韓國 컴퓨터情報學會 2007하계학술발표논문집&학회지
第15卷 第1號, 2007. 6.

센서 네트워크에서 통계적 여과 기법의 탐지능력 향상을 위한 경로 선택 기법

선 청 일*, 김 상 률*, 조 대 호*

A Path Selection Method for Improving the Detection Power of Statistical En-route Filtering in Sensor Networks

Chung Il Sun*, Sang Ryul Kim*, Tae Ho Cho*

요 약

많은 센서 네트워크 응용 분야에서 센서 노드들은 무인 환경에서 배치되므로, 물리적인 공격들과 노드가 가진 암호 키들이 손상되기 쉬운 취약성을 가진다. 위조 보고서는 훼손된 노드를 통해서 잠입할 수 있고 이 위조 보고서는 거짓 경보를 유발할 수 있을 뿐만 아니라, 네트워크의 제한된 에너지의 고갈을 야기한다. 이러한 문제점을 보안하기 위해 Ye 등은 통계적 여과 기법을 통해서 위조 보고서를 탐지하고 도중에 여과시키는 방안을 제시한다. 이 제안된 방안에서 각 노드는 검증을 위한 일정한 양의 정보를 가지며, 탐지 능력은 라우팅 경로의 선택에 의해 영향을 받는다. 본 논문에서는, 통계적 여과 기법의 위조 보고서 탐지 능력을 향상시키기 위한 경로 선택 방법을 제안한다. 각 노드는 베이스 스테이션으로부터 정해지는 각 경로들의 위조 보고서 탐지 능력을 평가하고 위조 보고서 침투 공격에 대해 가장 안전한 경로를 선택한다.

▸ Keyword : 센서 네트워크, 위조 보고서 탐지, 안전한 경로의 선택

• 제1저자 : 선청일
* 성균관대학교 전자전기컴퓨터공학과

Ⅰ. 서 론

무선 통신과 전자 공학의 진보는 낮은 전력을 가진 소형 노드로 이루어진 센서 네트워크의 개발을 가능하게 한다. [1] 탐지, 계산 그리고 무선 통신 능력들을 가진 소형 노드들은 센서 네트워크를 구성한다. [2]. 센서 네트워크는 물리적인 환경에서 새로운 단계의 다양한 응용 분야에 영향을 미칠 것으로 기대된다 [3]. 많은 응용 분야에서, 센서 네트워크는 개방적인 무인의 환경에서 배치되므로, 노드의 물리적인 파괴, 한정된 자원을 가진 노드의 에너지 소비 공격 등 여러 공격의 취약성을 가진다 [4].

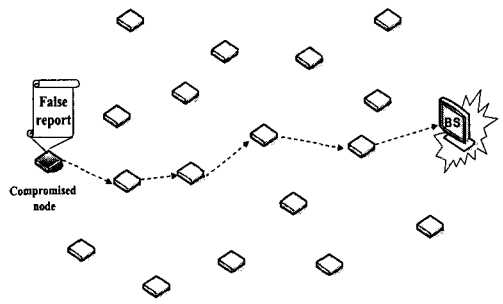

그림 1. 위조 보고서 침투 공격

또한, 공격자는 노드를 훼손시키고, 훼손된 노드를 통해 위조 감지 데이터를 네트워크에 침투시킬 수 있는데, 이는 거짓 경보를 유발할 수 있을 뿐만 아니라 네트워크의 제한된 에너지의 고갈을 야기 시킨다 [5]. 심각한 피해를 줄이기 위해선, 위조 감지 보고서는 가능한 빨리 탐지되어 제거해야 하며, 탐지 하지 못한 보고서는 베이스 스테이션에서 제거되어야한다 [6].

Fan Ye 등은 위조 보고서의 탐지와 여과를 위한 통계적 여과 기법(SEF: statistical en-route filtering scheme)을 제안하였다. 이 기법에서, 많은 감지 노드들은 다수의 메시지 인증 코드(MAC: message authentication code)를 포함하여 감지 보고서를 생성 한다. 메시지 인증 코드는 노드가 가진 암호 키를 사용하여 생성 되며, 이는 감지 보고서에 대한 동의를 의미 한다 [7]. 감지 보고서는 다수의 홉을 지나 베이스 스테이션으로 전달되는데, 만약 전달 노드가 리포트가 포함한 MAC을 생성하는데 사용한 키를 가지고 있다면 자신의 키를 이용하여 보고서를 검증하고, 그렇지 않다면 검증 과정 없이 보고서를 전달한다. 그러므로 통계적 여과 기법에서 탐지 능력은 라우팅 경로의 선택에 큰 영향을 받는다.

본 논문은 SEF의 탐지 능력을 향상시키기 위한 경로 선택 방법에 대해 제안한다. 라우팅 경로 생성을 위한 각 메시지들은 거치는 노드들의 키에 대한 정보를 포함한다. 이 정보를 이용해서, 각 노드는 베이스 스테이션으로부터 들어오는 각 경로의 탐지 능력을 평가한다. 그래서 각 노드는 위조 보고서 침투 공격에 대해서 가장 안전한 경로를 선택할 수 있고 초기에 발견함으로써, 에너지의 소모도 줄일 수 있다. 본 논문은 다음과 같이 구성된다. 2장에서는 SEF의 개요에 대해 설명하고 3장에서는 제안된 방법에 대해 자세히 설명한다. 마지막으로 4장에서는 결론을 논의한다.

2. 통계적 여과 기법(SEF)

이 기법에서, 베이스 스테이션은 사용자에 의해 전체 키 정보를 담고 있는 전체 키 풀(global key pool)을 임의의 값만큼의 구획(partition)으로 나눈다. 각 구획은 서로 다른 키들로 구성된다. 각 노드들은 네트워크에 배치되기 전에 전체 키 풀의 임의로 선택된 구획으로부터 작은 수의 키들을 적재한다.

실제 이벤트가 발생하면, 이벤트를 감지한 노드들 중 가장 감지 강도가 강한 노드를 CoS(center-of-stimulus) 노드로 선별하여 감지 보고서를 생성한다. 같은 이벤트를 감지한 주변 노드들은 자신의 키를 이용하여 MAC을 생성하고 이벤트 정보와 함께 CoS에게 전달한다. 전달된 MAC들은 보고서가 정상인지를 증명하는 역할을 한다. CoS는 보고서를 다수의 홉 방식으로 베이스 스테이션에 전달한다. 각 전달 노드들은 자신의 키를 이용하여 리포트 안에 포함되어있는 MAC이 정당한지를 검증한다. 보고서가 베이스 스테이션으로 전달되면, 전체 키 풀의 정보를 가지고 있는 베이스 스테이션에 의해 모든 MAC들이 검증된다.

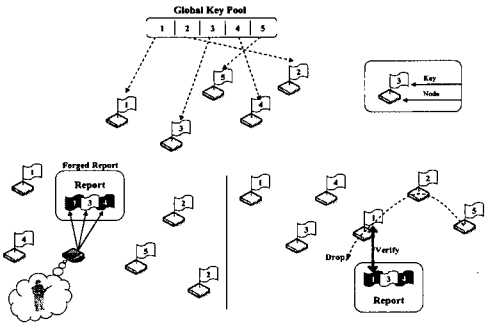

그림 2 위조 보고서 여과

그림 2와 같이 공격자는 훼손된 노드를 통하여 잘못된 MAC을 이용하여 위조 보고서를 생성할 수 있다. 하지만 위조 보고서는 보고서가 가지는 일정한 확률의 정확한 MAC들을 검증해서 도중에 제거 될 수 있다. 잘못된 MAC의 탐지할 확률은 보고서가 거치는 홉의 수에 따라 높아진다. SEF 방식은 공격자가 고정된 수의 훼손 구획으로 생성한 거짓 보고서를 탐지할 수 있다.

3. 경로 선택 방법

3.1 가정

라우팅 경로는 전달되는 조작 메시지에 의해 설립되며, 이 메시지는 네트워크 토폴로지의 변화 혹은 사용자의 요청에 의해 베이스 스테이션에서 브로드 캐스트 된다. 또한, 네트워크는 단일 라우팅 경로 프로토콜을 사용하며, 각 노드들은 베이스 스테이션으로부터 거리와 거짓 보고서 공격에 대한 안전 단계를 기반으로 라우팅 경로를 선택한다.

3.2 개요

본 논문에서는, 모든 조작 메시지들은 지나치는 노드들의 구획 식별 번호 정보들을 추가적으로 포함한다. 이 정보는 경로의 안전 단계를 평가하는데 사용된다. 조작 메시지가 네트워크를 통해서 멀티 홉 방식으로 전달되면서, 각 전달노드들은 메시지의 구획 식별 번호 정보를 갱신한다. 라우팅 경로는 베이스 스테이션으로 부터의 거리와 안전 단계를 고려한 평가 함수를 사용하여 노드에 의해 선택된다. 다양한 값을 가지는 안전 무게 요소에 의해 사용자는 안전성 혹은 에너지 소비에 우선순위를 둘 수 있다.

3.3 경로 선택법

베이스 스테이션은 다수의 구획으로 나누어진 전체 키 풀을 포함하고, 각 구획은 고유한 식별 번호를 가진다. 각 노드는 네트워크에 배치되기 전, 키 풀에서 임의로 선택된 한 구획으로부터 키를 가진다. 이 키들은 MAC들을 생성하거나 검증하는데 사용된다. 노드를 배치한 후, 라우팅 경로는 베이스 스테이션이 브로드 캐스트한 조작 메시지에 의해 설립된다. 대부분의 라우팅 프로토콜에서, 조작 메시지는 보내는 노드의 식별 번호와 베이스 스테이션으로 부터의 홉 수를 포함한다. 본 논문에서는, 각 조작 메시지에 추가적으로 비트로 이루어진 배열을 첨부한다. 이 배열은 지나온 노드들의 구획 식별 번호를 표시하는데 사용된다.

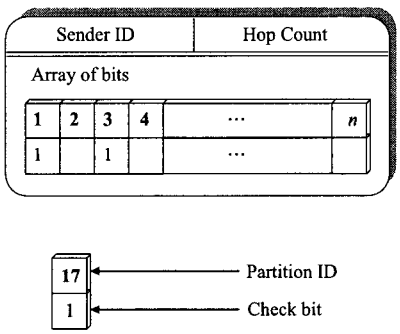

그림 3. 조작 메시지의 구조

전체 키 풀이 n개의 구획으로 나누어 질 때의 조작 메시지의 구조를 그림 3에서 보여준다. 노드가 조작 메시지를 전달 받으면, 노드는 메시지의 자신의 고유 식별 번호, 베이스 스테이션으로 부터의 홉 수를 저장하고 첨부된 배열에 자신의 키 정보를 이용하여 자신의 구획 식별 번호와 동일한 배열의 자리에 체크 비트를 이용하여 표시한다. 만약 도착한 메시지가 처음으로 전달 받은 조작 메시지라면, 노드는 자신의 키들의 구획 식별 번호를 메시지 안의 배열에 표기하고 홉 수를 증가시킨 후, 갱신 된 조작 메시지를 전달한다. 그림 3은 전 체 키 풀이 5개의 구획으로 나누어 졌을 때, 조작 메시지 내의 구획 식별 번호 배열이 어떻게 갱신되는지를 보여준다. 2번, 17번 그리고 1번 노드는 제각기 1번, 2번 그리고 16번의 구획으로부터 몇 개의 키들이 존재한다. 2번 노드가 조작 메시지를 수신할 때, 노드는 메시지에 자신의 정보를 적재한다. 만약 이 노드가 처음으로 조작 메시지를 수신했다면, 배열에 첫 번째 자리에

체크 비트를 기록한다(2번 노드는 1번 구획으로부터 키를 가지고 있다). 노드는 홉 수를 증가시키고 자신의 식별 번호를 기입 후 메시지를 갱신한다. 17번 노드는 메시지를 수신하면, 구획 식별 번호 배열 2번에 체크 비트를 기록한 후 메시지에 추가적인 정보를 입력하여 전달하게 된다. 1번 노드도 2번, 17번 노드와 같은 방법으로 메시지를 갱신하여 전달한다.

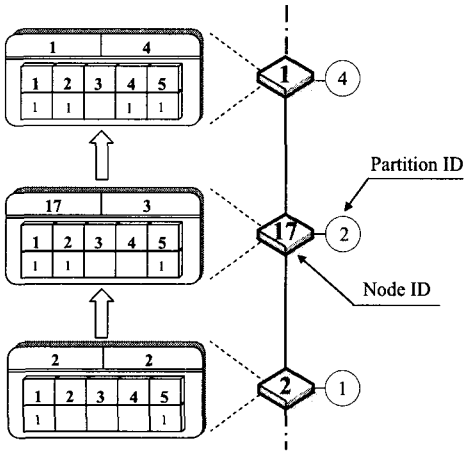

그림 4. 조작 메시지 전달

네트워크의 모든 노드들에게 메시지 전달이 끝난 후, 각 노드들은 구획 식별 번호 배열을 토대로 각 경로의 탐지 능력을 평가한다. 만약 어떠한 경로에 대한 배열에 모든 비트가 기록 되어있다면, 그 경로는 대부분의 위조 보고서를 탐지 할 수 있다. 즉, 그 경로는 위조 보고서 침투 공격에 대해 가장 안전하다고 할 수 있다. 어떠한 경로의 구획 식별 번호 배열에 적은 수의 체크 비트 혹은 배열이 비어있다면, 대부분의 보고서들은 검증되지 않고 전달될 것이다. 탐지 능력과 오버 헤드 사이에는 상관관계가 있다. 정상 보고서에 관해서, 전자의 경로가 후자의 경로 보다 에너지 소비 차원에서 더 비효율적일 것이다. 그림 5에서, 아래 경로가 구획 식별 배열이 모두 채워져 있기 때문에 위 경로 보다 위조 보고서 침투 공격에 안전할 것이다. 하지만 아래 경로는 보고서를 전달하는데 위 경로보다 에너지 소모가 클 것이다. 한편, 위 경로는 아래 경로보다 공격 받기 쉽지만, 보고서 전달에 있어 에너지 소모에 효율적일 것이다.

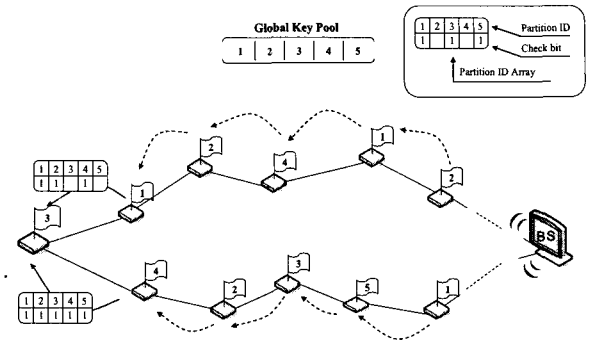

그림 5. 구획 식별 배열의 갱신

경로는 평가 함수에 의해 결정된다. 이 평가 함수는 경로의 탐지 능력과 홉 수를 토대로, 경로가 안전하면서 에너지 소비가 적은지를 판단하여 경로의 질을 결정한다. 평가 함수는 다음과 같은 식으로 표현된다.

$$Q(p) = D(p) + \omega \cdot P(p) \quad \cdots\cdots (1)$$

위 식에서 p는 경로를 나타내고, D(p)는 경로 p의 홉 수를 나타낸다. ω는 안전 요소로써 사용자에 의해 결정되며, P(p)는 경로 p로부터 수신한 구획 식별 배열에 체크 비트로 채워지지 않은 구획의 수를 나타낸다. 작은 Q(p)의 값을 가지는 경로일수록 더 좋은 경로가 된다. 예를 들어, 그림 6에서 위 경로의 질은 Q(위 경로) = D(위 경로) + 2·ω이고, 아래 경로의 질은 Q(아래 경로) = D(아래경로)이다. 그러므로 노드는 ω의 값이 0이 아니라면 라우팅 경로로써 아래 경로를 선택한다. ω의 값이 0이라는 것은 네트워크가 라우팅 경로를 설정하는데 탐지 능력을 고려하지 않는다는 것이다.

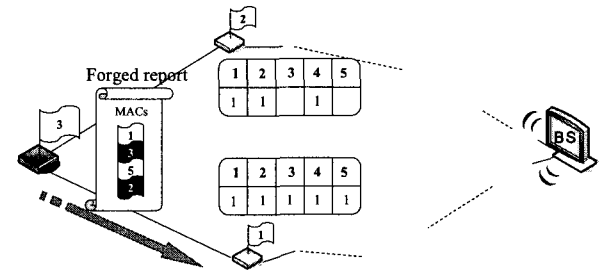

그림 6. 가장 안전한 경로 선택

4. 결론

본 논문에서는 SEF에서 탐지 능력을 향상시키기 위한 경로 선택 방법에 대해 보여주었다. 노드로 전해오는 경로의 구획 식별 배열을 사용하여, 각 노드는 위조 보고서 침투 공격에 대해 안전한 경로를 선택할 수 있다. 간단한 함수는 노드로 전해오는 경로의 질을 평가하여 노드로 하여금 경로를 선택할 수 있게 해준다. 이는 차후 시뮬레이션을 통하여 통계적 여과 기법과 본 논문에서 제안한 방법을 비교하여 효율성을 보여줄 것이다.

참고문헌

[1] K. Akkaya and M. Younis, "A Survey on Routing protocols for Wireless Sensor Networks", Ad hoc Netw., vol.3, no.3, pp.325-349, 2005.

[2] S.H Chi and T.H. Cho, "Fuzzy Logic based Propagation Litmiting Method for Message Routing in Wireless Sensor Networks", Lect. Notes Comput. Sc., vol.3983, pp.58-64, 2006.

[3] F. Ye, H. Luo and S. Lu, "Statistical En-Route Filtering of Injected False Data in Sensor Networks", IEEE J. Sel. Area Comm., vol.23, no.4, pp.839-850, 2005.

[4] B. Przydat다, D. Song and A. Perrig, "SIA: Secure Information Aggregation in Sensor Netwok", Proc. of Sensys, pp.255-265, 2003.

[5] W. Zhang and G. Cao, "Group Rekeying for Filtering False Data in Sensor Network: A predistribution and Local Collaboration-based Approach", Proc. of INFOCOM, pp.503-514, 2005.

[6] H. Yang and S. Lu, "Commutative Cipher based En-Route Filtering in Wireless Sensor Networks", Proc of VTC, pp.1223-1227, 2003.

[7] F. Li and J. Wu, "A Probabilistic Voting-based Filtering scheme in Wireless Sensor Networks", Proc. of IWCMC, pp.27-32, 2006.