

M-S2X 통신 활용을 위한 보안 위협 및 요구사항 분석

이성록* · 김미경** · † 장형진

*한국정보통신기술협회

요약 : 해양에서의 선박 대 선박, 선박 대 시설 등 장비 간 통신 서비스를 제공하기 위한 M-S2X 기술 적용 시 발생할 수 있는 보안 위협을 분석하고, 적용 가능한 보안요구사항을 도출하였다.

핵심용어 : M-S2X, 선박 중심 직접 통신, 보안

M-S2X 개요

- M-S2X (Maritime Ship to Everything)
 - 선박 중심 직접 통신
 - 해상에서 선박 간 통신(Ship-to-Ship), 선박-인프라통신(Ship-to-Infrastructure) 등 선박이 인프라 및 다른 선박과 통신하면서 해상 교통상황 등 정보를 공유/교환하기 위한 통신 기술을 의미

※ 출처: "초고해상도무선통신망 무선설비 다각화 및 통신망계 기술개발" 연구계획서, 선박해양플랜트연구소

V2X 보안 위협 및 보안 요구사항

- V2X 보안 위협에 따른 보안 요구사항

위협	보안 요구사항			
	인증	암호	데이터보호	물리적보호
가용성 손상	○			
데이터 손실	○	○	○	
중간자 공격	○	○	○	
부적절한 암호 사용		○	○	
부적절한 접근 통제	○		○	
부적절한 물리적 통제			○	○
악의적 프로그램 실행			○	
잘못된 설계 구현				
미흡한 사용자 권한 관리	○	○		
부적절한 인적 행위				○

V2X 기술 동향

- WAVE
 - IEEE 802.11a 무선랜 기술을 기반으로 자동차 주행 환경에 적합하도록 개정된 무선 통신 기술
- C-V2X
 - 이동통신 기술을 기반으로 차량간 통신에 적합하도록 개정된 무선 통신 기술
 - LTE 통신에서 5G 통신으로 변화 중

구분	WAVE (DSRC)	C-V2X
통신 기술	WiFi 기반	LTE, 5G 셀룰러 이동통신 기반
통신 거리	최대 1km	수 km
표준화	2012년 완료	2017년 완료
지연시간	0.1초 미만(100ms)	0.1초 미만(100ms)
전송 속도	최대 27Mbps	100Mbps 이상
경쟁	기술표준화 완료 오래 연구개발에 따른 안전성	커버리지, 전송속도 등 주요 성능 우수

M-S2X 보안 위협

- 보안 위협

분류	세부 항목
가용성 손상	DoS 공격으로 인한 내부 시스템 손상
	DoS 공격으로 인한 업데이트 방해
	단거리 통신 또는 센서 인식 방해
데이터 손실	의도하지 않은 서비스 중지
	메시지 차단
	데이터 변조
	데이터 삭제
	데이터 삽입
	의도하지 않은 데이터 손실
	의도하지 않은 데이터 유출
로그 데이터 조작	
	메시지 위·변조

† 교신저자 : chj760@tta.or.kr
* slping@tta.or.kr
** kimmi@tta.or.kr

M-S2X 보안 위협

● 보안 위협

분류	세부 항목
중간자 공격	세션 하이재킹
	스니핑 공격(sniffing attack)
	중간자 공격(MITM attack)
부적절한 암호 사용	암호키 노출
	취약한 암호화 사용
부적절한 접근 통제	서버에 논리적(네트워크) 비인가 접근
	중요정보 비인가 접근
	시스템 변조
	전자 ID 불법적 변경

M-S2X 보안 요구사항

● 보안 요구사항 세부 항목 - 1

보안 항목	세부 사항
인증	<ul style="list-style-type: none"> • 사용자 인증 • 인증정보의 안전한 사용 • 장치 인증 • 메시지 인증
암호	<ul style="list-style-type: none"> • 안전한 암호 알고리즘 사용 • 안전한 키 관리 • 안전한 난수 생성
데이터 보호	<ul style="list-style-type: none"> • 전송 데이터 보호 • 저장 데이터 보호 • 암호화/복호화 • 개인정보 보호 • 접근 통제 • 악성 프로그램 대응 • 안전한 복구

M-S2X 보안 위협

● 보안 위협

분류	세부 항목
부적절한 물리적 통제	USB 포트 등을 이용한 불법적 조작
	물리적 데이터 손실
	불법적 하드웨어 설치
	서버에 물리적 무단접근
악의적인 프로그램 실행	바이러스 감염
	변조된 펌웨어 업데이트
	악의적 메시지 수신
	악의적 소프트웨어 실행
	펌웨어 조작

M-S2X 보안 요구사항

● 보안 요구사항 세부 항목 - 2

보안 항목	세부 사항
물리적 보호	<ul style="list-style-type: none"> • 외부 입출력 포트 비활성화 • 내부 입출력 포트 접근 방어 • 악용 방지

M-S2X 보안 위협

● 보안 위협

분류	세부 항목
미흡한 사용자 권한 관리	불법적 권한 상승
	불법적 권한 획득
	시발 공격(Sybil attack)
	신원 사기 (Identity fraud)
부적절한 인적 행위	사용자 부주의

M-S2X 보안 요구사항

● 요구 사항 별 적용 범위 - 인증

- 시스템에 저장되어 있는 민감 정보에 비인가된 접근을 차단해야 함.

보안 항목	적용 범위				
	S2S	S2I	S2N	S2A	S2P
사용자 인증		○	○		
인증정보의 안전한 사용	○	○	○	○	
장치 인증	○	○	○	○	
메시지 인증	○	○	○	○	

M-S2X 보안 요구사항

TTA

● 요구 사항 별 적용 범위 - 암호

- 중요 정보 암호화를 통해 데이터 저장 및 전송 시 위·변조되는 것을 방지해야 함

보안 항목	적용 범위				
	S2S	S2I	S2N	S2A	S2P
안전한 알고리즘	○	○	○	○	○
안전한 키관리	○	○	○	○	○
안전한 난수 생성	○	○	○	○	○

14

M-S2X 보안 요구사항

TTA

● 요구 사항 별 적용 범위 - 데이터 보호

- 선박 중심의 통신 서비스 제공을 위해서 저장 및 전송되는 중요정보 및 민감정보는 안전하게 관리되어야 함

보안 항목	적용 범위				
	S2S	S2I	S2N	S2A	S2P
전송 데이터 보호	○	○	○	○	○
저장 데이터 보호	○	○	○	○	○
정보흐름통제	○	○	○	○	○
안전한 세션관리	○	○	○	○	○
개인정보 보호	○	○	○	○	○
접근통제	○	○	○	○	○
악성 프로그램 대응	○	○	○	○	○
안전한 복구	○	○	○	○	○

15

M-S2X 보안 요구사항

TTA

● 요구 사항 별 적용 범위 - 물리적 보호

- 중요 정보 암호화를 통해 데이터 저장 및 전송 시 위·변조되는 것을 방지해야 함

보안 항목	적용 범위				
	S2S	S2I	S2N	S2A	S2P
외부 입출력 포트 비활성화	○	○	○	○	○
내부 입출력 포트 접근 방어	○	○	○	○	○

16

후 기

본 논문은 해양수산부 해양수산과학기술진흥원의 지원을 받아 수행하는 “초고속해상무선통신망 무선설비 다각화 및 통신연계 기술개발 연구”의 일부 내용임을 밝힙니다.