Proceedings of KFIS Autumn Conference 2007 Vol. 17, No. 2.

# 센서네트워크 보안 효율을 위한 퍼지로직 기반의 향상된 키분배 방법[1)]

# FKDM: Fuzzy-based improved Key Dissemination Method for Secure efficiency in Sensor Networks

김병희[1], 조대호[2]

[1] 경기도 수원시 장안구 성균관대학교 정보통신공학부
E-mail: bhkim@ece.skku.ac.kr
[2] 경기도 수원시 장안구 성균관대학교 정보통신공학부
E-mail: taecho@ece.skku.ac.kr

**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 Yu와 Guan은 Dynamic En-route Filtering(DEF) 방법을 제안 하였다. DEF는 인증키 재분배를 통하여 필터링 효율을 강화 시키지만, 키 분배 효율을 높일수록 인증키를 분배에 사용되는 에너지 소비가 커지는 문제점을 가지고 있다. 본 논문에서는 인증키 분배에 소비되는 에너지를 줄이면서 효율적인 키 분배를 위해 퍼지 시스템 기반의 키 분배 거리 결정 방법을 제안하였다.

**Key Words** : 센서네트워크, 허위보고서, 필터링, 퍼지, 인증키

## 1. 서 론

최근 무선 통신의 발전과 초미세 전자기계 시스템의 발전은 저 비용의 센서 네트워크 구성을 가능하게 하였다. 저 비용의 센서네트워크는 사람을 대신하여 위한한 군사 지역에 이용될 뿐만 아니라 유통관리, 생산 관리, 환경 및 재난 관리, 에너지 관리, 의료 및 건강 서비스, 지능형 교통시스템등 수많은 분야에 응용될 것으로 예측되고 있다 [1,2]. 이러한 무선 센서네트워크는 제한된 베터리 용량, 한정된 무선통신 범위 그리고 작은 메모리 공간을 가지고 있는 많은 센서노드들과 센서 네트워크를 인터넷과 같은 기존 통신 인프라와 연결하여 센서노드들이 센싱한 정보를 모아서 사용자에게 전달해주는 베이스 스테이션(Base station)으로 구성되어 있다 [3].

많은 센서네트워크 응용분야에서 센서노드는 개별 관리가 어려운 개방된 환경에 배치된다. 이런 특징으로 인해, 공격자는 센서노드를 물리적으로 쉽게 획득(compromising)할 수 있으며 획득한 센서노드(compromised node)를 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 걸러 내야하며, 걸러지지 않은 허위보고서는 베이스 스테이션에서 발견하고 제거해야 한다.

최근 이러한 허위 경고 공격을 막기 위해 몇몇의 필터링 기반 보안 기법이 제안되었다. 그 중 하나가 Yu와 Guan이 제안한 동적 여과 기법(DEF: Dynamic En-route Filtering) [4] 방법인데, DEF는 센서노드들이 배치된 후 센서 네트워크의 변화에 따라 인증키를 재분배 하여 필터링 효율을 최적화시키는 방법을 사용하고 있다. DEF 방법은 인증키 재분배를 통하여 제안된 다른 기법[5,6]에 비해 센서네트워크 변화에 능동적으로 대응할 수 있는 장점을 가지고 있다. 하지만 DEF의 인증키 재분배 단계에서

1) 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음. (IITA-2007-C1090-0701-0028)

최적의 인증키 분배 방법을 고려하지 않은 문제점을 가지고 있다. 만약 인증키 분배 거리를 크게 한다면, 효율적으로 인증키가 분배 되겠지만 인증키 분배 메시지를 전달하기 위해 많은 에너지를 소비하게 되는 문제점 발생하게 된다. 반면 작은 인증키 분배 거리는 인증키 분배를 위해 소비되는 에너지는 줄어들지만 인증키가 효율적으로 분배되지 못하는 문제점이 발생하게 된다.

본 논문에서는, 퍼지 로직을 이용하여 센서 네트워크 상황에 맞는 인증키 분배 거리를 결정하는 방법을 제안 하였다. 센서네트워크의 평균 에너지 레벨과 클러스터 헤드 노드(CH: Cluster Head)와 베이스 스테이션과의 거리를 고려하여 최적의 인증키 분배 거리를 결정하게 된다.

본 논문은 다음과 같이 구성된다. 2장에서는 허위 경고 공격(False Positive Attack)과 이를 방어하기 위해 제안된 DEF에 대한 간단한 설명과 연구 동기를, 3장에서는 인증키 분배 거리를 결정하기 위해 제안된 방법에 대한 설명을, 마지막 4장에서는 결론과 향후 연구 과제에 대해 설명할 것이다.

## 2. 공격모델과 DEF

### 2.1 허위 경고 공격(False Positive Attack)

많은 센서네트워크 응용분야에서 센서노드는 센서노드별 관리가 어렵고, 개방된 환경에 배치된다. 이러한 센서노드의 취약점을 이용하여 공격자들은 배치된 센서노드를 물리적으로 쉽게 획득할 수 있으며, 획득한 센서노드가 가지고 있는 인증키를 이용하여 허위보고서를 만들어 센서네트워크에 전송할 수 있다.

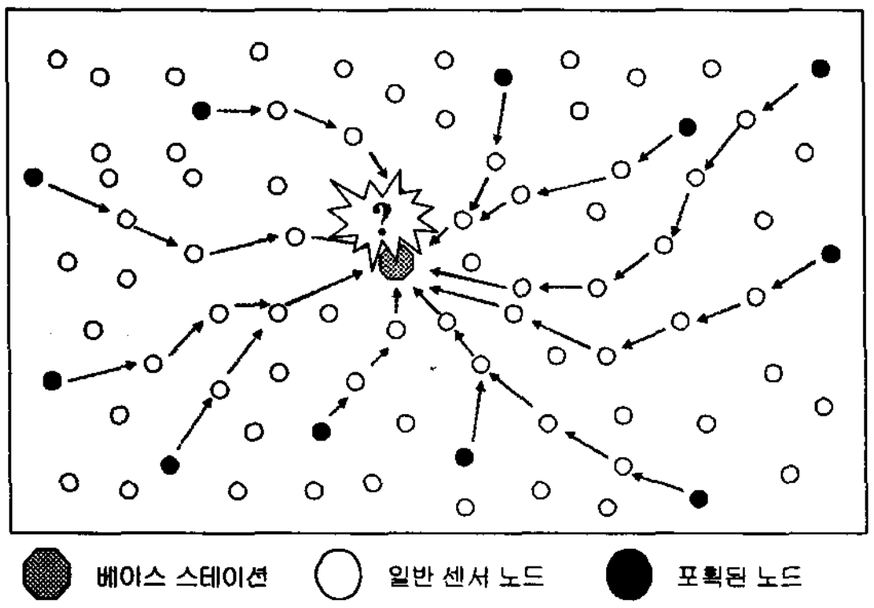


그림 1. 허위 경고 공격.

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.

### 2.2 동적 여과 기법(DEF: Dynamic En-route Filtering Scheme)

Yu와 Guan은 허위 경고를 일으킬 수 있는 허위보고서를 필터링 하기 위해 DEF 기법을 제안 하였다. DEF는 에너지 효율적인 면에서 다른 기법[5,6]에 비해 뛰어난 성능을 발휘하며 특히 규모가 큰 센서네트워크에서 보다 효율적이다. DEF는 *배치 전 단계(Pre-deployment phase)*, *배치 후 단계(Post-deployment phase)*, 그리고 *필터링 단계(Filtering phase)*로 구성되어 있다.

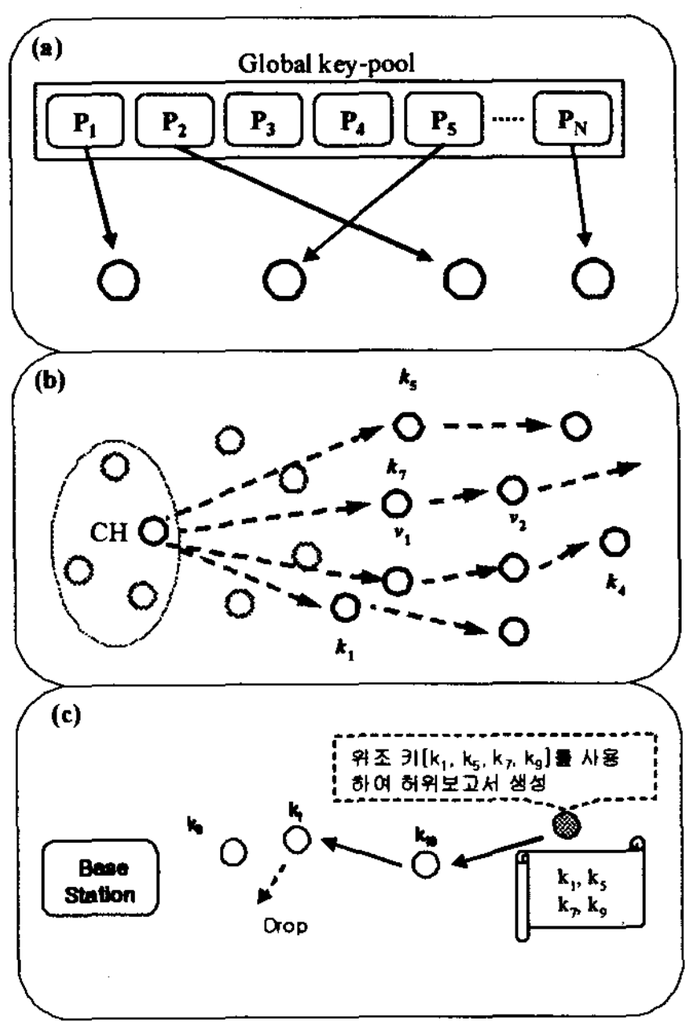


그림 2. DEF 구성 단계.

배치 전 단계(그림 2(a))에서 각각의 센서노드들은 글로벌 키 풀(Global key-pool)에서 인증키와 비밀 키를 랜덤으로 할당 받는다. 센서노드 수의 감소, 증가와 같은 센서네트워크에 변화가 발생하면 필터링 성능을 최적화시키기 위해 배치 후 단계(그림 2(b))를 실행하게 된다. 이 단계에서 센서 노드들은 자신이 가지고 있는 비밀키를 이용하여 인증키를 암호화하고 이를 CH로 보낸다. CH는 클러스터 지역 안에 있는 센서 노드들로부터 받은 암호화된 인증키를 분배하기 위해, 암호화된 인증키를 조합하여 키 분배 메시지를 생성하고, 생성한 키 분배 메시지를 센서노드들에 전송 한다. 키 분배 메시지를 받은 센서 노드들은 자신이 가진 비밀키와 같은 비밀키로 암호화된 인증키가 있는지 검사하여 없으면 다음 노드로 전송하고, 같

은 비밀키로 암호화된 인증키가 있다면 이를 해독하여 인증키를 획득한다. 센서네트워크에 관심 이벤트가 발생하면 이를 감지한 센서노드들은 자신이 가지고 있는 인증키를 이용하여 다른 센서노드와 협력하여 이벤트 리포터를 생성한다. 공격자는 획득하지 않은 센서노드의 인증키를 알 수 없기 때문에 위조 인증키를 만들어 허위보고서를 생성하여, 포획한 센서노드를 통해 허위보고서를 센서네트워크에 보내게 된다. 필터링 단계(그림 2(c))에서는 공격자에 의해 포획된 센서노드에서 만들어진 허위보고서를 필터링하여 걸러 낸다.

### 2.3 동기

DEF는 키 분배 메시지를 전달하기 위한 키 분배 거리를 고려하지 않았기 때문에 효율적으로 인증키를 분배하기 위해서는 키 분배 거리가 커야 한다. 하지만 키 분배 거리가 클수록 인증키 분배를 위해 많은 에너지가 소모되게 되는 문제점이 발생한다. 이러한 문제는 제한된 베터리 용량을 가지고 있는 센서 노드에게 치명적인 문제점이 될 수 있다. 그러므로 키 분배 거리는 센서네트워크 상황에 맞게 결정되어 에너지 소비를 줄여야 한다. 센서네트워크 상황에 맞는 키 분배 거리를 결정하기 위해, 퍼지를 이용한 키 분배 결정 방법을 제안하였다.

## 3. 퍼지를 이용한 인증키 분배 거리 결정 방법

### 3.1 가정 사항

- ▶ 베이스 스테이션은 센서 노드들에게 안전하게 메시지를 보낼 수 있는 메커니즘을 가지고 있다 (예: μTESLA [7]).
- ▶ 센서노드들은 관심지역에 배치된 후에 클러스터 지역을 자동으로 형성할 수 있는 메커니즘을 가지고 있다.

### 3.2 키 분배 거리를 결정하기 위한 퍼지로직

키 분배 거리를 결정하기 위해 퍼지로직에 사용하는 입력 파라미터는 센서네트워크의 에러지 레벨(ENERGY_LEVEL)과 베이스 스테이션과 CH와의 거리(DISTANCE)이다.

에너지 레벨(ENERGY_LEVEL): 센서 노드들은 교환이 용이하지 못한 제한된 용량의 베터리를 가지고 있다. 만약 센서네트워크의 에너지 레벨이 낮다면 인증키를 재분배 하는 것 보다 센서네트워크 수명을 유지해야 한다. 센서네트워크의 효율적인 관리를 위해서는 센서네트워크 에너지 레벨은 반드시 고려되어야만 한다.

베이스 스테이션과 CH의 거리(DISTANCE) : 베이스 스테이션과 CH와의 거리 역시 고려되어야만 한다. 만약 CH가 베이스 스테이션 가까이 있다면 키 분배를 위한 키 분배 메시지를 몇 홉만 보내면 될 것이다(그림 3(a)). 반면, 베이스 스테이션과 CH 거리가 멀다면 인증키를 분배하기 위해 센서노드들은 키 분배 메시지를 멀리 전달해야만 할 것이다 (그림 3(b)).

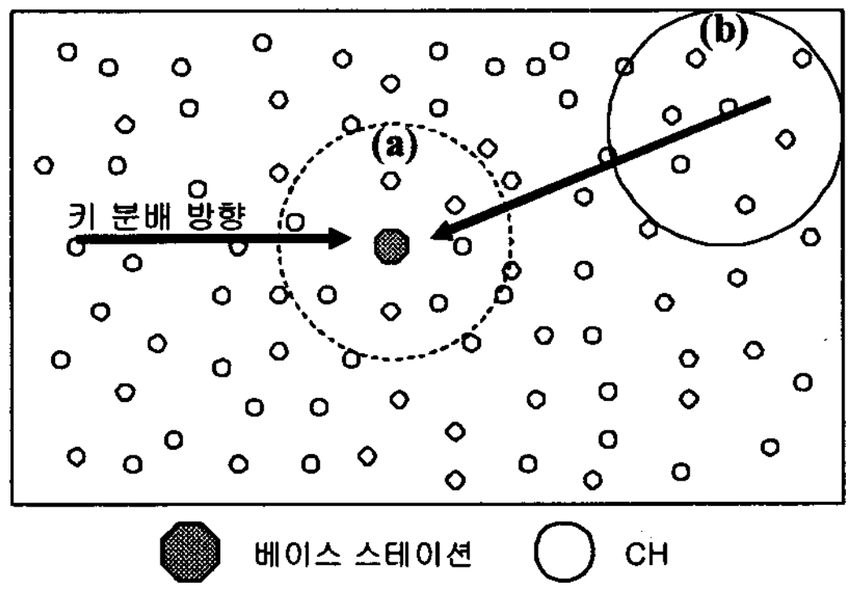


그림 3. 인증키 분배 방향.

퍼지를 이용하여 키 분배 거리를 결정하기 위한 입력 파라미터를 아래와 같이 정의하고 퍼지 멤버십 함수를 그림 4(a)와 (b)로 구성하였다.

ENERGY_LEVEL = {VL, L, E }

DISTANCE={N, AD, AW}

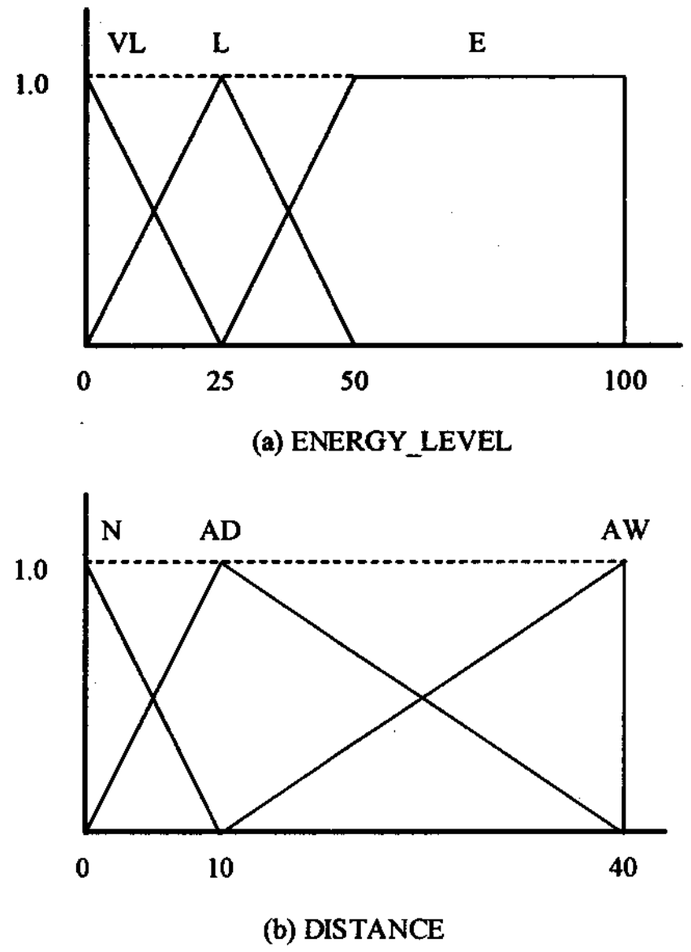


그림 4. 퍼지 입력 파라미터 멤버십 함수.

입력 파라미터를 이용하여 결정된 결과 키 분

배 거리는 아래와 같이 정의하고 퍼지 멤버십 함수를 그림 5와 같이 구성하였다.

DISSEMINATION_DISTANCE = {VS, S, ME, L, VL}

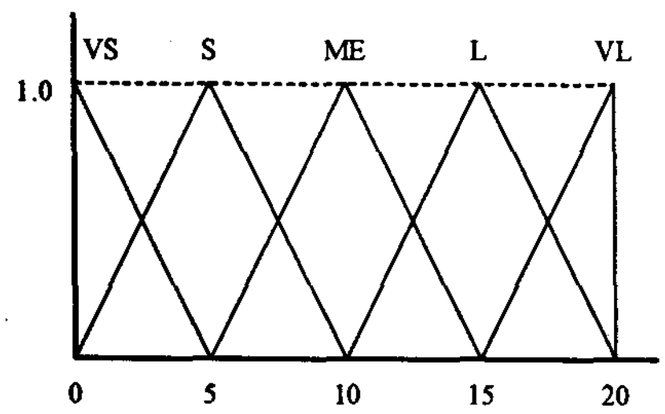


그림 5. 퍼지 결과 파라미터 멤버십 함수.

파라미터를 이용하여 키 분배 거리를 결정하기 위한 퍼지 규칙의 예를 표 1에 나타내었다.

표 1. 퍼지 규칙

| Rule # | IF | | THEN |
|---|---|---|---|
| | EL | D | DD |
| 01 | L | AD | S |
| 02 | L | A | ME |
| 03 | E | AD | L |
| 04 | E | A | VL |

### 3.3 동작 과정

제안한 퍼지기반 키 분배 거리 결정 방법에서 베이스 스테이션은 CH로부터 클러스터 지역 에너지 레벨과 베이스 스테이션과의 거리에 대한 정보가 담긴 메시지를 받게 된다. 베이스 스테이션은 CH로부터 받은 정보와 퍼지 시스템을 이용하여 키 분배 거리를 계산한다. 센서 네트워크에 변화가 발생하여 인증키 재분배가 필요하게 되면, 계산한 키 분배 거리 결과 값을 CH에 전달하여 인증키 재분배가 효율적으로 이루어 질 수 있도록 한다 (그림 6).

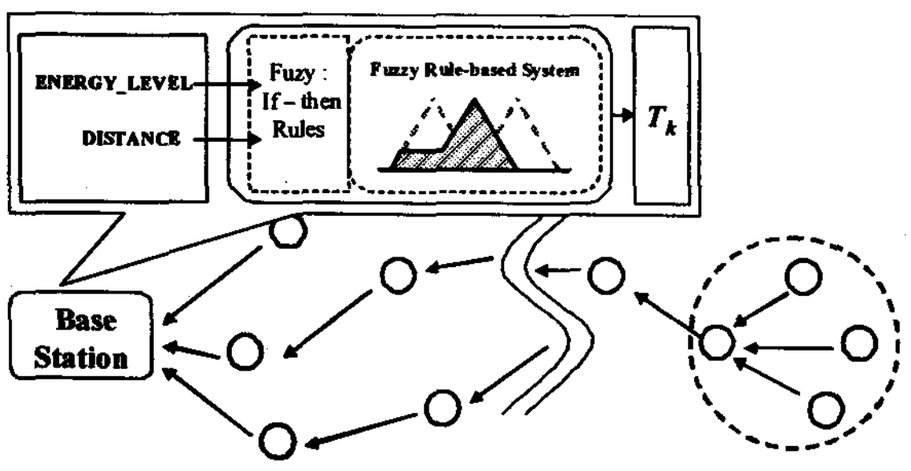


그림 6. 퍼지 기반 키 분배거리 결정 방법.

## 4. 결론 및 향후 과제

동적 여과 기법에는 고정된 키 분배 거리를 이용하여 인증키를 재분배하기 때문에 효율적인 인증키 분배가 이루어지지 않는 문제점을 가지고 있다. 이를 해결하기 위해 본 논문에서는 센서 네트워크 상황에 맞는 키 분배 길이를 결정하기 위해, 퍼지를 적용한 키 분배 결정 방법을 제안하였다. 향후 과제는 동적 여과 기법과 퍼지를 적용한 동적 여과 기법의 인증키 분배를 위한 에너지 소모량과 필터링 효율 등의 성능을 분석하기 위한 시뮬레이션을 수행하는 것이다. 그리고 동적 여과 기법에서 언제 인증키 분배가 이루어져야 하는지 결정 하는 방법을 연구하여 보다 향상된 동적 여과 기법을 제안 하고자 한다.

## 참 고 문 헌

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks," IEEE Commun. Mag, pp. 102-114, 2002.

[2] k. Akkaya, 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] Z. Yu, Y. Guan, "A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks," In Proc. Of SenSys, pp. 294-295, 2004.

[5] F. Ye, H. Luo, S. Lu, and L. Zhang "Statistical En-Route Filtering of Injected False Data in Sensor Networks," IEEE J. Sel. Area Comm. 23(4), pp. 839-850, 2005.

[6] S. Zhu, S. Setia, S. Jajodia, P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for filtering of Injected False Data in Sensor Networks," In Proc. of S&P, pp. 259-271, 2004.

[7] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, "SPINS: Security Protocols for Sensor Networks," Wirel. Netw., vol. 8, no. 5, pp. 521-534, Sep. 2002.