한국시뮬레이션학회 논문지
Vol. 23, No. 2, pp. 65-72 (2014. 6)
http://dx.doi.org/10.9709/JKSS.2014.23.2.065
ISSN 1225-5904

무선 센서 네트워크에서 확률적 투표 기반 여과 기법의 에너지 효율성을 위한 퍼지 로직 시스템 기반의 다음 이웃 노드 선택 기법

이재관[1] · 남수만[1] · 조대호[1†]

Fuzzy Logic based Next Hop Node Selection Method for Energy Efficient PVFS in WSN

Jae kwan Lee · Su Man Nam · Tae Ho Cho

ABSTRACT

Sensor nodes are easily compromised by attacker when which are divided in open environment. The attacker may inject false report and false vote attack through compromised sensor node. These attacks interrupt to transmission legitimate report or the energy of sensor node is exhausted. PVFS are proposed by Li and Wu for countermeasure in two attacks. The scheme use inefficiency to energy of sensor node as fixed report threshold and verification node. In this paper, our propose the next neighbor node selection scheme based on fuzzy logic system for energy improvement of PVFS. The parameter of fuzzy logic system are energy, hops, verification success count, CH select high the next neighbor node among neighbor nodes of two as deduction based on fuzzy logic system. In the experimental, our proposed scheme was improvement to energy of about 9% compare to PVFS.

Key words : Wireless sensor network, Probabilistic voting-based filtering scheme, Fuzzy logic system

요 약

무선 센서 네트워크에서 센서 노드들은 개방된 환경에 배치되기 때문에 공격자들을 통해 쉽게 훼손된다. 공격자는 훼손된 노드를 통해 허위 보고서 및 허위 투표 주입 공격을 할 수 있다. 이러한 공격은 센서 노드의 에너지를 고갈시키거나 정상 보고서의 전송을 막는다. 이 두 가지 공격에 대응하기 위해 Li와 Wu는 확률적 투표 기반 여과 기법을 제안하였다. 이 기법은 보고서 임계값과 검증 노드를 고정적으로 사용하기 때문에 센서 노드의 에너지를 비효율적으로 사용한다. 본 논문에서는 PVFS의 에너지 향상을 위해 퍼지 로직 시스템을 기반으로 다음 이웃 노드 선택 방법을 제안한다. 퍼지 로직 시스템의 매개변수들은 에너지, 홉의 수, 검증 성공 횟수이며, CH는 퍼지 로직 시스템을 기반으로 도출된 2개의 이웃 노드 중에서 상태 정보가 높은 다음 이웃 노드를 선택한다. 실험을 통해 제안 기법은 기존 기법과 비교하여 약 9%의 에너지가 향상되었고, 센서 노드들의 에너지 절감을 통해 전체 네트워크의 수명 연장을 기대한다.

주요어 : 무선 센서 네트워크, 허위 투표, 확률적 투표 기반 여과 기법, 네트워크 보안, 퍼지 로직 시스템

1. 서 론

무선 센서 네트워크(Wireless Sensor Network; 이하 WSN)는 무선 통신망을 기반으로 다수의 센서 노드와 하나의 싱크 노드로 구성된다. 이벤트가 발생할 때, 한 센서 노드는 그 이벤트를 감지하고 다수의 센서를 경유하여 싱크 노드까지 전달한다[1]. 이러한 WSN 응용분야는 홈 네트워크, 군사 시스템, 물류관리, 산림 화재 모니터링, 헬스케어 등에 사용된다[2]. WSN에서 사용하는 센서 노드의

* 이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2013R1A2A2A01013971).
접수일(2013년 7월 5일), 심사일(2014년 5월 15일), 게재 확정일(2014년 5월 15일)
[1] 성균관대학교 정보통신공학부
주 저 자 : 이재관
교신저자 : 조대호
E-mail; thcho@skku.edu

단점은 한정된 메모리와 에너지 자원, 낮은 대역폭을 가지고 있다. 또한, 센서 노드들은 개방된 환경에서 동작되기 때문에 공격자로부터 쉽게 훼손 된다[3]. 공격자는 노드의 물리적 취약점을 이용하여 악의적인 목적으로 일부 또는 특정 노드를 훼손시켜 허위 보고서 또는 허위 투표 주입 공격을 센서 네트워크에 주입한다.

Fig. 1은 센서 네트워크에서 발생되는 허위 보고서와 허위 투표 주입 공격을 보여준다. Fig. 1(A)은 훼손된 노드이며, Fig. 1(B)은 허위 투표들이 포함된 허위 보고서(fabricated report with false votes), 그리고 Fig. 1(C)은 허위 투표가 포함된 정상 보고서(false votes on real report)이다. 허위 보고서 주입 공격은 공격자가 존재하지 않는 보고서를 훼손한 센서 노드를 통해 주입하는 공격이며, 허위 투표 주입 공격은 정상 보고서에 허위 투표 정보를 주입하는 공격이다. 이러한 공격들은 센서 노드들의 불필요한 에너지 소모 및 원활한 데이터 통신을 방해한다. 이 두 가지 공격에 대응하기 위해 Li와 Wu는 확률적 투표 기반 여과 기법(Probabilistic Voting-based Filtering Scheme; 이하 PVFS)을 제안하였다[4]. PVFS는 보고서 전송 중에 보고서에서 탐지한 허위 투표 개수의 임계값($T_f = 2$)을 통해 두 공격 중 하나의 공격을 결정한다. 만약 그 보고서에서 탐지된 허위 투표의 수가 임계값에 도달하면, 그 보고서는 허위 보고서로 간주하여 검증 노드는 그 보고서를 여과하며, 임계값에 도달하지 않았다면, 그 보고서는 싱크 노드를 향해 전송된다. 이 기법은 이미 설정된 경로의 검증 노드를 통해 두 공격을 감지한다. 하지만 PVFS는 보고서 생성 후에 검증 노드를 고정적으로 사용하기 때문에

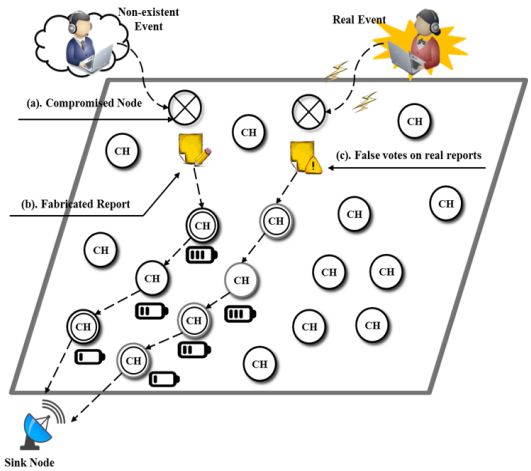

Fig. 1. False report and False votes injection attack

동적인 네트워크 상황에 비효율적이다.

본 논문에서는 고정적인 검증 노드를 동적으로 선택하기 위해 퍼지 로직 시스템을 기반으로 다음 이웃 노드 선택 기법을 제안한다. 이 제안 기법은 이벤트가 발생한 지역의 클러스터 헤드(Clsuter Head; 이하 CH)가 다음 이웃 노드 선택을 위해 자신을 기준으로 근접한 이웃 노드 중 무작위로 2개의 이웃 노드를 선택한다. 선택된 이웃 노드들은 퍼지 로직 시스템을 기반으로 상태 정보 값을 CH에 전송한다. 이때 CH는 상태 정보가 높은 이웃 노드에 보고서를 전송한다. 퍼지 로직 시스템에 사용되는 입력 매개변수들은 에너지(Energy; 이하 E), 홉의 수(Hops; 이하 H), 검증 성공 횟수(Verification Success Count; 이하 V)이며, 출력 변수는 다음 노드 결정(Decision of the Next; 이하 D)이다.

본 논문의 구성은 다음과 같이 구성된다. 2장에서는 관련 연구와 PVFS에 대한 배경 및 동기를 설명한다. 3장에서는 다음 이웃 노드 선택 기법에 대한 제안 기법을 설명하며, 4장은 제안된 방법을 기존의 방법과 비교한 결과들을 보여준다. 결론 및 향후 계획은 5장에서 설명한다.

2. 배 경

2.1 관련 연구

이번 장에서는, 본 연구에 대한 관련 연구(SEF[5], IHA[6], CCEF[7], BECAN[8])를 서술한다. 통계적 전달 중 여과 기법(Statistical En-Route Filtering of Injected False Data in Sensor Networks; 이하 SEF)은 허위 보고서 주입 공격에 대응하기 위해 제안되었다. 이 기법은 각 중간 노드에서 인증키를 사용해서 일정한 확률로 보고서를 검증한다. 검증한 보고서가 허위 보고서로 판단되면 그 보고서는 중간 노드에서 여과된다. 상호 간 홉 인증 기법(Interleaved Hop-by-hop Authentication Scheme; 이하 IHA)은 노드에서 감지한 이벤트 보고서를 전송 노드를 통해 전송 중 허위 보고서를 페어와이즈 키를 사용해서 탐지 및 폐기하는 기법의 하나이다. 가환 암호 기반 전달 중 여과 기법(Commutative Cipher based En-route Filtering in Wireless Sensor Networks; 이하 CCEF)은 허위 보고서 주입 공격을 방어하기 위해 감지 보고서에 서명과 검증에 대한 가환 암호를 사용한다. 대역폭 협력 인증 기법(A Bandwitdh-Efficient Cooperative Authentication Scheme; 이하 BECAN)은 공격자의 허위 데이터 주입 공격에 대응하기 위해, 보고서 생성 시, 주변 이웃 노드들이 사전에 공유된 Private Key로 보고서를 인증한다.

위 네 가지 기법은 허위 보고서 주입 공격을 통해 불필요한 에너지 고갈을 줄이기 위해 제안되었다. 하지만 이러한 기법들이 적용된 센서 네트워크에 허위 투표 주입 공격이 시도된다면, 그 기법들은 그 공격을 감지할 수 없다. 그래서 두 공격이 동시에 센서 네트워크에 주입되었을 때 효과적으로 감지할 수 있는 기법이 필요하다.

2.2 확률적 투표기반 여과기법

확률적 투표기반 여과기법은 보고서 임계값, 보안 임계값(T_f)과 검증 노드를 사용하며, 총 3단계의 동작과정을 수행한다. 1) 키 할당 단계에서는 센서 노드들이 클러스터 단위로 배치된 후 각 클러스터에 고유 키들을 할당한다. 2) 보고서 생성 단계에서는 어느 클러스터 지역에서 이벤트 발생 시 CH가 보고서를 생성한다. 3) 여과 단계에서는 확률적으로 선택된 검증 노드들이 허위 투표를 탐지해서 여과한다. 다음 Fig. 2는 키 할당 단계를 보여준다.

Fig. 2의 그림은 PVFS에서 키를 할당하는 단계를 보여준다. 센서 노드들이 클러스터 단위로 균일하게 배치된 후 Global Key Pool에서 각 클러스터에 각 파티션별로 키들을 할당한다. 파티션과 키 생성은 다음과 같다. $K_n = \{k_i : 0 \le i \le n-1\}$.

Fig. 3은 보고서 생성 단계를 보여준다. 한 클러스터에

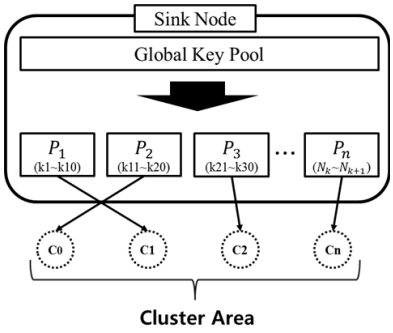

Fig. 2. Key assignment phase

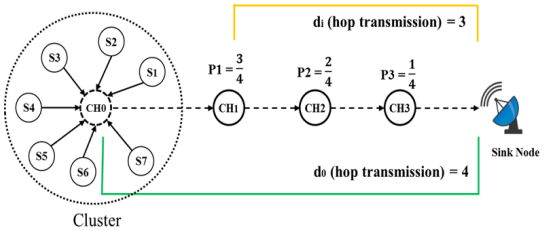

Fig. 3. Report generation phase

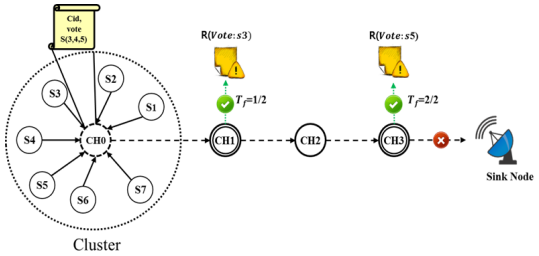

Fig. 4. False report drop phase

서 이벤트가 발생하면, CH0는 자신과 연결된 일반 노드들로부터 이벤트 정보가 담긴 투표를 전송받는다. CH0는 보고서를 생성한 후 노드로부터 받은 투표들을 그 보고서에 첨부한다. CH0는 전송할 보고서를 미리 설정된 검증 경로에 확률적 검증 노드 선택 방법은 다음과 같다.

확률공식 d_i/d_0에서 d_0는 소스 CH부터 싱크 노드까지 거리이며, d_i는 보고서 전달 경로 상의 CH부터 싱크 노드까지의 거리를 말한다. 예를 들면, CH1을 기준으로 d_0=4이고 d_i=3이므로 CH3이 검증 노드가 될 확률은 $p = 3/4$이다.

Fig. 4는 허위 보고서 여과 단계를 보여준다. CH0에서 생성된 보고서가 다음 검증 노드인 CH1에 전송되면 CH1은 그 보고서에 있는 투표들을 검증한다. 검증에 성공한 CH1은 보안 임계값에 도달됐는지 확인하고 도달하지 않았으면, 탐지한 투표를 레코드에 저장한다. 그리고 검증된 투표 정보를 보고서에 첨부한 후, 그 보고서를 CH2로 전송한다. CH2는 검증 노드가 아니므로 다음 검증 노드인 CH3에 보고서를 전송한다. CH3이 그 보고서에 첨부된 허위 투표 검증에 성공하면, 보안 임계값을 확인하고 임계값에 도달했으면 그 보고서를 허위 보고서로 간주하여 여과한다.

2.3 동기

WSNs에서 센서 노드들은 개방된 환경에 배치되기 때문에 공격자로부터 쉽게 손상된다. 공격자는 한 노드를 훼손해서 허위 보고서 및 허위 투표를 주입한다. 이 공격들을 효과적으로 방지하기 위해 PVFS는 검증 노드들을 통해 그 공격들을 감지한다. 하지만 기존 기법의 문제점은 센서 필드에서 검증 노드 및 일반 노드가 손상됐을 때, 인증키에 대한 재설정과 고정적인 검증 노드의 위치 재설정이 불가능하다. 인증키와 검증 노드를 재설정하려면, 싱크 노드로부터 모든 설정 값을 변경한 후 재분배되기 때문에 네트워크 수명에 많은 영향을 준다. 이러한 문제점

들은 센서 노드들의 자원 고갈과 함께 네트워크 수명이 줄어들게 된다. 따라서 제안 기법은 센서 노드의 에너지 향상을 위해 퍼지 로직 시스템을 기반으로 다음 이웃 노드 선택 기법을 제안한다.

3. 제안 기법

이 장에서는 가정, 동작 과정과 제안 기법에 대해 상세히 설명한다.

3.1 가정

본 논문에서는 다음과 같이 가정한다. 한 센서 필드에서 센서 노드들은 클러스터 기반으로 구성된다. 모든 센서 노드들은 센서 필드에 균일하게 배포되며, 고정적으로 배치된다. 그 일반 센서 노드들은 Mica2 mote로 구성되었으며, 제한된 메모리와 에너지를 가지고 있다. CH는 일반 센서보다 강한 하드웨어 향상과 글로벌 키를 가지고 있다. 각 센서 노드들은 고유 아이디, 위치 정보와 에너지양, BS로부터 거리, 허위 투표 검증 성공 횟수를 저장한다. 각 CH는 보고서를 생성하고 전송할 때, 다중 홉을 거쳐서 BS를 향해 전송한다.

3.2 동작 과정

제안 기법의 동작 과정은 다음과 같다. 센서 노드들이 특정 지역에 배치되기 전에 Global Key Pool에서 키들은 파티션 단위로 나뉘며, 보고서 임계값, 보안 임계값을 PVFS와 동일하게 설정한다. 그 후 노드들은 센서 필드에 클러스터 단위로 배치된다. 1) 키 할당 단계는 Global Key Pool에서 생성된 파티션을 각 클러스터에 할당한다. 각 클러스터 범위에 있는 센서 노드들은 1개의 키를 선택해서 메모리에 저장한다. 2) 보고서 생성 단계는 PVFS와 동일하다. 3) 다음 이웃 노드 선택과 검증 단계는 2)에서 생성된 보고서를 확률적으로 결정된 검증 노드에 보내지 않고, 다음 이웃 노드 선택을 위해 퍼지 로직 시스템을 이용한다. 퍼지 논리의 입력 매개변수는 에너지, 홉의 수, 검증 성공 횟수이며, 퍼지 규칙을 적용해서 센서 노드의 상태 값을 도출해 낸다. 예를 들어, 소스 CH에서 다음 이웃 노드에 보내기 위해 자신과 근접한 이웃 노드 2개를 임의로 선택한다. 선택된 이웃 노드들은 퍼지 로직 시스템을 기반으로 자신들의 상태 정보를 소스 CH에 전송한다. 소스 CH는 전송받은 상태 정보에서 가장 높은 값을 가진 이웃 노드로 해당 보고서를 전송한다. 해당 보고서를 받은 이웃 노드는 그 보고서의 투표들을 검증한다.

3.2.1 다음 이웃 노드 선택 알고리즘

Table 1은 보고서 전송 단계에서 CH가 보고서 전송을 위해 다음 이웃 노드를 선택하는 알고리즘이다. 알고리즘에서 N1과 N2는 이웃 노드들이며, D_{k_i}는 복호화된 투표를 나타낸다. 마지막으로 R.Bin[i]는 탐지된 허위 투표의 개수를 확인하는 보안 임계값이다. 그리하여, 이웃 노드는 Algorithm 1에 따라서 허위 투표를 검증한다. 따라서, 제안 기법의 실행시간은 $2n+4$이므로 시간 복잡도는 $O(n)$이다.

3.3 퍼지 로직 시스템

Fig. 5는 이웃 노드들이 퍼지 로직이 적용된 상태를 보여준다. 각 이웃 노드들은 퍼지 논리에 의해 상태 정보에 대한 결과 값을 도출해낸다. 다음 Fig. 6은 퍼지 논리 멤버십 함수들을 설명한다.

Table 1. Proposed method algorithm

Algorithm 1 CH(N1, N2)
1: while Hop >= 0
2: if Fitness (N1) > Fitness (N2) then
3: Forward R;
4: if D_{k_i}(Vote) = H(R.Report) then
5: R.Bin[i] ← 1;
6: if Fitness (N2) > Fitness (N1) then
7: Forward R;
8: if D_{k_i}(Vote) = H(R.Report) then
9: R.Bin[i] ← 1;
10: end if
11: end while
12: Count the number of verified false votes;
13: Filter R and EXIT if T_f has been reached;
14: if R.Bin[i] has been not reached(T_f);
15: Forward R, EXIT

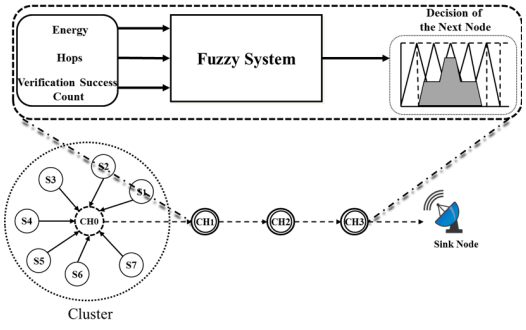

Fig. 5. Process of state decision

◎ 입력 매개변수
- 에너지(E) = {L(LOW), H(HALF), U(UPPER)}
- 홉의 수(H) = {S(SHORT), M(MIDDLE), L(LONG)}
- 검증 성공 횟수(V) = {L(LESS), I(INTERIM), O (OFTEN)}

Fig. 6은 제안된 퍼지 로직 시스템의 입력 값 3가지(E, H, V)에 대한 멤버십 함수이다.

3.3.1 에너지

센서 네트워크에서 사용되는 센서 노드는 기본적으로 한정된 에너지 자원을 가진다. 각 센서 노드들의 에너지 자원이 고갈된 상태에서 고정적인 임계값들과 검증 노드 설정은 전체 네트워크 마비를 초래할 수 있다. 따라서 센서 노드의 에너지 자원을 고려한 설정 값을 결정해야 한다.

3.3.2 홉의 수

홉의 수는 각 센서 노드가 싱크 노드까지 거리이다. 센서 노드의 에너지 소모를 줄이기 위해서는 보고서 전송 과정에서 허위 보고서가 높은 확률로 여과돼야 한다. 전송경로의 길이가 길면 허위 보고서 여과 확률이 높아지며, 전송 경로의 길이가 짧으면 허위 보고서 여과 확률이 낮아진다. 따라서 허위 트래픽 비율에 따라 홉의 수는 중요하다.

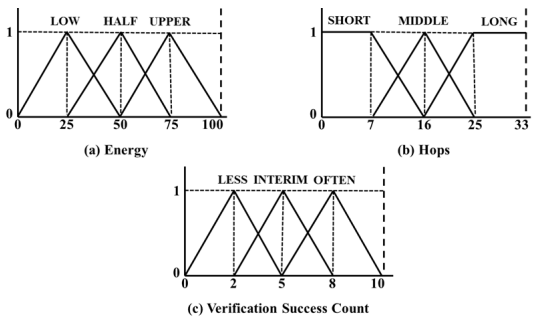

Fig. 6. Fuzzy input function

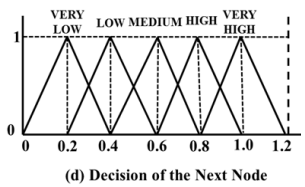

Fig. 7. Fuzzy output function

3.3.3 검증 성공 횟수

검증 성공 횟수는 이웃 노드가 허위 투표 검증에 성공했던 횟수를 말한다. 이웃 노드들이 허위 투표 검증 시 높은 확률로 탐지에 성공했기 때문에 다음 허위 투표도 높은 검증을 위해 검증 성공 횟수를 퍼지 논리에 적용하였다.

◎ 출력 매개변수
- 다음 노드 결정(D) = {VL(VERY LOW), L(LOW), M(MEDIUM), H(HIGH), VH(VERY HIGH)}

Fig. 7은 퍼지 출력 함수이다. 만약 에너지가 LOW이고 홉의 수가 SHORT, 검증 성공 횟수가 LESS이면 이웃 노드의 상태 값은 VERY_LOW 범위에서 결정된다. 이웃 노드들은 퍼지 출력 함수를 최대 1.2의 상태 값을 설정한다. 퍼지 로직 시스템 방법의 추론은 맘다니 모델의 min-max 합성방법[9]을 사용하며, 출력을 위한 역 퍼지 화 방법에서는 무게 중심 법을 사용한다[10]. 아래는 퍼지 규칙의 일부 예이다.

3.4 제안 기법의 예

Fig. 8은 소스 CH에서 다음 이웃 노드 선택과정을 보여준다. 기존 기법은 고정된 검증 노드들을 사용함으로써, 해당 노드들이 많은 연산 오버헤드와 불필요한 에너지 소모를 통해 전체 네트워크 수명을 단축한다. 본 논문에서, 제안한 기법은 여과 단계에 적용된다. 제안 기법은 기존 기법과 달리 보고서를 검증하기 위해 다음 이웃 노드를 유동적으로 선택한다. 예를 들어, 소스 CH는 생성된 보고서의 검증을 위해 자신과 근접한 이웃 노드 중 무작위로 2개를 선택한다. 선택된 이웃 노드들은 퍼지 로직 시스템을 기반으로 자신의 상태 정보를 소스 CH에 전송한다. 소

Table 2. Fuzzy if-then rules

No.	Input			Output
	E	H	V	D
1	L	S	L	VL
3	L	M	I	L
5	L	L	O	M
7	H	S	L	L
8	H	L	I	M
15	U	S	L	M
18	U	M	I	H
20	U	L	O	VH

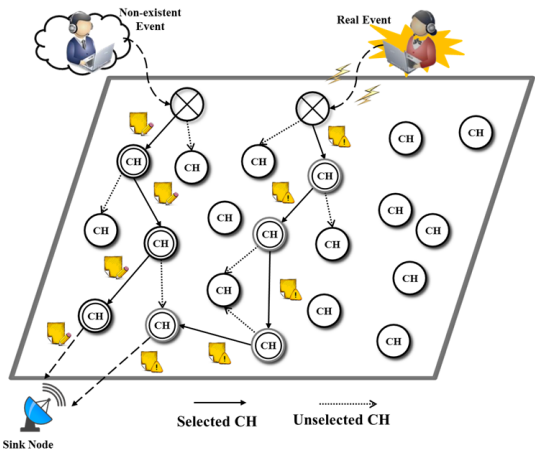

Fig. 8. Process of the next neighbor node selection

스 CH는 2개의 이웃 노드 중 높은 상태 정보를 가진 이웃 노드에 해당 보고서를 전송한다. 그 보고서를 전송받은 이웃 노드는 키를 통해서 투표들을 검증한다. 제안 기법은 에너지뿐만 아니라 보고서를 전달하는 홉의 수도 고려하였기 때문에 홉의 수가 짧을수록 불필요한 연산 오버헤드를 감소시킨다. 그러나 제안 기법에서 정상 보고서가 많을 경우 과도한 검증으로 연산 오버헤드가 있을 수 있다. 따라서 기존 기법은 CH들의 경로설정을 BS에서 설정했지만, 제안 기법의 경로 설정은 선택되는 이웃 노드들을 통해서 유동적으로 결정된다. 즉, 허위 보고서가 많을 경우 실험 결과에서 보이듯이 에너지가 향상된 것을 볼 수 있다.

4. 실험 결과

본 연구에서, 기존의 범용 시뮬레이터들(OMNet++[11], ns2[12], GloMoSim[13])은 WSN을 위한 전용 시뮬레이터로 개발되지 않았기 때문에 센서 네트워크의 성능을 측정하기 어렵다. 그래서 우리는 센서 네트워크의 공격, 기존 기법, 그리고 제안 기법의 성능을 측정하기 위해 C++로 구현한 실험 환경을 구축하였다. 본 논문에서, 제안기법의 효율성을 보이기 위해 실험 환경을 다음과 같이 가정했다[5].

Fig. 9는 공격이 연속으로 발생했을 때, 제안 기법과 PVFS의 Network Life Time을 비교한 것이다. 제안 기법은 공격 발생률이 높을수록, 센서 노드들의 에너지가 절약됨에 따라 전체 네트워크 수명이 연장된 것을 볼 수 있다.

Fig. 10은 공격률에 따른 허위 투표 탐지 개수를 나타

Table 3. Parameters

Parameter		Value
Nodes		6,000
Cluster Head		600
A Field Size		150x100m^2
Size	Report	36byte
	Vote	1byte
Energy Consumption	Transmit	16.25μJ
	Receive	12.5μJ
	Report Generation	70μJ
	Verification	75μJ
	Cipher	9μJ
Key number per a node		1
Security Threshold Value		5

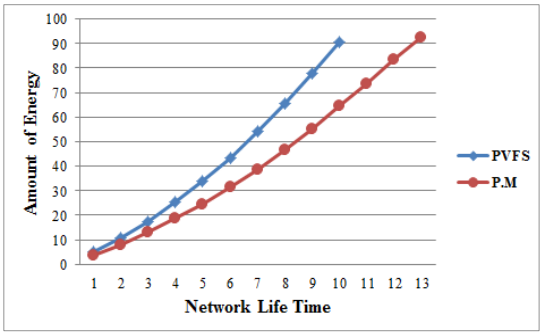

Fig. 9. Network life time

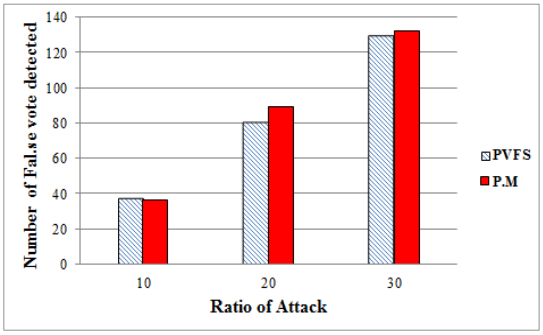

Fig. 10. Number of vote detected

낸다. 그림에서, 제안 기법은 PVFS보다 허위 투표에 대한 탐지 개수는 공격률이 10%일 때는 다소 적지만, 공격률이 20~30%일 때, 제안 기법이 PVFS보다 허위 투표 탐

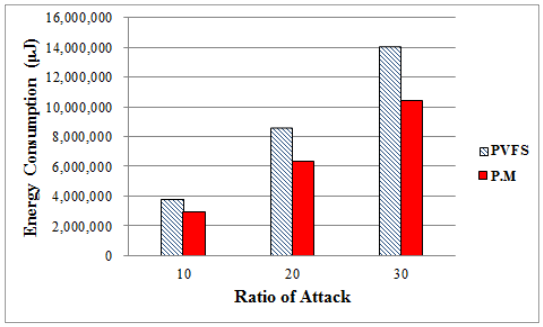

Fig. 11. Amount of energy consumption

지 개수가 높은 것으로 나타났다. 그 이유는 WSNs 환경에서 허위 이벤트 발생이 많아질수록, CH들의 투표 검증 횟수가 증가하기 때문이다. 따라서 투표 검증에 필요한 에너지가 증가하지만, 제안 기법을 통해 효율적으로 이웃 노드를 선택하기 때문에 보안성과 에너지가 향상되었다.

Fig. 11은 허위 보고서 비율에 따른 에너지 소모량을 보여준다. 기존 PVFS와 제안한 기법을 실험한 결과, 제안 기법이 약 9%의 에너지를 적게 소모하는 것으로 나타났다. 따라서 제안 기법은 센서 노드들의 에너지 자원을 효율적으로 사용하는 것을 확인할 수 있다.

5. 결론 및 향후 연구

보안 프로토콜 중 하나인 확률적 투표기반 여과기법은 허위 보고서와 허위 투표 주입 공격에 대응하기 위해 Li와 Wu가 제안 하였다. 그러나 고정적인 보고서 임계값, 보안 임계값 과 검증 노드 때문에 전송 경로에 있는 센서 노드들이 불필요한 에너지를 소비하게 된다. 본 논문은 센서 노드들의 에너지를 효율적으로 사용하기 위해서 퍼지 로직 시스템을 기반으로 다음 이웃 노드 선택 기법을 제안한다. 이웃 노드 선택 기준은 에너지, 홉의 수, 검증 성공 횟수로 결정된다. 제안 기법과 PVFS의 에너지 소비량을 비교하기 위해 시뮬레이션을 통한 전체 노드의 에너지 소모량을 측정하였다. 또한, 보안성을 비교하기 위해 허위 투표 탐지 개수를 비교하였다. 시뮬레이션 결과, 제안 기법은 PVFS보다 보안성은 다소 낮지만 에너지 측면에서 센서 노드들의 적은 에너지를 절약하며, 약 9%의 에너지 효율성을 보였다. 향후 연구로는 제안 기법의 보안성을 높이기 위해 상황에 따른 보안검증 확률 또는 보고서 임계값 결정 주기를 주제로 연구할 예정이다.

References

1. A. I. F, S. W, S. Y and C. E, “A Survey on Sensor Networks”, *IEEE Communications Magazine*, Vol. 40, pp. 102-116, 2002.
2. H. Alemdar and C. Ersoy, “Wireless sensor networks for healthcare: A survey”, *Computer Networks*, Vol. 54, pp. 2688-2710, 10, 2010.
3. 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.
4. F. Li and J. Wu, “PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks”, *International Journal of Security and Networks*, pp. 173-182, August, 27, 2008.
5. F. Ye, H. Luo, S. Lu and L. Zhang, “Statistical En-Route Filtering of Injected False Data in Sesnsor Networks”, *IEEE J. Sel. Area Comm*, Vol. 23, pp. 839-850, 2005, April, 2005.
6. S. S, J. S and P. N, “An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks”, *IEEE*, pp. 259-271, May, 2004.
7. H. Y and S. Lu, “Commutative Cipher Based En-route Filtering in Wireless Sensor Networks”, *IEEE*, pp. 1223-1227, Sept, 2004.
8. R. Lu, X. Lin, H. Zhu and X. Li, “BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks”, *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, Vol. 23, pp. 32-43, Jan, 2012.
9. R. Babuska, “Fuzzy Systems, Modeling and Identification”, *CiteSeerX, Delft University of Technology*, 2001.
10. 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.
11. A. Varga, “THE OMNET++ discrete event simulation system”, *In European Simulation Multiconference*, pp. 171-180, 2001.
12. S. Kim, M. Lee and I. Yeom, “Simulating IEEE 802.16 Uplink Scheduler Using NS-2”, *KAIST*, 2008.
13. X. Zeng, R. Bagrodia and M. Gerla, “GloModSim: A Library for Parallel Simulation of Large-scale Wireless Networks”, *IEEE*, pp. 154-161, 1998.

이 재 관 (windljk@skku.edu)

2009 백석대학교 정보보호학과 공학사
2013~현재 성균관대학교 전자전기컴퓨터공학과 석사과정

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

남 수 만 (sm38good@skku.edu)

2009 한서대학교 컴퓨터정보학과 이학사
2013 성균관대학교 전자전기컴퓨터공학과 공학석사
2013~ 현재 성균관대학교 전자전기컴퓨터공학과 박사과정

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

조 대 호 (thcho@skku.edu)

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