情報保護學會論文誌
第20卷 第1號, 2010. 2

안전한 M2M 통신 구축을 위한 상호인증 및 키 교환 프로토콜*

은 선 기,[1†] 전 서 관,[1] 안 재 영,[2] 오 수 현[1‡]
[1]호서대학교, [2]한국전자통신연구원

Mutual Authentication and Key Establishment Protocol to Implement Secure M2M Communication Environments*

Sun-Ki Eun,[1†] Seo-Kwan Jeon,[1] Jae-Young Ahn,[2] Soo-Hyun Oh[1‡]
[1]Hoseo University, [2]Electronics and Telecommunications Research Institute

요 약

최근 IT 기술이 발전하면서 보다 높아진 사용자의 편의성을 만족시키기 위해 다양한 형태의 통신 기술이 연구되고 있다. 다양한 연구들 가운데 기존 통신 형태와는 달리 사람의 제어나 관여 없이 디바이스 간에 통신 환경을 구축하는 M2M 통신이 주목받고 있다. 하지만 M2M 통신 환경의 특성으로 인해 데이터 노출, 데이터 도용, 데이터 불법 변경 및 삭제, 프라이버시 문제 등의 다양한 보안 위협에 보다 쉽게 노출될 가능성이 존재한다. 본 논문에서는 안전한 M2M 통신 환경을 구축하기 위해 고려해야 하는 보안 요구사항 도출하고 이를 구현하기 위해 필요한 보안 기능을 갖는 M2M 통신 아키텍처를 제안한다. 그리고 M2M 디바이스 및 게이트웨이 도메인과 M2M 네트워크 도메인 사이에 안전한 상호인증 및 키 교환을 제공하는 프로토콜을 제안한다. 제안하는 프로토콜은 재사용 공격, 위장 공격에 대해 안전하고 프라이버시 보호 및 추적을 방지할 수 있다는 장점이 있다.

ABSTRACT

Recently, as IT technologies developed, communication technologies of a various forms that satisfied convenience of user are being researched. Among various research, unlike traditional forms of communication, M2M communication is getting attention that without any control or involvement of people to establish communication between devices. However, the M2M communication could more easily be exposed to many security problems such as data exposure, data theft, unauthorized change and delete and privacy. Therefore, in this paper, we derive security requirements and propose the M2M communication architecture that provide a secure M2M communication environment. Also, we propose a secure mutual authentication and key establishment protocol between a M2M device or gateway domain and a M2M network domain. The proposed protocol is secure against replay attack, impersonation attack and protect a user privacy and tracing.

Keywords: M2M Communication, Security Architecture, Mutual Authentication, Key Establishment

I. 서 론

최근 IT 기술의 진보로 인해 통신 기술 또한 다양하게 변화하거나 새로운 형태의 기술이 생겨나고 있다. 그 중 새로운 형태의 통신 기술로써 사람의 제어나 관여 없이 디바이스 스스로 다양한 통신 기술을 이용하여 디바이스 간의 통신 환경을 구축하는 M2M (Machine-to-Machine) 통신 기술에 대한 연구가

접수일(2009년 10월 19일), 게재확정일(2009년 11월 30일)
* 본 논문은 2009년 한국전자통신연구원 위탁과제 지원에 의해 연구되었음.
† 주저자, eunsunki@gmail.com
‡ 교신저자, shoh@hoseo.edu

활발히 진행되고 있다[1]. 일반적으로 M2M 통신은 유선 또는 무선 통신 기술을 사용하여 디바이스 간의 연결을 설립하지만, 최근에는 디바이스 간의 무선 통신 기술만을 M2M 통신이라 칭하고 있다. 이러한 M2M 통신은 판매관리 시스템(POS: Point Of Sales)의 물류관리, 기계 및 설비의 원격 모니터링, 결제, 운송, 그리고 수도 및 전기 사용량을 자동 측정하는 스마트 미터기(smart meter) 등의 M2M 응용 분야에서 활발히 사용되고 있으며 앞으로는 더욱 많은 분야로 확산될 것으로 예상된다[2]. 또한 기존의 3GPP, TISPAN, WCDMA, HSDPA, GSM, W-LAN, 위성 등의 이동통신 및 무선 인터넷이나 Wi-Fi, Zigbee, 블루투스 등의 소출력 통신기술 등과 연계하여 보다 넓은 영역으로 서비스 범위의 확대하고 있다. 이와 같이 M2M 통신은 사용자에게 보다 편리한 통신 환경과 다양한 서비스를 제공할 것이다[3].

그러나 M2M 통신은 디바이스 간의 통신을 위해 다양한 무선 통신 기술을 이용하고 상대적으로 물리적 보안이 취약한 위치까지 디바이스가 배치됨으로써 데이터 노출, 데이터 도용, 데이터 불법 변경 및 삭제, 프라이버시 문제, 디바이스 도난 등의 다양한 보안 위협이 존재할 가능성이 있다[4][5][6].

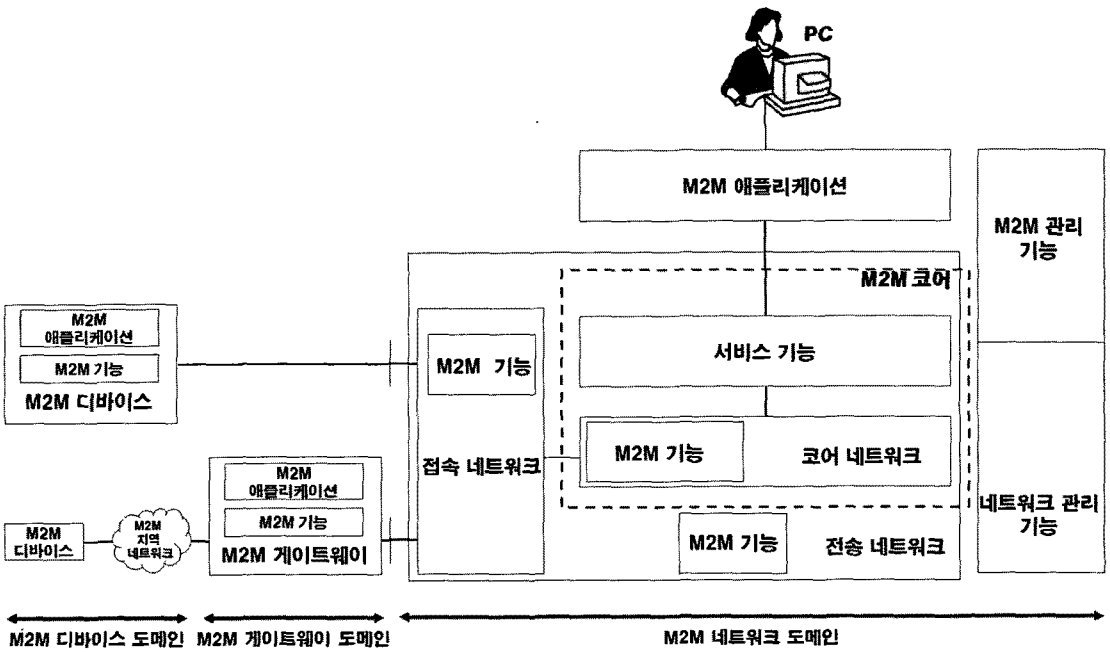
따라서 본 논문에서는 M2M 통신 아키텍처와 통신 인터페이스를 분석하고 M2M 환경에서 고려해야 하는 보안 요구사항을 도출함으로써, 보다 안전한 M2M 통신을 제공할 수 있는 보안성이 고려된 M2M 통신 아키텍처를 제안한다. 그리고 실제적인 M2M 통신 환경에서 M2M 디바이스 및 게이트웨이 도메인과 M2M 네트워크 도메인 사이에 상호인증 및 키 교환을 제공하는 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 관련연구로 M2M 통신 아키텍처, M2M 통신 인터페이스, 그리고 M2M 통신 환경의 보안 요구사항을 분석하고, 3장에서 보안 요구사항을 적용시킨 안전한 M2M 통신 아키텍처와 M2M 디바이스 및 게이트웨이 도메인과 M2M 네트워크 도메인 사이의 안전한 상호인증 및 키 교환 프로토콜을 제안한다. 그리고 5장에서는 제안하는 상호인증 및 키 교환 프로토콜의 안전성에 대해 분석하고 마지막으로 6장에서 결론을 맺는다.

II. 관련연구

2.1 M2M 통신 아키텍처

M2M 통신은 M2M 디바이스(device) 도메인, M2M 게이트웨이(gateway) 도메인, 그리고 M2M



[그림 1] M2M 통신 아키텍처

네트워크(network) 도메인으로 구성되며, 각 도메인 간에는 다양한 통신 기술을 통해 연결된다[7]. [그림 1]은 M2M 통신 아키텍처를 나타낸다.

o M2M 디바이스 도메인

M2M 디바이스 도메인은 M2M 디바이스와 M2M 디바이스들의 집합체인 M2M 지역(area) 네트워크로 구성된다.

• M2M 디바이스

M2M 기능(capability)과 통신 기능을 사용하여 애플리케이션을 구동시킬 수 있는 디바이스를 말한다. M2M 디바이스는 네트워크 도메인의 접속(access) 네트워크에 직접 접근하거나, M2M 지역 네트워크를 통해 M2M 게이트웨이에 접근하여 간접적으로 접속 네트워크에 접근한다.

• M2M 지역 네트워크

M2M 디바이스와 M2M 게이트웨이 사이의 연결성을 제공하는 네트워크로써 IEEE 802.15, Zigbee, 블루투스 등의 개인 영역 네트워크(personal area network) 또는 PLC, M-BUS, Wireless M-BUS 및 KNX 등의 지역 네트워크(local network)를 제공한다.

o M2M 게이트웨이

M2M 기능을 사용하여 M2M 디바이스들의 상호작용을 보호하고 M2M 디바이스가 네트워크 도메인의 접속 네트워크에 접근하도록 게이트웨이 역할을 제공한다.

o M2M 네트워크 도메인

M2M 네트워크 도메인은 접속 네트워크, 전송(transport) 네트워크, M2M 코어(core), M2M 애플리케이션, 네트워크 관리 기능, 그리고 M2M 관리 기능으로 구성된다.

• 접속 네트워크

M2M 디바이스 도메인과 M2M 코어의 코어 네트워크가 서로 통신할 수 있도록 네트워크를 제공하는 영역이다. 접속 네트워크를 지원하는 통신 기술로는 xDSL, HFC, PLC, 위성, GERAN, UTRAN, eUTRAN, W-LAN 및 WiMAX 등이 존재한다.

• 전송 네트워크

네트워크 도메인 영역에서 데이터의 전송을 담당한다.

• M2M 코어

코어 네트워크와 서비스 기능으로 구성되어 있다.

- 코어 네트워크 : IP의 연결성, 서비스 및 네트워크 제어 기능, 다른 네트워크와 상호연결, 그리고 로밍(roaming) 기능을 제공한다.
- 서비스 기능 : 다양한 애플리케이션의 기능을 제공하고 개방형 인터페이스를 통해 보다 많은 기능성(functionality)을 제공한다. 따라서 서비스 기능은 애플리케이션 개발을 보다 간략하고 최적화할 수 있도록 도와준다.

• M2M 애플리케이션

서비스 로직을 실행하고 개방형 인터페이스를 통해 서비스 기능을 이용한다.

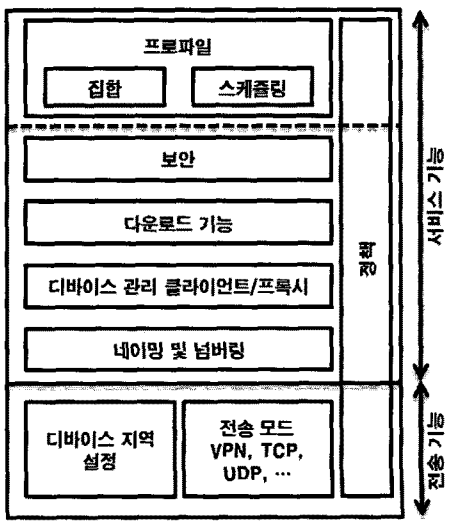
• 네트워크 관리 기능

접속, 전송 및 코어 네트워크를 관리하기 위한 감시, 통제, 오류 관리 등의 기능들로 구성된다.

• M2M 관리 기능

M2M 디바이스 및 게이트웨이, 서비스 기능, M2M 애플리케이션을 관리하기 위한 기능들로 구성된다. 사용자는 M2M 디바이스 설정 또는 사용량을 모니터링하기 위해 웹 또는 특정 애플리케이션을 이용하여 M2M 애플리케이션에 접속함으로써 M2M 서비스를 사용한다.

2.2 M2M 통신 인터페이스



[그림 2] M2M 게이트웨이

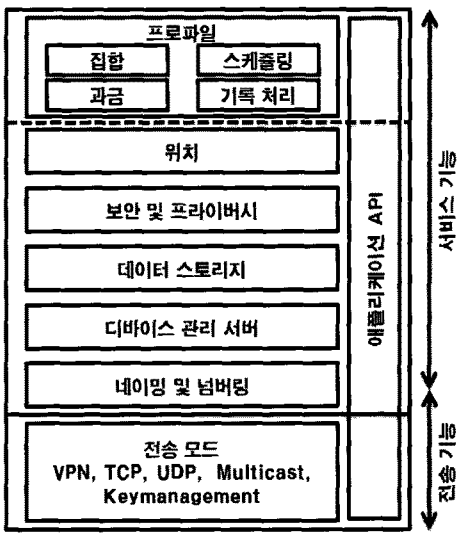
M2M 통신의 논리적 구조인 M2M 디바이스 도메인, M2M 게이트웨이 도메인 그리고 M2M 네트워크 도메인을 통신 기능을 제공하는 물리적 디바이스로 분류하면 M2M 게이트웨이와 M2M 서버로 구분된다. M2M 게이트웨이는 [그림 2]와 같이 나타낼 수 있다.

o M2M 게이트웨이

- M2M 지역 네트워크의 전송 설정 기능 : M2M 디바이스의 통신 모드를 설정하는 기능이다.
- 전송 기능 : M2M 서버와의 통신을 지원하기 위한 기능으로 네트워크 연결, TCP, UDP, VPN 및 터널 설정, 키 교환 및 암호 설정 등의 전송 기능을 지원한다.
- 네이밍 및 넘버링
- 디바이스 관리 클라이언트/프록시 : M2M 디바이스를 관리하기 위한 클라이언트/프록시 기능을 제공한다.
- 보안 : 서비스 기능 및 M2M 애플리케이션에 대한 기능을 제공한다.
- 프로파일 기능 : 데이터 집합, 데이터 전송 스케줄링과 같은 특정 사례의 경우 프로파일을 제공한다.

o M2M 서버

M2M 서버는 [그림 3]과 같이 나타낼 수 있다.



[그림 3] M2M 서버

- 전송 기능 : M2M 게이트웨이와의 통신을 지원하기 위한 기능으로 네트워크 연결, TCP, UDP, VPN 및 터널 설정, 키 교환 및 암호 설정 등의 전송 기능을 지원한다.
- 네이밍 및 넘버링
- 디바이스 관리 서버 : 디바이스 등록 및 설정, 디바이스 진단, 소프트웨어 업그레이드 등의 M2M 디바이스를 관리하기 위한 기능을 제공한다.
- 데이터 저장 : M2M 디바이스로부터 수집한 데이터를 저장하고 애플리케이션에 알맞게 가공한다.
- 보안 및 프라이버시 : 데이터의 기밀성 및 익명성을 제공함으로써 인증 데이터와 연관된 M2M 디바이스의 프라이버시 정보를 보호한다.
- 위치 : 디바이스의 위치 정보를 수집하여 서비스 요청이 있을 경우 M2M 애플리케이션에 알맞게 가공하여 제공한다.
- 프로파일 기능 : 데이터 집합, 데이터 전송 스케줄링, 과금, 데이터 처리 기능과 같은 특정한 경우에 프로파일을 제공한다.

2.3 M2M 통신의 보안 요구사항

M2M 통신은 다양한 통신 기술 및 디바이스를 이용하여 M2M 통신 환경을 구축한다. 하지만 이로 인해 데이터 노출, 데이터 도용, 데이터 불법 변경 및 삭제, 불법적 기기 사용, 개인 프라이버시 노출과 같은 다양한 보안 위협이 존재할 수 있다. 따라서 다양한 보안 위협에 대응하여 보다 안전한 M2M 통신 환경을 제공하기 위해 다음과 같은 보안 요구사항을 만족해야 한다.

• 데이터 기밀성

데이터 기밀성은 고의적이거나 의도하지 않은 불법 노출로부터 정보 또는 콘텐츠를 보호하는 것을 의미한다. M2M 디바이스로부터 수집되는 데이터의 경우, 디바이스의 위치정보나 요금 관련 정보 등 민감한 정보들이 네트워크를 통해 전송되므로 비 인가된 제 3자가 데이터의 내용을 알 수 없도록 암호화 등의 메커니즘을 이용하여 전송되는 정보를 보호해야 한다.

• 데이터 무결성

데이터 무결성은 송신측에서 발송한 메시지가 전송

되는 중에 고의적 또는 실수로 인해 메시지 변경이 일어나지 않았음을 확인하는 것으로 수신한 메시지와 발송한 메시지가 같음을 보장하는 것이다. M2M 통신의 경우 제 3자가 중간자 공격(man-in-the-middle attack)을 이용하여 디바이스와 서버 사이에 전송되는 메시지를 위·변조하는 공격이 가능하다. 따라서 이러한 보안 위협에 대응하기 위해 개체 사이에 전송되는 데이터의 무결성을 보장해야 한다.

• 디바이스 무결성

M2M 디바이스들의 경우 일반적으로 사람 또는 다른 보호 수단에 의해 보호되거나 감시되지 않는 상대적으로 물리적 보안이 취약한 장소에 배치된다. 또한 M2M 디바이스의 비용 감축 및 구현 용이성으로 인해 대부분 개방형 인터페이스를 지닌 플랫폼에서 구현된다. 이러한 취약성으로 인해 공격자는 M2M 디바이스에 악성 소프트웨어를 삽입하거나 M2M 디바이스의 사용 용도를 변경함으로써 네트워크를 오염 시키고 디바이스의 가용성을 침해할 수 있다. 따라서 이와 같은 위협에 대응하기 위해 M2M 디바이스의 하드웨어, 소프트웨어 및 펌웨어에 대한 무결성 검증이 필요하다.

• 시스템 가용성

가용성이란 보안의 대상이 되는 디바이스 또는 컴퓨터 시스템 자원들이 승인된 사용자들에 의해 적시에 사용 가능하도록 하여 생산 또는 업무의 연속성을 저해하지 않음을 보장하는 것을 의미한다. 따라서 사용자 또는 주체가 시스템 자원이나 정보를 요구할 경우에는 항상 접근 및 사용이 가능해야 한다. 하지만 승인된 사용자 또는 주체가 시스템 자원이나 정보에 접근하는 것을 차단하거나, 너무 오랜 접근시간을 요구한다면 시스템의 가용성이 손상된 것으로 생산 또는 업무의 연속성을 훼손하게 된다. 그러므로 M2M 통신 환경에서도 시스템의 가용성을 보장할 수 있는 적절한 보안 메커니즘이 요구된다.

• M2M 디바이스 인증

M2M 통신 환경에서 서버는 M2M 디바이스 또는 게이트웨이로부터 데이터를 수집하기 전에 데이터가 올바르고 정당한 디바이스에서 온 것인지를 검증해야 한다. 이와 같은 M2M 디바이스에 대한 인증을 제공하지 않을 경우, 공격자는 M2M 디바이스를 악의적으로 사용하여 정상적인 사용자의 M2M 서비스 사용을 방해하는 것이 가능하다. 따라서 이러한 보안 위협에 대응하기 위해 M2M 디바이스 인증 절차를 통해 서버는 데이터를 송신한 M2M 디바이스의 정당성을 검증해야 한다.

• M2M 서버 인증

M2M 디바이스 인증과 같이 M2M 디바이스나 게이트웨이는 M2M 서버에게 데이터를 송신하기 전에 통신하는 서버의 정당성을 검증해야 한다. M2M 서버에 대한 인증이 제공되지 않는 경우 공격자가 정당한 서버로 위장하여 정당한 디바이스들이 보내는 메시지를 수집함으로써 M2M 디바이스의 위치를 추적하거나 다른 프라이버시 관련 문제를 발생시킬 수 있다. 따라서 M2M 디바이스는 M2M 서버에게 메시지를 보내기 전에 정당한 M2M 서버인지 확인할 수 있는 안전한 인증 절차가 요구된다.

• 접근제어 및 인가

M2M 시스템은 부적절한 접근 및 인가 권한을 초과하는 애플리케이션 및 사용자의 행위를 방어하기 위한 접근제어 및 인가 메커니즘을 통해 보다 안전한 M2M 서비스를 제공할 수 있다.

• 네트워크 오용 방지

M2M 디바이스는 일반적인 전자제품과는 다르게 M2M 디바이스 소유자와 M2M 디바이스 사용자가 다를 수 있으며 이는 상대적으로 물리적 보안이 취약한 위치에 배치될 수 있음을 의미한다. 대표적인 예로 스마트 미터기의 경우 전력 사업자가 디바이스의 소유자이지만 스마트 미터기는 전력 사용자의 가정이나 사무실에 배치된다. 이로 인해 스마트 미터기들은 다른 디바이스 보다 상대적으로 도난의 위협에 쉽게 노출된다. 또한 공격자는 불법적으로 획득한 M2M 통신 모듈을 사용함으로써 허가권 없이 네트워크에 접속할 수 있게 된다. 이와 같이 고의적 또는 실수로 인한 M2M 통신 모듈의 불법적 사용으로 인해 M2M 통신 네트워크를 오염시킬 가능성 있다. 따라서 M2M 통신 모듈의 불법적 사용 및 통신 네트워크의 오염을 방어하기 위해 네트워크 오용 방지를 위한 M2M 보안 솔루

션이 요구된다.

• 프라이버시 보호

이동성을 제공하는 M2M 디바이스가 M2M 통신에 참여하기 위해 자신의 디바이스 식별자를 서버에게 전송할 경우, 공격자는 M2M 디바이스의 식별자를 수집함으로써 M2M 디바이스 또는 소유자의 위치 정보를 획득할 가능성이 있다. 또한 위치 정보를 통해 사용자 프라이버시와 관련된 정보를 추가적으로 획득할 수 있게 된다[1][8]. 따라서 M2M 디바이스의 위치 정보가 민감하게 사용되는 M2M 통신 환경에서는 통신에 참여하는 M2M 디바이스의 익명성 보장과 같은 프라이버시 보호가 요구된다.

• 추적성 방지

이동성을 제공하는 M2M 디바이스 경우 동일한 M2M 디바이스 식별자를 반복적으로 사용한다면 공격자는 보다 쉽게 M2M 디바이스나 이를 소유한 사용자의 위치 및 이동 경로를 추적하는 것이 가능하다. 따라서 M2M 디바이스의 이동성을 보장하면서 M2M 디바이스 및 소유자의 위치를 추적하는 것이 불가능하도록 적절한 보안 메커니즘을 적용해야한다.

• 부인 방지

M2M 통신 환경에서 메시지를 수신하고도 메시지가 전달된 사실이 없다고 수신측에서 주장하는 것을 방지하고 또는 역으로 메시지를 전송하지 않고도 메시지 전달을 주장하는 송신자 측의 부인을 방지하기 위해 서로간의 송수신 사실을 증명할 수 있는 부인방지 메커니즘이 요구된다.

III. 제안하는 상호 인증 프로토콜

본 장에서는 M2M 통신의 보안 요구사항을 M2M 통신 아키텍처에 적용시킴으로써 보다 안전한 M2M 통신 아키텍처를 제안한다. 또한 이러한 통신 아키텍처에 적용할 수 있는 M2M 디바이스 및 게이트웨이 도메인과 M2M 네트워크 도메인 사이의 상호 인증 및 키 교환을 제공하는 프로토콜을 제안한다.

3.1 보안 요구사항을 적용시킨 M2M 통신 아키텍처

보다 안전한 M2M 통신 환경을 제공하기 위해 M2M 통신 환경에서 만족해야 하는 보안 요구사항을 M2M 통신 아키텍처에 적용시킴으로써, M2M 통신 환경에 존재할 수 있는 다양한 보안 위협들로부터 안전한 통신 환경을 제공할 수 있다. 제안하는 M2M 통신 아키텍처는 [그림 4]와 같다. [그림 4]의 각 구성요소에서 제공해야 하는 보안 기능에 대한 자세한 설명은 다음과 같다.

① M2M 디바이스 보안

M2M 디바이스는 데이터 기밀성, 데이터 무결성, 디바이스 무결성, M2M 서버 인증, 접근제어 및 인가, 네트워크 오용 방지, 프라이버시, 추적성 및 부인방지에 대한 보안 요구사항을 만족해야 한다.

② M2M 게이트웨이 보안

M2M 게이트웨이는 데이터 기밀성, 데이터 무결성, 시스템 가용성, M2M 디바이스 인증, M2M 서버 인증에 대한 보안 요구사항을 만족해야 한다.

③ 접속 네트워크 보안

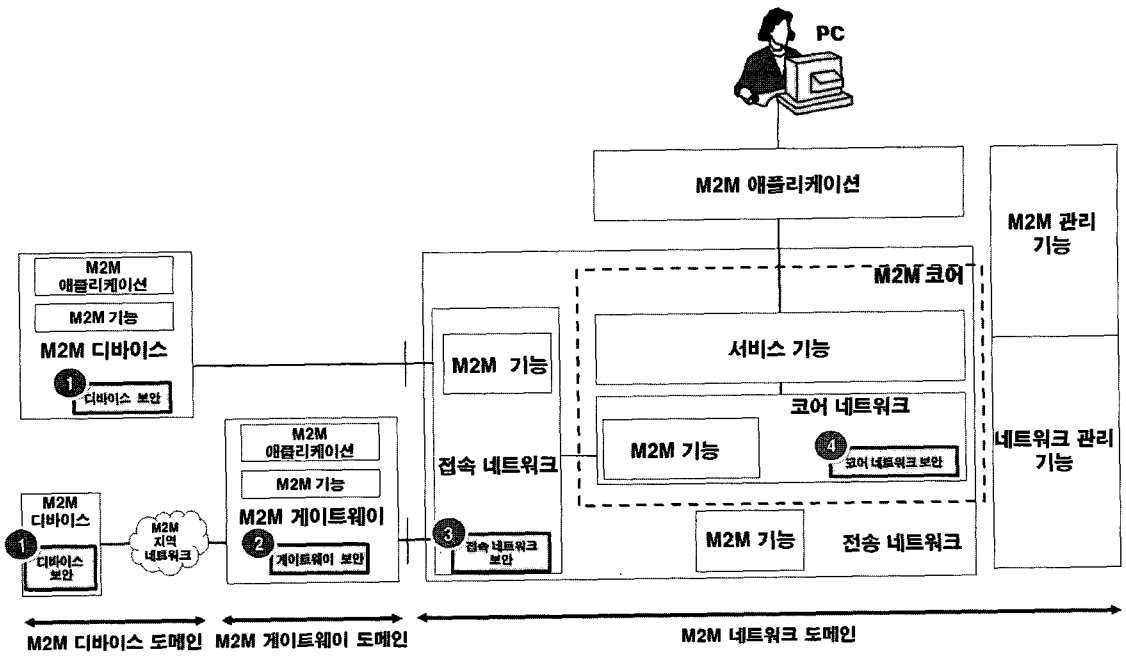
접속 네트워크는 데이터 기밀성, 데이터 무결성, 디바이스 인증에 대한 보안 요구사항을 만족해야 한다.

④ 코어 네트워크 보안

코어 네트워크는 접근제어 및 인가에 대한 보안 요구사항을 만족해야 한다.

3.2 상호인증 및 키 교환 프로토콜

본 논문에서 제안하는 프로토콜은 M2M 디바이스 및 게이트웨이 도메인과 M2M 네트워크 도메인 사이의 안전한 상호인증 및 키 교환을 제공한다. 본 논문에서는 M2M 디바이스 및 게이트웨이 도메인을 디바이스 표기하고 M2M 네트워크 도메인을 서버라 표기하여 기술한다. 제안하는 프로토콜은 사전 단계와 상호인증 및 키 교환 단계로 구성되며, 사전 단계는 상호인증 및 키 교환 단계에서 필요로 하는 파라미터를 공유하는 단계이다. 그리고 상호인증 및 키 교환 단계는 실질적으로 인증을 수행하는 단계로 임시 세션키를



〔그림 4〕 보안 요구사항을 적용시킨 M2M 통신 아키텍처

이용하여 디바이스 및 서버의 정당성을 확인한 후, 새로운 세션키를 설립한다[8].

3.2.1 가정 사항

제안하는 프로토콜에서는 디바이스는 이동성을 제공하지 않으며 항상 서버와 통신이 가능한 영역 내에 존재한다고 가정한다. 또한 디바이스 및 서버의 저장 장치는 신뢰기반의 컴퓨팅(trusted computing)을 기반으로 하여 부채널 공격 등의 물리적 공격에 대해 안전하다.

〔표 1〕 표기법

표기	의미
$I_{d/s}$	디바이스/서버의 식별자
PW_d	디바이스의 패스워드
T_d	디바이스의 타임스탬프
p	1024 bit 이상의 큰 소수
g	Z_p상의 원시원소
x_s	서버의 고정된 비밀키, $\gcd(x_s, p-1)=1$
y_s	서버의 고정된 공개키, $y_s \equiv g^{x_s} \bmod p$
r_d	디바이스의 랜덤수
PSK	상호인증 과정에서 메시지 암호화를 위해 사용하는 임시 세션키
SK	디바이스와 서버 사이의 세션키
$H(a)$	메시지 a의 해쉬 값
$\{a\}_{sk}$	대칭키 SK를 이용한 메시지 a의 암호화

3.2.2 표기법

제안하는 프로토콜에서 사용하는 표기와 의미는 〔표 1〕과 같다.

3.2.3 사전단계

상호 인증 및 키 교환을 수행하기 전에 사전 단계에서 디바이스 D는 자신의 식별자 I_d와 패스워드 PW_d를 서버에게 안전하게 전송한다. 서버 S는 자신의 고정된 공개키 $y_s \equiv g^{x_s} \bmod p$를 계산하여 디바이스 D에게 전송한다. 이러한 과정은 실제로 메시지 교환을 통해 이루어지기 보다는 디바이스를 배치하는 과정에서 디바이스 D와 서버 S에 각각의 파라미터들을 삽입하여 배치하는 방식이 적합하다. 또한 서버 S는 자신의 비밀키에 대한 역원 x_s^{-1} 값을 미리 계산하여 저장함으로써 프로토콜에 대한 계산의 효율성을 높일

수 있다.

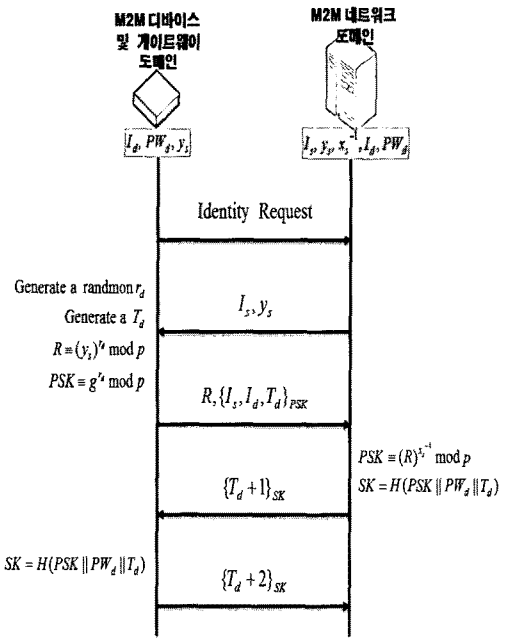
디바이스 D와 서버 S가 초기에 유지하는 정보는 다음과 같다.

- 디바이스 D : 디바이스 D의 식별자 I_d, 디바이스 D의 패스워드 PW_d, 서버 S의 공개키 $y_s \equiv g^x \bmod p$
- 서버 S : 서버 S의 식별자 I_s, 서버 S의 공개키 $y_s \equiv g^x \bmod p$, 서버 S의 비밀키에 대한 역원 x_s^{-1}, 디바이스 D의 식별자 I_d, 디바이스 D의 패스워드 PW_d

3.2.4 상호인증 및 키 교환 단계

사전 단계를 통해 각각의 파라미터를 나누어 갖은 디바이스 D와 서버 S는 다음의 과정을 통해 서로를 인증하고 보안통신을 위한 세션키 SK를 설립한다. 디바이스 D와 서버 S 사이에 상호 인증 및 키 교환 과정은 다음과 같다.

〔그림 5〕는 제안하는 프로토콜의 상호인증 및 키 교환 단계를 나타낸 것이다.



〔그림 5〕 제안하는 상호인증 및 키 교환 프로토콜

- 단계 1. 디바이스 D는 네트워크에 참여하기 위해 서버 S에게 식별자를 요청한다.
- 단계 2. 서버 S는 디바이스 D에게 자신의 식별자 I_s와 공개키 y_s를 전송한다.
- 단계 3. 디바이스 D는 랜덤수 r_d를 선택하고 서버 S의 공개키 y_s을 이용하여 $R \equiv y_s^{r_d} \bmod p$을 계산한다[9]. 그리고 타임스탬프 T_d을 생성하고 임시 세션키 $PSK \equiv g^{r_d} \bmod p$를 계산한 후, 임시 세션키 PSK을 이용하여 서버 S의 식별자 I_S, 자신의 식별자 I_d, 타임스탬프 T_d을 암호화하여 서버 S에게 전송한다.
- 단계 4. 서버 S는 전송받은 R과 자신의 비밀키에 대한 역원 x_s^{-1}을 이용하여 임시 세션키 $PSK \equiv R^{x_s^{-1}} \equiv g^{x_s \cdot r_d \cdot x_s^{-1}} \equiv g^{r_d} \bmod p$를 계산한다.
- 단계 5. 서버 S는 임시 세션키 PSK를 이용하여 서버 S의 식별자 I_S, 디바이스 D의 식별자 I_d, 타임스탬프 T_d을 복호한다. 그리고 디바이스 D의 식별자 I_d에 대응되는 패스워드 PW_d을 검색한 후에 임시 세션키 PSK, 디바이스 D의 패스워드 PW_d 그리고 타임스탬프를 연접하여 해쉬함으로써 세션키 $SK = H(PSK \| PW_d \| T_d)$을 생성한다.
- 단계 6. 서버 S는 생성한 세션키 SK을 이용하여 타임스탬프 T_d에 1을 더한 값을 암호화 시켜 전송한다.
- 단계 7. 디바이스 D는 임시 세션키 PSK, 자신의 패스워드 PW_d, 그리고 타임스탬프 T_d을 연접하여 해쉬함으로써 세션키 SK을 생성하고 $\{T_d+1\}_{SK}$을 복호함으로써 묵시적으로 서버의 비밀키에 대한 역원 x_s^{-1}을 가진 정당한 서버임을 확인한다.
- 단계 8. 디바이스 D는 서버 S와 동일한 세션키 SK 설립을 알리기 위해 타임스탬프 T_d에 2를 더한 후 세션키 SK로 암호화하여 서버 S에게 전송한다.
- 단계 9. 서버 S는 세션키 SK를 이용하여 메시지 $\{T_d+2\}_{SK}$을 복호하고 T_d+2 값을 확인함으로써 디바이스 D가 자신과 동일한 세션키 SK를 설립하였음을 확인하고 동시에 올바른 패스워드 PW_d을 가진 정당한 디바이스 D임을 인증한다.

IV. 안전성 분석

본 장에서는 제안하는 프로토콜의 안전성을 분석하기 위해 다양한 공격 모델을 정의하고, 제안하는 프로토콜이 정의한 공격 모델에 대해 안전하고 앞에서 기

술한 보안 요구사항을 만족한다는 것을 세부적으로 설명한다.

• 재사용 공격(replay attack)

재사용 공격은 공격자가 디바이스 또는 서버가 전송하는 데이터를 네트워크 중간에서 도청하여 수집함으로써, 이후 세션에서 수집된 메시지를 재사용하여 인증을 통과하는 방법이다. 제안하는 프로토콜에서 네트워크를 통해 수집되는 메시지들의 경우, 서버의 식별자 I_s와 공개키 y_s를 제외한 모든 메시지가 임시 세션키 PSK 또는 세션키 SK로 암호화 되어 전송된다. 이는 디바이스 D에서 생성한 랜덤수 r_d에 기반하여 임시 세션키 PSK와 세션키 SK가 생성됨으로 매 세션마다 다른 임시 세션키 PSK와 세션키 SK가 생성되고 따라서 전송되는 메시지 역시 매 세션마다 다르게 생성된다. 그러므로 제안하는 프로토콜에서는 이전 세션에 수집한 메시지를 다음 세션에 사용하는 경우에는 인증을 통과할 수 없으므로 재사용 공격에 대해 안전하다.

• 위장 공격(impersonation attack)

위장 공격은 공격자가 정당한 디바이스 또는 서버로 위장함으로써 정당한 개체를 속이거나 세션키를 설립하는 공격이다. 제안하는 프로토콜에서는 공격자가 서버로 위장하더라도 정당한 서버의 비밀키에 대한 역원값 x_s^{-1}을 알지 못하므로 올바른 임시 세션키 $PSK \equiv (R)^{x_s^{-1}} \bmod p$를 생성할 수 없다. 또한 공격자가 디바이스로 위장할 경우 정당한 디바이스의 패스워드 PW_d를 알 수 없으므로 서버와 동일한 세션키 SK을 생성할 수 없다. 이와 같이 공격자가 디바이스 D나 서버 S로 위장하더라도 제대로 된 임시 세션키 PSK 또는 세션키 SK를 설립할 수 없으므로 상호인증 및 키 교환 단계를 통과하지 못하게 된다. 따라서 제안하는 프로토콜은 위장 공격에 대해 안전하다.

• 상호 인증 및 키 교환

제안하는 프로토콜에서는 단계 7에서 디바이스 D는 임시 세션키 PSK, 자신의 패스워드 PW_d 그리고 타임스탬프 T_d을 연접하여 해쉬함으로써 세션키 SK을 생성한다. 생성한 세션키 SK를 이용하여 서버에게 받은 $\{T_d+1\}_{SK}$을 복호하고 T_d가 자신이 생성한 타임스탬프인지를 확인함으로써 정당한 서버인지를 확인하게 된다. 이는 정당한 서버만이 서버 S의 비밀키에 대한 역원 x_s^{-1}을 가지고 있고 올바른 임시 세션키 $PSK \equiv R^{x_s^{-1}} \equiv g^{x_s \cdot r_d \cdot x_s^{-1}} \equiv g^{r_d} \bmod p$와 세션키 $SK = H(PSK \| PW_d \| T_d)$를 생성할 수 있기 때문이다. 따라서 디바이스 D는 단계 7에서 묵시적으로 서버 S의 비밀키에 대한 역원 x_s^{-1}를 가진 정당한 서버임을 인증한다. 그리고 단계 9에서는 서버 S가 세션키 SK를 이용하여 디바이스 D에서 전송된 메시지 $\{T_d+2\}_{SK}$을 복호한 후, T_d+2를 검증함으로써 디바이스 D가 자신과 동일한 세션키 SK를 설립했고 정당한 디바이스 D임을 인증하게 된다. 이는 디바이스가 올바른 디바이스 D의 패스워드 PW_d을 가지고 있음으로 자신과 동일한 세션키 $SK = H(PSK \| PW_d \| T_d)$를 설립했음을 확인할 수 있다. 따라서 서버 S는 단계 9에서 디바이스 D가 올바른 패스워드 PW_d를 가진 정당한 디바이스임을 인증하고 동일한 세션키 SK 교환을 확인한다.

• 프라이버시 및 추적성 보호

제안하는 프로토콜에서는 프라이버시 보호를 위해 단계 3에서 디바이스 S의 식별자를 바로 전송하지 않고 임시 세션키 PSK로 암호화하여 전송함으로써 디바이스의 익명성을 제공한다. 또한 임시 세션키 PSK는 디바이스에서 생성하는 랜덤수 r_d로 인해 매 세션마다 새롭게 계산되므로 서버 S에게 전송하는 메시지 $\{I_s, I_d, T_d\}_{PSK}$ 역시 매 세션 새롭게 변경되고 이는 디바이스에 대한 추적성을 보호하게 된다.

따라서 제안하는 프로토콜에서는 프라이버시 및 추적성 보호를 제공한다.

V. 결 론

디바이스 간의 무선 통신을 의미하는 M2M 통신은 디바이스의 통신 모듈이 점차 소형화되고 다양한 통신 기술들이 생겨남에 따라 전 세계적으로 주목받는 기술로서 성장하게 되었다. 따라서 최근 들어 스마트 그리드와 같은 M2M 기술을 이용한 다양한 응용 분야가 생겨나고 있다. 그러나 다양한 통신 기술을 수용하고 사용자의 제어가 요구되지 않는 M2M 통신 환경의 특징으로 인해 M2M 통신을 위협하는 다양한 보안 위협이 꾸준히 증가하고 있다.

본 논문에서는 M2M 통신 아키텍처와 M2M 통신 환경에서 고려해야 하는 보안 요구사항을 분석함으로써 보다 안전한 M2M 통신 아키텍처를 제안하였다. 또한 M2M 통신 환경에서 디바이스간의 신뢰성을 제공하기 위해 M2M 디바이스 및 게이트웨이 도메인과 M2M 네트워크 도메인 사이의 상호인증 및 키 교환을 제공하는 프로토콜을 제안하였다. 제안하는 상호인증 및 키 교환 프로토콜은 재사용 공격, 위장 공격에 대해 안전하고 프라이버시 및 추적성을 보호할 수 있다는 장점이 있다.

본 논문에서 제안하는 프로토콜은 보다 안전한 M2M 통신 환경을 구축하기 위해 필수적으로 요구되는 보안 메커니즘으로 활용할 수 있으며, 다양한 M2M 응용 분야에 보다 향상된 안전성을 제공할 수 있을 것으로 기대한다.

참 고 문 헌

[1] ETSI, "ETSI TS 102 689 v 0.1.1 Machine-to-Machine communications(M2M); M2M service requirement," 2009.

[2] ETSI, "ETSI TR v 0.0.9 Machine-to-Machine communications(M2M); Smart Metering Use Cases," 2009.

[3] G. Lawton, "Machine-to-Machine technology gears up for growth," IEEE Computer Society, Sep. 2004.

[4] A. Aziz and W. Diffie, "A secure communications protocol to prevent unauthorized access, privacy and authentication for wireless local area networks," IEEE Personal Communications, vol. 1, no. 1, pp. 25-31, 1994.

[5] Y. Jiang, C. Lin, X. Shen, and M. shi, "Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks," IEEE Transactions on wireless communications, vol. 5, no. 9, pp. 2569-2577, Sep. 2006.

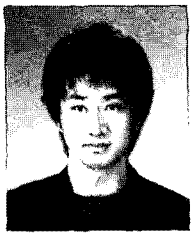
[6] 조영섭, 조상래, 유인태, 진승헌, 정교일, "유비쿼터스 컴퓨팅과 보안요구사항 분석," 정보보호학회지, 14(1), pp. 21-34, 2004년 2월.

[7] ETSI, "ETSI TS 102 690 v 0.06Machine-to-Machine communications(M2M); Functional architecture," 2009.

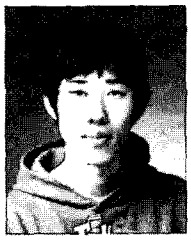
[8] K. Mangipudi, R. Katti, and H. Fu, "Authentication and Key agreement Protocols *Preserving Anonymity*," *International* Journal of Network Security, vol. 3, no. 3, pp. 259-270, Nov. 2006.

[9] W. Diffie and M.E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.

〈著者紹介〉



은 선 기 (Sun-Ki Eun) 학생회원
2008년 8월: 호서대학교 정보보호학과 졸업(공학사)
2009년 2월~현재: 호서대학교 정보보호학과 석사과정
〈관심분야〉 네트워크 보안, 보안 프로토콜, 시스템 평가 및 인증



전 서 관 (Seo-Kwan Jeon) 학생회원
2008년 2월: 호서대학교 정보보호학과 졸업(공학사)
2008년 3월~현재: 호서대학교 정보보호학과 석사과정
〈관심분야〉 암호학, 네트워크 보안, 보안 프로토콜

안 재 영 (Jae-Young Ahn)
1986년 1월: 성균관대학교 공과대학 전기공학과 졸업(공학사)
1997년 8월: 성균관대학교 공과대학 정보공학과 석사(공학석사)
2001년 8월: 성균관대학교 공과대학 정보공학과 박사(공학박사)
1986년 1월~현재: 한국전자통신연구원 표준연구센터 전문위원
2006년 9월~현재: 국내 ITU-T 연구위원회 SG2 분과 부위원장
〈관심분야〉 NGN/BcN, 식별체계

오 수 현 (Soo-Hyun Oh) 종신회원
1998년 2월: 성균관대학교 정보공학과 졸업(공학사)
2000년 2월: 성균관대학교 전기전자 및 컴퓨터공학과 석사(공학석사)
2003년 8월: 성균관대학교 전기전자 및 컴퓨터공학과 박사(공학박사)
2004년 3월~현재: 호서대학교 정보보호학과 교수
〈관심분야〉 암호학, 네트워크 보안 프로토콜