한국시뮬레이션학회 논문지
Vol. 16, No. 4, pp. 57-65 (2007. 12)

통계적 여과기법에서 훼손 허용도를 위한 퍼지 로직을 사용한 적응형 전역 키 풀 분할 기법

김상률[1] · 조대호[1†]

Adaptive Partitioning of the Global Key Pool Method using Fuzzy Logic for Resilience in Statistical En-Route Filtering

Sang-Ryul Kim · Tae-Ho Cho

ABSTRACT

In many sensor network applications, sensor nodes are deployed in open environments, and hence are vulnerable to physical attacks, potentially compromising the node's cryptographic keys. False sensing report can be injected through compromised nodes, which can lead to not only false alarms but also the depletion of limited energy resource in battery powered networks. 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 partition value represents a trade off between resilience and energy where the partition value is the total number of partitions which global key pool is divided. If every partition are compromised by an adversary, SEF disables the filtering capability. Also, when an adversary has compromised a very small portion of keys in every partition, the remaining uncompromised keys which take a large portion of the total cannot be used to filter false reports. We propose a fuzzy-based adaptive partitioning method in which a global key pool is adaptively divided into multiple partitions by a fuzzy rule-based system. The fuzzy logic determines a partition value by considering the number of compromised partitions, the energy and density of all nodes. The fuzzy based partition value can conserve energy, while it provides sufficient resilience.

Key words : Sensor Network, Global Key Pool, Partitioning, Fuzzy Logic

요 약

많은 센서 네트워크 응용에서, 센서 노드들은 개방된 환경에 배포되므로 노드의 암호 키 완전히 훼손하는 물리 공격에 취약하다. 위조 감지 보고서는 훼손된 노드를 통하여 네트워크에 주입될 수 있으며, 이는 거짓 경보를 울릴 수 있을 뿐만 아니라 전지로 동작하는 네트워크의 제한된 에너지 자원을 고갈시킬 수 있다. Fan Ye 등은 이에 대한 대안으로 전송과정에서 허위 보고서를 검증할 수 있는 통계적 여과 기법을 제안하였다. 이 기법에서 허위 보고서에 대한 검증이 가능한 인증키의 노출 정도인 훼손 허용도를 나타내는 분할 값은 전역 키 풀이 나눠진 구획들의 수로 소비 에너지와 서로 대치되는 관계에 있어그 결정이 매우 중요하다. 전체 구획들의 인증키가 노출될 경우 허위 보고서를 더 이상 검증을 할 수 없고 각 구획들의 노출되지 않은 나머지 인증키들은 인증키로써의 기능도 잃게 된다. 본 논문에서는 전역 키 풀 분할에 퍼지 규칙 시스템을 사용해 다수의 구획들로 나누는 퍼지 기반의 적응형 분할 기법을 제안한다. 퍼지 로직은 훼손된 구획의 수, 노드의 밀도와 잔여 에너지양을 고려하여 분할 값을 결정한다. 이 퍼지 기반의 분할 값은 충분한 훼손 허용도를 제공하면서 에너지를 보존할 수 있다.

주요어 : 센서 네트워크, 전역 키 풀, 분할, 퍼지 로직

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음. (IITA-2006-C1090-0603-0028)
2007년 11월 6일 접수, 2007년 11월 29일 채택
[1] 성균관대학교 정보통신공학부
주 저 자 : 김상률
교신저자 : 조대호
E-mail; taecho@ece.skku.ac.kr

1. 서 론

센서 네트워크는 감지, 계산, 및 무선 통신 능력을 지닌 소형 센서 노드(sensor node)들과 감지한 정보들의 집중국 역할과 사용자와 노드간의 게이트웨이 역할을 하는 베이스 스테이션(BS: base station)으로 구성된다. 기본적으

로 센서 노드들은 사용자가 정보를 얻고자 하는 지역에 뿌려지며, 어떠한 사건(event) 발생 시 각 센서 노드들은 감지한 주변 환경 정보를 담은 보고서(report)를 BS로 전달하고, BS는 인터넷과 같은 기존 통신 인프라를 통하여 사용자에게 해당 정보를 제공한다[1]. 이런 센서 네트워크는 전례가 없는 수준의 다양한 응용을 가능하게 할 것으로 기대되고 있다[2]. 많은 센서 네트워크 응용에서 센서 노드들은 개방된 환경에 배포되므로 물리적 공격에 취약하다[3]. 공격자(adversary)는 노드를 포획하여 노드의 모든 암호 키들을 훼손(compromising)할 수 있다. 또한 공격자는 그림 1과 같이 훼손된 노드(compromised node)를 이용하여 허위 정보를 담은 허위 보고서를 네트워크에 주입할 수 있으며, 이는 거짓 경보(false alarm)를 유발할 수 있을 뿐만 아니라 전지로 동작하는 네트워크의 제한된 에너지 자원을 고갈시킬 수 있다[4].

이러한 심각한 피해를 최소화하기 위해서는 센서 네트워크에 삽입된 허위 보고서를 가능한 빨리 발견하여 제거하여야 하며, 발견되지 못한 허위 보고서는 최소한 BS에서 발견되어 사용자에게 전달되지 않아야 한다[6]. 최근 몇몇 보안 기법들이 이러한 목적을 위하여 제안되었고, 그 중 하나가 Fan Ye 등[4]이 제안한 통계적 여과 기법(SEF: Statistical En-route Filtering)이다. 이 기법에서 보고서는 전역 키 풀(global key pool)이라 불리는 인증키들의 집합을 분할 값(partition value)으로 여러 구획(partition)들로 나눠 각 구획의 일부 인증키를 센서 노드들에게 분배된 상태에서 노드들간의 협력을 통해 각자 생성한 서로 다른 구획의 메시지 인증 코드(MAC: Message Authentication Code)들을 붙여 BS에 전달한다. 이렇게 보고서에 포함되는 MAC들의 수는 허위 보고서에 대한 보안강도를 나타내는 보안 경계 값(security threshold value)으로 이 값은 보안성과 보고서 전달시 소비되는 에너지양을 서로 상쇄시킨다. 그래서 기존에 이런 상쇄관계에 대한 대안으로 퍼지 규칙 시스템을 적용한 퍼지로직 기반의 보안 경계 값 결정 기법[7](DMTF: Determination Method of Security Threshold using Fuzzy Logic)을 제안하였다. 하지만 제안한 DMTF도 SEF와 마찬가지로 사전에 결정된 구획 값으로 나눠진 전체 구획의 수안에서 보안 경계 값을 결정해야하기 때문에 보안 경계 값을 결정 할 수 있는 값의 범위가 제한되어 있어 반복적인 노드 훼손으로 공격자가 모든 구획에서 일부 인증키를 획득하면 여과 기능을 상실하게 된다. 이렇게 전체 구획의 수는 허위 정보 검증이 가능한 전체 구획들의 최대 훼손정도를 나타내는 훼손 허용도로 보안에 있어서 매우 중요한 요소이다. 훼손된 구획의 수가 전체 구획의 수 미만일 때 까지는 훼손되지 않은 나머지 정상 구획의 인증키들을 가지고 허위 보고서를 검증할 수 있지만, 그 이상이 되면 모든 구획의 인증키가 훼손으로 더 이상의 여과기능을 수행 할 수가 없다. 또한 이 훼손 허용도는 보고서 전달시 소비되는 에너지와 서로 대치되는 관계를 가지고 있다. 만약 사용자가 큰 분할 값을 선택하여 훼손 허용도를 높이고자 하면 많은 수의 구획들로 나눠져서 인증키 훼손도에 대한 훼손 허용도가 증가하여 인증키 노출에 대한 보안강도가 커지게 되는 이점을 가질 수 있지만, 센서네트워크의 노드들이 큰 구획 수의 인증키를 분배받음으로써 노드들이 소유할 인증키 구획 종류에 대한 경우의 수가 커져 보고서 생성에 참여한 노드들이 MAC 생성에 사용한 서로 다른 구획의 인증키들과 일치하는 구획의 인증키를 경로 상에 있는 노드들이 소유하고 있을 확률이 낮아져 허위 여부에 대한 검증이 많은 수의 노드들 거치거나 BS에서 이루어져 많은 양의 에너지를 소모시킬 수도 있다. 반대로 이 구획의 수가 작으면 센서네트워크의 노드들이 적은 구획 수의 인증키를 분배받음으로써 노드들이 소유할 인증키 구획종류에 대한 경우의 수가 작아져 보고서 생성에 참여한 노드들이 MAC에 생성에 사용한 서로 다른 구획의 인증키들 중 일치하는 구획의 인증키를 전달 경로 상에 있는 노드들이 소유하고 있을 확률이 높아져 보고서 허위 여부에 대한 검증이 적은 수의 노드들 거쳐 이루어져 적은 양의 에너지를 소모시킬 수 있다. 하지만 적은 구획수로 인해 인증키 노출에 대한 훼손 허용도가 감소하고 이로 인해 공격자는 쉽게 보안 기법을 비효율적이거나 쓸모없게 만들 수 있다. 게다가 고정된 구획의 수는 효율적인 인증키 사용이 어렵다. 보고서 생성의 조건은 어떤 인증키냐가 아니라 어느 구획의 인증키냐 이기 때문에 공격자가 특정 구획의 인증키를 하나만 획득하면 그 구획의 나머지 인증키들은 필요 없게 된다. 다시 말해서 허위 보고서 검증은 공격자가 획득하지 못한 다른 구획의 인증키를 이용해 검증

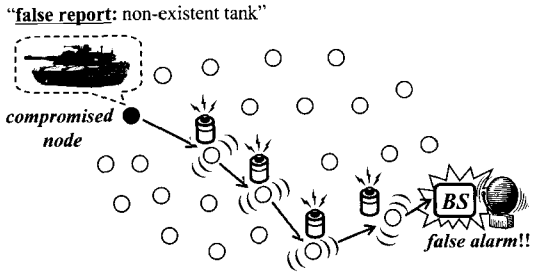


그림 1. 허위 보고서 삽입에 의한 거짓 경보 발생

하는 것이기 때문에 특정 구획의 인증키들 중에서 하나의 인증키가 공격자에게 획득되면 더 이상 그 구획에서 인증키가 필요치 않기에 나머지 인증키들은 검증기능을 상실하게 되는 것이다. 따라서 우리는 허위 보고서에 대한 충분한 훼손 허용도와 에너지 소비절감 뿐만 아니라 한 구획 안에 훼손되지 않은 인증키들의 효율적인 사용을 제공할 수 있는 전역 키 풀의 분할 값을 선택해야만 한다[5]. 본 논문에서는 Fan Ye 등이 제안한 통계적인 여과 기법[4]에서 전역 키 풀의 분할 값의 결정을 위하여 퍼지 로직을 적용한다. 퍼지 로직을 적용함으로써 충분한 훼손 허용도의 제공과 에너지 소비를 절감뿐 아니라 인증키의 효율적인 사용을 제공할 수 있는 전역 키 풀 분할 값을 결정할 수 있다. 퍼지 로직은 전역 키 풀을 나눈 구획들 중에서 노출된 인증키가 속한 훼손된 구획의 수, 노드의 밀도 및 노드의 에너지 수준, 이 세 가지 요소를 고려하여 전역 키 풀 분할 값을 결정한다. 이렇게 SEF에 퍼지 로직을 적용하여 전역 키 풀 분할 값을 결정함으로써 센서 네트워크에 충분한 훼손 허용도와 에너지 소모를 절감 시킬 수 있을 뿐만 아니라 한 구획 안에 훼손되지 않은 인증키들의 효율적인 사용을 제공할 수 있다. 퍼지 로직에 의한 전역 키 풀 분할 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 전역 키 풀 분할 값 결정을 위한 퍼지 로직을 설명하며, 4장에서는 퍼지기반의 적응형 전역 키 풀 분할기법의 효율성을 보여주는 시뮬레이션 결과를 보여준다. 마지막으로 5장에서는 결론을 내린다.

2. 배경 이론 및 동기

2.1 통계적 여과 기법

Fan Ye 등[4]이 제안한 통계적 여과 기법에서는 우선 허위 보고서를 검증을 위해 관심 지역에 노드를 배치하기 전에 그림 2와 같이 인증키 집합인 전역키 풀을 사용자가 임의로 결정한 분할 값으로 각 구획별로 서로 다른 인증키들로 나눈다.

이렇게 전역키 풀의 분할이 끝나면 보안 경계 값과 각 구획 당 노드에게 할당할 인증키의 수가 사용자에 의해 임의로 결정이 되고, 그 후 임의의 구획들에서 각각의 노드에게 서로 다른 구획의 인증키를 사용자가 지정한 개수만큼 할당하여 사용자가 정보를 얻고자 하는 관심 지역에 노드들을 배치시킨다.

그리고 그 지역에서 그림 3(a)와 같이 어떤 사건이 발생하여 사건이 발생한 위치의 주변 노드들이 사건정보를 감지하면, 감지 노드들 중 감지 강도가 제일 강한 노드가 보고서에 포함시킬 MAC들을 모으고, 보고서 생성을 하는 CoS(center of stimulus)라는 노드로 선정이 된다. 이 CoS 노드는 그림 3(b)와 같이 자신이 감지한 사건정보를 자신과 동일한 사건을 감지한 주변 노드들에게 브로드캐스트(broadcast)를 하고, 전달받은 주변 노드들은 자신들이 감지한 사건정보와 같을 경우 사건정보와 노드배치 전에 할당 받은 인증키, 그리고 단방향 해쉬함수(one-way hash function)를 이용해서 그림 3(c)와 같이 MAC을 생성해서, 그림 3(d)와 같이 CoS 노드에게 전달하고, CoS 노드는 전달받은 MAC들 중에서 서로 다른 구획의 인증키들로만 생성된 MAC들만을 사전에 사용자에 의해 정해

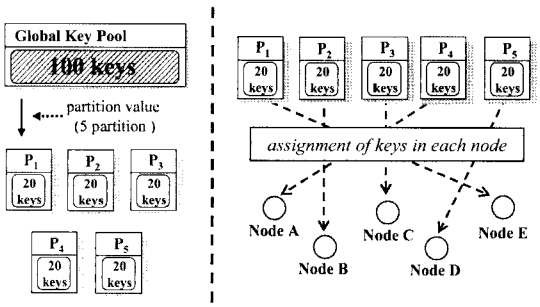


그림 2. 구획 값의 의한 전역키 풀의 분할과 배치 전의 노드에 인증키 할당

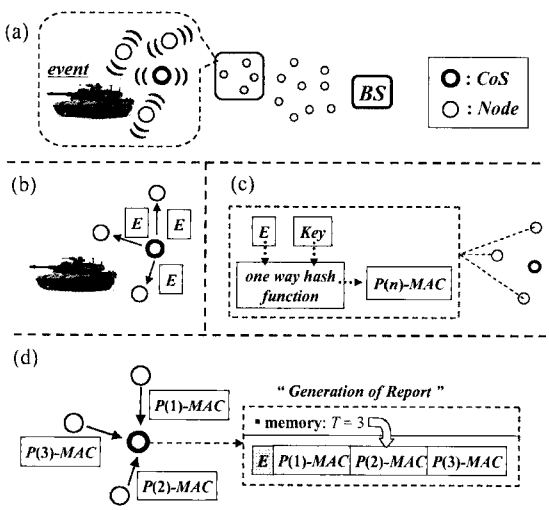


그림 3. 노드가 소유한 인증키를 이용한 MAC 생성과 보안 경계 값이 3인 보고서 생성

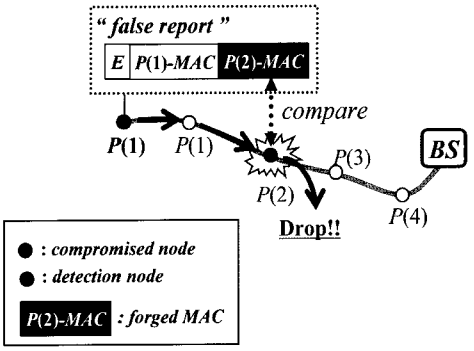


그림 4. 허위 보고서 여과과정

져 있던 보안 경계 값만큼만 사건정보에 덧붙여 하나의 보고서를 생성한다.

전역 키 풀이 4개의 구획으로 나눠지고, 보안 경계 값이 2로 설정된 센서 네트워크에서 그림 4와 같이 공격자가 노드 훼손을 통해 구획1의 인증키를 획득하게 되면, 공격자는 보안 경계 값 2를 만족시키기 위해 임의로 위조 MAC(forged MAC)을 만들어 허위 보고서에 붙여 센서 네트워크에 삽입할 것이다. 이 때 허위 보고서는 BS로 전달되는 경로상의 중간 노드들에게 검증을 받게 되고, 그 중 정상적으로 구획2의 인증키를 할당받은 노드가 이 위조 MAC의 허위여부를 판별한다. 또한 경로상의 중간노드들이 허위 보고서를 여과하지 못할 경우를 고려하여 모든 인증키들을 소유하고 있는 BS에서 보고서의 모든 메시지 인증코드들을 다시 한 번 검증하여 허위여부를 판별한다. 이렇게 통계적 여과 기법은 허위 보고서 삽입공격으로 인한 에너지 소모를 줄일 수가 있다.

2.2 연구 동기

SEF의 서로 다른 구획의 인증키로 만든 MAC들과 사건 정보를 붙이는 보고서 생성조건은 공격자가 그림 5와 같이 전체 구획들 중에서 일부 구획의 인증키를 노드 훼손을 통해 획득하여도 나머지 서로 다른 구획들의 인증키 정보가 없기 때문에 허위 정보에 붙일 충분한 MAC들을 생성해 낼 수 없어 보고서의 위조가 어려울 뿐만 아니라, 공격자가 임의로 만든 위조 MAC을 붙인 허위 보고서를 생성해도 보고서 전달 경로 상에 있는 노드들이 자신이 갖고 있는 특정 구획의 정상 인증키로 검증하여 여과시킨다. 이렇게 SEF에서는 전체 구획들의 인증키를 공격자가 모두 획득하기 전까지는 데이터에 대한 위조가 어렵다. 그래서 이 전체 구획의 수를 허위정보에 대한 인증이 가능한 서로 다른 구획의 인증키 노출정도를 뜻하는 훼손 허용도라고 한다. 이 훼손 허용도는 사전에 사용자에 의해서 한번 결정된 후 변하지 않는 고정된 값으로 훼손된 구획의 수가 이 전체 구획의 수 미만일 때 까지는 훼손되지 않은 나머지 정상 구획의 인증키들을 가지고 허위 보고서를 검증할 수 있으나, 그 이상이 돼버리면 모든 구획의 인증키가 훼손되기 때문에 더 이상의 여과기능을 수행할 수는 없는 문제점을 가지고 있다.

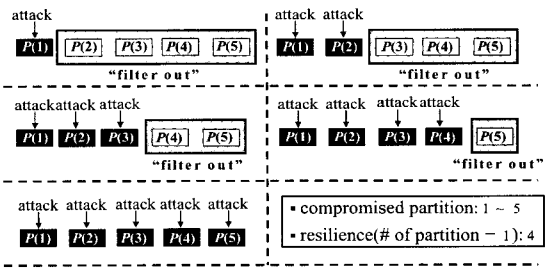


그림 5. 훼손된 구획 수에 따른 훼손 허용도

이때 사용자가 훼손 허용도를 높이기 위해 그림 6과 같이 큰 분할 값을 선택해서 많은 수의 구획들로 나누면 인증키 노출에 대한 훼손 허용도가 증가돼 보안강도는 커지지만, 센서네트워크의 노드들이 큰 구획 수의 인증키를 분배받음으로써 보고서를 생성한 노드와 BS경로사이에 있는 노드들이 소유하고 있을 인증키 구획종류에 대한 경우의 수가 커져 보고서 생성에 참여한 노드들이 MAC 생성에 사용한 서로 다른 구획의 인증키들과 일치하는 구획의 인증키를 경로 상에 있는 노드들이 소유하고 있을 확률이 낮아져 허위 여부에 대한 검증이 많은 수의 노드들 거치거나 BS에서 이루어져 많은 양의 에너지를 소모시킬 수도 있다. 반대로 이 구획의 수가 작으면 센서네트워크의 노드들이 적은 구획 수의 인증키를 분배받음으로써 보고서 생성에 참여한 노드들이 MAC 생성에 사용한 서로 다른 구획의 인증키들 중 일치하는 같은 구획의 인증키를 경로 상에 있는 노드들이 소유하고 있을 확률이 높아져 보고서 허위 여부에 대한 검증이 적은 수의 노드들 거쳐 이루어져 적은 양의 에너지를 소모시킬 수 있다. 하지만 적은 구획수로 인해 인증키 노출에 대한 훼손 허용도가 감소하고 이로 인해 공격자는 쉽게 보안 기법을 비효율적이거나 쓸모없게 만들 수 있고, 또한 여과 기능을 이미 잃은 상태에서도 MAC의 생성, 검증 및 전달을 계속함으로써 추가 비용을 발생시킬 수도 있다[8]. 이렇게 훼손 허용도 즉 구획의 수는 에너지와 서로 대치되는 관계를 가지고 있다.

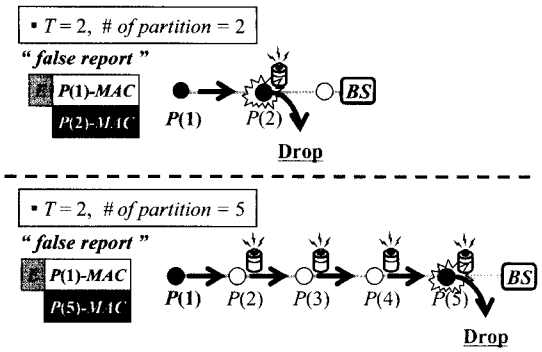


그림 6. 구획 수(훼손 허용도)와 에너지 소모의 관계

게다가 고정된 구획의 수는 효율적인 인증키 사용이 어렵다. 보고서 생성의 조건은 어떤 인증키냐가 아니라 어느 구획의 인증키냐 이기 때문에 공격자가 특정 구획의 인증키를 하나만 획득하면 그 구획의 나머지 인증키들은 필요 없게 된다. 다시 말해서 허위 보고서 검증은 공격자가 획득하지 못한 다른 구획의 인증키를 이용해 검증하는 것이기 때문에 특정 구획의 인증키들 중에서 하나의 인증키가 공격자에게 획득되면 더 이상 그 구획에서 인증키가 필요치 않기에 나머지 인증키들은 검증기능을 상실하게 되는 것이다. 따라서 우리는 허위 보고서에 대한 충분한 훼손 허용도와 에너지 소비절감 뿐만 아니라 한 구획 안에 훼손되지 않은 인증키들의 효율적인 사용을 제공할 수 있는 전역 키 풀의 분할 값을 선택해야만 한다[5]. 현재까지 전역 키 풀의 분할 값을 설정하는 데 권장되는 값은 없기 때문에, 네트워크의 설계자나 관리자가 결정해야 한다. 하지만 이 경우에도 이들이 만약 대상 센서 네트워크와 통계적 여과 기법에 대한 이해도가 떨어져서 잘못된 전역 키 풀 분할 값을 결정을 한다면 허위 보고서에 대한 인증에 많은 문제를 초래할 수 있다. 그러므로 숙련되지 않은 관리자가 네트워크 상황에 맞는 전역 키 풀 분할 값을 결정할 때 도움을 줄 수 있는 퍼지 규칙 시스템을 적용한 전역 키 풀의 적응형 분할 기법을 제안한다.

3. 퍼지 기반의 적응형 전역 키 풀 분할기법

3.1 가 정

▶BS는 훼손된 구획의 수, 노드의 밀도와 에너지 수준을 예측할 수 있다.

▶BS의 브로드캐스트 메시지 인증(예:μTESLA[9])을 통해 훼손된 구획의 수를 알 수 있다.

3.2 보안 경계 값의 변경

기존 SEF에서는 보안 경계 값이 전역 키 풀의 구획들 중에서 사용자에 의해 임의로 결정된 구획의 수로 그 수만큼의 서로 다른 구획의 MAC들을 보고서에 포함시켰으나, 본 논문에서는 인증키를 할당 받은 노드들이 배치된 상태에서 전역 키 풀을 재분할하여 구획의 수를 동적으로 변화시키는 방법이기 때문에 노드에 할당돼있는 인증키의 구획정보가 계속 바뀌어서 각 노드는 하나 이상의 구획정보를 가질 수 있고, 이런 구획 정보들을 가지고 한 노드는 하나 이상의 서로 다른 구획의 MAC들을 생성할 수가 있다. 따라서 본 논문에서는 각 노드는 원칙적으로 한 노드당 한 개의 MAC만을 생성하는 기존 SEF의 생성조건은 유지하고 대신 전체 구획들 중에 사용자가 선택한 일부 구획들의 수가 아닌 전체 구획들의 수를 보안 경계 값으로 하여 노드가 공격자에 의해 하나 이상의 서로 다른 구획 인증키를 노출해도 훼손된 구획의 수가 전체 구획의 수를 초과할 수 없도록 전체 구획의 수를 나타내는 분할 값을 보안 경계 값으로 변경한다.

3.2.1 새로운 분할 값의 결정 요소들

통계적 여과 기법에서 분할 값은 훼손된 구획의 수보다 커야 한다. 만약 훼손된 구획의 수가 분할 값(훼손 허용도)을 초과하게 되면, 공격자가 보고서에 포함시켜야 할 서로 다른 구획의 모든 인증키 정보를 얻을 수 있기 때문에 통계적 여과 기법은 허위 보고서를 검증할 수 없어 사용자가 요구하는 보안 수준을 만족할 수 없게 된다. 또한 주변 노드간의 밀도를 고려해야 한다. 사건 발생 시 그 사건을 감지한 하나 이상의 주변 노드들이 각각의 특정 구획의 인증키로 MAC을 생성하여 사건정보에 붙여 보고서를 생성하는데, 분할 값 즉 보안 경계 값보다 밀도가 작으면 충분한 개수의 MAC들을 생성해 낼 수 없기 때문에 정상적인 사건이 발생하여도 보고서의 생성/전달을 못해 사용자는 사건에 관한 어떠한 정보도 얻을 수 없다. 따라서 노드의 밀도는 분할 값 보다 커야 한다. 마지막으로 센서 네트워크의 센서 노드들은 제한된 에너지 자원을 갖고 있으므로 분할 값을 각각의 노드의 에너지 수준을 고려해서 결정해야 한다.

3.2.2 퍼지 로직의 입/출력 파라미터의 구성 및 범위

퍼지 로직의 입력 파라미터는 훼손된 구획의 수(x), 노드의 밀도(y), 그리고 노드의 에너지 수준(z)이며, 퍼지 로직의 출력 파라미터는 전체 키 풀의 분할 값(p)이다.

▶입력 파라미터

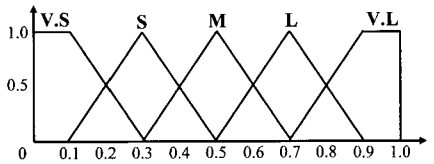
- x = { **V.S**(Very Small), **S**(Small), **M**(Medium), **L**(Large), **V.L**(Very Large) }
- y = { **V.L**(Very Low), **L**(Low), **M**(Medium), **H**(High), **V.H**(Very High) }
- z = { **V.S**(Very Small), **S**(Small), **H**(Half), **M**(Much), **V.M**(Very Much) }

▶출력 파라미터

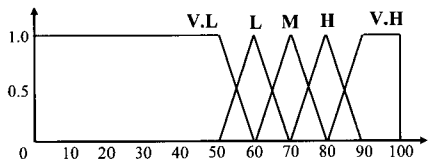
- p = { **V.S**(Very Small), **S**(Small), **M**(Medium), **L**(Large), **V.L**(Very Large) }

3.2.3 멤버십 함수

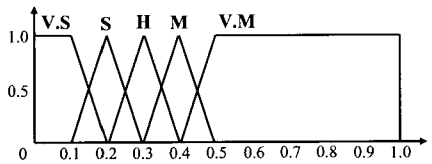
그림 7은 각각의 입력 파라미터의 멤버십 함수들이고, 그림 8은 출력 파라미터의 멤버십 함수이다.



(a) # of Compromised Partitions

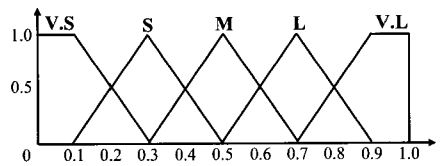


(b) Density of Nodes



(c) Energy

그림 **7.** 입력 파라미터 멤버십 함수



Partition value(= Threshold value)

그림 **8.** 출력 파라미터 멤버십 함수

3.2.4 퍼지 규칙

RULE 0: IF (x IS **V.S**) AND (y IS **V.L**) AND (z IS **V.S**) THEN (p IS **V.S**);

RULE 1: IF (x IS **V.S**) AND (y IS **V.L**) AND (z **S**) THEN (p IS **S**);

RULE 2: IF (x IS **V.S**) AND (y IS **V.L**) AND (z IS **H**) THEN (p IS **S**);

RULE 3: IF (x IS **V.S**) AND (y IS **V.L**) AND (z IS **L**) THEN (p IS **S**);

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

BS에서 현재 센서 네트워크에서 훼손된 구획의 수, 노드밀도 그리고 노드의 잔여 에너지양 이렇게 세 가지 요소 값과 퍼지 규칙 시스템을 가지고 현재 네트워크 상황에 충분한 훼손 허용도와 에너지 효율성, 그리고 인증키의 효율적인 사용을 제공할 수 있는 전역 키 풀의 분할 값을 그림 9와 같이 결정한다 . 그리고 이렇게 결정된 분할 값으로 전역 키 풀을 재분할하여 각 인증키들의 변경된 구획 정보와 새로운 보안 경계 값을 센서 네트워크에 브로드캐스트한다. 새로운 보안 경계 값과 구획정보를 전달

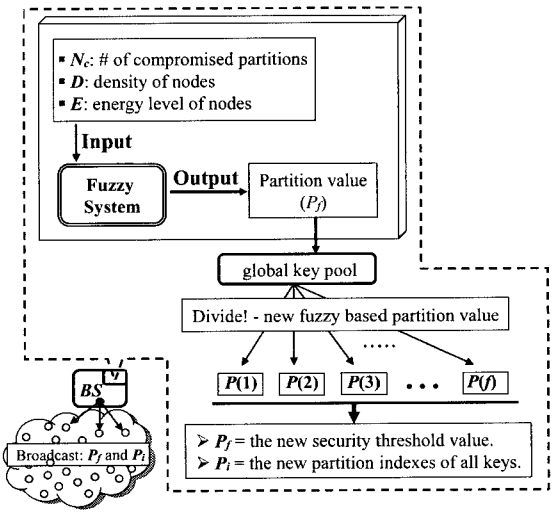


그림 **9.** 퍼지 로직에 의한 분할 값 결정

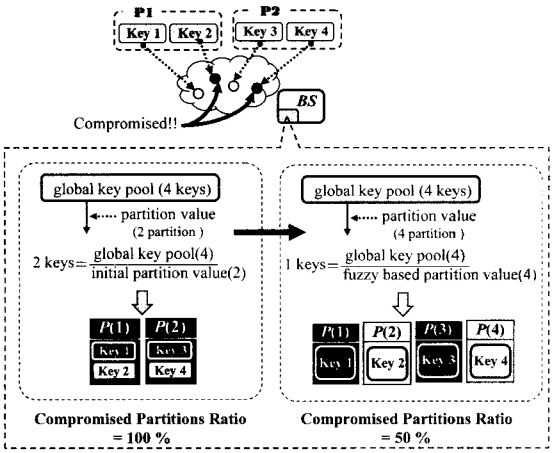


그림 10. 퍼지 로직에 의한 전역 키 분할

받은 노드들은 이 정보들을 가지고 보고서 생성과 여과 과정을 진행한다.

예를 들어 그림 10과 같이 구획1의 key1와 구획2의 key3가 공격자에 의해 노출 되었을 경우, 전역 키 풀의 훼손률이 100%로 SEF나 DMTF 경우 여과기능을 상실하게 되지만, 본 논문에서 제안한 퍼지 규칙 시스템을 통한 분할 값 결정 기법은 공격자에게 인증키가 노출 되었을 경우 새 분할 값을 결정하여 전역 키 풀을 재분할해 구획의 수를 증가시켜 정상키와 훼손된 키를 나누어 각각을 독립된 구획으로 만들어 전역 키 풀의 훼손율을 50%로 낮춘다. 이 과정을 통해 허위 보고서 삽입 시에도 구획 2,4의 key2와 key4로 여과 시킬 수 있다.

4. 실험 결과

이 시뮬레이션은 퍼지 기반 분할 값 결정의 효율성을 보이기 위하여 수행하였다. 시뮬레이션에서 사용되는 에너지 소모의 계산, 필터링 확률 등의 방법은 통계적 여과기법[6]에서 실험한 결과를 사용하였다. 즉, 각 노드는 보고서 송신에 16.25μJ/byte, 수신에 12.5μJ/byte를 소비하며, MAC 생성은 1개당 15 μJ을 소비한다. 또한 MAC의 크기는 하나가 8 bytes이며, 원본 보고서의 크기는 24 bytes이다. 전역키 풀을 나눈 구획들의 전체 개수는 총 15개이며, 서로 다른 구획의 일부 인증키를 획득한 훼손된 노드의 수를 19개까지 증가시키며 시뮬레이션을 수행하였다. 훼손된 노드의 수가 변경될 때마다, 퍼지 로직으로 새로운 분할 값을 결정하여 그 값을 새로운 보안 경계 값으로 설정하였다. 보안 경계 값 변경에 따른 계산 및 통신 비용은 무시했다. 시뮬레이션에서는 전체 구획의 수 15개에서 설정할 수 있는 최대 보안 경계 값 15를 설정한 SEF와 기존에 제안했었던 DMTF, 그리고 본 논문에서 제안한 퍼지 로직을 사용한 전역 키풀의 적응형 분할 (APMF: Adaptive Partitioning of the Global Key Pool Method using Fuzzy Logic), 이 세 기법을 다음 두 가지 측면에서 비교하였다. 첫째는 여과과정으로 인한 에너지 소모량의 비교, 둘째는 허위 보고서에 대한 여과율의 비교이다.

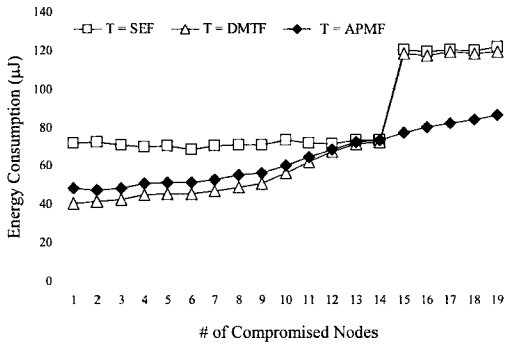


그림 11. 허위 보고서 여과로 인한 에너지 소모량

그림 11은 훼손된 구획의 수의 증가에 따라 허위 보고서를 여과할 때 소비되는 평균 에너지양으로 APMF가 SEF와 DMTF 보다 더 적은 에너지를 소모하는 것을 보여준다. 이 결과에서 SEF와 DMTF는 앞에서 언급한 문제점인 제한된 훼손 허용도를 보여준다. 우선 SEF는 인증키 훼손도의 변화에 상관없이 최대 보안 경계 값인 15가 적용된 상태이기 때문에 훼손된 노드의 수가 14일 때까지 다른 기법들보다 더 높은 여과율을 그림 12와 같이 제공하지만, 보안성과 에너지의 상쇄관계로 인해 허위 보고서 여과에 대한 에너지 소모도가 세 기법 중 가장 높다. 게다가 제한된 훼손 허용도로 훼손된 노드의 수가 14를 초과하면 모든 구획의 일부 인증키가 노출되어 SEF에서는 더 이상 여과 기능을 못하고 허위 보고서가 BS까지 전달되어 그림 11과 같이 급격히 에너지 소모량이 증가하게 된다. 그리고 DMTF는 훼손된 노드의 수가 14일 때까지 전체 구획 수 (p = 15) 안에서 퍼지 규칙 시스템으로 보안성과 에너지의 상쇄관계를 고려한 보안 경계 값의 결정으로 세 기법 중 그림 11과 같이 가장 낮은 에너지를 소모할 뿐만 아니라 그림 12와 같이 충분한 여과율을 제공한다. 하지만 DMTF 역시 훼손된 노드의 수가 14를 초과하면 전체 구획 수(p = 15) 이상의 보안 경계 값을 결정할 수 없기 때문에 그림 12처럼 여과기능을 상실하고 SEF와

마찬가지로 허위 보고서가 BS까지 전달되어 급격히 에너지 소모량이 증가하게 된다. 하지만 본 논문에서 제안한 APMF는 앞의 두 기법 DMTF, SEF와 같이 전체 구획의 개수 안에서 보안 경계 값을 결정하는 것이 아니라 인증키의 훼손도에 따라 전체 구획의 수를 증가시켜 그 값을 보안 경계 값으로 하는 것이기 때문에 SEF, DMTF와 달리 훼손 노드의 수가 14를 초과돼도 허위 보고서를 여과시킬 수 있기 때문에 그림 12와 같이 훼손 노드의 수 14개 이후에도 충분한 여과율을 보장할 수 있을 뿐만 아니라, 그림 11과 같은 가장 적은 에너지를 소모한다.

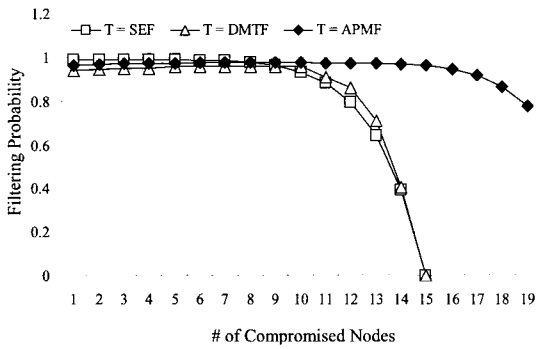


그림 **12.** 허위 보고서에 대한 여과율

그림 12는 훼손된 노드의 증가에 따른 각 기법들에 여과율을 비교한 것으로, APMF가 SEF, DMTF 보다 전체적으로 더 높은 여과율을 제공하는 것을 보여주는데, 그 이유는 퍼지 기반 시스템이 훼손 노드들 통해 공격자에게 노출된 훼손된 구획의 정도가 커질수록 큰 분할 값을 결정하여 전체 구획의 수를 증가시켜 훼손된 인증키와 훼손되지 않은 인증키를 서로 다른 구획으로 나누어 훼손되지 않은 인증키가 정보 검증을 할 수 있는 키로써의 기능을 유지할 수 있게 함으로써 충분한 훼손 허용도를 제공할 수 있기 때문이다. 하지만 SEF와 DMTF는 전체 구획의 수(P = 15)가 고정돼 있기 때문에 훼손도가 그 수의 이상이 되면 여과율이 0%가 되면서 허위 보고서에 대한 여과 기능을 상실하게 된다. 이처럼 훼손된 구획 수에 따라 동적으로 분할 값을 결정함으로써 보안 경계 값을 변경시켜, 제한된 훼손 허용도를 가지고 있는 SEF와 DMTF보다 APMF가 효율적인 여과 능력을 제공뿐만 아니라 높은 에너지 효율성을 제공해 주는 것을 확인할 수 있다.

5. 결 론

본 논문에서는 Fan Ye 등이 제안한 통계적인 여과 기법[5]에서 전역 키 풀의 분할 값 결정에 퍼지 로직을 적용하였다. 퍼지 로직은 전역 키 풀을 나눈 구획들 중에서 노출된 인증키가 속한 훼손된 구획의 수, 노드의 밀도 및 노드의 에너지 수준, 이 세 가지 요소를 고려하여 전역 키 풀 분할 값을 결정한다. DMTF는 통계적 여과 기법에 퍼지 로직을 적용함으로써 SEF에 충분한 보안 강도와 에너지 소모를 절감 시킬 수는 있었으나 SEF와 마찬가지로 고정된 전체 구획 수로 인해 제한적인 훼손 허용도라는 문제점을 갖고 있었다. 이 문제점을 해결하기 위해 본 논문에서는 공격자에 의한 훼손도 따라 전역 키풀을 나눌 분할 값을 퍼지로직을 사용해 결정하여 전체 구획의 수를 증가시켜 충분한 훼손 허용도를 제공하였다. 그 뿐만 아니라 이 분할 과정을 통해 한 구획 안에 훼손되지 않은 인증키들의 효율적인 사용을 제공할 수 있다. 그리고 이를 증명하기 위해 퍼지 로직에 의한 전역 키 풀 분할 값 결정의 효율성을 위한 시뮬레이션을 통해 SEF, DMTF와 본 논문에서 제안한 APMF의 허위 보고서에 대한 여과율과 에너지 소모량을 동시에 비교하였다. 그 결과 퍼지 기반 분할 값이 동적으로 변하는 네트워크 상황에 따라 충분한 훼손 허용도와 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. 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.
2. 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.
3. B. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," *ACM, Proceeding of SenSys*, pp. 255-265, 2003.
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. 김상률, 조대호 (2007), "통계적 여과 기법기반의 센서 네트워크를 위한 퍼지로직을 사용한 보안 경계 값 결정 기법", *한국시뮬레이션학회지*, 제16권, 제2호, pp. 27-35.
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)

2006 평택대학교 컴퓨터과학과 학사
2006～현재 성균관대학교 정보통신공학부 컴퓨터공학과 석사과정

관심분야 : 모델링 및 시뮬레이션, 인공지능, 네트워크 보안

조 대 호 (taecho@ece.skku.ac.kr)

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

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