한국시뮬레이션학회 논문지
Vol. 19, No. 1, pp. 161-171 (2010. 3)

센서 네트워크에서 클러스터 신뢰도 기반 정적 여과 확률 조절 기법

허수만[1] · 서희석[1†] · 이동영[2] · 김태경[3]

Static Filtering Probability Control Method Based on Reliability of Cluster in Sensor Networks

Suh Mahn Hur · Hee Suk Seo · Dong Young Lee · Tae Kyung Kim

ABSTRACT

Sensor Networks are often deployed in unattended environments, thus leaving these networks vulnerable to false data injection attacks in which an adversary injects forged reports into the network through compromised nodes. Such attacks by compromised sensors can cause not only false alarms but also the depletion of the finite amount of energy in a battery powered network. Ye et al. proposed the Statistical En-route Filtering scheme to overcome this threat. In statistical en-route filtering scheme, all the intermediate nodes perform verification as event reports created by center of stimulus node are forwarded to the base station. This paper applies a probabilistic verification method to the Static Statistical En-route Filtering for energy efficiency. It is expected that the farther from the base station an event source is, the higher energy efficiency is achieved.

Key words : Sensor Networks, False Report, Filtering, Probability, Cluster, Cluster reliability, Static Filtering

요 약

많은 센서 네트워크 응용분야에서 센서 노드는 개방된 환경에 놓이게 된다. 공격자는 개방된 환경에 놓인 센서 노드를 물리적으로 획득할 수 있으며, 포획한 노드를 이용하여 허위보고서를 센서네트워크에 삽입 시킬 수 있다. 삽입된 허위 보고서는 제한된 센서노드 에너지를 고갈 시키며, 허위 경보를 일으켜 심각한 문제를 야기 시킬 수도 있다. 이러한 공격을 막기 위해 Ye 등은 통계적 여과 기법(Statistical En-route Filtering) 방법을 제안하였다. 통계적 여과기법은 CoS(Center of Stimulus)로부터 생성된 이벤트 보고서가 베이스 스테이션으로 전송되는 동안 중간의 모든 노드들이 검증을 하게 된다. 본 논문은 통계적 여과 기법에 확률 검증 기법을 적용하여 에너지 효율적인 정적 확률 통계적 여과 기법을 제안하고자 한다. 베이스 스테이션과 이벤트 발생 지역까지의 거리가 멀어질수록 에너지 절약 효과가 극대화 될 것으로 기대된다.

주요어 : 센서 네트워크, 허위 보고서, 필터링, 확률, 클러스터, 클러스터 신뢰도, 정적 여과

1. 서 론

최근 무선 통신의 발전과 초미세 전자기계 시스템의 발전은 저 비용의 센서 네트워크 구성을 가능하게 하였다. 저 비용의 센서 네트워크는 사람을 대신하여 위험한 군사 지역에 이용될 뿐만 아니라 유통 관리, 생산 관리, 환경 및 재난 관리, 에너지 관리, 의료 및 건강 서비스, 지능형 교통시스템 등 수많은 분야에 응용될 것으로 예측되고 있다[1,2]. 이러한 무선 센서 네트워크는 제한된 배터리 용량, 한정된 무선통신 범위 그리고 작은 메모리 공간을 가지고 있는 많은 센서노드들과 센서 네트워크를 인터넷과 같은 기존 통신 인프라와 연결하여 센서노드들이 감지한 정보를 모아서 사용자에게 전달해 주는 베이스 스테이션으로 구성되어 있다[3-5].

많은 센서 네트워크 응용분야에서 센서노드는 개별 관리가 어려운 개방된 환경에 배치된다. 이런 특징으로 인해, 공격자는 센서노드를 물리적으로 쉽게 획득할 수 있

2009년 12월 30일 접수, 2010년 3월 8일 채택
[1] 한국기술교육대학교 컴퓨터공학부
[2] 명지전문대학교 정보통신과
[3] 서울신학대학교 교양학부
주 저 자 : 허수만
교신저자 : 서희석
E-mail; histone@kut.ac.kr

으며 획득한 센서노드를 이용하여 허위보고서를 쉽게 베이스 스테이션으로 보낼 수 있다. 허위보고서는 제한된 에너지 자원을 가진 센서노드의 수명을 단축시킬 뿐만 아니라 베이스 스테이션과 관리자의 중요한 결정에 혼란을 유발 시킬 수도 있다. 이러한 허위보고서의 피해를 최소화하기 위해서는 허위보고서를 전송 중에 발견하여 걸러내야 하며, 걸러지지 않은 허위보고서는 베이스 스테이션에서 발견하고 제거해야 한다.

최근 이러한 허위 경고 공격을 막기 위해 몇몇의 필터링 기반 보안 기법이 제안되었다. 그 중 하나가 Fan Ye 등이 제안한 통계적 여과 기법이다. 통계적 여과 기법은 CoS로부터 생성된 이벤트 보고서가 베이스 스테이션으로 전송되는 동안 중간의 모든 노드들이 검증에 참여하게 된다[6].

본 논문에서는 기존 통계적 여과 기법에서 허위보고서가 가장 많이 발견되고 여과되는 30홉 이내를 주목하였다. 이는 이벤트 발생 지역으로부터 일정 이하의 홉에만 이벤트 보고서 검증을 하고 일정 이상의 홉에는 검증을 적용하지 않는다는 것이다. 정상보고서가 이벤트 발생 지역에서 베이스 스테이션까지 가는데 중간의 모든 노드에서 검증하는데 소요되는 에너지를 줄이기 위함이다. 이를 위해 이벤트 발생지역의 노드들은 높은 확률로 검증을 하고 일정이상의 홉을 넘게 되면 검증 과정 없이 베이스 스테이션으로 포워딩한다. 본 논문은 통계적 여과 기법에 확률 검증 기법을 적용하여 에너지 효율적인 정적 확률 통계적 여과 기법을 제안하고자 한다.

2. 배 경 이 론

2.1 허위 경고 공격(False Positive Attack)

그림 1은 공격자가 포획한 센서노드를 이용한 허위 경고 공격을 보여주고 있다. 공격자에 의해 만들어진 허위보고서는 제한된 에너지 자원을 가지고 있는 센서노드의 수명을 단축시킬 뿐만 아니라, 베이스 스테이션에 전달되어 관리자의 판단에 혼란을 초래할 수도 있다.

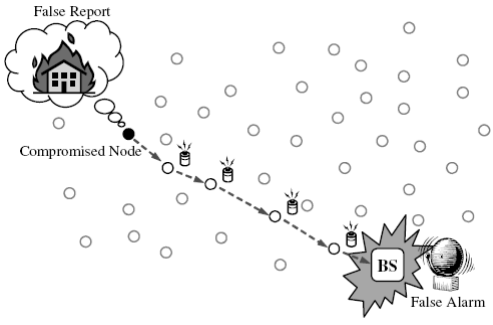


그림 1. 허위 경고 공격

2.2 통계적 여과 기법(SEF)

통계적 여과 기법에서 노드들에게 키를 할당 방법은 그림 2와 같이 베이스 스테이션의 특정 구획의 키들 중 사용자가 지정한 개수의 키를 각 노드에 저장한 후 관심지역에 배치하게 된다.

이벤트가 발생하면 이벤트를 탐지한 노드들 중 한 노드가 CoS로 선택이 된다. 그 주변노드들은 감지한 이벤트 데이터 메시지와 각각 자신이 소유한 키들 중에서 하나의 키를 임의로 선택해서 이벤트 데이터에 대한 MAC(Message Authentication Code)을 생성한다. 그리고 두 메시지를 CoS로 선택된 노드에 전달하면, CoS가 이벤트에 관한 보고서를 생성한다. 이 때 보고서는 서로 다른 구획의 키로 인증된 MAC으로 구성되어야 한다[7-9].

그림 3은 보고서 생성과 En-route 필터링 과정을 보여준다. T는 보안 임계값으로써 그림 3에서 T의 값은 3이다. CoS에서 작성된 보고서는 멀티 홉 방식으로 베이스 스테이션에 전달되며, 전달되는 동안 중간노드에서는 자신이 보유한 키들이 작성된 보고서에 사용되고 있는지 여부를 확인한다. 여기서 자신이 갖고 있는 키가 없으면 다음 노드로 전달하고, 그렇지 않으면 보고서에 관한 MAC을 구성하여 보고서에 사용된 메시지 인증코드와 비교하

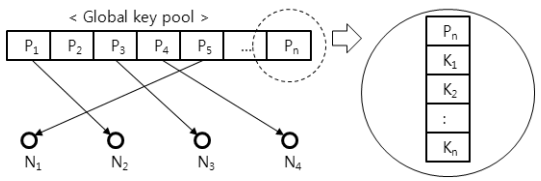


그림 2. 배치 전에 각 노드들에게 키 할당

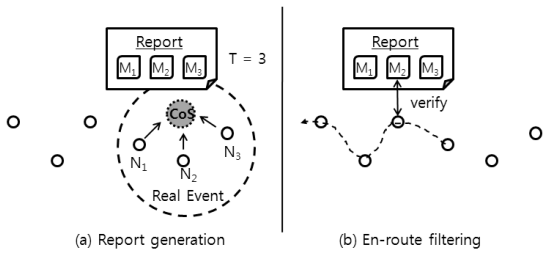


그림 3. 보고서 생성(a)과 En-route필터링(b)

여 정상적인 MAC인 경우에만 다음 노드로 전달하게 된다. 이와 같은 방법을 통하여 정상 메시지만 베이스 스테이션에 전달되고, 위조 메시지는 중간에서 여과되며 최악의 경우에는 모든 키를 소유한 베이스 스테이션에서 같은 방법으로 메시지에 사용된 모든 MAC을 검증하게 된다. 이러한 방법을 통하여 위조 메시지 공격에 대응할 수 있으며, 전체 네트워크에서 사용되는 에너지 소모를 줄일 수 있다.

3. 정적 확률 통계적 여과 기법

3.1 개요

정적 확률 통계적 여과 기법은 통계적 여과 기법에 에너지 효율적인 측면을 고려하고자 제안되었다. 초기 배치 시에는 통계적 여과 기법이지만 이벤트가 발생하고 CoS가 이벤트 보고서를 베이스 스테이션으로 보내는 과정에서 이벤트 보고서 패킷에 대한 검증 확률 여부가 일정 홉에 따라 결정되어지게 된다. 그림 4는 정적 확률 통계적 여과 기법을 예를 보여주고 있다.

본 논문에서는 무선 센서 네트워크에 대해 다음의 가정 사항을 가진다. 각 센서 노드는 이벤트 보고서를 보내온 CoS로부터의 홉 수를 알고 있다. 관심 지역의 노드들을 획득하여 훼손된 정보로부터 홉 수는 안전하다고 가정한다.

통계적 여과 기법 연구에서의 시뮬레이션 결과를 미루어 허위 보고서가 대부분 사라지는 30홉까지만 관심 홉으로 보고 검증 확률을 적용함으로써, 노드들이 이벤트 보고서를 검증할 때 소요되는 에너지를 줄이고자 한다. 정적 확률 통계적 여과 기법을 적용함으로써 이벤트 보고서에 대한 검증 확률을 선택적으로 낮춤으로써 에너지 절약 효과가 클 것으로 기대된다. 따라서 노드들의 수가 많고 관심 지역의 범위가 넓으며 허위 경고 공격이 집중적으로 일어나는 지역에 효과적으로 대처할 수 있다.

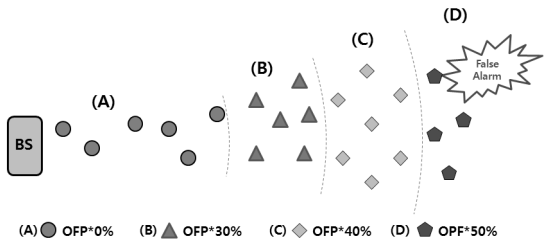


그림 4. 정적 확률 통계적 여과 기법의 개요

3.2 정적 확률 통계적 여과 기법

정적 확률 통계적 여과 기법은 각 노드가 이벤트 발생 지역의 CoS가 보내온 이벤트 보고서의 홉 수를 알고 있다고 가정한다. 이벤트가 발생한 지역의 CoS가 BS에게 보내는 이벤트 보고서는 다음과 같다. L_E는 이벤트 장소, t는 탐지시간, E는 이벤트 타입이다. 그리고 i는 노드, M_i는 i노드의 MAC이다.

$$\{L_E, t, E, i_1, M_{i1}, i_2, M_{i2}, \ldots, i_T, M_{iT}\} \quad (1)$$

정적 확률 통계적 여과 기법은 여기에 이벤트 발생 지역 CoS로부터의 홉 수를 함께 덧붙여 보내어지게 된다.

$$\{h, L_E, t, E, i_1, M_{i1}, i_2, M_{i2}, \ldots, i_T, M_{iT}\} \quad (2)$$

이렇게 보내어진 이벤트 보고서는 일정 홉 마다 정해진 확률에 따라 검증을 하게 된다. 일정 홉 이상이 되면 더 이상의 필터링 과정없이 베이스 스테이션으로 보내어지게 된다.

그림 5은 정적 확률 통계적 여과 기법의 예를 보여주고 있다. CoS A노드에서 발생한 이벤트는 일정 홉 수 만큼 검증확률 OFP(One-hop Filtering Probability)*50%로 이벤트 보고서를 검증하게 된다. 일정 홉을 지나면 검증확률 OFP*40%인 노드들을 거치게 된다. 또 다시 일정 홉을 지나게 되면 검증확률 OFP*30%인 노드들을 거치게 된다. 이후 이벤트 보고서는 검증과정 없이 곧바로 베이스 스테이션으로 전송되어 진다. CoS C노드에서 발생한 이벤트도 CoS A노드와 비슷한 과정을 거치게 된다. CoS A노드, CoS C노드에 비해 비교적 베이스 스테이션과 가까운 지역에서 이벤트가 발생한 CoS B노드는 검증확률이 적용되는 홉 수 내에서 베이스 스테이션으로 이벤트 보고서가 전송되는 것을 볼 수 있다.

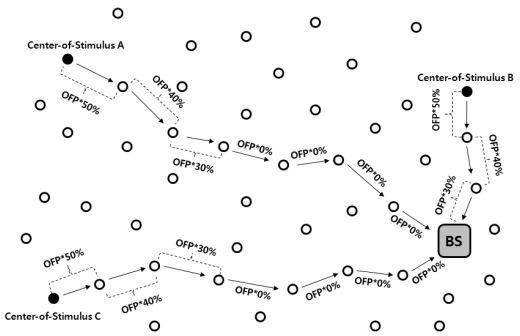


그림 5. 정적 확률 통계적 여과 기법의 예

4. 클러스터 신뢰도 기반 정적 확률 통계적 여과 기법

4.1 개요

클러스터 신뢰도 기반 정적 확률 통계적 여과 기법의 가정사항은 정적 확률 통계적 여과 기법에서와 같다. 다만 다른 점은 클러스터별로 일정 단위 홉 마다 검증하는 확률이 달라진다. 또한, 베이스 스테이션 검증 및 반응 단계에서 클러스터 별 신뢰도에 따른 정적 확률을 클러스터 노드들에게 반영할 때, 이웃 노드들끼리 주기적으로 주고받는 헬로우 메시지에 같이 담아서 보낸다고 가정한다.

클러스터 신뢰도 기반 정적 확률 통계적 여과 기법에서는 정적 확률 통계적 여과 기법에 클러스터의 개념을 도입하여 에너지 효율을 극대화 하고자 한다. 이벤트 보고서를 수신받은 베이스 스테이션은 각 클러스터 별 신뢰도를 계산한다. 신뢰도에 따른 정적 확률을 클러스터 별로 적용하여 허위 경고 공격이 빈번한 클러스터에는 높은 정적 확률을 적용하고 그렇지 않은 클러스터에는 낮은 정적 확률을 적용하여 에너지 효율을 극대화 하고자 제안하게 되었다.

클러스터 신뢰도 기반 정적 확률 통계적 여과 기법은 3가지 단계로 이루어진다. 네트워크 초기화 단계, En-route 필터링 단계, 베이스 스테이션 검증 및 반응 단계로 구성된다.

A. 네트워크 초기화 단계 : 네트워크 초기화 단계의 키 분배, 노드 배치 등은 통계적 여과 기법과 같다. 노드 배치 후 각 노드들은 자신의 이웃노드들을 발견하고 베이스 스테이션은 각 클러스터의 신뢰도를 관리하기 위한 테이블을 생성한다. 테이블에는 모든 클러스터들의 ID, 클러스터 별 정상 보고서의 수, 클러스터 별 허위 보고서의 비율, 클러스터 별 확률이 기록되어 진다.

B. En-route 필터링 단계 : En-route 필터링 단계는 각 중간 노드들이 홉에 따른 정적 확률에 따라 이벤트 보고서를 검증하는 단계이다. 이벤트 발생 지역 클러스터 헤드 노드로부터 단계적으로 일정 홉까지 정적 확률로 이벤트 보고서를 검증하고 일정 홉 이상으로부터 베이스 스테이션까지는 검증 과정 없이 베이스 스테이션으로 보내어지게 된다.

C. 베이스 스테이션 검증 및 반응 단계 : 이벤트 보고서를 수신한 베이스 스테이션은 이벤트 보고서의 모든 MAC을 검증한다. 허위 보고서이면 버려지게 되고 정상보고서만 정보로써 활용된다. 또한, 베이스 스테이션은 수신한 이벤트 보고서를 각 클러스터 별로 정상 보고서, 허위 보고서의 비율, 클러스터 별 정적 확률로 나뉘어 저장하게 된다. 클러스터 별 정적 확률은 퍼지로직에 의해 계산되고 추후 클러스터들의 정적 확률에 반영된다. 일정량의 이벤트 보고서가 쌓이게 되면 베이스 스테이션은 신뢰도에 변화가 있는 클러스터에 새로운 정적 확률을 전송하게 된다. 새로운 정적 확률을 수신한 클러스터의 노드들은 다음 이벤트 보고서를 검증하는데 새로운 정적 확률을 활용한다.

4.2 클러스터 신뢰도 기반 정적 확률 통계적 여과 기법

클러스터 신뢰도 기반 정적 확률 통계적 여과 기법을 이루고 있는 3가지 단계에 대해서 알아보자.

네트워크 초기화 단계에서, 이벤트 보고서를 수신한 베이스 스테이션은 허위보고서, 정상보고서를 판단하여 기록한다. 이렇게 기록된 자료들은 추후 클러스터별 검증 확률에 반영된다. 베이스 스테이션은 각 클러스터 별 ID와 정상 보고서(RVR : The number of recent valid reports), 허위보고서 비율(FTR : false traffic ratio), 클러스터별 확률(FP : The filtering probability)을 테이블에 저장한다.

표 1에서와 같이 베이스 스테이션은 각 클러스터들에 대한 ID, RVR, FTR, FP을 테이블에 기록한다. 초기의 RVR과 FTR의 값은 0이다. 초기의 클러스터들에 대한 FP의 값은 동일한 값을 갖는다.

En-route 필터링 단계에서는 정적 확률 통계적 여과 기법을 사용한다. 다른 점은 클러스터 별로 관리가 된다는 점이다. 그림 6과 같이 클러스터 1의 CoS A노드에서 발생한 이벤트는 일정 홉 수 만큼 검증확률 OFP*50%로 이벤트 보고서를 검증하게 된다. 일정 홉을 지나면 검증확률 OFP*40%인 노드들을 거치게 된다. 또 다시 일정 홉을 지나게 되면 검증확률 OFP*30%인 노드들을 거치게

표 1. 생성 테이블

ID	RVR	FTR	FP(%)
C1	0	0/0	50
C2	0	0/0	50
...	...	...	...

된다. 이후 이벤트 보고서는 검증과정 없이 곧바로 베이스 스테이션으로 전송되어 진다. 클러스터 2의 CoS B, CoS C노드에서 발생한 이벤트도 CoS A노드와 비슷한 과정을 거치게 된다.

베이스 스테이션 검증 및 반응 단계에서, 베이스 스테이션은 각각의 클러스터들로부터 수신한 이벤트 보고서들의 모든 MAC을 검증한다. 베이스 스테이션이 생성한 MAC과 비교하여 값이 같다면 정보로 활용되고 다르다면 버려지게 된다. 또한, 검증 결과에 따라 해당 클러스터들의 노드들이 보고서를 검증하기 위한 여과 확률을 갱신한다. 이웃 노드로부터 받은 이벤트 보고서가 정상 보고서로 판명되면 해당 노드를 위한 여과 확률을 일정 확률의 크기만큼 감소시키고 허위 보고서의 경우에는 일정 확률의 크기만큼 증가시킨다. 일정 확률은 퍼지로직에 의해 변경된다. 변경된 여과 확률은 일정 시간이 지나면 헬로우 메시지와 함께 해당 클러스터 노드들에게 브로드 캐스트 된다. 해당 노드들은 수신된 여과 확률을 다음 이벤트 보고서를 검증하는데 사용된다. 결과적으로 각 클러스터가 전송하는 이벤트 보고서의 신뢰성에 따라 해당 클러스터 노드들의 보고서에 대한 여과 확률이 결정된다.

그림 7은 클러스터의 이벤트 보고서 필터링 확률 감소의 한 예를 보여준다. 베이스 스테이션은 클러스터 1, 2로부터 각각 5개씩의 정상보고서를 받는다. 보고서를 받은 베이스 스테이션은 클러스터들의 RVR과 FTR을 기록하고 필터링 확률을 수정한다. 클러스터 1, 2에서 보낸 메시지에서 허위보고서가 검출되지 않음에 따라 확률이 감소하는 것을 볼 수 있다.

그림 8은 클러스터의 이벤트 보고서 필터링 확률 증가의 한 예를 보여준다. 베이스 스테이션은 클러스터 2로부터 2개의 허위보고서를 받고 클러스터 1로부터 아무런 메시지도 수신하지 않았다. 허위보고서를 받은 베이스 스테이션은 클러스터들의 RVR과 FTR을 기록하고 필터링 확률을 수정한다. 베이스 스테이션은 클러스터 2로부터 2개의 허위보고서를 받았다. 베이스 스테이션은 2개의 허위보고서를 탐지하고 드롭시킨다. 클러스터 2로부터 허위보고서를 받은 베이스 스테이션은 클러스터 2의 검증 확률을 증가시키고 클러스터 1의 검증 확률은 그대로 유지한다.

일정량의 이벤트 보고서가 쌓이면 베이스 스테이션은 각 클러스터 별로 새로운 정적 확률을 헬로우 메시지와 함께 반영한다. 그림 9는 클러스터 별 새로운 정적 확률이 반영되는 것을 보여주고 있다.

그림 10은 새로운 정적 확률이 반영되어 이벤트 보고서가 발생하였을 때 클러스터 별 다른 정적 확률이 적용됨을 보여준다. 클러스터 1의 노드들은 허위 경고 공격이 많지 않아 정적 확률이 낮아졌음을 볼 수 있다. 클러스터 2의 노드들은 허위 경고 공격이 일어남에 따라 초기 정적 확률을 유지하는 것을 볼 수 있다.

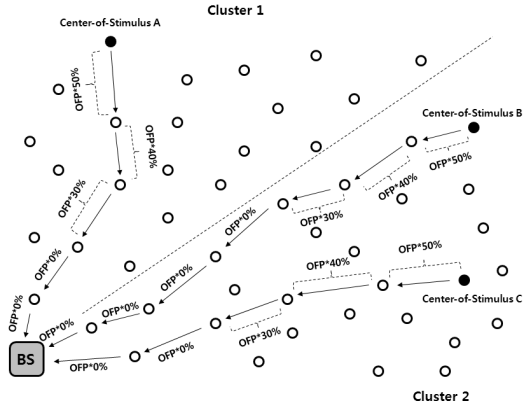


그림 6. En-route 필터링 단계

ID	RVR	FTR	FP (%)
1	5	0/5	50 → 40
2	5	0/5	50 → 40

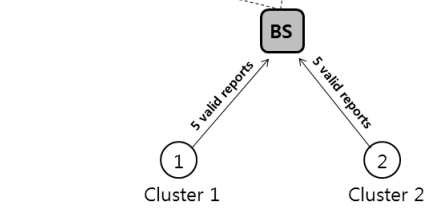


그림 7. 필터링 확률의 감소

ID	RVR	FTR	FP (%)
1	5	0/5	40
2	5	2/7	40 → 50

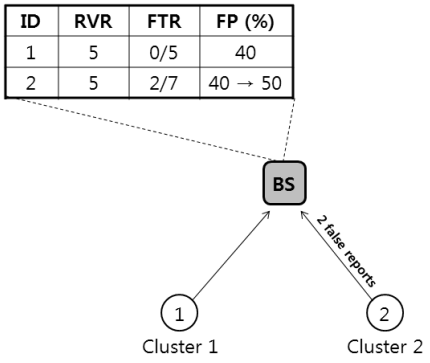


그림 8. 필터링 확률의 증가

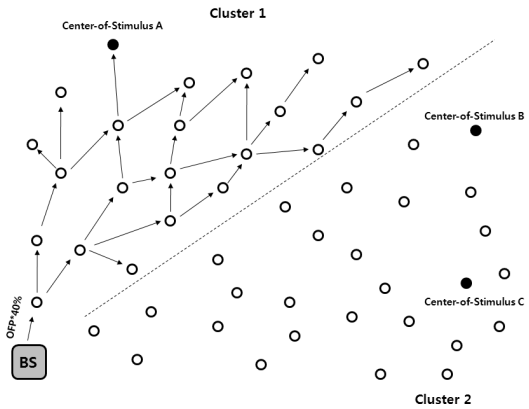


그림 9. 새로운 정적 확률 반영

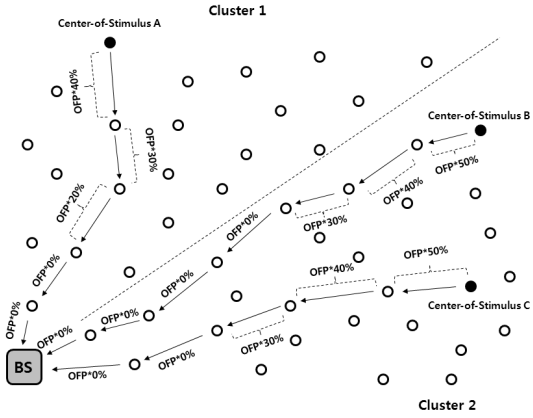


그림 10. 새로운 클러스터 신뢰도 정적 확률 통계적 여과 기법

5. 시뮬레이션 및 고찰

5.1 정적 확률 통계적 여과 기법의 실험 결과

본 논문에서 시뮬레이션을 위해 가정한 사항들은 다음과 같다. 센서 필드는 50m × 200m의 크기로 내부에는 600개의 센서 노드가 분포되어 있다. 전체 키 집합은 각각 100개의 키로 이루어져 있으며 10개의 키를 가진 10개의 키 분할로 나뉜다. 하나의 노드에는 하나의 키 분할에 속하는 6개의 키가 할당된다. 각각의 보고서에는 10개의 서로 다른 키 분할의 키로 만들어진 메시지 인증 코드가 포함된다. 메시지 송신/수신에 소모되는 에너지는 16.25/12.25μJ이며 여과 연산에는 75μJ이 소모된다. Ye[6] 실험은 총 300개의 정상 혹은 허위 보고서를 생성하여 그에 따른 처리에 소모되는 에너지를 구하는 방식으로

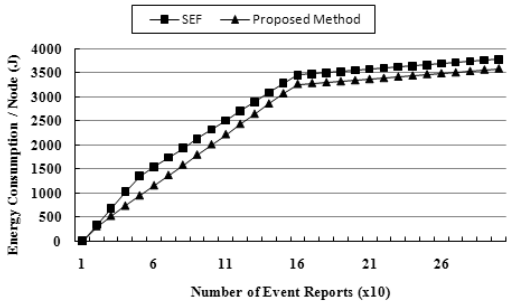


그림 11. 제안 기법과 SEF의 에너지 소모량

이루어졌다. 먼저 150개의 정상 보고서가 생성된 후 훼손된 노드에 의한 150개의 허위 보고서가 네트워크에 주입된다. 노드들의 초기 여과 확률은 50%이며 여과 확률을 조절하기 위한 단위 확률은 20%로 하였다. 최초 이벤트 보고서 전송으로부터의 홉 카운트를 기준으로 10홉마다 단위 확률 20%씩 낮추는 방식으로 진행하였다. 그리고 30홉 이후에는 이벤트 보고서 검증 없이 베이스 스테이션으로 곧바로 전송되게 하였다. 자체 개발한 시뮬레이션 툴을 사용한 본 실험은 크게 두 가지 방식으로 진행하였다. 첫 번째 실험은 관심 지역의 범위 내에 이벤트 발생지역으로부터 베이스 스테이션까지의 홉 수가 적은 실험이고, 두 번째 실험은 일정한 관심 지역의 범위에 충분한 수의 노드를 주입하여 이벤트 발생지역으로부터 베이스 스테이션까지의 홉 수가 많게 설정하여 실험하였다. 첫 번째 실험은 평균 홉이 18홉, 최대 홉이 39인 환경에서의 실험이고, 두 번째 실험은 평균 홉이 37홉, 최대 홉이 93홉인 환경에서 실험하였다. 다음은 첫 번째 실험의 결과이다. 그림 11은 제안 기법과 통계적 여과 기법의 에너지 소모량을 비교하여 보여준다.

그래프에서 보는 바와 같이 제안기법은 통계적 여과 기법에 비해 비슷하거나 약간의 에너지 절약 효과를 보여준다. 이 실험에서는 이벤트발생으로부터 10홉 단위로 확률을 20%씩 낮추어 진행하였다.

그림 12는 제안 기법과 통계적 여과 기법의 필터링 능력을 비교하여 보여준다. 제안 기법, 통계적 여과 기법 모두 비슷한 필터링 능력을 보여주고 있다.

다음은 두 번째 실험에 대한 결과이다. 이벤트 발생 지역으로부터 베이스 스테이션까지의 홉 수가 많게 설정한 두 번째 실험은 3가지로 나뉜다. 홉 수에 따른 정적 여과 확률의 적용이 에너지 효율에 어떻게 작용하는지 알아보기 위해서이다. 첫 번째, 5홉까지는 통계적 여과 기법과

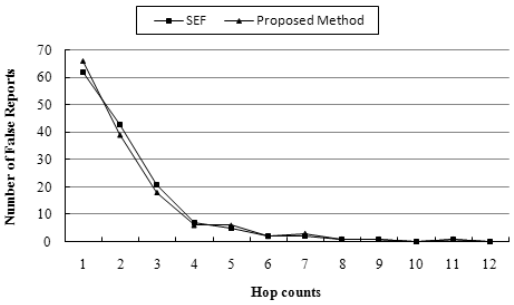
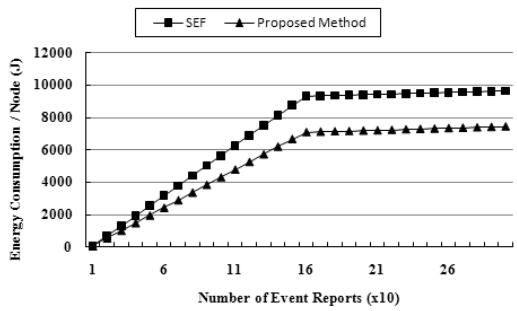
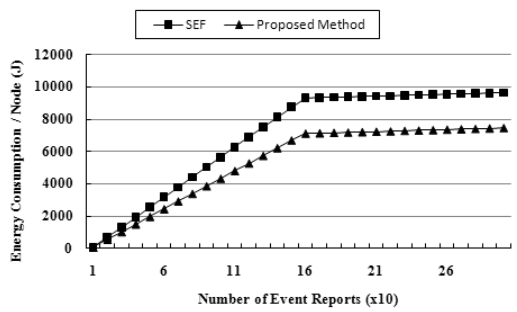


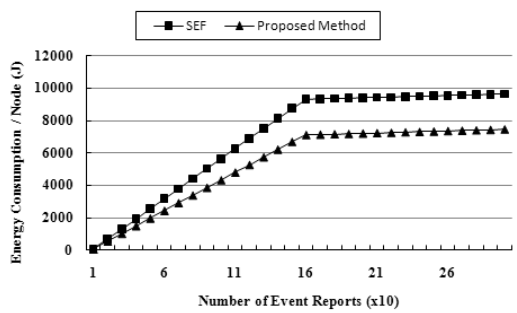
그림 12. 필터링 능력



(a) 첫 번째 실험 결과



(b) 두 번째 실험 결과



(c) 세 번째 실험 결과

그림 13. 제안 기법과 SEF의 에너지 소모량

같이 보고서를 검증하게 하였고 그 이후 15홉, 30홉까지는 확률을 20%씩 낮추었다. 30홉 이후부터는 검증 과정 없이 베이스 스테이션으로 보내어지게 하였다. 두 번째, 10홉까지는 통계적 여과 기법과 같이 보고서를 검증하게 하였고 그 이후 20홉, 30홉까지는 확률을 20%씩 낮추었다. 30홉 이후부터는 검증 과정 없이 베이스 스테이션으로 보내어지게 하였다. 세 번째, 15홉까지는 통계적 여과 기법과 같이 보고서를 검증하게 하였고 그 이후 25홉, 30홉까지는 확률을 20%씩 낮추었다. 30홉 이후부터는 검증 과정 없이 베이스 스테이션으로 보내어지게 하였다.

그래프에서 보는 바와 같이 제안 기법은 통계적 여과 기법에 비해 뛰어난 에너지 절약 효과를 보여준다. 일정 홉 이내에서 거의 필터링 되어진 허위보고서와 일정 홉 이후의 정상보고서에 대해 검증 확률 없이 전송함으로써 에너지 절약 효과가 있었다고 할 수 있다. 3가지 실험에서 각각의 제안 기법은 모두 비슷한 에너지 절약 효과를 보여준다. 홉 수 변화에 따른 에너지 소모량은 비교적 크지 않았다.

그림 14는 확률 적용 홉 수에 따른 에너지 변화를 보여주고 있다. 확률 적용 홉 수까지는 통계적 여과 기법과 같이 보고서를 검증하게 하였고 그 이후 확률 적용 홉 수 + 10홉, 확률 적용 홉 수 + 10홉~30홉까지는 단위 확률 20%씩 낮추어 진행하였다. 제안 기법의 확률 적용 홉 수에 따른 에너지 변화를 일반화하면 그림 15와 같다.

그림 15는 제안 기법의 확률 적용 홉 수에 따른 에너지 변화를 일반화한 것이다. 4홉에서 가장 에너지 절약 효과가 뛰어났다. 4홉에서 6홉까지 비슷한 에너지 소모량을 보여주다가 6홉 이후부터는 꾸준히 증가하는 것을 볼 수 있다.

그림 16은 확률 적용 홉 수에 따라 허위 보고서가 검출된 마지막 홉을 나타낸다. 적용 확률을 늘려감에 따라 필터링 능력이 꾸준히 좋아지고 있는 것을 볼 수 있다. 9홉

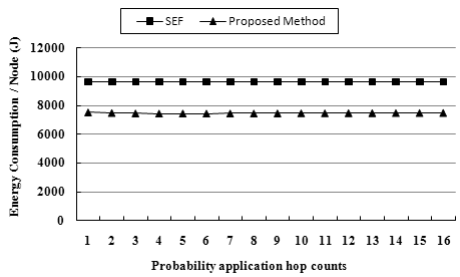


그림 14. 확률 적용 홉 수에 따른 에너지 변화

이후 부터는 일정한 필터링 능력을 보여주고 있다.

그림 17은 제안 기법과 통계적 여과 기법의 필터링 능력을 비교하여 보여준다. 그림 13의 두 번째 실험을 기준으로 실험하였다. 제안 기법, 통계적 여과 기법 모두 비슷한 필터링 능력을 보여주고 있다.

5.2 클러스터 신뢰도 기반 정적 확률 통계적 여과 기법

클러스터는 그림 18과 같이 2개의 클러스터로 나누어 구성하였다. 실험은 총 600개의 정상 혹은 허위 보고서를 생성하여 그에 따른 처리에 소모되는 에너지를 구하는 방식으로 이루어졌다. 먼저 150개의 정상 보고서가 생성된 후 훼손된 노드에 의한 150개의 허위 보고서가 네트워크에 주입된다. 베이스 스테이션에서 수신한 정상보고서, 허위보고서를 바탕으로, 퍼지로직(FFLL)을 통해 얻은 확률을 각 클러스터에 반영한다. 그 후 다시 150개의 정상 보고서가 생성된 후 훼손된 노드에 의한 150개의 허위 보고서가 네트워크에 주입된다. 노드들의 초기 여과 확률은 50%이며 여과 확률을 조절하기 위한 단위 확률은 20%로 하였다. 최초 이벤트 보고서 전송으로부터의 홉 카운트를 기준으로 일정 홉까지는 초기 확률 값인 50%를 적용하였다. 이후 일정 홉 + 10홉, 일정 홉 + 10홉～30홉까지 단위 확률 20%씩 낮추는 방식으로 진행하였다. 그리고 30홉 이후에는 이벤트 보고서 검증 없이 베이스 스테이션으로 곧바로 전송되게 하였다. 실험은 관심 지역의 범위에 충분한 수의 노드를 주입하여 이벤트 발생지역으로부터 베이스 스테이션까지의 홉 수가 많게 설정하여 실험하였다. 평균 홉이 37홉, 최대 홉이 93홉인 환경에서 실험하였다. 다음은 클러스터 신뢰도 기반 정적 확률 통계적 여과 기법의 실험결과를 보여준다. 실험은 3가지로 나누어 진행하였다. 홉 수에 따른 새로운 정적 여과 확률의 적용이 에너지 효율에 어떻게 작용하는지 알아보기 위해서이다. 첫 번째, 5홉까지 초기 정적 여과 확률로 보고서를 검증하게 하였고 그 이후 15홉, 30홉까지는 확률을 20%씩 낮추었다. 30홉 이후부터는 검증 과정 없이 베이스 스테이션으로 보내어지게 하였다. 두 번째, 10홉까지 초기 정적 여과 확률로 보고서를 검증하게 하였고 그 이후 20홉, 30홉까지는 확률을 20%씩 낮추었다. 30홉 이후부터는 검증 과정 없이 베이스 스테이션으로 보내어지게 하였다. 세 번째, 15홉까지 초기 정적 여과 확률로 보고서를 검증하게 하였고 그 이후 25홉, 30홉까지는 확률을 20%씩 낮추었다. 30홉 이후부터는 검증 과정 없이 베이스 스테이션

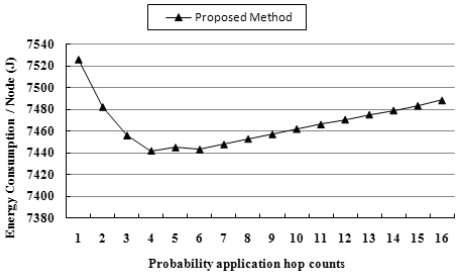


그림 15. 제안 기법의 에너지 변화

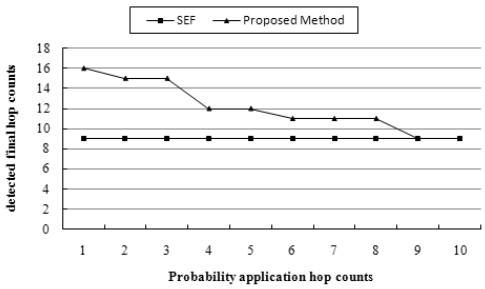


그림 16. 허위 보고서가 검출된 마지막 홉

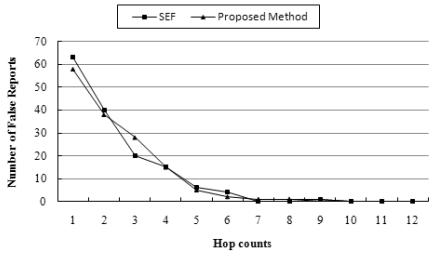


그림 17. 필터링 능력

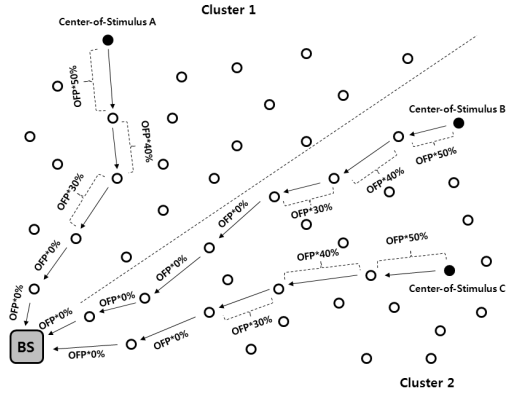


그림 18. 클러스터 실험 모형

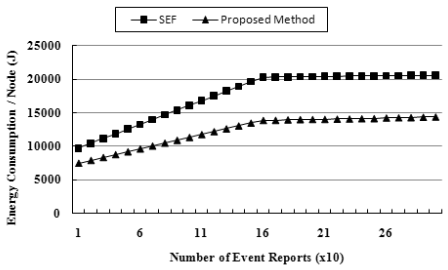
으로 보내어지게 하였다.

그림 19에서 보는 바와 같이 클러스터 신뢰도 기반 정적 확률 통계적 기법은 통계적 여과기법이나 정적 확률 통계적 여과 기법에 비해 뛰어난 에너지 절약 효과를 보여준다. 이벤트 보고서 300개까지는 정적 확률 통계적 여과 기법을 적용하였고 그 이후에는 클러스터별 신뢰도를 기반으로 하여 확률을 결정하였다. 정적 확률 통계적 여과 기법에서 정상보고서 150개, 허위보고서 150개, 클러스터 신뢰도 기반 정적 확률 통계적 여과 기법에서 정상보고서 150개, 허위보고서 150개를 생성하였을 때의 에너지 효율 그래프를 보여주고 있다.

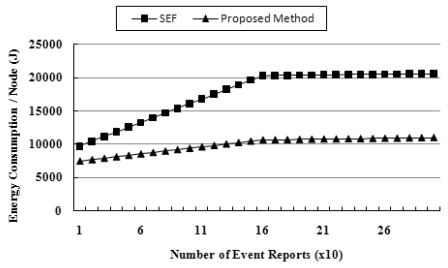
그림 20은 확률 적용 홉 수에 따른 에너지 변화를 보여주고 있다. 확률 적용 홉 수까지는 통계적 여과 기법과 같이 보고서를 검증하게 하였고 그 이후 확률 적용 홉 수 + 10홉, 확률 적용 홉 수 + 10홉~30홉까지는 단위 확률 20%씩 낮추어 진행하였다. 확률 적용이 늘어남에 따라 에너지 소모량이 점차 줄어들고 있는 것을 보여주고 있다. 6홉 이후부터 꾸준한 에너지 절약 효과를 보여주고 있다.

그림 21은 허위 보고서가 검출된 마지막 홉을 확률 적용 홉 수에 따라 보여주고 있다. 적용 확률을 늘려감에 따라 필터링 능력이 꾸준히 좋아지고 있는 것을 볼 수 있다. 9홉 이후 부터는 일정한 필터링 능력을 보여주고 있다.

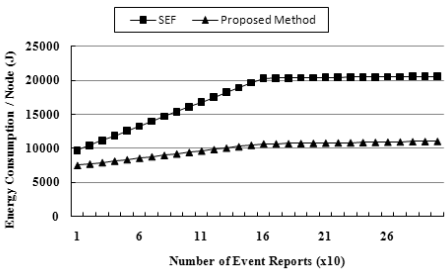
그림 22는 클러스터 신뢰도 기반 통계적 여과 기법과 통계적 여과 기법의 필터링 능력을 비교하여 보여준다. 그림 19의 두 번째 실험을 기준으로 실험하였다. 클러스



(a) 첫 번째 실험



(b) 두 번째 실험



(c) 세 번째 실험

그림 19. 제안 기법과 SEF의 에너지 소모량

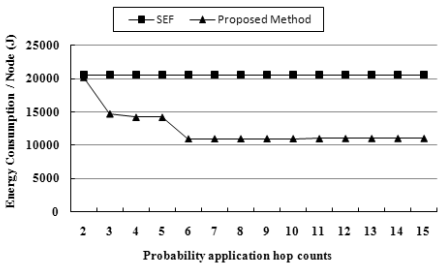


그림 20. 확률 적용 홉 수에 따른 에너지 변화

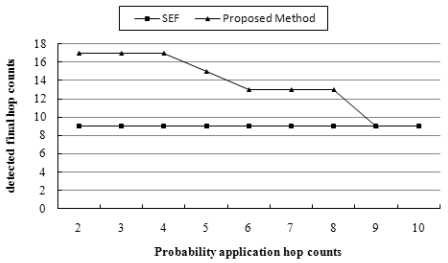


그림 21. 허위 보고서가 검출된 마지막 홉

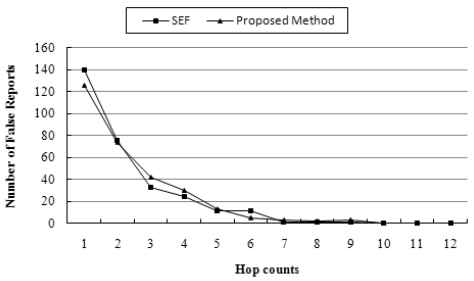


그림 22. 필터링 능력

터 신뢰도 기반 통계적 여과 기법, 통계적 여과 기법 모두 비슷한 필터링 능력을 보여주고 있다.

6. 결 론

본 논문에서는 센서 네트워크에서 에너지 효율적인 정적 확률 통계적 여과 기법 및 클러스터 신뢰도 기반 통계적 여과 기법을 제안하였다. 기존 통계적 여과 기법에서는 CoS가 클러스터노드들로부터 받은 MAC들을 모아 이벤트보고서를 생성하고 베이스 스테이션으로 전송하는 동안 중간의 모든 노드들이 검증을 하기 위해 참여하였다. 따라서 정상 보고서가 베이스 스테이션까지 가는데 중간 노드들의 불필요한 검증으로 에너지를 많이 소모하였다.

본 연구에서는 허위보고서가 가장 많이 발견되고 여과되는 CoS로부터 30홉 이내의 노드들에 관심을 갖고 검증에 참여하게 하였다. 이후에는 검증과정 없이 베이스 스테이션으로 보내어 에너지 절약 효과를 얻고 있다. 베이스 스테이션으로부터 이벤트 발생지역까지의 거리가 멀어지면 멀어질수록, 홉 수가 많아질수록, 관심 지역의 범위가 커질수록 더욱 더 좋은 에너지 절약효과를 얻을 수 있었다.

정적 확률 통계적 여과 기법을 보완한 클러스터 신뢰도 기반 정적 확률 통계적 여과 기법은 통계적 여과 기법이나 정적 확률 통계적 여과 기법에 비해 더 좋은 에너지 효율을 보여주고 있다. 클러스터의 신뢰도는 각 클러스터별로 수신한 정상 보고서의 수, 전체 이벤트 보고서에 대한 허위 보고서의 비율을 지표로 하였으며, 각 클러스터별 정적 확률의 계산은 퍼지 논리를 이용하여 수행하였다. 그리고 각 클러스터들에 대한 테이블을 생성하고 관리하는 것, 퍼지 로직에 의한 계산을 하는 것들을 베이스 스테이션에서 담당하고 있어 센서네트워크 노드들에게 오버헤드를 주지 않는다는 장점이 있다. 클러스터 신뢰도 기반 정적 확률 통계적 여과 기법 또한 베이스 스테이션으로부터 이벤트 발생지역까지의 거리가 멀어지면 멀어질수록, 홉 수가 많아질수록, 관심 지역의 범위가 커질수록 더욱 더 좋은 에너지 절약효과를 얻을 수 있다. 베이스 스테이션 검증 및 반응 단계에서 헬로우 메시지를 통해 새로운 정적 확률을 반영하기 위해서는 동기화가 되어야 할 것이다.

향후 연구 과제로는 다양한 확률 기법을 적용하여 보고 최적의 확률 여과기법을 찾는 방법을 연구하여 보다 향상된 확률 통계 여과 기법을 제안하고자 한다.

참 고 문 헌

1. I.F. Akvildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks,” IEEE Commun. Mag, pp. 102-114, 2002.
2. k. Akkaya and M. Younis, “A Survey on Routing Protocols for Wireless Sensor Networks,” Ad hoc Netw. 3(3), pp. 325-349, 2004.
3. B. Przydatek, D. Song., and A Perrig, “SIA: Secure Information Aggregation in Sensor Networks,” ACM, Proceeding of SenSys, pp. 255-265, 2003.
4. Xu, N. “A Survey of Sensor Network Applications,” Tech. Rep., University of Southern California. 2002.
5. Al-Karaki, J.N. and Kamal, A.E. “Routing techniques in wireless sensor networks: a survey,” IEEE Wireless Communication Magazine, vol. 11, no. 6, pp. 6-28. 2004.
6. 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.
7. H. Yang and S. Lu, “Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks,” in Proc. VTC, pp. 1223-1227, 2003.
8. S. Zhu, S. Setia, S. Jajodia, and P. Ning, “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. Z. Yu and Y. Guan, “A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks,” in Proc. SenSys, pp. 294-295, 2005.
10. W. Zhang and G. Cao, “Group Rekeying for Filtering False Data in Sensor Network: A predistribution and Local Collaboration-based Approach,” Proc. of INFOCOM, pp. 503-514, 2005.

허 수 만 (acaciasu@kut.ac.kr)

2007 공주대학교 컴퓨터공학과 학사
2007～현재 한국기술교육대학교 정보미디어학과 정보보호전공 석사

관심분야 : USN보안, 디지털 포렌식, 리버스 엔지니어링

서 희 석 (histone@kut.ac.kr)

2000 성균관대학교 산업공학과 학사
2002 성균관대학교 전기전자 및 컴퓨터공학과 석사
2005 (주)정보감리평가원 선임연구원
2005 성균관대학교 전기전자 및 컴퓨터공학과 박사
2005～현재 한국기술교육대학교 컴퓨터공학부 조교수

관심분야 : 네트워크 보안, 보안 시뮬레이션, 악성코드분석

이 동 영 (dylee@mail.mjc.ac.kr)

1993년 동아대학교 전자공학과(학사)
1993년～1997년 기아자동차 중앙기술연구소 연구원
1998년 성균관대학교 정보공학(석사)
2002년 성균관대학교 컴퓨터공학(박사)
2003년 2월～현재 명지전문대학 정보통신과 교수

관심분야 : 네트워크보안, 홈 네트워크, USN

김 태 경 (tkkim@stu.ac.kr)

1997년 2월 단국대학교 수학교육과 (이학사)
2001년 8월 성균관대학교 정보통신공학과 (공학석사)
2005년 8월 성균관대학교 전기전자및컴퓨터공학과 (공학박사)
2006년 3월～2008년 2월 서일대학 정보기술계열 정보전자전공 교수
2008년 3월～현재 서울신학대학교 교양학부 교수

관심분야 : 네트워크보안, 그리드 네트워크, USN