한국시뮬레이션학회 논문지
Vol. 20, No. 3, pp. 69-78 (2011. 9)

통계적 여과 기법이 적용된 센서 네트워크에서 에너지 효율적인 네트워크 관리를 위한 영역별 경로 재설정 주기 결정 기법

박 혁[1] · 조대호[1†]

Regional Path Re-selection Period Determination Method for the Energy Efficient Network Management in Sensor Networks applied SEF

Hyuk Park · Tae Ho Cho

ABSTRACT

A large-scale sensor network usually operates in open and unattended environments, hence individual sensor node is vulnerable to various attacks. Therefore, malicious attackers can physically capture sensor nodes and inject false reports into the network easily through compromised nodes. These false reports are forwarded to the base station. The false report injection attack causes not only false alarms, but also the depletion of the restricted energy resources in a battery powered network. The statistical en-route filtering (SEF) mechanism was proposed to detect and drop false reports en route. In SEF, the choice of routing paths largely affect the energy consumption rate and the detecting power of the false report. To sustain the secure routing path, when and how to execute the path re-selection is greatly need by reason of the frequent network topology change and the nodes's limitations. In this paper, the regional path re-selection period determination method is proposed for efficient usage of the limited energy resource. A fuzzy logic system is exploited in order to dynamically determine the path re-selection period and compose the routing path. The simulation results show that up to 50% of the energy is saved by applying the proposed method.

Key words : Sensor network, False report injection attack, SEF, Fuzzy system

요 약

대규모 센서 네트워크를 구성하는 센서 노드는 개방된 무인 환경에서 동작한다. 악의적인 공격자는 일부 센서 노드를 탈취하여 허위 보고서를 주입할 수 있다. 통계적 여과 기법은 이러한 허위 보고서 주입 공격에 대응하기 위한 기법으로 보고서 전달 과정 중에 허위 보고서를 검출하고 여과할 수 있는 방법을 제안하였다. 통계적 여과 기법에서는 적절한 전달 경로 설정을 통하여 허위 보고서 검출 성능 향상뿐만 아니라 에너지 효율 또한 높일 수 있다. 하지만 네트워크의 위상 변화와 노드의 에너지 고갈 등의 다양한 환경 변화로 인하여 전달 경로를 재설정해야 하는 경우가 빈번히 발생한다. 빈번한 경로 재설정은 과도한 에너지 소모를 유발하므로 적절한 경로 재설정 주기를 결정하는 것은 매우 중요하다. 본 논문에서는 센서 네트워크의 제안된 에너지를 효율적으로 사용하기 위한 영역별 경로 재설정 주기 결정 기법을 제안한다. 제안 기법은 퍼지 시스템을 이용해 각 영역의 경로 재설정 주기를 동적으로 결정한다. 또한 주기가 결정된 영역에 대해 적절한 보안 수준을 결정하고 해당 영역은 이를 적용하여 경로를 재설정한다. 시뮬레이션을 통하여 제안 기법이 경로 재설정에 사용되는 에너지 소모량을 최대 50% 이상 감소시켰음을 확인하였다.

주요어 : 센서 네트워크, 허위 보고서 주입 공격, 통계적 여과 기법, 퍼지 시스템

*이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2011-0004955).
접수일(2011년 6월 2일), 심사일(1차 : 2011년 8월 28일), 게재 확정일(2011년 8월 30일)
[1] 성균관대학교 정보통신공학부
주 저 자 : 박 혁
교신저자 : 조대호
E-mail; taecho@ece.skku.ac.kr

1. 서 론

최근 마이크로 전자 기계 시스템(MEMS) 기술, 무선 통신, 전자 공학의 진보는 저비용, 저전력의 다기능 소형 센서 노드 개발을 가능하게 하였을 뿐만 아니라 무선 센서 네트워크(wireless sensor network: WSN)의 발전에 큰 영향을 주었다. 기본적으로 무선 센서 네트워크는 다수의 센서 노드들과 하나 이상의 기지 노드(base station: 이하 BS)로 구성된다. 센서 노드는 감지, 계산, 무선 통신 모듈 등을 이용해 주변의 환경 정보를 감지하고 BS에 전달하는 임무를 수행하고, BS는 노드들로부터 전달받은 정보를 수집하여 인터넷과 같은 기존 통신 인프라를 이용해 사용자에게 전달하는 역할을 담당한다. 이러한 무선 센서 네트워크는 시간과 장소에 제약을 받지 않고 언제 어디서나 접속할 수 있는 유비쿼터스(ubiquitous) 환경을 구축할 수 있는 핵심 기술 중 하나로써 사람들의 관심은 더욱 확산되고 다양한 응용 분야에서 활용될 전망이다[1,2].

하지만 대부분의 응용 분야에서 센서 노드는 광범위하며 개방된 무인 환경에 배치되어 운용된다는 환경적 제약과 더불어 기본적으로 제한된 메모리 사이즈와 컴퓨팅 성능, 배터리 용량 등의 기능적 제약을 함께 가지고 있다. 이와 같은 제약 사항들은 악의적인 공격자로부터의 보안 위협에 쉽게 노출될 수 있다는 것을 의미한다[3]. 따라서 센서 노드의 제한된 메모리와 컴퓨팅 능력, 배터리 등을 사용함과 동시에 보안을 위협하는 다양한 공격들로부터 네트워크를 안전하게 보호하는 것에 대한 문제는 매우 중요한 이슈이며 지속적인 연구가 필요하다.

허위 보고서 주입 공격(false report injection attack)은 무선 센서 네트워크의 응용 계층에서 발생할 수 있는 공격 유형 중 하나이다[4]. 허위 보고서 주입을 위해 악의적인 공격자는 공격을 목표로 하는 센서 네트워크의 일부 센서 노드를 물리적으로 포획하여 센서 노드가 지닌 보안 관련 정보를 획득한다. 공격자는 탈취한 노드로부터 획득한 메시지 인증 코드(message authentication code: 이하 MAC)과 같은 보안 관련 정보를 이용하여 허위 보고서를 생성한 후, 포획한 센서 노드를 통해 센서 네트워크에 허위 보고서를 주입한다. 주입된 허위 보고서는 제한된 에너지 자원을 갖는 센서 노드의 불필요한 에너지 소모에 원인이 될 뿐만 아니라 도중에 여과되지 않고 BS까지 전달될 경우에는 허위 경보를 유발한다[5].

이러한 허위 보고서 주입 공격에 대응하기 위해 조기에 허위 보고서를 탐지하고 여과할 수 있는 다양한 기법들이 제안 되어왔으며, 제안된 기법들의 성능 향상을 위한 연구도 지속되어왔다[5-11]. Ye 등이 제안한 통계적 여과 기법(statistical en-route filtering scheme: 이하 SEF)은 허위 보고서 주입 공격에 대응할 수 있는 기법중 하나이다[5]. SEF에서 각 노드는 네트워크에 배치하기 전에 여러 개의 파티션(partition)으로 분할된 전역 키 풀(global key pool)의 임의로 선택된 하나의 파티션으로부터 보고서 생성 및 검증 시 인증키로 사용할 소수의 키를 랜덤하게 할당받는다. 이벤트가 발생하면 이를 감지한 노드는 할당받은 키를 이용해 보고서에 첨부되는 MAC를 생성하고 대표 노드(center of stimulus; CoS)에 전송하고 대표 노드는 수집한 MAC들를 첨부하여 보고서를 생성한다. 생성된 보고서는 다수의 전달 노드들을 경유하여 BS까지 전달되는데, 보고서 전달 과정에 참여하는 여러 전달 노드들은 자신이 소유한 키와 동일한 키로 만들어진 MAC에 한하여 해당 보고서를 검증한다. 따라서 SEF가 적용된 센서 네트워크에서 보다 빠른 허위 보고서 여과를 위해선 서로 다른 키를 가진 전달 노드들로 라우팅 경로를 구성하여 동일한 MAC의 중복 검증 횟수를 줄이고 다양한 보고서 즉 MAC을 검증할 수 있는 보안 메커니즘이 적용된 경로 구축이 매우 중요하다[9,10]. 하지만 보안 메커니즘이 적용된 경로를 유지하기 위해선 위상(topology) 변화가 자주 일어나는 센서 네트워크의 특징 및 각 노드의 기능적, 환경적 제약을 고려하여 지속적인 경로 재설정 및 관리가 필요할 것이다[1,2].

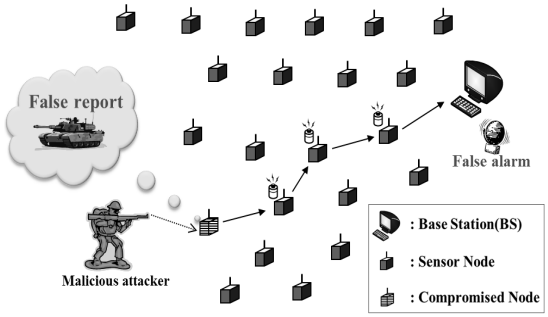

그림 1. 허위 보고서 주입 공격

본 논문에서는 SEF가 적용된 센서 네트워크에서 영역 단위로 구축한 보고서 전달 경로의 에너지 효율적인 관리를 위한 영역별 경로 재설정 주기 결정 기법을 제안한다. 제안 기법에서는 퍼지 시스템을 사용하여 여러 영역으로 분할된 센서 네트워크의 각 영역에 해당하는 잔여 에너지 수준, 허위 보고서 도달률, BS로부터의 거리, 이전 보안 강도 값을 고려하고 경로 재설정 여부 및 보안 강도 값을

동적으로 결정한다. 제안 기법은 퍼지 시스템을 이용하여 경로 재설정을 필요로 하는 영역에 대하여 제한적 경로 재설정 및 적절한 보안 강도 설정이 가능하므로 일정 보고서가 발생한 후 또는 일정 시간 경과 후에 경로를 재설정하는 고정된 경로 재설정 방법과 비교하여 경로 재설정에 사용되는 에너지 소모 및 보안 메커니즘이 적용된 경로 유지에 사용되는 에너지 소모를 줄일 수 있다.

본 논문은 다음과 같이 구성된다. 2장에서는 배경이론으로 SEF와 SEF의 허위 보고서 검출 성능 향상과 효율적인 경로 관리를 위해 제안된 기법 중 하나인 영역별 경로 설정 기법에 대해 간단히 설명한다[10]. 3장에서는 제안 기법을 설명하고 4장에서는 시뮬레이션 결과를 통하여 제안 기법의 성능을 보여준다. 마지막으로 5장에서는 결론을 내린다.

2. 배 경

2.1 통계적 여과 기법(SEF)

SEF는 센서 네트워크의 응용 계층에서 발생 가능한 공격 중 하나인 허위 보고서 주입 공격을 방어하기 위해 제안된 기법이다. SEF에서는 노드들이 협력적으로 이벤트 보고서를 생성하고 검증하며, 각 노드의 허위 보고서 검출 능력은 확률적으로 결정되는 특징을 가지고 있다. SEF는 배포 전 키 분배, 배포 후 보고서 생성, 중간 노드 여과 및 BS 검증 과정을 통하여 허위 보고서 검출을 위한 보안 메커니즘을 제공한다.

키 분배는 BS가 관리하는 전역 키 풀로부터 이루어진다. 전역 키 풀은 센서 네트워크에서 보고서 생성 및 검증에 사용되는 모든 키 정보를 포함한다. 전역 키 풀의 구조는 중복되지 않는 n개의 파티션(partition)이 고유한 인덱스를 가진 m개 키를 포함하는 총 n개의 독립된 집합과 같은 구조이다. 모든 노드는 대상(target) 네트워크에 배포되기 전에 전역 키 풀의 임의로 선택된 한 파티션으로부터 k개 키를 랜덤하게 할당 받아 저장하고 해당 네트워크에 배치된다. 그림 2는 전체 키 풀의 구조와 각 노드에 키를 분배하는 과정을 보여준다.

키 분배 과정을 거쳐 모든 노드들이 대상 네트워크에 안정적으로 배치된 후 이벤트가 발생하면 해당 이벤트를 감지한 노드들 중에서 가장 강하게 감지한 노드가 대표 노드로 선출된다. 대표 노드가 선출되면 동일한 이벤트를 감지한 주변 노드들은 자신이 소유한 키 중 임의로 하나를 선택하여, 이를 이용해 MAC을 생성한다. 또한 생성한 MAC과 MAC를 생성하는데 사용된 키의 인덱스는 해당

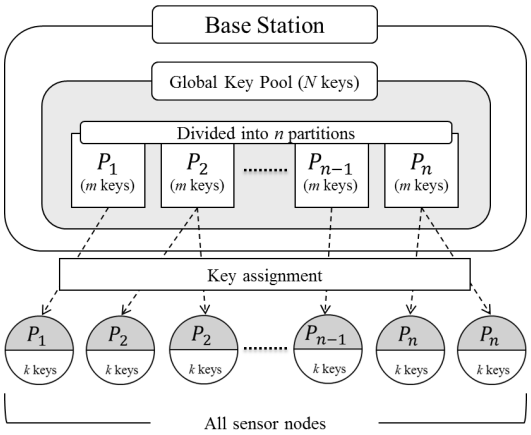

그림 2. 전체 키 풀의 구조 및 키 분배 과정

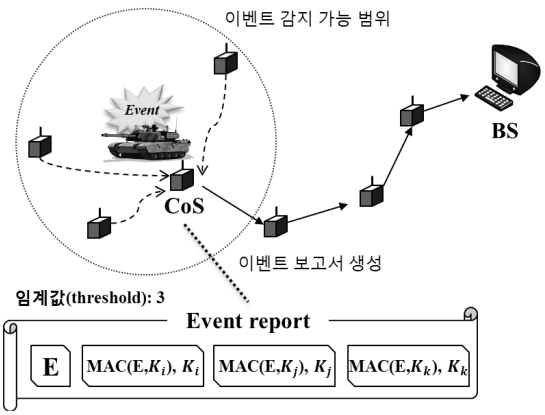

그림 3. 보고서 생성 과정

대표 노드로 전송한다. 대표 노드는 동일한 이벤트를 감지한 주변 노드들로부터 전달받은 MAC과 키 인덱스의 쌍(pair)을 모두 수집하여 파티션별로 MAC을 분류하고 서로 다른 파티션에 속하는 키로 만들어진 MAC이 정해진 임계값(threshold) 이상 존재하는지 확인한다. 만약 서로 다른 파티션으로 만들어진 MAC이 임계값 이상 존재한다면 정해진 수만큼의 서로 다른 파티션의 키로 생성된 MAC과 키 인덱스의 쌍을 임의로 선택하여 이벤트 정보와 함께 하나의 완성된 보고서를 생성한다. 그림 3은 동일한 이벤트를 감지한 노드들이 협력적으로 보고서를 생성하여 다수의 전달 노드를 거쳐 BS에 전달하는 과정을 보여준다.

보고서가 BS까지 전달되는 과정에서 전달 경로 상에 포함된 모든 중간 노드는 허위 보고서 검출을 위해 그림 4에 나타낸 바와 같은 보고서 검증 및 전달 과정을 거

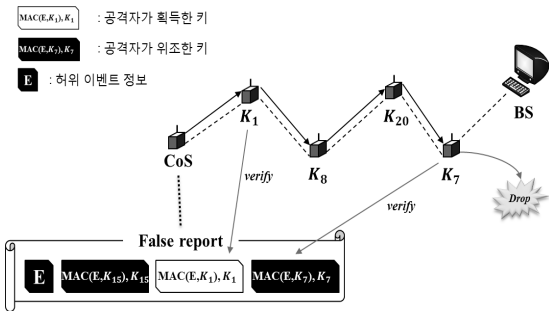

그림 4. 보고서 검증 및 전달 과정

친다. 보고서를 수신한 노드는 제일 먼저 임계값 이상의 서로 다른 키로 생성된 MAC이 존재하는지 확인한다. 만약 임계값 이상의 서로 다른 키로 생성된 MAC이 없다면 허위 보고서로 판단하여 해당 보고서를 제고하고, 반대의 경우에는 다음 검증 단계인 자신이 소유한 인증키로 생성된 MAC의 존재 유무를 확인한다. 자신이 소유한 키와 동일한 키로 생성된 MAC이 없는 경우에는 검증이 불가능하므로 다음 노드로 전송하고, 반대로 자신이 소유한 키와 동일한 키로 생성된 MAC이 있는 경우에는 해당 보고서를 검증할 수 있으므로 진위 여부가 확인된 보고서에 한해서만 다음 노드로 전송한다. 보고서 전달 과정을 거쳐 보고서가 BS까지 도착하게 되면 BS는 자신이 관리하고 있는 전체 키 풀에 저장된 모든 키 정보를 이용하여 최적으로 보고서를 검증하는 역할을 수행한다. SEF에서는 이러한 일련의 과정을 거쳐 보고서를 검증하고 허위 보고서를 여과할 수 있다.

2.2 영역별 경로 설정 기법(RSPSM)

영역별 경로 설정 기법(region segmentation based path selection method: 이하 RSPSM)에서는 SEF의 허위 보고서 검출 성능을 향상시키기 위해 대규모 센서 네트워크를 여러 개의 하위 영역으로 나누어 계층적으로 보고서 전달 경로를 구축하는 방법을 제안하였다. RSPSM은 그림 5에 나타낸 바와 같이 (a)특정한 노드(distinguishing node: 이하 DN) 배치, (b)광고 메시지 방송(broadcasting)을 통한 영역 설정, (c)영역별 경로 설정 단계를 통하여 보고서 전달 경로를 구축한다.

RSPSM을 적용하기 위해선 BS와 일반적인 센서 노드의 이외에 추가적으로 영역을 관리하는데 사용되는 DN을 대상 네트워크에 배치하여야한다. DN은 일정한 간격(m)으로 배치되며 컴퓨터 성능, 배터리 용량, 메모리 크기 등의 기능적 측면에서 일반적인 센서 노드보다 월등히 뛰

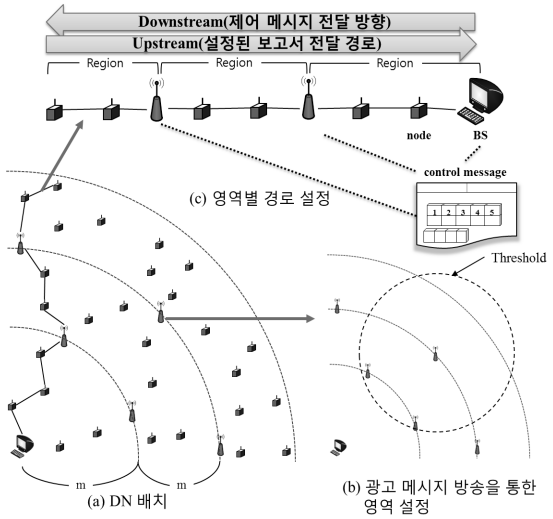

그림 5. 영역별 경로 설정

어난 성능을 가지고 있다.

DN과 모든 센서 노드가 대상 네트워크에 배치되면 BS와 모든 DN은 영역 설정을 위한 광고 메시지를 방송한다. 해당 네트워크에 배치된 모든 노드는 하나 이상의 BS 또는 DN으로부터 광고 메시지를 수신하고 네트워크에 배치되기 전에 영역 설정을 위해 설정된 수신 신호 세기(received signal strength indication: RSSI) 임계값과 BS 또는 DN으로부터 수신한 광고 메시지의 수신 신호 세기 값을 비교하여 영역의 소속 여부를 결정하고 영역 정보를 저장한다. 영역 설정 과정을 통해 모든 노드는 최소한 하나 이상의 영역에 포함될 수 있다.

영역 설정이 정상적으로 완료되면 영역 단위로 경로 설정이 가능하다. 영역별 경로 설정 단계에서는 경로 설정을 위한 제어 메시지(control message)가 각 영역의 최상의 노드인 BS 또는 상위 DN으로부터 플러딩(flooding)된다. 모든 노드는 자신이 소속된 영역의 경로 설정을 위한 제어 메시지를 수신했을 경우에만 제어 메시지에 포함된 경로 정보를 이용해 해당 경로를 평가하고 경로를 선택한다. 경로 평가는 평가 함수를 통해 이루어지며 식 (1)은 평가 함수 중 하나이다.

$$Q(p) = D(p) + \omega \cdot [P(p) + \sigma\{Cn\}] \quad (1)$$

평가 함수 Q(p)에 필요한 요소들의 값은 전달받은 제어 메시지로부터 획득할 수 있다. 식 (1)에서 D(p)는 거리를 나타내는 요소로써 경로 p의 홉 수를 의미한다. P(p)와 σ{Cn}는 보안과 관련된 요소들로써 P(p)는 경로 p의 제

어 메시지에 포함된 분할 배열의 체크 수가 0인 분할의 개수를 말하며, σ{Cn}는 n개로 분할된 분할 배열에서 각 체크 수의 값들로 구성된 집합의 원소들 간의 표준편차를 나타낸다. 마지막으로 ω는 보안 강도 요소로써, ω 값을 조절함으로써 선택되는 경로의 보안 강도를 조절할 수 있다. RSPSM은 이러한 일련의 과정을 거쳐 영역 단위로 보고서 전달 경로를 설정 및 보안 강도를 설정할 수 있다.

3. 제안 기법

3.1 동기

SEF가 적용된 센서 네트워크에서 이벤트가 발생하면 이벤트 주변의 모든 노드는 협력적으로 이벤트 보고서를 생성하고 BS에 전달한다. BS까지의 보고서 전달 과정에서 생성된 보고서는 다수의 전달 노드들을 경유하게 되며 허위 보고서 검증 및 여과는 생성된 보고서에 첨부된 MAC을 만들 때 사용된 키와 동일한 키를 가진 전달 노드가 해당 보고서를 수신했을 때 가능하다. 따라서 SEF가 적용된 센서 네트워크에서 다양한 이벤트 보고서의 허위 여부를 판단하기 위해선 각기 다른 키를 가진 노드들로 전달 경로를 구축함으로써 허위 보고서 검출 성능을 향상시킬 수 있다.

이러한 이유에서 SEF에 허위 보고서 검출 성능을 향상시키기 위해 다양한 경로 설정 기법이 제안되었다[9-11]. 이와 같이 보안 메커니즘을 적용한 보고서 전달 경로 설은 허위 보고서 검출 성능을 향상시킬 수 있는 좋은 방법임에도 불구하고 센서 네트워크의 잦은 위상 변화 또는 노드 간 로드 밸런싱, 네트워크의 보안 강도 변경 등 다양한 이유로 자주 경로를 재설정한다면 이는 제안된 에너지 자원을 갖는 센서 네트워크의 수명을 단축시킬 것이다. 따라서 보안 메커니즘이 적용된 보고서 전달 경로를 효율적

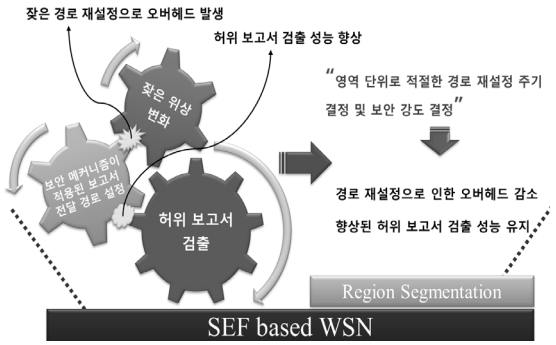

그림 6. 문제 제기 및 개선 방향

으로 관리하기 위해선 적절한 경로 재구축 시기 결정 및 구축된 경로의 적절한 보안 강도 설정은 필수적이다.

또한 대규모 센서 네트워크를 영역 단위로 관리할 수 있는 RSPSM과 같은 경로 설정 기법을 이용하여 영역 단위로 환경을 모니터링하고 차별화된 경로 재설정 여부 및 보안 강도를 결정한다면 보다 효율적인 네트워크 관리가 이루어질 것이다.

3.2 퍼지 시스템 기반 영역별 경로 재설정 여부 및 보안 강도 결정

3.2.1 제안 기법 적용을 위한 센서 네트워크 모델

본 제안 기법을 적용하기 위해 사용될 센서 네트워크 모델은 다음과 같다. 네트워크는 충분히 많은 수의 센서 노드와 소수의 DN, 하나의 BS로 구성된 대규모 센서 네트워크이며 이벤트가 발생하면 충분한 수의 노드들이 동일한 이벤트를 감지할 수 있다. 또한 SEF가 센서 네트워크에 적용되어 허위 보고서 주입 공격을 방어할 수 있고 SEF의 허위 보고서 검출 성능을 향상시키기 위해서 RSPSM을 사용해 보고서 전달 경로가 구축되었다. 네트워크에 존재하는 모든 영역의 보안 강도 값은 최소 0에서 최대 1까지 설정 가능하며 초기 설정 단계에서는 0.5로 동일하게 설정된다. 또한 BS는 각 영역의 최상위 노드인 상위 DN에 최단 경로로 메시지를 전송할 수 있다.

3.2.2 동작 과정

제안 기법에서는 영역 단위로 차별화된 경로 재설정 여부 및 보안 강도 값을 결정하기 퍼지 시스템을 이용하였다. 퍼지 시스템은 BS에 위치하며 각 영역의 경로 재설정 여부 및 보안 강도 값을 결정하기 위해 다음과 같은 경우 중 하나를 만족할 때 실행된다.

(1) 임계값 이상의 허위 보고서 도달률: BS에 도달하는 보고서 중 허위 보고서의 비율이 시스템에 설정한 최대치(임계값) 보다 높은 경우로써 현재 네트워크에 대규모 공격이 진행 중이거나 네트워크에서 설정된 보안 강도 값이 부적절한 경우이다.
(2) 일정 수만큼의 보고서가 발생한 후: 1번 경우가 발생하지 않고 현재 네트워크가 정상적으로 작동 중이지만 단 시간에 많은 이벤트가 발생한 경우이다.
(3) 일정 시간 경과 후: 1~2번 경우가 발생하지 않고 현재 네트워크가 정상적으로 작동 중이지만 오랜 시간 동안 같은 경로를 운용한 경우이다.

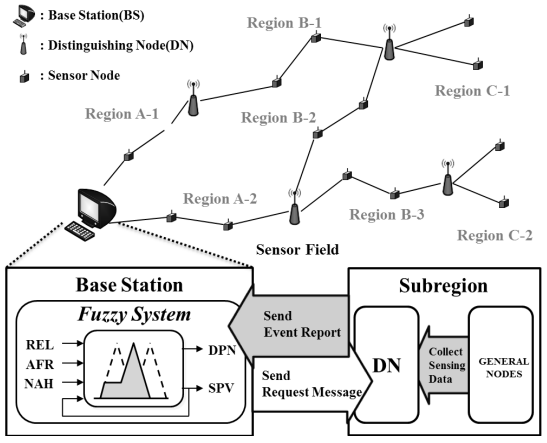

그림 7. 데이터 흐름 및 동작 과정

이와 같이 경로 재설정이 필요할 것이라고 예측되는 시기마다 퍼지 시스템을 이용해 각 영역의 경로 재설정 여부를 결정한다. 또한 퍼지 시스템이 실행되기 전에 BS는 각 영역으로부터 수신한 이벤트 보고서를 중심으로 퍼지 시스템에 사용될 입력 값들을 추출하여 퍼지 시스템에 전달한다. 퍼지 시스템은 BS로부터 전달받은 입력 값들을 계산하여 각 영역의 경로 재설정 여부 및 보안 강도 값을 출력 값으로 제공한다. 퍼지 시스템으로부터 출력 값을 제공받은 BS는 경로 재설정이 필요한 영역으로 판단된 영역의 최상위 노드인 상위 DN에게 경로 재설정 시 적용할 보안 강도 값을 포함한 경로 재설정 요청 메시지(request message)를 송신한다. 그림 7은 퍼지 시스템과 연관된 센서 네트워크 전체의 데이터 흐름과 퍼지 시스템 동작 과정을 보여준다.

3.2.3 퍼지 시스템의 입력 요소

각 영역의 경로 재설정 여부 및 보안 강도 값을 결정하기 위한 퍼지 시스템의 4가지 입력 값은 다음과 같다.

- REL(Remaining Energy Level; 잔여 에너지 수준): 이 요소는 각 영역에 소속된 노드들의 평균 잔여 에너지 수준을 나타낸다. 잔여 에너지 수준은 제한적인 에너지 자원을 갖는 센서 네트워크의 매우 중요한 이슈 중 하나이기 때문에 경로 재설정 여부 및 보안 강도를 결정하기에 앞서 충분히 고려되어야하는 요소이다. 만약 해당 영역의 잔여 에너지 수준이 너무 낮다면 다른 입력 요소들이 경로 재설정에 무게가 실리는 값으로 나타나는 경우라 할지라도 경로 재설정을 수행하지 않는다. 이러한 경우에는 전체 네트워크의 수명을 길게 유지하기위해 BS 또는 상위 영역에서 허위 보고서를 검증하도록 하는 것이 더욱 효율적인 결정이 될 것이다.
- AFR(Arrival False Report ratio; 허위 보고서 도달률): 이 요소는 각 영역으로부터 생성되어 BS에 도달한 이벤트 보고서 중 허위 보고서의 비율이 얼마인지를 나타낸다. 허위 보고서 도달률 값을 통해 현재 각 영역에 적용된 보안 수준이 적절한지를 판단할 수 있다. 만약 해당 영역에서 수집된 이벤트 보고서들 중 허위 보고서 도달률이 높은 경우에는 해당 영역의 노드들이 공격자에 의해 많이 훼손되거나 영역에 설정된 보안 강도 값이 상대적으로 낮게 설정되었다는 것을 뜻한다. 이러한 경우에는 경로 재설정을 통하여 보안 강도를 높게 설정하여 해당 영역의 보안 성능을 향상시킬 수 있다.
- NAH(the Number of Average Hops; 평균 홉 수): 이 요소는 각 영역과 BS 간의 거리를 나타내며 에너지 측면에서 전체 네트워크의 밸런스를 유지하기위한 중요한 요소 중 하나이다. 평균 홉 수 값 낮을수록 BS에서 가까운 영역임을 뜻한다. 일반적으로 네트워크 전체에서 고르게 이벤트가 발생한다고 가정할 경우 BS에 가까운 노드일수록 보고서 전달 즉 통신에 대한 에너지 소모가 심하다. 따라서 통신에 대한 오버헤드를 줄이기 위해 BS에서 가까운 영역은 보안 강도를 상대적으로 낮게 설정하여 BS에서 허위 보고서를 검증하도록 하는 것이 더욱 효율적인 결정이 될 것이다.
- (current Security Power Value: 현재 보안 강도 값): 이 요소는 현재 각 영역에 적용되어있는 보안 강도 수준을 나타낸다. 현재 적용되어있는 보안 강도 수준을 고려하여 경로 재설정 여부 및 경로 재설정 시 적용할 새로운 보안 강도 값을 보다 효율적으로 결정할 수 있다.

3.2.4 퍼지 멤버십 함수 및 규칙

퍼지 시스템에서 사용되는 각 입력 값에 대한 멤버십 함수는 여러 번의 퍼지화(fuzzification)와 실험을 반복적으로 수행하며 출력 값 즉 경로 재설정 여부 및 보안 강도 값을 결정하는데 가장 적절하게 영향을 미칠 수 있는 함수로 결정하였다. 그림 8은 각 입력 값에 대한 퍼지 멤버십 함수를 나타낸다.

그림 8의 (a)에 표현한 잔여 에너지 수준은 총 5개의 퍼지 집합으로 구성되어있고 (b)에 표현한 허위 보고서

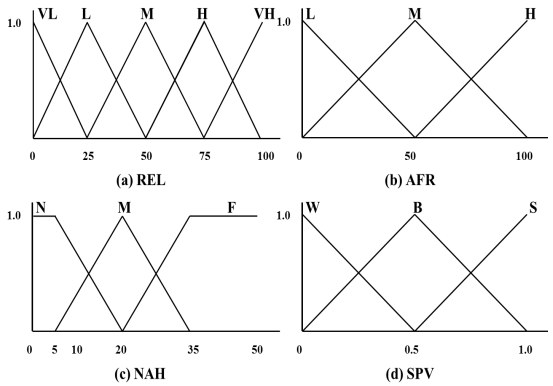

그림 8. 입력 값에 대한 퍼지 멤버십 함수

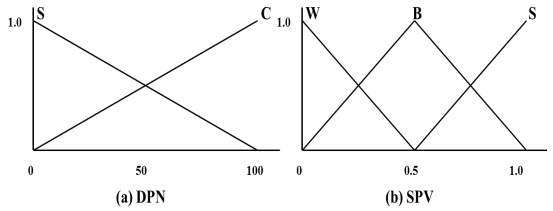

그림 9. 출력 값에 대한 퍼지 멤버십 함수

도달률, (c)에 표현한 평균 홉 수, (d)에 표현한 현재 보안 강도 값은 각각 총 3개의 퍼지 집합으로 구성되어있다. 각 입력 값에 대한 구성은 다음과 같이 표현할 수 있다.

- REL = {VL(Very Low), L(Low), M(Medium), H(High), VH(Very High)}
- AFR = {L(Low), M(Medium), H(High)}
- NAH = {N(Near), M(Middle), F(Far)}
- SPV = {W(Weak), B(balanced), S(Strong)}

그림 9는 출력 값에 대한 퍼지 멤버십 함수를 나타낸다. 그림 9의 (a)에 표현한 경로 재설정 여부(Do Path re-selection or Not do: DPN)은 총 2개의 퍼지 집합으로 구성되어있으며 (b)에 표현한 경로 재설정 시 적용할 새로운 보안 강도 값(new Security Power Value: SPV)은 총 3개의 퍼지 집합으로 구성되어있다. 각 출력 값에 대한 구성은 다음과 같이 표현할 수 있다.

- DPN = {S(Stay), C(Change)}
- SPV = {W(Weak), B(balanced), S(Strong)}

각 영역의 경로 재설정 여부 및 보안 강도 값 결정을 위한 퍼지 시스템에는 총 135(5×3×3×3)개의 퍼지 규칙이 적용되었다. 표 1은 퍼지 시스템에 적용된 퍼지 규칙들 중 몇 가지 규칙을 나타낸다.

표 1. 퍼지 If-then 규칙

Rule No.	Input				Output	
	REL	AFR	NAH	SPV	DPN	SPV
1	VL	L	N	W	S	-
15	L	M	F	W	S	-
67	M	M	N	B	C	W
89	VH	H	M	B	C	S
112	M	M	N	H	C	W

만약 퍼지 규칙 1(Rule 1)에 해당하는 조건과 같은 영역 즉, 해당 영역의 잔여 에너지 수준이 Very Low이고 해당 영역에서 발생한 보고서의 허위 보고서 비율이 Medium이며 BS로부터의 거리가 Near고 현재 설정된 보안 강도 값이 Weak로 설정된 경우에는 경로 재설정을 하지 않는다. 또한 경로 재설정이 필요 없는 영역으로 판단되었기 때문에 새로운 보안 강도 값 역시 적용될 필요가 없으므로 출력하지 않고 기존 보안 강도 값을 그대로 유지한다.

위에서 언급한 퍼지 입출력 값들과 퍼지 규칙들을 이용한 퍼지 시스템을 통해 출력 값이 도출되고 해당 영역이 경로 설정이 필요한 영역으로 결정되면, 동작과정에서 언급한 바와 같이 BS는 경로 재설정 요청 메시지에 새로 적용할 보안 강도 값 정보를 첨부하여 해당 영역의 최상의 노드인 상위 DN에 전달한다. 경로 재설정 요청 메시지를 전달 받은 상위 DN은 RSPSM에서 제안한 경로 설정 기법과 같은 방법으로 제어 메시지를 이용하여 해당 영역의 경로를 재설정한다.

4. 시뮬레이션

본 논문에서 제안한 영역별 경로 재설정 주기 결정 기법의 성능을 검증하기 위해 시뮬레이션을 수행하였다. 시뮬레이션은 제안 기법과 비교하기 위하여 제안 기법 이외에 고정된 주기마다 경로 재설정을 실행하는 두 가지 경로 재설정 방법을 사용하였다. 두 가지 경로 재설정 방법은 다음과 같다.

(1) 시간 기반 경로 재설정(time-based path re-selection): 센서 네트워크 운용 시간을 기준으로 일정한 시간마다 모든 영역의 보고서 전달 경로를 재설정하는 방법이다.

(2) 보고서 기반 경로 재설정(report-based path re-selection): 센서 네트워크에서 발생한 이벤트를 기준으로 일정한 수의 이벤트 보고서가 생성되면 모든 영역의 보고서 전달 경로를 재설정하는 방법이다.

위에서 언급한 두 가지 경로 재설정 주기 결정 방법은 제안 기법과 동일한 시뮬레이션 환경에서 적용되어 제안 기법의 성능을 검증할 수 있는 비교 대상으로 활용되었다. 시간 기반 경로 재설정은 매 1000초 마다 경로 재설정을 수행하였고, 보고서 기반 경로 재설정은 500개의 이벤트가 발생할 때 마다 매번 경로 재설정을 수행하였다. 시뮬레이션에 사용되는 가상 네트워크는 900×900 m^2의 크기로 구성하였다. 총 2,000개의 센서 노드와 9개의 DN, 1개의 BS를 배치하였으며 RSPSM에서 제안한 영역 설정 방법을 사용하여 18개의 하위 영역이 설정되었다. 전역 키 풀은 총 1,000개의 키들이 20개의 파티션으로 나뉘어 구성되었고 각 노드는 5개의 키들을 할당받았다. 영역 설정에 필요한 광고 메시지의 크기는 1 byte, 경로 설정에 사용되는 제어 메시지의 크기는 15 bytes, 이벤트 보고서의 원본 크기는 12 bytes으로 각각 설정되었으며 이벤트 보고서에 첨부되는 하나의 MAC의 크기는 1 byte로 설정되었다. 각 노드는 byte 당 송/수신에 사용되는 에너지로 16.56 μJ/12.5 μJ을 소비하고, MAC을 생성하는데 15 μJ를 소비한다[5,13,14]. 시뮬레이션을 진행하는 동안 임의로 선정된 위치에서 총 5000번의 이벤트를 발생시켰으며 그중 500개는 허위 보고서를 발생시켰다.

성능 평가 지표는 총 3가지로써 이벤트 발생에 따른 영역별 경로 재설정 횟수, 노드 당 평균 에너지 소모량, 허위 보고서 여과율이다.

그림 10은 네트워크에서 일정한 수의 이벤트 발생 시 생성되는 이벤트 보고서에 따른 하위 영역 단위로 실행된 누적 경로 재설정 실행 횟수를 보여준다. 보고서 기반 경로 재설정의 경우에는 매 500개의 이벤트가 발생할 때 마다 18개의 하위 영역 전체에서 경로 재설정이 실행되었고 시간 기반 경로 재설정 방법의 경우에는 네트워크 운용 시간 기준으로 매 1000초 마다 18개의 하위 영역 전체에서 경로 재설이 실행되었음을 확인할 수 있다. 반면에 제안 기법의 경우 제안한 퍼지 시스템을 사용해 각 영역단위로 경로 재설정 여부를 평가하고 결정함으로써 앞서 언급한 두 방법과 비교하여 경로 재설정 실행되는 횟수를 최대 50%이상 감소시켰음을 확인할 수 있다.

그림 11은 네트워크에서 일정한 수의 이벤트 발생 시 생성되는 이벤트 보고서에 따른 각 노드 당 평균 에너지 소모량을 보여준다. 제안 기법을 포함한 3가지 경로 재설정 주기 결정 방법에 대한 그래프의 정점은 경로 재설정에 사용되는 각 노드 당 최대 에너지 소모량을 나타낸다. 그래프를 통하여 제안 기법이 경로 재설정 실행 시에 사용되는 에너지 소모량을 다른 두 가지 방법과 비교하여 대폭 감소 시켰음을 확인할 수 있고 일반적인 네트워크 운용 시에는 에너지 소모량 측면에서 세 가지 방법 모두

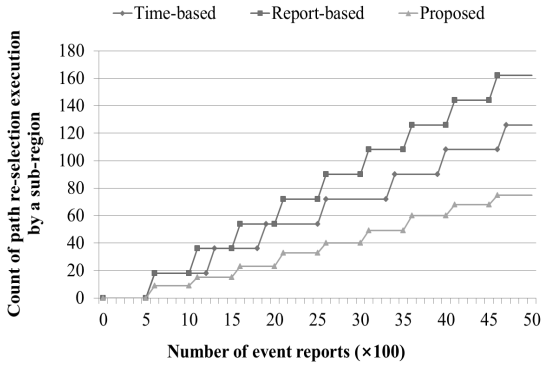

그림 10. 누적 경로 재설정 실행 횟수

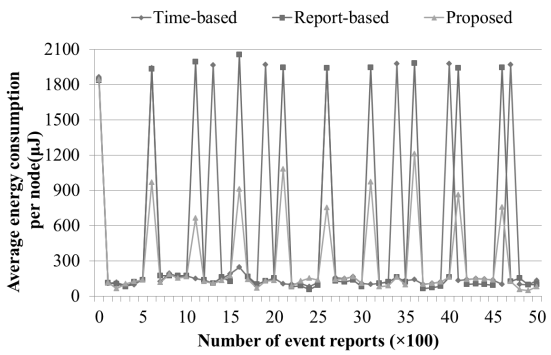

그림 11. 각 노드 당 평균 에너지 소모량

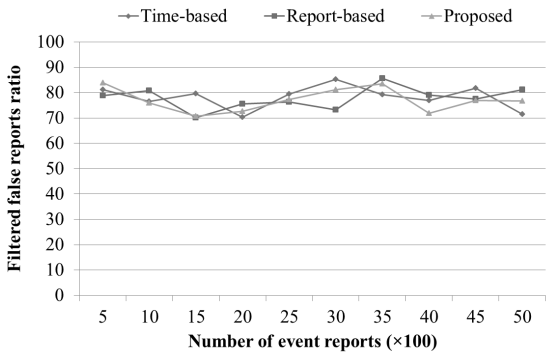

그림 12. 허위 보고서 여과율

별다른 차이가 없음을 확인할 수 있다.

그림 12는 네트워크에서 일정한 수의 이벤트 발생 시 생성되는 이벤트 보고서에 따른 허위 보고서 여과율을 보여준다. 그래프에서 확인할 수 있듯이 세 가지 경로 재설정 주기 결정 방법은 약간의 차이는 있지만 거의 동등한 성능으로 허위 보고서를 여과하였다.

위와 같은 시뮬레이션을 통하여 제안 기법은 고정적인 경로 재설정 주기를 갖는 두 가지 방법과 비교하여 기존에 향상된 허위 보고서 검출 성능을 유지하면서도 경로 재설정에 사용되는 에너지 소모량을 최대 50%이상 감소시켰음을 확인할 수 있다.

5. 결 론

본 논문에서는 퍼지 시스템을 사용하여 빈번히 경로 재설정 실행을 통해 사용되는 불필요한 에너지 소모를 줄이기 위한 영역별 경로 재설정 주기 결정 기법을 제안하였다. 퍼지 시스템은 각 영역의 잔여 에너지 수준, 허위 보고서 도달률, 평균 홉 수, 현재 보안 강도 값을 입력 값으로 사용하였다. 퍼지 시스템의 출력 값인 각 영역별 경로 재설정 여부 및 보안 강도 값을 이용해 각 영역의 경로 재설정 주기를 동적으로 결정하고, 주기가 결정된 영역은 해당 보안 강도 값을 적용하여 경로를 재설정한다. 시뮬레이션을 통하여 제안 기법이 허위 보고서 검출 성능을 유지하면서도 경로 재설정에 사용되는 에너지 소모를 줄일 수 있음을 검증하였다.

향후에는 본 연구에서 고려한 네 가지 입력 요소 이외에 경로 재설정 주기 결정에 영향을 주는 추가적인 입력 요소에 대한 연구를 진행할 예정이다. 또한 현재 연구된 퍼지 시스템을 허위 보고서를 여과 할 수 있는 다른 기법에도 적용할 예정이다.

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. 102-144, 2002.
2. J. Yick, B. Mukherjee and D Ghosal, “Wireless sensor network survey,” Computer Networks, vol. 52, no. 12, pp. 2292-2330, 2008.
3. 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.
4. C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Elsevier’s Ad Hoc Networks Journal, Special Issue on Sensor Network Protocols and Applications, vol. 1, no. 2-3, pp. 293-315, 2003.
5. 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.
6. Z. Yu and Y. Guan, “A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks,” ACM, Proc. of Sensys, pp. 294-295, 2005.
7. H. Yang and S. Lu, “Commutative Cipher Based En-route Filtering in Wireless Sensor Networks,” IEEE in Proc. of VTC, pp. 1223-1227, 2004.
8. F. Li and J. Wu, “A probabilistic voting-based filtering scheme in wireless sensor networks,” Proc. IWCMC, pp. 27–32, 2006.
9. C.I. Sun, H.Y. Lee and T.H. Cho, “A Path Selection Method for Improving the Detection Power of Statistical Filtering in Sensor Networks,” Journal of Information Science and Engineering, vol. 25, no. 4, pp. 1163-1175, 2009.
10. H. Park, S.Y. Moon, and T.H. Cho, “A Region Segmentation Based Path Selection Method for WSNs,” IJCSNS, vol. 11, no. 2, pp. 88-93, 2011.
11. B.H. Kim, H.Y. Lee and T.H. Cho, “Fuzzy Key Dissemination Limiting Method for the Dynamic Filtering-Based Sensor Networks,” Lect. Notes Computer Science, vol. 4681, pp. 261-272, 2007.
12. H. Park, C.H. Sun, and T.H. Cho, “A Secure Path Determination Method for Statistical En-route Filtering Based Wireless Sensor Network,” In Proc. of 3rd International Conference on Advanced Computer Theory and Engineering, vol. 2, pp. 603-607, 2010.
13. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, “System Architecture Directions for Networked Sensors,” In Proc. of ACM ASPLOS IX, pp. 93-104, 2000.
14. Xbow sensor networks, http://www.xbow.com

박 혁 (hpark@ece.skku.ac.kr)

2010 세명대학교 전자상거래학과 학사
2010～현재 성균관대학교 정보통신공학부 석사과정

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

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