M2M 기기에서 스마트폰 및 차량 인증 기법

여성권, 이근호
백석대학교 정보통신학부

Smart Phone and Vehicle Authentication Scheme with M2M Device

Seong-Gwon Yeo, Keun-Ho Lee
Division of Information Communication, Baeseok University

요 약 IT의 발전으로 기기 간 통신을 이용하는 M2M 시장이 급성장하고 있으며, 많은 기업들이 M2M 사업에 참여하고 있다. 본 논문에서는 텔레매틱스의 개념 및 차량 네트워크 보안의 취약성을 알아보았다. 차량 및 IT 기술의 융합과 이동통신망 기술의 발전은 사용자에게 제공되는 서비스의 질은 향상 시켰지만, 이로 인한 보안 위협은 다양해졌다. 텔레매틱스 사업에서 이동통신사업자의 참여로 생성될 수 있는 새로운 비즈니스 모델을 제시하였으며, 이러한 환경에서 발생 될 수 있는 차량 이동통신망 보안 취약성을 분석하였다. 이 중 발생할 수 있는 취약성을 해결하기 위한 방법으로 M2M 기기와 스마트폰 및 차량 상호 인증 기법을 제시하였다.

• **주제어** : 사물통신, 텔레메틱스, 스마트폰, 자동차 인증

Abstract As the developing of the information technology, M2M market that is using communication between devices is growing rapidly and many companies are involved in M2M business. In this paper, the concept of telematics and vulnerabilities of vehicle network security are discussed. The convergence of vehicle and information technology, the development of mobile communication technology have improved quality of service that provided to user but as a result security threats has diverse. We proposed new business model that be occurred to the participation of mobile carriers in telematics business and we analyzed mobile radio communication network security vulnerabilities. We proposed smart phone and Vehicle authentication scheme with M2M device as a way to solve vulnerabilities.

• **Key Words** : Machine to Machine, Telematics, Smart Phone and Vehicle authentication

1. 서론

최근 IT 및 이동통신 기술의 발전으로 많은 사람들이 스마트폰을 이용하고 있다. 급속도로 증가하는 스마트폰 보급률과 활용도로 인해 그동안 국내 사람들에게 잘 알려지지 않았던 M2M(Machine-to- Machine)시장에 대한 관심과 개발이 활발하게 이루어지고 있으며, 다양한 업체의 참여와 함께 M2M 통신에서의 보안 역시 큰 이슈가 되고 있다[1].

M2M은 우리의 주변에서 존재하는 기기간의 통신을 의미한다. M2M 통신은 사용자 및 업체의 컴퓨터와 가전제품, 자동차(M2M Device in Car), 스마트폰과의 연동이

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2011-0010457)
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2011년 10월 10일 수정일 2011년 11월 17일 게재확정일 2011년 12월 5일

가능하도록 해준다. 이러한 연동으로 인해 각 기기들은 주변에서 수집한 다양한 정보들을 분석하고 분류하여 유무선 네트워크와 이동통신, 전송매체를 이용하여 정보를 요청한 사용자나 또 다른 기기에게 전송한다. 사람과 기기 사이의 상호작용을 통해 다양한 데이터를 얻을 수 있으며, 수집된 데이터를 통해 다양한 서비스를 제공하기 위해 M2M 사업의 확장, 다수의 기업의 참여 및 연구가 활발히 진행되고 있다.

과거의 M2M 통신에서는 각 기기들 간에 정보 전달만을 수행하였지만, 현재의 M2M 통신은 기기를 넘어서 사람과 기기간의 정보 전달을 통해 사용자가 실시간으로 정보를 확인하는 수준까지 이르렀다. 이러한 환경으로 사용자는 신속하고 정확하게 정보를 제공 받을 수 있지만, 기기와의 데이터 전송 시 많은 보안 문제에 직면하게 되었다.

본 논문에서는 M2M의 응용분야인 텔레매틱스에 대해 살펴보고, 텔레매틱스의 보안 취약성과 스마트폰으로 텔레매틱스를 이용할 시 발생할 수 있는 취약성에 대해 분석한다. 이러한 분석을 통해 차량 내의 M2M 기기와 스마트폰의 상호 인증에 대한 기법을 제안한다.

2. 관련연구

2.1 M2M 보안 취약성

M2M에서의 네트워크 통신 방법은 기기간의 이동으로 인한 빈번한 형태 변화와 무선 채널을 사용하는 구조적인 취약점을 가지고 있다. 잦은 네트워크의 변화와 무선채널의 위험에 따른 정보 수집의 어려움과 안정적인 관리와 효율적인 해결방안이 요구된다. M2M 통신에서도 기존 보안의 특성을 이용하여 보안 위협요소로부터 안전한 정보수집 등의 서비스를 제공해야 한다. 가용성, 기밀성, 무결성, 인증, 부인봉쇄와 같은 요구들을 만족할 수 있는 보안 요소기술 개발이 필요하며, 다음의 보안 위협을 고려해야 한다.

- 기밀성 : M2M 통신 환경에서는 데이터 노출로 인한 위치, 개인정보, 과금 데이터 등의 민감한 정보를 전송을 하기 때문에 네트워크 어느 곳에서나 도청에 의해 수집되는 데이터 유출을 예방하기 위해 데이터의 기밀성을 보장해야 한다.
- 무결성 : 중간자(man-in-the-middle) 공격을 통한 데이터의 불법 변경 및 삭제, 위조된 데이터의 삽입 등에 대응하기 위한 무결성 보장이 필요하다.
- 가용성 : 서비스 거부공격(DoS)은 시스템의 가용성 및 생산성을 훼손함으로써 시스템 자원과 정보에 대한 접근 능력을 감소시킬 수 있다. 따라서 M2M 통신 환경에서도 주체 또는 디바이스들의 정보 접근 능력을 침해하지 않도록 시스템 가용성을 보장할 수 있는 보안 메커니즘이 필요하다.
- 개인정보보호 : 사용자의 개인정보 수집 및 도용은 M2M 디바이스가 사람의 일상과 밀접하게 연관되어 있으므로 사용자와 관련된 정보를 기록하게 된다. 이러한 사용자 데이터들의 불법적으로 노출 되는 경우, 개인 프라이버시 침해 문제가 발생할 수 있으므로 이를 방지 할 수 있는 보안 메커니즘이 필요하다. 이동성을 제공을 위한 위치추적의 경우 M2M 디바이스는 디바이스의 위치정보 노출로 인해 디바이스 및 디바이스 소유자의 위치나 이동 경로가 노출될 가능성이 존재한다. 따라서 이동성을 제공하면서 추적 불가능성을 제공할 수 있는 보안 메커니즘이 필요하다[2,3].

M2M에서 장비의 위협에는 기기간의 도청, 가로채기, 부인과 관련된 프라이버시 및 변조 위협요소가 있으며, Gateway에서는 불법 도용 및 접근을 통한 권한위배, 물리적인 침입, 재사용 공격 및 중간자 공격 등이 있다. M2M 네트워크에서는 불법침입, DOS 공격을 통한 마비, 바이러스, 웜, 자원고갈 등의 위협 요소가 있다[3].

2.2 텔레매틱스

M2M 시장을 살펴보면 다양한 응용분야가 있음을 알 수 있는데, 주요 응용분야로는 텔레매틱스, 물류관리, 지능 검침 시스템, 원격 자산 관리 시스템, 판매 관리 시스템(POS) 및 보안 관련 분야가 있다[4].

M2M 시장을 이끌고 있는 응용분야 중 하나인 텔레매틱스(Telematics)는 통신(telecommuncation)과 정보(informaics)의 합성어로, 차량의 위치파악기술, 양방향 통신이 가능한 무선 통신망과 차량 내 단말기를 통해 차량, 운전자, 탑승자에게 다양한 정보 및 서비스를 제공하는 것을 말한다.

즉, 위성위치확인시스템(GPS, Global Positioning System), 지리정보시스템(GIS, Geographic Information System)

과 무선통신망을 이용하여 차량 내 모든 탑승자에게 교통정보, 최적경로, 날씨정보, 도난방지, 도난차량 추적, 원격진단, 응급상황에 대한 대처, 인터넷, 전화 등을 제공하는 종합서비스라 할 수 있다[1].

2.3 텔레매틱스 보안 취약성

차량에서 사용하는 대표적인 네트워크로 VANET (Vehicular Ad-hoc Networks)이 알려져 있으며, 차량을 중심으로 차량 간 통신망(V2V Vehicle-To-Vehicle)과 차량과 인프라 통신망(V2I Vehicle-To-Infrastructure)으로 분류된다[5].

VANET도 기본적으로는 기존의 네트워크 기반의 무선 환경을 바탕으로 하고 있기에, 기존의 무선 네트워크 환경이 가지고 있는 보안 취약성을 그대로 가지고 있다[6].

다음은 VANET에서 나타날 수 있는 보안 취약성 중 일부이다.

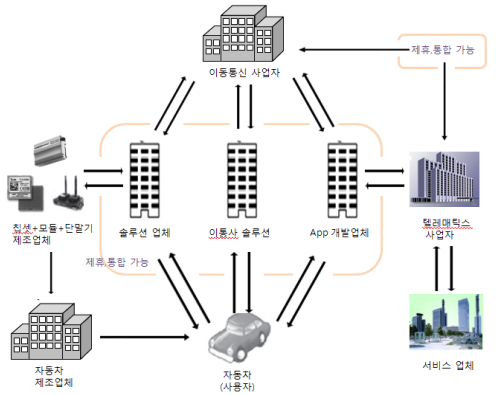
- The Sybil Attack[7] : 한명의 공격자가 네트워크상에서 여러 개의 환영노드들로 나타나서 혼란을 가중시키는 공격.
- 위조 공격 : 공격 차량에 의해 차량 간 네트워크 영역 내에서 다른 차량들을 거짓 정보로 오염시키는 공격.
- Jamming Attack : 차량 네트워크 영역 내에서 다른 차량의 통신에 장애를 유발하는 신호를 발생시켜 네트워크 통신을 마비시키는 공격.
- In-transit Traffic Tampering : 주행 중에 메시지를 전달하는 과정에서 공격 차량에 의한 메시지 삭제·변조를 통해 차량 통신을 방해하는 공격.

이외에도 주변 차량을 자신의 차량으로 오인하게끔 만드는 공격과 차량 내부의 다양한 정보 등을 위변조 하는 공격 등 많은 취약성이 존재하고 있다[1].

2.4 텔레매틱스의 새로운 비즈니스 모델

그림 1을 살펴보면 텔레매틱스 시장은 다수의 하부 업체들이 각각의 독립 분야를 맡아서 참여하는 구조로 되어 있다. 즉, End-User에게 서비스가 제공되는 과정에 있어서 텔레매틱스 서비스 사업자, 칩셋 공급업체, 모듈 업체, 단말제조업체, 이동통신사업자, 서비스업체(콘텐츠, 보험회사, 정비회사 등), 솔루션업체 등이 관여한다고 볼 수 있으며, 이외에도 다양한 업체의 참여가 이루어지고 있다.

다수의 업체 중 이동통신 사업자가 텔레매틱스 사업에 참여함으로써 차량 내 M2M 기기와 스마트폰의 통신을 이용하여 사용자는 다양한 정보를 얻을 수 있지만 이로 인한 새로운 보안 취약성이 존재 할 수 있다[1].



[Fig. 1] Telematics Business Model

2.5 차량 이동통신 기술 및 보안 취약성

이동통신은 1세대인 아날로그에서부터 4세대인 IMT-Adcanced까지 진화해 왔으며, 현재는 3세대인 WC-DMA/HSDPA를 주로 사용하고 있다. 이동통신기술의 발전으로 인해 사용자는 각종 사용자 디바이스(스마트폰, 태블릿PC, PDA, 노트북, 차량용 셋톱박스, PMP 등)로 사용자가 언제, 어디서든 차량의 상태를 파악할 수 있게 되었다. 사용자는 이동통신망을 이용하여 사용자 디바이스와 차량 단말기의 통신을 통해 차량에 대한 각종 정보를 고속의 데이터 전송으로 제공받을 수 있다. 그러나 인터넷 서비스가 스마트폰 환경에서도 구현이 되면서 이동통신망을 이용한 보안 취약성이 존재하게 됐으며, 이러한 취약성은 차량과 통신 중에도 발생 할 수 있다. 다음은 이동통신망을 이용해 사용자와 차량과의 통신 시에 나타날 수 있는 보안 취약성이며, 일부임을 밝혀둔다.

- 모바일 악성코드 : 어플리케이션에 악성코드가 삽입되어 사용자가 어플리케이션을 다운 받은 후 차량과 디바이스의 통신을 하면 개인정보 및 차량 정보가 유출되는 공격.

- 서비스 거부 공격 : Jamming Attack과 비슷한 공격으로 스마트폰에 다량의 데이터를 전송하여 서비스를 이용하지 못하게 하는 공격. 사용자는 차량 단말기와의 통신도 불가능.
- 무선 인터넷 중계기 공격 : 인터넷에 접속하기 위해 AP(Access Point)에 접속 시 스마트폰과 AP, 차량 단말기와 AP가 서로 주고받는 정보가 해커에 의해 해킹되는 공격.
- WiFi Phising : 해커가 자신의 노트북을 AP로 전환하여 DNS, DHCP, HTTP 등의 서비스를 활성화시켜 사용자를 유인하는 방법. 사용자 및 차량이 해커의 AP에 접속되어 개인정보가 유출되는 공격.
- 사용자 인증 위장 공격 : 허가받지 않은 사용자가 인증서버로부터 인증을 받아 통신을 요청한 사용자 대신에 차량 내 M2M 기기와 통신하여 개인정보 획득 및 차량 오작동을 시키는 공격.

위에서 언급한 바와 같이 차량의 M2M 기기와 스마트폰과의 통신 시 다양한 위험요인이 존재한다. 본 논문에서는 이 중 정당한 사용자로 위장하여 서버로부터 인증을 받아 위장 공격하는 방법에 대한 해결책을 제시하고자 한다[1].

3. M2M 기기와 스마트폰 상호 인증

차량 내 M2M 기기와 사용자의 디바이스(스마트폰, 태블릿PC, PMP등) 통신 환경은 무선 통신으로 이루어지며, 신뢰받지 않은 제 3자에 의한 위장공격을 차단해야 한다. 신뢰받는 무선 통신을 하기 위해서 상호 인증된 상태로 진행 될 수 있도록 인증 절차를 제안하였다. 두 기기가 제 3의 기관으로부터 인증을 받아 서로 신뢰된 상태에서 통신을 할 수 있게 하였다.

3.1 시나리오

사용자의 스마트폰 및 차량 내 M2M 기기(이하 MIC)와 신뢰 할 수 있는 제 3기관(이하 TTI)이 있다. 사용자가 스마트폰을 이용하여 MIC와의 통신을 원할 때, 사용자의 스마트폰은 TTI로 사용자의 아이디와 패스워드를 전송한다. 스마트폰은 사용자의 패스워드가 임시로 저장되지 않아야 하며, 패스워드 추측공격을 당하지 않아야 한다. TTI는 사용자 및 MIC의 정보를 보유하고 있으며, 등록 및 키 관리를 담당한다. 또한, 인증 받지 않은 사용자로부터 안전하다고 가정한다.

기존의 인증방식은 스마트폰과 MIC간의 통신을 위해서 스마트폰 사용자가 인증서버에 인증을 요청할 시 스마트폰 사용자만 인증서버로부터 인증을 받아 MIC는 스마트폰 사용자가 정당한 사용자인지 확인할 수 없는 상태에서 통신을 하였다. 또한 스마트폰 역시 MIC가 정당한 MIC인지 확인하지 못한 채 접속 되어 공격자가 정보를 획득 할 수 있다.

본 논문에서 제안하는 인증 방법은 스마트폰에서 MIC와의 통신을 위해 접속요청 시 스마트폰 사용자가 정당한 사용자인지 TTI로부터 인증을 받는다. MIC는 TTI로부터 정보를 받아 접속을 요청한 사용자가 TTI로부터 인증을 받은 사용자인지 확인 할 수 있다. 스마트폰 및 MIC가 TTI로부터 인증을 받아 상호 간 신뢰성 있고 안전한 통신이 가능하다.

3.2 상호 인증

사용자가 스마트폰을 이용하여 자신의 차량 내의 MIC에게 연결을 요청할 때 사용자는 TTI로부터 본인 인증을 받아 MIC와 안전하게 통신이 되어야 한다. 사용자가 인증을 위하여 단순히 ID와 패스워드만을 입력하여 인증을 받는 단순한 방식에서 벗어나 좀 더 복잡한 과정을 거쳐 인증을 받는 것이 안전하다.

- 1. 사용자는 자신의 ID와 패스워드를 스마트폰에 입력하면 스마트폰은 사용자의 ID, MAC 주소, 패스워드를 이용하여 만든 비밀 키를 TTI에게 보낸다.
- 2. TTI는 사용자의 패스워드를 기반으로 한 사용자의 마스터 키(UMK)를 찾아서 사용자 정보를 포함하고 있는 TGT-1과 세션 키를 만든다. TTI는 자신의 마스터 키(TMK)를 이용하여 TGT-1을 암호화하고 TGT-1과 세션 키를 사용자에게 보낸다.
- 3. 사용자는 암호화된 TGT-1과 세션키를 가지며, MIC와 접속할 준비가 됐다.
- 4. 사용자는 TTI에게 TGT-1와 세션키로 암호화한 TimeStamp를 보낸다. TTI는 TMK를 사용하여 TGT-1를 복호화하고 세션 키를 이용하여 TimeSta-mp를 복호화 한다. 사용자가 TTI의 세션키를 사용할 수 있기 때문에 TTI는 정당한 사용자인지를 확인 할 수 있다.

- 5. TTI는 사용자와 MIC를 위한 TGT-2를 각각 하나씩 만든다. 각 TGT-2에는 사용자 이름, MIC 이름, TimeStamp를 가지고 있으며 새로운 키인 KAB를 포함한다.
- 6. TTI는 서버의 TGT-2를 MIC의 마스터 키(MK)로 암호화 한다. TTI는 MK로 암호화 된 TGT-2를 사용자와 공유한 세션 키로 다시 암호화 하고 사용자에게 이것을 전송한다.
- 7. 사용자는 세션 키를 이용하여 MK로 암호화 된 TGT-2를 복호화 한다. 복호화로 인해 사용자는 MIC의 TGT-2와 KAB를 알 수 있다. 사용자는 KAB를 사용하여 TimeStamp를 암호화 하고 MIC에게 암호화 된 TimeStamp와 TGT-2를 보낸다. 두 가지를 받은 MIC는 MK를 사용하여 TGT-2를 복호화 하고 KAB를 이용하여 TimeStamp를 복호화 한다.

사용자와 MIC 모두 KAB를 가지고 있으며, 사용자가 TimeStamp를 암호화 하기 위해 KAB를 사용했기 때문에 사용자가 정당한 사용자인지 확인이 가능하다. 사용자 역시 MIC가 TimeStamp를 얻기 위해 KAB를 사용해야만 했기 때문에 MIC가 정당한 기기인지 알 수 있다.

3.3 검증 결과

기존의 인증방법에서는 사용자가 차량 내 M2M 기기와의 접속 요청 시 서버로 자신의 ID와 패스워드만을 이용하여 사용자가 정당한 사용자인지만을 확인하여 M2M 기기와의 접속이 허락됐다. 그러나 이러한 방법은 공격자가 사용자의 인증정보를 얻음으로써 접속을 요청한 사용자 대신에 M2M 기기와의 통신을 수행하여 사용자 정보를 수집, 도용, 변조, 삭제를 할 수 있다.

본 논문에서는 사용자가 제 3기관과의 암호화 및 키 교환을 통해 정당한 사용자 인지를 확인하고 M2M 기기 역시 제 3기관으로부터 사용자의 정보를 받아 정당한 사용자인지 1차 확인한 후, M2M 기기가 사용자와 키를 교환함으로서 사용자가 정당한 사용자인지 2차 확인을 한다. 이러한 암호화 및 키 교환으로 인해 사용자 역시 M2M 기기가 자신의 기기 맞는지에 대한 여부를 확인 할 수 있다.

4. M2M 기기와 차량 간 상호 인증

M2M에서 기기간의 인증을 위해 클러스터 인증 절차를 제안하였다. 무선으로 이루어지는 M2M 기기 간 통신에서 상호 신뢰할 수 있는 접속이 필요하다. 클러스터내에서 ClusterHead(CH)를 통해 차량 내 M2M 기기 및 신뢰 할 수 있는 제 3기관의 상호 인증이 이루어져 기기간의 안전한 통신을 할 수 있다.

4.1 클러스터링 기법

클러스터링은 네트워크에서 잦은 형태의 변화에 적용하기 위해서 사용하는 기법이다. 클러스터 내에 일반 기계나 기기들을 관리하고 인증해주는 클러스터헤드(CH)가 존재하여 다른 클러스터에서 클러스터내로 진입 시 CH간에 인증을 통해 상호 신뢰성을 보장해주는 기법이다[8].

4.2 시나리오

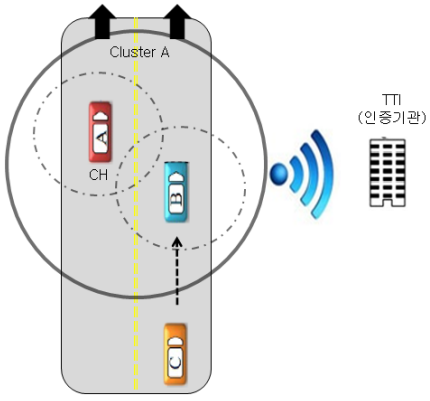
사용자의 차량 내 M2M 기기(이하 MIC)와 신뢰 할 수 있는 제 3기관(이하 TTI)이 있다. 본 논문에서는 사용자를 기준으로 사용자 차량을 CH로 선정한다. 사용자 주변 클러스터 내에는 사용자로부터 인증 받은 기기들이 존재하며, 사용자가 클러스터내의 기기들 중 가장 신뢰할 수 있는 기기를 CH로 선정한다고 가정한다. [그림 2]의 차량 A와 차량 B는 상호 인증 된 상태라 가정한다. TTI는 인증기관으로서 모든 기기에 대한 등록, 인증에 대한 모든 관리를 담당하며, 위장공격 및 무선 통신에 대한 가로채기 공격으로부터 안전하다고 가정한다. 사용자 차량(CH)은 TTI로부터 인증 받은 정당한 사용자이며, TTI로부터 인증을 받은 CH와 인증 된 주변 클러스터내의 기기는 하나의 네트워크가 된다.

네트워크 안으로 진입을 시도하려는 인증 받지 않은 기기에 대한 인증뿐만 아니라 TTI로부터 인증 받은 기기도 정당한 사용자라는 것을 증명할 수 있는 절차를 제안한다.

4.3 상호 인증

[그림 2]에서 하나의 클러스터에 진입하려는 차량 C는 상호 간 안전한 통신을 위하여 등록하여야 한다. 모든 기기는 통신을 위하여 인증서를 발급 받아 TTI에 등록을 해야 한다.

- 1. 차량 C가 클러스터 A에 진입을 하기 위해 차량 B에게 연결을 요청하고 자신의 인증서를 전송한다.
- 2. 요청을 받은 차량 B는 CH인 차량 A에게 차량 C에 대한 인증을 요청하고 차량 C에 대한 인증서를 전송한다.
- 3. 차량 A는 TTI에게 차량 C에 대한 정보를 전송한다.
- 4. TTI는 자신의 서버에서 차량 C에 대한 인증서값을 찾아 차량 A에게 전송한다.
- 5. 차량 A는 차량 B로부터 받은 값과 TTI로부터 받은 값을 비교한 후 차량 C가 정당한 사용자이면 접속 승인 메시지와 자신의 인증서 값을 차량 B에게 전송한다.
- 6. 차량 B는 차량 A로부터 받은 정보를 확인하여 자신의 인증서 값을 차량 C에게 전송한다.
- 7. 차량 C는 차량 B에게 받은 차량 A와 차량 B의 정보를 확인하고 이들의 정보와 자신의 인증서 값을 TTI에게 전송한다.
- 8. TTI는 받은 정보를 확인하여 차량 C에게 차량 A와 차량 B가 정당한 사용자임을 알려준다.



[Fig. 2] New Device Entry

4.4 검증 결과

클러스터내로 진입하려는 기기와 클러스터 내의 기기와 인증 시 신뢰 할 수 있는 인증기관의 도움을 받아 상호 인증을 받을 수 있다.

위의 스마트폰 인증 기법에서와 마찬가지로 공격자가 기기와의 통신과정 중에 인증정보를 얻음으로써 접속을 요청한 사용자 대신에 M2M 기기와의 통신을 수행하여 사용자 정보를 수집, 도용, 변조, 삭제의 가능성을 없앴다.

요청한 기기와 요청 받은 기기 모두 서버로부터 인증을 받도록 함으로서 정당한 사용자임을 알 수 있게 하였으며, 상호 인증을 통해 위장공격에 안전한 통신을 제공할 수 있다.

5. 결론

M2M 분야인 텔레매틱스를 중심으로 차량 네트워크 보안의 취약성을 알아보고 차량과 이동통신 기술의 융합으로 인해 생성될 수 있는 새로운 비즈니스 모델을 제시해 보았다. 또한, 이동통신망 기술의 발전으로 사용자와 차량의 통신 중에 발생 될 수 있는 보안 취약성을 살펴보았으며, 이 중 사용자와 차량 내 기기의 인증 취약성 공격에 대한 해결책을 제시하였다.

M2M 기기에서 정보를 수집할 때 텔레매틱스 사업자로부터 데이터를 전송 받는 방법 외에도 도로상에 있는 주변 차량으로부터 정보를 수집하는 방법이 있다. 이 경우 주변 차량이 정당한 차량인지의 인증 여부가 중요하다.

본 논문에서 제시한 방법은 사용자의 스마트폰, 차량 내 M2M기기, 제 3기관 모두가 상호 인증을 받음으로써 허가받지 않은 사용자로부터의 위장 공격을 예방 할 수 있다.

REFERENCES

[1] Seong-Gwon Yeo, Keun-Ho Lee, “A Security Survey in Telematics”, Journal of Korea Convergence Society, 2011.

[2] Keun-Ho Lee, “Analysis of Security Threat in Machine to Machine Communication”, Journal of The Korea Academia-Industrial Cooperation Society, Vol. 11, No. 1, pp. 416-419, 2010.

[3] Keun-Ho Lee, “Analysis of Security Threat in Machine to Machine Communication”, Journal of The Korea Academia-Industrial Cooperation Society, Vol. 11, No. 1, pp. 416-419, 2010.

[4] Yu-chang Kim, “The Trend of Technology and Prospect of M2M”, Telit Korea, p. 66, 2009.

[5] Seong-il Park "M2M Terminal in Mobile Communication Network", Journal of Information Science, Vol. 28, No. 9 pp. 40-43, 2010.

[6] Sang-u Kang, Se-jin Park, "Security Enhan-cement method design in VANET using Authenticated Boot of TPM", Journal of Korea Computer Congress, Vol. 36, No. 1(D), 2009.
[7] Douceur, J.: The Sybil Attack. In: First Intrnational Workshop on Peer-to-Peer Systems, March 2002, pp. 251-260, 2002.
[8] Gab-Sang Ryu, Keun-Ho Lee "Authentication based on Cluster in Machine to Machine", Journal of Korea Knowledge Information Technology Society, Vol. 5, No. 6, 2010.

저자소개

여 성 권(Seong-Gwon Yeo) **[학생회원]**

· 2006년 3월 : 백석대학교 입학
· 2012년 2월 : 백석대학교 졸업

<관심분야> : M2M, 이동통신 보안, 텔레매틱스

이 근 호(Keun-Ho Lee) **[종신회원]**

· 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
· 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
· 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 전임강사
· 2010년 9월 ~ 현재 : 백석대학교 쿰인성개발원 팀장

<관심분야> : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호