한국시뮬레이션학회 논문지
Vol. 20, No. 4, pp. 21-29 (2011. 12)

USN에서 중간 노드에서의 보고서 검증 시도 확률 평가 함수를 이용한 에너지 효율 향상 기법

이현우[1] · 문수영[1] · 조대호[1†]

A Method to Improve Energy Efficiency Using a Function that Evaluate the Probability of Attempts to Verify a Report at Intermediate Node in USN

Hyun Woo Lee · Soo Young Moon · Tae Ho Cho

ABSTRACT

Wireless sensor nodes operate in open environments. The deployed sensor nodes are very vulnerable to physical attacks from outside. Attackers compromise some sensor nodes. The compromised nodes by attackers can lead to false data injection into sensor networks. These attacks deplete the limited energy of sensor nodes. Ye et al. proposed the Statistical En-Route Filtering (SEF) as a countermeasure of the attacks. The sensor node in SEF examines the event reports based on certain uniform probability. Thus, the same energies are consumed in both legitimate reports and false reports. In this paper, we propose a method that each node controls the probability of attempts to verify a report to reduce energy consumption of sensor nodes. The probability is determined in consideration of the remaining energy of the node, the number of hops from the node to SINK node, the ratio of false reports. the proposed method can have security which is similar with SEF and consumes lower energy than SEF.

Key words : Wireless Sensor Network, Statistical En-Route Filtering, False Data Injection Attack

요 약

무선 센서 노드들은 개방된 환경에서 동작하기 때문에 외부의 물리적인 공격에 매우 취약하다. 공격자는 노드들을 훼손시켜서 센서 네트워크에 허위 보고서를 주입시킬 수 있다. 이러한 공격들은 센서 노드들의 에너지를 고갈시킨다. 이에 대응하는 보안 기법으로 Ye등은 중간 노드가 일정한 확률로 보고서를 검증하는 통계적 여과 기법을 제안하였다. 통계적 여과 기법은 모든 중간 노드가 같은 확률로 보고서 검증을 수행한다. 따라서 정상 보고서와 허위 보고서를 검증하는데 같은 에너지가 소모되므로 정상 보고서를 검증하는데 불필요한 에너지를 소모하게 된다. 본 논문에서는 각 중간 노드가 보고서 검증 시도 확률을 조절하여 센서 노드들의 에너지 소모량을 줄이는 기법을 제안한다. 보고서 검증 시도 확률은 한 노드의 잔여 에너지양, 현재 노드에서 기지 노드까지의 홉 수, 허위 보고서의 비율에 의해 결정된다. 보고서 검증 시도 확률을 조절하여 통계적 여과 기법과 비슷한 보안성을 유지하면서 에너지의 효율성을 높일 수 있다.

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

*이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2011-0004955).

접수일(2011년 7월 13일), 심사일(1차 : 2011년 11월 13일, 2차 : 2011년 12월 17일), 게재 확정일(2011년 12월 19일)

[1] 성균관대학교 전자전기컴퓨터공학과
주 저 자 : 이현우
교신저자 : 조대호
E-mail; taecho@ece.skku.ac.kr

1. 서 론

무선 센서 네트워크(Wireless Sensor Network)는 특정 지역에 많은 센서 노드(Sensor node)들이 배치되어 협력적으로 동작함으로써 이루어진다[1-3]. 그림 1은 무선 센서 네트워크의 동작 과정을 나타낸 것이다.

그림 1과 같이 센서 네트워크는 사용자가 얻고자 하는

데이터가 있는 지역에 센서 노드들이 배치된다. 이 지역에서 이벤트가 발생하면 센서 노드들이 이벤트를 감지하고 데이터를 처리하여 기지 노드(SINK)로 전달한다. 기지 노드는 센서 노드들로부터 받은 데이터를 기존 통신 인프라를 이용하여 사용자에게 전달한다[3]. 또한 센서 네트워크는 개방된 환경에서 동작하기 때문에 상대적으로 크기가 작고 무인 동작하는 센서 노드들은 외부의 공격에 의해 포획되고 훼손되기 쉽다[2]. 따라서 센서의 정보 도청이나 전체 네트워크를 마비시킬 수 있는 서비스 거부 등의 공격에 노출되어 있다[1,5]. 특히 허위 보고서 주입 공격(False Data Injection Attack)은 공격자가 센서 노드를 포획한 후, 허위 보고서를 생성하도록 하여 기지노드에게 전달한다[2]. 포획당한 센서 노드가 잘못된 이벤트 보고서를 생성함으로써 허위 경보를 울리게 할 뿐만 아니라 센서 노드의 제한된 에너지를 고갈시켜서 전체 센서 네트워크의 수명을 단축시킨다[2]. 이러한 허위 보고서 주입 공격에 대응하기 위해 많은 기법들이 제안되었다[6-8]. Ye(2005) 등이 제안한 통계적 여과 기법(Statistic En-Route Filtering)[2]은 각 중간 노드에서 인증키를 이용하여 일정한 확률로 보고서를 검증한다. 검증한 결과가 허위 보고서로 판단되면 보고서를 다음 노드에게 전달하지 않고 폐기한다. 따라서 허위 보고서를 조기에 검출하여 허위 보고서 주입 공격에 대응할 수 있다. 그러나 통계적 여과 기법은 허위 보고서와 정상 보고서를 모두 같은 확률로 검증하기 때문에 정상 보고서의 검증에 불필요한 에너지를 소모한다[4]. 본 논문에서는 각 중간 노드에서 보고서를 검증하는데 소모되는 에너지를 감소시키기 위해 보고서 검증 시도 확률을 조절하는 기법을 제안한다. 보고서 검증 시도 확률을 조절하여 각 보고서마다 다른 확률로 검증함으로써 모든 보고서를 같은 확률로 검증하는 통계적 여과 기법과 비슷한 보안성을 유지하면서 불필요한 에너지 소모를 감소시킬 수 있다.

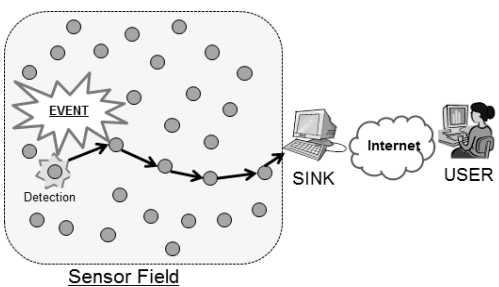


그림 1. 무선 센서 네트워크의 동작 과정

본 논문의 구성은 다음과 같다. 2장에서는 배경 이론으로 통계적 여과 기법에 대해서 설명한다. 3장에서는 제안 기법의 동기와 동작 과정에 대해 설명한다. 4장에서는 통계적 여과 기법과 제안 기법의 보안성과 에너지 소모량을 비교한 시뮬레이션 결과를 설명하고 마지막으로 5장에서는 결론을 맺는다.

2. 통계적 여과 기법

통계적 여과 기법은 무선 센서 네트워크에서 중간 노드들이 이벤트 보고서를 전달하는 과정에서 조기에 허위 보고서를 검출 및 제거하고 데이터 처리와 통신의 과부하를 낮추는 기법이다[2].

2장에서는 통계적 여과 기법의 동작 과정을 키 분배(Key Assignment) 및 보고서 생성 단계(Report Generation), 중간 노드 여과 단계(En-Route Filtering), 그리고 기지 노드 검증(Sink Verification)으로 나누어 설명한다.

2.1 키 분배 및 보고서 생성

센서 네트워크에서 센서 노드들은 특정 지역에 배치되기 전에 사용자로부터 보고서를 검증하는데 사용되는 인증키(Key)들을 할당 받는다. 모든 인증키는 기지 노드의 전역 키 풀(Global Key Pool)이 가지고 있다.

전역 키 풀은 N개의 인증 키들을 가지고 있으며 중첩되지 않는 n개의 파티션(Partition)들로 나누어져 있다. 각 파티션은 m개의 인증 키들을 가지며 각 인증키는 고유의 색인(Index)을 가지고 있다. 다음 그림 2는 통계적 여과 기법의 키 분배 과정을 나타낸 것이다.

그림 2와 같이 사용자는 전역 키 풀에서 무작위로 하나

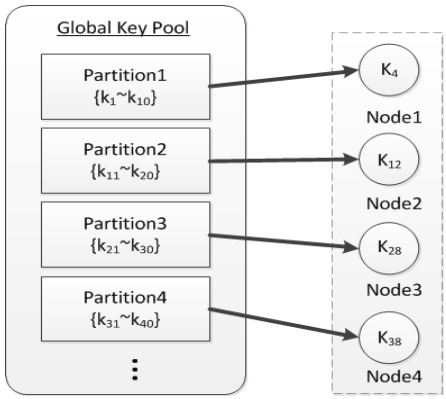


그림 2. 통계적 여과 기법의 키 분배 과정

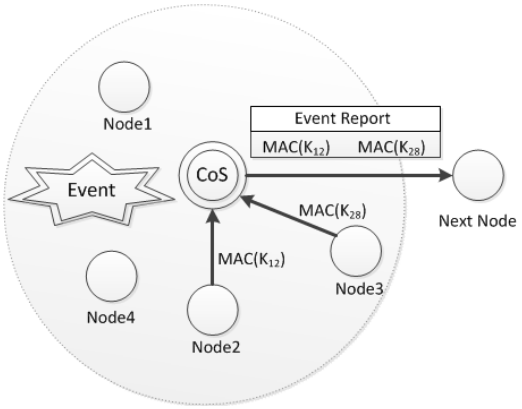


그림 3. 통계적 여과 기법의 보고서 생성 과정

의 파티션을 선택한다. 그리고 그 선택한 파티션이 가지고 있는 인증키들 중에서 임의로 몇 개의 인증 키들을 선택하여 각 노드에게 분배한다. 따라서 각 중간 노드는 이벤트 보고서를 검증하는데 사용되는 인증키들 중 하나를 소유할 확률을 갖는다. 다음 그림 3은 통계적 여과 기법에서 각 중간 노드들이 인증키를 이용하여 보고서를 생성하는 과정을 나타낸 것이다.

그림 3과 같이 키들을 배정 받은 센서 노드들은 특정 지역에 배치된다. 센서 노드가 배치된 지역에서 이벤트(Event)가 발생하면 같은 이벤트를 감지한 센서 노드들은 이벤트 감지 신호가 가장 강한 노드를 대표 노드(center-of-stimulus)로 선출한다. 그리고 자신이 가지고 있는 키들 중에서 하나를 선택하여 메시지 인증 코드(Message Authentication Code)를 생성한다. 대표 노드와 같은 이벤트를 감지한 노드들은 생성한 메시지 인증 코드를 대표 노드에게 전달한다. 대표 노드는 이벤트를 감지한 데이터와 이웃 노드에게서 받은 메시지를 포함하여 이벤트 보고서를 생성하고 다음 노드에게 전달한다.

2.2 중간 노드 여과

각 중간 노드가 이웃노드로부터 이벤트 보고서를 받으면 먼저 인증키 색인을 검사한다. 이벤트 보고서가 가지고 있는 인증키 색인의 수가 사용자가 지정한 이벤트 보고서의 인증키 색인의 수와 일치하지 않거나 한 파티션의 인증키 색인 수가 두 개 이상이면 그 이벤트 보고서를 폐기한다. 이벤트 보고서가 가지고 있는 인증키 색인의 수와 메시지 인증 코드의 수가 일치하고 각각의 인증키 색인이 모두 다른 파티션 소속이면 중간 노드는 자신이 가지고 있는 인증키 색인들과 이벤트 보고서의 키 색인들을 비교한다. 중간 노드가 이벤트 보고서의 인증키 색인들 중 하나라도 일치하는 키 색인을 가지고 있다면 그 인증키로 메시지 인증 코드를 생성하고 인증 키 색인이 일치하는 이벤트 보고서의 메시지 인증 코드와 비교한다. 중간 노드가 생성한 메시지 인증 코드와 이벤트 보고서의 메시지 인증 코드가 일치하면 정상 보고서로 판단하고 이벤트 보고서를 다음 노드로 전달한다. 그리고 일치하지 않으면 허위 보고서로 판단하고 그 이벤트 보고서를 폐기한다. 중간 노드의 인증키 색인들과 이벤트 보고서간에 일치하는 인증키 색인이 없다면 중간 노드는 이벤트 보고서를 다음 노드에게 전달한다.

2.3 기지 노드 검증

기지 노드는 모든 인증키를 가지고 있기 때문에 이벤트 보고서의 모든 메시지 인증 코드를 검증할 수 있다. 먼저 기지 노드는 이벤트 보고서를 받으면 이벤트 보고서의 키 색인들과 메시지 인증 코드들을 비교하고 일치하는 인증 키들을 이용하여 메시지 인증 코드를 재생성 한다. 기지 노드는 재생성한 메시지 인증 코드와 이벤트 보고서의 메시지 인증 코드들을 비교하여 일치하지 않는 메시지 인증 코드가 있으면 허위 보고서로 판단하고 그 이벤트 보고서를 폐기한다. 따라서 중간 노드 여과 단계에서 발견되지 않은 허위 보고서가 있더라도 기지 노드 검증을 통해 모든 허위 보고서를 검출할 수 있다.

3. 제안 기법

이 장에서는 제안 기법의 동기와 가정과 동작 과정을 설명한다.

3.1 동기

SEF는 모든 중간 노드가 허위 보고서와 정상 보고서를 같은 확률로 검증한다. 따라서 센서 네트워크에서 발생하는 이벤트 보고서들 중에서 정상 보고서의 비율이 매우 높은 경우, 센서 노드들이 많은 정상 보고서를 허위 보고서와 같은 확률로 검증함으로써 에너지를 낭비하게 된다. 센서 네트워크에서 정상 보고서 검증하는데 사용하는 에너지를 절약하기 위해 SEF를 개선한 검증 시도 확률을 조절하는 기법을 제안한다.

3.2 가정

본 논문에서는 다음과 같이 가정한다. 모든 센서 노드들은 고유의 식별자(Identification)를 가지며 기지 노드까

지의 홉 수 와 각 이웃 노드로부터 받은 최근 10개의보고서를 저장하고 자신의 잔여 에너지양을 확인할 수 있다. 또한 데이터 전송 범위 이내에 있는 모든 이웃 노드들에 대한 테이블 [이웃 노드 식별자, 보고서 검증 시도 확률]을 생성하고 관리한다.

3.3 동작 과정

센서 노드들은 특정 지역에 배치되기 전에 사용자에 의해 식별자와 인증 키들을 배정받는다. 사용자는 모든 노드들에게 고유의 식별자를 부여하며 보고서 검증 시도 확률을 도출하는데 고려되는 3가지 요소의 가중치를 정한다. 또한 인증키 배정 방식은 통계적 여과 기법과 같이 각 노드마다 사용자가 임의로 하나의 파티션을 선택하고 그 파티션에서 무작위로 몇 개의 인증 키들을 선택하여 할당한다. 키 분배가 끝난 후에 센서 노드들은 특정 지역에 배치된다. 배치된 각 노드들은 데이터 전송 범위 이내에 있는 모든 이웃 노드들을 검색하여 테이블을 생성한다. 이 테이블은 이웃노드의 식별자와 보고서 검증 시도 확률로 이루어져 있다. 이와 같이 각 이웃 노드에 따른 보고서 검증 시도 확률을 관리하는 이유는 어떤 이웃 노드로부터 이벤트 보고서를 수신 하는가에 따라 허위 보고서의 비율이 다를 수 있기 때문이다. 다음 그림 4는 각 노드가 저장하고 있는 이웃노드들의 초기 보고서 검증 확률들을 나타낸 것이다.

그림 4와 같이 모든 노드들의 초기 보고서 검증 시도 확률은 통계적 여과 기법과 같이 1로 동일하다. 노드의 배치와 이웃 노드들에 대한 테이블 생성이 끝난 후, 그 지역에서 이벤트가 발생하면 통계적 여과 기법과 같은 방식으로 이벤트 보고서를 생성한다. 이벤트가 발생했을 때 그 이벤트를 감지한 여러 노드들은 대표 노드를 선출한다. 그리고 자신이 보유한 인증키들 중에서 하나를 선택하고

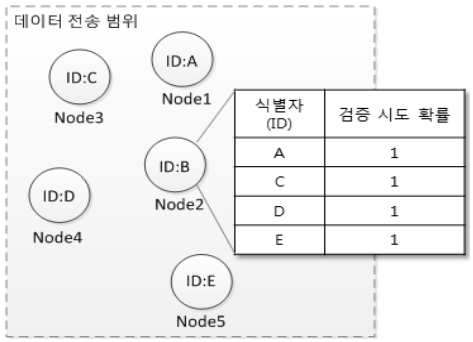


그림 4. 초기 보고서 검증 시도 확률

그 인증키를 사용하여 메시지 인증 코드를 생성한다. 생성한 메시지 인증 코드와 키 색인을 대표 노드에게 전달한다. 같은 이벤트를 감지한 이웃 노드들로부터 메시지 인증 코드를 받은 대표 노드는 이 메시지 인증 코드들을 포함한 이벤트 보고서를 생성하여 다음 노드에게 전달한다. 각 중간 노드가 이벤트 보고서를 받으면 먼저 이벤트 보고서가 가지고 있는 인증키 색인의 수를 확인한다. 다음 그림 5는 이벤트 보고서를 받은 노드가 메시지 인증 코드의 개수 확인을 나타낸 것이다.

그림 5와 같이 사용자가 지정한 각 이벤트 보고서의 메시지 인증 코드의 개수가 5개일 때 인증키 색인의 수가 이벤트 보고서의 메시지 인증 코드의 개수보다 더 많거나 또는 더 적으면 그 이벤트 보고서는 폐기된다. 따라서 이벤트 보고서의 인증키 색인의 수와 사용자가 지정한 메시지 인증 코드의 수가 일치해야 한다. 두 번째로 각 인증키 색인의 파티션이 겹치지 않는지 검사한다. 이벤트 보고서의 메시지 인증 코드들은 각각 중복되지 않는 파티션의 인증키 색인들로 이루어져야 한다. 이러한 파티션간의 중복 여부 확인을 그림 6에서 나타내었다.

그림 6과 같이 중복되는 파티션의 키 색인들이 있으면 중간 노드는 그 이벤트 보고서를 폐기한다. 그러나 이벤트 보고서의 인증키 색인의 수가 사용자가 지정한 이벤트 보고서의 메시지 인증 코드의 수와 같고 인증키 색인의 파티션이 모두 다르면 이웃 노드의 보고서 검증 시도 확률을 확인한다. 그림 7은 이벤트 보고서를 보낸 이웃 노드의 보고서 검증 시도 확률 확인을 나타낸 것이다.

그림 7과 같이 테이블에서 이벤트 보고서를 전달한 이

그림 5. 메시지 인증 코드 개수 확인

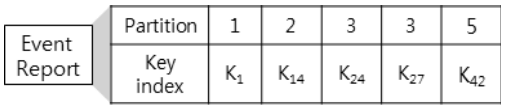


그림 6. 메시지 인증 코드들이 속한 파티션간의 중복 여부 확인

웃노드에 해당하는 보고서 검증 시도 확률을 확인하고 그 확률만큼 검증을 시도한다. 검증 방법은 통계적 여과 기법과 같이 메시지 인증 코드의 일치 여부를 검사한다. 그림 8과 9는 각각 이벤트 보고서가 정상 보고서 일 때와 허위 보고서일 때 보고서 검증 시도 확률 갱신을 나타낸 것이다.

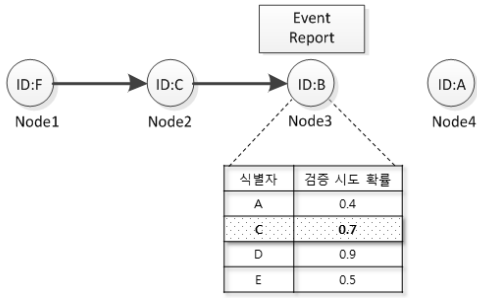


그림 7. 이벤트 보고서를 보낸 이웃 노드의 보고서 검증 시도 확률 확인

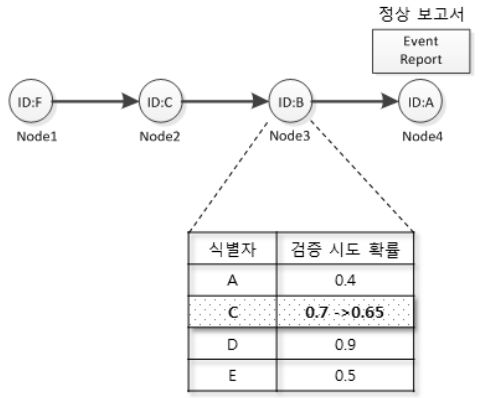


그림 8. 이벤트 보고서가 정상 보고서일 때 보고서 검증 시도 확률 갱신

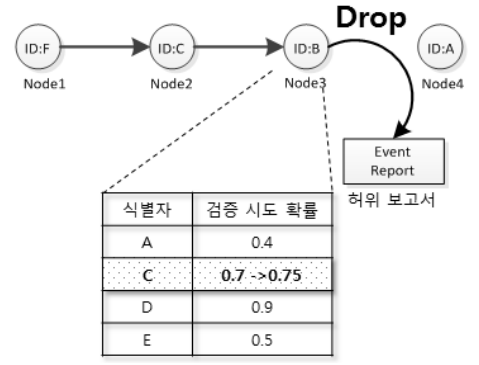
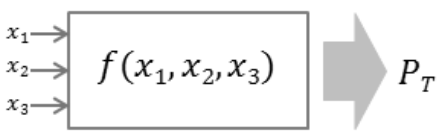


그림 9. 이벤트 보고서가 허위 보고서일 때 보고서 검증 시도 확률 갱신

검증한 결과가 그림 8과 같이 정상 보고서로 판단되면 테이블에서 이벤트 보고서를 전달한 이웃노드에 해당하는 보고서 검증 시도 확률을 낮추고 이벤트 보고서를 다음 노드로 전달한다. 하지만 그림 9와 같이 이벤트 보고서를 검증한 결과가 허위 보고서로 판단되면 테이블에서 이벤트 보고서를 전달한 이웃노드에 해당하는 보고서 검증 시도 확률을 높인다. 그리고 그 이벤트 보고서를 폐기한다. 따라서 어느 이웃노드들에 의해서 이벤트 보고서가 전달되었는가에 따라 보고서 검증 시도 확률이 다르게 적용된다. 위와 같은 이벤트 보고서를 검증하는데 사용되는 보고서 검증 시도 확률은 3가지 요소에 의해서 결정된다.

그림 10은 보고서 검증 시도 확률을 결정하는 요소 3가지를 나타낸 것이다.

그림 10과 같이 보고서 검증 시도 확률(P_T)은 한 노드의 잔여 에너지양(x_1), 현재 노드에서 기지 노드까지의 홉 수(x_2), 그리고 이벤트 보고서를 전달한 이웃노드로부터 받은 최근 10개의 보고서 중 허위 보고서의 비율(x_3)에 의해 결정된다. 한 노드의 잔여 에너지양(x_1),이 많아질수록 보고서 검증 시도 확률(P_T)이 높아지고 한 노드의 잔여 에너지양(x_1),이 적어질수록 보고서 검증 시도 확률(P_T)은 낮아진다. 또한 현재 노드에서 기지 노드까지의 홉 수(x_2)가 클수록 보고서 검증 시도 확률(P_T)은 높아지고 현재 노드에서 기지 노드까지의 홉 수(x_2)가 작을수록 보고서 검증 시도 확률(P_T)은 낮아진다. 그리고 이웃 노드로부터 받은 최근 보고서 10개 중에서 허위 보고서의 비율(x_3)이 높을수록 보고서 검증 시도 확률(P_T)은 높아지고 허위 보고서의 비율(x_3)이 낮을수록 보고서 검증 시도 확률(P_T)은 낮아진다. 위의 3가지 요소는 각각 비율로 환산된다. 식 (1)은 보고서 검증 시도 확률을 결정하는 3가지 요소가 비율로 환산을 나타낸다.



x_1 한 노드의 잔여 에너지 양

x_2 현재 노드에서 기지 노드까지의 홉 수

x_3 허위 보고서의 비율

그림 10. 보고서 검증 시도 확률 결정 요소

$$x_1 = \frac{\text{한 노드의 잔여 에너지양}}{\text{한 노드의 초기 에너지양}}$$

$$x_2 = \frac{\text{현재 노드에서 기지 노드까지의 홉수}}{\text{대표 노드에서 기지 노드까지의 홉수}}$$

$$x_3 = \frac{\text{허위 보고서의 개수}}{\text{최근 보고서 10개}} \quad (1)$$

식 (1)과 같이 중간 노드의 잔여 에너지양의 비율은 초기의 에너지양에 대한 현재의 잔여 에너지양으로 나타낸다. 현재 노드에서 기지 노드까지의 홉 수의 비율은 대표 노드에서 기지 노드까지의 홉 수에 대한 현재 노드에서 기지 노드까지 남아있는 홉 수로 나타낸다. 그리고 이벤트 보고서를 전달한 이웃노드로부터 받은 최근 10개의 보고서 중 허위 보고서의 비율은 이미 비율로 계산되었기 때문에 그 자체로 표현된다. 식 (1)에서 비율로 환산된 세 가지 요소에 식 (2)와 같이 사용자가 지정한 가중치가 부여되며 가중치가 부여된 세 가지 요소의 비율을 모두 합하여 보고서 검증 시도 확률을 도출한다.

$$P_T = \alpha x_1 + \beta x_2 + \gamma x_3 \quad (2)$$

α : 한 노드의 잔여 에너지양(x_1)에 대한 가중치
β : 현재 노드에서 기지 노드까지의 홉수(x_2)에 대한 가중치
λ : 허위보고서의 개수(x_3)에 대한 가중치

식 (2)에 의해 도출된 보고서 검증 시도 확률을 통해 각 노드의 허위 보고서 검출 확률을 구할 수 있다. 식 (3)은 각 중간 노드의 허위 보고서 검출 확률(P_D)을 도출한다.

$$P_D = P_1 \times P_T \quad (3)$$

P_D : 허위 보고서 검출 확률
P_1 : 한 노드가 허위 보고서를 검출할 수 있는 훼손되지 않은 키를 가지고 있을 확률

식 (3)에서 허위 보고서 검출 확률(P_D)은 보고서 검증 시도 확률(P_T)에 한 노드가 허위 보고서를 검출할 수 있는 훼손되지 않은 키를 가지고 있을 확률(P_1)[2]을 곱하여 도출되며 그 확률(P_1)은 식 (4)에 의해 결정된다.

$$P_1 = \frac{k(T - N_c)}{N} \quad (4)$$

T : 이벤트 보고서의 메시지 인증 코드 개수
N_c : 공격자의 메시지 인증 코드 개수
k : 한 노드가 가지고 있는 키의 개수
N : 전역 키 풀의 키 전체 개수

위의 수식들을 이용하여 통계적 여과 기법과 제안 기법의 허위 보고서 검출 확률(P_D)을 비교할 수 있다. 식 (5)는 통계적 여과 기법의 허위 보고서 검출 확률을 나타내고 식 (6)은 제안 기법의 허위 보고서 검출 확률을 나타낸 것이다.

· 통계적 여과 기법

$$P_{DS} = P_1 \times P_T (P_T = 1) \quad (5)$$

· 제안 기법

$$P_{DT} = P_1 \times P_T (0 \leq P_T \leq 1) \quad (6)$$

통계적 여과 기법과 제안 기법 모두 허위 보고서를 검출할 수 있는 훼손되지 않은 키를 가지고 있을 확률(P_1)이 같을 때, 통계적 여과 기법에서 보고서 검증 시도 확률(P_T)은 식 (5)와 같이 항상 1이다. 모든 중간 노드가 1만큼 보고서 검증을 시도하기 때문이다. 그러나 제안 기법에서의 보고서 검증 시도 확률(P_T)은 위에서 언급한 3가지 결정 요소에 따라 조절되기 때문에 식 (6)과 같이 0에서 1 사이의 값을 갖는다. 따라서 통계적 여과 기법에서 보고서 검증을 시도하는데 소모되는 에너지보다 제안 기법에서 보고서 검증을 시도하는데 소모되는 에너지가 적을 것이라는 것을 예측할 수 있다. 이러한 제안 기법의 에너지 효율성을 시뮬레이션을 통하여 결과를 확인하였다.

4. 시뮬레이션 및 결과

이 시뮬레이션은 통계적 여과 기법과 제안 기법을 비교하여 제안 기법의 보안성 및 에너지 효율성을 보이기 위하여 수행하였다. 시뮬레이션의 환경 변수는 다음과 같다. 너비 50 m, 높이 200 m의 지역에 600개의 센서 노드들이 배치된다. 전역 키 풀은 10개의 파티션으로 나누어져 있으며 각 파티션마다 10개의 인증 키들을 갖는다. 따라서 전역 키 풀은 총 100개의 인증키를 가지고 있다. 또한 한 노드의 초기 에너지양은 0.3 J이다. 다음 표 1은 제

안 기법을 수행할 때 각 센서 노드가 소모하는 에너지양[2]을 나타낸 것이다.

또한 이벤트 보고서의 크기는 20 $byte$이며 메시지 인증 코드 하나의 크기는 8 $byte$이다. 노드의 초기 보고서 검증 시도 확률(P_T)은 1이며 각 중간 노드가 허위 보고서를 검출할 수 있는 훼손되지 않은 인증키를 가지고 있을 확률(P_1)은 0.4이다. 보고서 검증 시도 확률을 얻기 위한 3가지 요소에 대한 가중치는 다음 표 2와 같다.

본 시뮬레이션에서는 가중치를 고르게 분포하기 위해 표 2와 같이 설정하였으나 사용자가 특정 지역의 특성에 맞게 조절할 수 있다. 본 논문의 제안 기법은 센서 네트워크에서 정상 보고서의 비율이 매우 높을 때, 정상 보고서를 검증하는 에너지를 절약하는 것을 목표로 한다. 따라서 허위 보고서의 발생 비율을 매우 낮게 설정해야 한다. 또한 검증 시도 확률 조절에 따른 SEF와 제안 기법의 보안성을 보여줄 수 있도록 허위 보고서 비율을 설정해야 한다. 센서 네트워크에서 발생하는 이벤트 보고서 중에서 위의 조건을 모두 고려했을 때 허위 보고서 비율이 10%일 때가 가장 적당하다고 판단하였으며 비교하기 위한 대조군으로 이보다 상대적으로 정상 보고서의 비율이 낮은 허위 보고서 비율 30% 일 때로 나누어 시뮬레이션 하였다. 그림 11은 이벤트 보고서 전체 개수 중 허위 보고서의 발생 비율이 10% 일 때 보안성을 비교하기 위해 통계적 여과 기법과 제안 기법에서 이벤트 보고서의 개수에 따른 허위 보고서의 개수를 나타낸 것이다.

허위 보고서의 개수는 중간 노드 여과 단계에서 검출되지 않고 기지 노드까지 도착한 허위 보고서의 개수를 의미한다. 실제 시뮬레이션 결과 통계적 여과 기법과 제안 기법의 검출되지 않은 허위 보고서의 차이 평균은 2.04개였다. 그림 12는 센서 네트워크에서 발생한 이벤트 보고서의 전체 개수 중에서 허위 보고서의 비율이 10%일 때 에너지의 효율성을 비교하기 위해 통계적 여과 기법과 제안 기법에서 이벤트 보고서의 개수에 따른 에너지 소모량을 나타낸 것이다.

그림 12와 같이 전반적으로 통계적 여과 기법보다 제안 기법의 에너지 소모량이 더 적은 것을 알 수 있으며 시뮬레이션 결과, 제안 기법이 SEF 보다 평균 5.9%의 에너지를 더 적게 소모하는 것으로 나타났다.

그림 13과 14는 센서 네트워크에서 발생한 이벤트 보고서의 전체 개수 중에서 허위 보고서의 비율이 30%일 때 통계적 여과 기법과 제안 기법에서 이벤트 보고서의 개수에 따른 허위 보고서의 개수를 나타낸 것이다.

그림 13 그래프에서 중간 노드 여과 단계에서 검출되지 않고 기지 노드까지 도착한 허위 보고서 개수의 평균은 2.12개였다. 허위 보고서의 비율이 10%일 때와 허위 보고서 개수가 거의 차이가 없음을 알 수 있다.

그림 14는 발생한 이벤트 보고서 전체 개수 중 허위 보

표 1. 센서 노드가 소모하는 에너지양

수행 작업	소모 에너지양
이벤트 보고서 송신	16.25 $\mu J/byte$
이벤트 보고서 수신	12.25 $\mu J/byte$
이벤트 보고서 검증	75 μJ

표 2. 검증 시도 확률 결정 요소들에 대한 가중치

검증 시도 확률 요소	가중치
한 노드의 잔여 에너지양(x_1)	0.3 (α)
현재 노드에서 기지 노드까지의 홉 수(x_2)	0.3 (β)
이웃노드로부터 받은 최근 보고서 10개 중 허위 보고서의 개수(x_3)	0.4 (λ)

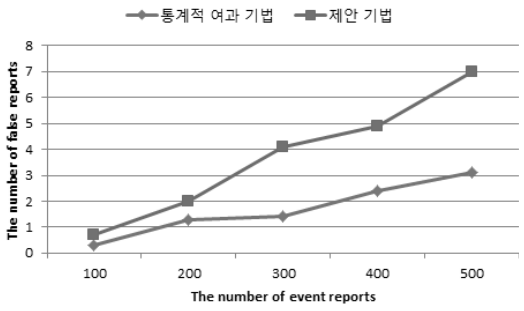


그림 11. 허위 보고서 발생 비율이 10%일 때 통계적 여과 기법과 제안 기법의 검출되지 않은 허위 보고서의 개수

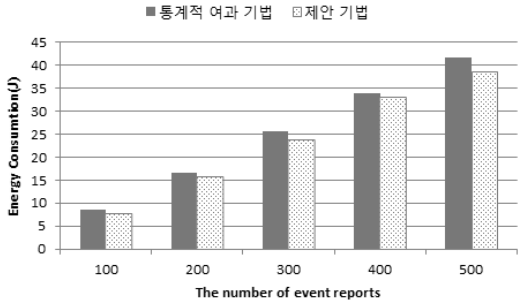


그림 12. 허위 보고서 발생 비율이 10%일 때 통계적 여과 기법과 제안 기법의 에너지 소모량 비교

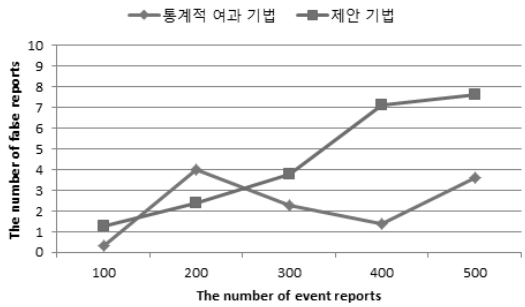


그림 13. 허위 보고서 발생 비율이 30%일 때, 통계적 여과 기법과 제안 기법의 검출되지 않은 허위 보고서의 개수

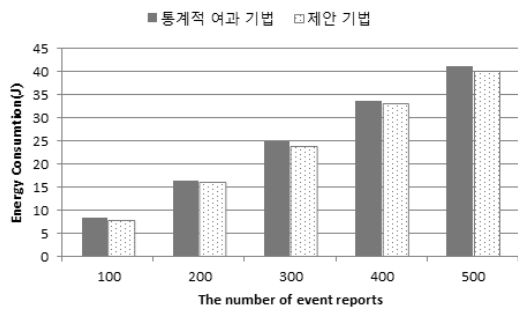


그림 14. 허위 보고서 발생 비율이 30%일 때 통계적 여과 기법과 제안 기법의 에너지 소모량 비교

고서의 비율이 30% 일 때 통계적 여과 기법과 제안 기법의 이벤트 보고서 개수에 따른 에너지 소모량을 비교한 것이다.

그림 14와 같이 통계적 여과 기법보다 제안 기법이 에너지 소모량이 더 적은 것을 알 수 있다. 실제로 시뮬레이션 결과, 제안 기법이 SEF보다 4.7%의 에너지를 적게 소모하는 것으로 나타났다. 또한 허위 보고서 비율이 10%일 때보다 통계적 여과 기법과의 에너지 소모량의 차이가 적다. 그 이유는 센서 네트워크 지역에서 발생한 허위 보고서의 비율이 증가하면서 보고서 검증 시도 확률이 증가했기 때문이다. 따라서 보고서 검증에 필요한 에너지가 증가하기 때문에 허위 보고서 비율이 10%일 때보다 통계적 여과 기법과의 에너지 소모량 차이가 적다.

5. 결 론

무선 센서 네트워크는 군사, 환경 등의 개방된 환경에서 동작하기 때문에 외부의 물리적인 공격에 매우 취약하다. 특히 허위 보고서 주입 공격은 공격자가 센서 노드를 포획하여 발생하지 않은 이벤트에 대한 보고서를 생성하여 다른 노드들에게 전달한다. 이러한 공격은 센서 노드들의 에너지를 고갈시켜 센서 네트워크의 수명을 단축시킨다.

허위 보고서 주입 공격에 대한 보안 기법 중 Ye(2005) 등 이 제안한 통계적 여과 기법은 보고서를 전달하는 중간 노드들이 일정한 확률로 보고서를 검증하여 허위 보고서를 검출하고 폐기시킨다. 통계적 여과 기법은 허위 보고서를 조기에 검출하여 센서 노드들의 에너지 고갈을 예방할 수 있다. 그러나 모든 노드가 정상 보고서와 허위 보고서를 같은 확률로 검증하기 때문에 허위 보고서의 발생 비율이 매우 낮은 경우에는 정상 보고서를 검증하는데 불필요한 에너지가 소모된다. 본 논문은 불필요한 에너지 소모를 줄이기 위해 본 논문에서는 센서 네트워크의 중간 노드들의 보고서 검증 시도 확률을 조절하는 기법을 제안하였다. 보고서 검증 시도 확률은 한 노드의 잔여 에너지 양, 현재 노드에서 기지 노드까지의 홉 수, 그리고 허위 보고서의 비율에 의해 결정된다. 통계적 여과 기법과 제안 기법의 에너지 효율을 비교하기 위해 시뮬레이션을 통해 발생한 이벤트 보고서 중 허위 보고서의 비율을 달리하여 이벤트 보고서의 개수에 따른 전체 노드의 에너지 소모량을 비교하였고 보안성을 비교하기 위해 이벤트 보고서 개수에 따른 검출되지 않은 허위 보고서의 개수를 비교하였다. 시뮬레이션 결과, 제안 기법은 통계적 여과 기법과 비슷한 보안성을 가지면서 더 적은 에너지를 소모하는 것을 알 수 있었다. 또한 센서 네트워크 지역에서 허위 보고서의 발생 비율이 낮을수록 통계적 여과 기법과 제안 기법의 에너지 소모량 차이가 많은 것을 알 수 있었다.

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. Ye, F., Luo, H. and Lu, S. Zhang, L. (2005), “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.
3. Al-Karaki, J.N., Kamal, A.E. (2004), “Routing Techniques in wireless sensor networks: a survey”, IEEE Wireless Communication Magazine, Vol. 11, No. 6, pp. 6-28.
4. Moon, S. Y., Cho, T. H. (2008), “Report Verification Probability Control Method for Energy Efficiency in Sensor Networks”, Thesis, University of sunkyunkwan,

pp. 2-3.
5. Karlof, Chris., Wagner, David. (2003), “Secure routing in wireless sensor networks: attacks and countermeasures”, Ad Hoc Networks Vol. 1, No. 2-3, pp. 293-315.
6. Zhen, Y, Yong, G. (2005), “A dynamic en-route scheme for filtering false data injection in wireless sensor networks”, Proceedings of the 3rd international conference on Embedded networked sensor systems, November San Diego, California, USA.
7. Hao, Y., Chris., Songwu, L. (2004), “Commutative cipher based en-route filtering in wireless sensor networks”, VTC2004-Fall. 2004 IEEE 60th , Vol. 2, No., pp. 1223-1227 Vol. 2, 26-29 Sept.
8. Sencun, Z., Seti, S., Jajodia, S. (2004), Peng, Ning., “An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks”, Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, pp. 259- 271, 9-12 May.

이 현 우 (hwoolee@ece.skku.ac.kr)

2009 경원대학교 인터넷미디어학과 학사
2011～현재 성균관대학교 정보통신공학부 석사 과정

관심분야 : 모델링 및 시뮬레이션, 무선 센서 네트워크, 인공지능

문 수 영 (moonmous@ece.skku.ac.kr)

2007 성균관대학교 정보통신공학부 학사
2009 성균관대학교 정보통신공학부 석사
2009～현재 성균관대학교 정보통신공학부 박사 과정

관심분야 : 무선 센서 네트워크, 모델링 및 시뮬레이션, 인공 지능

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