해상에서 실시간 TCP 링크관절 보안통신 연구

유재원*, 박대우**

호서대학교 벤처전문대학원

A Study of TCP LINK based Real-Time Secure Communication Research in the Ocean

Jaewon Yoo*, Dea-Woo Park**

Hoseo Graduate School of Venture

E-mail : peace.yoo@gmail.com, prof_pdw@naver.com

요 약

해상에서 이동하는 선박들은 가용 채널의 제한으로 지상과의 통신에 많은 제한이 발생하고 있다. 지상에선 무선 중계 시설, 유선 등 기반통신망을 통해 장거리 통신이 가능하게 된다. 또한, 공중에서 운행하는 항공기도 지상 기반통신망 및 고도에 따라 장거리 직선거리(LOS : Line of Sight) 통신이 가능하다. 반면, 해상에서는 해수면까지 직선거리 통신이 제한되기 때문에 위성을 통하거나, 수중에 설치된 통신 중계기기를 통한 통신 방식이 연구되어 왔다. 하지만, 위성 혹은 수중 중계방식은 지상시설과 동일 수준의 보안유지 및 대역폭 확보가 제한된다. 본 논문에서는 TCP 기반 링크관절을 이용한 실시간 해상 보안통신에 대해 연구하였다. 열악한 해상 통신환경에서 실시간 통신 및 보안을 제공할 수 있는 링크관절을 제안한다. 본 연구를 통해 해상에서 보다 안전하고 편리하게 통신을 할 수 있는 방안을 제시하였다.

ABSTRACT

Due to limited resource, marine communication is severely limited when compared to communications in land. Radio relay facilities, etc. based on a wired network through a long distance communication is possible. In addition, the aircraft is in the air, the ground-based network service based on long-range straight-line distance and elevation (LOS: Line of Sight) communications. On the other hand, the distance in a straight line to the sea, the sea level because communication is limited or through satellite, underwater communications relay equipment installed in the communication scheme has been investigated.. In this paper, using TCP-based real-time joint maritime security communication links were studied. Harsh marine environment, real-time communication that can provide secure communications and propose a LINK joint. In this study, more secure, and convenient communications at sea, a plan was presented to you.

키워드

링크관절, 보안통신, 해상이동 통신, 암호화, 위성통신

Key word

LINK, Secure communication, Marine mobile communication, Cryptography, Satellite Communication

Ⅰ. 서 론

육상 및 해상을 포함한 지상으로부터 대기권은 공기라는 단일매질로 이루어진 공간으로 구성되어있다. 따라서, 이 공간에 대한 전파 통신, 특히 장거리 통신분야에 있어서 해양보다는 용이한 상태이다. 위성통신, 지역중계망, 광통신망을 통해 음성 및 데이터 송·수신을 하게 된다. 이 중 위성통신망을 제외한 지역중계망, 광통신망의 경우, 신호증폭기 등 유선 통신지지 장치들이 필요하다. 또한, 통신 장치들은 동일 통제기구의 영역 내에서는 중앙통제를 통해 통신간 보안이 가능하다.

반면, 해양에서는 통신기반시설을 설치·운용하기가 해양 환경에 의해 제한된다. 해양에서 오고가는 선박의 경우, MOSCOS 위성통신망을 제외하고는 고정화된 통신망을 이용하기가 제한되며, 수중 잠수함의 경우, 더욱더 가용한 통신망이 축

소된다.

본 본문에서는 해상과 같이 열악한 통신환경에서의 보안성이 있고, 신뢰성이 보장된 데이터 통신에 대한 방법론을 제공한다.

II. 관련 연구

2.1 TCP · UDP 안전통신

데이터 통신에서 신뢰성 있는 전달은 OSI 7계층 중 물리계층 및 데이터링크 계층에서 통신전용선, 새로운 방식의 통신방식을 의미하나, 이는 기존 TCP/IP계층을 사용하는 응용체계의 근간을 해치는 것으로 논외로 한다.

TCP·UDP의 안전통신을 제공하는 것은 네트워크 계층이하 단계에서의 보안통신망을 제공해야 한다.

터널링을 통한 가상사설통신망(VPN) 등이 데이터링크 계층이하에서의 안전통신망이라 할 수 있을 것이다.

2.2 링크관절과 암호화

안전한 통신망을 제공하기 위해 링크관절구조 연구가 이루어지고 있다. Low, Middle, High 링크관절로 연결된 중요정보는 Middle 관절에 중간라우팅 정보를 전달하고 전달된 정보의 log기록을 삭제한다, 최종 해커에게 중요정보가 전달되어 유출되면 Stealth기능이 작동되면(ex)MAC주소 확인 등) 자폭되거나 백도어 작동, 랜섬웨어 등이 작동하고, Source IP를 역추적할 수 있는 기능을 탑재하는 개념이다[1].

2.3 해양통신 및 해양센서네트워크 기술

2.3.1 시스템 아키텍처

해양통신망 아키텍처는 시스템이 구축되는 해역의 수심, 네트워크 규모 및 수중 노드의 수, 응용 등에 따라 달라질 수 있다[2].

하지만, 해양통신망은 지상에서의 지상통신망에 비해 노드의 가격이 비싸고 설치가 용이하지 않기 때문에 네트워크의 강건성과 신뢰성을 높일 수 있는 아키텍처로 설계되어야 한다.

2.3.2 시스템 구성 요소 기능

수중에서 음파 및 전파를 전달하는 수중 릴레이 노드, 해수면에서 수중으로부터 전달된 해수면 게이트웨이 노드, 그리고 기존의 위성통신망을 통해 지상까지 연동할 수 있다[3].

2.4. 해상무선통신

2.4.1 해상이동통신

해상에서 이동하는 선박에서는 유선통신이 제한된다[4]. 따라서, 무선통신망이 유일한 통신수단이 될 수 밖에 없다[5]. 따라서, 주파수의 특성에 따라 연구가 그동안 진행 되었다. 표1은 주파수에 따른 통신방법이다.

표 1. 선박무선통신 사용주파수

명칭	약칭	통신 범위	통신 종류	대역 (MHz)	비고
초단파 (항구)	VHF	항구내	음성	150	70CH
초단파 (연근해)	VHF	50~100KM	음성·데이터	260	해상 이동통신
중파 (연근해)	MF	300KM	전보	500	
중단파 (연근해)	MF,HF	500KM	음성,전보	2	
단파 (원양)	HF	5대양	음성,전보	4~22	
극초단파	UHF	70KM	음성, 데이터	800	주파수 공용통신

2.4.1 수중이동통신

지상에서 정보를 전달하기 위한 반송파로 흔히 사용되는 전파(radio frequency, RF)를 수중에서 사용할 경우, 송신한 에너지는 산란, 굴절, 흡수 등의 물리적 현상에 의해 거리에 따라 급속히 감쇠하게 된다.

특히, 주파수가 높을수록, 즉, 파장이 짧을수록 신호의 세기는 더욱 빠르게 감쇠되는데, 가장 멀리까지 전달되는 초장파(3~30 kHz)를 사용할지라도 송출한 신호는 불과 30m 전후 밖에 도달하지 못하며 수신한 신호의 신뢰도도 매우 낮다.

또한, 공기와 달리 물을 매질로 하기 때문에 RF는 반송파로 적합하지 않다. 따라서, 그 대안이 음파를 들 수 있다. 음파는 계절 또는 해역 등에 따라 약간씩 변동하기도 하는데 일반적으로 1,450 ~ 1,550m/s의 범위의 값을 가지며 대기 중 음속보다 4.4배 정도 빠르다[2].

이 음파가 수중 환경에서는 통신매체의 한가지로 연구되어 지고 있다.

III. 해상이동시 보안통신 분석 및 설계

3.1 해상이동시 보안통신 분석

관련 연구에서 살펴보았듯이 해양에서의 통신은 근본적으로 데이터 통신에 한계를 가지고 있

다. 장거리 통신이 가능하기 위해서는 통신 인프라가 마련되어야 한다.

표 1.에서 보는 바와 같이 데이터 통신이 가능하기 위해서는 가능한 VHF·UHF대역을 기준을 볼 때 70km 마다 릴레이 노드가 위치하여야 통신이 가능하다. 하지만 중간 릴레이 노드에 대한 보안성 및 신뢰성이 확보가 제한된다면 안전한 통신은 제한 될 것이다.

또한, 수중에서 음파가 RF보다 전송속도면에서 우수하다는 점을 인식할 수 있으나, 음파의 주파수(20KHz대) 고려시 데이터 통신은 상당부분 제한이 된다.

3.2 해상이동시 보안통신 문제점・요구사항

해양에서의 보안통신은 전송매체의 거리 한계 극복 및 데이터 전송가능 여부, 해양환경에서의 릴레이 통신기기의 물리적 내구성 등이 보장이 되어야 할 것이다.

3.3 해상이동시 보안통신 설계

3.3.1. 단말단에서 보안통신

해상 혹은 수중에서 데이터통신이 가능하기 위해서는 우선적으로 데이터의 양을 최소화하기 위한 압축기술과 통신간 데이터 노출방지를 위해 암호화 기술이 요구된다.

또한, 암・복호화시 사용되는 킷값의 효율성을 위해 그림 1.과 같이 세션키 방식의 암호 알고리즘이 적합할 것이다.

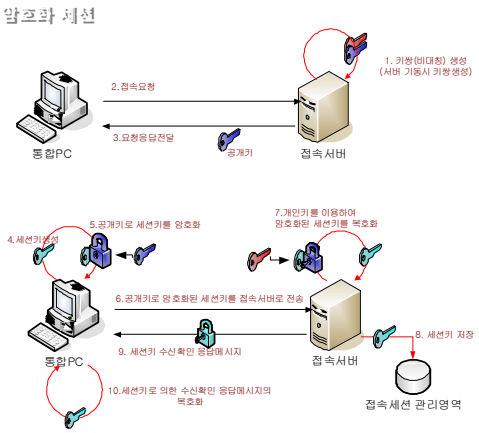

그림 1. 클라이언트와 서버간 암호화 세션

3.3.2. 중계단에서 보안통신

중계단은 해양에서의 선박 등 이동체에서 전송한 데이터의 전송책임 및 안전한 경로 설정의 책임을 지고 있다.

일반적인 라우팅 프로토콜에 의해 전송경로를 선정하고 통신을 하는 것은 전송 효율이나 안전성을 보장하기는 어렵다.

따라서, 중계장비가 통제가 효율적인 이루어져야 하며, 이동경로에 대한 보안성 및 신뢰성을 보장해야 한다.

3.3.3. 중앙통제센터

중계단에 대한 데이터 통신을 책임 지는 중계통제센터는 데이터 암호화와 경로설정을 위해 모든 트래픽을 관제하여야 한다.

또한, 데이터 전송에 사용되는 모든 자료에 대한 흐름제어, 부하분산, 인증 등의 역할을 수행하게 된다.

Ⅳ. 선박의 실시간 TCP링크관절 보안통신

4.1 실시간 OpenFlow 보안통신

TCP(Transport Control Protocol)는 3 hand-shake로 통해 end-to-end간 패이로드를 송·수신을 책임진다.

우선적으로 실시간 통신을 이용하기 위해서는 송신측은 중앙통제센터와 TCP 컨넥션을 통해 수신측에 대한 정보를 협의하고 중앙통제센터는 경로에 대한 경로와 안정성의 정도를 식별한다.

LINK관절은 국가 및 공공기관에서 인정하는 네트워크상 경유지를 대상으로 하며, 경유지에서는 중요 정보자산의 다음 경유지 혹은 목적지까지 안전한 전송을 보증하며 처리결과를 최초 발신지로 정보를 제공한다[1].

4.2 링크관절 보안 Protocol 설계

주요 정보자산의 자원식별번호 및 유통경로 등급을 포함하여 Self-Extracting 형태의 코드가 정보자산을 포함된다[1].

LINK관절 정보는 정보가 유통될 수 있는 구역을 사전에 지정하고 있으며, 구역정보가 벗어나서 실행될 경우 자폭하거나 백도어가 작동되어 실행환경에 대한 정보를 브로드캐스팅하여 전달한다[1].

LINK관절 정보는 중요 정보자산에 캡슐형태로 제공되며, 중요 정보자산에 Key-chain으로 연결되어 임의 개봉・열람을 방지한다[1].

4.3 SDN 기반 해양 보안통신망 아키텍쳐

해양환경에 맞추어 중계기기, 통제기구 및 단말시스템으로 구성된다. 중계기구는 해양 및 원거리 지역에 사전 설치되며, 소프트웨어 정의 네트워크의 개념을 따라 운용된다. 구성방식은 관련연구의 해양센서네트워크[3,4]와 동일하다.

원거리를 이동중인 선박에는 안전한 중계기기는 확보하기 힘들 수 있다. 이 경우, 선박에서는 연안 및 섬 중계기기 등을 통해 최기 중계기기까지 통신경로를 설정한다.

하지만, 태평양 한 가운데 경우에는 안전한 경로를 마련하기가 제한될 수 있다. 이 경우 단말장비인 선박에서는 성층권 비행선을 통해 위성 혹은 신뢰할수 있는 함정을 이용하여 Ad-Hoc으로 신뢰할 수 있는 네트워크를 구성할 수 있으며,

중앙통제센터로 한시적 중계기기를 등록하여 통신망을 구성하여 사용한다.

4.3 선박의 실시간TCP링크관절 보안통신

해양에서 선박 등 단말체계는 전달 정보와 링크정보에 따라 중앙통제센터에 네트워크 구성을 요청한다.

요청을 받은후 중앙통제센터는 중계기기를 연동하여 안전한 네트워크를 구성한 이후 단말체계로 구성정보를 전달하며 이를 통해 망 구성이 이루어진다.

중앙통제센터는 통신구간에 대해 보안관제를 지원하며, 침해 행위 등이 발생시 즉각적으로 대응하는 체계이다.

Ⅴ. 결 론

본 논문에서는 해양에서의 데이터 통신을 위해 정보통신망 구성방법과 SDN 기반으로 신뢰성이 확보되는 통신망에 대한 개념적 이론을 제시하였다.

중요 정보자산을 확보하고 있는 국가ㆍ공공기관에서 자료전송간 정보유출을 방지하고 실시간으로 역추적할 수 있도록 LINK관절 시스템개념을 적용해보았다.

향후 연구로는 통신환경이 열악한 소프트웨어 기반 네트워크의 보안성 및 신뢰성을 확보하기 위한 연구가 지속적으로 이루어 져야 할 것이다.

참고문헌

[1] 유재원, 박대우, Stealth 기능을 탑재한 LINK관절 IP역추적 방법, 한국정보통신 추계학술대회, pp91. 10월, 2013

[2] 박상준, 김창화 외, 수중통신과 해양 센서네트워크 기술, 정보과학회지, pp79 - 88, 7월, 2010

[3] 유재형, 김우성 외, SDN/OpenFlow 기술동향 및 전망, 정보보호학회지, pp65 - 72, 2월, 2014

[4] 김동하, 이성원, 초고속 클라우드 비디오서비스 실현을 위한 SDN기반의 다중 무선접속 기술 제어에 관한 연구, 방송공학회논문지, pp14 - 23, 1월, 2014

[5] 신현식, 한국의 해양통신 발전방향에 관한 연구, 한국전자통신학회 학술대회, pp65 - 71, 6월, 2013