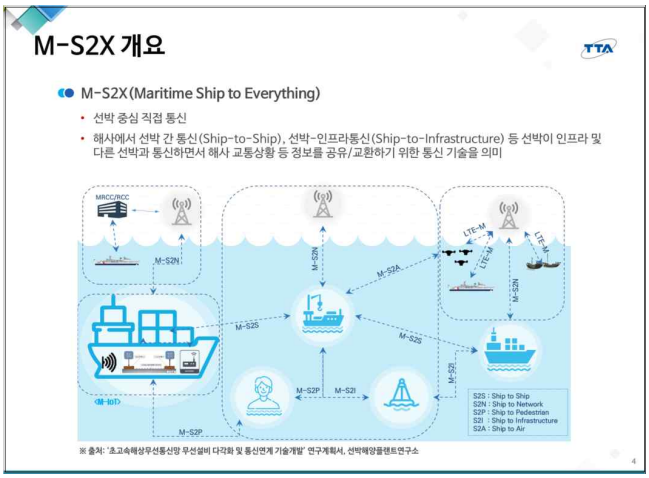
M-S2X 통신 활용을 위한 보안 위협 및 요구사항 분석

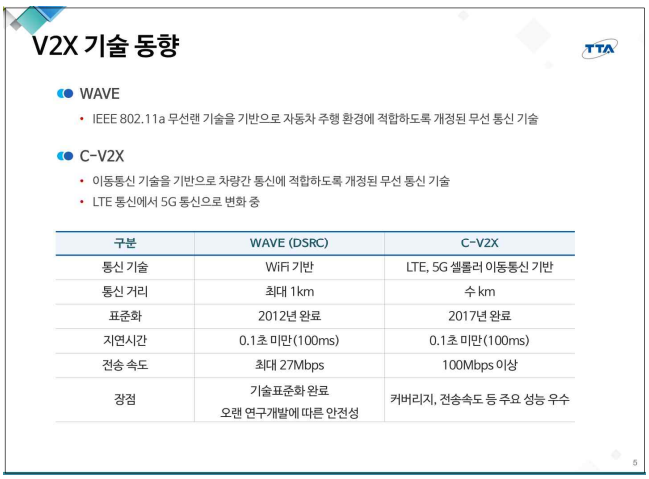
이성록* · 김미경** · † 장형진

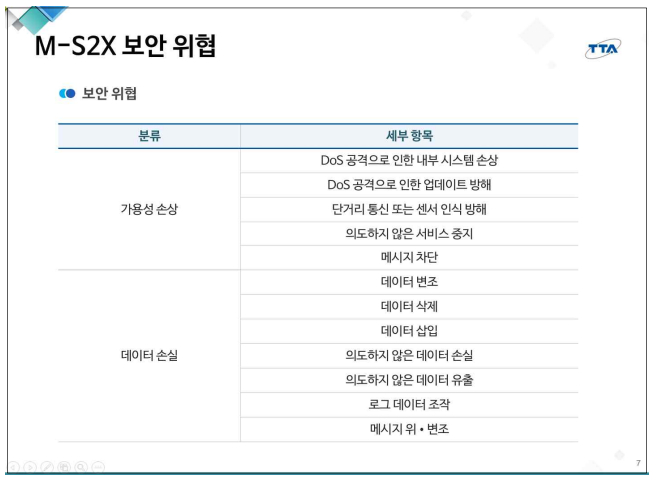
*한국정보통신기술협회

요 약 : 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







† 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

8

M-S2X 보안 요구사항

보안 요구사항 세부 항목 - 1

보안 항목	세부 사항
인증	• 사용자 인증 • 인증정보의 안전한 사용 • 장치 인증 • 메시지 인증
암호	• 안전한 암호 알고리즘 사용 • 안전한 키 관리 • 안전한 난수 생성
데이터 보호	• 전송 데이터 보호 • 저장 데이터 보호 • 정보흐름통제 • 개인정보 보호 • 접근 통제 • 악성 프로그램 대응 • 안전한 복구

11

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

9

M-S2X 보안 요구사항

보안 요구사항 세부 항목 - 2

보안 항목	세부 사항
물리적 보호	• 외부 입출력 포트 비활성화 • 내부 입출력 포트 접근 방어 • 악용 방지

12

M-S2X 보안 위협

보안 위협

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

10

M-S2X 보안 요구사항

요구 사항 별 적용 범위 - 인증

- 시스템에 저장되어 있는 민감 정보에 비 인가된 접근을 차단해야 함.

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

13

후 기

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