Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 1 pp. 382-389, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.1.382

효율적인 센서 네트워크 보안을 위한 확률적인 필터링 기법

김진수[1*], 신승수[2]
[1]동명대학교 항만물류학부, [2]동명대학교 정보보호학과

Probabilistic Filtering Method for Efficient Sensor Network Security

Jin-Su Kim[1*] and Seung-Soo Shin[2]
[1]**Division of Port & Logistics, Tongmyong University**
[2]**Dept. of Information Security, College of Information & Communication, Tongmyong University**

요 약 위조된 보고서 공격은 무선 센서 네트워크에서 이벤트가 발생한 위치에 대한 송신 응답과 같은 거짓 경보를 야기하는 것뿐만 아니라 제한된 량의 에너지를 고갈시킨다. 본 논문에서는 위조된 보고서를 필터링하기 위해 확률적인 보안 필터링 기법(PFSS: Probabilistic Filtering method for Sensor network Security)을 제안한다. 제안 내용은 클러스터 헤드와 기지국과의 거리를 이용하여 기지국까지의 중간 클러스터 헤드가 검증 노드인지를 확률적으로 선택하여 보안 검증에 필요한 에너지를 줄이고, 보안 처리에 따른 핫 스팟 문제를 완화시킨다. 제안된 기법의 성능은 수식 분석과 실험을 통하여 분석하였으며, 이를 통하여 제안된 기법이 기존의 보안 검증 처리에 비해 효율적임을 알 수 있다.

Abstract The fabricated report attack will not only cause false alarms that waste real-world response efforts such as sending response teams to the event location, but also drains the finite amount of energy in a wireless sensor network. In this paper, we propose a probabilistic filtering method for sensor network security (PFSS) to deal with filtering for the fabricated report. On the basis of filtering scheme, PFSS combines cluster-based organization and probabilistic verification node assignment using distance of from cluster head to base station for energy efficiency and hot spot problem. Through both analysis and simulation, we demonstrate that PFSS could achieve efficient protection against fabricated report attack while maintaining a sufficiently high filtering power.

Key Words : Wireless sensor network, Fabricated report, Probabilistic verification node assignment, Filtering scheme, Cluster-based organization, Hot spot problem

1. 서론

무선 센서 네트워크는 물리공간의 상태인 빛, 소리, 온도, 움직임 같은 물리적 데이터를 센서 노드에서 감지하고 측정하여 기지국으로 전달하는, 센서 노드들로 구성되는 네트워크이다. 이와 같이 무선 센서 네트워크의 주요 기능은 이벤트를 탐지하고 보고하는 것이며, 군사 감시, 방사능 감지, 산림 화재 모니터링 등과 같은 업무에 적합하다. 센서는 일반적인 환경 또는 적대적인 환경에서 이벤트를 탐지하는 데 사용하고, 이 때 적은 여러 센서 노드를 캡처하거나 위협할 수 있고 내부 공격을 시작할 수 있다. 그러한 공격 중 하나는 위조된 보고서 공격이고, 이는 위협적인 노드가 근처의 이벤트를 탐지한 것처럼 가장하거나 먼 지역으로부터 시작된 것처럼 거짓 보고서를 포워드 하는 것을 의미한다[1].

이러한 종류의 공격은 이벤트가 발생한 위치에 대한 송신 응답과 같은 거짓 경보를 야기하는 것뿐만 아니라 배터리 전력을 가진 무선 센서 네트워크에서 제한된 량의 에너지를 고갈시킨다. 위협적인 노드에 의해 주입된 위조 보고서는 적이 위협적인 노드의 모든 보안 정보를

*교신저자 : 김진수(kjs8543@tu.ac.kr)
접수일 11년 10월 31일 수정일 (1차 11년 12월 02일, 2차 11년 12월 30일) 게재확정일 12년 01월 05일

알기 때문에 연구해 볼만한 가치가 있다. 포워딩 프로세스(forwarding process)에서 주입된 위조 보고서를 필터링하기 위해 제안된 메카니즘은 F. Li[1]이 제안한 확률적인 투표 기반 필터링 기법, F. Ye[2] 및 H. Yang[3]이 제안한 일반적인 중간 라우트(en-route) 필터링 프레임워크를 이용한 위조 보고서 탐지, S. Zhu[4]이 제안한 주입된 홉-홉(hop-by-hop) 인증 스킴 등이 있다. 이러한 기법들은 적의 공격시 에너지를 과도하게 사용하지 않으면서 보안 검증 효율을 극대화시키기 위해서 주로 확률적인 방법을 이용한다.

본 논문에서는 위조된 보고서를 필터링하기 위해 확률적인 보안 필터링 기법(PFSS: Probabilistic Filtering method for Sensor network Security)을 제안한다. 제안 내용은 첫째, 송신 메시지에 송신시간 및 잔여 에너지량을 포함시켜 노드 오염 플래그를 이용한 노드의 오염 여부를 관리함으로써 메시지에 대한 보안을 효율적으로 처리한다. 둘째, 클러스터 헤드(CH: Cluster Head)와 기지국(BS: Base Station)과의 거리를 이용하여 BS까지의 중간 CH가 검증 노드인지를 확률적으로 선택하여 보안 검증에 필요한 에너지를 줄인다. 셋째, 확률적인 필터링 기법으로 기지국에 가까운 CH일수록 보안 검증 확률을 줄여, 보안 처리에 따른 핫 스팟 문제를 완화시킨다.

2. 보안 요구 사항

센서 네트워크 보안에 필요한 요구사항은 다음과 같다. 데이터 기밀성(Data Confidentiality), 데이터 인증(Data Authentication), 데이터 무결성(Data Integrity), 데이터 신선성(Data Freshness)이다.

이 장에서는 확률적인 보안 필터링 기법에서 필요한 보안 요구 사항 중에서 키 설정과 MAC에 대해서 알아본다. 먼저, 키 관리는 LEAP 프로토콜[5]과 같이 일부 노드의 노출이 근접 이웃 노드까지 노출시키는 위험을 최소화하기 위해 4개의 암호키를 사용한다. 4개의 암호 키는 개인키, 페어와이즈(pairwise) 키, 클러스터 키 및 그룹 키이다. 이러한 키를 설정하는 방법은 다음과 같다. 개인키 설정은 각 센서 노드의 배치 이전에 생성 및 로드되고, 기지국과 중요 데이터를 공유하는 키로서 센서 노드 u(각 노드가 가지는 유일 ID)를 $K_u^m = f_{K^m}(u)$ 을 이용하여 생성한다. 이 때, K_u^m은 노드 u에 대한 개인키, K^m은 컨트롤러만 알고 있는 마스터키, f는 의사 난수(pseudo-random) 함수[6]이다. 페어와이즈 키는 다른 센서 노드와 공유하는 키로서 그 키의 설정은 노드가 배치되기 전 키의 사전 분배, 노드가 배치된 후의 이웃 노드 탐색, 페어와이즈 키 설정 및 시간 만료된 키의 삭제 등의 4단계로 되어 있다. 이 때 노드 u는 노드 v로서 그의 페어와이즈 키(K_{uv})를 계산한다. 즉, $K_{uv} = f_{K_v}(u)$ 을 이용한다. 노드 v 역시 같은 방법으로 K_{uv}를 계산한다. 클러스터 키는 클러스터 내의 노드들이 공유하는 키로서 노드 u가 자신의 인접한 이웃 노드와 클러스터 키를 설정하고자 한다면, 우선 랜덤키 K_u^c를 생성하고 생성된 키를 각각의 이웃 노드와 공유하고 있는 페어와이즈 키로 암호화한다. 그리고 각각의 이웃 v_i에게 암호화된 키를 전송한다. 노드 v_i는 키 K_u^c를 복호화해서 테이블에 저장하고, 노드 u에게 자신의 클러스터 키를 되돌려 보낸다. 이 키는 하나의 클러스터 내에서 데이터를 공유할 때 사용된다. 마지막으로, 그룹 키는 센서 노드가 배치되기 전에 각 노드에게 할당되고, 주로 BS가 네트워크에 있는 모든 노드에게 메시지를 브로드캐스팅할 때 사용된다.

센서 네트워크에서 데이터 인증은 순수한 대칭 메카니즘을 통해서 성취될 수 있다. 송신자와 수신자는 통신된 데이터의 메시지 인증코드(MAC: Message Authentication Code)를 계산하기 위하여 비밀 키를 공유한다. 정확한 MAC이 도달했을 때 수신자는 송신자가 보낸 것이 확실하다는 것을 안다. 이러한 유형의 인증은 네트워크 노드에 대해 더 강력한 신뢰가 있는 가정을 두지 않고는 브로드캐스트 셋팅에 적용될 수 없다.

센서 네트워크는 기본적으로 이벤트를 감지할 수 있는 다수의 센서 노드들과 기지국으로 구성되어 있다. 이러한 노드들은 개방된 환경에 배치되므로 공격자로로부터 손쉽게 노출되고 훼손된다는 단점을 가지고 있다. 공격자는 훼손된 노드들을 통하여 허위 보고서 주입 공격 및 허위 MAC 삽입 공격이 가능하다. 허위 보고서 주입 공격은 허위 정보로 인한 사용자 혼란뿐만 아니라 허위 보고서가 기지국까지 전달되는 과정을 통해 발생할 수 있는 에너지 고갈로 인한 센서 네트워크 전체 동작의 마비를 초래할 수 있다. 허위 MAC 공격의 경우 정상 보고서에 잘못된 MAC을 삽입함으로써, 정상보고서를 마치 허위 보고서인 것처럼 위조하여 정상보고서가 기지국까지 정상적으로 전달되는 것을 저지하는 서비스 공격을 발생시켜 사용자에게 원활한 정보제공을 전달하지 못하게 할 수 있다[7].

본 논문의 센서 네트워크 클러스터링 모델에서는 센서 노드(CM: Cluster Member)에서 센싱된 데이터를 CH에 보내고, CH에서는 수신된 데이터를 병합하여 중간 CH를 거쳐 BS에 송신한다. CM에서 CH로 송신하는 메시지의

구조는 다음과 같다.

$$Message = \{N_{id},\ Da,\ MT,\ VCH_{id}(n),\ RE_{nid},\ \{MAC\}\} \quad (1)$$

이 때, N_{id}는 해당 노드에 대한 ID, Da는 데이터, MT는 메시지 전송시간, $VCH_{id}(n)$는 실제로 보안 검증 처리할 n개의 중간 CH의 ID, RE_{nid}는 N_{id}에 대한 에너지 잔량이다. MAC은 메시지 인증 코드로써 대칭키 즉, 클러스터 키를 사용하여 하나의 센서 노드에 의해 생성되고, 메시지를 인증하는 데 사용된다. 메시지가 다중 홉(multiple hops)을 거쳐 기지국으로 포워드 될 때 각 포워딩 노드(중간 CH)는 확률적인 기법으로 검증 노드로 선정되고, 선정된 노드는 메시지 안에 운반된 MAC의 정확성을 검증한다. 그리고 메시지 전송시간과 센서 노드의 에너지 잔량은 센서 노드의 오염도를 검증하는 데 사용한다. 이러한 메카니즘은 위조된 메시지를 처리하기 위한 효율성을 향상시킨다.

3. 확률적인 보안 필터링 기법

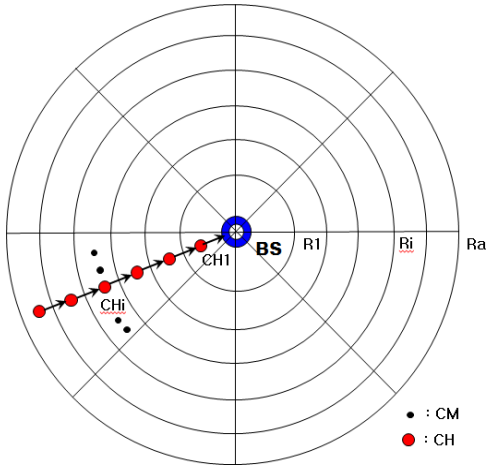
본 장에서는 센서 네트워크의 클러스터링 모델과 가정을 이용하여 보안을 기반으로 한 확률적인 필터링 기법을 제시한다.

3.1 클러스터링 모델과 가정

본 논문에서 제안하는 센서 네트워크는 그림 1과 같이 여러 개의 계층으로 구성된 클러스터링 모델이다.

클러스터링 모델의 전제 조건은 다음과 같다.

- 네트워크의 반지름은 Ra, 노드 수는 N이다.
- 네트워크는 여러 개의 계층(layer)으로 구성되고, i계층의 반지름은 R_i이다.
- 각 계층의 CH는 각 클러스터의 CM 중에서 주기적으로 선택한다.
- CM에서 센싱된 데이터는 CH에서 병합되고, 병합된 데이터는 여러 계층의 중간 CH를 거쳐 기지국으로 전송한다.
- 각 노드는 자기의 ID, 위치 및 잔여 에너지 정보를 가지고 있다. 또한 각 계층의 CH는 같은 섹터에 속한 다른 계층의 CH에 대한 ID와 위치 정보를 BS로부터 제공받는다.



[그림 1] 여러 계층으로 구성된 클러스터링 모델
[Fig. 1] Clustering Model with Multi Layer

3.2 보안을 기반으로 한 확률적인 필터링 기법

확률적인 보안 필터링 기법 (PFSS)은 다음과 같이 크게 4단계로 이루어진다.

- 1단계 : 이벤트가 발생된 센서 노드에서 센싱된 정보를 포함한 메시지를 해당 CH로 보내면, 그 데이터의 유사도를 검사하여 필터링하고 병합한다.
- 2단계 : CH에서는 1단계에서 병합된 데이터를 기지국으로 보내기 위해 확률적인 기법으로 실제로 보안 검증할 중간 CH를 선정한다. 그리고 메시지에 보안 검증할 중간 CH의 ID($VCH_{id}(n)$)를 추가한 다음, 그 메시지를 여러 계층의 중간 CH를 거쳐 기지국으로 전송한다.
- 3단계 : $VCH_{id}(n)$에 속하지 않은 중간 CH는 다음 계층의 중간 CH로 메시지를 그대로 전송하고, $VCH_{id}(n)$에 속한 중간 CH에서는 각 센서 노드의 MAC, 전송시간 및 에너지 잔량을 이용하여 데이터 오염도를 검사하고, 오염도가 심하다고 판단되면 해당 센서 노드를 폐기한다. 이때, 센서 노드의 오염도는 노드 오염 플래그를 이용하여 관리한다.
- 4단계 : 기지국에서는 수신된 데이터를 최종적으로 보안 검증한다.

1단계에서 데이터를 병합하는 과정은 수식 (2)와 같이 이전에 수신된 데이터와 유사한 경우 즉, F_{rate} 값이 1보다 작은 경우는 필터링 처리함으로써 데이터를 송수신하는 데 필요한 에너지를 줄인다. 데이터를 필터링하기 위한 필터링 율(rate)은 다음 수식과 같다.

$$F_{rate} = \frac{|SD_{\mathrm{nid}} - PD_{\mathrm{nid}}|}{TH_d} \quad (2)$$

이 때, SD_{nid}는 노드 ID에 대한 이전에 저장된 데이터이고, PD_{nid}는 노드 ID에 대해 현재 센싱된 데이터이다. 또한 TH_d는 센싱 데이터의 임계값으로써 센싱된 데이터와 이전에 저장된 데이터의 차가 TH_d보다 작으면 유사한 데이터로 간주하고 필터링 처리한다. 방사능 측정 모니터링을 예를 들면, 이전 센서 노드에서 측정된 방사능 측정치가 100nSv/h(나노시버트/시간), 현재 측정된 값이 100.5nSv/h일 경우, TH_d가 1nSv/h이면 이 데이터는 필터링 처리된다.

2단계에서 중간 클러스터 헤드를 선정할 때 CH와 BS와의 거리를 계산해야 한다. 클러스터 전체의 에너지 소비를 줄이기 위해서 클러스터 헤드의 위치는 가능한 중앙에 위치해야 한다. 이러한 경우에 CH_1 및 CH_i에서부터 BS까지의 거리는 다음 수식과 같다[8].

$$d_{CH_i \text{ to BS}} = \frac{\int_0^{R_1} r 2r \sin(\beta_1)\, dr}{R_1^2 \beta_1} = \frac{2}{3} R_1 \frac{\sin(\beta_1)}{\beta_1} \quad (3)$$

$$d_{CH_i \text{ to BS}} = \frac{\int_{R_{i-1}}^{R_i} r 2r \sin(\beta_i)\, dr}{(R_i^2 - R_{i-1}^2)\beta_i} = \frac{2}{3} \frac{(R_i^3 - R_{i-1}^3)}{(R_i^2 - R_{i-1}^2)} \frac{\sin(\beta_i)}{\beta_i} \quad (4)$$

단, i ≥ 2이고, β_i는 각 계층의 클러스터 수에 의해 결정되는 라디안 각도이다. 즉, $\beta_i = 2\pi/k_i$이다. k_i는 i번째 계층의 클러스터 수이다.

확률 수식 (5)를 이용하여 이벤트가 발생한 클러스터의 CH_e에서 BS로 가는 CH_i 중에서 검증 노드가 될 CH_i를 선정한다. CH_i가 검증 노드가 될 확률은 다음 수식과 같다.

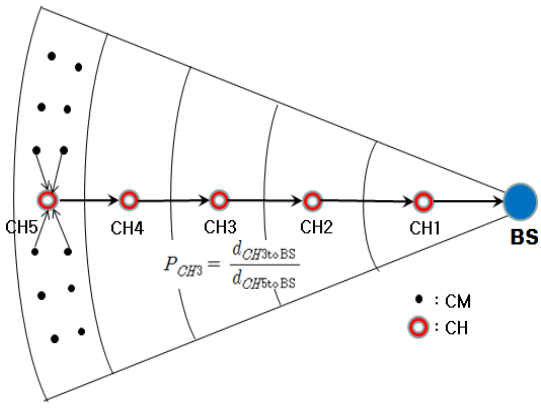
$$P_{CH_i} = \frac{d_{CH_i \text{toBS}}}{d_{CH_e \text{toBS}}} \quad (5)$$

이 때, $d_{CH_e \text{toBS}}$는 CH_e에서 BS까지의 거리이고, CH_i의 잔여 에너지율이 1보다 작으면 검증 노드에서 제외한다.

잔여 에너지율은 다음 수식과 같다.

$$RE_{rate} = \frac{RE_{\mathrm{nid}} / BE_{\mathrm{nid}}}{TH_{re}} \quad (6)$$

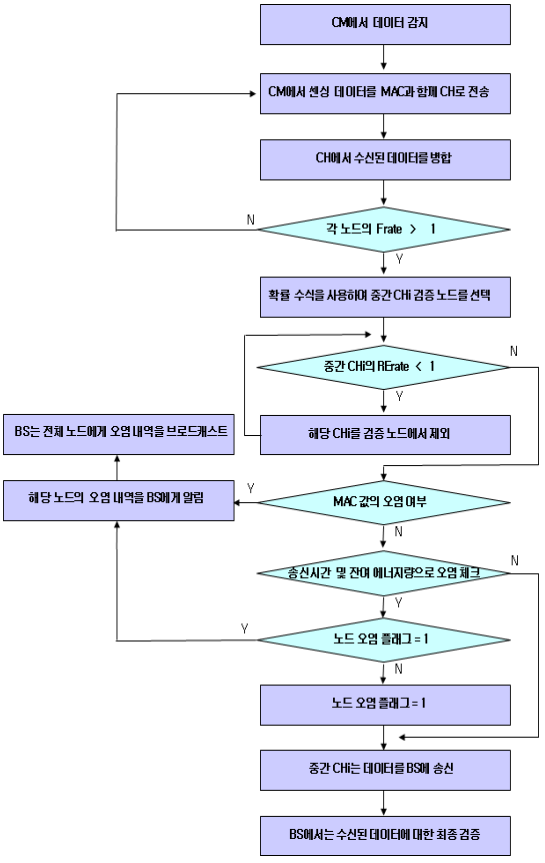
이 때, BE_{nid}는 노드 ID에 대한 초기 에너지이고, RE_{nid}는 노드 ID에 대해 현재 잔여 에너지이다. 또한 TH_{re}는 CH_i에 대한 잔여 에너지율 임계값이며, CH_i의 잔여 에너지율이 1보다 작으면 일반적인 데이터 송수신은 가능하지만 데이터를 보안 검증 처리할 에너지는 부족하므로, 보안 검증 처리 노드 대상에서 제외시킨다.



[그림 2] 검증할 CH_i 선택
[Fig. 2] CH_i Selection for Verification

그림 2는 5개의 계층으로 구성된 센서 네트워크이다. 이 때, 5계층에서 이벤트가 발생할 경우 CH_4에서 CH_1까지의 CH_i를 거쳐 BS까지 데이터를 포워딩할 때 데이터를 검증할 CH_i 선택 및 그에 대한 확률을 보여준다. $d_{CH5toBS}$가 2,000m, $d_{CH4toBS}$가 1,700m, $d_{CH3toBS}$가 1,300m, $d_{CH2toBS}$가 850m, $d_{CH1toBS}$가 350m인 경우, CH_4부터 CH_1까지의 CH_i가 검증 노드가 될 확률은 각각 0.85, 0.65, 0.43 및 0.18이 된다. 즉, BS에 먼 노드일수록 검증 노드가 될 확률이 높아지므로 BS까지 데이터를 송신하는 도중에 오염 정보를 가진 노드를 가능한 빨리 검증하여 찾아내도록 한다. 또한 BS에 근접할 노드일수록 검증 노드가 될 확률은 낮아지므로 BS 근처의 노드가 보안 검증으로 인한 핫 스팟 문제가 생길 가능성을 완화시킨다.

그림 3은 확률적인 보안 필터링 기법에 대한 순서도이고, 그 세부 내역은 다음과 같다.



[그림 3] 확률적인 보안 필터링 기법에 대한 순서도
[Fig. 3] Flowchart of PFSS

1) 센서 노드(CM)에서 데이터를 센싱하고, 그 데이터를 MAC과 함께 클러스터 헤드(CH)로 전송한다. 이때, 메시지의 구조는 식 (1)과 같다.
2) 클러스터 헤드는 센서 노드에서 보낸 데이터를 병합한다.
3) 클러스터 헤드는 센서 노드에서 보낸 데이터를 저장하고, 이전에 보낸 데이터와 비교하여 수식 (2)와 같은 필터링 율(F_{rate})이 1보다 작으면 이전 데이터와 유사하다고 판단하고 필터링 처리한다.
4) 클러스터 헤드는 기지국(BS)으로 가는 중간 클러스터 헤드 중에서 확률 수식 (5)를 이용하여 CH에서부터 BS까지 메시지를 검증할 CH_i를 선정한다. 이때 CH는 수식 (6)과 같은 CH_i의 잔여 에너지율이 1보다 작으면 검증 노드에서 제외하고, 아니면 해당 데이터를 CH_i로 전송한다.
5) 중간 검증 노드 CH_i는 이벤트가 발생한 CH로부터 수신된 모든 메시지에 대해 다음 로직을 반복 수행한다.
   - 각 센서 노드의 메시지 중 MAC 값을 보고 데이터 오염 여부를 검사한다. 해당 센서 노드의 데이터가 오염되었으면 CH_i는 그 사실을 BS에 통보하고, BS는 센서 노드의 오염 정보를 모든 센서 노드에게 브로드캐스팅하고 그 오염된 센서 노드는 폐기한다.
   - 각 센서 노드의 메시지 송신시간 및 잔여 에너지량을 보고 데이터 수신시간이 송신시간에 비해 너무 지체 되었거나 잔여 에너지량이 이전 잔여 에너지량에 비해 그 차이가 크면 해당 센서 노드가 오염되었을 가능성이 있으므로 오염 플래그(flag)를 처리한다. 이 때 오염 플래그가 0이면 오염 플래그를 1로 지정하여 해당 센서 노드에 대한 오염 경고 표시를 한다. 오염 플래그가 1이면 즉, 이전에도 이러한 사실이 발견된 경우는 위의 경우와 같이 BS는 센서 노드의 오염 정보를 모든 센서 노드에게 브로드캐스팅하고 그 오염된 센서 노드는 폐기한다.
6) 중간 클러스터 헤드는 오염이 되지 않은 데이터를 기지국으로 전송한다.
7) 기지국에서는 수신된 데이터를 최종적으로 검증한다.

4. 분석 및 실험

본 장에서는 제안한 확률적인 보안 필터링 기법을 분석하고, 그에 따른 위조 보고서 순회 가능 예상 홉수와 CH_1이 검증 노드로 수행할 확률에 대해 실험하고 그에 대한 효율성을 분석한다.

4.1 분석

본 절에서는 3장에서 제안한 확률적인 보안 필터링 기법을 두 가지 관점에서 분석한다. 첫째, 보안 필터링 효과를 분석하기 위해서 오염이 된 센서 노드가 탐지되기 전에 위조 보고서가 순회(traverse)할 수 있는 홉수(hop count)를 계산한다. 둘째, 보안 검증 처리로 인해 발생하는 핫스팟 문제에 대한 완화 효과를 분석하기 위해서 BS와 제일 가까운 1계층의 CH_1이 실제적으로 검증 노드로 수행될 확률을 계산한다.

첫 번째 분석으로 오염이 된 센서 노드가 탐지되기 전에 위조 보고서가 순회할 수 있는 홉수인 h_{dt}를 구하는 방법은 다음과 같다.

하나의 위협적인 노드(N_{cp})가 있다고 가정할 때, 위협

적인 노드 N_{cp}가 속한 클러스터의 CH에서 BS까지의 거리는 수식 (4)를 이용해서 구할 수 있다. 그리고 CH_i가 위조 보고서를 탐지하는 확률은 다음 수식과 같다.

$$P_i = \frac{d_{CH_i\text{toBS}}}{d_{CH_c\text{toBS}}} \bullet PD_{rate} \quad (7)$$

여기서, PD_{rate}는 MAC, 송신시간, 에너지 잔량 등의 보안 검증을 위한 데이터를 이용하여 오염 보고서의 오염 여부를 탐지할 수 있는 비율이다.

위협적인 노드 N_{cp}에 의해 주입된 위조 보고서는 CH_i를 거쳐 BS까지 다중홉 경로로 포워드된다. 모든 CH_i는 동일한 검증을 수행하기 때문에, 위조 보고서가 CH_i에 의해 탐지될 확률은 다음 수식과 같다.

$$P_x \bullet \prod_{k=(x+1)}^{h_{ep}} (1 - P_k) \quad (8)$$

여기서, h_{ep}는 BS에서 이벤트 지점(event point)까지의 홉수이고, x는 (h_{ep} - i + 1)이다. 이때, i는 $1 \leqq i \leqq h_{ep}$이다.

따라서 오염이 된 센서 노드가 탐지되기 전에 위조 보고서가 순회할 수 있는 예상 홉수인 h_{dt}는 다음 수식과 같다.

$$h_{dt} = P_{h_{ep}} + \sum_{i=2}^{h_{ep}} (i \bullet P_x \bullet \prod_{k=(x+1)}^{h_{ep}} (1 - P_k)) \quad (9)$$
$$+ (h_{ep} \bullet (1 - P_1) \bullet \prod_{k=(x+1)}^{h_{ep}} (1 - P_k))$$

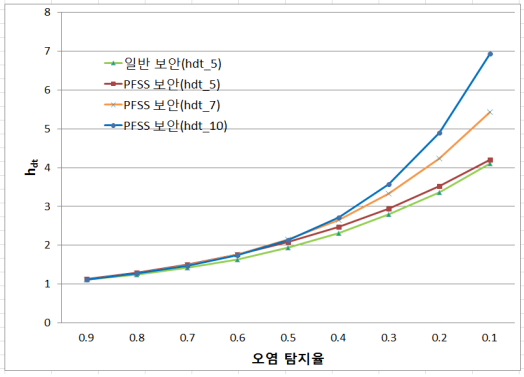
두 번째 분석으로 BS와 제일 가까운 1계층의 CH 즉 CH_1이 실제적으로 검증 노드로 수행될 확률은 다음 수식과 같다.

$$PE_{CH_1} = \frac{h_{dt}}{h_{ep}} \frac{d_{CH_1\text{toBS}}}{d_{CH_c\text{toBS}}} \quad (10)$$

수식 (10)에서 h_{dt} / h_{ep}는 오염 보고서가 CH_1 노드까지 도착할 수 있는 확률이고, $d_{CH_1\text{toBS}} / d_{CH_c\text{toBS}}$는 CH_1이 검증 노드가 될 확률이다. BS와 제일 가까운 1계층의 CH_1은 그 이전의 CH_i에서 수신된 메시지를 모아야 하므로 보안 검증 처리로 인해 핫스팟 문제가 더 많이 발생할 수 있다. PE_{CH_1}의 값은 이러한 핫스팟 문제의 완화 여부를 판단하는 기준으로 사용할 수 있다.

4.2 실험

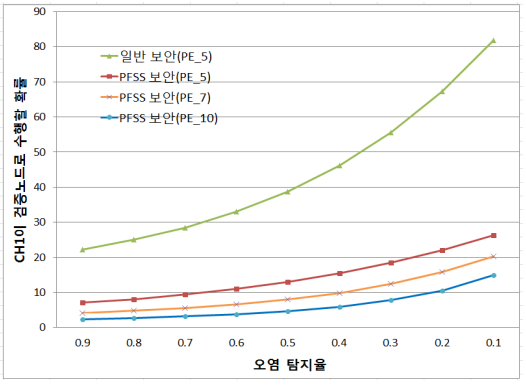
실험을 위해 사용될 수식 모델은 수식 (9) 및 (10)과 같다. 즉, 오염이 된 센서 노드가 탐지되기 전에 위조 보고서가 순회할 수 있는 예상 홉수인 h_{dt}를 네트워크 계층 크기별로 비교하여 확률적인 보안 필터링의 효과를 알아본다. 또한 BS와 제일 가까운 CH_1이 실제적으로 검증 노드로 수행될 확률인 PE_{CH_1}을 본 논문에서 제시한 PFSS 기법과 이러한 기법을 사용하지 않은 일반적인 보안 검증 기법을 비교하여 핫 스팟 문제가 완화되는지 알아본다. 실험 환경은 네트워크의 크기(R_a)가 1,000m이고, 각 계층의 클러스터 수가 16개인 경우에 계층수가 5개, 7개 및 10개에 대해 오염 탐지율에 따른 h_{dt} 및 PE_{CH_1}을 비교한다.



[그림 4] 위조 보고서 순회 가능 예상 홉수
[Fig. 4] Estimated Hop Count for Fabricated Report Traversal

그림 4는 네트워크의 계층수의 변화에 따라 오염 탐지율이 0.9에서 0.1까지의 h_{dt}를 비교한 것이다. 범례에서 일반 보안(hdt_5)은 일반적인 보안 검증 기법을 이용할 때 계층수가 5인 경우의 오염 탐지율에 따른 h_{dt} 값이다. 또한 PFSS 보안(hdt_5), PFSS 보안(hdt_7), PFSS 보안(hdt_10) 등은 PFSS 보안 검증 기법을 이용한 경우, 계층수가 각각 5, 7, 10일 때의 오염 탐지율에 따른 h_{dt} 값이다. 계층수가 5이고 오염 탐지율이 0.9, 0.8, 0.7인 경우 PFSS 기법과 일반 보안 기법의 h_{dt} 값을 비교하면 1.13, 1.30, 1.50과 1.11, 1.25, 1.43이다. 또한 두 기법의 PE_{CH_1}을 비교하면 7.1%, 8.1%, 9.5%와 22.2%, 25%, 28.5%이다. 이와 같이 본 논문에서 제안한 PFSS 보안 검증 기법과 일반적인 보안 검증 기법을 비교했을 때 h_{dt} 값은 큰

차이가 없고, BS와 제일 가까운 CH_1이 실제적으로 검증 노드로 수행될 확률인 PE_{CH_1}값은 차이가 많다. 즉, 오염이 된 센서 노드가 탐지되기 전에 위조 보고서가 순회할 수 있는 예상 홉수인 h_{dt}가 PFSS 기법과 일반적인 보안 검증 기법에서 큰 차이가 없으므로 PFSS 기법이 위조 보고서를 추출하고 처리하는 데 문제가 없고. 제안한 PFSS 보안 검증 기법을 이용하는 경우 수식 (5)의 CH_i가 검증 노드가 될 확률이 일반적인 보안 검증 기법에 비해 낮기 때문에 보안 검증에 소요되는 에너지 소모량이 줄어든다.



[그림 5] CH_1이 검증 노드로 수행할 확률
[Fig. 5] Execution Probability of CH_1 as Verification Node

그림 5는 네트워크의 계층수의 변화에 따라 오염 탐지율이 0.9에서 0.1까지의 CH_1이 실제적으로 검증 노드로 수행될 확률을 비교한 것이다.

범례에서 일반 보안(PE_5)은 일반적인 보안 검증 기법을 이용할 때 계층수가 5인 경우의 오염 탐지율에 따른 PE_{CH_1} 값이다. 또한 PFSS 보안(PE_5), PFSS 보안(PE_7), PFSS 보안(PE_10) 등은 PFSS 보안 검증 기법을 이용한 경우, 계층수가 각각 5, 7, 10일 때의 오염 탐지율에 따른 PE_{CH_1} 값이다. CH_1은 그 이전의 CH_i에서 수신된 메시지를 모아야 하므로 보안 검증 처리로 인해 핫스팟 문제가 더 많이 발생할 수 있다. 본 논문에서는 제시한 PFSS 기법과 일반적인 보안 처리 기법에 대해 CH_1이 실제적으로 검증 노드로 수행될 확률을 비교한다. 오염 탐지율이 0.8이고 계층 수가 5, 7, 10일 때 PFSS 기법의 PE_{CH_1} 값은 8.1%, 4.8%, 2.7%이고, 일반적인 보안 처리 기법의 PE_{CH_1} 값은 25.0%, 17.9%, 12.5%이다. 따라서 그림 1과 같이 여러 개의 계층으로 구성된 클러스터링 모델에서 PFSS 기법이 일반적인 보안 처리 기법에 비해 CH_1이 실제적으로 검증 노드로 수행될 확률이 작으므로 보안 검증 처리로 인한 핫스팟 문제를 완화시킨다.

5. 결론

본 논문에서는 위조된 보고서를 필터링하기 위해 확률적인 보안 필터링 기법(PFSS)을 제안한다. 제안 내용은 노드 오염 플래그를 이용한 메시지의 보안을 효율적으로 처리하고, CH와 BS와의 거리를 이용하여 BS까지의 중간 CH가 검증 노드인지를 확률적으로 선택하여 보안 검증에 필요한 에너지를 줄인다. 그래서 BS에 가까운 CH일수록 보안 검증 확률을 줄여 보안 처리에 따른 핫 스팟 문제를 완화시킨다. PFSS 기법의 성능은 수식 분석과 실험을 통하여 분석하였으며, 이를 통하여 PFSS 기법이 기존의 일반적인 보안 검증 기법에 비해 효율적임을 알 수 있었다.

실험 결과는 PFSS 기법을 이용한 경우가 일반적인 보안 검증 기법에 비해 위조 보고서 순회 가능 예상 홉수(h_{dt})가 큰 차이가 없고, 보안 검증에 소요되는 에너지는 줄어든다. 최악의 경우 즉, 오염 탐지율이 0.1인 경우를 보면, 계층수가 5, 10일 때 h_{dt}/h_{cp}가 84.0%, 69.3%이므로 같은 크기의 네트워크에서 계층수가 더 큰 경우가 필터링 효율이 더 좋아짐을 알 수 있다. 그리고 계층 수가 5이고 오염 탐지율이 0.9, 0.1일 때 CH_1이 검증 노드로 수행할 확률은 일반적인 보안 처리 방법은 22.2%, 81.9%이고 PFSS 기법은 7.1%, 26.4%이다. 그러므로 제시된 기법이 일반적인 보안 검증 기법에 비해 검증 노드로 수행될 확률이 낮고, 보안 검증 처리로 인한 부하가 작은 것을 알 수 있다.

향후에는 본 논문과 같이 네트워크의 계층별 클러스터 수를 고정적으로 지정한 시스템이 아니라 네트워크의 계층별로 클러스터 수가 변화하는 시스템에 대한 보안 필터링 연구가 필요하다.

References

[1] F. Li and J. Wu, "A probabilistic voting-based filtering scheme in wireless sensor networks," Proc. IWCMC, pp.27 - .32, July 2006.

[2] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-route Filtering of Injected False Data in Sensor Networks," IN *IEEE Proceedings of INFOCOM 2004*, 2004, pp.839-850.

[3] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh,

"Toward Resilient Security in Wireless Sensor Networks," In *ACM Proceedings of MobiHoc 2005*, 2005, pp.34-45.

[4] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering False Data in Sensor Networks," IN *IEEE Proceedings of Symposium on Security and Privacy 2004*, 2004, pp.259-271.

[5] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," In 10th ACM conference on Computer and communication security, pp. 62-72. 2003.

[6] O. Goldreich, S. Goldwasser, and S. Micali, “How to Construct Random Functions,” Journal of the ACM, Vol. 33, No. 4, 1986, pp 210-217.

[7] Sang-Jin Lee, Tae-Ho Cho, "The Desision Method for Security Threshold according to Dynamic Environment on Wireless Sensor Networks," Proceedings of KISS Spring Conference 2009 Vol. 19, No. 1

[8] S. Soro and W.Heinzelman, "Prolonging the Lifetime of Wireless Sensor Networks via Unequal Clustering," Proceedings of the 5th International Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (IEEE WMAN '05), April 2005.

김 진 수(Jin-Su Kim) **[정회원]**

- 1982년 2월 : 영남대학교 전기공학과 (공학사)
- 1990년 2월 : 숭실대학교 정보산업학과 (이학석사)
- 2007년 6월 : 영남대학교 컴퓨터공학과 (공학박사)
- 1992년 8월 : 정보처리 기술사
- 2006년 3월 ~ 현재 : 동명대학교 항만물류학부 교수

<관심분야>
데이터베이스, 센서 네트워크, 소프트웨어 공학

신 승 수(Seung-Soo Shin) **[정회원]**

- 2001년 2월 : 충북대학교 수학과 (이학박사)
- 2004년 8월 : 충북대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 동명대학교 정보보호학과 교수

<관심분야>
암호프로토콜, 네트워크 보안, USN, 스마트 카드