Journal of KIIT. Vol. 20, No. 11, pp. 163-185, Nov. 30, 2022. pISSN 1598-8619, eISSN 2093-7571 163
http://dx.doi.org/10.14801/jkiit.2022.20.11.163

사이버-전자 위협에 대한 드론 전투피해효과 모의 분석

서 상*, 김도훈**, 한상우***

Simulation and Analysis of Drone Combat Damage Effect Against Cyber-Electronic Threats

Sang Seo*, Dohoon Kim**, and Sangwoo Han***

이 연구는 국방과학연구소의 지원(계약번호: UE202077ID)을 받아 수행되었습니다

요 약

전술 드론을 임무 수행에 활용하기 위해서는 사이버-전자 위협에 따른 임무 수행 제한 요인을 파악하고 적절히 대응하기 위한 체계 운용 개념 정립과 함께, 작전 요구 능력에 대한 선제적 분석 또한 요구된다. 이를 위해서는 사이버-전자 위협에 의한 드론의 취약점을 분석하고, 위협이 가해졌을 때 드론의 전투피해를 평가하기 위한 모의 분석 기법이 연구되어야 한다. 이에 본 논문에서는 STRIDE 위협 모델링 기법을 이용하여 드론 표적 취약성을 분석하고, 드론의 전투피해를 분석할 수 있는 NS-3 기반 워게임 시뮬레이션 프레임워크를 제안한다. 제안하는 프레임워크는 범용 데이터 통신 프로토콜을 이용하는 드론의 애드혹 무선망을 모의 분석 대상으로 한다. 이를 통해 사이버-전자 위협에 따른 드론의 통신 품질 저하를 시뮬레이션하여 위협효과도를 산출함과 함께 위협 징후에 대한 탐지 및 대응 논리를 수립하기 위한 향후 연구 방향 또한 제시한다.

Abstract

In order to use drones for tactical mission execution, it is necessary to establish a concept of system operation and derive operational requirement capabilities to identify and properly respond against cyber-electronic threats. For this, simulation schemes should be studied to analyze the vulnerabilities of drones caused by cyber-electronic threats and to evaluate drone battle damage. Therefore, in this paper, we propose an NS-3(Network Simulator 3)-based simulation framework that possibly analyzes drone target vulnerabilities and drone battle damage using a threat modeling tool called STRIDE. The proposed framework targets ad-hoc-based wireless drone network using general-purpose data communication protocols. We simulate the degradation of the communication QoS(Quality of Service) of drones due to cyber-electronic threats and calculate threat effects, and then present research directions for simulating detection and response to threats.

Keywords
cyber-electronic threats, vulnerability analysis of drones, effectiveness analysis, network simulation

* 경기대학교 AI컴퓨터공학부 연구원
- ORCID: https://orcid.org/0000-0003-1524-3710
** 경기대학교 AI컴퓨터공학부 교수(교신저자)
- ORCID: https://orcid.org/0000-0001-6370-9744
*** 국방과학연구소 지상기술연구원
- ORCID: https://orcid.org/0000-0002-9529-9505

· Received: Oct. 14, 2022, Revised: Nov. 10, 2022, Accepted: Nov. 13, 2022
· Corresponding Author: Dohoon Kim
Department of Computer Science, Kyonggi University, Suwon 16227, Gyeonggi-do, Korea
Tel.: +82-31-249-1364, Email: karmy01@kyonggi.ac.kr

Ⅰ. 서 론

현대전 패러다임 변화에 따라, 과거의 소모전에서 네트워크 중심전 기반 동시 통합 작전 형태로 변화하고 있다. 이러한 요구에 따라 국방 분야에서도 드론을 활용하여, 차세대 전투플랫폼의 일부로 시범 운용하고 있다. 그리고 유무인 전투체계의 전투 효율을 유지하고 임무 수행 가능성을 보장하기 위해, 공세적 소프트킬(Soft-kill) 위협으로 인한 제한 요인을 식별 및 차단, 대응하기 위한 방어개념이 연구되고 있으며, 구간 암호화 및 공인인증 모듈[1]을 적용하는 방안이 유력 검토되고 있다[2].

하지만 현 단계에서는 소규모 통신망의 통신 채널 가용성 및 무결성 확보에만 집중할 뿐, 원격 드론을 겨냥한 전문화된 사이버-전자전[3-5]을 전면 차단하고 탐지, 대응하기 위한 보안 체계 운용 개념 연구는 미진한 상황이다. 또한 Mobile WiMAX[6] 및 LTE[7], WiFi[8] 등의 범용 무선 표준들로서 대상 드론의 원격제어 채널의 도메인 활용성을 추가 확장할 때, 관련 취약성과 전투피해 파급효과에 대한 검토 역시 필요한 시점이다. 더불어 사이버-전자전 상황에서 드론 통신부 및 페이로드부 전용 취약성을 겨냥한 위협 논리와 공격 시퀀스 모델링도 구체적이지 않음과 함께, 관련 효과도 분석도 국내외 모두 개념 연구 단계에 머무르는 실정이다.

즉 이러한 사이버-전자전 위협에 대한 분석과 교전 논리가 충분하지 않을 시, 고도화된 공세적 위협으로 인해 대상 무인체계의 임무 수행 가능성이 급격히 감소할 것으로 예상된다. 이 때 이러한 한계를 극복하기 위해서는 드론 표적 취약성 기반 사이버-전자전 위협 모의 개념이 반드시 고려되어야 하며, 민첩성(Agility)[9] 및 복원성(Resilience)[10] 확보와 관련된 경쟁적인 탐지 및 대응방책 논리도 연구되어야 한다. 이에 위협 유형별 드론의 전투피해를 분석할 수 있도록 설계된 통합 M&S(Modeling and Simulation) 프레임워크 연구가 반드시 필요하다.

이에 본 논문은 보안성 평가를 위해 표준화된 STRIDE 위협 모델링[11]을 활용하여 무선 드론에 대한 취약성을 분석함과 함께, 공세적 사이버-전자전 위협에 따른 위협효과도를 비교 분석할 수 있는 통합 M&S 프레임워크를, 오픈소스 네트워크 시뮬레이터인 NS-3[12]를 이용하여 제안한다. 그리고 각각 통신 전자전 기반 반응적 주파수형 재밍(Jamming)과 채널 홉핑형 항재밍(Anti-jamming), 사이버전 기반 스푸핑(Spoofing)형 중간자 공격, 봇넷형 디도스(DDoS) 공격, 블랙홀(Blackhole)[13]형 독립 라우팅 오염 공격, 웜홀(Wormhole)[14]형 협업 라우팅 오염 공격, 웜 파급에 따른 악성코드 장입 및 감염 공격과 같은 드론형 사이버-전자전 위협에 대한 드론 전투피해를 분석한다. 최종적으로 범용 통신 표준 각각에 대해서도 드론 페이로드부 영역 내 통신-위협 모의 모듈 형태로 구조화하여 위협효과도를 산출하고 비교한다.

이러한 연구를 통해 달성할 수 있는 주요 기여사항은 다음과 같다. 첫째, 네트워크화된 다종 군 무인기동체계 취약성에 기반한 사이버-전자전 무선위협 개념들을 국내외 최초 정립, 표준화할 수 있다. 둘째, 사이버-전자전 위협에 따른 아군 전투체계의 교전효과 분석을 수행할 수 있는 워게임 M&S 방법론 또한 실질 군 S/W 형태로 신규 도입, 적용할 수 있다. 셋째, 선제 분석된 워게임 효과도 결과에 근거하여, 지휘결심체계 하 복원성 및 민첩성을 고려한 능동대응전략 구성 역시 신속히 달성할 수 있다.

본 논문의 구성은 다음과 같다. 먼저 2절에서는 선행된 M&S 및 사이버-전자전 연구 사례들을 조사하고, 이를 제안 연구와 비교 분석, 평가한다. 다음으로 3절에서는 이산적 사건 모의(DEVS, Discrete Event Simulation)[15]에 근거한 NS-3 기반 드론형 사이버-전자전 교전 모의 분석 프레임워크를 주요 컴포넌트 구성 관계에 근거하여 정의하고, 표준화된 STRIDE 위협 모델링을 활용하여 드론 표적 취약성 요소들을 추가 분석 병행한다. 그 후 이러한 상관성에 근거하여 4절에서는 드론형 사이버-전자전 위협 유형과 관련 모의 시퀀스를 상세 설계하고, WiFi 및 Mobile WiMAX, LTE 기반 범용 데이터 통신 표준이 통합 적용될 군집드론 실험 환경을 주요 파라미터별로 구축한다. 그리고 5절에서는 드론형 사이버-전자전 위협 유형과 범용 데이터 통신 표준별로 구분된 모의 실험 결과들을 통신 및 위협 메트릭별로 산출하고, 비교 분석한다. 마지막으로 6절에서는 연구결과에 대한 고찰과 기대효과, 향후 연구방향을 서술하면서 본 논문을 맺는다.

II. 관련 연구

2.1 사이버-전자전 연구 배경 및 사례

현대전 개념이 다영역작전[16]으로 발전되고 있고, 사이버 공간이 전자기파 영역과 함께 제5의 전장으로 인식되면서, 두 영역의 시공간적 상관관계가 주목받게 되었다. 이에. 미국에서는 '사이버 전자전 활동(CEMA, Cyber Electromagnetic Activities)'[17]이라는 교본을 발간하여 사이버전과 전자전이 교차되는 공통 영역에 대한 융합을 수행하였으며, '사이버-전자전 공간(Space of cyber-electromagnetic warfare)'이라는 고유한 전장 개념을 새롭게 정립하였다.

더불어 이러한 신규 전장 개념을 중심으로, 전자전 능력으로 무선 전자기 스펙트럼에 악영향을 초래함과 동시에 사이버전 능력을 발휘함으로써, 마비 및 교란, 훼손, 누락, 감청, 조작, 위조, 기만 등 비물리적인 교전 효과를 달성하는 소프트킬 개념도 정립하였다. 그리고 '발사의 왼편(Left of launch)'[18]과 같이, 단순히 대상 지휘통신체계를 무력화시키는 것을 넘어, 교전 조건에 따라 감시정찰체계의 역량과 무장 투발까지 방해하거나 교란, 마비시키는 운용 개념을 수립하였다.

이러한 접근에 따라, 주요국들 중 극소수는 무기체계 개발단계에 수립된 사이버-전자전 개념을 초기 적용한 바 있다. 대표적으로 윈도우(Windows) 익스플로터(Exploiter) 장비이면서, 최대 12KM 거리 내에서 스파이 소프트웨어를 주입하여 대상 WiFi 네트워크를 손상시킬 수 있는 'Night Stand'[19]가 보고되었다. 러시아의 Krasukha[20]는 표적화된 저궤도 정찰 위성과 지상-공중 레이더 모두를 무력화시킴과 더불어, 적의 전자 시스템 모두에 대한 통신 교란 전파 또한 송출하여 공중 표적에 대응하는 공세적 전자 장비로서, 항공무인체계의 자폭과 납치, 추락 등을 유도하기 위해 주요로 운용되었다. 또한 사회공학적 해킹(Social-engineering hacking)[21] 심리전 수행을 위해 개량된 RB-341V Leer-3[22]가 도입됨으로서, WiFi 기반 액세스포인트 (AP) 대상이 아닌, GSM 및 3G, LTE 통신 장비을 겨냥하여 실제 전장에서 운용된 바 있다.

하지만 이러한 극소수의 국외 보고 사례들 또한, 모두 일관된 구조의 기존 무선통신 모듈을 보유한 유인 무기체계만을 대상으로 수행되었으며, 미국을 제외하고는 대부분 전자전 범위에 치중되어 있는 것으로 공식 보고된다. 한편, 국내에서는 별도 제원 정보와 운용 교범, 작전 유형, 동적 무인체계, 전투효과 등의 군 특수성과 고유성 모두를 고려하지 않은 챔버(Chamber) 환경 조건에서, 범용 WiFi 통신 모듈을 겨냥한 무선위협 시퀀스만을 채택하여 분석한 것으로 역시 보고[23]된다.

상기 문헌 조사를 통해, 드론에게 잠재적으로 발생 가능한 공세적 사이버-전자전 위협들에 대한 취약성 모델링이 요구되고, 위협 파급 효과에 따른 드론의 전투피해를 모의 분석하는 연구가 필요함을 다시 한번 확인할 수 있다. 이 때 이러한 모의 분석 연구의 고도화를 위해, 사이버-전자전 M&S 사례들을 분석한다.

2.2 전투효과 M&S 연구 사례

에이전트 행위 개념에 근거한 선행연구 사례로서, 먼저 Hayward 등[24]은 '능력', '환경', '임무'라는 3가지 매개 변수를 채택하여 전투분대의 전투 효율을 정량화하고, 워게임 실험 환경 내 주요 파라미터로서 적용하였다. 다음으로 Cil 등[25]은 2계층 하이브리드 에이전트 아키텍처를 함양한 ACOMSIM 워게임 프레임워크를 설계 구축함으로서, 다차원화된 동적 전장 환경 내 지휘관 지휘 결심과 관련된 소규모 교전 영향 분석을 병행하였다. Seo 등[26]은 플랫폼 및 무기, 독립-연합임무 기반으로 세분화된 워게임 DEVS 컴포넌트를 활용함으로서 다단계화된 합동 교전 객체 모의 모델을 구조화하였다. Connors 등[27]은 항공 임무 시나리오와 관련 전투 개체들을 적용하여, 파라미터별 SACM(Small Advanced Capability Missile) 무기체계의 공중전 효과도를 비교 분석하였다. Thompson 등[28]은 MANET(Mobile Ad hoc Network) 기반 모바일 애드혹 망에서 악성코드 장입 및 감염, 파급 행위를 기반으로 에이전트 기반 M&S 프레임워크를 구성하여, 보안성 강도에 따른 사이버 교전 비대칭성 감쇠도를 비교하고 무선망 보안 지속 유지의 중요성을 재확인하였다.

다음으로 행위 개념에 세부 통신 지표를 변인으로 고려한 선행연구 사례로서, 먼저 Shin 등[29]은 전파-가스 손실 모델 기반 수신신호세기(RSS, Received Signal Strength) 변화에 따른 네트워크중심전 환경 내 교전 효율성 증감 관계를, 신속한 의사결정 도입의 중요성과 함께 입증하였다. Li 등[30]은 결정점(Decision point) 기반 기지국 배치 프로세스를 모델링함으로서, 전장 환경 내 최적화된 셀룰러 통신을 지원하기 위한 통신 모의를 지표별로 비교 수행하였다. Akhtar 등[31]은 차량 흐름, 속도, 수신신호세기, 장애물 및 거리 분포 등의 이동성 개념이 포함된 오픈소스 기반 트래픽 시뮬레이터를 활용하여, 차량형 애드혹(VANET, Vehicle Ad hoc Network) 내 무선통신 토폴로지의 시공간적인 이산 변화를 모의하였다. Regragui 등[32]은 MANET 형태로 상호 연결된 지휘관과 분대원 간 보병 대형의 구성과 기동에 따른 통신 안정성 변화를 모의하고, 이에 대한 평가 검증을 병행하였다. Lee 등[33]은 분대 가시 통신(LOS, Line-Of-Sight) 가능성과 전투효과도 간의 통계적 상관성을 산출하기 위한 교전 모델링을 설계하였으며, 통신 중계기 도입에 따른 비가시 통신(NLOS, Non-Line-Of-Sight) 보장의 교전 효과도를 추가 분석하였다. 마지막으로 Seo 등[34]은 드론 기반 유무인협업체계를 겨냥한 임의 사이버-전자전 무선위협들에 대해, 패킷 전달율(PDR, Packet Delivery Ratio) 기반 통신 가용성 훼손 정도에 근거하여, 각 위협별 전투피해효과도 비교 분석을 수행하는 NS-3 기반 D-CEWS를 설계하였다.

2.3 문헌별 비교 및 연구 차별성 분석

Lee 등의 연구[33] 이전 선행된 워게임 M&S 연구들은 대부분 통신 가용성과 교전 효율성 간의 연관성을 고려하지 않았으므로, 기존 연구개념들로는 무인화 및 네트워크화 중인 통신체계 능력을 온전히 분석하지 못하는 한계성을 내포한다. 이에 Lee 등은 상위 지휘관 입회 하에 C2 통신에 의존적인 교전 모의 개념을 부가함으로써, 임무 지속 가능성 향상을 위한 LOS 및 NLOS 통신 보장의 중요성을 모의하였다. 하지만 Lee 등의 연구는 단순히 급변하는 전장 환경 요인에 따라 송수신이 불가한 가정으로서 개념화했기에, 여전히 공세적 사이버-전자전 위협 행위에 따른 비대칭적 열위 관계를 모의할 수 없었으며, 저충실도 행위 기반 단순 과업 형태로 모사함에 따라 패킷 기준의 무선통신 환경에 대해서도 모의하지 못하는 한계가 있다. 이에 대해 Thompson 등의 연구[28]에서는, 악성코드 감염에 근거한 응용 침해 행위로서 무선 애드혹 내 보안성 확보의 중요성을 간략히 제시한 바 있지만, 여전히 고유 무선통신 요소들과 제원 정보를 고려하지 않았다는 한계성이 잔존한다. 이러한 선행 연구의 한계성들을 모두 고려하여, Seo 등의 연구[34]는 사이버-전자전 위협 개시 전후에 따라, 대상 무인체계의 정찰 임무 지속 효율성을 비교 분석한 초기 연구를 수행하였으나, 정의된 위협 유형들이 도입된 이유가 명확히 서술되지 않았으며, 다양한 범용 통신 표준에 대해서도 비교 분석이 미비한 이슈가 잔존한다.

이러한 문헌 서술에 기반하여 기존 대비, 제안 연구가 사이버-전자전 교전 공간 내 표적 취약성이 식별된 다종 범용 통신 모듈들을 페이로드부에 탑재한 군집드론 지상전투플랫폼의 전투피해효과도를 분석할 수 있음과 함께, 항재밍과 같은 경쟁적 방호 개념 역시 구현 가능함을 확인할 수 있다. 이는 후술될 3절, 4절, 5절에서 상세히 언급하도록 한다.

III. 드론형 무선위협 모의 기법

3.1 드론형 무선위협 모의 프레임워크

제안하는 드론 무선위협 모의 프레임워크의 주요 아키텍처는 그림 1과 같이 총 6개의 컴포넌트(전장, 개체, 비행, 이동성, 통신, 평가)들로 구성된다.

개체 컴포넌트인 [Combat Entity]는 부여된 임무를 수행하는 드론과 사이버 위협 개체, 무선 주파수(RF, Radio Frequency) 및 페이로드 데이터 통신 형태로 드론 원격제어와 명령 하달을 병행하는 지상통제소(GCS, Ground Control Station), 적용된 범용 무선 통신 표준 및 임무 유형에 따라 별도 데이터 링크 기반으로 부가 정보를 송신하는 서비스 제공자(ZSP, Zone Service Provider) 등의 주요 직간접적인 교전 에이전트들을 개념화하여, 드론 외부 통신 개체별 상호 통신 관계를 모델링한다.

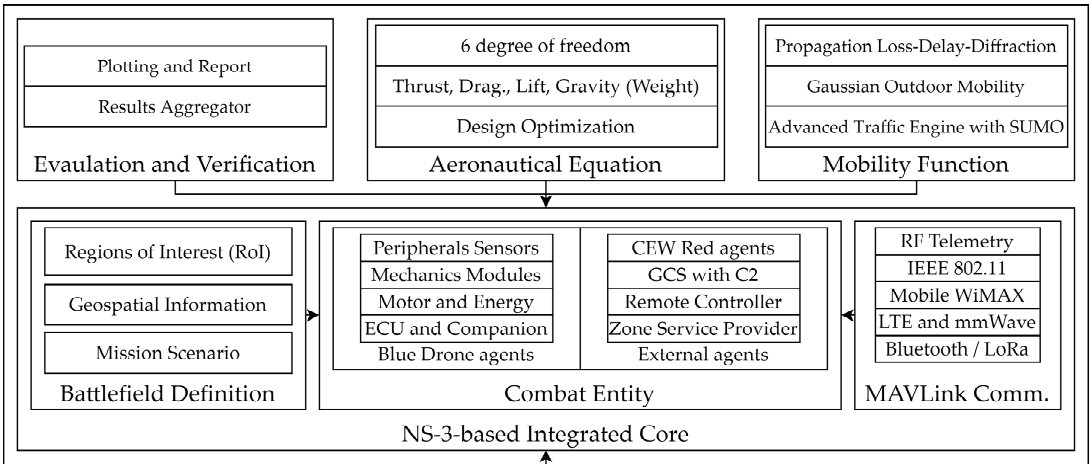


그림 1. NS-3 기반 드론형 무선위협 모의 프레임워크 개요도
Fig. 1. Major overview of drone-type cyber-electronic warfare combat framework based on NS-3

더불어 각 단일 드론 내 내부 기능별 상호 통신 관계를 추가 구성함과 함께, 위협 발생에 따른 이상 상태 여부를 판단하기 위해, 로터(Rotor) 기반 모터와 전자변속기(ESC, Electric Speed Controller) 배터리, 컴페니언 모듈 기반으로 내부 구조를 모델링한다.

다음으로 전장 컴포넌트인 [Battlefield Definition]은 사이버-전자전 무선위협을 개시하는 사이버 위협 개체와, 드론 표적 개체 간 국소화된 사이버-전자전 교전 공간을 관심영역 (RoI, Region-Of-Interest) 형태로 명세화하여, 위협 파급 범위를 한정한다. 통신 컴포넌트인 [MAVLink Communication]는 드론 내 장착된 통신부 내 RF 텔레메트리 모듈과 페이로드부 내 데이터 범용 통신 모듈(WiFi, Mobile WiMAX, LTE)을 중심으로 개체별 데이터 송수신 행위를 이산적으로 모의함으로서, 개체별 부여된 임무를 수행한다. 이동성 컴포넌트인 [Mobility Function]는 교전 개체별 방사된 RF 무선 전파신호의 수신신호세기 (RSS, Received Signal Strength)와 손실, 굴절, 지연 등을 세부 모사함과 함께, 비행 행위와 연관되는 임무점 및 경로점 기반 기동 트래픽 요소를 정형화한다. 항공 역학 컴포넌트인 [Aeronautical Equation]은 전투피해효과 분석 대상인 드론 개체의 6-자유도(Six-degree-of-freedom) 기반 요(Yaw)-피치(Pitch)-롤(Roll)과 함께, 추력 및 항력, 양력, 중력 등을 기존 개체 물리 함수에 가산하는 역할을 수행한다. 마지막으로 평가 컴포넌트인 [Evaluation and Verification]는 교전 개체별 사이버-전자전 위협 모의 완료에 따라 1차 산출된 PDR 기반 통신 가용성 훼손 정도를 최적화하여, 정규화된 전투피해효과도를 보고한다.

3.2 드론 위협 모델링

3.2.1 STRIDE 기반 드론 취약성 분석

다음으로 잠재적인 드론 취약점을 분석한다. 운용되는 대부분의 범용 드론의 통신 제원 정보와 고유 장비 특성, CVE(Common Vulnerabilities and Exposures) 공인 취약점 등은 대부분 공개되어 있므로, 사이버 위협 개체가 의도하면 필요한 신호정보를 신호분석기를 이용하여 사전 수집하여 사이버 표적 취약성을 예상, 파악하여 활용할 수 있다. 그리고 범용 드론 내 데이터 송수신 표준들은 대부분 전용화된 비공개 통신 프로토콜이 아닌 WiFi 및 LTE 등의 공개된 범용 통신 프로토콜이다. 또한 송수신되는 드론 비행 메시지 표준은 MAVLink (Micro Air Vehicle Link)에 기반을 두고 있으므로, 사이버 위협 개체가 고려해야 하는 침투 고려 범위를 대폭 축소할 수 있다. 더불어 드론 내 적용된 통신 채널 및 구간 암호화 기법의 대다수는 야전 환경에서 송수신 성능과 라우팅 등의 망 성능을 보장해야 한다. 즉 패킷 내 주요 데이터 및 인증값들이 위치한 페이로드 영역과 일부 상태 플래그에 대해서만 암호화할 뿐, 송수신자 정보가 포함된 헤더 영역에 대해서는 직접적으로 암호화하지 않는 것이다.

이를 모두 고려할 때, 암호화되지 않은 패킷 내 헤더 필드 정보들을 취약한 공격 표면(Attack surface)으로서 수집 완료 후, 악용(Exploit) 단계에서 활용하거나, 통신 기능성 자체를 훼손하는 위협 행위에 대해서는, 채널 구간 암호화 방식만으로는 온전한 사이버 방호 효과를 기대할 수 없을 것이다. 더불어 신호분석기를 이용한 표적 주변의 전파 환경 분석을 바탕으로, 드론의 주파수와 변조 방식, MAC(Media Access Control) 주소 등 고유제원 정보 일부를 파악하여 표적을 특정할 수 있다면, 사이버전 수행을 위한 전자전 위협을 병행할 수 있을 것이다. 이에 근거하여, 드론에 대한 사이버-전자전 위협을 잠재적으로 발생 가능할 것으로 판단된다.

이 때 이러한 드론 취약성을 모듈별로 도출함과 함께, 통신에 따른 행위 수행 기준과 연관된 위협 파급 과정까지 분석하기 위해, STRIDE[35] 기반 위협 모델링 기법을 활용한다. STRIDE는 인증 및 무결성, 부인방지, 기밀성, 가용성, 권한 부여와 같은 6가지 요소를 중심으로, 대상 체계의 보안성을 취약성 기준에서 평가 분석할 시 주요로 활용되는 위협 모델링 방법[36]이다. 이를 활용한다면 드론에 대한 통신 취약성을 모두 식별함과 함께, 사이버-전자전 교전 공간에서 공세적 위협 시퀀스들 중, 표적 취약성 프로파일링 생성 정보에 기인하여 공격을 개시하는 전처리 단계를 모의할 수 있을 것이다. 더불어 드론 관점에서도 취약성 기반 침투 행위가 성공하기 이전에 사전예방적으로 취약성을 자체 검토함과 함께, 연관된 위협 유형별로 방호대책을 모의함으로서, 탐지 및 대응 행위도 모의할 수 있을 것이다. 그에 따라 최종 구성한 STRIDE 기반 드론 위협 모델링은 표 1 내 주요 평가 속성들에 참조하여, 그림 2와 같은 데이터 플로우 다이어그램으로서 결정한다.

표 1. 드론 사이버-전자전 무선통신 취약성 분석을 위한 STRIDE 속성
Table 1. Properties of STRIDE for cyber-electronic warfare-based wireless communication vulnerability analysis on drone

Threat property	Definition(based cyber-electronic warfare)	Counter-measure
Spoofing Identity	Acquire mission authority related to the target entity by using the legal authentication data of other entities	Authentication
Tampering with data	Unauthorized modification, deception, and disinformation of target specialized data, codes and information	Integrity
Repudiation	Intentional denial of actions performed, avoiding the concept of cryptographic access and authentication	Non-repudiation)
Information disclosure	Loss of control and leakage of confidential information about illegal-unauthorized threat entities	Confidentiality
Denial-of-service	Damage or denial of service provision availability being performed by other entities	Availability
Elevation of privilege	Acquiring administrator service rights of illegal-rogue threat objects	Authorization

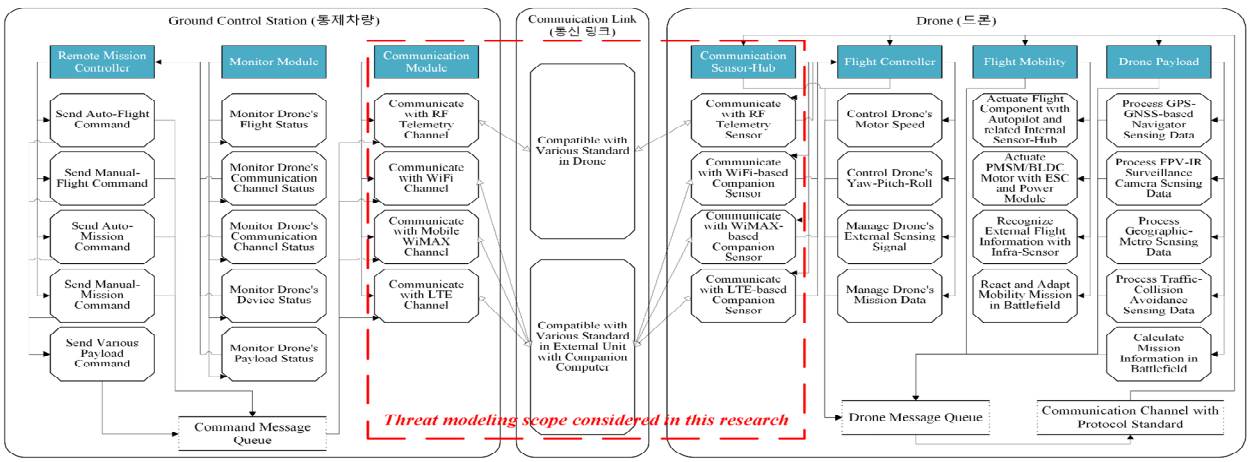


그림 2. STRIDE 기반 드론 위협 모델링 데이터 플로우 다이어그램
Fig. 2. STRIDE-based data flow diagram with threat modeling on tactical drone

이로서 전자변속기와 모터, 저장소, 비행 제어기 등과 같은 드론 내부 기능 컴포넌트와, GCS와 ZSP와 같은 드론 외부 통신 개체 관계 간 잠재적인 표적 취약성을 개념화하였으며, 그 중 통신 가용성 훼손 정도에 근거하여, NS-3 기반 전투피해평가 모의를 위한 측정 범위로서 RF-페이로드 통신 모듈별 상세 취약성 역시 추가 검토하였다. 그리고 이렇게 선제 식별한 취약점과 공격 표면을 참고하여, 발생 가능한 위협 유형들은 표 2와 같이 드론 통신 계층별 취약 접점별로 구분하여 분석하였다. 이를 통해 모의 가능한 주요 사이버-전자전 위협을 전자전 기반 반응적 주파수형 재밍과 채널 홉핑형 항재밍, 사이버전 기반 스푸핑형 중간자 공격, 봇넷형 디도스 공격, 블랙홀형 독립 라우팅 오염 공격, 웜홀형 협업 라우팅 오염 공격, 웜 기반 악성코드 장입 및 감염 공격 등으로 최종 분류 완료하였다.

3.2.2 드론형 사이버-전자전 무선위협 구체화

다음으로, 드론 표적 취약성에 근거하여 표 3과 같이 정의한 드론 무선위협 유형을 NS-3를 이용하여 공격 시퀀스 형태로 구현한다.

먼저 재밍과 같은 RF 통신 가용성 방해 행위는 수신 안테나 및 신호 가산 레벨에서의 별도의 대응 방책이 없으면 유선망 및 무선망 모두에서 항상 유효함을 보인다. 이는 표적 드론 중심으로 구성되는 무선 애드혹 망이 유선망보다 전자기적 대응방책을 구사할 실질 가능성이 작으므로, 상대적으로 취약할 가능성이 더 높다는 특질에 기인할 것이다. NS-3로 위협을 모의할 때는 표적 드론의 환경적 변화나, 항재밍 기반 대응방책 적용에 따른 인위적 변화를 고려하여, 재머 제원값을 변경하면서 적응적인 주파수형 재밍 전파를 방사하도록 그림 3과 같이 구현한다. 그리고 방사된 해당 악의적 재밍 전파에 노출될 때, RF 통신 가용성이 훼손됨에 따라 피해가 발생하도록 모의한다.

드론이 송수신하는 전문을 탈취하거나 GPS 데이터 스푸핑을 하는 중간자 공격의 경우, 무선망 내 소속된 단말기별 인증 행위가 유선망 대비 낮은 강도로 수행되며, 전파 도달거리의 변화에 따른 패킷 수신이 지연되는 구조적 취약성을 주요로 활용할 수 있을 것이다. 이에 따라 NS-3 기반 위협 모의 시에는 표적 드론에게는 마치 적법한 중계 드론 또는 지상제어기인 것처럼, 중계 드론 및 지상제어차량에게는 마치 적법한 표적 드론인 것처럼 도플갱어(Doppelganger) 형태로 교란, 가장(Impersonation), 기만함으로써, 적법한 신원 획득을 수행하도록 그림 4와 같이 정의한다. 그 후, 단순 전문을 도청하거나 GPS 위치 정보를 탈취함으로써, 표적 드론에 대한 전투피해가 발생하도록 한다.

표 2. STRIDE 기반 드론 공격 표면을 고려한 사이버-전자전 무선위협 유형 정의
Table 2. Definition of cyber-electronic warfare-based wireless threat considering STRIDE-based drone's attack surface

Threat property	Counter-measure	Determined CEW	Attack surface in drone
Spoofing Identity	Authentication	Man-In-The-middle Blackhole attack Wormhole attack	Datalink, network, transport layer (in packet header area)
Tampering with data	Integrity	Blackhole attack Wormhole attack	Transport layer (in packet header & payload area)
Repudiation	Non-repudiation	-	-
Information disclosure	Confidentiality	Man-In-The-middle Blackhole attack Wormhole attack	Datalink, network, transport layer (in packet payload area)
Denial-of-service	Availability	Jamming DDoS	Physical, network, session layer (in TCP/UDP socket, RF telemetry)
Elevation of privilege	Authorization	Malware injection and infection	Network, transport, session, application layer (in socket channel, service payload)

표 3. 드론형 사이버-전자전 무선위협 상세 분류
Table 3. Taxonomy of cyber-electronic warfare-based wireless threat on tactical drone

Category	Type	Definition	Related property in standard
Communication electronic warfare	Jamming	Electronic warfare-based threat that interferes with RF telemetry-based transmission and reception by targeting a communication channel within a certain intermediate frequency range of the target entity	Loss of availability
Cyber warfare	Man-In-The-Middle	Cyber warfare-based threat that steals packets (combat message, GPS.) sent/received by disturbing the legal authority between the target entity and the communication relay entity	Man-in-the-middle
	DDoS	Cyber warfare-based denial-of-service threat that uses a botnet composed of multiple zombie bots to deplete and paralyze the target entity's network resources	Loss of availability
	Blackhole attack	Cyber warfare-based threat that absorbs all transmitted packets by counterfeiting the target entity as if it possesses legitimate and optimal routing information	Man-in-the-middle
	Wormhole attack	Cyber warfare-based threat that absorbs all transmitted packets and evades the reputation score-based detection system by using the shortest hidden tunnel in order for multiple threat entities to perform cooperative malicious actions within the ad hoc network to which the target entity belongs	Man-in-the-middle
	Malware injection and infection	Cyber warfare-based threat that disrupts and disrupts the overall communication availability and service operation of the ad hoc network to which the target entity belongs through self-replication, propagation, and infection	Execution of malicious program

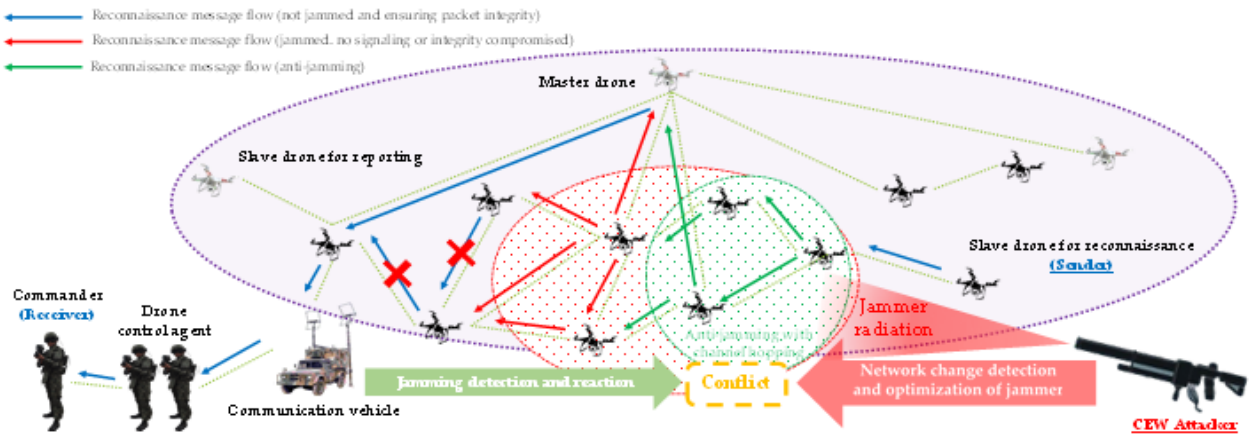


그림 3. 통신 전자전 기반 재밍 및 항재밍 교전 시나리오
Fig. 3. Combat scenario for electronic warfare-based jamming and anti-jamming

디도스와 같은 사이버전 가용성 방해 유형은 수신 대기 중인 소켓과 포트 서비스 자체에 통신 가용성 임계치 기준의 별도 대응 방책이 존재하지 않으면 유선망 및 무선망 모두에서 항상 유효함을 보인다. 그리고 디도스 위협 자체에 대한 대응방책을 운영에 따른 효율성 이슈 (디도스 범람 패킷을 탐지하여 무시하거나, 블랙홀 라우터 역할을 하는 노드로 중계하여 대응할 수 있으나, 비용이 높음)가 대두되는 한편, 표적 드론 중심으로 구성되는 무선 애드혹 망이 해당 대응방책을 보유할 가능성이 작으므로, 상대적으로 더 취약할 것이다.

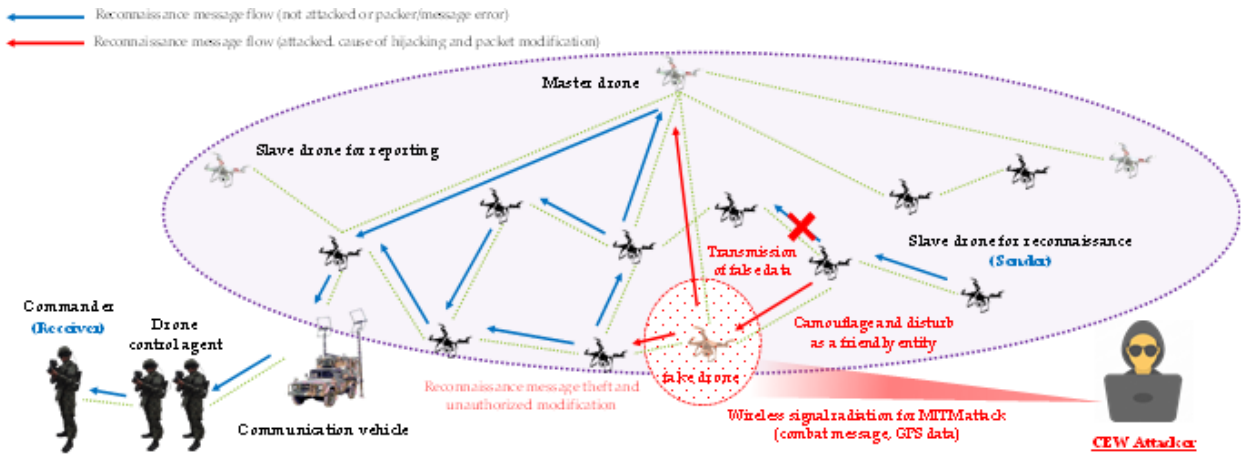


그림 4. 사이버전 기반 중간자 공격 시나리오
Fig. 4. Attack scenario for cyber warfare-based man-in-the-middle

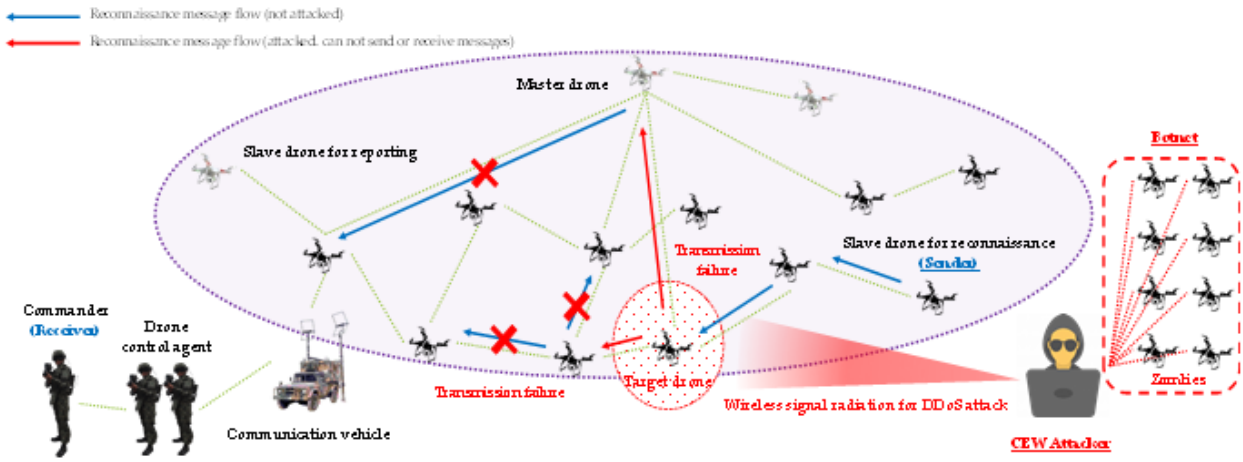


그림 5. 사이버전 기반 디도스 공격 시나리오
Fig. 5. Attack scenario for cyber warfare-based DDoS

이를 고려하여 NS-3 기반 위협 모의 시에는, 봇넷 좀비봇의 무작위 세션 개설 요청 행위 기반으로 표적 드론 UDP 소켓 내 패킷 수신 대기 큐와, 단편화 재조립 큐에 대한 서비스 범람을 수행하도록 그림 5와 같이 구성한다. 그리고 해당 디도스 공격에 따른 표적 드론의 네트워크 통신 가용성은 높이 훼손되도록 피해 범위를 조절한다.

다음으로 블랙홀형 단일 라우팅 오염 공격의 경우, 무선 애드혹 망에 소속된 드론 개체별로 라우팅 테이블을 각각 보유하고 있는 취약성을 주요로 활용한다. 즉 네트워크에 속한 임의 송신 개체가 특정 수신 개체에게 전문을 전달할 시, 해당 송신 개체는 자신이 보유한 라우팅 테이블을 통해 주변 개체들을 1차 식별하고, 그 주변 노드에게서 최적화된 라우팅 경로 정보를 수신받는 단계를 거친다. 이 때 만약 중간에 위협 개체가 침투한 후, 송신 개체에게 마치 최적의 라우팅 경로를 가지고 있으면서 수신 개체로 즉각 전달 가능한 것처럼 교란된 거짓 라우팅 경로 정보를 전달할 수 있다면, 위협 개체는 즉각 해당 비문을 획득, 도청, 수정할 수 있을 것이다. 이를 고려하여 NS-3 기반 위협 모의 시에는 표적 드론 개체가 속한 무선 애드혹 망에 위협 개체가 적법하게 참여하여 임의 배치된 후, 주변 노드에게 거짓 라우팅 정보를 전달함으로서 모든 송신 패킷들을 흡수하는 행위를 수행하도록 그림 6과 같이 정의한다. 그리고 단일 라우팅 오염 공격에 따른 드론 전체의 가용성 훼손 범위를 모의한다.

웜홀형 협업 오염 공격은 대상 애드혹 망의 규모가 크거나 평판 탐지 기반 라우팅 오염을 탐지하는 내부 대응방책이 존재하여 효과도가 감쇄되는 블랙홀 공격의 오염 범위를 확장한 유형으로, 위협 개체를 단수가 아닌 복수로서 추가 적법 진입하게 한 다음 위협 개체들끼리 은닉 채널로 시공간 동기화함으로써, 협업적인 악성 행위를 수행한다. 이에 따라 NS-3 기반 위협 모의 시에도 애드혹 망에 다수 위협 개체가 적법하게 합류한 후, 악성 풀 점유 기반으로 동기화된 패킷 흡수 행위를 협업 수행하도록 개량한다. 그리고 해당 다중 라우팅 오염 공격에 따른 망 내 송수신 탈취 범위를 개체별로 결정한다.

마지막으로, 네트워크 웜 기반 악성코드 장입 및 감염 공격은 무선 애드혹 망내 표적 드론 개체들이 독자적인 부하 분선으로 분할 통제되어, 개체가 아닌 네트워크 전체를 대상으로 한 위협 유형에 더 취약함을 활용한다. 이를 고려하여 NS-3 기반 위협 모의 시에는 웜 공격이 수신 대기 소켓에 기반한 점령 행위가 성공한 후에 순차 파급되도록 킬체인을 정형화함과 함께, 표적 드론을 기점으로 무차별적인 자가복제 및 소켓 통신 반복 생성을 통해 웜 확산이 유발되도록 그림 7과 같이 정의한다. 그리고 해당 악성코드 장입 및 감염 공격에 따른 극심한 트래픽 저하 및 가용 리소스 소모가 폭증함에 따른 드론 애드혹 망내 가용성 피해 범위를 조절한다.

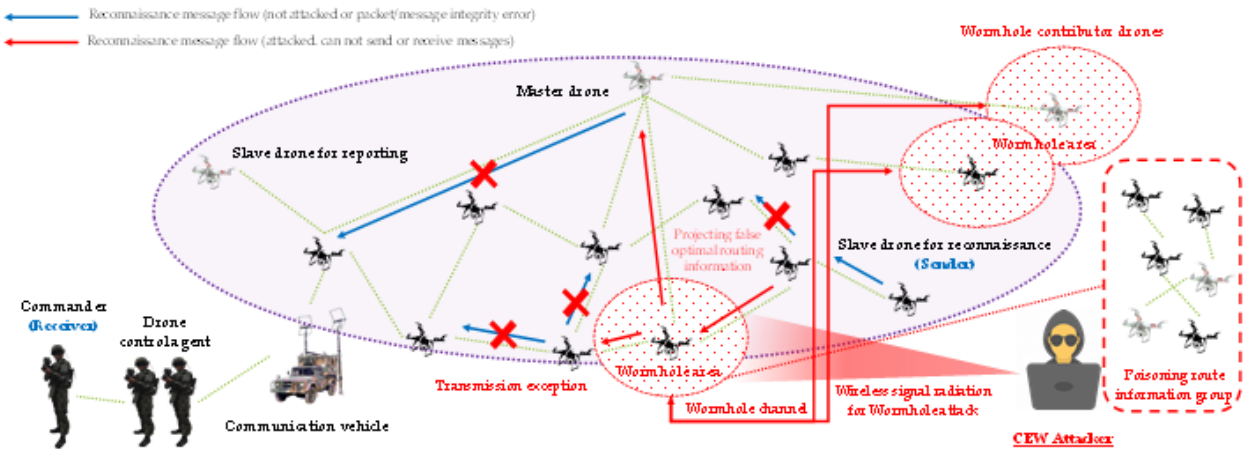


그림 6. 사이버전 기반 라우팅 오염 공격 시나리오(웜홀 공격 기반)
Fig. 6. Attack scenario for cyber warfare-based routing poisoning(based on Wormhole attack)

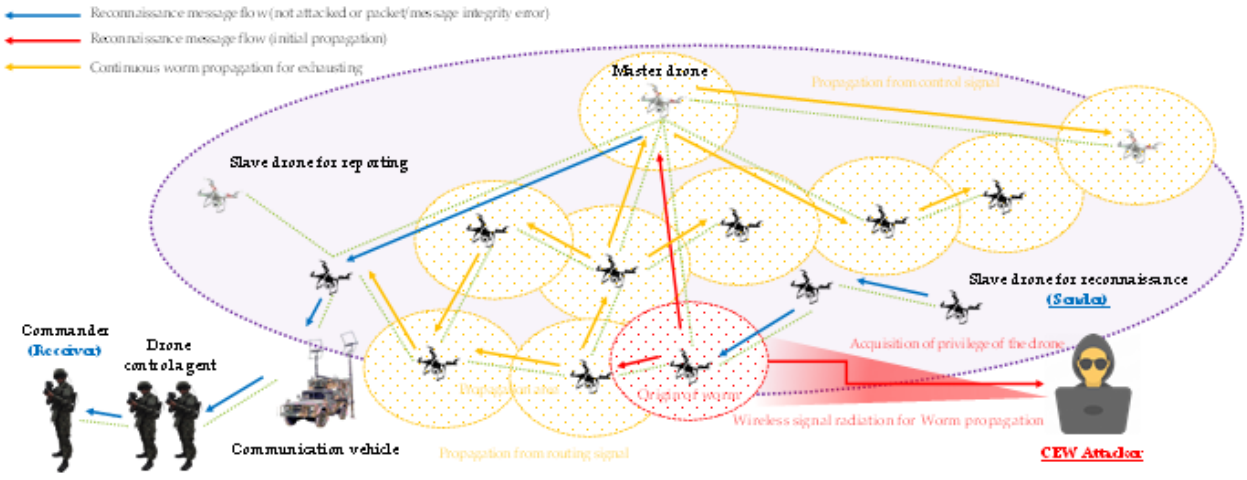


그림 7. 사이버전 기반 네트워크 웜 기반 악성코드 감염 공격 시나리오
Fig. 7. Attack scenario for cyber warfare-based malware infection with network worm

Ⅳ. 드론 무선위협 모의 실험

4.1 모의 환경 구성

드론에 대한 사이버-전자전 무선위협을 모의하고 전투피해효과를 산출하기 위한 교전 모의 환경을 그림 8과 같이, 사이버-전자전 무선위협을 방사하는 위협 개체인 사이버 위협 개체와 위협에 대한 교전 피해를 받는 군집형 드론 간 경쟁적 교전을 모의하기 위한 환경을 구성한다.

여기서 위협 개체는 표적 개체가 보유한 데이터 통신 모듈과 동일한 모듈을 보유하도록 구성한다. 그리고 WiFi와 달리, Mobile WiMAX, LTE와 같은 업-다운링크 기반 기지국 중계가 필수인 원격제어 환경에서는, 별도 기지국 개체와 기지국 중계 채널 등은 위협 대상에서 제외되도록 교전 효과 범위를 한정한다. 아울러, 단수 드론 개체에 대한 위협과 애드혹 망에 속한 다수 드론 개체에 대한 동시다발적/순차적 위협 및 피해를 모의한다.

즉 재밍과 중간자 공격, 디도스 공격은 단수 드론 개체에 대해서만 가용성 훼손이 발생하도록 정의하고, 라우팅 오염 공격은 타 표적 드론 개체로의 피해 파급이 동시 병행되도록, 악성코드 장입 및 감염 공격은 순차 파급되도록, 킬체인 기반 교전 효과 발생 범위 및 순서를 조정한다. 더불어 최종 도출된 임의 표적 드론 개체의 위협효과도에 대한 노이즈를 최소화하고자, 전자전 기반 재밍 공격을 제외한 나머지 사이버전 무선위협에 대한 방호 행위는 현 모의 단계에서는 생략한다.

4.2 위협별 주요 파라미터 결정

다음으로 그림 9와 같이 간략 분류된 위협 유형별로 드론 전투피해효과 비교 분석을 수행하기 위해, 모의 파라미터를 표 4와 같이 정한다.

먼저 주파수형 재밍의 경우 RF 텔레메트리 제원을 중점으로 반응형 재머의 교란 강도와 빈도, 가동시간 등을 결정하고, 항재밍 요소 역시 부연한다. 디도스 공격의 경우, 서비스 거부의 발현 유형과 좀비 봇넷 동작 시퀀스, 플러딩 패킷 형태를 결정한다. 블랙홀 공격과 웜홀 공격은 패킷 흡수를 수행하는 악성 노드의 개수와 은닉 채널의 존재 여부로서 구분하여 구현함과 함께, 권한 스푸핑에 대한 단순화된 시퀀스는 중간자 공격 내에 반영한다. 웜 기반 악성코드 감염 공격은 웜 전파 프로세스에 기반하여 정찰과 전달, 익스플로잇을 확률변인에 근거하여 산정한다.

Ⅴ. 주요 성능 평가

5.1 단일 표적 위협별 피해효과 민감도 분석

NS-3 기반 M&S 프레임워크를 이용하여 군집드론의 취약성을 겨냥한 사이버-전자전 위협을 모의하였으며, 그림 10-15와 같이 결과 분석을 하였다.

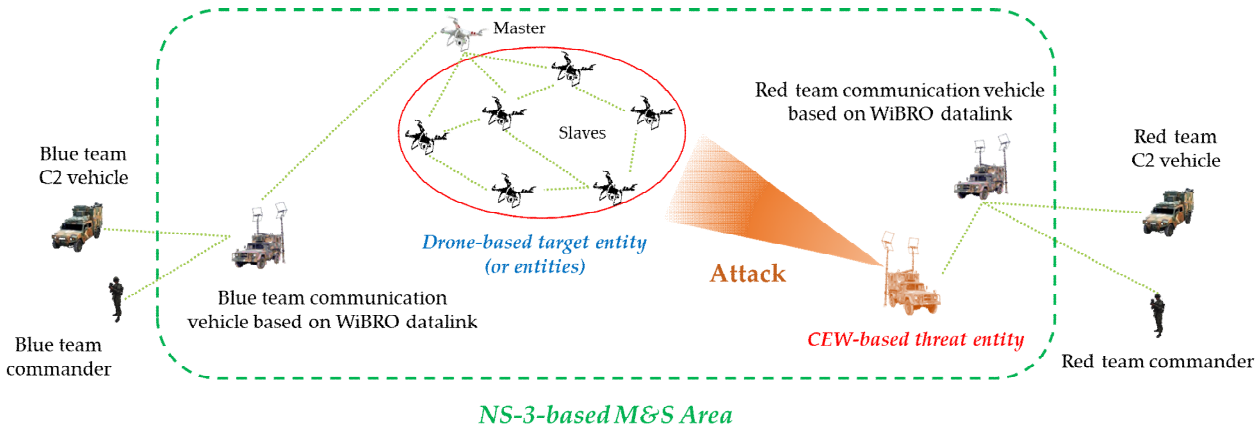


그림 8. NS-3 기반 드론형 사이버-전자전 교전 M&S 환경(Mobile WiMAX 통신 기준 예시)
Fig. 8. M&S environment of drone-type cyber-electronic warfare wireless threat based on NS-3

표 4. 드론 무선위협 유형별 NS-3 기반 주요 M&S 파라미터 정의 (Mobile WiMAX 통신 기준)
Table 4. Definition of major M&S parameters by drone wireless threat based on NS-3

Type	Major M&S parameter	Value
Common	Communication standard	IEEE 802.16e (mobile wimax)
	Transmission method	OFDM (orthogonal frequency division multiplexing)
	Modulation method	64-QAM
	Coding rate	3/4
	Transmission speed	1 Mbps ~ 25 Mbps
	Service class in up-downlink	BE (best-effort service), UGS (unsolicited grant service)
	QoS link scheduler	priority-based FIFO scheduler
	Noise figure	0.5 dB
	Time ratio on cyclic prefix	0.03125 (1/32 guard interval)
	Transmission power	46 dB
	Link duplexing	TDD (time division duplexing)
	Frame duration	5 ms (0.005 s)
	Bandwidth	30 MHz
	Intermediate frequency	2414 MHz (2.4GHz)
	Maximum queue size	1024
	Maximum delay tolerance time	20 ms (0.02 s)
	Propagation model	FriisPropagationLossModel
	Routing protocol	OLSR or AODV
	Tx gain	-1 dB
	Rx gain	-10 dB
Jamming	Jammer type	reactive
	Jamming mode	spot noise
	Jamming power	10 dB
	Jamming interval	5 ms (0.005s)
	Battery capacity In jammer	100 W
	Anti-jamming type	channel hopping
	Threshold for anti-jamming	50 %
Man-in-the-middle	Type of man-in-the-middle	MAC spoofing
	Strength of man-in-the-middle	low, medium, high
	Speed of man-in-the-middle	15 Mbps (low), 20 Mbps (medium), 25 Mbps (high)
DDoS	Type of DDoS	mxed (UDP flooding & Teardrop)
	Strength of DDoS	low, medium, high
	Speed of DDoS by zombie bots	1 Mbps (low), 2 Mbps (medium), 3 Mbps (high)
	Flooding packet size	2 MB (low), 3 MB (medium), 4 MB (high)
	Number of zombie bots in botnet	10
Blackhole attack and wormhole attack	Type of blackhole attack	packet absorbing with routing poisoning
	Type of wormhole attack	collaborative packet absorbing with multiple nodes
	Strength of routing pollution	low, medium, high
	Speed of routing pollution	1 Mbps (low), 2 Mbps (medium), 3 Mbps (high)
	Number of blackhole nodes	1
	Number of wormhole nodes	2
	Number of hidden channels	1
Malware injection and infection	Type of malware attack	network worm propagarion and infection
	Strength of malware attack	low, medium, high
	Speed of malware attack	15 Mbps (low), 20 Mbps (medium), 25 Mbps (high)
	Vulnerability identification probability	10 % (low), 20 % (medium), 30% (high)
	Success probability	40 % (low), 60 % (medium), 80 % (high)
	Maximum propagation allowed	100 (low), 200 (medium), 500 (high)
	Worm payload size	1024 byte (low), 256 byte (medium), 64 byte (high)

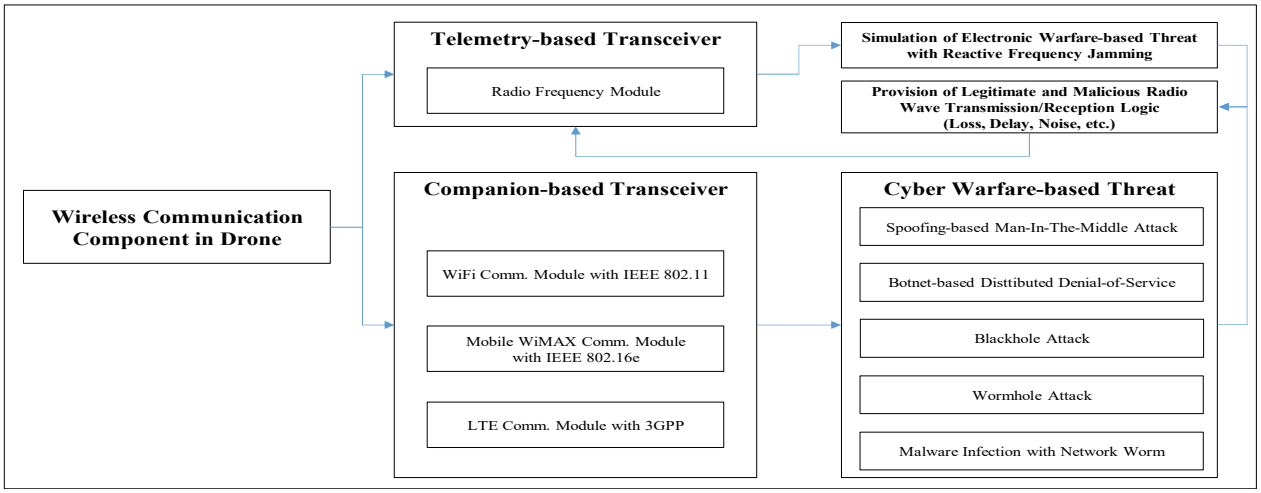


그림 9. 드론 무선위협 유형별 NS-3 기반 모의 블록도
Fig. 9. M&S-based Block diagram by drone wireless threat based on NS-3

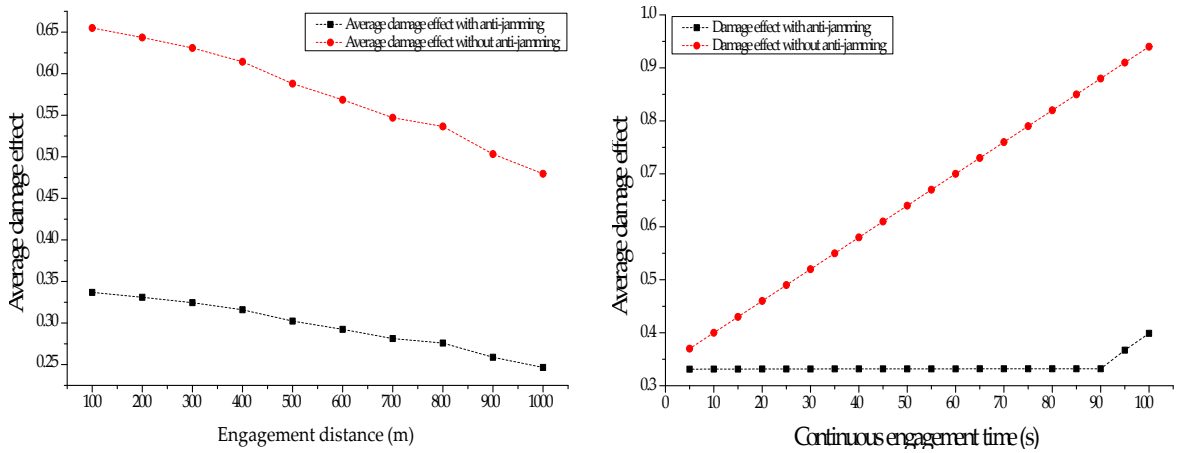
본 논문에서는 Mobile WiMAX 기반 통신 환경 내 표적 드론 개체에 대한 위협효과도를 교전 거리와 연속 파격 시간과 같은 주요 지표별로 비교한다. 그리고 통신 프로토콜 중에서, 유사한 무선통신 제원 정보를 포함하는 WiFi 및 WiMAX 간 전투피해 효과 비교 분석 또한 병행한다.

먼저 단일 Mobile WiMAX 표적 드론 개체를 대상으로 한 무선위협에 대한 위협효과도 비교 결과이다. 그림 10, 11과 같이 재밍의 경우, 위협 개체와 표적 개체 간 교전 거리가 증가함에 따라 재머가 방사하는 방해 전파의 신호세기가 감쇠되어, 항재밍의 적용 여부와 무관하게 해당 평균 위협효과도가 선형적으로 감소하는 방향을 보였다. 연속 피격 시간에 대해서는, 항재밍 기법이 적용되지 않은 경우에는 선형적 내부 재밍 상수에 따라 위협효과도가 증대되나, 항재밍이 적용된 경우에는 최소 보안 임계치 0.5(표적 개체가 자가 측정한 총 PDR이 50% 이하로 손실될 경우, 채널 홉핑 기반 대응방책을 수행함) 이하로 증감 추세가 지속 유지됨을 확인하였다. 더불어서 방해 전파가 표적 개체 수신 안테나로 전달되어야 하는 반응형 주파수 재머의 특성이 결과에 반영됨을 확인할 수 있다.

또한 재밍 행위에 의한 연속 피격 시간 및 교전 거리 간 상관관계에 따라서도, 교전 거리가 멀수록 연속 피격 시간에 따른 재밍 효과도의 경사도가 낮아짐을 확인할 수 있다. 즉 임의 100초 동안 연속 재밍당하는 표적 개체와 위협 개체 간 교전 거리가 각각 200, 1000m인 경우, 평균 최대 39% 차이 이상의 위협효과도를 나타냈다. 반면에 PDR 및 RSS 임계치를 통한 재밍 탐지 및 채널 홉핑으로서 능동대응하는 항재밍 환경에서는, 연속 피격 시간 90초 이전까지 교전 거리별로 위협효과도 증감 변동이 없다가, 최대치에 가깝게 누적 피격당한 95초 이후부터는 계단식으로 선형 증가한 후, 180초 이전까지 다시 증가 추세가 정체됨을 확인하였다.

다음으로 그림 12, 13과 같이 중간자 공격의 경우, 위협 개체와 표적 개체 간 교전 거리가 증가함에 따라 악성 전파 송달 거리도 증가하여, 수신신호세기 (RSSI) 감쇠로서 평균 위협효과도가 선형 감소함을 확인 가능하며, 연속 피격 시간에 따라서는 중간자 공격에 따른 평균 효과도가 선형 증대됨을 추가 확인할 수 있다. 반면에, 타 위협 유형들과 달리 공격 강도별로 상이하게 구분되는 각 위협효과도를 산출하지 않는데, 이는 스푸핑을 통해 침해하면, 타 위협들과 비교하여 공격 지속이 유리한 중간자 공격 특성이 반영된 것으로 분석될 수 있다.

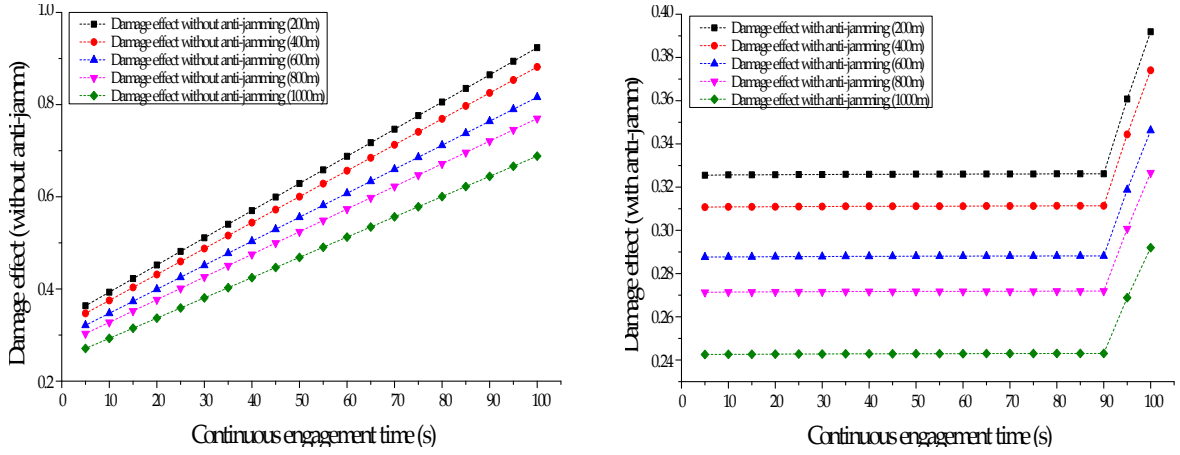
연속 피격 시간과 교전 거리의 상관관계 또한, 교전 거리가 멀수록 연속 피격 시간에 따른 중간자 공격의 피해효과가 하락함을 확인 가능하다. 즉 100초동안 중간자 공격을 연속 피격당한 표적 개체와 위협 개체 간 교전 거리가 각각 200m, 1000m인 경우, 평균 최대 28% 차이를 도출함을 보인다.



(a) (b)

그림 10. 드론 재밍 및 항재밍에 대한 교전 거리-연속 피격 시간별 평균 위협효과도 비교

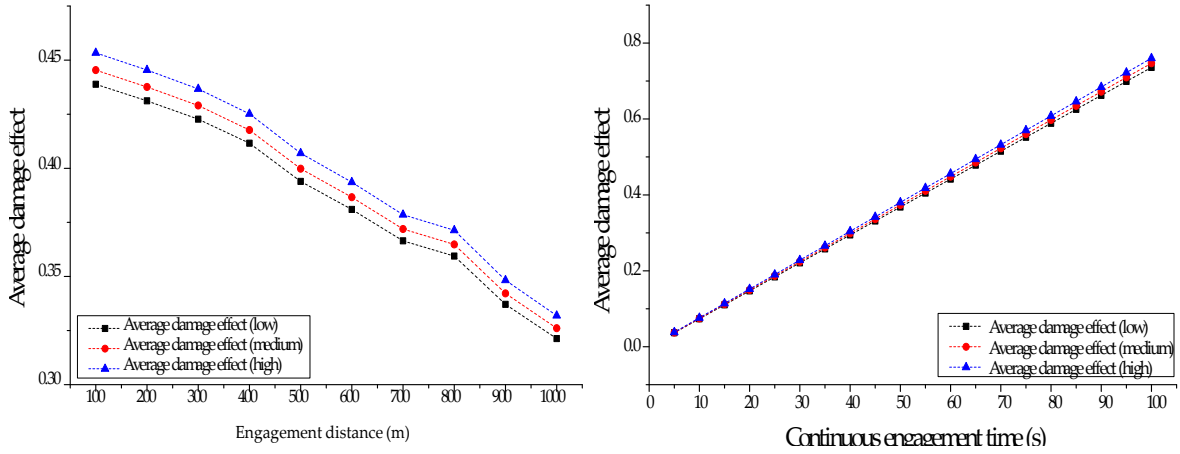
Fig. 10. Comparison of average damage effect by distance and continuous time for jamming and anti-jamming



(a) (b)

그림 11. 드론 재밍에 따른 교전 거리별 단일 위협효과도 비교

Fig. 11. Comparison of damage effect by distance against jamming



(a) (b)

그림 12. 드론 중간자 공격에 대한 교전 거리-연속 피격 시간 기반 공격 강도별 평균 위협효과도 비교

Fig. 12. Comparison of average damage effect by attack strength based on distance and continuous time for MITM

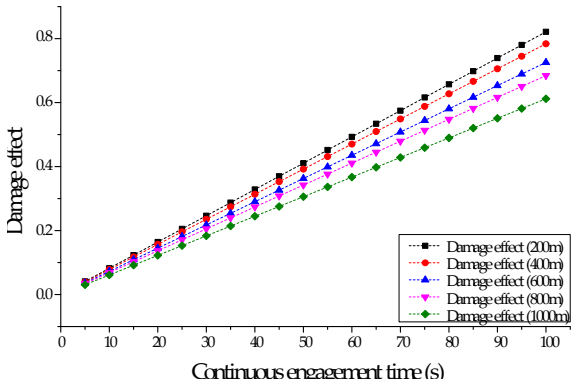
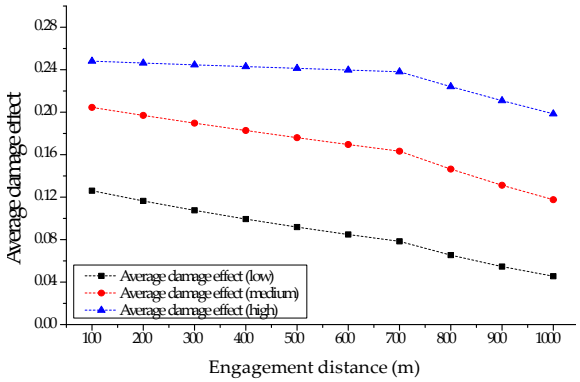


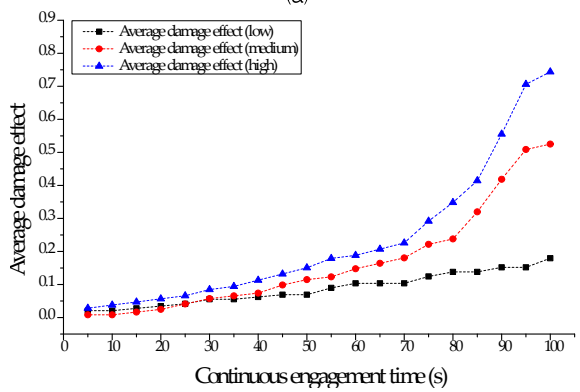
그림 13. 드론 중간자 공격에 대한 교전 거리별 단일 위협효과도 비교

Fig. 13. Comparison of damage effect by distance against MITM

단일 표적 위협 유형들 중에서 마지막으로 디도스 공격도, 그림 14, 15와 같이 위협 개체와 표적 개체 간 교전 거리가 점진적으로 증가할수록 관련 평균 위협효과도가 지속 감소되나, 공격 강도에 따라 각각 상이한 감소 추세를 보임을 확인할 수 있다.



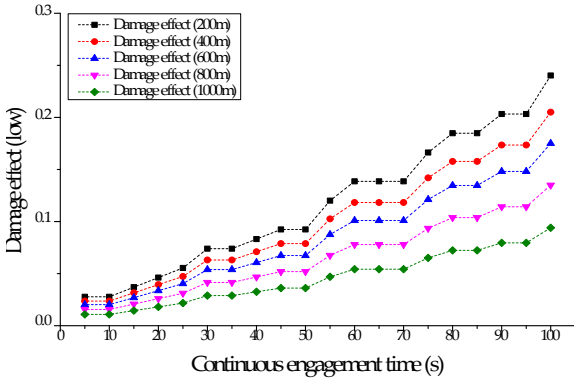
(a)



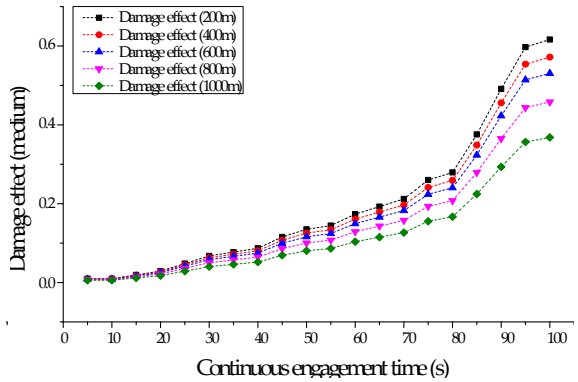
(b)

그림 14. 드론 디도스 공격에 대한 교전 거리-연속 피격 시간 기반 공격 강도별 평균 위협효과도 비교

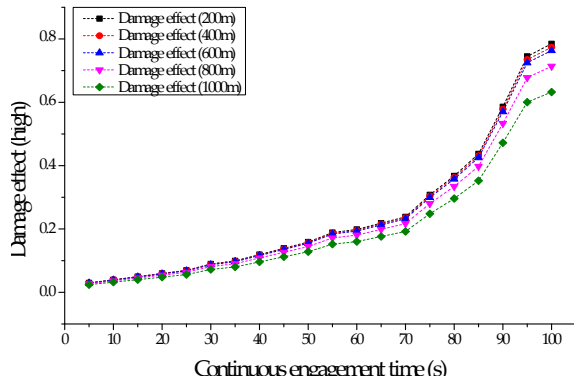
Fig. 14. Comparison of average damage effect by attack strength based on distance and continuous time for DDoS



(a)



(b)



(c)

그림 15. 드론 디도스 공격에 대한 교전 거리별 단일 위협효과도 비교

Fig. 15. Comparison of damage effect by distance against DDoS

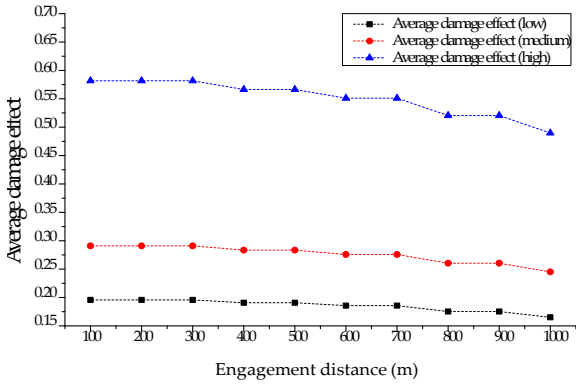
즉 저강도 디도스일 때는 선형적으로 감소하나, 고강도일 때는 700m 이전까지는 공격 성공률을 일정 수준 유지하는 차이점을 보임을 분석 가능하다. 더불어, 연속 피격 시간에 따라 평균 위협효과도이 모두 선형적으로 증가함과 함께, 공격 강도에 따라 경사도가 증가함을 확인할 수 있다. 즉 모두 75초 이전까지는 적은 양(Positive)의 경사도로 위협효과도가 증대되다가, 75초부터 고강도 및 중강도에서는 지수적 증가, 저강도에서는 동일한 선형적 증가로서

구분되는 것이다. 이는 곧 디도스가 다른 위협 대비, 표적 드론의 통신 가용성에 직접적 피해를 야기하므로, 서비스 거부 강도가 증대될수록 위협효과도 비례하여 증가하는 특성을 보이는 것으로 분석된다.

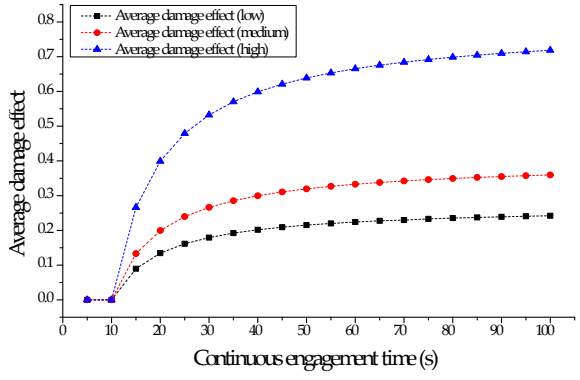
그리고 연속 피격 시간과 교전 거리의 상관관계는 교전 거리가 멀수록 연속 피격 시간에 따른 디도스 효과도가 하락함과 함께, 디도스 강도에 따라서도 분류 가능함을 보인다. 즉 저강도에서 100초 동안 연속 피격당하는 표적 개체와 위협 개체 간 교전 거리가 각각 200m, 1000m인 경우, 평균 최대 88% 차이 이상의 위협효과도를 산출하는 반면에, 중강도 및 고강도에서는 각각 평균 최대 42%, 24% 이상으로, 이전 대비 감소한 것을 확인하였다.

5.2 다중 표적 위협별 피해효과 민감도 분석

그림 16-21은 표적 드론 개체들이 소속된 Mobile WiMAX 애드혹 네트워크 전체를 대상으로 한 무선 위협에 대한 위협효과도 비교 결과이다.



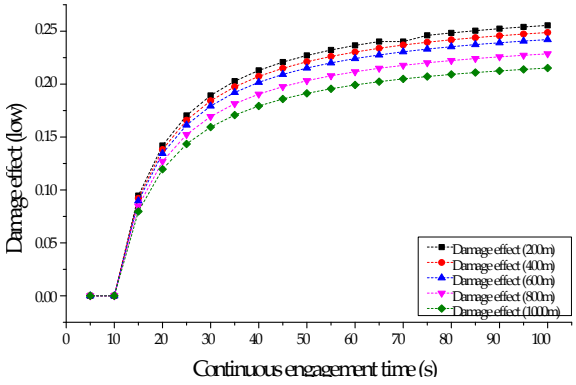
(a)



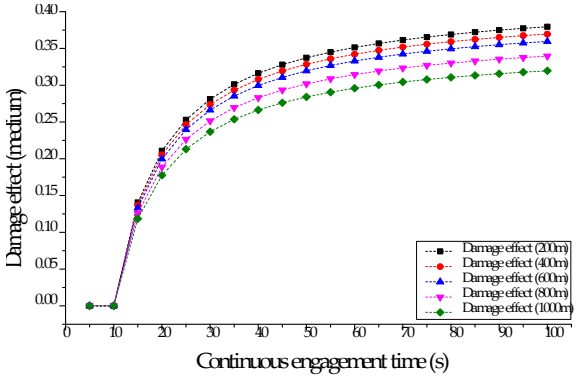
(b)

그림 16. 드론 블랙홀 오염 공격에 대한 교전 거리-연속 피격 시간 기반 공격 강도별 평균 위협효과도 비교

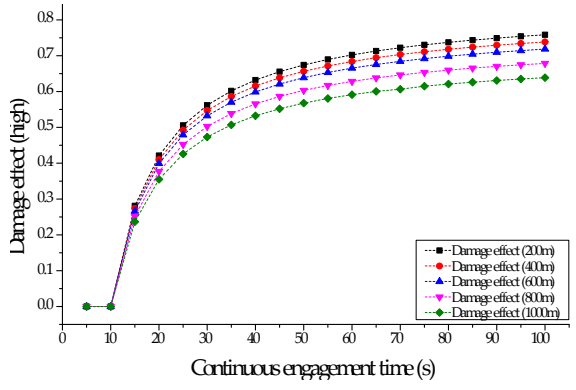
Fig. 16. Comparison of average damage effect by attack strength based on distance and continuous time for blackhole



(a)



(b)



(c)

그림 17. 드론 블랙홀 오염 공격에 대한 교전 거리별 단일 위협효과도 비교

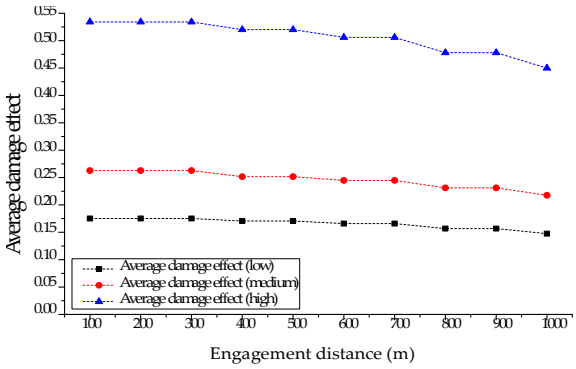
Fig. 17. Comparison of damage effect by distance against blackhole

먼저 그림 16, 17과 같이 블랙홀형 독립 라우팅 오염 공격의 경우, 위협 개체와 표적 개체 간 교전 거리에 따른 평균 위협효과도는 공격 강도에 따라 상이하게 감소되나, 강도별로 교전 거리 변화에 따라 큰 변화가 발생하지 않음을 확인할 수 있다. 그리고 연속 피격 시간에 따라서는 모두 로그 함수 형태로 평균 위협효과도가 증가함과 함께, 공격 강도에 따라 뚜렷하게 구분되는 경사도의 증가 추세를 확인할 수 있다.

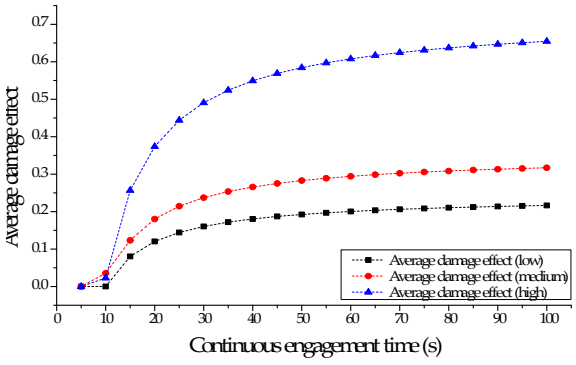
이는 블랙홀 공격이 애드혹 개체별로 독립 보유한 라우팅 테이블 내 최적 경로 정보들에 대해 모두 수정 완료한 후에는, 라우팅 경로에 대한 역정보화(Disinformation)와 함께 패킷 흡수를 수행하므로, 임의 표적 네트워크에 대한 악성 전파를 지속 방사할 필요가 없다는 사실에 근거한다. 즉 교전 거리가 증대되고 방사 시간이 감소되는 환경 조건에 대해서도 일정 수준의 전투피해효과 발현을 신속 보장 가능한 고유 특성이 반영된 것으로 분석될 수 있다.

연속 피격 시간과 교전 거리의 상관관계에 따라서도, 교전 거리가 멀수록 연속 피격 시간에 따른 블랙홀형 단일 라우팅 오염 공격의 효과도가 타 위협 유형 대비 소폭 하락함과 함께, 공격 강도 변화에도 이러한 효과도 증감 관계가 유사하게 지속됨을 확인할 수 있다. 즉 저강도에서 100초동안 블랙홀 공격을 연속 피격당하는 표적 개체와 위협 개체 간 교전 거리가 각각 200m, 1000m인 경우, 평균 최대 21% 차이 이상의 위협효과도를 산출함과 함께, 중강도 및 고강도에서도 거의 유사한 각각 평균 최대 19%, 18% 이상의 차이를 도출함을 확인하였다.

블랙홀 공격 개념에 은닉 통신 채널과 평판 공격 개념을 부가한 웜홀형 협업 라우팅 오염 공격의 경우에는, 그림 18, 19와 같이 교전 거리 변화에 따라 각 공격 강도별 평균 위협효과도의 증감 변화가 크게 발생하지 않음을 확인할 수 있다. 즉 저강도에서는 15~18%, 중강도에서는 22~27%, 고강도에서는 46~54% 구간에서 일정 유지됨을 보인다. 더불어, 연속 피격 시간에 따라서도, 공격 강도에 따라 뚜렷하게 구분되는 로그 함수 형태로 모두 증가함을 확인하였다. 그리고 연속 피격 시간과 교전 거리의 상관관계에 따라서도, 교전 거리가 멀수록 연속 피격 시간에 따른 웜홀형 복수 라우팅 오염 공격의 효과도가 소폭 하락함과 함께, 공격 강도 변화에도 이러한 효과도 관계가 블랙홀 공격 개념과 유사하게 유지됨을 보인다. 즉 저강도에서 100초 동안 웜홀 공격을 연속 피격당하는 표적 개체와 위협 개체 간 교전 거리가 각각 200m, 1000m인 경우, 평균 최대 30% 차이 이상의 위협효과도를 산출함과 함께, 중강도 및 고강도에서도 거의 유사하게 평균 최대 27%, 26% 이상의 차이를 도출함을 관측 가능하다.



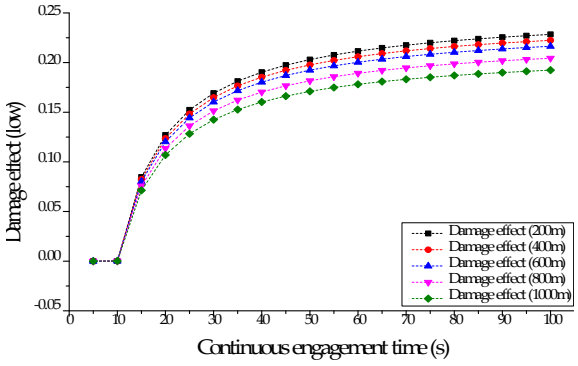
(a)



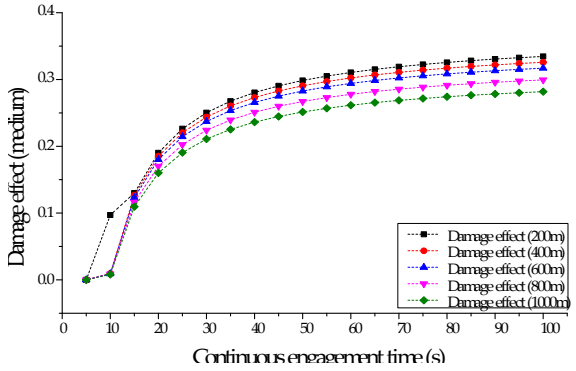
(b)

그림 18. 드론 웜홀 오염 공격에 대한 교전 거리-연속 피격 시간 기반 공격 강도별 평균 위협효과도 비교

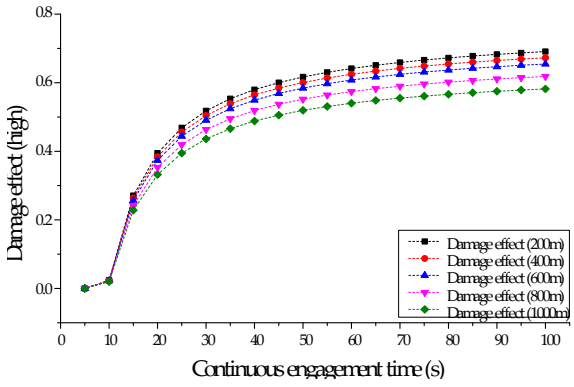
Fig. 18. Comparison of average damage effect by attack strength based on distance and continuous time for wormhole



(a)



(b)



(c)

그림 19. 드론 웜홀 오염 공격에 대한 교전 거리별 단일 위협효과도 비교

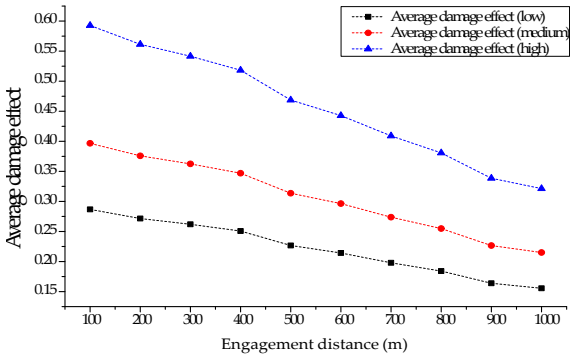
Fig. 19. Comparison of damage effect by distance against wormhole

다중 표적 위협 유형 중에서 마지막으로 네트워크 웜 기반 악성코드 장입 및 감염 공격의 경우에는, 그림 20, 21과 같이 위협 개체와 표적 개체 간 교전 거리에 따른 악성 풀 점유 기반 평균 위협효과도는 공격 강도에 따라 감쇠 분류됨과 함께, 교전 거리 변화에 따라서도 선형 감소함을 확인 가능하다. 또한 연속 피격 시간에 따른 평균 위협효과도가 모두 선형적 양의 형태로 증가됨을 관측할 수 있다.

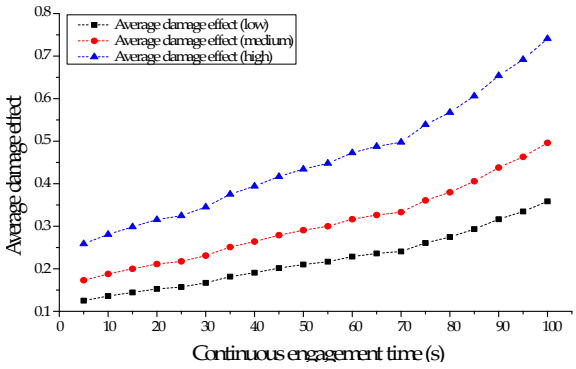
이는 웜 복제가, 무선 애드혹 망 내 표적 개체 간 상호 개설된 네트워크 소켓들을 겨냥한 확산 행위로서 독립 수행됨에 따라, 위협 개체의 별도 통제 없이도 침해된 이후부터는 해당 망 전체에 대한 통신 가용성 피해를 지속 강제 가능한 고유 특성을 보유한 것에 기인할 것이다. 더불어, 연속 피격 시간과 교전 거리의 상관관계에 따라, 교전 거리가 멀수록 연속 피격 시간에 따른 웜 기반 위협효과도가 선형 감소함과 함께, 공격 강도별 침해 성능 차이도 확인하였다.즉 저강도에서 100초 동안 악성코드 감염 공격을 연속 피격당하는 표적 개체와 위협 개체 간 교전 거리가 각각 200m, 1000m인 경우, 평균 최대 75% 차이 이상의 위협효과도를 산출하는 한편, 중강도에서도 저강도와 유사한 평균 최대 79% 차이, 고강도에서는 평균 최대 52% 차이를 도출함을 보인다.

5.3 통신 프로토콜별 피해효과 민감도 분석

마지막으로 그림 22, 23과 같이, WiFi 및 WiMAX 간 위협효과도 비교 분석을 수행한다.



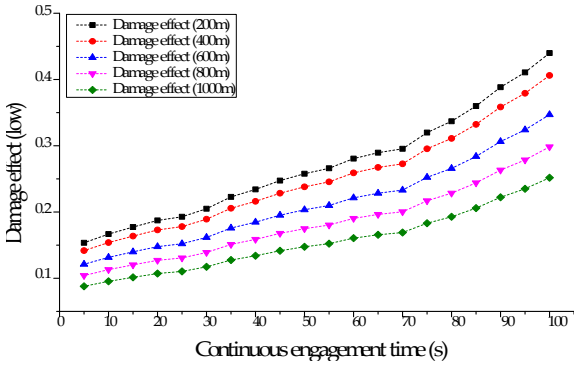
(a)



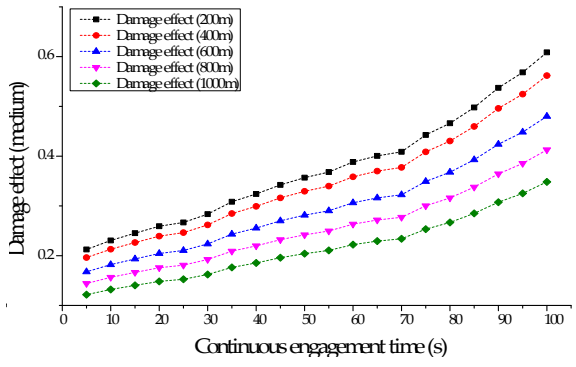
(b)

그림 20. 드론 악성코드 장입 및 감염 공격에 대한 교전 거리-연속 피격 시간 기반 공격 강도별 평균 위협효과도 비교

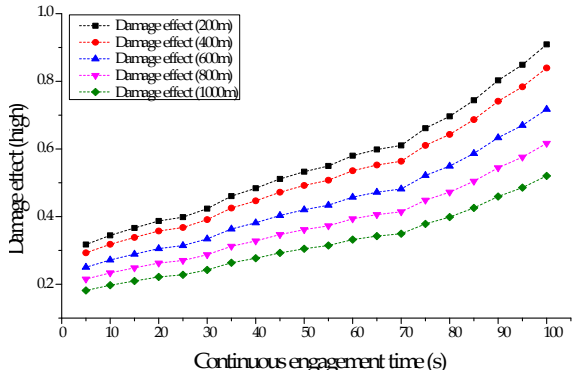
Fig. 20. Comparison of average damage effect by attack strength based on distance-continuous time for malware infection



(a)



(b)



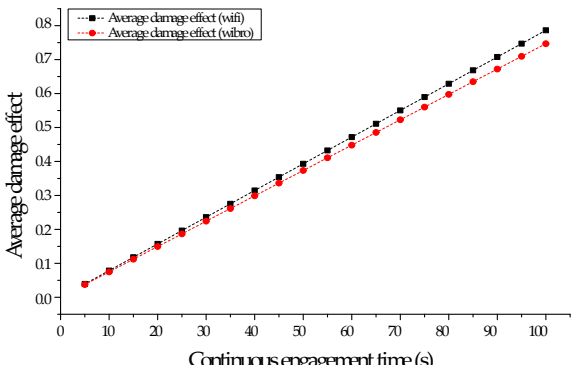
(c)

그림 21. 드론 악성코드 장입 및 감염 공격에 대한 교전 거리별 단일 위협효과도 비교

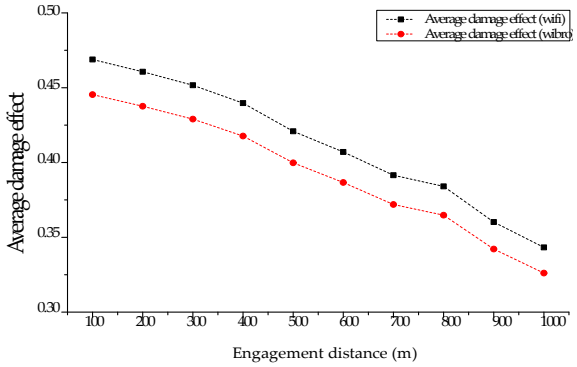
Fig. 21. Comparison of damage effect by distance against malware infection

먼저 중간자 공격에 대해서는 Mobile WiMAX보다 WiFi 통신 환경이 더 취약함을 확인할 수 있다. 즉 연속 피격에 따른 공격 지속에 대해서는 평균 6% 가량의 평균 위협효과도 차이를 도출함과 더불어, 피격 거리 기반으로도 16% 가량 높은 평균 위협효과도를 산출함에 따라 더 취약함을 보인다. 이는 IEEE 802.11 표준 기반 WiFi보다 IEEE 802.16e 표준 기반 Mobile WiMAX 내 연결 대기 큐와 QoS 링크, 로드 밸런싱 성능 처리 성능 등이 상대적으로 더 높다는 고유 특성 차이에서 비롯될 것이다.

다음으로, 악성코드 감염 공격에서도 Mobile WiMAX보다 WiFi 통신 환경이 더 취약함을 관측 가능하다. 즉 연속 피격에 따른 공격 지속에 대해서는 평균 20% 가량 더 높은 취약성을 도출하며, 피격 거리 기반으로도 43% 가량 더 취약함을 보인다. 이는 WiFi와 달리 Mobile WiMAX 내 기지국 개체의 업-다운링크 통신 채널 내 QoS 기반 서비스 플로우 처리 알고리즘이 별도 존재한다는 고유 특성 차이에서 비롯될 것이다.



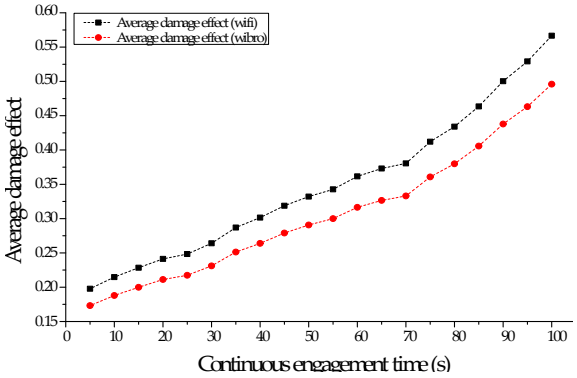
(a)



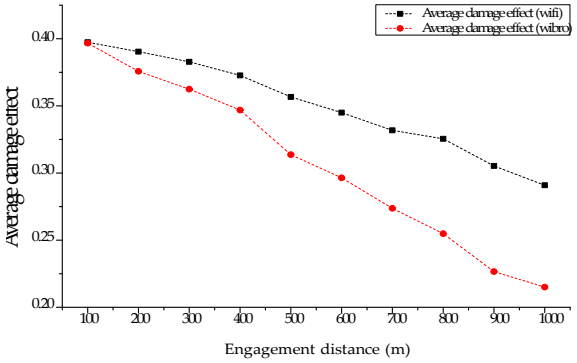
(b)

그림 22. WiFi-WiMAX 간 중간자 공격의 평균 위협효과도 비교

Fig. 22. Comparison of average damage effects against man-in-the-middle between WiFi-WiMAX



(a)



(b)

그림 23. WiFi-WiMAX 간 악성코드 감염 공격의 평균 위협효과도 비교

Fig. 23. Comparison of average damage effects against malware infection between WiFi-WiMAX

5.4 교전 메트릭에 따른 결과 요약

이러한 사이버-전자전 무선위협 M&S를 통해 다음과 같은 최종 정리가 가능하다.

먼저, 재밍 및 중간자 공격, 디도스 공격과 같은 단일 표적 대상 사이버-전자전 무선위협들에 대한 드론 교전피해의 경우, 교전 거리에 대해서는 선형 감소하고, 연속 피격 시간에 따라서는 선형 증가하는 상관관계를 최종 도출함을 확인할 수 있다.

다음으로 다중 표적 대상 무선위협들에 대한 드론 교전 피해 유형 중, 복수 노드별 평판 평가에 따른 애드혹 라우팅 행사가 결정되는 블랙홀형-웜홀형 라우팅 오염 공격의 경우, 교전 거리와는 무관하며 연속 피격 시간에 따라서는 로그 함수 형태로 증대됨을 확인할 수 있다. 반면에 웜 기반 악성코드 감염 공격의 경우에는 단일 표적 위협 유형들과 유사하게 교전 거리에 대해서는 선형 감소, 연속 피격 시간에 따라서는 선형 증대됨을 최종 도출한다.

Ⅵ. 고찰 및 결론

본 논문에서는 기존 선행 연구들의 한계성을 해결함과 더불어, 전문화된 무선위협별 전투피해 또한 분석하기 위해, NS-3 기반 드론형 사이버-전자전 교전 M&S 워게임 프레임워크를 최초 제안하였다.

이를 위해, 먼저 표준화된 STRIDE 위협 모델링을 활용하여 무선 드론에 대한 표적 취약성을 분석하여, 위협 논리를 정립하였다. 그리고 구성한 드론 취약성 및 위협 논리에 근거하여, 각각 통신 전자전과 사이버전과 관련된 드론 무선위협 알고리즘을 정형화하고, 소규모 군집드론 무선 애드혹 망을 겨냥한 진보된 침해 모의를 수행한 후, 산출된 위협효과도들을 주요 지표별로 비교하였다. 더불어 드론 페이로드부 내 통신 제원 정보 기반으로 독립 구현된 WiFi, Mobile WiMAX, LTE 환경별로 전용화된 민감도 분석 역시 병행하였다.

이를 통해, 표적 취약성 기반 사이버-전자전 위협에 대한 통신 표준별 고유한 위협효과도를 도출함을 보였으며, 침투 벡터 및 침입 경로 수에 따른 단일-다중 표적 대상 위협별 구분되는 전투피해효과 역시 추가 산출할 수 있었다. 더불어 결과에 따른 위협 징후 기반 탐지방안 및 관련 대응 방책 또한 개념적으로 검토하였다.

그러나 산출된 비교 분석 결과들 중에서 통신 전자전 기반 재밍을 제외한 나머지 사이버전 특화 위협 유형들의 경우에는, 항상 공격자가 우위에 있도록 사이버-전자전 교전을 한정 모의하였다.

더불어 위협 파급에 따른 대응방책 논리 구성과 함께, 이동 변이(MTD, Moving Target Defense) 기반 사전예방적 회피체계나 디코이(Decoy) 기반 사후대응적 무인격리시스템과 같이, 유무인협업체계에 전용화된 능동대응 논리 적용 또한, 피해효과도 감쇠 모의 측면에서 추가 고려되어야 할 것이다.

향후에는 무선위협에 따른 차단 및 탐지, 대응, 회피 기반 방호 요소들을, 제안된 M&S 프레임워크를 기반으로 추가 구현하여 최종 모의할 예정이며, 이를 통해 드론 기반 유무인협업체계에 대한 사이버-전자전 워게임 S/W를 더욱 발전시킬 계획이다.

References

[1] Cheon Jung Hee, et al., "Toward a secure drone system: Flying with real-time homomorphic authenticated encryption", IEEE Access, Vol. 6, pp. 24325-24339, Mar. 2018. https://doi.org/10.1109/ACCESS.2018.2819189.

[2] Army Modernization Strategy, https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf. [Accessed: Nov. 10, 2022]

[3] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, "A communications jamming taxonomy", IEEE Security & Privacy, Vol. 14, No. 1, pp. 47-54, Jan. 2016. https://doi.org/10.1109/MSP. 2016.13.

[4] N. Yasar, F. M. Yasar, and Y. Topcu, "Operational advantages of using cyber electronic warfare(CEW) in the battlefield", Proc. of the SPIE, Vol. 8408, No. 84080G, May 2012. https://ui.adsabs.harvard.edu/link_gateway/2012SPIE.8408E..0GY/doi:10.1117/12.919454.

[5] O. Askin, R. Irmak, and M. Avsever. "Cyber warfare and electronic warfare integration in the operational environment of the future: Cyber electronic warfare", Proc. of the SPIE, Vol. 9458, No. 94580H, May 2015. https://doi.org/10.1117/12.2189351.

[6] IEEE Standard for Local and Metropolitan Area Networks, https://ptolemy.berkeley.edu/projects/ofdm/ergen/docs/80216e.pdf. [Accessed: Nov. 10, 2022]

[7] ETSI. LTE., https://www.etsi.org/technologies/mobile/4G. [Accessed: Nov. 10, 2022]

[8] IEEE 802.11 Wireless Local Area Networks, The Working Group for WLAN Standards, https://www.ieee802.org/11. [Accessed: Nov. 10, 2022]

[9] Mireles Jose David, et al., "Metrics towards measuring cyber agility", IEEE Transactions on Information Forensics and Security, Vol. 14, No. 12, pp. 3217-3232, Dec. 2019. https://doi.org/10.1109/TIFS.2019.2912551.

[10] Linkov Igor and Alexander Kott, "Fundamental concepts of cyber resilience: Introduction and overview", Cyber resilience of systems and networks, pp. 1-25. May 2018. https://doi.org/10.1007/978-3-319-77492-3_1.

[11] Deborah J. Bodeau, Catherine D. McCollum, and David B. Fox, "Cyber threat modeling: Survey, assessment, and representative framework", MITRE Corp, Apr. 2018. [Accessed: Nov. 10, 2022]

[12] NS-3 network simulator. https://www.nsnam.org. [Accessed: Nov. 10, 2022]

[13] Al-Shurman Mohammad, Seong-Moo Yoo, and Seungjin Park, "Black hole attack in mobile ad hoc networks", Proc. of the 42nd annual Southeast regional conference, pp. 96-97, Apr. 2004. http://dx.doi.org/10.1145/986537.986560.

[14] Hu Yih-Chun, Adrian Perrig, and David B. Johnson, "Wormhole attacks in wireless networks", IEEE journal on selected areas in communications, Vol. 24, No. 2, pp. 370-380, 2006. https://doi.org/10.1109/JSAC.2005.861394.

[15] Misra Jayadev, "Distributed discrete-event simulation", ACM Computing Surveys(CSUR), Vol. 18, No. 1, pp. 39-65, Mar. 1986. https://doi.org/10.1145/6462.6485.

[16] Jones M. A. and J. Diaz de Leon, "Multi-domain operations", The Three Swords Magazine 36, pp. 38-41, 2020. [Accessed: Nov. 10, 2022]

[17] U.S Army, FM 3-38 Cyber Electromagnetic Activities, https://irp.fas.org/doddir/army/fm3-38.pdf. [Accessed: Nov. 10, 2022]

[18] Left of Launch: Countering Theater Ballistic Missiles. https://www.atlanticcouncil.org/wp-content/uploads/2017/07/Left_of_Launch_web_0731.pdf. [Accessed: Nov. 10, 2022]

[19] Night Stand, NSA. https://nsa.gov1.info/dni/nsa-ant-catalog/wireless-lan/index.html. [Accessed: Nov. 10, 2022]

[20] FoI. Russian Electronic Warfare, https://www.defence.lk/upload/ebooks/Russian%20Electronic%20Warfare.pdf. [Accessed: Nov. 10, 2022]

[21] Heartfield Ryan, and George Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks", ACM Computing Surveys(CSUR), Vol. 48, No. 3, pp. 1-39, Dec. 2015. https://doi.org/10.1145/2835375.

[22] Estonian Ministry of Defence, Russian;s Electronic Warfare Capabilities to 2025, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf. [Accessed: Nov. 10, 2022]

[23] Woocheol Kim, Soyeon Kim, and Hyuk Lim, "Malicious data frame injection attack without seizing association in IEEE 802.11 wireless LANs", IEEE Access, Vol. 9, pp. 16649-16660, Jan. 2021. https://doi.org/10.1109/ACCESS.2021.3054130.

[24] P. Hayward, "The Measurement of Combat Effectiveness", Operations research, Vol. 16, No. 2, pp. 314-323, Apr. 1968. https://doi.org/10.1287/opre.16.2.314.

[25] Cil I. and Mala M., "A multi-agent architecture for modelling and simulation of small military unit combat in asymmetric warfare", Expert Systems Appl., Vol. 37, No. 2, pp. 1331-1343, Mar. 2010. https://doi.org/10.1016/j.eswa.2009.06.024.

[26] K. M. Seo, C. Choi, T. G. Kim, and J. H. Kim,

"DEVS-based combat modeling for engagement-level simulation", Simul. Trans. Soc. Model. Simul. Int., Vol. 90, No. 7, pp. 759-781, Jun. 2014. https://doi.org/10.1177/0037549714532960.

[27] Connors C. D., Miller J. O., Lunday B. J., "Using agent-based modeling and a designed experiment to simulate and analyze a new air-to-air missile", J. Def. Model. Simul., Vol. 13, No. 3, pp. 321–330, Nov. 2015. https://doi.org/10.1177/1548512915616873.

[28] Thompson B. and Morris-King J., "An agent-based modeling framework for cybersecurity in mobile tactical networks", J. Def. Model. Simul., Vol. 15, No. 2, pp. 205-218, Nov. 2017. https://doi.org/10.1177/1548512917738858.

[29] Shin K., Nam H., and Lee T., "Communication Modeling for a Combat Simulation in a Network Centric Warfare Environment", In Proc. of the 2013 Winter Simulations Conference(WSC), Washington, DC, USA, pp. 1503-1514, Dec. 2013. https://doi.org/10.1109/WSC.2013.6721534.

[30] Li Y., Baccelli F., Dhillon H. S., and Andrews J. G. "Statistical Modeling and Probabilistic Analysis of Cellular Networks with Determinantal Point Processes", IEEE Trans. Commun, Vol. 63, No. 9, pp. 3405-3422, Jul. 2015. https://doi.org/10.1109/TCOMM.2015.2456016.

[31] Akhtar N., Ergen S. C., and Ozkasap O., "Vehicle mobility and communication channel models for realistic and efficient highway VANET simulation", IEEE Trans. Veh. Technol., Vol. 64, No. 1, pp. 248–262, Apr. 2014. https://doi.org/10.1109/TVT.2014.2319107.

[32] Regragui Y. and Moussa N., "Agent-based system simulation of wireless battlefield networks", Comput. Electr. Eng., Vol. 56, pp. 313-333, Nov. 2016. https://doi.org/10.1016/j.compeleceng.2016.07.007.

[33] Lee J., Shin S., Park M., and Kim C., "Agent-based simulation and its application to analyze combat effectiveness in network-centric warfare considering communication failure environments", Math. Probl. Eng., Dec. 2018. https://doi.org/10.1155/2018/2730671.

[34] Seo S., Han S., and Kim D., "D-CEWS: DEVS-Based Cyber-Electronic Warfare M&S Framework for Enhanced Communication Effectiveness Analysis in Battlefield", Sensors, Vol. 22, No. 9, pp. 3147, Apr. 2022. https://doi.org/10.3390/s22093147.

[35] Bora Ly and Romny Ly, "Cybersecurity in unmanned aerial vehicles(UAVs)", Journal of Cyber Security Technology, Vol. 5, No. 2, pp. 120-137, Nov. 2020. https://doi.org/10.1080/23742917.2020.1846307.

[36] Jacobsen Rune Hylsberg and Ali Marandi, "Security Threats Analysis of the Unmanned Aerial Vehicle System", MILCOM 2021-2021 IEEE Military Communications Conference, San Diego, CA, USA, Dec. 2021. https://doi.org/10.1109/MILCOM52596.2021.9652900.

저자소개

서 상 (Sang Seo)

2020년 2월 : 경기대학교 AI컴퓨터공학부(공학학사)
2022년 2월 : 경기대학교 AI컴퓨터공학부(공학석사)
2022년 3월 ~ 현재 : 경기대학교 AI컴퓨터공학부 소속 연구원

관심분야 : Cyber deception, M&S, military security, moving target defense, decoy

김 도 훈 (Dohoon Kim)

2005년 2월 : 고려대학교 수학/컴퓨터과학과(이학학사, 이중전공)
2007년 8월 : 고려대학교 컴퓨터과학과(이학석사)
2012년 2월 : 고려대학교 컴퓨터·전파통신학과(공학박사)
2018년 2월 : 국방과학연구소 선임연구원(사이버방호&정보보호)
2018년 3월 ~ 현재 : 경기대학교 AI컴퓨터공학부 교수
관심분야 : Network security, botnet, risk assessment

한 상 우 (Sangwoo Han)

2003년 2월 : 중앙대학교 컴퓨터공학부 (공학사)
2005년 2월 : 광주과학기술원 정보통신공학부 (공학석사)
2012년 2월 : 광주과학기술원 정보통신공학부 (공학박사)
2012년 ~ 현재 : 국방과학연구소 선임연구원
관심분야 : Defense modeling & simulation, combat effectiveness analysis