지상전투차량 전장관리체계 보안 적용 방안 연구

이승원, 노해환, 최훈*
LIG 넥스원, *충남대학교

seungwon.lee@lignex1.com, emessage@lignex1.com, *hc@cnu.ac.kr

A Study on Apply Security in the Battlefield Management System of Ground Fighting Vehicles

Lee Seung Won, No Hea Whan, Choi Ho*
LIG Nex1, *Chungnam National Univ.

요 약

오늘날 지상전투차량에 탑재된 전장관리체계는 기존 CDF(Common Data Format)에서 육군전술데이터링크 KVMF(Korean Variable Message Format) 방식으로 성능개량하면서 C4I 부체계와 상호운용성을 확보할 수 있게 되었다. 하지만 KVMF 기반 전문은 FM 무선망을 사용하여 공유하기때문에 적으로부터 쉽게 도청이나 데이터 변조·위조 등 다양한 보안 취약점이 노출되므로 추가적으로 보안 방안이 시급하다. 본 논문에서는 전장관리체계에 보안을 적용하는데 있었어, 기존 전장관리체계와 암호장비간에 종속성을 없애고 암호장비의 기능변경에 상관없이 적응적으로 호환할 수 있는 연동 모델을 제시한다.

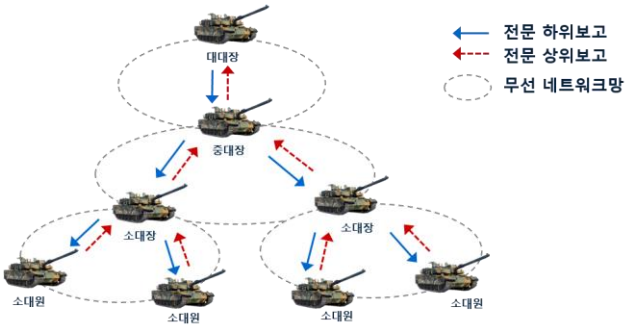
Ⅰ. 서 론

오늘날 전장은 ICT 기술이 급격하게 발전하면서 전장패러다임도 화력/기동 중심에서 네트워크 중심전(NCW: Network Centric Warfare)으로 전환하고 있다. 우리 지상군도 전차/장갑차와 같은 지상전투차량에 ICT 기술을 접목한 전장관리체계(BMS: Battlefield Management System)를 탑재하여 작전에 활용하고 있다.

BMS 는 전장상황을 인지하고 명령, 보고, 화력지원 등 실시간으로 정보공유가 가능하며 전술과 전략을 효과적으로 펼칠 수 있는 무기체계이다.

BMS 는 대표적으로 체계제어컴퓨터, 화면전시기, FM 무전기로 구성되며 체계제어컴퓨터는 데이터를 MIL-STD-188-220C 프로토콜 방식으로 FM 무전기를 통해 무선 신호를 전달한다.

다음 [그림 1]과 같이 BMS 는 지상전투차량에 탑재하여 대대장, 중대장, 소대장, 소대원 별로 독립적인 무선망을 형성하고 상/하위제대간에 망가입/탈퇴와 전문을 근실시간으로 공유할 수 있게 한다.



[그림 1] 지상전투차량 지휘통제 운용개념

또한 BMS 는 기존 CDF(Common Data Format) 전문 형식을 유지하다가 C4I 타체계와 상호운용성 문제를 제기하면서 오늘날 KVMF(Korean Variable Message Format) 전문형식으로 성능개량이 완료되었으며 C4I 합동지휘통제가 가능해졌다[1].

그러나 BMS 는 FM 주파수를 통해 무선통신을 하는 방식이기때문에 전장정보를 적으로부터 도청, 데이터 변조·위조, 교란 등 다양한 보안 취약점이 노출 되어있다. 이러한 무선통신 방식으로 공유되는 전문는 절대적으로 암호화가 필요하며 적으로부터 보호할 수 있는 보안 방책이 필수적이다.

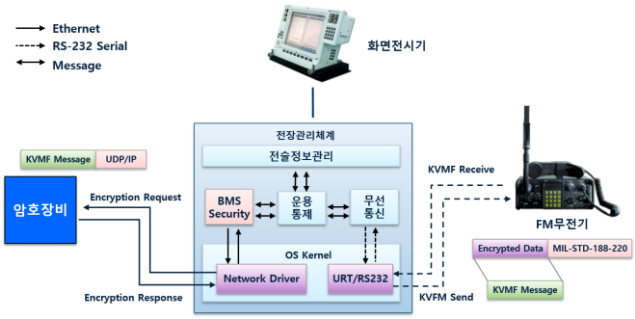
이에 따라, 본 논문에서는 BMS 의 기존 성능에 대한 영향성 없이 암호장비를 추가적으로 연동하는데 있었어, 호환성과 확장성을 확보할 수 있는 BMS Security 플러그 관리자를 제안한다.

Ⅱ. 본론

2.1 전장관리체계 보안 적용 방안

BMS 는 차량에 탑재된 다양한 센서를 제어하고 FM 무전기를 이용하여 무선으로 전장정보를 수집 및 공유할 수 있는 무기체계이다. BMS 는 다음 [그림 2]와 같이 운용통제, BMS Security, 무선통신, 전술정보관리 CSU 로 구성된다[3].

전술정보관리 CSU 는 KVMF 기반 상황도, 지도, 명령, 보고, 화력지원, 투명도 등 33 종 전문을 작성할 수 있도록 기능이 구성되어 있다. 또한 상위제대와 하위제대간에 망가입/탈퇴를 위해 사용자 ID, URN, 부대코드, IP Address 등 부대정보를 등록하고 운용환경을 설정할 수 있다.



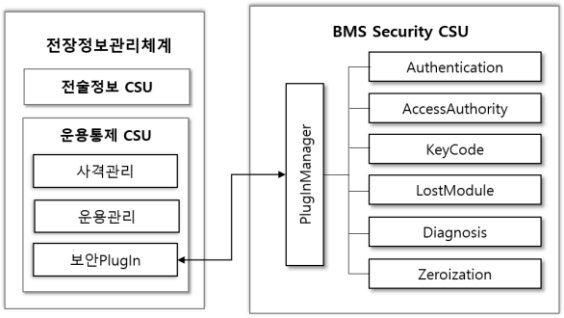
[그림 2] 전장관리체계 보안적용 방안 개요

운용통제 CSU 에는 전술정보관리 CSU 와 BMS Security CSU 로부터 메시지를 수신하고 Message Parsing 하는 동기화기능과 지상전투차량에 무장된 센서를 제어하고 관리하는 연동기능, 고장진단을 위한 자체점검 기능이 구성되어있다. BMS Security CSU 는 운용통제 CUS 와 무선통신 CSU 로부터 메시지를 수신하고 Message Parsing 하기 위한 동기화기능이 구성되고 암호장비에서 제공되는 기능을 실행할 수 있는 플로그인이 구성된다. 운용통제 CSU 는 BMS Security CSU 에게 전문 암호화 요청하고 암호화된 전문을 무선통신 CSU 에게 전송한다. 무선통신 CUS 는 FM 문전기를 사용하여 전문 송신을 위한 ACK 재전송, S/R(Segmentation & Reassembly), MIL-STD-188-220C 캡슐화, 인코딩작업이 진행된다[2].

2.2 BMS Security 플러그인 관리자 설계

다음 [그림 3]은 운용통제 CSU 와 BMS Security CSU 간에 연동을 위한 플러그인 관리자 설계 방안을 제시한다.

BMS Security CSU 는 Authentication, AccessAuthority, KeyCode, LostModule, Diagnosis, Zeroization 플러그인이 구성되어 있고 사용자 인증, 사용자 권한, 키코드관리, 분실모듈관리, 자체진단, 비상소거 기능이 정의되어있다.

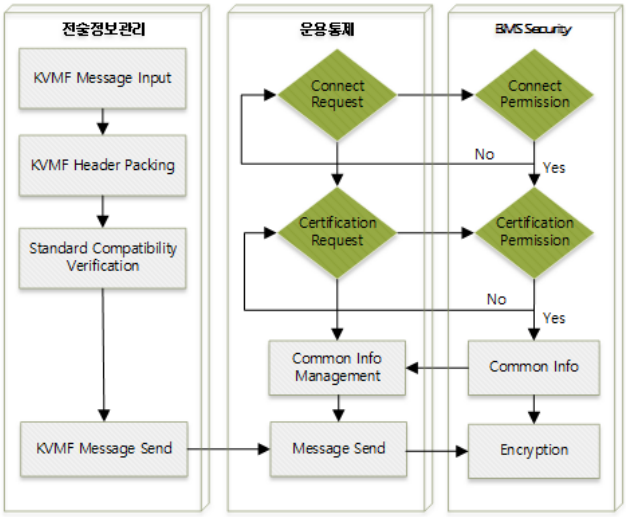


[그림 3] BMS Security 인터페이스 설계

PlugInManager 는 암호장비의 각 기능을 실행할 수 있는 플러그인을 운용통제 CSU 가 연결할 수 있도록 콜백방식 API 를 정의하였고 운용통제는 PlugInManager 을 참조하여 콜백함수를 호출함으로써 암호장비의 기능변화가 발생하여도 기존 BMS 의 성능에 대한 영향성이 없도록 설계되어있다.

다음 [그림 4]은 전장관리체계에서 KVMF 전문 암호화 처리되는 순서도이다.

체계제어컴퓨터인가 후 초기화되면 운용통제 CSU 는 BMS Security CSU 에 연결요청되고 연결 승인되면 사용자 인증이 요청된다. 사용자 인증 요청 후 승인되면 암호장비 상태정보가 수신되고 상태정보를 활용하여 암호장비를 제어하고 관리하게된다.



[그림 4] KVMF 전문 암호화 순서도

전술정보관리 CSU 에서 전문을 작성하고 KVMF 헤더로 캡슐화하여 운용통제 CSU 에 전송되고 운용통제 CSU 는 BMS Security CSU 에 암호화 요청하고 암호화된 전문을 획득하면 무선통신 CSU 에 전달되는 절차를 가진다.

Ⅲ. 결론

전장관리체계는 FM 무선망을 사용하여 KVMF 기반 전문을 공유하기 때문에 적으로부터 전장정보를 보호하기 위한 암호장비가 필수적이다. 전장관리체계에 암호장비를 연동하기위해서는 기존 시스템에 대한 성능영향성이 없어야하며 암호장비 기능변경에 대해 적응적으로 연동할 수 있어야한다. 본 논문에서는 암호장비에서 제공되는 각 기능을 실행하기 위한 플러그인을 정의하고 각 플러그인을 콜백함수로 연결할 수 있도록 API 가 정의된 플러그인 관리자 모델을 제안하였다. 이 모델을 통하여 전장관리체계는 암호장비로부터 종속성을 없애고 확장성과 호환성을 갖을 수 있는 암호장비 연동모델이 될 수 있다.

참 고 문 헌

[1] 박영배, 양용석, 양길석, “육군전술데이터링크(KVMF)활용 및 발전 제언”, 국방과 기술, pp. 44-49, 2011.

[2] AMSC N/A, Department of defense interface standard MIL-STD-188-220, 2005.

[3] 최일호, 김대영, 권철희, 이상명, “지상전투차량의 전장관리체계상에서 KVMF(Korea Variable Message Format) 구현”, 한국군사과학기술학회지, 제 16 권, 제 5 호, 2014.