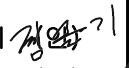
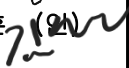


캡스톤디자인 II 계획서

제 목	국문	드론 기반 무선 네트워크의 보안 취약점 개선 및 알고리즘 개발
	영문	Improving security vulnerabilities and developing algorithms for drone-based wireless Networks
프로젝트 목표 (500자 내외)	<p>무선랜 디바이스의 통신 보안 취약점을 개선한 드론을 제작하는 것이다. 첫째, 무선랜 디바이스 간 교환되는 패킷을 암호화하여 데이터 도청 및 변조를 방지하고 통신의 기밀성을 보장한다.이 둘째, 인증해제 공격을 인지하고 대처할 수 있는 알고리즘을 개발하여, 공격 시도를 감지하면 즉시 사용자에게 알림을 제공한다. 셋째, GPS 신호의 진위 여부를 검증하는 신호 처리 알고리즘을 적용하여 GPS 스푸핑 공격으로부터 디바이스를 보호한다. 마지막으로, Wi-Fi와 RF (Radio Frequency) 신호를 동시에 받아 비교하는 과정을 통해 사용자 명령의 변조 여부를 판단하고, 변조 시 사용자에게 알린다. 이는 데이터의 신뢰성을 검증하고 데이터의 무결성을 보장한다. 이 프로젝트는 보안이 강화된 무선랜 디바이스를 구현하고, 실용적이고 상용화 가능한 보안 솔루션을 제시하는 것을 목표로 한다. 이를 통해 인명구조, 물류 및 시설 관리, 모니터링 등 다양한 분야에서 활용될 수 있는 저비용, 고신뢰성의 보안 드론을 개발하는 것이 최종 목표이다.</p>	
프로젝트 내용	<p>1. 통신 보안 개선 드론 제작 : 드론은 연결된 컨트롤러(사용자)의 명령에만 반응하며, 연결되지 않은 컨트롤러(공격자)는 드론의 정보를 볼 수 없다. 또한, 공격자가 사용자와 드론 간의 연결을 끊으려 시도할 경우, 드론은 이를 감지하고 사용자에게 알린다. 드론은 RF(Radio Frequency) 신호를 통해 얻은 현재 GPS 정보를 사용자에게 전송한다.</p> <p>2. 사용자 검증 알고리즘 : WIFI와 RF를 사용한 이중 통신 방식을 통해, WIFI로 받은 정보가 RF로 받은 정보와 일치하는지 검증하는 실험을 진행한다. 무선랜 연결을 통해 패킷을 암호화하고, RF 신호로 받은 명령으로 한 번 더 검증하여 TCP보다 빠르고 UDP보다 신뢰성 있는 통신 방식을 사용한다.</p> <p>3. 공격 탐지 알고리즘 : 인증 해제 공격을 받았을 경우 이를 인지하고 사용자에게 알리는 알고리즘을 개발한다. 또한, GPS 스푸핑을 감지하기 위한 신호 처리 알고리즘을 연구한다. RF 송/수신 기기에서 받은 GPS 정보를 신호의 세기에 따라 판단하는 신호 처리 알고리즘을 구현한다.</p>	
기대효과 (500자 이내) (응용분야 및 활용범위)	<p>인명구조 분야에서 무선랜 디바이스의 활용이 증가함에 따라, 신뢰할 수 있는 통신 시스템을 통해 구조 활동의 효율성과 안전성이 향상될 것이다. 신속하고 정확한 명령 전달이 가능해져 구조 작업이 더 원활하게 진행될 것이다.</p> <p>물류 및 시설 관리에서 드론의 역할이 확대됨에 따라, 보안이 강화된 무선랜 디바이스는 해킹 및 데이터 유출의 위험을 줄여 물류 시스템의 안전성을 높일 수 있다. 예를 들어, 창고나 공장의 물류 드론이 안전하게 운영됨으로써 자산 보호와 운영 효율성이 향상될 것이다.</p> <p>모니터링 및 감시 활동에서 디바이스의 보안 강화는 중요한 영향을 미친다. 보안이 강화된 기기는 공공 안전, 환경 감시, 농업 등 다양한 분야에서 데이터를 신뢰성 있게 수집하고 전달할 수 있다. 이를 통해 데이터의 무결성을 보장하고, 의사결정의 정확도를 높일 수 있다.</p> <p>이 프로젝트에서 개발된 기술과 알고리즘은 다른 무선랜 디바이스에도 적용될 수</p>	

	<p>있어, 스마트 홈, IoT 기기 등 다양한 분야에서 보안성을 향상시킬 수 있는 가능성을 제공한다.</p> <p>마지막으로, 본 프로젝트는 실용적이고 상용화 가능한 보안 솔루션을 제공함으로써 관련 산업의 발전에 기여할 것이다. 저비용으로 다양한 공격에 대비할 수 있는 기술을 개발함으로써, 중소기업 및 스타트업도 높은 수준의 보안 솔루션을 도입할 수 있게 된다. 이로 인해 전반적인 산업의 보안 수준이 향상되고, 새로운 비즈니스 기회가 창출될 것이다. 이 프로젝트는 드론 및 무선랜 디바이스의 보안을 강화하여 다양한 산업 분야에서 안전성을 추구하는 데 기여할 것이다.</p>			
중심어(국문)	드론	무선통신	와이파이	RF신호
Keywords (english)	drone	wireless-communication	wifi	RF
멘토	소속 BurnYoung	이름	유용길	
팀 구성원	학년 /반	학번	이름	연락처(전화번호/이메일)
	4	20211870	김슬기	01052691194/2011870@edu.hanbat.ac.kr
	4	20191759	홍준기	01048149218/honhg063@naver.com
	4	20201773	손성호	01094367994/20201773@edu.hanbat.ac.kr
<p>컴퓨터공학과와 캡스톤디자인 관리규정과 모든 지시사항을 준수하면서 본 캡스톤디자인을 성실히 수행하고자 아래와 같이 계획서를 제출합니다.</p> <p style="text-align: center;">2024년 7월 5일</p> <p style="text-align: right;">책임자 : 김슬기  지도교수 : 김태훈 </p>				

캡스톤디자인 계획서(양식)

1. 캡스톤디자인의 배경 및 필요성

무선랜은 전파를 통신 매개로 이용하기 때문에 보안을 고려하지 않고 이용한다면 유선랜에 비해 보안이 취약하다. 무선랜을 이용하는 다양한 디바이스의 경우, 군사용 디바이스는 항공기 또는 순항미사일의 방어시스템 수준으로 보안이 철저한 반면, 상용되는 저가형 디바이스들은 보안이 취약하거나 보안을 고려하지 않은 상태에서 활용되는 경우가 많다. 이러한 경우, 공격자가 디바이스의 제어권을 쉽게 획득하여 정보를 유출하거나 디바이스를 조작할 가능성이 있다.

기술이 발전함에 따라 무선랜 디바이스는 인명구조, 물류 및 시설 관리, 그리고 모니터링, 탐사 및 수색 등 다양한 분야에서 적극적으로 활용되고 있다. 하지만 무선랜을 사용하는 디바이스가 보안 위협을 받는다면 생명을 구할 수 있는 기회를 놓칠 수도 있고, 물류나 시설 관리를 위해 사용되던 디바이스가 해킹당한다면 시설의 보안이 약화되거나 물류 과정이 마비될 수 있을 것이다. 실제로 활용 중인 무선랜 디바이스가 보안 위협을 받는다면 위와 같은 다양한 피해가 예상된다. 따라서 무선랜 디바이스의 해킹에 대한 대응책을 마련하고 보안을 강화하는 것이 매우 중요하다.

2. 캡스톤디자인 목표 및 비전

무선랜 신호와 RF 신호를 동시에 받아 비교하게 될 경우, 동기화 과정에서 딜레이가 발생하여 무선랜만 사용할 때보다 신호 처리가 느려질 수 있다. 이러한 단점은 무선랜 신호를 받되, RF 신호는 무선랜 신호를 검증하는 과정에 사용하여 사용자의 명령이 변조되었다고 판단될 경우 사용자에게 알리는 알고리즘을 실험함으로써 보완할 수 있다.

선행 연구가 없는 이 알고리즘을 실험하여 해당 알고리즘의 성능 또는 상용화 가능성에 대해 알아볼 수 있다. 보안 알고리즘을 추가한 드론을 제작하고 실험하며, 직접 하이재킹을 시도하여 알게 된 취약점들을 토대로 저비용으로 다양한 공격으로부터 보안이 가능한 방향으로 드론을 개선할 수 있다.

3. 캡스톤디자인 내용

무선랜을 사용해 명령을 교환하는 디바이스를 타겟으로 한 캡스톤 프로젝트에서 실행한 실험들을 토대로, 통신 보안 취약점을 개선한 드론을 제작한다. 제작된 드론의 경우, 연결된 컨트롤러(사용자)와 연결되지 않은 컨트롤러(공격자) 중 사용자 컨트롤러의 명령에만 제어된다. 연결되지 않은 컨트롤러는 드론과 연결된 컨트롤러(사용자)로부터 전송되는 정보를 볼 수 없다. 또한, 공격자가 드론과 사용자 간의 연결을 끊으려 시도할 경우, 드론은 이를 감지하고 사용자에게 알린다. 드론은 RF(Radio Frequency) 신호를 통해 얻은 현재 GPS 정보를 사용자에게 전송한다.

패킷의 암호화 및 패킷 교환은 무선랜 연결을 통해 이루어지며, RF 신호로 받은 명령으로 한 번 더 검증하여 TCP보다는 빠르고 UDP보다는 신뢰성을 가지는 통신 방식을 사용한다. 인증 해제 공격을 받았을 경우 이를 인지하고 사용자에게 알리며, GPS 스푸핑을 감지하기 위한 신호 처리 알고리즘을 갖춘다.

드론을 제작하기 전 WIFI 와 RF를 사용한 이중 통신에서 같은 정보를 보내어 WIFI로 받은 정보를 RF로 받은 정보가 똑같은지 검증하는 실험 후 해당 알고리즘의 성능 및 실현 가능성에 대해 연구한다.

RF 송/수신 기기에서 받은 GPS 정보를 신호의 세기에 따라 판단하는 신호처리 알고리즘을

구현, 인증해제 공격을 감지하는 알고리즘 구현 후 직접 재밍,인증해제 공격를 시도하며 알고리즘 실험.

위 세 가지 알고리즘을 탑재한 드론을 제작하고 하이재킹을 시도하며 추후 연구에 대한 가능성을 분석한다.

4. 캡스톤디자인 추진전략 및 방법

비교적 생소한 RF 통신 방식에 대한 자료를 수집하고 이해를 우선적인 목표로 한다. Python 라이브러리를 통해 WiFi, RF 신호를 동시에 처리해보고 이 과정에서 상호 보완하는 방법을 찾는다. 보안 알고리즘을 구상한 후 하드웨어 전문 멘토의 도움을 받아 기존 보안 취약점이 개선된 자체 드론을 제작하고, 테스트를 진행하여 추가적인 개선을 진행한다.

수행 내용	7	8	9	10	11
자료수집 및 설계방식 구상					
WiFi, RF 신호 동기화 시도					
보안 알고리즘 구현					
보안 취약점 개선 드론 제작					
드론 구동 및 추가 개선					
보고서 및 전시회 준비					

학번	이름	역할
20211870	김슬기	드론 프레임 제작
20191759	홍준기	WIFI 연결
20201773	손성호	RF 신호 연결

5. 캡스톤디자인 결과의 활용방안

기존에 존재하던 WiFi, RF를 같이 이용하는 드론들은 각 통신 방식마다 처리하는 데이터를 분리하여 이용하기에 상호 간에 공유한다는 점이 없었다. 그러나 이 캡스톤디자인에서 제작하고자 하는 방식의 드론은 기존의 방식에 더해 상호 보완적인 보안을 제공한다. 개인정보 보호, 사유재산 보호라는 사회적 이슈에 적절하게 이용될 수 있고, WiFi와 RF를 동시에 이용하는 다른 분야에도 응용한다면 보안 측면에서 큰 영향을 끼칠 수 있다.

6. 참고문헌

1. 국내 무선랜(WiFi) 보안 운영 현황 및 정책 방향, 한국인터넷진흥원, 2011, 백종현.
2. Vulnerability Case Analysis of Wireless Moving Vehicle, 한국융합학회논문지, 2018, 오상윤.

캡스톤디자인 II 계획발표 채점표

팀 구성원	학년/반	학 번	이 름				
제 목							
항목			점수				
			1	2	3	4	5
1. 프로젝트 주제의 필요성이나 중요성이 적절히 서술되었는가?							
2. 국내외 동향(문제 제기), 주요 기능(특징 포함) 및 범위가 적절히 서술되었는가?							
3. 기대효과(사회적, 기술적, 경제적 파급효과)가 적절히 서술되었는가?							
4. 추진 전략과 수행방법이 적절한가?							
5. 팀 구성과 역할 분담이 적절히 이루어졌는가?							
합계							
*수정 및 개선 의견							
<div style="text-align: center;">2013년 월 일</div> <div style="display: flex; justify-content: space-between; margin-top: 20px;"> 심사위원 : (인) </div>							

※ 채점은 각 영역별 5점 만점을 기준으로 채점함.(상 5, 중 3, 하 1)

※ 계획서와 발표내용을 참고하여 채점표에 따라 평가함.