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

센서 네트워크에서 퍼지 로직과 가환 암호를 기반으로 하는 위조 보고서 여과 기법[1)]

A Forged Report Filtering Scheme in Sensor Networks Based on Fuzzy Logic and Commutative Cipher

이해영, 조대호

경기도 수원시 성균관대학교 정보통신공학부
E-mail: {sofware, taecho}@ece.skku.ac.kr

요 약

센서 네트워크에서 공격자는 훼손된 노드들 이용하여 위조 보고서를 네트워크에 주입할 수 있다. Yang과 Lu는 이러한 위조 보고서를 전달 중에 여과하기 위하여 가환 암호 기반 여과 기법을 제안하였다. 그러나 이 기법에서는 클러스터 헤드가 훼손된 경우에 위조 보고서를 전달 중에 여과할 수 없는 문제가 있다. 본 논문에서는 클러스터 헤드 훼손 여부에 관계없이 보고서를 전달 중에 여과할 수 있는 퍼지 로직 및 가환 암호 기반 위조 보고서 여과기법을 제안한다. 기본적으로 제안된 방법은 가환 암호를 기반으로 감지 보고서를 생성 및 검증하며, 보조 검증 수단으로 대칭 암호를 사용한다. 에너지 소비 절감을 위하여 퍼지 규칙 기반 시스템이 계산 비용이 큰 가환 암호 검증의 확률과 보조 검증 수단 사용 여부를 결정한다.

Key Words : 센서 네트워크, 위조 보고서 주입 공격, 퍼지 로직, 가환 암호, 보안

1. 서 론

센서 네트워크는 주위를 감시하는 수많은 작은 센서 노드와 감지 값을 수집하는 몇 개의 기지 노드(base station; 이하 BS)로 구성된다 [1]. 많은 응용 분야에서 센서 네트워크는 개방된 환경에 배포되므로 노드의 암호 키를 완전히 훼손하는 물리적 공격에 취약하다 [2]. 공격자는 훼손된 노드들을 사용하여 허위 경보뿐만 아니라 배터리로 구동되는 네트워크의 제한된 에너지 자원의 소진을 초래할 수 있는 위조 감지 보고서들을 네트워크에 주입할 수 있다(그림 1) [3]. 피해를 최소화하기 위하여 위조 보고서들은 가능한 한 빨리 전달 중에 여과되어야하고, 여과되지 못한 위조 보고서들은 후에 BS에서 여과되어야한다 [4]. 위조 보고서들을 전달 과정 중에 여과하기 위하여 연구자들은 대칭 암호 기반의 보안 기법들을 제안하고 있다. 각각의 기법들은 고유한 장점들을 가지고 있지만, 훼손된 노드의 수가 고정된 임계값을 초과하면 비효율적이거나 심지어 쓸모없게 될 수도 있다 [5]. 근본적인 이유는 이러한 기법들이 전달 중 여과 능력을 달성하기 위하여 대칭키를 공유하는 접근법을 따르기 때문이다. 센서 노드들 간의 대칭키 공유 없이 위조 보고서 주입 공격을 방어하기 위하여, Yang과 Lu는 가환 암호 기법 기반 전달 중 여과 기법(commutative cipher-based en-route filtering scheme; 이하 CCEF) [4]을 제안하였다. CCEF는 감지 보고서의 서명과 검증에 가환 암호를 사용함으로써 대칭 암호 기반 기법들보다 노드 훼손에 대한 높은 보안 강도를 제공할 수 있다. 그러나 CCEF에서는 클러스터 헤드(cluster head; 이하 CH)가 훼손된 경우 위조 보고서가 전달 중에 여과되지 않는 문제가 있다. 본 논문에서 CCEF의 노드 훼손에 대한 높은 보안 강도를 유지하면서도 훼손된 CH가 주입한 위조 보고서를 전달 중에 보고할 수 있는 퍼지 로직 및 가환 암호 기반 여과 기법(fuzzy logic and commutative cipher-based filtering scheme; 이하 FCCF)을 제안한다. 먼저 통계적 전달 중 여과 기법(statistical en-route filtering scheme; 이하 SEF) [3]의 대칭키 임의 분배 방법을 CCEF에 적용하여 훼손된 CH의 위조 보고서를 전달 중에 여과할 수 있는

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

가환 암호 기반 확률적 여과 기법(commutative cipher-based probabilistic filtering scheme; 이하 CCPF)을 제안한다. 그리고 CCPF의 문제점인 높은 에너지 소비를 개선하기 위하여, 퍼지 규칙 기반 시스템이 허위 트래픽 비율, CH까지의 거리, 그리고 에너지 수준을 고려하여 적응적으로 CCEF와 CCPF 중 하나를 선택하는 FCCF를 제안한다.

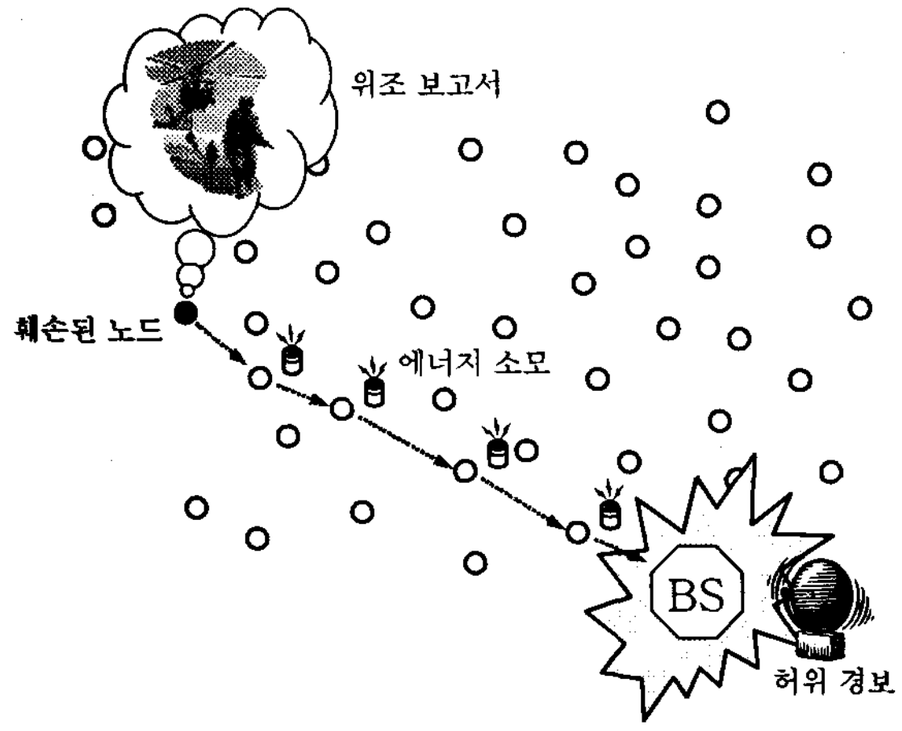

그림 1. 위조 보고서 주입 공격.

2. 가환 암호 기반 여과 기법(CCEF)

Yang과 Lu는 센서 노드간의 대칭키 공유 없이 위조 보고서 주입 공격을 방어하기 위하여 CCEF [4]를 제안하였다. CCEF는 감지 보고서의 서명과 검증에 임의의 메시지 M과 임의의 두개의 키 K_1과 K_2에 대하여,

$$CE(CE(M,K_1),K_2) = CE(CE(M,K_2),K_1), \quad (1)$$

를 만족하는 가환 암호 CE를 사용한다. 그 결과 CCEF는 대칭키 기반 보안 솔루션들보다 노드 훼손에 대한 높은 보안 강도를 제공할 수 있다. 각 노드의 배포 전에 BS와만 공유되는 유일한 키가 노드에 탑재된다. 각 세션에 대하여 BS는,

$$CE(CE(M,K_s),K_w) = M, \quad (2)$$

을 만족하는 두개의 키 K_s와 K_w를 준비한다. 그리고 BS는 관심 지역의 임의의 한 노드를 CH로 선택하고 CH를 향하여 질의를 보낸다. 각 질의는 CH의 키로 암호화한 K_s와 평문의 K_w를 포함한다. 전달 노드들은 추후 보고서 검증을 위하여 K_w를 저장한다(그림 2(가)). CH와 이웃 노드들이 협력하여 질의에 대한 보고서를 생성한다. 보고서는 CH가 K_s를 사용하여 생성된 메시지 검증 코드(message authentication code; 이하 MAC)와 이웃 노드들이 그들의 키들로 생성한 MAC들로 서명된다. 보고서는 BS를 향해 질의가 전달된 역방향 경로를 통하여 전달된다. 모든 전달 노드들은 식 (1)과 K_w를 사용하여 보고서를 검증한다(그림 2(나)). 가환 암호 계산 비용은 대단히 크므로, CCEF는 전달 노드가 검증 확률 P,

$$P = 1 / a^h, \quad (3)$$

를 가지고 보고서를 검증하는 확률적 접근법을 사용한다. 여기서 a는 네트워크 설계자가 결정하는 보안 파라미터이며, h는 BS와 CH 사이의 홉 수이다. CCEF에서 공격자는 CH를 훼손하여 K_s를 획득할 수 있다. 이를 사용하여 생성한 위조 보고서들은 전달 중에 여과되지 않으므로, 전달된 노드들의 제한된 에너지 자원의 고갈을 유발할 수 있다는 문제점이 있다.

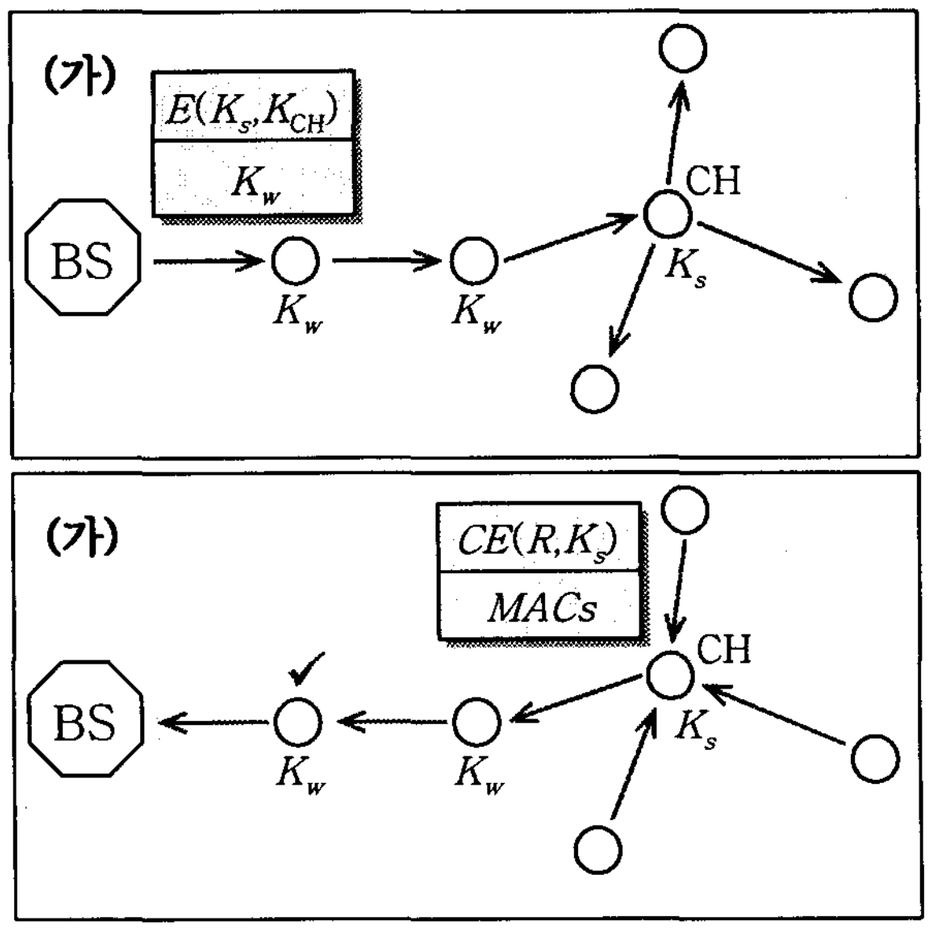

그림 2. 가환 암호 기반 여과 기법.

3. 퍼지 로직 및 가환 암호 기반 위조 보고서 여과 기법(FCCF)

3.1 가정

우리는 수많은 센서 노드들로 구성된 큰 규모의 센서 네트워크를 고려한다. 센서 노드들은 가환 암호 계산이 가능하다. BS는 허위 트래픽 비율, CH에서 BS까지의 홉 수, 전달 노드들의 에너지 수준을 알거나 추측할 수 있다. 허위 트래픽 비율을 얻기 위하여 폐기된 보고서의 수를 기록하고 이를 BS에 보고하는 훼손에 저항력이 있는 노드들을 배포할 수 있다.

각 노드들은 네트워크의 일정 지역을 커버할 수 있을 것이다.

3.2 가환 암호 기반 확률적 여과 기법 (CCPF)

BS는 k개의 키를 가지며 p개의 중복되지 않는 구획으로 나누어지는 전역 키 풀을 관리한다. 모든 키는 유일한 키 색인을 가진다. 모든 센서 노드는 배포 전에 임의로 선택된 전역 키 풀의 하나의 구획에서 n개($n < k / p$)의 키들과 이들의 키 색인들을 탑재한다. 각 노드는 BS와만 공유하는 유일한 키를 추가적으로 탑재한다. 각 세션에 대하여 BS는 식 (2)를 만족하는 두개의 키 K_s와 K_w를 준비한다. 그리고 관심 지역의 임의의 한 노드들 CH로 선택하고 질의를 구성한다. 질의에는 CH의 키로 암호화한 K_s와 평문의 K_w가 포함된다. BS는 CH에 여러 홉을 거치면서 전달되도록 질의를 내보낸다. 질의에 대한 응답으로 감지 보고서가 CH와 이웃 노드들의 협력으로 생성된다. 보고서는 1) CH가 K_s를 사용하여 생성한 MAC, 2) 참여 노드들 중 t개의 노드들이 전역 키 풀의 각기 다른 구획의 키들로 생성한 t개의 MAC들과 키들의 키 색인들, 3) t개의 노드들이 BS와만 공유하는 키들로 생성한 MAC들을 포함한다. 보고서는 질의가 전달된 경로의 역으로 BS에게 전달된다. 전달 노드가 보고서를 받으면 t개의 MAC들과 서로 다른 구획의 키 색인들이 있는지 확인한다. t보다 적은 MAC들이나 키 색인들이 있거나, 동일 구획에서 한개 이상의 키 색인이 있다면 보고서는 버려진다. 만약 노드가 t개의 키 색인들이 가리키는 키들 중 하나를 가지고 있다면, 이를 사용하여 보고서를 검증한다. 만약 노드가 키들 중 하나도 가지고 있지 않다면 식 (3)의 확률 P를 가지고 K_w를 사용하여 보고서를 검증한다. 검증에 실패하면 보고서는 폐기되며, 성공하면 BS를 향하여 전달한다. 보고서는 BS에서 마지막으로 검증된다. CCPF는 보조 검증 수단으로 사전에 임의 분배된 대칭키를 사용하므로 CH 훼손 여부에 관계없이 위조 보고서들이 전달 중에 여과할 수 있다. 또한 두 가지 검증 수단 사용으로 CCEF보다 조기에 위조 보고서들의 탐지가 가능하여, 위조 보고서들의 전달에 의한 심각한 에너지 소비를 줄일 수 있다. 그러나 정상 보고서의 경우, 이러한 이중 검증으로 인하여 추가적인 에너지 소비가 발생하는 문제가 있다.

3.3 퍼지 로직에 의한 여과 기법 전환

각 세션에 대하여 BS는 퍼지 규칙 기반 시스템을 사용하여 현 네트워크 상황에 대한 CCEF와 CCPF의 적합도를 평가한다. 적합도 평가에는 허위 트래픽 비율, BS와 CH 간의 홉 수, 에너지 수준이 고려된다(그림 3). BS가 CH로 보내는 질의에는 CCEF와 CCPF 중 어떤 여과 기법을 사용하여 보고서를 검증할 것인지가 포함된다. CCPF는 이중 검증으로 CCEF보다 위조 보고서를 조기에 탐지할 수 있으므로, 허위 트래픽 비율이 높은 경우 에너지를 절약할 수 있다. 그러나 허위 트래픽 비율이 낮은 경우에는 중복 검증으로 CCEF보다 많은 에너지를 소비한다. 그러므로 여과 기법 적합도 평가에는 허위 트래픽 비율을 고려해야 한다. CH부터 BS까지의 거리가 가까운 경우에는 위조 보고서 전달보다 CCPF의 이중 검증에 더 많은 에너지를 소비할 수 있으므로 가능한 한 검증을 피하는 편이 나을 것이다. 이에 반해 CH와 BS 사이의 거리가 먼 경우에는 보고서 검증보다 위조 보고서 전달에 더 많은 에너지가 소비될 수 있으므로 가능한 한 빨리 검증하는 편이 나을 것이다. 그러므로 여과 기법 적합도 평가에는 CH와 BS간의 거리를 고려해야한다. 에너지는 센서 네트워크에서 반드시 고려되어야만 하는 가장 중요한 자원이다. 일반적으로 센서 노드들을 제한된 능력을 가지고 배포 후 주의 받지 않으므로 전원의 공급이나 교체가 제한된다 [1]. 전달 노드들의 에너지 수준이 낮은 경우, CCPF보다 CCEF를 선택하여 가능한 한 검증을 회피하는 편이 네트워크의 수명을 연장할 수 있을 것이다. 그러므로 여과 기법의 적합도 평가에는 에너지 수준이 고려되어야 한다. 이러한 퍼지 규칙 시스템에 의한 여과 기법 전환은 노드 훼손에 대한 CCPF의 높은 보안 강도를 유지하면서도 CCEF의 상대적으로 높은 에너지 효율을 제공할 수 있다. 결과적으로 대상 네트워크에게 충분한 보안 강도를 제공하면서 네트워크의 수명을 늘릴 수 있을 것이다.

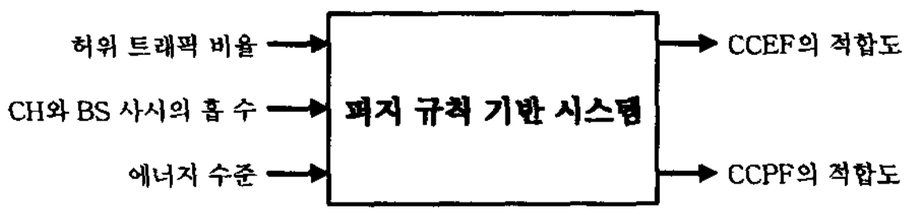

그림 3. 퍼지 규칙 기반 시스템.

3.4 퍼지 로직 설계

그림 4는 입력 매개변수들과 출력 변수들에 대한 멤버십 함수들이다. 퍼지 변수들에서의 레이블들은 다음과 같다.

- 허위 트래픽 비율 = {낮음, 보통, 높음}
- CH와 BS 사이의 홉 수 = {가까움, 보통, 멈}
- 에너지 수준 = {매우 낮음, 낮음, 충분함}
- 여과 기법의 적합도 = {매우 낮음, 낮음, 보통, 높음, 매우 높음}

표 1은 제안된 퍼지 규칙 기반 시스템의 퍼지 규칙들의 일부이다.

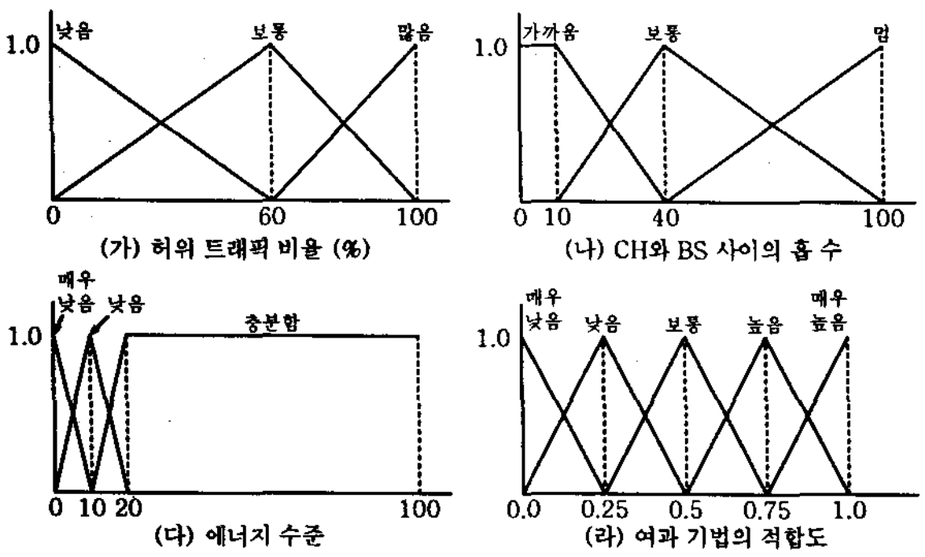

그림 4. 퍼지 멤버십 함수들.

표 1. 퍼지 규칙들.

규칙 번호	허위 트래픽 비율	CH-BS 사이의 홉 수	에너지 수준	FCCF	CCPF
1	높음	멈	충분함	매우 높음	매우 낮음
2	높음	멈	낮음	보통	보통
3	높음	멈	매우 낮음	매우 낮음	매우 높음
4	높음	보통	충분함	높음	낮음
5	높음	보통	낮음	낮음	높음

3.5 여과 효율

CCPF에서 전달 노드가 대칭 암호를 사용하여 보고서를 검증할 수 있는 확률 P_p는,

$$P_P = (t / p)\cdot(n\cdot p / k) = t\cdot n / k, \quad (4)$$

이며, 가환 암호를 사용하여 보고서를 검증할 수 있는 확률은 식 (3)과 같다. CCPF에서는 대칭 암호를 사용하여 검증할 수 있는 경우, 가환 암호를 사용하는 검증은 수행하지 않으므로, CCPF에서 한 노드가 보고서를 검증할 수 있는 확률 P_{CCEF}는,

$$P_{CCEF} = P_p + (1 - P_P)\cdot P \quad (5)$$

으로 계산할 수 있다. 만약 $n = k / p$이고 $t = p$라면, $P_P = 1$이 되어 항상 대칭 암호만을 사용하여 보고서를 검증할 것이므로 CCEF의 노드 훼손에 대한 높은 보안 강도의 이점을 유지할 수 없다. 그러므로 CCEF의 높은 보안 강도를 유지하면서도 대칭 암호의 검증이 적절하게 발생할 수 있도록 P_P를 선택하는 것이 매우 중요하다.

4. 결론 및 향후 과제

본 논문에서 CCEF의 노드 훼손에 대한 높은 보안 강도를 유지하면서도 훼손된 CH가 주입한 위조 보고서를 전달 중에 보고할 수 있는 FCCF를 제안하였다. 먼저 SEF의 대칭키 임의 분배 방법을 CCEF에 적용하여 훼손된 CH의 위조 보고서를 전달 중에 여과할 수 있는 CCPF를 제안하였으며, CCPF의 높은 에너지 소비를 개선하기 위하여, 퍼지 규칙 기반 시스템이 허위 트래픽 비율, CH까지의 거리, 그리고 에너지 수준을 고려하여 적응적으로 CCEF와 CCPF 중 하나를 선택하는 FCCF를 제안하였다. 추후 시뮬레이션을 통하여 FCCF를 최적화할 예정이며, 적응형 보안 매개변수 결정 기법 [6]과의 결합을 통하여 보안 강도를 유지하면서도 에너지 소비를 더욱 줄일 수 있는 방법을 연구할 것이다. 또한 적절한 검증 확률 P_P를 결정하는 방법에 관하여 연구할 예정이다.

참 고 문 헌

[1] S.H. Chi and T.H. Cho, "Fuzzy Logic Based Propagation Limiting Method for Message Routing in Wireless Sensor Networks," Lect. Notes in Comput. Sci., Vol. 3983, pp. 58-64, 2006.

[2] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," Proc. SenSys, pp. 255-265, 2003.

[3] 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.

[4] H. Yang and S. Lu, "Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks", Proc. VTC, pp. 1223-1227, 2003.

[5] W. Zhang and G. Cao, "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach", Proc. INFOCOM, pp. 503-514, 2005.

[6] H.Y. Lee and T.H. Cho, "Fuzzy Security Parameter Determining Method for the Commutative Cipher Based Filtering in Sensor Networks", Lect. Notes in Comput. Sci., Vol. 4706, pp. 573-583, 2007.