[차세대이동통신] Machine-to-Machine(M2M) 통신을 위한 보안 프로토콜 표준화 동향

M2M communication이란 용어 그대로 사물 대 사물간의 통신을 통해 모든 객체간의 정보를 공유하고 이를 기반으로 이용자에게 다양한 정보 제공 및 서비스 편리성을 제공하기 위한 기술로서 2000년대 후반부터 많은 관심을 받아오고 있는 기술이다. 기존의 연산, 통신 및 네트워킹 기능을 가지고 있는 소형 디바이스들이 주변의 정보를 자동으로 획득하거나, 주변 기기들과 통신을 통해 정보의 상호 공유를 통해 서비스를 제공하였지만, 최근에는 계량기, 센서 그리고 자동차에 이르기까지 다양한 사물에도 이러한 기능들의 제공이 요구되어지고 있는 실정이다. 이에 따라, 표준화 기구마다 조금씩 상이한 명칭을 사용하게 되었으며, 현재 M2M, IoT, MTC 등의 명칭들이 사용 중에 있다. M2M은 현재 ETSI에서 사용하는 명칭이며, ETSI TS 102 689 표준을 통해 M2M 서비스 요구사항을 정의하고 있으며, 본 표준을 통해 다양한 서비스 요구사항뿐만 아니라 이를 만족시키기 위한 다양한 기능들을 정의하고 있다. 이외에도, M2M 기능구조, 스마트미터링 Use case 등 다양한 use case 관련 표준들을 개발 중에 있다. MTC(Machine Type Communication)는 3GPP에서 표준화가 진행중인 것으로, ETSI의 M2M 구조에서 전송 네트워크를 3GPP로 한정하는 기술로 현재 3GPP TS 22.368 표준을 통해 서비스 요구사항 및 통신 시나리오 등을 정의하고 있다. ITU-T에서는 현재 SG16을 통해 2011년부터 IoT-GSI를 만들어 Y.2060 표준(IoT reference model 등)을 개발하고 있으며, SG17과 연계하여 USN 기반 보안 표준 3건을 공동으로 개발하였다. 또한, ITU-T에서는 2012년 1월에 Focus Group on M2M service layer(FG M2M)을 설립하여 M2M 프로토콜 및 API, M2M service layer 요구사항, use case 관련 분야의 표준을 개발하고 있다. 본 표준화 보고서는 지난 2013년 8월 26일부터 9월 4일까지 스위스 제네바에서 개최된 ITU-T SG17 정기회의에서 제안된 M2M 통신 보안 관련 동향을 소개하고자 한다.

M2M 통신을 위한 부분 암호화(Fractional cryptography) 기반 보안 프로토콜 기술의 필요성

최근 융합 기술에 대한 관심이 지속적으로 높아지고 있고, 무선 네트워크 기술 발달 및 다양한 사물(소형 디바이스, 자동차, 계량기, 책상 등)간의 통신 및 정보공유의 요구가 증가됨에 따라 사물간 또는 기기간 통신에 대한 기술이 빠르게 진화되고 있다. 이에 따라, 국제 표준화 기구에서도 관련 기술 및 표준화 개발에 많은 노력을 기울이고 있는 실정이다. 일반적으로 사물 통신을 위해서는 최소한의 연산능력 요구 및 적은 통신량이 필수 조건이며, 사물간의 안전한 통신 및 정보공유를 위해 통신 보안 기술이 반드시 필요하다. M2M 기술의 급속한 발전과 이를 기반으로 다양한 서비스가 확산될 경우, M2M 통신 시스템은 해커들의 공격목표가 되기 쉽다. 따라서, 이러한 해킹 위협에 대처하기 위해서는 M2M 통신을 이용한 정보 공유시 이를 안전하게 보호하기 위한 보안 프로토콜이 요구되며, 이러한 보안 프로토콜은 반드시 사물들의 낮은 연산 능력과 적은 메모리 공간의 특성을 고려하여 개발되어야 한다. 따라서, 지난 8-9월 ITU-T 표준화 회의를 통해 제안된 "Secure communication protocol using fractional cryptography for

M2M communication" 신규과제와 같이 적은 통신량으로 원하는 안전성을 제공할 수 있는 기술들이 필요하다. 본 신규과제에서 제안한 기술은 전송되는 데이터에 대해서 일부 특정 부분만을 Masking하여 암호화 및 복호화를 처리하는 기술로, 다양한 사물간 통신에 적용하기에 적합하다고 할 수 있다.

표준화 진행 상황 및 표준화 회의 결정사항

금번 회의에 제안된 M2M 통신을 위한 부분 암호화(Fractional cryptography) 기반 보안 프로토콜(Secure communication protocol using fractional cryptography for M2M communication) 신규 과제는 전송되는 데이터 패킷에 일부 부분만을 선정하여 암호화하여 전송하는 기술로서 최소한의 데이터 암호화를 통해 통신량을 줄일 수 있는 장점을 가지고 있지만, 해당 프로토콜에 대한 안전성 및 신뢰성은 좀 더 검토가 필요한 상황이다. 또한, 미국, 영국 등에서는 본 기술의 경우 ITU-T SG17에서 개발하는 것보다는 IETF, ISO/IEC 등 기존에 통신 보안 프로토콜을 주로 개발하는 표준화 기구를 통해 표준화를 추진하는 것이 적합하다고 주장하며 신규 아이템 채택에 반대의견을 제시하였다. 이에 따라, 최종 SG17 Plenary 회의를 통한 신규 아이템 채택은 실패하였으나, 차기 회의에서 ITU-T SG17 내에서 개발 중인 IoT, 스마트그리드 서비스 모델 등에 적합한 보안 프로토콜을 개발하여 다시 제안하기로 하였다.

시장 전망 및 국내 표준화 활동에의 제언

금번 SG17 회의를 통해 제안된 M2M 통신을 위한 부분 암호화(Fractional cryptography) 기반 보안 프로토콜과 같은 기술은 향후 M2M, IoT, 사물지능통신 등 현재 국내에서 개발 중인 다양한 서비스 분야에 적용 가능한 기술로, 안전성만 입증이 된다면 다양한 분야의 사물지능통신 기반 서비스에 적용이 가능하다. 따라서, 국내에서도 이러한 M2M 통신에 적용 가능한 암호 프로토콜 기술에 대한 개발 노력 및 애플리케이션 레벨에서의 보안 기술 개발을 통해, 향후 다가올 사물지능통신 분야의 거대 시장에서 보안 분야가 한 축을 담당할 수 있도록 철저한 준비가 필요하다. 현재 국내에서는 TTA의 TC7 PG708을 중심으로 사물지능통신 관련 국내 표준을 개발 중에 있으며, 보안 관련 부분은 TC5를 중심으로 개발되고 있다. 표준화의 경우 개발 시점이 매우 중요하기 때문에, 타 국가보다 먼저 사물지능통신 보안 기술에 대한 다양한 표준 개발 노력을 통해 해당 분야의 표준 시장을 선점하는 것이 시급하다. 또한, 최근에 미국, 영국, 독일 등의 국가에서는 이미 권고 자체를 규제로 인식하고, 법제도적 이슈가 포함될 수 있는 권고안에 대해서는 철저한 사전 검토 및 대응이 강화되고 있다. 따라서, 국내에서 관련 표준 개발 시 개발 초기 단계에서부터 면밀한 기술 검토 및 개발을 통해, 국내 표준 기술이 SG17 본 회의에서 채택될 수 있도록 표준화 전문가들의 많은 노력이 필요하다고 생각된다.

백종현 (KISA 수석연구원, ITU-T SG17 Q6 라포처, jhbaek@kisa.or.kr)