2005년도 대한전자공학회 추계종합학술대회 제28권 제2호

# 홈네트워킹 미들웨어 보안 시스템 설계 및 구현

이 호 상, 이 정 균, 이 기 영
인천대학교 정보통신공학과
전화 : 032-770-8615

# Design and Implementation of HomeNetworking Middleware Security System

Ho-Sang Lee, Jeong Kyun Lee, Ki Young Lee
Dept. of Information & Telecommunication Engineering, University of Incheon
E-mail : hahaite@hahaite.net

## Abstract

In this paper, a secure system is studied and designed for omenetworking middleware based on sensor network security algorithm. Many sensor networks have mission-critical tasks, so it is clear that security needs to be taken into account at design procedure.

First, We study homenetworking middleware model in Jini. And we design a security system is applied by SPINS algorithm for moddleware model. Then we firgure out proper secrecy, authentication, broadcast authentication mechanisms in this model.

## I. 서론

유비쿼터스 네트워크는 어디서나 주위의 모든 대상과 네트워크를 형성할 수 있다는 것을 의미한다. 센서 네트워크는 유비쿼터스 컴퓨팅 구현을 기반 네트워크로 초경량, 저전력과 제한된 컴퓨팅 능력을 가진 노드들로 이루어진 무선 네트워크를 일컫는다.

이러한 센서네트워크로 이루어진 홈네트워크는 댁 가정 내 모든 기기를 하나의 네트워크로 연동시켜 가정 안에서 뿐만 아니라 외부에서도 가정의 모든 장비들을 관찰하거나 제어할 수 있는 기술을 말한다. 홈네트워킹 미들웨어는 사용자와 댁 내 장치의 중간에 위치하여 장치를 제어하고 상호 정보교환을 보장하며 집밖과 집안을 오가는 멀티미디어 서비스를 가능하게 하는 기술이다.

홈네트워킹 미들웨어는 가정이라는 사생활이 보장되어야 하는 공간에 위치하기에 장비, 즉 노드간의 보안이 매우 중요하다 할 수 있다. 이에 본 연구는 LookUp 서버를 이용하는 홈네트워킹 미들웨어 구조에 데이터 기밀성과 인증, 그리고 브로드캐스트 인증을 제공하는 보안 메커니즘인 SPINS를 적용하는 시스템을 설계, 구현하여 보았다.

II 장에서는 홈네트워킹 미들웨어 기술 중의 하나인 Jini 기반의 미들웨어 구조를 소개한다. III 장에서는 II 장에서 소개되는 구조에 적용될 SPINS에 대해 중점적으로 알아본다. IV 장에서는 홈네트워킹 미들웨어에 적용된 SPINS를 설계하고 구현한 것에 대해 설명하고, V장에서 결론을 맺는다.

## II. 홈네트워킹 미들웨어

### 2.1 홈네트워킹 미들웨어

홈네트워킹 미들웨어는 홈네트워크 환경에서 각종 가전기기, 정보기기 등을 상황에 맞게 구성하고 제어하며 상호 연동을 이루는 프레임워크를 말한다. 미들

웨어 기술로는 MicroSoft 사의 UPnP, Sun MicroSystem 사의 Jini, 일본의 AV 가전업체들이 제안한 HAVi 등이 있으며 서로 기술력을 경쟁하고 있다.

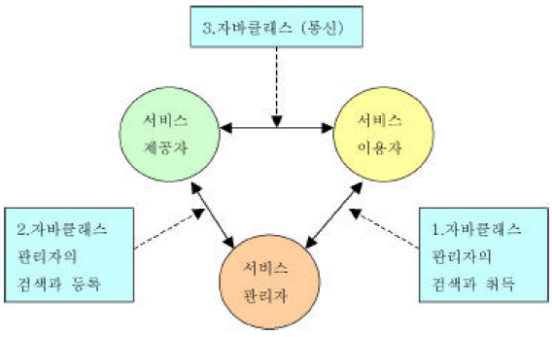
| | Jini | UPnP | HAVi |
|---|---|---|---|
| 기반 Network | IP Network | IP Network | IEEE 1394 |
| 기반 S/W | Java2, RMI | HTTP, HTML, XML | Object-Oriented |
| 운영방식 | C/S | C/S | P2P |
| Plug&Play | Jini 자체 feature | UPnP' SSDP | 1394 media's feature |
| 취약분야 | Stream 처리 | Stream 처리 | IP Network 기반 접속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

<표 1> Home 네트워킹 미들웨어 솔루션 비교

### 3.2 Jini 시스템

Jini는 선 마이크로시스템사에서 개발한 미들웨어로서 Java를 기반으로 한다. 그러므로 JVM(java Virtual Machine) 위에서 동작하기 때문에 운영체제나 기타 하드웨어 플랫폼에 무관하게 동작하게 된다. Jini 시스템은 서비스 이용자(client), 서비스 제공자(device), 서비스 관리자(lookup Server) 세부분으로 구성된다.

이 세 구성 요소는 Discovery, Join, Lookup, Service Invocation의 4 단계를 거쳐 서비스 제공자가 제공하는 서비스를 이용할 수 있다. 먼저, 서비스 제공자는 Discovery 프로토콜을 이용하여 Lookup 서비스를 찾고, 이렇게 찾은 lookup 서비스에 서비스 제공자의 서비스를 Join을 통하여 등록한다. 클라이언트는 사용할 수 있는 서비스에 관한 위치 정보 등을 Lookup 서비스를 통해 파악하고 최종적으로 lookup 과정을 통해 검색된 서비스를 호출하여 서비스를 받게 된다.




<그림 1> Jini의 구성 요소

## III. 센서 네트워크 보안

### 3.1 센서네트워크 보안의 취약성

USN(Ubiquitous Sensor Network) 이란 모든 사물에 컴퓨팅 및 커뮤니케이션 기능을 부여하여 언제, 어디서나, 무엇이든 통신이 가능한 환경을 구현하기 위한 것이다.

센서가 부착되어 데이터를 감시, 수집, 전송하는 센서노드는 다음과 같은 특징을 갖는다.

- 노드의 저전력, 저비용(low cost)
- 작은 기억공간
- 낮은 컴퓨팅 능력
- 배터리의 사용 -> 수명문제

결국 센서노드의 배치가 물리적인 환경에 그대로 노출되어 있음에도 불구하고 다른 유무선망에서 사용하는 강력한 보안 메커니즘을 적용시킬 수 없다. 즉 센서 네트워크에 보안 요소를 적용시키기 위해서는 복잡한 알고리즘을 피해야 하고, 오버헤드 발생이 적어야 하며, 센서노드에서의 처리량을 줄이는 것이 관건이라 할 수 있다.

| 항목 | 사 양 |
|---|---|
| CPU | 8-bit, 4MHz |
| Storage | 8Kbytes instruction flash<br>512 bytes RAM<br>512 bytes EEPROM |
| Communication | 916 MHz radio |
| Bandwidth | 10 Kbps |
| Operation System | Tiny OS |
| OS code space | 3500 bytes |
| Available Code Space | 4500 bytes |

<표 2> SmastDust nodes의 특성 [#]

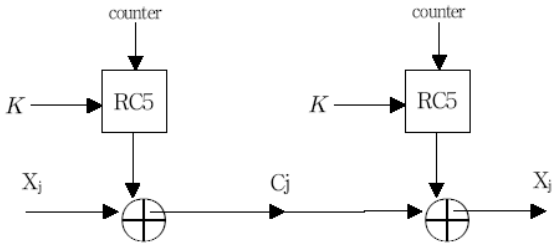
### 3.2 SPINS

미 버클리 대학에서 연구, 개발한 SPINS(Security Protocols for Sensor Networks)는 센서 네트워크의 제약환경을 고려한 보안 알고리즘의 하나이다. SPINS는 크게 데이터의 기밀성을 제공하기 위한 SNEP(Secure Network Encryption Protocol)과 BS(Base Station)에서 각 노드에 브로드캐스킹되는 데이터의 인증을 보장하는 $\mu$TESLA로 구성되어 있다.

(가) SNEP

SNEP는 데이터 전송 시 기밀성을 제공하게 된다. 이 때 데이터를 암호화하는데 센서노드의 부하를 줄이고 오버헤드가 크게 발생하지 않는 ciper-block chaining(CBC) 방식을 사용하며 암호화 알고리즘은 RC5가 사용된다. 또한 전단계에서 사용하는 암호화 키를 Counter mode(CTR)로 암호화 하는 방식을 취한다. A에서 B로 전송되어지는 메시지 다음과 같다.

$A \rightarrow B : \{D\}_{<K_{AB},C_A>}, MAC(K'_{AB}C_A||\{D\}<K_{AB},C_A>)$



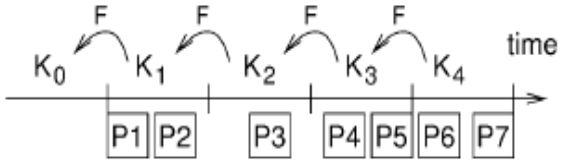

<그림 2> SNEP의 암호화 과정

(나) μTESLA

센서 네트워크에서 센서노드가 asymmetric mechanism을 통해 브로드캐스팅을 수행하는 것은 컴퓨팅 파워, 통신부하, 저장공간 등의 문제점으로 인해 적용시키는 데에 어려움이 따른다. 이에 μTESLA는 BS가 각 노드에 단방향 키체인 방식(one-way key chain) 방식을 사용한다. 이 때 시간이 지날수록 시간 간격에(time interval) 따라 이전 키의 영향을 받아 새로운 키가 생성된다. 수신자는 송신자로부터 Kn+1로 생성된 인증 패킷을 받았을 경우,

$$K_n = F(K_{n+1})$$

을 통해 이전 키를 알아낼 수 있다. 이 때 송수신자는 시간 간격이 일치하지 않으면 이전 키를 알아낼 수 없다.

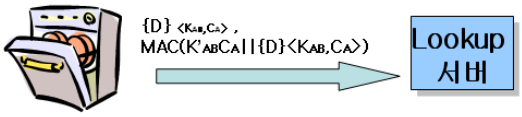



<그림 3> μTESLA의 단방향 키체인 방식

## IV. 미들웨어 보안시스템 설계 및 구현

### 4.1 SNEP 설계 및 구현

SNEP 는 SPINS 알고리즘에서 데이터의 기밀성과 인증을 제공하게 된다. 그러므로 Jini의 통신 구조에서 Lookup 서버와 기기간 메시지 교환 시 SNEP를 적용하였으며 <그림 4> 과 같다.




<그림 4> 센서노드 메시지의 SNEP 구현

구체적인 절차는 아래와 같다.

① 송신자는 BS와 공유하고 있는 마스터키 x를 이용하여 암호키 K를 생성한다. 그리고 이 키와 카운터값을 이용하여 메시지를 암호화 한다.

② 송신자는 1)과 마찬가지로 x 를 이용하여 인증키 K′ 를 생성하며 이를 이용하여 인증 메시지를 생성하여 수신자에 전송하게 된다.

③ 수신자는 마스터키와 이미 송신자와 동기화가 이루어져있는 카운터값을 이용하여 데이터 복호화와 인증을 수행한다.

④ 송신자가 다시 메시지를 전송할 경우, 마지막으로 사용한 카운터에서 증가한 값을 이용하여 암호화를 이루며 이 카운터값은 BS만이 알고 있다.

### 4.2 μTESLA 설계 및 구현

홈네트워크 미들웨어의 lookup 서버는 일반적으로 가정 내 하나가 존재하여 여러 가전기기와 서로 통신을 하게 된다. 즉 센서네트워크에서 BS 역할을 담당하는 곳이라 할 수 있다. 그러므로 필요시 BS는 노드역할을 하는 모든 가전기기에 메시지를 줄 수 있으며 이 경우 브로드캐스팅 인증을 제공하게 된다.

세부 구현단계는 다음과 같다.

① n 길이의 키체인 생성을 위해 송신자는 마지막 키 Kn을 선택한다.

Kn -> Kn-1 -> Kn-2 -> ... -> K0

Kj = F(Kj+1)

② 시간을 time interval로 나누고, 키 체인의 키와 매핑시킨다. 이 때 interval i에 생성되는 MAC 생성 알고리즘 입력키로 Ki를 사용한다.

③ interval i가 경과한 후부터 δ interval 후에 Ki를 노출시킨다.

④ 수신자는 one-way function을 이용해, 가지고 있던 Kv와 Ki를 Kv=Fi-v(Ki) 를 이용하여 매핑을 시행하고, 매핑이 되면 interval v~i 동안 보내졌던 모든 패킷이 인증되게 된다.

## Ⅳ. 결론 및 향후과제

본 연구에서는 lookup 서버를 이용해 댁내 노드를 제어하는 홈네트워크 미들웨어 Jini 구조에 데이터의 기밀성, 인증과 브로드캐스트 인증을 제공하는 SPINS 보안 알고리즘을 적용시켜 보았다. SNEP 알고리즘을 이용해 센서노드에 부하를 많이 일으키지 않으면서 충분한 기밀성을 제공할 수 있었고, 기존 TESLA 방식을 센서 네트워크에 적용시킬 수 있도록 고안된 $\mu$TESLA를 통해 브로드캐스트 인증을 실행시킬 수 있었다.

본 연구를 통해 보안에 상대적으로 많은 취약점을 가질 수 있는 홈네트워크 미들웨어에 보다 효율적인 보안 시스템을 구현할 수 있었다.

향후 과제로는 가상망이 아닌 실제 노드에 시스템을 적용시켜 보안강도가 체크되어야 할 것이며 다른 센서 네트워크 보안 알고리즘의 연계도 같이 고려되여야 할 것이다.

## 참고문헌

[1] 나재훈 외, “센서 네트워크 보안 연구 동향”, 전자통신동향분석 20권 1호, pp112-122, 2005.1

[2] 박춘식, “유비쿼터스 네트워크와 시큐리티 고찰”, 정보보호학회지 14권 1호, pp12-23, 2004.2

[3] 박종욱 외, “유비쿼터스 센서 네트워크의 정보보호 이슈와 동향”, 한국통신학회지 21권 6호. pp715-727

[4] 서운석 외, “센서 네트워크 보안 프로토콜 소개와 향후 과제”, 정보과학회지 22권 12호, pp60-66 2004.12

[5] 김연숙 외, “홈 네트워크에서의 미들웨어”,

[6] Elaine Shi 외, “Designing Secure Sensor Networks″, IEEE Wireless Communications, pp38-43, 2004.12

[7] 서승우, “Security Issues in Sensor Networks″, NetSec-KR 2005, pp305-325, 2005.4

[8] A.Perrig 외, “SPINS : Security Protocols for Sensor Networks ″, Proc. of the 7th ACM/IEEE International Conference on MobiCom. 2001