WSN 환경에서 토큰을 이용한 오용키 탐지 기법

강동민*, 박민우*, 박선호*, 정태명**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail : {dmkang, mwpark, shpark}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Misused Key Detection Scheme Using Token in WSN

Dong-Min Kang*, Min-Woo Park*, Seon-Ho Park*, Tai-Myoung Chung**
*Dept. of Electrical and Computer Engineering, Sungkyunkwan University
**School of Information Communication Engineering, Sungkyunkwan University

요 약

무선 센서 네트워크에서 키 관리는 센서노드들 간의 안전한 통신을 위해 필요하다. 초경량, 저전력, 단거리의 통신 제약을 갖는 센서노드들은 공격자에 의해 보다 쉽게 키가 노출 될 수 있다. 특히 확률적 키 분배 방식을 사용하는 환경에서는 키가 공격자에 의해 노출 될 경우 정상적인 센서노드간의 통신에 잘못된 정보를 삽입 할 수 있어 무선 센서 네트워크의 기능에 치명적인 영향을 준다. 이때 공격자에 의해 노출되어 악용된 키를 오용키(Misused Key)라고 하며, 본 논문에서는 토큰(token)을 사용하여 기존의 방법보다 에너지 효율적인 토큰 오용키 탐지 기법을 제안한다.

1. 서론

확률적 키 분배 방법을 사용하는 무선 센서 네트워크에서 보안 서비스를 제공하기 위해 많은 연구가 이뤄지고 있다. 확률적 키 분배 방법은 대칭키를 사용하면서도 적은 저장 공간을 사용 한다는 장점이 있지만, 두 센서노드 사이의 비밀키를 또 다른 센서노드가 알 수 있다. 따라서 확률적 키 분배 방법을 사용할 경우, 두 센서노드 사이의 비밀키가 공격자에게 드러날 수 있으며, 노출된 키를 통해 공격자가 메시지 삽입/변조 등을 수행할 경우 이러한 키를 오용키라 한다. 오용키는 무선 센서 네트워크에서 오작동을 유발할 수 있다. 본 논문에서는 무선 센서 네트워크가 정상적으로 동작할 수 있는 환경 구성을 위해 토큰(token)을 이용한 오용키 탐지 기법을 제안한다.

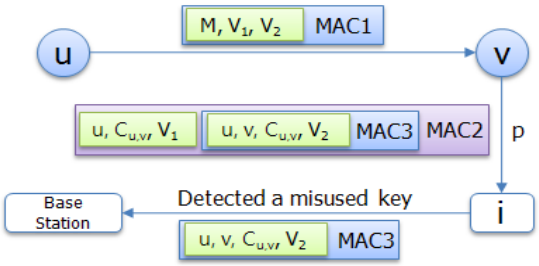
본 논문의 구조는 다음과 같다. 2 장에서는 Liu 와 Dong 의 오용키 탐지 기법에 대해 살펴보고, 3 장에서는 본 논문에서 제안하는 토큰을 이용한 오용키 탐지 기법에 대해 소개하며, 4 장에서는 성능평가를 통해 본 논문의 효율성을 증명하고, 5 장에서는 본 논문의 결론에 대해 제시한다.

2. Liu 와 Dong 의 오용키 탐지

Liu 와 Dong 은 확률적 키 분배를 사용하는 무선 센서 네트워크에서 센서노드들 사이의 오용키 탐지 기법을 제안했다. Liu 와 Dong 의 메인 아이디어는 누적된 해쉬값(committing value)과 각 노드와 베이스 스테이션(BS) 사이에 공유한 비밀값을 사용하는 것이다. 누적된 해쉬값은 단방향 통신에 대한 키의 오용여부를 판단하기 위해 사용되며, 각 노드와 BS 사이의 비밀값은 메시지를 인증하기 위해 사용된다.

2.1 동작과정

Liu 와 Dong 의 오용키 탐지 기법은 (그림 1)과 같이 동작한다.



(그림 1) Liu 와 Dong 의 오용키 탐지 기법

일반적인 센서노드 u 는 클러스터 헤더가 되는 노드 v 에게 M, V_1, V_2 를 전송한다. M 은 노드 u 의 메시지이고, V_1 과 V_2 는 오용키 여부를 검증 받기 위해 사용되는 값으로 $V_1 = H(C_{u,v}||H(K_{u,i})$, $V_2 = H(C_{u,v}||K_u)$로 계산된다. 앞의 식에서 $C_{u,v}$ 는 누적된 해쉬값으로, 노드 v 와 각각의 노드 u 가 독립적으로 관리한다. 노드 u 는 메시지를 전송할 때마다 메시지를 누적하여 $C_{u,v}$ 에 저장하고, 같은 방법으로 노드 v 도 노드 u 로부터 수신한 메시지를 누적하여 $C_{u,v}$ 에 저장한다. 검증노드 i 는 p 확률로 노드 u 와 노드 v 의 각 $C_{u,v}$ 를 비교하여 값이 다르면 키가 오용되었다고 판단하고 BS 에게 이를 알려 다시 키 분배를 한다.

2.2 Liu 와 Dong 의 문제점

Liu 와 Dong 의 오용키 검증 기법은 오용키 검증 시 모든 노드의 $C_{u,v}$ 를 비교 해야만 오용키를 탐지 할 수 있어 에너지 소비가 크다. 또한 오용키를 탐지할 수

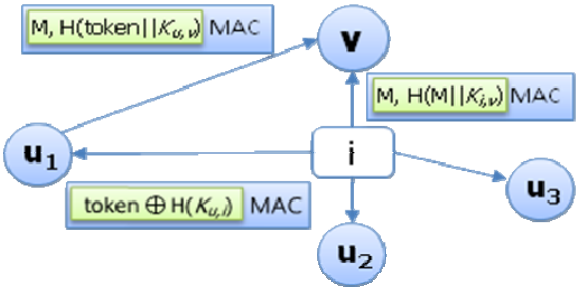
는 있지만 조작된 노드를 찾을 수 없기 때문에 계속적으로 키를 오용하여 메시지를 전송한다면, 통합된 데이터가 정확하지 않아 사용할 수 없게 되고, 키 분배를 다시 해야 하는 오버헤드가 발생한다.

3. 제안하는 토큰 오용키 탐지 기법

본 장에서는 Liu 와 Dong 기법의 문제점을 효율적으로 개선한 토큰 오용키 탐지 기법을 제안한다.

3.1 동작과정

제안하는 토큰 오용키 탐지 기법의 동작과정은 3 단계로 나뉘며, (그림 2)와 같이 동작 한다.



(그림 2) 토큰 오용키 탐지 기법의 동작과정

첫 번째 단계는 검증노드 i 가 토큰을 생성하고 클러스터 헤더 v 에게 전송하는 단계이다. 토큰값은 랜덤 하게 생성하여, 토큰을 받은 노드 외 다른 노드가 토큰을 예측 할 수 없게 한다. 또한 메시지 M 은 검증노드 i 가 만든 토큰들의 값이므로, 노드 v 에게 전송하는 과정에서 다른 노드들이 알 수 없도록 노드 v 와 노드 i 의 비밀키를 사용하여 전송한다.

두 번째 단계는 검증노드 i 가 각 노드(u_1, u_2, u_3)에게 토큰을 전송하는 단계이다. 검증노드 i 는 각 노드 u 와 검증노드 i 만 알고 있는 비밀키를 해쉬한 H($K_{u,i}$)와 토큰을 XOR 연산하여 각 노드에게 순차적으로 전송 한다. XOR 연산은 토큰과 두 노드간의 비밀키가 드러나지 않게 하기 위해 사용되며, 노드 u 는 H($K_{u,i}$) 값을 알고 있으므로 토큰 값을 얻어낼 수 있다.

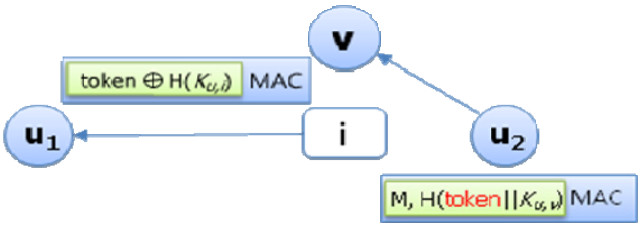
세 번째 단계는 토큰을 받은 노드 u 가 노드 v 에게 메시지를 전송하는 단계이다. 토큰을 받은 노드 u 는 메시지 M 과 $H(token||K_{u,v})$을 전송한다. 확률적 키 분배 방식을 사용하기 때문에 다른 노드들에게 $K_{u,v}$ 가 노출될 수 있지만, 다른 노드들는 토큰값을 알지 못하므로 메시지를 생성 할 수 없다. 또한 메시지를 전송할 때마다 토큰값에 +α를 계산하여, 다음 메시지 전송시 다른 노드들이 토큰값의 해쉬값을 유추하지 못하게 한다. 노드 v 는 받은 메시지의 해쉬값을 비교하여 오용 여부를 판단 하고, 오용키가 탐지되면 메시지를 차단한다. 이러한 과정을 거쳐 검증된 메시지만을 노드 v 가 통합하여 BS 에게 전송한다.

위의 1, 2 단계는 네트워크가 전개 되었을 경우와 클러스터 헤더가 변경되었을 경우에 발생하며, 노드들 사이의 데이터 전송은 3 단계에서 진행된다.

제안한 기법은 통합된 데이터의 정확성을 보증하기 위해 오용키 탐지 빈도 p 를 100%로 하여 인증된 데이터만을 통합하므로 보안성을 강화 할 수 있다.

3.2 시나리오

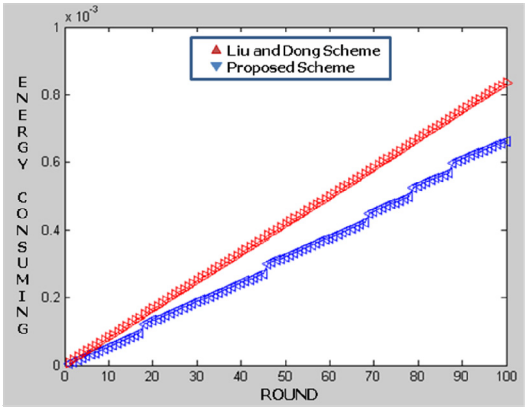
(그림 3)은 노드 u_1 이 토큰을 받았을 때, 노드 u_2 가 노드 u_1 과 노드 v 사이의 비밀키를 오용하여 u_1 인척 메시지를 전송하는 경우이다. 그러나 토큰값을 알지 못하므로, 노드 v 에게 오용키가 탐지 되고 메시지는 차단된다.



(그림 3) 오용키 탐지 예

4. 성능평가

토큰 오용키 탐지 기법의 성능 평가를 위해 Liu 와 Dong 기법과의 에너지 소비량을 비교 했다. 에너지 소비량은 무선 센서 네트워크의 수명과 직결되는 중요한 요소로 무선 센서 네트워크에서 매우 중요한 성능평가 요소로 꼽힌다. 성능평가 툴로는 매틀랩을 사용했으며, 성능평가의 오용키 탐지 빈도 p 는 100%로 설정했다. 성능평가 결과 제안한 토큰 오용키 탐지 기법이 에너지를 약 20% 적게 소모했다.



(그림 4) 에너지 소비율 비교

5. 결론

제안한 토큰 오용키 검증 기법은 검증된 메시지만을 받아 통합된 메시지가 정확한 데이터임을 보증한다. 오용키 탐지 빈도 p 를 100%로 할 때, 검증노드 i 에게 전송하는 오버헤드를 줄이므로 에너지 효율적이다. 성능 평가를 통해 이를 증명하였으며, 약 20%의 에너지 소비를 줄였다.

향후 연구로는 토큰의 제약을 해결하면서 에너지 효율적인 오용키 탐지 기법에 대해 연구하겠다.

참고문헌

[1] D. Liu and Q. Dong, “Detecting Misused Keys in Wireless Sensor Network”, IPCCC2007, Apr. 2007.

[2] D. M. Kang, M. W. Park, S. H. Park and T. M. Chung, “Misused Key Detection Mechanism in Wireless Sensor Network Using Group Key”, KSII2009, June. 2009