노드의 연결성과 일반 노드의 커버리지 분석

정 균 락*

Analysis of the Connectivity of Monitoring Nodes and the Coverage of Normal Nodes for Behavior-based Attack Detection in Wireless Sensor Networks

Kyun-Rak Chong*

요 약

무선 센서 네트워크에서 센서들은 획득한 정보를 관리 노드로 전달하기 위해 서로 통신을 해야 하므로 공격에 취약한데 쓰레기 패킷 주입 같은 공격은 기존의 암호화 같은 방식을 사용해서는 퇴치하기 어렵다. 그래서 행위 기반 탐지가 대두되었는데 특정 감시 노드들이 이웃한 일반 노드의 통신을 감청하여 불법적인 패킷을 탐지하게 된다. 감시 노드들은 일반 노드들에 비해 더 많은 에너지를 사용하기 때문에 최소의 감시 노드들로 전체 또는 최대한 넓은 범위의 네트워크를 커버하는 것이 필요하다. 감시 노드는 일반 노드 중에서 선택될 수도 있고 일반 노드와 서로 다른 종류일 수도 있다. 본 연구에서는 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.

▸ Keywords : 행위 기반 공격 탐지, 무선 센서 네트워크, 센서 배치

Abstract

In wireless sensor networks, sensors need to communicate with each other to send their sensing data to the administration node and so they are susceptible to many attacks like garbage packet injection that cannot be prevented by using traditional cryptographic approaches. A behavior-based detection is used to defend against such attacks in which some specialized monitoring nodes

•제1저자 : 정균락 •교신저자 : 정균락
•투고일 : 2013. 9. 25, 심사일 : 2013. 10. 29, 게재확정일 : 2013. 11. 25
* 홍익대학교 컴퓨터공학과 (Dept. of Computer Engineering, Honglk University)
※ 이 논문은 2012학년도 홍익대학교 학술연구진흥비에 의하여 지원되었음

overhear the communications of their neighbors to detect bad packets. As monitoring nodes use more energy, it is desirable to use the minimal number of monitoring nodes to cover the whole or maximal part of the network. The monitoring nodes can either be selected among the deployed normal nodes or differ in type from normal nodes. In this study, we have developed an algorithm for selecting the predefined number of monitoring nodes needed to cover the maximum number of normal nodes when the different types of normal nodes and monitoring nodes are deployed. We also have investigated experimentally how the number of monitoring nodes and their transmission range affect the connection ratio of the monitoring nodes and the coverage of the normal nodes.

▸ Keywords : behavior-based attack detection, wireless sensor network, sensor deployment

I. 서 론

무선 센서 네트워크는 물리적 또는 환경적인 상태들을 감시하기 위해 관심 지역에 배치된 다량의 센서들로 이루어져 있으며 환경 감시, 재난 관리, 침입 탐지, 전쟁지역 경계 등 응용 분야가 매우 다양하다. 센서들은 획득한 정보를 전달하기 위해 서로 통신을 해야 하므로 공격에 취약한데 쓰레기 패킷 주입 같은 공격은 기존의 인증이나 암호화 같은 방식을 사용해서는 퇴치하기 어렵다[1, 2, 3]. 그래서 행위 기반 탐지가 대두되었는데 특정 감시 노드(monitoring node)들이 전송되는 패킷을 스니핑(sniffing)하고 분석하는 공격 탐지 시스템 모듈을 실행시켜 이웃한 일반 노드(normal nodes)들의 전송 패킷이 합법적인지를 판단하게 된다. 감시 노드들은 일반 노드들에 비해 더 많은 에너지를 사용하기 때문에 최소의 감시 노드들로 전체 또는 최대한 넓은 범위의 네트워크를 커버하는 것이 필요하고 또 공격이 탐지되면 신뢰할 수 있는 감시 노드들로 이루어진 경로를 따라 관리 노드로 보고하는 것이 필요하다[4].

무선 센서 네트워크나 애드 혹 네트워크에서 감시 노드들은 먼저 일반 노드들을 임의로 배치하고 이 중에서 감시 노드를 선택하는 방법[4, 5]과 처음부터 성능이 다른 일반 노드와 감시 노드를 구분해서 배치하는 방법이 있다[6, 7, 8]. [4]에서는 무선 센서 네트워크에서 행위 기반 공격 탐지 및 보고 문제를 정의하고 휴리스틱 알고리즘을 제안하였는데, 여기서는 일반 노드들을 임의로 배치하고 이 중에서 일부 노드를 선택해서 감시 노드로 사용하였다. 애드 혹 네트워크에서 공격 탐지를 위한 체계가 [7]에서 제안되었는데, 두 종류의 인사이더 노드를 사용한다. 인사이더 노드는 IDS(intrusion detection system) 실행이 가능한 노드가 감시 노드이고, 가능하지 않은 노드가 일반 노드이다.

행위 기반 탐지가 성공적으로 동작하기 위해서는 관심 지역에 배치된 다수의 감시 노드들이 관리 노드까지 감시 노드들로 이루어진 경로를 따라 통신이 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. 또 성능이 다른 두 종류의 감시 노드와 일반 노드를 배치하는 경우에는 감시 노드는 일반 노드에 비해 네트워크 자원을 많이 사용하므로 프로세싱 파워, 배터리 지속 시간, 전송 범위 등 성능이 좋은 센서를 사용하게 되는데 감시 노드의 전송 범위는 감시 노드의 연결 비율에 직접적인 영향을 주게 된다.

본 연구에서는 [4]에서 정의된 행위 기반 공격 탐지 및 보고 문제를 확장하여 두 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. 또 무선 센서 네트워크 애플리케이션에서에서 성능 평가를 위한 배치 모델은 포아송(Poisson) 분포나 가우스(Gauss) 분포가 많이 사용되고 있으므로 실험을 위한 데이터 생성은 포아송 분포와 가우스 분포를 사용하였다[9].

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대

해 살펴보고, 3장에서는 두 종류의 감시 노드와 일반 노드가 배치되었을 때 행위 기반 공격 탐지 문제를 정의하고 제안된 알고리즘에 대해 기술한다. 4장에서는 실험 결과에 대해 분석하고, 5장에서 결론을 맺는다.

II. 관련 연구

최근에 무선 센서 네트워크나 애드 혹 네트워크에서 침입 탐지에 관한 연구가 많이 진행되어 왔다. 무선 센서 네트워크에서 행위 기반 공격 탐지와 보고 문제는 [4]에서 연구되었는데, 이 문제가 NP-하드임을 증명하였고, 실험을 통해 최단 경로 트리를 사용하는 알고리즘이 그리디 알고리즘에 비해 효과적임을 보였다. 여기서는 일반 노드들을 임의로 배치하고 이 중에서 일반 노드의 커버리지가 최대가 되면서 관리 노드로부터 도달 가능한 K개의 일반 노드를 선택해서 감시 노드로 사용하였다. 최단 경로 알고리즘을 사용하기 위해서는 가중 그래프를 생성해야 하는데 제안된 알고리즘은 간선에 비용을 할당할 때 노드의 차수만 고려하여 인접한 노드의 일부가 중복되게 계산되는 문제점이 있고, 최단 경로를 선택할 때도 초기에 계산된 정적인 커버리지만 고려하는 단점을 가지고 있다. [5]에서는 이러한 단점을 개선하여 인접한 노드들이 중복되지 않게 간선에 비용을 할당하는 방법을 제안하였고, 최단 경로가 선택되면 커버리지를 다시 계산하여 다음 최단 경로를 선택하는 동적인 알고리즘을 제안하였다.

무선 메쉬 네트워크에서 행위 기반 탐지는 [6]에서 연구되었는데 이웃 노드의 행위가 합법적인지를 판단하기 위해 감시 노드들이 이웃 노드의 통신을 감청하게 된다. 일반 노드와 감시 노드가 서로 전송 범위 안에 위치하고 무선 주파수가 같은 채널에 맞추어져 있으면 감시 노드는 일반 노드의 행위가 합법적인지를 판단할 수 있게 되고 일반 노드는 그 감시 노드에 의해 커버된다고 한다. 감시 노드들은 일반 노드들에 비해 더 많은 에너지를 사용하기 때문에 네트워크 자원을 고갈시키고 결과적으로 네트워크 수명을 단축시키게 된다. 그러므로 최소의 감시 노드들로 전체 또는 최대한 넓은 범위의 네트워크를 커버하는 것이 필요하다. 이 연구에서는 다채널에서 최대 커버리지 문제를 정의하고 이 문제가 NP-하드임을 증명하였고, 정수 선형 계획법을 사용하여 최적해를 구하는 방법을 제시하였다. 선형 계획 라운딩을 기반으로 하는 확률적 라운딩 방법과 결정적 라운딩 방법을 제안하고 모의실험을 통해 그 결과를 비교하였다.

애드 혹 네트워크에서 악용 탐지를 위한 체계가 [7]에서 제안되었는데 탐지 시스템 구조로 패킷 전달과 루트 탐사와 같은 시스템 태스크를 수행하는 인사이더 노드와 네트워크상에서 통신만을 하는 아웃사이더 노드가 있다. 인사이더 노드는 침입 탐지 시스템(IDS) 실행이 가능한 데, 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, 근사 알고리즘과 인사이더가 고정되어 있지 않고 움직일 때 IDS 액티브 인사이더를 선택하는 휴리스틱을 제안하였다.

[8]에서는 [7]의 연구를 확장하여 인사이더 노드들이 작동 실패, 절전형 모드, 악의적인 공격 등에 의해 동작이 정지될 때, 침입 탐지를 위한 확률적 프레임워크를 개발하였다. 이 모델에서 인사이더는 동작 가능 상태와 동작 불가능 상태로 구분되며 동적으로 한 상태에서 다른 상태로 변할 수 있다. 또 주어진 침입 탐지 확률을 얻기 위해 각 인사이더는 다수의 IDS 액티브 인사이더에 의해 커버 되어야 하는 데 확률적 분석을 통해 이 값을 계산하였고, 정수 계획법을 사용하여 최적해를 구하는 방법과 근사해 구하는 분산 알고리즘을 제안하였다.

센서 배치에 관한 연구들도 많이 진행되어 왔는데, 무선 센서 네트워크에서 성능 평가를 위한 모델로서 센서의 분포는 포아송 분포나 가우스 분포가 주로 사용되고 있다. 포아송 분포는 균일한 Q◦S를 제공하고 가우스 분포는 센서들이 배치점을 중심으로 배치되기 때문에 더 효과적인 환경 감시나 이동 타겟 탐지를 위한 개선된 Q◦S를 제공한다.

[9]에서는 하이브리드 방식의 임의 센서 배치 방법을 제안하였는데 센서의 일부는 포아송 분포를 사용하여 배치하고 중요한 지점은 가우스 분포를 사용하여 배치한다. 다수의 배치점을 설정하여 각 배치점을 중심으로 센서를 배치하는 방법이 [10]에서 연구되었는데 배치점이 k개이고 센서의 수가 n개이면 각 배치점에 n/k개의 센서들을 가우스 분포에 따라 배치한다. 이를 위한 멀티 레벨 침입 모델을 제안하고 이론적 분석과 실험을 실시하였다.

고정적인 센서와 모바일 센서를 같이 배치하는 문제가 [11]에서 연구되었다. 모든 센서는 처음에 배치 지역에 임의로 산포되고 그 다음 모바일 센서들을 커버리지와 에너지 소모를 고려해서 최소 비용으로 이동시킨다. 멀티 라운드 센서 배치 방법이 [12]에서 제안되었는데 센서들을 직선 벨트를 따라 여러 번에 걸쳐 배치한다. 또 센서들의 목표 지점과 실제 안착된 지점에 대한 편차 정보가 없을 때에는 파일럿 배치를 제안하였는데 소수의 센서들을 실험적으로 배치한 후 실제 안착된 지점들의 분포를 조사하여 다음 라운드에서 나머지 센

서들을 배치하는 방법이다.

III. 문제 정의와 알고리즘

무선 센서 네트워크는 그래프 G = (V, E)로 표현할 수 있는 데 여기서 V는 센서(노드)들의 집합이고 E는 통신 링크들의 집합이다. V는 감시 노드들의 집합 V_M과 일반 노드들의 집합 V_N으로 이루어진다. 감시 노드는 전송되는 패킷을 스니핑하고, 공격 탐지 시스템 모듈을 실행시켜 이웃 노드들의 전송 패킷이 합법적인지를 판단한다. 또 감시 노드 중에는 공격에 대한 정보를 수집하는 특별한 싱크 노드 s가 있으며 이 노드를 관리 노드라고 한다. 일반 노드는 센싱한 정보를 감시 노드로 전송한다. 서로 다른 두 노드가 있을 때 두 노드의 거리가 두 노드의 전송 범위 중 최소값보다 작으면 두 노드는 간선으로 연결된다.

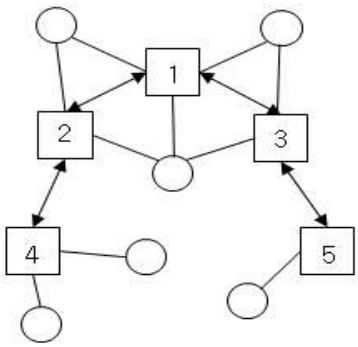


그림 1. 행위 기반 공격 탐지의 예
Fig. 1. An Example of the Behavior-based Attack Detection

임의의 감시 노드 u에 대해 AM(u)를 u와 인접한 감시 노드들의 집합이라 하고, AN(u)를 u와 인접한 일반 노드들의 집합이라 한다. X를 감시 노드들의 집합이라 할 때 X와 인접한 감시 노드들의 집합 $AM(X) = \bigcup_{u \in X} AM(u)$이고, X에 의해 커버되는 일반 노드들의 집합 $AN(X) = \bigcup_{u \in X} AN(u)$이다.

서로 다른 타입의 감시 노드와 일반 노드가 배치되었을 때 행위 기반 공격 탐지(BBAD) 문제는 최대 감시 노드의 수 K가 주어졌을 때, 다음을 만족하는 감시 노드 집합 $M \subseteq V_M$를 찾는 문제인데, M에 의해 유도되는 서브그래프는 연결되어 있다.

(1) $s \in M$,
(2) $|M| \leq K$
(3) $|AN(M)| + 1/|M|$이 최대

위의 조건에서 (1)은 관리 노드가 M에 속하고 M에 속한 감시 노드들로 이루어진 서브그래프가 연결되어 있으면 일반 노드에 의해 탐지된 정보가 감시 노드들로 이루어진 경로를 통해 관리 노드로 보고될 수 있음을 의미한다. (2)는 감시 노드의 최대 수가 관리 노드를 포함해서 K보다 작거나 같아야 하고, (3)은 커버할 수 있는 일반 노드의 수가 같은 두 개 이상의 M이 존재할 때는 M의 크기가 작은 집합을 선택하는 것이 네트워크 자원을 적게 소모하기 때문에 바람직함을 의미하고 있다[4].

그림 1에 BBAD 문제의 예가 나타나 있다. 여기서 사각형 노드가 감시 노드이고 그 중 관리 노드는 1번 노드이며 원형 노드가 일반 노드이다. K = 3이면 감시 노드 1, 2와 5번이 선택되고, 커버되는 일반 노드의 수는 5개가 된다.

그림 2에 제안된 알고리즘이 나타나 있다. 여기서 M은 선택된 감시 노드의 집합이고, N은 M에 의해 커버되는 일반 노드의 집합이다. 알고리즘의 개요를 보면 먼저 M에 관리 노드를 집어넣는다. 관리 노드와 연결된 감시 노드 중에서 새로 커버되는 일반 노드의 수가 최대가 되는 감시 노드를 선택해서 M에 추가한다. 그 다음 M에 포함된 감시 노드와 연결된 감시 노드 중에서 새로 커버되는 일반 노드의 수가 최대가 되는 감시 노드를 선택해서 M에 추가한다. 이 과정을 선택된 감시 노드의 수가 K가 되거나 더 이상 새로 커버되는 일반 노드가 없을 때까지 반복한다.

이 방법은 현재 고려중인 감시 노드 중에서 새로 커버되는 일반 노드가 없으면 감시 노드의 수가 K 개가 되지 않았는데도 알고리즘이 종료되게 된다. 그림 1의 예에서 K = 4라고 하면 먼저 감시 노드 1번이 선택되고 이 노드와 연결된 3개의 일반 노드가 커버된다. 그 다음 감시 노드 1번과 연결된 감시 노드 2번과 3번을 보면 새로 커버되는 일반 노드가 하나도 없으므로 알고리즘은 감시 노드 1번만 선택하고 종료하게 된다.

제안 알고리즘은 이러한 경우 한 단계 더 나아가서 감시 노드 2번과 3번에 연결된 감시 노드 4번과 5번 중에서 새로 커버되는 일반 노드가 더 많은 4번 노드를 선택하는데 감시 노드는 모두 연결되어야 하므로 감시 노드 2번도 같이 선택한다. 감시 노드 3번은 선택되더라도 새로 커버되는 일반 노드가 없고, K = 4이므로 감시 노드 3번과 5번을 모두 선택할 수는 없으므로 알고리즘이 종료된다. 그러므로 모두 3개의 감시 노드가 선택된다.

그림 2의 알고리즘에서 parent(i)는 감시 노드 i와 연결되

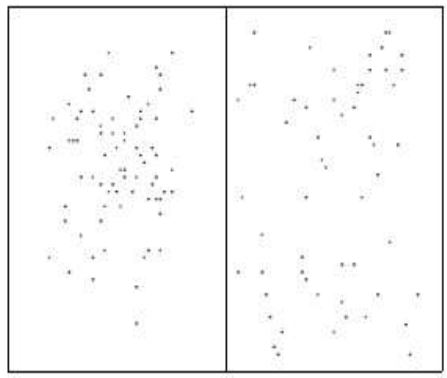
어 있는 부모 감시 노드를 가리킨다. 부모 감시 노드가 여러 개 일 경우에는 첫 번째 만나는 부모 감시 노드를 가리킨다. 알고리즘에서 변수 pair가 참이면 현재 선택된 감시 노드 v와 v의 부모 감시 노드를 같이 선택한다.

IV. 실험 결과 및 분석

제안된 알고리즘은 C 언어를 사용해서 Intel(R) Core(TM) 2 CPU를 가진 PC에서 구현되고 실험되었다. 센서 노드는 감시 노드와 일반 노드 두 종류를 1000 x 1000 정방형 필드에 배치하는데 일반 노드의 수는 1000개를 사용하였고, 감시 노드의 수는 100부터 500까지 100개씩 증가시키면서 실험하였다.

```
BBAD Algorithm
{
   M = {s};
   C = {s} ∪ AM{s};
   N = AN(s);
   pair = false;
   while (|M| < K and |N| < |V_N|) {
      Let v be the node in V_M-M and in C
      such that |AN(v)-N|>0 is maximum;
      if (v exists) {
         if (pair) {
            P = {parent(v)};
            pair = false;
         }
         else P = ∅;
         M = M ∪ {v} ∪ P;
         C = C ∪ {v} ∪ AM(v)∪ P;
         N = N ∪ AN(v);
      }
      else {
         if (pair || (|M| ≥ K-1) break;
         pair = true;
         for (each v in V_M-M and in C)
            for (each u in AM(v) and
                  not in C) {
               C = C ∪ {u};
               parent(u) = v;
            }
      }
   }
   return M;
}
```

그림 2. BBAD 알고리즘
Fig. 2. BBAD Algorithm



(a) 가우스분포 (b) 포아송분포
그림 3. 센서 배치의 예
(a) Gauss Dist. (b) Poisson Dist.
Fig. 3. Sensor Deployment Example

일반 노드의 전송 범위(t)는 50이라 하고, 감시 노드의 전송 범위는 일반 노드의 1배부터 4배까지를 사용하였다. 각 감시 노드의 수와 전송 범위에 대해 데이터를 임의로 10개씩 총 200개를 생성하여 실험하였다. 두 감시 노드의 거리가 전송 범위 안에 있으면 서로 통신을 할 수 있다고 가정한다. 감시 노드와 일반 노드는 두 노드의 거리가 일반 노드의 전송 범위 안에 있으면 통신 가능하다.

센서 노드의 분포는 포아송 분포와 가우스 분포를 사용하였다. 그림 3에서 보는 바와 같이 가우스 분포는 평균 주변에 많은 노드들이 분포하기 때문에 대부분의 노드들이 중앙에 모여 있게 되고 반면에 포아송 분포에서는 노드들이 배치 영역 전체에 널리 퍼져 분포하게 된다. 그러므로 분포에 따라 연결 가능한 감시노드의 수와 커버되는 일반 노드의 수가 많이 달라진다.

1. 포아송 분포

포아송 임의 배치 모델은 배치 영역의 넓이가 A이고 센서 노드의 수가 N이라고 하면 밀도 $\lambda = N/A$인 포아송 분포를 따른다 [9]. 그러므로 실험에서는 1000 X 1000 영역에 1000개의 센서를 배치하였으므로 $\lambda = 1/1000$이 된다.

감시 노드들이 일반 노드로부터 획득한 정보를 관리 노드로 전달하기 위해서는 관리 노드와 감시 노드들이 연결되어 있어야 한다. 배치 영역에 감시 노드를 산포하면 어떤 감시 노드들은 다른 감시 노드들과의 거리가 전송 범위를 벗어나 고립되게 된다. 그러므로 공격 탐지 시스템이 성공적으로 동작하기 위해서는 배치된 전체 감시 노드의 수에 대한 연결된 감시 노드들의 수의 비율이 중요하게 된다. 표 1에 배치된 감시 노드의 수와 전송 범위에 대한 감시 노드의 연결 비율(%)

이 나타나 있다. 여기서 M은 배치된 감시 노드의 수이고 P는 전송 범위이다. 감시 노드의 전송 범위가 t일 때는 감시 노드의 수와 관계없이 전체적으로 감시 노드의 연결 비율이 매우 낮은 것을 알 수 있다. 이 표에서 보면 감시 노드의 연결 비율이 약 99% 정도가 되게 하기위해서는 전송 범위가 2t인 감시 노드를 약 300개 정도 산포하거나 전송 범위가 3t인 감시 노드를 200개 정도 산포하면 된다. 그러므로 감시 노드들의 가격이 주어지면 총비용이 최소가 되는 경우를 선택할 수 있다.

표 2에 감시 노드의 수와 감시 노드의 전송 범위에 따른 커버된 일반 노드의 비율(%)이 나타나 있다. 전송 범위가 t일 때는 감시 노드의 수가 증가해도 일반 노드의 커버율이 매우 낮은 것을 알 수 있다. 또 전송 범위가 2t에서 3t가 되면 감시 노드의 수가 100일 때는 일반 노드의 커버율은 약 39%, 200일 때는 약 6%가 향상되었고, 감시 노드의 수가 300이상일 때는 일반 노드의 커버율은 1%미만 향상되었다. 또 전송 범위가 3t에서 4t가 되면 감시 노드의 수에 관계없이 일반 노드의 커버율은 별로 향상되지 않았다.

2. 가우스 분포

본 실험에서는 평균 u = 500, 표준편차 σ = u/3인 가우스 분포에 따라 감시 노드와 일반 노드들을 임의 배치하였다. 표 3에 가우스 분포에서 감시 노드의 수와 전송 범위에 대한 감시 노드의 연결 비율이 나타나 있다. 이 표에서 보면 전송 범위가 t이고 감시 노드의 수가 100인 경우를 제외하고는 감시노드의 연결 비율이 70%이상임을 알 수 있다. 감시 노드의 연결 비율이 약 99%가 되게 하기위해서는 전송 범위가 2t인 감시 노드를 약 400개 정도 산포하거나 전송 범위가 3t인 감시 노드를 약 100개 정도 산포하면 된다.

표 1. 포아송 분포에서 감시 노드의 수와 전송 범위에 대한 감시 노드의 연결 비율
Table 1. The connection ratio of the monitoring nodes under the Poisson distribution

	M=100	M=200	M=300	M=400	M=500
P = t	1.8	2.4	3.0	6.4	15.0
P = 2t	20.4	93.8	99.4	99.9	100.0
P = 3t	96.0	100.0	100.0	100.0	100.0
P = 4t	99.8	100.0	100.0	100.0	100.0

표 2. 포아송 분포에서 감시 노드의 수와 전송 범위에 대한 일반 노드의 커버율
Table 2. The coverage ratio of the normal nodes under the Poisson distribution

	M=100	M=200	M=300	M=400	M=500
P = t	0.8	1.6	2.8	6.1	14.6
P = 2t	10.2	72.4	88.2	94.4	97.1
P = 3t	49.0	78.1	89.0	94.6	97.1
p = 4t	51.4	78.1	89.0	94.6	97.1

표 3. 가우스분포에서 감시 노드의 수와 전송 범위에 대한 감시 노드의 연결 비율
Table 3. The connection ratio of the monitoring nodes under the Gauss distribution

	M=100	M=200	M=300	M=400	M=500
P = t	29.6	73.3	82.8	86.5	89.7
P = 2t	92.0	96.8	98.2	98.9	99.2
P = 3t	98.8	99.7	99.7	99.8	100.0
p = 4t	99.8	100.0	100.0	100.0	100.0

표 4. 가우스 분포에서 감시 노드의 수와 전송 범위에 대한 일반 노드의 커버율
Table 4. The coverage ratio of the normal nodes under the Gauss distribution

	M=100	M=200	M=300	M=400	M=500
P = t	30.7	73.6	82.4	86.5	89.7
P = 2t	76.5	88.2	92.3	94.5	96.0
P = 3t	78.4	89.2	92.8	94.9	96.3
p = 4t	78.5	89.3	92.9	94.9	96.3

표 4에 감시 노드의 수와 감시 노드의 전송 범위에 따른 커버된 일반 노드의 비율이 나타나 있다. 전송 범위가 t이고 감시 노드의 수가 100인 경우를 제외하고는 일반 노드의 커버율이 일반적으로 높은 것을 알 수 있다. 전송 범위가 t에서 2t가 되면 감시 노드의 수가 100일 때는 일반 노드의 커버율은 약 46%, 200일 때는 약 15%가 향상되었고 300이상일 때는 6%에서 10% 정도 향상되었다. 또 전송 범위가 2t에서 3t가 되면 일반 노드의 커버율은 최대 2%정도 향상되었고, 전송 범위가 3t에서 4t가 되면 포아송 분포와 마찬가지로 감시 노드의 수에 관계없이 일반 노드의 커버율은 별로 향상되지 않았다.

가우스 분포와 포아송 분포를 비교해보면 감시 노드의 연결 비율과 일반 노드가 커버된 비율이 가우스 분포가 더 높은 것을 알 수 있는데, 분포 특성상 가우스 분포는 중심 부근에 노드들이 많이 분포하기 때문이다.

V. 결 론

무선 센서 네트워크에서 센서 노드들은 소리, 움직임, 온도, 진동 같은 다양한 데이터를 수집해서 특정한 관리 노드로 보내게 된다. 센서들은 획득한 정보를 전달하기 위해 무선으로 서로 통신을 해야 하므로 공격에 취약한데 이런 공격을 막기 위해서 보통 사용하는 기법이 행위 기반 탐지이다. 행위 기반 탐지에서는 특정 감시 노드들이 이웃의 통신을 감청하여 불법적인 패킷을 탐지하게 되는데 공격이 탐지되면 신뢰할 수 있는 감시 노드들을 따라 관리 노드로 보고하는 것이 필요하다. 또, 감시 노드들은 일반 노드들에 비해 더 많은 에너지를 사용하기 때문에 최소의 감시 노드들로 네트워크를 커버하는 것이 필요하다.

본 연구에서는 서로 다른 두 종류의 감시 노드와 일반 노드가 배치되어 있을 때, 커버되는 일반 노드의 수가 최대가 되도록 주어진 수의 감시 노드를 선택하는 알고리즘을 개발하였고, 이 알고리즘을 사용하여 감시 노드의 수와 전송 범위가 감시 노드의 연결 비율과 일반 노드의 커버리지에 어떤 영향을 미치는 지 실험을 통해 비교하였다. 본 연구의 결과는 행위 기반 탐지를 사용하는 무선 센서 네트워크에서 목표 커버리지의 달성에 필요한 감시 노드의 수와 전송 성능을 제시함으로써 센서들의 비용을 절감하는데 유용하게 사용될 수 있다. 향후 다수의 배치점이 있을 때 감시 노드의 전송 범위가 일반 노드의 커버리지에 미치는 영향에 대해 연구할 계획이다.

참고문헌

〔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. Sheela, C. Naveenkumar and G. Mahadevan, "A noncryptographic method of sinkhole attack detection in wireless sensor networks," IEEE Intl. conference on recent trends in Information Technology(ICRTIT 2011), pp. 527-532, 2011

〔3〕 W. T. Zhu, "Node replication attacks in wireless sensor networks : bypassing the neighbor-based detection scheme," Intl. Conference on Network Computing and Information Security, pp. 156-160, 2011

〔4〕 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

〔5〕 K. Chong, "An Improved Algorithm using Shortest Path Tree for Behavior-based Attack Detection and Reporting Prblem in Wireless Sensor Networks," Journal of KIISE : Information Netwoking, vol. 39, no. 4, pp.365-370, August 2012

〔6〕 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

〔7〕 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

〔8〕 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

〔9〕 U. Wang, M. Wilkerson, and X. Yu, "Hybrid Sensor Deployment for Surveillance and Target Detection in Wireless Sensor Networks," IEEE , 2011

〔10〕 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

〔11〕 Xue Wang and Sheng Wang, "Hierarchical Deployment optimization for Wireless Sensor Networks," IEEE Transactions on Mobile Computing, vol. 10, no. 7, pp. 1028- 1041, July, 2011

〔12〕 G. Yang and D. Quio, "Multi-Round Sensor Deployment for Guaranteed Barrier Coverage," IEEE INFOCOM, 2010

저 자 소 개

정 균 락

1980년 2월 : 한국과학기술원 전자계산학 석사

1991년 2월 : 미네소타대학교 컴퓨터공학 박사

1991년 ~ 현재 : 홍익대학교 컴퓨터공학과 교수

관심분야 : 네트워크 알고리즘, 이동 통신, 무선 센서 네트워크, VLSI 알고리즘

Email : chong@cs.hongik.ac.kr