한국시뮬레이션학회 논문지
Vol. 19, No. 1, pp. 53-61 (2010. 3)

무선 센서 네트워크에서 통계적 여과 기법의 에너지 효율 향상을 위한 퍼지논리를 적용한 동적 경계값 결정 기법

최현명[1] · 이선호[1] · 조대호[1†]

Dynamic Threshold Determination Method for Energy Efficient SEF using Fuzzy Logic in Wireless Sensor Networks

Hyeon Myeong Choi · Sun Ho Lee · Tae Ho Cho

ABSTRACT

In wireless sensor networks(WSNs) individual sensor nodes are subject to security compromises. An adversary can physically capture sensor nodes and obtain the security information. And the adversary injects false reports into the network using compromised nodes. If undetected, these false reports are forwarded to the base station. False reports injection attacks can not only result in false alarms but also depletion of the limited amount of energy in battery powered sensor nodes. To combat these false reports injection attacks, several filtering schemes have been proposed. The statistical en-routing filtering(SEF) scheme can detect and drop false reports during the forwarding process. In SEF, The number of the message authentication codes(threshold) is important for detecting false reports and saving energy. In this paper, we propose a dynamic threshold determination method for energy efficient SEF using fuzzy-logic in wireless sensor networks. The proposed method consider false reports rate and the number of compromised partitions. If low rate of false reports in the networks, the threshold should low. If high rate of false reports in networks, the threshold should high. We evaluated the proposed method's performance via simulation.

Key words : WNS, False report injection attack, SEF, Fuzzy-logic

요 약

무선 센서 네트워크에서 독립된 센서 노드는 보안 위험에 노출되어 있다. 공격자는 센서 노드를 물리적으로 포획할수 있고 보안 정보를 얻을 수 있다. 또한 공격자는 포획한 노드를 통해 네트워크에 허위 보고서를 주입할 수 있다. 만약 이러한 허위보고서가 검출되지 않는 다면 허위 보고서는 기지 노드까지 전달될 것이다. 이러한 허위보고서 주입공격은 잘못된 경보를 울릴 뿐만 아니라 제한된 배터리로 동작하는 센서 노드의 에너지를 낭비하게 만든다. 이러한 허위 보고서 주입 공격에 대응하기 위해서 제안된 기법 중 통계적 여과기법은 허위보고서를 전달 과정 중에 검출하고 제거하기 위한 기법이다. 통계적 여과 기법에서 메시지 인증 코드의 수(보안 경계값)는 허위 보고서 검출과 에너지 절약에 있어서 매우 중요하다. 본 논문에서는 무선 센서 네트워크에서 통계적 여과 기법의 에너지 효율 향상을 위한 퍼지논리를 적용한 동적 경계값 결정 기법을 제안한다. 제안 기법은 허위 보고서 비율과 훼손된 파티션의 수, 노드의 잔여 에너지 수준을 고려하여 경계값을 결정한다. 만약 허위 보고서의 비율이 낮다면, 시스템은 네트워크의 경계값을 낮게 설정할 것이고 그렇게 하여 에너지 소모를 최소화 한다. 반대로 허위 보고서의 비율이 높다면, 경계값 역시 높게 설정하여 네트워크에 충분한 보안 수준을 제공한다.

주요어 : 무선 센서 네트워크, 허위 보고서 주입 공격, 통계적 여과 기법, 퍼지논리

* 이 논문은 교육과학기술부의 재원으로 시행하는 한국과학 재단의 연구 지원 프로그램으로 지원받았습니다. (No. 2009-0076504)
2009년 9월 3일 접수, 2009년 12월 29일 채택
[1] 성균관대학교 정보통신공학부
주 저 자 : 최현명
교신저자 : 조대호
E-mail; taecho@ece.skku.ac.kr

1. 서 론

무선 센서 네트워크는 많은 수의 감지 노드들과 하나 혹은 그 이상의 기지 노드들로 구성된다 [1]. 감지 노드는 크기가 작고 제한된 에너지를 가지며 주위 환경 정보를

수집하여 기지 노드(Base Station)로 수집한 정보를 전송한다[13]. 기지 노드는 각 노드들로부터 수집한 정보를 처리하여 사용자에 제공한다. 이러한 특징을 가진 무선 센서 네트워크는 전장의 감시와 정찰 등 군사적 목적과 산불 감지, 강수량 파악 등 환경적 목적, 체온이나 심박수 측정을 통한 환자의 상태 파악과 같은 의학적 목적 등 다양한 응용분야에서 활용될 것으로 기대되어 진다[8].

많은 무선 센서 네트워크는 감지 노드들이 개방된 환경에 배치되어 독립적으로 환경의 정보를 수집하여 무선 통신을 통해 수집한 정보를 전달한다. 또한 노드들은 크기가 소형이고 가격이 싸야 하기 때문에 계산 능력이나 저장 능력, 무선 통신 범위 등이 제한적이고 배터리로 동작하기 때문에 에너지 소모에 민감하다[1]. 이러한 소형의 감지 노드들은 공격자에 의한 물리적 위험에 취약하다[2]. 공격자가 노드를 물리적으로 포획하게 되면 노드가 가지고 있던 비밀키와 같은 중요한 정보가 공격자에게 노출이 된다. 공격자는 이 비밀키를 사용해 네트워크에 허위 정보를 주입할 수 있게 된다[3]. 이렇게 주입된 허위 정보가 기지 노드에 전달되면 사용자에게 잘못된 정보를 제공하는 문제뿐만 아니라 허위 정보가 네트워크에서 노드를 통해 기지 노드로 전달되는 과정에서 노드의 제한된 에너지를 불필요하게 소모하게 되어 전체 네트워크의 수명을 단축한다[5].

공격자에 의한 노드의 물리적 포획과 허위 보고서 주입을 막는 것은 현실적으로 불가능하다. 따라서 허위 보고서가 네트워크에 주입되면 최대한 빨리 허위 보고서를 검출하여 이를 제거해야 한다[5]. 또한 만약에 허위 보고서를 전달과정에서 검출하지 못하여 기지 노드까지 전달되어도 기지 노드에서 허위 보고서를 발견하여 사용자에게 잘못된 정보를 제공하는 일이 없도록 하여야 한다.

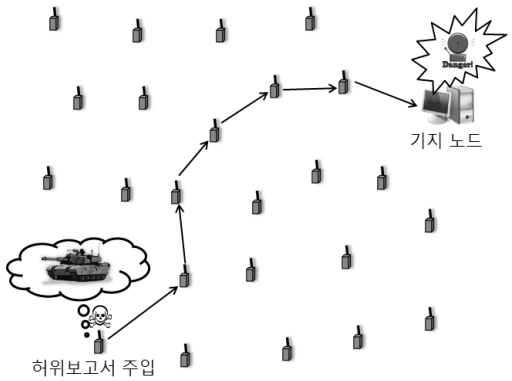


그림 1. 허위 보고서 주입공격

이러한 허위 보고서의 조기 검출과 제거를 위해 센서 네트워크에서의 다양한 허위 보고서 여과 기법들 [4-12]이 제안되었다. Ye 등[5]이 제안한 통계적 여과 기법(Statistical En-route Filtering, SEF)은 노드를 환경에 배치하기 전에 인증키의 집합인 전역 키 풀(gobal key pool)을 여러 개의 구획(partition)으로 나누고 각 노드마다 하나의 구획과 그 구획에 속한 일부 인증키를 랜덤하게 할당한 후 노드를 환경에 배치한다. SEF에서는 사건이 발생하면 그 사건을 감지한 주위의 여러 노드들이 협력하여 사건의 보고서를 만들고 이를 대표 노드(Center of Stimulus, CoS)가 기지 노드로 전달한다. 이때 보고서에는 같은 사건을 감지한 여러 노드에서 보내온 메시지 인증 코드가 포함되어 이 메시지 인증 코드를 검증함으로써 보고서가 정상 보고서인지 허위 보고서인지 판단하게 된다. 이때 보고서에 몇 개의 서로 다른 메시지 인증 코드가 포함되는지에 따라 허위 보고서의 여과율과 보고서 전송에 소모되는 에너지의 양이 결정되는 경계값(threshold)이다. 이 경계값이 크면 많은 수의 메시지 인증 코드가 보고서에 포함되어야 하기 때문에 보고서의 크기가 커지고 이를 전송하는데 소모되는 에너지가 많아진다. 하지만 메시지 인증 코드의 수가 많으므로 전달과정에서 허위 보고서를 검출할 수 있는 여과율이 증가된다. 반대로 경계값이 작으면 적은 수의 메시지 인증 코드를 보고서에 포함하므로 보고서의 크기가 작아지는 반면 허위 보고서의 여과율은 감소된다. 또한 공격자에 의해 훼손된 인증키 구역의 수가 이 경계값 보다 많다면 허위 보고서는 검출 되지 못한다. 따라서 이 경계값을 결정하는 일은 매우 주요한 일이다.

또한 SEF는 전체 보고서 중 허위 보고서의 비율이 높은 경우 에너지의 효율이 증가하고 허위 보고서의 비율이 낮은 경우에는 에너지 효율이 감소한다[5]. 하지만 이 경우에도 공격자에 의해 훼손된 노드의 수가 경계값보다 작다면 기지 노드에서 허위 보고서를 검출 할 수 있기 때문에 사용자에게 잘못된 정보가 전달되는 것을 막을 수 있다.

본 논문에서는 Fan Ye 등이 제안한 SEF[5]에 퍼지로직을 적용하여 경계값을 동적으로 결정하는 기법을 제안한다. 제안 기법은 훼손된 구획의 수와 허위 보고서의 비율, 현재 경계값을 퍼지 입력으로 하여 새로운 경계값을 결정한다. 기존에 제안된 기법인 퍼지로직을 사용한 보안 경계 값 결정 기법(DMTF)[11]과 비교하여 본 논문의 제안 기법은 허위 보고서의 비율과 훼손된 구획의 수를 고려하여 경계값을 결정함으로 DMTF에서 허위 보고서의 비율

을 고려하지 않고 여과 확률과 훼손된 구획의 수만 고려하여 허위 보고서의 비율이 아주 작은 경우에도 높은 경계값을 결정하는 문제를 해결하고 네트워크의 보안성을 유지하면서 에너지 효율을 높일 수 있다.

본 논문은 다음과 같이 구성된다. 2장에서는 배경이론으로 SEF에 대한 간단한 설명을 한다. 3장에서는 연구를 시작하게 된 동기를 설명하고 경계값 결정을 위한 퍼지논리를 설명한다. 4장에서는 제안기법의 효율성을 보여주는 시뮬레이션 결과를 보여준다. 5장에서는 결론을 내린다.

2. 통계적 여과 기법(SEF)

Fan Ye 등은 네트워크에 주입된 허위 보고서를 전달 과정에서 검출하고 제거하기 위해 SEF[5]를 제안하였다. SEF에서는 정상 보고서에 같은 사건을 감지한 주위의 여러 노드들이 생성한 메시지 인증 코드(MAC)을 포함시킨다. 보고서가 여러 노드를 거쳐 기지 노드로 전달되는 과정에 전달 노드들은 잘못된 MAC을 가진 보고서를 검출하여 이 보고서를 제거한다. 만약 전달 과정에서 검출되지 않은 허위 보고서는 기지 노드에서 최종적으로 모든 MAC을 검증하여 잘못된 MAC을 검출하여 제거 할 수 있다. SEF는 노드 배치 전 키 분배, 배치 후 보고서 생성, 전달 과정에서 허위 보고서 검출의 과정으로 동작한다.

2.1 키 분배

기지 노드는 전역 키 풀(global key pool)을 가지고 이 전역 키 풀을 중복되지 않게 n개의 구획으로 나눈다. 각 구획의 m개의 키를 가지고 각 키는 고유한 키 번호를 가진다. 노드가 배치되기 전에 사용자는 임의로 하나의 구획을 선택하고 그 구획에 속한 키 중 임의의 k개의 키를 선택한다. 이렇게 선택된 키와 키의 색인들을 노드에 저장하고 모든 노드에 키와 키 색인들이 저장되면 사용자는 노드를 관심 지역에 배치한다.

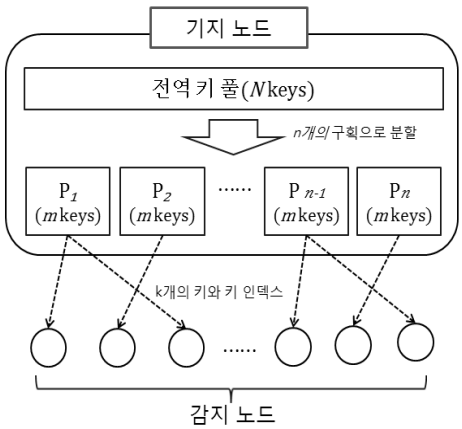


그림 2. 노드 배치 전 키 분배

2.2 보고서 생성

사건이 발생하면 그 사건 주위의 모든 감지 노드들은 사건을 감지하고 대표 노드를 선출한다. 그리고 사건을 감지한 노들은 자신이 가진 인증키 중 하나를 임의로 선택하고 그 인증키를 사용해 메시지 인증 코드(MAC)을 생성한다. MAC은 미리 약속된 암호화 방식을 사용해 만든다. 감지 노드들은 생성한 MAC과 MAC을 생성하는데 사용된 키의 번호를 같이 대표 노드로 전송한다. 대표 노드는 주위의 노드들로부터 받은 MAC과 키 번호의 쌍 중 경계값 만큼의 서로 다른 구획의 키로 만들어진 MAC과 키 번호의 쌍을 임의로 선택하여 사건 정보에 첨부하여 보고서를 생성하고 기지 노드로 전송한다.

2.3 허위 보고서 검출

보고서는 여러 노드를 거쳐 기지 노드까지 전송되는데 이 전달 과정에 있는 모든 노드들이 허위 보고서 검출을 위해 아래와 같은 과정을 거친다.

1) 보고서에 포함되어 있는 MAC과 키 번호의 쌍의 수가 정확히 경계값과 같은지 검사한다. 만약 같지 않다면 이 보고서는 제거된다.
2) 보고서에 포함되어 있는 키 번호들이 모두 서로 다른 구획의 키로 이루어져 있는지 검사한다. 만약 같은 구획의 키가 중복되어 있다면 이 보고서는 제거된다.

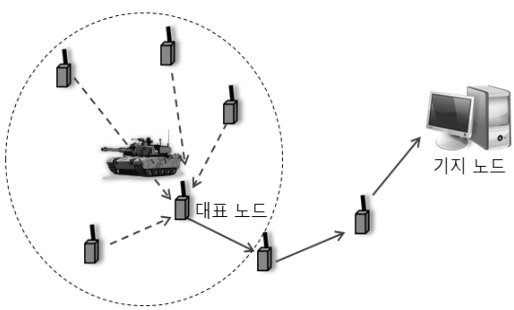


그림 3. 사건 보고서 생성

3) 만약 보고서에 포함되어 있는 키와 같은 키를 전달 노드가 가지고 있다면 그 키를 사용해 사전 정보를 MAC으로 만들어 보고서에 포함된 MAC과 같은지 확인한다. 만약 같지 않다면 이 보고서는 제거된다.
4) 1-3번 과정 중 어느 것도 해당되지 않는 다면 다음 노드로 보고서를 전달한다.

이러한 과정을 통해 SEF는 전달 과정에서 허위 보고서를 검출 할 수 있다. 하지만 만약에 전달 과정에서 허위 보고서가 검출 되지 않고 기지 노드까지 도달했더라도 기지 노드는 모든 키를 가지고 있기 때문에 보고서에 포함된 모든 MAC을 검증하여 허위 보고서를 최종적으로 여과하는 역할을 한다.

그림 4는 이러한 전달과정에서의 허위 보고서 검출을 보여준다. 그림 4는 경계값이 2인 경우에 공격자에 의해 포획된 노드가 단독으로 허위 사건 정보를 보고한다. 공격자는 자신이 획득한 키(K_3)를 사용해 MAC을 만들고 경계값 만큼의 MAC을 채우기 위해서 부족한 MAC을 임의로 위조하여 보고서를 전송한다. K_2 키 가진 노드는 자신이 가진 키로 허위 보고서의 MAC을 검사 할 수 없고 경계값 만큼의 MAC을 허위 보고서가 가지고 있기 때문에 다음 노드에게 보고서를 전달한다. K_3 키를 가지고 있는 노드는 자신이 가진 K_3 키를 이용해 보고서의 MAC (E, K_3)를 검증하였으나 K_3는 공격자에 의해 알려진 키이기 때문에 정상적인 MAC으로 판단하여 다음 노드로 보고서를 전달한다. K_1 키를 가진 노드는 자신이 가진 K_1 키로 MAC(E, K_1)을 검사하고 자신이 만든 MAC과 보고서에 있는 MAC이 일치 하지 않음을 알고 이 보고서를 허위 보고서라 판단하고 다음 노드로 전달하지 않고 제거한다.

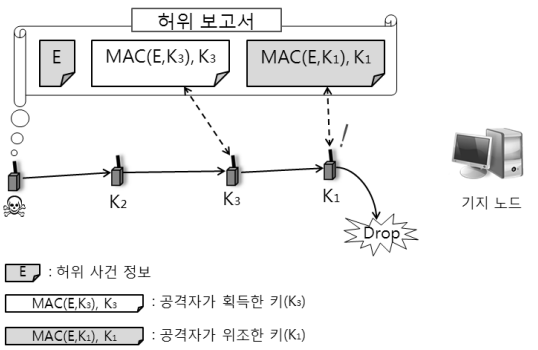


그림 4. 전달과정에서 허위 보고서 검출

3. 제안 기법

3.1 동기 및 가정

SEF 기법은 사건이 발생하면 사건 주위의 모든 노드가 협력하여 사건 보고서를 기지 노드로 전달한다. 이때 전달되는 보고서에는 사전에 정해진 경계값 만큼의 MAC이 포함된다. 경계값이 큰 경우에는 허위 보고서에 대한 충분한 여과율을 제공하지만 총 보고서 중 허위 보고서의 비율이 낮거나 공격자에 의해 포획된 노드의 수가 적어 키 구획의 훼손율이 낮은 경우에는 보고서의 전송, MAC 생성, 검증에 따른 에너지 소모가 크게 된다. 반대로 경계값이 작은 경우에는 에너지 소모는 줄어드는 반면 허위 보고서 여과율이 떨어진다. 최악의 경우 공격자에 의해 훼손된 구획의 수가 경계값 보다 크다면 허위 보고서를 기지 노드에서 조차 검출해 낼 수 없게 되고 이미 여과 기능을 상실한 MAC의 전송과 검증에 불필요한 에너지 소모가 일어나게 된다.

허위 보고서의 여과율과 보고서 전달시 소모되는 에너지를 결정짓는 경계값의 결정은 SEF에서 다른 어떤 요소보다 중요한 문제이다. 본 논문에서는 전체 보고서 중 허위 보고서의 비율과 공격자에 의해 훼손된 구획의 수, 현재의 경계값을 입력으로 하는 퍼지논리를 통해 네트워크 상황에 가장 적합한 경계값을 도출해 낸다.

전체 보고서 중 허위 보고서의 비율이 경계값 결정에 중요한 이유는 허위 보고서를 검출하여 제거하기 위한 통계적 여과 기법은 정상 보고서에는 불필요한 추가적인 에너지 소모이다. 따라서 허위 보고서의 비율이 낮은 경우 전달 과정에서 보고서의 허위 유무를 검출하기 위해 경계값을 높이는 것은 에너지 낭비이다. 따라서 일정 수준 이상의 허위보고서가 네트워크에 주입된 경우에 보안 경계값을 높게 결정하는 것이 효율적이다.

또한 경계값이 공격자에 의해 훼손된 구획의 수 이하로 낮아질 경우 공격자는 어떤 키도 위조하지 않고 자신이 가진 키로 충분히 보고서를 생성할 수 있다. 이러한 보고서는 허위 보고서이지만 시스템은 이를 검출 할 수 없다. 이것은 SEF 기법이 가지는 약점이다. 따라서 훼손된 구획의 수 이하로 경계값을 낮추어서는 안 된다. 이것은 네트워크의 보안 수준을 유지하는데 있어서 필수적이다.

허위 보고서의 비율과 훼손된 구획의 수를 알기 위해서 우리는 그림 5(a)와 같이 네트워크에 감지 노드와 기지 노드 외에 사용자의 공격에 강한 상태 측정 노드를 추가로 배치한다. 이렇게 추가로 배치된 상태 측정 노드는 클러스터를 형성해 자신의 구역에서 일어나는 허위 보고서

의 검출을 모니터링 해 기지 노드로 주기적으로 보고한다. 또한 자신의 구역에서 노드가 공격자에 의해 훼손되어 어떤 키 구획이 공격자에게 노출되었는지 알 수 있다고 가정한다. 이것은 자신의 클러스터 내에서 브로드캐스트 메시지 인증(예:μTESLA[14])을 통해 가능하다.

본 논문에서는 무선 센서 네트워크에 대해 다음과 같이 가정한다. 노드는 제한된 메모리와 처리능력을 가지고 배터리로 동작하기 때문에 제한된 에너지를 가진다. 또한 네트워크는 충분히 많은 수의 노드들로 이루어져 있어 사건이 발생하면 충분한 수의 노드들이 같은 사건을 감지할 수 있다. 기지 노드는 충분한 처리능력과 메모리 자원을 가지고 있고 에너지의 제한이 없으며 공격자의 물리적인 포획이나 정보 유출의 위험이 없다고 가정한다.

3.2 동작과정

제안 기법은 노드가 관심 지역에 배치되기 전 전역 키 풀을 구획으로 나누고 키를 분배하는 과정은 SEF와 같다. 또한 노드를 배치하기 전에 경계값을 초기값으로 설정하는 것도 SEF와 동일하다. 하지만 SEF는 경계값이 초기에 설정되면 변하지 않지만 제안 기법에서는 주기적으로 네트워크의 상태를 측정해 필요하다면 경계값을 재설정 한다는 차이점이 있다. 경계값의 재설정을 위해 제안 기법은 퍼지논리를 이용하였다. 퍼지 논리의 입력값은 전체 보고서 중에서 허위 보고서의 비율, 공격자에 의해 훼손된 구획의 수 그리고 현재 설정된 경계값으로 하고 퍼지 룰을 적용해 현재 네트워크에 가장 알맞은 경계값을 도출해내고 이를 각 노드에게 알려주어 경계값을 재설정한다.

퍼지논리의 입력값 중에 전체 보고서 중에서 허위 보고서의 비율을 알기 위해 우리는 그림 5(a)와 같은 네트워크의 상태를 측정하기 위한 상태 측정 노드를 추가로 배치하였다. 상태 측정 노드는 사건의 감지나 보고서의 전달 과정에는 전혀 개입하지 않는다. 대신에 자신의 범위 안에 있는 노드들과 통신을 하여 그 노드의 상태를 파악하고 이를 기지 노드로 전달한다. 이때 기지 노드로 전달되는 네트워크 상태 정보는 허위 보고서를 해당 클러스터에서 얼마나 제거를 하였는지, 공격자에 의해 훼손이 되었을 것으로 판단되는 노드와 그 노드가 가지고 있는 키의 구획 등이다. 만약 노드가 허위보고서를 발견하여 이를 제거한다면 이 노드는 자신이 허위보고서를 검출하였고 제거하였다고 자신의 상태 측정 노드에 이러한 정보를 알려야 한다. 상태 측정 노드는 노드로부터 허위 보고서를 전달받아 훼손되었을 것으로 예상되는 노드를 찾아낸다. 이러한 정보를 일정한 주기마다 기지노드로 전달한다. 기지 노드는 각 상태 측정 노드들로부터 네트워크의 상태에 관한 정보를 받아 현재 전체 네트워크의 상태를 알 수 있게 된다.

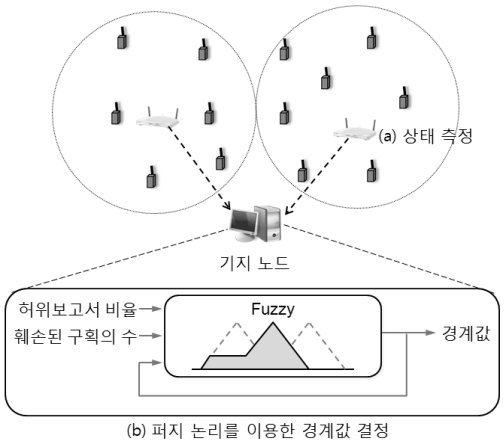


그림 5. 경계값 결정 과정

기지 노드는 허위 보고서의 비율과 훼손된 구획의 수 그리고 현재의 경계값을 입력으로 하여 현재 네트워크의 상황에 가장 적합한 새로운 경계값을 도출해 낸다. 새로운 경계값이 만약 현재의 경계값과 다르다면 기지 노드는 새로운 경계값을 각 상태 측정 노드로 전달하고 각 상태 측정 노드는 자신의 클러스터에 있는 각 노드들에게 전파한다.

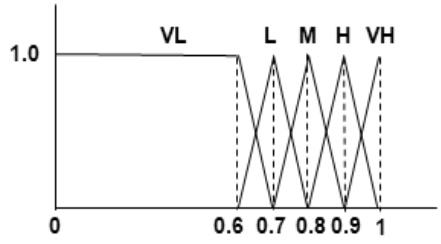
3.3 퍼지논리의 입/출력 함수와 룰

제안 기법은 SEF에서의 경계값을 결정하기 위해 퍼지 논리를 적용하였다. 퍼지 논리의 입력값은 네트워크상의 허위 보고서 비율, 훼손된 구획의 수 그리고 현재의 경계값이다.

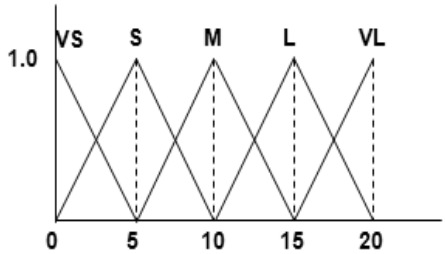
그림 6은 입력 함수를 나타낸다. 각 입력함수는 자신이 경계값에 미치는 영향을 잘 반영하게 설계되었다. 특히 그림 6(a)인 허위 보고서 비율은 전체 네트워크의 보고서 중 허위 보고서가 60% 이하인 경우에는 경계값을 최소화하여 허위 보고서 필터링에 추가적인 에너지 소모를 줄이는 것이 에너지 효율적이다. 이는 그림 9의 시뮬레이션 결과에서 확인 할 수 있다.

각 입력값은 아래와 같이 구성된다.

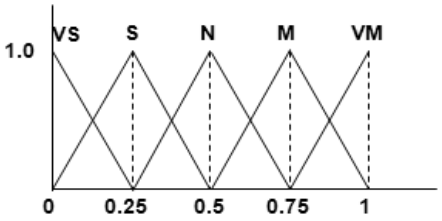
허위 보고서 비율 = {Very_Low, Low, Medium, High, Very_High}
훼손된 구획의 수 = {Very_Small, Small, Medium, Large, Very_Large}



(a) 허위 보고서 비율



(b) 훼손된 구획의 수



(c) 현재의 경계값

그림 6. 퍼지 입력 함수

현재의 경계값 = {Very_Small, Small, Normal, Much, Very_much}

그림 7은 퍼지 출력 함수를 나타낸다.

새로운 경계값 = {Very_Small, Small, Normal, Much, Very_much}

퍼지 룰은 입력값과 출력값을 고려하여 총 125개의 퍼지 룰을 적용하였다. 아래는 퍼지 룰의 일부 예이다.

RULE 2: IF Medium AND Very_small AND Very_small THEN Very_small;
RULE 8: IF High AND Very_small AND Small THEN Small;
RULE 28: IF High AND Small AND Very_small THEN Normal;

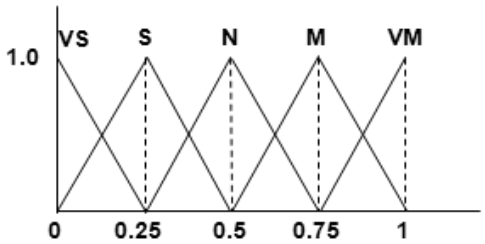


그림 7. 퍼지 출력 함수

RULE 64: IF Very_high AND Medium AND Nomal THEN Much;
RULE 84: IF Very_high AND Large AND Small THEN Very_much;

만약 허위 보고서의 비율이 Medium이고 훼손된 구획의 수가 Very_Small이고 현재 경계값은 Very_Small인 경우에는(Rule 2) 새로운 경계값을 Very_Small로 설정한다. 이것이 의미하는 것은 허위 보고서의 비율이 Medium의 범위에 들어가고 훼손된 구획의 수가 아주 작은(Very_Small) 경우에 현재 보안 경계값이 아주 작다면(Very_Small) 새로운 경계값도 Very_Small의 범위에서 결정된다.

이 경우 새로운 경계값과 현재 경계값은 Very_Small로 값은 범위를 가지지만 다른 입력값에 따라 같은 값이 나올 수도 있고 다른 값이 나올 수도 있다.

퍼지 추론 과정을 거쳐 퍼지 출력값이 도출되면 이를 경계값으로 변환한다. 퍼지 출력 함수에서 1을 최대 경계값으로 설정한다. 예를 들어 네트워크의 전체 파티션의 수가 25개인 경우 최대 경계값은 25이다. 퍼지를 통한 출력값이 0.5가 나왔다면 경계값은 0.5 * 25를 반올림한 값인 13이 된다.

이러한 과정을 거쳐 결정된 경계값이 만약 현재 경계값과 새로운 경계값이 다른 값이라면 기지 노드는 새로운 경계값을 상태측정 노드를 통해 전체 노드로 전파하여 네트워크의 경계값을 새로운 경계값으로 설정한다.

4. 시뮬레이션 결과

제안 기법의 성능을 측정하기 위한 시뮬레이션을 수행하였다. 시뮬레이션은 SEF를 기반으로 수행되었기 때문에 에너지 소모량의 계산, 필터링 확률 등의 방법은 SEF에서 실험한 결과를 사용하였다. 각 노드는 보고서 전송 시 16.25μJ/Byte, 수신 시 12.5μJ/Byte를 소모하고 메시

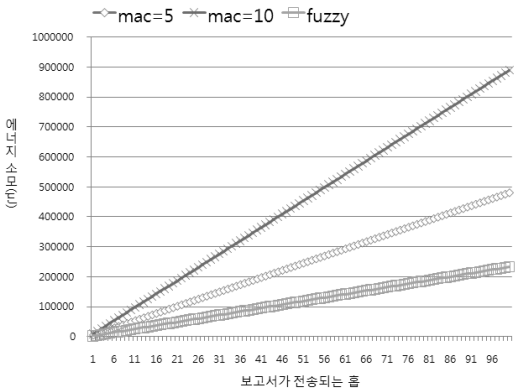


그림 8. 정상 보고서 전송 시 보고서가 전송되는 홉에 따른 에너지 소모량

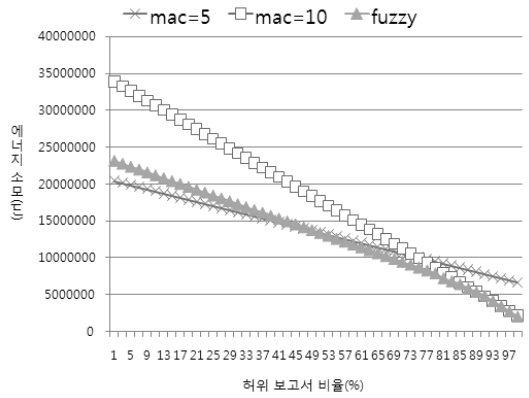


그림 9. 허위 보고서 전송 시 허위 보고서의 비율에 따른 에너지 소모량(훼손된 구획의 수 = 4, 보고서가 전송되는 홉 = 100)

지 인증 코드 생성 시 15μJ을 소모한다. 사건 보고서의 원본은 24Bytes이고 각 메시지 인증 코드는 1Byte의 용량을 차지한다. 전역 키 풀은 1000개의 키로 구성되고 25개의 구획으로 나누었다. 각 노드는 30개의 키를 가진다.

그림 8은 공격자에 의한 공격이 없는 네트워크에서 경계값이 5와 10으로 고정된 SEF와 퍼지논리를 적용한 제안기법의 보고서가 전소되는 홉의 수에 따른 에너지 소모량을 나타낸다. 경계값이 5와 10으로 고정된 SEF는 허위 보고서가 없음에도 불구하고 고정된 경계값을 유지하므로 제안기법보다 많은 에너지를 소모함을 알 수 있다. 제안 기법은 공격자에 의한 공격이 없는 상황에서는 허위 보고서의 비율이 0이고 훼손된 노드의 수도 0이기 때문에 최소한의 경계값을 유지하기 때문에 에너지 소모를 줄일 수 있다.

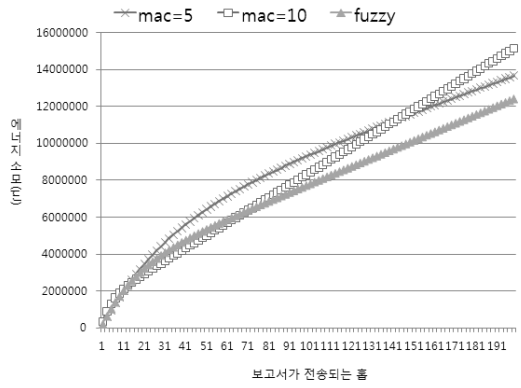


그림 10. 허위보고서 비율이 80%일 때, 보고서가 전송되는 홉의 수에 따른 에너지 소모량(훼손된 구획의 수 = 4)

그림 9는 공격자에 의해 훼손된 구획의 수가 4이고 보고서가 전달 되는 홉이 100 인 경우에 전체 보고서 중 허위 보고서의 비율에 따른 에너지 소모량을 보여준다. 허위 보고서의 비율이 낮은 경우 경계값을 5로 고정한 SEF와 제안 기법이 경계값을 10으로 고정한 SEF에 비해 낮은 에너지 소모를 보여준다. 이것은 정상 보고서가 많은 경우 일부 허위 보고서를 여과하기 위해 많은 수의 MAC을 보고서에 포함하는 것이 비효율 적임을 보여준다. 허위 보고서 비율이 70%일 때부터 경계값 10인 SEF가 경계값이 5인 SEF보다 낮은 에너지 소모를 보이고 퍼지를 적용한 제안기법은 이보다 낮은 에너지 소모를 보여준다. 제안 기법은 허위 보고서 비율에 따라 네트워크의 상황에 맞게 경계값을 결정하기 때문에 낮은 에너지 소모를 유지할 수 있다.

그림 10은 허위 보고서의 비율이 80%일 때 보고서가 전달되는 홉의 수에 따른 에너지 소모를 보여준다. 보고서가 전달 되는 홉의 수가 130 홉 이하인 경우에는 경계값을 10으로 고정한 SEF가 5로 고정한 SEF 보다 낮은 에너지 소모를 보이지만 보고서를 130 홉 이상 전달하는 대규모의 네트워크에서는 다시 경계값을 5로 고정한 SEF가 더 낮은 에너지 소모를 보여준다. 이것은 허위 보고서 여과를 위한 메시지 인증 코드는 정상 보고서 전달에는 오버헤드로 작용하기 때문에 허위 보고서 여과율을 높이기 위해 높은 경계값을 유지하는 것은 비 효율적임을 보여준다. 제안 기법은 네트워크 상황에 맞는 최적의 경계값을 유지하므로 낮은 에너지 소모를 보여준다.

그림 9와 그림 10에서 DMTF 기법은 mac=5인 경우와 같은 결과를 보여준다. 그 이유는 DMTF 기법은 허위 보

고서의 비율을 고려하지 않고 설계된 기법이기 때문에 훼손된 구획의 수가 4 인 경우 경계값을 5로 고정한다.

5. 결 론

본 논문에서는 공격자에 의한 허위 보고서 주입 공격에 대응하기 위한 여러 가지 기법 중 통계적 여과 기법에서 네트워크의 상황을 고려한 경계값 결정을 위해 퍼지논리를 적용하였다. 제안 기법에서 고려한 퍼지 입력값은 허위 보고서의 비율과 공격자에 의해 훼손된 구획의 수, 현재 네트워크에 적용된 경계값이다. 퍼지 출력값인 새로운 경계값이 현재 경계값과 다른 값이라면 네트워크에 새로운 경계값을 적용한다. 시뮬레이션을 통하여 제안 기법의 효율성을 확인하였다. 제안 기법은 허위 보고서의 비율이 높고 보고서가 전달되는 홉의 수가 많은 대규모의 네트워크에서 뛰어난 성능을 보였고 그 이외의 경우에도 SEF와 비교해 충분한 보안성을 제공하였다. 향후에는 네트워크의 허위 보고서 비율과 공격자에 의해 훼손된 노드의 수를 더욱 정확히 예측하여 제안 기법의 성능을 높일 수 있는 연구를 계속 할 것이다.

참 고 문 헌

1. I.F. Akyldiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci., “A Survey on Sensor Networks,” IEEE Wireless Communication Magazine, vol. 40, no. 8, pp. 102-116, 2002.
2. J.N. Al-Karaki and A.E. Kamal., “Routing techniques in wireless sensor networks: a survey,” IEEE Wireless Communication Magazine, vol. 11, no. 6, pp. 6-28, 2004.
3. Chris Karlof and David Wagner, “Secure routing in wireless sensor networks: attacks and countermeasure,” IEEE SPNA, pp. 113-127, 2002.
4. Przydatek, B., Song, D., and Perrig, A., “SIA: Secure Information Aggregation in Sensor Networks,” ACM, in Proc. of SenSys, pp. 255-265, 2003.
5. F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical En-route Filtering of Injected False Data in Sensor Networks,” IEEE Journals on Selected Areas in Communications, vol. 23, no. 4, pp. 839-850, 2005.
6. H. Yang and S. Lu, “Commutative Cipher Based En-route Filtering in Wireless Sensor Networks,” IEEE in Proc. of VTC, pp. 1223-1227, 2004.
7. Yu Z and Guan Y, “A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks,” In Proc. SenSys, pp. 294-295, 2005.
8. Zhu S, Setia S, Jajodia S, and Ning P, “An Interleaved Hop-by- Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks,” In Proc. S&P, pp. 259-271, 2004.
9. F. Li and J. Wu, “A probabilistic voting-based filtering scheme in wireless sensor networks,” Proc. IWCMC, pp. 27–32, 2006.
10. Lee, H.Y., Cho, T,H., “Fuzzy Adaptive Selection of Filtering Schemes for Energy Saving in Sensor Networks,” IEICE Trans. Commun. E90--B(12), 3346-3353, 2007.
11. 김상률, 조대호, “통계적 여과 기법기반의 센서 네트워크를 위한 퍼지로직을 사용한 보안 경계 값 결정 기법,” 한국시뮬레이션학회지, 16(2), pp. 27-35, 2007.
12. H.Y. Lee, T.H. Cho, “Key Inheritance-Based False Data Filtering Scheme in Wireless Sensor Networks,” Lect. Notes Comput. Sc. vol. 4317, pp.116-127, 2006.
13. Buttyan, L. et al, “Statistical Wormhole Detection in Sensor Networks,” Lecture Notes in Computer Science. 3813, 128-141, 2005.
14. Perrig, A., Szewczyk, R., Tygar, J., Wen, V. and Culler, D. “SPINS: Security Protocols for Sensor Networks,” Wirel. Netw., vol. 8, pp. 521-534, 2002.

최 현 명 (hmchoi@ece.skku.ac.kr)

2009 계명대학교 컴퓨터공학과 학사
2009～현재 ～성균관대학교 정보통신공학부 석사

관심분야 : 모델링 및 시뮬레이션, 무선 센서 네트워크, 인공 지능, 임베디드 시스템

이 선 호 (sunholee@ece.skku.ac.kr)

2009 경원대학교 인터넷미디어학부 학사
2009～현재 성균관대학교 정보통신공학부 석사

관심분야 : 무선 센서 네트워크, 모델링 및 시뮬레이션, 인공 지능, 정보 보안

조 대 호 (taecho@ece.skku.ac.kr)

1983 성균관대학교 전자공학과 학사
1988 Univ. of Alabama 전자공학과 석사
1993 Univ. of Arizona 전자 및 컴퓨터공학과 박사
1995～현재 성균관대학교 정보통신공학부 교수

관심분야 : 무선 센서 네트워크, 모델링 및 시뮬레이션, 지능 시스템, 모델링 방법론