JPNT 15(1), 129-136 (2026)
https://doi.org/10.11003/JPNT.2026.15.1.129

JPNT Journal of Positioning, Navigation, and Timing

WAD-RNSS 지상시스템 안정성 및 가용성 보장을 위한 보안 아키텍처 적용 방법

이상진, 최증원, 박영일, 김선진, 우지연, 정희수, 김동욱†

A Method to Implement a Security Architecture for Stability and Reliability in Wide-Area Differential Regional Navigation Satellite System (WAD-RNSS) Ground Segment

Sang-Jin Lee, Jeung Won Choi, Youngil Park, Sunjin Kim, Jiyeon Woo, Heesoo Jeong, Donguk Kim†
Agency for Defense Development, Daejeon 34186, Korea

ABSTRACT

The wide-area differential regional navigation satellite system (WAD-RNSS) integrates wide-area differential navigation technology with a regional navigation satellite system (RNSS) to provide navigation and correction signals as a unified service. The WAD-RNSS ground segment, which consists of reference stations, a master control station, and ground antennas, is in charge of generating information for navigation and correction signals. To ensure system stability, it is necessary to implement a security architecture to protect against threats. This paper presents a method to apply a security architecture to the WAD-RNSS ground segment.

Keywords: WAD-RNSS, ground segment, security architecture, network security
주요어: 광역보정기반 지역위성항법, 지상시스템, 보안 아키텍처, 네트워크 보안

1. 서론

Wide-area differential regional navigation satellite system (WAD-RNSS)는 기존 RNSS 시스템에 광역보정 항법기술을 접목하여 지상에서 방송궤도력과 보정정보를 생성하고 위성에서 항법 신호와 보정 신호를 함께 방송함으로써 사용자에게 좀 더 정밀한 위치 정보를 제공할 수 있다 (Kim et al. 2021, 2023). WAD-RNSS 지상시스템은 사용자에게 제공되는 방송궤도력과 보정정보를 생성하기 위한 핵심 기능을 담당 하므로 (Kim et al. 2023), 안정성 확보가 필수적이다. 본 논문에서는 WAD-RNSS 지상시스템의 안정성 확보를 위한 보안 아키텍처 적용 방법론을 제시하고자 한다.

2. 보안 아키텍처 개요

보안 아키텍처의 목적은 시스템에 대한 무결성, 가용성, 기밀성을 보장하여 안정성을 확보하는 것이다. International Telecommunications Union (ITU)에서는 보안 아키텍처 적용을 위한 권고 문서인 ITU-T X.805를 발행하였다. 해당 문서는 시스템 Fig. 1과 같이 ITU-T X.805는 대상 시스템을 응용, 서비스, 인프라 계층으로 분류하고 각 계층별로도 사용자, 제어, 관리 평면으로 분류하여 시스템 내부의 취약점과 외부로부터의 공격과 위협들로부터 8개로 분류된 다차원 보안서비스를 적용했을 때 도출되는 정보보호 요구사항을 획득해서 시스템에 대한 안정성을 확보하도록 하였다 (ITU 2003).

WAD-RNSS 지상시스템에 대한 보안 아키텍처 적용을 위해서

Received Feb 13, 2026 **Revised** Feb 25, 2026 **Accepted** Mar 06, 2026

†**Corresponding Author** E-mail: donguk319@add.re.kr

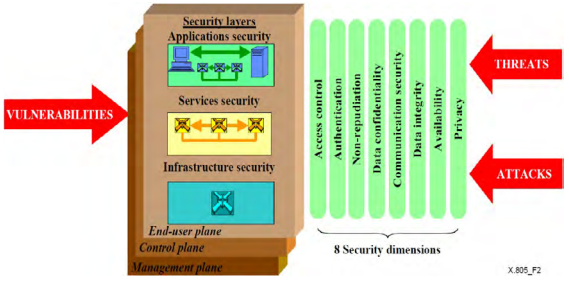

Fig. 1. Applying security dimensions to security layers & planes (ITU 2003).

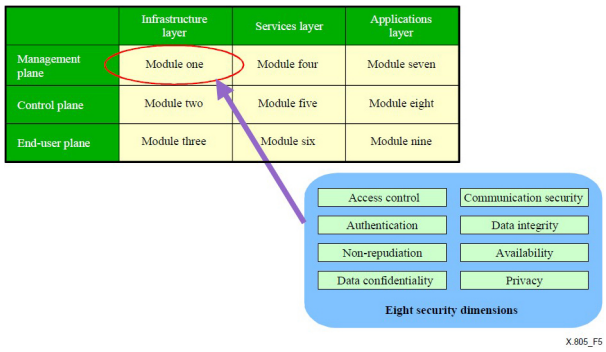

Fig. 2. Security architecture in a tabular form (ITU 2003).

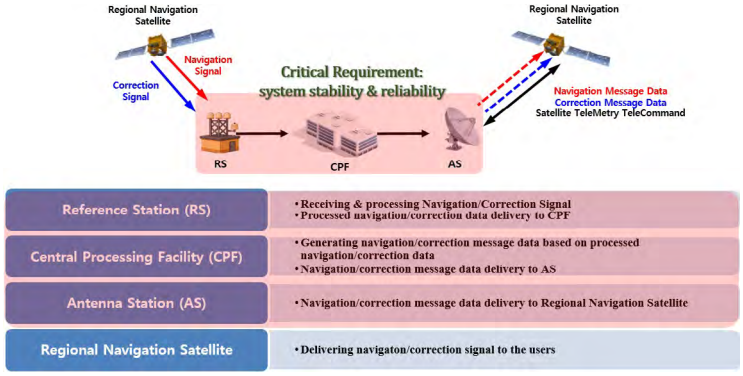

Fig. 3. The construction of ground segment in WAD-RNSS.

는 Fig. 2와 같이 3개의 계층(인프라, 서비스, 응용)과 3개의 평면(관리, 제어, 사용자)에 따른 매트릭스 구축이 필요하다. 매트릭스가 구축됨에 따라 보호 대상 시스템이 9개의 모듈로 나뉘어지게 되며, 각 모듈별로 취약성과 외부의 공격과 위협으로부터 8개의 보안차원을 적용하여 정보보호 목표와 요구사항을 도출하게 되는 것이다.

3. WAD-RNSS 지상시스템 보안 아키텍처 적용 방법

3.1 취약성 및 위협 분석

보안 아키텍처 적용을 위해서는 대상 시스템에 대한 구조 분석과 이를 기반한 내/외부 취약성 분석이 반드시 선행되어야 한다.

3.1.1 구조분석 (Fig. 3)

WAD-RNSS 지상시스템의 주요 역할은 사용자에게 전달할 항법/보정 메시지 데이터 생성 및 전달이며, 항법신호를 수신하고 중앙처리국에 측정치 데이터를 전달하는 Reference Station (RS, 기준국)과 측정치를 기반으로 위성에 대한 위치 정보 또는 보정정보가 담긴 항법/보정메시지 데이터를 생성하는 Central Processing Facility (CPF, 중앙처리국), 그리고 중앙처리국에서 생성한 항법/보정메시지 데이터를 항법위성에 전달하기 위한 Antenna Station (AS, 안테나국)으로 구성되어져 있다.

3.1.2 구조분석 - 구성요소 (Fig. 4a)

"구조분석"을 통해 WAD-RNSS 지상시스템에 대한 상위 개념으로의 분석이 완료되면, 이를 ITU-T X.805에서 정의하는 계층과 평면측면에서 세부 구성 요소로 분류하며, 다음과 같이 구분될 수 있다.

1) 계층 (시스템을 구성하는 물리적 및 논리적 요소 구분)

인프라 계층: 데이터 전송을 위한 전송 장비(또는 장치)들에 대한 보호 요소들을 정의하는 계층으로써 WAD-RNSS 지상국(RS↔CPF↔AS) 간의 데이터 유통을 위한 네트워크 통신 장비(또는 장치)들, 단말, 그리고 서버 등이 해당 계층의 대상으로 볼 수 있음. (Fig. 4a 내 network device (L2/L3), terminal, server, DB (DateBase) 그리고 붉은색 선)

서비스 계층: 서비스 제공자와 사용자 간에 전송 및 연결을 위해 필요한 서비스에 대해 보호 요소들을 정의하는 계층으로써 WAD-RNSS 지상시스템에서는 WAD-RNSS 지상국(RS↔CPF↔AS) 간 안정적인 데이터 유통을 위해 활용되는 통신사 전용망(임대회선)이 해당 계층의 대상으로 볼 수 있음.

응용 계층: 운용자(또는 사용자)가 서비스 제공(또는 접근)을 위해 활용하는 응용 소프트웨어를 구분하는 계층으로써 WAD-RNSS 지상시스템에서는 Monitoring and Control (M&C) 소프트

https://doi.org/10.11003/JPNT.2026.15.1.129

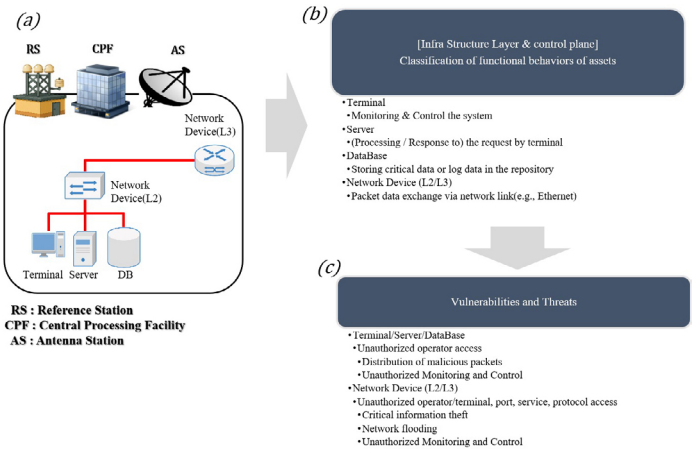

Fig. 4. The classification of functional behaviors of assets & related threats in WAD-RNSS ground segment.

Table 1. The classification of attack types and analysis into WAD-RNSS (case: infrastructure layer, control plane).

Module 2: Infrastructure layer, control plane		
Vulnerabilities and threats		Attack types
(External) Unauthorized access	Distribution of malicious packets	[External malicious traffic intrusion] - Malware: Malware is malicious software designed to infect systems (e.g., Viruses, worms, Trojan Horse, etc.) - Phishing: Phishing is malicious software designed to steal critical data (or information) via e-mail or web site. - DDoS: Distributed Denial of Service attack
	Unauthorized M&C	[Packet sniffing] - ARP spoofing attack: ARP spoofing allows a malicious person to intercept packet, modify the traffic, or prevent network traffic. - Wi-Fi packet sniffing: Wi-Fi packet sniffing is the attack intercepting and analyzing data packets over a wireless network → In general, attackers take advantage of unencrypted Wi-Fi networks.
(Internal) Unauthorized operator/ terminal, port, service, protocol access	Critical data theft	[False positive or negative alarm attack] - False positive attack: Leads to alert fatigue into the system. - False negative attack: Indicates weak or misconfigured security controls.
	Network flooding	[DDoS] - Volumetric attacks (e.g., UDP flooding, ICMP flooding) - Protocol attacks (e.g., SYN flooding, HTTP flooding)
	Unauthorized M&C	Refer to attack type column “Packet sniffing” attack

웨어가 해당 계층의 대상으로 볼 수 있음

2) 평면 (시스템의 운영 및 관리 등과 같은 활동 측면에서의 보안 기능을 구분)

관리 평면: WAD-RNSS을 운용하기 위한 운용, 관리, 유지보수 등 관리자 측면에서의 활동

제어 평면: WAD-RNSS을 운용하기 위한 정보들의 유통과 관련된 활동 (Fig. 4b)

사용자 평면: WAD-RNSS 사용자의 서비스 활용과 네트워크 접근과 관련된 활동

“구조분석-구성요소” 분석결과에서 확인할 수 있듯이, ITU-T X.805에서 정의하고 있는 계층과 평면 중 서비스/응용 계층 그리고 관리/사용자 평면의 경우 시스템이 제공하고자 하는 서비스 대상에 따른 종속성이 강하다. 예를 들면, WAD-RNSS 지상시스템을 계층측면에서 분석했을 때 서비스 계층은 전용망, 응용 계층은 M&C 소프트웨어로 분류할 수 있으며, 두 계층 모두 유통하는 데이터의 중요도에 따라 보안대책이 상이할 수 있다. 데이터의 중요도의 경우 WAD-RNSS 활용하는 기관의 내부지침(또는 규정)에 따라 정의하므로 보안 아키텍처 설계시에도 특정 부분은 해당 지침에 종속된다. 평면 측면에서도 관리 평면은 운용, 관리, 유지보수 등의 활동으로 계층 측면과 마찬가지로 내부지침에 종속되며, 사용자 평면의 경우에는 대부분 위성체와 수신기(사용자)에서의 anti-jamming, spoofing 신호 식별 기술 또는 인증 기술들로 본 논문에서 정의하는 지상시스템 보안 아키텍처 내용에서는 벗어나게 된다.

위와 같은 이유로 본 논문은 WAD-RNSS 지상시스템 관점에서 항법/보정메시지라는 주요 정보 생성과 유통측면에서 일반화 적용이 가능한 인프라 계층 그리고 제어 평면에 한정하여 취약성 및 위협 분석 그리고 이에 대응되는 보안대책에 대하여 기술하고자 한다.

WAD-RNSS 지상시스템에 대한 구조분석 후, 계층과 평면으로 세부 구성요소들이 분류되면 이를 기반으로 내/외부 취약성 분석 및 위협을 분석하게 된다 (Fig. 4c). Table 1의 “Vulnerabilities and threats” 컬럼은 WAD-RNSS 지상시스템을 인프라 계층과 제어 평면 관점에서 취약성과 위협을 분석한 내용으로 내부 취약성은 비인가 접근, 외부 취약성은 운용자/단말/포트/서비스/프로토

Table 2. Example of implementing the security architecture for WAD-RNSS (case: infrastructure layer, control plane) (Lee et al. 2025).

Module 2: Infrastructure layer, control plane		
Security dimension	Security objectives	Security activities
Access control	Ensure that only authorized personnel or devices are allowed to perform administrative or management activities on the network device or communications link.	Only authorized personnel are allowed to access the network device and storage via Identification (ID) and PassWord (PW). NAC can provide the function preventing unauthorized IP address or MAC address from accessing network devices.
Authentication	Verify the identity of the person or device performing the administrative or management activities on network device or communication link.	When accessing the control terminal for performing administrative or management activities, only authorized personnel are allowed while checking the ID and PW. When PW is stored, it must be encrypted using SHA-256 (one-way hash function) and TLS is used when transmitting.
Non repudiation	Provide a record identifying the individual or device that performed each administrative or management activity on the network device or communications link and the action that was performed. This record can be used as proof of the originator of the administrative or management activity.	Log and daily backup below items for tracking responsibility when security accident is occurred. - account access behavior: log-in success/failure, log-out - history of changing or configuring information for account - history of access denial: access ID/IP, the reason of denial and date of access The record of log must be stored into independent offline storage and retained for two years. * Storage access must be allowed only authorized personnel.
Data confidentiality	Protect the configuration information of network devices and communications links against unauthorized modification, deletion, creation, and replication. This protection applies to configuration information resident in the network device or communications link, as well as configuration information that is in transit or stored in offline systems.	Only authorized personnel or devices are allowed to access the network device and storage via ID and PW. In case of transmitting the information over Wide Area Network (WAN), it must be encrypted at each level according to the importance.
Communication security	In the case of remote management of a network device or communications link, ensure that the management information only flows between the remote management stations and the devices or communications links that are being managed. The management information is not diverted or intercepted as it flows between these endpoints.	Prevent unauthorized IP address, MAC address, port, service protocol via NAC. Security vulnerabilities such as well-known port, service and protocol are blocked in principle, but can be used with administrator approval when necessary (In this case, related history must be recorded or stored).
Data integrity	Protect the configuration information of network devices and communications links against unauthorized modification, deletion, creation, and replication. This protection applies to configuration information resident in the network device or communications link, as well as configuration information that is in transit or stored in offline systems.	Only authorized personnel or devices are allowed to access the network device and storage via ID and PW.
Availability	Ensure that the ability to manage the network device or communications link by authorized personnel or devices cannot be denied. This includes protection against active attacks such as Denial of Service (DoS) attacks as well as protection against passive attacks such as the modification or deletion of the administrative authentication information.	[LAN] Unauthorized IP address or MAC address, port, services and protocols must be prevented from accessing network devices. In principle, port, service and protocol know to be vulnerable must be blocked but can be used with administrator approval when necessary. (In this case, related history must be recorded or stored.) [WAN] Unauthorized external access and harmful packets are prevented via UTM. It is necessary to provide Monitoring function for UTM blocking history.
Privacy	Ensure that information that can be used to identify the network device or communications link is not available to unauthorized personnel or devices. Examples of this type of information include a network device's IP address or DNS domain name.	The information of network devices, servers, terminals and protocol for system are documented and systematically managed. Also, only authorized personnel is allowed to access information.

콜 접근으로 분류되며, 내부 취약성에 따른 위협은 유해 패킷 유통과 비인가자 관제 시도 그리고 외부 취약성에 따른 위협은 민감 정보 탈취, 네트워크 과부하, 비인가자 관제 시도로 분류된다.

3.2 공격 분석

WAD-RNSS 지상시스템에 대한 취약성 및 위협 분석 완료후에는 각 위협에 따라 발생 가능한 공격들을 분류하게 된다. Table 1의 "Attack types" 컬럼은 WAD-RNSS 지상시스템 위협에 따라 발생할 수 있는 공격 유형들을 분석한 내용이다.

3.2.1 외부취약성 – 유해 패킷 유통

유해 패킷 유통과 관련된 공격에는 Malware, Phishing, Distributed Denial of Service (DDoS) 공격 등이 있으며, Malware는 시스템을 감염시키기 위한 악의적인 소프트웨어로써

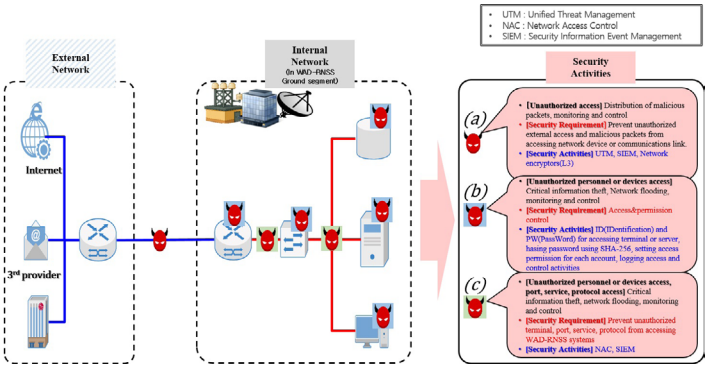

Fig. 5. The classification of functional behaviors of assets in WAD-RNSS ground segment.

바이러스, 웜, 트로이목마 등이 이에 해당한다. Phishing 역시 악의적인 소프트웨어로써 주요 데이터에 대한 탈취 목적으로 이메일 또는 웹사이트 상에 Malware를 심어 공격 대상에게 전파하는 방법으로 공격을 시도한다. 마지막으로 DDoS는 대상 시스템에 무의미하거나 악의적인 트래픽을 과도하게 발생시켜 시스템을 마비시키는 공격이다.

3.2.2 외부취약성 – 비인가자 관제 시도

비인가자 관제 시도와 관련된 공격에는 패킷 스니핑(packet sniffing)이 있으며, 관련 종류에는 Address Resolution Protocol (ARP) 스푸핑(spoofing)과 Wi-Fi 패킷 스니핑 공격이 있다. ARP 스푸핑은 패킷에 대한 도청, 데이터 변조, 서비스 거부의 목적으로 악의적인 사용자가 Media Access Control (MAC) 주소와 Internet Protocol (IP) 주소를 매핑 시켜주는 ARP 프로토콜의 취약성을 이용하여 악의적인 사용자의 IP를 정상적인 MAC 주소에 매핑 시키는 공격이다. Wi-Fi 패킷 스니핑은 주요 정보 탈취를 목적으로 무선 네트워크가 일반적으로 암호화되지 않는다는 취약성을 활용하여 유통 패킷을 가로채는 공격이다.

3.2.3 내부취약성 – 주요 정보 탈취

주요 정보 탈취에 따른 위협으로는 주요 정보를 기반으로 오류 긍정 알람(false positive alarm)과 오류 부정 알람(false negative alarm) 공격이 있으며, 오류 긍정 알람 공격은 발생하지 않은 오류 발생시켜 시스템의 피로도를 높이는 공격이며, 오류 부정 알람 공격은 발생한 오류를 탐지하지 못하게 하여 시스템이 위협 또는 공격으로부터 제대로 된 조치를 할 수 없도록 하는 공격이다.

3.2.4 내부취약성 – 네트워크 과부하

네트워크 과부하와 관련된 공격에는 DDoS 공격이 있으며, 관련 종류에는 Volumetric과 프로토콜 두가지 타입의 공격이 있다. Volumetric 공격 명칭처럼 공격 대상 시스템에 대량의 무의미한 패킷을 유통시켜 과부하를 유발시키는 공격으로 User Datagram Protocol (UDP)과 Internet Control Message Protocol (ICMP) 플러딩(flooding) 공격이 있다. UDP 플러딩은 Transmission Control Protocol (TCP)처럼 패킷을 전송을 위한 세션 채결이 필요하지 않는다는 취약성을 활용하여 패킷을 무작위적으로 전송하여 시스템에 과부하를 주는 공격이며, ICMP 플러딩 공격은 ICMP 에코 요청/응답 메시지(ping)를 무작위적으로 전송하여 시스템에 과부하를 주는 공격이다.

프로토콜 공격은 해당 프로토콜의 취약성을 활용하여 시스템에 과부하를 주는 공격으로 SYNchronize (SYN), HyperText Transfer Protocol (HTTP) 플러딩 공격이 있다. SYN 플러딩은 TCP의 세션 연결 시 사용되는 메시지를 악의적으로 활용하며, HTTP는 사용자(클라이언트)가 웹사이트 서버에 요청하는 메시지인 HTTP GET/POST를 악의적으로 활용하여 시스템 과부하를 주는 공격이다.

3.2.5 내부취약성 – 비인가자 관제시도

해당 공격은 “외부취약성-비인가자 관제시도”와 내용이 동일하다.

3.3 보안 요구사항에 다른 활동(보안대책) 정의

외부 공격으로부터 시스템에 대한 안정성과 가용성을 보장하기 위한 보안대책(또는 활동)을 실현화 하고자, 보안 요구사항 식별을 위해서는 앞서 기술한 바와 같이 WAD-RNSS 지상시스템에 대한 취약성 및 위협 분석이 선행되어야 한다. 이를 위해 본 논문에서는 WAD-RNSS 지상시스템에 대한 구조 분석과 분석 결과를 기반으로 ITU-T X.805에서 정의한 계층에 매핑 시켰으며, 이를 평면에 기반해서 취약성 및 위협을 분석하고 관련 공격들을 식별하였다. Table 2는 8개의 보안 차원 관점에서 WAD-RNSS 지상시스템에서 발생 가능한 공격 유형별로 적용해야 할 보안 요구사항을 식별한 내용이며, Fig. 5는 도출된 보안 요구사항을 달성하기 위해 적용되어야 하는 보안장비 및 소프트웨어 기능들에 대하여 구체화한 내용으로 각각의 내용은 아래와 같다.

1) 접근제어

정의: 인가된 개인 또는 장치만 네트워크 장치나 오프라인 저장소에 있는 제어 정보에 접근할 수 있도록 허용.

관련 보안대책: 네트워크 장치 및 저장소 접근시에는 유일한

개인식별자와 비밀번호를 통해서만 접근이 가능하도록 함.

보안대책 적용(Fig. 5c): Network Access Control (NAC) 장비를 활용하여 미승인 IP 주소 또는 MAC 주소 접속을 차단함.

2) 인증

정의: 네트워크 장치의 제어 정보를 관제하거나 수정하는 사람 또는 장치는 검증을 통해 허용.

관련 보안대책: 네트워크 관제용 SW를 접근시에는 유일한 개인식별자와 비밀번호를 통해 사전에 인가된 사용자만 접근 가능하도록 통제함.

보안대책 적용(Fig. 5b): 네트워크 관제용 SW 접근용 계정 생성 및 관리. 비밀번호의 경우 저장시에는 SHA-256 이상의 해쉬함수를 활용하여 해쉬 값 형태로 저장하고, 전송이 필요한 경우에는 Transport Layer Security (TLS)를 활용함.

3) 부인방지

정의: 네트워크 장치에 대한 제어 정보를 관제하거나 수정한 각 개인 또는 장치에 대한 식별과 저장 기록은 제공해야 함.

관련 보안대책: 침해사고시 책임추적, 장비관리 등을 위해 아래 사항들에 대해 로그를 기록하고 일일단위 백업 실시 (계정 접속 행위, 계정 정보의 변경 정보, 계정 접근 거부 이력).

보안대책 적용(Fig.5b): 로그기록은 별도의 저장매체에 주기적으로 백업하며 2년간 보관함.

4) 데이터 기밀성

정의: 네트워크 장치 또는 오프라인 저장소에 저장된 제어 정보들을 허가되지 않은 접근이나 열람으로부터 보호해야 함. 네트워크 장치에 대한 제어 정보가 전송되는 동안 허가되지 않는 접근이나 열람으로부터 보호되어야 함.

관련 보안대책: 네트워크 장치 또는 저장소에 접근시에는 유일한 개인식별자와 비밀번호를 통해 접근 가능하도록 함. 정보를 Wide Area Network(WAN)-외부로 전송시에는 회선용 암호장비를 통해 암호화함.

보안대책 적용(Figs. 5a,b): 네트워크 장치 또는 저장소 접근을 위한 계정생성 및 관리. WAN 구간에 회선용 암호장비를 설치함.

5) 통신보안

정의: 네트워크를 통해 전송되는 제어정보는 사전에 정의된 목적지로만 전송되어야 하며, 중간에 우회되거나 가로채이지 않아야 함.

관련 보안대책: 보안에 취약하다고 알려진 포트, 서비스, 프로토콜 차단이 원칙이나, 불가피하게 사용이 필요한 경우 관련 관리자에게 승인을 얻어 사용하며, 관련 이력에 대하여 기록 또는 저장함.

보안대책 적용(Fig. 5c): NAC 장비를 활용하여 미승인 IP/MAC 주소, 포트, 서비스, 프로토콜은 차단함.

6) 데이터 무결성

정의: 네트워크 장치에 있는 제어정보, 네트워크에 유통되거나 오프라인 저장소에 저장된 정보는 허가되지 않은 수정, 삭제, 생성, 그리고 복제로부터 보호되어야 함.

관련 보안대책: 네트워크 장치 및 저장소 접근시에는 유일한 개인식별자와 비밀번호를 통해서만 접근이 가능해야 함.

보안대책 적용(Fig. 5b): 네트워크 장치 및 저장소 접근을 위한 계정 생성 및 관리.

7) 가용성

정의: 네트워크 장치들은 항상 허가된 장치로부터 제어정보를 수신할 수 있도록 보장해야 함.

관련 보안대책: 보안에 취약하다고 알려진 포트, 서비스, 프로토콜 차단이 원칙이나, 불가피하게 사용이 필요한 경우 관련 관리자에게 승인을 얻어 사용하며, 관련 이력에 대하여 기록 또는 저장함.

보안대책 적용(Figs. 5a,c): Local Area Network (LAN) 구간은 NAC 장비를 활용하여 미승인 IP/MAC 주소, 포트, 서비스, 프로토콜은 차단함. WAN 구간의 네트워크 경계부분은 Unified Threat Management (UTM) 장비를 통해 비인가 외부 접근과 유해 패킷을 차단하고 해당 기록에 대하여 관제 및 기록함.

8) 정책

정의: 네트워크 장치 또는 링크를 식별할 수 있는 정보를 허가되지 않은 단말이나 장치가 접근할 수 없도록 보장해야 함.

관련 보안대책: 시스템을 구성하는 네트워크 장비, 서버, 단말기 별 포트, 서비스, 프로토콜 등을 문서화하여 체계적으로 관리함.

보안대책 적용(Fig. 5c): Security Information Event Management (SIEM) 소프트웨어를 적용하여 보안 관제 및 정책을 구성함.

4. 결론

WAD-RNSS 지상시스템은 사용자가 자신의 위치를 계산할 수 있도록 지원해주는 항법/보정정보라는 주요 정보를 생성하는 곳으로 보안 취약성 발생하게 될 경우 서비스 전체에 대한 신뢰성과 안정성 저하가 발생할 수 있다. 본 논문에서는 ITU-T X.805 문서에서 제공하고 있는 방법론에 따라 WAD-RNSS 지상시스템에 대한 구조 분석과 그에 따른 취약성 및 위협 분석을 진행하였고 이를 토대로 보안 요구사항 및 보안 대책을 적용해보았다. 본문 내용에서 확인할 수 있듯이 식별된 공격들에 대한 적절한 대응책 또는 방안들을 확보함으로써 주요 정보에 대한 기밀성과 무결성을 보장할 수 있었고 이를 통해 시스템에 대한 안정성과 신뢰성이 확보됨을 확인할 수 있었다.

ACKNOWLEDGMENTS

이 연구는 정부(방위사업청)의 재원으로 국방과학연구소의 지원을 받아 수행된 연구임 (274345901).

AUTHOR CONTRIBUTIONS

Conceptualization, S.-J. Lee and D. Kim; methodology. S.-J. Lee, J.-W. Choi, and Y. Park; formal analysis, S.-J. Lee, S. Kim, J. Woo, and H. Jeong; validation, S.-J. Lee and D. Kim; writing—original draft preparation, S.-J. Lee; writing—

review and editing, S.-J. Lee, J.-W. Choi, Y. Park, S. Kim, J. Woo, H. Jeong, and D. Kim; visualization, S.-J. Lee, S. Kim, J. Woo, H. Jeong, and D. Kim; Supervision, D. Kim.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

International Telecommunication Union (ITU) 2003, Security architecture for systems providing end-to-end communications, Recommendation ITU-T X.805.

Kim, D., Lee, K., Choi, J. W., Park, Y., & Lee, S. 2023, A Study on Architecture of Wide-Area Differential Regional Navigation Satellite System (WAD-RNSS), 2023 IPNT Conference, Jeju, Korea, 1-3 Nov 2023, pp.419-421. https://ipnt.or.kr/2023proc/24

Kim, D., So, H., & Park, J. 2021, Performance Analysis of Wide-Area Differential Positioning Based on Regional Navigation Satellite System, JPNT, 10, 35-42. https://doi.org/10.11003/JPNT.2021.10.1.35

Lee, S.-J., Kim, J., Choi, J. W., Park, Y., Kim, S., et al. 2025, Implementing the security architecture for Wide-Area Differential Regional Navigation Satellite System (WAD-RNSS) Ground System, 2025 IPNT Conference, Jeju, Korea, 4-8 Nov 2025, pp.523-526. https://ipnt.or.kr/2025proc/48

Sang-Jin Lee is a senior researcher of Agency for Defense Development (ADD) in the Republic of Korea. He received the B.S. degree in software and security engineering from Baekseok University and the M.S. degree in electrical/electronic computer engineering from Sungkyunkwan University, Republic of Korea in 2007 and 2010. His research interests include navigation system architecture, Satellite-Based Augmentation System (SBAS), security, and system.

Jeung Won Choi is a principal researcher of Agency for Defense Development (ADD) in the Republic of Korea. He received the B.S., M.S., and Ph.D. degrees in Computer Science from Chungnam National University in 1989, 1993, 1997 respectively. In 1997, he joined ADD, where he is currently a principal researcher. In 2013, he joined the department of Weapon System Engineering from University of Science and Technology, Daejeon, Republic of Korea, as a Faculty Member, where he is currently a professor. His research interests are tactical communication, satellite communication, cognitive radio, and global position system.

Youngil Park is a researcher of Agency for Defense Development (ADD) in the Republic of Korea. He received his master's degree in 2006 from Department of Electronic Engineering, Graduate School of Electro-Communications in Japan. He has been working for the ADD since Feb. 2013. His research interests include navigation satellite control, construct Monitoring station in SBAS.

Sunjin Kim is a researcher of Agency for Defense Development (ADD) in the Republic of Korea. He received his bachelor's degree in 2018 and the master's degree in 2023 from the mechanical and aerospace engineering of Korea Advanced Institute of Science and Technology (KAIST). He worked in the field of ionospheric environment research using navigation signal in KAIST GNSS laboratory. He has been working for the ADD since Sep. 2023. His research interests include navigation system architecture, Satellite-Based Augmentation System (SBAS), ionospheric disturbances, and ionospheric modeling.

Jiyeon Woo is a researcher of Agency for Defense Development (ADD) in the Republic of Korea. She received the B.S. degree in Aerospace Information System Engineering from Konkuk University, Seoul, Republic of Korea, in 2022, and the M.S. degree from same university in 2024. Her research interests include GNSS-based relative navigation, satellite orbit design, and orbit determination.

Heesoo Jeong is a researcher of Agency for Defense Development (ADD) in the Republic of Korea. She received the B.S. degree in Electrical and Electronics Engineering from Konkuk University, Seoul, Republic of Korea, in 2023, and the M.S. degree from same university in 2025. Her research interests include satellite navigation systems, software GNSS receivers, and vector-based navigation signal processing.

Donguk Kim is a senior researcher of Agency for Defense Development (ADD) in the Republic of Korea. He received the bachelor's degree in 2013 and the Ph.D. degree in 2020 from the mechanical and aerospace engineering of Seoul National University (SNU). He worked in the field of centimeter-level GNSS augmentation systems and technology in SNU GNSS laboratory. He has been working for the ADD since Dec. 2019. His research interests include navigation system architecture, Satellite-Based Augmentation System (SBAS), Real-Time Kinematic (RTK), and anti-jamming/anti-spoofing algorithm.

https://doi.org/10.11003/JPNT.2026.15.1.129