M2M(Machine to Machine) 통신에서의 보안 위협 분석

이근호*
*백석대학교 정보통신학부
e-mail:root1004@bu.ac.kr

Analysis of Security Threat in Machine to Machine Communication

Keun-Ho Lee*
*Division of Information and Communication Information
BaekSeok University

요 약

IT관련 제품(데스크톱, 노트북, 스마트폰 등)과 자동차, 선박, 자판기 등 기계(Machine)관련 제품과의 융합이 이뤄지고 있으며 각 장비간의 통합 융합으로 변화됨에 따라 네트워크 시스템과 S/W에 대한 보호가 더욱 어려워지고 있는 상황이다. 이러한 문제는 산업계 내에서 다양한 그룹의 사용자들이 다양한 장비를 사용하므로 더 복잡해지며, 결국에는 수많은 기계장치의 사용자 수준에 따라 다른 수준의 보안이 필요하게 된다. 본 논문에서는 차세대 이동통신의 한분야인 M2M(Mahcine to Machine) 통신에 대한 동향 소개와 M2M의 보안 위협요소 분석을 통한 키관리 기법과 Threshold 암호 기법을 소개한다.

1. 서론

유비쿼터스라는 개념이 제시되면서 언제어디서나 원하는 정보를 쉽게 얻을 수 있는 개념이 우리 생활에까지 파고들면서 유비쿼터스 관련 산업이 크게 활성화되고 있다. 유비쿼터스로의 발전단계를 보면 단순 가전제품간의 융합에서 다양한 Device간의 융합으로 새로운 서비스가 제공되고 있으며, 이런 Device가 기계간의 M2M(Machie to Machine) 환경으로 산업간의 융합으로 변화되고 있다. 현재 국내·외에서는 M2M 통신 기술 확보를 위한 많은 연구가 진행되고 있다. 특히 이동통신 사업자와 단말 제조업체간에 신규 Biz Model 발굴 협력을 통해 M2M 사업을 본격화 하고 있다. 3GPP, WWRF, ITU-T, 802.16m 등 4G 차세대 네트워크에 대한 연구가 세계적으로 활발하게 진행되고 있으며, Device간에 융합(Convergence)에 따른 새로운 Biz Model 발굴이 이뤄지고 있다. 4G 네트워크에서는 융합에 따른 새로운 Biz Model로 차세대 네트워크 기반에서 M2M으로 영역이 확장되고 있는 상황이다.

본 논문에서는 M2M에 대한 정의와 기술동향을 통한 구현기술, M2M에서의 보안 위협요소에 대한 분석을 통해 향후 보안 적용 분야중 키관리와 Threshold 암호기법에 대해서 살펴보고자 한다.

2. Machine to Machine Comunication

M2M은 우리 일상 생활 속에 기계들과의 관계와 기기들간의 네트워킹에 관한 개념이다. 이러한 개념은 기계들이나 기기들이 원격지에 통신망과 같은 이동통신을 통해서 자신의 데이터를 전송하는 것이다. 사람과 사물 사이의 상호작용을 통해 위치, 건강, 온도 등 다양한 데이터를 얻을 수 있다. 전기통신과 자동화 프로세서를 위한 정보 기술의 결합으로 IT 시스템과 같은 모든 기업의 유동 자산을 통합하여 부가가치를 창출하는 차세대 네트워크이다[1,3].

2.1 M2M Application 및 업체 동향

M2M은 수없이 많은 환경과 다양한 종류의 기기들을 통해서 활용되고 있다. 성공적으로 활용되고 있는 곳은 이동통신 산업의 기지국 및 중계기, 가스 송유관, MP3 다운 가능한 핸드폰, 자동판매기, 물류 및 유통을 위한 운송수단, 보안시스템, 전자 계량기의 원침검침, 게임 시스템, 가전제품 등이 있다. 이러한 다양한 곳에서의 활용을 통한 새로운 Application 들이 지속적으로 생성되고 새로운 시장의 개척을 가능하게 하고 있다. 시스템 통합업체와 서비스 제공업체가 새롭고 부가가치적인 서비스를

제공할 새로운 기회를 가지고 있다[1].

2.2 M2M 구현 기술

M2M의 구현기술은 요소기술과 망 액세스 기술로 분류할 수 있다.

요소기술에는 텔레매틱스, RFID, Software Application 으로 나눌 수 있다. 텔레매틱스는 차내 컴퓨팅 시스템의 기능을 포함하는 무선통신과 정보서비스가 통합된 형태의 차내 정보제공 시스템 및 서비스로 정의한다. RFID는 식별번호가 부여된 IC 칩을 무선 안테나와 함께 물체에 쉽게 부착하여 다양한 모양과 크기의 RFID 태그에 내장하여 무선 단말에 의하여 읽혀 네트워크에 연결된 컴퓨터에 의해 데이터처리를 한다. Software Application은 시스템 통합 산업의 분야로 확장되며, 사용자의 환경과 요구에 가장 적합한 정보시스템 구축, 운영하기 위한 컨설팅에서부터 시스템 설계, 개발, 통합, 구축, 관리, 교육, 유지 보수를 전반적으로 수행하는 산업으로 발전한다.

망 액세스 기술에는 Mobile 3G와 4G에 대한 차세대 이동통신에 대한 음성 서비스외에 대량의 데이터나 동영상을 고속으로 주고 받는 멀티미디어 서비스가 제공된다. IEEE802.11x는 무선랜 응용방식으로 적외선(Infrared) 방식, 협대역(Narrow Band) 방식, 대역확산(Spread Spectrum) 방식의 기술을 활용한다. Zigbee는 저속 전송속도를 갖는 홈오토메이션 및 데이터 네트워크를 위한 표준기술로서 버튼 하나의 동작으로 집안 어느 곳에서나 가전제품에 대한 제어를 통해 홈오토메이션 등에 적용할 수 있는 기술들이 M2M 통신의 기술로 사용되고 있다[2].

2.3 M2M 표준 동향

M2M 표준에 대해서는 이동통신 사업자의 움직임이 활발하게 진행되고 있으며, 3GPP 표준내에서 Machine 간의 통신을 촉진시키기 위한 MTC (Machine Type Communication) 그룹을 만들어 활발하게 진행하고 있다. 또한 새로운 응용 서비스 중의 하나로써 기계장치들 간의 통신을 촉진시키기 위한 요구사항들을 정리하고 발전시키기 위해 S1 그룹 3GPP Meetings에서 TR(Technical Report) 22.868(Study on facilitating machine to machine communication in 3GPP system)에 대한 연구를 시작하여 지금까지 발전시켜 왔다. MTC에 대상이 되는 장비로는 기존에 통신을 위한 목적으로 만들어진 휴대폰, 컴퓨터와 같은 통신 장비뿐 아니라 지금까지 독립된 장비였던 담배 자판기, 건강 진단 장비 그리고 차세대 전력 시스템으로 떠오르고 있는 스마트 그리드(Smart Grid)의 전력 검침 시스템 등이 있다. 사용자들은 MTC를 통해서 자신의 장비들을 모니터링하고 관리 할 수 있게 된다. 사용자들은 인터넷과 같은 통신을 통해서 자신의 장비들의 현재 상황을 모니터링하고 관리할 수 있으며, 필요에 따라서는 적절한 명령을 내려 직접 장비가 있는 곳으로 가지 않아도 효율적으로 작업을 할 수 있게 될 것이다. 이를 위해서는 외부에 사용자를 인증하고 사용자가 장비를 직접 관리하는 것과 동일한 수준의 서비스를 제공하여야 하는데 이를 위해서는 3GPP 내에 MTC을 위한 네트워크 서버가 존재하여 machine들을 관리하는 표준화가 진행 중이다.

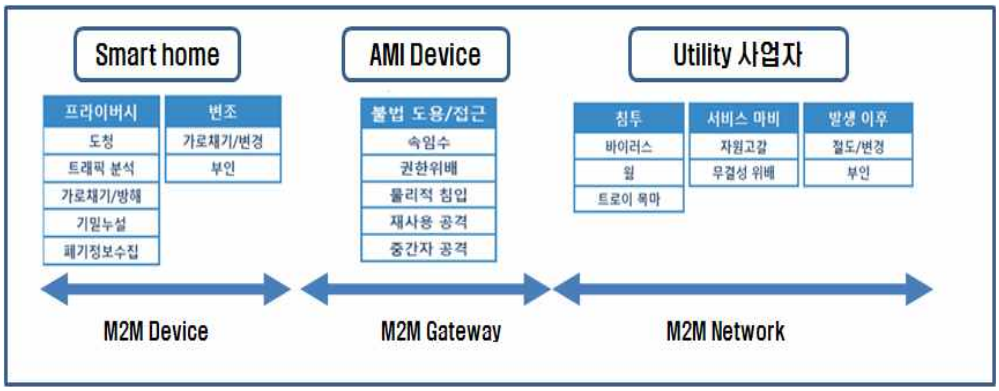
3. Machine to Machine 보안 동향

MTC가 사용될 경우 사용자는 장비가 있는 곳이 아니라 외부에서도 사용자가 소유하고 있는 장비들은 손쉽게 제어 및 관리를 할 수 있어야 한다. 이러한 시스템이 구축되기 위해서는 MTC 시스템이 기기간 망과 연결되어서 동작하되 귀중한 장비들과 장비들 안의 관리 데이터 등의 보안을 완벽하게 유지하고 제공할 수 있어야 한다. 그러나 현재까지는 TR 등에서 MTC을 이용한 사용 시나리오의 일반적인 장비의 경우 통신 가능성을 염두에 두고 설계되지 않고 보안 시스템을 탑재하고 있지 않아서 여러 가지 침입 등에 노출되어 있는 실정이다. 이러한 경우 악의적인 사용자가 MTC을 이용하여 여러 경로를 통해 장비를 임의로 제어하여 심각한 위험이 초래되며, 장비 내부에 있는 정보들이 외부에 노출될 수 있을 뿐만 아니라 장비를 이용하여 사용자의 관리 시스템에 침투하는 등의 많은 피해를 줄 수 있다. 따라서 향후 종합적이고 발전된 형태의 MTC 네트워크 구축을 위해서는 개발 단계에서부터 다양한 종류의 위협 사니리오를 분석하고 이에 따른 MTC 네트워크를 구현하는 것이 필수적이다.

MTC는 사용자의 직접적인 행동이 수반되지 않는 기계장치들 간의 데이터 통신의 한 형태로써 사용자의 직접적이고 즉각적인 행동 없이 기계들 간의 통신이 안전하게 가능하도록 해야 한다. 따라서 USIM/ISIM을 이용한 응용프로그램 등을 활용하여 원격으로 기계들을 안전하게 제어, 관리 할 수 있는 방법들과 같은 보안적인 측면이 크게 부각되고 있다.

차세대 네트워크 환경에서 M2M을 안전하게 제공하기 위한 보안 요구사항들은 다음과 같다.

- To investigate candidate security solutions those



[그림 1] M2M 환경에서의 보안 요소

allow provisioning to take place in a secure manner
- To investigate candidate signaling procedures for provisioning remote management of USIM/ISIM application in a M2M equipment
- To identify what functionality of the current USIM/ISIM application has to be covered by remote management of the USIM/ISIM application
- To identify what other functionality that may need to be added due to the new USIM/ISIM application provisioning method
- The study may identify principle requirements for protected storage and the execution environment

4. Machine to Machine 보안 기술

M2M의 특징을 기반으로 예상되는 보안 위협에 대처할 수 있는 위협 시나리오는 그림 1의 M2M Device, Gateway, Network에서의 기준을 통해서 보안 위협 요소를 살펴보고자 한다.

4.1 M2M 보안 요소

M2M 네트워크의 빈번한 형태 변화 특성과 함께 무선 채널을 사용하는 구조적으로 취약한 보안 위협 요소가 존재하므로 M2M 네트워크 보안 위협요소에 대한 안정적이고 효율적인 극복 방안이 요구된다. 보안은 M2M 네트워크를 구성함에 있어 가장 중요한 이슈 중의 하나이며, 유용성(Availability), 기밀성(Confidentiality), 무결성(Integrity), 인증(Authentication), 부인봉쇄(Non-repudiation)와 같은 요구들을 충분히 만족할 수 있는 프로토콜이 요구되어 지고 이에 부합하는 내용의 보안 요소기술 개발이 필요하다. M2M Device간에 도청, 가로채기, 부인과 관련된 프라이버시 및 변조 위협요소가 있다. M2M Gateway에서는 불법 도용 및 접근을 통한 권한 위배, 물리적 침입, 재사용 공격, 중간자 공격의 위협요소가 있다. M2M 네트워크에서의 보안 위협 요소로는 침투, 서비스 마비에 대한 바이러스, 웜, 트로이목마, 자원고갈 등의 위협이 존재한다.

4.2 M2M 보안 고려 사항

무선 링크를 사용하는 것과, 제한된 자원, 물리적인 자원의 제한, 빈번하게 형태가 바뀌는 네트워크의 특성을 감안할 때 다음과 같은 상황에 충분한 고려사항이 필요하다.
- 무선 링크의 사용으로 인한 도청(eavesdropping)
  : 인가되지 않은 비밀 정보 접근, 기밀성 훼손
- 네트워크 외부 적의 공격(active attacks)
  : 메시지 삭제, 변조
- 변질된 이동 Machine(compromised node)로부터 오는 부적절한 정보 및 공격
- 빈번한 네트워크 형태의 변화를 극복할 수 있는 라우팅 프로토콜

위에서 언급한 바와 같이 각 이동 Machine과 각 Machine간의 클러스터(M2M 근접통신시)의 이동 Machine에 대한 관리의 책임을 지고 있는 클러스터 헤드(CH: Cluster Head)와 신뢰할 수 있는 인증 메커니즘을 통해 네트워크 밖의 외부 적의 공격이나 인가되지 않은(unauthorized node) 사용으로 네트워크를 보호할 뿐 아니라, 변질된 Machine이나 심지어 CH까지 변질되었을 경우에도 이를 발견하고, 변질된 Machine을 배제하고서도 효율적인 라우팅과 안정성을 제공할 수 있는 알고리즘이 요구된다.

4.3 키 관리(Key Management Service)

공개키 암호기법의 우수성을 이용하여 라우팅 정보와 데이터 트래픽에 대한 정보를 보호한다. 클러스

터 키는 모든 클러스터에 대해 유일하게 존재하고 클러스터에 속하는 모든 이동 Machine에게 분배된다. 이 키는 CH 에 의해 생성되어 시스템 공개키로 암호화되고 클러스터 멤버에게 분배된다. 각 이동 Machine은 공개/개인키 쌍을 가지고 있으며, 키 관리를 위한 CA(Certification Authority)를 두어 키의 바인딩과 주기적인 갱신을 담당한다.

CA는 공개/비밀 키 쌍을 가지고 있으며, 공개키는 다른 모든 Machine 에게 분배되고, 비밀키를 가지고 인증서를 서명 분배한다. 어떤 한 이동 Machine이 더 이상 신뢰할 수 없거나 네트워크 영역을 벗어나게 되면 그 Machine의 공개키는 폐지된다.

4.4 Threshold 암호화 기법

CA는 전체 네트워크에 대한 보안을 책임지는 개체로서 외부 적의 집중적인 공격의 대상이 되므로, 만일 하나의 CA를 사용하고자 한다면 집중된 외부 공격으로 인하여 CA가 정상적인 역할을 수행하지 못하거나 혹은 적에게 변질되어 악용될 경우 상당히 심각한 문제를 야기시킬 수 있다. CA를 이용한 서비스가 사용 가능하지 못하다면, 이동 machine들은 다른 이동 machine들의 현재 공개 키를 획득할 수 없고, 다른 이동 machine들과의 안전한 교신이 불가능하게 된다. 만일 CA가 적에 의해 변질되어 비밀키를 적에게 누설 한다면 적은 그 비밀 키를 이용하여 비밀키로 거짓된 인증서를 발행할 수 있게 된다. 이러한 문제점을 해결하기 위하여 Threshold 기법을 이용하여 시스템 키 관리 서비스의 책임을 각 CH 에게 분할해서 분배하고, (n, t+1) Threshold Cryptography를 이용하여 2-tier 계층 구조의 중요한 요소인 각 CH의 신뢰 여부를 확인하며, 클러스터 헤드가 변질된 경우 하위 계층에 속한 이동 machine 중 새로운 클러스터 헤드 역할을 수행할 노드를 신속하게 재생성하여 네트워크를 구성한다.

5. 결론

차세대 네트워크 기술의 한 분야인 M2M에 대한 향상된 기술력을 확보하기 위한 이동 통신에서의 M2M 통신기술 분야의 업체동향을 통한 기술 표준 동향을 소개하였다. 기술표준에 따른 요소기술을 통해 발전되어야할 M2M 필요 기술을 통한 안정성이 보장되는 M2M 시스템 구축이 필요하다. M2M 시스템에서의 존재 가능한 보안 요소를 살펴보았고, 보안요소를 기반으로 고려해야 할 사항들과 키를 관리하는 방법에 대한 제안을 통해 좀더 보안 위협 요소 관점에서 안정성을 제공할 수 있는 방법을 소개하였다. Threshold 기법을 통한 시스템키 관리의 방법을 제안하여 향후 M2M 보안 위협에 대한 안정성을 살펴보았다. 보안 방법들을 좀 더 활용할 수 있는 분야를 구체적으로 도출하고 이를 만족시킬 수 있는 보안 요소 기술리스트에 대한 추가적인 연구가 필요하다. 또한 예상되는 위협 요소 이외의 다른 위협이 존재 할 수 있으므로, 추후 보안 위협을 찾을 수 있는 방법론도 함께 제시하고 도출된 요구사항들을 종합하여 M2M을 설계하는데 필수적인 기술에 대한 연구 진행이 필요하다.

참고문헌

[1] 한국정보산업연합회 조사연구팀, “M2M 기술 및 비즈니스 사례,1 :M2M 비즈니스 개요”,한국정보산업연합회 정보산업 통권 제233호, pp. 94-98, 2005.

[2] 한국정보산업연합회 조사연구팀, “M2M 기술 및 비즈니스 사례2 :M2M 구현기술”,한국정보산업연합회 정보산업 통권 제233호, pp. 68-72, 2005.

[3] 김유창, “기기 간 통신(M2M0의 기술 동향과 전망”, 월간전자부품 2009년 7월호, pp. 66-71, 2009.

[4] Dong-Hoon Kim, Jun-Yeob Song, Seuk-Keun Cha, "Introduction of Case Study for M2M Intelligent Machine Tools", 2009 IEEE International Symposium on Assembly and Manufacturing, pp 408-411, 2009

[5] Inhyok Cha, Yogendra Shah, Andreas U. Schmidt, Andreas Leicher, Michael Victor Meyerstein, "Trust in M2M Communication-Addressing New Security Threats", Wireless World Research Forum, pp 69-75, 2009