[별첨 5]

하드웨어 보안모듈기반 LoRa 통신 보안 기술

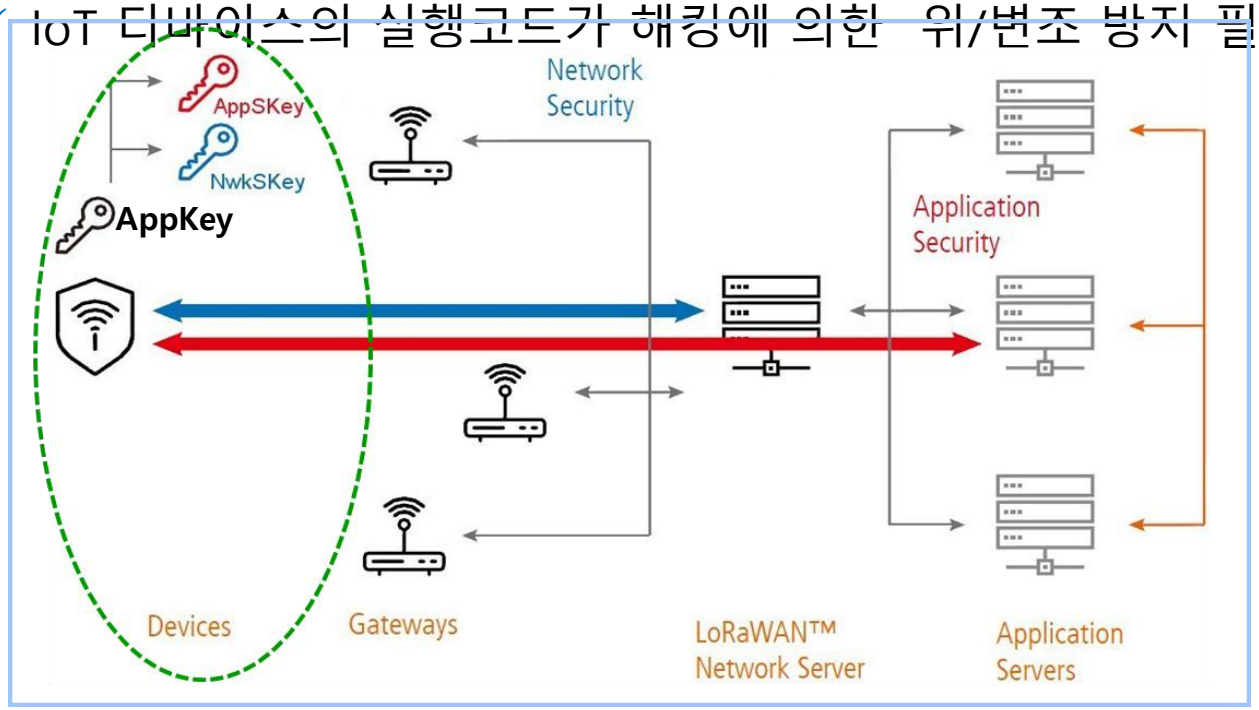
전용성 (ysjeon@etri.re.kr)
미래암호공학연구실

ETRI 한국전자통신연구원
www.etri.re.kr
지능화융합연구소/정보보호연구본부

목 차

▣ LoRa는 저전력의 넓은 면적 네트워크을 위한 솔루션

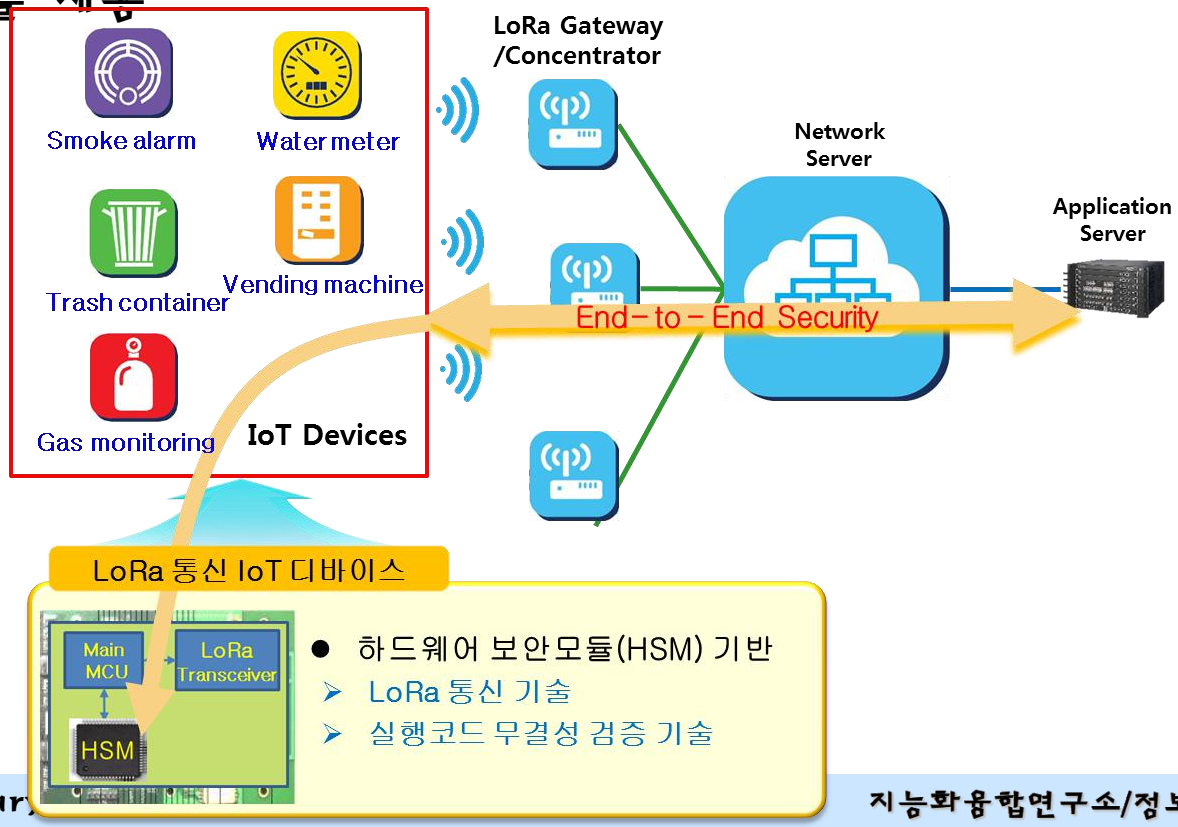
- ❖ End-to-End Security를 보장하기 위해서는 IoT Device에 대한 보안이 중요
  - ✓ IoT 디바이스에 저장되어 있는 중요정보(암호키 등)의 보호 필요
  - ✓ IoT 디바이스의 실행코드가 해킹에 의한 위/변조 방지 필요



* AppSKey(Application Session Key), NwkSKey(Network Session Key)

■ 하드웨어 보안모듈기반 LoRa 통신 보안 기술

- ❖ LoRa 통신에 필요한 중요정보를 **하드웨어 보안모듈**에 안전하게 저장하고, 암호처리를 하드웨어 보안모듈 내부에서 수행함으로써 LoRa 통신의 안전성을 보장
- ❖ 하드웨어 보안모듈을 이용하여 Main MCU의 실행코드의 무결성을 검증하는 기능을 제공



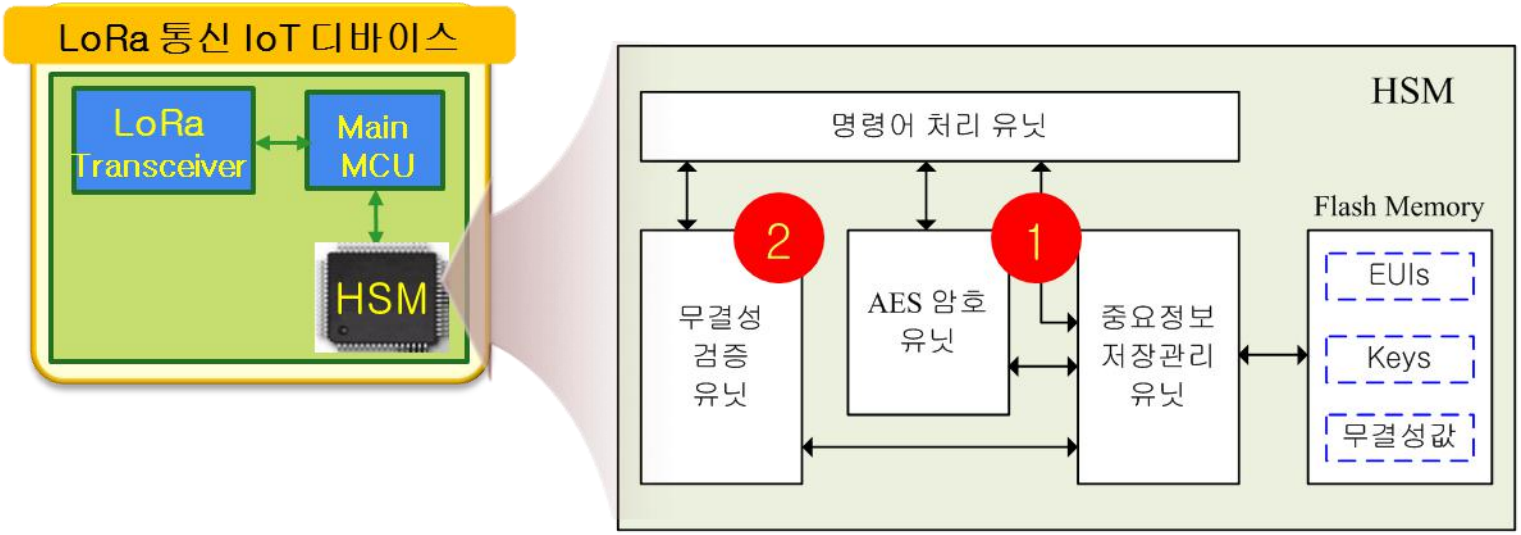
▣ 기술이전 내용 및 범위

❖ (1) 하드웨어 보안모듈 기반 LoRa통신 기술

- 상세설계서, 시험절차서 및 결과서, 소스코드

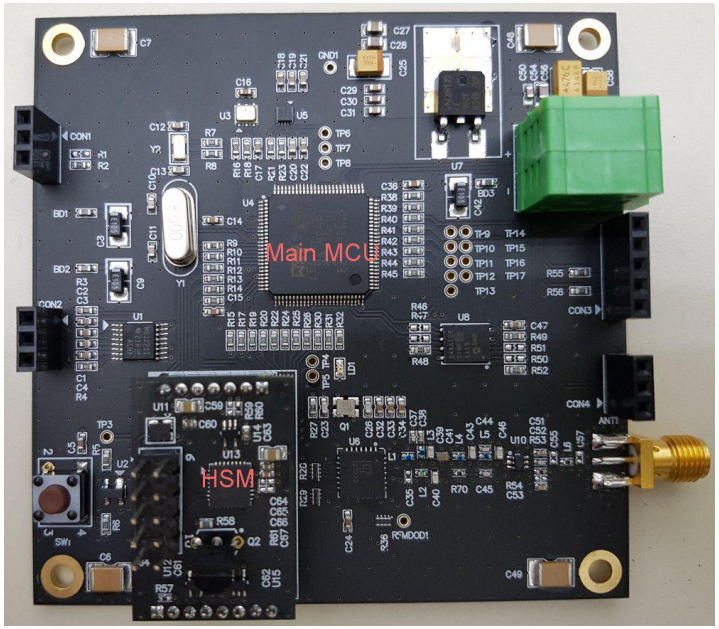
❖ (2) 하드웨어 보안모듈 기반 실행코드 무결성 검증 기술

- 상세설계서, 시험절차서 및 결과서, 소스코드

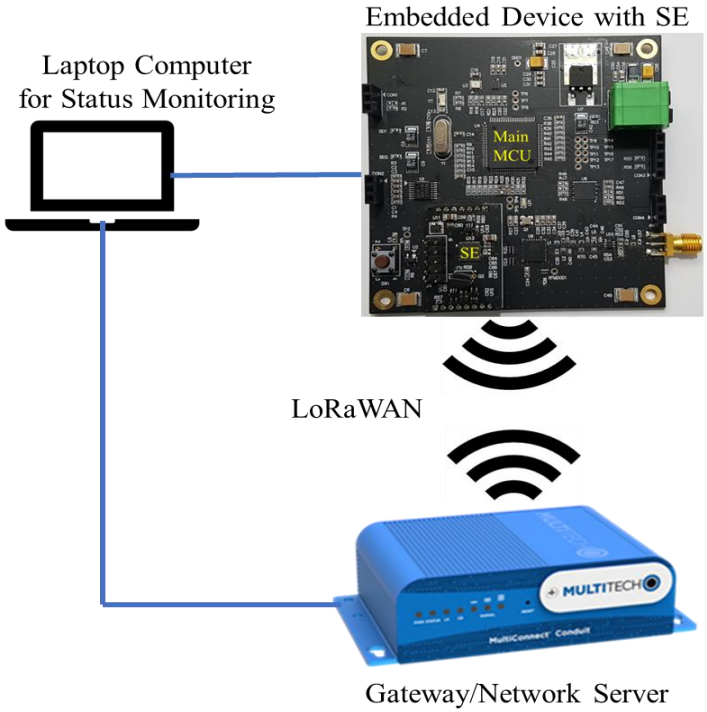


▣ 기술개발 현황

- ❖ 하드웨어 보안모듈 기반 LoRa통신 기술 개발
- ❖ 하드웨어 보안모듈 기반 실행코드 무결성 검증 기술 개발



< 하드웨어 보안모듈(HSM)기반 LoRa통신 보드 >



< HSM기반 LoRa통신 및
실행코드 무결성 검증 기술 test 환경>

▣ 기술 개발 현황

❖ 기술성숙도(TRL : Technology Readiness Level) 단계 :

구 분	단계	정 의	세 부 설 명
기초 연구 단계	1	기초 이론/실험	▪기초이론 정립 단계
	2	실용 목적의 아이디어 특허 등 개념정립	▪기술개발 개념 정립 및 아이디어에 대한 특허 출원 단계
실험 단계	3	실험실 규모의 기본성능 검증	▪실험실 환경에서 실험 또는 전산 시뮬레이션을 통해 기본성능이 검증될 수 있는 단계 ▪개발하려는 부품/시스템의 기본 설계도면을 확보하는 단계
	4	실험실 규모의 소재/부품/시스템 핵심성능 평가	▪시험샘플을 제작하여 핵심성능에 대한 평가가 완료된 단계 ▪3단계에서 도출된 다양한 결과 중에서 최적의 결과를 선택하려는 단계 ▪컴퓨터 모사가 가능한 경우 최적화를 완료하는 단계
시작품 단계	5	확정된 소재/부품/시스템 시작품 제작 및 성능 평가	▪확정된 소재/부품/시스템의 실험실 시작품 제작 및 성능 평가가 완료된 단계 ▪개발 대상의 생산을 고려하여 설계하나 실제 제작한 시작품 샘플은 1~수개 미만인 단계 ▪경제성을 고려하지 않고 기술의 핵심성능으로만 볼 때, 실제로 판매가 될 수 있는 정도로 목표 성능을 달성한 단계
	6	파일롯 규모 시작품 제작 및 성능 평가	▪파일롯 규모(복수 개~양산규모의 1/10정도)의 시작품 제작 및 평가가 완료된 단계 ▪파일롯 규모 생산품에 대해 생산량, 생산용량, 불량률 등 제시 ▪파일롯 생산을 위한 대규모 투자가 동반되는 단계 ▪생산기업이 수요기업 적용환경에 유사하게 자체 현장테스트를 실시하여 목표 성능을 만족시킨 단계 ▪성능 평가 결과에 대해 가능하면 공인인증 기관의 성적서 확보
실용화 단계	7	신뢰성평가 및 수요기업 평가	▪실제 환경에서 성능 검증이 이루어지는 단계 ▪부품 및 소재개발의 경우 수요업체에서 직접 파일롯 시작품을 현장 평가(성능 및 신뢰성 평가) ▪가능하면 인증기관의 신뢰성 평가 결과 제출
	8	시제품 인증 및 표준화	▪표준화 및 인허가 취득 단계
사업화	9	사업화	▪본격적인 양산 및 사업화 단계 ▪6-시그마 등 품질관리가 중요한 단계

3. 경쟁기술과 비교

▣ “하드웨어 보안모듈기반 LoRa통신 보안 기술”의 특징 및 장점

- ❖ IoT 디바이스가 LoRa통신에 필요한 키들을 물리적 해킹 방지가 가능한 “하드웨어 보안모듈”에 저장함은 물론이고, 이 하드웨어 보안모듈 내에서 암호화도 수행함으로써 LoRa통신의 보안성을 높일 수 있음

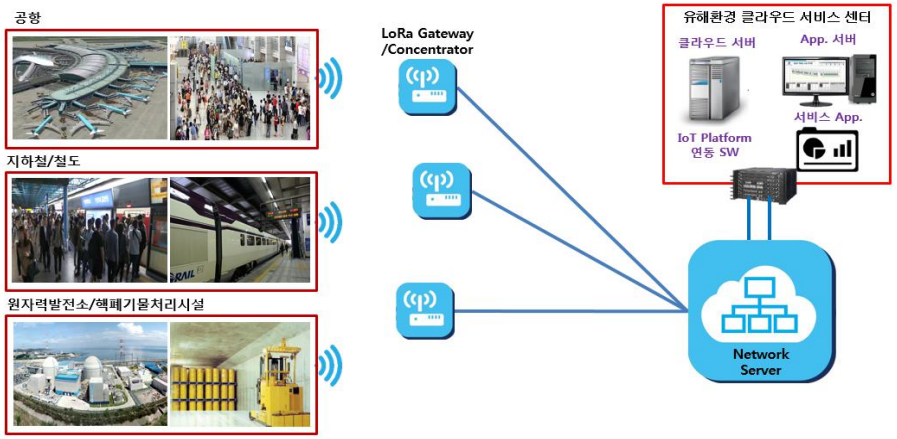
▣ 관련기술과 비교

- ❖ LoRa를 상용화한 SK telecom에서는 협력사(와이솔, 솔루엠 등)를 통해 LoRa통신 모듈을 제작하여 판매하고 있음. 그러나 이들 LoRa통신 모듈에는 별도의 하드웨어 보안모듈을 장착하고 있지 않음
- ❖ 또한 본 기술은 “하드웨어 보안모듈”을 이용하여 디바이스의 실행코드의 무결성을 검증하도록 하고 있음

4. 기술의 사업성 1/2

▣ 예상 응용 제품 및 서비스

❖ 보안성이 요구되는 IoT서비스(보안구역, 국가기반시설분야 등)에 적용



▣SWOT 분석

S 강점: 기존의 LoRa통신 IoT디바이스에 비해 우수한 보안성	**W 약점**: 하드웨어 보안모듈을 장착함으로써 디바이스의 단가 상승
O 기회: IoT 디바이스 해킹 사례 증가, IoT 디바이스 사용자들의 보안 관심 및 우려도 증가	**T 위협**: Io(S)T 기기 및 서비스를 겨냥한 새로운 보안위협의 증가

4. 기술의 사업성 2/2

▣ 사업성

- ❖ 5G통신망이 상용화됨에 따라 IoT환경은 급속도록 발전할 것이며, 이에 따라 IoT디바이스를 위한 LoRa통신 시장의 빠른 성장 예상
- ❖ 본 기술이 적용된 LoRa통신 모듈은 기존 제품에 비해 보안성이 훨씬 강화됨에 따라 높은 가격을 받을 수 있음

▣ 기술이전 업체 조건

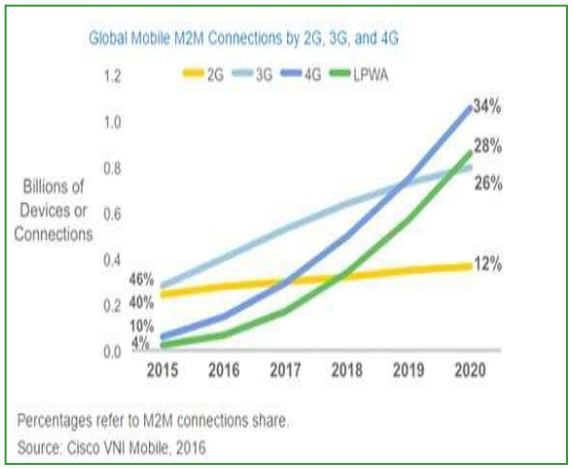
- ❖ 본 기술을 적용한 LoRa통신 모듈 개발 및 테스트를 위한 작업 필요
- ❖ 업체가 하드웨어 보안모듈용 칩에 대한 수급 필요

▣ 사업화의 애로점과 극복(개선)방안

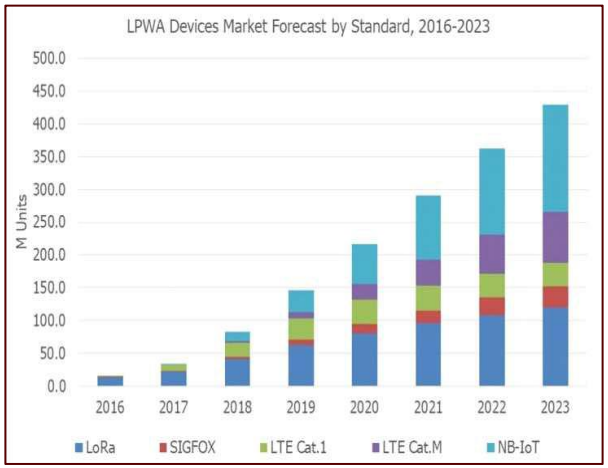
애로점	극복(개선)방안
하드웨어 보안모듈을 장착함으로써 디바이스의 단가 상승	하드웨어 보안모듈을 이용함으로써 보안성이 향상됨으로 인해, 제조 단가상승을 상쇄할 수 있음을 지속적으로 홍보

▣ 현황 및 시장 전망

- ❖ 2020년까지 800억대 IoT 기기 연결 예상
- ❖ IoT 시장의 무선기술 중에서 LPWA의 가파른 성장이 예측
- ❖ 세계 IoT 보안 시장: 연평균 44% 성장, 2022년 43억달러 예상
- ❖ 국내 IoT 보안 시장: 2022년까지 14조원 규모 예측 (세계시장규모의 3%로 예측)



<무선시장 예상점유율>



<LPWA 무선시장 예상 점유율>

<IoT 보안 시장 예상 규모>

감사합니다.

www.etri.re.kr

※ 하단의 문의처 소개후, 발표후 개별기술 상담이 가능함을 다시 한 번 안내함

♣ 연락처 : 지능화융합연구소(정보보호연구본부), 전용성 책·연 (042-860-5855, ysjeon@etri.re.kr)