Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.5, Oct. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.5.1135

사고 유발 관점에서의 무인지상차량 보안 요구사항에 관한 연구

김 동 훈,[1†] 이 상 진[2‡]
[1,2]고려대학교 (대학원생, 교수)

Research on Security Requirements for Unmanned Ground Vehicles from an Incident-Induced Perspective

Dong-hoon Kim,[1†] Sang-jin Lee[2‡]
[1,2]Korea University (Graduate Student, Professor)

요 약

본 논문은 무인지상차량에 대한 위협모델링을 통해 사고 유발 관점에서 무인지상차량이 안전하게 운용될 수 있는 보안요구사항을 도출하였다. 무인지상차량의 구성 요소를 분석하고 각 요소에서 발생할 수 있는 취약점을 수집하고 위협을 분석하여 충돌, 급정거 사고를 유발할 수 있는 공격 트리를 작성하였다. 공격 트리에서 보안 요구사항을 도출하고 UN에서 발간한 자율주행차량 위협 및 보안 요구사항이 제시된 문서 UN R155 Annex 5 에서 사고 유발 관점의 위협에 대응되는 보안 요구사항을 선정하여 본 논문에 제시한 보안 요구사항과 비교하였다. 본 논문의 보안 요구사항을 활용하면 무인지상차량의 원활한 도입과 운용에 도움이 될 것으로 기대한다.

ABSTRACT

This paper derives security requirements to ensure the safe operation of unmanned ground vehicles from the perspective of accident causation through threat modeling. By analyzing the components of unmanned ground vehicles and identifying potential vulnerabilities in each element, we constructs attack trees that could lead to accidents such as collisions and sudden stops. From these attack trees, security requirements are derived. These requirements are then compared with the security requirements corresponding to accident causation threats as outlined in the UN's document on autonomous vehicle threats and security requirements, UN R155 Annex 5. The comparison highlights how the security requirements proposed in this paper align with those established by the UN. The application of the security requirements proposed in this paper is expected to facilitate the smooth introduction and operation of unmanned ground vehicles.

Keywords: Unmmand Ground Vehicle, Incident-Induced Perspective, Security Requirement, STRIDE Threat Modeling

I. 서 론

자율주행 차량은 군에서 정찰 임무를 수행하기 위해 활발히 개발되고 있다. 2006년, 미군은 무인 지상 차량(Unmanned Ground Vehicle, UGV)을 활용한 폭발물 제거 임무를 아프가니스탄에서 수행하였다 [1]. 이러한 무인지상차량은 위험 지역에 대한 폭발물 탐지 작업을 효과적으로 수행하며 군사 작전의 안전성을 높였다. 2017년, 러시아는 자율주행 전투 차량인 Uran-9를 공개하며, 정찰 및 전투 지원 임무에서의 자율주행 기술 적용 가능성을 시사했다 [2]. 2021년에는 이스라엘이 자율주행 정찰 차량인

Received(08. 02. 2024), Modified(09. 06. 2024), Accepted(09. 10. 2024)
† 주저자, hoon0754@gmail.com
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

Jaguar를 도입하여 국경 지역의 정찰 임무를 수행하고 있다 [3]. 이러한 시도들은 군에서 자율주행 차량을 정찰 임무에 활용하려는 노력을 보여주며, 기술 발전과 함께 군사 작전의 효율성과 안전성을 높여주고 있다.

자율주행차량은 사이버물리시스템으로 소프트웨어가 다양한 물리시스템을 제어하는 형태의 분산 제어 시스템이다. 이와 같은 성격으로 인해 사이버 공격과 물리적 공격 모두 취약하다는 문제를 안고 있다.

무인지상차량은 카메라, 라이다(LiDAR), 레이더(RADAR) 등을 사용하여 주변 환경을 인식하고 주행 경로를 결정한다. 이러한 센서들은 외부 신호를 받아들이기 때문에 해커들이 조작된 신호를 보내거나 센서를 교란시켜 잘못된 정보를 전달할 수 있다. 또한, 무선 통신을 통해 중앙 서버와 데이터를 주고받기 때문에 해커들이 중간에서 신호를 가로채거나 변조할 수 있는 취약점을 갖고 있다. 이러한 무선 통신 취약점은 특히 군사 작전이나 긴급 상황에서 큰 문제를 초래할 수 있다. 이러한 취약성 때문에 자율주행 차량의 사이버 보안은 물리적 특성과 함께 고려되어야 한다.

무인지상차량의 사이버 보안을 강화하기 위해서는 기능적 안전성뿐만 아니라 의도적인 공격에 대한 대응도 중요하다. ISO 26262는 자동차 전기 및 전자 시스템의 기능적 오작동에 의한 사고를 방지하기 위한 국제 표준이다. 이 표준은 시스템 내 잠재적 고장을 사전에 식별하고 예방하기 위한 안전 메커니즘을 제공한다. 반면, 본 연구는 의도적인 공격에 의한 사고를 방지하는 것을 목표로 하며, 무인지상차량의 사고 유발 요소를 분석하고 대응책을 마련하는 데 중점을 둔다. ISO 26262가 기능적 안전성에 중점을 두는 것과 달리, 본 연구는 악의적인 위협에 대응하는 보안적 측면을 주요 고려 대상으로 삼고 있다.

본 논문에서는 무인지상차량의 사이버-물리 공격으로 인한 사고 유발을 방지하기 위해 Microsoft 사의 위협 모델링 기법을 중심으로 무인지상차량의 위협을 식별했으며, 민간 자율주행차량의 사이버-물리 취약점을 바탕으로 무인지상차량에서도 적용 가능한지 판단하여 이를 통해 최종적으로 무인지상차량의 사고를 유발하는 공격 시나리오와 보안 요구사항을 도출하였다.

본 논문의 2절에서는 자율주행차량의 사이버-물리 취약점에 관한 연구와 자율주행차량의 위협모델링에 관한 연구를 소개한다. 3절에서는 자율주행차량의 사이버-물리 취약점을 토대로 무인지상차량의 위협과 무인지상차량에서 발생할 수 있는 사고 유발 공격 시나리오를 분석한다. 4절에서는 무인지상차량 사고 유발 공격 시나리오를 통해 보안 요구사항을 도출하고 평가한다. 마지막으로 5절에서는 결론을 제시한다.

II. 관련 연구

2.1 자율주행차량 취약점 관련 연구

2.1.1 자율주행차량 사이버 취약점 관련 연구

자율주행 차량의 Controller Area Network (CAN) 통신 채널은 차량 내 전자 제어 유닛(ECU) 간의 통신을 담당하는 중요한 시스템이다. 이 통신 채널은 저비용, 고속 데이터 전송, 신뢰성 등의 장점으로 인해 널리 채택되었다. CAN 통신은 메시지 기반 프로토콜로, 각 메시지는 고유의 식별자를 가지고 있어 네트워크 상의 모든 ECU가 이를 수신하고 필요한 경우 처리할 수 있다. 그러나 CAN 통신 채널은 인증 메커니즘의 부재, 메시지 우선순위 알고리즘, 네트워크 접근성, 보안 기능의 부족으로 인해 취약한 통신 채널로 알려져 있다.

El-Rewini[4]는 차량에 탑재되는 센서에 대한 사이버 보안 공격과 그로 인한 잠재적 위험을 분석하였다. H. Ueda[5]는 공격자가 ECU 소프트웨어를 악성프로그램으로 대체 후, CAN 네트워크에 메시지를 전송할 수 있는 취약점을 공개했다. K. Iehira[6]는 공격자가 다른 ECU에서 발생하는 메시지와 동시에 메시지를 생성하여 bus-off 상태를 유도하고 메시지를 누락시킬 수 있는 취약점을 공개했다. G. Bloom[7]은 나아가 CAN 침입탐지 시스템을 우회하여 bus-off 상태를 발생시키는 공격기법을 제시한 바 있다.

ECU는 현대 차량의 필수적인 구성 요소로, 각종 전자 시스템을 제어하고 관리하는 역할을 한다. 차량 한 대에는 수십 개에서 수백 개에 이르는 ECU가 설치되어 있으며, 이들은 엔진 제어, 브레이크 시스템, 에어백, 인포테인먼트 시스템 등 다양한 기능을 수행한다. ECU는 차량의 센서로부터 데이터를 수집하고 이를 처리하여 적절한 제어 명령을 내림으로써 차량의 성능과 안전성을 보장한다. 전자제어유닛은 CAN 통신 채널을 통한 상호 연결성, 암호 및 인증 메커니즘 부재, 업데이트의 어려움, 물리적 접근 용이성으로 인

해 사이버 공격에 취약하다.

MC. Chow[8]는 공격자는 ECU 펌웨어 업데이트 시 인증 과정이 없어 CAN, JTAG, OBD 포트를 통해 악성 펌웨어를 업데이트할 수 있는 공격이 가능하다. 이러한 펌웨어 변조 공격으로 정상적인 동작을 수행하면서 차량 상태에 관한 정보 유출이 가능함을 증명하였다. I. Rouf[9]는 타이어 공기압 모니터링 시스템에 메시지 인증 과정이 없어 무선으로 메시지 도청과 조작이 가능함을 밝혔다.

2.1.2 자율주행차량 물리적 취약점 관련 연구

자율주행차량의 카메라는 주변 환경을 실시간으로 인식하고 분석하여 차량의 주행 경로와 장애물 감지를 지원하는 핵심 센서이다. D. Davidson[10]은 프로젝터를 통해 카메라 센서 입력을 위조하는 공격을 제시하였다. C. Yan[11]은 카메라 센서에 강한 빛(LED, Laser)을 지속적으로 노출시켜 카메라 센서를 손상시키는 공격을 제시하였다. El-Rewini[4]는 카메라에 다수의 노이즈 또는 객체를 주입하여 사물 인식 부하를 통한 서비스 거부 공격이 가능함을 증명하였다.

자율주행차량의 LiDAR 센서는 레이저를 사용하여 주변 환경의 3D 구조를 고해상도로 스캔하고 지도화하여 자율주행차량의 정밀한 위치 인식과 장애물 감지를 지원하는 센서이다. H. Shin[12]은 자율주행차량의 LiDAR는 인코딩되지 않는 펄스를 방출하기 때문에 가짜 물체를 생성하는 스푸핑 공격이 가능함을 제시하였다. Y. Cao[13]는 자율주행차량의 LiDAR 펄스를 가로막거나 변경하여 실제 물체를 인식하지 못하게 하는 스푸핑 공격을 제시하였다.

자율주행차량의 센서 융합 기술은 카메라, LiDAR, RADAR 등 다양한 센서에서 수집한 데이터를 통합하여 더 정확하고 신뢰성 높은 환경 인식을 가능하게 하는 기술이다. Hallyburton[14]은 공격자는 2D 감지(카메라)의 3D 불확실성을 이용해 카메라-라이다 센서 융합 과정에서 물체의 거리를 조작 가능한 공격을 제시하였다. (초보적인 스푸핑 공격은 인식 알고리즘에서 방어 가능) Y. Zhu[15]는 공격자는 드론을 이용해 카메라, LiDAR, RADAR 센서 인식을 방해하여 전방의 물체를 인식하지 못하게 하고 주변과의 충돌을 유도할 수 있음을 발표하였다.

자율주행차량의 RADAR는 전파를 발사하고 반사된 신호를 수신하여 주변 물체의 거리와 속도를 측정하고, 자율주행차량의 장애물 감지 및 주행 안전성을 강화하는 센서이다. C. Yan[11]은 전파 신호를 조작하여 물체의 거리를 조작하거나 장애물을 생성할 수 있으며 또한 전파 신호에 노이즈를 주입하여 물체를 인식하지 못하게 하는 공격을 제시하였다.

자율주행차량의 GPS는 위성 신호를 이용하여 차량의 정확한 위치를 실시간으로 추적하고 지도와 결합하여 차량 경로 계획을 돕는 센서이다. KC. Zeng[16]은 공격자가 GPS를 스푸핑하여 가짜 경로로 운전하도록 유도하는 공격을 재현했다.

자율주행차량의 IMU(Inertial Measurement Unit)는 가속도계와 자이로스코프를 사용하여 차량의 가속도, 속도, 방향 및 기울기를 측정하여 차량의 움직임을 인식하는 센서이다. Y. Tu[17]는 공격자는 음향 신호를 주입하여 가속도 측정계를 방해하고 지상 이동체의 방향을 바꾸는 공격을 발표하였다.

ECU에서는 E. Pozzobon[18]이 보안 기능이 구현된 ECU 플래시 메모리에서 fault injection attack을 통해 데이터를 추출하여 역공학을 통해 펌웨어를 추출할 수 있는 취약점을 발견하였다. E. Saeedi[19]는 ECU에서 발생하는 전자기적 신호를 분석하여 비밀키를 추출할 수 있는 공격이 가능함을 증명하였다. Y. Shoukry[20]는 ABS(Anti-lock Brake System)의 휠 속도 센서 전자기적 약점을 이용해 ABS 주변에 악의적인 전자기 액추에이터를 배치하여 휠 속도를 조작하는 공격이 가능함을 보였다.

2.2 위협 모델링

위협 모델링은 시스템의 보안 위협을 체계적으로 분석하고 식별하는 과정으로, 시스템이 직면할 수 있는 잠재적인 공격 벡터와 취약점을 발견하여 이를 방어하기 위한 보안 요구사항을 도출하는 데 사용된다. 이 과정은 주로 자산, 위협, 취약점, 그리고 방어 조치 간의 관계를 이해하는 데 중점을 둔다. 대표적인 위협 모델링 기법으로는 STRIDE[21]가 있으며, 이는 각 단계별로 잠재적 위협을 식별하고 대응책을 마련하는 데 도움을 준다. 또한, 개인정보 보호와 관련된 위협을 분석하기 위해 LINDDUN[22]과 같은 기법도 사용된다. 위협 모델링 도구로는 Microsoft의 Threat Modeling Tool[23], OWASP Threat Dragon[24] 등이 있다. 이들 도구는 시각적 다이어그램과 자동화된 분석 기능을 제공하여 사용자가 보다 쉽게 위협을 식별하고 관리할 수 있도록 돕는다. 본

논문에서는 무인지상차량의 보안 요구사항을 도출하기 위해 STRIDE 기법을 사용하였다.

무인지상차량의 경우, 복잡한 구조와 다양한 센서, 제어 시스템, 통신 채널로 인해 보안 요구사항을 도출하는 것이 어려울 수 있다. STRIDE 기법은 이러한 복잡성을 단순화하여 체계적으로 접근할 수 있는 틀을 제공한다. 무인지상차량의 통신 채널에서 발생할 수 있는 스푸핑 공격을 탐지하고 방어하는 요구사항을 도출하거나, 센서 데이터의 변조를 방지하기 위한 조치를 정의할 수 있다. STRIDE는 이러한 과정에서 모든 가능한 공격 벡터를 분류하고 분석함으로써, 세부적인 보안 요구사항까지 포괄적으로 다룰 수 있게 한다.

2.3 자율주행차량 위협 모델링

박민주[25]는 자율주행자동차에서 발생할 수 있는 위협을 모델링하고 보안을 위해 점검이 필요한 요소들을 체크리스트로써 제안하였다. 차량, 그리드, 인프라, 센터와 같이 자율 주행 환경 전체에 대한 위협 모델링으로 주행 환경에 집중하여 보안 요구사항을 도출하였다. 차량의 경우 사이버 영역의 공격만 고려하고 있으며 물리적 공격을 고려하지 않았다는 한계점이 있다.

UN은 차량 사이버 보안과 소프트웨어 업데이트 관리를 강화하기 위해 UN Regulation No. 155 및 UN Regulation No. 156을 도입했다 [26]. 이 규제들은 차량 제조업체가 사이버 보안 위협으로부터 차량을 보호하고 안전한 소프트웨어 업데이트를 보장하도록 요구한다. UN Regulation No. 155 Annex5에서는 자율주행차량에서 발생할 수 있는 사이버 보안 위협을 식별하고 이에 대응하는 완화 방안이 제시되었다. 한국인터넷진흥원은 자율주행차 보안모델[27]을 통해 UN Regulation No.155 Annex5 에서 명시한 위협과 각 위협에 대응되는 완화 방안을 토대로 보안 요구사항을 제시하였다.

본 논문에서는 UN Regulation No.155 Annex5에 제시된 자율주행차량의 위협과 대응되는 완화 대책을 기준으로 사고 유발 관점의 무인지상차량 보안 요구사항을 평가하였다.

III. 무인지상차량 위협모델링

3.1 무인지상차량

본 논문에서는 밀렘로보틱스(Milrem Robotics)의 THeMIS UGV를 참고하여 일반적인 무인지상차량의 기능을 모델링하였다. THeMIS UGV는 전투, 감시정찰, 폭발물 제거 등 다양한 목적으로 작전에 활용될 수 있으며 목표물 추적, 자율주행, 원격제어 기능을 탑재하고 있다 [45].

무인지상차량은 센서, 주행, 동력 시스템과 각 시스템의 입출력을 통제하는 통제 시스템으로 구성된다. 무인지상차량과 민간 자율주행차량은 여러 측면에서 유사하나, 사이버 보안 위협을 식별하고 대응하는 데 중요한 몇 가지 차이점이 존재한다.

첫째, 인포테인먼트 시스템의 부재이다. 민간 자율주행차량은 사용자 편의를 위한 다양한 인포테인먼트 시스템을 탑재하고 있으나, 군용 무인지상차량은 이러한 시스템이 설치되지 않는다.

둘째, 차량-사물 간 통신(V2X, Vehicle-to-Everything) 기능의 부재이다. 민간 자율주행차량은 교통 신호, 다른 차량, 인프라 등과 통신하는 V2X 기술을 사용하여 주행의 안전성과 효율성을 높인다. 반면, 군용 무인지상차량은 이러한 통신 기술을 사용하지 않는다.

셋째, 원격 제어 기능이다. 군용 무인지상차량은 원격 제어를 통해 군 작전 중에 안전한 거리에서 운용될 수 있다. 반면, 민간 자율주행차량은 주로 자율적인 운행을 목표로 설계되어 원격 제어 기능이 제한적이다.

이러한 기능적 차이점 외에도 운용되는 환경의 차이점도 있다. 본 논문에서는 무인지상차량의 위협분석 과정에서 전자전, 물리적 접근 등 전장 환경에 특화된 요소를 고려하였으며, 자율주행차량의 취약점을 군사적 환경에 맞춰 적절히 조정하여 분석하였다.

3.2 데이터 흐름도 작성

데이터 흐름도(DFD, Data Flow Diagram)는 시스템 내에서 데이터가 어떻게 흐르고 처리되는지를 시각적으로 표현하는 도구이다. 데이터 흐름도는 시스템 분석 및 설계 과정에서 광범위하게 사용되며, 이를 통해 시스템의 기능적 요구사항을 명확히 하고, 데이터의 이동 및 변환 과정을 쉽게 이해할 수 있다. 무인지상차량의 환경 인식, 자율주행, 명령 송수신, 명령 수행 등 무인수색에 필요한 과정을 분석하여 Fig.1.과 같이 나타냈다.

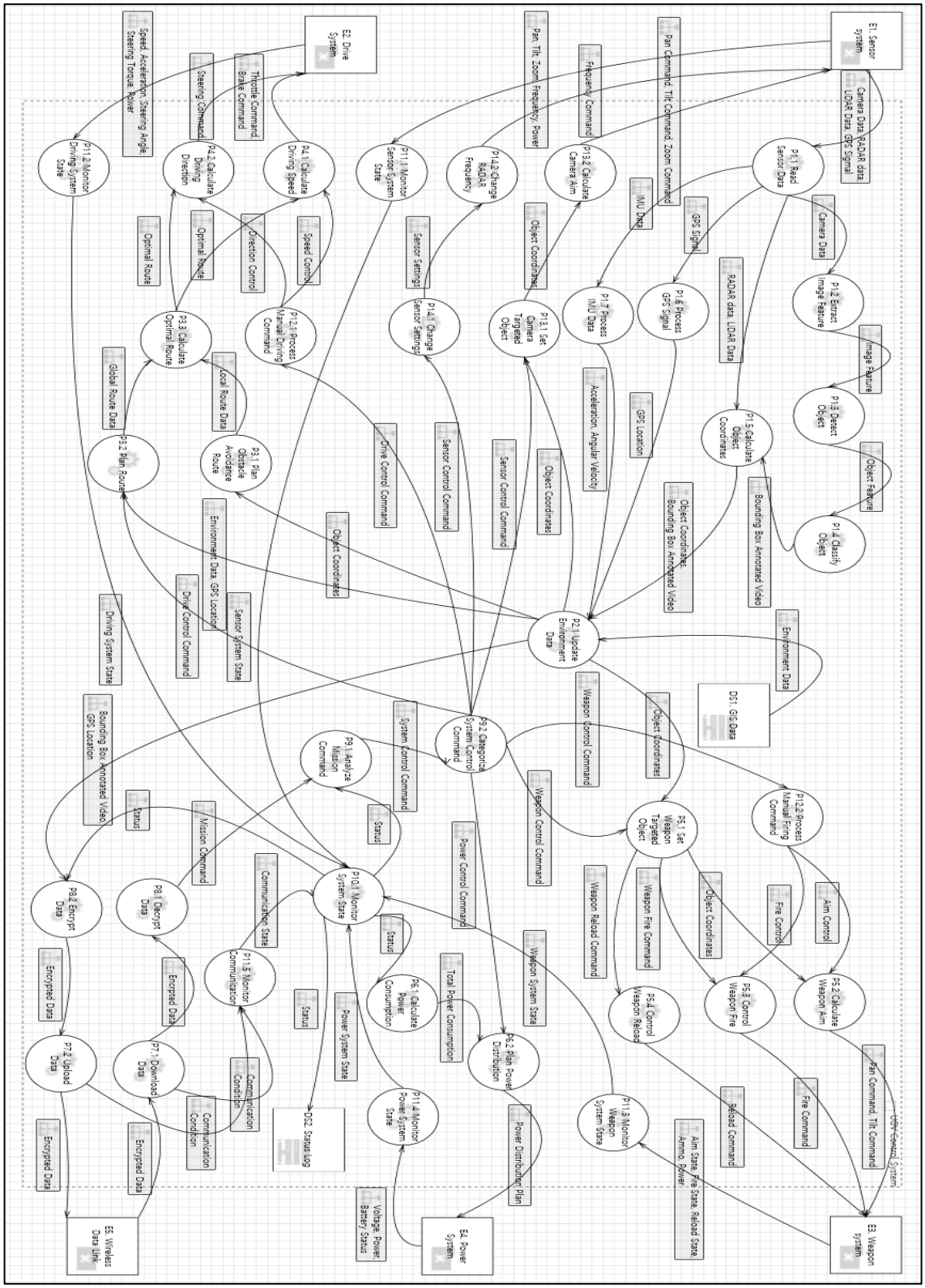

Fig. 1. UGV DFD Level 2

3.3 무인지상차량 공격 라이브러리 작성

무인지상차량 공격 라이브러리는 논문 43건, CVE 53건의 자료를 수집하였다. 센서(Camera, LiDAR, RADAR, GPS, IMU), 센서 융합, 통신(CAN, Wireless), ECU 등 무인지상차량을 구성하는 요소에서 총 107개의 취약점을 수집하여 데이터베이스화 하였다[28]. Table 1은 자율주행차량에 탑재된 카메라의 취약점, Table 2는 자율주행차량에 탑재된 LiDAR와 RADAR의 취약점, Table 3은 Camera-LiDAR 센서 융합 과정에서 발생하는 취약점, Table 4는 자율주행차량에 탑재된 GPS와 IMU의 취약점, Table 5는 자율주행차량의 네트워크 관련 취약점, Table 6은 자율주행차량에 탑재된 ECU 관련 취약점이다.

Table 1. Attack library of camera

No	Type	Attack Method	Ref
AL3	S,E	Improper access control	[28]
AL5	I	Insecure permissions	[28]
AL7	S	Improper access control	[28]
AL11	E	Remote code execution	[28]
AL15	S	Integer overflow	[28]
AL32	I	BLE command injection	[28]
AL33	E	Firmware command injection	[28]
AL39	S,T	Sensor input spoofing	[10]
AL40	S,D	Blinding attack	[11]
AL41	S,D	Sensor input denial of service	[4]

Table 2. Attack library of LiDAR/RADAR

No	Type	Attack Method	Ref
AL42	S,I	Replaying LiDAR pulse	[4]
AL43	S	Spoofing LiDAR pulse to create fake point cloud	[12]
AL44	S,D	Jamming LiDAR pulse to remove point cloud	[13]
AL45	S	Spoofing RADAR system to alter object distandce	[11]
AL46	S,D	Jamming RADAR system to remove detected object	[11]

Table 3. Attack library of Camera-LiDAR sensor fusion

No	Type	Attack Method	Ref
AL67	S	Frustrum attack	[14]
AL68	S	Multiple sensor attack	[15]

Table 4. Attack library of GPS/IMU

No	Type	Attack Method	Ref
AL47	S,T	Spoofing GPS to make UAV overflight	[29]
AL48	S,T	Spoofing GPS to make UAV malfunction	[30]
AL49	S,T	Spoofimg GPS to control UAV flight route	[31]
AL50	T	Modificating firmware to tampering GPS	[28]
AL51	I	Modificating firmware to obtain GPS	[28]
AL60	I	Insecure encryption algorithms	[28]
AL63	S	Spoofing GPS to trigger fake navigation route	[32]
AL64	S,T	Aucoustic injection attack for UAV	[33]
AL66	S,T	Aucoustic injection attack for UGV	[17]

Table 5. Attack library of network

No	Type	Attack Method	Ref
AL69	S	CAN message injection while updating firmware	[28]
AL75	S,I	CAN message Sniffing	[34]
AL77	D	CAN flooding	[34]
AL78	S,T	CAN message MITM	[34]
AL79	R	CAN deauthentication	[34]
AL84	S	CAN message attack	[35]
AL85	D	CAN bus off attack	[36]
AL88	I	Wireless communication deauthentication	[37]
AL90	T	Wireless communication MITM	[38]
AL95	S,D	ROS deauthentication	[39]
AL96	T,I	ROS MITM	[40]
AL97	E	ROS2 malware	[41]
AL98	S,I	ROS2 key interception	[42]
AL99	S,I	Unencrypted wireless packet	[43]

Table 6. Attack library of ECU

No	Type	Attack Method	Ref
AL100	S	Deauthentication	[8]
AL101	I	Code injection	[8]
AL102	I	Side channel attack	[19]
AL103	I	Fault injection attack	[18]
AL106	T	ABS(Anti-lock Brake System) jamming attack	[20]
AL107	S,I	TPMS(Tire Pressure Monitoring System) deauthentication	[9]

3.4 위협 분석

Fig. 1.의 DFD에서 공격 라이브러리를 활용해 시스템의 각 구성요소를 분석한 후, 표준화된 위협 모델링 기법 STRIDE에 따라 157개의 위협을 도출하였다. 위협 분석 결과는 위협 분석 데이터베이스에 기술하였다[44]. 주요 위협은 자율주행처리 Process에서 발생하는 것을 확인하였다. 자율주행처리 Process는 센서의 취약점과 더불어 내·외부 통신 취약점의 영향을 동시에 받는다.

3.5 공격 트리 작성

공격트리는 공격목표를 달성하기 위해 필요한 공격 방법을 조건에 따라 트리 형식으로 표현한 것이다. 본 논문에서는 3.4절에서 수행한 위협 분석 결과를 바탕으로 충돌 공격목표와 급정거 공격목표에 대한 공격 트리를 작성하였다. Fig. 2.는 충돌 공격 목표를 달성하기 위한 공격 트리, Fig. 3.은 급정거 공격 목표를 달성하기 위한 공격트리이다.

충돌 유도 공격트리는 차량 충돌을 유도하기 위해 사용되는 공격 시나리오를 공격 과정과 공격 표면까지 포괄적으로 설명한다. 충돌 유도 공격은 시스템 제어권 탈취, 브레이크 동작 제한 상태 유발, 비정상 주행 유도, 차량 센서 혼선 유발을 통해 독립적으로 실행할 수 있으며 차량의 보안 능력과 상황에 따라서 주어진 시나리오 중에서 다수의 시나리오를 요구할 수 있다. 예를 들어 비정상 주행을 유도하더라도 충돌 방지 기능이 정상적으로 동작하는 경우 충돌은 일어나지 않을 수 있다. 이러한 상황에서 차량 센서 혼선을 유발하거나 브레이크 동작을 방해하여 충돌방지 기능을 방해하고 충돌을 유도할 수 있다.

급정거 유도 공격트리는 차량의 급정거를 유도하기 위해 사용되는 공격 시나리오를 공격 과정과 공격 표면을 나타내었다. 급정거 유도 공격은 시스템 제어권 탈취, 브레이크 동작 유발, 엑셀 동작 제한 상태 유발, 차량 센서 착시 유발, 조작된 정지 명령 하달을 통해 독립적으로 실행될 수 있으며 충돌 유도 공격 시나리오와 마찬가지로 차량의 보안 능력과 상황에 따라서 주어진 시나리오 중에서 다수의 시나리오가 동시에 실행될 필요가 있다.

두 가지 공격 시나리오에서 공통적으로 센서에 물리적인 공격이 가해질 수 있다. 충돌 유도 공격 과정에서는 센서 신호 조작 또는 인식 처리 부하를 가해 전방에 존재하는 장애물 인식을 방해하여 충돌을 유도하며 반대로 급정거 유도 공격 과정에서는 실제로 존재하지 않는 장애물을 센서 신호 조작을 통해 생성하여 급정거를 유도한다.

IV. 사고 유발 관점 무인지상차량 보안 요구사항 도출

4.1절에서는 사고 유발 관점에서 무인지상차량의 보안요구사항을 제시하고 공격 시나리오에 대해 논문과 컨퍼런스에서 제시한 대책을 나열하였다. 4.2절에서는 UN Regulation No.155 Annex5에 제시된 자율주행차량의 위협과 대응되는 완화 대책을 기준으로 사고 유발 관점의 무인지상차량 보안 요구사항을 평가하였다.

4.1 사고 유발 관점 무인지상차량 보안 요구사항

보안 요구사항 도출 과정에서 공격 트리의 최하위 노드를 차단하여 상위 공격 목표의 달성을 저지하는 전략을 적용하였다. 3.5절에서는 충돌, 급정거 유도 공격트리의 최하위 노드에서 다수의 공격 방법을 식별하였다. 그리고 식별된 공격 방법을 기준으로 대응할 수 있는 16개의 보안 요구사항을 도출하였다. Table 7에는 무인지상차량이 사고 유발 관점의 공격에서 안전하기 위한 보안 요구사항을 나열하였다.

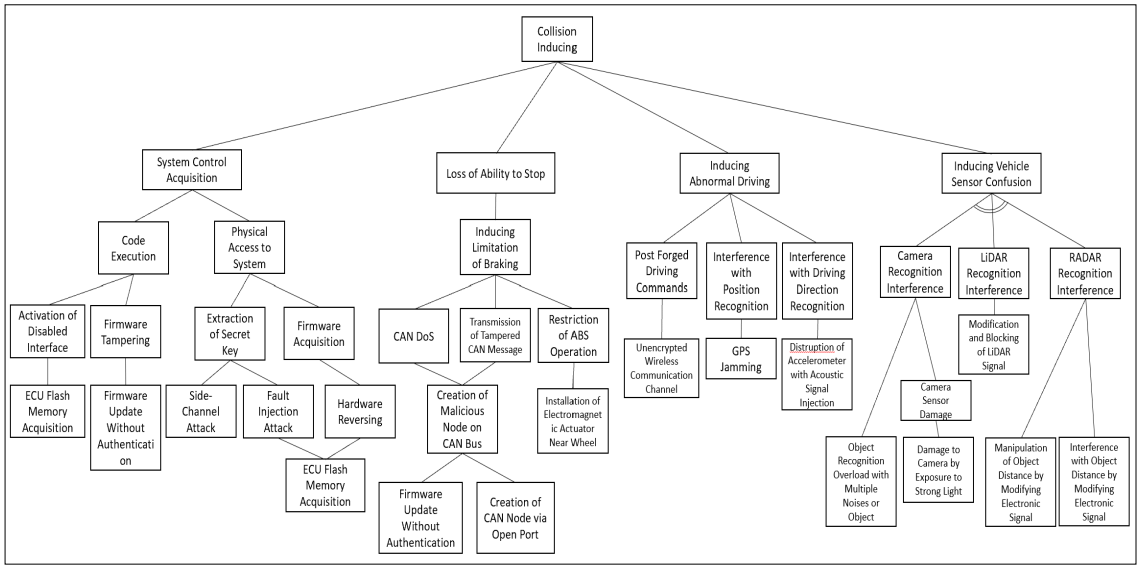

Fig. 2. Attack tree of collision inducing scenario

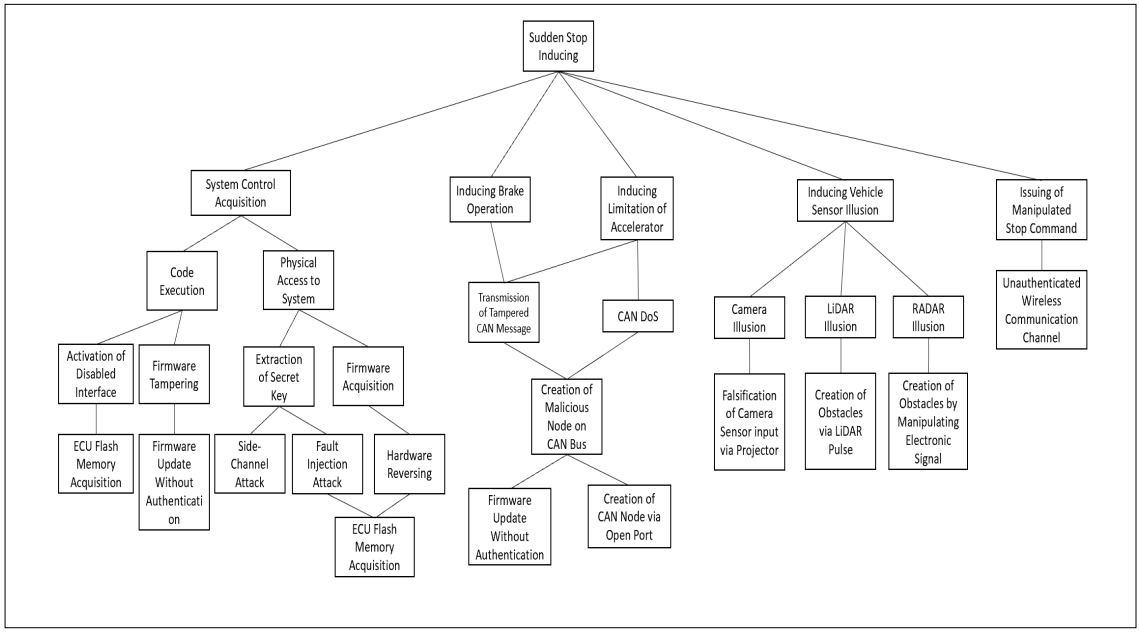

Fig. 3. Attack tree of sudden stop inducing scenario

4.2 사고 유발 관점 무인지상차량 보안 요구사항 평가

4.1절에서 도출한 사고 유발 관점의 무인지상차량 보안 요구사항과 UN의 R155 Annex 5[23]에서 제시한 자율주행차량 보안 요구사항을 비교하였다. UN R155 Annex 5에서 사고 유발 관점의 보안 요구사항을 식별하기 위해 3.5절에서 식별한 공격 방법을 기준으로 데이터 무단접근, 개발 잔여물 사용을 통한 ECU 접근, 업데이트 절차 오용, 암호화 키 추출, 하드웨어 조작, 네트워크 설계 발생 취약점, 시스템 물리적 조작, 파일 및 데이터 무단 접근의 8가지 위협을 선정하고 대응되는 보안 요구사항을 추출하였다.

Table 8에서는 본 논문에서 도출한 보안 요구사항을 기준으로 UN R155 Annex 5에서 제시하는 보안대책을 비교하였다. 본 논문에서는 사고 유발이 가능한 위협에 대해 공격 대상과 실제 적용 가능한 공격 방법이 동반된 보안 요구사항을 제시하였다.

UN의 R155 Annex 5에서는 단순히 시스템에 대한 무단 접근을 방지하고 탐지하기 위한 조치를 강구해야 한다고 제시하였으나 본 논문에서는 ECU 부채널 공격, 결함 주입 공격, 역공학 공격을 통해 시스템에 무단 접근이 가능함을 제시하고 이와 같은 공격에 안전해야 함을 제시하였다. 또한, UN은 센서에 대한 데이터 조작 공격이 서로 다른 센서의 데이터를 상호 연관시키는 것으로 완화될 수 있다고 제시하였지만 다중 센서 융합 기술도 데이터 조작 공격에 안전하지 않으므로 개별 센서가 공격에 안전해야 함을 도출하였다. 이와 같이 무인지상차량의 사고 유발 관점에서 보다 구체적인 공격 방법과 대응책을 제시하였다.

그러나 UN R155가 자율주행차량의 종합적인 보안 전략을 제공하는 반면, 본 논문은 무인지상차량의

Table 7. Security requirements for UGV to be safe from attacks aimed at causing accidents

No	Security Requirement	Attack Method
SR1	Blocking the acquisition of ECU flash memory	1.1.1.1.1 1.1.2.1.2.1 1.1.2.2.1.1...
SR2	Unauthorized personnel must be physically access-controlled	1.1.1.1.1 1.1.2.1.2.1 1.1.2.2.1.1...
SR3	Measures must be taken to prevent the activation of disabled interfaces	1.1.1.1
SR4	Firmware updates require an authentication process	1.1.1.2.1 1.2.1.1.1.1 1.2.1.1.2.1...
SR5	ECUs must be secure against side-channel attacks	1.1.2.1.1 2.1.2.1.1
SR6	ECU flash memory must be secure against fault injection attacks	2.1.2.1.2.1
SR7	ECU flash memory must be secure against reverse engineering	2.1.2.2.1.1
SR8	Connections should be made to secure networks	1.3.1.1 2.5.1
SR9	The system must be capable of detecting and responding to GPS-based attacks	1.3.2.1
SR10	The system must be capable of detecting and responding to acoustics-based attacks	1.3.3.1
SR11	Camera sensors should not be overloaded with object recognition	1.3.1.1.1
SR12	Camera sensors must be secure against exposure to intense light	1.3.1.1.2.1
SR13	The system should distinguish between natural environments and images projected by a projector	2.4.1.1
SR14	LiDAR sensors must be secure against signal manipulation	1.3.1.2.1 2.4.2.1
SR15	RADAR sensors must be secure against signal manipulation	1.3.1.3.1 1.3.1.3.2 2.4.3.1
SR16	The system must be secure against multi-sensor attacks involving Camera-LiDAR.	1.3.1 2.4

Table 8. Comparative assessment of security requirements

UN R155 Annex 5 Threat	UN R155 Annex 5 Mitigations	No	Security Requirement
Gaining unauthorized access to files or data	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data.	SR1	Blocking the acquisition of ECU flash memory
		SR2	Unauthorized personnel must be physically access-controlled
Using remainders from development can permit access to ECUs or permit attackers to gain higher privileges	Cybersecurity best practices for software and hardware development shall be followed.	SR3	Measures must be taken to prevent the activation of disabled interfaces
Misuse or compromise of update procedures	Secure software update procedures shall be employed Security controls shall be implemented for storing cryptographic keys	SR4	Firmware updates require an authentication process
Extraction of cryptographic keys	Security controls shall be implemented for storing cryptographic keys e.g. Security Modules	SR5	ECUs must be secure against side-channel attacks
Manipulation of OEM hardware,e.g.unauthorised hardware added to a vehicle to enable man-in-the-middle" attack	Measures to prevent and detect nauthorized access shall be employed	SR6	ECU flash memory must be secure against fault injection attacks
		SR7	ECU flash memory must be secure against reverse engineering
Network design introduces vulnerabilities	Cybersecurity best practices for software and hardware development shall be followed.	SR8	Connections should be made to secure networks
Physical manipulation of systems can enable an attack	Data manipulation attacks on sensors or transmitted data could be mitigated by correlating the data from different sources of information	SR9	The system must be capable of detecting and responding to GPS-based attacks
		SR10	The system must be capable of detecting and responding to acoustics-based attacks
		SR11	Camera sensors should not be overloaded with object recognition
		SR12	Camera sensors must be secure against exposure to intense light
		SR13	The system should distinguish between natural environments and images projected by a projector
		SR14	LiDAR sensors must be secure against signal manipulation
		SR15	RADAR sensors must be secure against signal manipulation
		SR16	The system must be secure against multi-sensor attacks involving Camera-LiDAR

사고를 유발하는 특수한 상황에 대한 보안 전략을 제시한다는 한계가 있다. 또한, 최신 보안 동향 및 기술 발전을 반영하지 못하므로 무인지상차량의 사고 유발이 가능한 공격에 대한 지속적인 관찰이 필요하다.

V. 결 론

기존 연구에서는 자율주행차량의 물리적 특성을 충분히 고려하지 않은 위협 모델링을 수행하였다. 이로 인해 자율주행차량의 물리적 취약점을 설명하지 못하는 한계가 있었다. 본 논문에서는 무인지상차량에 대

해 기존 사이버 공격에만 치중된 위협모델링을 사이버-물리 영역으로 확장하여 무인지상차량이 실질적으로 인명 피해를 일으킬 수 있는 조건과 이를 보완할 수 있는 보안 요구사항을 제시하였다.

본 논문에서 도출한 보안 요구사항의 평가를 위해 사고 유발 관점의 위협 7개를 선정하여 UN R155 Annex 5에서 제시하는 보안대책을 비교하였으며 본 논문에서는 사고 유발이 가능한 위협에 대해 공격 대상과 실제 적용 가능한 공격 방법이 동반된 보다 구체적인 보안 요구사항을 제시하였다.

무인지상차량으로 인해 인명피해가 발생하면 원인 해결까지 지속적인 운용이 불가능할 수 있다. 따라서 본 논문에서 제시한 보안 요구사항은 무인지상차량에서 비롯되는 인명 피해를 막는 것을 넘어 무기체계의 원활한 도입과 운용에 도움이 될 것으로 기대한다.

References

[1] U.S. Department of Defense, "Unmanned Systems Roadmap 2007-2032", Dec. 2007.

[2] Novichkov, Nikolai. "New Russian combat UGV breaks cover, Uran-9 readies for service," IHS Jane's International Defense Review, pp. 30, Oct. 2016.

[3] Israel Defense, "'Jaguar': The IDF's Newest, Most Advanced Robot", May. 2021.

[4] Z. El-Rewini and K. Sadatsharan, "Cybersecurity attacks in vehicular sensors." IEEE Sensors Journal, vol. 20, no. 22, pp. 13752-13767, Nov. 2020.

[5] H. Ueda, R.Kurachi, H. Takada and T. Mizutani, "Security authentication system for in-vehicle network," SEI Technical Review, no. 81, pp. 5-9, Oct. 2015.

[6] K. Iehira, H. Inoue and K. Ishida, "Spoofing attack using bus-off attacks against a specific ECU of the CAN bus," 2018 15th IEEE Annual Consumer Communications & Networking Conference, pp. 1-4, Jun. 2018.

[7] G. Bloom, "WeepingCAN: A stealthy CAN bus-off attack." Workshop on Automotive and Autonomous Vehicle Security. pp. 1-6, Feb, 2021.

[8] Chow, Man Chun, Maode Ma and Zhijin Pan. "Attack models and countermeasures for autonomous vehicles." Intelligent Technologies for Internet of Vehicles. Springer International Publishing, pp. 375-401. 2021.

[9] I. Rouf, R. Miller and T. Taylor. "Security and privacy vulnerabilities of In-Car wireless networks: A tire pressure monitoring system case study." 19th USENIX Security Symposium. Aug, 2010.

[10] D. Davidson and H. Wu, "Controlling UAVs with sensor input spoofing attacks." 10th USENIX workshop on offensive technologies. Aug, 2016.

[11] Yan, Chen, Wenyuan Xu, and Jianhao Liu. "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle." Def Con, vol. 24, no. 8, pp. 109, Sep, 2016.

[12] H. Shin, D. Kim, Y. Kwon and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications." Cryptographic Hardware and Embedded Systems - CHES 2017: 19th International Conference, Springer International Publishing, pp. 445-467, 2017.

[13] Y. Cao, S. Hrushikesh and P. Naghavi, "You can't see me: Physical removal attacks on lidar-based autonomous vehicles driving frameworks." 32nd USENIX Security Symposium. pp. 2993-3010, May, 2023.

[14] R. Hallyburton, Y. Cao, "Security analysis of Camera-LiDAR fusion

against Black-Box attacks on autonomous vehicles." 31st USENIX Security Symposium. pp. 1903-1920. Aug. 2022.
〔15〕 Y. Zhu, C, Miao, H. Xue, Y. Yu, L. Su, C. Qiao, "Malicious Attacks against Multi-Sensor Fusion in Autonomous Driving." Proceedings of the 30th Annual International Conference on Mobile Computing and Networking. pp. 436-451, May. 2024.
〔16〕 K. Zeng, S. Liu, Y. Shu, D. Wang, H. Li and Y. Dou, "All your GPS are belong to us: Towards stealthy manipulation of road navigation systems." 27th USENIX security symposium. pp. 1527-1544, Aug. 2018.
〔17〕 Y. Tu, Z. Lin, I. Lee and X. Hei, "Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors." 27th USENIX security symposium. pp. 1545-1562, Aug. 2018.
〔18〕 E. Pozzobon, J. Mottok and V. Matousek. "Fuzzy fault injection attacks against secure automotive bootloaders", Ruhr-Universität Bochum, pp.2-20, 2023.
〔19〕 Saeedi, Ehsan, and Yinan Kong. "Side-channel vulnerabilities of automobiles." Transaction on IoT and Cloud Computing, vol. 2, no. 2, pp. 1-8, 2014.
〔20〕 Y. Shoukry, P. Martin and P. Tabuada, "Non-invasive spoofing attacks for anti-lock braking systems." Cryptographic Hardware and Embedded Systems-CHES 2013: 15th International Workshop, Springer Berlin Heidelberg, pp.55-72, May, 2013.
〔21〕 R. Khan, K. McLaughlin and D. Laverty, "STRIDE-based threat modeling for cyber-physical systems." 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe. IEEE, pp. 1-6, Sep, 2017.
〔22〕 N. Shevchenko, T. Chick and P. Riordan, "Threat modeling: a summary of available methods." Software Engineering Institute| Carnegie Mellon University, pp. 1-24. Jul, 2018.
〔23〕 Van Landuyt, Dimitri, and Wouter Joosen. "A descriptive study of assumptions in STRIDE security threat modeling." Software and Systems Modeling, pp.1-18, Mar. 2022.
〔24〕 E. Bygdås, "Evaluating threat modeling tools: Microsoft TMT versus OWASP Threat Dragon." 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment. IEEE, pp. 1-7. Jun. 2021.
〔25〕 Min-Ju Park, Ji-Eun Lee, Hyo-Jeong Park, Yeon-sup Lim. Analysis of Self-driving Environment Using Threat Modeling. Jouranl of Information and Security, 22(2), pp. 77-90, Jun. 2022.
〔26〕 United Nation, "UN Regulation No. 155 - Cyber security and cyber security management system", E/ECE/TRANS/505/Rev.3/Add.154, pp. 1-30, Mar. 2021.
〔27〕 Korea Internet & Security Agency, "Self-driving vehicle security model", pp. 1-30. Dec. 2022.
〔28〕 Dong-Hoon Kim, "UGV Attack Library", https://docs.google.com/spreadsheets/d/1Am3rjUDXjsQK5mPLASDuHr6zUtVOd8oipJ7aLUdQApM/edit?usp=sharing, Sep. 2024.
〔29〕 Kerns and J. Andrew, "Unmanned aircraft capture and control via GPS spoofing." Journal of field robotics, vol. 31, no. 4, pp. 617-636, Apr. 2014.
〔30〕 Seo, Seong-Hun, et al. "Effect of

spoofing on unmanned aerial vehicle using counterfeited GPS signal." Journal of Positioning, Navigation, and Timing 4.2, pp. 57-65, 2015.
[31] He, Daojing, Sammy Chan, and Mohsen Guizani. "Drone-assisted public safety networks: The security aspect." IEEE Communications Magazine 55.8, pp. 218-223, 2017.
[32] K. Zeng, S. Liu, Y. Shu, D. Wang, H. Li and Y. Dou, "All your GPS are belong to us: Towards stealthy manipulation of road navigation systems." 27th USENIX security symposium. pp. 1527-1544, Aug, 2018.
[33] T. Trippel, O. Weisse and W. Xu, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks." 2017 IEEE European symposium on security and privacy. IEEE, pp. 3-18. Apr, 2017.
[34] H. Jo, and W. Choi. "A survey of attacks on controller area networks and corresponding countermeasures." IEEE Transactions on Intelligent Transportation Systems vol. 23, no. 7, pp. 6123-6141, May, 2021.
[35] P. Thirumavalavasethurayar, "Implementation of replay attack in controller area network bus using universal verification methodology." 2021 International Conference on Artificial Intelligence and Smart Systems. IEEE, pp. 1142-1146, Mar, 2021.
[36] K. Lehira, H Inoue and K. Ishida. "Spoofing attack using bus-off attacks against a specific ECU of the CAN bus." 2018 15th IEEE annual consumer communications & networking conference. IEEE, pp. 1-4, Jan, 2018.
[37] C. Rani, H. Modares and R. Sriram, "Security of unmanned aerial vehicle systems against cyber-physical attacks." The Journal of Defense Modeling and Simulation vol. 13, no. 3, pp. 331-342, Nov. 2015.
[38] J. Yaacoub, H. Noura, O. Salman and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations." Internet of Things, vol.11, pp. 1-39. Sep, 2020.
[39] S. Jeong, "A study on ros vulnerabilities and countermeasure." Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction. pp. 147-148. Mar, 2017.
[40] R. Teixeira and I. Maurell, "Security on ROS: analyzing and exploiting vulnerabilities of ROS-based systems." 2020 Latin American robotics symposium, IEEE, pp. 1-6, Nov, 2020.
[41] R. Herberth, S. Korper and T. Stiesch, "Automated scheduling for optimal parallelization to reduce the duration of vehicle software updates." IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2921-2933, Jan, 2019.
[42] Lawrence, John. "ROS2 prevalance and security." Rochester Inst. Technol., Rochester, NY, USA, Rep. CSEC. pp. 793, May, 2020.
[43] Mount, Mike, and Elaine Quijano. "Iraqi insurgents hacked Predator drone feeds, US official indicates." CNN. com, 2009.
[44] Dong-Hoon Kim, "UGV Threat Analysis", https://docs.google.com/spreadsheets/d/10xxKTUpXF8ORzliFLwDVh06yRZeNz9UPg5oQbYD-o4g/edit?usp=sharing, Sep. 2024.
[45] A. Kaasen, G. Grov and F. Mancini, "Towards data-driven autonomous cyber defence for military unmanned vehicles-threats & attacks." Military Communications Conference 2022. IEEE, pp. 861-866, Nov. 2022.

〈저자소개〉

김 동 훈 (Dong-hoon Kim) 정회원
2019년 2월: 고려대학교 사이버국방학과 학사
2020년 2월~현재: 고려대학교 일반대학원 석사과정
〈관심분야〉 정보보호, 보안공학, 디지털포렌식

이 상 진 (Sang-jin Lee) 종신회원
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~현재: 고려대학교 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
〈관심분야〉 디지털포렌식