무선 센서 네트워크에서 에너지 효율적인 오용키 탐지 방법

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

A Energy Efficient Misused Key Detection in Wireless Sensor Networks

Min-Woo Park*, Jong-Myoung Kim*, Young-Ju Han**, Tai-Myoung Chung***
*Dept. of Electrical and Computer Engineering, Sungkyunkwan University
**Dept. of Computer Engineering, Sungkyunkwan University
***School of Information Communication Engineering, Sungkyunkwan University

요 약

무선 센서 네트워크에서 각각의 센서 노드들은 무선 통신을 통해 서로 간에 통신을 수행한다. 과거에는 이러한 센서 노드간의 통신을 제 3 자로부터 안전하게 지키는 것이 중요한 보안 이슈였다. 특히 보안 서비스를 제공 하기 위한 키 관리 기법들이 주요 연구방향이었다. 하지만 안전하게 만들어진 확률론적 키(key)를 기반으로 하는 키 사전분배 방법은 공격받은 다른 노드로 인해 자신의 키가 노출 될 수 있다. 공격자는 노출된 공유키(shared key)를 통해 노출되지 않은 정상 노드(non-compromised node) 사이의 대칭키(pairwise key)를 얻을 수 있으며, 공격자는 네트워크에 심각한 영향을 줄 수 있는 메시지 삽입 및 수정 공격을 감행할 수 있다. 이와 같은 오용된 키를 폐기하고 메시지 삽입 및 수정 공격을 막기 위해 Liu and Dong 은 오용키 탐지 방법을 제안하였다. 하지만 이들의 방법에는 한계점이 있어 이를 보완하기 위한 에너지 효율적인 오용키 탐지 기법을 제안한다.

1. 서론

무선 센서 네트워크는 무선 통신이 가능한 작은 크기의 제한된 성능을 지닌 다수의 센서 노드들로 구성된다. 센서 노드들은 장착된 센서들을 통해 주변 정보를 수집하고 이를 베이스스테이션(Basestation)에 제공하는 역할을 한다. 무선 센서 네트워크는 군사, 학문, 기업, 관측 등 다양한 분야에서 연구되고 있다.

센서 노드들은 서로간의 무선 통신을 통해 베이스스테이션까지 수집한 정보를 전달하는데, 이때 무선 통신의 특성상 도청이나 전파방해 등에 매우 취약한 성격을 띤다. 이러한 사항을 보완하기 위해 무선 센서 네트워크는 암호화나 인증 등 다양한 보안 서비스를 필요로 한다. 하지만 센서 네트워크를 구성하는 센서 노드들은 대개 낮은 성능을 가진다. 따라서 일반적인 애드혹(ad hoc) 환경에서 사용하는 보안 서비스를 도입 하는 것은 무리가 있다. 제한된 계산 능력과 저장 능력, 그리고 낮은 파워로 인해 무선 센서 네트워크에서 암호방식은 많은 계산 능력을 필요로 하는 공개키 방식보다 비교적 적은 계산능력으로 가능한 대칭키 방식이 주로 사용된다. 특히, 대칭키 방식 중에서도 저장능력의 제약 등으로 인해 모든 노드가 대칭키를 분배하는 방법이 아닌 확률적인 방법으로 키를 분배하는 확률론적 키 사전분배 방법을 사용한다.

확률론적 키 사전분배 방법에 따른 키 분배 시 하나의 공유키를 2 개 이상의 센서 노드가 나눠 가지는 경우가 많다. 따라서 통신하는 두 노드가 공격자에 의해 조작되지 않은 노드(non-compromised)일 지라도 두 노드 사이의 공유키가 공격받은 다른 노드를 통해 드러날 수 있다. 그렇게 되면 공격자가 조작되지 않은 두 센서 노드 사이의 메시지를 임의로 삽입 또는 수정이 가능해지며, 이러한 목적으로 악용되는 키를 오용키라고 부른다. (그림 1)은 오용키와 일반 센서 노드들 간의 관계를 나타낸 것이다. 오용키를 통해 공격자가 자신이 원하는 메시지를 삽입하면 무선 센서 네트워크가 잘못된 정보를 취급하게 되어 매우 치명적인 결과를 낳게 된다.

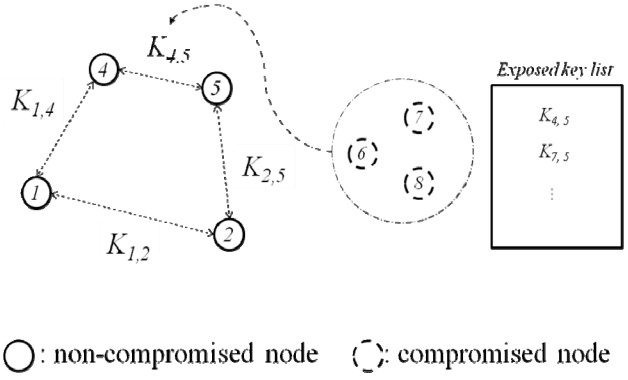
따라서 오용키의 사용을 검증하고 이를 막는 것이 무선 센서 네트워크의 정상적인 동작을 위해 필수적이다.

최근 오용키 검증을 위한 연구가 진행되고 있다. Liu 와 Dong 의 검증 노드(detecting node)를 통한 검증 방법이 대표적인 오용키 검증 방법에 속한다. 하지만 이들의 메커니즘은 불필요한 보고(reporting) 메시지를

매번 전송하여야 하며, 오직 단방향의 통신에 대해서만 오용키를 탐지할 수 있는 등 많은 한계점을 가진다.

본 논문에서는 불필요한 보고 메시지를 삭제하면서 동시에 양방향 통신에 대한 인증을 가능하게 하는 에너지 효율적인 오용키 검증 방법을 제안한다.

본 논문의 구조는 아래와 같다. 2 장에서는 Liu and Dong 의 오용키 탐지 방법에 대해 살펴보고, 3 장에서는 본 논문에서 제안하는 에너지 효율적인 오용키 탐지 기법에 대해 소개하며, 4 장에서는 에너지 측면에서의 성능 평가를 통해 에너지 효율을 비교하며, 5 장에서는 본 논문의 결론과 향후 과제에 대해 제시한다.



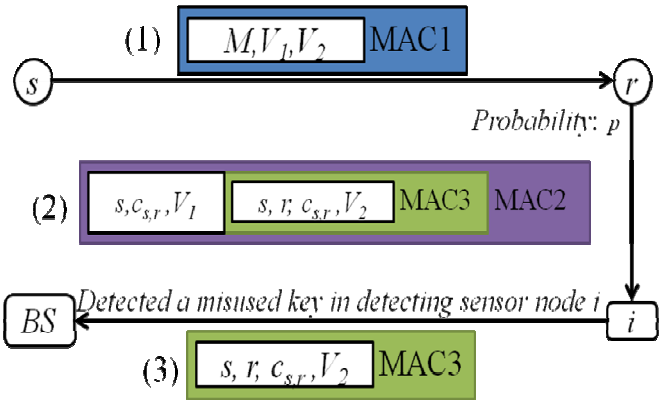
(그림 1) 오용키의 예

2. Liu 와 Dong 의 오용키 검증 과정

2.1 동작 과정

오용키를 검증 하기 위해 Liu 와 Dong 은 특수한 센서 노드를 도입한 분산 검증 메커니즘을 제안하였다. 오용키 검증을 위해 추가된 센서 노드를 검증 노드라고 부르며, 검증 노드는 다른 일반적인 센서 노드와 다른 특수한 노드로 오직 검증에만 사용 되는 노드이다. 검증 노드는 각각의 센서 노드들과 유일하게 나눠가진 유일키(unique key)를 가지고 있으며, 이를 통해 검증 작업을 수행한다. 이러한 유일키는 각각의 센서 노드가 BS 와 나눠가진 비밀키(K_s)와 검증 노드를 식별값 $ID(i)$의 해쉬값 $H(K_s||i)$을 통해 생성된다. 검증 노드와 센서 노드간의 유일 키는 기존의 센서 노드가 BS 와 공유하고 있는 키로부터 계산되는 값이므로 각 센서 노드는 추가적인 메모리 부하(overhead)는 들지 않는다. 이러한 검증 노드는 물리적으로 대량의 정보를 저장하여야 하기 때문에 다른 센서 노드와 물리적인 차이점을 가진다.

Liu 와 Dong 의 검증 방법은 (그림 1)과 같다. 그림에서 노드 s, r 은 각각 메시지를 전송하는 센서 노드와 수신하는 센서 노드이다. Liu 와 Dong 의 검증 방법에서는 s 가 r 로 보내는 단방향의 메시지에 대해서만 오용키 검증이 가능하다. 노드 i 는 앞서 설명한 검증 노드로 검증 받기를 위하는 수신 노드 r 이 검증을 요청하는 경우에만 검증을 수행한다. BS 는 베이스스테이션으로 최종적으로 센서 노드 s 와 r 사이의 공유키가 공개되었는지 확인한다.



(그림 2) Liu 와 Dong' s 오용키 검증 방법

Liu 와 Dong 의 방법은 2 차례에 걸쳐서 검증을 수행한다. 첫 번째 검증은 검증 노드 i 에서 이루어 지며, 두 번째 검증은 베이스스테이션 BS 에서 이루어진다. 오용키 검증을 위해 센서 노드 s 는 지속적으로 검증에 사용되는 검증값 V_1, V_2 를 노드 r 에게 전송한다. 이때 V_1 은 아래 수식 (1)과 같이 구해진다. $H(K_s||i)$는 앞서 살펴본 센서 노드 s 와 검증 노드 i 사이의 유일한 키를 나타낸다. 수식 (1)의 $C_{s,r}$ 은 검증을 위해 사용하는 변수로 누적 해쉬값(cumulative hashed value)이라 부른다. 누적 해쉬값은 센서 노드 s 가 센서 노드 r 에게 보낸 메시지와 누적 해쉬값을 함께 해쉬 함수를 통해 계산한 값으로 수식 (2)와 같다. 누적 해쉬값의 초기값은 0 과 같다. 누적 해쉬값은 센서 노드 s 와 r 이 각각 독립적으로 관리하고 있으며, 두 값이 달라지면, 이는 임의의 메시지가 삽입되었거나, 수정되었음을 의미한다. 검증 노드 i 는 s 로부터 받은 V_1 과 메시지 (2)에 포함된 센서 노드 r 의 $C_{s,r}$ 값을 바탕으로 두 노드의 $C_{s,r}$ 를 비교 할 수 있다.

$$V_1 = H(C_{s,r} \| H(K_s \| i)) \quad (1)$$

$$\begin{cases} C_{s,r} = 0 \\ C_{s,r} = H(C_{s,r} \| M) \end{cases} \quad (2)$$

검증 노드 i 는 오용키를 발견할 시 메시지(3)을 BS 로 전달한다. 메시지 (3)에 포함되어 있는 V_2 값은 수식 (3)과 같이 구해진다. 이때 K_s 는 BS 와 센서 노드 s 사이의 유일한 키로 이를 알고 있는 BS 만이 센서 노드 s 와 r 의 누적 해쉬값을 비교할 수 있다. BS 의 2 차적인 검증을 통해 오용키가 재차 확인되면 BS 는 센서 노드 s, r 사이의 공유키를 폐기시키고 새로운 키를 분배한다.

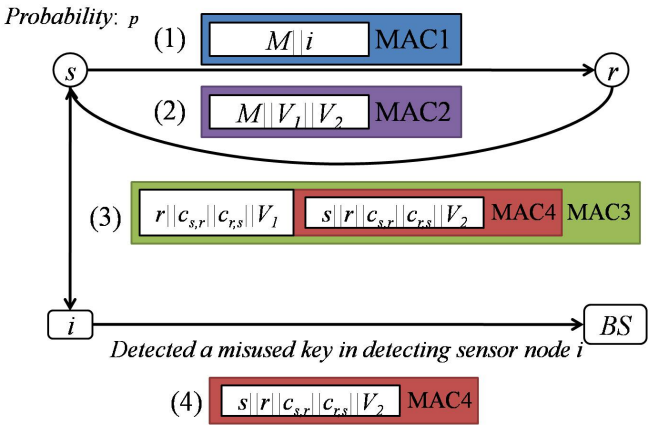
$$V_2 = H(C_{s,r} \| K_s) \quad (3)$$

2.2 한계점

Liu 와 Dong 의 검증 방법은 몇 가지 한계점을 가진다. 첫째, 검증 과정은 실제로 센서 노드 r 에 의해 확률 p 에 따라 수행 되지만, 센서 노드 s 는 불필요한 V_1, V_2를 매번 센서 노드 r 에게 전송하여야 한다. 이는 제한된 전력을 가지는 센서 노드의 에너지를 고갈시켜 무선 센서 네트워크에게 매우 치명적이다. 둘째, 검증 과정이 단방향에 대해서만 이루어 진다. 즉, s 가 r 에게 전송하는 메시지 사이에 오용키를 통해 삽입 또는 변조 된 메시지가 있는지 찾을 수 있다. 그 역방향인 r 이 s 에 전달하는 메시지에 대해서는 따로 검증 과정을 수행하여야지 오용키를 검증할 수 있어 비효율 적이다. 셋째, Liu 와 Dong 의 검증 방법에서는 검증 과정 중에 인접한 검증 노드의 목록을 넘겨주는 과정에 대해 정의되지 않았다. 따라서 검증 과정을 수행하기 위해서는 두 센서 노드 간의 통신이 이루어지기 이전에 목록에 대한 교환이 필요하다. 이러한 추가적인 메시지도 무선 센서 네트워크에서는 지양해야 하는 사항이다.

3. 에너지 효율적인 오용키 탐지 방법

본 논문에서는 Liu 와 Dong 의 비효율적인 측면을 보완하여 에너지 효율적인 오용키 탐지 방법에 대해 제안한다.



(그림 3) 제안하는 메커니즘의 동작 과정

제안 하는 메커니즘의 동작 과정은 (그림 3)과 같다. s 와 r 은 각각 센서 노드이며, i 는 센서 노드 s 와 인접한 위치에 있는 검증 노드이며, BS 는 베이스스테이션을 나타낸다. 이때 센서 노드 s, r 은 서로 메시지를 송수신하며, 이때 송수신하는 메시지에 대하여 각각 두 개의 누적 해쉬값 $C_{s,r}$ 과 $C_{r,s}$ 를 독립적으로 관리한다. 누적 해쉬값은 Liu 와 Dong 의 메커니즘과 동일한 방법으로 계산된다. 센서 노드 r 은 오용키 검증을 위해 V_1 과 V_2 를 생성하여 s 에게 전달하며, 이를 수신한 s 는 검증 노드 i 에게 오용키 검증을 요청한다. 이때 V_1 과 V_2 는 각각 식 (4), (5)와 같이 구해지며, V_1 를 계산할 때 필요한 검증 노드의 식별자는 센서 노드 s 를 통해 전달 받는다. 식별자 i 는 센서 노드 s 에 인접한 검증 노드들 중 하나로 s 에 의해 선택되어 전달된다.

$$V_1 = H(C_{s,r} \| C_{r,s} \| H(K_r \| i)) \quad (4)$$

$$V_2 = H(C_{s,r} \| C_{r,s} \| K_r) \quad (5)$$

센서 노드 s 는 r 로부터 전달받은 V_1, V_2 와 자신의 $C_{s,r}$ 과 $C_{r,s}$ 를 이용하여 메시지 (3)을 만들어 검증 노드에게 전달한다. 검증 노드 i 는 메시지 (3)을 수신하면 첫 번째 값을 읽어 들여 검증에 필요한 공유키 $H(K_r||i)$를 구해낸후, 센서 노드 s 의 $C_{s,r}$ 과 $C_{r,s}$ 값을 통해 수식 (4)와 같이 V_1'값을 계산한다. 그 결과 수신한 V_1과 계산한 V_1'가 같다면 두 센서 노드 s, r 사이에는 오용키가 없었던 것으로 판단한다.

두 값이 다르다면, 검증 노드 i 는 오용키를 탐지한 것으로 판단하고 베이스스테이션에 메시지 (4)를 전달한다. 베이스스테이션은 메시지 (4)에 포함된 V_2 와 센서 노드 식별자 r 을 통해 검증에 사용되는 키 K_r 을 구해낸다. 그 후 센서 노드 s 의 $C_{s,r}$ 과 $C_{r,s}$ 값를 통해 V_2'를 구하여 수신한 V_2 와 비교한다. 비교 결과 두 값이 다르면 오용키가 발생된 것으로 판단하고 센서 노드 s 와 r 사이의 공유키를 폐기시킨다. 그렇지 않다면 오용키가 없는 것으로 판단하고 검증 과정을 종료한다.

4. 성능 평가

에너지 효율적인 오용키 탐지 기법은 불필요한 검증 메시지를 전송하지 않고, 한번의 검증을 통해 양방향 검증을 수행함으로써, 기존의 Liu 와 Dong 의 오용키 검증 방법에 비해 에너지 효율을 대폭 증가시켰다. 매틀랩을 통한 시뮬레이션으로 제안 하는 메커니즘과 Liu 와 Dong 의 오용키 검증 방법의 에너지 효율을 비교하였다.

4.1 실험 환경

<표 1> 실험 환경

Parameter	Value
Eelec	50nJ
Efs	10pJ/bit/m2
Emp	0.0013pJ/bit/m4
Size of CV	8 bytes
Size of Cs,r	8 bytes
Size of message	80 bytes
Size of node ID	4 bytes
Size of MAC	8 bytes
Average of d	6 m

무선 센서 네트워크에서 메시지의 크기는 미약하다. 메시지 내용은 주로 온도나 조도, 습도와 같은 환경정보가 보통이기 때문이다. 그에 비해 오용키 검증에 사용되는 V_1 과 V_2 는 해쉬값으로 일반적으로 8 bytes 정도의 크기로 메시지의 크기를 생각할 때 센서 노드

에 큰 부하로 작용한다. 따라서 불필요한 V_1 과 V_2 의 송수신을 줄여 에너지 효율을 극대화 하였다. 에너지 효율은 실제 first order radio model 을 사용하였다. 에너지 소모량은 아래 수식 (6), (7)과 같다.

$$E_{trans} = \begin{cases} l \times (E_{elec} + E_{fs} \times d^2), ifd \le \sqrt{\frac{E_{fs}}{E_{mp}}} \\ l \times (E_{elec} + E_{fs} \times d^4), ifd > \sqrt{\frac{E_{fs}}{E_{mp}}} \end{cases} \quad (6)$$

$$E_{recive} = l \times E_{elec} \quad (7)$$

성능 평가 결과 제안하는 메커니즘이 Liu 와 Dong 의 오용키 검증 방법에 비해 높은 에너지 효율을 보였다. 그 결과는 아래 <표 2>와 같다. <표 2>는 각각 검증 확률 p 에 따라 평균적인 에너지 효율을 나타낸 표이다. 표로 볼 때 평균 36%가량 본 논문에서 제안하는 메커니즘이 Liu 와 Dong 의 오용키 검증 방법에 비해 효율적인 것으로 나타났다.

<표 2> 평균 에너지 효율

Probability p	Energy Saved
p = 0.05	29%
p = 0.1	44%
p = 0.2	35%
Average	36%

5. 결론

본 논문에서는 에너지 효율적인 오용키 검증 방법에 대해서 살펴 보았다. 제안하는 메커니즘은 기존의 Liu 와 Dong 의 오용키 검증 방법의 한계점을 개선하고, 불필요한 메시지 수를 대폭 줄이면서도, 중복해서 수행해야 하였던 양방향 검증을 한번의 검증을 통해 수행할 수 있는 새로운 메커니즘을 제안하였다. 제안하는 메커니즘의 성능 평가를 위해 first order radio model 을 통해 메시지 전송에 소모되는 에너지 효율을 매틀랩을 통해 시뮬레이션 하였다. 그 결과 평균적으로 본 논문에서 제안하는 메커니즘의 에너지 효율이 36%가량 높게 나왔다.

향후 시뮬레이션에 그치지 않고 제안 하는 검증 메커니즘을 실제로 구현을 통해 성능 평가를 수행하도록 하겠다. 또한, 보다 효율적인 오용키 검증 방법에 대한 연구를 지속할 것이다.

참고문헌

[1] S. A. CAMTEPE and B. YENER. Key distribution mechanisms for wireless sensor networks: A survey. Technical report, Rensselaer Polytechnic Institute, March 2005.

[2] P. N. Donggang Liu and W. Du. Group-based key predistribution in wireless sensor networks. Proc. 2005 ACM Wksp. Wireless Security, September 2005.

[3] L. Eschenauer and V. Gligor. A key management scheme for distributed sensor networks. Proc. 9th ACM Conf. Comp. and Commun.Sec., November 2002.

[4] A. P. Haowen Chan and D. Song. Random key predistribution schemes for sensor networks. Proc. IEEE Sec. and Privacy Symp., May 2003.

[5] D. Liu and Q. Dong. Detecting misused keys in wireless sensor networks. IPCCC 2007, April 2007.

[6] M. M. M. Eltoweissy and R. Mukkamala. Dynamic key management in sensor networks. IEEE Communications Magazine, 44:122–130, August 2006.

[7] V. Mhatre and C. Rosenberg. Design guidelines for wireless sensor networks: Communication, clustering and aggregation. Ad. Hoc. Networks, 2:45–63, January 2004.

[8] A. P. C. Wendi B. Heinzelman and H. Balakrishnan. An application-specific protocol architecture for wireless microsensor networks. IEEE Transaction on Wireless Communications, 1(4):660–670, October 2002.

[9] Y. S. H. S. C.Wenliang Du., Jing Deng. and P. K. Varshney. A key management scheme for wireless sensor networks using deployment knowledge. IEEE INFOCOM2004, March 2004.

[10] M. W. Park, J. M. Kim, Y. J. Han, T. M. Chung, "A Misused Key Detection Mechanism for Hierarchical Routings in Wireless Sensor Network", NCM2008, Sep, 2008.