한국시뮬레이션학회 논문지
Vol. 19, No. 1, pp. 125-131 (2010. 3)

동적 여과 기법 기반 센서 네트워크의 에너지 효율을 높이기 위한 키 재분배 결정 방법

선청일[1] · 조대호[1†]

A Key Redistribution Method for Enhancing Energy Efficiency in Dynamic Filtering based Sensor Networks

Chung Il Sun · Tae Ho Cho

ABSTRACT

In wireless sensor networks application, sensor nodes are randomly deployed in wide and opened environment typically. Since sensor networks have these features, it is vulnerable to physical attacks in which an adversary can capture deployed nodes and use them to inject a fabricated report into the network. This threats of network security deplete the limited energy resource of the entire network using injected fabricated reports. A dynamic en-route filtering scheme is proposed to detect and drop the injected fabricated report. In this scheme, node executes the key redistribution to increases the detection power. It is very important to decide the authentication key redistribution because a frequent key redistribution can cause the much energy consumption of nodes. In this paper, we propose a key redistribution determining method to enhance the energy efficiency and maintain the detection power of network. Each node decides the authentication key redistribution using a fuzzy system in a definite period. The proposed method can provide early detection of fabricated reports, which results in energy-efficiency against the massive fabricated report injection attacks.

Key words : Sensor Network, Fabricated report, Dynamic filtering scheme, Security, Authenticated key distribution

요 약

무선 센서 네트워크 응용 분야에서, 센서 노드는 광범위하고 열린 공간에 무작위로 배치된다. 센서 네트워크의 이러한 특징 때문에, 센서 네트워크는 공격자에 의한 노드의 포획과 획득한 노드를 사용하여 네트워크의 허위 보고서를 삽입하는 등, 물리적 공격에 취약하다. 이러한 네트워크 보안 위협은 삽입된 허위 보고서를 이용하여 전체 네트워크의 한정된 에너지를 고갈시킨다. 동적 여과 기법은 네트워크에 삽입된 허위 보고서를 탐지하고 제거하기 위해서 제안되었다. 이 기법에서, 센서 노드는 탐지 성능을 향상시키기 위하여 배치 후 인증키를 재분배한다. 빈번한 인증키 재분배는 노드의 한정된 에너지의 소모를 유발할 수 있으므로 인증키 재분배의 결정은 매우 중요하다. 본 논문에서는 네트워크의 탐지 성능을 유지하고 에너지 효율을 높이기 위한 인증키 재분배 결정 방법을 제안한다. 각 노드는 일정한 주기에 맞추어 퍼지 시스템을 사용하여 인증키 재분배 여부를 결정한다. 제안 기법은 허위 보고서의 이른 탐지를 보장하고, 그 결과로 허위 보고서 삽입 공격에 대한 에너지 효율성을 보인다.

주요어 : 센서 네트워크, 허위 보고서, 동적 여과 기법, 보안, 인증키 분배

1. 서 론

무선 통신 및 전자 미세 기술의 진보는 무선 센서 네트워크의 저 전력, 저 비용, 그리고 고 성능의 센서 노드의 개발을 가능하게 했다[1]. 무선 센서 네트워크는 실세계를 감시할 수 있는 특징을 가지며 군사 지역, 산림 관리 그리고 물류 관리 등과 같은 환경에서 작동이 가능하다[2]. 센

* 이 논문 또는 저서는 2009년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2009-0076504).
2009년 11월 30일 접수, 2010년 3월 11일 채택
[1] 성균관대학교 정보통신공학부
주 저 자 : 선청일
교신저자 : 조대호
E-mail; taecho@ece.skku.ac.kr

서 네트워크는 주변 환경을 감지하고 감지한 데이터를 전송하는 다 수의 센서 노드와 전송된 감지 데이터를 수집하는 소수의 기지 노드로 구성된다. 센서 노드는 컴퓨팅 능력, 최소한의 저장 공간, 일회적 배터리, 폭 좁은 대역폭 그리고 제한적인 메모리를 가진다[3]. 기본적인 센서 네트워크 응용에서, 센서 노드는 노드간의 무선 통신 범위내의 노드들과 직접적인 무선 통신이 가능하며, 범위 밖의 노드와의 통신은 메시지 전달에 의존한다[4]. 센서 노드는 무인의 환경에 무작위로 배포되며, 시간이 지남에 따라 파괴, 훼손 혹은 배터리의 수명이 다함으로써 노드는 불능이 된다. 센서 네트워크는 환경적 제약으로 인해 물리적 취약점을 가진다. 따라서 악의적 목적을 가진 공격자는 일부의 센서 노드를 포획하여 센서 노드가 지닌 정보를 획득할 수 있고 허위 데이터를 삽입하여 전달 노드를 통해 기지 노드로 전달되면서 전달 노드의 에너지를 불필요하게 소모시켜 네트워크 전체의 한정된 에너지 자원을 고갈시킨다. 허위 보고서에 의한 피해를 줄이기 위해서는 전달 도중에 발견하여 여과시켜야하며, 제거하지 못한 허위 보고서는 기지 노드에 의해 제거되어야 한다.

허위 보고서를 탐지하여 여과하기 위한 다양한 여과기법[5-8]이 제안되었다. Yu와 Guan이 제안한 동적여과기법(dynamic en-route filtering scheme; 이하 DEF)[7]은 허위 보고서 삽입 공격에 대응할 수 있는 방법이다. DEF에서 이벤트 보고서 메시지 인증 코드(message authentication code; 이하 MAC)를 첨부하여 이벤트 보고서의 허위 유무를 판별하는데 사용된다. 이벤트 보고서는 전달 노드에 의해 기지 노드로 전달되며, 전달 노드는 이벤트 보고서 내의 MAC과 비교하여 보고서의 허위 유무를 판단한다. 만약 이벤트 보고서가 허위로 판단된 경우, 전달 노드는 허위 이벤트 보고서를 즉시 여과시켜 폐기한다. DEF에서는 허위 보고서 탐지 효율 및 보안성을 위해 인증키 재분배 방식을 사용한다. 제안된 기법에서는 센서 네트워크 상황을 고려하지 않고 이벤트 보고서 발생 횟수에 따라 인증키를 재분배한다. 이러한 재분배 방식은 보안 강도가 높은 네트워크 상황에서 불필요한 재분배로 인한 노드의 많은 에너지 소모를 유발한다. 따라서 인증키 재분배에 따른 불필요한 에너지 소모를 줄이기 위해서는 네트워크 상황을 고려하여 재분배시기를 판단하고 결정하는 방법이 필요하다.

본 논문에서는 효율적인 검증 성능을 유지하면서 센서 노드의 에너지 절약을 위한 인증키 재분배 결정 방법을 제안한다. 제안 기법에서는 센서 네트워크 상황을 고려하여 인증키 재분배 여부를 결정한다. 제안 기법에서 센서 네트워크의 상황을 판단하고 재분배를 결정하기 위하여 클러스터 헤드(cluster head; 이하 CH)는 일정한 주기에 퍼지 시스템을 사용하여 재분배 여부를 결정한다. 퍼지 시스템은 네트워크 상황에 따라 검증 성능을 높이기 위해 인증키의 재분배 여부를 결정한다.

본 논문의 2장에서는 DEF에 대해 설명하고 3장에서는 제안한 기법에 대하여 논한다. 그리고 4장에서는 시뮬레이션 결과를 보이고, 마지막으로 5장에서는 결론 및 향후 과제에 대하여 서술한다.

2. 동적 여과 기법

Yu와 Guan은 센서 네트워크에서 발생하는 허위 보고서 삽입 공격에 대응하기 위하여 동적여과기법(dynamic en-route filtering scheme)을 제안하였다. DEF는 훼손 노드를 통해 네트워크 내로 삽입되는 허위 보고서를 빠르게 탐지하고 제거하기 위한 방법을 제공한다. DEF는 기본적으로 클러스터 기반의 센서 네트워크에서 사용된다. 클러스터 기반의 센서 네트워크는 중복된 데이터 전달을 막아 불필요한 에너지 소모를 방지할 수 있다[9,10]. DEF는 다음 세 가지 단계로 구성된다.

배포 전 단계(pre-deployment phase)는 초기 배포 전 실행된다. 이 단계에서 센서 노드는 시드 키(seed authentication key)와 전체 키 풀(global key pool)에서 임의적으로 선택된 1 개의 z-key, l+1 개의 y-key를 미리 적재한다(그림 1). 센서 노드는 시드 키(seed key)를 이용하여 이벤트 보고서를 생성하고 검증한다. y-key와 z-key는 다른 센서 노드에게 인증키를 재분배할 때 사용된다. 센서 필드 내에 이벤트가 발생하면, 이벤트를 감지한 센서 노드들은 CH에게 이벤트 감지 정보에 노드가 소유한 인증키로 생성한 MAC을 덧붙여 전달한다.

여과 단계(filtering phase)에서, 전달 노드들은 이벤트

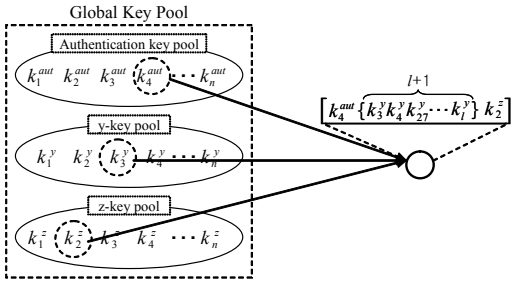

그림 1. 배포 전 단계

보고서의 허위 유무를 판단하기 위하여 보고서를 검증한다. 자신의 소유한 인증키로 만든 동일한 MAC이 이벤트 보고서 내에 존재할 경우, 자신의 인증키를 이용하여 MAC을 검증하고 허위로 판단될 경우, 보고서를 제거한다. 만약, 동일한 인증키를 가지고 있지 않다면 기지 노드를 향하여 전달 경로 상의 노드에게 전달한다. 그림 2는 DEF의 여과 단계를 보여준다. 훼손 노드에서 발생한 허위 보고서는 훼손 노드의 인증키 외에 부정한 MAC들을 생성하여 보고서를 생성한다. 그림에서 보듯이 N_1은 공격자에 의해 훼손되었으며 부정한 6과 37의 인증키를 생성한다. 전달과정에서 올바른 37번 인증키를 가진 노드에 의해 부정한 키가 적발되며, 해당 보고서는 즉시 폐기된다.

배포 후 단계(post-deployment phase)는 초기 실행 후, 센서 네트워크의 환경 혹은 토폴로지가 변화할 경우 실행된다. 이 단계는 각 클러스터에 따라 독립적으로 실행된

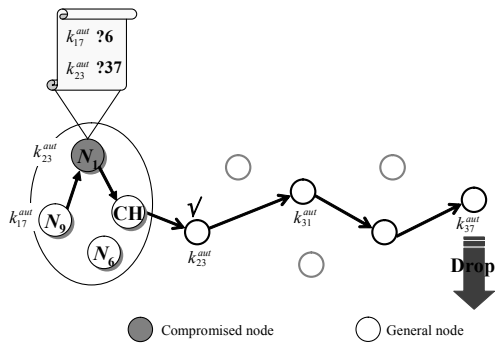

그림 2. 여과 단계

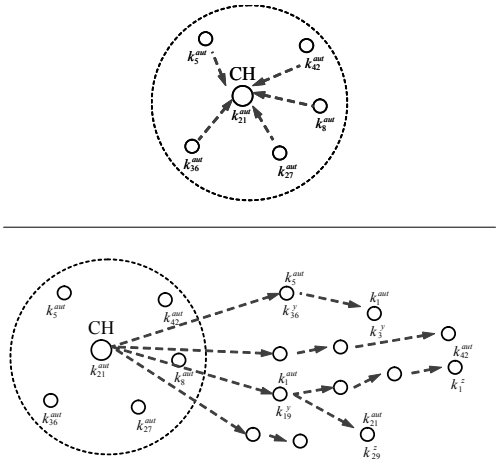

그림 3. 배포 후 단계

다. 모든 클러스터 노드들은 자신이 소유한 인증키를 l+1개의 비밀 키들을 이용하여 암호화를 수행하며 암호화된 인증키를 CH에 전달한다. 클러스터 노드들로부터 암호화된 인증키를 받은 CH는 전달 경로 상의 전달 노드에게 수신한 인증키를 분배한다. 전달 노드는 자신이 소유한 비밀 키와 비교하여, 동일한 비밀 키로 인증키가 암호화되었을 경우 자신의 비밀 키를 이용하여 복호화 한다(그림 3).

3. 인증키 재분배 결정 방법

3.1 동기

DEF에서, 인증키 재분배 시기 및 결정은 센서 네트워크의 검증 성능을 높이기 위해 매우 중요하다. 이 단계는 센서 노드의 많은 에너지 소모를 유발하므로 신중하게 고려되어야 한다. 센서 노드의 한정된 에너지 자원은 재충전이 어렵고 모두 소진 시, 해당 노드는 사용할 수 없어 센서 노드의 에너지 보존은 매우 중요한 과제이다. 본 논문에서는 인증키 재분배 결정 방법에 대해 제안하며, 재분배 결정 시 센서 네트워크의 상황 및 노드의 상태를 고려하여 재분배 여부를 결정한다. 이러한 결정은 센서 네트워크의 검증 성능을 유지하며 노드 및 네트워크의 에너지 소모를 줄일 수 있다.

3.2 가정

센서 네트워크는 다수의 센서 노드와 한 개의 기지 노드로 구성된다. 각 센서 노드는 센서 필드에 무작위로 배치된 후 자동적으로 클러스터를 구성하는 메커니즘을 가진다. 또한, 모든 센서 노드는 고유한 식별 번호를 가지며, 기지 노드로부터 전송되는 브로드캐스트 메시지를 검증할 수 있다. 기지 노드 및 CH는 공격자에 의해 훼손될 수 없으며, 기지 노드는 전체 키 풀을 소유하여 모든 허위 보고서에 대하여 검증이 가능하다. CH는 일정한 시간에 따라 해당 클러스터 내의 노드들 중 에너지 수준이 가장 높은 노드로 변경될 수 있다. 또한, 기지 노드는 모든 노드의 키 할당 상태를 알 수 있고 전체 네트워크의 에너지 수준도 알 수 있다.

3.3 개요

인증키 재분배 결정을 위해서 본 제안 기법에서는 퍼지 규칙을 사용한다. 배포 후 단계에서, 각 클러스터는 사용자에 의해 미리 결정된 주기에 따라 인증키 재분배를 결정한다. 미리 정해진 주기에 CH는 퍼지 규칙을 사용하

여 인증키를 재분배할지 혹은 재분배하지 않고 다음 주기에 재분배할지를 결정한다. 퍼지 규칙 시스템은 해당 클러스터에서 발생한 허위 보고서 발생량, 클러스터 지역 내의 평균 에너지량, 그리고 기지 노드와 클러스터 지역과의 거리를 입력 요소로 하여 재분배 여부를 결정한다.

3.4 퍼지 시스템의 입력 요소

퍼지 시스템을 구성하는 입력요소는 다음과 같다.

• 허위 보고서 발생량(False Traffic Ratio; 이하 FTR)

재분배 결정을 위해 퍼지 시스템을 적용하는 해당 클러스터 지역에서 만약 허위 보고서 발생량이 많다면, 그 지역의 일부 노드들은 이미 공격자에 의해 훼손되어 일부의 인증키가 노출되었다고 할 수 있다. 따라서 검증 성능을 위해서는 인증키를 재분배하여 검증 성능을 높여야 한다. 반대로 해당 지역에 허위 보고서 발생량이 적거나 혹은 없으면 해당 클러스터 지역은 상대적으로 인증키가 안전하므로 인증키의 재분배가 빈번하게 발생할 필요가 없다.

• 평균 잔여 에너지양(Average Remaining Energy; 이하 ARE)

인증키를 재분배 시 많은 에너지 자원이 소비되므로 신중하게 결정되어야 한다. 만약 재분배를 시행하는 CH의 에너지 자원이 적거나 혹은 클러스터 지역 내의 노드들의 평균 잔여 에너지량이 적을 경우, 인증키 재분배로 인해 에너지 고갈로 인한 노드의 사용이 불가할 수 있다. 따라서 해당 클러스터 지역의 평균 에너지량을 고려하여 재분배 여부를 결정하여 에너지 자원을 절약 및 검증 성능을 유지할 수 있다.

• 거리(Hops; 이하 H)

CH와 기지 노드와의 거리 또한 인증키 재분배 결정에 영향을 미친다. 만약 기지 노드와 재분배 결정이 필요한 클러스터 지역의 거리가 가깝다면, 빈번한 인증키의 재분배의 발생은 노드의 불필요한 에너지 소모를 유발한다. 근접한 거리에서 발생한 허위 보고서는 전달 도중 여과될 확률보다 기지 노드에서 탐지되어 여과될 확률이 높다. 따라서 먼 거리에 위치한 클러스터 지역에서의 인증키 재분배가 근접 거리에 위치한 클러스터 지역보다 빈번한 인증키 재분배가 필요하다.

3.5 퍼지 규칙 시스템

퍼지 시스템의 변수들의 맴버쉽 함수(membership function)는 그림 4와 같다. 다음은 퍼지 입력 변수들의 범위 및 구성을 보여준다.

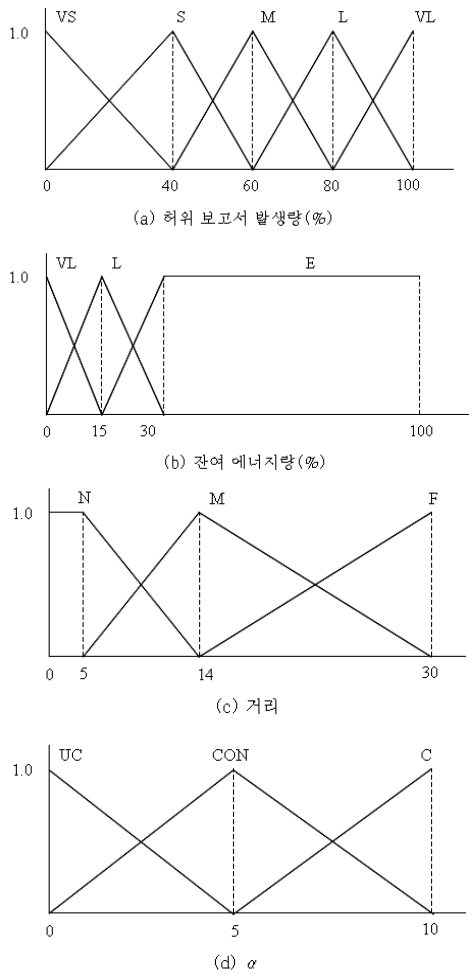

그림 4. 퍼지 맴버쉽 함수

• 허위 보고서 발생량 = {VS(Very Small), S(Small), M(Medium), L(Large), VL(Very Large)}
• 평균 잔여 에너지량 = {VL(Very Low), L(Low), E(Enough)}
• 거리 = {N(Near), M(Middle), F(Far)}

표 1은 퍼지 규칙 기반 시스템의 몇 가지 규칙들이다. 규칙 12에서, 허위 보고서 발생량은 작고(small) 해당 클러스터 지역의 평균 잔여 에너지량은 충분하다(enough). 하지만 해당 클러스터 지역의 CH는 기지 노드와 근접한 곳에 위치한다. 이것은 보고서 전달 시, 전달 경로 상에 검증을 위한 노드의 수가 적다는 것을 의미하며 해당 클러스터 지역에서 발생한 허위 보고서는 기지 노드에서 여

표 1. 퍼지 규칙들

규칙 번호	IF			TEHN
	FTR	ARE	H	α
1	VS	VL	N	UC
12	S	E	N	UC
19	M	L	M	CON
32	L	L	F	C
43	VL	E	M	C

과될 확률이 더 높다. 그러므로 평균 잔여 에너지량이 많더라도 키 분배로 인한 에너지 소비 절감을 위해 키 재분배를 시행하지 않는다.

퍼지 시스템의 출력 요소는 α = {UC(Unchanged), CON(Consider), C(Change)}이고, 그림 4(d)처럼 맴버쉽 함수가 구성된다. 퍼지 규칙은 인증키 재분배 결정 값 α은 기본적으로 잔여 에너지량과 허위 보고서 발생량을 기반으로 결정된다. 에너지량이 적더라도 허위 보고서 발생량이 많다면 재분배를 결정한다. 또한, 허위 보고서 발생량이 매우 적더라도 에너지량이 많다면 네트워크 보안 유지를 위해 재분배를 결정한다. 재분배 결정 값 α에 따라 사용자가 미리 정해놓은 주기 P가 되면 CH는 인증키 재분배를 결정한다.

인증키 재분배는 사용자가 미리 설정해 놓은 주기 P에 의해 퍼지 시스템을 적용하여 결정한다. 예를 들어, 특정 클러스터 지역의 CH_k에서 초기 주기 P_i에서 재분배 결정을 시도한다. 재분배 결정은 다음과 같이 진행된다.

- α = UC

인증키 재분배가 필요하지 않으므로 재분배를 실시하지 않는다. 다음 주기 P_i+1에서 다시 인증키 재분배 결정을 위한 퍼지 시스템을 이용한다.

- α = CON

재분배를 다음 주기 P_i+1전인 $P_i + P/2$에 재분배 결정 여부를 위한 퍼지 시스템을 다시 실시한다. 만약, 재분배가 결정된다면 재분배를 실시하고 다시 α = CON일 경우 위와 식을 이용하여 P_i+1에 인증키 재분배 여부를 결정한다.

- α = C

인증키 재분배가 필요한 시점이므로 인증키 재분배를 즉시 실시한다. UC와 마찬가지로 다음 주기 P_i+1에서 다시 인증키 재분배 결정을 위한 퍼지 시스템을 이용한다.

예를 들어, 사용자가 각각의 CH마다 재분배 결정 주기 P값을 10으로 결정하면, CH는 이벤트 보고서 초기 10회 전송 후 퍼지 시스템을 이용하여 재분배를 결정한다. CH는 기지 노드로부터 해당 클러스터 지역의 허위 보고서 발생량 및 거리에 대한 보고서를 수신하고 주위 노드의 잔여 에너지량을 계산하여 퍼지 시스템을 적용한다. 만약 α이 UC라면 다음 재분배 주기인 P_i+1회에 다시 결정하게 되며, CON이라면 $P_i + P/2$회인 이벤트 보고서 15회 발생 후 인증키 재분배를 결정한다. 마지막으로 α값이 C라면, 즉시 재분배를 실시한다.

4. 시뮬레이션 결과

제안 기법의 효율성을 보여 주기 위해서, 본 논문에서는 기존의 DEF와 제안 기법이 적용된 DEF를 시뮬레이션을 통하여 비교한다. 시뮬레이션에 사용되는 가상의 센서 네트워크는 $500\times500m^2$ 크기로 구성되고, 1000개의 CH와 9000개의 일반 센서 노드를 무작위로 배치한다. 각 센서 노드들은 임의적으로 5개의 y-key와 1개의 z-key를 소유한다. 클러스터 지역의 CH는 10홉을 거쳐 전달 노드들에게 인증키 재분배를 위한 메시지를 전달한다. 각 CH는 Hill Climbing[11] 방법을 통해 전달 노드들을 선택한다. 이벤트 보고서를 생성하기 위해서는 각각의 다른 키로 생성된 5개의 MAC이 필요하다. 각 노드는 바이트 당 송, 수신 에너지로 16.25μJ, 12.5μJ을 소비한다. 이벤트 보고서의 크기는 24바이트이고 각 MAC 사이즈는 1바이트이다. 초기 재분배 주기 P는 10으로 고정된다.

그림 5는 고정된 주기, P = 5, 10, 15, 20에 따라 허위 보고서 탐지율을 보여준다. 기존 DEF는 주기 P값에 따라 의무적으로 키 재분배를 실시한다. 그림에서 볼 수 있듯이, 제안 기법(FD)과 P = 5일 때 가장 많은 허위보고서를 탐지하고 제거한다. 한편, P가 증가할 수 록 DEF는 허위 보고서 탐지효율을 떨어지는데 이는 공격자에 의해 노출된 훼손 키들을 이용한 허위 보고서를 제거하지 못하기 때문이다. 그러므로 인증키 재분배는 느슨하게 발생할 경우 충분한 탐지 능력을 보장하지 않는다.

그림 6은 인증키 재분배 결정 방법에 따른 에너지 소모량을 보여준다. 그림에서 보듯이, P가 클수록 인증키 재분배에 의한 에너지 소모가 적다는 것을 볼 수 있다. 반대로, P가 작을수록 허위 보고서에 의한 에너지 소모는 적

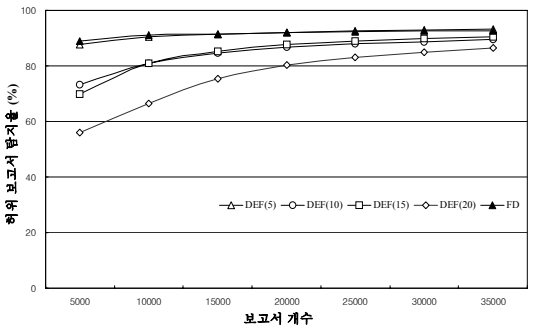

그림 5. 허위 보고서 탐지율

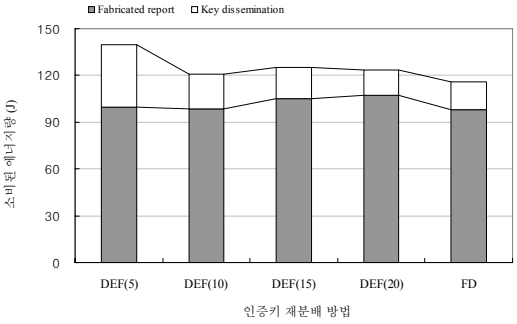

그림 6. 에너지 소모량

다는 것을 알 수가 있다. FD는 P = 5일 때와 유사한 허위 보고서에 의한 에너지 소모와 P = 15일 때와 비슷한 인증키 재분배에 의한 에너지를 소모한다. 이는 충분한 검증 효과를 유지하면서, 인증키 재분배에 의한 에너지 효율을 보장한다는 것을 나타낸다.

5. 결론 및 향후 과제

본 논문에서 퍼지 시스템을 사용하여 센서 네트워크의 동적 여과 기법에서 탐지 성능을 유지하면서 에너지 효율을 높이기 위한 인증키 재분배 결정 방법에 대하여 제안하였다. 퍼지 시스템은 네트워크의 허위 보고서 발생량과 클러스터 노드의 잔여 에너지량, 그리고 기지 노드와의 거리를 기반으로 적용되었다. 시뮬레이션 결과는 퍼지 시스템의 사용으로 네트워크의 허위 보고서 검증 성능 유지 및 효율적 에너지 소비를 보장하였다.

향후 과제로써, 본 연구에서 고려한 세 가지 입력 요소 외에 네트워크의 동적 변화에 대응하기 위한 추가적인 입력 요소를 고려하여 동적 토폴로지 변화에 맞는 인증키 재분배 결정에 대하여 연구할 것이다. 또한, 인증키 재분배를 시행하는 다른 여과 기법들에 적용할 예정이다.

참 고 문 헌

1. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks,” IEEECommun. Mag., vol. 40, no. 8, pp. 102-114, Aug. 2002.
2. C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” Ad Hoc Netw., vol. 1, no. 2-3, pp. 293-315. Sep. 2003.
3. D. Braginsky and D. Estrin, “Rumor Routing Algorithm for Sensor Networks,” In Proc Of The First ACM Workshop on Sensor Networks and Applications (WSNA), 2002.
4. K. Akkaya and M. Younis, “A Survey on Routing Protocols for Wireless Sensor Networks,” Ad hoc Netw., vol. 3, no. 3, pp. 325-349, May 2005.
5. H. Yang and S. Lu, “Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks,” Proc. of VTC, pp. 1223-1227, Oct. 2003.
6. F. Li and J. Wu, “A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks,” Proc. of IWCMC, pp. 27-32, Jul. 2006.
7. Z. Yu and Y. Guan, “A Dynamic En-Route Scheme for Filtering False Data Injection in Wireless Sensor Networks,” In Proc. Of SenSys, 2005.
8. 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, Apr. 2005.
9. D. Estrin, R. Govindan, J. Heidemeann, and S. Kumar, “Next Century Challenges: Scalable Coordination in Sensor Networks,” In Proc. of the 5th annual ACM/IEEE international conference on Mobile computing and networking, pp. 263-270, 1999.
10. C.C. Huang, M.H. Guo, and R.S. Chang, “A Weight-based Clustering Multicast Routing Protocol for Mobile Ad hoc Network,” Internet Protocol Tec. 1(1), pp. 10-18, Num. 2005.
11. D.B. Skalak, “Prototype and Feature Selection by Sampling and Random Mutation Hill Climbing Algorithms,” In Proc. of Eleventh International Machine Learning, pp. 293-301, 1994.

선 청 일 (cisun@ece.skku.ac.kr)

2007 경원대학교 소프트웨어학부 공학사
2009 성균관대학교 전자전기컴퓨터공학과 공학석사
2009～현재 성균관대학교 전자전기컴퓨터공학과 박사과정

관심분야 : 무선 센서 네트워크, 모델링 시뮬레이션, 네트워크 보안, 지능 시스템

조 대 호 (taecho@ece.skku.ac.kr)

1983 성균관대학교 전자공학과 공학사
1987 University of Alabama 전자공학과 공학석사
1993 University of Arizona 전자 및 컴퓨터공학과 공학박사
1995～현재 성균관대학교 정보통신공학부 교수

관심분야 : 무선 센서 네트워크, 모델링 시뮬레이션, 지능 시스템, 모델링 방법론, 네트워크 보안 시뮬레이션, 전사적 자원 관리