[10-55]

Kerblet : WPAN용 커버로스 기반의 간단한 인증 프로토콜

*조승현, *남혜진, *윤종호, **전영애
*한국항공대학교 정보통신공학과
**한국전자통신연구원
*acidburn@hau.ac.kr, *queen@windct.com, *yoonch@mail.hau.ac.kr, **yajeon@etri.re.kr

Kerblet : A Simple Authentication Protocol based on Kerberos for WPAN

*Seung-Hyeon Cho, *Chong-Ho Yoon, **Young-Ae Jeon
*Department of Information and Communication Engineering, Hankuk Aviation University
**Electronics and Telecommunications Research Institute

요 약

WPAN환경에서 보안 피코넷을 운영하기 위해서는 피코넷 내부 단말간의 신뢰가 필수적이다. 그러나 현재 IEEE 802.15.3표준에서는 보안 피코넷의 기본 동작 절차 및 운영만을 언급할 뿐, 각 단말에 대한 인증방법에 관하여는 다루고 있지 않다. 또한, 피코넷에서의 인증을 위해서 기존에 제안되었던 방법들은 대역폭의 낭비와 단말에서의 부하와 같은 문제점들을 가지고 있다. 따라서, 본 논문에서는 WPAN에서 각 단말을 인증하고, 보안 피코넷 운용을 위한 키를 분배할 수 있는 새로운 프로토콜인 Kerblet을 제안한다. 제안된 Kerblet프로토콜은 기존의 커버로스 프로토콜을 기반으로, WPAN환경에 맞게 경량화하고 절차를 단순화 한 것으로서, 기존의 방법들보다 효율적인 인증절차와 키분배방식을 가지고 있다. 즉, WPAN은 가정용 무선 네트워크 환경이므로, Kerblet에서는 pre-shared key방식을 사용하고, 인증절차를 4단계로 줄였으며, 고정길이의 패킷 형식을 사용함으로써, WPAN 단말에서 예상되는 부하와 인증절차로 인한 대역의 낭비를 감소시켰다.

1. 서론

Wireless Personal Area Network(WPAN) 피코넷에서의 보안은 다음과 같은 두 가지 모드로 제공된다[1].

- □ **모드 0 – Open :** Security membership이 요구되지 않기 때문에 페이로드에 대한 보호(데이터 무결성 및 암호화)를 하지 않는다.
- □ **모드 1 – Secure membership and payload protection :** 각 단말(DEV)은 피코넷에 연결하기 위하여 우선 piconet coordinator(PNC), 또는 다른 단말과의 보안연계(secure relationship)를 맺어야 한다. 이후, 데이터에 대한 무결성과 암호기능을 지원한다. 또한 제어메시지에 대한 무결성 또는 암호에 의한 보호도 지원된다. 단, 비컨 메시지에 대해서는 무결성만 지원된다.

특히, 모드1을 사용하는 경우, 각 단말이 피코넷에 가입하여 PNC와의 보안연계의 설정뿐만 아니라, 다른 단말과의 직접 통신을 위하여 해당 단말과의 점대점 보안연계를 맺을 수도 있다.

이때, 쌍방간의 암호 및 메시지 인증용 키는 대칭키이며, 이 키를 갱신할 경우, Distribute Key Request와 Key Request 제어메시지가 사용된다. 물론, 이러한 메시지에 수납되어 전송되는 키는 이전 키로 암호화되어 전송된다.

하지만, 이러한 보안멤버쉽(피코넷 group member)이나 단말간 보안연계의 설정, 그리고 세션키 확보과정 등은 IEEE 802.15.3표준에서 다루어지지 않고, 평문형식의 security information 메시지를 사용한 송수신절차만을 규정하고 있기 때문에, 이 메시지를 사용하여 해당 멤버쉽이나 비밀키를 별도의 상위 키분배 및 인증 방식을 사용하여 분배하는 방법들이 제안되어 있다[4].

본 논문에서는 단말이 PNC에 연결설정(association)된 후, PNC와 단말간의 보안멤버쉽 설정을 위한 인증절차 및 비밀키 분배과정을 위하여, 기존의 복잡한 커버로스 인증프로토콜을 간략화한 Kerblet프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 제 2 장에서는 802.15.3에 규정된 보안관련 기본동작을 요약 정리하고, 새로운 인증프로토콜의 필요성을 제시한다. 제 3장에서는 WPAN에서의 인증과 키분배를 위한 새로운Kerblet 프로토콜을 제안하며, 제 4 장에서는 결론을 맺는다.

2. WPAN 환경에서의 보안[1]

2.1 WPAN에서 사용되는 키의 종류

WPAN에서 키는 프레임의 용도와 해당 단말의 멤버쉽 상태에 따라 다음과 같은 4가지의 키가 사용된다.

- □ PNC 관리키 : PNC와 다른 모든 단말간의 제어메시지에 대한 보호용 키.
- □ 피코넷 그룹 데이터키 : PNC와 주고받는 모든 데이터 및 일부 제어 프레임, 그리고, 비컨의 보호용이다. 즉, 비컨, 데이터, PNC Information, Probe, Announce, Channel Status, Transmit Power