RUPI기반 로봇 환경에 적합한 키 관리 기술

김건우*, 한종욱

*한국전자통신연구원

Key Management Technology for RUPI-based Robot Environment

Geon-woo Kim*, Jong-wook Han

*Electronics and Telecommunications Research Institute

E-mail : kimgw@etri.re.kr

요 약

RUPI 기반 로봇 서비스는 다양한 성능을 지원하는 로봇과 서버간의 연동을 통해서 융통성과 확장성을 보장하는 로봇 기반 서비스를 제공한다. 이러한 로봇 서비스를 제공하는데 있어서 안전성 보장은 필수 요소이다. 하지만 로봇 서비스에 적용되는 각 노드의 다양한 성능을 보장하기 위해서는 각 서비스에 맞는 보안 메커니즘이 적용되어야 하며, 이를 위해서 효율적인 키 관리 구조가 선행되어야 한다. 따라서 본 논문에서는, RUPI 기반 로봇 환경에 적합한 키 관리 구조를 제안한다.

ABSTRACT

RUPI-based robot service provides a variety of robot services guaranteeing extensibility and flexibility by communications between heterogeneous robots and servers. While providing robotic services, the guarantee of safety is essential. However, as to support a variety of capability of each node deployed in robotic services, security mechanisms that are suitable for each service must be applied. Also, efficient key management structure must be preceded. Therefore, in this paper, we propose a key management structure suitable for RUPI-based robot environment.

키워드

로봇 보안, 로봇 키 관리, RUPI 보안

Ⅰ. 서 론

홈네트워크는 이동통신, 초고속 인터넷 등 유·무선 통신 네트워크를 기반으로 가정 내의 A/V, 데이터통신 및 정보가전 기기들이 네트워크로 상호 연결되어 기기·시간·장소에 구애받지 않고 다양한 서비스를 제공받을 수 있는 가정 환경을 구축하여 국민들에게 편리하고, 안전하고, 즐겁고, 윤택한 삶을 제공할 수 있는 새로운 IT 기술 이용 환경이라 할 수 있다 [1].

이러한 홈네트워크 서비스의 하나로서 로봇에 관한 많은 연구와 개발이 현재 활발히 진행 중이다. 로봇 서비스는 인터넷과의 연결로 인하여 인터넷에서 발생되고 있는 다양한 사이버 공격에 그대로 노출되어 있어 해킹, 악성코드, 웜 및 바이러스, 서비스 거부 공격, 통신망 도·감청 등에 보안 취약성을 내포하고 있다 [2]. 또한 정상적인 홈네트워크 사용자일지라도 사용자의 권한과 특성을 고려해서 서로 다른 서비스를 제공해야 할 필요성이 있다. 또한 제한된 성능을 지원하는 Thin-client 로봇에는 기존 보안 메커니즘을 그대로 적용하기에는 많은 어려움이 있다.

따라서 본 논문에서는, 지능형 로봇 환경의 제약사항을 고려해서 보안 메커니즘을 적용하고 수행하기 위한 키 관리 기술을 제안한다.

제 2절에서는 키 관리 구조, 키 분배 프로토콜을 제안하고, 제 3절에서는 결론을 맺는다.

II. 본 론

지능형 로봇 환경을 구성하는 로봇은 지원하는 성능에 따라 Rich-client 로봇과 Thin-client 로봇으로 나눌 수 있다. Rich-client 로봇은 일반적으로 컴퓨터와 비슷한 H/W 성능과 계산 능력을 보유하고 있으며, 비교적 복잡하고 다양한 기능을 수행한다. 반면 Thin-client 로봇은 간단한 임베디드 운영체제 조차 탑재되지 않고 단순한 회로 소자만으로 구성되어 있다.

따라서 로봇 보안 시스템은 이러한 로봇의 성능적 제약 사항을 고려해서 설계되어야 하며, 다양한 보안 메커니즘을 가능하게 하는 키 관리 또한 신중하게 개발되어야 한다.

2.1 키 관리 개요

본 논문에서 제안하는 키 관리 구조는 크게 두 계층으로 구분할 수 있다. 즉, Thin-client와 같은 저성능 로봇을 위한 대칭키 관리 구조와 그 외 고성능 로봇 및 서버를 위한 공개키 관리 구조로 구성되어 있다.

지능형 로봇 보안 시스템을 위한 키 관리 개요를 보면 그림 1과 같다.

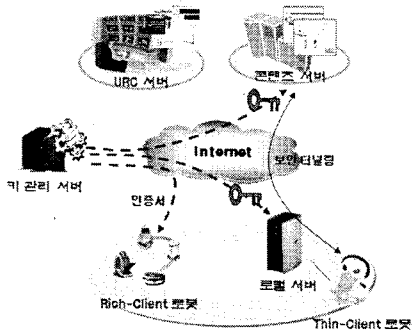

그림 1. 로봇 키 관리 개요

네트워크 로봇 서비스는 URC 서버와 콘텐츠 서버와 같은 로봇 서버군, Rich-client 로봇과 Thin-client 로봇으로 대표되는 로봇군, 및 Thin-client의 외부 기능을 대표하고 중간 서버 역할을 수행하는 로컬 서버로 구성된다. 단, 로컬 서버는 어플리케이션에 따라 서버군과 로봇군의 영역에 포함된다.

로봇 서비스에서 운용되는 모든 노드간 통신은 외부의 불법 접근으로부터 안전하게 보호되어야 한다. 또한 교환되는 콘텐츠의 신뢰성을 보장할 수 없으면 사용자에게 예상치 못한 결과를 초래할 수 있으며, 개인 프라이버시 침해를 가져올 수 있다. 따라서, 모든 세션에는 상호 인증 모듈이 선행되어야 하며, 이러한 상호 인증에는 통신하고자 하는 두 노드만 알고 있는 비밀 정보를 공유하고 있어야 한다. 키 관리 스킴은 크게 공개키 방식과 대칭키 방식이 있다. 공개키 방식은 인증서를 사용한 PKI 방식으로서, 대규모 인증 도메인이나 인터넷 상에서 일반적으로 사용된다. 확장성과 안전성이 뛰어난 장점이 있지만, 상대적으로 많은 연산을 필요로 하는 단점이 있다. 반면, 대칭키 방식은 크기가 제한된 인증 도메인에서 주로 사용되며, 적은 연산을 요구하지만 확장성을 지원하는데 단점이 있다.

2.2 키 관리 구조

네트워크 로봇 서비스에 운용되는 노드와 키 관리 개체간의 연관 관계를 보면 표 1과 같다.

표 1. 로봇 개체와 키 개체간 연관 관계

키 개체 / 로봇 개체	CA 서버	키 서버	키 클라이언트
URC 서버	Y	Y	Y
콘텐츠 서버	Y	Y	Y
Rich-client 로봇			Y
Thin-client 로봇			Y

표 1에서 보는 바와 같이, CA는 로봇 서비스를 제공하는 로봇 개체가 아닌 공인된 CA 서버를 적용하거나, URC 서버나 콘텐츠 서버, 또는 도메인 내의 별도의 사설 인증서를 관리하는 CA 서버를 운용할 수 있다.

키 서버는 대칭키를 운용하기 위한 서버로서, 다음과 같은 기능을 제공한다.

- 대칭키 생성 및 분배
- 대칭키 재분배
- 대칭키 폐기
- 대칭키 관련 정책 관리 및 운용

또한, 모든 로봇 개체는 키 클라이언트로 동작한다.

키 관리 서버는 다양한 보안 요구사항을 수용하고 비교적 많은 개수의 대칭키를 관리할 수 있어야 한다. 또한, 키 관련 보안 정책을 관리함으로써, 적용될 키 알고리즘, 키 길이, 및 키 재분배 사이클을 운용한다.

키 관리 서버는 물리적으로 한정된 서비스 도메인에만 적용되는 것이 아니라, 인터넷을 통해서 많은 인증 도메인 내의 모든 키 클라이언트를 관리해야 하기 때문에, 계층적 키 관리 서버를 구축할 수 있어야 한다. 더불어, 다른 인증 도메인내의 키 관리 서버와도 신뢰관계를 구축할 수 있는 기능을 제공해야 한다.

본 논문에서 제안하는 키 관리 구조를 보면 그림 2와 같다.

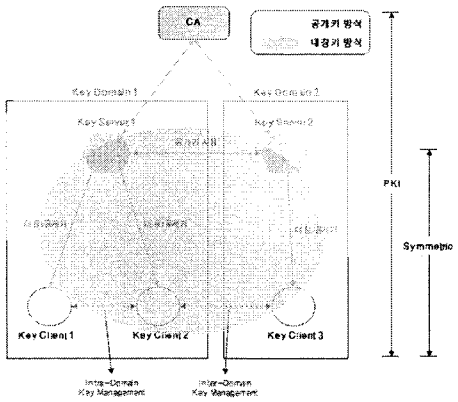

그림 2. 키 관리 구조

하나의 키 도메인 내에는 하나의 키 서버가 운용되며, 로봇의 범주에 따라 대칭키 방식과 공개키 방식을 동시에 적용할 수 있다. 키 도메인 내에서의 통신을 위해서, 통신하고자 하는 두 노드에 적용된 키를 이용하면 된다.

단, 다른 키 도메인에서 운용되는 키 클라이언트와 통신하고자 하는 경우에는 조금 더 복잡한 과정이 추가된다. 만일 공개키를 사용하는 경우에는 CA 서버를 통해서 상호 인증서를 검증하면 되지만, 대칭키를 사용하는 경우에는 상호 키 관리 서버를 인증하는 과정을 필요로 한다. 즉 키 도메인 내에서 사용되는 대칭키는 로컬 키 관리 서버에 의해서 발급된 키로서, 해당 키 도메인 내에서만 유효하다. 따라서 로컬에서만 유효한 키를 외부 도메인에서 사용하기 위해서는 두 키 도메인에서 동작하는 키 관리 서버간의 상호 인증 과정을 선행한 후, 이들 간의 신뢰 관계를 기반으로 서로의 대칭키를 신뢰한다.

2.3 세션키 분배 플로우

위의 과정을 통해서 상호 키를 인증한 후에는 세션을 사용될 대칭키를 생성하고 분배해야 한다. 두 노드가 공개키를 사용하는 경우, SSL과 같은 방식을 사용해서 세션키를 공유하면 된다.

따라서 본 절에서는 대칭키를 사용할 경우, 세션키를 생성하고 분배하는 플로를 보여준다.

그림 3은 대칭키를 이용한 세션키 생성 과정을 보여준다.

- 키 서버는 두 키 클라이언트에 대칭키를 분배한 후 대기한다.
- 키 클라이언트2와 통신하고자 하는 키 클라이언트1은 c1_nonce를 생성해서 키 서버에 전송한다.
- 이를 수신한 키 서버는 s1_nonce와 encrypted_c1_nonce를 키 클라이언트1에 전송한다.
- 키 클라이언트1은 수신한 encrypted_c1_nonce를 검증하고 encrypted_s1_nonce를 전송한다.
- 키 서버는 encrypted_s1_nonce를 검증한 후, 키 클라이언트2와 공유할 세션키를 생성해서 전송한다.

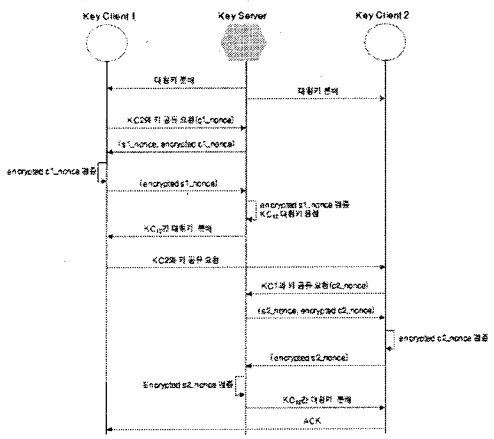

그림 3. 대칭키를 이용한 세션키 분배 플로우

- 키 클라이언트1은 키 클라이언트2에 세션키 공유를 요청한다.
- 키 클라이언트2는 c2_nonce를 생성해서 키 서버에 요청한다.
- 키 서버는 s2_nonce와 encrypted_c2_nonce를 키 클라이언트2에 전송한다.
- 키 클라이언트2는 수신한 encrypted_c2_nonce를 검증한 후, encrypted_s2_nonce를 전송한다.
- 키 서버는 encrypted_s2_nonce를 검증한 후, 키 클라이언트1에 분배한 세션키를 전송한다.
- 세션키를 수신한 키 클라이언트2는 키 클라이언트1에 응답 메시지는 전송한다.
- 두 노드간 안전하게 분배된 세션키를 사용해서 안전한 통신을 수행한다.

III. 결 론

RUPI 기반 로봇 서비스는 다양한 성능을 지원하는 로봇과 서버간의 연동을 통해서 융통성과 확장성을 보장하는 로봇 기반 서비스를 제공한다. 이러한 로봇 서비스를 제공하는데 있어서 안전성 보장은 필수 요소이다. 하지만 로봇 서비스에 적용되는 각 노드의 다양한 성능을 보장하기 위해서는 각 서비스에 맞는 보안 메커니즘이 적용되어야 하며, 이를 위해서 효율적인 키 관리 구조가 선행되어야 한다.

따라서 본 논문에서는, 지능형 로봇 환경의 다양한 특성을 고려한 키 관리 구조를 제안하고, 대칭키를 이용해서 세션키를 생성하고 분배하는 플로우를 제안한다.

참고문헌

[1] 김정원, 정보통신부, "홈 네트워크 산업 활성화 정책 방향", 정보과학회지, 2004, 09, 제 22권 제 9호 통권 제 184호

[2] 한종욱, 김도우, 주홍일, 한국전자통신연구원, "홈 네트워크 보안 프레이워크 구축을 위한 고려사항", 정보과학회지 2004, 09, 제 22권 제 9호 통권 제 184호