사물인터넷 시대의 사이버 물리 시스템 보안 기술 동향

김 영 식
조선대학교 정보통신공학과

Ⅰ. 서 론

정보통신 기술이 발전하면서 향후 2020년이 되면 최소 260억 개 이상의 사물들이 인터넷에 연결될 것으로 전망되고 있다. 2013년 가트너의 예상에 따르면 2020년까지 1조 9천억 달러 이상의 부가 가치가 사물인터넷(Internet of Things)으로부터 창출될 것으로 전망된다. 이때에는 기존의 개인용 컴퓨터나 휴대용 스마트기기 뿐만 아니라 다양한 웨어러블 기기, 센서, 구동기(actuator)들이 네트워크에 연결되어 복합적인 정보 처리, 분석, 저장이 가능할 것으로 전망된다. 더 나아가 다양한 산업용 네트워크도 사물인터넷과 연결 및 연동될 것이다.

여러 요소 기술이 통합된 사물인터넷에서는 대규모 보안 사고가 일어날 수 있는 최적의 환경을 제공할 것으로 우려되고 있다.

실제 기존 휴대폰 수요의 포화, 통신 및 솔루션 시장의 성장, 스마트 그리드 2030과 같은 그린 ICT 정책 추진 및 사회 안전망에 대한 수요 증대, 그리고 무엇보다 다양한 무선통신 기술의 등장 및 발전과 그에 따른 모듈의 가격 하락이 사물인터넷 시대를 뒷받침할 것으로 보고 있다. 특히 스마트폰을 뒤이은 차기 주력 IT 주요 성장 동력으로 "사물인터넷"이 주목을 받고 있으며, 전 세계 이동통신사 및 제조업체 중심으로 M2M/IoT 사업 모델 발굴 및 새로운 시장 창출을 위한 노력이 다방면으로 이루어지고 있다[1].

사물인터넷은 네트워크 연결성 및 상호작용 확대를 통해서 사용자 편의성을 극대화하고 새로운 서비스 및 부가가치 창출이 가능하도록 만들어주지만, 동시에 새로운 보안 문제들이 더 큰 규모로 일어날 수 있는 최적의 환경을 제공해 줄 것으로 우려되고 있다. 무엇보다 사물인터

넷은 기존의 여러 요소 기술이 통합되어 서비스를 구성하는데, 각 요소 기술 자체의 보안 취약성의 결합되어 새로운 취약성이 발생할 수 있다. 2014년 HP사의 조사에 의하면 현재 IoT 기기의 70%가 암호화되지 않은 네트워크로 데이터를 전송하고 있으며, 2014년 가트너에 따르면 22%의 기업이 IoT로 인해 새로운 위협에 직면할 것으로 보고 있다. 특히 현재 사용 중인 많은 산업 네트워크들이 현재와 같이 보안문제에 대비가 부족한 상태로 사물인터넷 기기를 통해 인터넷에 연결이 되면 편의성 및 효율 증대 못지않게, 국가적 재난을 초래할 수 있는 보안 사고를 일으킬 가능성이 매우 높아진다. 이러한 우려는 사물인터넷이 확대되기 위해서는 반드시 해소되어야 하는 것으로 보고 있다[2].

이 논문에서는 사물 인터넷 보안을 위한 필수적인 요구사항들 및 연구 동향에 대해서 살펴보고자 한다. 또한 사이버 물리 시스템(cyber physical system)을 중심으로 보다 세부적인 보안 특성 및 방향에 대해서 고찰해 보고자 한다. 이를 위해 제2장에서는 사물인터넷 기술의 기본 개요에 대해 설명하고 제3장에서는 그에 따른 보안 요구사항들을 살펴본다. 제4장에서는 사이버물리시스템을 중심으로 보안 이슈 및 연구 현황에 대해서 살펴보고 마지막에 결론을 맺을 것이다.

사물인터넷은 "상호 작용 가능한 정보통신 기술에 근거한 현존하는 혹은 진화된 (물리적 혹은 가상적) 사물들을 서로 연결함 으로써 보다 발전된 서비스가 가능하도록 만들어 주는 정보 사회를 위한 범세계적 기반시설"로 정의된다.

Ⅱ. 사물인터넷 기술 개요

사물인터넷의 세부 요소 기술들은 현재에도 지속적으로 발전 및 진화하고 있기 때문에, 이 절에서는 먼저 사물인터넷의 대략적인 특징에 대해서 살펴보고자 한다.

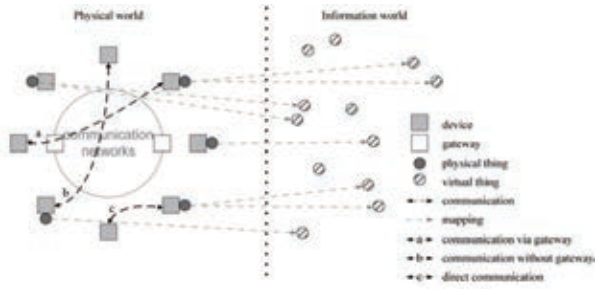
사물인터넷에서는 기존의 네트워크에 연결된 장치들과 함께, 개인용, 가정용 및 산업용 장치들, 공공 인프라용 장비, 헬스케어 장비 등 네트워크에 연결되는 모든 단위 장치들을 통틀어서 사물로 부른다. 2008년에 이미 네트워크에 연결된 사물들의 개수가 전 세계 인구수를 초과하였다. 사물인터넷은 또한 기존의 언제 어디서나(any time and any where) 통신이 가능하도록 하는 패러다임이 어떤 것(any thing)도 연결 가능한 새로운 방식으로 더욱 확대된 것으로 볼 수 있다.

오늘날 다양한 산업용, 가정용, 개인용, 스마트 센서들이 출시되고 있으며, 이미 일부 제품들은 프로그램이 가능한 상태로 만들어졌으며 통신 기능을 갖추어 네트워크에 연결이 가능하다. 향후 센서들은 사물인터넷을 구성하는 가장 기초적인 사물들이 될 것이다. 사용자들이 많은 사물들을 소유하고 있으면서 사물들 간의 네트워크를 통해 정보를 수집하고 제어할 수 있는 새로운 서비스를 이용할 수 있게 된다.

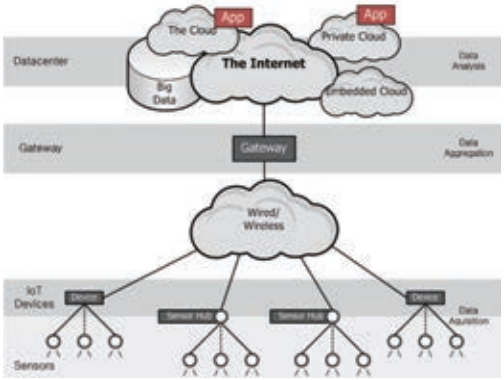
사물인터넷을 구성하는 사물의 종류와 범위가 다양하기 때문에, 사물들은 복잡한 이기종 네트워크간의 연결을 통해서 물리적 논리적으로 연결된 유무형의 자원을 이용하게 된다. 사물인터넷에 대해 ITU-U Y.2060에서는 다음과 같이 설명하고 있다.

"상호 작용 가능한 정보통신 기술에 근거한 현존하는 혹은 진화된 (물리적 혹은 가상적) 사물들을 서로 연결함으로써 보다 발전된 서비스가 가능하도록 만들어 주는 정보 사회를 위한 범세계적 기반시설[3]"

이 때 사물들은 〈그림 1〉에서 표현된 것처럼 통신 네트워크에 통합되어 관리되는 물리 세계의 각종 객체가 될 수도 있고, 정보 세계에서 존재하는 가상의 객체가 될 수도 있다. 여기서 물리적 사물(physical thing)의 경우는 실제 자연 상의 데이터를 감지하거나 영향을 줄 수 있는



〈그림 1〉 사물 인터넷의 물리적/가상적 객체간의 관계



〈그림 2〉 사물인터넷 아키텍처

네트워크에 물리적 연결이 가능한 장치들로서 환경 감지 시설, 산업용 로봇, 생산품, 전자 장치 등 다양한 것들이 해당될 수 있다. 또한 가상적 사물(virtual thing)이란 저장되거나 처리되거나 접근 가능한 멀티미디어 콘텐츠나 응용 소프트웨어 같은 것들이 해당된다.

사물인터넷의 기본 구조는 〈그림 2〉와 같이 나타낼 수 있다. 사물인터넷을 구성하는 기저에는 다양한 센서가 존재하여 데이터를 수집하고 센서들은 센서용 허브를 통해서 네트워크에 유무선으로 연결될 수 있다. 이 때 센서들은 기존에 활용되는 센서와 함께 새로운 형태의 센서들이 추가로 네트워크를 이루게 된다. 이를 위해 네트워크는 경량이면서도 더 많은 데이터를 처리할 수 있는 형태로 진화할 것이다. 수집된 데이터는 게이트웨이를 통해서 인터넷 망으로 모두 연결되고, 클라우드 서버에서 데이터가 저장되거나 처리되거나 접근 가능해지며, 빅데이터 분석을 통해서 수집된 정보에 대한 다양한 수준의 의미 있는 정보들이 추출될 것이다.

사물인터넷 초기에는 현재 보편화된 RFID와 무선 센서 네트워크(wireless sensor network)를 기반으로 성장할 것이다. 이미 기존의 RFID 기술은 물류 체계를 위한 통합 정보 시스템으로 활용되고 있으며, 네트워크에 연결 가능한 스마트 RFID가 출시되고 있다. 또한 관련 기술로서 NFC (near field communication) 장치들도 이미 활용 중에 있다. 또한 수백 또는 수천 개 이상의 원격 모트(mote)로 구성되어 정보를 수집하고 전달해 줄 수 있는 무선 센서 네트워크에 대한 연구도 이미 20년 가까이 진행이 되어 왔다. 센서들의 네트워크는 여러 게이트웨이를 통해서 네트워크에 연결될 수 있다.

그러나 RFID나 무선 센서 네트워크가 사물인터넷의 전체라 생각할 수는 없다. 무엇보다 사물인터넷이 가능하도록 만들어 주는 새로운 통신 기술의 발달을 고려해야만 한다. 특히 M2M 통신 기술은 사물인터넷을 위한 사물간 통신을 가능하도록 만들어 주는 핵심 요소 기술로 활용될 것이다.

보안 측면에서는 사물인터넷 보안을 위해서 기존의 보안 기술들을 단순 통합하는 방식들이 적용되지 못할 것이다. 이미 RFID 기술이나 무선 센서 네트워크 기술에서 각각의 시스템을 위한 고유의 보안 요구 사항들이 오랜 기간 연구되었고, 보안 요구 사항을 달성하기 위한 여러 메커니즘과 프로토콜들이 제안되었다.

기존의 기술들이 사물인터넷 안에서 보안성을 유지하거나 강화할 수 있는 방안에 대한 연구가 필요하다. 또한 사물인터넷을 위한 새로운 보안 요소 기술들이 사물인터넷이 시작되는 현재부터 동시에 고려되고 설계되어야 한다.

그러나 초기 사물인터넷이 기존의 RFID와 무선 센서 네트워크를 바탕으로 성장한다고 해서, 보안 기술 역시 RFID나 무선 센서 네트워크를 위해 개발된 것을 단순히 결합한다고 간단히 해결되지 못할 것이다. 사물인터넷이라는 이용가능한 자원이나 연결성이 극대화된 환경은 더 낮은 자원과 통신 능력을 가정한 기존의 RFID 보안이나 무선 센서 네트워크 보안 메커니즘들과 맞지 않는다. 사물인터넷이라는 더 큰 프레임 속에서 RFID가 활용되면 기존 시나리오에서 고려되지 못한 새로운 보안 취약성이 등장할 수 있다.

따라서 기존의 기술들을 어떻게 새로운 사물인터넷 체계에 보안을 유지하거나 강화된 형태로 통합할 것인지에 대한 연구가 필요한 상황이다. 혹은 기존 기술들과 독립적으로 사물인터넷을 위한 새로운 보안 요소 기술들이 사물인터넷 기술 개발시부터 동시에 고려되고 설계되어야 한다. 다음에는 사물인터넷의 특성을 고려한 보안 요구 사항은 어떤 것들이 있으며 이로부터 어떻게 보안 기술이 개발 및 적용되어야 할지에 대해서 논의할 것이다.

Ⅲ. 사물인터넷 보안 기술

1. 일반적인 사물인터넷 보안 요구 사항

많은 다른 보안 시스템들과 마찬가지로 사물인터넷에서도 기밀성(confidentiality), 무결성(integrity), 가용성(availability) 세 가지 요소는 가장 기본적인 보안 서비스로 요구된다.

기밀성은 허가된 사용자 외에는 메시지 내용을 알거나 유추할 수 없도록 만들어 주는 것을 의미한다. 이를 통해 공격자에 의해서 전송되는 메시지에 대한 분석이 이루어지는 것을 방지한다. 송신자는 전송하는 데이터에 대한 암호화 및 복호화 알고리즘을 적용할 수 있다.

무결성은 메시지가 수신됐을 때 수신자는 메시지가 전송 중에 변경되지 않았음을 보증하는 것을 의미한다. 이때 사용되는 암호학적 수단은 대칭키 암호의 메시지 인증 코드(message authentication code)를 사용하거나 비대칭키 암호의 전자 서명(digital signature)을 사용할 수 있다. 이에 더하여 메시지 수신자가 수신된 메시지 송신자의 신원을 확인하고 검증할 수 있도록 만들어 주는 메시지 소스 인증이 함께 제공될 수 있다.

가용성은 사용자가 시스템 서비스를 정해진 시간에 정해진 만큼 이용할 수 있도록 보장해 주는 것을 의미한다.

다수의 사물들이 동시에 동작하기 때문에 일정 사물들을 그룹으로 분류하여 그룹 내의 보안을 보장해 줄 수 있다. 공유된 비밀키는 메시지 인증에는 직접 사용하지 않으며 그 대신 비대칭키 암호나 TESLA(Timed Efficient Stream Loss-tolerant Authentication)와 같은 발전된 대칭키 인증 방식을 사용한다[5].

데이터 송신자가 전송 후에 데이터 송신 사실을 부인하지 못하도록 하는 부인방지 기능도 중요하다. 이는 일반적으로 공개키 알고리즘의 개인키를 사용해서 전송되는 데이터에 대한 전자서명을 생성함으로써 달성할 수 있다.

트래픽 흐름에 대한 기밀성 보장도 필요할 수 있다. 공격자가 특정 노드에서 나오거나 그 노드로 들어가는 트래픽 패턴을 검사하여 언제 어떤 특정한 기능이 실행되는지를 판단하는 등 관련 사실이나 정보를 유추하는 것을 방지하는 것을 의미한다. 이를 위해서는 통신 데이터 내부에서 암호화 되고 위조된 메시지를 임의적으로 주입시키거나 두 노드 사이에서 교환되는 데이터 패킷의 크기를 임의로 조정할 수 있다. 기본적인 사물인터넷 보안 기능을 통해 달성 가능한 보안 기능은 〈표 1〉에 제시되어 있다.

〈표 1〉 사물인터넷을 위한 보안 분야[4]

항목	보안 요구사항
시스템 신뢰성	서비스 가용성
	인프라 가용성
	인프라 무결성
	인프라 신뢰성
	부인방지 (서비스에서 사용자)
	계정관리
통신 스택 서비스 계층	서비스 접근 제어/권한관리
	서비스 인증
	서비스 평판 측정
	서비스 신뢰성
통신 스택 네트워크 계층	네트워크 수준 익명화
	기밀성
사용자 서비스 프라이버시	인프라 사용시 사용자 프라이버시 보호
	서비스 사용시 사용자 프라이버시 보호
	사용자 대상 서비스의 프라이버시 보호

사물인터넷 보안에서는 인터넷에 연결되는 다양한 사물들의 연산능력을 고려한 경량화된 알고리즘이 필요하다. 또한 수많은 사물들에 대한 분산된 보안 관리가 가능해야 한다.

기본적인 보안 기능 이외에 사물인터넷에서 사용되는 장치들은 〈표 2〉에 제시된 보안 기능이 별도로 필요하다. 모든 보안 요소 기술들은 사물들 간에 완전하게 분산된 보안 관리가 지원될 수 있어야 한다. 또한 경량화된 보안 솔루션이 필요하며 분산되고 자발적인 보안 관리가 있어야 한다.

이 때 높은 수준의 보안이 필요한 응용에서는 알고리즘의 복잡도가 상대적으로 높아지며, 필요한 연산량도 그에 따라 증가한다. 따라서 보호하고자 하는 정보의 가치에 따라서 보안 수준은 다르게 적용되어야 한다. 특히 사물인터넷에 연결된 장치들 중에는 가용 연산 수준이 매우 미약한 장치들이 존재한다. 이런 장치들에는 특정한 보안

〈표 2〉 사물인터넷을 위한 보안 기능

사물인터넷 보안 기능	보안 기능에 대한 설명
사물인터넷 장치를 위한 보안 부팅 지원	사물인터넷 상에서 동작하는 각 장치들이 안전한 보안 연산 환경을 보장하기 위해서는 처음 스위치가 켜 졌을 때 펌웨어에 대한 인증 값을 검증하여 무결성을 확인할 수 있는 보안 부팅(secure booting) 기술이 필요함. 이를 위해서는 운영체제 외적으로 별도의 장치에 의해서 전자서명과 같은 암호학적 연산이 동작될 수 있어야 함.
경량 암호 및 분산된 자발적 보안 설정 지원	프라이버시 보호 및 암호화 방식은 단순하고 작은 장치에서도 적용 가능한 경량 암호화(lightweight encryption) 솔루션이 필요함. 최소 260억 개 이상의 사물들이 네트워크에 연결되기 때문에 보안 관리자에 의해서 모든 사물들에 대한 보안 파라미터를 적절하게 관리하는 것은 불가능함. 따라서 관리자가 없이도 자발적으로 인증 및 보안을 위한 설정이 이루어지도록 해야 함.
사물들 간의 가상 사설망 설정 및 관리 지원	공공 네트워크를 통해서 중요한 데이터를 전송하는 경우에는 사물들 간에 가상 사설망(virtual private network)을 설정하고 해제하는 것이 가능해야 함. 또한 각 장치들에 할당된 제한된 대역폭과 임베디드 장치의 간헐적 네트워크 연결 특징을 유지하면서 동시에 소프트웨어 업데이트와 보안 패치가 전달되는 메커니즘 또한 구성되어야 함.
빅데이터 분석에 대한 프라이버시 보호 기능	사물인터넷 상으로 많은 센서로부터 수집된 정보는 빅데이터 분석이 적용되는데 이 때 프라이버시 보호 기능이 제공되어야 하며, 사물인터넷 데이터에 대해서도 적절한 프라이버시 보호 기능 및 익명화 기술이 적용될 수 있음.
심층 패킷 정보감시 기능 지원	심층 패킷 정보감시(deep packet inspection, DPI)가 가능한 방화벽과 침입방지 시스템이 구성되어야 한다. 필요에 따라 특정 장치를 목적지로 하는 트래픽에 대한 DPI 솔루션이 적용되어야 함.

메커니즘이 적용되지 못하거나 이런 장치로 인해 전체 시스템의 보안 수준이 떨어질 우려가 있다.

기존의 네트워크에서는 보안 관리자에 의해서 이런 설정들이 개별로 관리될 수 있지만 사물인터넷의 방대한 수의 개체들 사이의 개별 보안 설정을 분산적이면서 자발적인 방식으로 설정이 가능해야 한다.

2. 환경적 제약

M2M 환경에서는 이종 노드간 연결이 고려되어야 한다. 이 때 노드의 성능에 따라서 크게 세 가지 환경으로 구분할 수 있다.

먼저 자원이 매우 제약된 센서 노드에 대해서는 공개키 적용이 어렵다. 대부분의 연산 능력이 제안된 태그 형태의 사물들이 이에 해당하게 된다.

그 외 다른 센서 노드들에 대해서는 비대칭 암호의 공개키 연산만 적용 가능할 수 있다. 비대칭 암호에서 공개키를 사용하는 암호화나 전자서명검증 연산의 경우에는 개인키를 사용하는 연산에 비해서 상대적으로 더 적은 연산량을 사용하게 된다.

끝으로 유선으로 연결된 원격 서버 같은 장치들은 외부 전원에 연결되어 있고 자체적으로 높은 연산 능력을 갖고 있기 때문에, 많은 에너지, 연산량, 저장 능력 등을 활용할 수 있다. 이런 경우에는 모든 보안 메커니즘이 어려움 없이 구현 가능할 것이다.

3. 종단-종단 보안 대 홉 단위 보안

보안 통신이 적용되는 단위도 크게 두 가지로 나누어 볼 수 있다. 첫 번째는 한쪽 끝에서 전송하는 메시지에 보안 알고리즘이 설정/적용된 후에 네트워크를 통해 전송되면, 마지막 종단에서 대응되는 보안 메커니즘을 통해 정보를 복구할 수 있는 종단-종단(end-to-end) 보안이 있다. 이에 대비해서 송신자와 수신자를 잇는 경로상의 모든 노드들 사이 회선 수준에서 홉 단위(hop-by-hop)로 보안을 설정/적용할 수 있다.

전자의 경우에는 종단간 사용하는 알고리즘이 동일해야 하며 높은 보안 수준을 위해서는 연산 전에 공통의 암호 비밀키를 공유하는 프로세스가 진행되어야 하고 양쪽 종단이 동일한 복잡도의 알고리즘을 적용해야 한다. 그러나 한쪽 종단이 센서인 경우 이렇게 설정하면 센서에서 과도한 연산이 필요하게 되고, 따라서 연산이 불가능하거나 가능하더라도 많은 연산으로 인한 배터리 수명 감소 등의 문제가 생길 수 있다.

홉 단위로 보안을 적용하는 경우에는 송신자에서 목적지로 이어지는 경로 상의 모든 중간 노드들의 모든 쌍에 대해서 보안 설정이 적용되어야 한다. 하지만 회선 상에서는 보안이 적용되어 전달되지만 노드 내부에서는 평문 접근도 가능하기 때문에 공격자가 노드들을 침해하는 경우 전송 메시지에 대한 암호 해독 없이도 정보획득이 가능할 수 있다. 실제 시스템에서는 두 가지 방식이 복합적

으로 적용될 수 있으며, 관리자에 의한 설정이 없이도 상황에 맞게 적용가능해야 한다.

4. 보안키 설정 문제

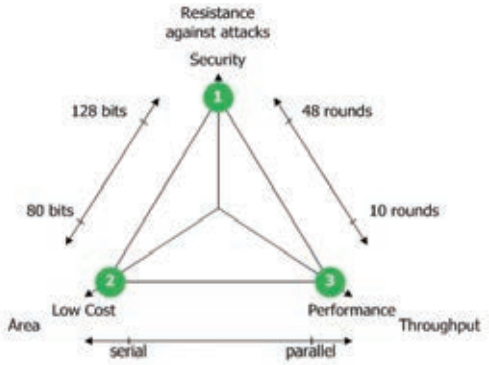
보안을 위해서 다수의 인증키 교환(authenticated key exchange, AKE) 프로토콜을 사용할 수 있다. EAP(Extensible Authentication Protocol)의 경우 다양한 인증 수단을 허용하고 있기 때문에 보안키 설정을 위한 하나의 후보군으로 고려될 수 있다. 이 경우 마스터키로부터 파생된 세션키들이 배포되어 보안 메커니즘에 적용된다. 또는 기존의 프로토콜이 아니라 사물인터넷을 위한 또 다른 키 설정 시스템을 구성할 수도 있다.

5. 프록시 재암호화

이종 네트워크 내에서의 다양한 장치들이 하나의 네트워크로 연결이 되면 프록시 재암호화(proxy re-encryption)를 지원할 수 있어야 한다. 프록시 재암호화는 일반적으로 네트워크상의 한 노드 B가 B의 공개키로 암호화되어 자신에게 전달되는 메시지를 제3자인 C에게 자신의 개인키를 밝히지 않은 채로 전달해 주는 것을 의미한다. 이 경우 B은 자신의 메시지 중 하나를 프록시 재-암호화 하도록 지정할 수 있고 이 메시지는 C에게 전달될 수 있다. 일반적으로 C가 암호화된 메시지를 읽을 수 있도록 새로운 키가 생성된다. 이런 방식은 관리자 권한 양도, 이메일 재전송이나, 사법 집행 감시, 콘텐츠 재분배 등 여러 분야에서 필요한 기술이다.

6. 경량 암호의 필요성

RFID 태그, 센서, 비접촉 방식의 스마트카드나 헬스케어 단말 등 사물인터넷에 연결될 수 있는 많은 사물들은 배터리, 배터리, 메모리 등 연산능력이 매우 제한되어 있다. 이를 위해서는 이런 환경에서 사용가능할 수 있는 경량화된 암호 메커니즘이 활용되어야 한다. 〈그림 3〉에서는 경량 암호 설계시 고려되어야 할 요소들이 표시되어 있다. 가장 핵심적인 요소는 "보안", "저비용", "성능" 으로 볼 수 있으며, 이를 위해 저항 가능한 공격 수준, 장치를 구현하기 위한 하드웨어 크기나 소프트웨어 코드 길이, 그리고 알고리즘의 처리율 등이 고려되어야 한다.



〈그림 3〉 경량 암호 설계

국내에서도 사물인터넷을 위한 경량화된 비밀키 암호 알고리즘 표준인 LEA가 와 암호학적 해시 함수인 LSH가 새롭게 개발되었다.

국내에서도 사물인터넷을 위한 경량화된 비밀키 알고리즘이 개발되었다. 2013년에는 128비트 비밀키 기반의 블록 암호인 LEA (lightweight encryption algorithm)이 국내 표준으로 지정되었다. 또한 2014년에는 암호학적 해시 알고리즘인 LSH가 발표되었으며 국내 표준화 작업이 진행 중에 있다[6-7].

7. 포스트 양자 암호에 대한 고려

현재 널리 사용되는 대부분의 공개키 암호는 RSA처럼 매우 큰 합성수의 소인수분해가 어렵다는 사실에 근거하거나 큰 수의 이산로그문제(discrete logarithm problem, DLP)가 풀기 어렵다는 사실에 근거하고 있다. 그러나 1994년 Shor에 의해서 양자컴퓨터상에서 고속으로 소인수분해하는 알고리즘이 개발되고, 이어서 양자컴퓨터상에서 이산로그문제와 타원곡선 상의 이산로그문제(elliptic curve-discrete logarithm problem, EC-DLP)를 고속으로 해결하는 알고리즘이 개발되었다. 이로 인해 오늘날 널리 사용되는 RSA, DSA, 타원곡선 암호와 같은 공개키 암호 알고리즘들은 양자컴퓨터가 실용화되면 더 이상 사용할 수 없게 된다. 특히 사물인터넷이 보편화된 2020년 이후에는 양자컴퓨터 기술은 더욱 발전해 있을 것으로 전망된다. 따라서 사물인터넷을 위한 보안

시스템도 양자컴퓨터 상의 알고리즘에 대해서도 안전성을 보장할 수 있는 방식이 사용되어야 한다. 최근에는 격자 기반의 암호 중에서 경량화된 공개키 암호 방식이 국내에서 개발되어 소개되기도 하였다[8].

8. 보안 인지 프로세스

수백 억 개의 사물이 네트워크에 연결되어 있는 경우에는 각 장치들에 대해서 세부적인 보안 설정이 쉽지 않게 된다. 따라서 사물인터넷 보안 시스템은 분산된 세팅과 보안 관리가 가능해야 한다. 이러한 요구 조건의 일환으로 사물인터넷 장치들의 클러스터가 보안 인지 및 자가 치유 프로세스가 고려될 수 있다[9]. 이러한 과정은 기본적으로 "관찰", "계획", "행동", "학습" 등 네 가지 단계로 이루어진다. 관찰 단계에서는 클러스터 주변의 보안 이벤트를 감지하거나 이전 단계의 학습 결과를 통해서 새로운 정보를 받아들인다. "계획" 단계에서는 수집된 정보를 기반으로 보안과 관련된 특정 메커니즘을 계획하고 설정한다. 그리고 "행동" 단계에서는 계획된 메커니즘을 실제로 시행하고 시행 결과에 대한 새로운 기계학습과정을 거쳐서 새로운 인지 프로세스를 추출할 수 있다. 이러한 학습 단계의 존재는 단순한 적응적 보안 과정과 보안 인지과정을 구별해 주게 된다.

보안 시스템의 자가 치유(self healing) 프로세스를 통해서 주변의 변화나 새로운 보안 상황에 대해서 보안 시스템이 문제점에 일차적으로 대응하면서 새로운 환경에 적응 및 진화가 가능하도록 만들 수 있다.

사물인터넷의 등장과 함께, 인더스트리 4.0이라는 새로운 생산 시스템이 고려되고 있다. 그러나 미국의 노스폴 토이 사례나, 스턱넷의 경우에서 보는 것처럼 연결성 확대를 통해 새로운 보안 위협이 등장할 수 있다.

Ⅳ. 산업 제어 시스템 상에서의 사물 인터넷 보안

사이버 물리 시스템(cyber physical system, CPS)이란 실제 물리 세계의 시스템을 센서와 구동기를 통해 정보통신 기기와 연결시킨 복합 시스템으로 물류, 헬스케어, 정보통신, 에너지 기술 등에 활용되는 산업 제어 시스템을 의미한다. 대표적인 사이버 물리 시스템으로 스마트 그리드가 있다. 스마트 그리드에서는 전력 그리드에 각종 스마트 센서, 구동기, 그리고 SCADA 기반의 제어 시스템이 덧씌워진 형태를 갖추고 있다.

특히 최근에는 독일을 중심으로 산업 제어 시스템에 대한 새로운 모델인 인더스트리 4.0 (Industry 4.0)이 거론되고 있다. 인더스트리 4.0은 산업용 네트워크에 연결된 각종 센서와 구동기가 게이트웨이를 통해 인터넷에 연결이 되고, 여기에 급격하게 발달된 정보통신 기술과 공장 자동화 기술이 함께 융합되면서 만들어지게 된다[10].

사이버 물리 시스템은 사물인터넷에 연결되는 또 하나의 중요한 영역일 뿐만 아니라 보안 문제에 특히 민감한 영역이라 할 수 있다. 이 절에서는 사이버 물리 시스템의 보안 현황에 대해서 두 가지 사례를 중심으로 살펴보도록 한다.

1. 사이버 물리 시스템 보안사건 사례

이 장에서는 실제로 사이버 물리 시스템에서 일어난 대표적인 보안 사례를 살펴봄으로써 사물인터넷 보안 문제의 중요성을 재고해 보도록 한다.

미국의 장난감 회사인 노스폴 토이(North Pole Toys)에서는 2011년에 기존의 전통적인 생산 체계를 완전히 개편하여 새로운 자동화된 산업 제어 시스템을 실제 제품 생산에 도입하였다. 이를 통해 인터넷을 통해서 사용자가 자신이 원하는 형태로 일정 수준에서 장남감에 대한 맞춤 제작 요청을 할 수 있게 되었다. 공장의 생산 시스템은 고립된 망으로 직접 인터넷에 연결하지는 않았기 때문에, 인터넷에서 소비자로부터 수집된 주문은 메인 서버로 수집된 후에 공장 시스템에 USB 스틱을 통해서 전달하는 방식을 사용하였다.

그러나 2011년 미국 추수감사절 전날에 어떤 박스에는 여러 장남감이 동시에 포장되고, 다른 박스는 빈 박스로 포장이 되는 오류가 발견되었다. 처음 이 문제를 발견했을 때에는, 생산용 PLC(programmable logic

controller)에 버그가 있는 것으로 생각되었지만, 분석 결과 어떤 오류도 발견되지 않았다. 그러나 보안 전문가에게 공장 시스템과 메인 서버에서 "kAndyKAn3"으로 알려진 웜이 발견되었고, 바로 이 웜에 의해서 생산 시스템에 교란이 일어났음이 확인되었다. 이런 문제는 공장 생산 시스템이 인터넷과 분리되어 고립된 상태로 운영됐음에도 일어난 것이다[11].

노스폴 토이의 사례에서는 장난감 제조업이라는 비교적 사회적 문제의 폭이 제한된 시스템이 웜에 감염되었다면, 보다 심각한 산업용 제어 시스템 보안 사고의 사례로서 이란 핵발전소에서 일어난 스턱넷(Stuxnet)이 있다.

2010년 6월에 이란 핵발전소의 한 엔지니어의 컴퓨터에서 VirusBlokAda 악성코드가 발견되었다. 이 코드에 의해서 이란 핵발전소의 원심분리기에서 주기적으로 비정상적인 회전수 변화가 발생했고, 이로 인해 생긴 원심분리기의 과부하로 인해서 핵발전소 장비의 수명이 크게 단축되는 결과를 초래하였다. 조사 결과 이 악성코드는 핵발전소의 특정한 기능에 손상을 줄 수 있도록 정교하게 설계된 것으로, 핵발전소의 네트워크가 외부와 연결되지 않았음에도, 내부 직원의 노트북 및 USB 스틱을 통해서 악성코드가 전달되도록 만들어졌다. 이러한 장비 고장률의 급격한 증가는 핵발전소의 전체 안전성을 위협하고 유사시에는 방사능 유출 등 국제적 재난으로까지 발전될 수 있는 잠재력을 갖고 있다는 점에서 충격을 주었다[12].

두 가지 산업 시스템 보안 침해 사고 사례에서는 모두 산업 시스템이 인터넷에 직접 연결되지 않고 격리되어 있는 상태에서 일어난 것이다. 네트워크의 연결성이 제한되어 있는 상황에서도 악성코드에 감염이 이루어지고 문제가 생길 수 있음을 보였다. 이는 만일 사물인터넷처럼 연결성이 극대화된 환경에서는 이런 문제는 더욱 쉽게 일어날 수 있음을 의미한다. 전력망이 순식간에 마비되거나 발전소 시설이 파괴되고 공장의 생산이 비정상적으로 이루어질 수 있다. 따라서 이러한 사고를 예방하거나 방지하고, 문제가 생겼을 때 바로 해결될 수 있는 사물인터넷시대의 사이버 보안 시스템을 위한 연구 및 대책 마련이 시급하다고 할 수 있다.

산업 제어 시스템에서는 기밀성, 무결성, 가용성, 적시성 및 오류에 대한 강인성이 갖춰져야 한다. 또한 많은 제어 시스템의 기반이 되는 SCADA 보안에 대한 연구도 시급한 상황이다.

2. 사이버 물리 시스템의 보안 취약성

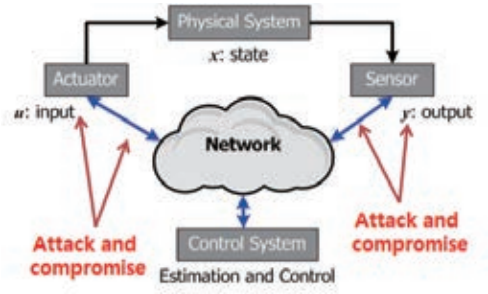
사물인터넷과 사이버 물리 시스템 등 다양한 요소 기술의 성공적 결합함으로써, 인더스트리 4.0 모델이 실제로 성공하게 되면 새로운 생산 모델로 효율성 및 효용성이 급격히 증가될 것이다. 그러나 이를 위해서는 다양한 보안 문제에 대해 면밀한 검토와 함께 대비책이 필요하다. 특히 현재의 에너지 그리드, 상하수도, 물류, 운송 등의 네트워크들은 외부의 악의적 공격에 매우 취약한 구조를 갖고 있다[13-14].

따라서 사이버 물리 시스템의 제어 장치들이 실제로 외부의 다양한 공격에 저항이 가능한지 엄밀한 분석이 필요하다. 특히 허가되지 않은 사용자가 인증을 회피하여 시스템에 접근하거나 서비스 거부 공격에 대응할 수 있는 시스템이 마련되어야 한다.

특히 외부의 물리적 공격에 살아남아야 한다. 단순히 데이터를 백업 하는 것만으로는 충분하지 않을 수 있기 때문에, 일부 장치들이 동작하지 않는 경우에 일어날 수 있는 가능성들을 평가하고 산정하며 시스템의 전체 기능을 유지될 수 있어야 한다. 구성요소가 침해되더라도 시스템 성능을 유지할 수 있는 최대 한계를 분석하고 파악할 수 있어야 한다.

동작 오류뿐만 아니라 외부에 노출된 장비가 공격자에게 침해된 경우에도 안전이 보장될 수 있어야 한다. 특히 다양한 사물들이 사용되는 경우에는 공격자에 의해서 특정 장치가 하나 이상 악성 장비로 동작할 수 있다. 이런 장치들은 외부로 내부의 주요 정보를 전송할 뿐만 아니라 시스템 전체 기능을 마비시킬 수 있다. 따라서 외부에서 공격자에게 침해받은 시스템을 정상적인 장치들과 구분할 수 있는 기술이 필요하다. 보안 시스템으로 인한 오버헤드 및 연산량을 최소화할 수 있어야 한다.

사이버 물리 시스템에서는 사이버 시스템과 실제 물리 시스템이 거대 규모로 동시에 동작하고 있다. 이런 경우



〈그림 4〉 사이버 물리 시스템 모델

에 시스템의 자원 스케쥴링 및 선점(preamption) 문제가 발생할 수 있다. 다양한 장치들의 상호 연결 및 일정 수준의 격리를 제공할 수 있어야 한다.

〈그림 4〉는 사이버 물리 시스템에 대한 시스템 관점의 모델을 나타내 주고 있다. 그림에 의하면 네트워크를 통해서 제어 시스템은 구동기와 센서를 조정할 수 있다. 센서와 구동기는 물리 시스템에 실제로 연결되어 있으면서 사이버 시스템에 대한 입력 및 출력 값을 각각 제공해 줄 수 있다. 그리고 센서와 구동기를 통한 입력 및 출력에 맞추어서 물리 시스템의 실제 상태가 변화하게 된다.

제어 시스템에서는 전통적인 기밀성, 무결성, 가용성 외에, 적시성(timeliness) 및 오류에 대한 강인성(fault tolerence)을 갖추어야 한다.

현재 많은 제어 시스템 네트워크들은 SCADA (Superevisory Control and Data Acquisition System)에 기반을 두고 있다. SCADA 시스템은 산업의 여러 공정, 기반시설, 산업 설비를 통한 작업 과정을 감시하고 제어하는 컴퓨터 시스템으로 설계되었다. 그러나 사물인터넷과 같은 광범위한 네트워크 연결성에 대한 고려 없이 설계되었으며, 특히 외부 공격 가능성 및 시나리오에 대한 고려 없이 설계 되었다는 문제가 있기 때문에, 추가적인 보안 시스템이 마련되어야 한다.

Ⅵ. 향후 연구 및 결론

지금까지 사물인터넷의 특징 및 그에 따른 보안 요구사항을 살펴보았다. 특히 사이버 물리 시스템을 중심으로 사물인터넷 시대의 가능한 보안 이슈에 대해서 이론적 설명과 함께 실제 사고 사례를 살펴보았다. 사물인터넷은 차세대 정보통신 분야의 성장 동력으로서 주목받고 있지만, 침해 사고나 외부의 공격을 사전에 예방하거나 대응할 수 있는 보안 알고리즘 프로토콜에 대한 연구가 매우 중요한 것을 알 수 있다. 사물인터넷의 안정적인 보안 달성을 위해서는 기존의 알고리즘이나 프로토콜들의 단순한 결합으로는 부족하며, 사물인터넷 환경에 걸맞게 연산량 및 전력소비 차원의 경량화 및 분산된 보안 설정 관리 등 새로운 개념의 보안 메커니즘 및 프로토콜 개발이 향후 절실히 요구된다.

참 고 문 헌

[1] 미래창조과학부, "사물인터넷(IoT) 정보보호 로드맵," 2014년 10월.

[2] 김호원, 김동규, "IoT 기술과 보안," 한국정보보호학회지, 22권, 1호, pp. 7–13, 2012년 2월.

[3] ITU–T Y.2060: Overview of the Internet of things, June 2012.

[4] A. Serbanati, et al., "IoT–A Project Deliverable D4.2 – Concepts and Solutions for Privacy and Security in the Resolution Infrastructure," Feb. 2012.

[5] A. Perrig, D. Song, R. Canetti, J.D. Tyger, B. Briscoe, "Timed Efficient Stream Loss–Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction," RFC 4082, June 2005.

[6] TTA, "128비트 경량 블록 암호 LEA," 정보통신단체표준, 2013년 12월.

[7] D.–C. Kim, et al., "LSH: A New Fast Secure Hash Function Family," in Proc. ICISC 2014, LNCS 8949, pp. 286 – 313, 2015.

[8] J.H. Cheon, H.T. Lee, J.H. Seo, "A New Additive Homomorphic Encryption based on the co–ACD Problem," in Proc. ACM SIGSAC Conf. Computer and Commun. Security, 2014, pp. 287–298.

[9] A. Riahi, et al., "A systemic and cognitive approach for IoT security," in Proc. Int. Conf. Computing, Networking, and Commun., 2014.

[10] J. Lee, B. Bagheri, H.–A. Kao, "A Cyber–Physical Systems architecture for Industry 4.0–based manufacturing systems," Manufacturing Letters, vol. 3., pp. 18–23, 2015.

[11] Tofino Security, https://www.tofinosecurity.com/blog/major-manufacturer-admits-plc-security-breach

[12] Stuxnet, https://en.wikipedia.org/wiki/Stuxnet

[13] C. Neuman, "Challenges in security for cyber-physical systems," in Proc. DHS: S&T workshop on future directions in cyber-physical systems security, 2009.

[14] E.K. Wang, et al., "Security issues and challenges for cyber physical system," in Proc. the 2010 IEEE/ACM Int'l Conf. Green Computing and Commun. & Int. Conf. Cyber, Physical and Social Computing, 2010. p. 733-738.

김 영 식

- 2001년 2월 서울대학교 전기공학부, 공학사
- 2003년 2월 서울대학교 전기컴퓨터공학부, 공학석사
- 2007년 2월 서울대학교 전기컴퓨터공학부, 공학박사
- 2007년 3월~2010년 8월 삼성전자 시스템 LSI 사업부, 책임연구원
- 2010년 9월~현재 조선대학교 정보통신공학과, 조교수

〈관심분야〉
사물인터넷보안, 제어시스템 보안, 포스트양자암호