Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Logical Subnet Configuration Scheme Using Cryptography in Tactical Data Link Environment

Seung-Bae Ji[1], Cheol Jin[1], Kyung-Mi Park[1], Heon-Jai Park[*2], Chang-Ho Park[2], Jeong-Hyun Ahn[3], Kang Lee[3]

[1]*Agency for Defense Development*
[2]*Link Nine System Corp.*
[3]*SsangYong Information & Communications Corp.*

ABSTRACT

TDL provides common situation awareness and simultaneous decision making power through real-time and near real-time information sharing to all warfighters. Accordingly, The ROK forces, which have to carry out various operational missions, make various efforts to acquire TDL for joint and combined operations in various weapons systems such as command post, ship, airplane, tanks, and etc. However, it takes a lot of money to acquire such ability. Accordingly, there is a need for an alternative for minimizing the cost increase and improving the TDL operation capability in the existing operation. In this paper, we propose an alternative method to expand the TDL through logical subnet configuration using ARIA encryption technology instead of adding individual network through the acquisition of new equipment. The proposed logical subnet configuration method shows that various logical subnets can be configured for each group on the TDL sharing information in the existing broadcast network. Through the system implementation, we confirmed the validity and feasibility of the technique. In the future, based on this paper, it is expected that further study on the ROK TDL subnet operation method and the performance improvement of each weapon system platform. Through these studies, we hope to contribute to the improvement of ROK military mission performance and economic military operation.

KEYWORDS: TDL(Tactical Data Link), Logical Subnet, Cryptography, ARIA(Academy, Research Institute, Agency), DLP(Data Link Processor)

ARTICLE INFO: Received 16 August 2017, Revised 31 August 2017, Accepted 13 October 2017.

[*]Corresponding author is with Link Nine System Corp., (420. Migun Techno World 1-cha, Yongsan-dong) 199, Techno 2-ro, Yuseong-gu, Daejeon, 34025, Republic of KOREA.
E-mail address: tompy@lnsystem.co.kr

1. 서 론

전술데이터링크(TDL : Tactical Data Link)는 모든 전투원(Warfighter)에게 실시간(Real-time) 혹은 근실시간(Near Real-time) 정보공유를 통해 공통상황인식(Common Situational Awareness)과 동시 의사 결정력을 제공하며, 공유된 전술 정보에 대한 정보융합(Data Fusion)으로 감시/타격 및 지휘통제 체계 간 교전통제 등의 전술 작전을 수행하는 기능을 제공하여, 서로 다른 군사전력 체계들 간에 실시간 지능-감시-정찰(ISR : Intelligence, Surveillance & Reconnaissance) 자료공유를 위한 필수적인 요소가 되었다. 이와 같은 중요성에 따라 각국에서는 전술데이터링크를 구축하여 운용 중에 있으며, 대부분의 국가에서 미국의 전술데이터링크인 Link-11과 Link-16을 운용하고 있고, NATO 국가의 경우 Link-22 운용을 확대하고 있다. 특히, 미국은 Link-11, Link-16, Link-22 및 VMF를 기반으로 협동교전능력(CEC : Cooperative Engagement Capability) 및 전술표적추적(TTNT : Tactical Targeting Network Technology) 데이터링크 개발에 주력하는 등 전 세계 전술데이터링크 발전을 선도하고 있다.

우리 군에서도 전술데이터링크를 무선(VHF/UHF, HF) 또는 위성 통신을 이용하여 방송망(Broadcast) 방식으로 운용하고 있으나, 망 특성 상 다양한 네트워크 구성이 어렵고, 별도 채널의 망 구성을 위해서는 관련 전술데이터링크 구성 장비를 새롭게 구성해야 하므로 많은 비용이 발생한다.

현재 시분할다중접속(TDMA : Time Division Multiple Access) 통신방식을 적용하는 한국형 합동전술데이터링크(Link-K)에서 일부 기술개발을 진행하고 있으나 단기간 내 적용이 어려운 상황이며, 타 전술데이터링크(Link-11, KVMF 등)에 적용할 수 없는 제한점을 가지고 있다. 즉, 우리 군에서 운용하는 전술데이터링크는 군 무선 통신망(VHF/UHF, HF) 또는 위성 통신망에서 전술상황의 실시간 공유를 위해 방송망(Broadcast) 방식으로 전파되며, 한 노드가 송신한 정보는 모든 노드가 동일하게 수신되는 운용 구조를 가지고 있어 동일 네트워크 통신망 상에서 개별 네트워크 구성이 곤란하다. 또한, 개별 가입자 그룹별 서브넷 구성을 위해서는 기존 무선 또는 위성용 데이터링크 터미널 장비를 수정 또는 교체가 필요하게 되는데, 이에 따른 추가적인 장비 교체 비용이 발생한다. 이러한 전술데이터링크 운용상의 제약점과 과다한 교체 비용 발생을 해결하기 위해 기존 방식의 시스템에서 추가적인 장비 도입이나 과도한 SW의 수정 없이 동일한 효과를 낼 수 있는 그룹별 논리적 서브 네트워크를 구성하는 방법이 요구된다.

또한, 논리적 서브넷 구성을 위해 본 연구에서는 블록암호화 기술인 ARIA(Academy, Research Institute, Agency)를 적용하였다. ARIA 암호 알고리즘은 전자정부 구현 등으로 다양한 환경에 적합한 암호 알고리즘이 필요함에 따라 국가보안기술연구소(NSRI) 주도로 학계, 국가정보원 등의 암호기술 전문가들이 힘을 모아 개발한 국가 암호화 알고리즘으로써, 경량 환경 및 하드웨어 구현을 위해 최적화된 범용 블록 암호화 알고리즘이다.

실제 군 전술데이터링크에 적용되는 암호화 알고리즘은 전술데이터링크별로 별도 개발되어 적용되어 운용할 예정이며, 본 연구에서는 군 전술데이터링크에서 방송망(Broadcast) 방식으로 정보를 공유하는 전술데이터링크 참여 노드에 대해 기 개발되어 공개된 ARIA 암호 알고리즘을 이용하여 가입자 그룹별로 별도 네트워크를 구성할 수 있는 논리적 서브넷 구성 방법을 제안하고, 연구에 대한 결과물을 시스템 상 구현함으로써 서브넷 구성의 가능성을 확인하고자 한다.

2. 관련연구

2.1 전술데이터링크 운용현황

전장상황의 실시간 공유 및 효율적 지휘통제를 위해 각국에서 운용중인 주요 전술데이터링크를 정리하면 다음의 <표 1>와 같다[1].

표 1. 각국의 전술데이터링크 운용현황
Table 1. Tactical Data Link Operation Status of Each Country

Nation	Link-11/16/22, VMF				ETC
USA	Link-16	Link-11/11B	Link-22	VMF	CEC, TTNT, CDL
England	Link-16	Link-11	Link-22	VMF	CDL, STDL, IBS, BOWMAN, HeATS
France	Link-16	Link-11	Link-22		Link X, Link Y
Turkey	Link-16	Link-11/11B	Link-22		IJMS, Link-1
Sweden	Link-16	Link-11	Link-22	VMF	OPTASK Link, TADCOM
Norway	Link-16	Link-11/11B			Link-1
Netherlands	Link-16	Link-11/11B	Link-22		HDL, SATCOM, EUROGRID, TCDL, CDL
Australia	Link-16	Link-11		VMF	TCDL, Link-1
Canada	Link-16	Link-11	Link-22		
Denmark	Link-16				
Japan	Link-16	Link-11			

우리 군에서 운용하는 전술데이터링크의 무기체계별 적용 현황 및 계획을 살펴보면 <표 2>와 같다.

표 2. 우리 군 무기체계별 전술데이터링크 적용 현황/계획
Table 2. Status and Plan of TDL by ROK Weapon System

Weapon system	KOREAN TDL			US/NATO TDL	
	Link-K	KVMF	ISDL	Link-16	Link-11
Command & Control		△	○	○	○
Army Surveillance & Reconnaissance		△			
Maneuver		△			
Warship	△		○	○	○
Aircraft	△	△		○	○
Firepower		△			
Protect		△			

Legend : △ Planning ○ Operation

2000년대 초반까지 각 무기체계들 사이의 자료 교환은 전적으로 미국/NATO 표준을 준용한 전술데이터링크 장비 및 SW에 의존하여 수행되어 왔으나, 2000년 대 중반 이후부터 우리 군은 미국 육군의 전술데이터링크인 VMF와 해/공군의 Link-11/16을 각각 KVMF 및 ISDL, Link-K로 국산화하여 발전시켜 왔고 실전에 배치되어 운용되거나 운용할 예정이다[2].

2.2 전술데이터링크 구성

전술데이터링크는 일반적으로 전술정보 송·수신을 위해 <그림 1>과 같이 호스트 컴퓨터, 데이터링크 처리기(Data Link Processor), 암호장비, 데이터링크 터미널 장비, 통신장비 등의 분리된 요소들로 구성되며, 무선 및 위성 통신망을 사용하여 방송망(Broadcast) 방식으로 전술상황을 공유한다.

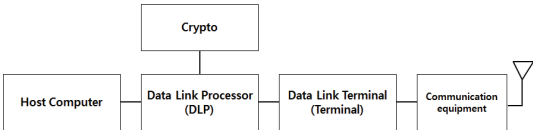


그림 1. 전술데이터링크 일반 구성
Figure 1. General Configuration of Tactical Data Link

호스트 컴퓨터는 운용자에게 전술상황을 전시하여 전장상황을 공유 하도록 하는 기능을 담당하고, 데이터링크 처리기에서는 전술데이터링크별 메시지 및 프로토콜을 처리하는 역할을 수행한다. 데이터링크 터미널 장비는 전술데이터링크의 핵심 구성요소로써 망 통제 및 모뎀 기능을 수행하며, 통신장비는 변·복조된 신호를 송·수신하는 기능을 수행한다. 보안장비는 메시지를 암·복호화 하는 MSEC((Message Security)과 통신기의 송·수신 신호를 암·복호화 하는 TSEC(Transmission Security)으로 구분 운용되며, 암호화 유형은 <표 3>와 같다[3].

표 3. 암호화 유형
Table 3. Type of Security

Type	Type of Security
MSEC	Encryption of Message Data
TSEC	Encryption of Waveform: • Jitter • Pseudorandom noise • Frequency-hopping pattern

2.3 미군 운용 사례

미군의 Link-16 전술데이터링크에서는 TDMA 통신 구조를 이용하여 동일 네트워크 상에서 다수의 참여 노드가 별개의 그룹망을 구분하여 사용할 수 있도록 멀티넷(Multiple nets) 운용 방식을 채택하여 적용하고 있다.[4]

Link-16의 TDMA 구조는 1개의 타임슬롯이 7.8125 msec의 주기를 가지게 설계되었고, 98,304개의 타임슬롯이 1개의 에폭(Epoch)으로 구성된다. 이때, 에폭(Epoch)은 12.8분의 주기를 가지게 되며, 24시간을 기준으로 볼 때 112.5 에폭(Epoch)으로 구성된다. 그러나 12.8분이라는 에폭(Epoch)의 주기는 실시간성이 요구되는 전술데이터링크 특성을 고려할 경우 네트워크를 설계하고 관리하기에는 너무 광범위한 시간 주기를 가지게 되어, 프레임(Frame)이라는 새로운 개념을 도입하였다. 프레임(Frame)은 12초 주기로 에폭(Epoch)을 세분화하여 64개의 프레임(Frame)으로 관리 및 운용될 수 있도록 하고, 각 참여노드별로 아래 수식 1을 이용하여 타임슬롯을 할당하여 운용한다[5].

$$TS = I_n + (TS_i \times TS_n) \quad (1)$$

TS: 타임슬롯 번호 I_n: 시작번호
TS_i: 지정된 RRN의 Set내 타임슬롯 간격
TS_n: 지정된 RRN의 타임슬롯 개수 범위

이러한 프레임을 싱글넷(Single net)으로 구분하고 이를 쌓아 올린 구조의 멀티넷을 구성하여 운용한다. 이러한 멀티넷 구조는 동일 타임슬롯에서 다른 그룹과 별도의 메시지 교환을 위해 참여 그룹별로 허용되게 운용함으로써 그룹별 서브넷을 구성할 수 있도록 지원한다.

2.4 블록 암호 알고리즘

국내에서 사용되는 블록 암호 알고리즘에는 SEED, ARIA(Academy, Research Institute, Agency), HIGHT 등 다양한 블록 암호화 알고리즘이 존재한다. 이중 SEED-128은 128비트 키만을 지원하므로 활용 분야가 제한적이며, HIGHT 암호 알고리즘은 RFID, USN 등과 같이 저전력·경량화를 요구하는 컴퓨팅 환경에서 기밀성을 제공하기 위해 2005년 KISA, ETRI 부설연구소 및 고려대가 공동으로 개발한 64비트 블록암호 알고리즘이다. ARIA는 차분 공격, 선형 공격과 같은 보안 공격에 비교적 안정적이다. 키의 크기에 비례해 AES와 유사하게 12, 14 혹은 16번의 라운드 함수를 반복 수행하며, 우정사업본부에서는 최근 일반적인 암호화 대상 항목인 주민등록번호, 외국인등록번호, 여권번호, 운전면허번호 등 고유식별번호 외에 성명, 주소, 전화번호, 이메일 등 두개 이상의 정보를 조합하여 개인을 식별할 수 있는 개인신상정보까지 ARIA-256을 적용해 암호화했다.[6] 또한, 2003년 벨기에 루벤 대학의 성능평가에서 우리나라의 SEED나 일본의 암호화 알고리즘인 Camellia 보다 데이터 처리속도 등 성능 면에서 2배가량 우수하다.[7]

본 연구에서는 보안공격에 비교적 안정적이며, 128/192/256비트 암호화키를 지원하는 ARIA 암호 알고리즘을 적용하였으며, 주요사양은 아래와 같다. 이 알고리즘은 휴대형 기기 및 모바일 환경에 적합하도록 암호화 작업에 소요되는 메모리 등 하

드웨어 자원 및 전력 소비를 최소화하고, 안전성과 효율성을 동시에 고려해서 특수설계된 것이다.

- 기본 구조 : ISPN(Involution SPN) 구조
- 입출력 크기 : 128비트
- 키 크기 : 128, 192, 256비트
- 라운드 키 크기 : 128비트
- 라운드 수: 키 크기에 따라 12, 14, 16 라운드

내부 함수는 세단계로 치환계층, 확산 계층, 라운드 키 삽입으로 이루어져 있으며, 치환계층은 테이블 참조로 구현하는 것이 일반적이며 최적의 선택이라 할 수 있다. 확산계층(Diffusion layer)은 ARIA 알고리즘을 다른 동종 블록암호 알고리즘(AES, Camellia 등)과 구별 짓는 주요 부분이며 <그림 2>과 같이 16x16 대합이진행렬을 사용한다.

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15} \end{pmatrix} = \begin{pmatrix} 0&0&0&1&1&0&1&0&1&1&0&0&0&1&1&0 \\ 0&0&1&0&0&1&0&1&1&1&0&0&1&0&0&1 \\ 0&1&0&0&1&0&1&0&0&0&1&1&1&0&0&1 \\ 1&0&0&0&0&1&0&1&0&0&1&1&0&1&1&0 \\ 1&0&1&0&0&1&0&0&1&0&0&1&0&0&1&1 \\ 0&1&0&1&1&0&0&0&0&1&1&0&0&0&1&1 \\ 1&0&1&0&0&0&0&1&0&1&1&0&1&1&0&0 \\ 0&1&0&1&0&0&1&0&1&0&0&1&1&1&0&0 \\ 1&1&0&0&1&0&0&1&0&0&1&0&0&1&0&1 \\ 1&1&0&0&0&1&1&0&0&0&0&1&1&0&1&0 \\ 0&0&1&1&0&1&1&0&1&0&0&0&0&1&0&1 \\ 0&0&1&1&1&0&0&1&0&1&0&0&1&0&1&0 \\ 0&1&1&0&0&0&1&1&0&1&0&1&1&0&0&0 \\ 1&0&0&1&0&0&1&1&1&0&1&0&0&1&0&0 \\ 1&0&0&1&1&1&0&0&0&1&0&1&0&0&1&0 \\ 0&1&1&0&1&1&0&0&1&0&1&0&0&0&0&1 \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{pmatrix}$$

그림 2. ARIA의 16x16 확산 계층
Figure 2. ARIA 16x16 Diffusion layer

라운드 키 삽입 단계부분은 키 스케줄에서 생성된 라운드 키와 라운드 함수 입력간의 XOR연산으로 이루어져 있으며, 각 암호화 라운드 키는 생성된 마스터 키(MK)를 이용하여, <그림 3>과 같은 방법으로 생성된다.

$$\begin{aligned}
ek_1 &= (W_0) \oplus (W_1^{\gg 19}), & ek_2 &= (W_1) \oplus (W_2^{\gg 19}), \\
ek_3 &= (W_2) \oplus (W_3^{\gg 19}), & ek_4 &= (W_0^{\gg 19}) \oplus (W_3), \\
ek_5 &= (W_0) \oplus (W_1^{\gg 31}), & ek_6 &= (W_1) \oplus (W_2^{\gg 31}), \\
ek_7 &= (W_2) \oplus (W_3^{\gg 31}), & ek_8 &= (W_0^{\gg 31}) \oplus (W_3), \\
ek_9 &= (W_0) \oplus (W_1^{\ll 61}), & ek_{10} &= (W_1) \oplus (W_2^{\ll 61}), \\
ek_{11} &= (W_2) \oplus (W_3^{\ll 61}), & ek_{12} &= (W_0^{\ll 61}) \oplus (W_3), \\
ek_{13} &= (W_0) \oplus (W_1^{\ll 31}), & ek_{14} &= (W_1) \oplus (W_2^{\ll 31}), \\
ek_{15} &= (W_2) \oplus (W_3^{\ll 31}), & ek_{16} &= (W_0^{\ll 31}) \oplus (W_3), \\
ek_{17} &= (W_0) \oplus (W_1^{\ll 19})
\end{aligned}$$

그림 3. ARIA 라운드 키 생성식
Figure 3. ARIA Round Key Generation Equation

3. 시스템 구축 방안

3.1 기존 전술데이터링크 운용개념

우리 군에서 운용되는 전술데이터링크의 운용방식을 살펴보면 Link-11의 경우 Roll-Call 모드 형태로 HF 통신망을 이용하여 운용되며, Link-16 및 Link-K의 경우 TDMA 통신구조를 이용하여 UHF 무선 통신망으로 주로 운용된다. 또한, KVMF의 경우 지상군에서 주로 운용되는 VHF FM무전기를 이용하여 MIL-STD-188-220 통신 프로토콜에 따라 주로 운용된다. 이처럼 전술데이터링크를 탑재한 무기체계들은 무선(HF/UHF) 및 위성 통신을 이용하여 방송망(Broadcast) 방식으로 운용된다.

이때, 무선 통신망을 이용한 전술데이터링크 운용시 송신노드에서 송신한 메시지는 네트워크 전 가입노드에서 수신되며, 수신노드에서는 해당 메시지 처리여부를 판단하여, 해당 메시지를 운용자에게 전시되도록 처리한다.

<그림 4>에서 보는 바와 같이 노드 10에서 송신한 메시지는 동일 네트워크에 가입한 노드 20, 노드 30, 노드 40에서 모두 수신하며, 수신된 메시지에 대한 처리는 각 노드에서 수행하는 운용방식이다.

- 통신환경 : 방송망(Broadcast) 방식으로 동작
- 노드 10에서 송신한 메시지는 망에 가입한 모든 노드가 수신(노드 20, 노드 30, 노드 40)

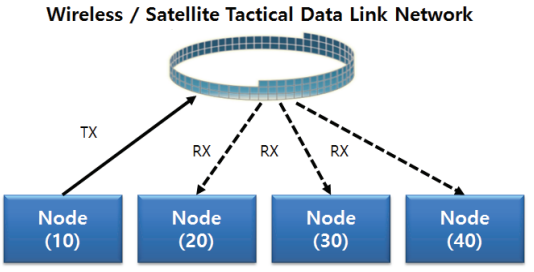


그림 4. 기존 전술데이터링크 운용방식
Figure 4. Existing tactical data link operation method

3.2 논리적 서브넷 적용 전술데이터링크 운용개념

기존 전술데이터링크 운용 방식 적용에 따른 추가 전술데이터링크 통신망 구성을 위해서는 기존 무선 또는 위성용 데이터링크 터미널 장비를 추가해야 하는 단점이 있다. 이에 대한 개선 방안으로 본 연구에서는 암호화 기법을 활용하여 추가 전술데이터링크 네트워크를 구성할 수 있는 방법을 제시한다. 즉, 추가 전술데이터링크 네트워크는 논리적 서브넷 개념으로 전술데이터링크는 기존 전술데이터링크와 동일하게 방송망(Broadcast) 방식으로 동작하나, 그룹별 그룹 키에 따른 암호키가 서로 상이하여 수신한 노드가 대상 그룹이 아닐 경우 수신한 메시지를 미처리하게 하는 운용방식을 제공하게 된다. 이를 통해 동일 그룹키를 보유한 송수신 노드들이 동일 그룹키별로 논리적인 전술데이터링크 네트워크망을 추가로 보유할 수 있는 효과를 가지게 되며, 이를 통해 작전별, 임무별로 별도의 네트워크를 구성할 수 있게 한다.

세부적 운용방식은 <그림 5>에서 보는 바와 같이 그룹 1에 노드 10, 노드 20이 가입되고, 그룹 2에 노드 30, 노드 40이 가입될 경우 그룹 1의 노드 10에서 송신한 메시지는 동일 그룹인 노드 20만 수신하여 처리하고, 타 그룹인 노드 30과 노드 40은 수신은 가능하나 암호키가 논리적 그룹별로 상이하여 수신 메시지를 처리하지 못하게 되어 논리적 서브넷 구성이 가능하다.

- 통신환경 : 방송망(Broadcast) 방식으로 동작
- 노드 10에서 발생한 메시지는 동일 1그룹에 가입한 노드만 수신(노드 20)
- 노드 30에서 발생한 메시지는 동일 2그룹에 가입한 노드만 수신(노드 40)

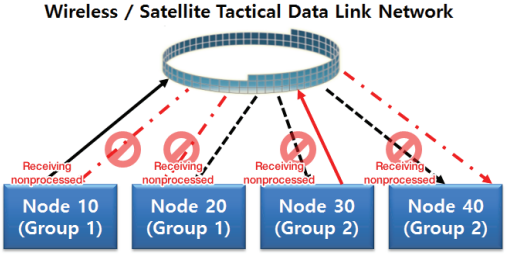


그림 5. 논리적 서브넷이 적용된 전술데이터링크 운용방식
Figure 5. Tactical data link operation with logical subnet

3.3 시스템 구성 방안

암호화 기법을 이용한 논리적 서브넷 구성을 위해 <그림 6>과 같이 기존 전술데이터링크 구성에서 데이터링크 처리기(DLP : Data Link Processor) 내에 서브넷 암호화 SW 모듈을 탑재하여 전술데이터링크를 구성한다. 이때, 전술정보의 송신은 호스트 컴퓨터에서 송신할 전술정보를 데이터링크 처리기에서 전술데이터링크 메시지로 변환하고, 변환된 평문의 메시지를 데이터링크 처리기내 서브넷 암호화 SW 모듈에서 그룹키를 이용하여 암호화한 후, 암호장비를 이용하여 다시 암호화를 실시한다. 이후, 암호화된 메시지는

데이터링크 터미널로 전달하여 신호변환 및 프로토콜 제어를 통해 군용 통신장비를 이용하여 송신하게 된다. 수신측에서는 앞서 설명한 과정의 역과정을 통해 송신된 메시지에 대해 수신 처리하게 된다.

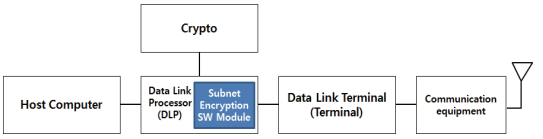


그림 6. 암호화 기법을 적용한 논리적 서브넷 시스템 구성
Figure 6. General Configuration of Tactical Data Links

3.4 그룹키 생성 및 메시지 송수신 처리절차

블록 암호 알고리즘인 ARIA에 적용되는 그룹키(암호키) 생성은 그룹별로 고유의 그룹번호(Group Number)를 지정하여 임의번호(Random Number)와 배타적 논리합(EOR : Exclusive OR)으로 조합하여 그룹 키를 생성하고 전술데이터링크망 설계 정보와 함께 대상 노드별로 배포하여, 데이터링크 처리기내 서브넷 암호화 SW 모듈에서 운용하도록 한다.

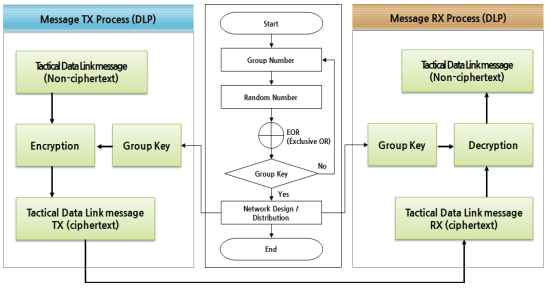


그림 7. 논리적 서브넷에서의 암호화된 메시지 송수신 처리
Figure 7. Transmitting and receiving encrypted messages on logical subnets

전술데이터링크 참여 노드들은 <그림 7>에서 보는 바와 같이 평문 메시지를 데이터링크 처리기내 서브넷 암호화 SW 모듈을 이용하여 메시지를 암호화하여 송신하며, 수신 노드에서는 동일 그룹 그룹키에 따라 수신된 암호화 메시지에 대해 정상적인 복호화 과정을 거쳐 메시지를 확인할 수 있다. 그러나 그룹 키(암호키)가 다른 타 그룹 수신노드의 경우 복호화 실패에 따라 메시지를 처리할 수 없게 되며 이에 따라 메시지 암호화를 통한 논리적 서브넷 구성이 가능하게 된다.

4. 실험 및 확인

본 장에서는 그룹키 생성 절차에 따라 블록 암호 알고리즘인 ARIA에서 사용할 수 있는 암호키를 생성하는 소프트웨어를 구현하고 이를 적용한 암호화 및 복호화 결과 값을 확인하여 논리적 서브넷 구성 가능성을 고찰한다.

4.1 그룹키 생성 SW

그룹키 생성 SW는 사용자가 지정한 그룹번호와 임의번호를 활용하여 그룹키를 생성한다. 이때, ARIA 암호 모듈에서 해당 그룹키를 사용 가능하도록 설정 값을 다음과 같이 지정하였다.

- 입출력 크기 : 128 비트
- 키 크기 : 192 비트
- 라운드 키 크기 : 128 비트
- 라운드 수 : 14 라운드

표 4. 그룹별 설정 값
Table 4. Group Setting Values

Group	Group Number	Random Number	Target Node	Group Key
Group 1	1	23	10, 20	0102030405 06070809 0a0b0c0d 0e0f1027 28292a2b 2c2d2e
Group 2	2	45	30, 40	0203040506 0708090a 0b0c0d0e 0f10113d 3e3f4041 424344

상기 기본 설정 값에 따라 2개 그룹의 그룹키를 각각 생성하기 위해 <표 4>와 같이 각 그룹별 설정

값을 임의로 지정하고 그룹키 생성 SW에 의해 생성된 결과 값을 <그림 8>과 같이 확인할 수 있다.

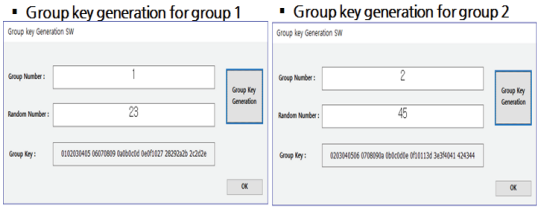


그림 8. 그룹키 생성 결과
Figure 8. Group key generation result

4.2 그룹키의 서브넷 암호화 SW 모듈 적용

그룹키 생성 SW에 의해 생성된 각 그룹별 그룹키를 이용하여 평문의 전술정보를 블록 암호화 알고리즘 ARIA가 적용된 서브넷 암호화 SW 모듈을 이용하여 암호화 및 복호화를 수행하여 처리결과를 살펴보았다.

<그림 9>은 그룹 1에서 생성한 그룹키를 서브넷 암호화 SW 모듈에 적용할 경우, 그룹1의 참여 노드에서 정상적으로 암호화 및 복호화가 이루어지고 있음을 보여준다.

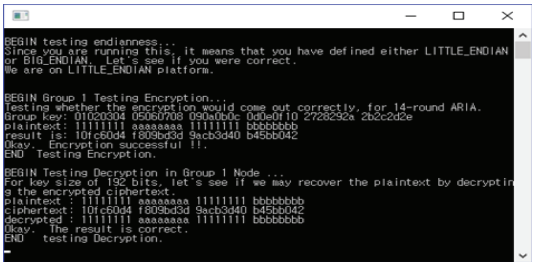


그림 9. 그룹키 적용 서브넷 암호화 SW 모듈 처리 결과
Figure 9. Subnet Encryption SW module processing result with group key applied

<그림 10>은 서브넷 암호화 SW 모듈을 이용하여 각 그룹별 별도 서브넷을 구성할 경우, 그룹 1에서 암호화된 내용을 그룹 2에 속한 노드에서 복호화 처리되지 않음을 보여준다.

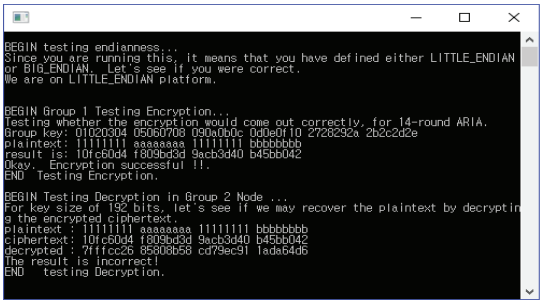


그림 10. 타 그룹키 적용에 따른 서브넷 암호화 SW 모듈 처리 결과
Figure 10. Subnet Encryption SW module processing result with other group key applied

그룹키 적용에 따른 서브넷 처리결과를 종합하면 <표 5>와 같이 동일한 암호화 입력 값에 대해 다르게 복호화 결과 값을 보여 주고 있다.

표 5. 서브넷 암복호화 처리 결과
Table 5. Subnet encryption/decryption result

Div.	Contents	Note
Plain Text	11111111 aaaaaaaa 11111111 bbbbbbbb	
Encryption Input Value	10fc60d4 f809bd3d 9acb3d40 b45bb042	
Group 1 Decryption Result	11111111 aaaaaaaa 11111111 bbbbbbbb	Correct
Group 2 Decryption Result	7fffcc26 85808b58 cd79ec91 1ada64d6	Incorrect

4.3 전술데이터링크의 논리적 서브넷 적용 운용화면

전술데이터링크 운용에 있어 서브넷 암호화 SW를 탑재하여 논리적 서브넷을 구성한 데이터링크 처리기(DLP)는 타 그룹 키가 적용된 암호화 전문을 복호화 할 수 없게 되어 해당 메시지를 삭제하고, 관련 전술정보를 호스트 컴퓨터상의 전술화면에

전시할 수 없도록 하여 별도 장비 및 통신망 운용 없이 논리적인 서브넷 운용이 가능하다. 이러한 논리적 서브넷 구성에 따른 각 그룹별 전술데이터링크 호스트 컴퓨터 전술 운용화면은 <그림 11>과 같이 동일한 전술정보를 송신하게 되지만 구성된 논리적 서브넷에 따라 전시되는 적 정보들이 서로 차이를 보이고 있음을 알 수 있다.

이때, 아군 정보에 대해서는 모든 참여노드가 알 수 있어야 되지만, 개별 임무별로 적 정보를 선택적으로 수신하여 전시할 수 있는 차이를 보이며, 이러한 차이로 인해 작전 임무별, 운용 기능별로 논리적 서브넷 구축이 가능함을 확인할 수 있다.

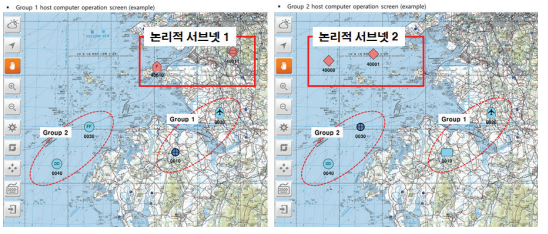


그림 11. 호스트컴퓨터 운용화면(예시)
Figure 11. Host computer operation screen(Example)

5. 결 론

전술데이터링크는 모든 전투원에게 실시간 혹은 근실시간 정보공유를 통해 공통상황인식과 동시 의사 결정력을 제공한다.

현재 우리 군은 합동 및 협동작전을 위한 한국형 전술데이터링크(Link-K, KVMF)와 연합작전을 위한 선진국 전술데이터링크(Link-11, Link-16)를 운용하고 있고 지휘소, 함정, 항공기, 전차 등 다양한 무기체계 플랫폼에 전술데이터링크 능력을 확보하기 위해 노력하고 있으나, 각 군 및 무기체계별로 다양한 작전 임무를 수행해야하고 운용 기능별 전술망 소요가 증가함에 따라 이를 해결하기 위해 추가 장비의 설치 또는 수정에 많은 비용이 수반된다. 이와 같은 서브넷의 소요 증가에 따른 우리 군 전술데이터링크 운용능력 확보를 위한 대안으로 암호화 기법을 이용한 논리적 서브넷 구축 방안에 대하여 연구하였다.

본 연구에서 제안하는 논리적 서브넷 구성 방법으로 기존 방송망(Broadcast) 방식의 전술데이터링크에 비해 다양한 그룹별 논리적 서브넷 구성이 가능함을 확인할 수 있었으며, 전술데이터링크를 탑재하여 운용하는 모든 플랫폼에서 하드웨어 수정 또는 교체 없이 작전 임무별, 운용 기능별 서브넷 구성 및 활용이 가능할 것으로 판단된다.

본 연구결과가 향후 우리 군 전술데이터링크 서브넷 운용방식 연구와 관련된 사업 추진 비용절감에 조금이나마 도움이 되길 기대한다.

References

[1] H. J. Park, *Study of interoperability between data links*, Defense Agency for Technology and Quality, p. 21, 2015.

[2] H. J. Park, Y. K. Park, K. M. Park, H. J. Park, S. W. Kim, and J. W. Lee, *Application plan of Korean TDL forwarding standards for ROK military future weapon system*, 2015 KIISE Conference, PyeongChang, Korea, pp. 1104-1106, Dec. 2015.

[3] P. S. Stanley, *Understanding voice and data link networking*, NORTHROP GRUMMAN, pp. 2-20, 2013.

[4] DoD, *Tactical data link(TDL) 16 message standard, MIL-STD-6016E*, Jul. 2012.

[5] H. J. Park, C. H. Park, S. J. Kim, C. Jin, S. B. Ji, J. H. Ahn, and K. Lee, *Study on time slots allocation methods of TDMA radio link-K*, 2016 KIMST Conference, Jeju Island, Korea, Jun. 2016.

[6] Status of domestic self-developed block cipher algorithm, http://www.boannews.com/media/view.asp?idx=54009, Mar. 2017.

[7] J. S. Han, and J. K. Choi, *Implementation of ARIA block encryption algorithm*, 35th KIPS Spring Conference, Jeju Island, Korea, May 2011.

[8] D. I. Yang, *Introduction to information security*, Hanbit Academy, Jun. 2013.

[9] National Security Research Institute, A*RIA algorithm specification*, Ver. 1.0, pp. 9, May 2004.

[10] J. S. Kim, S. J. Kim, and M. Y. Lim, *Overview of tactical data link technology*, *Communication*. Korean Institute of Information Scientists and Engineers(KIISE), Vol. 25, No. 9, pp. 18-28, Aug. 2007.

[11] S. R. Jung, and H. S. Shin, *Analysis on technology development of NCW and tactical data link*, J. Korea Institute Electronic Communication Science (KIECS), Vol. 7, No. 5, pp. 991-998, Oct. 2012.

[12] H. K. Back, S. M. Jung, and J. S. Lim, *Trends of tactical data link technologies for network centric operations*, Korean Institute of Information Scientists and Engineers (KIISE), Vol. 28, No. 7, pp. 59-69, Jul. 2010.

[13] Easy to see ARIA algorithm, http://stk001.blog.me/120111610638, Jul. 2017.

[14] ARIA, SEED algorithm ratio, http://cafe.naver.com/nsis/37994, Jul. 2017.

[15] ARIA encryption algorithm, http://blog.naver.com/etruelove/140149098241, Jul. 2017.

전술데이터링크 환경에서 암호화 기법을 이용한 논리적 서브넷 구성기법

지승배[1], 진철[1], 박경미[1], 박헌제[2], 박창호[2], 안정현[3], 이강[3]

[1] *국방과학연구소*
[2] *(주)링크나인시스템*
[3] *쌍용정보통신(주)*

요 약

전술데이터링크는 모든 전투원에게 실시간 혹은 근실시간 정보공유를 통해 공통상황인식과 동시 의사결정력을 제공한다. 현재 한국군은 합동 및 협동작전을 위한 한국형 전술데이터링크(Link-K, KVMF)와 연합작전을 위한 선진국 전술데이터링크(Link-11, Link-16)를 운용하고 있고 지휘소, 함정, 항공기, 전차 등 다양한 무기체계 플랫폼에 전술데이터링크 능력을 확보하기 위해 노력하고 있으나, 각 군 및 무기체계별로 다양한 작전 임무를 수행해야하고 운용 기능별 전술망 소요가 증가함에 따라 이를 해결하기 위해 추가 장비의 설치 또는 수정에 많은 비용이 수반된다. 이와 같은 서브넷의 소요 증가에 따른 한국군 전술데이터링크 운용능력 확보를 위한 대안으로 암호화 기법을 이용한 논리적 서브넷 구축방안에 대하여 연구하였다. 본 연구에서 제안하는 논리적 서브넷 구성 방법으로 기존 방송망(Broadcast) 방식의 전술데이터링크에 비해 다양한 그룹별 논리적 서브넷 구성이 가능함을 확인할 수 있었으며, 전술데이터링크를 탑재하여 운용하는 모든 플랫폼에서 하드웨어 수정 또는 교체 없이 작전 임무별, 운용 기능별 서브넷 구성 및 활용이 가능할 것으로 판단된다. 본 연구결과가 향후 한국군 전술데이터링크 서브넷 운용방식 연구와 관련된 사업 추진 비용절감에 조금이나마 도움이 되길 기대한다.

감사의 글

본 논문은 국방과학연구소 주관 다중 전술데이터링크(TDL) 프로토콜 통합 처리 기술 개발 사업의 일환으로 수행하였음.

Seung-Bae Ji received the bachelor's degree in the Department of Electronic Engineering from the Sogang University in 2001. He received the M.S. degree in the Department of Electronic Engineering from KAIST in 2003. From 2003 to 2006, he was a researcher at SAMSUNG SDS. He has been a senior researcher at Agency of Defense Development since 2006. His current research interests include NCW, Tactical Data Link Systems and Protocols, Link-K

E-mail address: seungbae@add.re.kr

Cheol Jin received the bachelor's degree and the M.S. degree in the Department of Computer Science from Soongsil University in 1986 and 1988, respectively. He has been a principal researcher at Agency of Defense Development since 1988. His current research interests include Tactical Data Link, Software Engineering.

E-mail address: cjn1614@add.re.kr

Kyung-Mi Park received the bachelor's degree in the Department of Electrical and Electronic Engineering from the Korea University in 2005. She received the M.S. degree in the Department of Radio Engineering from Korea University in 2007. She has been a senior researcher at Agency of Defense Development since 2007. Her current research interests include NCW, Link-K, Link-16.

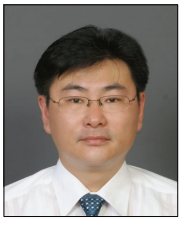
E-mail address: kmipark@add.re.kr

Heon-Jei Park received the bachelor's degree in the Department of Electrical Engineering from the ROK Naval Academy in 1995. He received the M.S. degree in the Department of Industrial Engineering from Hannam university in 2013. He has been a president at Link Nine System since 2014. His current research interests include Tactical Data Link, KVMF, Link-K, Link-16.

E-mail address: tompy@lnsystem.co.kr

Chang-Ho Park received the bachelor's degree in the Department of Oceanography from the ROK Naval Academy in 1995. He received the M.S. degree in the Department of Social Welfare from Daejeon university in 2008. He completed Ph.D. in the Department of Military Science and Informatics at Kongju National University. He has been a director at Link Nine System since 2015. His current research interests include Tactical Data Link, Defense Modelling & Simulation, Warfighting Experimentation.

E-mail address: radarsite200@lnsystem.co.kr



Jeong-Hyun Ahn received the bachelor's degree in the Department of Economics from the Kyunghee University in 1997. He has been a Engineer at SsangYong Information & Communications corp. since 1997. His current research interests include Tactical Data Link, Link-K, Link-16.

E-mail address: puppy70@sicc.co.kr

Kang Lee received the bachelor's degree in the Department of Computer Engineering from the Hongik University in 2008. He has been a Engineer at SsangYong Information & Communications corp. since 2007. His current research interests include Tactical Data Link, Link-K, Link-16.

E-mail addres: lk@sicc.co.kr