한국정보전자통신기술학회논문지(jkiiect)'18-06, Vol.11 No.3
논문 18-11-03-290 http://dx.doi.org/10.17661/jkiiect.2018.11.3.290

비가입형 TDL 메시지 분석기에 관한 연구

황병한*, 이정웅*

A Study on Non-participating TDL Message Analyzer

Byoung-Han Hwang*, Jung-Woong Lee**

요 약 현재•미래전은 신속한 전투상황 공유 및 정확한 전투지휘/통제를 통한 네트워크 중심전 양상을 나타내며, 다양한 전술데이터링크(Tactical Data Link, TDL)에서 전술메시지가 운용되고 있다. 데이터 링크 처리기(Data Link Processor, DLP)가 처리하는 TDL 메시지를 모니터링하기 위해, 메시지 분석기는 일반적으로 시스템 개발 중에 하나의 구성품으로 개발된다. 또한 DLP가 처리하는 TDL 메시지를 메시지 분석기로 전달하기 위해 DLP와 메시지 분석기 사이의 인터페이스 메시지는 인터페이스 규격(Interface Control Documents, ICD)에 정의되어야 한다. 본 논문에서는 DLP와 직접 통신하지 않고 DLP로 전달되는 TDL 계층에서 제공하는 UDP 또는 TCP 패킷을 이용한 방법을 제시한다. JREAP-C와 같은 전술데이터 응용메시지 표준의 헤더정보를 이용, 수집된 패킷을 대상으로 후보패킷을 빠르게 필터링하고, 헤더에 포함된 전체 데이터 크기 정보를 이용하여, 완성된 메시지를 검증한다. 기존 방법은 시스템 구성 및 ICD에 반영되어야 하는 제약사항이 존재하지만, 본 논문에서 제안한 방법은 DLP와 직접 통신하지 않기 때문에 기존 방법이 갖는 제약사항 없이 JREAP-C, Link-K와 같은 전술데이터 응용 메시지를 분석하는 것이 가능하다.

Abstract Modern warfare exhibit a NCW (Network Centric Warfare) aspect through quick situation awareness and Command and Control. And Tactical messages operate on various tactical data links (TDLs). For monitoring TDL messages processed by data link processor(DLP), message analysers are generally developed as a component during system development. In addition, in order to forward TDL messages processed by DLP to the message anayzer, the interface messages between DLP and message analysers should be defined interface control document(ICD). We propose the methods using UDP or TCP packets provided by TDL layers that are delivered to DLP without communicating directly with DLP. Depending on TDL message standards and Interface Control Documents(ICDs), we design the message analyzer which communicates with data link processor using internal messages. Using known header field information from the TDL application standard such as JREAP-C, we can quickly filter candidate packets against collected packets and use the full data size information contained in the headers to verify the completed message. Because the methods proposed in this paper do not communicate directly with DLP, the methods proposed in this paper are enable to analyze the TDL application messages such as JREAP-C or Link-K without constraints in existing methods that should be reflected in the system configuration and ICD.

Key Words : Non-participating, JREAP-C, Link-K, Message Analysis, Tactical Data Link, TDL

1. 서론

현재•미래전은 정보우위를 통한 네트워크 중심전으로 지리적으로 흩어져 있는 센서, 지휘통제, 슈터체계들을 네트워크로 연결하고, 체계 간 TDL 메시지를 송수신함으로써 전장상황인식 및 전투 지휘통제 관련 전술정보를 공유한다. 호스트체계는 데이터링크처리기 (Data Link Processor, DLP)를 이용하여 이더넷 기반 TDL에 인터페

*WeUNUS Co.
Received April 30, 2018 Revised May 07, 2018 Accepted June 04, 2018

이스 노드로 가입하고, TDL 메시지를 주고받는다[1][2].

그림 1은 일반적인 메시지 분석기의 설계 예시이다. TDL 메시지 분석도구는 일반적으로 아래와 같이 두 가지 방법으로 이뤄진다. 첫 번째는 그림1의 ①과 같이 인터페이스 노드의 DLP에서 송/수신되는 메시지를 수집 및 분석하는 방법이다. 두 번째는 그림1의 ②와 같이 DLP에서 처리되는 메시지를 수집하고, 사전 정의된 인터페이스 규격에 따라 캡슐화하여 메시지 분석기로 전달하는 방법이다. 이 두 가지 방법은 메시지를 수집하고, 분석을 위한 기능이나 외부로 통신하는 기능을 고속처리가 필수적인 DLP에서 부가적으로 처리해야 하기 때문에 성능적인 측면에서 부담이 된다.

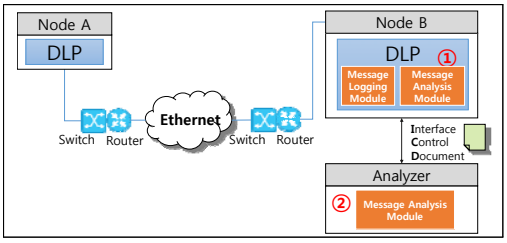

그림 1. 일반적인 메시지 분석기 설계
Fig. 1. General Design for Message Analyzer

이러한 DLP의 성능적인 부담과 메시지 수집 및 인터페이스 규격관리 등의 필요성은 호스트 체계 설계 제약사항으로 이어진다.

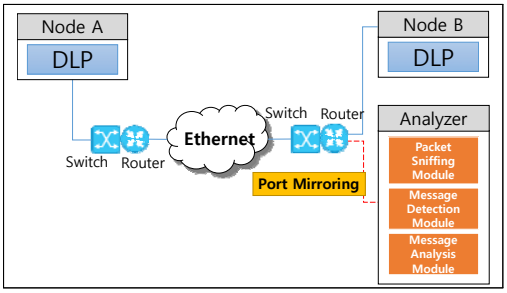

그림 2, 비가입형 메시지 분석기 설계
Fig. 2. Proposed Design for Non-participating Message Analyzer

그림 2는 비가입형 메시지 분석기에 대한 설계 예시이다. Node B를 포트 미러링을 통해 이더넷 기반 TDL에 인터페이스 노드로 직접 가입하지 않고, Node B가 연결된 라우터/스위치의 포트 미러링 기능을 이용한 메시지를 수집하고 분석하는 방법이다. 본 논문은 그림 1의 일반적인 메시지 분석도구의 문제점을 해결하기 위해 그림 2와 같이 TDL에 가입하지 않고 모니터링이 가능한 비가입형 전술메시지 분석기를 제안한다.

2. 관련 연구

2.1 패킷 스니핑

이더넷은 LAN 상에서는 모든 호스트가 같은 선(wire)을 공유하도록 되어 있으며, 같은 네트워크의 컴퓨터는 다른 컴퓨터가 통신하는 모든 트래픽을 볼 수 있다. 네트워크 인터페이스 카드(일반적으로 NIC 카드)는 네트워크의 성능 및 효율적인 통신을 위하여 자신의 MAC address를 갖는 트래픽만을 보도록 하는 필터링기능과 모든 트래픽을 보는 기능인 무차별 모드(promiscuous mode)를 제공한다. 패킷 스니핑은 NIC 카드의 무차별 모드를 세팅함으로써 동일 LAN 상의 모든 패킷을 수집하고, 패킷을 분석하는 일종의 도청 행위이다[3].

2.2 이더넷기반 TDL 메시지

TDL 메시지 표준은 HTTP, FTP 등의 공개 인터넷 표준과는 다르게 보안상의 이유로 공개되지 않는다. 하지만 TDL 메시지도 링크계층인 IP와 전송계층인 TCP/UDP에 의해 캡슐화되어 송수신된다.

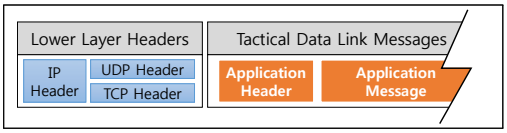

그림 3. 이더넷기반 TDL 메시지
Fig. 3. based TDL Message Structure on Ethernet

그림 3은 이더넷 기반의 캡슐화된 TDL 메시지 구조이다. 라우팅을 위한 IP 헤더와 데이터 전송을 위한 TCP/UDP 헤더를 포함한 하위계층 헤더 정보와 TDL 메시지로 구성된다. TDL 메시지는 응용계층의 전송버퍼와 이더넷 프레임이 제공하는 MTU 제약에 의해 단일 또는 복수 개의 이더넷 프레임으로 구성될 수 있다.

2.2.1 JREAP-C 메시지

JREAP(Joint Range Extension Application Protocol)은 Link-16의 가용 범위(주파수 도달범위)를 확장하기 위해 사용되는 프로토콜로서 통신 매체에 따른 A,B,C가 있으며, 이 중 JREAP-C는 IP기반 네트워크를 통한 범위 확장에 사용된다.

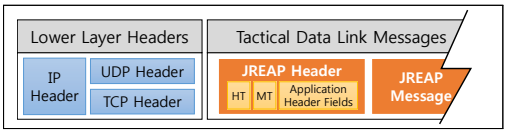

그림 4. JREAP-C 메시지 구조
Fig. 4. JREAP-C Message Structure

그림 4는 캡슐화된 JREAP-C 메시지 구조이다. JREAP-C의 헤더는 A,B,C를 구분할 수 있는 헤더 형식(Header Type, HT)와 메시지를 구분할 수 있는 메시지 형식(Message Type, MT)와 메시지 크기 정보 등을 포함한 세부 필드 정보로 구성된다[4][5].

2.2.2 유선 Link-K 메시지

Link-K는 한국형 합동전술데이터링크를 의미하며, 다양한 무기체계를 유선, 무선, 위성의 통신매체로 연결하고 한국군이 현재 수행중인 육•해•공 합동작전에 최적화된 전술 데이터링크이다.

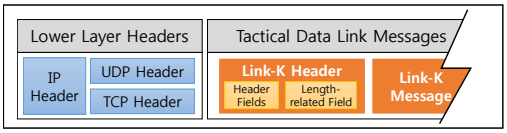

그림 5. 유선 Link-K 메시지 구조
Fig. 5. Wired Link-K Message Structure

그림 5는 Link-K 중 이더넷을 기반으로한 유선 Link-K 메시지 구조이다. Link-K의 헤더는 메시지 암호화여부 및 크기와 관련된 정보 등을 포함한 세부 필드 정보를 포함한다[6][7].

3. 비가입형 분석기 구현방안

3.1 전체 시스템 구성

본 논문에서 제안하는 메시지 분석기는 스위치 환경에서 다른 호스트의 트래픽을 스니핑하기 위해 포트 미러링을 사용하였고, 패킷을 수집하기 위해 패킷 스니핑 기술을 적용하였다. 수집된 패킷내 전술메시지를 탐지하고, 탐지 과정과 분석과정을 분리하여 처리 속도를 개선하고자 한다.

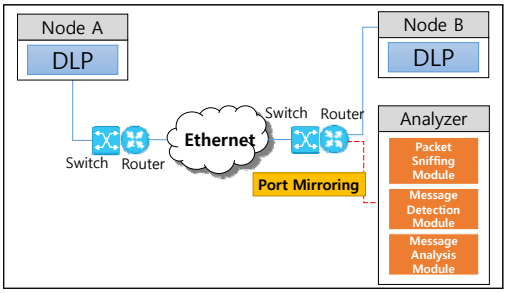

그림 6. 메시지 분석기의 전체 구성도
Fig. 6. Overall Configuration Diagram for Proposed Message Analyzer

그림 6은 본 논문에서 제안하는 비가입형 메시지 분석기의 전체 시스템 구성도이다. 패킷 스니핑 모듈은 들어오는 이더넷 패킷 중 메시지 전송에 사용되는 TCP 또는 UDP 패킷만 캡처하여 TDL 메시지 탐지 모듈로 전달한다. TDL 메시지 탐지 모듈은 TCP 또는 UDP 세그먼트를 대상으로 TDL 메시지 여부를 판단하고, 메시지로 판단시 조립을 위해 내부 버퍼에 저장한다. 메시지 조립이 완성되면 TDL 메시지 분석 모듈로 전달한다. TDL 메시지 분석 모듈은 조립된 메시지를 대상으로 메시지를 분석하고, 분석 결과를 출력한다.

3.2 패킷 스니핑 모듈

패킷 스니핑 모듈은 패킷 스니핑에 의해 유입되는 트래픽 중 TDL 메시지 전송에 사용되는 TCP/IP와 UDP/IP를 대상으로 패킷을 수집한다. 스위치에 연결된 호스트를 대상으로 포트 미러링을 하는 경우 스위치에 대한 부가적인 CPU 부하를 유발하기 때문에, 네트워크 성능을 고려하여 탭장비를 사용할 수도 있다. 일단 감시대상 트래픽이 메시지 분석모듈로 전달되면, 패킷 스니핑 모듈은 패킷 수집 라

이브러리를 이용하여 패킷을 수집하고, 수집된 패킷은 TDL 메시지 탐지 모듈로 전송한다.

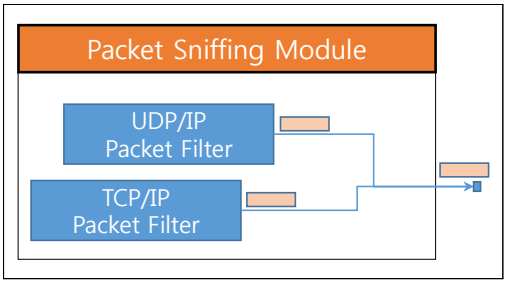

그림 7. 패킷 스니핑 모듈
Fig. 7. Packet Sniffing Module

그림 7은 패킷 스니핑 모듈의 내부 구조이다. 수집된 패킷 대상을 최소화하기 위하여, 전송계층 프로토콜인 TCP와 UDP로 각각 나누어 처리한다. 또한 분석대상 범위를 동적으로 설정하기 위한 출발지(IP,Port번호), 목적지(IP, Port 번호) 등의 필터를 포함하고 있다.

3.3 TDL 메시지 탐지 모듈

TDL 메시지 탐지 모듈은 먼저 TDL 메시지를 탐지하고, 탐지된 UDP 또는 TCP 패킷을 대상으로 TDL 메시지를 조립한다. TDL 메시지 탐지는 TDL 메시지 표준별로 각각 처리된다.

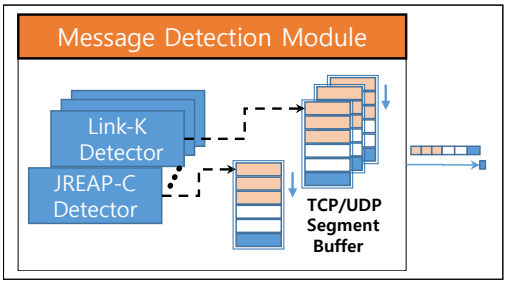

그림 8. TDL 메시지 탐지 모듈
Fig. 8. TDL Message Detection Module

그림 8은 TDL 메시지 탐지 모듈의 내부 구조이다. TDL 메시지 탐지는 JREAP-C, Link-K 등과 같은 전술데이터링크 메시지 표준을 이용하여 특정 필드의 고정 값 또는 유효 범위를 검증함으로써 가능하다. 일단 메시지가 탐지되면 TDL 프로토콜, 출발지(IP,Port번호), 목적지(IP, Port 번호)별로 생성하여 각각 UDP 또는 TCP 버퍼(이하 세그먼트 버퍼)에 저장한다. 메시지가 조립되기 전에 연결이 종료되거나 새로운 메시지가 탐지되면 세그먼트 버퍼는 초기화된다. 메시지가 조립되면 세그먼트 버퍼 전체를 연결하여 TDL 메시지 분석 모듈로 전달하고, 세그먼트 버퍼는 초기화된다.

3.4 TDL 메시지 분석 모듈

TDL 메시지 분석 모듈은 조립된 TDL 메시지와 프로토콜 등의 정보를 이용하여 각 메시지 표준별로 전용 해석기를 이용하여 분석한다. 분석된 결과는 화면으로 출력하거나, 사후분석 등을 위해 파일 또는 DB 등에 저장한다.

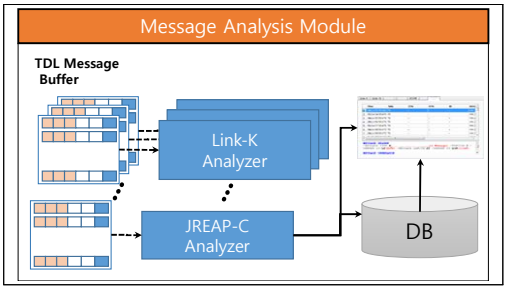

그림 9. TDL 메시지 분석 모듈
Fig. 9. TDL Message Analysis Module

그림 9는 TDL 메시지 분석 모듈의 내부구조 이다.

3.5 기존 방법과의 차이점

전술메시지 분석기 혹은 모니터링 도구는 공개 또는 확보 가능한 표준이 아닌, 군사기밀보호가 이뤄지는 국방 전술메시지 관련 분석기로, 주로 국방 시스템(체계) 개발 중에 구현된다. 일반적으로 데이터링크 처리기(DLP)가 처리하는 메시지를 메시지 분석기로 전달해야 하기 때문에, 내부 처리를 위한 별도의 필드를 추가한 인터페이스 메시지를 정의하고, 통신을 수행해야 하는 제약사항이 존재한다.

본 논문에서 제안한 비가입형 메시지 분석기는 구성품이 아닌 별도의 SW로 개발이 가능하기 때문에 TDL 메시지 표준과 DLP가 처리하는 메시지의 인터페이스 규격(Interface Control Document, ICD)만 제공된다면 국

방 시스템 개발 단계와 상관없이 구현이 가능하다. 이러한 장점 외에도 이더넷 패킷을 대상으로 하기 때문에, 네트워크 정보와 결합하여 국방 전술망 내에서 사이버 공격에 대한 이상 징후 판단에도 활용이 가능하다.

4. 결론 및 향후연구과제

전술데이터링크(TDL)에 연결되는 호스트체계는 전술데이터링크처리기(DLP)를 통해 TDL 메시지를 주고받는다. 일반적으로, 호스트체계 또는 전술데이터링크 체계를 구현하는 과정에서 전용 메시지 분석기를 구현하며, 이러한 분석기는 직접 또는 간접적으로 전술데이터링크에 가입하여야 한다. 또한, 실 체계 운용 시 분석기는 처리 성능이 각별히 요구되는 DLP 체계 내부에 구현하는 대신, DLP를 통해 최소의 내부 메시지를 받아 별도로 구현한다. DLP와 분석기간 통신을 위해 인터페이스 표준이 사전에 정의되고 관리되어야 한다. 본 논문은 전술데이터링크에 직접 가입하지 않고, 분석대상 호스트를 포트 미러링 등의 방법을 이용함으로써 DLP의 성능 부하와 설계 제약사항의 문제점이 해결 가능한 비가입형 분석기를 제안한다. 또한 네트워크 트래픽을 직접 모니터링함으로써 전술메시지 내용 외에 일반적인 네트워크 트래픽 정보를 결합이 가능하다. 향후, 네트워크 부하측정, 공격 노드 추적 및 방어 등 전술데이터링크 침입탐지시스템 또는 방화벽으로 발전 가능할 것으로 판단한다.

REFERENCES

[1] Sangrae Jung, Hyunshik Shin, "Analysis on Technology Development of NCW and Tactical Data Link", Journal of The Korea Institute of Electronic Communication Sciences, Vol. 7, No. 5, pp.991~998, 2012.

[2] Dongil Kim, "Study of tactical data link processor test tool", Proceedings of the International Conference on Instrumentation and Control Systems(CICS), pp. 180-181, 2013.

[3] Junsang Jeon, Younseo Jeong and Wooyoung Soh, "Design of Packet Generator for TCP/UDP Protocols Using Packet Sniffing and IP Spoofing," Journal of Korea Computer Congress, Vol. 32, No. 2, pp. 649~651, Nov, 2005.

[4] US Department of Defense(DOD), "The Joint Range Extension Application Protocol (JREAP)", Mil-Std-3011B, 8 February, 2013.

[5] US Department of Defense(DOD), "Tactical Data Link(TDL) 16 Message Standard", MIL-STD-6016E, 20 July, 2012.

[6] Defense Information Technical stAndard(DITA), "Link-K Message", MND-STD-0018, 2014.

[7] Defense Information Technical stAndard(DITA), "Link-K Host Interface Message", MND-STD-0029, 2014.

저자약력

황 병 한(Byoung-Han Hwang) **[정회원]**

- 1994 부산대학교 전자공학과 (공학사)
- 1999 부산대학교 전자공학과 (공학석사)
- 1994 ~ 2000년 삼성전자(주) 전임연구원
- 2015년 ~ 현재 위우너스(주) 기업부설연구소 연구소장

<관심분야> 지휘통제(C2)체계, 전술데이터링크(TDL)

이 정 웅(Jung-Woong Lee) **[정회원]**

- 1994 서울대학교 분자생물학과(이학사)
- 1998 ~ 2003년 쌍용정보통신(주) D-연구소 과장
- 2003 ~ 2010년 (주)휴니드테크놀러지스 정보전력개발단 수석연구원
- 2010 아주대학교 정보시스템감리과(공학석사)
- 2011년 ~ 현재 위우너스(주) 대표이사

<관심분야> 지휘통제(C2)체계, 전술데이터링크(TDL)