SDN 기반 저궤도 위성-IoT 통신 시스템을 위한 위협 모델링 및 보안 분석

박준범, 이유경, 박현수, 이지연, 황동운, 송경영*, 장민호*, 장지웅*. 박종서

한국항공대학교, *울산과학대학교

parkjb@kau.ac.kr, nunomi0@kau.ac.kr, hyeonsu0328@kau.ac.kr, jiyeon23001@kau.ac.kr, bewise2015@kau.kr

kysong@uc.ac.kr, mhjang@uc.ac.kr, jwjang@uc.ac.kr, jspark@kau.ac.kr

Threat modeling and security analysis for SDN-based low earth orbit satellite-IoT communication system

JunBeom Park, Yukyung Lee, Hyunsu Park, Jiyeon Lee, Dongwun Hwang,

KyoungYoung Song*, Minho Jang*, Jiwoong jang*, Jongsou Park

Korea Aerospace University, *Ulsan college

요 약

최근 저궤도 위성과 IoT 기기가 통합된 통신 네트워크에 대한 연구가 활발하게 진행되고 있으며, 이를 통해 지리적으로 넓은 커버리지를 확보하면서 다양한 산업에서 실시간 통신과 효율적인 데이터 전송이 가능해지고 있다. 그러나 통합된 위성-IoT 통신 네트워크는 제한된 대역폭, 낮은 전력 요구사항, 다양한 이기종 장치 구성 등으로 인한 보안 문제가 발생하고 있다. 이를 해결하기 위해 SDN(Software Defined Networking)을 활용하여 위성-IoT 통신 시스템을 관리하는 연구가 진행되고 있다. 하지만 SDN 컨트롤러 및 스위치에 대한 자체적인 보안 문제도 있고, 통합된 SDN 기반 위성-IoT 통신 시스템에서의 새로운 보안 문제도 존재한다.

따라서 본 논문에서는 SDN 기반 저궤도 위성-IoT 통신 시스템을 위한 위협 모델링 및 보안 분석을 수행하여 통신 시스템의 보안 취약점을 식별하고, 잠재적인 공격 벡터 및 위협 시나리오를 파악하고자 한다. 모델링 및 분석을 위해 TV-HARM(Threat Vector Hierarchical Attack Representation Model)을 활용하였고, 이를 통해 SDN 기반 저궤도 위성-IoT 통신 시스템에서 발생할 수 있는 다양한 위협을 계층적으로 분석하였다. 각 노드의 초기 보안 점수, 손상 시 보안 점수, OS 패치 후 보안 점수 및 물리적 보안 점수를 통합한 종합 보안 점수를 산출하였으며, Betweenness Centrality Metric을 사용하여 보안 평가를 수행하였다. 본 논문은 위성-IoT 통신 시스템의 기본적인 보안 분석을 제공하며, 위성과 IoT 노드들의 보안 취약점을 식별하고 개선할 수 있는 방향성을 제시하였다.

Ⅰ. 서 론

저궤도 위성과 IoT(Internet of Things)를 결합한 통합 네트워크 시스템은 농업, 환경 모니터링, 물류 관리, 재난 대응 등 다양한 산업 분야에서 실시간 통신과 효율적인 데이터 전송을 가능하게 하여 큰 주목을 받고 있다[1]. 이러한 통합 네트워크는 지리적으로 광범위한 지역을 커버할 수 있지만, 제한된 대역폭, 낮은 전력 요구사항, 다양한 이기종 장치 구성 등으로 인해 보안 문제가 발생할 수 있다. 특히 IoT 장치와 위성 간 통신 채널에서 발생할 수 있는 보안 취약점은 시스템 전체의 신뢰성과 안전성을 저해할 수 있다.

SDN은 이러한 통합 네트워크의 관리와 보안 문제 해결에 중요한 역할을 한다. SDN은 네트워크 관리를 중앙에서 제어할 수 있게 하여 네트워크 트래픽을 동적으로 조정하고, 새로운 서비스나 장치를 쉽게 통합할 수 있게 한다. 하지만 중앙 집중화된 SDN 컨트롤러는 전체 네트워크를 관리하기 때문에 공격의 주요 표적이 될 수 있다. 공격자가 컨트롤러를 장악할 경우, 이는 전체 네트워크를 침해하거나 악의적으로 조작할 수 있는 위험을 증가시킨다.

본 논문에서는 SDN 기반 저궤도 위성-IoT 통신 시스템을 위한 위협 모델링 및 보안 분석을 수행하였다[2]. 이를 위해 TV-HARM[3]을 적용하여 시스템에서 발생할 수 있는 다양한 위협을 계층적으로 분석하였다.

분석 과정에서 CVSS(Common Vulnerability Scoring System)와 CVE(Common Vulnerabilities and Exposures)를 사용하여 각 노드의 보안 취약점을 평가하였다. 이러한 평가를 통해 초기 보안 점수, 손상 시 보안 점수, OS 패치 후 보안 점수 및 물리적 보안 점수를 산출하였다.

또한 Betweenness Centrality Metric을 사용하여 각 노드의 중요성을 평가하고 보안 취약점을 식별하였다. Betweenness Centrality 지표는 네트워크 내에서 특정 노드가 다른 노드들과의 통신을 중개하는 정도를 나타내며, 이를 통해 시스템 내에서 중요한 노드를 식별하고 보안 강화 방안을 제시할 수 있다. 본 연구는 이러한 분석을 통해 SDN 기반 저궤도 위성-IoT 통신 시스템의 보안을 평가하고 보안 취약점을 식별하여, 향후 연구에서 개선 방안을 도출할 수 있는 실질적인 가이드라인과 근거를 제시하였다.

Ⅱ. 본론

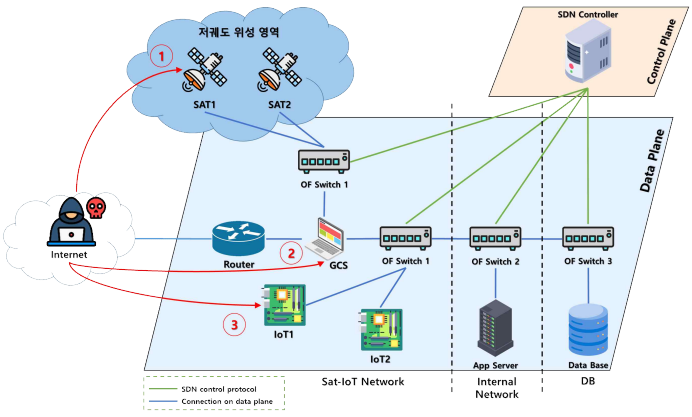


그림 1. 위성-IoT 네트워크의 시스템 모델 및 공격 벡터

저궤도 위성 과 IoT의 통합 네트워크의 보안 문제를 해결하기 위해, 본 연구에서는 SDN과 TV-HARM을 활용하여 보안 분석 및 위협 모델링을 수행하였다[4]. 공격 시나리오를 구성하여 각 노드들의 보안 취약점과 보안 점수를 산출하였다.

A. 위성-IoT 네트워크 시스템 개요

위성-IoT 네트워크는 다양한 구성 요소로 이루어져 있으며, 각 요소는 특정 기능과 역할을 수행한다. 본 연구에서는 위성, GCS(Ground Control System), IoT 장치들, 그리고 이들을 연결하는 네트워크 구성 요소들을 포함하는 시스템 모델을 설계하였다. 이러한 시스템 모델을 통해 잠재적인 공격 벡터를 식별하고 분석하였다.

그림 1은 위성-IoT 네트워크의 시스템 모델과 잠재적인 공격 벡터를 나타낸다. 시스템 모델은 위성 통신 모듈, IoT 장치, 지상 통제 시스템 간의 통신 경로를 보여주며, 각 공격 경로에서 발생할 수 있는 보안 취약점을 분석하였다. 이 시스템에서는 다음과 같은 주요 공격 벡터가 식별된다: 저궤도 위성을 통한 공격, IoT 모듈을 통한 공격, GCS를 통한 공격, SDN 컨트롤러를 직접 타겟으로 한 공격. 이러한 공격 경로는 빨간색 화살표로 표현하였으며, 해당 경로와 공격 벡터를 식별하고 분석함으로써 보안 대책을 마련할 수 있다.

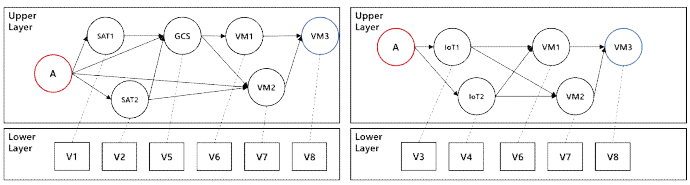
B. 시스템 보안 취약점 정보

표 1. 노드들의 CVSS 보안 취약점

ID	Node	CVE ID	CVSS BS	Impact
v1	SAT1	CVE-2018-13379	9.8	5.9
v2	SAT2	CVE-2014-0326	9.3	10.0
v3	IoT1	CVE-2023-3595	9.8	5.9
v4	IoT2	CVE-2023-6248	10.0	6.0
v5	GCS	CVE-2021-3156	7.8	5.9
v6	VM1	CVE-2022-26809	9.8	5.9
v7	VM2	CVE-2021-34473	9.1	5.2
v8	VM3	CVE-2021-34527	8.8	5.9

표 1은 위성-IoT 통신 시스템의 다양한 호스트들에 대한 CVSS (Common Vulnerability Scoring System) 보안 취약점을 나타낸다. 각 호스트의 주요 보안 취약점을 설정하고 그에 맞춰 CVSS 기본 점수(BS)와 영향점수(Impact)를 책정하였다. SAT1의 보안 취약점인 CVE-2018-13379의 경우, Viasat KA-SAT 네트워크 공격에 이용되었다 [5]. 해당 공격으로 인해 Viasat의 고속 위성 광대역 서비스 및 보안 네트워킹 서비스가 침해되었다. 표에 따르면 IoT2와 V1, VM1의 CVSS 기본 점수와 영향 점수가 가장 높게 나타났으며, 이는 이 노드들이 특히 높은 보안 위험에 노출되어 있음을 의미한다.

C. TV-HARM을 활용한 노드 구성 및 공격 시나리오



(a) tv_{12} when OFS1, OFS2 is compromised (b) tv_3 when OFS2 is compromised

그림 2. 노드들의 데이터 흐름 위협 모델

우리는 TV-HARM을 활용하여 위성-IoT 통신 시스템의 데이터 흐름 위협 모델을 구축하였다. 그림 2는 SAT와 IoT를 대상으로 한 두 가지 시나리오의 데이터 흐름을 시각화한 것이다.

(a) 위성 노드 기반 데이터 흐름 위협 모델(Threat Vector 1-2)

그림 2(a)는 위성 2개(SAT1, SAT2)로 구성된 통신 네트워크에서 OFS1(OpenFlow Switch)과 OFS2가 손상된 것을 가정하여 구성되었다. 이 모델은 SAT1 및 SAT2를 통해 GCS와 연결된 VM1, VM2, 그리고 최종 타겟인 VM3로의 접근 경로를 나타낸다.

(b) IoT 노드 기반 데이터 흐름 위협 모델(Threat Vector 3)

그림 2(b)는 IoT 2개로 구성된 통신 네트워크에서 OFS2만 손상된 경우를 보여준다. 이 모델은 IoT1과 IoT2를 통해 VM1 및 VM2로의 접근 경로를 나타내며, 최종 타겟은 VM3이다.

TV-HARM으로 구성한 데이터 흐름 위협 모델은 시스템의 보안 취약점을 시각적으로 식별하고, 잠재적인 공격 경로를 분석할 수 있게 한다.

D. 위성-IoT 네트워크 시스템 개요

표 2. Betweenness centrality metric을 적용한 보안 평가 및 점수

Threat Vector	Node	Initial	OFS1 Compromised	OFS2 Compromised	OS Patch	Physical Security	Average	Betweenness Centrality
tv12	IOT1	0.33	1	0.5	0.5	0.33	0.532	0
	IOT2	0.33	1	0.5	0.5	0.33	0.532	0
	VM1	0.5	1	0.2	1	0.67	0.674	0.5
	VM2	0.5	1	0.2	0.67	0.67	0.608	0.5
Threat Vector	**Node**	**Initial**	**OFS1 Compromised**	**OFS2 Compromised**	**OS Patch**	**Physical Security**	**Average**	**Betweenness Centrality**
tv3	SAT1	0.67	0.33	0.50	0.33	1.00	0.566	0.00
	SAT2	0.67	0.33	0.50	0.33	1.00	0.566	0.00
	GCS	0.50	0.50	0.33	0.50	0.50	0.466	1.00
	VM1	0.50	0.50	0.20	1.00	0.67	0.574	0.33
	VM2	0.50	0.50	0.20	0.67	0.67	0.508	0.33

연구 내용을 토대로 Betweenness Centrality Metric을 사용하여 저궤도 위성-IoT 통신 시스템의 보안 평가를 수행하였다. 표 2는 TV-HARM을 기반으로 도출된 두 가지 시나리오(tv12, tv3)에 대한 노드들의 보안 점수를 나타낸다. 각 노드의 초기 보안 점수, OFS1 및 OFS2 손상 시 보안 점수, OS 패치 후 보안 점수, 물리적 보안 점수, 그리고 종합 보안 점수 및 Betweenness Centrality 지표를 포함한다.

결과적으로 위성 공격 시나리오에서는, GCS 노드가 SAT 노드들에 비해 보안적으로 더 취약하고 Betweenness Centrality 지표가 높기 때문에, 공격 시 전체 네트워크의 안정성과 가용성에 치명적인 영향을 미칠 수 있는 매우 중요한 노드로 간주된다. IoT 시나리오에서는 IoT 노드가 상대적으로 보안이 취약하나 Betweenness Centrality 지표가 낮기 때문에 네트워크에서의 중요도는 상대적으로 낮다고 볼 수 있다.

Ⅲ. 결론

본 논문에서는 SDN 기반 저궤도 위성-IoT 통신 시스템의 보안 취약점을 분석하기 위해 TV-HARM과 Betweenness Centrality Metric을 활용하여 네트워크 내 각 노드의 보안 점수를 평가하였다. 결과적으로, GCS와 VM 노드가 네트워크 내에서 중요한 역할을 수행하고 있으며, 이들 노드가 손상될 경우 전체 네트워크에 큰 영향을 미칠 수 있음을 확인하였다. 따라서 이러한 취약점을 해결하고 네트워크의 안정성을 확보하기 위해, GCS와 VM 노드 및 통신 시스템에 대한 암호화 통신, 보안 프로토콜 개선 및 경량화, 통신 노드 인증 프레임워크 구축 등의 연구가 반드시 이루어져야 할 것이다.

ACKNOWLEDGMENT

본 결과물은 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 첨단분야 혁신융합대학사업(차세대통신)의 연구 결과입니다.

이 성과물은 산업통상자원부의 재원으로 한국산업기술진흥원(KIAT)의 지원을 받아 수행된 연구임.

(P0017124, 2024년 산업혁신인재성장지원사업)

참 고 문 헌

[1] M. Centenaro et al., “A Survey on Technologies, Standards and Open Challenges in Satellite IoT,” IEEE Commun. Surv. Tutorials, vol. 23, no. 3, 2021, pp. 1693 - 1720.

[2] W. Jiang, "Software defined satellite networks: A survey," Digital Communications and Networks, Volume 9, Issue 6, 2023, pp. 1243-1264.

[3] T. Eom, J. B. Hong, S. An, J. S. Park, and D. S. Kim, "A Systematic Approach to Threat Modeling and Security Analysis for Software Defined Networking," IEEE Access, vol. 7, pp. 137432-137445, Sep. 2019

[4] J. Mendonça, M. Kim, R. Graczyk, M. Völp and D. D. Kim, "Security Modeling and Analysis of Moving Target Defense in Software Defined Networks," 2022 IEEE 27th Pacific Rim International Symposium on Dependable Computing (PRDC), Beijing, China, 2022, pp. 141-151

[5] "Space Cyber Attack Post-Mortem: A Viasat Attack Investigation," Space Security, 2022.
(https://www.spacesecurity.info/space-cyber-attack-post-mortem-a-viasat-attack-investigation/)