유비쿼터스 네트워크에서의 상호인증 프로토콜

조영복° 김동명, 이상호
충북대학교 네트워크 보안연구실
{bogi0118°, shlee}@netsec.cbnu.ac.kr, dmkim@mail.ddc.ac.kr

A Mutual Authentication Protocol in Ubiquitous Network

Youngbok Cho° Dongmyung Kim Sangho Lee
Dept. of Network Security Laboratory Chungbuk National Univ.

요 약

유비쿼터스 네트워크의 보안요구사항을 살펴보면 센서의 위치, 저 전력으로 인한 성능의 제약, 브로트 캐스팅에 의한 통신 등 들 수 있다. 그 중이 논문에서는 저 전력으로 인한 성능의 제약측면을 고려한 상호인증 (Mutual Authentication)프로토콜을 새롭게 제안한다. 상호인증 프로토콜은 $RM(RegisterManager)$와 AM(Authentication Manager)로 구성되며 RM과 AM을 통해 각 센서 노드들의 한정된 전력문제를 해결하였고 가 각 센서노드에서의 메시지의 길이와 오퍼레이션 수를 최소화함으로 전력 낭비를 해결하였다. 또한 제안하는 프로토콜은 센서노드간의 상호인증을 통한 세션키 분배를 통해 안전한 통신이 가능하다.

1. 서 론

유비쿼터스란 말은 이미 차세대 정보통신 기술의 키워드로 자리를 잡았다. 특히 우리나라가 정보통신강국으로서의 위상을 확고히 하기 위해서는 유비쿼터스 네트워크 기술의 확보가 필수적인 과제로 인식되고 있으며 컴퓨터 기술과 다양한 응용분야에서 사용자들이 인지하기 힘들 정도로 빠른 속도로 발전하고 있다[1].

유비쿼터스 네트워크 환경의 특징이 사용자 중심으로서 사용자가 처한 상황이나 환경을 네트워크가 지능적으로 파악하여 사용자의 네트워크 환경을 최적화시켜 사용자가 어디에서나 네트워크에 편리하게 연결하는 것이다[2].

이 논문에서는 유비쿼터스 환경에서의 각 센서노드의 배터리에 저장된 한정된 전력을 고려한 상호인증 프로토콜을 제안한다. 상호인증 프로토콜은 RM과 AM으로 구성하여 한정된 전력을 지닌 센서 노드에서 최소한의 계산과정으로 연산에 소모되는 전력소비를 막아주고 상호인증을 통한 세션키를 발급하여 안전한 통신을 제공한다.

이 논문의 구성은 다음과 같다. 2장에서는 관련 연구, 3장에서는 제안하는 상호인증 프로토콜을 소개하고, 4장에서는 상호인증 프로토콜의 평가, 5장에서는 결론 및 향후 연구에 대해 기술한다.

2. 관련연구

유비쿼터스 환경의 센서 네트워크의 보안 프로토콜로 UC 버클리에서 개발한 SPINS(Security Protocols for Sensor Networks)는 리소스가 제한된 무선통신 환경에서 두개의 기본 구조인 μTESLA와 SNEP로 구성 된다[8].

SPINS은 하나의 대칭적인 암호화 함수로 암호화, 인증코드, 랜덤 수 생성 등을 제공하며 MAC을 위한 8Byte의 메시지를 할당하기 때문에 낮은 통신 오버헤드를 갖는다. 또한 SPINS는 데이터 알고리즘의 효율성에 초점을 두고 설계되었으며 센서 노드에 마스터 키가 저장된 상태로 노드가 발급된다.

SPINS의 μTESLA는 일방향 해쉬 체인을 사용하고 MAC 키 생성을 시간대로 분할하여 브로드케스트 하는데 시간 간격이 너무 작으면 해쉬 체인이 빨리 소모된다. 또한 특성상 시간대를 분할하는 것은 전체 네트워크의 전력소모를 가져올 수 있다는 문제점을 가지고 있다.

유비쿼터스 네트워크의 기술적 한분야로 홈 네트워크를 말하고 있다. 국내에서 발표된 홈 네트워크 기반에서의 센서 노드의 효율성에 관한 논문으로 Feige-Fiat-Shamir 인증 방식을 이용한 프로토콜이다[9]. 이 프로토콜은 크게 서비스 등록 단계, 임시 그룹 설정을 위한 센서의 초기 등록 과정, 임시 그룹 설정 단계, 임시 그룹 서비스 요청 단계, 임시 그룹의 삭제로 총 5단계로 수행된다. 그런 각각의 단계에서 매 Operation에서 모듈라 연산을 사용하여 보안성을 갖출 수 있으나 센서 노드에 많은 계산적 부담을 가져오게 된다.

또한 Feige-Fiat-Shamir 인증방식은 특성상 많은 키의 길이를 가지게 된다. 키의 길이가 커지는 것은 센서 노드에서는 많은 부담이 될 것이다. 따라서 센서 노드의 계산적 부담을 줄이기 위해서는 빠른 암호 알고리즘을 사용하는 것은 물론이고 수행되는 Operation 또한 적어야 할 것이다.

3. 제안 프로토콜

이 논문에서는 관련연구에서의 초경량, 저전력 알고리즘의 장점을 최대한 살리면서 [5][6][7][8][9]에서의 문제로 제시

되었던 Operation 수를 최소로하여 센서노드의 부담을 줄여주는 상호인증 프로토콜을 제안 한다. 또한 [9]에서 발생되는 모듈라 연산, 너무 긴 키 길이로 센서 노드의 계산적 부담이 발생되는 문제점을 해결하여 전력소모를 줄이고 동시에 안정성을 높이기 위해 센서노드의 상호인증을 통한 세션키를 발급하여 안전한 통신이 가능한 프로토콜을 제안한다. 제안하는 상호인증 프로토콜은 RM과 AM으로 나누어 설계하여 등록과정과 인증과정에서 사용한다.

이 논문에서 제안하는 프로토콜을 수행하기 위해 유비쿼터스 환경에서는 아래의 요구사항을 만족해야 한다.

첫째 제한된 센서 네트워크 환경을 고려하여 서브 시스템간의 통신은 AM (Authentication Manager)로 가정한다.

둘째 AM은 자신의 서브로 연결된 센서 노드들의 정보(개인키, 아이디)를 알고 있다.

셋째 한번 인증된 센서 노드는 통신이 끝날 때 까지는 별도의 인증을 하지 않는다. (단 자신의 RM과 서로 다른 RM에 등록된 센서 노드와 통신을 원할 때 즉, 초기 통신이 이루어지는 단계에서는 새롭게 인증을 시작해준다.)

위의 세 가지 요구사항을 기반으로 제안하는 상호인증 프로토콜에서 사용될 시스템 계수를 [표3-1]에 정의하였다.

[표3-1] 시스템 계수

표 기	설 명	표 기	설 명
Entitty	User의 디바이스	PK_A	*NodeA*의 개인키
ID_A	*NodeA*의 아이디	$\{ID_A \mid PK_A \mid TS$	*NodeA*의 메시지
PW	*NodeA*의 패스워드	TS	*TimeStamp*
Sig_A	*NodeA*의 서명	SK_{AM}	AM과 각*Node*간의 세션키
IDK	*NodeA*의 아이디 해쉬값	$PIN_{A_{new}}$	*NodeA*의 디바이스ID번호

유비쿼터스 네트워크상의 모든 센서 노드는 자신을 포함한 네트워크에 존재하는 RM을 통해 자신의 정보를 등록 요청한다. 사용자는 등록과정에서 사용자 정보와 디바이스 정보를 함께 등록하며 이 정보를 이용해 RM에서 개인키를 생성하도록 한다.

센서 노드의 등록과정을 통한 RM에서의 개인키 발급 과정은 다음과 같다.

① $NodeA$가 RM에게 자신의 정보를 함수 f를 사용해 전송하여 등록을 요청한다.
(함수 f는 주어진 모든 정보를 XOR연산을 한다.)

$$NodeA \rightarrow RM : f(ID_A \| PW_A \| PIN_{Adiv} \| TS \| Sig_A)$$

RM는 수신한 메시지를 이용해 사용자 정보와 디바이스 정보를 추출 한다.

$$RM(Verify) : ID_A, PIN_A, Sig_A, TS$$

② RM은 $InfoDB$를 통해 ID와 PIN을 검색하여 없으면 처음 등록으로 인정하고 IDK와 개인키를 생성 한다. (중복등록을 방지하기위해 DB를 한번의 검색과정을 거친다)

$$RM : IDK = h(IPI \| PIN)$$
$$PK = h(IDK \| PW)$$

③ RM은 개인키가 생성된 노드에 대해서는 $ID_A, IDK_A, PIN_A, Sig_A$을 $InfoDB$에 저장한다. (노드의 정보를 모두 기록함으로 나중에 노드가 제시한 서명이나 모든 정보가 $InfoDB$에 저장된 내용과 일치해야 동일 노드로 판단한다.)

$$RM \rightarrow InfoDB : ID_A, IDK_A, PIN_A, Sig_A$$

④ RM은 생성된 개인키 PK_A와 사용자 ID와 디바이스정보 PIN을 해쉬한 값 IDK_A값을 $NodeA$에게 전송한다.

$$RM \rightarrow EntityA : PK_A, IDK_A$$

제안하는 상호인증 프로토콜은 기존의 연구와는 달리 RM에서 키 생성을 수행하여 센서 노드에 전달하기 때문에 센서 노드의 계산적 부하로 인한 전력 소비를 방지할 수 있다. 또한 [6]에서의 서비스 등록과정에서 센서 노드가 두 번의 Operation을 수행하면서도 모듈라 연산으로 갖는 계산적 부담에 비해 상호인증 프로토콜은 센서노드 자체에서는 한번의 XOR 연산만으로 등록과정을 마친다. 등록과정을 마친 센서노드는 인증을 통해 세션키를 발급받게 된다. 센서 노드의 계산적 부하를 줄이기 위해 AM에서 상호인증을 통한 세션키를 발급한다. [그림 3-2]는 센서 노드 A와 B사이의 인증과정을 나타낸 것이다.

인증과정은 다음과 같다

① $NodeA$는 $NodeB$와 통신을 하기 위해 요청 메시지를 AM에게 자신의 개인키로 암호화해서 전송한다.(메시지는 자신의 IDK_A와 재전송 공격을 위해 TS와 자신이 통신하고자 하는 $NodeB$의ID_B를 자신의 개인키로 암호화해서 전송한다.)

$$Node\,A \rightarrow AM : ID_A, Mas\ ,\ Mas = E\{IDK_A, TS, ID_B\}PK_A$$

AM는 $NodeA$에게 받은 *Mas*가 현재 영역에서 유효한 정보인지를 $InfoDB$를 통해 확인 한다

$$AM \rightarrow Info\ DB : Verify : IDK_A(ID, PIN, Sig)_A$$
$$Verify : TS$$
$$Search : ID_B, PK_B$$

($InfoDB$ 을 통해 ID_B, PK_B을 AM은 가지고 와서 다음단계에 $NodeB$에서 전달된 메지를 확인하고 인증하기 위해서 사용한다)

② AM는 $NodeB$에 *Mas* 메시지를 요청한다. ($NodeA$의 통신요청을 알리는 메시지를 전송)

$$AM \rightarrow Node\ B : Req\ \ Mas\ ,\ Mas = (call\ ID_A)$$

③ $NodeB$는 AM에게 *Mas* 메시지를 보낸다.

$$Node\ B \rightarrow AM : Res\ ID_B, Mas\ ,\ \ Mas\ E\{IDK_B, TS, ID_A\}PK_B$$

AM은 $NodeB$로 받은 *Mas* 를 $InfoDB$를 통해 ①에서 검색한 값과 동일한지 확인한다.

$$AM \rightarrow keyDB :\ \ Verify : IDK_B(ID, PIN, Sig)_B$$

확인을 마치면 $NodeA, B$는 AM을 통해 상호인증이 이루어지고 메시지 교환에 사용될 세션키를 AM은 생성한다.

$$SK_{AM} = H(PK_A + PK_B)$$

④ AM은 생성된 세션키를 각 $NodeA, B$에게 각각의 개인키로 암호화 하여 전달한다.

$$AM \rightarrow Entity\ A : \{SK_{AM}\}_{ID_A}$$
$$AM \rightarrow Entity\ B : \{SK_{AM}\}_{ID_B}$$

$NodeA, B$의 통신을 위해 AM은 상호인증을 통한 안전한 세션키를 발급한다. 각 센서 노드는 최소한의 오퍼레이션으로 두 노드간 상호인증이 이루어진다.

4. 제안 프로토콜의 평가

이 논문에서 제안한 상호인증 프로토콜은 센서 노드에서 연산시 소모되는 전력소모를 최대한 줄여 각 센서 노드의 계산적 부하를 줄이도록 설계되었다. 동시에 센서 노드의 보안적 안정성을 위해 상호인증, 사용자와 디바이스 인증, MITM Attack, 기밀성, 무결성 등을 제공하는 프로토콜이다.

제안하는 상호인증 프로토콜은 기존의 많은 저전력 프로토콜들처럼 보안적 안정성을 만족하면서 각 노드에서 발생되는 적은 오퍼레이션으로 전력낭비를 해결하기 위한 프로토콜이다. 따라서 제안하는 프로토콜을 평가하기 위해 각 등록단계, 인증단계에서 센서노드에서 발생되는 오퍼레이션을 [6]에서 제안한 Feige-Fiat-Shamir 인증방식을 이용한 프로토콜과 서로 비교 평가해보았다.

[표4-2] 인증 단계에서의 센서노드 Operation

Operation	센서노드의 Operation	
	[6]프로토콜	제안프로토콜
Massage 전달횟수	4회	4회
노드에서의 암호화	0회	1회
노드에서 모듈라 연산	3회	0회
노드에서 해쉬 연산	2회	0회

저 전력을 고려해야 하는 센서 노드에서 [6]프로토콜에서는 3회의 모듈라 연산을 통한 계산적 부담을 많이 가져올 수 있었다. 이는 한정된 전력을 가진 센서 노드로서는 많은 오버헤드를 갖는 오퍼레이션이다. 또한 이 프로토콜에서 사용한 Feige-Fiat-Shamir은 키 사이즈가 매우 커진다는 단점을 가지고 있어 센서 노드에서는 계산하기에 많은 오버헤드를 주고 있다.

따라서 이 논문에서 제안하는 상호인증 프로토콜은 센서 노드에서의 저 전력 문제를 해결하기 위해 센서 노드간 통신의 오퍼레이션 수를 줄여 노드의 최적화를 통해 센서 노드에서의 전력 감소를 해결하면서도 안정성을 고려한 프로토콜이다.

5. 결론

이 논문에서 제안하는 상호인증 프로토콜은 유비쿼터스 네트워크상의 센서노드가 갖는 제한적인 배터리에 의존하여 사용되어지는 저 전력 문제를 고려하였다. 센서 노드의 저 전력 문제를 해결하기 위한 방법으로 센서노드에서의 계산적 오버헤드로 인한 전력소비를 막아주고 노드간의 상호인증을 통한 세션키 발급으로 안전한 통신이 가능하도록 하여 보안적 안전성인 상호인증, 세션키 설정, 사용자와 디바이스 인증, MITM 공격, 효율성, 기밀성, 무결성을 만족하는 상호인증 프로토콜 상호인증 프로토콜을 제안하였다.

이 논문에서 제안한 상호인증 프로토콜은 센서 노드의 오퍼레이션을 줄이면서도 기존 보안적 안전성을 그대로 유지할 수 있는 프로토콜이다. 센서 노드의 저 전력을 고려하기 위해 센서 노드에서의 오퍼레이션수를 줄이기 위해 *RM*과 *AM*으로 나누어 설계하여 대부분의 연산을 수행하도록 하였다. 또한 *AM*에서 TS을 Verify하게 함으로 재전송 공격이나 메시지의 freshness을 증명하였다. 향후에는 제안한 상호인증 프로토콜의 Operation을 통한 인증에 걸리는 시간과 소비전력을 시뮬레이션을 통한 연구가 요구된다.

참고문헌

[1] 김대영,도윤미, 박노성,,"센서 네트워크 기술" *한국정보처리학회학회지* , pp85-95, 2003.

[2] 박춘식, "유비쿼터스 네트워크와 시큐리티 고찰", *한국정보보호학회지*, pp12-20, 2004.

[3] Duk-Dong Lee " Ubiquitous Network and sensor technology", *Telecommunications Review*, 13-1,91-104, 2003

[4] H. Chan, A. Perrig, D. Song, "Random Key Predistribution Schemes for Sensor Networks," To *appear in Proc. of the IEEE Security and Privacy Symposium 2003*, May 2003.

[5] Prasanth Ganesan, Ramnath Venugopalan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu , "Analyzing and Modeling Encryption Overhead for Sensor Network Nodes ", *WSNA'03*, September 19, 2003

[6] Kaan Y"uksel, Jens-Peter Kaps, and Berk Sunar, "Universal Hash Functions for Emerging Ultra-Low-Power Networks ", *CNDS 2004*

[7] Gunnar Gaubatz, Jens-Peter Kaps, Berk Sunar, "Public Key Cryptography in Sensor Networks-Revisited", *ESAS 2004*

[8] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, "SPINS: Security Protocols for Sensor Networks ", *Mobile Computing and Networking 2001 Rome, Italy Copyright 2001 ACM*

[9] Laurent Bussard, Yves Roudier "Authentication in Ubiquitous Computing", *Workshop on Security in Ubiquitous Computing UBICOMP 2002*, Göteborg Sweden, 29 Sept 2002

[10] L.Echenauer, V.D.Gligor, " A Key-Management scheme for Distributed Sensor Networks", *In proceedings of the 9th computer communication security*, Nov 2002