韓國 컴퓨터情報學會 2007하계학술발표논문집&학회지
第15卷 第1號, 2007. 6.

센서네트워크에서 통계적 여과를 위한 퍼지기반의 적응형 전역 키 풀 분할 기법

김 상 률*, 선 청 일*, 조 대 호*

Fuzzy based Adaptive Global Key Pool Partitioning Method for the Statistical Filtering in Sensor Networks

Sang-Ryul Kim*, Chung-Il, Sun*, Tae-Ho Cho*

요 약

무선 센서 네트워크의 다양한 응용분야에서, 일어나는 심각한 보안 위협 중 하나가 공격자가의 노드 훼손을 통해 발생하는 보안정보 훼손된 및 위조된 보고서의 삽입이다. 최근에 Fan Ye 등은 이런 위협에 대한 대안으로 전역 키 풀을 전체 센서네트워크에 나누어서 할당하고, 전송 경로 중에 있는 노드들이 미리 할당 받은 각자의 보안정보인 인증키를 이용해서 위조 보고서를 판단하는 통계적 여과기법을 제안하였다. 그러나 이 기법에서는 노드들의 훼손으로 인한 일부 인증키가 훼손 됐을 시 고정된 몇 개의 구획으로 나뉜 전역 키 풀 때문에 훼손된 키의 구획에 속해 있는 나머지 훼손되지 않은 인증 키들이 여과과정에서 인증키로써의 기능을 할 수 없게 된다. 본 논문에서는 전역 키 풀의 분할 여부 결정에 퍼지 로직을 적용하여 전역 키 풀을 네트워크 상황에 맞추어 나누는 적응형 분할 결정 기법을 제안한다. 전역 키 풀의 구획은 오염된 구획의 비율, 오염된 키의 비율, 노드의 에너지 비율을 고려하여 퍼지로직에 의해 분할 여부를 결정한다.

▸ Keyword : 센서 네트워크, 퍼지 로직, 전역 키 풀, 위조 보고서 여과

• 제1저자 : 김상률
* 성균관대학교 정보통신공학부

Ⅰ. 서 론

무선 센서 네트워크는 센싱, 계산, 무선 통신 능력을 가지고 있는 소형 센서 노드들 과 베이스 스테이션으로 구성된다. 센서 노드들은 일반적으로 센서 노드들이 배치되는 영역인 센서필드 내에 흩뿌려지며, 각 센서 노드는 센싱한 데이터를 외부에 있는 베이스 스테이션까지 전달한다. 그리고 베이스 스테이션은 센서 네트워크를 인터넷과 같은 기존 통신 인프라와 연결하여, 사용자가 수집한 데이터에 접근할 수 있다[1].

하지만 많은 센서 네트워크 응용에서 센서 노드들은 개방된 환경에 배포되기 때문에, 각 노드들은 물리적 공격에 취약하다[2]. 공격자는 노드를 포획하여 노드의 모든 암호 키들을 훼손(compromising)하고, 이렇게 훼손된 노드(compromised node)를 이용하여 그림 2와 같이 위조 감지 보고서(false sensing report)를 네트워크에 삽입할 수 있는데, 이것은 거짓 경보(false alarm)를 유발할 수 있을 뿐만 아니라 센서 노드의 제한된 에너지 자원을 고갈시킬 수 있다[3]. 이러한 심각한 피해를 최소화하기 위해서는 위조 보고서를 가능한 한 빨리 발견하여 제거하여야 하며, 발견되지 못한 보고서는 최소한 베이스 스테이션에서 발견되어야 한다 [4].

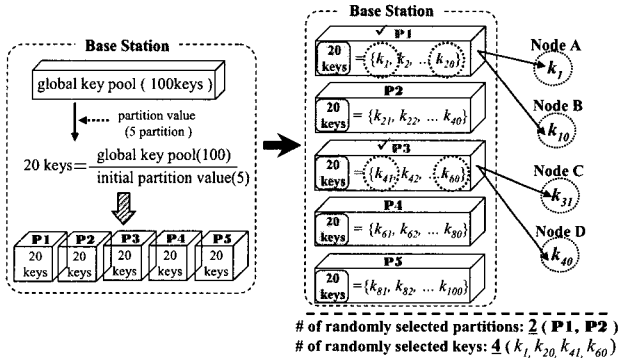
최근 몇몇 보안 기법이 이러한 목적을 위하여 제안되었고, 그 중 하나가 Fan Ye 등[2]이 제안된 통계적 여과 기법(SEF: Statistical En-route Filtering)인데, 이 기법에서는 고정된 몇 개의 구획으로 나누어진 전역 키 풀 때문에 공격자가 특정 구획의 일부 인증키를 훼손시키면, 훼손된 인증키가 속해 있는 그 구획의 나머지 훼손되지 않은 인증키들 까지도 위조 보고서를 검증할 수 있는 인증키로써의 기능을 상실하게 돼는 문제점을 갖고 있다.

본 논문에서는 전역 키 풀의 분할 여부 결정에 퍼지 로직을 적용하여 전역 키 풀을 네트워크 상황에 맞추어 나누워서 구획의 수를 증가시켜 인증키의 효율적인 사용을 보장하는 적응형 분할 결정 기법을 제안한다. 이 기법에서는 훼손된 구획의 비율, 훼손된 키의 비율, 노드의 잔여 에너지 비율을 고려한 퍼지로직에 의해 분할 여부를 결정하게 된다. 본 논문은 다음과 같이 구성된다. 2장에서는 배경이론으로 통계적 여과 기법에 대한 간단히 설명과 연구 동기를, 3장에서는 분할 여부 결정을 위한 퍼지 로직에 대해 설명하며, 4장에서는 결론과 향후 연구 과제는 논의된다.

2. 배경이론

2.1 통계적 여과 기법(SEF)

Fan Ye 등[2]이 제안한 통계적 여과 기법에서는 〈그림 2〉와 같이 베이스 스테이션에서 가지고 있는 전역 키 풀을 사용자가 임의로 정한 분할 값(partition value)으로 나눈다. 그렇게 되면 각 구획은 서로 다른 키들로 나누어지게 된다. 그리고 사용자에 의해 임의로 선택된 구획에서 사용자가 임의로 지정한 개수만큼의 키들을 각각의 노드에게 할당 한다. 이 모든 과정이 끝나면 사용자가 정보를 얻고자 하는 지역에 노드들을 배치시킨다.

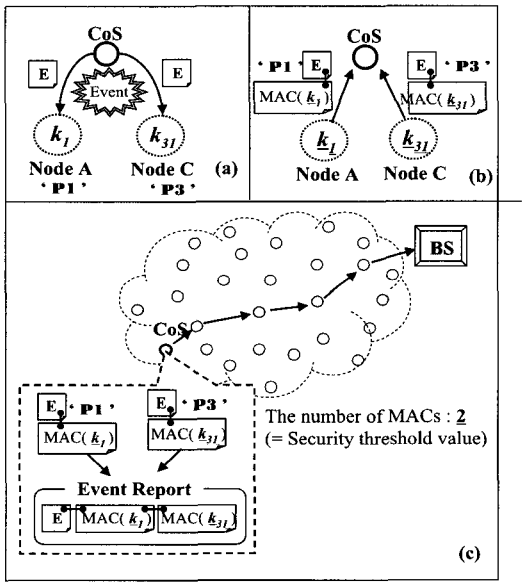


〈그림 1〉 전역 키 풀의 분할과 사용자 임의에 의한 배치 전 노드에 인증키 할당

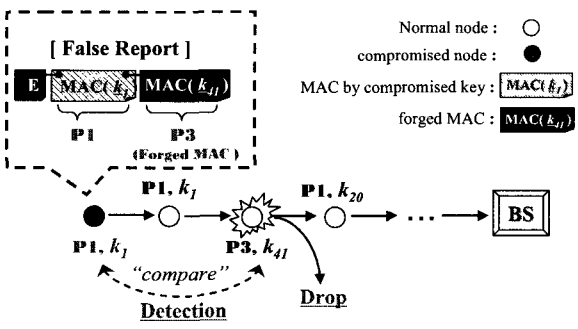
이렇게 배치된 상태에서 어떤 이벤트가 발생하게 되면, 이벤트를 감지한 노드들 중에서 그 센싱 강도가 제일 강한 노드가 CoS(center of stimulus)로 선정이 되고, 이 CoS는 〈그림 3(a)〉와 같이 자신이 센싱한 동일한 이벤트를 센싱한 노드들에게 이벤트 정보를 브로드캐스트하고, 전달받은 노드들은 이 정보를 자신이 센싱한 내용과 비교 후 같다면, 〈그림 3(b)〉와 같이 자신이 가지고 있는 키를 사용해 생성한 MAC과 이벤트 정보를 CoS에게 전달한다. 이렇게 해서 전달받은 각각의 MAC들을 CoS는 〈그림 3(c)〉과 같이 미리 사용자에 의해 임의로 정해져 있던 MAC의 길이(=보안 경계 값)만큼의 MAC들을 이벤트 정보에 덧붙여서 하나의 이벤트 보고서를 생성 후 멀티 홉 방식으로 베이스 스테이션에 전달하고 나면, 〈그림 4〉와 같이 만약 공격자가 위조 보고서를 생성해서 전달할 경우

전달 경로에 있는 중간노드들이 각각 가지고 있는 인증키 정보를 가지고 위조 보고서에 대한 검증을 하게 된다.

이와 같은 방법을 통하여 정상 보고서만 베이스 스테이션에 전달되고, 위조 보고서는 중간노드에서 여과된다. 만약 중간노드를 통해 여과되지 않았다면, 모든 키를 소유하고 있는 베이스 스테이션에서 같은 방법으로 보고서에 사용된 모든 MAC를 검증하게 된다. 이러한 방법을 통하여 위조 메시지 공격에 대응할 수 있으며, 전체 네트워크에서 사용되는 에너지 소모를 줄일 수 있다.



〈그림 2〉 센싱한 이벤트 보고서의 생성



〈그림 3〉 MAC을 이용한 위조 보고서의 탐지 및 여과

2.2 동기

SEF에서의 전역 키 풀의 구획의 수는 고정돼 있기 때문에 훼손된 구획의 수가 이 고정된 구획수를 넘어가면 더 이상 위조 보고서에 대한 여과를 할 수가 없다. 또한, 훼손된 노드를 통해 특정 구획의 일부 키가 훼손되면, 그 구획의 나머지 훼손되지 않은 키들은 인증키로써의 기능을 못하게 된다. 왜냐하면, SEF 여과과정에서 요구하는 이벤트 보고서의 MAC은 서로 다른 구획 당 한 개씩의 키로 생성된 MAC들이기 때문에 공격자는 각 구획 당 키를 한 개 씩만 알아내면, 구획 내에 있는 나머지 키들에 대해 몰라도 SEF에서 검증 할 수 없는 위조 보고서를 만들 수 있기 때문에 나머지 훼손되지 않은 키들 인증키로써의 기능을 못한다. 그러므로 동적인 네트워크 상황에 맞게 전역 키 풀의 분할 여부를 결정할 수 있도록 통계적 여과 기법에 퍼지 로직의 적용을 제안하였다.

3. 퍼지 기반의 전역 키 풀 분할결정

3.1 가정

- 베이스 스테이션은 훼손된 구획의 비율, 훼손된 키의 비율, 노드의 에너지 비율을 예측할 수 있다.
- 훼손된 구획의 비율과 훼손된 키의 비율은 베이스스테이션의 브로드캐스트 메시지 인증(예: μTESLA[4])을 통해 예측할 수 있다.
- 주변노드들의 밀도가 충분해서 보안 경계 값 만큼의 충분한 MAC 길이를 구성할 수 있다.

3.2 보안 경계 값의 변경

기존 SEF에서는 나눠진 전역 키 풀의 구획들 중에서 사용자에 의해 임의로 선택된 구획의 수를 보안 경계 값으로 하였으나, 본 논문에서는 네트워크 상황에 따라 전역 키 풀의 구획 수가 동적으로 변화되기 때문에 각 키에 대한 구획정보가 계속 변하게 된다. 따라서 본 논문에서는 나눠진 전역 키 풀의 총 구획의 수를 보안 경계 값으로 한다.

3.3 분할 여부의 결정 요소

전체 구획에서 훼손된 구획의 비율이 높으면 그 비율이 낮아질 때 까지 전역 키 풀을 분할해야 한다. 왜냐하면, 훼손된 구획의 비율이 높다는 말은 훼손된 키를 포함하고 있는 구획의 수가 많다는 것을 의미하고, 이것은 이런 훼손

구획들을 제외한 나머지 소수의 구획들에 있는 인증키로만 위조 보고서를 검증해 내야 하는 것을 의미하기 때문이다. 또한 훼손된 키의 비율을 고려해야한다. 전역 키 풀에서 훼손된 키의 비율이 아주 커지면 위조 보고서를 검증할 수 있는 키의 수가 너무 적어지게 되고, 이로 인해 전역 키 풀의 구획 수를 증가 시켜도 훼손된 구획의 비율이 더 이상 낮아지지 않게 된다. 따라서 훼손된 키의 비율이 아주 높을 경우에는 키를 이용한 위조 보고서 여과를 종료시키고 이벤트 정보만 전달한다. 마지막으로 센서 네트워크의 센서 노드들은 제한된 에너지 자원을 갖고 있으므로 보안 경계 값인 전역 키 풀의 전체 구획의 수를 분할 시켜 증가 시킬 것인가를 각각의 노드의 에너지 수준을 고려해서 결정해야 한다.

3.4 퍼지로직의 입/출력 파라미터 및 규칙

입력 파라미터는 훼손된 구획의 비율(CPR: compromised partition ratio), 훼손된 키의 비율(CKR: compromised key ratio), 그리고 노드의 잔여 에너지 비율(RER: remaining energy ratio)이다. 그리고 출력 파라미터는 전역 키 풀의 분할 화(partitioning of global key pool)로 총 세 가지 형태로 나타난다. 첫 번째는 전역 키 풀에 더 이상의 구획화가 필요 없음을 뜻하는 Do nothing(NOT)이고, 두 번째는 전역 키 풀의 구획화가 필요함을 나타내는 Divide(DIV), 그리고 세 번째는 전역 키 풀의 훼손도가 너무 커서 위조된 보고서에 대한 여과 능력을 상실해서 인증키를 이용한 SEF의 모든 여과과정의 종료 시켜 에너지 소비를 줄이는 Disable(DIS)이다.

▶ x (CPR: compromised partition ratio) = { VERY_LOW, LOW, MEDIUM, LARGE, VERY_LARGE }

▶ y (CKR: compromised key ratio) = { VERY_LOW, LOW, MEDIUM, LARGE, VERY_LARGE }

▶ z (RER: remaining energy ratio) = { VERY_LOW, LOW, MEDIUM, LARGE, VERY_LARGE }

▶ p (partitioning of global key pool) = { NOT, DIV, DIS }

아래는 퍼지규칙들이다.

RULE 0: IF (x IS VERY_LOW) AND (y IS VERY_LOW) AND (z IS VERY_LOW) THEN (p IS NOT);

RULE 1: IF (x IS VERY_LOW) AND (y IS VERY_LOW) AND (z IS LOW) THEN (p IS NOT);

RULE 2: IF (x IS VERY_LOW) AND (y IS VERY_LOW) AND (z IS MEDIUM) THEN (p IS NOT);

RULE 3: IF (x IS VERY_LOW) AND (y IS VERY_LOW) AND (z IS LARGE) THEN (p IS NOT);

RULE 4: IF (x IS VERY_LOW) AND (y IS VERY_LOW) AND (z IS VERY_LARGE) THEN (p IS NOT);

3.4 동작과정

〈그림〉과 같이 베이스 스테이션에서 예측한 전역 키 풀을 나눈 구획들 중에서 훼손된 구획의 비율, 훼손된 키의 비율, 그리고 각 노드의 잔여 에너지 비율 등의 여과율에 큰 영향을 주는 이 세 가지 요소를 가지고 현재 네트워크 상황에서 위조된 보고서의 여과에 전역 키 풀의 재분할(DIV)이 필요한지, 필요치 않은지(NOT) 또는 전역 키 풀의 훼손도가 너무 커져서 위조된 보고서에 대한 여과 능력을 상실하여 인증키를 이용한 SEF의 모든 여과과정을 종료 시켜(DIS) 이벤트 보고서의 길이를 줄여서 노드의 에너지 소비를 줄일지에 대한 결정을 한다.

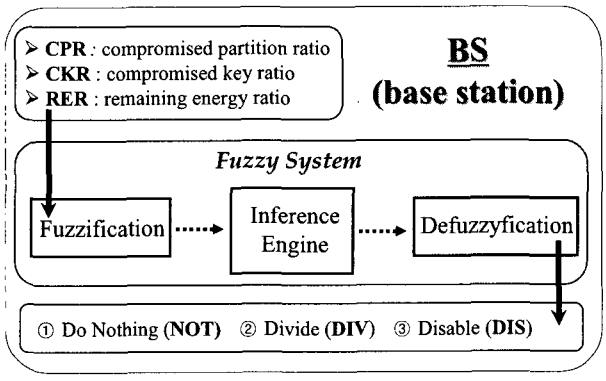
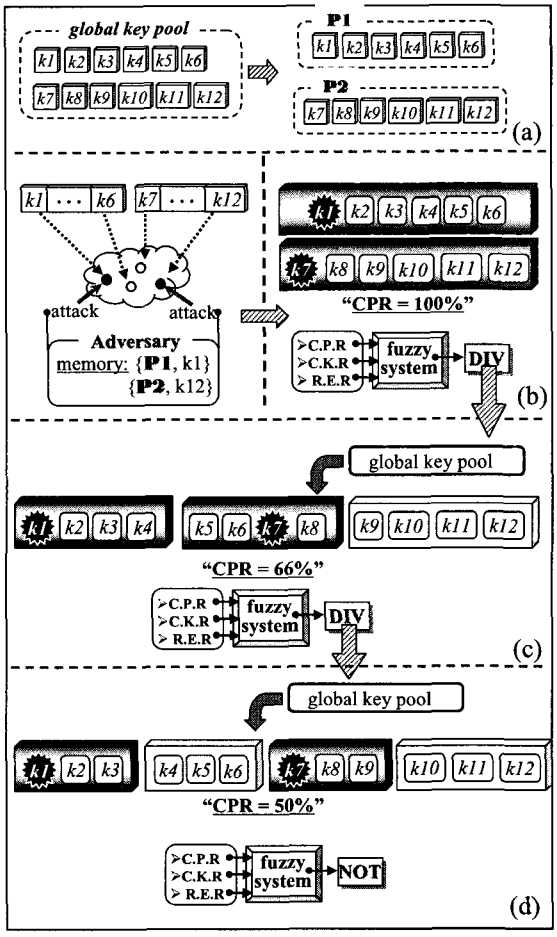


그림 4 퍼지 로직을 이용한 분할 여부의 결정

예를 들어 〈그림 (a)〉와 같이 최초 2개의 구획으로 나누어진 전역 키 풀의 키들 중에서 구획1의 k1과 구획2의 k7을 노드 훼손시켜 공격자가 획득했을 때, 훼손된 구획의

비율이 100%가 됨으로써, 훼손되지 않은 키들 k2, k3, k4, k5, k8, k9, k10, k11, k12까지도 인증키로써의 기능을 상실됨으로써 위조 보고서에 대한 검증을 할 수 없게 된다. 하지만 〈그림(b)〉와 같이 퍼지 로직을 통해 전역 키 풀의 재분할(DIV)이 결정되고, 이 결정에 따라 구획의 수를 〈그림(c)〉와 같이 전역 키 풀의 분할 중지를 의미하는 NOT 또는 SEF의 인증 기능 종료를 의미하는 DIS가 나올 때 까지 반복해서 증가시켜, 훼손된 키와 훼손 되지 않은 키를 서로 다른 구획으로 나누어서 훼손된 키의 비율이 100%에서 50%까지 감소하는 것을 볼 수 있다. 이 분할을 통해 훼손되지 않은 인증키가 위조 보고서를 검증할 수 있는 인증키로써의 기능을 할 수 있게 된다.



〈그림 5〉 퍼지 로직에 의한 전역 키 풀의 분할 여부 결정

4 결론 및 향후 과제

통계적 여과 기법에서 고정된 몇 개의 구획으로 나누어진 전역 키 풀 때문에 공격자가 특정 구획의 일부 인증키를 훼손시키면, 훼손된 인증키가 속해 있는 그 구획의 나머지 훼손되지 않은 인증키들 까지도 위조 보고서를 검증할 수 있는 인증키로써의 기능을 상실하게 돼는 문제점을 갖고 있다. 이를 해결하기 위해 본 논문에서는 전역 키 풀의 분할 여부 결정에 퍼지 로직을 적용하여 전역 키 풀을 네트워크 상황에 맞추어 나누워서 구획의 수를 증가시켜 인증키의 효율적인 사용을 보장하는 적응형 분할 결정 기법을 제안한다. 이 기법에서는 훼손된 구획의 비율, 훼손된 키의 비율, 노드의 잔여 에너지 비율을 고려한 퍼지로직에 의해 분할 여부를 결정한다. 향후 과제로는 통계적 여과 기법과 퍼지 기반의 적응형 통계적 여과기법의 평균 에너지 소비량과 여과율 등의 성능 분석을 위한 시뮬레이션을 수행하는 것이다. 그리고 시뮬레이션 결과의 비교분석을 통하여 제안한 기법의 효율성를 증명하고, 실제로 적용 가능한 분야를 제시하고자 한다.

참고문헌

[1] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," *ACM,Proceeding of SenSys*, pp. 255-265, 2003

[2] F. Ye, H. Luo, and S. Lu, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," IEEE, IEEE Journals on Selected Areas in Communications, vol. 23, No. 4, pp. 839-850, 2005.

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

[4] 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.