Journal of the Korea Academia-Industrial Cooperation Society
Vol. 12, No. 11 pp. 5238-5244, 2011

http://dx.doi.org/10.5762/KAIS.2011.12.11.5238

무선 센서네트워크에서 침입탐지를 위한 탐지노드 활성화기법 연구

성기택[1*]
[1]동명대학교 정보보호학과

A Study on the Activation Technique of Detection nodes for Intrusion Detection in Wireless Sensor Networks

Ki-Taek Seong[1*]
[1]**Department of Information Security, TongMyong University**

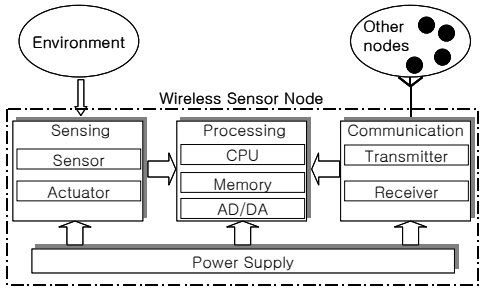
요 약 최근 무선센서네트워크 분야는 군사, 생체, 건강관련 광범위한 응용분야에서 많은 주목을 받아 왔다. 대부분의 센서네트워크가 높은 보안성을 요구하는 임무의 기능을 수행한다. 외부로부터의 공격에 대한 네트워크 보안, 효율적인 암호화 시스템, 보안 키 관리 및 인증 부분에서 많은 연구가 이루어져 왔지만, 내부 위협으로부터 네트워크를 보호에 관한 연구는 미비하다. 본 논문에서는 센서네트워크에서의 모든 패킷을 관찰하는 탐지노드를 활성화하는 노드 선택방법을 제안하였다. 제안된 방법은 최적화식으로 모델링되었으며, 접근방법의 검정을 위하여 경험적 Greedy 알고리즘 기반의 시뮬레이션 결과를 나타내었다.

Abstract Recently, wireless sensor networks have become increasingly interesting areas over extensive application fields such as military, ecological, and health-related areas. Almost sensor networks have mission-critical tasks that requires very high security. Therefore, extensive work has been done for securing sensor networks from outside attackers, efficient cryptographic systems, secure key management and authorization, but little work has yet been done to protect these networks from inside threats. This paper proposed an method to select which nodes should activate their idle nodes as detectors to be able to watch all packets in the sensor network. Suggested method is modeled as optimization equation, and heuristic Greedy algorithm based simulation results are presented to verify my approach.

Key Words : Sensor networks, Intrusion detection, Network security, Greedy algorithm

1. 서론

유비쿼터스에 대한 관심과 최근의 전자 및 기계기술의 발달로 인하여, 무선통신장치와 다양한 종류의 센서 및 마이크로프로세서의 집적화가 가능하게 되었으며, 이와 함께 센서노드의 발전과 함께 무선 센서네트워크(WSN: wireless sensor networks)에 관한 연구가 활발히 진행되고 있다. 다수의 센서노드들에 의하여 무선 통신 네트워크를 형성하는 센서네트워크는 지역의 탐지, 생물학적 환경탐지, 지형지물의 탐지, 건강관리 등의 다양한 분야에서 적용되고 있다. 그림 1은 하나의 센서노드에 대한 기본적인 구조를 보여주고 있다[1].



[그림 1] 센서노드의 구조
[Fig. 1] Sensor node architecture

*교신저자 : 성기택(ktseong@tu.ac.kr)
접수일 11년 09월 05일 수정일(1차 11년 10월 04일, 2차 11년 11월 03일) 게재확정일 11년 11월 10일

이러한 센서네트워크는 전통적인 컴퓨터 네트워크와는 달리 많은 제한 요건을 갖는 특수한 네트워크이므로 기존의 보안 기술을 직접 적용할 수 없다. 센서네트워크는 소형이며 독립적으로 운영되어야 하는 등의 자원적 제한이 있으며, 일반적인 네트워크와는 달리 물리적 공격과 함께 다양한 위협환경이 존재하는 환경에 분포되어 운영될 수 있다.

네트워크 관점에서 공격에 대한 방어 수단은 3가지로 요약될 수 있다. 첫 번째로는 방어로서 다양한 암호화, 방화벽 운영, 인증기법, 바이오인식 등의 기술이 적용가능하며, 두 번째로서는 탐지이다. 탐지의 대상으로서는 각종 침입, 다양한 공격, 자원의 잘못된 사용(misuse), 데이터의 상관, 악의적인 행위, 네트워크의 상태 또는 토폴로지(topology)의 상태변화 등이 있다. 세 번째로는 대응으로서 응답(예를 들면 통신종료, IP 주소의 블러킹 등), 공격에 대한 방어, 그리고 네트워크의 재구성이 있다[2]. 외부로부터 공격을 막는 것이 우선이지만 침입당한 후 사실을 인지하는 것도 대단히 중요하며, 센서네트워크에서의 침입탐지기술에 대한 다양한 연구가 이루어져 왔다.

본 연구에서는 기존의 침입탐지방법과는 달리 센서네트워크에서의 유휴노드를 이용한 방법을 제안하였다. 이후의 논문 구성은, 2장에서 센서네트워크에서의 보안개념과 침입탐지 및 관련 연구에 관하여 기술하고, 3장에서는 탐지노드에 대한 문제의 정의 및 수식화, 그리고 이를 해결하는 알고리즘을 제안하고, 4장에서는 제안된 알고리즘의 시뮬레이션 결과를 보이고, 5장에서는 시뮬레이션의 결과를 통한 본 연구의 결론을 기술하였다.

2. 센서네트워크에서의 보안

2.1 보안요구사항

센서네트워크에서의 보안은 일반적인 보안기법과 동일하게 암호화 중심이 이루어지지만, 자체가 갖는 여러 가지 제한사항 때문에 기존의 보안 방법들이 직접 이용될 수 없다. 센서네트워크가 가져야할 일반적인 보안 요구사항은 다음과 같다[3].

- 데이터 비밀성 (confidentiality)
- 데이터 무결성 (integrity)
- 데이터 신선성 (freshness)
- 자율구성(self-organization)
- 시간 동기성
- 보안의 국지성
- 인증

센서네트워크 특성상 다양한 공격에 노출될 수 있으며 공격의 형태는 다음과 같이 분류된다[4].

- 보안 및 인증체제에 대한 공격 : 일반적인 표준의 암호화 기술로 방어 가능.
- 네트워크 가용성에 대한 공격 : DOS (denial-of-service) 공격이 대표적인 예.
- 무결성에 대한 은밀한 공격 : 예를 들면 외부 노드를 센서네트워크의 일원으로 참여 시켜 오염된 정보를 전송시킴.

센서네트워크에서의 네트워크계층 별 공격 및 방어개념을 요약하면 표 1과 같다[5].

[표 1] 네트워크계층에서의 공격 및 방어
[Table 1] Attacks and defenses as network layers

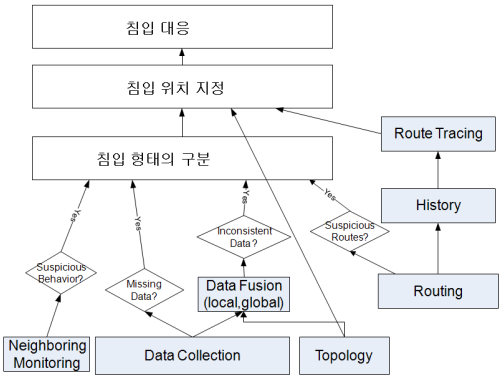
네트워크 계층	공격	대응방법
물리계층	jamming, tampering	spread-spectrum, priority message 등
링크계층	collision, exhaustion, unfairness,	error-correction code, small frame 등
네트워크 및 라우팅	selective forwarding sinkhole, sybil wormholes	authentication, probing 등
전송	flooding desynchronization	client puzzles , authentication 등

물리계층에서의 공격들은 노이즈에 강한 확산 스펙트럼과 같은 변복조 기법을 사용할 수 있으며, 프레임의 충돌과 같은 링크계층에서의 공격은 프레임의 크기를 줄이거나 오류교정코드와 같은 인코딩 기법이 적용가능하다. 네트워크 및 라우팅 계층에서의 공격은 네트워크를 구성하는 노드들의 상호 인증기법 등을 이용하여 대응가능하다. 그러나 이상과 같은 대응만으로는 센서네트워크에서 높은 보안성을 기대할 수 없다. 그 이유는 센서 노드들은 일정시간 동작을 수행한 이후에는 자원고갈 등의 이유로 기능의 저하가 올 수 있으며, 이러한 부실한 노드를 통하여 외부로부터 오염된 데이터가 주입되어 전송될 수 있기 때문이다. 만일 부실한 노드를 통하여 네트워크 내부로 침입이 되었다면 암호화나 인증과 같은 방법은 무의미하므로 일단 침입을 당하였으면 이를 인지하는 방법이 반드시 필요하다.

2.2 센서네트워크에서의 침입탐지

센서네트워크 침입탐지는 외부로부터 침입에 의한 이상행위(anomaly)의 탐지(AID : anomaly based intrusion detection)와 자원의 악용(misuse)을 탐지(MID : misuse intrusion detection)하는 것으로 분류된다[6]. 이와 같은

외부로부터 침입을 탐지하는 시스템의 예로, E. Ngai는 셀(cell) 기반의 센서네트워크 침입탐지시스템 (IDS : Intrusion Detection System) 구조를 그림 2와 같이 제안하였다[2].



[그림 2] 센서네트워크 IDS 구조
[Fig. 2] IDS architecture in sensor networks

본 논문에서는 그림 2의 이웃노드의 관찰을 통한 IDS 구현 기법에 관한 사항이다.

2.3 관련 연구

센서네트워크에서의 IDS 기술로서 이와 유사한 ad-hoc 네트워크에서의 IDS 기술을 이용을 고려할 수 있으나 다음과 같은 이유로 직접적인 적용은 적합하지 않다. 먼저 ad-hoc의 경우 사람에 의하여 관리되지만 센서네트워크는 전적으로 자체관리시스템이다. 컴퓨팅 자원의 경우 ad-hoc이 훨씬 풍부하다. 센서네트워크는 보다 특수한 환경에서 적용되기 때문에 하드웨어 또는 통신기법이 특별하다. 또한 노드의 분포밀도에 있어서 센서네트워크가 대단히 높다[7].

센서네트워크에서의 IDS 기술과 관련하여, Anjum 등은 탐지전용노드를 사용하여 최소 컷 집합 (minimum cut - set)과 최소영역집합 (minimum dominating - set)개념을 이용하여 탐지노드의 수를 최소화하는 방법을 제안하였으며[8], Agah 등은 네트워크 트래픽 부하와 Markov 결정 프로세스를 기반으로 하는 게임기법이 탐지기법에 적용할 수 있음을 증명하였다[9]. Loo 등은 클러스터링 구조의 네트워크에서 정상적인 트래픽 양식을 모델링하여 이를 네트워크로의 침투 시 나타나는 이상행위 때의 트래픽과 비교함으로서 비정상적인 행위를 탐지하는 방법을 제안하였고[10], Su 등은 클러스터 기반의 네트워크에서 네트워크를 구성하는 노드를 클러스터 헤더와 일반노드 두 가지로 분류하여 상호 모니터링 함으로써 보안성을 높이고 에너지 효율성을 제고토록 하였다. Roman 등은 [12]에서 "spontaneous watchdog" 개념을 사용하여 이웃하는 노드가 전송되는 패킷을 관찰하는 탐지노드로 설정하되 하나의 패킷을 감지하는 탐지노드의 수가 하나만 존재하도록 하는 확률적인 모델을 IDS에 적용하여 에너지 효율성을 제고하였지만 제안한 방식이 난수에 의한 확률모델이므로 모든 패킷을 모니터하지 못할 경우도 있다. A. Abduvaliyev 등은 AID 와 MID 기능을 하는 모듈을 복합적으로 사용하는 hybrid 방식의 (eHIDS) 구조를 제안하고 클러스터 기반으로 운영함으로써 통신량과 계산 량을 절약하는 기법을 소개하였다[14].

본 연구에서는 기존의 방법과는 다른 방법을 제안한다. IDS의 구성요소가 되는 탐지노드는 잉여노드로 남아 있는 유휴노드를 이용하였다. 여기서 유휴노드를 탐지노드로 선정하되 네트워크 전체에 존재하는 패킷을 관찰함과 동시에 에너지 효율성을 고려한 방법을 제안하였다.

3. 탐지노드 선택문제

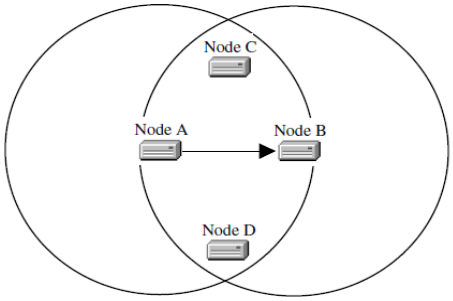
본 연구에서의 IDS기능은 활동 중인 네트워크에서 발생되는 모든 패킷을 관찰하고 분석하여 패킷들이 특정노드로 향하는 이상행위를 탐지하여 외부로 알려주는 것이다. 따라서 별도의 침입탐지 하드웨어를 갖는 노드를 사용하지 않고 모든 노드가 동일하며 단지 패킷의 이상행위를 관찰하는 부가적인 소프트웨어 기능이 추가되어 있는 것으로 가정한다.

센서노드는 일반적으로 에너지 효율적인 운영을 위하여 임무를 수행할 때(활동상태 : active mode)와 그렇지 않을 때(유휴상태: idle mode)로 구분하여 운영되며 노드가 유휴상태에 있더라도 패킷 수신은 가능하다. [13]에 의하면, 센서노드로 사용되는 MICA2 mote제품은 무선통신에서 송신 시 0.027J, 수신/유휴상태에서 0.01J, 슬리핑(sleeping)상태에서는 0.001J의 에너지를 사용한다. 따라서 탐지노드로서 무선통신을 관찰(통신수신)할 때와 유휴노드로서의 에너지 소비가 동일하기 때문에 유휴노드가 탐지노드가 되어 IDS 기능을 할지라도 부가적인 에너지소모가 제한적이라 할 수 있다. 부가적인 에너지소모 부분은 수신된 패킷의 주소와 같은 단순비교 연산 등의 수행에 소모되는 에너지와 이상행위 탐지 시 이를 알려주기 위한 알림패킷을 전송할 때 사용되는 사용하는 에너지 정도이다. 예를 들면 sinkhole 공격의 경우 패킷의 전송방향만으로도 침입여부를 판단할 수 있다.

유휴노드 중에서 탐지노드를 선택에 관하여 설명하면 다음과 같다.

3.1 탐지노드 조건

탐지노드가 되는 원리를 설명하면 다음과 같다. 그림 3에서 활동노드 A, B에서의 통신 반경을 원으로 나타낸 것이며 크기는 동일하다고 가정한다. 노드 C, D는 유휴 상태이다.



[그림 3] 탐지노드 선정 원리
[Fig. 3] Principle of selection for detector

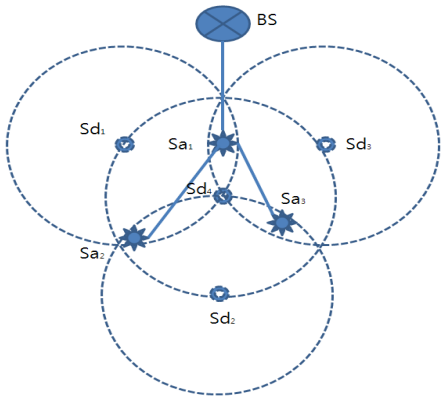
노드 A에서 노드 B로 패킷이 전송된다면 이웃하는 노드C와 D는 노드 A의 통신반경이내에 있으므로 패킷수신이 가능한 위치에 있기 때문에 패킷을 관찰하는 탐지노드로 선정될 수 있다[7]. 즉, 활동 중인 네트워크를 구성하는 노드 집합은 N={A,B}이며, N을 관찰 할 수 있는 IDS의 집합 N_{IDS} ={{C}, {D}, {C, D}} 세 개의 집합이 가능하다. 즉, C 또는 D만으로 관찰가능하며 C와 D를 공동으로 하여도 관찰가능하다. 그러므로 IDS를 구성하는 탐지노드의 조건은 다음과 같이 정의한다.

탐지노드조건 : 네트워크에서 발생되는 트래픽을 관찰할 수 있도록 모든 활동노드의 통신반경 내에 존재하는 유휴노드

3.2 에너지효율적인 탐지노드선정문제

그림 4에서 Sd_i는 탐지 노드, Sa_j는 동작노드를 나타내며, 현재 운영되고 있는 네트워크는 BS와 Sa_j의 집합과 실선으로 연결된 네트워크라 가정한다. (단, 1≦i≦4, 1≦j≦3 인 정수).

그림 3의 탐지노드선정 원리에 따라, 그림 4에서 BS로 가는 경로를 제외하고 모든 Sa_j 노드로 구성된 네트워크 상에서 전송되는 모든 패킷을 탐지하기 위해서는 모든 경로를 관찰하는 탐지노드가 필요하다.



[그림 4] 센서네트워크 예
[Fig. 4] A example of sensor networks

그림 4에서 실선으로 연결된 네트워크 전체를 관찰하는 탐지노드는 Sd_i이다. 네트워크를 구성하는 노드의 집합은 N = $\{Sa_1, Sa_2, Sa_3\}$이며, 유휴상태노드이면서 탐지노드인 Ni = $\{Sd_1, Sd_2, Sd_3, Sd_4\}$이다. 각 Sd_i가 관찰할 수 있는 Sa_j를 나타내면 다음과 같다.

$Sa_1 = \{Sd_1, Sd_2\}$, $Sa_2 = \{Sd_2, Sd_3\}$, $Sa_3 = \{Sd_1, Sd_3\}$,
$Sa_4 = \{Sd_1, Sd_2, Sd_3\}$

N을 관찰하는 집합 N_{IDS}는 조건에 따라 두 가지 형태로 구할 수 있다.

1) 교집합을 허용하지 않는 집합(disjoint set) :
$N_{disjoint}1 = \{Sd_1, Sd_2\}$, $N_{disjoint}2 = \{Sd_3, Sd_4\}$

2) 교집합을 허용하는 집합(intersection set) :
$N_{is}1 = \{Sd_1, Sd_2\}$, $N_{is}2 = \{Sd_2, Sd_3\}$, $N_{is}3 = \{Sd_1, Sd_3\}$,
$N_{is}4 = \{Sd_3\}$

여기서 IDS의 수명을 고려한다면, 각 노드의 초기 에너지가 1이라고 가정하면, disjoint set 경우는 (식 1)과 같다.

$$\text{T(disjoint set)} = \text{time}(N_{disjoint}1 + N_{disjoint}2) = 1 + 1 = 2 \quad (1)$$

그리고 intersection set 경우는 (식 2)과 같다

$$\text{T(intersection set)} = \text{time}(N_{is}1 + N_{is}2 + N_{is}3 + N_{is}4) = 0.5 + 0.5 + 0.5 + 1 = 2.5 \quad (2)$$

(식 1)과 (식 2)의 비교로부터 노드를 선정하는 조건에 따라 IDS 에너지효율성이 제고됨을 알 수 있다. IDS의 수명을 최대화하는 탐지노드를 선정하는 문제를 다음과 같이 정의하였다

최적탐지노드선택 문제 : 전체 센서노드 집합 U에서 유휴 센서노드 집합 C와 현재 활동 중인 노드 집합 R이 주어졌을 때(U = C + R), 활동 중인 노드를 관찰하는 센서들의 집합과 각각에 대응하는 에너지 값을 구하되 전체 에너지의 합이 최대가 되도록 한다.

최적탐지노드선택문제를 모델링하기 위하여 다음과 같이 정의한다. 전체 유휴노드의 수가 n개이고, 특정 활동노드 k의 통신반경이내에 존재하는 유휴노드 집합을 C_k라 한다. 활동 중인 모든 노드를 관찰하는 유휴노드의 집합이 p개 있을 경우 각각을 $S_1, S_2, \cdots, S_p$라 하고 각 집합에 대응하는 에너지를 $t_1, t_2, \cdots, t_p$라 할 때 최적탐지노드선택문제는 전체 에너지의 합($t_1 + \cdots + t_p$)을 최대화하는 것과 같다. 여기서 다음과 같은 두 가지 제한조건을 설정한다. 첫 번째, 임의의 활동노드 k를 관찰하는 유휴노드는 최소 1개 이상 존재해야 한다. 두 번째, 노드 k를 관찰하는 유휴노드의 집합이 사용할 수 있는 에너지는 초기 에너지 이하의 값을 갖도록 한다. 예를 들면 임의의 활동노드를 관찰하는 유휴노드가 3개 있고 각각의 초기 에너지 값이 '1'이라면 이 세 개의 노드 집합이 관찰하는데 사용할 수 있는 최대 에너지는 '1'이고 만일 각 노드의 에너지 값이 0.5, 0.7, 0.9라 하면 관찰하는데 사용할 수 있는 최대 에너지는 0.5 이상의 값을 가질 수 없다.

이상의 내용을 조합하면 두 개의 제한 조건을 갖는 최적화식으로 표현가능하며 다음과 같다.

$$\text{Maximize} \quad t_1 + \cdots + t_p \tag{3}$$

$$\text{subject to} \quad \sum_{j=1}^{p} x_{ij} t_j \le 1 \;\forall\, s_i \in C$$

$$\sum_{i \in C_k} x_{ij} \ge 1 \;\forall\, r_k \in R, j = 1, \cdots, p$$

$$\text{where} \quad x_{ij} = 0,1 \,(x_{ij} = 1 \text{ if and only if } s_i \in S_j)$$

여기서 x_{ij}는 특정 활동노드 k를 관찰할 수 있는 유휴노드를 의미하며, 존재하면 '1', 존재하지 않으면 '0'의 값을 갖는다. 또한 모든 노드가 갖는 에너지의 초기 값은 '1'로 가정한다.

4. 시뮬레이션 및 고찰

3장에서 정의된 "최적탐지노드선택문제"는 (식 3)과 같은 최적화문제이며 NP(Nondeterministic polynomial) 문제이다. 이를 해결하는 알고리즘으로써, 단순하여 실행속도가 빠른 Greedy 알고리즘을 선택하였다. 그 이유는 일반적으로 센서네트워크가 다수의 노드로 운영되므로 노드의 수가 많은 경우 계산시간 부하가 될 수 있기 때문이며, 또한 논문에서는 최적의 결과를 도출하기 보다는 제안한 개념의 유효성을 확인하고자 함이기 때문이다.

개발한 알고리즘은 일반 Greedy 알고리즘에 부가하여, 연구를 통하여 얻은 지식을 적용한 발견적 Greedy (Heuristic Greedy) 기법을 사용하였으며 내용은 다음과 같다.

```
Greedy Heuristic (C, R, w)
1: set lifetime of each sensor to 1
2: SENSORS = C
3: i=0
4: while each target is covered by at least one sensor
   in SENSORS do
5:   /*a new set cover Ci will be formed */
6:   i = i + 1
7:   Ci = ∅
8:   TARGETS = R
9:   while TARGETS = ∅do
10:    /*more targets have to be covered */
11:    find a critical target r_critical ∈ TARGETS
12:    select a sensor s_u ∈ SENSORS with greatest
       contribution, that covers rcritical
13:    Ci = Ci ∪ s_u
14:    for all targets r_k ∈ TARGETS do
15:      if r_k is covered by s_u then
16:        TARGETS = TARGETS −r_k
17:      end if
18:    end for
19:  end while
20:  for all sensors s_j ∈ Ci do
21:    lifetime s_j = lifetime s_j −w
22:    if lifetime s_j = 0 then
23:      SENSORS = SENSORS - s_j
24:    end if
25:  end for
26: end while
27: return i-number of set covers and the set covers C1, C2, ...,
Ci
```

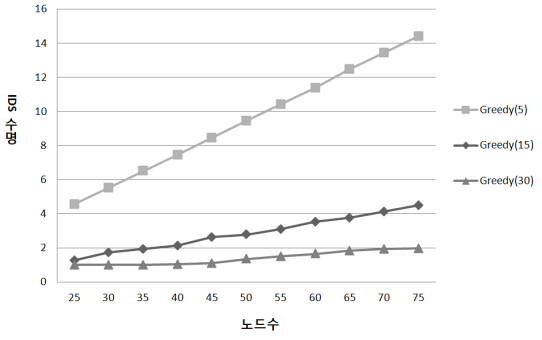
알고리즘에서, C는 모든 노드집합, R은 관찰해야할 활동 중인 노드의 집합, w 는 노드의 수명을 나타내는 값으로 초기 값은 '1'이며 1회 탐지노드로 활동하면 $w \in (0,1]$의 크기만큼 감소된다. TARGET은 활동 중인 노드 집합이다. 줄 14에 나타낸 바와 같이 기본적으로 모든 노드를 관찰하는 집합만을 대상으로 하기 때문에 전역 관찰을 기본적으로 만족한다. 줄 5부터 19까지가 발견적 기법이 적용되었다. 11의 $r_{critical}$은 이웃하는 유휴노

드들의 수와 잔존에너지를 고려하여 선택하였다. 그 이유는 유휴노드를 균등하게 활용하여 전체 에너지 소비를 균등하게 하는 효과를 기대할 수 있기 때문이다. 하나의 C_i가 구해지면 C_i를 구성하는 모든 노드의 에너지는 w 만큼 감소되고 다시 처음으로 돌아가 새로운 C_i를 구하게 된다. 결과적으로 IDS의 수명은 C_i가 구해졌을 때 사용가능한 최소의 잔존에너지의 합이 된다.

시뮬레이션에 사용된 프로그램은 JAVA (SE version 1.6.0_24)로 구현되었으며, HP prolient ML350(INTEL ZEON 3.0GHz, 4CPU), MS Windows server 2003 SE에서 수행되었다.

시뮬레이션에서는 활동노드 수의 변화와 노드의 통신반경의 변화에 따른 IDS의 수명 값을 관찰하여 제안한 방법의 유효성을 확인하고자 하였다. 활동노드 수의 증가는 관찰해야할 노드의 증가를 의미하며 따라서, 전체노드를 관찰할 수 있는 탐지노드의 집합 수는 적어지며 결과적으로 IDS의 수명은 짧아진다. 노드의 통신반경은 활동노드를 관찰할 수 있는 유휴노드의 수에 관계된다. 통신반경이 길어지면 탐지노드의 수가 증가되고 탐지노드 집합의 수가 증가하며 결과적으로 IDS의 수명이 길어짐을 추정할 수 있다. 시뮬레이션의 결과가 추정한 결과와 일치하면 제안한 방법의 유효성이 확인된다.

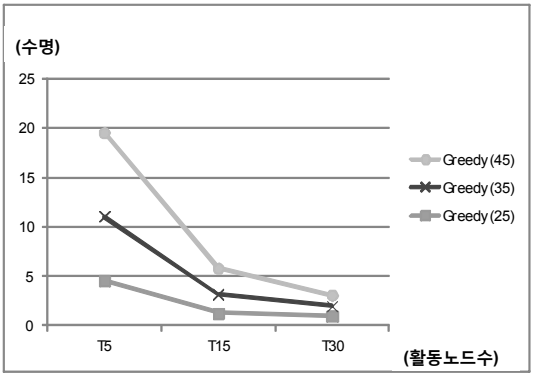
그림 5는 전체 노드 수가 증가 될 때 활동하는 노드의 수 변화에 따른 IDS 수명에 미치는 영향을 나타내었다.



[그림 5] 활동노드수의 변화에 따른 IDS 수명
[Fig. 5] Lifetime of IDS as the no. of active nodes

그림 5에서는 활동노드의 수를 5, 15, 30 으로 증가시키며 결과를 관찰하였으며, 각 경우를 Greedy(5), Greedy(15), Greedy(30)로 표시하였다. 즉, 분포되는 전체 노드 수의 증가(25 → 75)에 따라 IDS의 수명변화를 나타내었다. 그림 5에서, 전반적으로 전체 노드수가 증가함에 따라 IDS의 수명이 길어짐을 보이고 있고, 관찰해야할 노드의 수가 많은 경우보다 적은 경우에서의 IDS수명이 길어지고 있음 보이고 있으므로 추정한 결과와 일치하고 있다.

그림 6에서, 활동노드의 수가 5, 15, 30으로 증가시키면서 통신반경을 45, 35, 25로 했을 경우에 IDS의 수명변화를 나타내었으며 각각을 Greedy(45), Greedy(35), Greedy(25)로 표시하였다.



[그림 6] 노드 통신반경 변화에 따른 IDS 수명
[Fig. 6] Lifetime of IDS as the sensing range of detect nodes

그림 6에 의하면, 활동노드 수의 증가는 그림 5의 경우와 같이 IDS의 수명이 짧아지는 공통된 특성보이고 있으며, 통신반경이 큰 경우가 분포되는 노드의 수에 상관없이 일관되게 통신반경이 작은 경우보다 IDS의 수명이 길어지는 결과를 보이고 있으므로 추정한 결과와 일치하여, 본 연구에서 제안한 방법의 유효성이 확인되었다.

5. 결 론

본 논문에서는 센서네트워크에서 전송되는 모든 패킷을 관찰하여 네트워크 내부 침입에 대한 이상행위를 탐지하는 침입탐지 기술을 제안하였다. 기존의 방법과는 달리 IDS를 구성하는 탐지노드를 선정함에 있어서, 모든 유휴노드를 대상으로 하였으며, 활동노드를 관찰하는 유휴노드의 집합을 IDS 구성요소로 선정하되 IDS 수명을 최대화하는 문제를 정의하고 이를 최적화식으로 모델링하였다. 최적화식의 해를 위하여, 본 연구를 통하여 얻어진 경험적 지식을 Greedy 알고리즘에 적용하여 시뮬레이션을 수행하였다. 활동노드 수와 노드의 통신반경의 변화에 따른 IDS 수명에 대한 시뮬레이션을 수행하여 결과를 검토하여 제안한 방법의 유효성을 확인하였다. 그리고 제안된 방법은 BS에서 라우팅 알고리즘과 연동하여 운영될

수 있다.

제안된 방법에서 유도된 최적화식은 다양한 방법의 해가 있을 수 있으므로 보다 효율성을 갖는 방법에 대한 연구가 필요하다. 또한 대량의 노드가 적용되는 경우 계산량의 문제가 대두될 수 있으므로 클러스터 기반에서 운영 가능하도록 확장성을 갖는 알고리즘에 대한 추후 연구가 필요하다.

References

[1] Yi Zou, “COVERAGE-DRIVEN SENSOR DEPLOYMENT AND ENERGY-EFFICIENT INFORMATION PROCESSING IN WIRELESS SENSOR NETWORKS”, PhD Thesis, Duke University, 2004.

[2] Edith C.H. Ngai, “Intrusion Detection for wireless Sensor Networks”, The Chinese University of Hong Kong Department of Computer Science and Engineering Ph.D. Term 2 paper, pp. 29-37, 2005.

[3] Yang Xiao, “Security in Distributed, GRID, and Pervasive Computing", Chapter 17(Wireless Sensor Network Security: A Servey), CRC Press, 2006.

[4] E. Shi, A. Peerig, "Designing Secure Sensor Networks, "Wireless Communications Magazine, vol. 11, no. 6, 2004.

[5] Y. Wang; G. Attebury; B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, 2006

[6] I. Sato, Y. Okazaki, and S. Goto. An improved intrusion detection method based on process profiling. IPSJ Journal, 43(11):3316–3326, 2002.

[7] R. Roman; J. Zhou; J. Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks," in Proc. CCNC'06, 2006.

[8] F. Anjum; D. Subhadrabandhu; S. Sarkar; R. Shetty, "On Optimal Placement of Intrusion Detection Modules in Wireless Sensor Networks,” BROADNETS'04, 2004.

[9] A. Agah; S. Das; K. Basu, "Intrusion Detection in Sensor Networks: A non-cooperative Game Approach," IEEE ISNCA, 2004.

[10] C. Loo; M. Ng; C. Leckie; M. Palaniswami, "Intrusion Detection for Routing Attacks in Sensor Networks," Int'l. Journal of Distr. Sensor Networks, vol. 2,, 2006.

[11] C. Su; K. Chang; Y. Kuo; M. Horng, "The New Intrusion Prevention and Detection Approaches for Clustering-Based Sensor Networks,” IEEE WCNC, 2005.

[12] R. Roman; J. Zhou; J. Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks," in Proc. CCNC'06, 2006.

[13] MICA2 Radio Stack for TinyOS. http://www.tinyos.net/tinyos-1.x/doc/mica2rad, 2007.

[14] A. Abduvaliyev, et al., " Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks", 2010 Intl. Conference on Electronics and Information Engineering, Vol. 2 25-29, 2010.

성 기 택(Ki-Taek Seong) **[정회원]**

- 1990년 3월 : 부경대학교 전자통신공학과 (석사)
- 2007년 8월 : 부경대학교 정보시스템과 (공학박사)
- 1991년 2월 ~ 1998년 2월 : 국방과학연구소 선임연구원
- 1998년 3월 ~ 2006년 2월 : 동명대학 모바일웹마스터과 조교수
- 2006년 3월 ~ 현재 : 동명대학교 정보보호학과 조교수

<관심분야>
네트워크보안, 센서네트워크보안