Proceedings of KFIS Autumn Conference 2007 Vol. 17, No. 2.

센서 네트워크에서 거짓 보고서 탐지 능력을 향상시키기 위한 퍼지 기반의 경로 선택 방법[1)]

Fuzzy based Path Selection Method for Improving Detection Power in Sensor Networks

선청일[1], 조대호[2]

[1] 수원시 장안구 성균관대학교 정보통신공학부
E-mail: cisun@ece.skku.ac.kr
[2] 수원시 장안구 성균관대학교 정보통신공학부
E-mail: taecho@ece.skku.ac.kr

요 약

센서 네트워크 응용 분야에서 센서 노드들은 무인 환경에서 배치되므로, 물리적인 공격들과 노드가 가진 암호 키들이 손상되기 쉬운 취약성을 가진다. 공격자는 노드를 훼손시켜 위조 보고서를 침투 시킬 수 있고, 이는 거짓 경보를 유발시켜 네트워크의 제한된 에너지의 고갈을 야기한다. 이러한 문제점을 보안하기 위해 최근 연구자들은 통계적 여과 기법을 통해서 위조 보고서를 탐지하고 도중에 여과시키는 방안을 제시하였다. 이 제안된 방안에서 각 노드는 검증을 위한 일정한 양의 정보를 가지며, 탐지 능력은 라우팅 경로의 선택에 의해 영향을 받는다. 본 논문에서는, 퍼지를 사용하여 통계적 여과 기법의 위조 보고서 탐지 능력 향상을 위해 네트워크 전체 상황을 고려하여 거짓 보고서 침투 공격에 대해 가장 안전한 경로를 선택하는 방법을 제안한다.

Key Words : 센서 네트워크, 거짓 보고서 필터링, 경로 선택 방법, 퍼지 로직

1. 서 론

저 전력, 탐지, 계산 그리고 무선 통신 능력을 가진 소형 노드들은 전자 공학의 진보와 더불어 센서 네트워크의 개발을 가능하게 한다.[1,2] 많은 응용 분야에서, 센서 네트워크는 소형 노드들로 구성되고 무인의 환경에 무작위로 배치된다. 센서 노드는 물리적인 파괴, 한정된 에너지 소비 공격, 노드의 암호 키 손상 등 여러 공격의 취약성을 가진다.[3] 또한, 공격자는 노드를 훼손시키고, 훼손된 노드를 통하여 위조 감지 데이터를 네트워크에 침투시킬 수 있는데, 이는 거짓 경보를 유발할 수 있을 뿐만 아니라 네트워크의 제한된 에너지의 고갈을 야기 시킨다.[4] 이러한 피해를 줄이기 위해선, 위조 감지 보고서는 가능한 빨리 탐지되어 제거해야 하며, 탐지 하지 못한 보고서는 베이스 스테이션에서 제거되어야 한다.[5]

Fan Ye 등은 위조 보고서의 탐지와 여과를 위한 통계적 여과 기법(SEF: statistical en-route filtering scheme)을 제안하였다. 이 기법에서, 이벤트를 감지한 많은 노드는 다수의 메시지 인증 코드(MAC: message authentication code)를 포함한 감지 보고서를 생성한다. 메시지 인증 코드는 각 노드가 가진 암호 키를 이용하여 생성되며, 암호 키는 노드가 네트워크에 배치되기 전 모든 노드에게 분배된다.[6] 감지 보고서는 다수의 홉을 지나 베이스 스테이션으로 전달된다. 전달 과정에서 만약 전달 노드가 보고서가 포함한 MAC을 생성하는데 사용한 키를 가지고 있다면 자신의 키를 사용하여 보고서를 검증한다.

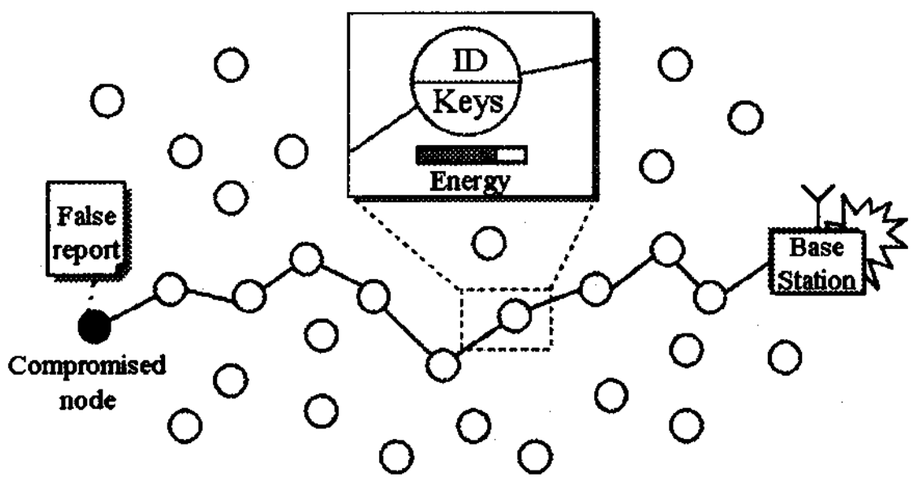


그림1. 훼손 노드를 통한 위조 보고서 공격

1) 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2007-C1090-0701-0028)

위조 감지 보고서를 탐지하고 빠르게 여과하기 위해선 라우팅 경로 상에 전달 노드들은 많은 키 정보를 가지고 있어야 한다. 위조 감지 보고서가 전달 노드에게 탐지 되지 않고 베이스 스테이션으로 전달되어 여과되면, 노드의 에너지 소모뿐만 아니라 네트워크 전체의 에너지 소모를 일으킨다. 위조 감지 보고서를 탐지하고 여과하기 위해선 많은 키 정보를 가지는 안전 경로를 선택해야 하고, 이를 통하여 네트워크 전체의 에너지 소모를 줄일 수 있다. 그러므로 통계적 여과 기법에서 탐지 능력은 라우팅 경로의 선택에 큰 영향을 받는다.

본 논문은 SEF의 탐지 능력을 향상시키기 위해 퍼지를 이용하여 경로 선택 방법을 제안한다. 라우팅 경로 생성을 위한 각 조작 메시지들은 거치는 노드들의 키 정보를 포함하고, 수집된 정보를 사용해서 각 노드는 베이스 스테이션으로부터 들어오는 각 경로를 평가한다. 각 노드는 보안 비중 값, 구획 식별 번호 정보 그리고 베이스 스테이션과의 거리를 변수로 퍼지 규칙을 사용하여 라우팅 경로를 결정한다. 그래서 위조 보고서 침투 공격에 대해서 가장 안전한 경로를 선택하고 초기에 위조 탐지 보고서를 발견함으로써, 에너지 소모도 줄일 수 있다. 본 논문은 다음과 같이 구성된다. 2장에서는 통계적 여과 기법의 개요에 대해 설명하고 3장에서는 제안된 방법에 대해 자세히 설명한다. 마지막으로 4장에서는 결론을 논의한다.

2. 통계적 여과 기법(SEF)

통계적 여과 기법에서, 베이스 스테이션은 사용자에 의해 전체 키 정보를 담고 있는 전체 키 풀을 P개의 구획으로 나눈다. 각 구획은 n/P개의 키들로 구성된다.(전체 키의 개수 n) 각 노드들은 네트워크에 배치되기 전에 전체 키 풀의 임의로 선택된 구획에서 작은 수의 키들을 적재한다. 전체키 풀의 분할 및 구획 선택, 각 구획 당 노드에게 할당할 인증키의 수는 사용자에 의해 결정된다.

네트워크에 실제 이벤트가 발생하면, 이벤트 발생지역에서 이벤트를 감지한 노드들 중 가장 감지 강도가 강한 노드를 CoS(center-of-stimulus)노드로 선별한다. CoS 노드는 이벤트가 발생한 곳으로부터 가까운 노곳에 위치한 노드가 보고서 생성과 보고서에 포함시켜야할 메시지 인증 코드를 모으는 역할을 한다. CoS는 자신이 감지한 이벤트 정보를 같은 이벤트를 감지한 주변 노드에게 브로드캐스트하고, 이벤트 정보를 전달받은 주변 노드들은 자신이 감지한 이벤트 정보와 같은 정보인지 확인한다. 이벤트 정보가 같으면 각 노드들은 자신의 키, 이벤트 정보를 해쉬 함수를 사용하여 MAC(메시지 인증 코드)을 생성하고, MAC생성 시 사용된 키와 함께 CoS에게 전달한다. CoS는 전달 받은 이벤트 감지 노드들의 정보를 하나의 보고서로 생성하여 다수의 홉 방식으로 베이스 스테이션으로 전달한다. 각 노드들은 자신의 키들을 이용하여 보고서에 포함된 MAC이 정상인지를 검증 한다.

공격자에 의해 훼손된 노드가 위조된 키를 이용하여 MAC을 생성하고 위조 보고서를 만들 수 있다. 위조 보고서는 베이스 스테이션으로 전달되면서, 전달 노드들이 가지는 정상키로 검증될 수 있다. 만약 이 과정에서 전달 노드들이 위조 보고서를 제거 하지 못하고 베이스 스테이션으로 전달되면, 모든 키를 가지고 있는 베이스 스테이션에서 다시 한 번 검증하게 된다. 이와 같이, 통계적 여과 기법은 위조 보고서 삽입 공격에 대응할 수 있다. 하지만, 위조 보고서가 전달 과정에서 여과되지 않고 베이스 스테이션까지 전달되어 여과된다면 네트워크 및 노드의 에너지 소모가 커질 것이다. 에너지 소모를 줄이기 위해서는 전달과정에서 빠르게 탐지되어 여과되어야 한다. 위조된 보고서가 탐지 될 확률은 전달 경로 상에 전달 노드가 여러 구획의 키 정보를 가지는 것에 영향을 받는다. 전달 경로 상에 노드들이 여러 구획의 키 정보를 가지면, 위조된 보고서의 잘못된 MAC정보를 탐지할 확률이 높아져 제거할 수 있으면 에너지의 소모 또한 줄일 수 있다.

3. 퍼지 기반의 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 프로토콜을 사용하며, 각 노드는 베이스 스테이션으로부터의 거리, 보안 비중 값, 구획 식별 번호 정보 등을 고려하여 라우팅 경로를 선택한다.

3.2 경로 선택을 위한 퍼지 로직의 적용

3.2.1 경로의 평가 값 결정 요소들

각 노드는 베이스 스테이션으로부터 들어오는 경로의 질을 평가하여 선택한다. 각 경로의 선택 값은 베이스 스테이션으로부터의 거리, 보안 비중 값, 구획 식별 번호 정보를 고려하여 결정된다. 베이스 스테이션으로부터 거리가

멀수록 지나치는 노드의 수가 많아 위조 보고서를 탐지할 확률은 높아지고, 또한 조작 메시지 내의 키의 정보가 많으면 탐지할 확률이 높아진다. 보안 비중 값은 전체 네트워크의 에너지 수준과 위조 보고서 탐지 여과율을 고려하여 사용자가 결정한다.

3.2.2 퍼지 로직의 입, 출력 파라미터

입력 파라미터는 노드와 베이스스테이션으로부터의 거리(H), 보안 비중 값(w), 조작 메시지내의 키의 정보(P)이며, 출력 파라미터는 경로의 선택 값(Q)이다.

▪ 입력 파라미터

H(Hops) = {NEAR, FAR, VERY_FAR}

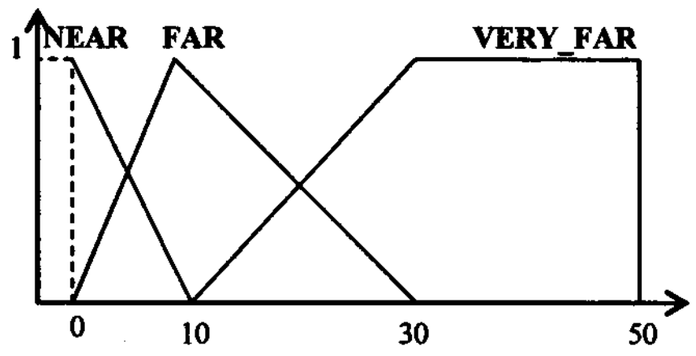
W(security weight factor) = {VERY_SMALL, SMALL, MEDIUM, LARGE, VERY_LARGE}

P(Partition value) = {LOW, MEDIUM, HIGH}

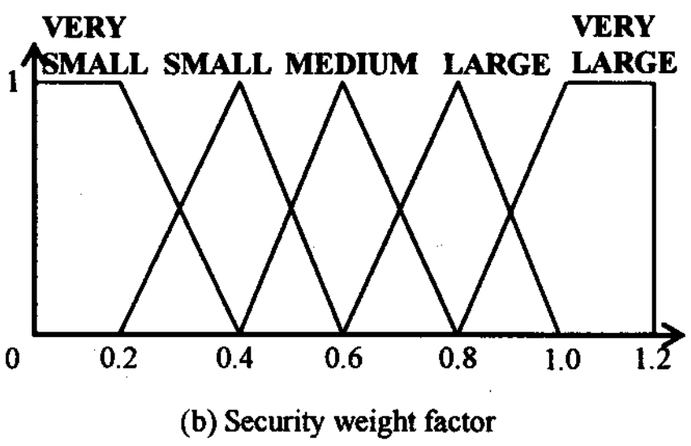
▪ 출력 파라미터

Q(Quality of a path) = {VERY_LOW, LOW, MEDIUM, HIGH, VERY_HIGH}

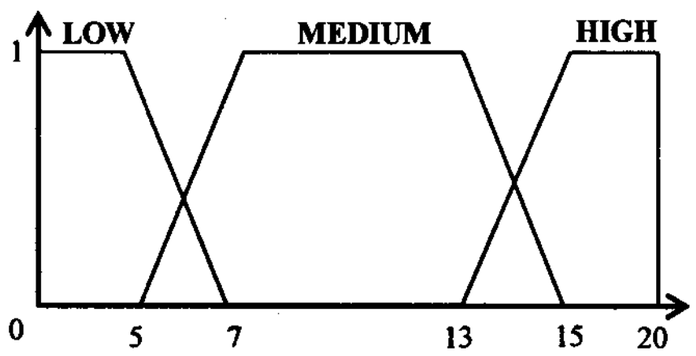
3.2.3 멤버십 함수



(a) Hops of a node

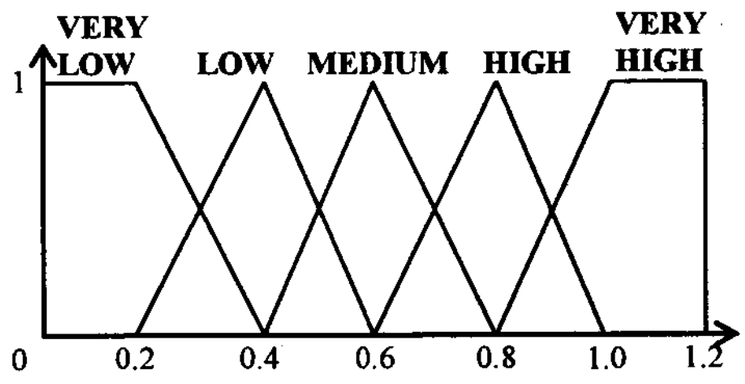


(b) Security weight factor



(b) # of set partition array

그림2. 입력 파라미터 멤버십 함수



(d) Quality of a path

그림3. 출력 파라미터 멤버십 함수

3.2.4 퍼지 규칙

RULE 0: IF (H is NEAR) AND (W is VERY_SMALL) AND (P is LOW) THEN (Q is VERY_LOW)

RULE 1: IF (H is NEAR) AND (W is SMALL) AND (P is LOW) THEN (Q is VERY_LOW)

RULE 9: IF (H is NEAR) AND (W is LARGE) AND (P is MEDIUM) THEN (Q is MEDIUM)

RULE 35: IF (H is FAR) AND (W is LARGE) AND (P is HIGH) THEN (Q is HIGH)

3.2.5 추론

추론에는 퍼지 이론의 추론 모델 중 하나인 만다니(mandani) 모델의 min-max 합성법을 사용하고, 실수 값 출력을 위한 역 퍼지화(defuzzification)방법에는 무게 중심 법(Center of Area)을 사용한다.

3.2.6 경로 선택법

베이스 스테이션은 다수의 구획으로 나누어진 전체 키 풀을 포함하고, 각 구획은 고유한 식별 번호를 가진다. 각 노드는 네트워크에 배치되기 전, 사용자에 의해 임의의 한 구획으로부터 키를 가진다. 이 키들은 이벤트 감지 시 MAC을 생성하거나 보고서 전달 시 검증하는 역할을 한다. 노드가 네트워크에 무작위로 배치된 후, 라우팅 경로는 베이스 스테이션이 브로드 캐스트 한 조작 메시지에 의해 설립된다. 대부분의 라우팅 프로토콜에서, 조작 메시지는 보내는 노드의 식별 번호와 베이스 스테이션으로 부터의 거리를 포함한다. 본 논문에서는, 조작 메시지에 추가적으로 구획 식별 번호를 저장할 수 있는 배열을 첨부한다. 이 배열에는 베이스 스테이션에서 나눈 구획수와 동일한 크기이며, 지나온 노드들의 구획 식별 번호를 표시한다.

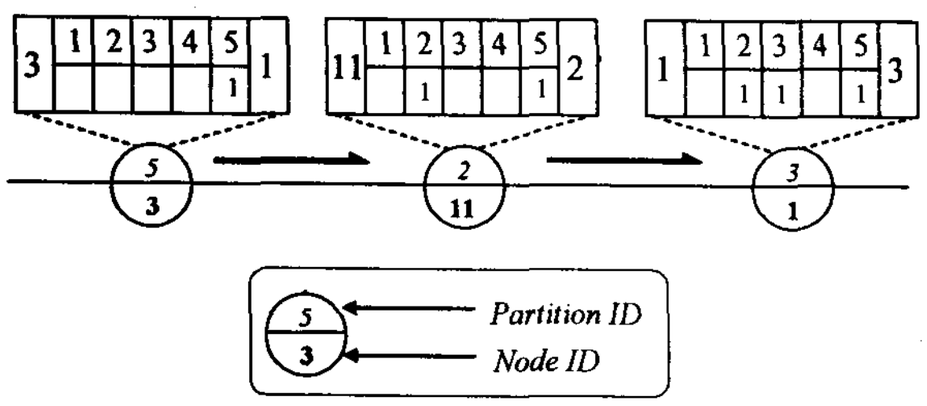


그림4. 조작 메시지 전달

그림 4는 전체 키 풀이 5개의 구획으로 나누어 졌을 , 조작 메시지 내의 구획 식별 번호 배열이 어떻게 갱신되는지 보여준다. 3번, 11번 그리고 1번 노드는 각각 5번,2번 그리고 3번의 구획에서 몇 개의 키들을 가지고 있다. 3번 노드는 조작 메시지를 수신한 뒤, 조작 메시지에 자신의 식별번호 3을 기록하고 구획 식별 번호 2를 동일 배열자리에 기록한다. 마지막으로 홉 카운트를 증가시키고 다음 노드인 11번 노드에게 전달한다. 11번 노드도 같은 과정을 통해 다음노드에게 전달한다.

네트워크의 모든 노드들에게 메시지 전달이 끝난 후, 각 노드들은 구획 식별 번호 정보, 홉 수, 보안 비중 값을 토대로 각 경로의 탐지 능력을 평가한다. 만약 어떠한 경로에 대한 배열에 모든 비트가 기록되어있다면, 그 경로는 대부분의 위조 보고서를 탐지할 수 있을 것이다. 즉, 그 경로는 위조 보고서 침투 공격에 대해 가장 안전하다고 할 수 있다. 각 노드는 경로 선택 시, 전달되는 조작메시지의 구획 식별 번호 정보, 베이스 스테이션으로부터의 거리 그리고 사용자가 미리 결정한 보안 비중 값을 입력 값으로 퍼지 시스템을 사용하여 각 경로의 선택 값을 평가한다. 경로 선택 값이 큰 경로를 선택함으로써, 위조 보고서 침투 공격에 대한 탐지 능력을 향상시키고, 빠르게 제거함으로써 에너지의 소모도 줄일 수 있다.

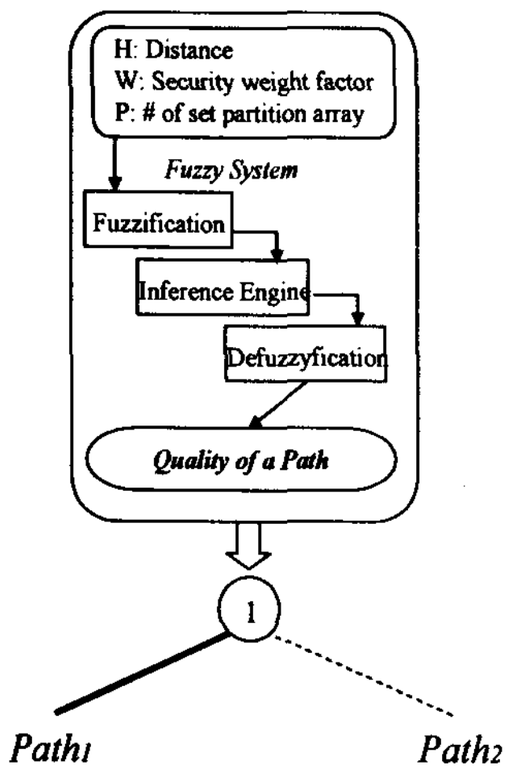


그림5. 퍼지 로직을 이용한 경로 선택

4. 결론

본 논문에서는 통계적 여과 기법에서 탐지 능력을 향상시키기 위해 퍼지 시스템을 이용한 경로 선택 방법에 대해 제안하였다. 노드로 전해 들어오는 경로의 구획 식별 번호 정보, 베이스 스테이션으로부터의 거리, 사용자가 정의한 보안 비중 값을 입력 값으로 퍼지 시스템을 사용하여 경로의 선택 값을 평가하여 안전도가 높은 경로를 선택할 수 있다. 차후 시뮬레이션을 통하여 통계적 여과 기법과 본 논문에서 제안한 방법을 비교하여 위조 보고서 탐지 능력과 에너지 소비에서 효율성을 보여줄 것이다.

참 고 문 헌

[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] 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.

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

[4] 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.

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

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