

명세서

발명의 명칭: 선박 NMEA 프로토콜 기반 침투 테스트 방법 및 장치, 그리고 선박 내부에서 CBS의 접속을 제어하는 방법 및 장치 기술분야

- [1] 본 발명은 선박의 특수성을 고려하여 선박 내에서 사용되는 NMEA(National Marine Electronics Association) 프로토콜을 위한 침투 테스트(penetration test)를 수행할 수 있고, 선박 내부의 항해, 통신, 추진 등의 제어 시스템에 접속하는 CBS의 블루투스, GPS, WiFi 등 무선 통신 기능을 활용하여 복수의 선박 장치들을 인증할 수 있는 선박 NMEA 프로토콜 기반 침투 테스트 방법 및 장치, 그리고 선박 내부에서 CBS의 접속을 제어하는 방법 및 장치에 관한 것이다.

배경기술

- [2] 조선해양산업에 ICT 기술이 융합되면서 선박에 대한 사이버 위험 또한 증가했다. 이에 따라 국제기구에서 사이버 보안 요구 사항을 제시했고, 그 중 IACS는 보안 요구 사항에 대한 테스트를 요구하고 있다. 하지만, 테스트에 대한 구체적인 방법은 제시되지 않는다.
- [3] 침투 테스트(Penetration Test)는 시스템의 보안 평가를 위한 시뮬레이션 사이버 공격이다. 육상에서의 Penetration Test는 웹, 정보 시스템, 모바일 등 ICT 시스템과 스마트 팩토리 등 OT 시스템을 대상으로 한다. 자동차의 경우, 자동차에서 사용하는 특수 프로토콜인 CAN 프로토콜을 위한 침투 테스트(Penetration Test) 방법이 있다.
- [4] 그러나 현재까지는 선박을 위한 침투 테스트 방법이 없으며, 선박을 대상으로 침투 테스트를 수행하기 위해서는 선박에서 사용하는 특수한 네트워크 환경을 고려해야 한다. 따라서 육상에서의 침투 테스트 방법은 선박의 특수성이 반영되지 않는다는 점에서 한계가 존재하는 문제점이 있다.
- [5] 또한, 선박 CBS란 선박 내에서 사용/설치되는 컴퓨터 기반 시스템(Computer Based System)으로 정의한다.
- [6] 일반적으로 CBS는 승선한 선장, 선원이 사용하는 모바일앱, 태블릿PC, 노트북, PC 등의 단말을 포함하고, 선박에 설치되는 전자해도시스템, 통합항해시스템 등 항해, 통신 시스템을 포함한다.
- [7] CBS는 ID와 비밀번호를 입력하고 사전에 정의된 인증자 데이터베이스에서 두 정보가 모두 확인되는 경우 인가된 사용자임을 확인한다.
- [8] 그러나 ID, 비밀번호가 해킹, 악성코드 등 그 밖의 방법으로 노출된 경우 선박 내부에서 사용되는 항해, 통신, 제어 장치에 접속하는 행위를 방지할 방안이 없다는 문제점이 있었다.
- [9] 관련 선행문헌으로는, 대한민국 등록특허 제10-0694248호(2007.03.27.), 대한민국 등록특허 제10-2328275호(2021.11.17.)이 공개되어 있다.

발명의 상세한 설명

기술적 과제

- [10] 본 발명의 목적은 선박 내부에서 NMEA 프로토콜에 대한 침투 테스트를 수행할 수 있으며, 장치를 통해 간단하고 빠르게 NMEA 침투 테스트를 수행할 수 있는, 선박 NMEA 프로토콜 기반 침투 테스트 방법 및 장치를 제공하는 것을 목적으로 한다.
- [11] 본 발명의 다른 목적은 선박의 운항관리, 항해관리 등 선박 내부에서 인가된 선원 및 시스템에 한해 접속되어야 하는 중요 시스템을 식별하여 원격지에서의 사이버공격을 예방할 수 있도록 하는 선박 내부에서 CBS의 접속을 제어하는 방법 및 장치를 제공하는 것을 목적으로 한다.

과제 해결 수단

- [12] 상기 기술적 과제를 달성하기 위한 본 발명의 일 측면에 따른 선박 NMEA 프로토콜 기반 침투 테스트 방법은, 침투 테스트 장치를 선박 네트워크 중 선박 제어 네트워크에 연결하는 네트워크 연결 단계; 및 상기 네트워크 연결 단계를 통해 연결된 네트워크를 침투 테스트 장치의 확인부에서 패킷 캡처와 패킷 분석을 통해 NMEA 문장 구조 형식 및 특징을 추출하여 NMEA 통신 구간인지 확인하는 확인 단계를 포함하며; 상기 확인 단계를 통해 NMEA 통신 구간인 경우, 침투 테스트 장치의 공격 방법 선택부에서 공격 방법을 선택하는 공격 방법 선택 단계; 상기 공격 방법 선택 단계를 통해 선택된 공격 데이터를 생성하는 공격 데이터 생성 단계; 상기 공격 데이터 생성 단계를 통해 생성된 공격 데이터와 공격이 수행되는 시간 동안의 네트워크 패킷을 저장하는 공격 데이터 저장 단계; 상기 공격 데이터 저장 단계를 통해 저장된 공격 데이터와 공격이 수행되는 시간 동안의 네트워크 패킷을 선박 네트워크로 전송하는 공격 데이터 전송 단계; 및 상기 공격 데이터 전송 단계를 통해 전송된 공격 데이터를 분석하는 공격 데이터 분석 단계를 포함하여 침투 테스트를 수행할 수 있다.
- [13] 또한, 본 발명의 일 측면에 따른 선박 NMEA 프로토콜 기반 침투 테스트 방법은, 상기 공격 방법 선택 단계에서, 상기 공격 방법은, 위조 NMEA 데이터 전송, 리플레이(replay) 공격 및 서비스 거부 공격 중 어느 하나를 선택할 수 있다.
- [14] 본 발명의 일 측면에 따른 선박 NMEA 프로토콜 기반 침투 테스트 방법은, 상기 공격 방법 선택 단계에서, 상기 공격 방법은 새로운 공격 방법의 업데이트가 가능하다.
- [15] 또한, 본 발명의 일 측면에 따른 선박 NMEA 프로토콜 기반 침투 테스트 방법에서, 상기 공격 데이터 분석 단계는, 전송된 NMEA 공격 데이터의 양과 전송 시간을 분석하고 테스트 결과를 획득할 수 있다.
- [16] 또한, 본 발명의 다른 측면에 따른 선박 NMEA 프로토콜 기반 침투 테스트 장치는, 선박 제어 네트워크에 연결하여 침투 테스트를 수행하는 침투 테스트 장치에 있어서, 네트워크를 패킷 캡처와 패킷 분석을 통해 NMEA 문장 구조 형식

및 특징을 추출하여 NMEA 통신 구간인지 확인하는 확인부; 상기 확인부를 통해 NMEA 통신 구간인 경우, 침투 테스트 장치가 공격 방법을 선택하는 공격 방법 선택부; 상기 공격 방법 선택부를 통해 선택된 공격 데이터를 생성하는 공격 데이터 생성부; 상기 공격 데이터 생성 단계를 통해 생성된 공격 데이터와 공격이 수행되는 시간 동안의 네트워크 패킷을 저장하는 공격 데이터 저장부; 상기 공격 데이터 저장부를 통해 저장된 공격 데이터와 공격이 수행되는 시간 동안의 네트워크 패킷을 선박 네트워크로 전송하는 공격 데이터 전송부; 및 상기 공격 데이터 전송부를 통해 전송된 공격 데이터를 분석하는 공격 데이터 분석부를 포함하여 침투 테스트를 수행할 수 있다.

- [17] 또한, 본 발명의 일 측면에 따른 선박 NMEA 프로토콜 기반 침투 테스트 장치는, 상기 공격 방법 선택부에서, 상기 공격 방법은, 위조 NMEA 데이터 전송, 리플레이(replay) 공격 및 서비스 거부 공격 중 어느 하나를 선택할 수 있다.
- [18] 또한, 본 발명의 일 측면에 따른 선박 NMEA 프로토콜 기반 침투 테스트 장치는, 상기 공격 방법 선택부에서, 상기 공격 방법은 새로운 공격 방법의 업데이트가 가능하다.
- [19] 또한, 본 발명의 일 측면에 따른 선박 NMEA 프로토콜 기반 침투 테스트 장치는, 상기 공격 데이터 분석부는, 전송된 NMEA 공격 데이터의 양과 전송 시간을 분석하고 테스트 결과를 획득할 수 있다.
- [20] 또한, 상기 기술적 과제를 달성하기 위한 본 발명의 다른 측면에 따른 선박 내부에서 CBS의 접속을 제어하는 장치는, 선박 내부의 항해, 통신, 추진 등의 제어 시스템에 ID와 비밀번호를 인증하고 통신부를 통해 로그인 하는 CBS(Computer Based System); 상기 CBS의 로그인 또는 구동 시 위치정보를 송신하는 비콘송신기; 상기 비콘송신기로부터 위치 정보를 수신하여 상기 CBS의 장치 정보가 등록되어 있는 정보와 일치하는지 확인하는 비콘 관리서버; 상기 비콘 관리서버에서 확인 시 비콘 정보의 사각지대에 위치하는 경우 CBS는 GPS 정보를 위치확인부에 전송하고, 위치확인부에서 수신된 GPS 정보와 AIS 데이터베이스를 비교하는 항해정보 확인부; 및 상기 비콘 관리서버 또는 항해정보 확인부를 통해 정보가 일치하는 경우 본선 내부의 시스템으로 연결되도록 제어하는 인증부를 포함하여, 선박 내부에서 CBS의 접속을 제어할 수 있다.
- [21] 또한, 본 발명의 다른 측면에 따른 선박 내부에서 CBS의 접속을 제어하는 장치에서, 상기 인증부는, CBS가 선박내부에 설치된 비콘 메시지를 수신하는 경우 또는 CBS의 위치정보가 항해경로와 일치하는 경우 본선 내부의 시스템으로 연결되도록 제어하는 것을 특징으로 한다.
- [22] 또한, 본 발명의 또 다른 측면에 따른 선박 내부에서 CBS의 접속을 제어하는 방법은, 선박 내부의 항해, 통신, 추진 등의 제어 시스템에 ID와 비밀번호를 인증하고 통신부를 통해 CBS(Computer Based System)를 로그인 하는 로그인 단계; 상기 로그인 단계를 통해 CBS의 로그인 또는 구동 시 위치정보를 비콘송신기를 통해 송신하는 위치정보 송신 단계; 상기 위치정보 송신 단계를 통해 비콘송신기로부터

터 위치 정보를 수신하여 상기 CBS의 장치 정보가 비콘 관리서버에 등록되어 있는 정보와 일치하는지 확인하는 비교 판단 단계; 상기 비교 판단 단계에서, 상기 비콘 정보가 확인되지 않는 비콘 정보의 사각지대에 위치하는 경우 CBS는 GPS 정보를 위치확인부에 전송하고, 위치확인부에서 수신된 GPS 정보와 AIS 데이터베이스를 항해정보 확인부에서 비교하는 항해정보 확인 단계; 및 상기 비교 판단 단계 또는 항해정보 확인 단계를 통해 정보가 일치하는 경우 본선 내부의 시스템으로 연결되도록 인증부를 통해 제어하는 인증 단계를 포함하여, 선박 내부에서 CBS의 접속을 제어할 수 있다.

- [23] 또한, 본 발명의 또 다른 측면에 따른 선박 내부에서 CBS의 접속을 제어하는 방법에서, 상기 인증 단계는, CBS가 선박내부에 설치된 비콘 메시지를 수신하는 경우 또는 CBS의 위치정보가 항해경로와 일치하는 경우 본선 내부의 시스템으로 연결되도록 제어하는 것을 특징으로 한다.

발명의 효과

- [24] 본 발명에 따르면, 선박 내부에서 NMEA 프로토콜에 대한 침투 테스트를 수행할 수 있으며, 장치를 통해 간단하고 빠르게 NMEA 침투 테스트를 수행할 수 있는 효과를 갖는다.
- [25] 또한, 본 발명에 따르면 선박의 운항관리, 항해관리 등 선박 내부에서 인가된 선원 단말기 및 시스템에 한해 접속되어야 하는 중요 시스템을 식별하여 원격지에서의 사이버공격을 예방할 수 있도록 하는 효과를 갖는다.

도면의 간단한 설명

- [26] 도 1은 본 발명에 따른 선박 NMEA 프로토콜 기반 침투 테스트 장치가 사용되는 네트워크 분류를 나타내는 블록 구성도이다.
- [27] 도 2는 본 발명에 따른 선박 NMEA 프로토콜 기반 침투 테스트 방법의 흐름을 나타내는 순서도이다.
- [28] 도 3은 본 발명의 실시예에 따른 선박 내부에서 CBS의 접속을 제어하는 장치의 구성을 나타내는 도면이다.
- [29] 도 4는 본 발명의 실시예에 따른 선박 내부에서 CBS의 접속을 제어하는 방법의 흐름을 나타내는 순서도이다.

발명의 실시를 위한 형태

- [30] 본 발명의 목적과 기술적 구성 및 그에 따른 작용 및 효과에 관한 자세한 사항은 본 발명의 명세서에 첨부된 도면에 의거한 상세한 설명에 의해 보다 명확하게 이해될 것이다.
- [31] 본 명세서에서 사용되는 용어는 단지 특정한 실시예를 설명하기 위해 사용되는 것으로 본 발명을 한정하려는 의도가 아니다. 예컨대, 본 명세서에서 사용되는 '구성된다' 또는 '포함한다' 등의 용어는 발명에 기재된 여러 구성요소들 또는 여러 단계들을 반드시 모두 포함하는 것으로 해석되지 않아야 하며, 그 중 일부 구성요소들 또는 일부 단계들을 포함하지 않거나 또는 추가적인 구성요소들 또

는 단계들을 더 포함할 수 있는 것으로 해석되어야 한다. 또한, 본 명세서에서 사용되는 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한 복수의 표현을 포함한다.

- [32] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 설명함으로써 본 발명을 상세히 설명한다. 이하에서 설명되는 실시예들은 본 발명의 기술사상을 당업자가 용이하게 이해할 수 있도록 제공되는 것으로서, 이에 의해 본 발명이 한정되는 것으로 해석되어서는 안되며, 본 발명의 실시예들은 이 분야의 통상의 기술자에게 다양한 응용을 가질 수 있음은 당연하다.
- [33] 본 발명에 따른 선박 NMEA(National Marine Electronics Association) 프로토콜 기반 침투 테스트 장치(20)는, 도 1을 참조하면, 선박 네트워크(10)에 연결될 수 있으며, 선박 네트워크(10)는 관리 네트워크(11)와 선박 제어 네트워크(12)와 기구 네트워크(13) 및 전용 연결(14)을 포함할 수 있다.
- [34] 이때, 침투 테스트(Penetration Test) 장치(20)는 선박 제어 네트워크(12)에 연결되어 선박 내에 사용되는 네트워크가 NMEA 통신 구간인지 확인할 수 있다.
- [35] NMEA라고 주로 불리는 NMEA 프로토콜은 시간, 위치, 방위 등의 정보를 전송하기 위한 규격이다.
- [36] NMEA 프로토콜은 미국의 The National Marine Electronics Association에서 정의되었으며, 사용되는 데이터들은 주로 자이로컴퍼스, GPS, 나침반, 관성항법장치(INS) 등이 있다.
- [37] 또한, 본 발명의 다른 측면에 따른 선박 NMEA 프로토콜 기반 침투 테스트 장치(20)는, 선박 제어 네트워크에 연결하여 침투 테스트를 수행하는 침투 테스트 장치에 있어서, 연결된 네트워크를 패킷 캡처와 패킷 분석을 통해 NMEA 문장 구조의 형식 및 특징을 추출하여 NMEA 통신 구간인지 확인하는 확인부(21)와, 상기 확인부(21)를 통해 NMEA 통신 구간인 경우, 침투 테스트 장치(20)가 공격 방법을 선택하는 공격 방법 선택부(22)와, 상기 공격 방법 선택부(22)를 통해 선택된 공격 데이터를 생성하는 공격 데이터 생성부(23)와, 상기 공격 데이터 생성부(23)를 통해 생성된 공격 데이터와 공격이 수행되는 시간 동안의 네트워크 패킷을 저장하는 공격 데이터 저장부(24)와, 상기 공격 데이터 저장부(24)를 통해 저장된 공격 데이터 및 네트워크 패킷을 선박 네트워크로 전송하는 공격 데이터 전송부(25) 및 상기 공격 데이터 전송부(25)를 통해 전송된 공격 데이터를 분석하는 공격 데이터 분석부(26)를 포함할 수 있다.
- [38] 또한, 침투 테스트 장치(20)는, 공격 방법 선택부(22)에서, 공격 방법은, 위조 NMEA 데이터 전송, 리플레이(replay) 공격 및 서비스 거부 공격 중 어느 하나를 선택할 수 있다.
- [39] 또한, 침투 테스트 장치(20)는, 공격 방법 선택부(22)에서, 공격 방법은 새로운 공격 방법의 업데이트가 가능하다.

- [40] 이것에 의해 공격 방법 선택부(22)를 통해 사용자가 테스트를 진행하기 원하는 공격 방법이나 새로운 공격 방법의 업데이트를 통해 다양한 침투 테스트를 수행할 수 있다.
- [41] 또한, 침투 테스트 장치(20)의 공격 데이터 분석부(26)는, 전송된 NMEA 공격 데이터의 양과 전송 시간을 분석하고 침투 테스트 결과를 획득할 수 있다.
- [42] 따라서, 침투 테스트 장치(20)를 통해 간단하고 빠르게 NMEA 침투 테스트(penetration test)를 수행할 수 있다.
- [43] 또한, 본 발명의 다른 측면에 따른 선박 NMEA 프로토콜 기반 침투 테스트 방법은, 침투 테스트 장치(20)를 선박 제어 네트워크(12)에 연결하는 NMEA 통신을 통해 연결하는 네트워크 연결 단계(S10); 및 상기 네트워크 연결 단계(S10)를 통해 연결된 선박 네트워크를 확인부(21)에서 패킷 캡처와 패킷 분석을 통해 NMEA 문장 구조의 형식 및 특징을 추출하여 NMEA 통신 구간임을 확인하는 확인 단계(S20)를 포함한다.
- [44] 확인 단계(S20)를 통해 NMEA 통신 구간 여부를 확인하고, NMEA 통신 구간이 아닌 경우 침투 테스트가 종료된다.
- [45] 또한, 확인 단계(S20)를 통해 NMEA 통신 구간인 경우, 침투 테스트 장치(20)의 공격 방법 선택부(22)에서 공격 방법을 선택하는 공격 방법 선택 단계(S31)로 진행되며, 이후에 상기 공격 방법 선택 단계(S31)를 통해 선택된 공격 데이터를 공격 데이터 생성부(23)에서 생성하는 공격 데이터 생성 단계(S32)로 진행되고, 이후에 상기 공격 데이터 생성 단계(S32)를 통해 생성된 공격 데이터를 공격 데이터 저장부(24)에 저장하는 공격 데이터 저장 단계(S33)로 진행되며, 이후에 상기 공격 데이터 저장 단계(S33)를 통해 저장된 공격 데이터를 선박 네트워크로 공격 데이터 전송부(25)를 통해 전송하는 공격 데이터 전송 단계(S34)로 진행되고, 이후에 상기 공격 데이터 전송 단계(S35)를 통해 전송된 공격 데이터를 공격 데이터 분석부(26)에서 분석하는 공격 데이터 분석 단계(S36)로 진행될 수 있다.
- [46] 또한, 선박 NMEA 프로토콜 기반 침투 테스트 방법은, 공격 방법 선택 단계(S31)에서, 상기 공격 방법은, 위조 NMEA 데이터 전송, 리플레이(replay) 공격 및 서비스 거부 공격 중 어느 하나를 선택할 수 있다.
- [47] 또한, 선박 NMEA 프로토콜 기반 침투 테스트 방법은, 상기 공격 방법 선택 단계(S31)에서, 상기 공격 방법은 새로운 공격 방법의 업데이트가 가능하다.
- [48] 또한, 선박 NMEA 프로토콜 기반 침투 테스트 방법에서, 상기 공격 데이터 분석 단계(S36)는, 전송된 NMEA 공격 데이터의 양과 전송 시간을 분석하고 테스트 결과를 획득할 수 있다.
- [49] 따라서, 본 발명에 따르면, 선박 내부에서 NMEA 프로토콜에 대한 침투 테스트를 수행할 수 있으며, 장치를 통해 간단하고 빠르게 NMEA 침투 테스트를 수행할 수 있는 효과를 갖는다.

- [50] 도 3은 본 발명의 실시예에 따른 선박 내부에서 CBS의 접속을 제어하는 장치의 구성을 나타내는 도면이고, 도 4는 본 발명의 실시예에 따른 선박 내부에서 CBS의 접속을 제어하는 방법의 흐름을 나타내는 순서도이다.
- [51] 도 3 및 도 4를 참조하면, 본 발명에 따른 선박 내부에서 CBS의 접속을 제어하는 장치는 ID, 비밀번호에 추가적으로 선박 내부에서 사용되는 CBS의 기기정보를 이용하여 접속을 제어하는 인증 장치 및 방법에 관한 것이다.
- [52] 도 3에 도시된 바와 같이, 본 발명에 따른 선박 내부에서 CBS의 접속을 제어하는 장치는, 통신부(100), 비콘송신기(140), 비콘 관리서버부(150), 위치확인부(160), 항해정보 확인부(170), 인증부(180) 및 AIS(Automatic Identification System) 데이터베이스(200)를 포함할 수 있다.
- [53] 이때 비콘 관리서버부(150)는 비콘 관리서버에 등록된 데이터베이스를 의미할 수 있다.
- [54] 또한, CBS(Computer Based System)는 선박 내부의 항해, 통신, 추진 등의 제어 시스템에 ID와 비밀번호를 인증하고 통신부(100)를 통해 로그인 하는 컴퓨터 기반 시스템을 의미한다.
- [55] 통신부(100)는, 블루투스(bluetooth, 110)와 GPS(120) 및 와이파이(WiFi, 130)을 포함할 수 있다.
- [56] 또한, 비콘송신기(140)는 CBS의 로그인 또는 구동 시 위치정보를 송신하며, 비콘송신기(140)로부터 위치정보를 수신하여 CBS의 장치 정보가 등록되어 있는 정보와 일치하는지 비콘 관리서버부(150)에서 확인할 수 있다.
- [57] 또한, 비콘 관리서버부(150)에서 확인 시 비콘 정보의 사각지대에 위치하는 경우 CBS는 GPS 정보를 위치확인부(160)에 전송하고, 위치확인부(160)에서 수신된 GPS 정보와 AIS 데이터베이스(200)를 항해정보 확인부(170)에서 비교한다.
- [58] 또한, 비콘 관리서버부(140) 또는 항해정보 확인부(170)를 통해 비교하는 정보가 일치하는 경우 본선 내부의 시스템으로 연결되도록 제어하는 인증부(180)를 포함하며, 인증부(180)를 통해 선박 내부에서 CBS의 접속을 제어할 수 있다.
- [59] 즉, 비콘 관리서버부(140)에서 비교 정보 중 어느 하나를 확인할 수 없는 경우 항해정보 확인부(170)를 통해 비교 정보를 비교한다.
- [60] 또한, 인증부(180)는, CBS가 선박내부에 설치된 비콘 메시지를 수신하는 경우 또는 CBS의 위치정보가 항해경로와 일치하는 경우 본선 내부의 시스템으로 연결되도록 제어할 수 있다.
- [61] 이것에 의해 운항관리, 항해관리 등 선박 내부에서 인가된 선원 단말기 및 시스템에 한해 접속되어야 하는 중요 시스템을 식별하여 원격지에서의 사이버공격을 예방할 수 있는 효과를 갖는다.
- [62] 또한, 본 발명의 다른 측면에 따른 선박 내부에서 CBS의 접속을 제어하는 방법은, 로그인 단계(S110), 위치정보 송신 단계(S120),비교 판단 단계(S130), 항해정보 확인 단계(S140) 및 인증 단계(S150)를 포함할 수 있다.

- [63] 보다 구체적으로 본 발명에 따른 선박 내부에서 CBS의 접속을 제어하는 방법은, 선박 내부의 항해, 통신, 추진 등의 제어 시스템에 ID와 비밀번호를 인증하고 통신부를 통해 CBS(Computer Based System)를 로그인 하는 로그인 단계(S110)와, 상기 로그인 단계(S110)를 통해 CBS의 로그인 또는 구동 시 위치정보를 비콘 송신기를 통해 송신하는 위치정보 송신 단계(S120)와, 상기 위치정보 송신 단계(S120)를 통해 비콘송신기로부터 위치 정보를 수신하여 상기 CBS의 장치 정보가 비콘 관리서버에 등록되어 있는 정보와 일치하는지 확인하는 비교 판단 단계(S130)와, 상기 비교 판단 단계(S130)에서, 상기 비콘 정보가 확인되지 않는 비콘 정보의 사각지대에 위치하는 경우 CBS는 GPS 정보를 위치확인부에 전송하고, 위치확인부에서 수신된 GPS 정보와 AIS 데이터베이스를 항해정보 확인부에서 비교하는 항해정보 확인 단계(S140) 및 상기 비교 판단 단계(S130) 또는 항해정보 확인 단계(S140)를 통해 정보가 일치하는 경우 본선 내부의 시스템으로 연결되도록 인증부를 통해 제어하는 인증 단계(S150)를 포함하여, 선박 내부에서 CBS의 접속을 제어할 수 있다.
- [64] 또한, 인증 단계(S150)는, CBS가 선박내부에 설치된 비콘 메시지를 수신하는 경우 또는 CBS의 위치정보가 항해경로와 일치하는 경우 본선 내부의 시스템으로 연결되도록 제어하는 것을 특징으로 한다.
- [65] 따라서, 본 발명에 따르면 선박의 운항관리, 항해관리 등 선박 내부에서 인가된 선원 단말기 및 시스템에 한해 접속되어야 하는 중요 시스템을 식별하여 원격지에서의 사이버공격을 예방할 수 있도록 하는 효과를 갖는다.
- [66] 이상 설명된 본 발명에 따른 실시예는 다양한 컴퓨터 구성요소를 통하여 실행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수 있다. 컴퓨터 판독 가능한 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM 및 DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical medium) 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 실행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령어의 예에는 컴파일러에 의하여 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용하여 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위하여 하나 이상의 소프트웨어 모듈로 변경될 수 있으며 그 역도 마찬가지이다.
- [67] 이상에서 설명되는 실시예들은 본 발명의 기술사상을 당업자가 용이하게 이해할 수 있도록 제공되는 것으로서, 이에 의하여 본 발명이 한정되는 것으로 해석되어서는 안되며, 본 발명의 실시예들은 본 발명의 사상 및 범위를 벗어나지 않

는 범위 내에서 다양하게 수정 및 변형될 수 있음은 이 기술의 분야에서 통상의 지식을 가진 자에게 자명하다. 따라서 그러한 수정예 또는 변형예들은 본 발명의 특허청구범위에 속한다 하여야 할 것이다.

서열목록 Free Text

- [68] 10: 네트워크(network)
- [69] 11: 관리 네트워크(Administrative Networks)
- [70] 12: 선박 제어 네트워크(Shipboard Control Networks)
- [71] 13: 기구 네트워크(Instrument Networks)
- [72] 14: 전용 연결(Dedicated Connections)
- [73] 20: 침투 테스트 장치
- [74] 21: 확인부
- [75] 22: 공격 방법 선택부
- [76] 23: 공격 데이터 생성부
- [77] 24: 공격 데이터 저장부
- [78] 25: 공격 데이터 전송부
- [79] 26: 공격 데이터 분석부
- [80] 100: 통신부
- [81] 110: 블루투스(bluetooth)
- [82] 120: GPS(Global Positioning System)
- [83] 130: 와이파이(WiFi)
- [84] 140: 비콘 송신기
- [85] 150: 비콘 관리서버부
- [86] 160: 위치 확인부
- [87] 170: 항해 정보 확인부
- [88] 180: 인증부
- [89] 200: AIS(Automatic Identification System)

청구범위

- [청구항 1] 침투 테스트 장치를 선박 네트워크 중 선박 제어 네트워크에 연결하는 네트워크 연결 단계; 및
 상기 네트워크 연결 단계를 통해 연결된 네트워크를 침투 테스트 장치의 확인부에서 패킷 캡처와 패킷 분석을 통해 NMEA 문장 구조 형식 및 특징을 추출하여 NMEA 통신 구간인지 확인하는 확인 단계를 포함하며;
 상기 확인 단계를 통해 NMEA 통신 구간인 경우,
 침투 테스트 장치의 공격 방법 선택부에서 공격 방법을 선택하는 공격 방법 선택 단계;
 상기 공격 방법 선택 단계를 통해 선택된 공격 데이터를 생성하는 공격 데이터 생성 단계;
 상기 공격 데이터 생성 단계를 통해 생성된 공격 데이터와 공격이 수행되는 시간 동안의 네트워크 패킷을 저장하는 공격 데이터 저장 단계;
 상기 공격 데이터 저장 단계를 통해 저장된 공격 데이터와 공격이 수행되는 시간 동안의 네트워크 패킷을 선박 네트워크로 전송하는 공격 데이터 전송 단계; 및
 상기 공격 데이터 전송 단계를 통해 전송된 공격 데이터를 분석하는 공격 데이터 분석 단계를 포함하여 침투 테스트를 수행하는, 선박 NMEA 프로토콜 기반 침투 테스트 방법.
- [청구항 2] 청구항 1에 있어서,
 상기 공격 방법 선택 단계에서,
 상기 공격 방법은, 위조 NMEA 데이터 전송, 리플레이(replay) 공격 및 서비스 거부 공격 중 어느 하나를 선택할 수 있는, 선박 NMEA 프로토콜 기반 침투 테스트 방법.
- [청구항 3] 청구항 2에 있어서,
 상기 공격 방법 선택 단계에서,
 상기 공격 방법은 새로운 공격 방법의 업데이트가 가능한, 선박 NMEA 프로토콜 기반 침투 테스트 방법.
- [청구항 4] 청구항 1에 있어서,
 상기 공격 데이터 분석 단계는,
 전송된 NMEA 공격 데이터의 양과 전송 시간을 분석하고 테스트 결과를 획득하는, 선박 NMEA 프로토콜 기반 침투 테스트 방법.
- [청구항 5] 선박 제어 네트워크에 연결하여 침투 테스트를 수행하는 침투 테스트 장치에 있어서,
 네트워크를 패킷 캡처와 패킷 분석을 통해 NMEA 문장 구조 형식 및 특징을 추출하여 NMEA 통신 구간인지 확인하는 확인부;

상기 확인부를 통해 NMEA 통신 구간인 경우, 침투 테스트 장치가 공격 방법을 선택하는 공격 방법 선택부;
 상기 공격 방법 선택부를 통해 선택된 공격 데이터를 생성하는 공격 데이터 생성부;
 상기 공격 데이터 생성 단계를 통해 생성된 공격 데이터와 공격이 수행되는 시간 동안의 네트워크 패킷을 저장하는 공격 데이터 저장부;
 상기 공격 데이터 저장부를 통해 저장된 공격 데이터와 공격이 수행되는 시간 동안의 네트워크 패킷을 선박 네트워크로 전송하는 공격 데이터 전송부; 및
 상기 공격 데이터 전송부를 통해 전송된 공격 데이터를 분석하는 공격 데이터 분석부를 포함하는, 선박 NMEA 프로토콜 기반 침투 테스트 장치.

[청구항 6]

청구항 5에 있어서,
 상기 공격 방법 선택부에서,
 공격 방법은, 위조 NMEA 데이터 전송, 리플레이(replay) 공격 및 서비스 거부 공격 중 어느 하나를 선택할 수 있는, 선박 NMEA 프로토콜 기반 침투 테스트 장치.

[청구항 7]

청구항 6에 있어서,
 상기 공격 방법 선택부에서,
 공격 방법은 새로운 공격 방법의 업데이트가 가능한, 선박 NMEA 프로토콜 기반 침투 테스트 장치.

[청구항 8]

청구항 5에 있어서,
 상기 공격 데이터 분석부는,
 전송된 NMEA 공격 데이터의 양과 전송 시간을 분석하고 테스트 결과를 획득하는, 선박 NMEA 프로토콜 기반 침투 테스트 장치.

[청구항 9]

선박 내부의 항해, 통신, 추진 등의 제어 시스템에 ID와 비밀번호를 인증하고 통신부를 통해 로그인 하는 CBS(Computer Based System);
 상기 CBS의 로그인 또는 구동 시 위치정보를 송신하는 비콘송신기;
 상기 비콘송신기로부터 위치 정보를 수신하여 상기 CBS의 장치 정보가 등록되어 있는 정보와 일치하는지 확인하는 비콘 관리서버부;
 상기 비콘 관리서버에서 확인 시 비콘 정보의 사각지대에 위치하는 경우 CBS는 GPS 정보를 위치확인부에 전송하고, 위치확인부에서 수신된 GPS 정보와 AIS 데이터베이스를 비교하는 항해정보 확인부; 및
 상기 비콘 관리서버 또는 항해정보 확인부를 통해 정보가 일치하는 경우 본선 내부의 시스템으로 연결되도록 제어하는 인증부를 포함하는, 선박 내부에서 CBS의 접속을 제어하는 장치.

[청구항 10]

청구항 9에 있어서,
 상기 인증부는, CBS가 선박내부에 설치된 비콘 메시지를 수신하는 경우 또는 CBS의 위치정보가 항해경로와 일치하는 경우 본선 내부의 시스템으

로 연결되도록 제어하는 것을 특징으로 하는, 선박 내부에서 CBS의 접속을 제어하는 장치.

- [청구항 11] 선박 내부의 항해, 통신, 추진 등의 제어 시스템에 ID와 비밀번호를 인증하고 통신부를 통해 CBS(Computer Based System)를 로그인 하는 로그인 단계;
 상기 로그인 단계를 통해 CBS의 로그인 또는 구동 시 위치정보를 비콘송신기를 통해 송신하는 위치정보 송신 단계;
 상기 위치정보 송신 단계를 통해 비콘송신기로부터 위치 정보를 수신하여 상기 CBS의 장치 정보가 비콘 관리서버부에 등록되어 있는 정보와 일치하는지 확인하는 비교 판단 단계;
 상기 비교 판단 단계에서, 비콘 정보가 확인되지 않는 비콘 정보의 사각지대에 위치하는 경우 CBS는 GPS 정보를 위치확인부에 전송하고, 위치확인부에서 수신된 GPS 정보와 AIS 데이터베이스를 항해정보 확인부에서 비교하는 항해정보 확인 단계;및
 상기 비교 판단 단계 또는 항해정보 확인 단계를 통해 정보가 일치하는 경우 본선 내부의 시스템으로 연결되도록 인증부를 통해 제어하는 인증 단계를 포함하는, 선박 내부에서 CBS의 접속을 제어하는 방법.

- [청구항 12] 청구항 11에 있어서,
 상기 인증 단계는,
 CBS가 선박내부에 설치된 비콘 메시지를 수신하는 경우 또는 CBS의 위치정보가 항해경로와 일치하는 경우 본선 내부의 시스템으로 연결되도록 제어하는 것을 특징으로 하는, 선박 내부에서 CBS의 접속을 제어하는 방법.