플랫 구조의 센서 네트워크 환경에 적용 가능한 키 합의 프로토콜[1)]

민선미° 윤은준 김우헌 유기영
경북대학교 컴퓨터공학과 정보보호연구실
{msm20°, ejyoon, whkim}@infosec.knu.ac.kr, yook@knu.ac.kr

A Key Agreement protocol applicable for Flat structured Sensor Networks

Seon-Mi Min° Eun-Jun Yoon Woo-Hun Kim Kee-Young Yoo
Dept. of Computer Engineering, Graduate School, Kyoungpook National University, Daegu, Korea

요 약

센서 네트워크는 다수의 센서 노드들을 이용하여 특정위치의 물리적 데이터를 수집함으로써 이를 베이스 스테이션에게 전달해 주는 초소형, 저가, 저전력 무선 통신 기술이다. 센서 네트워크의 센서 노드들은 제한된 전력을 가지기 때문에 센서 노드의 에너지 소모를 줄이며 신뢰성 있게 데이터를 전송하는 프로토콜의 설계가 중요시 되고 있다. 본 논문에서는 이러한 센서 네트워크 환경의 특성을 고려하여 대칭키(Symmetric key)방식을 기반으로 플랫 구조의 센서 네트워크 환경에 적용 가능한 키 합의 프로토콜을 제안한다. 제안하는 프로토콜은 세션키 생성 단계에서 센서의 ID와 랜덤수를 이용하여 세션키를 생성하고 통신하는 노드 중 한 노드가 세션키를 확인한다. 이 노드는 세션키 확인 단계를 통해 데이터 전송 시 세션키 확인에 필요한 정보를 전송하여 상호 세션키 확인이 이루어지게 하며, 세션키 생성 단계와 확인 단계가 정당하게 이루어지면, 이후에 발생하는 세션키는 서브 프로토콜을 이용하여 생성함으로써 효율적으로 통신함을 보인다.

1. 서 론

센서 네트워크(sensor network)란 다수의 센서들을 관심 클러스터에 임의로 설치하여 그 클러스터의 물리적 데이터를 센싱하고 주어진 통신경로를 통해 중앙의 베이스 스테이션으로 전송하는 것을 말한다. 즉, 센서에 네트워크 개념을 적용하여 컴퓨팅 능력과 무선 통신 능력을 갖는 센서 노드가 자율적으로 네트워크(self-organizing)를 형성하고, 여기서 발생한 데이터를 네트워크를 통하여 원격지로 전송하는 기술이다[1].

이러한 센서 네트워크를 보다 다양한 분야에 활용하기 위해서는 에너지문제와 보안문제가 우선적으로 해결되어져야 한다. 센서 노드는 제한된 에너지를 가지고 있을 뿐만 아니라 실제로 이를 이용하는데 있어서 센서 노드의 배터리 교환이나 충전이 어렵기 때문에 각 센서 노드들의 에너지 소모를 줄이는 것이 센서 네트워크 환경에 중요하다. 또한 악의적인 공격자에 의해 전송되는 데이터가 노출 또는 변경되는 것은 심각한 문제를 야기 시킬 수 있으므로 센서 네트워크에서 보안을 위해 신뢰성 있는 보안 프로토콜의 설계가 요구된다.

센서 네트워크는 센서 노드와 베이스 스테이션만을 갖는 플랫 구조(flat structure)와 게이트웨이 노드까지 가지는 계층적 구조(hierarchical structure)로 분류한다[2]. 계층적 구조를 가지는 센서 네트워크 환경에서는 게이트웨이 노드가 해당 지역의 모든 데이터를 수집 및 처리하기 때문에 조기 에너지 소멸로 빈번하게 새로운 게이트웨이를 지정해야 하는 문제점이 있다. 그러나 플랫 구조의 센서 네트워크 환경은 센서 노드가 수집한 데이터를 자신과 가장 가까운 노드에게 보내어 베이스 스테이션으로 전송하게 함으로써 계층적 구조에서 가지는 게이트웨이 재지정의 문제점을 피할 수 있다. 따라서 본 논문에서는 이러한 센서 네트워크 환경의 특성을 고려하여 대칭키 방식을 기반으로 노드간의 공유된 비밀 정보를 이용하여 해당 세션에서 사용될 세션키를 생성 및 합의한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안하는 키 합의 프로토콜을 기술하며, 3장에서 이 프로토콜의 보안성 및 안전성을 분석한다. 마지막으로 4장에서 결론을 맺는다.

2. 제안하는 키 합의 프로토콜

본 장에서는 제안하는 프로토콜에 사용되는 용어의 정의와 가정을 제시하고, 플랫 구조의 센서 네트워크 환경에 적용 가능한 키 합의 프로토콜을 제안한다.

제안하는 프로토콜에서 사용되는 용어는 다음과 같다.

- BS : 베이스 스테이션
- S_A : 센서 A
- S_B : 센서 B
- DID_A : A의 디바이스 ID
- ID_A : 해당 세션에서 A의 ID
- K_{AB} : A와 B의 사전 공유 비밀키
- sk_{AB} : A와 B의 세션키
- R : 랜덤수
- $PVER$: 문자열 결합

노드 A는 라우팅 알고리즘이 적용된 경로를 따라 자신의 앞뒤에 위치한 두 개의 노드(BS, B)와 각각의 비밀키인 K_{BSA}, K_{AB}를 미리 저장하여 통신한다.

제안하는 키 합의 프로토콜은 ID 요청 메시지를 베이스 스테이션에게 전송하여 ID를 부여받고, ID와 랜덤수를 이용하여 세션키를 생성한다. 세션키 생성과정에서 BS와 S_A의 세션키는

1) 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음

S_A, S_A와 S_B의 세션키는 S_B만이 확인함으로, 수집된 데이터의 전송이 필요한 경우 세션키의 확인정보를 보내어 상호 세션키 확인이 이루어지게 한다. 세션키 생성 단계와 확인 단계가 정당하게 이루어지면, 이후의 세션키 생성에는 서브 프로토콜을 사용함으로써 세션키 생성에 필요한 연산과정을 줄여 노드의 에너지 소모를 감소시킨다.

2.1 세션키 생성 단계

세션키는 ID와 랜덤수를 이용하여 생성한다. 세션키 생성 단계는 다음과 같다.

(1) $S_B \rightarrow S_A : (DIID_B PVERR_B)_{K_{AB}}$
경로를 따라 베이스 스테이션에서 가장 멀리 있는 노드 S_B가 S_A에게 ID 요청 메시지를 전송한다. 이때 메시지는 S_B와 S_A사이의 세션키 생성에 필요한 랜덤수(R_B)를 포함하며, 두 노드가 공유하고 있는 비밀키로 암호화하여 전송된다.

(2) $S_A \rightarrow BS : (DIID_A PVERDIID_B PVERR_A)_{K_{BSA}}$
S_A는 받은 메시지를 복호화하여 랜덤수를 저장하고, BS에게 S_B와 자신의 ID 요청 메시지를 전송한다. 이때 사용되는 랜덤수(R_A)와 비밀키는 (1)에서 사용되는 것과 같은 역할을 수행한다.

(3) $BS \rightarrow S_A : ID_{AB}, X_{BSA}, (R_{BS} PVERR'_{BS})_{R_A}$
BS는 수신한 메시지를 사전에 공유한 비밀키로 복호화 한 후, DID를 확인하고 해당 노드의 세션 ID를 부여한다. BS는 세션키 생성에 필요한 랜덤수(R_{BS})를 선택한 후 ID 정보(ID_{AB})와 세션키(sk_{BSA}) 생성 및 확인에 필요한 정보(X_{BSA})를 다음과 같이 생성하여 S_L에게 전송한다. 이때 BS와 S_A간의 세션키는 해당 ID와 선택한 랜덤수 그리고 S_A에서 받은 R_A를 이용하여 생성된다. BS의 전송 메시지 내용 중 R'_{BS}는 다음 세션의 세션키 생성에 필요한 랜덤수이다.

$$ID_{AB} = (ID_A PVERID_B PVERID_{BS})_{K_{BSA}}$$
$$sk_{BSA} = h(ID_{BS} PVERID_A PVERR_{BS} PVERR_A)$$
$$X_{BSA} = h(ID_{BS} PVERsk_{BSA} PVERR_{BS})$$

(4) $S_A \rightarrow S_B : ID'_{AB}, X_{AB}, (R_A PVERR'_A)_{R_B}$
먼저 S_L는 BS로부터 수신한 정보를 이용하여 다음과 같이 세션키(sk'_{ESA})와 세션키 확인 정보를 생성한 후 BS가 생성한 세션키(sk_{ESA})와 세션키 확인 정보와 동일한 지 확인한다.

$$sk'_{BSA} = h(ID_{BS} PVERID_A PVERR_{BS} PVERR_A)$$
$$X'_{BSA} = h(ID_{BS} PVERsk'_{BSA} PVERR_{BS})$$
$$X_{BSA} \stackrel{?}{=} X'_{BSA}$$

이후 S_L는 해당 ID와 자신의 랜덤수 그리고 단계 (1)에서 S_L로부터 받은 랜덤수를 이용하여 S_L와의 세션키(sk_{AB})를 생성한다. 생성한 세션키를 S_L가 확인 할 수 있도록 ID정보(ID'_{AB})와 세션키 확인 정보(X_{AB})를 다음과 같이 생성하여 S_L에게 전송한다. S_L의 메시지 내용 중 R'_A는 다음 세션의 세션키 생성에 필요한 랜덤수이다.

$$ID'_{AB} = (ID_A PVERID_B)_{K_{AB}}$$
$$sk_{AB} = h(ID_A PVERID_B PVERR_A PVERR_B)$$
$$X_{AB} = h(ID_A PVERsk_{AB} PVERR_A)$$

(5) S_B는 S_A로부터 받은 정보를 이용하여 다음과 같이 S_A와 동일한 방법으로 세션키(sk'_{AB})를 생성하고, S_L와 동일한 세션키가 생성되었는지를 확인 정보(X'_{AB})로 확인한다.

$$sk'_{AB} = h(ID_A PVERID_B PVERR_A PVERR_B)$$
$$X'_{AB} = h(ID_A PVERsk'_{AB} PVERR_A)$$
$$X_{AB} \stackrel{?}{=} X'_{AB}$$

(1)부터 (5)까지의 과정을 통하여 BS과 S_A, S_L과 S_L의 세션키가 생성되었다.

2.2 세션키 확인 단계

BS과 S_L의 세션키는 S_A, S_A과 S_B의 세션키는 S_B만이 확인하였음으로 상대방도 세션키를 확인할 수 있도록 데이터 전송 시 세션키 확인에 필요한 정보를 보낸다. 데이터는 S_B로부터 BS로 전송되며, 데이터 전송 시에 이루어지는 세션키 확인 단계는 다음과 같다.

(1) $S_B \rightarrow S_A : (M_E)_{sk'_{AB}}, X_Z$
S_B는 ID와 자신의 세션키 그리고 랜덤수를 이용하여 세션키 확인 정보(X_Z)를 생성하고, 보내고자 하는 메시지(M_B)를 세션키로 암호화한 후 암호화된 메시지와 확인 정보를 S_L에게 전송한다.

$$X_Z = h(ID_B PVERsk'_{AB} PVERR_B)$$

(2) $S_A \rightarrow BS : (M_A PVERM_B)_{sk'_{BSA}}, X_Y$
S_A는 S_B로부터 받은 메시지를 통해 자신이 생성한 세션키가 S_B의 것과 동일한지 다음과 같이 확인한다.

$$X'_Z = h(ID_B PVERsk_{AB} PVERR_B)$$
$$X'_Z \stackrel{?}{=} X_Z$$

S_A는 자신이 보내고자 하는 메시지와 받은 메시지 그리고 BS과 S_A의 세션키를 BS가 확인할 수 있도록 세션키 확인 정보(X_Y)를 BS에게 전송한다.

$$X_Y = h(ID_A PVERsk'_{BSA} PVERR_A)$$

(3) BS는 S_A로부터 받은 정보를 이용하여 자신이 만든 세션키가 S_A의 것과 동일한지 다음과 같이 확인한다.

$$X'_Y = h(ID_A PVERsk_{BSA} PVERR_A)$$
$$X'_Y \stackrel{?}{=} X_Y$$

(1)부터 (3)까지의 과정을 통하여 BS과 S_A, S_A과 S_B의 세션키가 상호 확인되었다.

2.3 서브 프로토콜 수행 단계

세션키 생성 단계와 확인 단계가 정당하게 이루어지면, 이후

에 발생하는 세션키는 다음과 같은 서브 프로토콜을 수행함으로써 생성된다.

(1) $S_B \rightarrow S_A : (M'_B PVERR''_A)_{sk''_{AB}}$

S_E는 이전 세션에서 생성된 합법한 세션키(sk'_{AB})와 세션키 생성 단계 (4)에서 전송된 랜덤수(R'_A)를 이용하여 다음과 같이 세션키(sk''_{AB})와 확인 정보(X''_{AB})를 생성한다. S_B는 S_E에게 메시지와 함께 다음 세션의 세션키 생성에 필요한 랜덤수(R''_A)를 암호화하여 전송한다.

$$sk''_{AB} = h(sk'_{AB} PVERR'_A)$$
$$X''_{AB} = h(sk''_{AB} PVERR'_A)$$

(2) $S_A \rightarrow S_{BS} : (M'_A PVERM'_B PVERR''_{BS})_{sk''_{BSA}}$

S_A는 (1)과 동일한 방법으로 세션키(sk^*_{AB})를 생성하고, 이를 (1)에서 받은 세션키와 동일한 지 다음과 같이 확인한다.

$$sk^*_{AB} = h(sk_{AB} PVERR'_A)$$
$$X^*_{AB} = h(sk^*_{AB} PVERR'_A)$$
$$X''_{AB} \stackrel{?}{=} X^*_{AB}$$

S_A는 BS와의 세션키를 생성하기 위해 과거 세션키와 세션키 생성 단계 (3)에서 받은 랜덤수(R'_{BS})의 해쉬값을 다음과 같이 계산한다. 이전에 받은 메시지와 자신의 메시지 그리고 다음 세션키 생성에 필요한 랜덤수를 암호화하여 BS에게 전송한다.

$$sk''_{BSA} = h(sk'_{BSA} PVERR'_{BS})$$
$$X''_{BSA} = h(sk''_{BSA} PVERR'_{BS})$$

(3) BS는 (2)와 동일한 방법으로 세션키를 생성하고, 이를 (2)에서 받은 세션키와 동일한 지 다음과 같이 확인한다.

$$sk^*_{BSA} = h(sk_{BSA} PVERR'_{BS})$$
$$X^*_{BSA} = h(sk^*_{BSA} PVERR'_{BS})$$
$$X''_{BSA} \stackrel{?}{=} X^*_{BSA}$$

(1)부터 (3)까지의 과정을 통하여 여러 세션에서 독립적인 세션키가 생성되었다.

3. 안전성 분석

센서 네트워크 환경의 키 합의 프로토콜에 필요한 보안 요구사항은 인증, 익명성, 세션키의 상호제어를 보장하고, 위장공격, 알려진 키 공격, 재전송공격 등에 안전해야 하다.

(1) **인증** : 제안한 프로토콜은 키생성과정에서 S_A와 S_B, 키확인 과정에서 BS와 S_E가 생성된 세션키를 확인함으로써 세션키의 상호인증이 이루어지게 하였다.

(2) **익명성** : 해당 세션의 세션 ID를 노드 둘만이 공유한 비밀키로 암호화하기 때문에 공격자가 세션 ID와 관련된 메시지를 얻는다하더라도 이 메시지를 복호화 할 수 없음으로 통신의 익명성을 보장받게 된다.

(3) **세션키의 상호제어** : S_A와 S_B, BS의 세션키 생성에 사용된 정보는 각 노드가 선택한 랜덤수와 노드 ID로 그 양이 동일하여 한 노드의 정보가 노출된다 하더라도 해당 세션키 노출에는 큰 영향을 미치지 않는다.

(4) **위장공격** : 악의를 가진 공격자가 키 생성과정에서 BS와 S_A사이의 통신에 끼어들어 정당한 사용자인 척하여 메시지를 보내더라도 수신한 노드측에서 세션키에 대한 동일여부를 확인하기 때문에 위장공격은 이루어 질 수 없다. 따라서 제안한 프로토콜은 위장 공격에 안전하다.

(5) **알려진 키 공격** : 세션키를 생성하는데 사용된 랜덤수가 매 세션마다 모두 다른 값이 사용되기 때문에 이전 세션의 세션키가 노출되더라도 현재의 세션키에는 아무런 영향을 미치지 않는다. 따라서 제안한 프로토콜은 알려진 키 공격에 안전하다.

(6) **재전송공격** : 각 세션마다 다른 랜덤수를 사용하기 때문에 한번 수신된 랜덤수가 다른 세션에서 다시 전송된 것은 공격자에 의해 재전송되었음을 의미한다. 제안한 프로토콜은 재전송공격의 인지가 가능함으로 재전송공격에 안전하다.

4. 결론 및 향후과제

본 논문에서는 플랫 구조의 센서 네트워크 환경에 적용가능한 프로토콜을 제안하였다. 제안한 프로토콜의 세션키 생성 단계에서는 노드가 각각의 ID와 랜덤수를 이용하여 세션키를 생성하고, 세션키 확인 단계에서 데이터 전송 시 세션키 확인에 필요한 정보를 보냄으로써 세션키를 상호 확인할 수 있도록 하였다. 세션키 생성 단계와 확인 단계가 정당하게 이루어지면 다음 세션의 세션키 생성 시 서브 프로토콜을 이용함으로써 네트워크에 참여하는 노드의 에너지 소모를 줄였으며, 제안한 키 합의 프로토콜이 인증, 익명성, 세션키 상호제어를 보장하고, 위장공격, 알려진 키 공격, 재전송공격에 안전함을 보였다.

향후과제로는 메시지를 수신한 노드가 세션키 확인 단계에서 전송되는 메시지를 자신의 메시지와 함께 압축하여 베이스 스테이션으로 전송하게 되는데 이때, 노드가 악의를 가지고 다른 노드에게서 받은 메시지를 변경 또는 위조할 수 있다. 그러므로 송수신하는 메시지들에 대한 무결성 보장하는 기법들이 연구되어져야 할 것이다.

[참고문헌]

[1] S. Zhu, S. Setia and S. Jajodia, "LEAP : Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *Proc. 10th ACM conference on Computer and communications security*, pp.62-72, 2003.

[2] C. Intanagonwiwat, R. Govindan, D. Estrin and J. Heidemann, "Directed Diffusion for Wireless Sensor Networking," *IEEE/ACM Transactions on Networking*, pp.2-16, 2003.

[3] S. Schmidt, H. Krahn, S. Fishcher and D. Watjen, "A Security Architecture for Mobile Wireless Sensor Networks," *1st European Workshop on Security in Ad-Hoc and Sensor Networks*, pp.166-172, 2004.

[4] H. Chan and A. Perring, "PIKE : Peer Intermediaries for Key Establishment in Sensor Networks," *IEEE INFOCOM*, 2005.

[5] A. Perring, R. Szewczyk, V. Wen, D. Culler and J.D. Tyger, "SPINS : Security Protocols for sensor Networks, *Wireless Networks*," *Wireless Networks*, pp.521-534, 2002.

[6] C. Boyd and A. Mathuria, "Protocol for Authentication and Key Establishment," *Springer Verleg*, 2003.

[7] D.W. carman, P.S. Kruus and B.J. Matt, "Constraints and Approaches for Distributed Sensor Network Security," *NAI Labs Technical Report 00-010*, 2000.