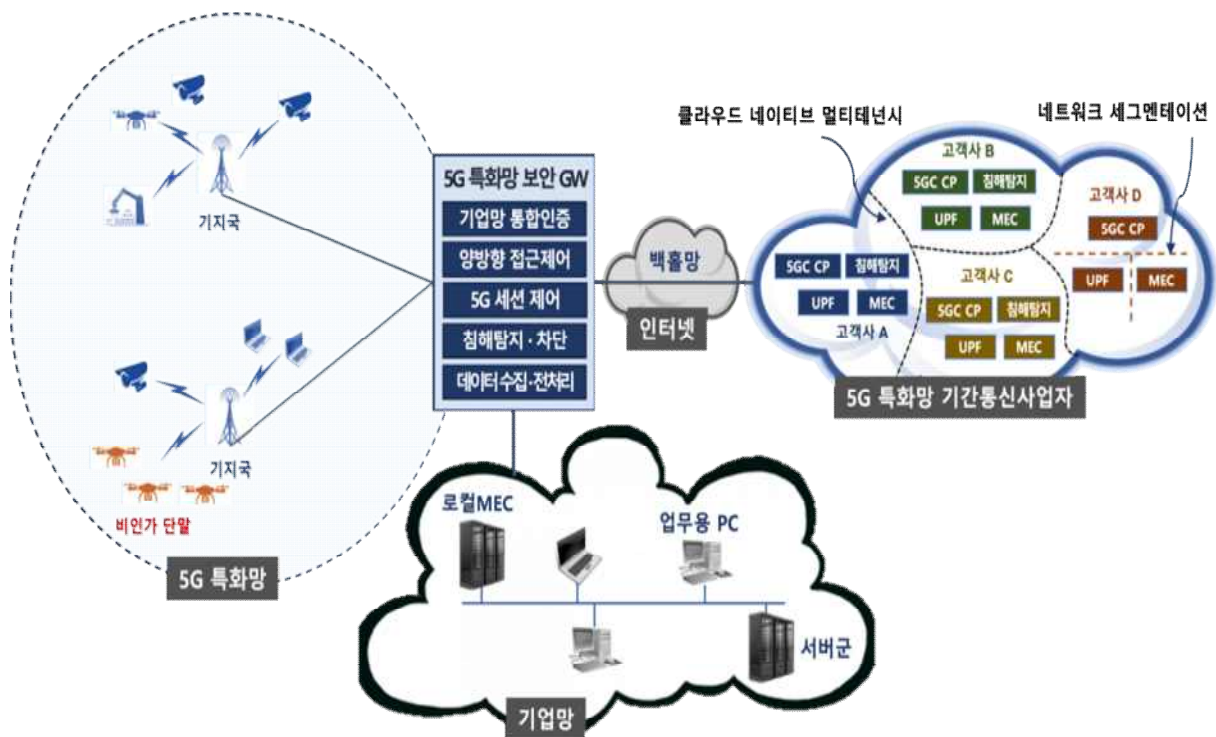


관리번호	2024-099	(지정공모형)
기술분류	대분류(차세대보안)-중분류(네트워크보안)-소분류(무선네트워크 보안)-세분류(이동 통신망 보안)	
중점분야	AI(), AI반도체(), 5G·6G(), 양자(), 메타버스(), 사이버보안(√)	
기획유형	임무지향형R&D(√), 문제해결형R&D(), 기술축적형R&D()	
과제명	특화망·기업망 통합보안을 위한 5G 특화망 보안 기술개발	

1. 개요

- 5G 이동통신망은 전국 단위 망을 통해 범용 서비스를 추구하나 주파수 특성상 4G 대비 셀 커버리지 제약으로 전국망 구축이 어려워, 수요처 건물·토지 등 제한된 영역에서 맞춤형 융합서비스 실현이 용이한 5G 특화망이 빠르게 확산되고 있음
- 5G 이동통신망과 달리, 특화망은 기간통신사업자 망과 연계된 다양한 구축 유형이 존재하고 수요처의 기존 망과도 연계·통합되어야 하므로, 안전한 5G 특화망 서비스를 위해서는 외부망과 연계된 환경에서 통합보안을 반드시 제공해야 함
- 그러나, 3GPP 표준에서 정의하는 단말과 코어망 구간 사이의 보안을 제공하는 5G 보안 기술만으로는 5G 특화망 서비스의 보안을 보장할 수 없음
- 따라서, 외부망 연계 등으로 공격접점이 확대된 5G 특화망에서 지능화·고도화되는 보안위협으로부터 특화망 서비스를 안전하게 보호하기 위해서는 기간통신사업자망과 수요처의 망(기업망)이 통합된 환경에서의 보안모델 정립 및 지능형 침해대응 기술개발이 시급함



<5G 특화망·기업망 통합보안 개념도>

2. 현황 및 필요성

- **(기존 기술현황)** 전 세계적으로 5G 특화망(이음5G) 구축 및 도입이 빠르게 확산되고 있으나, 5G 특화망에 대한 보안 모델이 부재하고, 안전한 5G 특화망을 바탕으로 디지털 대전환을 위한 사이버보안 기술 연구는 아직 미흡한 실정임
 - 과학기술정보통신부는 5G 특화망 정책방안('21.1.26), 5G 특화망 주파수 공급방안('21.6.29), 5G 특화망 가이드라인('21.10.) 등의 발표를 통해 5G 특화망(이음 5G) 활성화 정책을 강화하고 있음
 - 네이버클라우드, LG CNS, ETRI 등 25개 기관 46개소에 대해 이음5G 주파수 할당 또는 지정을 완료('23.10. 기준)하는 등, 다양한 산업 영역에서의 이음5G 도입 및 구축이 지속해서 확산될 전망
 - 과학기술정보통신부는 '30년까지 약 1,000개소의 5G 특화망 구축 및 약 3조 원의 투자가 촉진될 것으로 전망 ('22.12.01)
 - 독일, 일본, 영국, 미국 등은 우리나라보다 일찍 5G 특화망(Private 5G) 서비스를 도입했으며, 제조, 물류, 교육 등 다양한 분야에서의 적용 사례 증가
 - **(정부지원 필요성)** 정부의 5G 특화망 활성화 정책 추진에 따라 다양한 산업 영역에서의 **주 국가적 5G 특화망 기반 안전한 디지털 대전환을 보장하고, 6G 보안의 핵심 요소기술 및 IPR을 선제적으로 확보**하기 위해 정부의 지원이 시급함
 - 전 세계적으로 5G 특화망에 기반한 맞춤형 융합서비스 실현이 가속화될 것으로 전망됨에 따라, 5G 특화망 보안모델 및 솔루션 부재로 인한 디지털 대전환의 차질이 발생하지 않도록 5G 특화망 보안 기술개발이 시급함
 - 주파수 대역 특성상 6G는 불가피하게 5G 특화망과 같은 지역화(localization)·분산화로 인한 외부망 연계·통합이 더욱 심화될 것이므로, 6G 보안의 요소기술 개발 및 지식재산권 확보를 위해 정부 지원이 요구됨
 - **(기술성)** 현재 5G 특화망 구축 및 도입이 확산되고 있으나, 5G 특화망에 대한 보안위협 분석 및 사이버 공격의 탐지·대응 기술 연구는 미흡한 실정임
 - 5G 특화망이 독립망 형태 외에도 5G 특화망 기간통신사업자를 통한 서비스형 구축이 더 큰 비중을 차지할 것으로 전망됨에 따라 구축 유형별 보안성을 강화하기 위한 보안 모델의 연구가 필요함
 - 5G 특화망이 궁극적으로 기존 기업·기관망을 대체하거나 완전한 통합이 이루어질 것으로 전망됨에 따라, 5G 특화망과 기업·기관망 간 보안위협이 상호 침투되지 않도록 탐지·차단할 수 있는 망 연계 또는 통합 보안 기술개발이 필요함*
- * 5G 특화망을 우리나라보다 먼저 도입한 독일, 영국, 일본, 미국의 기업을 대상으로 조사한 설문에 따르면, 5G 특화망 구축시 가장 큰 장애 요소로서 수요기관이 보유한 기존 네트워크 및 시스템과의 통합 문제를 꼽은 바 있음 (The Economist Group, 2021)
- 5G 특화망의 확대를 통한 국내 기업과 기관의 디지털 전환을 지원하기 위해, 잠재된 보안 우려를 해소하고 안전한 서비스 환경을 제공하는 보안 기술이 필요함

- (경제성) 초고속 성장하는 5G 특화망 보안 시장에서 국내 보안기업의 기술 및 시장 경쟁력 제고
 - 글로벌 5G 보안 시장이 '22년 13억 달러에서 '27년 72억 달러로 5.5배(연평균 41.6%) 초고속 성장하며, 핵심 수요는 5G 특화망이 견인할 것으로 전망함 (Marketsandmarket.com)
 - 이와 같이 초고속 성장이 전망되는 특화망 중심의 해외 5G 보안 시장으로의 국내 보안기업 시장 진출 기반 확보 및 수출 경쟁력 강화
 - 글로벌 보안기업으로부터 국내 5G 특화망 시장 잠식을 차단하고 국내 보안기업의 경쟁력 확보 기반 마련

3. 수요분석

- (주요 수요처) 5G 특화망(이음 5G) 및 5G 이동통신서비스 이해당사자
 - 5G 특화망 수요(예정)기관 (민간기업 및 정부·공공기관)
 - 5G 특화망 기간통신사업(예정)자
 - 5G 특화망 네트워크 장비 및 솔루션 제공 기업 (특히, 국내 보안기업)
 - 5G 이동통신사업자 등
- (협력방안) 실질적인 5G 특화망 보안 모델 정립과 연구개발 결과물의 실효성 검증을 위해 5G 특화망 수요기관, 기간통신사업자, 5G 특화망 네트워크 장비 및 솔루션 제공 기업이 포함된 연구협의체를 구성하고, 연 2회 이상 연차별 개발 기술에 대한 요구사항·방향성 검토 및 결과물 통합·검증 실시

4. 연구목표

- 최종목표 : 기존 기업망과의 신뢰 통합을 보장하고 안전한 5G 특화망 서비스 이용 환경을 제공하기 위한 5G 특화망 보안 모델 정립 및 지능형 침해대응 기술 개발
 - 5G 특화망 보안 모델 개발
 - 기간통신사업자 클라우드 기반 5G 특화망 백홀 보안 기술 개발
 - 외부망과의 보안을 위한 HW 기반 5G 특화망 보안 게이트웨이 개발
 - 지능형 5G 특화망 침해위협 탐지 및 보안 상황 가시화 기술 개발
 - 5G 특화망·기업망 통합 보안 검증 환경 구축 및 실증

○ 단계별 목표

구분	단계별 연구목표
1단계	▪ 5G 특화망 구축 유형별·서비스별 보안 모델 개발 ▪ 5G 특화망 백홀 보안 시제품 개발 ▪ HW 기반 5G 특화망 보안 게이트웨이 시제품 개발
2단계	▪ HW 기반 5G 특화망 보안 게이트웨이 상용시제품 개발 ▪ 지능형 5G 특화망 침해위협 탐지 및 보안상황 가시화 기술 상용시제품 개발 ▪ 5G 특화망·기업망 통합 보안 검증 환경 구축 및 실증

○ 정량적 연구개발목표

성능지표	단위	연구개발 목표치		연구개발 전 국내 수준	세계 최고수준 (보유국/보유기관)
		1단계(24~25)	2단계(26~27)		
1	5G 특화망 보안취약성 검증 및 진단 항목	개	2	5	-
2	5G 특화망 보안 게이트웨이 트래픽 처리 성능	Gbps	20	100 ¹⁾	-
3	자가학습 기반 침해탐지의 전이·변환 모델 평균 탐지정밀도 ²⁾	F1-Score ³⁾	90 ⁴⁾	95	93.04 ⁵⁾ (호주, Univ. of Queensland)

1) 5G 특화망 보안 게이트웨이 트래픽 처리 성능 목표치 설정 근거는 현재 5G 이동통신사업자의 백본 회선 용량이 100Gbps 인 점, 향후 5G 특화망 서비스 트래픽 처리량 폭증 가능성, 연구개발 과제로서 상용화 시점 등을 복합적으로 고려하여 산정함

2) 평균 탐지정밀도란, 자가학습 기반 침해탐지 모델의 정밀도와 이 모델을 他 환경에 전이·변환한 모델의 정밀도의 산술 평균값

3) $F1\text{-score} = 2 \times (\text{precision} \times \text{recall}) / (\text{precision} + \text{recall}) = TP / [(TP + 1/2(FP + FN))]$

* TP:true positive, FP:false positive, FN:false negative

4) 1단계 연구개발 목표는 단일 자가학습 기반 침해탐지 모델의 탐지정밀도이며, 2단계 연구개발 목표는 전이·변환 모델의 평균 탐지정밀도임

5) 서로 다른 데이터셋에 대해 모델 전이를 통한 탐지정밀도의 평균값

* E. Caville, et.al., "Anomal-E: A Self-Supervised Network Intrusion Detection System based on Graph Neural Networks", Knowledge-Based Systems, Vol. 258, pp.1-11, 2022

5. 연구내용

① 5G 특화망 보안 모델 개발

- 5G 특화망 보안취약성 분석 및 구축 유형별 보안 위협 도출
- 5G 특화망 구축 유형별 인증·무결성·기기 신뢰성 등 보안 요구사항 분석
- 5G 특화망 구축 유형별·서비스별 보안 모델 설계
- 5G 특화망 보안취약성 검증 및 진단 도구 개발

② 기간통신사업자 클라우드 기반 5G 특화망 백홀 보안 기술 개발

- 클라우드 네이티브 네트워크 기반 패킷 필터링 및 QoS 제어 기술 개발
- 공유형 특화망 코어 보호를 위한 클라우드 네이티브 멀티테넌시 기술 개발
- 공유형 특화망 코어에서의 침해 확산 차단을 위한 네트워크 세그멘테이션 기술 개발

③ 외부망과의 보안을 위한 HW 기반 5G 특화망 보안 게이트웨이 개발

- 3GPP 인증 표준*과 연동 가능한 5G 특화망·기업망 통합·다중 인증 기술 개발
- 단말 인증 및 권한 정보 기반 5G 특화망·기업망 간 동적 양방향 접근제어 기술 개발
- 5G 특화망·기업망 간 동적 5G 서비스 세션** 경로 제어 기술 개발
- 지능형 침해위협 탐지를 위한 데이터셋 수집, 로컬 전처리 및 최적화 기술 개발

* 인증 관련 3GPP 표준 프로토콜로는 대표적으로 5G-AKA와 EAP-AKA' 프로토콜을 꼽을 수 있음

** 5G 특화망의 구축 유형에 따라 경로 제어해야 할 5G 서비스 세션은 5G 네트워크 구조에서의 N3, N6 또는 N9 트래픽으로 달라질 수 있음

④ 지능형 5G 특화망 침해위협 탐지 및 보안 상황 가시화 기술 개발

- 5G SBA NF* 기반 클라우드 네이티브 지능형 침해위협 탐지 플랫폼 개발
- 5G 특화망 데이터 불균형/比 라벨링을 고려한 자가학습 기반 침해위협 탐지 기술 개발
- 특화망 서비스 및 수요기관별 고유 특성을 고려한 AI 모델 전이·변환 기술 개발
- 5G 특화망 무선 신호 기반 지능형 비인가·허위 단말 탐지 기술
- 5G 특화망 네트워크 이상징후 모니터링, 추적 및 실시간 가시화 기술 개발

* 5G SBA NF: 5G 코어망의 서비스 기반 구조(Service Based Architecture)를 따르는 네트워크 기능(Network Functions)으로서, 5G 코어망과의 긴밀한 연동을 위해서는 5G 코어망의 기본 기능(예, AMF, SMF 등)과 동일한 구조와 표준 기반 인터페이스를 따라야 함

⑤ 5G 특화망·기업망 통합 보안 검증 환경 구축 및 실증

- 상용 5G 특화망 장비 기반 통합 보안 실증 테스트베드 환경 구축
- 실증 효과성 제고를 위한 검증 항목 도출 및 실증 시나리오 개발
- 5G 특화망 보안 기술의 실효성 검증을 위한 실증서비스

6. 기대 효과

- 이음 5G 도입 기업·기관의 보안 우려를 해소하고 안전한 서비스 이용 환경을 보장함으로써 산업 전반의 디지털 대전환 가속화
- 초고속 성장하는 5G 특화망 보안 시장에서 국내 보안기업의 기술·시장 경쟁력 제고 및 시장 잠식 차단
- 2027년까지 72억 달러(Marketsandmarkets.com 추산) 규모로 초고속 성장이 예상되는 특화망 중심의 글로벌 5G 보안 시장 진출 기반 확보
- 5G 특화망 기반 융합서비스(스마트공장, 스마트시티, 자율이동체 등)에서 보안을 강화하고, 고도화되는 사이버 공격으로부터 ICT 자산을 안전하게 보호
- 현재 3GPP를 통해 표준화가 진행중인 5G-Advanced 기술뿐만 아니라, ITU에서 비전 논의가 진행중인 미래 6G 보안을 위한 핵심원천기술 확보

7. 지원기간/예산/추진체계

- 연구개발기간 : 4년 이내 (1단계 2년→2단계 2년)
- 정부지원연구개발비 : '24년 18억원 이내(총 정부지원연구개발비 90억원 이내)

구분		기간	개월수	정부지원연구개발비
1단계	1년차	'24.4월~'24.12월	9개월	1,800 백만원 이내
	2년차	'25.1월~'25.12월	12개월	2,400 백만원 이내
2단계	3년차	'26.1월~'26.12월	12개월	2,400 백만원 이내
	4년차	'27.1월~'27.12월	12개월	2,400 백만원 이내
합계		-	45개월	9,000 백만원 이내

* 연차별 정부지원연구개발비는 당해연도 예산심의결과에 따라 변동될 수 있음

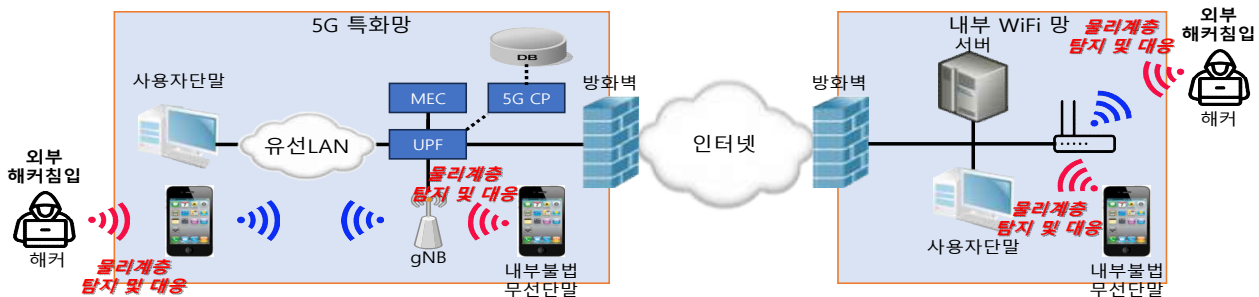
- 주관기관 : 제한없음

연구유형	기초연구 (), 응용연구 (), 개발연구 (√)	TRL (4)~(7)단계
과제특징	경쟁형(), 경쟁형(챌린지)(), SW자산뱅크등록(), 공개SW(), 기술료비징수() 국제협력R&D(), 정책지정(), 혁신도약형(√), 표준화연계(), 사회문제해결형(), 일자리연계(), 소재부품장비(), 규제샌드박스(), 연구데이터공개(), 사업화연계(), IP-R&D연계()	
구분		기술분야명/팀명
책임PM(과제기획위원장)		보안·블록체인
담당 팀장		사이버보안팀
		성명
		정현철
		김남훈

관리번호	2024-102	(품목공모형)
기술분류	대분류(차세대보안)-중분류(네트워크보안)-소분류(무선네트워크보안)-세분류(무선근거리통신망보안)	
중점분야	AI(), AI반도체(), 5G·6G(), 양자(), 메타버스(), 사이버보안(√)	
기획유형	임무지향형R&D(√), 문제해결형R&D(), 기술축적형R&D()	
품목(문제)명	무선 통신채널 멀티모달 속성을 활용한 보안 핵심기술 개발	

1. 품목(문제) 정의

- (개념) 본 개발은 무선 통신 환경에서 새롭게 발생하는 보안위협을 해결하기 위해 물리적 특성을 활용하는 보안기술을 통해 대책을 마련하고자 함
 - 무선 통신망의 운용 시 물리계층을 통해 발생하는 취약성을 극복하고, 더 안전하고 효율적인 무선 통신을 실현하기 위해서 무선 통신망 물리계층의 고유특성을 활용하는 물리계층 보안 핵심기술을 개발 및 실증 추진
 - 기존의 무선 통신 보안 문제를 해결하기 위해 물리적 특성과 계층간 상호인증을 중점으로 다루며, 이를 통해 보다 강력한 무선 통신보안 기술을 마련



<무선 통신망 물리계층 고유특성을 활용한 물리계층보안 개념도>

- (목표) 무선 통신망의 물리계층 고유특성을 활용하여 디바이스 인증과 물리계층보안을 강화하며, 무선 디바이스를 정확하게 식별·인증하고 악의적 활동을 탐지하고 대응하는 보안기술 및 실증 플랫폼 개발

As is	To Be
○ (상위계층 보안 기술) 무선 통신망의 상위 계층에서 보안을 제공하며, 계산 복잡도 기반의 수학적 알고리즘(암호)을 사용하여 보안을 구현(예 : TLS 보안 프로토콜 등) ○ (무선계층 보안 취약) 물리계층에서의 취약성으로 인해 외부 공격자가 무선 통신을 도청하거나 조작할 수 있는 위험이 있으며, 물리계층에서의 취약성을 보완할 대책이 부재하며, 공격을 감지하거나 방어할 방법이 제한적임(예, 무선 신호 스니핑 등) ○ (계층간 상호인증 미제공) 무선 통신망의	○ (물리계층 보안 기술) 무선 통신망의 물리 계층에 보안을 적용하기 위해, 무선 통신 디바이스의 물리적 특성과 무선 통신 물리 계층의 고유 특성을 활용하여 보안을 구현 ○ (무선계층 보안 강화) 물리계층 보안 기술을 통해 무선 통신망의 물리적 취약성을 보완하고 외부 공격자의 무단 접근을 어렵게 할 뿐만 아니라 무단 접근을 탐지하고 방어하는 데 도움을 줌으로써 보안대책이 강화되며, 무선 통신망이 더 안전해짐 ○ (계층간 상호인증 제공) 무선 통신망의 상위

As is	To Be
상위계층과 물리계층 간에 상호인증이 고려되지 않아 물리계층 취약성으로 전반적인 무선 통신 환경 보안 취약점 발생	계층과 물리계층 간 강력한 상호인증을 제공하여 물리계층 취약성에 대한 보안대책을 강화

○ (연구내용)

- 전파 신호의 특징, 무선 채널의 특징 등 무선 통신의 물리계층 고유특성 실시간 추출 및 이의 비정형성을 이용한 고비도(High-Security) 보안 크리덴셜 생성 기술 개발
- 생성된 고비도 보안 크리덴셜 기반의 RoT(Root of Trust) 유도 및 이를 이용한 디바이스 식별·인증 및 다계층 협력 비정상 행위 탐지·대응 기술 개발
- 다양한 무선 통신 물리계층(WLAN, WPAN 등) 고유특성 활용 다계층 보안 실증 시나리오 개발 및 시나리오 기반 보안 기능 실증 플랫폼 개발
- * (다양한 무선 통신 활용 연구) 본 개발을 통해 다양한 근거리 무선 통신망(예, Wi-Fi, Bluetooth, NFC, RFID, Zigbee, LoRa 등) 뿐만 아니라 이동 통신망(예, 5G, LTE 등)에도 적용할 수 있는 물리계층 보안 핵심기술로 활용할 수 있도록 개발

2. 현황 및 필요성

- (기존 기술현황) 현재까지 개발된 무선통신 보안 기술은 대부분 무선통신의 상위 계층에서 제공되며, 주로 수학적 알고리즘을 활용한 계산 복잡도 기반의 암호 알고리즘을 사용
 - 무선통신 보안 취약성이 나타나고 있으며 이를 활용한 무선통신 구간에서의 공격이 증가하고 있는 상황임
 - * (취약성 사례1) 일부 자동차는 무선통신을 사용하여 차량 문을 잠그거나 여는 데에 RFID 또는 무선신호를 사용하며, 공격자가 이러한 신호를 잡아서 나중에 차량에 접근하거나 훔칠 수 있는 사례 존재
 - * (취약성 사례2) WiFi 네트워크의 신호 재전송은 공격자가 무선 네트워크에 접근하지 않은 장소에서 네트워크 트래픽을 중계할 수 있게 하며, 이를 통해 트래픽 도청, 중요 정보 탈취, 또는 악의적인 중간자 공격이 발생
 - 기존 무선통신 보안 기술은 무선통신의 물리계층의 고유한 특성을 활용하지 못하고 있기때문에 물리적 상호인증 및 데이터링크 계층 보호에 있어 한계점 존재
 - * (한계점 사례1) 물리 계층 무선신호의 스니핑 공격을 실시하는 악의적인 공격자는 무선신호를 수신하여 정보를 스니핑하거나 변조할 수 있으며, 이러한 공격은 상위계층의 보안 기술을 통해 감지하는데 한계가 있음
 - * (한계점 사례2) 공격자는 물리 계층에서 무선 신호를 조작하고 재전송하는 것을 통해 거짓 인증을 수행할 수 있으며, 이러한 공격은 물리 계층의 고유한 특성을 활용하는 공격으로 상위계층의 보안 기술을 통한 대책 마련에 한계 존재
- (해외 연구현황) 무선통신 네트워크 기술의 고도화와 더불어 사이버 공격 기법도 진화하고 있어서 더 다양한 사이버 위협에 대응할 수 있게 연구 중임
 - (미국) MIT, Georgia 공대 등에서 무선 통신 보안과 관련된 다양한 연구가

이루어지고 있으며, 특히, 전파 신호의 특징을 활용한 보안 기술 및 무선 네트워크에서의 새로운 보안 프로토콜에 대한 연구를 진행 중임

- (중국) 칭화대학교(Tsinghua University)에서는 무선 통신 보안 및 디바이스 인증과 관련된 연구를 수행하고 있으며, 전파 신호를 활용한 보안 기술과 무선 네트워크에서의 신뢰성을 향상시키는 연구를 진행하고 있음
- (일본) 정보통신기술연구기구(NICT)에서는 무선 통신 보안과 관련된 연구를 활발히 진행하고 있으며, 특히, 다양한 무선 통신 기술에 대한 보안 측면에서의 연구를 실시하고 있음
- (유럽) 유럽연합 사이버보안 기관인 ENISA는 무선 통신 보안과 관련하여 다양한 연구와 가이드를 제공하고 있으며, 특히 무선 통신의 새로운 보안 동향과 취약점에 대한 연구를 수행하고 있음

○ **(해외 업체현황)** 해외에서 다양한 기업에서 물리계층 보안과 관련한 개발 및 산업 적용이 이뤄지고 있음

- (CommScope) 물리계층 보안을 통한 데이터 보호 강화를 위해 물리계층 위협 모니터링/검출 시스템 개발 및 제공
- (Kumu Networks) 무선 통신에서의 물리계층 보안 기술을 개발하는 기업 중 하나이며, 특히, 전이중(Full-Duplex) 무선 통신에 관한 연구와 개발을 수행하고 있으며, 물리계층 보안을 통해 무선 네트워크 통신 안전성을 강화함
- (Raytheon BBN Technologies) 무선 통신 및 네트워크 보안 분야에서 연구 및 개발을 수행하는 회사로 물리계층 보안을 포함한 다양한 보안 솔루션을 제공
- (Huawei) 5G 네트워크 및 물리계층 보안 기술에 중점을 두고 연구 및 개발 수행
- (Rohde & Schwarz) 통신 및 보안 분야에서 다양한 솔루션을 제공하는 글로벌 기업 중 하나이며, 무선 통신 분야에서의 물리계층보안 기술을 개발하고 있음

○ **(필요성)** 5G 네트워크, 사물인터넷(IoT) 분야 등 무선통신 환경에서 안전한 통신 환경 제공과 더불어, 스마트 홈, 스마트 도시, 자동차 통신, 산업 자동화 및 기타 IoT 응용 분야에서 물리계층 취약성을 이용한 공격 시도에 대한 대책마련 필요

- 특히, 군사 및 국방 분야에서 물리계층의 고유특성을 활용하여 무선 통신의 보안성을 강화하는 것이 필요하며, 이를 통해 안전한 통신 환경을 지원할 필요 있음
- 물리계층 보안 기술 개발과 연구는 미래 무선통신 및 보안 분야에서 중요한 역할을 할 것으로 예측되며, 국가안보 및 산업 보안을 강화하는 데 중요

3. 수요분석

○ **(주요 수요처)**

- (정부 및 군사 기관) 무선 통신망 구축 및 운용 시 국가 및 군사 업무에 필수적인 보안 요구사항이 필요한 곳으로 물리계층 보안 강화된 무선 통신 운용 필요
- (통신 기업 및 네트워크 제공업체) 기업 업무에 또는 서비스 제공에 활용되는 무

선 통신망의 안전성 확보가 필요한 곳으로, 새로운 물리계층 보안 기술의 도입을 통해 네트워크의 보안을 강화할 필요가 있음

- (산업 자동화 및 스마트도시 프로젝트) 산업 자동화 및 스마트 도시 프로젝트에서는 IoT 및 무선 통신을 적극적으로 활용하고 있으며, 이러한 프로젝트에서 안전한 무선 통신망 활용을 위해 물리계층 보안은 필수적임
- (스마트 기기 제조/사용업체) 무선통신(IEEE 802.11, IEEE 802.15 등) 기반 스마트 기기(스마트 미터, 스마트 가로등, 자동차용 스마트 키 등)를 제작 또는 사용하는 기업에서 불법적인 접속을 물리계층부터 원천 차단하는 서비스로 활용 가능
- **(협력방안)** 성공적인 기술 개발을 위해 수요처와 협력하여 실제 보안 요구사항을 파악하고 이를 바탕으로 물리계층 보안 기술을 개발하는 방안 추진 고려
 - 또한, 수요처와 함께 시범사업 및 필드 테스트를 수행하여 개발된 기술의 성능을 검증하고 보안 문제에 대한 해결책 테스트를 고려하고, 수요처와의 지속적인 정보 교류를 통해 보안 이슈에 대한 인사이트를 공유하고, 공동 연구 및 협력 프로젝트 추진고려

4. 기대 효과

- **(정책적)** 무선 통신망 운용에 따른 보안 정책 강화 및 표준 확립
 - 물리계층보안 기술의 개발을 통해 국가는 무선 통신망 보안 정책을 강화할 수 있으며, 민감한 정보와 데이터를 무선 통신망을 통해 유통 시 안전성 보장
 - 본 사업 개발 결과물을 활용하여 보안 규제 및 표준을 개선하고 정립하는 데 도움이 될 것으로 예상
- **(기술적)** 무선 통신망 보안 기술 혁신과 보안 강화 가능
 - 물리계층 보안 기술은 무선 통신망 보안에 있어 새로운 접근 방식을 제공하며, 기존의 수학적 알고리즘에 의존하는 기술보다 더 강력한 보안 대책 제공
 - 무선 통신 간 안전한 통신을 보장하여 스마트시티, 스마트홈, 산업자동화 등 다양한 IoT 응용 분야의 보안을 강화하는 것이 가능해짐
- **(사회적)** 5G 등 무선 통신망 보안 강화와 더불어 국내 활용처 증대
 - 무선 통신망에서의 물리계층보안 적용은 5G 네트워크 및 기존 무선망의 보안성을 향상시킴으로써 국민적 신뢰성 확보에 기여
 - 특히, 군사 및 국방 분야에서의 무선 통신 보안을 강화하여 국가 안전과 군사 통신의 신뢰성 확보 가능
- **(경제성)** 보안 산업 성장 및 수출 기회 확대 가능
 - 물리계층보안 기술의 개발은 국내 보안 산업의 성장을 촉진하고 국내 기업의 경쟁력 강화에 기여
 - 무선 통신 보안 기술의 혁신은 국내 기술 기업에 수출 기회를 확대할 것이며, 국가의 수출 활성화에 기여

5. 개발기간/예산/추진체계

- 연구개발기간 : 3년 이내
- 정부지원연구개발비 : ‘24년 13억원 이내(총 정부지원연구개발비 47.66억원 이내)

구분	기간	개월수	정부지원연구개발비
1년차	'24.4월~'24.12월	9개월	1,300 백만원 이내
2년차	'25.1월~'25.12월	12개월	1,733 백만원 이내
3년차	'26.1월~'26.12월	12개월	1,733 백만원 이내
합계	-	33개월	4,766 백만원 이내

* 연차별 정부지원연구개발비는 당해연도 예산심의결과에 따라 변동될 수 있음

- 주관기관 : 제한없음

연구유형	기초연구 (), 응용연구 (), 개발연구 (√)		TRL (4)~(7)단계
과제특징	경쟁형(), 경쟁형(챌린지)(), SW자산뱅크등록(), 공개SW(), 기술료비징수() 국제협력R&D(), 정책지정(), 혁신도약형(√), 표준화연계(), 사회문제해결형(), 일자리연계(), 소재부품장비(), 규제샌드박스(), 연구데이터공개(), 사업화연계(), IP-R&D연계()		
구분		기술분야명/팀명	성명
책임PM(과제기획위원장)		보안·블록체인	정현철
담당 팀장		사이버보안팀	김남훈