위성체 내부 시스템 Taxonomy 구축 및 이상 징후 탐지를 위한 서브시스템 부호 식별 체계

정해린*, 김혜정*, 김은서*, 조승현*, 박기웅†
*세종대학교 정보보호학과 학부생
† 세종대학교 정보보호학과 교수
22011754@sju.ac.kr, 22011770@sju.ac.kr, 22011767@sju.ac.kr, 3145jiug@sju.ac.kr,
woongbak@sejong.ac.kr

Development of an Internal Satellite System Taxonomy and Subsystem Identification Codes for Anomaly Detection

Hae-Lynn Jung*, Hye-Jeong Kim*, Eun-Seo Kim*, Seung-Hyeon Jo*,
Ki-Woong Park†
*Dept. of Computer Information Security, Sejong University
† Dept. of Computer Information Security, Sejong University

요 약

우주 산업의 비약적 성장으로 위성 시스템의 활용 범위가 확대되고 있다. 그러나 보안 분석의 중요성에 비해 내부 데이터 구조를 체계적으로 분석한 연구는 미진한 실정이다. 본 논문에서는 위성체 보안 위협 식별을 위해 서브시스템별 특성을 정의하고, 잠재적 취약성을 제시한다. 또한, 데이터 간 상관관계를 활용하여 비정상 행위 탐지를 위한 기반을 마련하고, 데이터 중심의 분석 관점을 제안한다.

1. 서론

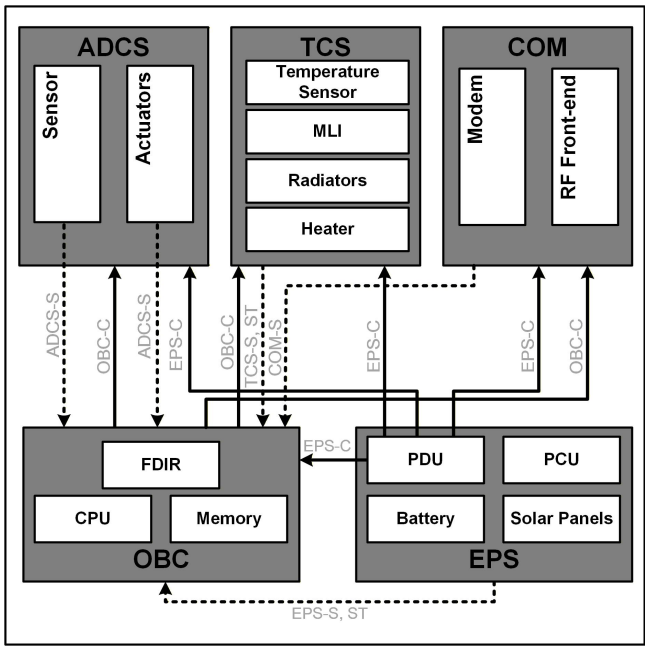
위성 시스템은 통신, 정찰, 기상 관측 등 임무 수행을 위한 핵심 인프라로 활용되고 있다. 그러나 이러한 발전과 더불어 보안 위협 가능성이 확대되고 있다. 이에 따라 위성 보안을 위한 탐지 및 대응 기법이 제안되고 있으나, 관련 연구는 초기 수행 단계에 머물러 있어, 위성 내부 가용 데이터의 종류와 구조를 체계화한 선행 연구는 부족한 실정이다[1]. 위성은 OBC, COM, ADCS, EPS, TCS 등 임무별 서브시스템으로 구성되어 있으며, 각 서브시스템은 서로 다른 특성의 물리적·논리적 데이터를 생성한다. 본 논문에서는 이러한 데이터를 유형별로 분류하고, 서브시스템 간 데이터 관계를 기반으로 이상 징후를 해석할 수 있는 분석 관점을 제시하며, 이를 바탕으로 위성체 내부 이상 탐지를 위한 데이터 중심의 구조를 마련하고자 한다.

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 연구는 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 정보보호핵심원천기술개발(Project No. RS-2026-25519773, 30%; RS-2024-00438551, 10%), 실감콘텐츠핵심기술개발(Project No. RS-2023-00228996, 20%), 대학ICT연구센터(ITRC) (Project No. ,10% IITP-2026-RS-2021-II211816, 10%), 한국연구재단(NRF) 핵심연구사업 (Project No. RS-2026-25481431 30%)의 지원을 받아 수행된 연구임.

2. 위성체 주요 서브시스템 기능 및 보안 취약점

본 장에서는 위성체 내 주요 서브시스템의 역할과 보안 취약점을 분석한다. [그림 1]은 위성체를 구성하는 핵심 서브시스템 간의 상호 연결 관계 및 구성 요소를 도식화한 것이다. 시스템 제어를 담당하는 OBC를 중심으로 각 서브시스템이 데이터와 명령을 교환하는 구조를 보여준다.



[그림 1] 위성체 주요 서브시스템 상호 연결 구조도

- OBC (On-Board Computer)

위성의 중앙 제어 장치인 OBC는 지상국 명령, 각 모듈의 상태 모니터링 및 데이터 패킹 등 시스템 전반의 실시간 운영을 담당한다. 우주 환경에 따른 하드웨어 제약으로 Stack Canary나 ASLR (Address Space Layout Randomization)과 같은 보안 기법 적용이 미비하며, 상용 부품에 내재된 기지 취약점을 기반으로 한 메모리 오염 및 원격 코드 실행 공격에 취약하다.

- COM (Communication System)

COM은 지상국과 위성 간 RF (Radio Frequency) 링크를 통해 데이터 패킷의 송수신을 전담하는 통신 서브시스템이다. 공개된 주파수 대역과 광범위한 신호 도달 범위로 인해 물리적 도청 및 신호 간섭에 취약하다. 특히 암호화 및 메시지 인증이 누락되어 있는 구형 우주 통신 프로토콜을 사용할 경우 패킷 스니핑이 가능하며, 이를 기반으로 정상 명령을 재사용하는 재전송 공격을 통해 시스템의 오작동을 유발하거나 내부 정보 유출로 이어질 수 있다[2].

- ADCS (Attitude and Orbit Control System)

ADCS는 자이로스코프 및 Star Tracker 등의 정밀 센서를 통해 위성의 자세와 궤도를 측정하고, 반동 휠(Reaction Wheel)을 구동하여 임무 목적에 부합하는 목표 자세를 유지하는 서브시스템이다. 센서 데이터에 대한 무결성 검증 체계가 미흡할 경우, 제어 알고리즘의 결정론적 특성을 악용한 센서 스푸핑 공격이 가능하다. 이러한 공격은 위성의 지향성 상실 혹은 자세 제어 권한 탈취를 초래한다[3].

- EPS (Electrical Power System)

EPS는 태양 전지판(SA, Solar Array)을 통한 전력 생성, 배터리 관리, 그리고 전력 분배를 담당하는 에너지 관리 서브시스템이다. 전력 소모 패턴은 내부 동작 상태를 반영하는 사이드 채널 정보를 포함하며, 이를 통해 시스템 상태 추론이 가능하다. 또한 소프트웨어 기반 과부하 보호 로직이 변조될 경우 비정상적인 전력 소모가 유도되며, 이는 배터리의 조기 고갈 및 시스템 가용성 저하로 이어진다.

- TCS (Thermal Control System)

TCS는 Heater와 라디에이터를 제어하여 OBC와 배터리 등 주요 구성 요소의 온도를 적정 범위 내로 유지하는 열 제어 서브시스템이다. 온도 제어 로직이 OBC에 통합되어 있고, 일부 하드웨어 보호 메커니즘이 소프트웨어 설정에 의존한다. 이러한 구조는 소프트웨어적 간섭을 가능하게 하며, 결과적으로 특정 부품의 과열 또는 동결을 유도하는 Thermal Sabotage 공격으로 이어질 수 있다.

3. 데이터 분류 및 연계 분석

본 장에서는 각 서브시스템에서 수집 가능한 지표를 식별하고, 이를 기반으로 탐지할 수 있는 위협을 기술한다. <표 1>은 위성체 내에서 수집 가능한 지표를 서브시스템별로 분류한 것이다.

<표 1>에 나열된 데이터들은 위성의 상태를 판단하는 기준이 되며, 각 지표 간의 상관관계를 통해 다음과 같은 보안 위협을 조기에 탐지할 수 있다. 서브시스템의 단독 지표 분석을 통해 식별 가능한 대표적인 보안 위협은 다음과 같다. OBC의 경우, 확인된 프로세스 목록에 알 수 없는 CMD$_{OBC\text{-}C\text{-}PROC}$가 실행 중이거나 설정 파일의 해시값$_{OBC\text{-}P\text{-}HASH}$이 예고 없이 변경된 경우, 비인가 코드 실행을 의심할 수 있다. 또한, 특정 프로세스가 CPU나 Memory를 과도하게 점유하여 임무의 실시간성을 저해하는 경우 가용성 침해로 판단할 수 있다. ADCS의 경우, Star Tracker가 보고하는 자세 데이터$_{ADCS\text{-}S\text{-}START}$와 실제 구동기의 토크 명령$_{ADCS\text{-}C\text{-}TPQ}$이 물리적으로 일치하지 않는 경우, 센서 데이터 변조를 의심할 수 있다. 예를 들어, ADCS의 운용 모드$_{ADCS\text{-}ST\text{-}MODE}$가 Detumbling가 아님에도 구동기가 비정상적인 회전수를 기록하는 경우, 제어권이 탈취되었을 가능성이 높다.

다중 서브시스템 간 데이터 상관관계를 통해 식별 가능한 대표적인 보안 위협은 다음과 같다. EPS의 태양전지판 발전 전압 변화 패턴$_{EPS\text{-}S\text{-}SA}$과 TCS의 면별 온도 구배 데이터$_{TCS\text{-}P\text{-}GRAD}$ 비교 분석 시, 환경 데이터를 기반으로 한 간접적인 궤도 정보 유출로 인한 기밀성 침해를 탐지할 수 있다. 공격자가 직접적인 위치 데이터에 대한 권한을 획득하지 못했더라도, 위성이 지구 그림자에 진입하는 Eclipse 시점의 전압 급락이나 각 면의 열역학적 변화 패턴을 역공학하면 위성의 실시간 위치 및 전략적 궤도 정보를 충분히 유추해낼 수 있기 때문이다. EPS의 태양전지판 발전 전압 데이터$_{EPS\text{-}S\text{-}SA}$와 COM의 패킷 송신량$_{COM\text{-}P\text{-}PKT}$ 및 TCS의 히터 가동 상태$_{TCS\text{-}ST\text{-}HTR}$ 연계 분석 시, 전력 고갈을 유도하는 가용성 침해를 탐지할 수 있다. 위성이 Eclipse 시점에 진입하여 전력 생산이 차단된 상태임에도 불구하고 OBC의 프로세스 목록상 정상 임무로 위장된 고전력 컴포넌트(통신 서브시스템, Heater 등)가 비정상적으로 가동된다면, EPS의 배터리 전압이 급격히 강하하기 때문이다. ADCS의 자세 데이터$_{ADCS\text{-}P\text{-}ATT}$와 EPS의 발전 효율$_{EPS\text{-}P\text{-}EFF}$ 및 COM의 수신 신호 강도$_{COM\text{-}S\text{-}RSSI}$ 연계 분석 시, 물리량 모순을 활용한 로직 기만에 따른 무결성 훼손을 탐지할 수 있다.

구분	센서/원시 데이터 (S, Sensor/Raw)	상태 데이터 (ST, Status)	처리/계산 데이터 (P, Process/Calc.)	제어/명령 데이터 (C, Control/CMD)
OBC	CPU 온도 OBC-S-TEMP	Process ID OBC-ST-PID	Throughput (Data/sec) OBC-P-TPUT	S/W Bus 메시지 OBC-C-BUS
	Clock Tick OBC-S-TICK	활성 소켓 수 OBC-ST-SOCK	File Hash OBC-P-HASH	Process CMD OBC-C-PROC
	-	로드된 커널 서브시스템 OBC-ST-KERN	Resource Utils (CPU/Mem/Swap) OBC-P-UTTL	-
		Uptime OBC-ST-UPTM	-	
EPS	Battery V/T EPS-S-BATT	SoC (State of Charge) EPS-ST-SOC	전력 소비 통계 EPS-P-STAT	Load Shedding 규칙 EPS-C-SHED
	SA V/I/Temp EPS-S-SA	전압 변동률 EPS-ST-VVAR	전력 효율치 EPS-P-EFF	스위치 제어 명령 EPS-C-SW
	Bus V/I EPS-S-BUS	-	Battery 수명 예측 EPS-P-BATTL	전력 분배 설정 EPS-C-PDU
ADCS	IMU(3-axis Rate) ADCS-S-IMU	운용 모드 ADCS-ST-MODE	Attitude Sol. ADCS-P-ATT	구동기 토크 명령 ADCS-C-TPQ
	MAG Vector ADCS-S-MAG	지향 정확도/Jitter ADCS-ST-ACCU	B-bot Data ADCS-P-BBOT	휠 회전 속도 명령 ADCS-C-RW
	Sun Vector(태양광 입사각) ADCS-S-SUNV	Momentum 포화도 ADCS-ST-MOM	위성체 위치/속도/시각 ADCS-P-PVT	자기 토커 전류 인가량 ADCS-C-MTQ
	Star Tracker Data ADCS-S-START			추력기 밸브 개폐 시간 ADCS-C-VLV
	GPS ADCS-S-GPS	-	-	-
TCS	면별 온도 TCS-S-FTEMP	온도 안정성/균일성 TCS-ST-STAB	온도 구배(Temp Gradient) TCS-P-GRAD	Threshold Settings TCS-C-THRES
	열 유속 TCS-S-FLUX	Heater/Radiator On/Off TCS-ST-HTR	열 저장량/전달량 TCS-P-STOR	냉각 루프 제어 명령 TCS-C-COOL
	유체 압력/유량 TCS-S-FLUID	Event log TCS-ST-EvLOG	센서 Calibration TCS-P-CAL	Heater 제어 규칙 TCS-C-HRULE
COM	CMC SMPS V/I COM-S-PWR	Beacon 활성화 여부 COM-ST-BCN	통신 모드 상태 COM-P-MODEC	통신 모드 전환 명령 COM-C-MODE
	RF Front-end 장치별 온도 COM-S-HWTEMP	Error Count(CRC/Overrun) COM-ST-ERR	송수신 및 드롭 패킷 수 COM-P-PKT	Beacon On/Off COM-C-BCN
	RSSI COM-S-RSSI	인증 실패 횟수 COM-ST-AUTHF	HMAC 인증 결과 COM-P-HMAC	HMAC 재동기화 명령 COM-C-RSYNC
	-	시퀀스 동기화 상태 COM-ST-SYNC	-	프레임 인증 규칙 COM-C-FAUTH

<표 1> 위성체 주요 서브시스템 데이터의 유형별 분류

공격자가 ADCS 제어 로직을 변조하여 정상 자세를 지시하더라도, 실제 위성이 회전하여 지향각이 틀어진다면 물리적 인과관계에 따라 필연적으로 태양광 발전 효율이 저하되고 통신 신호가 감쇄하기 때문이다[4].

4. 결론 및 향후 연구

본 논문에서는 위성체 서브시스템 데이터를 유형별로 분류하고, 데이터 간 상관관계를 고려한 이상 징후 분석 관점을 제시하였다. 수집 데이터를 센서/원시 데이터, 상태 데이터, 처리/계산 데이터, 제어/명령 데이터로 부호화하여 식별 체계를 구축함으로써, 통합적인 해석이 가능함을 확인하였다. 향후 연구에서는 위성체 내부 이상 징후 감지 시스템을 설계하여 수집된 데이터들의 상관관계를 활용하고자 한다. 본 연구에서 제안한 분류 체계는 향후 수집 매트릭스 구성을 통한 데이터 수집 경로 최적화 및 효율적인 이상 탐지 시스템 설계에 기여할 것으로 기대된다.

참고문헌

[1] James Pavur, Ivan Martinovic, “Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight”, Journal of Cybersecurity, 8, 1, 1-18, 2022.

[2] James Pavur, et al., “A tale of sea and sky on the security of maritime VSAT communications”, *2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA,* 2020, pp. 1384-1400.

[3] Benjamin Cyr, et al., “Position Paper: Space System Threat Models Must Account for Satellite Sensor Spoofing”, *SpaceSec 2023, San Diego, CA,* 2023.

[4] National Aeronautics and Space Administration (NASA), *Space Security Best Practices Guide (Version 1.0)*, Washington, D.C., NASA Office of the Chief Engineer, 2023.