그룹 키 환경에서 지연 응답을 이용한 에너지 효율적인 오용키 탐지 방법

박민우, 한영주, 정태명
성균관대학교 정보통신공학부
e-mail : {mwpark, yjhan}@imtl.skku.ac.kr,
tmchung@ece.skku.ac.kr

A Misused Group Key Detection Mechanism based on Delayed Response

Min-Woo Park, Young-Ju Han, and Tai-Myoung Chung
School of Information Communication Engineering, Sungkyunkwan University

요 약

무선 센서 네트워크가 배포된 지역에 대하여 주기적으로 감시 값을 수집해야 하는 경우 라우팅 방법으로 계층적인 형태의 라우팅 방법을 주로 사용한다. 계층적인 형태의 라우팅 방법에는 특히, 클러스터를 구성하여 클러스터 리더가 클러스터에 속한 다른 노드들로부터 값을 모아 베이스 스테이션으로 전송하는 클러스터 기반 라우팅 방법이 일반적이다. 클러스터 기반 라우팅 방법의 경우 센서 노드간의 보안 서비스를 위해 그룹 키를 사용하는 경우가 있는데, 이 경우 그룹 키를 알고 있는 노드가 복수개 존재하기 때문에 그룹 키의 오용 가능성이 존재한다. 본 논문에서는 오용된 그룹 키를 탐지하기 위해 지연 응답 방법을 이용한 오용된 그룹 키 탐지 방법을 제안한다.

1. 서론

무선 센서 네트워크는 특정 지역에 분포하여, 그 지역에서 일어나는 이벤트를 관찰하기 위한 용도로 이용된다. 이때, 센서 노드로부터 수집된 값이 잘못된 경우 치명적인 피해를 일으킬 수 있어 센서 노드의 안정적인 동작은 필수적이다. 하지만 무선 센서 네트워크를 구성하는 센서 노드는 크기나 가격에 있어 크게 제한된다. 이로 인해 각 센서 노드는 계산 능력이나 메모리, 전력 등에서 매우 낮은 성능을 띤다. 특히 전력은 무선 센서 네트워크의 수명과 직결되는 요소로 무선 센서 네트워크에서 매우 중요한 디자인 요소로 꼽힌다.

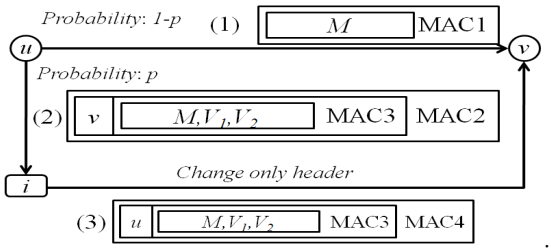
클러스터 기반 라우팅 방법은 분포된 센서 노드들을 위치에 따라 몇 개의 클러스터로 그룹화 한 후 클러스터의 리더가 클러스터 내에 존재하는 다른 센서 노드들로부터 값들을 모아 베이스 스테이션으로 전달하는 방법이다. 이 경우 상대적으로 먼 거리에 위치한 베이스 스테이션으로 송신하는 메시지의 수가 줄어들어 전체 에너지 소비 측면에서 효율적인 라우팅 방법으로 많이 연구되고 있다.

클러스터 기반 라우팅 방법을 사용하는 무선 센서 네트워크에서는 센서 노드간의 보안 서비스를 위해 메시지를 송·수신 하는 두 노드의 페어와이즈(pair-wise) 키를 사용하거나 클러스터 내의 센서 노드들이 공유하고 있는 그룹 키를 사용한다. 그룹 키를 사용하는 경우 하나의 메시지로 전체 센서 노드에 메시지를 전달할 때 용이하다. 하지만 그룹 키는 다수의 노드들이 동일한 키를 이용하기 때문에 해당 그룹 키가 오용될 위험이 존재한다. 본 논문에서는 이와 같이 그룹 키가 오용되는 경우 효과적으로 탐지하는 방법에 대해 제안한다.

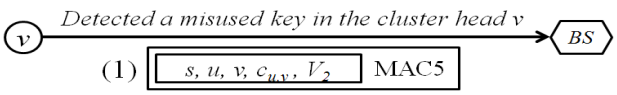
본 논문은 2장에서 오용키 탐지 기법에 대해 설명하고, 3장에서 본 논문에서 제안하는 오용키 탐지 기법에 대해 설명한다. 4장에서는 에너지측면에서의 성능 평가를 수행하며 5장에서는 본 논문의 결론 및 향후 연구 방향에 대해 제안한다.

2. 오용키 탐지 기법

확률적 키 분배 방법을 통해 키를 분배하는 환경에서 특정 페어와이즈 키가 오용되었는지 여부를 탐지하기 위한 방법은 Liu와 Dong에 의해 처음 제안되었으며, 그 후 클러스터 기반의 라우팅 기법을 사용하는 환경 보다 에너지 효율적인 탐지 기법인 자발적 탐지 기법이 제안되었다[1]. 자발적 탐지 기법의 동작 과정은 아래 (그림 1), (그림 2)와 같다[2].



(그림 1) 자발적 탐지 기법의 동작과정 (1)



(그림 2) 자발적 탐지 기법의 동작과정 (2)

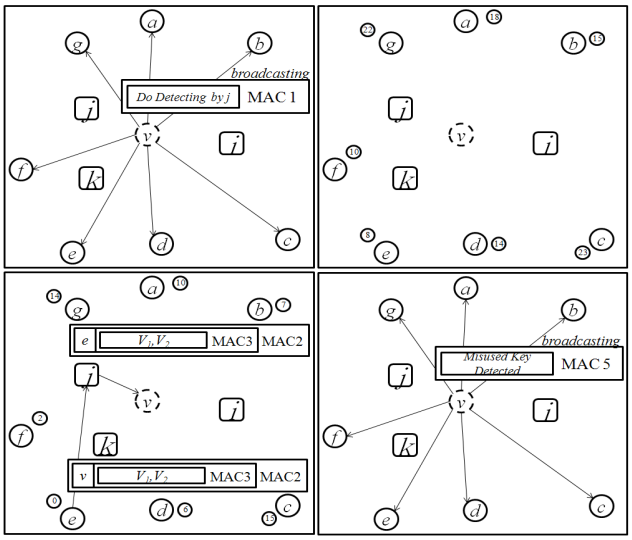
2.1 한계점

자발적 탐지 기법은 오용 키 탐지과정에서 클러스터 리더에 집중되는 오버헤드를 분산 시킬 수 있어 효율적이지만, 클러스터 내에 센서 노드가 n개 존재 할 때, n-1회의 검증과정이 모두 완료되기 전까지는 그룹 키의 오용여부를 탐지할 수 없다는 한계가 있다. 특히, 그룹 키의 오용 여부를 검증 중간에 밝혀진 후에도 각 센서 노드들의 오용키 검증 과정이 독립적으로 이루어지기 때문에 불필요한 검증 과정이 지속해서 진행되는 한계가 있다.

3. 지연 응답을 통한 그룹 키 검증 방법

본 논문에서는 지연 응답을 이용하여 자발적 탐지 기법의 한계점을 보완하는 방법을 제안 하였다.

그룹 키의 경우 클러스터를 구성하는 n-1개의 센서 노드 중에서 단 하나의 센서 노드에서라도 오용 사실이 밝혀지면 다른 센서 노드의 오용 여부의 검증이 불필요하다. 따라서 그룹 키의 오용 검증은 오용 검증을 알리는 메시지와 오용이 탐지되었음을 알리는 메시지를 추가하여 불필요한 검증 과정이 지속되는 것을 막을 수 있다. 동작 과정은 아래 (그림 3)과 같다.

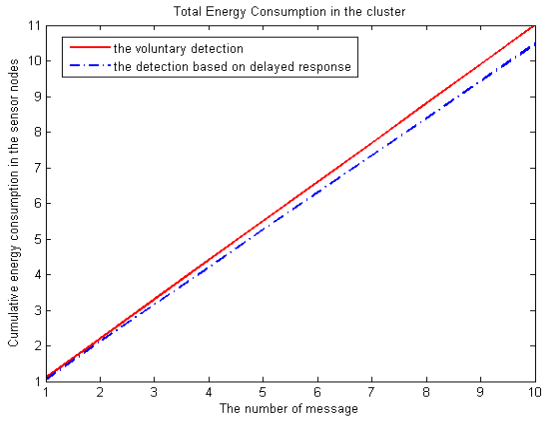


(그림 3) 지연 응답을 이용한 그룹 키 오용 여부 탐지

a, b, c, d, e, f, g 노드는 클러스터 내 센서 노드를 나타내며, v는 클러스터 리더, i, j, k는 안전 노드를 나타낸다[2]. v는 확률 p에 따라 그룹 키의 오용 여부를 탐지를 위해 센서 노드들에게 Do detecting 메시지를 브로드캐스팅 한다. 이때 메시지에는 안전 노드의 번호가 명시되어 있어야 한다. Do detecting 메시지를 수신한 각 센서 노드는 난수를 생성하여 타이머로 삼으며, 각각 타이머가 만료될 시기에 자발적 탐지 방법을 이용하여 그룹 키의 오용 여부를 탐지한다. 이때 v에서 그룹 키의 오용 여부가 밝혀지면, v는 이 사실을 다른 모든 노드에게 전달하여 그룹 키가 오용되었음을 알린 후 탐지 과정을 중단한다.

4. 성능 평가

본 논문에서는 지연 응답을 이용한 에너지 효율적인 그룹 키 오용 탐지 기법을 제안하였다. 아래 그래프는 지연 응답을 적용한 경우의 전체 노드의 에너지 소비 정도와 자발적 탐지 방법을 이용한 그룹 키 오용 탐지 시 전체 노드의 에너지 소비 정도를 비교한 것이다.



(그림 4) 전체 에너지 소비량

시뮬레이션은 결과는 매틀랩을 통해 10개의 노드로 이루어진 클러스터 내에서 100개의 메시지를 전송하는 과정에서 그룹 키의 오용 여부를 탐지를 일만회 반복한 것의 평균값으로 약 4.7%의 성능 향상을 보였다.

5. 결론 및 향후 연구

본 논문에서는 그룹 키를 사용하는 환경에서 자발적 탐지 방법의 에너지 효율을 증대시키기 위한 방안으로 지연 응답을 제안하였다. 이 경우 클러스터 리더가 오용 키 검증 과정의 시작과 종료를 알리는 추가적인 메시지가 필요 하지만, 전체의 노드의 에너지 효율로 보았을 때 보다 효율적인 성능을 나타냈다.

향후에는 그룹 키의 오용 여부가 탐지 되었을 때 보다 효율적으로 그룹 키를 재분배 하는 방법에 대한 연구를 진행할 것이다.

참고문헌

[1] D. Liu and Q. Dong, “Detecting Misused Keys in Wireless Sensor Networks”, IPCCC2007: Perform. Comp. and Comm. Conf., pp.272-280, April 2007.

[2] Min-Woo Park, Jong-Myoung Kim, Young-Ju Han and Tai-Myoung Chung, "A Misused Key Detection Mechanism for Hierarchical Routings in Wireless Sensor Network", NCM2008, pp.47, September 2008.