M2M에서 클러스터 기반의 인증

류갑상*, 이근호**

요약

IT 발전에 따라 많은 장치간의 통신과 네트워킹의 수용이 이뤄지고 있다. 기계간의 통신을 위한 M2M(Machine to Machine) 사업이 급격하게 발전되어 지고 있다. M2M 통신은 무선통신에서 차후 개척분야의 하나로 여겨지고 있다. 본 논문에서 M2M에서 인증 기법을 제공하기 위해서 클러스터링 기법 기반의 안전한 클러스터를 제안하였다. 그리고 M2M 클러스터 구조 기반에 대한 보안 위협요소를 자세하게 표현하였다. 제안한 절차는 ACM(Authentication based on Cluster in M2M)이라 명하고, 클러스터내에서 기계간에 상호 신뢰 관계를 위한 인증 절차를 설계하였다.

Authentication based on Cluster in Machine to Machine

Gab-Sang Ryu*, Keun-Ho Lee**

ABSTRACT

As the developing of the information technology, more and more devices are with the capacity of communication and networking. The M2M(Machine to Machine) businesses which communicate with the Machines have been developing rapidly. The M2M communication is viewed as one of the next frontiers in wireless communications. In this paper, we propose a secure cluster based on a clustering scheme that provides an authentication scheme in M2M. We present detailed security threats against M2M cluster architecture. Our proposed procedure, called ACM(Authentication based on Clusters in M2M), designs an authentication procedure that relies on mutual trust between machines in clusters.

Key Words : M2M(Machine to Machine), Authentication, Cluster, Information Security, Information Technology

* 동신대학교 컴퓨터학과(✉gsryu@dsu.ac.kr)
** 백석대학교 정보보호전공
· 제1저자(First Author) : 류갑상 · 교신저자(Correspondent Author) : 이근호
· 접수일(2010년 10월 20일), 수정일(1차 : 2010년 11월 19일), 게재확정일(2010년 11월 23일)

Ⅰ.

최근 IT분야의 급격한 발전은 유비쿼터스 환경으로 빠르게 진화가 이뤄지고 있다. 유비쿼터스 환경은 IT 분야를 기반으로 한 융합분야의 발전과 함께 많은 새로운 분야의 연구가 이뤄지는 계기가 되었다. 그중에서 장치와 기계간의 통신을 위한 M2M (Machine to Machine)은 이동통신 사업자와 연구자들간의 주요 기술 분야로 대두되고 있다.

M2M은 Machine to Machine, mobile to Machine, 그리고 Machine to mobile의 통신을 의미한다. M2M은 기계들과 우리의 일상생활 속에 널리 퍼져있는 기기장비간의 네트워킹에 관한 개념이다.

M2M 통신은 기기의 기구들을 컴퓨터의 본체에서부터 일상적인 전자제품들까지 연결해 사용이 가능하도록 해 줄 것이다. 예를 들면, 집안에서의 가전제품과 자동차등의 운송수단을 비롯한 사람이 거주하는 건물 등에서 사용된다. 이 개념은 기계들이나 기기들이 원격지에서 이동통신과 전송매체를 통해서 자신이 원하는 데이터를 전송하는 것이 가능하도록 하는 것이다.

현재의 M2M 통신 개념은 GSM망을 넘어 다양한 유무선 네트워크를 활용하는 개념으로 확장되어가고 있다. 이러한 개념은 기계들이나 기기들이 원격지에 통신망과 같은 이동 통신을 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 IT시스템과 같은 모든 기업의 유동 자산을 통합하여 부가가치를 창출하는 차세대 네트워크이다 [1,2].

본 논문에서는 M2M에 대한 정의와 현재 진행되는 표준에 대해서 살펴보고, 클러스터링 기법에 대한 설명과 M2M에서 발생가능한 보안 위협요소에 대한 분석을 통해 클러스터기반의 인증에 대한 기법을 제안한다.

Ⅱ. ᵩ N

2.1 M2M ḱ

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 장치간의 융합으로 새로운 서비스가 제공되고 있으며, 이런 장치가 기계간의 M2M 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, 장치간에 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.

2.2 ḱ

클러스터링은 네트워크에서 잦은 형태의 변화에 적용하기 위해서 사용하는 기법이다. 클러스터내에 일반 기계나 기기들을 관리하고 인증해주는 클러스터 헤드(CH: Cluster Head)가 존재하여 다른 클러스터에서 클러스터내로 진입시 CH간에 인증을 통해 상호 신뢰성을 보장해주는 기법이다. 그림 1은 노드 2, 4, 9 노드가 각 클러스터내의 CH의 역할을 수행한다. 3 노드의 경우는 게이트웨이 역할을 수행한다. 노드 넘버의 경우는 각 장치와 기계를 나태내며, 노드에 의한 가중치를 노드번호 옆에()표기하여, 가중치의 비중에 따라 CH로 선출된다[4].

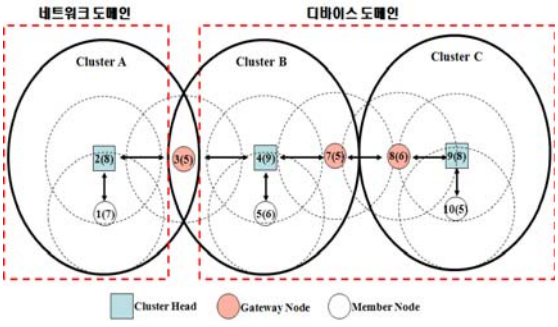

그림 1. 클러스터 구조
Fig. 1 Architecture of the Cluster

2.3 M2M

M2M에서의 네트워크는 기기나 기계간의 이동으로 인한 빈번한 형태 변화와 무선 채널을 사용하는 구조적인 취약점을 가지고 있다. 잦은 네트워크의 변화와 무선채널의 위험에 대한 안정적이고 효율적인 해결 방안이 요구된다. 안정적인 M2M 네트워크를 구성함에 있어 가장 중요한 이슈 중의 하나는 보안관련 요소이다. 보안의 특성을 통한 가용성(Availability), 기밀성(Confidentiality), 무결성(Integrity), 인증(Authentication), 부인봉쇄(Non-repudiation)와 같은 요구들을 충분히 만족할 수 있는 프로토콜이 요구되어 지고 이에 부합하는 보안 요소기술 개발이 필요하다.

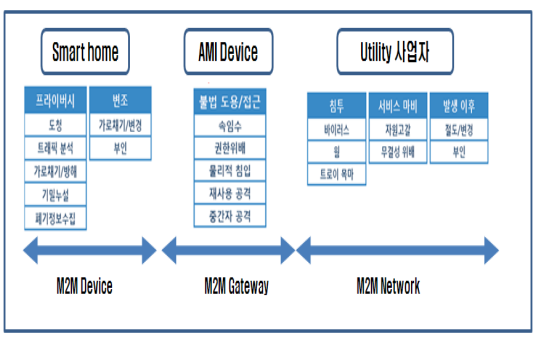

그림 2. M2M에서의 보안 요소
Fig. 2 Security Factor in M2M

그림 2를 기준으로 하여 M2M에서의 장치의 위협에는 기기간의 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 존재한다. M2M 네트워크에서 불법침투, 서비스 거부를 통한 마비, 바이러스, 웜, 트로이목마, 자원고갈 등의 보안 위협 요소가 있다[3].

무선 채널을 통한 링크 사용과 제한된 자원, 물리적인 자원의 제한, 빈번하게 형태가 바뀌는 네트워크의 특성을 감안하여 다음의 고려사항을 살펴보아야 한다.

- 무선 링크의 사용으로 인한 도청(eavesdropping)
: 인가되지 않은 비밀 정보 접근, 기밀성 훼손
- 네트워크 외부 적의 공격(active attacks)
: 메시지 삭제, 변조
- 변질된 이동 기계(compromised node)로부터 오는 부적절한 정보 및 공격
- 빈번한 네트워크 형태의 변화를 극복할 수 있는 라우팅 프로토콜

위에서 언급한 바와 같이 각 이동 기계와 각 기계간의 네트워크를 클러스터(M2M 근접통신시)기반으로 구성하여 이동 기계에 대한 관리효율성을 높일 수 있도록 네트워크를 구성할 필요가 있다. 클러스터 기반으로 네트워크를 구성시 클러스터 내의 기계들에 대한 책임과 관리를 위한 클러스터 헤드(CH: Cluster Head)를 선출하여 신뢰할 수 있는 인증 메커니즘을 통해 네트워크 밖의 외부 적의 공격이나 인가되지 않은(unauthorized node) 사용으로 네트워크를 보호해야 한다. 또한 변질된 기계이나 심지어 CH까지 변질되었을 경우에도 이를 발견하고, 변질된 기계를 배제하고서도 효율적인 기계간의 통신이 이뤄질 수 있도록 안정성을 제공해야한다[1,2,3].

M2M에서의 기밀성, 무결성, 게이트웨이 및 서버 인증, 프라이버시보호 및 추적성, 장치 인증, 시스템 가용성 등의 보안의 조건을 위해서는 다음의 보안 위

협을 고려해야 한다.

- 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.

- 중간자(man-in-the-middle) 공격을 통한 데이터의 불법 변경 및 삭제, 위조된 데이터의 삽입 등에 대응하기 위한 무결성 보장이 필요하다.

- M2M에서 장치에 대한 불법 도용 및 용도 변경이 상대적으로 쉬워 물리적 보안이 허술한 장소에 배치됨에도 불구하고 자본 절약, 기능성, 유동성 및 개발 용이성의 장점으로 인해 개방형 인터페이스를 지닌 플랫폼에서 구현이 가능하고, 장치에 악성 소프트웨어 삽입 또는 장치 변경으로 인해 악성 장치 및 게이트웨이로 용도가 변경될 수 있음으로 M2M 장치의 무결성 검증 메커니즘이 필요하다.

- 서비스 거부공격(DoS)은 시스템의 가용성 및 생산성을 훼손함으로써 시스템 자원과 정보에 대한 접근 능력을 감소시킬 수 있다. 따라서 M2M 통신 환경에서도 주체 또는 장치들의 정보 접근 능력을 침해하지 않도록 시스템 가용성을 보장 할 수 있는 보안 메커니즘이 필요하다.

- 사용자의 개인정보 수집 및 도용은 M2M 장치가 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 장치는 장치의 위치정보 노출로 인해 장치 및 장치 소유자의 위치나 이동 경로가 노출될 가능성이 존재한다. 따라서 이동성을 제공하면서 추적 불가능성을 제공할 수 있는 보안 메커니즘이 필요하다.

- M2M에서 장치가 위장하여 공격하는 경우에는 서버에 전송되는 데이터를 수집하기 전에 데이터가 올바르고 정당한 장치 또는 게이트웨이로부터 전송되었는지 확인하는 검증 절차가 필요하다. 반대로 장치의 경우에도 수신되는 데이터가 올바르고 정당한 게이트웨이 또는 서버로부터 전송 되었는지 확인하는 검증 절차가 필요하다. 따라서 M2M 환경에서는 자신과 통신하는 상대방 개체에 대한 정당한 개체인지를 검증하는 상호 인증 절차가 반드시 필요하다[1,2,3].

III. ḱ

M2M에서 장치간의 인증을 위해서 M2M 장치를 클러스터 기반에서 인증하기 위한 절차를 제안하였다. M2M의 통신 환경은 대부분 무선으로 이루어져 있고 무선을 이용하기 위해서는 신뢰할 수 있는 기기간의 접속이 필요하며, 신뢰할 수 있도록 클러스터내에서 ClusterHead(CH)를 통해서 기계간에 상호 인증이 이루어져 장비간의 안전한 통신을 할 수 있다.

3.1 ㅛ

본 논문의 시나리오는 여러 산업분야에서 사용할 수 있지만 그중에서도 지능형 자동차를 통한 VANETs(Vehicular Ad-hoc NETworks)분야에서 차량간의 클러스터 구성을 위한 기반으로 구성하고자 한다.

M2M 기반 구조에서 그림 2에서 장치간의 통신하는 부분을 두 영역(장치, Network)의 그림 1과 같이 구성하고, 장치 도메인 내의 다른 장치 간의 그룹으로 2개의 클러스터 구조로 형상을 구성한다. 그림 1의 네트워크 도메인의 ClusterHead(CH) 노드 2는 네트워크상에 존재하는 인증서버로서 모든 장치에 대한 등록 및 관리를 담당한다고 가정한다. CH가 클러스터내에 가중치를 기반으로 가장 큰값

을 갖는 노드를 CH로 선정하며, 가중치의 경우는 CH로서의 역할을 수행할 수 있는 장치나 기계로 구성한다. 가중치의 조건에는 남은 에너지량과 인증을 위한 인증서 관리 등을 다룰 수 있는 기능을 포함하고 있다. CH의 역할을 하는 장치가 인증서를 이용한 프로토콜로 위장공격에 안전하다고 가정한다. 게이트웨이의 경우는 외부 네트워크나 다른 클러스터의 구성으로부터 연결이 필요할 때 기기로 위장 시 사용자의 비밀 정보를 알아내기 위한 공격을 할 수 없으며, 위장된 기기가 정당한 사용자로 위장하여 재전송 공격 등이 가능하지 않아야 한다.

기존의 M2M 인증은 기기간의 통신을 위해서 인증서버에 통신을 요청한 기기에 대해서만 인증과정을 거친다. 통신을 요청한 기기에 대해서만 정당한 사용자인지 확인하게 되면 통신에 응답하는 기기가 정당한 기기인척 위장한 기기와 통신이 성립될 수 도 있다. 이럴 경우 정당한 기기인척 위장한 기기와의 통신으로 통신을 요청한 정당한 기기는 위험에 노출될 수 있다.

이 논문에서 제안하는 매커니즘은 이를 해결하기 위한 대안으로 기존 M2M에서 통신요청 기기에 대한 인증뿐만 아니라 통신에 응답하는 기기도 인증서버로부터 인증을 받은 CH에 의해서 통신하는 두 기기 간의 신뢰성과 안전성을 제공한다.

요즘 무선은 사용자가 쉽게 이용 가능하게 되어 있고 이에 따라 무선을 사용하는 사용자가 늘어가고 있다. 무선에서의 안전한 인증을 위해 M2M 인증서버의 인증서를 이용한 방법으로서 인증서버로부터 통신 요청 기기뿐만 아니라 요청에 응하는 기기도 인증 받아 좀 더 신뢰성 있고 안전한 통신이 가능하다.

3.2 تي

M2M에서 장치 도메인내의 클러스터 C에 새로운 장치 노드 11이 들어오는 그림 3의 경우처럼 새로운 장치가 클러스터에 들어오게 되면 노드 11이 안전하게 사용 될 수 있도록 등록하여야 한다. 기존 WPA 프로토콜은 인증서를 도입한 것으로 모든 기계들은 인증서를 발급 받아 인증서버에 등록을 해야하는 특징을 가지고 있다. CH9와 새로운 노드 11의 경우 안전한 통신을 하기 위해서 인증서버 CH2에 대한 인증서 요구가 필요하며 절차는 그림 4와 같이 아래의 절차적인 방법을 통한 인증이 중요하다.

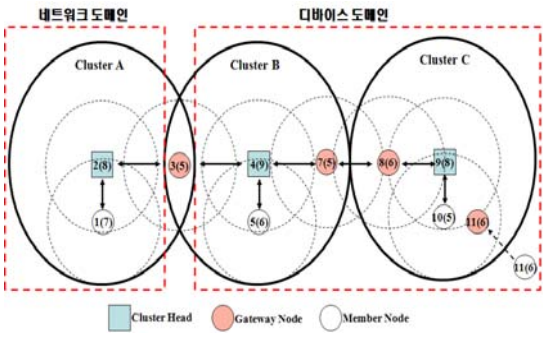

그림 3. 장치 도메인에 새로운 장치 진입
Fig. 3 Entry new 장치 in 장치 domain

- 1. 장치 노드 11이 CH 9 에게 연결을 요청하면 WAP의 모드 중 하나인 EAP가 시작된다.

- 2. 연결 요청을 받은 CH 9는 네트워크 도메인에 있는 인증서버 역할을 하는 CH 2에 연결하기 위해서 CH 4에게 노드 11에 대한 인증을 요청하게 된다.

- 3. CH 4는 CH 2에게 노드 11의 인증을 요구한다.

- 4,5. CH 2 인증서버는 상호 인증을 위해 CH 4와 CH 9 모두에게 신분확인을 요구한다.

- 6,7. CH 9와 CH 2는 자신의 인증 정보를 서버에게 보낸다.

- 8. CH 2 서버는 CH 4에 인증서값을(패스워드)를 요구한다.

- 9. CH2 서버는 CH 9에게 노드 11의 인증서값을 요구한다.

- 10. CH 4는 인증서 값을 CH 2서버에게 전송한다.

- 11. CH 9는 노드 11의 인증서 값을 CH 2 서버에게 전송한다.

- 12, 13. CH 2 서버는 CH 2와 CH 9가 정당한 사용자임을 확인하면 확인된 정보와 함께 EAP-TLS를 이용해 통신에 사용될 WEP 키 값을 보낸다.

- 14. 서버에게 받은 WEP 키를 이용해 노드 11과 CH 9는 클러스터 C와 B에서 안전하게 통신을 한다. 이때 보낸 WEP KEY 값은 두 장치의 연결이 종료될 때까지만 사용되며 다음 연결 시에는 새로운 KEY 값을 할당 받아 통신한다.

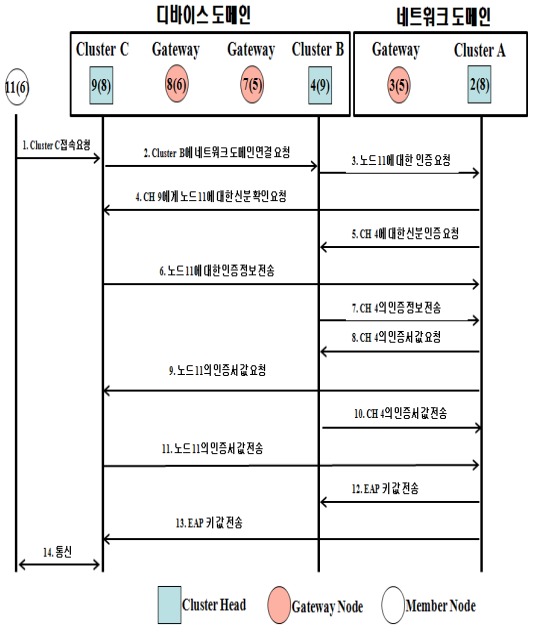

그림 4. 장치 도메인에 새로운 장치 인증
Fig. 4 Authentication new device in device domain

3.3 ‹e ä¸

기존의 Cluster 이전에 새롭게 집인하는 장치에 대해서는 WPA 프로토콜은 TKIP를 통한 무결성 제공과 EAP를 이용한 인증을 제공한다. 인증 서버가 통신을 요청한 기기에 대해서만 인증을 제공을 하고 통신 대상 기기에 대한 인증을 제공하지 않아 위장공격에 취약하다.

반면 이 논문에서 제안한 ACM(Authentication based on Clusters in M2M) 상호인증 매커니즘은 기존의 인증을 그대로 유지하되 통신을 요청한 기기와 통신 대상 기기 모두 서버로부터 인증을 받도록 함으로서 요청 기기가 정당한 지와 대상 기기가 정당한 사용자 인지 모두 인증을 받기 때문에 상호 인증을 통해 위장공격에 안전한 통신을 제공할 수 있다. 또한 이러한 상호 인증 과정을 통해 서버로부터 통신에 사용될 키를 제공받아 사용하므로 기존의 TKIP를 이용한 무결성을 좀 더 신뢰할 수 있게 한다.

표. 1 기존 M2M와 비교
Table 1. Compare of the exist M2M

	무결성	인증	위장공격
Exist M2M	○	○	X
ACM	○	○	○

IV. ä

M2M 간의 통신은 보안에 취약하며 유선과 무선 상에서 나타날 수 있는 보안 취약점이 모두 M2M의 취약점이 될 수 있다. 이에 M2M 간의 안전한 통신을 위해서 기기간의 신뢰할 수 있는 상호 인증이 필요하다. 장치의 종류에 관계없이 서로 안전하게 통신 가능한 다양한 M2M 인증 프로토콜