Journal of The Korea Society of Computer and Information
Vol. 22 No. 8, pp. 63-72, August 2017
www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.08.063

Security Architecture for T4 Class Common Data Link

Sang-Gon Lee*, Hoon-Jae Lee**, Hyeong-Rag Kim***, Young-Jae Ryu****

Abstract

In this paper, we propose a security architecture for HDLC-based T4 class common data link. The common data links are composed of point-to-point, multi-to-point, and point-to-multi mode. For multi-to-point mode, one node has a bundle of point-to-point links with different end-point on the other side of the links. Thus multi-to-point mode can be considered as a bundle of point-to-point mode. Point-to-multi mode is broadcasting link. For point-to-point mode we adopted robust security network scheme to establish a secure data link, and for multi-to-point mode we use broadcast encryption scheme based on ID-based cryptography to distribute encryption key for broadcasting message encryption. We also included MACsec technology for point-to-point data link security. Computational and communicational complexity analysis on the broadcast encryption have been done.

▸Keyword: RSN, EAP, 802.1x, 802.11i, HDLC, CDL, ID-based cryptography, Broadcast encryption

I. Introduction

현대의 전쟁 형태는 정보통신 기술 및 정보통신 망 기술의 발달로 현대 정보통신망을 기반으로 각 제대(梯隊,echelon) 간을 네트워크를 연결하여 전장 상황, 전투 체계 통제, 타격 체계통제 등의 정보를 교환하여 전투 수행능력을 향상 시키는 네트워크중심전(NCW, Network Centeric Warfare)으로 변화하고 있다[1,2]. NCW를 위한 중심 네트워크로써 디지털 전술데이터링크(TDL, Tactical Data Link)는 음성 통신 이외에 지휘 통제 및 명령 사항을 다수의 작전 통신 장비 플랫폼으로 전파하는 능력을 제공한다. 하지만 무인기, 조기 경보 통제기와 같은 감시 및 정찰 시스템으로부터 수집한 고해상도의 영상정보를 전송하기에는 적합하지 않아 이를 유통하기 위한 별도의 데이터링크 기술을 공용데이터링크(CDL, Common Data Link)이라 한다[1,3].

공용데이터링크는 미래 네트워크중심전 수행 시 요구되는 효과적인 고해상도 영상정보 전송 및 근접항공 등의 전술작전 지원을 위한 정보공유를 위해 다중 플랫폼 공용데이타링크(MP-CDL, Multi-Platform Common Data Link)로 발전하고 있으며, 주로 감시 및 정찰을 위한 유·무인기에 적용될 예정이다. 미국과 이스라엘이 CDL 개발 및 운영 분야의 선진국이라고 할 수 있다[4]. 한편 우리 군에서도 우리 실정에 맞는 공용데이타링크 개발의 필요성을 인식하고 각 제대별 무인기를 통합 운용하기 위한 다중플랫폼 영상정보용 공용데이터링크(MPI-CDL, Multi-Platform Image and Intelligence Common Data Link)를 개발하였으며, 현재 상용화를 위한 시험단계에 착수한 상태이다[1,4].

이스라엘의 MP-CDL은 IP 네트워킹을 통해 UAV가 획득한 영상정보를 실시간으로 원하는 제대에 제공할 수 있다. 즉, UAV 획득 영상정보를 원하는 어떠한 사용자라 하더라도 IP 네트워크로 연결되기만 하면 원하는 정보를 볼 수 있다. 특히, 중계의 경우에는 지상의 유선 기반 IP 네트워크를 통해 보다 쉽게 통달거리를 확장시킬 수 있다.

아직 MPI-CDL 데이터링크에서의 보안 프로토콜에 관하여 알려진 연구가 없다. 본 연구에서는 HDLC 기반 MPI-CDL에

First Author: Sang-Gon Lee, Corresponding Author: Hoon-Jae Lee
*Sang-Gon Lee (nok60@dongseo.ac.kr), Div. of Computer Engineering, Dongseo University
**Hoon-Jae Lee (hjlee@dongseo.ac.kr), Div. of Computer Engineering, Dongseo University
***Hyeong-Rag Kim (hrkim@pohang.ac.kr), Dept. of IT& Electronics, Pohang University
****YoungJae Ryu, ADD
• Received: 2017. 08. 09, Revised: 2017. 08. 15, Accepted: 2017. 08. 22.
• This work was supported by ADD.

적합한 데이터링크 보안 구조를 제안하고자 한다. 2장에서는 MPI-CDL에 관하여 기술하고, 3장에서는 HDLC와 무선 LAN 데이터링크보호에 관하여 기술하며, 4장에서는 HDLC 기반 MPI-CDL을 위한 데이터링크 보안기법을 제안하고자 한다, 마지막으로 5장에서는 결론으로 마무리 한다.

II. Preliminaries

1. MPI-CDL[1]

MPI-CDL은 기존의 점대점 운용모드를 기반으로 하는 공용 데이터링크와 호환이 가능하면서도 향상된 전송속도, 점대다, 중계운용모드를 지원하는 국내 공용데이터링크 기술이다[4,5]. 그림 1은 MPI-CDL에서 예상되는 운용모드를 나타낸다.

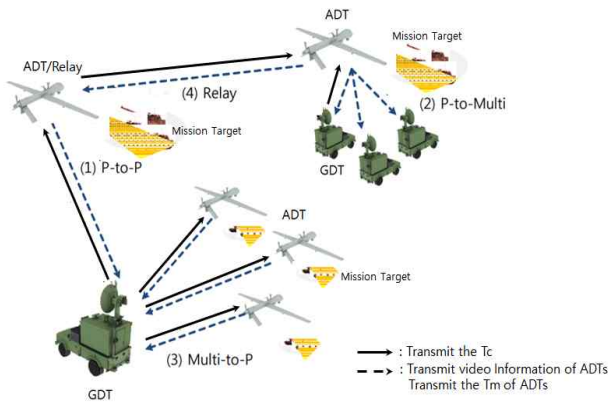

Fig. 1. Operation Modes of MPI-CDL

네트워크 구성 장비는 지상장비(GDT, Ground Data Treminal)와 공중장비(ADT, Air Data Terminal)로 구성되며, 공중장비는 중계장비(ADT/Relay)의 기능을 수행하기도 한다. 각 장비 간 별도의 데이터 링크를 형성한다. ADT-GDT와 ADT-ADT/Realy-GDT 간 송·수신하는 Tm(Telemetar) 및 Tc(Telecontrol) 메시지는 각각 장치의 상태 및 운행에 관련된 제어 메시지를 의미한다.

MPI-CDL에서는 점대점(P-to-P), 점대다(P-to-Multi), 다대점(Multi-to-P), 중계(Relay) 등의 4가지 모드를 지원한다. 점대점 운용모드는 지상장비와 탑재장비 사이에 지향성/무지향성 안테나를 사용하여 일대일 링크를 운용하는 모드이며, 점대다 운용모드는 단일 탑재장비가 다수의 지상장비와 통신하는 형태로, 탑재장비는 무지향성 안테나를 사용하여 브로드캐스팅 한다. 다대점 운용모드는 다수의 탑재장비가 단일 지상장비와 통신하는 형태로, 주파수 대역이 탑재장비마다 각각 할당되어 나누어 통신하고, 지상장비는 무지향성 안테나로 운용하게 된다. 중계 운용모드는 원거리의 탑재장비가 다른 탑재 장비의 중계를 통해 지상장비와 통신하는 형태이며, 중계장비, 탑재장비의 동시 제어가 가능하고 중계장비와 탑재장비의 IP로 최종 수신노드를 판단 후, 두 장비(탑재장비, 중계장비)의 영상을 다중화하여 지상장비에 전송한다.

기존의 MPI-CDL은 45Mbps 전송속도를 제공한다. 다수의 플랫폼과 링크를 구성하는 링크를 구성하는 상황에서는 전송속도가 저하되기 때문에, 다수 링크를 통해 동시 다발적으로 회소한의 영상정보를 전송하기 위해서는 T4급 (274Mbps) 정도의 충분한 전송속도를 제공할 필요가 있다.

그림 1에 나타낸 바와 같이 점대점, 다대점, 그리고 중계 등의 모드에서는 양방향 통신이 가능하므로 양방향 인증이 가능하다. 하지만 점대다 모드에서는 일방향 브로드캐스팅 모드로 운용되므로 나머지 모드들과는 다른 방식의 링크보안 기술이 적용되어야 한다.

2. HDLC

2.1 Station Type, Setup Mode and Transmission Mode of HDLC

HDLC는 ISO3009와 ISO4335에서 정의된 데이터링크 전송 제어 프로토콜이다. 스테이션의 유형은 3개로 나누어 진다. 1차 스테이션은 링크의 제어를 전적으로 관장하며 명령을 2차 스테이션에 보낸다. 2차 스테이션은 1차 스테이션의 제어 하에서 응답을 보내는 동작을 한다. 혼합 스테이션은 1차 스테이션과 2차 스테이션의 기능을 가지며 명령과 응답을 생성한다.

링크설정 모드는 불균형(unbalanced) 모드와 균형 모드의 두 가지로 나누어 진다. 균형(unbalanced) 설정에서는 한 개의 1차 스테이션과 여러 개의 2차 스테이션으로 구성되는데 1:N 통신에 적합하다. 균형(balanced) 설정에서는 두 개의 혼합 스테이션으로 구성되며 1:1 통신에 적합하다.

HDLC 전송모드는 세 가지 모드로 나누어 진다. Normal Response Mode(NRM)는 1:N 통신에서 Unbalanced 설정과 함께 사용되는데, 1차 스테이션이 전송을 시작한다. 즉, 2차 스테이션은 1차 스테이션의 폴링(polling)에 응답하여 데이터를 1차 스테이션으로 전송하게 된다. Asynchronous Balanced Mode(ABM)에서는 1:1 통신에서 Balanced 설정과 함께 사용되는데 어느 쪽이든지 통신을 시작할 수 있다. 그래서 폴링의 오버헤드가 없기 때문에 가장 많이 사용되고 있다. 마지막으로 Asynchronous Response Mode(ARM)는 1:N 통신에서 Unbalanced 설정과 함께 사용되는데, 2차 스테이션은 1차 스테이션의 허락 없이도 전송을 시작한다. 하지만 비교적 잘 사용되지 않는 모드이다.

2.2 HDLC Frame Structure

아래 그림 2는 HDLC 프레임 구조를 나타낸다. 동기방식 전송을 사용하며 단일 프레임 포맷이 사용된다.

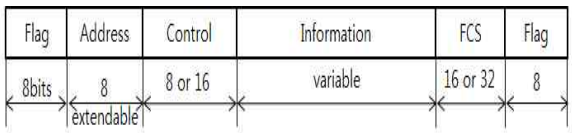

Fig. 2. HDLC Frame Structure

프레임 양 끝단에 flag 비트 패턴 01111110로 프레임의 시작과 끝을 알린다. 수신기는 프레임의 시작과 끝을 인식하기 위하여 flag를 탐색한다. 주소필드를 사용하여 프레임을 전송하거나 수신할 2차 스테이션을 식별한다. 보통 8비트 인데 7비트의 배수로 확장될 수 있다. 가장 왼쪽 비트는 마지막 옥텟인지(1) 혹은 아닌지(0)를 나타낸다. 주소 값이 11111111이면 1차 스테이션이 브로드케스팅 할 때 사용된다. 아래 그림은 확장된 주소의 형식을 나타낸다. 제어필드는 그림 3과 같이 프레임 유형에 따라 구조가 다르다.

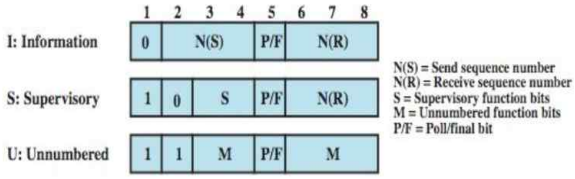

Fig. 3. Control Field of HDLC

프레임 유형은 I(Information)-프레임, S(Supervisory)-프레임, U(unnumbered)-프레임으로 나누어 진다. 그림 4는 프레임 유형별 메시지 형식을 나타낸다. I-프레임의 제어필드는 사용자(상위 계층)에게 데이터를 전송하는 것과 관련하여 흐름제어와 오류제어를 위한 piggyback이 적용된다. S-프레임의 제어필드는 piggyback을 적용하기 불가능 하거나 적절하지 않은 상황에서 ARQ에 사용된다. 예를 들어 스테이션이 보낼 데이터가 없을 경우가 이에 해당된다. S 프레임에는 Receive Ready (RR), Receive Not Ready (RNR), Reject (REJ), 그리고 Selective Reject (SREJ) 등 4 가지 프레임이 있다.

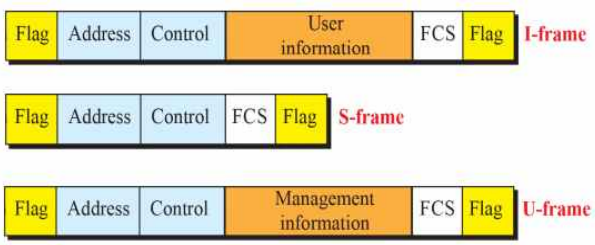

Fig. 4. Massage Format for HDLC Frames

U-프레임은 보조적인 링크제어 기능을 제공한다. U-프레임은 링크 관리에 사용된다. 그리고 사용자 데이터 전송에도 사용될 수 있다. 연결된 장치 간에 세션 관리와 제어 정보를 교환한다. 어떤 U-프레임은 정보 필드를 포함하고 있어서 시스템 관리 정보 혹은 사용자 데이터를 위해 사용될 수 있다. 위의 그림 3에서 첫 번째 두 비트 (11)이 U-프레임을 의미한다. 프레임 유형을 표기하는 5비트(P/F 비트 이전 2비트와 P/F 비트 이후 3비트)는 32개의 서로 다른 유형을 생성할 수 있다.

U-프레임은 프레임 유형 구분으로 5비트를 사용하는데 32개 보다 더 작은 프레임 유형이 사용 중이지만, 어떤 프레임 유형은 프레임이 전송되는 방향에 따라 (요청 혹은 응답) 서로 다른 의미를 가진다. 좌측에서 1, 2번 비트로 프레임 종류를 구분한다. Poll/Final (p/f) 비트의 사용은 상황에 따라 의미가 다르게 해석된다. 명령어 프레임에서 링크 끝단의 스테이션으로부터 응답을 요구할 때 p 비트를 1로 설정한다. 요청 프레임에 대한 응답을 나타내기 위하여 프레임이 f 비트를 1로 설정한다.

정보(Information) 필드와 FCS(fame check sequence)는 I-프레임과 몇몇 U-프레임에서 필드로 존재한다. 옥텟의 배수인 길이를 가지며 가변적이다. FCS는 오류검출을 위하여 사용되는데, 16 혹은 32비트 CRC(cyclic redundancy check)이다.

2.3 HDLC Operation

기본적으로 HDLC 동작은 I 프레임, S 프레임, 그리고 U 프레임의 교환으로 이루어지는데 3단계 과정으로 구성되어 있다.

1단계 : 초기화 단계 - 링크 양단의 어느 쪽이든 6개의 set-mode 명령을 사용하여 초기화를 요청할 수 있다.

2단계 : 데이터 전송 - 흐름제어와 오류제어를 하게 되며, I 프레임과 S 프레임(RR. RNR, REJ, SREJ)을 사용한다.

3단계 : 절단(Disconnect) - 오류(fault)를 통보 받았거나 상위 계층 사용자로 부터의 요청에 의하여 이루어지며 DICS(disconnect) 프레임을 보낸다.

그림 5는 HDLC의 동작 예시로서 링크 설정과 해지 및 양방향 데이터 전송을 나타낸다.

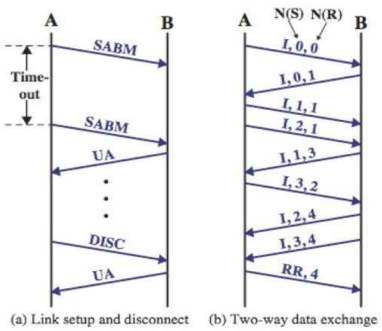

Fig. 5. HDLC Operation Example

3. Wireless LAN Data Link Security

802.11은 WLAN(Wireless LAN) 링크 보호 기술로서 많은 보안 결점이 발견되었다[6]. 802.11에 이어서 보안성이 증명된 기술들을 사용하여 보안성을 향상시킨 802.11i가 표준화 되었다.

802.11i는 인증방식, 키 교환방식, 암호알고리즘 등을 규정하는데, 인증 방식으로는 802.1x 기반 EAP 인증 프로토콜 사

용을 사용하며, 키 교환 방식은 사용되는 구체적인 EAP(Extensible Authentication Protocol) 인증 프로토콜에 따라 달라진다. 인증이 성공적으로 이루어지면 세션 키를 만들게 되고 암호 알고리즘을 사용하여 메시지 인증, 기밀성 그리고 무결성을 제공하게 된다. MACsec 무선링크 보안기술은 802.11i와 비슷하나 암호화 과정이 다소 다르다.

3.1 RSN (Robust Security Network)

EAP는 RSN 보안 채널 설정 프로토콜을 위한 메시징 프레임 워크를 제공한다. 그림 6은 RSN 무선 LAN 링크 보안기술의 계통도를 나타낸다. Pre-RSN은 RSN 이전의 무선 LAN 보안 기술을 의미하며 비도가 낮은 암호기술인 WEP-40 혹은 WEP-140을 사용하여 보안이 취약하다. 그리고 인증 방식에서도 사전 공유 키 인증 방식만 제공하였다. RSN은 암호알고리듬으로 RC-4를 채택한 TKIP을 WPA-1이라 부르고, AES를 채택한 CCMP를 WPA-2라 부른다. 인증방식으로는 사전에 대칭키를 공유하는 Shared key 방식과 802.1x/EAP 기반 인증방식이 있는데, 사용자가 많은 곳에서는 802.1x/EAP/Radius를 사용하는 경우 WPA-Enterprise라 부르고, 사용자가 적은 가정 혹은 소규모 사무실 환경에서 Shared key를 사용하는 경우 WPA-Personal이라 부른다. 802.1x/EAP 인증 기술은 인증기법에 따라 많은 종류가 존재한다. 대표적인 기법으로는 EAP-TSL, EAP-TTLS, Protected EAP(PEAP), EAP-FAST 등이 있다[7].

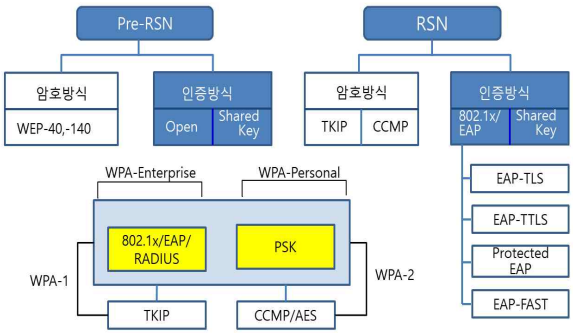

Fig. 6. RSN Data Link Security Technology Architecture for WLAN

3.2 EAP(Extensible Authentication Protocol)

EAP는 RFC 3747로 정의된 무선 네트워크와 포인터-to-포인터 연결에서 자주 사용되는 범용 인증 프레임워크이다. 802.1x는 LAN 상에서의 EAP를 구현한다. 그림 7은 LAN에서 EAP가 적용되는 구조를 나타낸다. EAPoL은 LAN 상에서 EAP 클라이언트(supplicant)로부터 인증자(Authenticator)로 EAP 메시지를 나르는데 사용되는 프로토콜이다. 인증 서버(Authentication Server)는 클라이언트와 단일 방향 또는 양방향 인증을 실시하는 백앤드 서버이다. 인증자와 인증 서버가 서로 다른 시스템에 존재하는 경우 RADIUS 혹은 Diameter 프로토콜을 사용하여 EAP 인증 메시지를 교환하게 된다. 클라이언트의 수가 많지 않을 경우 인증자와 인증 서버는 단일 시스템에 존재할 수 있다.

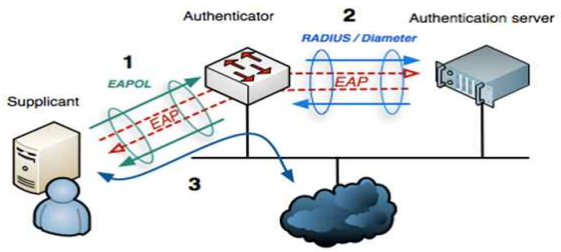

Fig 7. RSN WLAN Data Link Security with 802.1x/EAP Source from [8]

LAN에서 인증자는 유선 LAN의 경우 액세스 계층 스위치, 무선 LAN에서는 AP(Access Point)에서 구현된다. 인증자는 인증 서버로부터 클라이언트가 성공적으로 인증되었다는 메시지를(EAP-Success) 수신한 경우에 한하여 클라이언트가 LAN으로의 접속을 허용한다.

그림 8는 PPP(Point-to-Point) 혹은 이더넷(Ethernet) 상에서 EAP 메지의 캡슐화 형식을 나타난다. EAP는 Request, Response, Success 그리고 Failure 등 네 가지의 메시지가 있다.

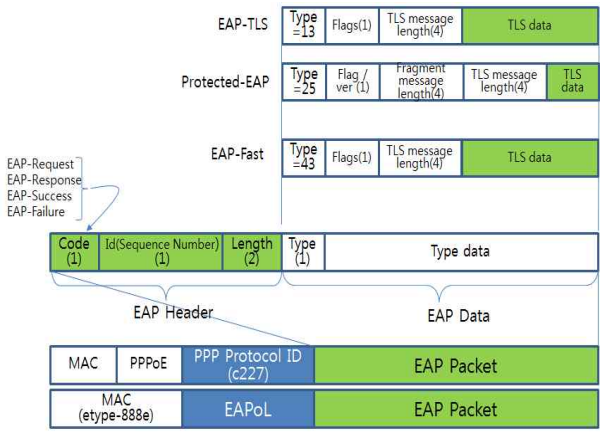

Fig. 8. EAP Packet Format over PPP or Ethernet

그림 9는 802.1x/EAP 메시지 흐름도를 나타낸다. 클라이언트의 인증요청 메시지(EAPoL-START)의 의하여 인증과정이 시작된다. 인증자는 클라이언트의 식별자(ID)를 획득하여 인증 서버에게 전달한다. 이어서 특정 EAP 프로토콜을 사용하여 인증처리 과정이 실행된다. 인증처리 과정이 종료되면 인증 서버는 성공/실패의 결과를 인증자에게 전달한다. 아울러 인증이 성공적으로 완료된 경우 인증 서버는 클라이언트와 공유한 암호키를 인증자에게 전달한다.

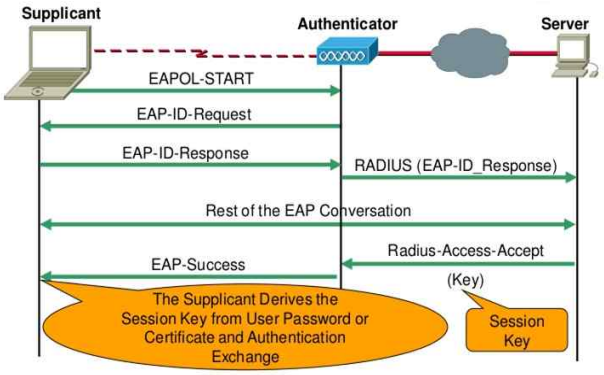

Fig. 9. Message Flow of 802.1x/EAP

3.3 RSN 4-Way Handshaking

단계 1에서는 RSN 지원여부 탐색과정, 개방 시스템 인증 및 결합(association)이 이루어진다.

단계 2에서는 802.1x/EAP 또는 PSK에 의한 사용자 인증 및 PMK(Pairwise master key)을 확보하는 단계로서 상호인증 방법으로는 802.1x/EAP 인증 방식 혹은 PSK(pairwise shared key) 인증방식 중 선택하여 사용할 수 있다. PMK 생성 방법에 있어서 802.1x/EAP 인증의 경우 LAN에 접속하려는 단말과 LAN 내부에 있는 인증서버가 상호 인증 후 MSK(Master Session Key)를 공유하게 된다. MSK로부터 PMK를 생성한다. AP용 MSK는 인증서버가 전달한다. PSK에 의한 사용자 인증의 경우 PSK로 부터 PMK 생성한다.

단계 3에서는 EAPoL-Key 프레임을 사용하여, 상대방에 대한 PMK 보유를 확인하고, 무선 구간 보호용 키를 생성하고 전달한다.

단계 4에서는 암호화된 데이터 패킷을 상호 교환하게 된다.

IV. Data Link Protection Scheme for HDLC-based MPI-CDL

1. Applying EAP on Point-to-Point Data Link of HDLC-based MPI-CDL

그림 10은 HDLC 기반 MPI-CDL 네트워크에서 데이터 링크 계층 보안을 위한 802.1x/EAP 인증 기술 적용 방안을 나타낸다. 최우선은 지상장비가 인증구조의 센터가 된다. N:1 구조는 점대점의 다중 연결로 볼 수 있다. 그리고 지상장비와 중계기 간에는 점대점 데이타 링크 구조이다, 일단 중계기는 지상장비로부터 인증을 받고나면 임무기에 대하여 인증자와 인증서버의 역할을 할 수 있다. 1:N 방송 구조에서는 사전에 대칭키를 설정한 상태에서 데이터를 암호화하여 전송하게 된다.

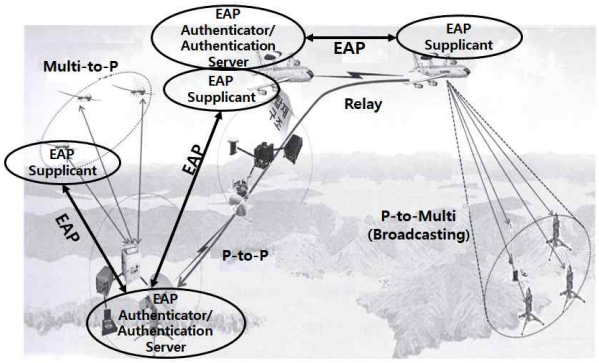

Fig. 10. EAP Authenticated MPI-CDL Data Link over HDLC

그림 11은 본 논문에서 제안하는 EAP-보안인증 적용을 위한 HDLC 링크 관리 메시지의 캡슐화 구조를 나타낸다. 링크 관리 메시지 전송을 위하여 U-프레임을 이용한다.

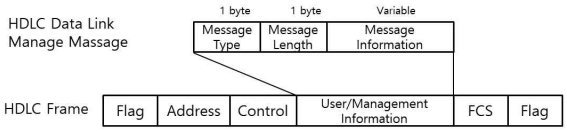

Fig. 11. Data Link Management Message Format over HDLC

표 1은 HDLC에서 인증을 위한 링크관리 메시지의 종류를 나타낸다. 메시지는 기능별로 채널설정, 인증절차, 채널종료, 그리고 방송채널 설정을 위한 것으로 구분된다. 그리고 각 메시지를 전송할 HDLC 프레임의 종류가 지정되어있다.

Table 1. Data Link Management Messages over HDLC

Link Manage	Message name/ID	HDLC Frame	Function
Channel Establishment	Auth offer / 1	SAMB	When SAMBA is sent by Authenticator for channel request, it carries RSNIE including available Cipher suit and AKM Suit for secure channel establishment.
	Association Request / 2	UI	Supplicant uses UI to carry RSNIE containing Cipher suit and AMK suit as secure channel association message.
	Auth Reply / 3	UA	Authenticator uses UA to carry reply message for Association Request (Success/Fail).
Authentication	EAP Data / 4	UI	UI are used to carry protocol message during EAP authentication process.
Channel Disconnect	DISC Request / 5	DISC	Supplicant uses DISC to carry disconnection request message to Authenticator.
	DISC Agree / 6	UA	Authenticator uses UA to carry disconnection agreement message to Supplicant.
Broadcast channel management	Broadcast Cipher Suit Request / 7	SNRM	The primary station uses SNRM to carry Cipher Suit information for secure channel establishment in 1:N broadcasting mode.
	Broadcast Key Distribute / 8	UI	The primary station uses UI to carry group key transfer protocol messages for channel protection in 1:N broadcasting mode.

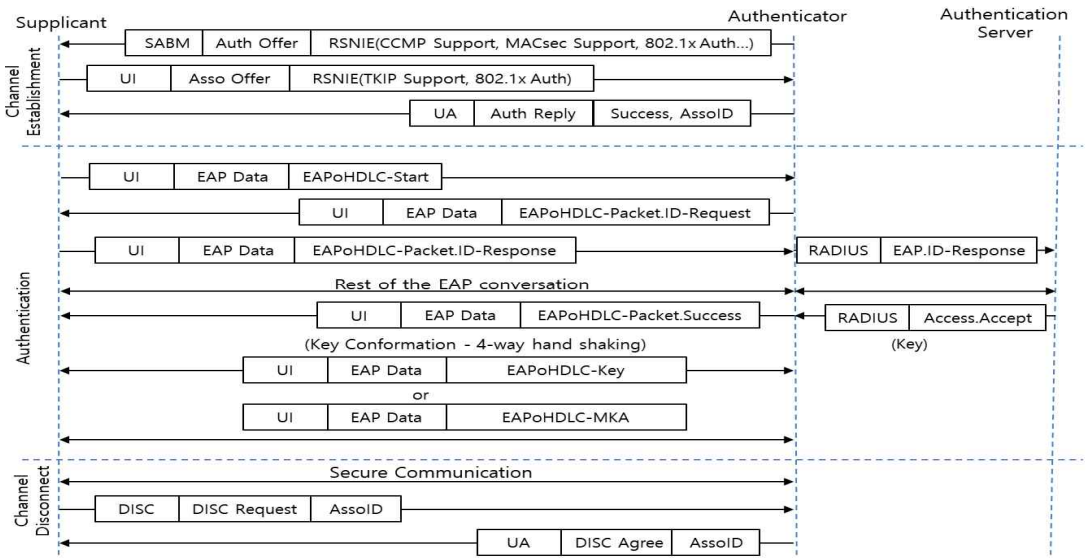

Fig. 12. EAP Procedure for MPI-CDL Data Link over HDLC

SAMB : Set asynchronous balanced mode
SARM : Set asynchronous mode
UI : Unnumbered Information
UA : Unnumbered Acknowledgement
DISC : Disconnect

그림 12는 HDL기반 MPI-CDL 점대점 혹은 점대다 데이터링크에서 EAP 프로토콜의 메시지 흐름을 나타난다.

단계 1: 채널 설정

채널설정 동안 클라이언트와 인증자는 1) 데이터 트래픽 기밀성, 무결성 보호를 위한 주요 보안 기능, 2) 상호 인증을 위한 인증 기법, 3) 암호학적 키 관리 접근법, 4) 사전인증 능력 등을 협의한다. 인증자가 인증지원 제공 사항들을 보내면, 클라이언트는 이용 가능한 인증 스팩으로 보호연관(security association) 요청을 한다. 이에 응답하여 인증자는 보호연관 식별자(AssoID)를 포함한 인증 승인 메시지를 보낸다.

링크 보호연관에 관해서는 보안정책과 암호학적 키 등을 포함하여 RSN Information Element(RSNIE)라는 이름으로 802.11에서 사용하며 메시지 포맷은 그림 13과 같다. MPI-CDL 점대점 링크에서는 그룹전송이 없으므로 원 메시지 포맷에서 그룹 키에 관한 필드는 제외하였다.

기밀성과 무결성 보호를 위하여 802.11i에서는 보안 파라미터로 cipher suite는 1) 00-0F-AC-04(CCMP-default), 2)00-0F-AC-02(TKIP-optional), 3) 00-0F-AC-05(WEP-104), 4) 00-0F-AC-01(WEP-40)등이 있다. MACsec의 적용을 고려하여 5)00-0F-AC-06(GCM-AEC-128, MACsec default), 6) 00-0F-AC-07(GCM-AEC-256),7) 00-0F-AC-08(GCM-AEC-XPN-128), 8) 00-0F-AC-09(GCM-AEC-XPN-256)을 추가한다. 표 2는 IEEE에서 지정한 MACsec cipher suite 들의 이름 및 주요 서비스 내용을 나타낸다.

인증과 키 관리를 위한 보안 파라미터로 AKM(Authentication and Key Management) Suit로 1) 00-0F-AC-01 (802.1X) 2) 00-0F-AC-02 (PSK, pre-shared key), 그리고 3) 00-0F-AC-03 (FT over 802.1X) 등이 있다.

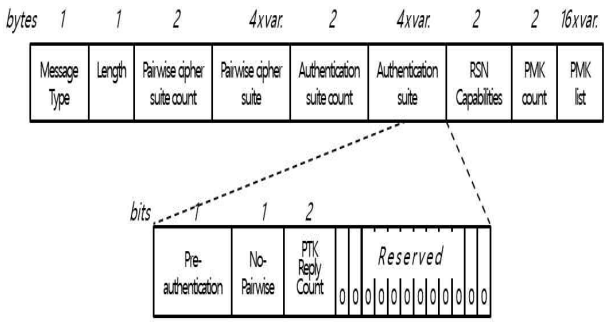

Fig. 13. Message Format of RSNIE

Table 2. MACsec Cipher suit

Cipher Suite Name	Services provided		Mandatory/ Optional
	Integrity Only	Integrity and confidentiality	
GCM-AES-128	Yes	Yes	Mandatory
GCM-AES-256	Yes	Yes	Optional
GCM-AES-XPN-128	Yes	Yes	Optional
GCM-AES-XPN-256	Yes	Yes	Optional

단계 2: 인증(Authentication)

HDLC에서 EAP를 적용하기 위하여 EAPoL처럼

EAPoHDLC를 정의한다. EAPoHDLC는 표 3과 같이 4개의 메시지를 갖는다. 그림 14는 EAPoHDLC 메시지 형식을 나타낸다. 이 메시지는 그림 12에서와 같이 HDLC의 UI 프레임을 사용하여 전송되며 표 1의 EAP 관련 링크관리 메시지 중 EAP data 메시지에 캡슐화 되어 전송된다.

인증과정은 클라이언트가 EAPoHDCL-Start 메시지를 인증자에게 보내어 인증요청에 의하여 인증과정이 착수된다. 인증이 성공적으로 이루어지면 클라이언트와 인증 서버는 동일한 키를 공유하게 된다.

IEEE 802.1X에서 사용되는 인증 알고리듬으로는 EAP Transport Layer Security (EAP-TLS), Protected EAP Microsoft Challenge Handshake Authentication Protocol Version 2 (PEAP-MSCHAPv2), and EAP Flexible Authentication via Secure Tunneling (EAP-FAST) 등이 있다[8]. HDLC 기반 MPI-CDL 데이터링크에 적합한 특정 EAP 기법 선정에 관한 연구는 본 논문의 연구범위에서 제외한다.

Table 3. Type and Function of EAPoHDLC Messages

Message name	Function	Direction
EAPoHDCL -Start	Client check if an authenticator exist and notify that it is ready to start authentication process.	Su → Au
EAPoHDCL -Key	After successful mutual authentication, an encryption key is established. Used to verify that each ends have the right key.	Su ↔ Au
EAPoHDLC -Packet	Used to transfer EAP messages.	Su ↔ Au
EAPoHDLC -MKA	Used to transfer MACSec Key Agreement (MKA) protocol messages.	Su ↔ Au

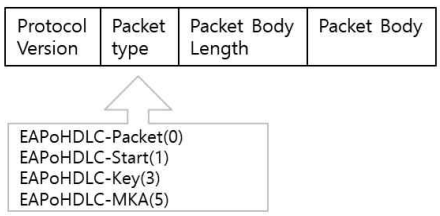

Fig. 14. EAPoHDLC Message Format

EAP 과정에서 성공적으로 인증이 실행되면 인증 서버는 인증자에게 공유키를 전달한다. 인증자는 전달 받은 키가 클라이언트와 동일한 키를 보유하고 있는지 확인하는 4 단계 공유 키 확인 및 세션 키 생성 과정을 거치게 된다. EAPoL의 키 분배 및 관리 기술을 적용한다면 기존의 RSN에서 제공하는 EAPoL-Key 메시지를 활용하게 된다[6]. MACsec을 적용하는 경우에는 MACsec Key Agreement(MKA)를 사용하여야 한다[9]. MPI-CDL을 위한 링크 보안 구조에서는 표 3과 같이 EAPoL-Key를 EALoHDLC-Key로 정의하고 MAK를 EALoHDLC-MKA로 정의하였다.

단계 3 : 데이터 교환

4 단계 공유 키 확인 및 세션 키 생성 과정을 거쳐 생성된 세션 키를 사용하여 보안 데이터 채널을 구성하게 된다. 이때 HDLC의 I-프레임을 사용하여 그림 5(b)와 같이 양방향 데이타 교환이 이루어진다.

단계 4 : 채널종료

클라이언트나 인증자는 HDCL DISC 프레임을 사용하여 채널 종료를 요청하면 링크의 다른 쪽 스테이션은 UA 프레임을 사용하여 채널 종료를 수락하게 된다. 양 방향 메시지에는 각각 보호연관 식별자 AssoID를 포함하게 되므로 링크 절단 시 이와 관련된 보호 연관도 제거한다.

2. Channel Protection Scheme for T4 Class Point-to-Multi Mode Data Link

그림 1의 운용 모드에서 나타낸 바와 같이 점대점, 다대점, 그리고 중계 등의 모드에서는 양방향 통신이 가능하므로 양방향 인증이 가능하다. 하지만 점대다 모드에서는 일방향 브로드캐스팅 모드로 운용되므로 양 방향 인증을 할 수 없으며 단지 GDT에서 ADT를 인증하는 것 만 가능하다. 나머지 모드들과는 다른 방식의 링크보안 기술이 적용되어야 한다.

브로드캐스팅 모드는 사전에 공유한 키에 의한 키 공유 확인으로 인증하는 것이 보편적이다[10]. 이 때 작전 기간 동안 정적/수동으로 공유키가 각 장비에 주입될 수 있다. 만약 GDT가 탈취될 경우 패스워드가 노출되어 패킷을 사전에 수집한 경우 정보가 적군에 노출 될 수 있다. 그리고 동적으로 키가 공유되지 않는 경우 탈취 이후의 정보도 적군에 노출될 수 있다. 이 경우 전 방향 안전성(forward secrecy)에 취약 하게 된다. 따라서 점대다 모드에서는 방송키의 동적 생성 및 삭제, 멤버 관리 등의 키 관리를 매우 엄격히 할 필요가 있다. 본 절에는 이러한 제약조건에 적합한 동적 키 생성 및 전달 기술로 신원기반 방송암호 기법[11]을 적용한다.

2.1 ID-based Public Key Crypto System

신원기반 공개 키 암호 시스템에 관련된 주요 개체로는 신뢰하는 키 생성 센터(Trusted Key Generation Center, KGC)와 사용자들이다. 두 개의 그룹 G_1과 G_2에 대하여 겹선형(bilinear) 페어링 연산 $e : G_1 \times G_1 \rightarrow G_2$를 정의한다. 시스템 공개 파라미터 $params = \{G_1, G_2, q, P, P_{pub}, H_1, H_2\}$을 공개한다. 여기서 임의의 생성자 $P \in G_1$, 암호학적 해쉬함수 $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : G_2 \rightarrow \{0,1\}^*$와 같이 정의되며, 시스템 셋업 단계에서 KGC는 임의의 난수 $s \in Z_q^*$를 생성하고 공개 키 $P_{pub} = sP$를 계산한다. 그리고 마스트 키 s를 안전하게 보관한다. 사용자용 개인 키 분배 단계로서 사용자는 자신의 신원정보 ID를 KGC에 제출한다. 이어서 KGC는 사용자의 공개 키 $Q_{ID} = H_1(ID)$

를 계산하고 이에 대응하는 개인 키 $S_{ID} = s\,Q_{ID}$를 계산하여 사용자에게 안전하게 전달한다.

2.2 ID-based Broadcast Encryption for Key Distribution[11]

(1) 암호화 및 복호화 과정

사용자들 $U = (ID_i | i = 1,...,n)$에게 공통키를 분배하고자 한다. 각 사용자는 공개/개인 키 쌍 (Q_i, S_i)를 가지고 있다. 사용자 집합 U에게 공통키 k를 분배하는 과정은 다음과 같다.

암호문은 아래 수식 (1)과 같다. 이 암호문을 방송수신자 집합 U에게 전송한다.

$$(U_i, 1 \le i \le n, V) = (rP, rQ_{V_2}, rQ_{V_3}, \dots, rQ_{V_n}, V) \quad (1)$$

여기서 $U_1 = rP$, $U_i = rQ_{V_i}$, $2 \le i \le n$, $Q_{V_1} = \sum_{i=1}^{n} Q_i$, $Q_{V_2} = Q_1 + Q_2$, $Q_{V_3} = Q_1 + Q_3$, ..., $Q_{V_n} = Q_1 + Q_n$, $V = k \oplus H_2(e(P_{pub}, rQ_{V_1}))$ 로 주어진다.

이제 수신자 ID_i는 자신의 개인키 S_i를 사용하여 식 (2)를 계산하여 방송 암호용 비밀 키 k를 복호한다.

$$k = V \oplus H_2(e(P_{pub}, rQ_{V_1})) \quad (2)$$

$$= V \oplus H_2\left((e(U_1, x_1 S_i).e\left(P_{pub}, \sum_{i=2}^{n} x_i U_i\right)\right) \quad (3)$$

식 (1)과 식 (3)에서 알 수 있듯이 수신자 ID_i는 자신의 개인키 S_i와 수신된 값 $U_i, i = 2,...,n$, 그리고 수신 측에서 간단히 $n \times n$ 행렬식을 풀어 간단히 구할 수 있는 $x_i, i = 1,...,n$ 값으로부터 암호를 풀 수 있다.

(3) 암호 알고리즘 복잡도 분석

식 (1)~(3)으로 주어지는 방송 암호기법을 사용하여 그림 1의 임무기에서 100대의 지상장비로 방송 암호용 키를 분배할 경우 가정하여 통신량과 계산량을 분석한다.

암호화와 복호화에 필요한 계산적인 복잡도는 표 4와 같이 분석된다. 표에서 n은 방송신호를 수신할 지상장비의 수를 말한다. 계산 량을 지배하는 것은 타원곡선 곱셈과 페어링(paring)이다. 나머지 항목은 이 두 요소에 비하여 무시할 만하다.

표 5는 MIRACL 암호 패키지의 밴치마킹 자료에서 발췌한 타원곡선 암호 계산 요소별 속도를 나타낸다[12]. AES 128 비트 및 256비트 암호에 준하는 비도를 갖는 타원곡선 암호 알고리즘의 계산속도이다. 표 6은 표 4와 5로부터 수신장비가 100개인 경우 각 장치에서 소요되는 방송 암호 및 복호에 소요되는 계산 속도를 나타낸다.

통신량은 11회 브로드케스팅에 식 (1)에서와 같이 타원곡선 요소 101개를 전송하야 한다. 128비트 등가 강도를 가정하면 512비트 유한체 상에서 타원 곡선을 구현하는 경우, 타원곡선 점 한 개에 513비트를 전송하여야 한다. 따라서 약 50kbits의 데이터 전송이 요구된다. 256비트 등가 강도의 경우 약 64kbis의 데이터 전송이 요구된다. 하지만 이것은 오직 보안 채널 설정 시 1회에 한하여 요구된다.

본 절에서 제시한 암호알고리듬을 사용하여 방송용 키를 전송할 경우 다양한 장점이 있다. 키를 재설정 할 때 마다 키 분배 센터에서 렌덤하게 세션 키를 선택할 수 있으며, 각 세션키는 상호 독립적이다. 그래서 전 방향 안정성(forward secrecy)과 후 방향 안전성(backward secrecy)을 제공해 준다. 또한 키 분배를 위한 별도의 보안 채널이 요구되지 않고 한 라운드 방송만으로 키를 분배할 수 있다. 사용자 그룹에 변화에 있더라도 1회 키 전달 방송만으로 키를 재설정 할 수 있으므로 다른 복잡한 키 재설정 프로토콜이 필요하지 않다.

Table 4. Computational Complexity Analysis of Broadcast Encryption Scheme[11]

Operations	Encryption by the Center	Decryption by each user
EC Point Addition in G_1	2n-2	n-1
Scalar multiplication in group G_1	n+1	n
Paring	1	2
Hashing	1	1
XOR	1	1
Solving a set of linear equation with n variables using Cramer's Rule	-	1

Table 5. Computational Speed Bench Marking for Broadcast Encryption Scheme[11]

[msec]

*Operation		†AES-128bit equivalent	‡AES-256bit Equivalent
Scalar Multiplication		2.57	1.26+16.04=17.3 **(0.43+5.44=5.87)
***Pairing	Single	19.00	33.91(30.45)
	One More	N.A	6.59(3.42)

* 2.4GHz, Intel i5, 520 CPU

** ( ) 안은 Pre-computation 사용 시의 수행시간

*** paring에서 AES-128의 경우 Type-1 Paring $G_1 \times G_1 \rightarrow G_T$, AES-256의 경우 Type-3 $G_1 \times G_2 \rightarrow G_T$ pairing

† : GF(p), p = 512비트 Modulo

‡ : GF(p), p = 640비트 Modulo

Table 6. Computation speed of broadcast encryption for each entity with 100 receivers.

[msec]

Device \ AES level	128bit	256bit
Center	278.57	623.32
Receiver	295.00	620.87

(4) MPI-CDL 점대다 모드에서의 채널 보호 방안

1.2절에서 언급한 바와 같이 HDCL에서 주소는 데이터 프레임을 수신할 스테이션의 주소를 의미한다. 특히, 주소 값이 모두 일일 때(11111111) 방송 주소이며 주소는 7비트 단위로 확장가능하다. HDLC 프로토콜에서 NRM에서는 오직 1차 스테이션만 데이터 전송을 시작할 수 있는 방송모드이므로 MPI-CDL 점대다 링크에 적합하다[13]. 2차 스테이션은 1차 스테이션의 Poll에 응답하여 데이터를 전송할 수 있으므로, 그림 1에서와 같이 Point-to-Multi 모드에 서 특정 GDT에서 ADT로 선택적 데이터 전송도 가능하다.

그림 15는 HDLC 기반 점대다 방송채널 보호방안을 나타낸다. 안전한 채널 설정은 2 단계로 이루어진다. 먼저 브로드 캐스팅 키 전달에 관련된 암호방식 및 시스템 파라미터, 브로트 캐스팅 패킷 암호방식 등의 정보를 포함하는 Broadcast Cipher Suit Request 메시지(표 1참조)를 SNRM 프레임으로 캡슐화하여 방송한다. 이어서 [11]의 방송암호 기법을 사용하여 방송 데이터 암호를 위한 비밀 키를 전송하는 Broadcast key Distribution 메시지를 UI 프레임으로 캡슐화하여 방송한다. 그 이후에는 안전한 방송이이루어 지며 방송 종료 후에는 DISC 프레임으로 채널을 종료한다.

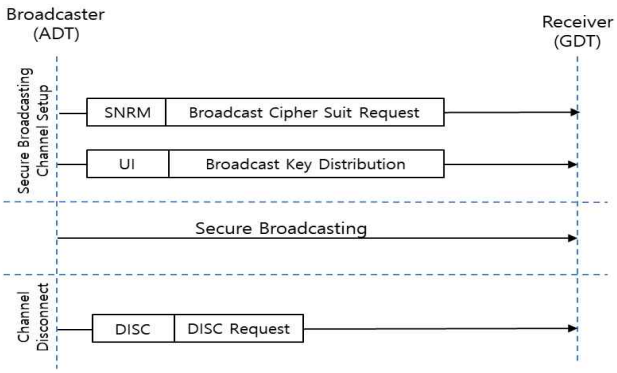

Fig. 15. Securing Point-to-Multi Broadcasting Channel over HDLC

V. Conclusion

본 논문에서는 HDLC 프로토콜을 기반으로 하는 MPI-CDL 네트워크에서 데이터 링크 보안을 위한 방법으로 무선 LAN 및 이동통신망 등에서 널리 사용되고 있는 EAP 방식의 RSN 기술을 적용하는 방안에 관하여 연구하였다. 그리고 기존의 RSN 보다 더 높은 안전성을 제공하는 MACsec을 적용하는 방안도 제시하였다.

점대점 모드와 다대점 모드는 양방향 통신이므로 EAP 방식의 RSN을 적용할 수 있으나, 점대다 모드는 일 방향 방송 채널이므로 안전한 방송용 암호 키를 공유 기술을 적용하여야 한다. 본 연구에서는 타원곡선 암호 기술을 활용하여 1회 방송 데이터 전송으로 안전하게 암호 키를 전송 할 수 있는 방안을 제시하였다. 아울러 계산적, 통신적인 측면에서 복잡도를 분석하여 실용 가능성도 파악하였다.

REFERENCES

[1] W.-P. Kang, J.-Y. Song, K.-H. Lee, D,-H. Lee, S.-J. Jung, H.-J. Choi. “Analysis of Common Data Link Technology Trends for the Next Generation Korean Common Data Link Development”, The J. of Korea Inform. and Commun. Society, vol.39C no.3, pp.209-222, March, 2014.

[2] E. S. Lim, "Concept of tactical data link employment and next C4ISR system," Quart, J. Defence Policy Stud., vol. 74, pp. 49-83, 2007.

[3] J. S. Kim, S. J. Kim, and M. Y Lim, "Overview of tactical data link technology," J. KISSE, vol. 74, no, 9, pp. 18-28, Sept. 2007.

[4] J. S. Eum and B. O. Ahn, "Development trends and preview point of MPI-CDL in Israel," KIDA Defense Weekly, no. 1404, Apr. 2012.

[5] J. M. Chung, K. C. Park, T. Y. Won, U. H.Oh, D. C. Ko, S. J. Hong, C. B. Yoon, H.Kim, and U. Y. Pak, “Standardization strategy for the image and intelligence common data link,” The J. Korean Inform. Commun. Mag., vol. 28, no. 4, pp. 41-50, Apr. 2011.

[6] Sheila Frankel, Bernard Eydt, Les Owens, Karen Scarfone, NIST Special Publication 800-97 - Establishing Wireless Robust Security Networks: Guide to IEEE 802.11i. Feb. 2007, NIST. URL- http://nvlpubs.nist.gov/nistpubs /Legacy/SP/nistspecial-publication800-97.pdf

[7] https://en.wikipedia.org/wiki/Extensible_Authenticatio n_Protocol

[8] https://en.wikipedia.org/wiki/IEEE_802.1X

[9] IEEE, 802.1x-2010, http://standards.ieee.org/getie ee802/download/802.1X-2010.pdf

[10] Jeremy Horwitz, “A Survey of Broadcast Encryp tion,” Jan. 2003 URL- http://xenon.stanford.edu/ ~horwitz/pubs/broadcast.pdf

[11] Du, Xinjun, et al. "An ID-based broadcast encrypti on scheme for key distribution." IEEE Transactions on broadcasting, vol 51, no.2 pp.264-266, June 2005.

[12] https://libraries.docs.miracl.com/

[13] https://en.wikipedia.org/wiki/High-Level_Data_Link_ Control

Authors

Sang-Gon Lee received the B.S., M.S. and Ph.D. degrees in Electronics Engineering from Kyungpook National University, Korea, in 1986, 1988 and 2003, respectively Dr. Sang-Gon Lee joined the faculty of the Department of Electronic Communication at Changshin University, Changwon, Korea, in 1997 and is currently a Professor in the Division of Computer Engineering, Dongseo University. He is interested in cryptography, design and analysis of cryptographic protocols, network security, software defined network, block chain.

Hoon-Jae Lee received the B.S., M.S. and Ph.D. degree in Electrical Engineering from Kyungpook national university in 1985, 1987 and 1998, respectively. Dr. Lee had been engaged in the research on cryptography and network security at Agency for Defense Development from 1987 to 1998. Since 2002 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor. His current research interests are in security communication system, side-channel attack, USN & RFID security. He is a member of the Korea institute of Information security and cryptology, IEEE Computer Society, IEEE Information Theory Society and etc

Hyeong-Rag Kim received the B.S., M.S. and Ph.D. degrees in Electronics Engineering from Kyungpook National University, Korea, in 1992, 1994 and 2010, respectively Dr. Kim joined the faculty of the Department of Information&Telecommunications at Pohang University, Pohang, Korea, in 1996. He is currently a Professor in the Department of IT&Electronics, Pohang University. He is interested in channel coding, cryptography and network security.