한국시뮬레이션학회 논문지
Vol. 16, No. 2, pp. 27-35 (2007. 6)

통계적 여과 기법기반의 센서 네트워크를 위한 퍼지로직을 사용한 보안 경계 값 결정 기법

김상률[1] · 조대호[1†]

Determination Method of Security Threshold using Fuzzy Logic for Statistical Filtering based Sensor Networks

Sang-Ryul Kim · Tae-Ho Cho

ABSTRACT

When sensor networks are deployed in open environments, all the sensor nodes are vulnerable to physical threat. An attacker can physically capture a sensor node and obtain the security information including the keys used for data authentication. An attacker can easily inject false reports into the sensor network through the compromised node. False report can lead to not only false alarms but also the depletion of limited energy resource in battery powered sensor networks. To overcome this threat, Fan Ye *et al.* proposed that statistical en-route filtering scheme(SEF) can do verify the false report during the forwarding process. In this scheme, the choice of a security threshold value is important since it trades off detection power and energy, where security threshold value is the number of message authentication code for verification of false report. In this paper, we propose a fuzzy rule-based system for security threshold determination that can conserve energy, while it provides sufficient detection power in the SEF based sensor networks. The fuzzy logic determines a security threshold by considering the probability of a node having non-compromised keys, the number of compromised partitions, and the remaining energy of nodes. The fuzzy based threshold value can conserve energy, while it provides sufficient detection power.

Key words : Sensor network, False report filtering, Fuzzy logic

요 약

개방된 환경에 배치된 센서 네트워크의 모든 센서 노드들은 물리적 위협에 취약하다. 공격자는 노드를 물리적으로 포획하여 데이터 인증에 사용하는 인증키와 같은 보안 정보들을 획득할 수 있다. 공격자는 포획된 노드, 즉 훼손된 노드들 통해 허위 보고서를 센서 네트워크에 쉽게 삽입시킬 수 있다. 이렇게 삽입된 허위 보고서는 사용자로 하여금 허위 경보를 유발시킬 수 있을 뿐만 아니라, 전지로 동작하는 센서 네트워크의 제한된 에너지를 고갈시킨다. Fan Ye 등은 이런 위협에 대한 대안으로 전송과정에서 허위 보고서를 검증할 수 있는 통계적 여과 기법을 제안하였는데, 이 기법에서는 허위 보고서에 대한 보안성과 소비 에너지양이 서로 대치되는 관계에 있기 때문에, 허위 보고서 검증을 위한 메시지 인증 코드의 수를 나타내는 보안 경계 값의 결정은 매우 중요하다. 본 논문에서는 충분한 보안성을 제공하면서 에너지를 보존할 수 있는 보안 경계 값 결정을 위한 퍼지 규칙 시스템을 제안한다. 퍼지 로직은 노드가 훼손되지 않은 인증키를 가지고 있을 확률, 훼손된 구획의 수, 노드의 잔여 에너지를 고려하여 보안 경계 값을 결정한다. 퍼지 기반 보안 경계 값은 충분한 보안성을 제공하면서 에너지를 보존할 수 있는 보안 경계 값을 결정 할 수 있다.

주요어 : 센서 네트워크, 허위 보고서 여과, 퍼지 로직

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음. (IITA-2006-C1090-0603-0028)
* 이 연구에 참여한 연구자(의 일부)는 2단계 BK21 사업의 지원비를 받았음.
2007년 3월 5일 접수, 2007년 6월 14일 채택
[1] 성균관대학교 정보통신공학부
주 저 자 : 김상률
교신저자 : 조대호
E-mail; taecho@ece.skku.ac.kr

1. 서 론

최근 마이크로 전자 기기 시스템과 무선 통신 기술의 진보는 저비용의 센서 네트워크의 발전을 가져왔다[1]. 센서 네트워크는 주변 환경 정보를 수집할 수 있는 감지 기능과, 정보 처리 기능, 무선 통신 기능을 가지고 있는 소형 센서 노드(sensor node)들과 감지한 정보들의 집중국 역할과 사용자와 노드간의 게이트웨이 역할을 하는 베이스 스테이션(BS: base station)으로 구성된다. 기본적으로 센서 노드들은 사용자가 정보를 얻고자 하는 지역에 뿌려지며, 각 센서 노드들은 감지한 주변 환경 정보를 베이스 스테이션으로 전달하고, 베이스 스테이션은 인터넷과 같은 기존 통신 인프라를 통하여 사용자에게 해당 정보를 제공한다[2]. 이런 센서 네트워크는 전례가 없는 수준의 다양한 응용을 가능하게 할 것으로 기대되고 있다[3].

하지만 많은 센서 네트워크 응용분야에서 센서 노드들이 개방된 환경에 배치되기 때문에, 공격자에 의한 물리적 공격에 취약하다[4]. 만약 공격자가 노드를 포획하여 인증키와 같은 보안 정보를 획득하면, 공격자는 획득한 인증키로 허위 정보를 담은 허위 보고서(false report)를 생성해서, 이 허위 보고서를 공격자에게 포획당한 훼손된 노드(compromised node)를 통해 그림 1과 같이 센서 네트워크에 삽입할 수 있다. 이 공격으로 공격자는 허위 보고서를 사용자에게 전달해서 허위 정보로 인한 허위 경보(false alarm)를 유발시킬 수 있을 뿐만 아니라, 전달 경로상에 있는 센서 노드들이 허위 보고서를 검증하지 못하고 베이스 스테이션까지 전달함으로써 센서 노드들의 제한된 에너지 자원이 소모되어 센서 네트워크의 수명이 단축된다[5].

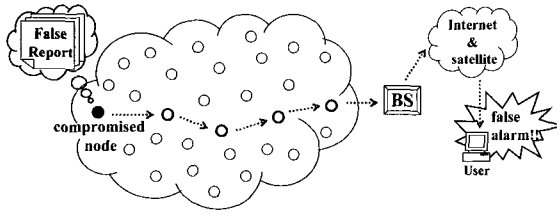


그림 1. 허위 보고서 삽입에 의한 거짓 경보 발생

이러한 심각한 피해를 최소화하기 위해서는 센서 네트워크에 삽입된 허위 보고서를 가능한 한 빨리 발견하여 제거하여야 하며, 발견되지 못한 허위 보고서는 최소한 베이스 스테이션에서 발견돼서 사용자에게 전달되지 않아야 한다[6]. 최근 몇몇 보안 기법이 이러한 목적을 위하여 제안되었다. Zhu 등[3]은 상호배치 인증(interleaved authentication)을 통하여 허위 보고서를 발견할 수 있는 기법을 제안하였고, Zhang 등[7]은 꼬인 다중 경로 라우팅(braided multipath routing) 기반 네트워크에서 허위 보고서 여과를 위한 상호 배치 인증 기법을 제안하였다. 그리고 Fan Ye 등[5]은 노드 배치 전에 인증키들의 집합인 전역 키 풀(global key pool)을 여러 개의 구획(partition)으로 나눠 서로 다른 구획의 인증키들을 모든 센서 노드들에게 나누어 할당해서 노드들이 서로 협력하여 허위 보고서를 검증하는 통계적 여과 기법(statistical filtering scheme)을 제안하였다. 이러한 보안 기법들에서는 센서 노드들이 어떠한 사건(event)을 감지하고 사건에 대한 정보를 담은 보고서(report)를 사용자에게 전달할 때 같은 시간에 동일한 사건을 감지한 다수의 노드들의 서로 다른 인증키로 생성된 서로 다른 메시지 인증 코드(MAC: message authentication code)들을 허위 보고서 검증을 위해 보고서에 포함시켜 전달해야만 한다. 이렇게 보고서에 포함되는 메시지 인증 코드들의 수는 보안 기법들에서 허위 보고서에 대한 여과 능력을 결정짓는 보안 경계 값(security threshold value)으로, 이 값은 허위 보고서에 대한 보안성과 제한된 에너지를 가지고 있는 센서 노드의 보고서 전달시 소비되는 에너지양을 상쇄시킨다. 보안 경계 값이 크면, 공격자가 노드 훼손을 통해 획득한 인증키로 생성한 메시지 인증 코드 외에 다수의 서로 다른 메시지 인증 코드들을 허위 보고서에 포함시켜야만 하기 때문에 보고서의 위조가 어렵게 되지만, 보고서에 포함시켜야 할 메시지 인증 코드의 수가 커지면 보고서의 크기가 커져 보고서 전달에 많은 에너지를 소비한다. 반대로 보안 경계 값이 작으면, 보고서의 크기가 작아져 에너지 소비가 작아지게 되지만, 훼손된 노드의 수가 이 값을 초과하는 경우 보고서에 포함돼야 하는 모든 인증키들을 공격자가 획득할 수 있기에 보안 기법의 여과 기능을 비효율적 또는 쓸모없게 만들 수가 있다[8]. 따라서 이 보안성과 소비 에너지와의 상쇄관계를 고려하여 허위 보고서에 대한 충분한 보안성을 제공하면서도 에너지 소비를 절감시킬 수 있는 보안 경계 값을 선택해야만 한다[5].

본 논문에서는 Fan Ye 등이 제안한 통계적인 여과 기법[5]에 보안 경계 값 결정을 위한 퍼지 로직을 적용한다. 퍼지 로직을 적용함으로써 충분한 보안성의 제공이 가능할 뿐 아니라 에너지 소비도 절감할 수 있는 보안 경계 값을 결정할 수 있다. 퍼지 로직은 노드가 공격자에게 노출되지 않은 인증키를 소유하고 있을 확률, 전역 키 풀을 나

눈 구획들 중에서 노출된 인증키가 속한 훼손된 구획의 수, 노드의 잔여 에너지양, 이 세 가지 요소를 고려하여 보안 경계 값을 결정한다. 이렇게 통계적 여과 기법에 퍼지 로직을 적용하여 보안 경계 값을 결정함으로써 센서 네트워크에 충분한 보안성을 제공할 뿐만 아니라 에너지 소모도 절감시킬 수 있다. 퍼지 로직에 의한 보안 경계 값 결정의 효율성은 본 논문의 후반부에서 시뮬레이션 결과를 통해 보여준다. 본 논문은 다음과 같이 구성된다. 2장에서는 배경이론으로 통계적 여과 기법에 대한 간단한 설명과 본 연구를 진행하게 된 동기를 설명한다. 3장에서는 보안 경계 값 결정을 위한 퍼지 로직을 설명하며, 4장에서는 퍼지기반의 적응형 통계적 여과기법의 효율성을 보여주는 시뮬레이션 결과를 보여준다. 마지막으로 5장에서는 결론을 내린다.

2. 배경 이론 및 동기

2.1 통계적 여과 기법

Fan Ye 등[5]이 제안한 통계적 여과 기법에서는 어느 특정 노드가 공격자에게 포획을 당해 그 안에 있던 인증키와 같은 보안 정보가 노출되어도, 허위 보고서를 검증하기 위해 보안 정보를 각 노드가 아닌 모든 노드들에게 나누어서 할당한다. 이 과정은 아래와 같다.

사용자의 관심 지역에 노드를 배치하기 전에 인증키 집합인 전역키 풀을 사용자가 임의로 결정한 구획 값(partition value)으로 나누면 각 구획별로 서로 다른 인증키들이 나누어지게 된다. 예를 들어 그림 2와 같이 베이스 스테이션이 100개의 인증키 집합인 전역키 풀을 가지고 있고, 사용자가 임의로 결정한 구획 값이 5라면 전역키 풀은 5개의 구획으로 나눠지고 각 구획 당 20개의 서로 다른 인증키를 갖게 되는 것이다.

전역키 풀의 분할이 끝나면 보안 경계 값, 구획 선택, 각 구획 당 노드에게 할당할 인증키의 수가 사용자에 의해 임의로 결정이 되고, 그 후 선택된 구획들에서 각각의 노드에게 서로 다른 구획의 인증키를 사용자가 지정한 개수만큼 할당한다. 그림 4에서 사용자가 임의로 보안 경계 값은 2로, 구획은 구획1과 구획3을, 할당할 인증키의 수는 1로 결정해서 선택된 구획 안에 있는 인증키들로만 각 노드에게 사용자가 결정한 할당키의 개수 1만큼 할당한다. 이런 과정을 통해 모든 노드에 인증키가 할당이 되고나면 사용자가 정보를 얻고자 하는 관심 지역에 노드들을 배치시킨다.

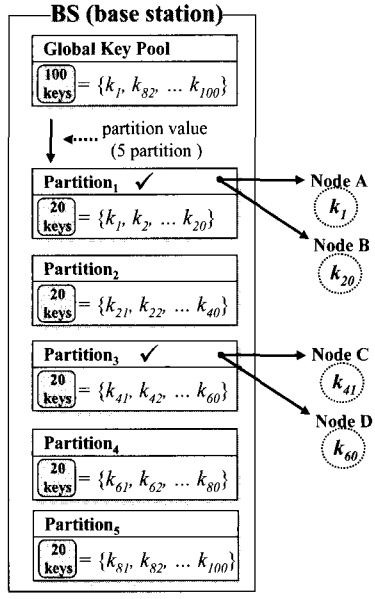


그림 2. 구획 값의 의한 전역키 풀의 분할과 배치 전의 노드에 인증키 할당

위 과정을 통해 인증키를 할당받은 노드들이 배치된 지역에서 어떤 사건이 발생하게 되면 사건이 발생한 그 주변의 하나 이상의 노드들이 그 사건을 감지한다. 그리고 사건을 감지한 노드들 중에서 감지 강도가 제일 강한, 다시 말해서 사건이 발생한 곳으로부터 가장 가까운 곳에 위치한 노드가 보고서 생성과 보고서에 포함시켜야할 메시지 인증 코드들을 모으는 역할을 하는 CoS(center of stimulus)라고 하는 노드로 선정이 된다. 이렇게 선정된 CoS 노드는 우선 자신이 감지한 사건정보를 자신과 동일한 사건을 감지한 주변 노드들에게 그림 3(a)과 같이 브로드캐스트(broadcast)를 하고, CoS 노드에게서 사건정보를 전달받은 주변 노드들은 자신들이 감지한 사건정보와의 동일여부를 검사한다. 그리고 전달받은 사건정보와 자신이 감지한 사건정보가 일치하면, 사건정보와 배치 전에 할당 받은 인증키, 그리고 단방향 해쉬함수(one-way hash function)를 이용해서 그림 3(b)과 같이 메시지 인증 코드를 생성해서 메시지 인증 코드와 메시지 인증 코드 생성에 사용한 인증키 정보를 한 쌍으로 해서 그림 3(c)과 같이 CoS 노드에게 전달하고, CoS노드는 전달받은 메시지 인증 코드들 중에서 서로 다른 구획의 인증키들로만 생성된 메시지 인증 코드들만을 사전에 사용자에 의해 정해져 있던 보안 경계 값만큼 사건정보에 덧붙여 서로 다른 구획의 인증키로 생성된 메시지 인증 코드들을 포함한 하나의 보고서를 그림 3(d)과 같이 생성한다.

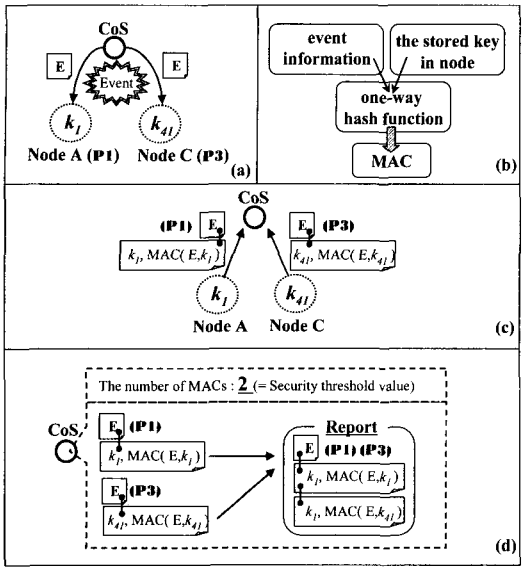


그림 3. 노드가 소유한 인증키를 이용한 MAC 생성과 보안 경계 값이 2인 보고서 생성

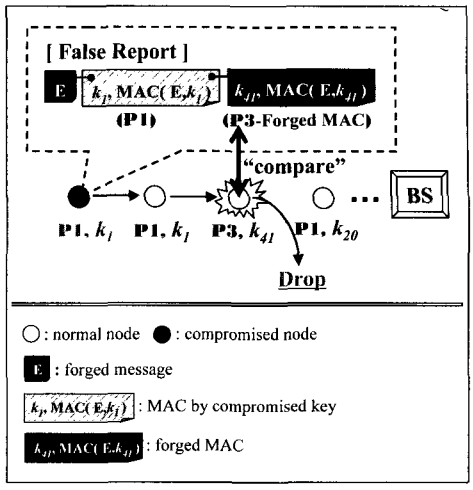


그림 4. 허위 보고서 여과과정

이와 같이 생성된 보고서는 멀티 홉(multi hop) 방식으로 베이스 스테이션으로 전달이 되고, 그 전달되는 경로에 있는 중간노드들은 아래와 같은 4가지 검사과정으로 허위 여부를 검증한다.

- ▶ 인증키 정보가 없는 메시지 인증 코드의 존재 유무 검사.(YES: next check, NO: drop)
- ▶ 보고서의 메시지 인증 코드의 수와 보안 경계 값과의 동일 유무 검사.(YES: next check, NO: drop)
- ▶ 중간노드에서 가지고 있는 인증키 정보와 보고서의 메시지 인증 코드의 인증키 정보와 일치 여부 검사. (YES: next check, NO: forward)
- ▶ 중간노드에서 가지고 있는 인증키와 보고서의 메시지 인증 코드들 중에서 일치하는 인증키 정보가 있을 경우 그 인증키를 가지고 메시지 인증 코드를 생성 후 비교.(YES: forward, NO: drop)

그림 4는 센서 네트워크에서 공격자가 훼손된 노드를 통해 삽입한 허위 보고서가 전달 경로 상에 있는 중간노드의 허위 보고서가 판별해서 더 이상 다음 노드로 전달되지 않는 여과과정을 보여주고 있다. 그림 4에서 보면 보안 경계 값이 2로 설정된 센서 네트워크에서 공격자는 노드 훼손을 통해 구획1의 key1정보를 획득하였으나, 나머지 획득하지 못한 구획2의 인증키 정보는 알 수가 없기 때문에 임의로 구획2의 key41이라는 인증키 정보만 붙인 위조 메시지 인증 코드(forged MAC)를 만들어 허위 보고서에 붙여서 전달하였고, 이 허위 보고서를 받은 중간노드 중에 정상적으로 구획2의 key41을 할당받은 노드가 이 위조 메시지 인증 코드를 정상 인증키로 검증해낸다.

이같은 방법을 통하여 허위 보고서는 중간노드에서 여과가 되고, 정상 보고서만 베이스 스테이션에 전달되게 된다. 만약 이 과정을 통해서도 중간노드들이 허위 보고서를 여과하지 못한다면, 모든 인증키들을 소유하고 있는 베이스 스테이션에서 다시 한 번 같은 방법을 통해서 보고서에 안에 있는 모든 메시지 인증 코드들을 검증하게 된다. 이렇게 통계적 여과 기법은 허위 보고서 삽입 공격에 대응함으로써, 전체 네트워크에서의 삽입공격으로 인한 에너지 소모를 줄일 수가 있다.

2.2 동기

통계적 여과 기법에서 허위 보고서 검증을 위한 보고서에 포함되는 메시지 인증 코드의 수를 나타내는 보안 경계 값의 결정은 보안성과 전송을 통해 소비되는 에너지가 대치되는 관계에 있기 때문에 매우 중요하다[5]. 그림 5와 같이 보안 경계 값이 크면, 공격자가 노드 훼손을 통해 획득한 인증키로 생성한 메시지 인증 코드 외에 다수의 서로 다른 메시지 인증 코드들을 허위 보고서에 포함시켜야만 하기 때문에 보고서의 위조가 어렵게 되고, 많은 메시지 인증 코드들로 여과가 빨리 일어나게 되지만, 센서 네트워크에 공격자에 의한 훼손도가 없는 정상적인 상황에서도, 큰 보안 경계 값만큼의 많은 메시지 인증 코드들을 정상 보고서 안에 포함시켜야 하기 때문에 보고서 전

달에 많은 에너지가 소모된다[6]. 반대로 보안 경계 값이 작게 되면 보고서의 위조가 쉬워지고, 여과가 잘 되지는 않지만, 정상적인 상황에서 정상 보고서를 전달할 때 에너지가 적게 소모된다. 그러나 훼손된 노드의 수가 이 값을 초과하게 되었을 때, 만약 공격자가 보안 경계 값만큼의 서로 다른 구획의 인증키들을 획득하였다면, 통계적 여과 기법에서 요구하는 서로 다른 구획의 인증키로만 이루어진 메시지 인증 코드들을 포함한 보고서의 형태를 만족시킬 수 있기 때문에, 공격자는 검증될 수 없는 허위 보고서로 보안 기법을 비효율적이거나 쓸모없게 만들 수 있고, 또한 여과 기능을 이미 잃은 상태에서도 메시지 인증 코드의 생성, 검증 및 전달을 계속함으로써 추가 비용만을 발생시킬 수도 있다[8].

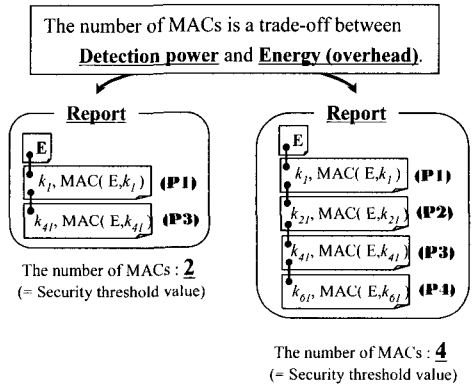


그림 5. 보안 경계 값에 의한 보안성과 에너지의 대치되는 관계

따라서 통계적 여과기법에서 이 보안 경계 값의 결정은 매우 중요하다. 아직까지 통계적 여과 기법의 보안 경계 값을 설정하는 데 권장되는 값이 없기 때문에 네트워크의 설계자나 관리자가 이 값을 결정해야 하는데, 만약 이들이 대상 센서 네트워크와 통계적 여과 기법에 대한 이해가 부족하다면, 잘못된 보안 경계 값의 결정할 수 있고, 이로 인해 많은 센서 네트워크의 많은 에너지 자원의 낭비를 초래할 수가 있다. 그러므로 숙련되지 않은 관리자가 센서 네트워크 상황에 맞는 보안 경계 값을 결정할 때 도움을 줄 수 있도록 퍼지 로직을 적용하기로 하였다.

3. 퍼지 기반의 통계적 여과 기법

3.1 가정

- 베이스 스테이션은 인증키 집합인 전역키 풀을 나눈 구획들 중에서 노출된 인증키가 속한, 즉 훼손된 인증키가 속해 있는 구획인 훼손된 구획의 수, 노드 에너지 수준을 예측할 수 있다. 단, 여기서 훼손된 구획의 수는 베이스 스테이션의 브로드캐스트 메시지 인증(예:μTESLA[9])을 통해 예측할 수 있다.
- 노드들의 밀도가 충분해서 보안 경계 값만큼의 메시지 인증 코드들을 생성할 수 있다.
- 모든 노드는 충분한 개수의 인증키를 할당받는다.

3.2 보안 경계 값 결정을 위한 퍼지 로직의 적용

3.2.1 새로운 보안 경계 값의 결정 요소들

통계적 여과 기법에서 보안 경계 값은 공격자에게 노출된 인증키, 즉 훼손된 인증키가 속한 구획인 훼손된 구획의 수보다 커야 한다. 만약 훼손된 구획의 수가 보안 경계 값을 초과하게 되면, 공격자가 보고서에 포함되어야 할 서로 다른 구획의 모든 인증키 정보를 얻을 수 있기 때문에 통계적 여과 기법은 더 이상 허위 보고서에 대한 여과 기능을 수행할 수 없다. 따라서 훼손된 구획의 수를 고려해 보안 경계 값을 결정해야 한다. 그리고 노드들이 공격자에게 노출되지 않은 훼손되지 않은 인증키를 가지고 있을 확률 역시 고려되어야 한다. 왜냐하면 이 확률은 각 노드의 개별 여과 능력을 보여주는 값으로써 현재 센서 네트워크에 환경에 적용돼 있는 보안 경계 값이 현재 훼손도에서 어느 정도의 여과 수준을 제공할 수 있는지를 보여줄 수 있는 값이기에 이 정보를 가지고 보안 경계 값을 더 증가시킬지, 감소시킬지를 결정할 수 있기 때문이다. 마지막으로 센서 네트워크의 센서 노드들은 제한된 에너지 자원을 갖고 있으므로 보안 경계 값을 각각의 노드의 에너지 수준을 고려해서 결정해야 한다.

3.2.2 퍼지 로직의 입/출력 파라미터의 구성 및 범위

퍼지 로직의 입력 파라미터는 노드들이 훼손되지 않은 인증키를 가지고 있을 확률(x), 훼손된 구획의 수(y), 그리고 노드의 잔류 에너지 수준(z)이며, 퍼지 로직의 출력 파라미터는 보안 경계 값(t)이다.

◉ 입력 파라미터

x (probability of a node having non-compromised keys)
= { VERY_SMALL, SMALL, MEDIUM, LARGE, VERY_LARGE }

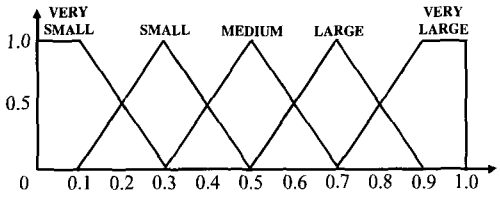
y (the number of compromised partition)
= { VERY_LOW, LOW, MEDIUM, HIGH, VERY_HIGH }

z (remaining energy)
= { SMALL, MEDIUM, MUCH }

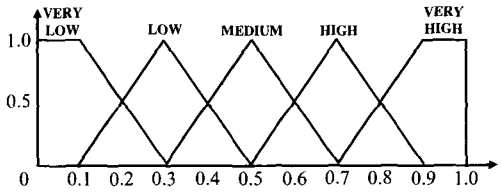
◉ 출력 파라미터
t (security threshold value)
= { VERY_SMALL, SMALL, MEDIUM, LARGE, VERY_LARGE }

3.2.3 멤버십 함수

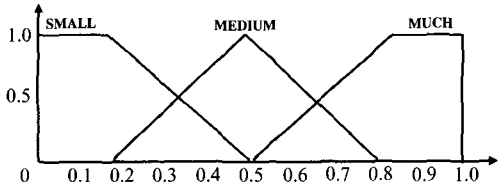
그림 6은 각각의 입력 파라미터의 멤버십 함수들이고, 그림 7은 출력 파라미터의 멤버십 함수이다.



(a) probability of a node having non-compromised keys

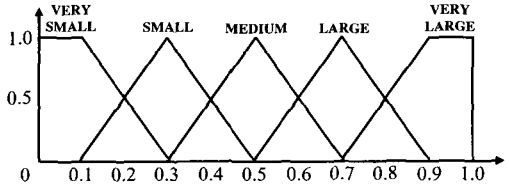


(b) # of compromised partitions



(c) remaining energy

그림 6. 입력 파라미터 멤버십 함수



(d) security threshold value

그림 7. 출력 파라미터 멤버십 함수

3.2.4 퍼지 규칙

RULE 0: IF (x IS VERY_SMALL) AND (y IS VERY_LOW) AND (z IS SMALL) THEN (t IS VERY_SMALL);

RULE 1: IF (x IS VERY_SMALL) AND (y IS VERY_LOW) AND (z IS MEDIUM) THEN(t IS SMALL);

RULE 2: IF (x IS VERY_SMALL) AND (y IS VERY_LOW) AND (z IS MUCH) THEN (t IS SMALL);

RULE 3: IF (x IS VERY_SMALL) AND (y IS LOW) AND (z IS SMALL) THEN(t IS VERY_ SMALL);

RULE 4: IF (x IS VERY_SMALL) AND (y IS LOW) AND (z IS MEDIUM) THEN (t IS MEDIUM);

3.2.5 추론

추론에는 퍼지 이론의 추론모델 중 하나인 맘다니(mandani) 모델의 min-max 합성방법(composition)을 사용하고, 실수 값 출력을 위한 역 퍼지화(defuzzification) 방법에는 무게 중심법(COA: Center of Area)을 사용한다.

3.2.6 동작과정

베이스 스테이션에서는 현재 센서 네트워크 상황에 맞는 보안 경계 값을 결정하기 위해 두 가지 과정을 거치게 된다. 하나는 현재 센서 네트워크에 환경에 적용돼 있는 보안 경계 값이 현재 훼손도에서 어느 정도의 여과 수준을 제공할 수 있는지를 보여주는 값인 노드들이 훼손되지 않은 인증키를 가지고 있을 확률을 계산하는 것이고, 또 하나는 이 계산으로 나온 확률 값과 훼손된 구획의 수, 그리고 각 노드의 잔여 에너지 수준을 가지고 퍼지 시스템에 넣어 현재 네트워크 훼손도와 노드의 에너지수준에 맞는 보안 경계 값을 결정한다.

① 노드가 훼손되지 않은 인증키를 가지고 있을 확률
- T : 보안 경계 값
- N_c : 훼손된 구획의 수
- k : 각 노드가 가지고 있는 키의 수
- n : 전체 구획의 수
- m : 각 구획 당 할당된 키의 수

$$p = \frac{T - N_c}{n} \cdot \frac{k}{m} = \frac{k(T - N_c)}{N} \quad (1)$$

노드들은 관심지역에 배치되기 전에 사용자에 의해 결정된 전역키 풀을 나눈 구획의 전체 개수(n)와 각각의 구획 당 할당된 인증키의 수(m), 그리고 각각의 노드 당 할당된 인증키의 수(k)와 현재 네트워크에 적용돼 있는 보안 경계 값(T)과 현재 훼손돼 있는 구획의 수(N_c)를 입력 값으로 사용해서 노드들이 훼손되지 않은 인증키를 가지고 있을 확률을 식 (1)을 사용해서 그림 8과 같이 베이스 스테이션에서 계산한다.

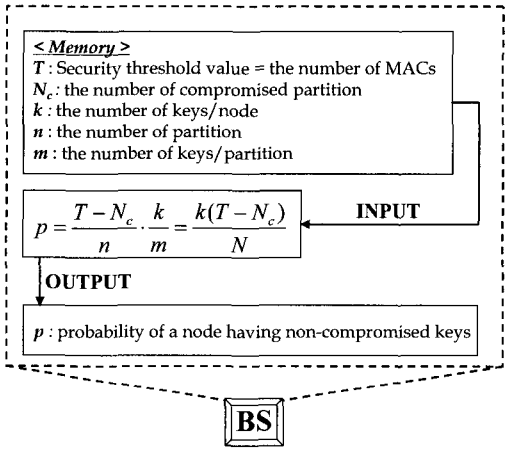


그림 8. 노드들이 훼손되지 않은 인증키를 가지고 있을 확률계산

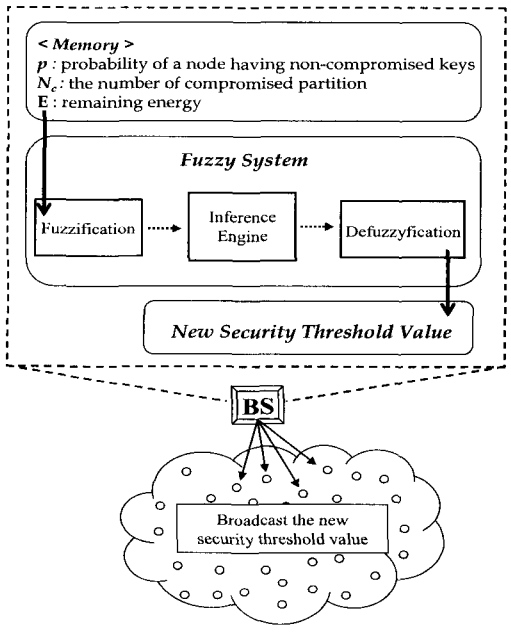


그림 9. 퍼지 로직을 이용한 새로운 보안 경계 값 결정

② 퍼지시스템의 의한 보안 경계 값 결정과 변경

앞에서 베이스 스테이션에서 계산한 노드들이 훼손되지 않은 인증키를 가지고 있을 확률과, 훼손된 구획 수, 그리고 노드의 에너지 수준, 즉 현재 센서 네트워크에 적용된 보안 경계 값의 여과 수준과 현재 센서 네트워크의 훼손도, 그리고 현재 센서 노드들의 잔여 에너지 수준을 입력 값으로 하여 퍼지 시스템을 통해 현재 네트워크 상황에 충분한 보안성과 에너지 효율성을 제공할 수 있는 보안 경계 값을 그림 9와 같이 결정하고, 결정된 새로운 보안 경계 값을 전체 센서 네트워크에 브로드캐스트 한다.

4. 실험 결과

이 시뮬레이션은 퍼지 기반 보안 경계 값 결정의 효율성을 보이기 위하여 수행하였다. 시뮬레이션에서 사용되는 에너지 소모의 계산, 필터링 확률 등의 방법은 통계적 여과 기법[1]에서 실험한 결과를 사용하였다. 즉, 각 노드는 보고서 송신에 16.25μJ/byte, 수신에 12.5μJ/byte를 소비하며, 메시지 인증 코드 생성은 1개당 15μJ을 소비한다. 또한 메시지 인증 코드의 크기는 하나가 8bytes이며, 원본 보고서의 크기는 24bytes이다. 전역키 풀을 나눈 구획들의 전체 개수는 총 22개이며, 공격자에게 노출된 인증키가 속한 훼손된 구획의 수를 19개까지 증가시키며 시뮬레이션을 수행하였다. 훼손된 구획의 수가 변경될 때마다, 퍼지 로직으로 새로운 보안 경계 값을 결정하였다. 보안 경계 값 변경에 따른 계산 및 통신비용은 무시했다.

시뮬레이션에서는 퍼지 시스템에 의해 결정되는 보안 경계 값과 노드 배치 전 사용자에 의해 결정되는 고정 보안 경계 값인 10, 20을 다음 세 가지 시뮬레이션 환경에서 비교하였다. 첫째는 정상 보고서를 전달할 경우의 에너지 소모량의 비교, 둘째는 허위 보고서 여과과정으로 인한 에너지 소모량의 비교, 셋째는 허위 보고서에 대한 여과율의 비교이다.

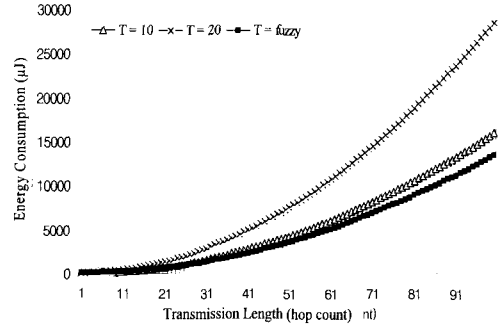


그림 10. 정상 보고서 전송 시 소비되는 에너지

그림 10은 센서 네트워크 환경에서 전송 거리에 따른 정상보고서의 소비 에너지를 비교하여 나타낸 것으로, 고정된 보안 경계 값 10, 20이 퍼지 기반 보안 경계 값보다 더 많은 에너지를 소비하는 것을 볼 수 있다. 이처럼 퍼지 기반 보안 경계 값의 에너지 소모율이 낮은 이유는 센서 네트워크에 공격자에 의한 훼손이 없는 상황에서 허위 보고서에 대한 여과 기능이 불필요하기 때문에 퍼지 시스템에서 최소한의 보안 경계 값을 결정하여 보고서에 적은 수의 메시지 인증 코드들만 포함돼서 전송이 되지만, 그에 비해 고정된 보안 경계 값 10, 20은 공격자에 의한 훼손여부와 상관없이 항상 많은 수의 메시지 인증 코드들을 보고서 안에 포함시켜야만 하기 때문에 위와 같이 센서 네트워크에 공격자에 의한 훼손이 없을 경우에 비효율적인 에너지 소모가 이루어진다.

그림 11은 훼손된 구획에 의한 허위보고서 생성 시 통계적 여과 기법 기반의 센서 네트워크에서 허위 보고서를 여과할 때 소비되는 평균 에너지양이다. 그림은 퍼지 기반의 보안 경계 값이 노드 배치 전에 사용자에 의해 임의로 결정된 고정된 보안 경계 값 10, 20보다 더 적은 에너지를 소모하는 것을 보여준다. 이 결과에서 고정된 보안 경계 값 10, 20은 앞에서 언급한 보안 경계 값에 의한 보안성과 에너지의 대치되는 관계를 보여준다. 보안 경계 값 10은 훼손된 구획의 수가 9개일 때까지는 20보다는 낮은 에너지 소모량을 보여주지만, 훼손된 구획의 수가 보안 경계 값을 10을 초과하면서 그림 16에서 보이는 것처럼 더 이상 여과 기능을 하지 못하고 허위 보고서가 베이스 스테이션까지 전달되기 때문에 그래프와 같이 급격히 에너지 소모량이 증가하게 된다. 반대로 보안 경계 값 20은 그림 16에서 보이는 것처럼 훼손된 구획의 수가 19개일 때까지 허위 보고서에 대한 충분한 보안성을 유지해주지만, 훼손된 구획의 수가 적을 경우에도 항상 20이라는

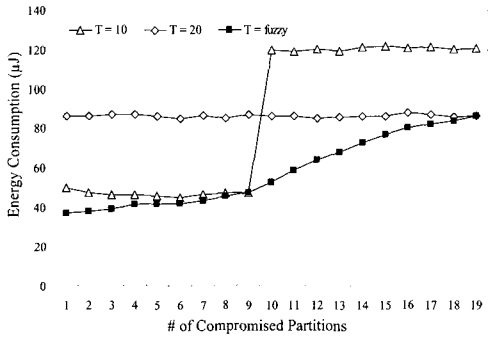


그림 11. 허위 보고서 여과에 소비되는 평균 에너지양

보안 경계 값을 유지해야 하기 때문에 에너지 소모량이 너무 크게 된다. 그에 비해 퍼지 기반 보안 경계 값은 퍼지 시스템의 의해서 훼손도가 낮으면 작은 보안 경계 값으로, 훼손도가 높으면 큰 보안 경계 값으로 결정되기 때문에 고정된 보안 경계 값 10, 20 보다 더 효율적인 에너지 소비를 보장한다.

그림 12는 훼손된 구획의 수의 증가에 따른 각각의 보안 경계 값들의 여과율들을 비교한 것으로, 퍼지 기반 보안 경계 값이 고정된 보안 경계 값 10, 20보다 더 높은 여과율을 제공하는 것을 보여주는데, 그 이유는 퍼지 기반 시스템이 훼손된 구획의 증가에 따라 보안 경계 값을 증가시켜 훼손도에 대한 그 여과 능력을 증가시키기 때문이다. 하지만 고정된 보안 경계 값 10, 20은 그 값이 고정돼 있기 때문에 훼손된 구획의 수가 증가함에 따라 그 여과율이 점점 감소하게 될 뿐만 아니라, 고정된 보안 경계 값 (T = 10)을 훼손된 구획의 수가 초과하는 경우(N_c)에는 여과율이 0%가 되면서 허위 보고서에 대한 여과 기능을 상실하게 된다. 이처럼 퍼지 기반 보안 경계 값은 훼손된 구획 수에 따라 동적으로 보안 경계 값을 변경함으로써, 고정된 보안 경계 값보다 효율적인 여과 능력을 제공해 준다.

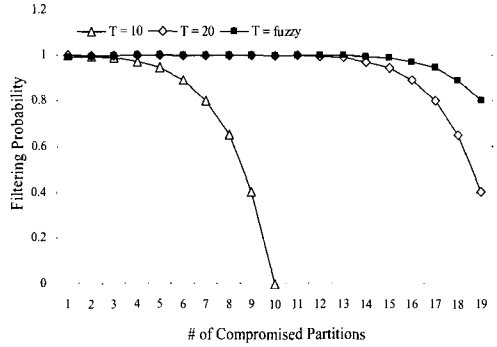


그림 12. 허위 보고서에 대한 여과율

위의 시뮬레이션 결과들을 통해 퍼지 시스템의 의해서 동적으로 변하는 퍼지 기반 보안 경계 값이 고정 보안 경계 값보다 높은 에너지 효율성과 여과율을 제공해주는 것을 확인할 수 있다.

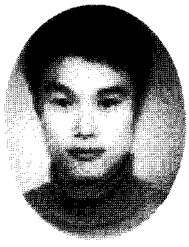
5. 결 론

본 논문에서는 통계적 여과 기법에서 보안성과 에너지 소모량을 상쇄시키는 보안 경계 값 결정에 퍼지 로직을 적용하였다. 퍼지 로직은 노드가 훼손되지 않은 인증키를 가

지고 있을 확률, 훼손된 구획의 수, 노드의 잔여 에너지 수준을 고려하여 보안 경계 값을 결정한다. 퍼지 로직을 적용함으로써 충분한 여과율의 제공이 가능할 뿐만 아니라 에너지 소비도 절감할 수 있다. 퍼지 로직에 의한 보안 경계 값의 효율성을 보이기 위해 훼손이 없는 정상적인 상황의 센서네트워크에서 정상 보고서를 전달할 경우의 에너지 소모량을 비교하였고, 공격자에 의한 훼손이 있을 시에 고정된 보안 경계 값과 허위 보고서에 대한 여과율과 에너지 소모량을 동시에 비교하였다. 그 결과 퍼지 기반 보안 경계 값이 동적으로 변하는 네트워크 상황에 따라 충분한 보안성을 보장할 뿐만 아니라 효율적인 에너지 소비를 제공해 주는 것을 시뮬레이션 결과를 통하여 확인할 수 있었다. 향후에는 다양한 환경과 공격에 대응하고 효율적인 퍼지 로직을 구성하는 방법에 대하여 연구할 것이다.

참 고 문 헌

1. Akyildiz, F., Su, W., Sangkarasubramaniam, Y. and Cayirci, E. (2002), "A Survey on Sensor Networks" IEEE Communications Magazine, pp. 102-114.
2. Al-Karaki, J.N., Kamal, A.E. (2004), "Routing techniques in wireless sensor networks: a survey", Wireless Communications, IEEE, Vol. 11, No. 6, pp. 6-28.
3. Zhu, S., Setia, S., Jajodia, S. and Ning, P. (2004), "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks", IEEE, in Proc. of S&P, pp. 259-271.
4. Przydatek, B., Song, D. and Perrig, A. (2003), "SIA: Secure Information Aggregation in Sensor Networks", ACM, in Proc. of SenSys, pp. 255-265.
5. Ye, F., Luo, H. and Lu, S. (2005), "Statistical En-Route Filtering of Injected False Data in Sensor Networks", IEEE, IEEE Journals on Selected Areas in Communications, vol. 23, No. 4, pp. 839-850.
6. Yang, H. and Lu, S. (2003),"Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks", IEEE, in Proc. of VTC, pp. 1223-1227.
7. Zhang, Y., Yang, J. and Vu, H. T. (2006), "The Interleaved Authentication for Filtering False Reports in Multipath Routing based Sensor Networks", IEEE, in Proc. of IPDPS, pp. 1-10.
8. Zhang, W and Cao, G. (2005), "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach", IEEE, in Proc. of INFOCOM, pp. 503-514.
9. Perrig, A., Szewczyk, R., Tygar, J., Wen, V. and Culler, D. (2002), "SPINS: Security Protocols for Sensor Networks", Wirel. Netw., Vol. 8, pp. 521-534.



김 상 률 (srkim@ece.skku.ac.kr)

2005년 평택대학교 컴퓨터과학과 학사
2006년~현재 성균관대학교 정보통신공학부 컴퓨터공학과 석사과정

관심분야 : 모델링 및 시뮬레이션, 인공지능, 네트워크 보안

조 대 호 (taecho@ece.skku.ac.kr)

1983년 성균관대학교 전자공학과 학사
1987년 Univ. of Alabama 전자공학과 석사
1993년 Univ. of Arizona 전자 및 컴퓨터공학과 박사
1993년~1995년 경남대학교 전자계산학과 전임강사
1995년~1999년 성균관대학교 전기전자 및 컴퓨터공학부 조교수
1999년~2002년 성균관대학교 전기전자 및 컴퓨터공학부 부교수
2002년~2004년 성균관대학교 정보통신공학부 부교수
2004년~현재 성균관대학교 정보통신공학부 교수

관심분야 : USN, 모델링 및 시뮬레이션, 지능 시스템, 네트워크 보안