한국시뮬레이션학회 논문지
Vol. 20, No. 4, pp. 31-40 (2011. 12)

무선 센서 네트워크에서 통계적 여과 기법의 에너지 효율을 향상시키기 위한 보안 경로 주기 선택 기법

남수만[1] · 선청일[1] · 조대호[1†]

The Secure Path Cycle Selection Method for Improving Energy Efficiency in Statistical En-route Filtering Based WSNs

Su-Man Nam · Chung-Il Sun · Tae-Ho Cho

ABSTRACT

Sensor nodes are easily exposed to malicious attackers by physical attacks. The attacker can generate various attacks using compromised nodes in a sensor network. The false report generating application layers injects the network by the compromised node. If a base station has the injected false report, a false alarm also occurs and unnecessary energy of the node is used. In order to defend the attack, a statistical en-route filtering method is proposed to filter the false report that goes to the base station as soon as possible. A path renewal method, which improves the method, is proposed to maintain a detection ability of the statistical en-route filtering method and to consume balanced energy of the node. In this paper, we proposed the secure path cycle method to consume effective energy for a path renewal. To select the secure path cycle, the base station determines through hop counts and the quantity of report transmission by an evaluation function. In addition, three methods, which are statistical en-route filter, path selection method, and path renewal method, are evaluated with our proposed method for efficient energy use. Therefore, the proposed method keeps the secure path and makes the efficiency of energy consumption high.

Key words : Sensor Network, Statistical En-route Method, Secure Path Cycle Selection

요 약

센서 노드는 악의적인 공격자들에 의해 물리적인 공격들에 쉽게 노출된다. 공격자는 훼손 노드를 이용하여 센서 네트워크에 다양한 공격을 발생시킬 수 있다. 그 중 응용 계층에서 발생하는 허위 보고서 삽입 공격은 훼손된 노드를 통해 네트워크 내에 위조 보고서를 주입한다. 주입된 위조 보고서는 BS까지 전달될 경우 허위 경보뿐만 아니라 노드의 불필요한 에너지 소모를 유발한다. 이러한 공격을 방어하기 위해 통계적 여과 기법은 BS까지 전달되는 허위 보고서를 전달 과정 중 가능한 빨리 여과시키기 위해 제안되었다. 이 기법의 성능 향상을 위해 제안된 기법 중 경로 갱신 기법은 통계적 여과 기법의 탐지 능력 유지하고 노드의 균형 있는 에너지 소모를 위해 제안되었다. 본 논문은 경로 경신 방법에서 경로 갱신에 필요한 에너지의 효율적인 소비를 위해 보안 경로 주기 결정 방법을 제안한다. 보안 경로 주기를 선택하기 위해 BS에서 센서 노드들의 홉 수와 보고서 전송량을 고려하여 평가 함수를 통해 결정한다. 그리고 시뮬레이션을 통해 위 3가지 기법들과 제안 기법을 비교하여 에너지 효율성을 평가한다. 그러므로 제안 기법은 보안 경로 설정을 유지하면서, 네트워크 내에 균형 있는 에너지 소비의 효율을 높인다.

주요어 : 센서 네트워크, 허위 보고서, 통계적 여과 기법, 보안 경로 주기 선택

*본 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2011-0004955).

접수일(2011년 7월 13일), 심사일(1차 : 2011년 11월 30일), 게재 확정일(2011년 11월 30일)

[1] 성균관대학교 정보통신공학부
주 저 자 : 남수만
교신저자 : 조대호
E-mail; taecho@ece.skku.ac.kr

1. 서 론

무선 센서 네트워크(wireless sensor network; 이하 WSN)는 무선 통신의 급격한 발전으로 저비용, 저 저력을 이용한 작은 크기의 다기능 센서 노드 개발이 상용되었으며, 여러 분야에서 응용, 설계되어 사용하고 되고 있다[1-2].

WSN은 보통 수많은 센서의 집합체인 센서 필드(sensor field)와 베이스 스테이션(base station; 이하 BS)으로 구성된다. 한 센서 노드(sensor node)는 감지(sensing), 계산(computing), 그리고 무선 통신(wireless communication) 모듈로 구성되며, 어떠한 사건(event) 발생 시 센서 노드들은 사람 또는 주위의 사물이나 환경을 바탕으로 감지한 정보를 모아 보고서(report)로 생성하여 BS로 전달하고, BS는 인터넷 또는 통신 인프라를 통해 사용자에게 해당 정보를 제공한다. 기본적인 센서 네트워크 응용은 인프라 없이 노드 간의 직접적인 무선 통신할 수 있고 개방적인 무인 환경에 무작위 배포로 적합하지만, 시간의 경과로 파괴, 훼손 혹은 배터리의 수명으로 노드의 기능을 상실할 수 있다.

또한, 환경적인 제약으로 악의적인 공격자로부터 다양한 공격 패턴에 노출되어 있다[3]. 악의적인 공격 패턴의 방어, 센서 노드의 제한된 처리 능력, 그리고 효율적인 배터리 사용에 대한 문제는 여러 방면에서 연구가 진행되고 있으며, 계속해서 심도 있는 연구가 필요하다[4,6].

다양한 공격 패턴 중, 그림 1과 같이 응용 계층에서 발생하는 허위 보고서 삽입 공격(false report injection attacks)은 공격자가 센서 네트워크에서 하나 이상의 노드(노드 A)를 탈취하고 그 노드를 훼손시킨 후, 훼손된 노드들을 통해 허위 보고서를 주입시켜 네트워크에 침투시킨다. 위 그림처럼, 이러한 공격이 노드 B, C, 그리고 D를 거쳐서 BS까지 전달된다면, 허위 경보를 유발하여 사용자에게 피해를 줄 뿐만 아니라 노드 B, C, D의 에너지는 급감한다. 따라서 전체 네트워크는 불필요한 에너지 소비로 센서 수명을 단축하게 하여 네트워크의 기능을 상실시킨다[5,6].

허위 보고서 삽입 공격을 방어하기 위해 다양한 여과 기법이 제안되었다[7-9]. Fan Ye 등이 제안한 통계적 여과 기법(statistical en-route filtering scheme; 이하 SEF)[9]은 빠른 계산과 통신을 통해 다수의 홉을 거쳐 BS까지 전달되는 허위 보고서를 노드 자신들이 소유한 키들을 통해 허위 보고서가 BS에 도달하기 전 가능한 한 빨리 여과하는 것에 목적을 둔다. SEF에서 허위 보고서 탐지 능력을 향상시키기 위한 경로 선택 방법(path selection method; 이하 PSM)[10]은 초기의 경로를 설정할 때, 제어 메시지를 플러딩(flooding)하여 BS로부터 받은 각 노드가 소유한 하나의 구획을 제어 메시지에 포함된 파티션 식별 보관소(partition ID array)에 있는 체크 비트(check bit)를 하나씩 검사하여 보안 경로를 선택하게 된다. 네트워크 수명의 연장과 원활한 통신량 분배를 위한 경로 갱신 방법(path renewal method; 이하 PRM)[11]은 부모 노드의 에너지 소모가 미리 설정된 임계 값보다 작을 때, 부모 노드가 소유한 자식 노드 하나를 선택하여 자식 노드의 범위 안에 있는 새 부모 노드를 선택하고 변경한다. 이를 통해 한 노드에 집중되는 통신을 분산시켜 네트워크 전체의 에너지 소비를 균일하게 유지한다.

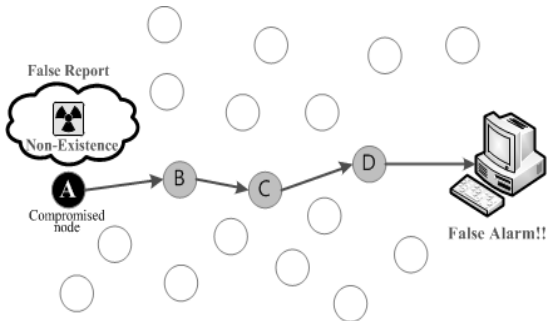

그림 1. 허위 보고서 삽입 공격

본 논문은 PRM을 통하여 효율적인 보안 경로 주기 결정을 제안한다. 제안된 기법은 모든 노드의 정보를 통해 노드를 평가하여 경로 결정의 효율적인 시기를 결정한다. 그러므로 각 노드는 균형 있는 에너지 소모와 PSM의 보안성을 유지할 수 있다. 본 논문의 구성은 다음과 같다. 2장에서는 SEF, PSM, PRM에 대한 설명과 본 연구를 진행하게 된 동기를 설명하고, 3장에서는 제안 기법을 논한다. 4장에서는 시뮬레이션 결과를 통해 평가하고, 5장에서는 관련 연구를 간략하게 소개한다. 마지막으로 6장에서는 결론 및 앞으로 과제에 대하여 서술한다.

2. 배경 이론 및 동기

2.1 통계적 여과 기법(SEF)

SEF은 허위 보고서를 BS가 받기 전, 허위 보고서가 전달되는 과정에서 노드의 키들을 통해 가능한 한 빨리 여과하여 확률적으로 결정하는 특징이 있다. 이 기법의 동작 과정은 크게 키 분배, 보고서 생성, 그리고 보고서 전달 및 검증 과정으로 나누어진다. 기지 노드는 네트워크 안에 사용되는 임의의 개수(P 개)만큼 구획(partition)으로 나눈다. 각 구획은 n 개의 키들로 구성된다. 각 노드는 네트워크에 배치되기 전, 전역 키 풀의 선택된 구획에서 키들을 받아 적재시킨다. 그림 2는 이러한 전역 키 풀의 구조와 키 분배 과정을 나타내고 있다.

그림 3(a)와 같이 이벤트가 발생할 때, 비슷한 지역에 있는 노드 중에서 가장 강하게 감지한 노드를 대표 노드

(center of stimulus; 이하 CoS)로 선출한다. CoS 노드는 같은 이벤트를 감지한 주변 노드에 브로드캐스트(broadcast)를 하고, 전달받은 주변 노드들은 자신이 받은 이벤트와 같다면, 이벤트 정보와 메시지 인증 코드(message authentication code; 이하 MAC) 생성해서 CoS 노드에 보낸다. CoS 노드는 받은 MAC 중에서 서로 다른 구획의 MAC만 모아 미리 사용자에 의해 설정된 보안 경곗값만큼 선택해서 이벤트 정보와 함께 하나의 보고서를 생성하고 같은 경로에 있는 노드에 전송한다.

그림 3(b)에서 CoS를 통해 생성된 정상 보고서(Report 1)와 허위 보고서(Report 2)는 다수의 홉을 통과하여 BS까지 전달되는 과정이다. 보안 경곗값은 3으로 설정되어 있고, Report 2는 공격자가 보안 경곗값을 만족하게 하기 위해 한 개의 위조 MAC(forged MAC)를 만들어 허위 보고서를 센서 네트워크에 삽입하는 과정이다. Report 1은 동일 경로 상에 있는 중간 노드들의 키들을 통해 검증을 받고 정상적으로 BS까지 전달된다. BS는 다시 한 번 자신이 소유한 전체 키들과 비교하여 허위 여부를 판별한다. Report 2는 경로 상의 중간 노드에 검증을 받지만, 정상적으로 구획 12의 인증키를 할당받은 중간 노드를 통해 위조 MAC으로 결정된다. SEF은 허위 보고서 삽입 공격을 여과하여 센서 간에 불필요한 전송을 줄이기 때문에 에너지 소모를 줄일 수 있다.

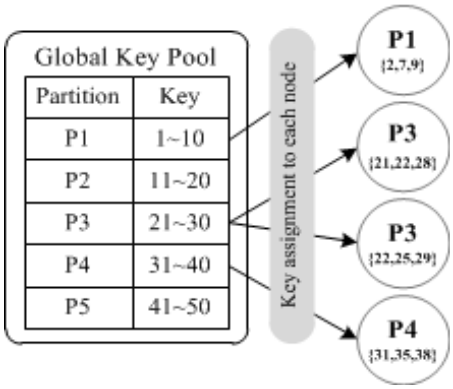

그림 2. 전역 키 풀의 구조 및 키 분배

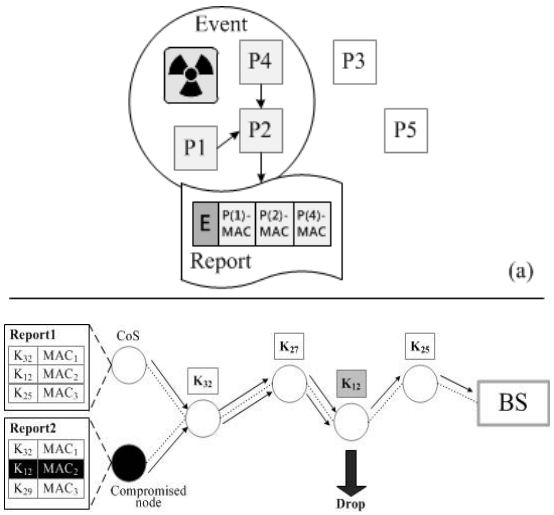

그림 3. 보고서 생성 및 허위 보고서 여과 과정

2.2 경로 선택 기법(PSM)

[10]에서는 SEF의 허위 보고서 탐지 능력을 향상하기 위하여 PSM을 제안하였다. 이 기법에서는 경로 설정을 위해 BS로부터 제어 메시지(control message)가 플러딩(flooding)된다. 제어 메시지는 경로 상에 있는 노드들의 구획을 표시하는 배열이 있고, 체크가 된 구획에 대해서는 다시는 갱신되지 않는다. 한 노드가 제어 메시지를 받았을 때, 포함된 구획의 정보를 기반으로 한 평가함수를 통해 보안 경로를 설정한다. 또한, 이 기법의 특징은 사용자가 보안 강도 요소를 조절하여 보안 경로를 변경할 수 있다.

그림 4는 BS로부터 나오는 제어 메시지 플러딩 및 갱신 과정이다. 제어 메시지는 목적지 노드(destination node)까지 가는 동안 노드들의 구획을 제어 메시지 체크 비트에 표시한다. 구획 5(P5)을 가진 목적지 노드는 제어 메시지들을 통해 두 경로의 구획 상태를 점검하여 하나의 경로를 선택한다. PSM은 목적지 노드까지 키 구획의 정보를 카운트하여 보안 경로를 설정하고, 허위 보고서 탐지 능력을 향상하게 시킨다.

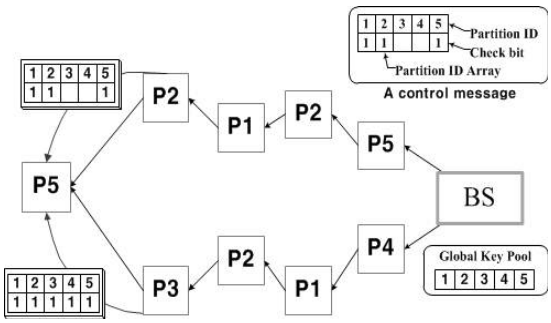

그림 4. 보안 경로 선택 방법

2.3 경로 갱신 기법(PRM)

[11]에서는 PSM의 노드의 에너지 능력을 향상하기 위해 PRM을 제안하였다. 이 기법에서는 네트워크 내에 전체적인 에너지 소비 불균형을 줄여 네트워크 수명을 연장하고, 보고서를 전송하는 노드는 자식 노드, 전송을 받는 노드는 부모 노드로 정의한다. 경로를 경신할 때, 모든 부모 노드의 에너지 잔량을 감사한다. 만약 부모 노드의 에너지 잔량이 설정된 임계 값보다 작다면, 부모 노드는 에너지 상태가 좋은 자식 노드를 선택하고, 그 자식 노드는 이웃하는 범위 내에서 새로운 부모 노드를 찾아 경로를 경신한다.

그림 5는 경로 갱신 방법의 예를 보여준다. 그림 5에서 부모 노드 S_0는 C_0, C_1 그리고 C_2의 자식 노드를 가진다. 만약 S_0의 에너지 잔량이 임계값보다 작다면 하위 노드 중, 에너지 잔량이 가장 많은 C_0에게 EM(eviction message; 이하 EM)을 보낸다. EM을 수신한 C_0는 자신의 주변 노드에 새로운 부모 노드 선출을 위한 정보 메시지를 요청한다. C_0는 주변 노드들의 정보를 통해 새로운 부모 노드 S_1을 선출하고 기존 부모 노드인 S_0에 FM(fare message; 이하 FM)을 전송하여 부모 노드의 변경을 알린다. 그리고 S_0는 자식 노드 목록에서 C_0을 삭제한다.

2.4 동기

PRM를 통하여 효율적인 경로 갱신을 발생하기 위해서는 적절한 경로 주기 선택이 중요하다. 예를 들어 네트워크 내에 경로 갱신이 빈번히 일어나면 새 부모 노드 탐지와 메시지 전달을 통해 불필요한 에너지 소모가 높고, 경로 갱신이 적절하게 일어나지 않으며 노드의 불균형 에너지 소모가 유발되고 네트워크 수명을 단축하게 한다. 그러므로 센서 네트워크 내에 적절한 경로 갱신 결정은 중요하다. 본 논문은 노드의 홉 수, 전송한 양을 고려하여 평가 함수를 통해 경로 갱신을 결정하여 노드의 에너지 효율을 높인다.

3. 제안 기법

3.1 가정

센서 네트워크는 한 개의 BS와 다수의 센서 노드들로 구성된다. 각 센서 노드는 센서 필드 내에 무작위로 배치되고, 고유한 식별 번호를 가진다. 최초의 보안 경로 설정은 PSM을 통해 이루어지고, 모든 경로는 단일 전송 프로토콜(single path routing protocol)을 사용하여 보고서가 BS까지 전달한다. 그리고 BS는 각 노드의 홉 수, 전송한 양, 그 외 기본 정보를 가지며, 상태 변화 시 정보를 갱신하고 CoS로부터 받은 정상 보고서의 수를 안다.

3.2 개요

BS는 모든 노드의 ID, 홉 수, 전송한 양 등 기본적인 정보를 관리 유지한다. 전체 노드의 정보 구조를 기반으로 각 노드는 평가를 받고, 각 노드가 받은 평가 결과와 사용자 강도 요소를 통해 평가 함수에 적용한다. 노드의 상황에 맞는 경로 갱신의 주기 결정은 모든 노드의 에너지 균형을 유지하며 전체 네트워크 수명을 연장할 수 있다.

3.3 동작 과정

모든 노드의 균형 있는 에너지 소비를 위해 보안 경로 경신 주기 결정은 중요하다. 네트워크 내에 노드별 에너지 소비는 홉 수와 보고서의 전송한 양에 영향이 있다. 한 노드의 홉 수가 상대적으로 다른 노드들보다 높다라면, 보고서를 BS에 보낼 때 동일 경로 상에 있는 중간 노드들의 에너지 소모는 많을 것이다. 또한, 한 노드의 전송한 양이 다른 노드들보다 크다면, 그 노드는 에너지 소모가 클 것이다. 그래서 한 노드의 높은 홉 수와 전송한 양은 불균형한 에너지 소비를 유발해 전체 네트워크의 수명을 단축하게 하는 원인이 된다.

그림 6은 노드 관리 테이블 구조를 보여준다. 노드 관

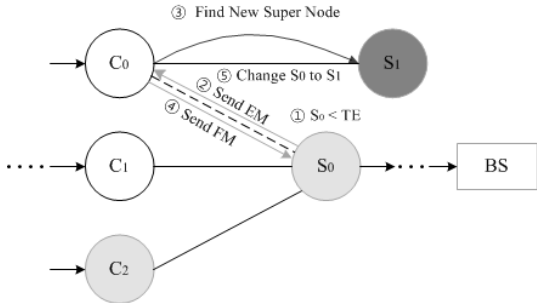

그림 5. 경로 갱신 과정의 예

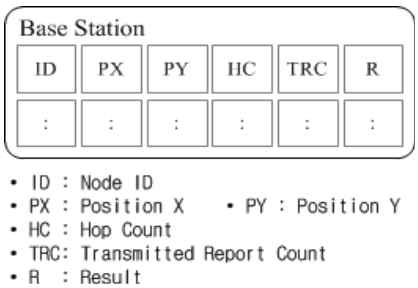

그림 6. 노드 관리 테이블 구조

리 테이블에서 ID는 노드의 ID, PX은 노드의 X 위치, PY은 노드의 Y 위치, HC(hop count; 이하 HC)는 홉 수, TRC(transmitted report count; 이하 TRC)은 보고서 전송한 양, 그리고 R은 노드 평가의 결과 값으로 정의한다. BS는 보고서가 각각 노드 상태 정보를 갱신하고, 결과 값도 같이 갱신하여 최신의 상태로 유지한다.

그림 7은 BS에서 노드 관리 테이블을 통해 노드의 ID, HC, 그리고 TRC 등의 정보를 갱신하는 모습이다. 그림 7(a)은 보고서가 BS까지 전달되는 다운스트림 방향(downstream)으로 노드들의 상태 정보와 BS의 노드 관리 테이블 상태를 보여주고 있다. BS의 RRC(received report count; 이하 RRC)은 50으로 BS가 받은 정상 보고서의 수를 나타낸다.

그림 7(b), (c)은 보고서가 CoS 노드와 훼손된 노드로부터 다운스트림 방향으로 다수의 홉을 거쳐 BS에 전달되고 있다. 그림 7(b)에서 노드 1은 CoS 노드로 정상 보고서를 노드 2, 3을 거쳐 BS까지 전달하는 그림이다. 정상 보고서가 BS에 전달되었을 때, BS의 RRC는 50에서 1이 증가한다. 또한, BS의 노드 관리 테이블은 다수의 노드를 경유한 노드들의 TRC를 1만큼 증가시킨다. 그림 7(c)의 경우 노드 1은 훼손 노드로써 허위 보고서를 삽입하여 BS까지 전달한다. 하지만, 허위 보고서는 노드 2에서 MAC 비교를 통해 여과되었고, 다시는 노드 3을 거쳐 같은 경로에 있는 다수의 노드에 전달하지 않는다. 노드 2는 여과한 허위 보고서를 BS에 알리지만, RRC를 증가시키지 않는다. 노드 2를 통해 정보를 전달받은 BS는 노드 1의 TRC만 증가시키고, 노드 2, 3과 같은 경로 상에 있는 노드들의 TRC는 그대로 둔다.

그림 8은 제안 기법의 동작 순서도를 차례대로 보여준다. 그림 8에서 ①은 초기 SEF에서 BS가 모든 노드에 구획 및 키들을 할당하는 과정이다. 각각의 노드는 하나의 구획을 가지며 사용자가 정의한 키의 개수만큼 할당받는다. ②번은 PSM을 통해 제어 메시지를 플러딩하여 각각 노드의 구획 정보를 참조하여 보안 경로를 설정한 과정이다. ③번부터 ⑦번은 제안 기법의 처리 과정이다.

표 1은 그림 8에서 제시한 동작 과정의 ③번에서 ⑦번까지 해당하는 보안 주기 결정 알고리즘이다. 라인 1, 2에서 CV(critical value)와 EN(evaluated node)은 각각 사용자가 정의한 임계 값과 평가된 노드의 결과 값이다. 그림 ③번에서 BS는 보고서를 받을 때 노드 상태 HC와 TRC 정보를 변경한다(라인 5). 그림-④번은 알고리즘 라

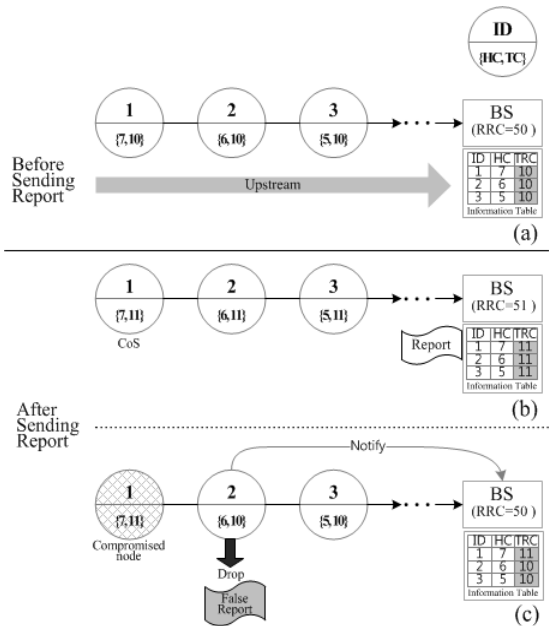

그림 7. 노드 관리 테이블 갱신의 예

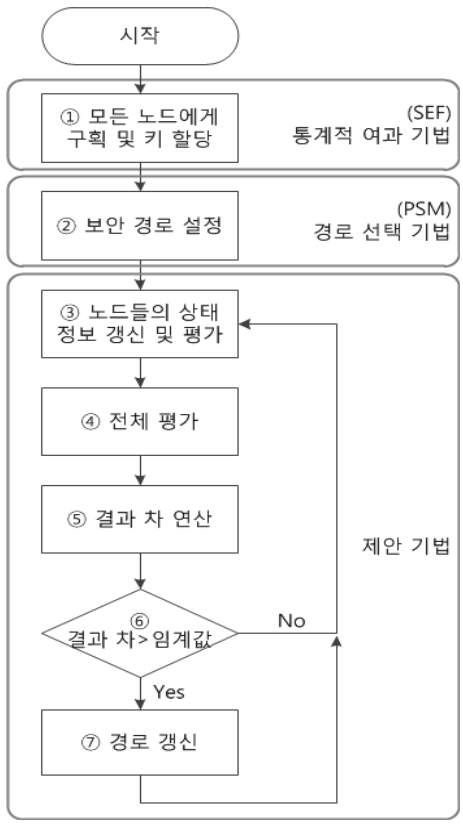

그림 8. 제안 기법 동작 과정 순서도

표 1. 보안 주기 결정 알고리즘

```
 1: Critical_Value CV;
 2: Evaluated_Node EN;
 3: Routing_Path RP;
 4:
 5: Each Node is updated;
 6:
 7: FOR I = 1 TO N THEN
 8: {
 9:     Node[I] is evaluated.
10:     Result = Result + EN[I];
11: }
12:
13: New = Result;
14: Diff = New - Old;
15:
16: IF Diff > CV THEN
17: {
18:     RP is changed;
19:     Old = New;
20: }
```

인 7~11까지를 표현하고 있으며, BS는 각 노드의 정보와 함께 노드 평가 함수로 결과 값을 추출하고, 평가한다. 라인 7에서 N은 한 센서 필드에 존재하는 총 노드의 개수를 의미하고, 식 (1), 식 (2) 평가 함수를 통해 노드 관리 테이블에 결과 값을 갱신한 다음(라인 10), 각각 노드의 결과 값에 누적시킨다(라인 11). 그림-⑤에서 이전 결과 값과 새로 추출된 결과 값의 차를 계산하고(라인 14), 전달된 결과 차이 값을 통해 그림-⑥번에서 사용자가 정의한 임계 값과 비교를 한다(라인 14). 만약 그림-⑥과 라인 16 과정에서 얻어진 결과가 임계 값보다 작다면, ③, ④, ⑤, ⑥을 반복 수행한다. 그러나 결과 값이 임계 값보다 크다면, PRM을 통해 전체 네트워크의 경로가 설정되고(그림⑦과 라인 18~19), 다시 ③, ④, ⑤, ⑥번을 반복 수행한다.

3.4 평가 함수

네트워크 내의 경로 갱신을 위한 주기 결정 평가 함수는 각 노드의 홉 수, 각 노드가 전송한 보고서의 양, 그리고 BS가 받은 정상 보고서의 수를 간주하여 결정한다.

$$RTR_i = \frac{TRC_i}{RRC_i} \times 100 \quad (1)$$

표 2. BS의 노드 관리 테이블

Nodes Information Table in BS

RRC=100		ω=0.5 or ω=0.9	
ID	HC	TRC	N(i)
1	7	10	17
2	6	15	21
3	5	20	25

$$N(i) = HC_i + RTR_i \quad (2)$$

식 (1), (2)에서 i은 노드의 ID이고, 식 (1)은 BS가 받은 정상 보고서의 양(RRC)과 한 노드가 보낸 보고서의 양(TRC)을 통해 한 노드가 보낸 보고서의 비율(RTR)을 알 수 있다. 한 노드의 에너지 소비는 홉 수(HC)와 노드가 보낸 보고서의 비율(RTR)에 영향이 크다. 각각의 노드는 식 (2)를 통해 평가되어 진다.

$$F(R) = \sum_{i=1}^{n} F(N_i) \cdot \omega \quad (3)$$

식 (3)은 식 (2)에서 평가받은 각 노드의 결과 *N(i)*을 통해 경로 갱신 여부를 결정하게 된다. 만약 *F(R)*이 사용자가 설정한 임계 값을 초과한다면, PRM을 통해 경로를 갱신하게 된다. ω은 사용자가 미리 정의한 주기 결정 강도이다.

주기 결정 강도 요소 ω은 범위가 0≤ω≤1까지이다. 만약 ω가 0이라면, 재 경로 갱신은 전혀 이루어지지 않고 이미 설정된 경로를 계속 유지하게 된다. 만약 ω가 1이라면, 경로 갱신은 빈번하게 일어나게 된다. 표 2에서 BS는 RRC은 100이다. RTR1, RTR2, RTR3은 각각 10/100×100 = 10, 6/100×100 = 15, 20/10 ×100 = 20이다. 그리고 N(1)은 7+10 = 17, N(2)은 6+15 = 21, N(3)은 5+20 = 25가 된다. 사용자 주기 결정 강도가 0.5라면, (17+21+25)×0.5 = 31.5가 되고, 주기 결정 강도가 0.9라면, (17+21+25)×0.9 = 41.4가 된다. 만약 주기 결정 임계 값이 40이고 평가 함수를 통한 이전 결과 값 차이가 0인 상태라면, ω가 0.5의 상태에서는 경로 갱신이 실행되지 않고 대기하며, ω가 0.9일 때 PRM을 통해 경로가 갱신된다.

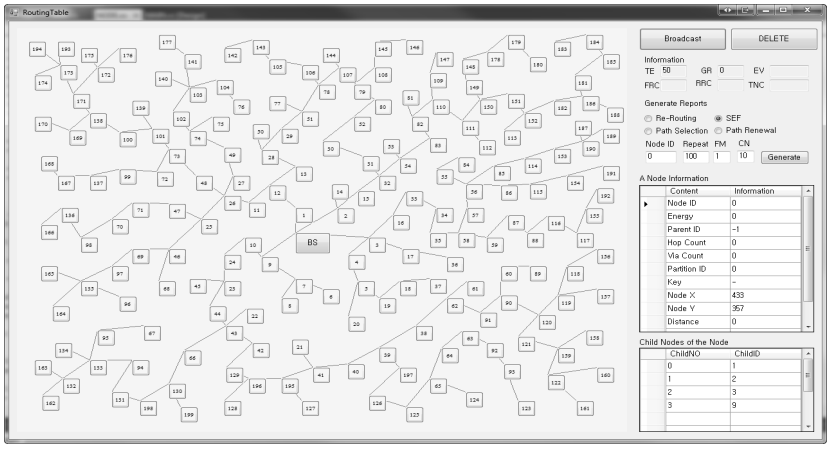

그림 9. 센서 네트워크 모델

4. 실험 결과

본 논문에서 시뮬레이션은 효율적인 제안 기법의 성능을 보여주기 위해 SEF, PSM PRM과 비교하여 평가한다. 그림 10은 시뮬레이션에 사용되는 센서 네트워크 모델이다. 그림 왼쪽 구역은 센서 필드 안에 센서 노드들과 중간에 BS를 구성하였고, 노드별로 경로가 설정된 상태이며 모든 전송은 단일 전송 프로토콜(single path routing protocol)을 사용하여 BS까지 보고서를 전달한다. 오른쪽 구역은 파라미터 설정 및 노드들의 상태 정보를 확인할 수 있는 영역으로 나누었고, SEF, PSM, PRM 그리고 제안 기법을 선택할 수 있으며 보고서 생성의 양, 허위 보고서의 양, 훼손된 노드의 비율을 입력할 수 있다. 이때 보고서의 생성은 특정 한 노드와 무작위별로 노드에서 발생할 수 있다.

시뮬레이션 파라미터는 표 3과 같이 정의하였고 이벤트는 무작위로 생성되며 시뮬레이션에서 사용되는 에너지 소모의 계산 등은 SEF[9]에서 실험한 결과를 사용하였다. 시뮬레이션의 환경 구성은 아래 표와 같이 진행한다.

그림 9는 라운드가 200인 구간에서 제안 기법(the proposed method; 이하 PM)과 SEF, PSM, PRM의 평균 에너지 소모량을 보여준다. 이 결과를 통해 제안 기법은 네트워크 상태에 따른 주기 갱신으로 다른 기법들보다 에너지 소모량이 적다. $\omega = 1.0$일 때 에너지 소모가 가장 적다. 따라서 경로 갱신에 따른 주기 결정은 각 노드의 에너지 소모를 줄이고, 균형 있는 에너지 소모를 통해 센서 네트워크의 수명을 늘리는 방법이 될 수 있다.

그림 11은 보안 경계 구역이 4인 한 보고서에서 허위

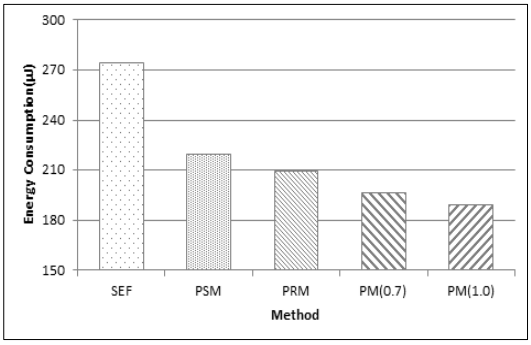

그림 10. 제안 기법별 평균 에너지 소비량

표 3. 시뮬레이션 파라미터

Parameter		Value
Nodes		200
A Field Size		50 m × 50 m
Size	Report	12 bytes
	MAC	1 bytes
Energy Consumption	Transmit	16.56 μJ
	Receive	12.5 μJ
	MAC generation	15 μJ
Global Key Pool		10
keys Number per a Node		5
Security Limit per a Report		4

MAC을 1, 2, 3개를 삽입시켜 허위 보고서가 이동한 평균 홉 수이다. 그림 11에서 보듯이 제안 기법을 기존 SEF보다 허위 보고서를 빠르게 탐지하여 여과하며 PSM

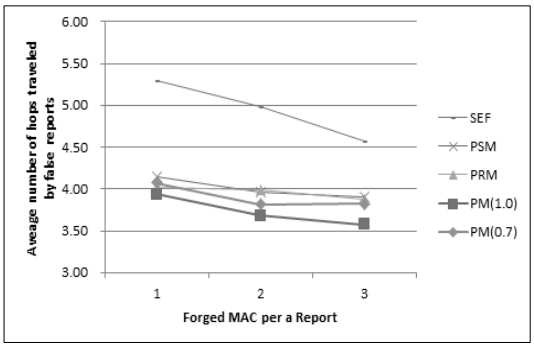

그림 11. 허위보고서가 이동한 평균 홉 수

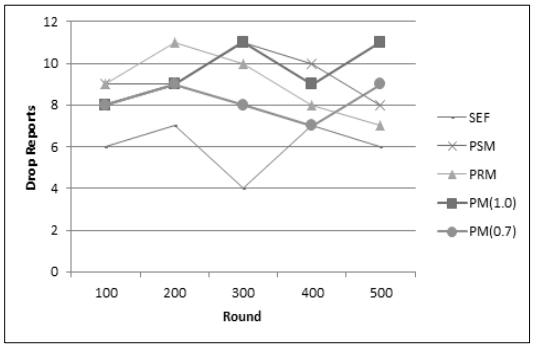

그림 12. 여과된 허위 보고서의 개수(forged MAC = 1)

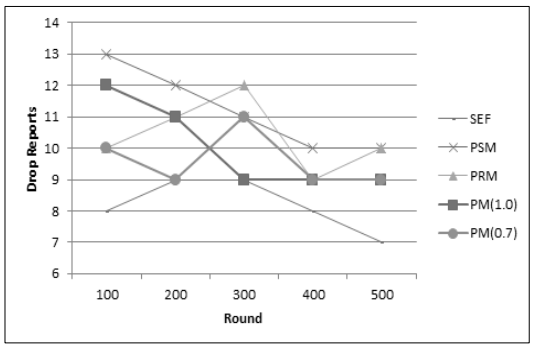

그림 13. 여과된 허위 보고서의 개수(forged MAC = 2)

과는 유사한 탐지 성능을 보인다. 제안 기법에서 ω = 1.0일 때 허위 보고서가 이동한 평균 홉 수는 다른 기법들보다 차이가 미미하지만, 다른 기법들보다 적은 홉에서 허위 보고서 필터를 통해 다음 부모 노드에 전달되는 거짓 보고서를 줄일 수 있으므로 네트워크의 에너지 향상이 기대된다.

그림 12, 13은 보안 경계 구역이 4인 한 보고서 안에 오염된 MAC의 개수가 각각 1, 2개 삽입된 경우, 여과된 허위 보고서의 개수를 보여주고 있다. 두 그림에서 보듯이, 본 제안 기법(ω= 0.7, 1.0)이 SEF보다 허위 보고서 탐지 성능이 우수하므로 더 높은 허위 보고서를 추출을 통해 BS로 유입되는 불량 보고서를 막기 때문에 홉이 작은 노드들의 에너지를 보존시킬 수 있다.

시뮬레이션 결과를 통해 볼 수 있듯이, 제안 기법은 각 노드의 에너지 소비 측면에서 다른 기법들보다 효율적이다. 또한, 허위 보고서 여과 측면에선 기존 SEF보다는 뛰어난 성능을 보이며 PSM, PRM과는 유사한 성능을 보인다. 따라서 제안 기법은 기존 제안 기법인 SEF, PSM 그리고 PRM과 비교했을 때, 노드의 에너지 측면에서 향상된 성능을 보이며 이는 센서 네트워크의 노드 수명을 연장할 수 있다.

5. 관련연구

무선 센서 네트워크에서 라우팅 경로는 네트워크 보안 유지를 위해 중요하다. 이러한 보안 경로를 지속시키기 위해선 상황에 맞는 경로 재설 및 관리가 요구된다. [12]에서 제안된 지역 분할 및 지역적 경로 선택 기법(region segmentation and regional path selection method; 이하 RSRPSM) 구별된 선택 노드를 이용하여 전체 경로 설정보다 구역별로 경로 선택을 통해 에너지 소비를 줄인다. [13]에서 제안된 영역별 경로 재설정 주기 결정 기법(regional path re-selection period determination method)에서는 퍼지 시스템을 이용해 각 영역의 경로 재설정 주기를 동적으로 결정하고, 주기가 결정된 영역에 대해 적절한 보안 수준을 결정한다. 본 논문에서는 지역 분할 및 지역적 경로 선택 기법과 영역별 경로 재설정 주기 결정 기법보다 전체 네트워크에서 노드들의 균형 있는 에너지 소비를 위해 PRM을 통하여 효율적인 경로 갱신을 수행하기 위해 적절한 주기를 선택한다.

6. 결론 및 향후 과제

본 논문에서는 제안 기법을 사용하여 센서 네트워크의 허위 보고서 탐지 성능을 유지하면서 에너지 효율을 높이기 위한 보안 경로 갱신 주기 결정 방법을 제안하였다. 허위 보고서 삽입 공격에 대응하기 위해 SEF을 이용하여 PSM을 기반으로 보안성은 높일 수 있었으나, 균형 있는 에너지 소비를 위해 보안 경로 주기 결정 시점 또한 중요

하다. 제안 기법은 노드의 홉 수, 보고서를 전송한 양, 그리고 BS가 받은 보고서의 양을 기반으로 경로 갱신을 위한 주기를 결정한다. 시뮬레이션 결과를 통해 보았듯이, 제안 기법 사용으로 에너지 절약을 SEF보다 약 28.31%, PSM보다 약 13.82%, 그리고 PRM보다 약 9.45%의 성능이 향상되었고(ω = 1.0), 네트워크 내에 보안성은 유지가 되었다. 따라서 제안 기법을 통해 센서 네트워크의 수명을 연기시킬 수 있다.

앞으로 입력 요소를 기반으로 퍼지 시스템에 적용하여 네트워크 상황에 따른 주기 결정 방법에 대해여 연구할 것이다.

참 고 문 헌

1. K. Akkaya and M. Younis (2005), “A Survey on Routing protocols for Wireless Sensor Networks,” Ad hoc Netw., Vol. 3, No. 3, pp. 325-349.
2. I. F. Akyildiz, W. Su, Sankarasubramaniam and E. Cayirci (2002), “Wireless sensor networks: a survey,” Computer Networks, Vol. 28, Issue. 4, pp. 393-422.
3. X. Du, H. H. Chen (2008), “Security in Wireless Sensor Networks: IEEE Wireless Commun. Soc. Vol. 15, Issue. 4, pp. 60-66.
4. W. Zhang and G. Cao (2005), “Group rekeying for filtering false data in sensor networks: a predistribution and local collaboration-based approach”, proc. of INFOCOM, Vol. 1, pp. 503-514.
5. J. N. Al-Karaki and A. E. Kamal (2004), “Routing techniques in wireless sensor networks: a survey,” IEEE Wireless Communication Magazine, Vol. 11, pp. 6-28.
6. C. Karlof et al. (2003), “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Elsevier’s Ad Hoc Networks Journal, Special Issue on Sensor Network Protocols and Applications, Vol. 1, No. 2-3, pp. 293-315.
7. Z. Yu and Y. Guan (2005), “A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks,” ACM, Proc. of Sensys, pp. 294-295.
8. W. Zhang and G. Cao (2005), “Group Rekeying for Filtering False Data in Sensor Network: A predistribution and Local Collaboration-based Approach,” Proc. of INFOCOM, pp. 503-514.
9. F. Ye, H. Luo and S. Lu (2005), “Statistical En-Route Filtering of Injected False Data in Sensor Networks,” IEEE J. Sel. Area Comm., Vol. 23, No. 4, pp. 839-850.
10. C.I. Sun, H.Y. Lee, and T.H. Cho (2009), “A path selection method for improving the detection power of statistical filtering in sensor networks,” J. Inf. Sci. Eng., Vol. 25, pp. 1163-1175.
11. J. M. Kim, Y. S. Han, H. Y, Lee, and T. H. Cho (2011), “Path Renewal Method in Filtering Based Wireless Sensor Networks,” Sensors 2011, Vol. 11, pp. 1396-1404.
12. H. Park, S. Y. Moon and T.H. Cho (2011), “A Region Segmentation Based Path Selection Method for WSNs,” International Journal of Computer Science and Network Security, Vol. 11, No. 2, pp. 88-93.
13. 박혁, 조대호 (2011), “통계적 여과 기법이 적용된 센서 네트워크에서 에너지 효율적인 네트워크 관리를 위한 영역별 경로 재설정 주기 결정 기법,” 한국시뮬레이션학회 논문지, 제20권 제3호, pp. 69-77.

남 수 만 (smnam@ece.skku.ac.kr)

2009 한서대학교 컴퓨터정보학과 이학사
2011～현재 성균관대학교 전자전기컴퓨터공학과 석사과정

관심분야 : 무선 센서 네트워크, 모델링 시뮬레이션, 네트워크 보안

선 청 일 (cisun@ece.skku.ac.kr)

2007 경원대학교 소프트웨어학부 공학사
2009 성균관대학교 전자전기컴퓨터공학과 공학석사
2009～현재 성균관대학교 전자전기컴퓨터공학과 공학박사과정

관심분야 : 무선 센서 네트워크, 모델링 시뮬레이션, 네트워크 보안, 지능 시스템

조 대 호 (taecho@ece.skku.ac.kr)

1983 성균관대학교 전자공학과 공학사
1987 University of Alabama 전자공학과 공학석사
1993 University of Arizona 전자 및 컴퓨터공학과 공학박사
1995～현재 성균관대학교 정보통신공학부 교수

관심분야 : 무선 센서 네트워크, 모델링 시뮬레이션, 지능 시스템, 모델링 방법론, 네트워크 보안 시뮬레이션, 전사적 자원 관리