한국정보전자통신기술학회논문지(jkiiect)'16-02, Vol.9 No.1
논문 15-09-01-049 http://dx.doi.org/10.17661/jkiiect.2016.9.1.049

표준 AIS 프로토콜 분석을 통한 보안 AIS 프로토콜 제안

이정수*, 허욱*, 김재환*, 정성욱*

A Secure AIS Protocol Suggestion with Analyses of the Standard AIS Protocol

Jung-Su Lee*, Ouk Heo*, Jae-Hwan Kim*, Sung-Wook Chung*

요 약 최근 몽골 선적 화물선 침몰사고, 진도 세월호 여객선 침몰사고 등 해양 사고는 끊임없이 발생하고 있다. 이러한 해양 사고 발생 건수를 줄이기 위해 국제표준에 따라 국내선박은 AIS(Automatic Identification System) 시스템을 의무 장착하고 있다. AIS 시스템은 선박 항해를 위한 정보들의 통신 프로토콜 체계이나 프로토콜 분석결과 표준 AIS 프로토콜은 보안성을 전혀 고려하지 않고 있음을 알 수 있다. 또한, The FUNcuve Dongle Pro+라는 위성 통신 수신기를 이용하면 손쉽게 AIS 무선 프로토콜을 Hijacking 할 수 있다. 따라서 본 논문에서는 AIS 시스템의 표준 프로토콜의 보안 취약점을 분석하고 안전한 선박통신을 위해 송수신자의 MAC Address를 표기하여 신뢰성을 확보하고, VPN Tunnelling 암호화 기법을 이용하여 DATA 전송 시 안전한 전송을 할 수 있는 프로토콜에 대해 제안한다. 그리고 본 논문에서 제안하는 프로토콜 구조를 사용하는 경우, 통신정보의 Hijacking 발생시 보다 안전한 데이터 송수신을 할 수 있음을 확인한다. 그래서 제안된 보안 AIS 프로토콜을 통하여 앞으로의 선박 안전 기술에 영향을 미칠 것으로 기대된다.

Abstract Recently, marine accidents such as the sinking accident Mongol freighter ship and the sinking accident of Sewol ferry in Jindo continuously happen. In order to decrease the number of these marine accidents, Korean ships are obliged to follow the AIS(Automatic Identification System) system. The AIS protocol includes all information for sailing ships. However, the standard AIS protocol does not provide any security function, In addition, it is possible to hijack the standard AIS protocol in case of using a satellite communication device called FUNcuve Dongle Pro+. Therefore, this paper analyzes weak points of the security in the standard AIS protocol. Furthermore, this paper ensures reliability by marking the MAC Address of sender and receiver for secure communication and suggests the protocol that can securely send data, using the VPN Tunnelling method. Therefore, the suggested AIS protocol provides the secure communication to the AIS protocol and protect the messages in the AIS protocol, which can serve safe voyages by decreasing the marine accidents

Key Words : Ship Network, Marine Accident, AIS Protocol, Weak points in AIS, Secure AIS Protocol

1. 서 론

컴퓨터기술의 발달로 컴퓨팅파워 및 계산능력은 급격히 증가하였으며, 유무선 네트워크기술과 여러 프로토콜의 등장으로 여러상황에서의 네트워크가 시간과 장소에 상관없이 실시간으로 가능하게 되었다.

특히, 우리나라는 삼면이 바다로 둘러싸인 지리적 특성으로 바다를 활용하는 해운항만산업이 크게 발전하였으며, 21세기 IT 시대로 들어서면서 해운항만 시스템 또한 IT 시스템 체계로 발전하였다. 하지만 해운항만산업이 발전함에 따라 불가피하게 해양 사고도 자주 발생하고 있다. 해양경찰청

This research is financially supported by Changwon National University in 2015~2016
* Corresponding Author : Department of Computer Engineering, Changwon National University(swchung@changwon.ac.kr)
Received February 2, 2016 Revised February 8, 2016 Accepted February 13, 2016

그림 1. 한국 남부지역 선박상태 예시
Fig. 1. Example of Southern Area's Ships

의 연도별 [해양 사고 발생 현황에 따르면 2010년 737건, 2011년 946건, 2012년 726건, 2013년 638건, 2014년 몽골 선적 화물선 침몰, 진도 세월호 여객선 침몰사고 등 많은 해양사고 건수가 발생하였음을 알 수 있다[1].

[그림1]에서 확인할 수 있듯이 우리나라 또한, 해양사고 발생 건수를 줄이기 위해 2005년 각국의 선박은 SOLAS(Safety of Life at Sea)에 따라 자동 원격 인식 신호 송수신이 가능한 시스템 AIS(Automatic Identification System)를 의무 장착하게 되었으며, 국내도 이를 채택하고 있다. AIS는 디지털 VHF 무선 트랜스폰더 시스템으로, 해당 시스템이 탑재된 선박은 어느 해역을 항해 중이던 선상의 누구에 의한 간섭 없이도 지속적인 상태로 운용될 수 있다.

AIS 시스템이란 항해를 하기 위한 정보들, 선박의 위치정보 등을 수·송신하는 시스템이다. 이러한 AIS 시스템 사용이 의무화되기 시작하면서 항해하기 위한 정보들, 선박의 정보들은 AIS 시스템에 모두 담겨 통신된다. 하지만 AIS 표준 프로토콜 프레임(Frame)에 대한 규칙이 존재하지 않는다. 따라서 표준 프로토콜 프레임에 대한 보안 기능 또한 규정되지 않는다. 즉, AIS 표준 프로토콜 프레임은 간단한 오류 점검(Checksum) 기능도 없기에 해킹 공격에 대해 많은 취약점을 가지게 된다. 또한, 무선통신 중 공중망을 지나가며, 누구나 The FUNcube Dongle Pro+ 위성통신 수신기로 손쉽게 AIS 무선 프로토콜 프레임을 Hijacking할 수 있었다. 이러한 취약점을 해결하기 위해 AIS 표준 프로토콜 프레임에 대한 연구가 반드시 필요하다.

본 논문에서는 선박이 항해할 때 필요한 모든 정보를 담고 있는 AIS 표준 프로토콜 프레임을 변형하여 송수신자의 MAC Address를 추가하고 데이터 안전성 보장을 위해 데이터 앞부분에 VPN tunneling기법을 사용해 데이터를 보안화하는 방법을 제안한다. 본 논문은 2장에서 해상교통관제서비스 시스템과 AIS 시스템에 대해 설명한다. 3장에서는 AIS 표준 프로토콜 프레임의 보안 취약점을 분석한다. 4장에서 AIS 표준 프로토콜 프레임의 취약점 해결을 위한 방안 제시한다. 5장에서 제시한 방안에 대해 검증 하고, 마지막으로 6장에서 결론을 맺는다.

2. 이론적 배경

2.1 해상교통관제서비스 시스템

해상교통관제 서비스(VTS) 시스템은 항만 및 연안해역 등 선박 교통량이 폭주하거나 항행 여건상 불리한 해역에서 운항 중인 선박에 대한 안전운항 및 준법 항행 여부를 감시하는 서비스이다. VTS 시스템은 필요하면 선박의 통항을 지도 관리, 항행 안전정보 제공을 통해 선박안전사고를 미리 방지함으로써 해상에서의 인명과 선박의 안전 및 해양 환경을 보호하기 위한 시스템이다.

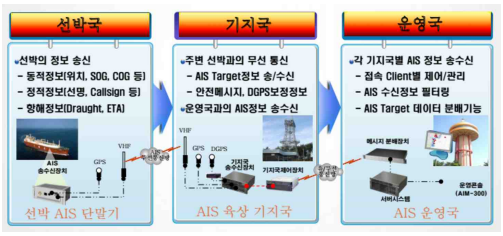

그림 2. AIS 선박 네트워크 시스템
Fig. 2. AIS Ship-Network System

[그림2[에서 확인할 수 있듯이 VTS 시스템은 과거 무선통신에만 의존하던 재래방식과는 달리 레이더, CCTV 등 첨단과학 감시 장비를 이용한다. 첨단 장비를 이용해 항만을 드나드는 선박들의

항로 이탈 여부·진행 방향·속력·선박 상호교차 시간 등 운항정보를 실시간으로 파악·제공한다. VTS 시스템은 항만 운영의 효율성을 향상하고 선박안전 확보를 위한 항만 서비스이다[2].

VTS는 넓은 의미로는 기존의 항로표지를 포함하는 것으로 등대, 등부표, 도등과 같은 항로표지는 VTS의 일종이라 할 수 있으나, 일반적인 좁은 의미로는 레이더에 의한 통항 선박 감시와 선박 통항의 조정 서비스 등을 의미한다. VTS를 설치하는 목적에 대해 IMO의 VTS 지침에는 일정한 수역에서의 항행 원조, VTS 수역에서 효율적인 교통 흐름을 조정하기 위한 선박 이동의 관리, 해당 선박에 관련된 자료의 취급, 사고 수습에 참여 및 관련된 활동에 대한 지원 등으로 규정하고 있다.

VTS 시스템은 해상 안전 및 항만 운영의 핵심 기능으로서 단순한 안전 수행 기능만이 아닌 선박 운항 데이터 수집, 해운·항만물류정보 서비스, 항해 지원 서비스, 동향 관리, 교통 조직 서비스, 기업 활동 예측성 부여, 기타 연관 활동 지원 등, 크게 선박 통항 관리기능(연안 VTS)과 항만 운영 기능(항만 VTS)으로 대변할 수 있다.

하지만 조선과 IT(정보통신)기술을 융합한 선박통합네트워크인 '스마트십'의 개발이 속도를 내면서 선박 정보보호에 대한 기술검토가 시급한 시점이다. 또한, 선박추적시스템(AIS)의 결함을 이용해 선박을 해킹하는 시연이 지난해 연말 블랙캣 해킹대회에서 시연되기도 했다.

2.2 AIS 시스템

AIS는 Automatic Identification System의 약자로, 자동 원격 인식 신호 송수신 시스템이다[3]. AIS 시스템이 탑재된 선박은 어느 해역을 항해 중이던 선상의 누구에 의한 간섭 없이도 지속적인 상태로 운용할 수 있다. 선박과 선박 간, 선박과 해안 기지국 간의 통신을 위해 해사용 이동 주파수대역 내의 2개 VHF 주파수 채널(87, 88)이 사용되고 있는데 각 채널은 9.600bps의 전송률을 가지며, 분당 2,250개의 정보 전송이 가능하다.

[그림3[에서 보면 AIS전체 구조는 매우 간단하다. AIS는 2개의 독립된 수신기와 1개의 송신기로 구성되어 있으며, 수신기는 2개의 채널에서 동시에 정보를 수신한다. GPS 수신기는 정확한 시간, 선박 위치, 항해 데이터를 전송하며, 선박용 AIS의 통신 프로세서는 이들 정보를 방위계 등 선박 센서로부터의 데이터 및 선명, 호출부호 등의 정적 자료, 항해 관련 자료 등을 함께 송신하고 있다. 관제센터에서는 육상 기지국으로부터 정보를 수신하여 모니터에 표시하여 관리한다.

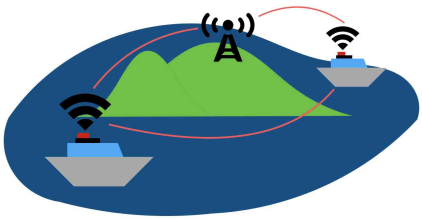

그림 3. AIS Network 구조
Fig. 3. Structure of AIS Networks

우리나라는 2002년 7월부터 모든 신규 여객선과 총톤수 300톤 이상의 화물선에는 AIS 장착이 의무화되었다(선박안전법 시행규칙 제 73조). 즉, 우리나라 선박 정보는 AIS 시스템에 선박의 정보 및 항해하기 위한 정보가 모두 담겨 통신하게 되어있다. 선박의 모든 정보가 담겨 통신하기 때문에 별도의 보안기능이 반드시 필요하지만, AIS 표준 프로토콜 프레임에 보안 기능은 존재하지 않는다. 따라서 AIS 표준 프로토콜 프레임에 대한 지식이 있다면, 다양한 해킹 공격을 할 수 있다.

2.3 기존 AIS 연구 차이점

[4][5]에서는 AIS를 활용하여 선박 위치를 찾아내는 알고리즘을 구현하였다. 하지만, AIS정보를 활용하여 선박을 위치를 찾아내지만 정보를 찾는 동안 생겨나는 취약점 상태는 다루지 않고 있다. 그래서 본 논문에서는 AIS정보를 수집하는 단계, 송

신하는 단계에서 생겨나는 보안 취약점에 대해서 구체적으로 다룬다.

3. AIS 표준 프로토콜 프레임 취약점 분석

3.1 통신과정에서의 데이터 노출 취약점

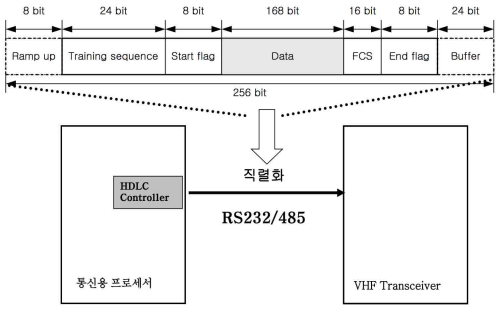

그림 4. 보안 기능 없는 AIS 구조
Fig. 4. AIS Structure without Security

AIS 프로토콜 프레임은 선박을 VHF 송·수신 장치에서 기지국 VHF 송·수신 장치로 AIS 무선 통신을 하게 된다. 무선 통신 데이터에는 선박의 동적정보, 정적정보, 항해정보 등 선박이 항해하는데 필요한 정보를 모두 송신을 하게 된다. 하지만 [그림4]에서 확인할 수 있듯이 보안장치가 없어 The FUNcube Dongle Pro+ 위성통신 수신기를 사용하면, 무선통신 중 공중망을 지나가며 손쉽게 AIS무선 프로토콜 프레임을 Hijacking 할 수 있다.

3.2 프로토콜 프레임 구조 취약점

[그림 5]는 현재 해상교통관제센터에서 통신하는 AIS 표준 프로토콜 프레임이다. [그림 6]는 현재 네트워크 계층에서 사용되는 표준 IP 프로토콜 프레임이다. [그림 5]의 AIS 표준 프로토콜 프레임은 매우 간단하게 프로토콜 프레임이 형상화되어 있다. 하지만 [그림 6] IP프로토콜 프레임은 송신지와 수신지 표시로 신뢰성을 주며, 헤더 오류 점검 기능으로 전송 중에 발생한 오류의 존재 여부를 수신 측이 알 수 있도록 전해준다. 반면에 AIS 표준 프로토콜 프레임은 헤더 오류 점검 기능과 송·수신자의 정보가 담긴 데이터가 없다. 그러므로 해커는 프록시(Proxy) 서버를 이용하여 AIS 프로토콜 프레임 데이터안에 송신지 배위치, 동적정보 및 정적정보에 접근 후 변조할 수 있다. 만일 해커가 위 정보를 변조 하여도 프로토콜 프레임 구조상 수신 측에서 변조 여부를 알 수 있는 방법은 없다.

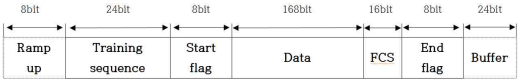

그림 5. AIS 표준 프로토콜 프레임
Fig. 5. AIS Standard Protocols Frame

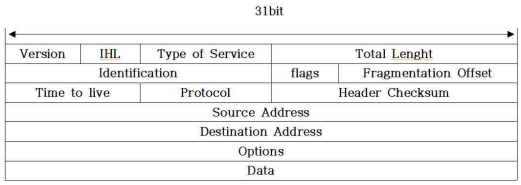

그림 6. IP 프로토콜 프레임
Fig. 6. IP Protocol Frame

3.3 AIS 표준 프로토콜 프레임 전송 흐름

AIS 프로토콜 프레임은 전원 인가 후, 1분 동안 수신하여 프레임 지도를 완성한다. 그 후 4가지의 채널 접속 프로토콜 프레임을 결정하게 된다. 기본으로 SOTDMA 프로토콜 프레임을 사용하지만 필요에 따라 프로토콜 프레임 변경이 가능하다. 메시지 전송은 주기에 따라 전송을 하는데 정적, 동적, 항해관련, 안전 관련으로 나누어 전송한다[6]. AIS Protocol는 기존의 네트워크 통신과 같이 Network Layer 방식과 동일하게 통신한다. 1Layer에서는 Bit-Stream의 전송 담당하며, 2Layer에서는 MAC(Media Access Control) 데이터링크에 접속하는 방법, DLS(Data Link Service) 데이터링크 activation과 release, 데이터 전송, 감지, 제어 방법, LME(Link Management Entity) : 물리계층, DLS, MAC 관리, 3Layer는 채널 연결 시도와 유지, 채널갂 패킷 분배, 데이터링크 정체 해결, 마지막으로 데이터를 젂송 패킷의 정확한 크기로 젂홖, 데이터 패킷의 순서화, 상위 계층의 인터페이스 프

로토콜 수행한다.

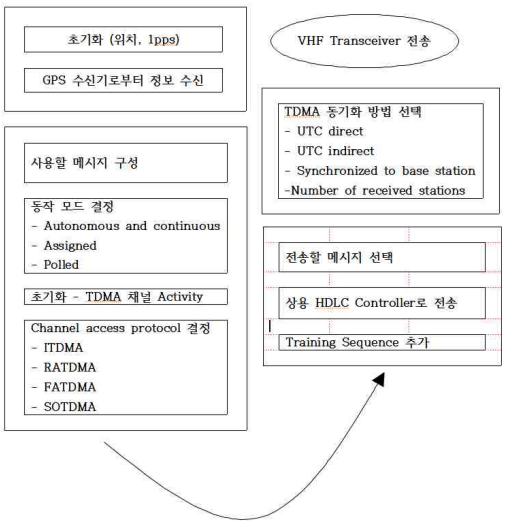

그림 7. AIS 데이터 흐름 정의
Fig. 7. AIS Data flow definition

채널 접속 프로토콜 프레임 4종류

1. ITDMA(Increment TDMA)

데이터 링크 진입 시, 보고 속도 변경 시, 안전 관련 메시지 공표 시 사용

2. RATDMA(Random Access TDMA)

데이터 링크 진입 시, 첫 전송 슬롯 전송 시, 비반복적 문자 전송 시 사용

3. FATDMA(Fixed Access TDMA)

Base와 Control Station이 반복적인 메시지를 전송할 때 사용

4. SOTDMA(Self-Organized TDMA)

Autonomous와 Continuous 모드 동작 시, 채널 충돌 해결, 반복적인 문자 전송, 채널 상태 확인 가능

위와 같은 4가지의 방법으로 채널에 접속하게 된다.

3.4 취약점 분석 결과

AIS 표준 프로토콜 프레임에는 송·수신 오류 점검 기능이 내포되지 않아 수신한 값이 올바른 값인지 확인할 수 없었다. 또한, The FUNcube Dongle Pro+ 위성통신 수신기만 있다면 AIS 무선통신을 Hijacking 할 수 있는 취약점을 발견하였다. 또한, AIS 무선통신은 통신 과정 중 보안화 작업이 이루어지지 않아 누구나 쉽게 위조 및 변조를 할 수 있었다. 즉 AIS 프로토콜 프레임은 인증 절차 및 데이터 유효성 및 신뢰성 검증이 매우 부족한 상태로 드러났다.

4. 보안 AIS 시스템 제안

4.1 VPN Tunnelling 기법

VPN(Virtual Private Network)은 공중 네트워크를 통해 회사 및 단체에서 사용하는 내용을 외부 사람에게 드러내지 않고 통신할 목적으로 쓰이는 사설 통신망이다[7]. VPN을 구성하면서 가장 중요한 핵심 기술이 Tunnelling 기술이다. 공용 네트워크를 사용하면 Hijacking 및 패킷 위·변조가 발생할 수 있다. Tunnelling은 이런 문제를 해결해 줄 수 있는 기술로 종단간 통신 경로를 캡슐링과 인캡슐링 과정을 통해 논리적인 단일망으로 연결시켜주는 역할을 한다. Tunnelling 프로토콜 프레임에는 PPTP, VTP, L2F, L2TP, IPSec 등이 있다. VTP, L2F 프로토콜 프레임은 하드웨어에 지나치게 의존하기 때문에 독자적인 망으로 VPN 서비스를 제공하려는 서비스 제공업자에게 적합한 방식이며, 암호화를 이용해 데이터를 보호하는 방법에는 PPTP, IPSec, DES 등의 프로토콜 프레임을 사용한다[8]. VPN Tunneling에서는 기존의 사설망 VPN기법과 망 보안 Tunnelling기법을 적용한 개념이다.

4.2 보안 AIS 시스템 제안

데이터에 대한 신뢰성을 유지하기 위해 [그림 8]와 같이 데이터 앞부분에 VPN Tunnelling을 적용하였다. 기존 AIS 표준 프로토콜 프레임은 별도의 인증 절차 없이 데이터에 접근을 허용 하였지만, VPN Tunnelling이라는 하나의 인증 절차를 두어 기지국에서 조금 더 신뢰 있는 정보를 받아

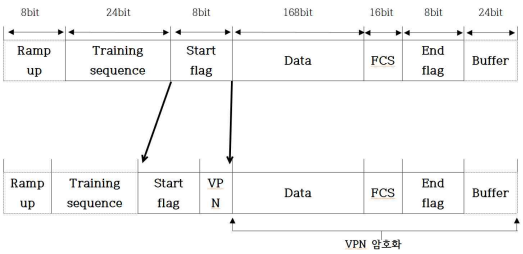

그림 8. VPN 적용한 AIS 프로토콜 프레임
Fig. 8. VPN protocols applied AIS frame

볼 수 있게 된다. 또한 [그림 9]와 같이 Sequence Number 앞에 송·수신자의 MAC Address를 추가함으로써 기존의 표준 AIS 프로토콜 프레임과 달리 제안하는 AIS 프로토콜 프레임 구조는 선박이 실제 존재하는지에 대한 신뢰성을 높여 줌으로 선박에 대한 관리와 신뢰성을 높여주는 선박 관리 시스템을 운영할 수 있다.

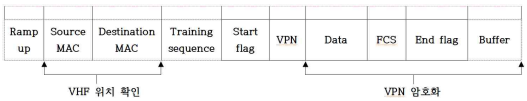

그림 9. 제안하는 AIS 프로토콜 프레임 구조
Fig. 9. AIS frame structure protocol to offer

4.3 시스템 보안목적 도출

AIS 표준 프로토콜 프레임은 위·변조가 용이하였다. 또한, 송·수신지가 불문 명해 D·Dos공격에 취약하였다. 기존의 AIS 장치에는 정상적인 신호를 체크할 수 있는 기능이 없어 모든 AIS송신 신호를 정상적인 신호로 측정한다. 그래서 제안하는 시스템에서는 기존의 공중망 Hijacking기술의 방어 체계로 Tunneling 기법을 AIS 통신 체계에 접목 시키며, 송신자와 수신자의 신뢰성을 대표적으로 지킬 수 있는 기술 MAC을 기지국 데이터에 저장함으로 문제점 해결 방안을 구상하였다. 공격적으로는 송신자·수신자 MAC을 기지국에 저장시켜 전송하여 D·Dos공격을 차단하고, 선박과 기지국 간의 데이터 전송에 대한 안정성을 높여준다. 또한, VPN Tunnelling 기법을 AIS 표준 프로토콜 프레임에 적용함으로 AIS 표준 프로토콜 프레임에 적용함으로써 전송되는 데이터에 접근을 어렵게 하고 해커가 Hijacking 공격을 하였을 때도 보안화가 되어있어, 데이터를 보호할 수 있다.

5. 검증결과

5.1 시뮬레이션 실험 환경

[표 1]은 제안하는 시스템을 검증하기 위해 가상 시뮬레이션 환경이다. [표 1]의 Computer OS, 수신기, 송신지, MAC Address 모두 해커의 시뮬레이션 환경이다. 해커는 The FUNcuve Dongle Pro+ 수신기를 이용하여 공중망에서 선박과 기지국간에 주고받는 정보를 Hijacking 하는 도구이다. 송신기는 해커가 가상의 패킷을 만들어 선박 또는 기지국에 보낼 때 사용한다. MAC Address는 수신측에서 보관하며 매칭 데이터로 사용된다.

표 1. 시뮬레이션 실험환경
Table 1. Experimental Environments for Simulations

Factor	Value
Computer OS	Windows Sever 2008
수신기	The FUNcuve Dongle Pro+
송신기	광대역/HAM/370~970MHz /28소/20MM
MAC Address	BC-5F-F4-5B-44-2C

5.2 VPN Tunnelling 기법 적용 검증

기존의 AIS 표준 프로토콜 프레임은 데이터에 대한 신뢰성을 유지하지 못한다. 해커가 공중망 Hijacking을 통해 패킷을 분석할 경우 복호화와 같은 절차 없이 데이터에 손쉽게 접근할 수 있기 때문이다. 이러한 접근은 데이터의 위·변조가 용이하였다.

첫 번째 제안하는 AIS 프로토콜 프레임은 데이터의 앞부분에 VPN Tunnelling 기법을 적용하여 해커가 공중망 Hijacking으로 데이터을 가로채내어도 데이터에 대한 정보를 알아보지 못하도록 보안화하였다. 그 결과 해커가 패킷에 접근하였을 경우

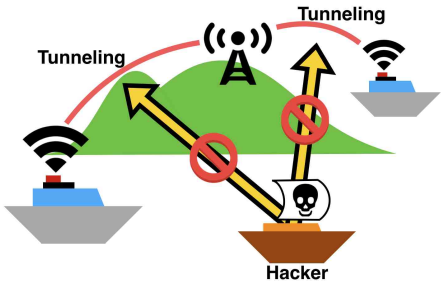

그림 10. Tunneling 기법
Fig. 10. Tunneling Method

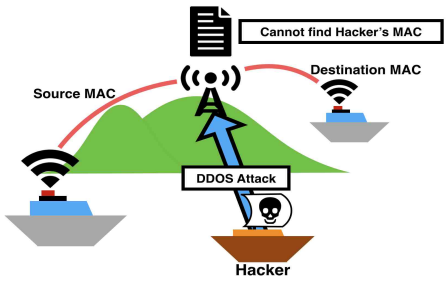

그림 11. MAC 검증 기법
Fig. 11. MAC Verification Method

VPN 패킷 내의 데이터에 대한 정보를 올바르게 볼 수 없다는 것을 확인 하였다. [표 2]는 표준 AIS 프로토콜 프레임, VPN IP프로토콜 프레임, 제안하는 AIS 프로토콜에 대한 비교 검증 결과이다. 검증 결과, 제안하는 AIS 프로토콜 프레임은 D·Dos 공격, Hijacking 공격, 위조 및 변조 공격이 불가능함을 확인 할 수 있다. 또한 위험도도 기존의 AIS 표준 프로토콜 프레임에 비해서는 낮아졌다. 데이터 앞부분에 VPN Tunnelling을 적용함으로써 보안화되어 신뢰성이 높아짐을 확인할 수 있다. 또한, VPN 패킷 안에는 TTL(Time to live)이 적용되어 해커가 프로토콜 프레임을 변조하였을 때 기지국까지 올바르게 전달되지 않는 것을 확인할 수 있었다. 그 이유는 Hacker의 중간자 역할로 인해 TTL 시간이 1이 감소하여 기지국까지 TTL시간이 부족한 현상을 겪게 된다. 그로 인해 정상적인 통신이 불가능해 지는 현상을 확인 할 수 있었다.

5.3 송·수신지 표시 검증

AIS 표준 프로토콜 프레임에 Training sequence 앞부분에 송신자 MAC, 목적지 MAC Adress 값을 추가하여 전송함으로써 송신자와 수신자 간의 신뢰성을 확보할 수 있었다. 송신자 IP와 목적지IP값을 적용하였을 때에는 선박에 대한 고유 IP값을 확인할 수 없었으며, 대역폭이 넓어 IP 필터링 시스템을 적용하기에는 어려운 점이 있었다. 또한, 선박 간에 내부 IP를 사용한 경우에는 기지국에서 해당 IP의 주인을 판단하는 근거가 모호한 상태이다. 그러므로 기존의 AIS 표준 프로토콜 프레임과 똑같이 동적·정적 정보로 판단하여야 했다. 하지만 기지국 장비와 선박의 MAC Address 매칭 시스템을 이용하면 VHF 장비의 MAC Address를 통해 송·수신지에 대한 신뢰성이 유지되는 것을 확인할 수 있었다. 기지국에서 MAC Address를 관리·통제하며 선박과 기지국 장비의 지속적인 MAC Address 업데이트 및 확인 작업을 한다면, 기존의 AIS 표준 프로토콜 프레임보다 정보의 송·수신자에 대한 신뢰성 확보가 쉬워짐을 확인할 수 있었다.

표 2. 기존 프로토콜 프레임과 비교 검증
Table 2. Comparison of Existing Protocols and Suggested Protocol

프로토콜 분류	표준 AIS	VPN IP	제안 AIS
D·Dos	가능	가능	불가능
Hijacking	가능	불가능	불가능
위조·변조	가능	불가능	불가능
위험도	높음	중간	낮음
신뢰성	하	중	상

2가지 제안한 보안 기법은 표준 AIS의 문제점인 신뢰성 부족과, 해커의 Hijacking 문제점을 보안할 수 있는 방법을 위에서 제시한 내용이다. 기존 연구 환경에서 수신기 The FUNcuve Dongle Pro+에서 VPN Tunnelling을 통한 보안 기법은 패킷 수신은 가능하나 TTL부분을 통해 재대로 해석

하기가 싶지 않은 상태였다. 또한, MAC 주소를 통해 송신자정보와 수신자 정보를 데이터화 시켜 기존에 저장된 정보가 아닌 주소는 Loss 시키는 방법으로 수신자측은 표준 AIS보다 높아졌다.

6. 결론

최근 주목받고 있는 항만 시스템 중 하나인 AIS 표준 프로토콜은 일반적인 선박네트워크의 특성상 보안문제에 취약성이 있는 프로토콜이다. 본 논문에서는 이러한 AIS 표준 프로토콜 프레임에 대한 취약점을 분석하였다. 그 결과 항만 시스템은 D·Dos, Hijacking을 통한 위·변조 공격에 매우 취약한 것으로 드러났다. 이에 따라 본 논문에서는 위와 같은 문제점을 인지하고 AIS 표준 프로토콜 프레임에 보안 기능을 추가하여 신뢰성 있는 프로토콜 프레임 구조를 제안하였다. 제안한 2가지의 기능 중 첫 번째 기능인 VPN Tunnelling 기능은 데이터에 대한 접근 제한 및 신뢰성 유지가 가능토록 하였으며 두 번째, 송·수신지 확인을 위한 MAC Address에 대한 정보를 추가함으로 기존의 AIS 표준 프로토콜 프레임에 더욱 신뢰성 있는 프로토콜 프레임으로 발전하였다.

그러나 표준 AIS 프로토콜은 현재 누구나 쉽게 해킹이 가능한 상태이다. 본 논문에서는 표준 AIS 프로토콜에 VPN 기법을 적용하여 상대적으로 해킹위험이 줄어드는 것을 확인하였고 본 논문이 제안한 AIS 프로토콜은 더욱 해킹 보안성이 우수함을 보여주었다. 또한, 이러한 AIS 표준 프로토콜 프레임에 대한 분석 및 기술 개발은 앞으로의 VHF 송신기 개발, AIS 프로토콜 프레임 분석, 채널 접속 알고리즘으로 확장될 수 있으리라 예측된다.

현재 우리나라의 선박 시스템은 매우 중요한 경제발전에 기여하고 있다. 하지만 제대로 된 선박 운영에 대한 매뉴얼과 안전한 선박과의 통신을 위한 정책이 없다면 선박 사고는 끊임없이 발생할 것이다. 선박 사고를 줄이기 위해서는 우리나라 선박에 대한 엄격한 규제와 안전한 항해를 위한 정확한 데이터가 반드시 필요하다. 그렇기에 이러한 정보를 수집하여 송·수신하는 AIS 표준 프로토콜 프레임에 대한 보안은 중요한 문제로 대두할 것으로 생각한다. AIS 표준 프로토콜 프레임의 발전은 우리나라의 선박 안전 시스템에 크게 기여 할 것이며, 이를 통해 우리나라에 항만 경제 발전에도 큰 기여를 할 것으로 기대된다.

REFERENCES

[1]e-Country index(Statistical Office) “Marine accident statistics”, http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1770.

[2] Seeung-Geun Kim, Changho Yun, Sea-Moon Kim, Yong-Kon Lim, “BaseBand Receiver Design for Maritime VHF Digital Communications”, 「KICS」, v36권 no8 (2012), pp.438-449.

[3] M-J Kim, S-B Hong, “The Future Prospect of the Vessel Traffic Safety Management in View of Developing AIS Network in Korea ”, 「Journal of the Korea Marine Authority」, V25 no4(2001), pp.735-746.

[4] Seo Jeong Lee, In Hwan Park, ‘Database Design and Implementation for Vessel AIS Information Application’ Div. of IT, Korea Maritime University, Pusan 606-791, Korea, pp. 343～348

[5] Jung-Sik Jeong, Won-Jae Yang, “A Study on the Enhancement of Utilization of Automatic Identification System”, 「Marine Environmet & Safety」, v9 no2(2003), pp.15-21.

[6] Min-ho Seo, Geonung Kim, “Vessel Positional Information Service using AIS and XML ”, 「Korea Institute of Information and Communication Engineering」, v15 no12(2011), pp.2590-2598.

[7] Moon H Kang, Tai M Chung, “VPN(Virtual Private Network) Overview of technology”, 「KIISC review / v.9 no.4,(1999), pp.3-10.
[8] Jung-Tae Kim, “Design of High-speed VPN System for Network Processor with Embedded Crypto-module”, 「Kiice」, v11 no5(2007), pp.926-932.

저자약력

이 정 수 (Jung-Su Lee) [정회원]

- 2016년 2월 : 창원대학교 컴퓨터공학과 (컴퓨터공학사)

<관심분야> 정보통신, 정보보안, 네트워크

허 욱 (Ouk Heo) [정회원]

- 2016년 2월 : 창원대학교 컴퓨터공학과 (컴퓨터공학사)

<관심분야> 정보경영, 정보통신, 시스템

김 재 환 (Jae-Hwan Kim) [정회원]

- 2011년 2월 : 창원대학교 컴퓨터공학과 (컴퓨터공학사)

<관심분야> 정보보안, 정보통신, 프로토콜

정 성 욱 (Sung-Wook Chung) [정회원]

- 2005년 5월 : CISE dept. Univ. of Florida, USA, (MS)
- 2010년 8월 : CISE dept. Univ. of Florida, USA, (Ph.D)
- 2010년 10월 ~ 2012년 2월 : KT 종합기술원 중앙연구소 선임연구원
- 2012년 3월 ~ 현재 : 창원대학교 컴퓨터공학과 조교수

<관심분야> 분산멀티미디어시스템, 홈네트워크