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

퍼지 논리를 이용한 센서 네트워크에서의 임계값 기반 여과 기법[1)]

Threshold-Based En-Route Filtering in Sensor Networks using Fuzzy Logic

문수영[1], 조대호[2]

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

요 약

대부분의 센서 네트워크에서 센서 노드들은 열린 환경에서 독립적으로 동작하므로 보안 공격에 취약하다. 허위 보고서 삽입 공격에서 공격자는 허위 경보를 발생시키거나 혹은 네트워크 내 에너지의 고갈을 목적으로 포획된 노드들을 통해 허위 보고서를 네트워크에 삽입한다. 이러한 허위 보고서를 조기에 검출, 제거하기 위해 많은 여과 기법들이 제안되었다. 가환 암호 기반 여과 기법에서 각각의 중간 노드는 확률에 기반 하여 보고서 인증을 수행한다. 따라서 허위 보고서가 여과되지 않거나 정상 보고서가 여러 번 인증 받을 가능성이 있다. 또한 네트워크의 상태 변화에 적응하기 어렵다. 본 논문은 퍼지 논리를 이용한 무선 센서 네트워크에서의 임계값 기반 여과 기법을 제안한다.

Key Words : Wireless Sensor Networks, Fuzzy Logic, False Reports, Filtering Scheme

1. 서 론

센서 네트워크는 감지, 처리, 전송 기능을 가지고 있는 작고 저렴한 센서 노드들로 이루어져 있다 [1,2]. 센서 네트워크에서 센서 노드들은 일반적으로 열린 환경에서 독립적으로 동작하기 때문에 보안 공격에 취약하다 [3]. 허위 보고서 공격에서 공격자는 훼손된 노드를 통하여 네트워크 내에 허위 보고서를 삽입시킨다. 이러한 허위 보고서는 허위 경보를 발생시키거나 네트워크 내 노드들의 에너지를 고갈시키게 된다.

이러한 허위 보고서를 조기에 검출, 제거하기 위한 목적으로 센서 네트워크에서의 허위 보고서 여과 기법들이 제안되었다. 가환 암호 기반 여과 기법 (CCEF: Commutative Cipher based En-Route Filtering scheme) [4] 에서 베이스 스테이션 (BS: Base Station)은 두 개의 서로 다른 키를 이용하여 선택된 노드와의 세션 (session)을 생성한다. 이벤트가 발생하면 선택된 노드는 이웃 노드들과 협동하여 보고서를 생성한 후 중간 노드들을 통해 BS로 전송한다. 중간 노드들은 가환 암호 방식을 사용하여 미리 정해진 확률에 따라 보고서를 검증하고 허위 보고서인 경우 제거하게 된다.

CCEF에서 개별 중간노드는 확률에 기반 하여 독립적으로 보고서 검증 여부를 결정한다. 따라서 네트워크 내에서 여과 연산이 필요 이상으로 여러 번 수행되거나 한 번도 수행되지 않을 가능성이 존재한다. 따라서 비효율적인 에너지 소모가 발생하게 된다. 이러한 이유에서 본 논문에서는 퍼지 논리를 사용한 센서 네트워크에서의 임계값 기반 여과 기법을 제안한다. 제안 방식에서 개별 중간 노드는 0에서 1 사이의 적합도 (Fitness Value)를 가지고 BS는 이 값과 임계값을 기준으로 여과 연산을 수행할 노드들을 결정하게 된다.

본 논문의 나머지 섹션의 구성은 다음과 같다. 섹션 2에서는 CCEF에 대하여 간략하게 소개한다. 섹션 3에서는 제안 기법에 대한 자세

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

한 설명을 한다. 섹션 4는 제안 기법의 성능을 CCEF와 비교하여 예측한다. 섹션 5에서는 결론을 내린다.

2. 가환 암호 기반 여과 기법 (CCEF)

CCEF에서 센서 노드들은 가환 암호를 사용하여 보고서의 생성과 인증을 한다. 가환 암호 (CE) 는 암호 방식의 하나로 임의의 메시지 M과 두 개의 서로 다른 키 K_1과 K_2에 대해 다음과 같은 수식을 만족시킨다.

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

CCEF에서의 가정은 다음과 같다. 센서 노드들은 초기 배치 후 움직이지 않으며 제한된 메모리와 에너지 자원, 감지 범위를 가진다. 센서 노드들은 각자 고유한 키와 ID를 할당 받는다. 센서 노드들은 네트워크 내 위치 정보 컴포넌트로부터 자신의 위치 정보를 획득할 수 있다. 네트워크는 요청-응답 형식으로 동작한다 [4].

CCEF에서 네트워크의 동작은 초기화 단계, 세션 설정 단계, 보고서 생성 단계, 중간 여과 단계, BS 검증 단계, 그리고 세션 유지 및 종료 단계의 6 단계로 이루어진다. 초기화 단계에서는 각 노드가 위치 정보 컴포넌트로부터 자신의 위치 정보를 획득하여 BS에 보고한다. 세션 설정 단계에서는 BS가 관심 지역 내의 임의의 노드를 클러스터 헤더 (CH: Cluster Header) 노드로 선정하고 세션을 생성하기 위해 두 개의 키 K_s 와 K_w를 준비한다. K_s 와 K_w는 다음의 식을 만족한다.

$$CE(M,K_w)=CE^{-1}(M,K_s) \quad (2)$$

CE^{-1}은 가환 암호 복호화 연산을 의미한다.

K_s는 세션 키로 보고서를 생성하는데 사용된다. K_w는 증명 키 (witness key)로 보고서를 검증하는데 쓰인다. 그 후 BS는 CH 노드에게 요청 메시지를 전송한다. 요청 메시지는 1) 요청 ID (QID), 2) CH 노드 ID , 3) CH 노드의 고유키로 암호화된 세션 키 ($\{K_s\}K_{CH}$), 4) 증명키의 4 부분으로 이루어진다. 요청 메시지를 전달하는 중간 노드들은 추후 보고서 검증을 위해 요청 ID와 증명 키 쌍을 메모리에 저장하고 다음 노드로 전달한다. 요청 메시지를 수신한 CH 노드는 세션 키를 복호화하고 이웃 노드들에 보고서를 전달한다. 보고서 생성 단계에서 CH 노드는 이웃 노드들과 협력하여 최종 보고서를 생성한다. 최종 보고서는 두 개의 메시지 인증 코드 (MAC: Message Authentication Code)를 포함한다. 세션 MAC은 세션 키를 이용하여 이벤트 정보를 가환 암호 방식으로 암호화하여 만들어진다. 노드 MAC은 CH 노드의 이웃 노드들로부터 받은 MAC들을 압축하여 만들어진다. 최종 보고서는 1) 요청 ID (QID), 2) 이벤트 정보 (R), 3) 세션 MAC (MAC_{Ks}), 4) 노드 MAC (NMAC)으로 구성된다. CH 노드는 최종 보고서를 중간 노드들을 통해 BS에게 전달한다. 중간 여과 단계에서 개별 중간 노드는 보고서의 요청 ID에 대응하는 {요청 ID,증명 키} 쌍이 저장되어 있는지 확인하여 없으면 해당 보고서를 삭제하고 일치하는 쌍이 있다면 가환 암호 방식을 이용해 다음에 오는 수식과 같이 보고서를 검증하게 된다.

$$CE(CE(R,K_s),K_w)=R \quad (3)$$

이 때 가환 암호 방식은 에너지 소모가 크기 때문에 미리 정해진 확률에 기반 하여 보고서 검증을 수행할 것인지를 결정하게 된다. 이 확률은 보안 매개 변수 (security parameter) α와 BS에서 CH 노드까지의 홉 수 (hop count) h에 의해 정해진다.

$$P=\frac{h}{\alpha} \quad (4)$$

식 (4)에서 알 수 있듯이 CCEF에서 중간 노드들의 여과 연산 수행 여부는 보안 매개 변수 α에 크게 좌우 된다. α 값이 작을 경우 검출 강도는 높아지지만 네트워크의 오버헤드가 늘어나며 α 값이 클 경우 네트워크의 오버헤드는 줄어드나 허위 보고서 검출 강도가 낮아지게 되는 트레이드-오프 (trade-off) 관계를 가지고 있다 [5].

3. 제안 기법

3.1 가정

본 논문에서 제안 기법은 다음과 같은 가정을 갖고 있다. 노드들은 초기 배치 후 움직이지 않는다. 또한 제한된 메모리와 에너지 자원, 그리고 좁은 감지 범위를 갖는다. 노드들은 고유키를 할당 받고 위치 정보를 획득할 수 있

다. 노드들은 충분히 조밀하게 배치되어 이웃 노드들과 협력 하에 보고서를 생성할 수 있다. BS는 네트워크 내 허위 보고서의 비율과 노드들의 잔여 에너지를 추정할 수 있다. 네트워크는 BS가 CH 노드에게 요청 메시지를 보내고 CH 노드가 BS에게 보고서를 보내는 방식으로 동작한다. 또한 네트워크의 상태는 동적으로 변화한다. 예를 들어, 네트워크 내 허위 보고서의 비율은 시간에 따라 변할 수 있다.

3.2 동기

CCEF 방식에서 개별 노드는 확률에 따라 독립적으로 보고서 검증을 수행하므로 보고서에 따라 필요 이상의 여과 연산을 거치거나 한 번도 거치지 않을 수 있다. 정상 보고서의 경우는 중간에 검증될 필요가 없으며 허위 보고서의 경우 중간 노드에서 적어도 한 번 검증되어야 한다. 허위 보고서를 여과하고 동시에 불필요한 에너지 소모를 줄이기 위해서는 적은 수의 노드가 여과 기능을 수행하는 것이 유리하다. 확률 기반 여과 기법에서는 여과 연산의 횟수를 제한하기가 어렵기 때문에 임계값을 기반으로 하여 여과 노드를 지정하는 것이 효율적이다.

3.3 개요

제안 기법은 기존의 CCEF와 비교하여 세션 설정 단계와 중간 여과 단계에서만 차이점을 가진다. 세션 설정 단계에서 BS는 관심 지역 내 CH 노드를 선택한 후 BS에서 CH 노드까지의 경로 내 노드들에 대해서 퍼지 논리를 사용하여 여과 기능을 수행할 노드 (여과 노드)로서의 적합도를 계산한다. 그 다음 BS는 임계값을 기준으로 해당 경로 내 여과 노드를 최대 2개 설정하여 중간 노드들을 통해 CH 노드에게 요청 메시지를 보낸다. 요청 메시지는 1) 요청 ID, 2) CH 노드 ID, 3) CH 노드 키로 암호화된 세션 키(K_s), 4) 증명 키 (K_w), 그리고 5) 여과 노드들의 ID 집합으로 구성된다. 요청 메시지를 전달하는 중간 노드들은 {요청 ID, CH 노드 ID}의 쌍을 저장한다. 그리고 자신의 ID가 여과 노드들의 ID 집합에 속하는지 확인하여 속하면 앞으로 수신할 보고서에 대해 여과 연산을 준비한다.

보고서 생성 후 CH 노드가 중간 노드들을 통해 BS로 보고서를 전송하면 중간 노드들은 보고서 내 요청 ID에 해당하는 {요청 ID, CH 노드 ID} 의 쌍이 존재하는지 확인하고 없으면 보고서를 삭제한다. 해당 쌍이 존재하는 경우 자신이 여과 노드이면 가환 암호를 이용하여 여과 연산 (보고서 인증) 을 수행한다.

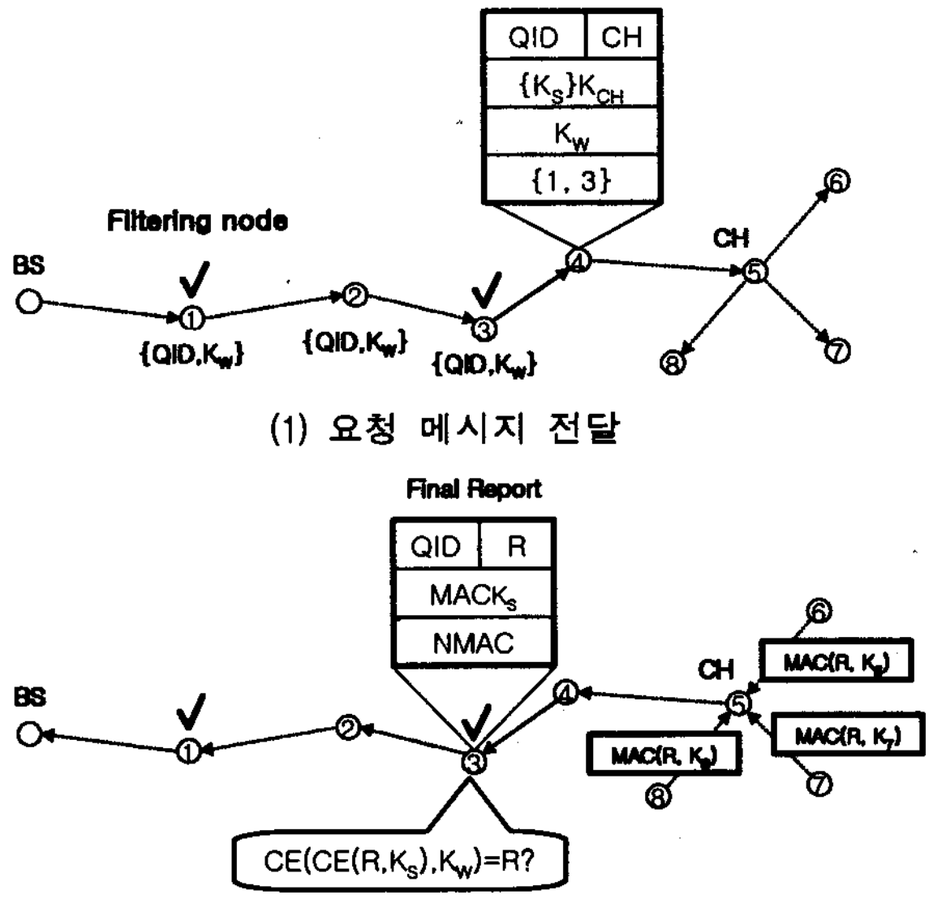

그림 1. 제안 기법 동작 개요

3.3 인자

중간 노드의 여과 노드로서의 적합도를 계산하기 위한 퍼지 함수의 인자로는 1) 각 노드의 에너지 (NE: NODE ENERGY), 2) 보고서 생성 과정에 참여하는 이웃 노드의 수 (NM: NUM MAC), 3) 네트워크 내 허위 보고서의 비율 (FTR) 이 있다.

노드 에너지가 적거나 보고서 생성 과정에 참여하는 이웃 노드의 수가 많은 경우, 또는 네트워크 내 허위 보고서의 비율이 낮은 경우는 적합도가 낮아지게 된다. 하지만 노드 에너지가 충분하고 보고서 생성에 참여하는 이웃 노드의 수가 적고 네트워크 내 허위 보고서의 비율이 높은 경우는 적합도가 커지게 된다.

3.4 퍼지 논리 설계

제안 기법에서 각 노드의 잔여 에너지와 허위 보고서 비율은 추정 값이기 때문에 오차를 가지고 있다. 또한 주어진 인자의 값은 기준에 따라 크고 작음을 다르게 판단할 수 있다. 이러한 불확실성과 애매성 때문에 복잡한 계산 없이 최적의 해를 구하기 위해 퍼지 논리가 필

요하다. 제안 기법에서 퍼지 함수의 인자와 결과값 (적합도) 에 대한 멤버십 함수는 다음과 같다.

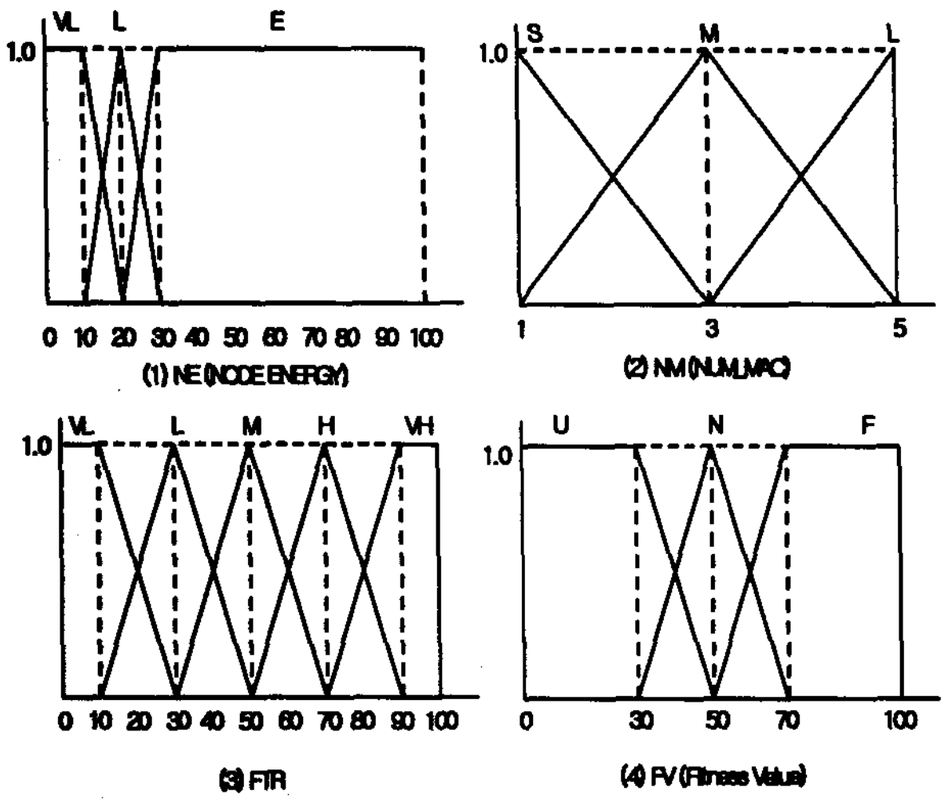

그림 2. 멤버십 함수

표 1은 해당 퍼지 함수의 IF-THEN 규칙을 보여준다.

표 1. IF-THEN 규칙

Rule#	NE	NM	FTR	FV
1	VL	S	VL	U
15	VL	L	VH	U
25	L	M	VH	F
31	E	S	VL	U
42	E	L	L	N
45	E	L	VH	F

4. 성능 비교

CCEF 방식과 제안 방식의 성능을 허위 보고서와 정상 보고서에 대한 평균 에너지 소모량으로 나누어 예측하여 비교해 보면 표 2와 같다.

표 2. 보고서 하나에 대한 평균 에너지 소모

	정상 보고서	허위 보고서
CCEF	$h \cdot e_t + \frac{1}{a} \cdot e_a$	$ah \cdot e_t + e_a$
제안 방식	$h \cdot e_t + fc \cdot e_a$	$AH \cdot e_t + e_a$

표 2에서 e_t는 MAC을 포함한 메시지를 한 홉 전송하는데 드는 에너지이며 e_a는 한 번의 가환 암호 연산에 필요한 에너지이다. a와 h는 각각 보안 매개 변수와 해당 경로의 홉 수를 의미한다. 제안 기법에서 fc 는 정상 보고서가 인증 받는 횟수이며 AH는 허위 보고서가 진행하는 평균 홉 수를 의미한다. a=0.25 이고 h=20 인 경우 fc<4 이고 AH<5 이면 제안 기법이 CCEF 보다 에너지 소모를 적게 하게 된다. CH 노드로부터 근접한 위치에 여과 노드를 지정함으로써 fc와 AH 값을 모두 줄일 수 있고 결과적으로 에너지 소모를 줄일 수 있다.

5. 결론

본 논문에서는 허위 보고서 여과 기법의 하나인 CCEF의 동작 과정을 분석하고 확률 기반 여과 방식의 문제점을 보완하는 임계값 기반 여과 방식을 제안하였다. 앞으로의 과제는 제안된 방식의 성능을 증명할 수 있는 시뮬레이션을 수행하고 기존의 여과 방식들과 비교하는 것이다.

참 고 문 헌

[1] I. F. Akyldiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci., "A Survey on Sensor Networks," IEEE Wireless Communication Magazine, Vol. 40, no. 8, pp. 102-116, 2002.

[2] J.N. Al-Karaki, and A.E. Kamal, "Routing techniques in wireless sensor networks: a survey," IEEE Wireless Communication Magazine, Vol. 11, no. 6, pp. 6-28, 2004.

[3] F. Ye, H. Luo, S. Lu, and L. Zhang, "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, 2005.

[4] H. Yang and S. Lu, "Commutative Cipher Based En-route Filtering in Wireless Sensor Networks," IEEE in Proc. of VTC, pp. 1223-1227, 2004.

[5] H. Y. Lee, and T.H. Cho "Fuzzy Security Parameter Determining Method for the Commutative Cipher Based Filtering in Sensor Networks," LNCS 4706, pp. 573-583, Aug. 2007.