韓國 컴퓨터情報學會 論文誌
第10卷 第2號, 2005. 5.

2005-10-2-2-8

유비쿼터스 센서 네트워크에서의 저전력 상호인증 프로토콜

조영복*, 정윤수**, 김동명**, 이상호***

A Low-Power Mutual Authentication Protocol in Ubiquitous Sensor Networks

Young-Bok Cho*, Youn-Su Jung**, Dong-Myung Kim***, Sang-Ho Lee****

요 약

유비쿼터스 센서 네트워크에서 모든 센서노드들은 한정된 배터리로 통신에 참여하게 된다. 기존의 인증방식을 사용하는 경우 많은 연산 수행이 필요하여 센서노드의 배터리를 과다하게 소모하여 센서노드의 동작 기간이 상대적으로 짧아지므로 네트워크 유지에 많은 어려움이 존재한다. 이 논문에서는 센서노드의 인증과정에서 전력 소비문제를 해결하기 위해 $RM(RegisterManager)$과 $AM(AuthenticationManager)$을 도입한 네트워크 구조를 제시하고, 노드의 상호인증을 통한 세션키를 발급하는 저전력 상호인증 프로토콜을 제안한다. RM과 AM은 개별 센서노드에서 안전성을 보장하기 위해 수행되는 키 생성 및 암/복호화, 인증 과정을 센서노드 대신 처리하여 빠른 연산속도로 알고리즘을 처리한다. 따라서 센서노드의 인증에 소요되는 알고리즘 수행시간이 동일 서브넷에 존재하는 경우 평균 2.96%, 서로 다른 서브넷에 존재하는 경우 평균 12.91% 빠르게 수행된다. 따라서 제안 방식은 센서 노드가 더 오랜 시간 통신에 참여할 수 있도록 하며, 센서네트워크의 크기가 증가할수록 효율적이다.

Abstract

All sensors in Ubiquitous sensor network have to communicate with limited battery. If we adopt current authentication, there are difficulties to keep sensor network because heavy calculation in each sensor needs more power and lifetime of sensor could be short relatively because of the effect. This paper suggests network structure which is using $RM(RegisterManager)$ and $AM(AuthenticationManager)$ to solve power problem on authentication, and suggests mutual-authentication protocol with low power which supports a session key by mutual-authentication. RM and AM manage algorithm with fast calculation to keep the safety by doing key generation, encryption/decryption, authentication instead of each sensor node. Processing time to authenticate sensor node is 2.96% fast in the same subnet, and 12.91% fast in different subnet. Therefore, the suggested way provides expanded lifetime of censor node and is more effective as sensor network size is bigger and bigger.

▸ Keyword : Ubiquitous Sensor Network, Authentication, Security

• 제1저자 : 조영복
• 접수일 : 2005.04.13, 심사완료일 : 2005.05.20
* 충북대학교 전자계산학과 석사과정, ** 충북대학교 전자계산학과 박사과정
*** 충북대학교 전기전자컴퓨터공학부 교수
※이 논문은 2004년도 충북대학교 학술 연구 지원 사업의 연구비 지원에 의하여 연구되었음

Ⅰ. 서 론

유비쿼터스 센서 네트워크는 유비쿼터스 환경의 네트워크 모델의 초기 모델이라고 할 수 있어, 최근 이와 관련된 폭넓은 연구와 개발이 진행되고 있다. 유비쿼터스 센서 네트워크는 다수의 소형 센서 노드들로 구성되며, 온도, 빛, 소리 등과 같은 물리 데이터를 비용 효율적인 방식으로 수집하는데 주로 사용된다. 또한 유비쿼터스 센서 네트워크는 설치 및 사용이 용이하고 비용이 적게 든다는 장점이 있으며, 이러한 장점으로 인하여 최근 사무 및 가정 자동화를 비롯하여 군사 및 의료 목적 등으로 널리 사용되고 있다. 특히 우리나라는 정보 통신 강국으로서의 위상을 확고히 하기 위해서 유비쿼터스 센서 네트워크 기술의 확보가 필수적인 과제로 인식되고 있다[1]. 유비쿼터스 센서 네트워크는 사용자 주변의 주변기가 통신을 가능하게 함으로써 자율적으로 정보를 수집하고 관리하는 구성요소이다[2][3]. 유비쿼터스 센서네트워크의 가장 큰 제약점 중 하나는 배터리라는 한정된 에너지에 의존하여 동작하는 센서노드의 에너지 소비 절약 문제이다. 이러한 에너지 소비 문제와 관련하여 특히 안전한 통신을 위하여 노드간의 통신마다 발생하는 인증을 효율적으로 처리하는 방안이 모색되어야 한다.

이 논문에서는 유비쿼터스 센서 네트워크 환경에서 저전력으로 동작하는 안전한 상호인증이 가능한 프로토콜을 제안한다. 제안 프로토콜은 센서노드보다 연산성능이 좋은 RM과 AM, 일반 센서노드가 최단 노드로 구성된 센서 네트워크 환경을 기반으로 동작하며, 센서노드의 오퍼레이션을 최소화함으로써 전력소비를 줄이고 상호인증을 통한 세션키를 발급하여 통신을 원하는 센서노드사이 안전한 통신을 제공한다. 이 과정에서 AM은 서브넷 통신 및 인증을 담당하고 RM은 노드인증을 수행하도록 설계한다. 또한 제안 환경에서는 노드간 상호인증을 기반으로 통신이 이루어지며 서로 다른 RM에 등록된 센서노드와 통신이 필요한 경우 AM을 통한 인증을 수행하도록 설계한다. 이와 같은 접근은 센서노드에서만 수행되던 많은 오퍼레이션을 RM과 AM에게 분담시킴으로써 각 센서 노드의 계산적 부담을 줄여주어 궁극적으로 더 오랜 시간 통신에 참여할 수 있게 할 것이다.

이 논문의 구성은 다음과 같다. 2장에서는 초경량, 저전력 암호기술 및 보안 프로토콜에 대해 기술하고, 3장에서는 저전력 상호인증 프로토콜을 제안, 4장에서는 제안 프로토콜의 실험환경을 제시하고 저전력 측면과 안전성 측면의 평가 결과를 제시하고, 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

유비쿼터스 센서 네트워크의 센서노드는 주로 배터리로 에너지를 공급받고 통합센서 장치로 구성되며 아주 적은 데이터 처리능력과 단거리 무선 통신이 가능하다[4]. 예를 들면 Smart Dust 와 WINS가 센서 네트워크를 적용한 사례이다[4]. 센서 네트워크의 응용분야가 넓어지면서 센서노드의 보안성은 매우 중요한 위치를 점하고 있으며, 보안성 제공을 위하여 통신이 암호화되고 인증되어야 한다. 그러나 센서노드는 배터리에 저장된 한정된 용량의 에너지에 의지해서 동작하므로, 높은 안전성을 위해 많은 오퍼레이션 수행으로 인한 에너지 소비의 절약 방안은 중요한 과제이다.

2.1 초경량, 저 전력 암호화 기술

국내외적으로 센서노드의 한정된 전력을 고려한 초경량, 저 전력 암호화 기술들이 많이 연구되고 있다. [5][6]의 논문은 대표적인 초경량 저 전력 암호 기술들 중에 하나로 다양한 하드웨어 플랫폼에서의 암호 알고리즘들의 수행속도를 평가한 논문들이다. 이 방법들은 암호 알고리즘들 중 보다 빠른 암호 알고리즘을 사용하여 저 전력 문제를 해결하고자 하였다. [5],[6]은 대칭키 방식으로 통신에서 사용될 비밀키를 노드가 미리 가지고 있는 방식이다. 그러나 이방식의 문제점은 임의의 한 노드에서 비밀 키가 누출된다면 더 이상 이 비밀 키를 가진 노드와는 안전한 통신은 할 수 없다.

이 문제를 해결하기 위해서는 센서노드에서는 최소한의 정보만을 소유해야 하며, 이 정보를 통해 원하는 세션에서 안전한 통신을 위한 세션키를 생성해야만 할 것이다. 그러나 유비쿼터스 센서 네트워크에서의 센서노드는 매우 경량화 되어야 하기 때문에 키 생성이나 안전성을 위한 암/복호화 과정의 오퍼레이션을 크게 기대할 수 없다. [5],[6]의 논문에서는 센서노드에서 대칭키 방식을 사용해 "SmartDust"의

MOTES나 RFID등과 같은 초경량, 저 전력 응용환경에 이용하였다. 센서노드를 사용하는 SmartDust의 노드 프로토타입의 특성은 〈표 1〉과 같다.

표1 스마트더스트 노드의 프로토타입
Table.1 SmartDust Nodes Prototype

CPU	8-bit, 4MHz
Storage	8 Kbytes instruction flash 512 bytes RAM 512 bytes EEPROM
Communication	916 MHz radio
Bandwidth	10Kbps
Operating System	TinyOS
OS code space	3,500bytes
Available code space	4,500bytes

[7]의 논문에서는 경량(lightweight) 센서노드에 탑재 가능한 저 전력 공개키 암호로 Rabin Ntru를 구현하였다. Robin Scheme은 인수분해 문제의 어려움에 기반한 RSA의 특별한 하나의 형태로 1979년 Rabin이 제안하였다. NtruEncrypt는 SVP(Shortest Vector Problem)의 어려움에 기반 해 1996년 Hoffstein, Pipher, Silverman이 제안한 방식으로[18], 센서노드에서 공개키 기반으로 모든 노드의 공개키 및 개인키를 위한 계산적 능력을 요구하게 된다. 그러나 가장 큰 문제점은 한정된 에너지와 낮은 계산 능력을 지닌 센서노드가 키 생성을 위해 많은 오퍼레이션을 수행한다는 점이다.

2.2 보안 프로토콜

센서 네트워크에서의 안전성을 고려한 보안 프로토콜로는 UC 버클리에서 개발한 SPINS(Security Protocols for Sensor Networks)이 있다. SPINS는 리소스가 제한된 무선통신 환경에서 두개의 기본구조인 μTESLA와 SNEP로 구성된다[8]. 하나의 대칭적인 암호화 함수로 암호화, 인증코드, 랜덤 수 생성 등을 제공하며 MAC을 위한 8Byte의 메시지를 할당하기 때문에 낮은 통신 오버헤드를 갖는다. SPINS는 데이터의 비밀성, 인증, 무결성을 보장하기 위한 SNEP라는 프로토콜과 데이터를 브로드케스트하는 것에 대한 인증을 위한 μTESLA라는 프로토콜을 제안하여 자원 제한적인 센서 네트워크에서의 안전한 통신에 대한 방법을 제시하였다. 또한 데이터 알고리즘의 효율성에 초점을 두고 설계되었고 센서노드에 마스터키가 저장된 상태로 센서노드가 발급된다. SPINS의 μTESLA는 일방향 해쉬 체인을 사용하고 MAC 키 생성을 시간대로 분할하여 브로드케스트 한다. 브로드케스트 할 때 시간 간격이 너무 작으면 해쉬 체인이 빨리 소모되므로 시간간격을 고려해야 한다. SPINS에서는 특성상 시간대를 분할하는 것은 전체 네트워크의 전력소모를 가져올 수 있다는 문제점을 가지고 있다. 또한 비밀통신을 위해 마스터키를 노드에 저장한 상태로 노드가 발급되기 때문에 안전성 측면에 문제가 있고 센서노드 메모리에도 부담이 된다.

Feige-Fiat-Shamir 인증 방식을 이용한 프로토콜[9]은 센서노드의 효율성에 관해 기술한 논문이다. [9]에서 제안된 프로토콜은 크게 5단계로 수행된다. 각 단계는 서비스 등록 단계, 임시 그룹 설정을 위한 센서의 초기 등록 과정, 임시 그룹 설정 단계, 임시 그룹 서비스 요청 단계, 임시 그룹의 삭제이다. 각 단계에서 보안성을 위해 모듈러 연산을 사용한다. 그러나 센서노드에서 모듈러 연산의 사용은 계산적 많은 오버헤드를 부여한다. 또한 Feige-Fiat-Shamir 인증방식은 특성상 많은 키의 길이를 가지게 된다. 키의 길이가 커지는 것은 센서노드의 메모리측면에서는 많은 부담이 된다.

III. 저전력상호인증 프로토콜의 설계

유비쿼터스 센서 네트워크는 기존 유선 네트워크와 달리 한정된 전력 낮은 연산능력, 작은 메모리에 제약 사항이 있으며, 그 중 가장 큰 제약 사항은 센서 노드가 배터리에 저장된 한정된 에너지에 의존해서 동작되는 점이다. 즉, 어떤 센서노드가 저장된 에너지를 모두 소비하게 된다면 그 노드는 더 이상 통신에 참여할 수 없게 되어, 센서 네트워크의 기능을 상실하게 된다. 이 논문에서는 노드간 인증에 있어 소비되는 전력소비를 줄이며 안전한 저전력 상호 인증 프로토콜을 제시한다.

제안 프로토콜에서는 위 그림과 같이 등록단계와 인증단계로 구분한다. 센서노드의 안전한 통신을 위해 키 생성, 암/복호화 및 인증을 통한 많은 오퍼레이션으로 가져올 수 있는 센서노드의 통신상 오버헤드를 줄이기 위해 RM과 AM을 기반으로 동작한다. RM과 AM의 도입으로 센서노드

에서 수행되어지는 인증 관련 연산 중 많은 부분을 연산성능이 좋은 AM에서 처리하도록 함으로 한정된 배터리 소모 문제를 해결하며 센서노드의 보안적 안전성을 만족하도록 한다. (그림 1)은 두 노드가 동일한 서브넷 안에서 센서노드의 인증과정, (그림 2)는 두 노드가 서로 다른 서브넷간의 인증과정의 흐름이다.

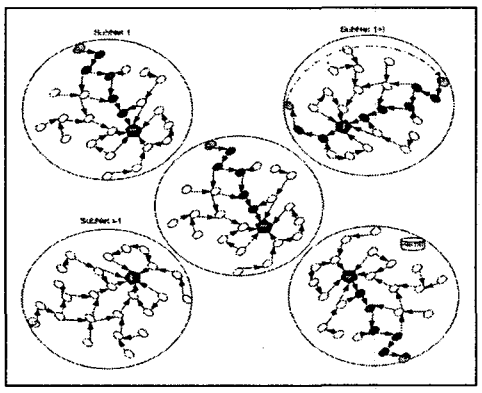

그림 1. 동일 서브넷 인증과정
Fig.1 Same subnet authentication process

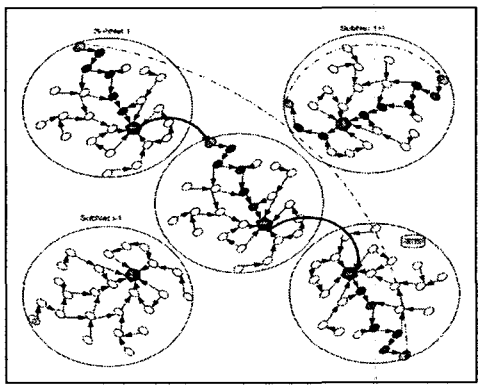

그림 2. 다른 서브넷 인증과정
Fig.2 Other subnet authentication process

제안 프로토콜은 인증을 위한 세션키 분배를 위해 센서노드에서 수행되는 연산을 최대한 줄이고 이를 상대적으로 처리 성능이 우수한 RM과 AM이 수행하도록 설계한다. 유비쿼터스 센서 네트워크는 아래의 요구사항을 만족한다고 가정한다.

① 각 센서노드는 [18]에서 제안한 AODV 라우팅 프로토콜을 사용하여 hop-by-hop 경로를 설정한다.

② 하나의 서브넷에 존재하는 센서의 수는 최대 50개 이내로 한정하며 하나의 서브넷에는 각각 하나의 RM과 AM이 존재하며 서브 시스템간의 통신은 AM(Authentication Manager)로 구성된다.

③ 자신이 속한 서브넷이 아닌 다른 서브넷의 센서노드와 통신을 원할 때 AM을 통해 서로 다른 서브넷에 존재하는 센서 노드간 인증을 수행한다.

④ 센서노드에서는 파라미터로 등록과정에서 ID, PW, TS와 인증과정을 마친 후 ID, PW, TS, PK을 유지하며, 각 파라미터의 표현을 위하여 각 16byte씩의 메모리를 할당한다.

⑤ RM과 AM은 각각 자신의 기능 수행을 위하여 관련 데이터베이스를 유지하며 센서노드의 ID, PW, PIN, PK 등의 센서 노드의 정보를 테이블로 가지고 있다.

센서노드가 최초로 서브넷에 진입할 때 등록단계를 수행하며, 통신을 위해 인증단계를 거쳐 세션키를 발급받아 통신에 참여할 수 있도록 제안된 저전력 상호인증 프로토콜의 주요 파라미터들은 〈표 2〉와 같다.

표2 제안 프로토콜의 시스템 계수
Table.2 Proposed protocol system notation

표 기	설 명
$NodeA$	센서 노드 A
ID_A	$NodeA$의 아이디
PW_A	$NodeA$의 패스워드
IDK_A	$NodeA$의 아이디 해쉬값
PK_A	$NodeA$의 개인키
$\{ID_A \mid PK_A \mid TS\}$	$NodeA$의 메시지
TS	$Timestamp$
SK_{AM}	AM과 각$Node$간의 세션키

3.1 등록과정

(그림 3)에서와 같이 유비쿼터스 센서 네트워크상의 모든 센서노드는 자신이 속한 서브넷에 존재하는 RM_i을 통해 자신의 정보를 등록 요청하며, 이 등록단계에서 사용자 정보와 디바이스 정보를 함께 등록한다. (그림 4)는 RM_i에서 이 정보를 이용하여 등록 요청한 센서노드의 개인키를 생성하여 발급 하는 세부 과정이다.

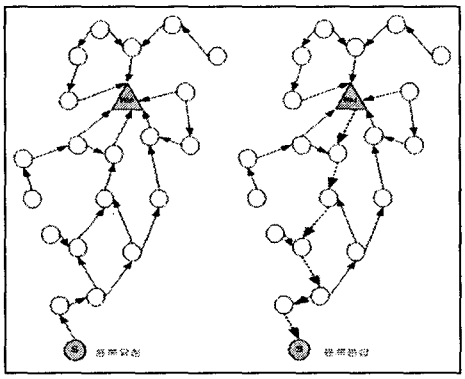

그림 3. 노드의 등록
Fig.3 Node register

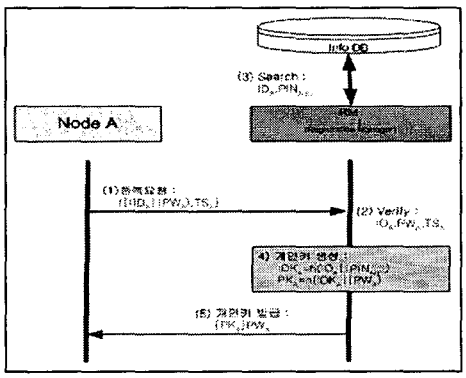

그림 4. RM을 통한 등록과정
Fig.4 Register through RM

서브넷에서 센서노드A의 등록과정 (그림 4)는 다음과 같다.

① $NodeA$가 자신이 속한 서브넷의 RM_i에게 자신의 등록에 필요한 파라미터를 함수 f를 통해 전송하여 등록을 요청한다. (함수 f는 주어진 모든 정보를 XOR연산을 수행한다.) RM_i은 수신한 메시지를 이용하여 사용자 정보와 센서노드 정보를 확인한다.

$$NodeA \rightarrow RM_i : f\{(ID_A \mid\mid PW_A), TS_A\}$$
$$RM_i(Verify) : ID_A, PW_A, TS_A$$

② RM_i은 자신이 유지하고 있는 $InfoDB$을 통해 등록신청 센서노드의 $Node\ ID$를 검색하여 ID_A의 IDK_A키와 개인키PK_A를 생성 한다.

$$RM_i : IDK_A = h(ID_A \mid PIN_A),$$
$$PK_A = h(IDK_A \mid TS_A)$$

③ RM_i은 해당 센서노드의 ID_A, IDK_A, PK_A, TS_A을 $InfoDB$에 추가하여 저장한다. (TS값을 저장함으로 메시지의 재전송 공격을 방지할 수 있다.

$$RM_i \rightarrow InfoDB : IDK_A, PK_A, TS_A$$

④ RM_i은 생성된 개인키 PK_A와 IDK_A값을 $NodeA$에게 전송한다.

$$RM_i \rightarrow NodeA : PK_A, IDK_A$$

제안 프로토콜은 기존 인증 방식에서와는 달리 RM_i을 통하여 인증에 필요한 개인키를 생성하며 센서노드에 전달함으로써 센서노드의 계산적 오버헤드로 인한 전력 소비를 방지할 수 있다. [7]이 제안한 프로토콜에서는 서비스 등록 과정에서 센서노드가 두 번의 Operation으로 RC5를 통한 암호화 연산을 수행했고 [6]의 논문에서는 SAFER을 사용하여 암/복호화를 수행하였으나, 제안 방식에서는 센서노드 자체에서 한번의 XOR연산과 Rabin을 사용한 한 번의 암호화를 사용하여 RM에 등록을 마치고 개인키를 발급 받는 특징을 갖는다.

3.2 인증과정

등록과정을 마친 센서노드는 임의의 상대 노드와 통신하기 위해 AM을 통한 키 교환 및 세션키 생성을 수행한다. 즉, AM은 통신하고자 하는 센서노드 A, B의 상호 인증을 거쳐 통신에 사용될 안전한 세션키를 생성하며 분배하게 된다. 인증을 위한 통신 과정은 크게 두 노드가 동일 서브넷 안에서의 통신과 두 노드가 서로 다른 서브넷의 센서노드간 통신으로 나누어 구성한다.

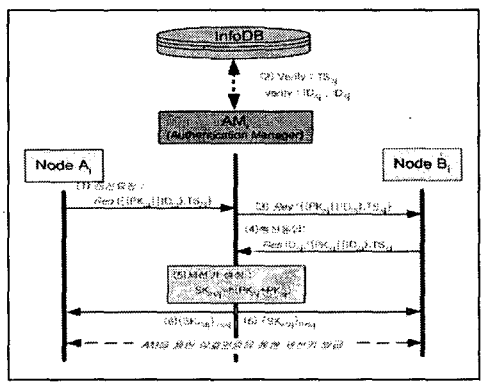

그림 5. 두 노드가 동일 서브넷에서 AM의 인증
Fig.5 Authentication that use AM in same subnet

(그림 5)는 두 노드가 동일 서브넷에서 AM_i을 통한 세션키 발급으로 $Node A_i$는 $Node B_i$의 안전한 통신을 위한 인증과정을 나타낸 것으로 흐름은 다음과 같다.

① $Node A_i$는 $Node B_i$와 통신을 하기 위해 인증 요청 메시지를 AM_i에게 전달한다. 메시지는 자신의 PK_{A_i}, 통신을 요구하는 상대 노드의 ID_{B_i}를 함수 f 한 결과와 TS_{A_i}를 함께 전송한다. (TS_{A_i}을 전송함으로 메시지의 재전송 공격이나 Freshness를 보장해 줄 수 있다.)

$$Node A_i \rightarrow AM_i : f\{(PK_{A_i} \mid ID_{B_i}), TS_{A_i}\}$$

② AM_i는 $Node A_i$로부터 수신한 메시지가 현재 서브넷에서 유효한 ID인지를 $Info DB$을 통해 확인한 후, 동일한 서브넷에 존재하는 경우 $Node B_i$의 ID_{B_i}, PK_{B_i}을 $Info DB$을 통해 획득하며 이 정보는 $Node B_i$에게 전달받은 메시지를 확인하고 인증하기 위해 사용한다.

$$AM_i \rightarrow Info\ DB : Verify : ID_{A_i}, ID_{B_i}, TS_{A_i}$$

③ AM_i는 $Node B_i$에 $(ID_{B_i} \mid PK_{A_i}), TS_{A_i}$ 메시지를 전송하며($Node A_i$의 통신요청을 알리는 메시지를 전송), $Node B_i$는 AM_i로부터 수신한 메시지를 확인한 후 응답 메시지를 전송한다. 이 과정에서 $Node B_i$는 $Node A_i$의 PK_{A_i}을 획득하게 된다.

$$AM_i \rightarrow Node\ B_i : Res\ f\{(ID_{B_i} \mid PK_{A_i}), TS_{A_i}\}$$

④ $Node B_i$는 AM_i에게 자신의 PK_{B_i}을 확인시키기 위한 메시지를 전달하며, AM_i은 $Node B_i$로부터 받은 메시지는 $Info DB$을 통해 ②에서 검색한 값과 동일한지 확인한다. AM_i은 $Node A_i$, $Node B_i$의 PK_A, PK_B을 확인하고 상호인증이 이루어지고, 메시지 교환에 사용될 세션키를 생성한다.

$$Node B_i \rightarrow AM_i : ID_{B_i}, f(PK_{B_i} \mid ID_{A_i}), TS_{B_i}$$
$$AM_i : SK_{AM_i} = h(PK_{A_i} + PK_{B_i})$$

⑤ AM_i은 각 $Node A_i$, $Node B_i$에게 생성된 세션키를 각각의 개인키로 암호화하여 전달한다.

$$AM_i \rightarrow Node A_i : \{SK_{AM_i}\}_{PK_{A_i}}$$
$$AM_i \rightarrow Node B_i : \{SK_{AM_i}\}_{PK_{B_i}}$$

위와 같이 $Node A_i$, $Node B_i$간의 통신을 위해 AM_i는 상호인증을 통한 세션키를 생성하며, AM에서 생성된 세션키는 $Node A_i$, $Node B_i$에 개인키로 암호화되어 각 노드에 발급된다. $Node A_i$, $Node B_i$는 세션키 획득을 위해 한 번의 복호화만을 수행하면 가능하다.

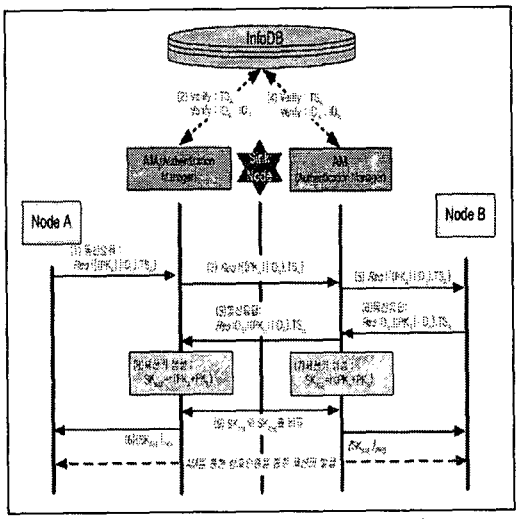

그림 6. 두 노드가 다른 서브넷에서 AM의 인증
Fig.6 Authentication that use AM in other subnet

다음은 (그림 6)은 두 노드가 서로 다른 $SubNet_i$와 $SubNet_j$에 존재하는 각각 $Node A_i$와 $Node B_j$간의 상호인증을 수행한 후 세션키를 발급하는 과정이다.

① $Node A_i$는 $Node B_j$와 통신을 하기 위해 인증 요청 메시지를 AM_i에게 전달한다. 메시지는 자신의 PK_{A_i}, 통신을 요구하는 상대 노드의 ID_{B_j}를 함수 f 한 결과와 TS_i를 함께 전송한다.

$$Node A_i \rightarrow AM_i : Req\ f\{(PK_{A_i} \mid ID_{B_i}), TS_{A_i}\}$$

② AM_i는 $Node A_i$로부터 수신한 메시지가 현재 서브넷에서 유효한 ID인지를 $Info DB$을 통해 확인한 후, 두 노드가 동일한 서브넷에 존재하지 않음을 확인하고 $Node B_j$가 존재하는 서브넷 AM_j를 찾아 $Node A_i$에게 받은 메시지를 전달한다.

$AM_i \rightarrow Info\ DB : Verify : ID_{A_i}, ID_{B_j}, TS_{A_i}$

$AM_i \rightarrow AM_j : Req\ f\{(PK_{A_i} \mid ID_{B_j}), TS_{A_i}\}$

③ AM_j은 AM_i로부터 전달받은 메시지를 $InfoDB$를 통해 확인 후 $Node B_j$에게 전달한다.

$AM_j \rightarrow Info\ DB : Verify : ID_{A_i}, ID_{B_j}, TS_{A_i}$

$AM_j \rightarrow Node B_j : Req\ f\{(PK_{A_i} \mid ID_{B_j}), TS_{A_i}\}$

④ $Node B_j$는 AM_j에게 자신의 PK_{B_j}을 확인시키기 위한 메시지를 전달하며, AM_j은 $Node B_j$로부터 받은 메시지는 $InfoDB$을 통해 ③에서 검색한 값과 동일한지 확인한다.

$Node B_j \rightarrow AM_j : Res ID_{B_j},\ f\{(ID_{A_i} \mid PK_{A_i}), TS_{A_i}\}$

⑤ AM_i, AM_j은 $Node A_i$, $Node B_j$의 PK_{A_i}, PK_{B_j}을 통해 상호인증이 이루어지고, 메시지 교환에 사용될 세션키를 생성한다. 각 AM_i, AM_j에서 생성된 세션키를 비교하여 동일한 키임을 확인한다.

$AM_i : SK_{AM_{A_i}} = h(PK_{A_i} + PK_{B_j})$

$AM_i : SK_{AM_{B_i}} = h(PK_{A_i} + PK_{B_j})$

$AM_i \leftrightarrow AM_j : Compare\ (SK_{AM_{A_i}} == SK_{AM_{B_i}})$

⑥ AM_i, AM_j은 동일하게 생성된 세션키 $SK_{AM_{A_i}}, SK_{AM_{B_i}}$을 각 노드의 개인키로 암호화 하여 노드에 전달하게 된다.

$AM_i \rightarrow Node A : \{SK_{AM_{A_i}}\}_{PK_{A_i}}$

$AM_j \rightarrow Node B : \{SK_{AM_{B_i}}\}_{PK_{B_i}}$

Ⅳ. 성능평가

유비쿼터스 센서 네트워크 환경에서 센서노드의 생존기간(lifetime) 연장을 위해 배터리의 전력 소모를 줄이는 일은 매우 중요한 과제이다. 이를 위해 유비쿼터스 센서 네트워크의 구조화와 RM/AM 노드의 도입을 통하여 센서노드에서 수행하던 키 생성, 암/복호화 및 인증과정을 RM/AM을 통해 수행하도록 하였고 센서노드에서는 키 동의와 안전성을 위한 메시지의 확인과정을 수행하도록 함으로써 센서노드에서의 연산 부담을 최소화하여 센서노드에서 수행되는 연산이 적어지면 그 만큼 전력소모량이 감소하게 된다.

4.1 저전력 측면에서의 평가

센서 노드에서 안전성 보장을 위해 키 설정, 암/복호화 및 인증을 위한 과중한 오퍼레이션 수행으로 센서노드의 한정된 전원을 사용한다면 얼마가지 않아 노드의 수명이 끝나고 통신에 더 이상 참여할 수 없는 커다란 문제점을 갖게 된다. 따라서 제안하는 프로토콜을 저전력 측면에서 평가하기 위해 다음의 실험 환경을 가정한다[18].

- 센서 네트워크의 수 : 각 서브넷의 크기는 평가를 위해 [18]에서 제시된 50개미만의 센서들로 구성됨을 가정하고 각 서브넷에는 RM/AM이 존재하며 최대 서브넷의 수는 9개로 구성한다.
- RM/AM의 위치와 센서 노드간의 관계 설정 : RM/AM은 하나의 서브넷에 존재하며 상호 통신이 가능하다. 모든 센서 노드는 RM/AM과 통신이 이루어지며 센서 노드가 하나의 서브넷에 들어오게 되면 RM을 통해 등록을 하고 등록을 마친 센서 노드는 AM을 통해 인증을 마친 후 세션키를 발급받아 통신에 참여하게 된다.
- 임의의 센서 노드간의 경로 길이 : $Node A \rightarrow Node B$까지 통신을 위한 노드간 경로길이는 두 노드가 동일 서브넷인 경우의 최단 경유 노드 5, 최장 경유노드 13으로 한다. 그러나 두 노드가 서로 다른 서브넷 즉 가장 먼 서브넷 안의 노드와 통신이 이루어질 경우 경로길이는 최단 경유노드 10, 최장 경유노드 27로 한다.
- RM/AM 노드와 센서 노드들의 연산 능력 : RM/AM은 2.4GHz, 250kbps, 868/915Mhz 정도 단말로 일반 센서노드보다 뛰어난 연산능력을 가지고 있으며 센서노드들은 앞에서 서술한 스마트더스트에서 정의된 노드정도의 연산능력을 가지고 있다.

위에서 정의된 실험환경을 기반으로 저전력 평가를 위해 센서노드에서 수행되는 오퍼레이션 수행시간을 [16]을 기반으로 측정하였다. 노드 수행시간 계산을 위해 $Node A \rightarrow Node B$ 의 통신을 위한 노드의 인증 흐름을 살펴보면 Karl 방식의 경우는 두 노드가 동일 서브넷에 존재하는 경우 $Node A_i \rightarrow Node B_i$, 서로 다른 서브넷에 존재하는

경우 $Node\,A_i \rightarrow Node_i \rightarrow Node_j \rightarrow Node\,B_j$ 와 같은 방식의 흐름을 가지며 제안 방식의 경우 두 노드가 동일 서브넷에 존재하는 경우 $Node\,A_i \rightarrow AM_i \rightarrow Node\,B_i$, 다른 서브넷에 존재하는 경우 $Node\,A_i \rightarrow AM_i \rightarrow AM_j \rightarrow Node\,B_j$ 와 같은 경로를 가진다. 〈표 3〉은 Karl 방식과 제안방식에서의 각 노드에서 수행되는 알고리즘의 수행시간을 계산하여 비교한 것이고 (그림 7)은 알고리즘 수행시간을 그래프로 나타낸 것이다.

표3 센서노드의 수행시간 단위: μs/byte
Table.3 Operation time of sensor node

수행기능	Karl 방식				제안 방식			
	동일 서브넷		다른 서브넷		동일 서브넷		다른 서브넷	
	최단거리	최장거리	최단거리	최장거리	최단거리	최장거리	최단거리	최장거리
Inqurity	0.67969	1.69922	1.35938	4.078125	0.00085	0.00085	0.00085	0.00085
Key generation	0.61719	1.54297	1.23438	3.703125	0.00077	0.000771	0.00154	0.00154
Key Agrement	1.01563	2.53906	2.03125	6.09375	2.53906	6.601563	5.07813	13.71094
Encryption	3.31563	8.28906	6.63125	19.89375	3.24219	8.429688	6.48438	17.50781
Decryption	12.26367	30.65918	24.5273	73.58201	12.3047	31.99219	24.6094	66.44531
Authentication	2.16875	5.42188	4.3375	13.01250	0.00061	0.000605	0.00121	0.00121
계	20.06055	50.15137	40.12109	120.36328	18.08901	47.02651	36.17548	97.66767

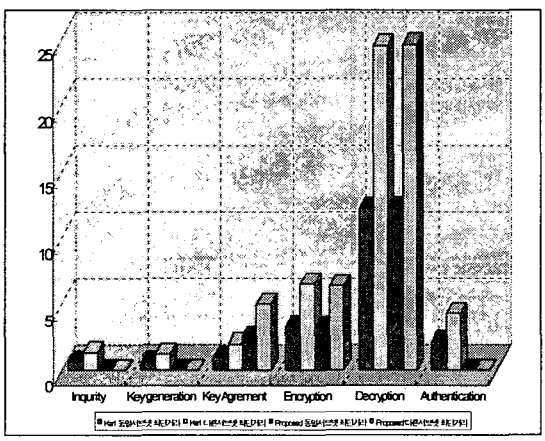

그림 7. 알고리즘 수행시간
Fig.7 Algorithm operation time

Karl의 방식에서 통신을 원하는 두 노드가 동일서브넷 통신인 경우 최단거리 인증 수행시간은 20.06055μs/byte, 최장거리 인증 수행시간은 50.15137μs/byte이지만 제안 방식에서 두 노드가 최단 거리 인증 수행시간은 18.08901 μs/byte, 최장 거리 인증수행시간은 47.02651μs/byte이다. 따라서 Karl 방식보다 최단거리에서의 인증 수행은 1.972%, 최장 거리에서는 3.125% 만큼 빠른 연산 처리를 수행하게 된다. 또한 두 노드가 서로 다른 서브넷에 존재하는 경우, Karl 방식에서는 최단거리 노드간 인증 수행시간은 40.12109μs/byte, 최장거리 노드간 인증수행시간은 120.36328μs/byte이나, 제안 방식에서는 각각 36.175485 μs/byte와 97.66767μs/byte로 소요되어 Karl방식보다 3.946%와 3.126% 빠른 수행시간을 갖는다. (그림 8)은 인증 알고리즘을 수행하는 전체 노드의 수행시간 이다.

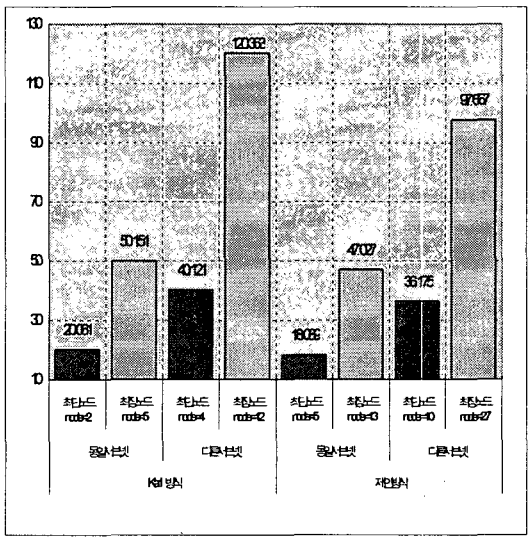

그림 8. 전체 수행시간
Fig.8 Total operation time

제안 방식은 센서노드의 계산적 부담을 줄이기 위해 별도의 RM/AM 노드를 도입하여 서브넷을 구성함으로써 센서노드간 경유 노드의 수는 Karl 방식보다 두 노드가 동일 서브넷에 존재하는 경우 평균 4, 두 노드가 서로 다른 서브넷에 존재하는 경우 평균 11개로 증가하였지만 인증 수행시간은 두 노드가 동일한 서브넷에 존재하는 경우 2.959%, 다른 서브넷에 존재하는 경우 12.911% 만큼 향상되었다. 또한 인증에 소요되는 수행시간은 서브넷의 수가 커질수록 그 효과가 높아지므로 많은 센서노드로 구성된 유비쿼터스 센서 네트워크 환경에 매우 효율적인 인증 방식이라 할 수 있다. (그림 9)는 제안 방식을 Karl 방식과 비교하여 제안방식의 수행시간이 얼마나 빠른지를 나타낸 그래프이다.

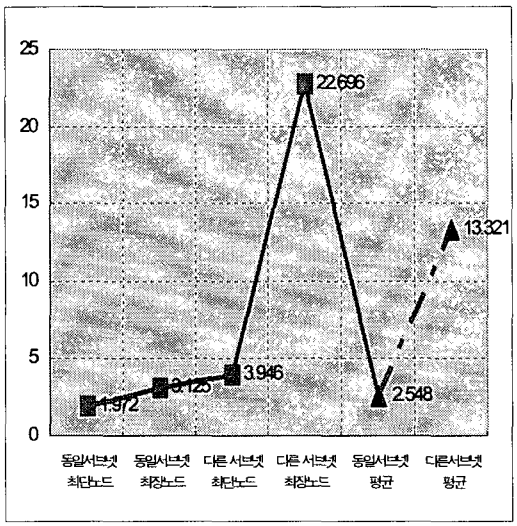

그림 9. 노드별 수행시간의 Karl방식과의 비교
Fig.9 Comparison with karl method of operation time by node

기존 Karl이 제안한 상호인증보다 두 노드가 동일 서브넷 통신과 서로 다른 서브넷 통신의 평균 7.935%정도 더 빠른 수행시간을 제공하여 각 센서가 통신에 참여할 수 있는 시간을 연장할 수 있게 된다.

4.2 안전성 측면에서의 평가

유비쿼터스 센서 네트워크는 특정 지역이나 환경으로부터 데이터를 수집하기 위해 해당 지역에 다량의 센서노드들이 임으로 설치되고 서로 협력하여 자체 알고리즘과 프로토콜을 통해 형성된 네트워크로 수집된 정보 전송에 있어 악의를 가진 공격자에 의해 전송되어지는 데이터의 유출 및 위/변조는 매우 심각한 문제를 야기하게 될 수 있다. 따라서 센서노드의 상호인증을 위한 세션키 설정을 기반으로 제안 프로토콜의 안전성을 평가한 결과는 〈표 4〉와 같다.

표4 제안 프로토콜의 안전성 평가 결과
Table.4 Safety estimation of proposal protocol

항목	설 명
상호인증	- $f\{ID_A \mid ID_B\}, TS$, AM에서 각 센서노드가 보낸 메시지를 통해 상호인증을 수행하고 $TS(TimeStamp)$을 메시지에 포함하여 전송함으로 센서노드의 재전송 공격이나 Freshness를 보장
MITM 공격	-$SK_{AM} = h(PK_A + PK_B)$ $NodeA, B$의 개인키는 AM에서 IDK 값을 생성해서 PW 값과 해쉬를 해서 개인키 PK를 생성
기밀/무결성	- $f\{ID_A \mid ID_B\}, TS$ 센서노드의 프라이버시 정보를 전송할 경우 전송되는 데이터에 대한 기밀성과 무결성을 제공하기 위해 암호화 및 타임스탬프를 사용하여 전송하는 데이터에 대한 안전성을 유지.

기존 Karl의 방식에서는 각 디바이스의 PIN을 초기 Key로 사용하였기 때문에 MITM 공격에 매우 취약함을 보여주었으나, 〈표 4〉에서 보는 바와 같이 제안 방식에서는 세션키를 각 노드의 개인키를 통한 세션키를 발급함으로 MITM공격에도 안전함을 보여주고 있다.

V. 결 론

유비쿼터스 센서 네트워크 환경에서 모든 센서노드들은 배터리에 저장된 한정된 전력을 가지고 통신에 참여한다. 기존의 인증 방식에서는 센서노드에서 키 생성 및 암/복호화, 인증을 위한 연산으로 발생하는 오버헤드로 인해 센서노드의 많은 전력을 안전성을 위해 소모하였다. 이 논문에서는 센서노드의 전력 소비 문제를 해결하고 노드간 상호인증을 통한 안전한 세션키 발급을 위해 RM과 AM을 도입하여 상호인증을 수행하는 프로토콜을 제안하였다.

제안 프로토콜은 한정된 전력을 지닌 센서노드의 많은 오퍼레이션으로 발생하는 오버헤드를 최적화하기 위해 노드간 통신을 RM과 AM을 통해 이루어지도록 설계하여 인증이나 키 생성 등을 RM과 AM을 통해 수행하도록 하고 센서노드는 키 동의와 안전성을 위한 메시지의 암/복호화 과정만을 수행함으로써 센서노드에서의 수행시간을 최소화하였다. 그 결과 인증 처리를 위한 노드간 평균 경로 길이는 기존 방식보다 동일 서브넷의 길이는 4, 서로 다른 서브

넷의 경우는 11로 길어지지만 실제 인증 수행시간은 동일 서브넷의 경우 평균 8.03234%, 서로 다른 서브넷 통신인 경우 평균 14.34510%정도 향상되어 소비 전력을 그만큼 줄일 수 있어 노드의 배터리 수명이 연장할 수 있다. 또한 안전성 측면에는 Karl의 방식에서 취약성을 보였던 MITM 공격을 제안 방식에서는 개인키와 PIN의 해쉬 값을 이용하여 개인키를 생성함으로 MITM 공격에도 안전하며 효율성, 기밀성, 무결성 등을 보장함을 보였다.

참고문헌

[1] 김대영, 도윤미, 박노성, "센서 네트워크 기술", 한국정보처리학회학회지 , 2003 Page(s):85-95.

[2] 박춘식, "유비쿼터스 센서 네트워크와 시큐리티 고찰", 한국정보보호학회지, 2004 Page(s):12-20.

[3] Duk-Dong Lee, "Ubiquitous Network and sensor technology", Telecommunications Review, 13-1. 2003 Page(s):91-104.

[4] H. Chan, A. Perrig, D. Sung, "Random Key Predistribution Schemes for Sensor Networks", the IEEE Security and Privacy, 2003 Symposium on 11-14 May, 2003 Page(s):197-213.

[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 Page(s):151-159.

[6] Karl E Persoon and D. Manivannan, "Secure Connection in Bluetooth Scatternets", System Sciences. 2003. Proceedings of the 36th Annual Hawaii International Conference on 6-9 Jan. 2003 Page(s):10-19.

[7] Gunnar Gaubatz, Jens-Peter Kaps, Berk Sunar, "Public Key Cryptography in Sensor Networks -Revisited", European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004),LNCS 3313, Heidelberg, Germany, August 6, 2004 Page(s)2-18

[8] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler "SPINS: Security Protocols for Sensor Networks", Wireless Networks, September 2002 Volume 8, 2002 Page(s)521-534

[9] Roy Want, Trevor Pering, Gunner Danneels, Mutha Kumar, Murali Sundar, John Light, "Personal Server: Changing the Way We Think about Ubiquitous Computing", UbiComp 2002, Springer LNCS 2498, Page(s)194 - 209

[10] L. Echenauer, V. D. Gligor, "A Key-Management scheme for Distributed Sensor Networks", In proceedings of the 9th computer communication security, Nov 2002, Page(s):41-47

[11] Jalal Al-Muhtadh, "A Flexible Privacy-Preserving Authentication Framework for Ubiquitous computing environments", in the International Workshop on Smart Appliances and Wearable Computing (IWSAWC2002),Vienna, Austria, July 2, 2002 Page(s):771-776

[12] Ross Anderson, "A New Family of Authentication Protocols" Operating Systems Review, 1998 Page(s):32-35

[13] Dong-wook Cho, Yeon-yi Choi, Hee-do Kim, Dong-ho Won, "이동통신 환경에 적합한 상호인증을 제공하는 키 분배 프로토콜의 설계", 한국정보보호학회 논문지 2000, 6 v.10,v2, 2000 Page(s):21-30.

[14] Zan Li, Yilin Chang and lijun Jin, "A Novel Family of Frequency Hopping Sequences for Multi-Hop Bluetooth Networks", Consumer Electronics, IEEE Transactions on Vol.49, Issue 4, November 2003 Page(s):1084-1089

[15] http://www.eskimo.com/~weidai/benchmarks.html, "Crypto++ 5.2.1 Benchmarks"

[16] J.Hoffstein, J.Pipher, J.H.Silverman, "NTUR:A new high speed public key cryptosystem", in Algorithmic Number Theory (ANTS III),Portland, OR, June 1998, Lecture Notes in Computer Science 1423(J.P.Buhler,ed). Springer-Verlag. Verlin. 1998 Page(s):267-288

[17] 정유열, "낮은 계산량을 이용한 효율적인 WTLS 시스템 구현에 관한 연구", 한국컴퓨터정보학회논문지 2003, Vol8,N3, Page(s):138-143

[18] Hyun M. Park, Soo B. Kim, Yeong M. Jang, "IEEE 802.15.4 센서 네트워크에서 전력을 고려한 Routing Protocol", Next Generation Communication Software NCS 2004, 한국통신학 회 2004, Page(s) 785-790

[19] 박택진,박준식,박재두, "차세대 이동통신용 고효율, 저전력 VCO에 관한 연구", 한국컴퓨터 정보학회논문지 2002,9 Vol7, N3, Page(s):109-114

저 자 소 개

조 영 복

2005년~현재 충북대학교
전자계산학과 (석사과정)

정 윤 수

2005년~현재 충북대학교
전자계산학과 (박사과정)

김 동 명

2003년~2005년 충북대학교
전자계산학과 (박사과정수료)
2002년~현재 대덕대학
평생교육원 전임교수

이 상 호

1989년 숭실대학교 대학원
전자계산학과 (Ph. D)
1981년~현재 충북대학교
전기전자컴퓨터 공학부 교수