Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.7.779

공장 및 생산 자동화에 있어 안드로이드 기반의 보안성이 강화된 모바일장비관리시스템 구현

유흥식* · 선기현** · 김성운***

In the Automation Environment of Factory and Production, the Implementation of Security-enhanced Mobile Device Management System using Android-based Smart Phones

Hyung-Cik Yu* · Ki-Hyun Seon** · Sung-Un Kim***

요 약

안드로이드 기반의 스마트폰을 공장자동화 및 생산자동화 분야에서의 활용이 중요하게 여겨지고 있다. 일반적으로 OMA DM 표준은 공장자동화 및 생산자동화 환경을 위한 중요한 인프라 구조 기술이다. 본 논문에서는 OMA DM 플랫폼 설계 및 구현에 대해 연구한다. 개발된 프로토타입은 세 가지 모듈 즉 DMS, FUMO 그리고 SCOMO로 구성된다. 그리고 EAP 및 AES 개념을 응용한 보안 모듈도 제시되었다. 제안된 보안 모듈은 공장자동화를 위해 안드로이드 기반의 스마트폰을 활용한 DMS, FUMO 및 SCOMO 모듈 간 통신에서 안전한 통신을 보장하기 위해 적용된다. 시뮬레이션 결과에 의하면 구현된 해당 프로토타입은 공장자동화 환경에서 좋은 성능을 보이며 보안성을 보장하면서 여러 공장자동화, 생산자동화 및 사무자동화 환경에서 활용이 가능하다.

ABSTRACT

Utilizing smart phones based on android applications in the field of FA(Factory Automation) or PA(Production Automation) is being deployed actively. In general, MDM(Mobile Device Management) is a crucial infra-structure to build such a FA or PA environment. In this paper, we suggest an open mobile device management platform and implement its prototype. The developed prototype consists of three modules such as DMS(Device Management Server), FUMO(Firmware Update Management Object) and SCOMO(Software Component Management Object). In addition, we suggest a security module based on the concept of the EAP (Extensible Authentication Protocol) and the AES (Advanced Encryption Standard). The suggested security module's prototype is applied to guarantee the data integrity in the process of communicating among DMS, FUMO and SCOMO for the purpose of utilizing smart phones based on android applications in a FA field. We also evaluate the performance of the implemented security prototype. According to our simulation results, the implemented prototype has a good performance in a FA environment and can be utilized in the other FA, PA or OA(Office Automation) environment with guaranteeing the security.

키워드

OMA DM, MDM System, FUMO Server, SCOMO Server, OMA DM Security
모바일 장비관리시스템, FUMO 서버, SCOMO 서버, OMA DM 보안, 무선 보안

* 부경대학교 정보통신공학과 박사과정수료(paul.yu@unomic.com)
** 부경대학교 정보통신공학과 석사(white8768@pknu.ac.kr)
*** 교신저자(corresponding author)부경대학교 정보통신공학과 교수(kimsu@pknu.ac.kr)
접수일자 : 2014. 05. 26 심사(수정)일자 : 2014. 06. 23 게재확정일자 : 2014. 07. 11

Ⅰ. 서 론

각종 분석에 의하면 스마트폰 기술의 기하급수적인 보급으로 여러 가지 산업 분야 생산과정에서 직원 한 명이 평균 5.1대의 해당 기기를 사용하고 있으며, 기기 당 평균 47개의 서비스가 응용되어 생산 현장에서 활용되고 있다. 특히 이러한 응용들의 관리를 위해 안드로이드 기반 모바일장비관리시스템(MDM : Mobile Device Management) 개발과 사용되는 스마트폰 앱 및 해당 펌웨어 서비스에 있어 보안 문제가 매우 중요한 기술로 부상되었다.

이러한 중요성을 고려하여 국내외에서는 다양한 기술을 개발하고 있으나 공장자동화나 생산자동화 부문에 효과적으로 활용되는 모바일장비관리시스템 개발 및 보안 모듈 구현은 부족한 현실이다[1-2].

현재 모바일장비관리시스템 산업은 MDM 시장에서 MAM(Mobile Application Management) 시장으로 급속히 진화되어가는 과정으로 경쟁력 있는 공장자동화 및 생산자동화 과정에서 효율적인 모바일 단말기의 활용과 응용 적용 과정에서의 보안 문제는 더욱더 중요한 기술로 인식되고 있다. 특히 국내의 경우 이러한 용도로 응용되는 모바일 단말기 관련 보안 기술들은 안랩과 같은 특정회사에서 주도적인 역할을 담당하고 있지만 공장 및 생산 자동화를 위한 MDM 혹은 MAM 등과 연계하는 기술에서는 미흡한 실정이다. 더군다나 해당 모바일 앱 관련 보안 문제는 OMA 표준에서 규정하고 있는 MD5(Message-Digest algorithm 5)에 기반을 둔 보안모듈은 이미 90년대 후반 그 취약성이 확인되었고 실용적인 부분에서도 적용대상이 모바일 단말이라는 특성으로 인해 문제점을 안고 있어 상호운용성과 관계된 애플리케이션 위·변조 예방 및 메시지 보안등의 핵심 기술 에 대한 접근 없이 기존 보유 기능 위주의 플랫폼 구축으로 근본적인 MDM/MAM 보안 핵심 기술에 대한 대비책이 부족한 현실이다[1-2].

본 연구는 OMA DM(Open Mobile Alliance Device Management) 표준에 기반한 FOTA(Firmware over-the-air) 기능적 특성을 고려한 모바일 단말관리를 위한 DM(Device Management) 서버기능과 펌웨어 관리를 위한 FUMO(Firmware Update Management Object)와 소프트웨어 및 관련 콘텐츠까지 관리하는 SCOMO(Software Component Management Object)를 설계 및 구현한다. 이 과정에서 서버와 단말 간 통신에 활용되는 무선 통신 구간 보안성을 기존의 OMA DM 표준 기반에서 응용되어지는 보안 모듈인 OMA DM 보안 기술보다 강화된 형태로 구현한다. 기존의 OMA DM 보안기술은 무선 환경에서 외부로부터의 공격에 대해 한계가 존재하고, 이러한 한계를 분석하여 뛰어난 보안성을 보장하기 위해 본 연구에서는 상호인증서 기반의 EAP(Extensible Authentication Protocol) 인증방식과 128비트 이상의 긴 비밀 키를 활용하는 암호화 알고리즘인 AES (Advanced Encryption Standard) 알고리즘[3]을 각각 적용하여 FUMO 또는 SCOMO 동작에서 서버와 단말 간에 활용되는 무선 통신 구간의 무결성을 보장하여 보안성(Open Mobile Alliance, “OMA Device Management Security, Approved Version 1.2.1”)을 강화한다.

Ⅱ. 연구개발 내용

2.1 모바일장비관리시스템 전체 구조

본 연구의 개발 목표 시스템은 서버-클라이언트로 구분되며 서버에 해당하는 FMS(Factory Management System)과 DMS(Device Management Server)로 구성되며, 클라이언트 구성은 DM Client와 FUMO, SCOMO Agent로 구성되며, 그 내용(Open Mobile Alliance, “OMA Device Management Protocol, Approved Version 1.2.1”)은 그림 1과 같다.

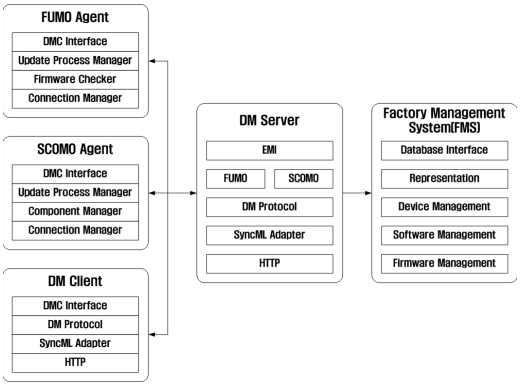


그림 1. 개발 목표시스템 구조도
Fig. 1 Target system for development

FMS는 공장자동화시스템의 소프트웨어 버전 정보를 저장하고 업데이트 발생시 이를 DMS로 알려 처리할 수 있도록 한다. DMS에는 펌웨어 관리를 위해, FUMO 모듈이 단말과 통신을 통해서 해당 기기의 펌웨어 업데이트를 관리하며, SCOMO 모듈은 모바일 앱의 버전관리 및 파라미터에 의한 내부 기능 제어와 콘텐츠 관리(Open Mobile Alliance, “OMA Device Management Protocol, Approved Version 1.2.1”)를 담당한다.

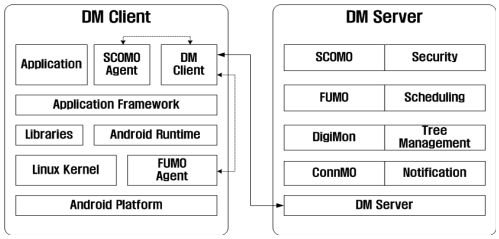


그림 2. DM 서버-클라이언트 구성도
Fig. 2 DM server-client configuration

그림 2는 DMS와 DMC(DM Client) 구성도이다. DMC의 경우 안드로이드 환경기반의 단말장치에서 구성되는 소프트웨어 구조로 DMS로부터 DMC가 제어명령을 수신후 SCOMO 혹은 FUMO Agent로 해당 명령을 전달한다. 이때 FUMO Agent는 운영체제 업데이트를 위해 커널과 동일한 시스템 영역에 구성한다.

2.2 OMA DM 구현

OMA DM 표준 규격의 구성은 DM Protocol, Representation(표현 계층) 및 Security(보안)과 같이 분류되며, 그림 3의 점선으로 표시된 부분이 OMA DM 기본규격(Open Mobile Alliance, “OMA Device Management Protocol, Approved Version 1.2.1”)이다.

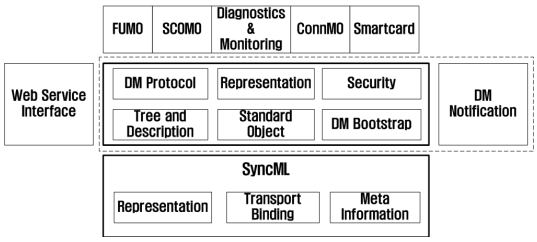


그림 3. OMA DM 표준 규격 구조
Fig. 3 Structure of OMA DM standard

Web Service Interface(웹 서비스 인터페이스), FUMO, SCOMO 등은 부가규격으로 정의된다. OMA DM에서는 플랫폼 독립적인 데이터 동기화 표준규격으로 이용되는 SyncML (Synchronization Markup Language) 전체 표준 규격 중에서 표현계층(Presentation layer), 전송바인딩(Transport Binding) 및 메타정보(Meta Information)만 사용되고 이를 SyncML 공통규격(Open Mobile Alliance, “SyncML Device Management Security”)으로 정의한다.

본 연구에서는 SyncML 공통규격 및 OMA DM 기본규격을 설계 구현하였으며, 부가기능 중에서 FUMO 및 SCOMO 기능, 웹 인터페이스 규격(Open Mobile Alliance, “SyncML Device Management Security”)을 구현하였다.

그림 4는 DM MO(Management Object, 관리객체) 구조를 설명한 것이다. DM 서버로부터 모바일단말기기를 제어하기 위해서 MO를 이용하여 모바일기기 내부의 DM 클라이언트로 관리 정보를 전송한다. 이때 DM 인터페이스는 DM 프로토콜을 이용해서, 응용 MO(Open Movile Alliance, “SyncML DM Standardized Objects, Version 1.1.2”)를 DM 클라이언트로 전송하게 된다. DM 클라이언트는 수신된 MO를 기반으로 모바일기기 내부 자원을 제어할 수 있도록 단말플랫폼이 지원하는 기능을 기반으로 인터페이스를 정의하고 구현하였다. 본 연구에서는 안드로이드 플랫폼 기반으로 한다.

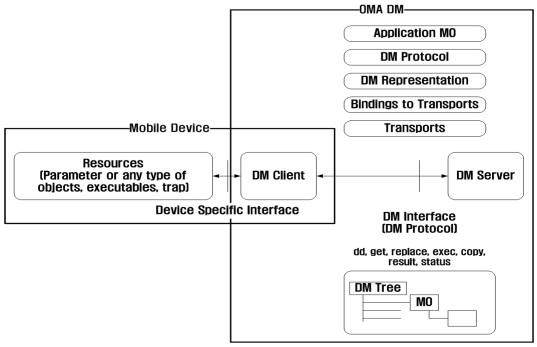


그림 4. DM MO 구조
Fig. 4 DM MO configuration

OMA DM 서버에서 처리하는 내용은 크게 세 가지로 구분할 수 있다. 첫 째로 현재 사용 중인 단말을

체크하는 기능으로, 단말 동작 시 등록 키(Key) 값을 받거나 Heartbit 메시지를 받을 때 접속 데이터 및 Key 데이터를 저장하여, GCM(Google Cloud Messaging) 메시지를 보내거나 웹을 통해 관리자 페이지에서 상태정보를 관리하기 위해서 사용된다.

둘째로 배포명령의 기능을 가진다. 배포명령에서 배포는 일반 배포와 테스트 배포로 구분하고, 일반 배포는 SCOMO에서 필요로 하는 소프트웨어 배포와 FUMO 기능지원을 위한 펌웨어 배포로 구분된다. 앱과 펌웨어는 같은 동작하기 때문에 크게 구분할 필요는 없고, 일반 배포와 테스트 배포는 배포 방식에서 차이를 가진다. 테스트 배포는 스케줄 정보가 없는데 반해 일반 배포는 배포 시작시간과 종료시간을 설정하여 지정된 시간에만 푸쉬(Push) 메시지를 전송할 수 있다. 그리고 일반 배포명령은 중간에 배포 중지명령이 내려질 수도 있기 때문에 배포를 시작하기 전에 배포 상태를 체크한 후 동작을 취한다.

셋째로 관리(Management) 명령을 수행한다. 관리 명령으로는 Lock, Unlock, Wipe 및 DMA 삭제가 포함되며, 관리 명령은 배포와는 다르게 하나의 단말에만 명령 전달이 가능하면 되므로 관리자 페이지에서의 데이터 확인과정 없이 바로 작업 등록 후 메시지(Open Movile Alliance, “SyncML DM Standardized Objects, Version 1.1.2”)를 전달한다.

2.3 OMA FUMO 구현

FUMO 서비스는 단말기기의 펌웨어 업그레이드를 위해 사용되는 OMA 규격으로 DM 서버가 클라이언트로 메시지 및 명령 수행을 진행할 수 있도록 구성하며, FUMO 에이전트는 단말에 내장된 펌웨어의 버전 관리를 위해서 DM 클라이언트와 정보 교환 및 명령 전달기능을 담당하게 된다. 그림 5에서 보는 바와 같이 DM 서버는 EMI(External Management Infrastructure)와 DMWSI(Device Management Web Service Interface)를 통해서 펌웨어 업그레이드가 필요한 단말 및 버전 정보(Open Mobile Alliance, “SyncML Representation Protocol, version 1.0.1”)를 DM 단말에 전송하게 된다. DM 서버는 푸쉬 초기화를 통해서 DM 클라이언트와 통신을 준비하고 클라이언트는 Device Information Exchange 단계에서 현재 펌웨어 버전과 단말 정보를 서버로 전송한다.

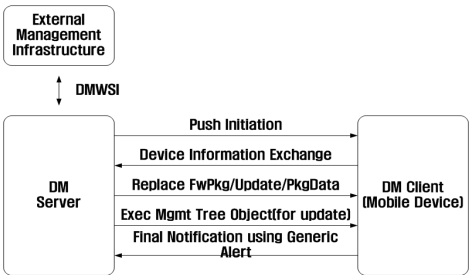


그림 5. FUMO 서버-클라이언트 메시지 프로세스
Fig. 5 Message process for FUMO server-client

이때 서버에서는 EMI로부터 수신된 버전정보와 비교해서 업데이트가 필요하다고 판단되면 Replace 명령을 통해서 펌웨어 업데이트를 수행하도록 한다. 수행완료시 DM 클라이언트는 Generic Alert을 통해서 완료를 서버로 통보하게 된다.

본 연구에서 구현한 OMA DM 기반의 FUMO 모듈의 차별성은 서버와 클라이언트 시스템간의 연동 부분에 있어서 보안성 지원을 위한 별도의 모듈을 삽입한 것이다. 이와 같은 시스템의 특징은 외부로부터 일어날 수 있는 각종 위협들의 차단을 목적으로 제시한 것이다.

이때 서버에서는 외부의 관리시스템으로부터 여러 상황을 점검 및 판단하여 서비스를 진행할 수 있도록 협업을 진행할 수 있는데, 본 연구에서는 이 과정에서 구성되는 외부관리시스템 인터페이스를 이용해서 인증 서버로부터 보안성 검토를 거쳐 서비스를 진행 할 수 있도록 설계 되었다. 이와 같이 보안성 지원 FUMO 모듈의 업데이트 프로세스는 그림 6과 같다.

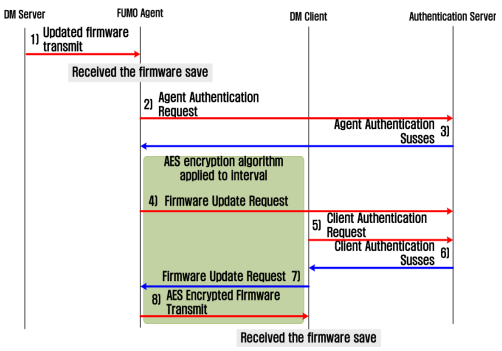


그림 6. 단말의 펌웨어 업데이트 과정
Fig. 6 Client firmware update procedure

그림 6에서 DM 서버에서 FUMO Agent로 업데이트된 펌웨어를 전송한다. FUMO Agent는 새로운 펌웨어 업데이트 내용을 확인하고 저장한 후, 자신의 정보를 담은 Agent 인증 요청 메시지를 인증 서버로 전송하고 이에 대한 응답을 수신하여 인증 절차를 거친 후, 인증이 성공한 경우, 단말로 펌웨어 업데이트 요청 메시지를 전송하고, 인증이 실패한 경우에는 통신을 중단한다. 인증 절차 이 후에 AES 알고리즘 적용으로 보호된 무선 통신구간을 통해 펌웨어 업데이트 요청 메시지를 DM 클라이언트로 전송한다.

펌웨어 업데이트 메시지를 수신한 DM 클라이언트는 단말 인증을 위해 자신의 정보를 담은 단말 인증 요청 메시지를 인증서버로 전송하고, 이에 대한 응답을 수신하여 인증 절차를 거친 후, 인증이 성공한 경우, DM 클라이언트는 FUMO Agent에 펌웨어 업데이트를 요청하게 되고, FUMO Agent에서 업데이트된 펌웨어를 전송한다. 반면 인증이 실패한 경우에는 통신을 중단한다.

마지막으로 DM 클라이언트에서 수신한 AES 알고리즘으로 암호화된 펌웨어를 복호화하여 단말의 펌웨어 업그레이드를 진행함으로서 종료된다.

위와 같이 펌웨어 업그레이드 과정에서 허가된 사용자만이 통신을 가능하도록 하여 외부로부터 발생 가능성이 있는 위조 또는 변조로부터 사전에 차단하고, 2차적으로 AES 알고리즘을 활용한 암호화된 데이터 전송으로 이중적인 구조의 보안 체계를 제공한다.

2.4 OMA SCOMO 구현

SCOMO 서비스는 단말기 내부의 소프트웨어에 대한 관리를 목적으로 이용된다[1]. 본 연구에서는 보안성이 강화된 SCOMO를 구현하기 위해서 모바일 단말기가 서버로부터 앱 다운로드를 시도할 때, AES 알고리즘을 적용한 보안 모듈을 활용하여, 암호화된 앱을 단말에서 다운로드 받을 수 있도록 구성하기 때문에 위조 및 변조로부터 보안된 통신 지원이 가능하다. 이러한 SCOMO 서버와 단말 간의 전체 동작구조는 그림 7과 같다.

그림 7에서 최초의 연결은 DM서버를 이용해서 단말과 연동하게 된다. 이때 수신된 내부 정보를 기반으로 SCOMO 서버는 SCOMO 단말 모듈과 메시지를 송·수신하여 관리가 필요한 소프트웨어의 상세 정보

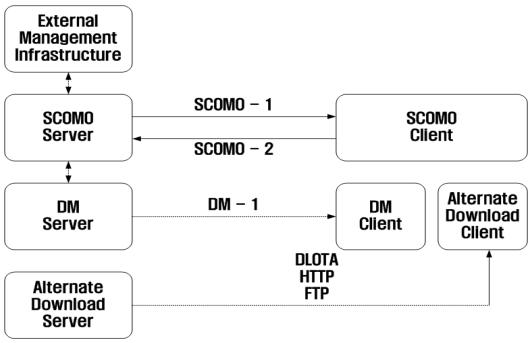


그림 7. SCOMO 동작 방법
Fig. 7 SCOMO process diagram

에 대해서 DC(Deployment Component, 구성요소배치)를 이용한다. DC는 Active, Inactive, Removed의 상태정보로 구성되며, 구성은 그림 8과 같다. 구성요소배치는 소프트웨어 자원에 대한 세부정보를 가지고 있고, 소프트웨어 요소와 메타데이터로 구분된다.

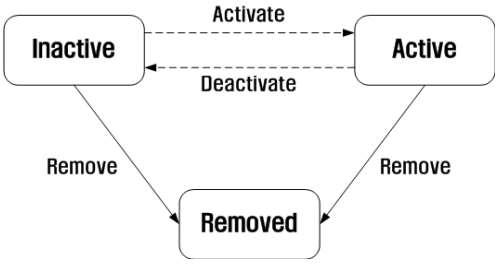


그림 8. DC 상태정보
Fig. 8 DC status information

이 소프트웨어 요소는 애플리케이션, 바이너리, 라이브러리 혹은 UI(User Interface), 인증, 라이선스 등의 형태를 포함하며, 메타데이터는 다양한 속성정보(구성요소에 대한 ID, 이름, 버전)를 가지고 있다. 그리고 DC 상태 정보를 통해서 현재 소프트웨어의 기능 및 제어를 수행할 수 있다. 이와 같은 DC를 활용하여 본 연구에서 구현한 보안이 강화된 SCOMO를 이용한 앱 및 콘텐츠 다운로드 과정을 도식화하면 그림 9와 같다.

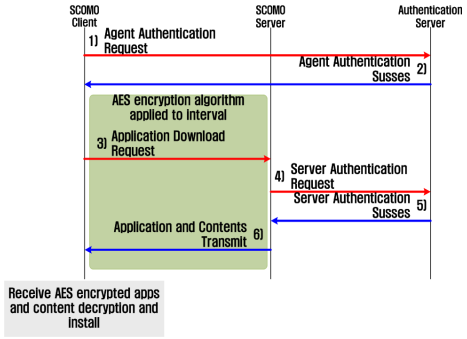


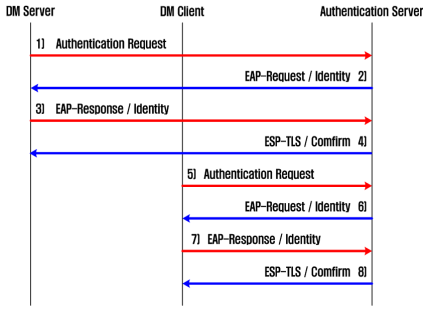
그림 9. SCOMO 앱 및 콘텐츠 다운로드 과정
Fig. 9 SCOMO app. and content download process

그림 9의 과정으로 앱 다운로드를 진행하려고 하는 단말이 인증 서버를 활용하여 단말인증을 요청을 통해 인증 절차를 수행하고 인증 서버는 단말의 인증을 허가한다. 이후에 인증된 단말은 SCOMO 서버로 앱 다운로드를 요청하고, 요청을 받은 SCOMO서버는 인증 서버를 활용한 인증 절차를 수행하고 인증 서버는 서버의 인증을 허가한다. 이러한 인증절차가 성공적으로 종료되면 SCOMO 서버는 AES 알고리즘을 적용한 암호화된 앱 및 콘텐츠를 전송하고, 단말에서 수신한 AES 암호화된 앱 및 콘텐츠를 복호화한 후, 단말에 설치하면서 SCOMO 앱 및 콘텐츠 다운로드가 종료된다.

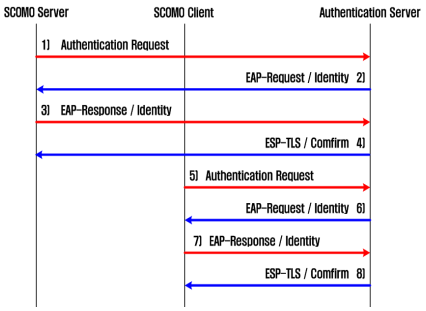
2.4 모바일장비관리시스템 보안 모듈 구현

기존 OMA DM의 경우 별도의 인증 서버의 보안성 검토 과정 없이 MD5(Message-Digest algorithm 5)[4] 혹은 HMAC(Hash-based Message Authentication Code)만을 적용하기 때문에 위조 및 변조에 대해 완전한 무결성 보장이 어렵다.

본 연구 개발에서는 기존의 단점을 보완하는 방법으로 인증 서버를 활용한 인증 절차인 EAP(Extensible Authentication Protocol)를 간단한 형태로 변형 적용하여, 간결하고 빠른 인증 절차를 구현하였다. 이를 기반으로 기존의 OMA DM Security 방법보다 간단하고 빠른 인증 절차를 통해 허가 받지 않은 공격자로부터 1차적인 위조 또는 변조의 시도를 차단하고, 인증 된 단말에 한해서 AES(128bit)로 암호화된 데이터를 송·수신하여 악의적인 공격자로부터 2차적인 위조 또는 변조의 시도를 차단한다. 이러한 인증 서버의 동작 구조는 다음 그림 10과 같은 인증 절차를 갖는다.



(a) FUMO 기능일 경우 인증 절차
(a) FUMO authentication procedure



(b) SCOMO 기능일 경우 인증 절차
(b) SCOMO authentication procedure

그림 10. FUMO 및 SCOMO 인증 절차
Fig. 10 FUMO and SCOMO authentication procedures

위와 같은 과정을 적용하기 때문에 외부 공격자로부터 악의적인 공격에 취약한 FUMO와 SCOMO 동작에서 위조 또는 변조의 공격 시도로부터 보호된 무선 통신구간을 활용한 데이터 전송이 가능하다.

III. 성능 평가

3.1 모바일장비관리시스템 성능 평가 환경

모바일장비관리시스템 성능 평가는 크게 두가지 형태로 OMA DM 서버 기반의 FUMO 및 SCOMO에 대한 서버 성능 평가로 구성되며, 시스템 성능 평가 구조도는 다음 그림 11과 같다.

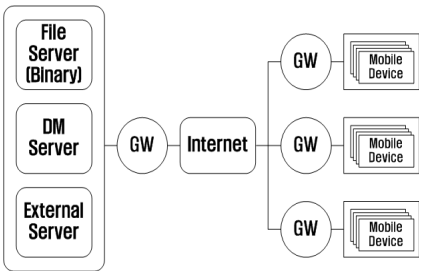


그림 11. 시스템 성능 평가 구조도
Fig. 11 System diagram for performance evaluation

성능 평가를 위해서 OMA DM, FUMO 및 SCOMO 서버를 구성하고 데이터를 전송하기 위한 파일서버와 펌웨어 및 소프트웨어 업데이트 명령 전송을 위한 외부 서버를 별도로 구성한다. 외부 서버의 성능의 사양은 표 1과 같다.

표 1. 성능 평가 서버 사양
Table 1. Server spec. for performance evaluation

	Server Specifications		
	DM server FUMO, SCOMO	File	External Management
CPU	Intel Xeon QuadCore 1.8GHz	Intel Xeon QuadCore 1.8GHz	Intel Xeon QuadCore 1.8GHz
RAM	16GB	8GB	8GB
OS	CentOS 6.4 64bit		

표 1과 같이 서버는 DM Server(FUMO, SCOMO)와 File 그리고 External Management와 같이 크게 3가지 형태로 구성되고, 테스트 모바일 단말기기의 사양은 표 2와 같다.

표 2. 테스트 모바일 단말기 사양
Table 2. Mobile device spec. for performance test

	Mobile device Specifications
CPU	ARM Dual Core 1GHz
RAM	1GB (DDR2)
Network	WiFi 802.11 b/g/n
OS	Android 2.2

위와 같은 성능 평가 환경을 구성한 후, 진행된 FUMO와 SCOMO의 평균 업데이트 시간은 다음 표 3과 같다.

표 3. FUMO / SCOMO 평균 업데이트 시간
Table 3. Average update time for FUMO/SCOMO

	Group					(Unit : Sec)
	A	B	C	D	E	F
Device	50	100	150	200	250	300
FUMO (200MB)	145	160	220	270	313	456
SCOMO-1 (3MB)	6	8	20	25	28	36
SCOMO-2 (10MB)	17	21	28	53	61	74

표 3의 성능 평가는 각각 100회씩 진행한 결과값을 평균 시간으로 표기하였다. 가장 큰 업데이트 시간은 300개의 단말로 구성된 F그룹으로 FUMO 테스트를 진행할 때 평균 450초이다. 그리고 가장 적은 업데이트 시간으로 테스트 완료된 것은 SCOMO-1(3MByte) 테스트로 3MByte의 소프트웨어를 업데이트 할 때 가장 적은 시간이 소요되었으며, 그 결과는 그림 12와 같다.

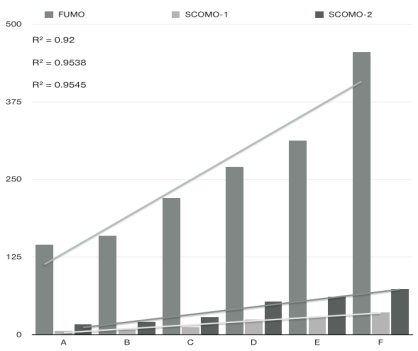


그림 12. FUMO / SCOMO 평균 업데이트 시간
Fig. 12 Average update time for FUMO / SCOMO

본 논문에서 개발된 FUMO와 The Eclipse Foundation의 OMA DM 시뮬레이션과 성능을 비교한 평가 결과로 그림 13과 같다. 본 연구에서 개발된 OMA

DM FUMO가 평균 36% 성능이 우수한 것을 입증하였다. 이와 같은 결과는 업데이트 수행을 일괄처리방식(Batch Processing)으로 구현한 Koneki와 비교하여 본 연구에서 사용된 라운드로빈 스케줄링(Round Robin Scheduling, RR) 방식의 세션관리 및 재전송기법이 성능향상과 밀접한 연관이 있음을 확인하였다. 또한 본 연구에서 구현된 OMA DM 서버의 성능의 우수성이 검증되었다.

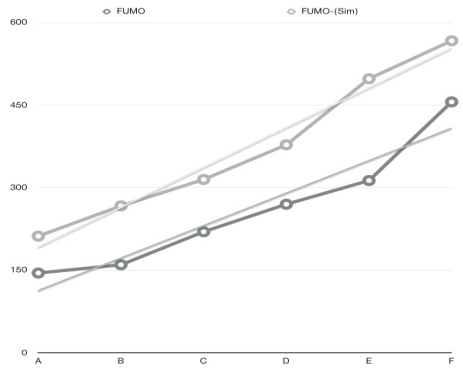


그림 13. FUMO 성능비교
Fig. 13 FUMO performance evaluation

표 4. FUMO 성능비교
Table 4. FUMO performance comparison chart

	Group					(Unit : ms)
	A	B	C	D	E	F
Device	50	100	150	200	250	300
Proposed Module	210	255	318	375	490	580
Koneki Module	148	165	220	267	310	412

그림 13과 표 4의 결과에서 제안한 모듈이 기존의 모듈에 비해 업데이트 시간은 조금 더 소요되지만 실질적으로 활용되는 환경에서는 체감하는 차이가 많지 않다. 그러나 제안 모듈에서는 다음 3.2절에 기술된 보안 모듈을 삽입하여 무선 구간에서의 안전성을 확보하였다는 것에 의미가 있다.

3.2 모바일장비관리시스템 보안 모듈 성능 평가

본 연구에서 제안한 보안 모듈의 성능 평가를 위해 우선적으로 기존의 무선 통신 구간에서의 보안 위협에 대해 분석하였다.

기존의 무선 통신 구간에서의 보안 위협[5] 종류로는 전파간섭, 도청, 삭제, 삽입, 허위, 위조, 변조 등이 존재하고, 각각의 정의를 살펴보면 전파 간섭은 허가받지 않은 공격자가 불법 주파수대역을 임의로 사용하여 송신자와 수신자간의 전송 메시지에 교란 신호(jamming 신호)를 추가시켜 전파를 교란하는 공격이다. 둘째로 도청의 경우 기밀 데이터를 전송하고자 할 경우 공격자가 단순히 수동적으로 중간에서 기밀 데이터가 포함된 전송 메시지를 수집하고, 공격자는 수집된 메시지를 분석하여 메시지에 포함된 기밀 데이터를 알아내는 공격이며, 셋째로 삭제의 경우 공격자가 기밀 데이터를 중간에서 수집하여 전체 또는 일부를 삭제하는 공격이다. 넷째로 삽입은 변조에 해당하며 공격자가 송·수신자가 주고받는 메시지 사이에 다른 메시지를 삽입하는 공격이고, 다섯째로 허위는 위조에 해당하며, 허가받지 않은 공격자가 송신자가 생성하여 송신한 메시지인 것처럼 허위 메시지를 생성한 후 수신자로 전송하는 공격이다. 이와 같은 위협들을 정리한 내용은 다음과 같다.

본 연구에서는 기술적 보안 위협에 초점을 두어, 앞에서 나열한 무선구간의 기술적 보안 위협들을 정리하면 우선 도청 위협은 sniffing(스니핑) 공격이 대표적으로 위조 및 변조 등의 다양한 공격에 기반이 되는 위협이다[6]. 삭제 위협의 경우 삭제 위협 및 삽입 위협이 복합적으로 적용될 경우 변조의 형태로 나타난다. 삽입 위협은 앞에서 언급하였듯이 도청 위협을 기반으로 하여 복합적으로 적용될 경우 변조의 형태(Hijacking 등)로 나타나며, 허위 위협은 공격자가 허위 메시지를 전송하는 위협으로 도청 위협을 기반으로 허위 위협이 적용되는 경우가 바로 위조(spoofing 등)공격에 해당된다.

AP 위장 위협은 불법 AP를 설치하여 인가된 AP인 것처럼 위장하는 위협으로 단말에서 송신하는 데이터 내의 사용자 정보가 노출될 수 있고 또한 서비스 거부(DoS: Denial of Service) 공격으로 이어질 수 있다. 마지막으로 단말 복제는 비인가자가 허가받은 단말로 위장하는 공격이다. 이러한 무선 통신 구간에

서의 보안 위협에 대해 기존의 MD5와 HMAC을 활용한 OMA DM Security와 제안한 보안 모듈을 비교한 결과는 표 5와 같다.

표 5. 기존 보안모듈과 제안 보안모듈 비교
Table 5. Performance comparison for the proposed security module

Risk of incident	Lgacy security modules		Proposed security modules	
	MD5	HMAC	EAP	AES
Power Interception	○	○	○	○
Noise			○	○
Jamming	○			○
Sniffing			○	
Modification			○	○
Hijacking			○	○
Fabrication	○	○	○	○
Spoofing	○			○
AP camouflage	○	○	○	
Device replication	○	○	○	

표 5와 같이 기존의 OMA DM 표준에서 제안하는 보안 모듈로 활용되는 MD5와 HMAC을 활용하였을 경우, 인증 절차만을 수행하는 단순한 방법으로 인해서 무선 구간에서의 위험사건들 중 잡음 삽입, 재밍, 스니핑, 변조, 세션하이재킹, 스푸핑의 공격에 취약한 단점이 있다. 하지만 EAP 인증 절차와 AES 알고리즘을 활용한 2중구조의 형태를 가지고 있는 제안된 보안 모듈은 모든 위험사건에 대비하여 기존의 OMA DM에서 활용되는 보안모듈인 OMA DM Security보다 무선 통신구간에서 위협사건들로부터 무결성이 보장된 통신 지원이 가능하다.

또한 표 5의 결과를 검정하기 위해서는 실제 환경에서 직접적인 실험이 요구되지만, 이는 대량의 모바일 단말기의 동원이 필요해 실질적이고 비용적인 측면에서 불가능하다. 그러므로 실험 상황을 쉽게 제어하기 위해 시뮬레이션 환경으로 구성하여 진행하였다. 그 내용은 무선 통신구간에서의 위협 사건을 무작위로 생성하여 DM 서버, FUMO 및 SCOMO 사이에서 전달되는 프레임을 송·수신하는 과정에서 위협사건들의 방어 능력을 검정하는 과정으로 시뮬레이션을 진행하였으며 그 결과는 표 5와 같고. 이러한 검정을 통해 기존의 OMA DM Security보다 제안한 보안모듈이 공장자동화 또는 사무자동화 등의 업무자동화에 활용되는 모바일 장비관리시스템의 기능적 특성으로 활용되는 FUMO와 SCOMO의 동작과정에서 더욱 안정성이 보장된 통신 지원이 가능함을 입증하였다. 그 결과는 표 6과 같다.

표 6. 제안된 보안모듈 성능 평가
Table 6. Performance evaluation of the proposed security module

Risk of incident	Proposed security modules	
	EAP	AES
Power Interception	100%	100%
Noise	100%	100%
Jamming		100%
Sniffing	100%	
Modification	100%	100%
Hijacking	100%	100%
Fabrication	100%	100%
Spoofing		100%
AP camouflage	100%	
Device replication	100%	

표 5 및 표 6과 같은 결과를 통해 기존의 MD 5와 HMAC을 활용한 OMA DM에서 제안한 OMA DM Security는 각종 무선 통신 구간에서의 보안 위협에 대해서 완전한 무결성을 지원할 수 없다. 그러나 본 논문에서 제안한 보안 모듈은 각종 보안 위협에 대해서 완전한 무결성 지원이 가능함을 입증하였다.

Ⅳ. 결 론

공장 자동화나 사무자동화에 편리한 스마트폰의 활용은 생산 원가나 제품의 품질 및 생산성 향상을 위해 필수불가결한 사항으로 인식되고 있다. 해당 시스템을 제공하기 위해 안드로이드 기반 모바일장비관리시스템을 활용한 스마트폰 앱 및 펌웨어 서비스 구현과 필요한 정보의 전달과정에서의 보안 문제는 매우 중요한 기술이다.

국내외의 모바일장비관리시스템과 관련하여 연구 개발된 구현들은 공장자동화나 생산자동화에 초점을 맞춘 특화된 형태의 접근과는 약간 거리가 있다. 더군다나 해당 모바일 앱 관련 보안 문제는 OMA 표준에서 규정하고 있는 MD5에 기반 된 보안모듈은 이미 90년대 후반 그 취약성이 확인되었고 실용적인 부분에서도 적용 대상이 모바일단말이라는 특성으로 인해 문제점을 가지고 있다.

본 연구에서는 이와 같은 중요성을 고려하여 OMA DM 표준 기반의 기능적 특성으로 단말 기기의 펌웨어 관리를 위한 FUMO와 소프트웨어 및 관련 컨텐츠까지 관리하는 SCOMO를 설계 및 구현하였고, 또한 공장자동화, 생산자동화, 그리고 업무자동화 등의 분야에 효과적으로 활용하여 외부 공격자로부터 취약한 무선 통신 구간에서의 보안을 강화하였다.

결과적으로 본 연구에서 구현된 프로토타입은 공장자동화 부분에서 응용되어 그 성능이 검정되었으며 다양한 분야의 공장자동화나 생산자동화, 설비 자동화 그리고 업무자동화 부문에 효과적으로 활용되는 스마트폰 앱 및 펌웨어 개발과정에서 보안이 검정된 서비스 제공에 효과적으로 활용이 가능하다.

감사의 글

본 논문은 교육부의 재원으로 지원을 받아 수행된 산학협력 선도대학(LINC) 육성사업의 연구결과물입니다(CD20131088, 공장 및 생산 자동화에 있어 스마트폰 앱서비스 개발 및 활용을 위한 안드로이드 기반 모바일장비관리시스템의 보안모듈개발).

References

[1] T. Kim, "OMA Standardization - OMA Device management," *TTA J.*, vol. 97, Feb. 2005, pp. 114-119.

[2] S.-R. Cho and K.-J. Choi, "Design and Implementation of the OMA DM Client on the Open Mobile Terminal Platform," In *Proc. the Institute of Electronics and Information Engineers,* Seoul, Korea, Nov. 2006, pp. 188-191.

[3] W.-Y. Jeong and S.-K. Lee, "A Study on the Self-Key Generation Algorithm for Security Elevation in Near Field Communications," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 7, no. 5, 2012, pp. 1027-1032.

[4] C.-S. Lee, "A Study on MD5 Security Routing based on MANET," *J. of The Korea Institute of Electronic Communication Sciences,* vol. 7, no. 4, 2012, pp. 797-803.

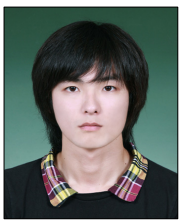
[5] S.-J. Park and J.-H. Park, "Current Status and Analysis of Domestic Security Monitoring Systems," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 9, no. 2, 2014, pp. 261-266.

[6] S. Liu, L. Lazos, and M. Krunz, "Thwarting Inside Jamming Attacks on Wireless Broadcast Communications," In *Proc. of the Fourth ACM Conf. on Wireless Network Security WiSec'11*, Hambourg, Germany, June 2011, pp. 29-40.

저자 소개

유흥식(Hyung-Cik Yu)

1993년～1997년 경성대학교 전산통계학과 학사
1997년～1999년 경성대학교 전산학과 석사
1999년～2011년 부경대학교 정보통신공학과 박사 수료
2006년 12월～현재 ㈜유노믹 대표이사
※ 관심분야 : 수중 센서 네트워크, 센서네트워크, 이동통신, 방송기술



선기현(Ki-Hyun Seon)

2012년 2월 동명대학교 정보통신공학과(공학사)
2014년 2월 부경대학교 대학원 정보통신공학과 석사(공학석사)
※ 관심분야 : 무선네트워크 보안기술, 유비쿼터스 센서네트워크

김성운(Sung-Un Kim)

1982년～1985년 한국전자정보통신연구소 연구원
1985년～1995년 한국통신연구개발원 선임연구원 실장
1989년～1993년 프랑스 파리 7대학 석 · 박사
1995년～현재 부경대학교 정보통신공학과 교수
※ 관심분야 : 무선네트워크 보안기술, 열차제어신호 전송 기술, 센서네트워크, 수중 센서네트워크, 센서 노드 이동성 지원 기술, USN, DWDM, RWA 알고리즘