# 홈 네트워킹을 위한 미들웨어 보안시스템 구현

설정환* · 이기영*

# Implementation of Middleware Security System for Home Networking

Jeong-Hwan Seol* · Ki Young Lee*

이 논문은 인천대학교 2006년도 자체연구비 지원에 의하여 연구되었음

## 요 약

본 연구에서는 센서 네트워크 보안 메커니즘을 홈네트워크 구조에 적용한 시스템을 설계하고 이를 홈네트워크 미들웨어의 가상망에 구현하였다. 홈네트워크 미들웨어의 기본구조는 lookup 서버가 서비스 노드와 일대일 또는 브로드캐스트 통신 방식의 구조이며, 여기에 요구되는 보안요소는 일대일의 통신인 경우에는 기밀성과 인증, 브로드캐스트일 경우에는 브로드캐스트 인증의 보장이다. 센서 네트워크 보안 기술인 SPINS는 기밀성과 인증을 보장하는 SNEP와 브로드캐스트 인증을 제공하는 μTESLA 부분으로 구성되는데 이를 홈네트워크 미들웨어의 기본구조에 적용한 시스템을 설계하였다. MAC 생성을 위한 CBC-MAC, 메시지 신선성을 제공하는 CTR, 메시지의 랜덤 특성을 보장하여 주는 PRF 방식, 그리고 센서노드에 사용될 암호화 알고리즘으로는 낮은 연산량으로 충분한 보안성을 갖는 RC5를 이용하였다. 구현된 결과는 CTR 모드로 인해 공격자가 키를 습득하더라도 새로운 메시지를 복호화 할 수 없었으며 상호 MAC 교환으로 인해 정당한 사용자로부터 전송되었다는 것을 인증할 수 있었다. 이 구현 결과는 향후 효율적이고 안전한 홈 네트워크 시스템 개발에 응용될 수 있을 것으로 기대한다.

## ABSTRACT

In this paper, a system with sensor network security mechanism which can be applied to home network structure is designed and it is implemented on a virtual network of a home network middleware. The basic structure of home networking middleware supports one-to-one (unicast) or broadcast communication mode between the lookup server and service nodes on the network. Confidentiality and authentication are key security factors of the one-to-one communication and user authentication is crucial for broadcasting mode. One of the sensor network's security techniques SPINS consists of SNEP and μTESLA. The SNEP ensures confidentiality and authentication, and μTESLA provides broadcast authentication. We propose a SPIN based home network middleware and it is implemented by using the CBC-MAC for MAC generation, the counter mode (CTR) for message freshness, the pseudo random function (PRF) and RC5 as encryption algorithm. The implementation result shows that an attacker cannot decrypt the message though he gets the secure key because of CTR mode. In addition, we confirmed that a received message of the server is authenticated using MAC.

키워드

Home Networking, Middleware, SPINS, μTESLA, SNEP

* 인천대학교 정보통신공학과

접수일자 2008. 04. 07

## Ⅰ. 서 론

1990년대 중반 인터넷의 활발한 보급은 많은 사람들의 생활양식을 비약적으로 바꾸어놓는데 큰 역할을 하였다. 인터넷이 보편화된 후에는 많은 분야의 일을 인터넷에 연결된 단말기로 처리할 수 있게 되었고 네트워킹의 응용이 많은 사회 분야에서 개발되고 사용되고 있다. 최근 활발히 논의되고 있는 USN (Ubiquitous Sensor Network)은 우리 주변의 물리적 현상을 감지하는 센서 장치에 네트워크 개념을 추가해 사물의 존재 여부 및 위치 등의 정보를 네트워크와 연동, 실시간으로 관리, 제어하는 개념이다. USN의 센서 노드는 일회성, 저전력, 작은 기억공간, 제한된 계산 능력 등의 특징을 갖는다. USN의 통신 수단으로는 Zigbee, Bluetooth 등의 무선망을 사용하게 되는데 이러한 무선망 사용으로 인해 도청, 감청, 패킷 스푸핑(packet spoofing) 등의 공격을 당하기 쉬우며 위에서 언급한 센서 노드의 제약사항으로 인해 지금까지 연구된 강력한 보안 알고리즘을 적용시키는데 한계가 있다.

홈네트워크는 사생활이 보장되어야 하는 환경이기에 보안이 더욱 중요한 문제가 될 수 있다. 특히 홈네트워크 미들웨어는 가정 내의 여러 센서로부터 데이터를 전송받아 제어 기능을 수행해야 함으로 보안 문제가 더욱 중요시 될 수밖에 없다. 홈네트워크 보안에는 기밀성 보장이 무엇보다 중요하며 또한 공격자가 센서 노드로 위장하여 공격하는 경우를 대비하여 BS(base station)와 노드간 인증이 이루어져야 한다. BS에서 각 노드로 패킷을 브로드캐스트 할 경우, 모든 노드에 대한 인증 또한 이루어져야 한다[1],[2].

본 연구에서는 데이터 기밀성, 노드 인증과 BS에서의 브로드캐스트 인증을 제공할 수 있는 SPINS (Security Protocols Sensor Networks) 알고리즘을 정리하고 이 보안 알고리즘을 홈 네트워킹 미들웨어 기술 중에 하나인 Jini의 통신구조에 맞도록 설계, 구현하고 그 성능을 평가하였다. 본 논문의 구성은 다음과 같다. Ⅱ장에서는 홈네트워크 미들웨어 통신 시스템을 정리하였고 Ⅲ장에서는 SPINS를 분석하였다. Ⅳ장은 제안한 보안시스템을 설명하였고 Ⅴ장과 Ⅵ장에서는 각각 구현 결과 및 분석, 그리고 논문의 결론을 기술하였다.

## Ⅱ. 홈네트워킹 미들웨어

홈네트워킹 미들웨어는 홈네트워크 환경에서 AV 기기, 백색가전, 정보기기 등 다양한 정보가전기기들을 사용자 간섭 없이 연결, 구성하고 유연하게 제어하며 상호 연동을 보장하는 프레임워크이다. 현재 Jini, HAVi, 그리고 UPnP 방식이 활발히 연구되고 있다.

### 2.1. Jini

Jini는 썬 마이크로시스템사에서 개발한 미들웨어로서 Java를 기반으로 한다. 시스템 운영방식은 Client/Server 방식으로 홈네트워킹 게이트웨이의 표준인 OSGi (Open System Gateway Initiative)의 근간을 이루고 있다. Jini 시스템은 서비스 이용자, 서비스 제공자 서비스 관리자의 세부분으로 구성된다[3].

### 2.2. HAVi

HAVi(Home Audio/Video Interoperability)는 홈네트워크에 연결된 다양한 벤더의 디지털 오디오 및 비디오 장치간의 상호 기능성을 제공하는 표준이다. HAVi는 PC와 주변 기기에는 적용되지 않으며 상위의 OSI 계층에 대해서만 표준안이 규정되기 때문에 주로 어플리케이션과 서비스에만 중점적으로 되어있는 단점을 가진다. 그러나 다른 HAVi 디바이스의 기능을 사용하고 탐지할 수 있으므로 다른 방에 있는 오디오나 비디오 조작도 가능한 장점이 있다.

### 2.3. UPnP

UPnP(Universal Plug and Play)는 Microsoft사에서 제안한 것으로 IP 네트워크망과 XML, Soap 기술을 기반으로 개발된 윈도우플랫폼용 홈 네트워킹 미들웨어 솔루션이다. UPnP는 플러그앤 플레이 개념을 확장하여 사용자에게 어떤 작업도 요구하지 않고 기기를 네트워크에 접속시킨다. UPnP는 모든 홈네트워크 디바이스의 미디어에 관계없이 공통의 인터페이스를 제공하게 된다. 그러므로 어플리케이션 입장에서는 UPnP를 통해 하부 미디어에 독립적일 수 있다[4].

지금까지 살펴본 세 미들웨어를 비교해보면 표 1과 같다.

표 1. 홈네트워킹 미들웨어 비교[4]
Table 1. Comparison of homenetwork middleware

| | Jini | UPnP | HAVi |
|---|---|---|---|
| 기반 Network | IP Network | IP Network | IEEE 1394 |
| 기반 S/W | Java2, RMI | HTTP, HTML, XML | Object-Oriented |
| 운영방식 | C/S | C/S | P2P |
| Plug&Play | Jini 자체 feature | UPnP' SSDP | 1394 media's feature |
| 취약분야 | Stream 처리 | Stream 처리 | IP Network 기반 접속 |
| Standard | Jini 2.0 | UPnP 1.0 | HAVi 1.1 |

## Ⅲ. SPINS

### 3.1 SPINS

센서 네트워크 보안의 대표적인 기술인 SPINS는 2002년 미 버클리 대학에서 연구된 메커니즘이다. SPINS는 센서노드와 신뢰성 있고 강력한 자원을 가지고 있는 BS로 구성된다. SPINS는 크게 두 부분으로 나누어지며 데이터의 기밀성과 인증을 제공하는 SNEP(Secure Network Encryption Protocol)와 BS에서 브로드캐스팅되는 데이터의 인증을 제공하기 위한 μTESLA로 구성되어 있다. SPINS는 SNEP와 μTESLA를 제공하기 위해 표 2와 같이 시스템을 가정한다[5].

표 2. 시스템 가정
Table 2. System assumptions

| | |
|---|---|
| 시스템 | BS는 각 센서 노드에 똑같은 특성을 가진다<br>BS는 충분한 메모리와 암호키를 가지고 있다 |
| 통신 형태 | 노드 → BS ( 예 : 측정한 데이터 전송)<br>BS → 노드 ( 예 : 노드에 요청)<br>BS → 모든 노드 ( 예 : 질의, 전체 네트워크의 재구성) |

### 3.2 SNEP

SNEP는 전송 시 메시지 당 8바이트의 낮은 오버헤드를 발생시키며, 양단간 카운터를 이용하여 암호화시키는 장점을 가진다. 데이터 기밀성을 제공하기위한 SNEP의 암호화 방식은 CBC(Cipher block chain) 방식을 사용하여 데이터를 암호화한다. CBC 방식의 암호화 기법은 공격자에 의해 암호화키를 도청당할 경우, 모든 메시지를 바로 복호화 할 수 있게 된다. 그래서 SNEP는 카운터 모드(CTR)를 적용하여 데이터의 기밀성을 보장한다[6]. SNEP는 올바른 송신자가 데이터를 전송하였는지 검증하기 위해서 메시지 인증 코드 (MAC - Message Authentication Code)를 사용한다. SNEP에 의해 노드 A에서 B로 메시지를 보내는 경우, 아래와 같이 세 가지의 구조로 나타낼 수 있다[7],[8].

첫째, 데이터 인증만 보장하는 경우

A → B : D, MAC(K'AB, D)

둘째, 데이터 인증과 기밀성을 함께 보장하는 경우

A → B : {D}<KAB, CA>,MAC(K'AB, CA | {D}<KAB, CA>)

셋째, 비표(nonce)를 이용하여 인증과 기밀성을 보장하는 경우

A → B : NA, Request

B → A : {Response}<KBA,CB>, MAC(K'BA, NA| CB | {Response}<KBA, CB>)

{Response}<KBA, CB>)

여기서 A와 B는 센서노드 또는 BS이고, D는 전송하는 데이터이다. KAB 와 K'AB는 각각 A와 B가 공유하는 암호화키와 MAC 키를 나타낸다. NA는 A가 생성한 비표이고 CA는 A에서 IV로 사용된 카운터이다.

### 3.3 μTESLA

μTESLA는 기존의 TESLA 기법을 센서 네트워크에 적합하게 개조한 메커니즘으로 브로드 캐스트 인증을 제공하는 기법이다[5],[8]. TESLA 방식은 비대칭 암호화 기법으로 높은 연산량과 오버헤드를 발생시켜 센서 네트워크에 적용시키는데 어려움이 있다.

μTESLA에서 제일 처음 수행될 일은 길이 n의 키체인을 생성하는 일이다. 단방향 함수에 사용될 Kn을 생성하고 이 Kn을 이용하여 K0까지 만들어낸다. 키가 생성되면 시간을 일정한 간격으로 나누고, 키 체인의 키와 매핑 시킨다. 이 때 interval i가 경과한 후부터 δ interval 후에 Ki를 노출시킨다. 그림 1은 μTESLA에서의 단방향 키체인 방식을 보여주고 있다.

단방향 키체인 방식은 그림 1과 같이, 수신자가 주어진 키를 이용하여 자가 인증 (self-authenticating)을 하게 된다. 이때 송신자와 수신자가 시간 간격을 맞추기 위해서 시간동기화가 이루어져야 한다. 시간 동기화는 수신

자, 즉 노드가 비표와 함께 요청메시지를 송신자인 BS에게 전송하면 BS는 응답메시지에 시간동기화를 위한 시간정보를 응답하는 방식으로 이루어진다[8].

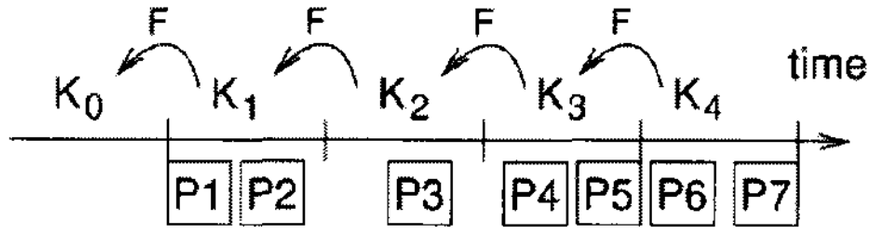



그림 1. μTESLA 의 단방향 키체인 방식
Fig 1. The μTESLA one-way key chain

## Ⅳ. SPINS를 적용한 홈네트워크 미들웨어 보안 시스템 구현

### 4.1 홈네트워크 미들웨어 설계

본 논문에서는 홈네트워킹 미들웨어의 가장 일반적인 구조라 할 수 있는 썬 마이크로소프트사의 Jini 구조에 SPINS 보안 메커니즘을 적용시키고자 한다. Jini는 크게 서비스 제공자와 이 서비스를 이용하는 클라이언트, 그리고 서비스 제공자와 클라이언트를 연결해주는 역할을 하는 lookup 서버 세부분으로 구성된다. 그림 2에 Jini의 기본 구조를 나타내었다.

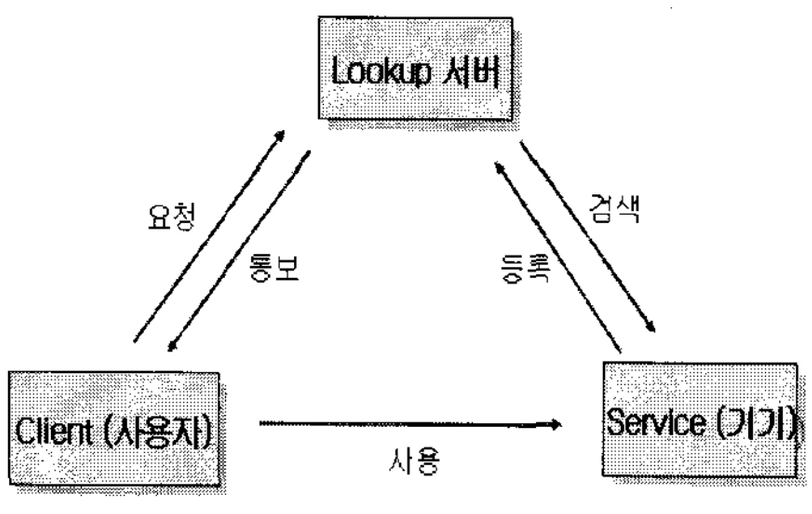



그림 2.Jini 의 기본 구조
Fig 2. Jini's fundamental form

### 4.2 홈네트워크 미들웨어의 SPINS 적용

lookup 서버는 서비스 제공자(기기)와 Bluetooth나 Zigbee 등의 근거리 통신망을 이용하여 메시지를 주고받는다. lookup서버는 메시지를 통해 서비스 제공자를 제어할 수 있으며 서비스 제공자는 여러 형태의 데이터를 lookup 서버에게 보내준다. 이에 홈네트워크는 보안 요구사항으로 프라이버시가 매우 중요하게 다루어져야 하며, 이러한 해결책으로 데이터의 기밀성과 인증은 필수적인 요소라 할 수 있다.

이러한 환경은 III장에서 노드-BS 사이에 기밀성과 인증을 제공하고 BS-모든 노드(all nodes)간 브로드캐스트 인증을 제공하는 SPINS를 적용하기에 적당하다 할 수 있다. 그림 3은 Jini의 기본 구조에 SPINS가 적용된 시스템을 나타내고 있다.

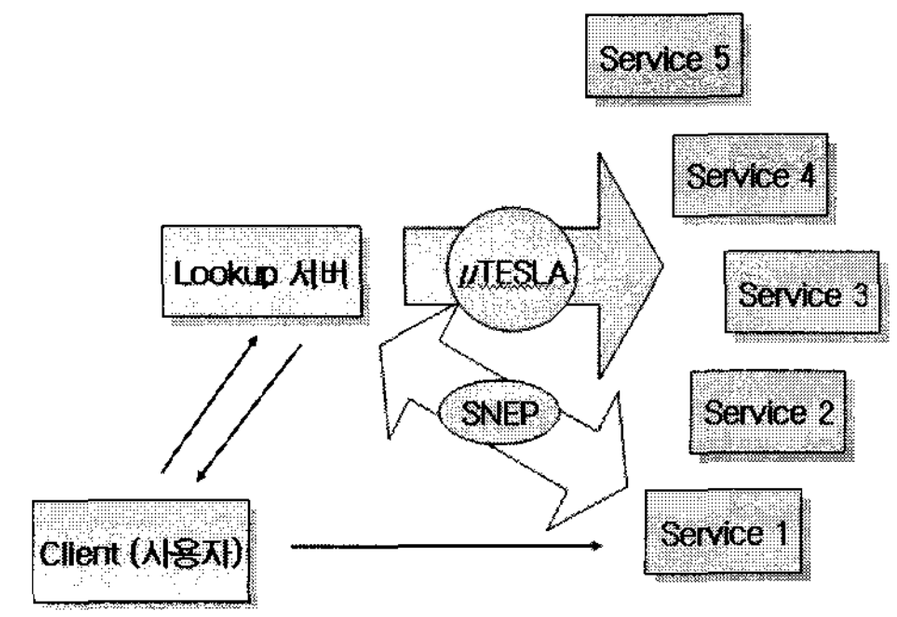



그림 3 SPINS가 적용된 Jini 구조
Fig 3. Jini applied by SPINS

### 4.3 SNEP 구현을 위한 설계

노드 A에서 B로 SNEP를 사용하여 메시지를 전송할 경우 그림 4와 같다. 비밀키 KAB는 데이터를 암호화하기 위해 사용되는 키로서 RC5 알고리즘에 IV에 카운터를 이용해 생성한다. RC5 에 사용되는 키는 A와 B가 서로 공유하고 있는 마스터키 XAB를 사용한다. 송신자는 생성된 KAB를 사용하여 데이터를 암호화한다. RC5 에 사용되는 키는 A와 B가 서로 공유하고 있는 마스터키 XAB를 사용한다. 송신자는 생성된 KAB를 사용하여 데이터를 암호화한다. 비밀키 생성과 마찬가지로 RC5를 사용한다. MAC를 추출하기 위해서는 인증키를 생성해야 한다. 인증키는 RC5를 이용한 PRF를 이용하여 생성한다. RC5에 사용되는 키는 마스터키이며 IV는 카운터이다. MAC 키가 생성되면 MAC를 만들어낼 수 있다. MAC 또한 MAC 키와 마찬가지로 RC5를 이용한 PRF를 이용하여 생성할 수 있다. 위 과정을 거쳐 송신자가 데이터를 전송한 후, 다음 데이터 전송시 IV는 counter에서 (count + 1) 로 증가하게 된다. 결국 비밀 키도 바뀌게 되며 같은 메시지라도 다르게 암호화가 이루어지게 된다.

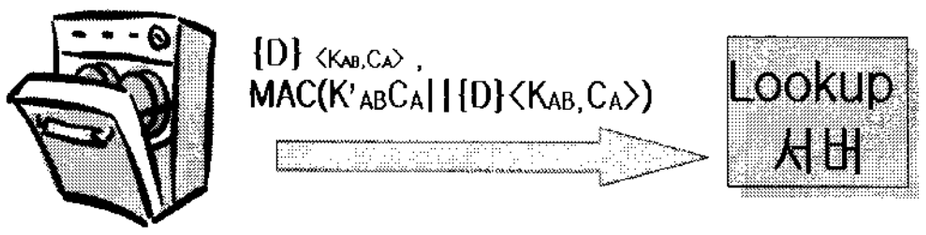



그림 4. SNEP에 의한 메시지 전송
Fig 4. Message transmission by SNEP

### 4.4 μTESLA 구현을 위한 설계

μTESLA는 BS가 모든 노드에게 메시지를 전송할 경우, 각 노드는 메시지가 정당한 송신자(BS)로부터 보내진 것인지 인증과정을 제공하는 프로토콜이다. μTESLA는 각 노드들에게 데이터 전송 시 시간간격 i마다 RC5를 이용한 PRF를 통해 비밀키를 변경시킨다. 그러므로 수신자는 송신자가 보낸 패킷의 키를 생성하기 위해 BS와 시간 동기화가 되어있어야 한다. 만약 시간 동기화가 이루어져있지 않다면 다음 과정을 통해 동기화를 이룬다.

① BS는 다음 전송할 패킷의 인증을 위해 랜덤하게 Kn을 생성한다.

② 노드 A는 BS에게 시간 동기화를 위해 비표를 전송한다.

③ BS는 동기화를위해 A에게 메시지를 전송한다.

BS → A : TS | Ki | Ti | Tint | δ

MAC( KBA , Nonce | TS | Ki | T )

④ A는 KBA 를 생성하여 BS가 보낸 메시지임을 인증한다.

수신자가 브로드캐스팅 패킷을 인증하는 과정은 다음과 같다.

① 노드와 시간 동기화가 맞춰졌으면 BS는 각 노드들에게 패킷을 전송하는데 이 때, Ki는 공개하지 않는다. BS → A : Msg, MAC( Ki, Msg )

② B는 전송된 패킷을 저장 공간에 저장한다.

③ BS는 일정한 시간간격 δ 만큼 지나면 Ki를 공개한다.

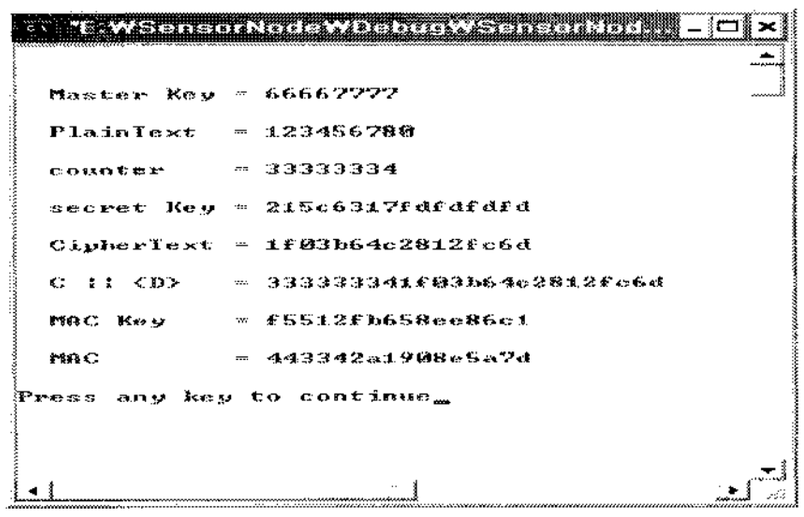
④ BS가 지금 Ki를 공개하듯이, 이전에 공개한 키를 Kv 라 한다. A는 PRF를 통해 Kv로 부터 Ki를 매핑시킬 수 있으며 Kv=Ki 가 성립할 경우 BS가 interval v~i 사이에 보낸 패킷의 인증이 이루어진다.

## V. 구현결과 및 분석

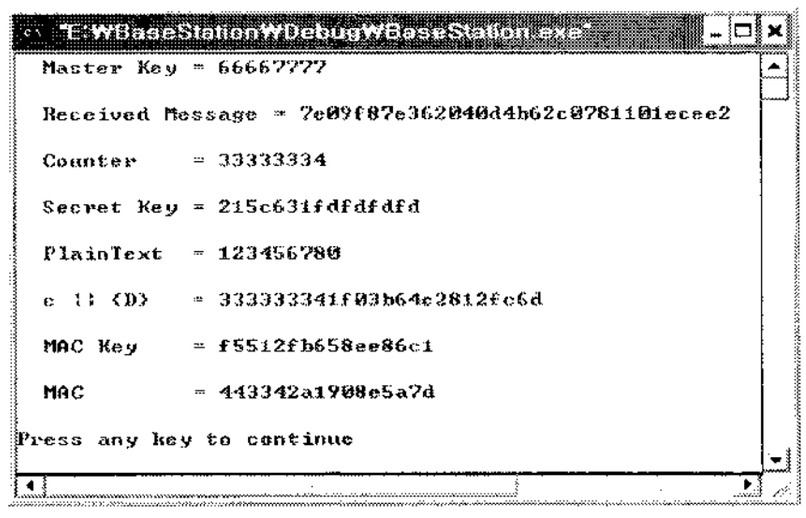
본 연구에서는 Visual Studio 6.0을 이용하여 C로 MAC을 생성하고 카운터 증가에 따른 메시지 비교 및 μTESLA의 키 생성을 구현하여 보안성의 보장을 확인하였다.

### 5.1 SNEP

그림 5.(a)는 노드 A에서 평문과 마스터키, 카운터가 주어졌을 때 생성된 MAC 값을 보여주고 있다. 수신자에게는 [CipherText | MAC]의 형식의 메시지가 전송된다. 그림 5.(b)는 노드 A가 메시지를 암호화하고 MAC과 함께 노드 B에게 보낸 것을 나타낸다. 노드 B는 미리 알고 있는 A의 카운터를 이용해 비밀키를 생성하고 메시지를 복호화하는 과정을 볼 수 있다. 또한 MAC키를 생성하고 A 노드의 MAC 값과 일치를 확인하여 정당한 송신자로부터의 메시지임을 확인할 수 있다. 또한 결과를 보면 복호화 하는 시간이 암호화하는 시간보다 빠르다는 것을 확인할 수 있다.



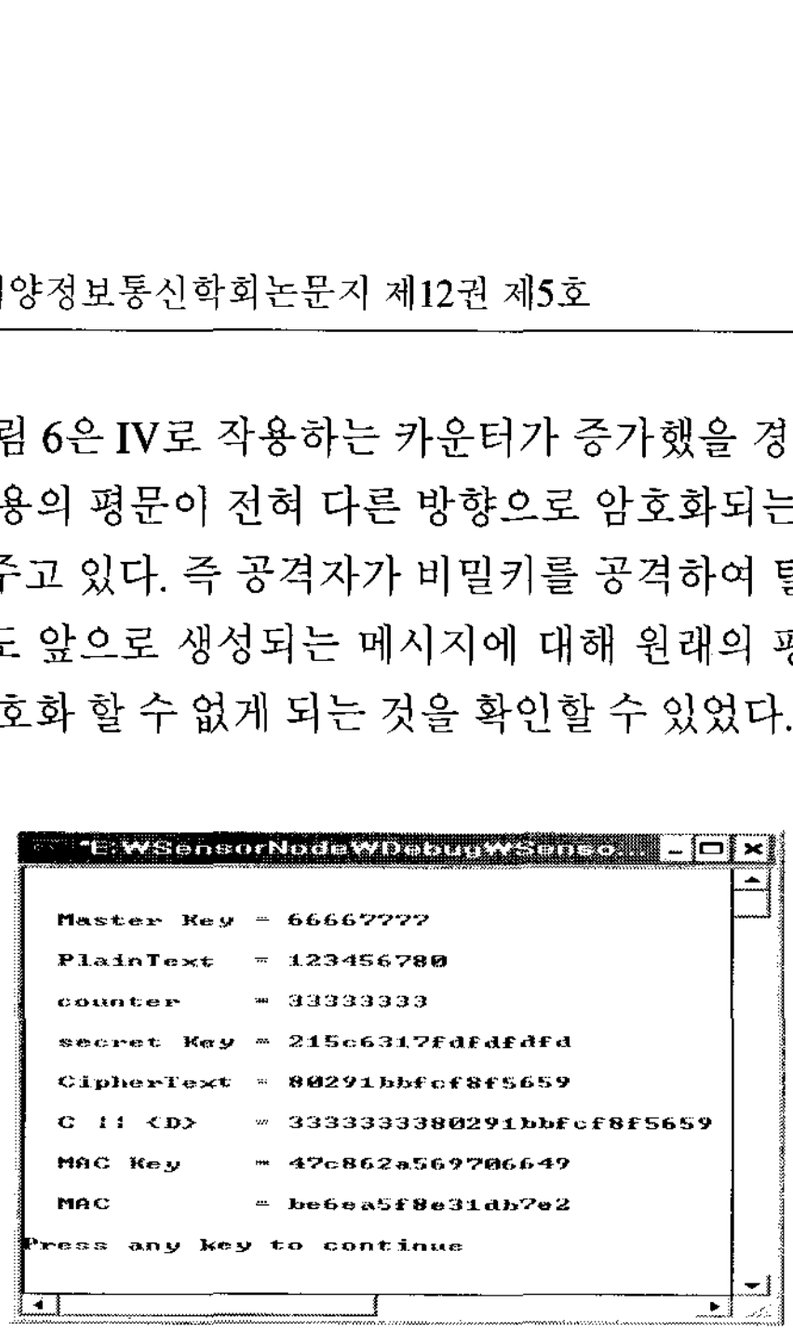

(a) 노드 A의 MAC 생성




(b) 노드 B에 의한 암호화 및 인증

그림 5. MAC 생성과 SNEP 구현
Fig 5. MAC generation and Implementation of SNEP

그림 6은 IV로 작용하는 카운터가 증가했을 경우, 같은 내용의 평문이 전혀 다른 방향으로 암호화되는 것을 보여주고 있다. 즉 공격자가 비밀키를 공격하여 탈취하더라도 앞으로 생성되는 메시지에 대해 원래의 평문으로 복호화 할 수 없게 되는 것을 확인할 수 있었다.




(a) 카운터 초기화

(b) 카운터의 증가

그림 6. 카운터 증가로 인한 암호문의 비교
Fig 6. Comparison of ciphertext by counter increasement

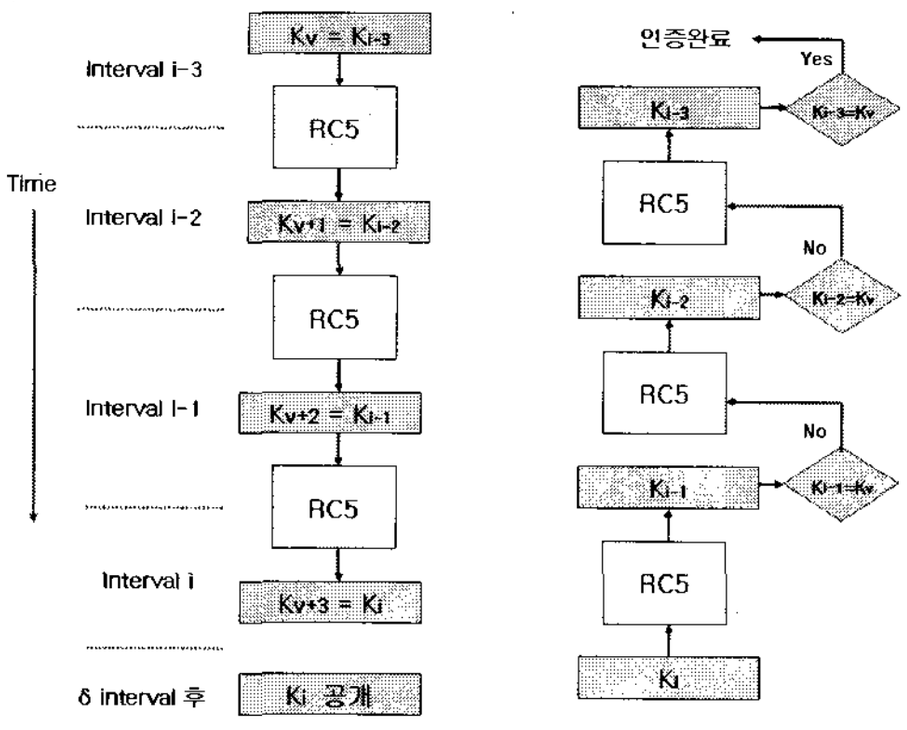
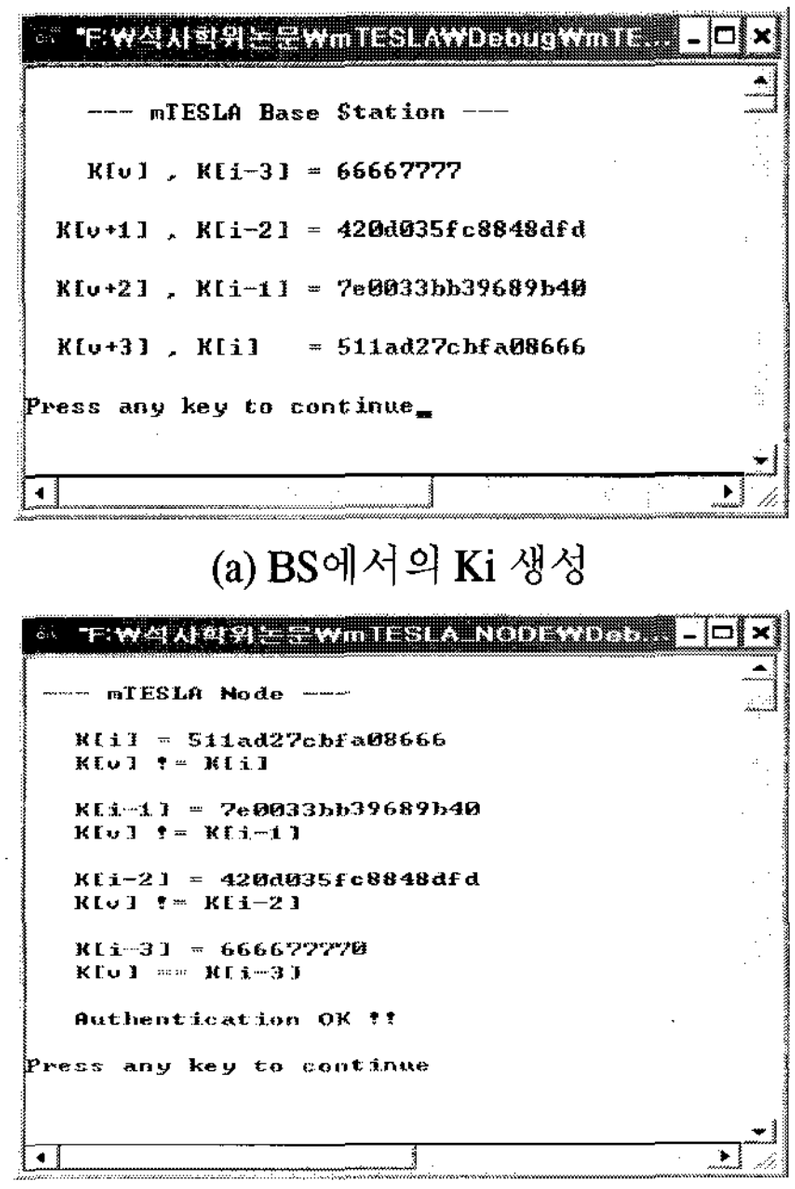



그림 7. μTESLA의 브로드캐스팅 인증
Fig 7. μTESLA's broadcasting authentication




(a) BS에서의 Ki 생성

(b) 노드의 키와 생성된 키의 비교

그림 8. μTESLA 인증의 구현
Fig 8. Implementation of μTESLA authentication

### 5.2 μTESLA

μTESLA는 메시지의 기밀성을 요구하지 않으므로 키 전송을 중심으로 구현하였다. 구체적인 개요는 그림 7과 같고, 그림 8은 생성된 키와 노드들의 키를 비교하여 인증을 수행한 결과를 나타낸다.

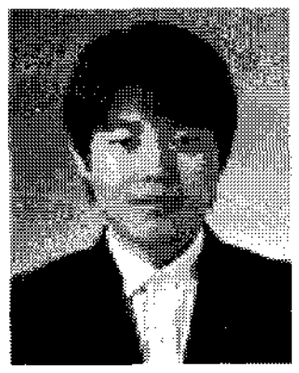
### 5.3 라운드 변화에 따른 성능평가

SNEP는 RC5 알고리즘을 이용한 PRF에 의해 키를 생성한다. RC5는 일반적으로 이전의 데이터를 순환시키는 방법으로 암호화하는데, 라운드 횟수를 10에서 60까지 10회씩 증가시키며 측정하여 보았다. 그 결과 SPINS에서 사용하는 보안 알고리즘은 라운드 횟수에 따라 연산량이 산술적으로 증가하는 것을 알 수 있었다. 이는 라운드횟수가 약간의 변동이 있더라도 연산량에 미치는 영향은 상대적으로 크지 않아 센서 노드의 연산량 부담을 줄일 수 있는 요소로 볼 수 있다.

## VI. 결론

본 연구에서는 센서 네트워크 보안 메커니즘을 홈네트워크 구조에 적용한 시스템을 설계하고 이를 홈네트워크 미들웨어의 가상망에 구현하였다. 센서 네트워크 보안 기술인 **SPINS**는 기밀성과 인증을 보장하는 **SNEP**와 브로드캐스트 인증을 제공하는 **μTESLA** 부분으로 구성되는데 이를 홈네트워크 미들웨어의 기본구조에 적용한 시스템을 설계하였다. **MAC** 생성을 위한 **CBC-MAC**, 메시지 신선성을 제공하는 **CTR**, 메시지의 랜덤특성을 보장하여 주는 **PRF**와 센서노드에 사용될 암호화 알고리즘으로 낮은 연산량으로 충분한 보안성을 갖는 **RC5**를 이용하였다. 구현된 결과는 **CTR** 모드로 인해 공격자가 키를 습득하더라도 새로운 메시지를 복호화 할 수 없었으며 상호 **MAC** 교환으로 인해 정당한 사용자로부터 전송되었다는 것을 인증할 수 있었다. 또한 **RC5**의 라운드 변화에 따른 연산량을 측정하여 노드에 갑작스런 부하를 주지 않음을 확인하였다.

## 저자소개

**설 정 환(Jeong-Hwan Seol)**

2006년 인천대학교 정보통신공학과 공학사
2008년 인천대학교 정보통신공학과 공학석사
※관심분야: 인터넷프로토콜, 센서네트워크보안

**이 기 영(Ki Young Lee)**

1982년 연세대학교 전기공학과
1984년 연세대학교 대학원 전기공학과 공학석사
1987년 Univ. of Colorado, ECE, M.S.
1993년 Univ. of Alabama, ECE, Ph.D.
1994년~현재: 인천대학교 정보통신공학과 교수
※관심분야: 인터넷 트래픽 제어 및 프로토콜, USN, 네트워크 보안시스템


## 참고문헌


[1] 한종욱 외2인, "홈네트워크 보안 기술 동향", 한국통신학회지 제23권 9호, pp.113-124, 2006년.

[2] 이전희, "홈네트워킹을 위한 경량화된 보안 메커니즘 설계 및 구현", 건국대학교 컴퓨터정보통신공학과 석사학위논문, 2003년.

[3] W. Keith Edwards, "Core Jini", 영한출판사, 2002.

[4] 고광우, "장애허용을 제공하는 경량 홈 네트워킹 미들웨어 설계 및 구현", 건국대학교 컴퓨터정보통신공학과 석사학위논문, 2003년.

[5] Adrian Perrig et al, "SPINS : Security Protocols for Sensor Networks", Wireless Networks Journal, vol.8 pp.521-534, 2002.

[6] William Stallings, "Cryptography and Network Security", Pretice-Hall, 2003.

[7] 나재훈 외 2인, "센서네트워크 보안 연구동향", 전자통신 동향분석, 제20권1호, pp.12-22, 2005년.

[8] E. Shi and A. Perrig, "Designing Secure Sensor Networks", IEEE Wireless Communications, vol.11, no.6, pp.38-43, 2004.