Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.4, Aug. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.4.625

이기종 전술통신망 종단간 암호화 통신을 위한 메커니즘*

박 철 용,[1†] 김 기 홍,[1] 류 재 철[2‡]
[1]한국전자통신연구원 부설연구소, [2]충남대학교

A mechanism for end-to-end secure communication in heterogeneous tactical networks*

Cheol-Yong Park,[1†] Ki-Hong Kim,[1] Jae-Cheol Ryou[2‡]
[1]The Attached Institute of ETRI, [2]ChungNam National University

요 약

전술통신망은 이기종 다양한 특성의 통신장비로 구성된 네트워크가 복합적으로 운용되고 있다. 이러한 구성으로 인해 종단간 통신을 위해 기종별 데이터 포맷으로 변환하기 위한 망연동 게이트웨이를 적용하고 통신 정보보호를 위해 네트워크별 암호기술이 적용되고 있다. 이는 이기종 망간 암호화된 데이터를 직접 전송할 수 없고 통신데이터의 재가공 및 처리지연의 문제점이 있다. 서로 다른 전술통신망 사이에 위치하는 망연동 게이트웨이에서 통신데이터에 대한 재가공과 암호화 데이터에 대한 복호화 및 재암호화가 요구된다. 본 논문에서는 전술통신망에서 이기종간 종단간 암호화 통신을 위한 통신방식을 제안한다. 제안한 방식을 이용하여 PSTN과 UHF 통신망간 게이트웨이에서 재가공, 재암호화, 전송 지연요소 등을 없애 실시간 음성 및 데이터 통신을 가능하게 한다. 또한, 종단간 정보보호를 위해 단대단 정보보호 방식을 적용한다. 이를 통신망에 적용하여 기존 방식 대비 제안한 방식의 성능을 비교 분석한다. 제안한 방식은 기존방식의 문제점을 해결하고 이기종 전술통신망간 종단간 암호화 통신이 가능함을 확인하였다.

ABSTRACT

Tactical networks is being operated in configuration that consisting of a variety of characteristics communication equipments and heterogeneous networks. In this configurations, end-to-end communication can be achieved using interworking gateway for converting the data format of the network and using encryption algorithm of the networks. The use of mechanism results in a problem that secure data cannot be transferred directly, reprocessing and processing delay of communication in heterogeneous tactical networks. That is, for encoding and decoding of data, the decryption of encrypted data and re-encryption processing must be required at the gateway between different networks. In this paper proposes to mechanism for end-to-end secure communication in heterogeneous tactical networks. Using the proposed method, end-to-end secure communication between heterogeneous tactical networks(PSTN-UHF networks) which removes the necessity of a gateway for converting data into data formats suitable for network to remove a transmission delay factor and enable real-time voice and data communication and achieve end-to-end security for heterogeneous tactical networks. we propose a novel mechanism for end-to-end secure communication over PSTN and UHF networks and evaluate against the performance of conventional mechanism. Our proposal is confirmed removal of security vulnerabilities, end-to-end secure communication in heterogeneous tactical networks.

Keywords: End-to-end, Secure, Heterogeneous, Tactical, Gateway, Network, Communication

접수일(2014년 4월 2일), 수정일(2014년 5월 28일), 게재확정일(2014년 6월 12일)
* 이 논문은 한국전자통신연구원-산업융합원천기술개발사업(No.10047528)의 지원을 받아 수행된 연구임.
† 주저자, parkcy@ensec.re.kr
‡ 교신저자, jcryou@home.cnu.ac.kr(Corresponding author)

I. 개 요

군의 최근 전술통신망은 전장 환경의 이동성 및 생존성 등을 고려하여 여러 환경에 구축을 하면서 다양한 통신장비 및 네트워크 환경이 구축되어 복합적으로 운용되고 있다. 특히 여러 네트워크 환경이 구축되어 이기종 망간의 데이터 전송도 필요하게 되면서 종단간 단말 사이 통신시 보안이 매우 중요한 이슈가 되고 있다. 특히 전술 통신망 중에서 유선 전술통신인 PSTN (Public Switched Telephone Network)망과 무선 전술통신인 UHF(Ultra High Frequency) 통신망은 많은 관심의 대상이 되어 왔다. UHF 통신은 300MHz~3000MHz를 사용하는 통신으로 군의 무선 전술통신에 매우 중요하다. UHF는 다른 무선 주파수에서는 적용할 수 없는 많은 장점이 있다. 현장에서의 통신 및 전 세계 군사위성에서 주로 사용되며 다양한 군사 서비스와 여러 기관에서 지휘, 통제, 통신, 컴퓨터 정보 감시 및 정찰 등 다양한 목적으로 사용되고 있다[1]. UHF 채널의 음성 및 데이터에 대한 보안은 아날로그 방식의 스크램블러 방식[2]의 취약점으로 인해 현재 음성은 낮은 속도의 음성코덱[3]을 통한 음성 처리 후 암호화 알고리즘을 이용하고 데이터의 경우 저전송 데이터[4]를 암호화하여 보호 하고 있다.

전술통신망에서 이기종의 다양한 통신환경에서 단대단(end-to-end)의 통신 보안을 위해서는 암호화된 데이터가 다른 네트워크로 들어가기 전에 망연동 게이트웨이(gateway)에서 암호화된 데이터에 대해 다시 복호화 후 통신환경 및 전송 포맷에 대한 부분을 고려하여 네트워크에 적합한 통신방식을 적용하여 암호화해야 한다. 이 경우 종단 네트워크의 최종 사용자에게 무결성이 보장된 보안서비스를 제공하기 어렵다. 종단간 암호통신시 게이트웨이에서의 복호화 후 재 암호화방식은 치명적인 보안취약점이 발생 할 수 있으며, 네트워크 프로토콜에 맞는 데이터 포맷으로의 변환, 재가공 등 추가적인 데이터처리에 따른 전송지연, 이기종 네트워크에 대한 통신장비 상호 운용성에 따른 비신뢰성 전송 등의 심각한 단점이 존재하게 된다.

이기종 네트워크간 암호화 통신에 대한 연구는 GSM (Global System for Mobile Communications) 망에서 휴대폰과 PSTN의 이기종 네트워크에 대한 통신 기술 및 보안문제에 대한 연구가 진행되었다. 이 중에는 GSM의 음성채널을 통해 암호화된 음성데이터를 전송하기 위한 방식과 장치를 제안하였다[5]. 또 다른 연구는 GSM과 PSTN간 암호통신에 대한 기술을 제시[6]하였으며 GSM 망에서 선형예측코딩(LPC:Linear Predictive Coding) 디지털 변조방식을 사용하여 암호화된 음성방식[7]이 제시되었다.

직교진폭변조(QAM:Quadrature Amplitude Modulation) 및 직교 주파수 분할 코딩(OFDM : Orthgonal Frequency Division Multiplexing) 변조 방식을 기초로 한 모뎀을 이용하여 GSM 음성채널을 통해 암호통신을 사용하는 방식[8]이 제안되기도 했다.

전술 무선 네트워크와 PSTN에 관한 음성 암호통신 분야에서도 여러 연구가 발표되었다. 협대역 UHF 망에서 디지털 음성을 암호화하여 암호 통신에 대한 전송품질 및 성능을 분석한 연구[9]와 VHF/UHF채널에서 암호 통신 상호 운용성 프로토콜(SCIP; Secure Communication Interoperability Protocol)에 대한 성능 및 효율에 대한 분석[10] 연구도 발표되었다. HF 채널을 통해 음성 암호통신에 대한 전송품질을 분석한 논문[11]도 발표되었으며 PSTN을 통한 안전한 음성 및 데이터 통신에 관한 방식[12][13]도 제안되었다.

그러나 위에서 언급한 문헌의 암호화 통신 방식은 GSM과 PSTN의 암호방식에 따라 게이트웨이가 적용되어 있으며 디지털 신호처리 기술이나 모뎀 기술이 전술통신망이나 PSTN에 각각에 맞게 적용되어 있다. 기존 UHF망와 PSTN의 단대단 디지털 음성보안통신[14]은 이기종 네트워크에 대한 직접적 암호통신은 음성에 대한 부분은 있으나 데이터에 대한 통신방식은 나타나 있지 않으며 시험결과 모뎀에서의 통신지연 요소 등 세부적인 분석 및 실제 이기종 전술통신망에 대한 시험결과가 나타나 있지 않다.

본 논문에서는 UHF망과 PSTN의 이기종 전술통신망에서 종단간 단대단 암호화 통신에 대한 방식을 제안하고 실제 UHF 망과 PSTN간 종단간 암호통신 시험을 통해 성능을 분석하고 통신데이터에 대한 전송지연 및 통신 측면에서 제안한 시스템에 대한 분석을 통해 기존 게이트웨이를 사용하는 방식에 비해 성능 향상 및 전송 지연이 감소함을 보인다. 제안한 방식의 시스템은 PSTN과 UHF망 종단간 설치한다. 비교분석을 위해 음성에 대한 품질, 음성 스펙트럼 측면, 암호화 통신데이터에 대한 전송지연에 대해 시험을 실시하고 특성을 분석한다. 이러한 결과를 통해 향후 다른 전술 환경에서 이기종 망간 다양하고 효율적이며 신뢰성 있는 종단간 단대단 암호화 통신 기술 설계에

활용한다.

제안된 방식을 사용하여 성능 비교시 음성의 품질 측정 방식중 하나인 MOS (Mean Opinion Score) 점수로 측정시 기존 방식에 비해 음질을 개선 할 수 있었으며 PSTN 및 UHF망 환경에서 기존의 방식에 비해 최대 50 %이상 종단간 전송 지연을 줄일 수 있었다. 추가적으로, 이기종 전술통신망에서 암호화된 데이터를 재가공 없이 단대단 통신을 할 수 있는 방식이 기존 방식과 가장 큰 차이점이다.

현재 제안한 방식은 이기종 망간 단대단 암호통신에 대한 포괄적인 방식의 제안이며 이러한 결과는 다른 이기종 망의 단대단 통신 및 암호통신에 대해 다양하고 효율적으로 신뢰할 수 있는 암호통신 기술을 설계하는데 사용할 수 있다.

본 논문의 구성은 기존 방식의 통신 방식 및 암호통신에 대해 기술하고 제안한 통신방식 및 암호통신 방식과 시험시스템에 대해 설명한다. 시험결과는 음성에 대한 암호통신 결과와 성능에 대한 분석과 데이터 암호화 통신에 대한 전송시간 시험 결과를 제시하고 결론을 맺는다.

II. 기존 운용방식

기존 PSTN 망과 UHF망 사이에 종단간 음성 통신 또는 데이터 통신을 하기 위해서는 PSTN과 이기종 망인 UHF망 사이에 위치한 게이트웨이를 거쳐야 한다. 또한 각각의 망에서 전달 받은 음성 및 데이터는 게이트웨이에서 각 망에서 정의한 데이터 규격에 맞게 변환, 재가공되어 망 내 전달하고자 하는 사용자에게 전송된다.

Fig.1.은 기존의 PSTN과 UHF망 간의 이기종 망간 음성 및 데이터통신에 대한 네트워크 구성도이다.

음성 일반통신의 경우 사용자의 PSTN용 전화기를 통하여 UHF망의 사용자 송수화 핸드셋으로 음성 통화를 하기 위해서 전화기의 음성을 PSTN망에 적합하게 PCM(Pulse Code Modulation) 신호로 변환 후 게이트웨이로 전송한다. 전송된 신호는 게이트웨이에서 PCM 음성신호를 음성 진폭변조(AM : Amplitude Modulation)하여 무선 망의 사용자 무전기로 전송한다. 전송된 AM 신호는 무전기에서 복조하여 송수화 핸드셋으로 음성을 듣게 된다. 역방향의 음성 송수신 경우도 역변환하여 동일방식으로 통신한다.

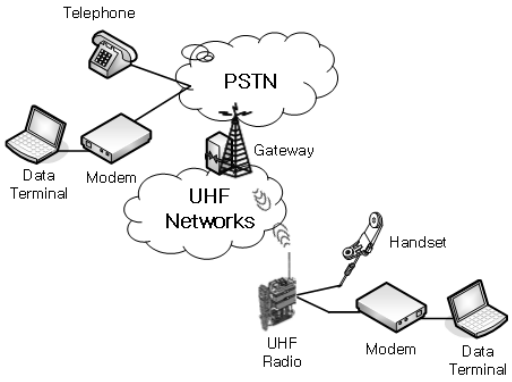


Fig. 1. Conventional network configuration

음성 암호통신의 경우 PSTN용 전화기에 정보보호방식(음성용 암호화 장치의 경우 아날로그는 스크램블방식, 디지털방식의 경우 별도의 디지털 음성처리부를 적용하여 암호화)을 적용하여 게이트웨이와 암호통신을 수행한다. 게이트웨이에서는 전송된 암호화 신호를 UHF망에 적합한 정보보호방식(음성용 암호화 장치의 경우 아날로그는 스크램블방식, 디지털방식의 경우 별도의 디지털 음성처리부를 적용하여 암호화)으로 재가공(복호 후 재암호화)하여 무선으로 UHF 무전기로 전송하여 송수화 핸드셋으로 수신 하면서 암호화 통신을 수행한다.

데이터 일반통신의 경우 사용자의 데이터 전송용 단말기(PC 또는 데이터 전송 전용 단말기)에서 PSTN망으로 데이터 전송을 위해 PSTN용 모뎀을 통해 게이트웨이로 데이터를 전송한다. 전송된 데이터는 게이트웨이에서 PSTN 데이터를 UHF 망에 적합하게 데이터를 재가공(데이터 단편화 및 채널코딩)하고 데이터를 진폭변조(AM)하여 무전기로 전송하고 무전기에서 수신된 데이터는 복조하여 데이터 전송용 단말기에 표시한다. 반대의 경우에도 역변환하여 통신한다.

데이터 암호통신의 경우 사용자의 데이터 전송용 단말기에서 정보보호방식이 적용된 데이터를 모뎀을 통해 게이트웨이로 전송하여 전송 단말기와 게이트웨이간 암호통신을 하는 방식과 데이터 전송용 단말기의 데이터를 전송단에 적용된 정보보호방식을 이용하여 모뎀을 통해 게이트웨이로 전송하여 모뎀과 게이트웨이간 암호통신을 한다. 그 후 게이트웨이에서는 전송된 데이터를 UHF망에 적합한 정보보호방식(암호방식-스크램블방식 또는 디지털암호화 방식)을 적용하

여 UHF 무전기를 이용하여 무선으로 전송하고 수신측 전송용 단말에서 데이터를 받아 암호통신을 한다. 무선 전송시 정보보호 방식은 데이터 전송용 단말기 자체에 적용하여 게이트웨이와 전송 단말기간 암호통신을 하는 방식과 무선채널 정보보호방식을 적용하여 게이트웨이와 무전기간 암호통신을 수행한다.

음성 및 데이터 암호통신의 정보보호 방식 적용시 PSTN 유선망에서는 비트오류율(BER:Bit Error Rate)에 크게 문제가 없어 암호동기를 유지하기 위한 방식은 고려하지 않아도 되나 UHF 망은 무선망으로 비트오류율을 감안하여 암호화 방식 적용시 암호동기를 유지하기 위한 동기화 방식 등이 적용된다. 또한, UHF 망은 데이터 전송속도에 있어서 PSTN보다 열악하기 때문에 데이터를 단편화하여 전송하게 되므로 망연동 게이트웨이에서는 이러한 암호동기를 유지하기 위한 방식과 데이터 단편화 및 재합성을 위한 방식이 적용되어야 한다. 추가적으로 무선 환경의 영향에 따라 인터리빙, 채널부호화, waveform 등 다양한 전송 방법을 고려하여 데이터 전송 방식을 구성해야 한다.

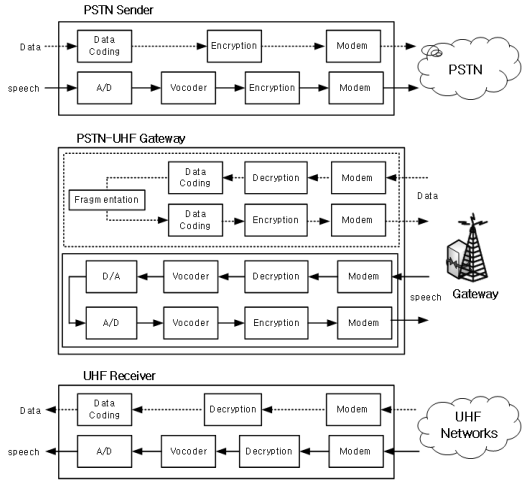


Fig. 2. Block Diagram of conventional mechanism

Fig.2.는 기존방식의 PSTN과 UHF간 종단간 암호화통신을 위한 블록도이다.

음성통신은 게이트웨이를 거치는 동안 각각의 망에 적합하게 음성 decoding후 다시 encoding되면서 재가공에 따른 지연요소를 가지고 전송된다. 데이터 통신은 각각의 망에 적합한 데이터 포맷 및 전송속도, 채널코딩, 전송데이터 크기를 가지고 전송되기 때문에 PSTN에서 전송되는 데이터를 UHF망에 적합하게 데이터에 대한 단편화 등 데이터 재가공 후 전송된다. 이는 실시간성이 절대적으로 보장되어야 하는 음성통신의 경우 전송지연 요소로 작용되며 데이터의 전송에 있어서도 각각의 망에 적합한 별도의 변환프로토콜 및 모뎀 등의 장치가 게이트웨이에 필연적으로 필요하게 된다.

정보보호 측면에서도 이기종 망간 음성/데이터의 암호화 통신시 PSTN에 적합한 정보보호 방식이 게이트웨이를 거치면서 필연적으로 UHF망에 적합한 정보보호 방식으로 재가공(복호화 후 재암호화) 되므로 이 때 게이트웨이에서 재암호화에 따른 보안취약점이 존재하게 된다. 종단의 사용자 관점에서 이러한 재암호화는 신뢰할 수 없는 망연동 게이트웨이의 경우 도청, 변조에 따른 데이터 무결성을 보장할 수 없어 사용자 데이터가 보안에 취약할 수밖에 없다. 암호화 방식에 있어서도 음성에 대한 정보보호 방식과 데이터에 대한 정보보호 방식이 게이트웨이에 각 망별로 필요하게 된다.

시스템 상호 운용성 측면에 있어서도 각각의 네트워크 환경에 따라 암호방식 뿐만 아니라 데이터 속도, 비트에러율(BER:Bit Error Rate), 보코더, 모뎀 등이 네트워크별로 상이하여 각 시스템을 네트워크에 적용시 각각의 시스템이 필요하게 되어 다양한 통신장비가 필요하게 되는 등 기존방식은 시스템 상호 운용 효율성이 떨어진다.

III. 제안하는 방식

앞 절에서 언급한 바와 같이 기존 방식의 문제점을 개선하고자 이기종 망간 통신시 통신지연 요소가 되는 음성 및 데이터에 대한 변환(재가공)에 있어 PSTN과 UHF망의 통신환경에 적합한 음성 코덱인 MELP 코덱을 보코더에 적용하여 단대단 음성 통신시 지연요소를 효율적으로 줄이고 각 망에 적합한 데이터 포맷의 변환방식을 음성 채널로 데이터를 전송하기 위한 QAM모뎀을 이용하여 이기종 망간 음성채널로 데이터를 전달하는 방식을 적용하여 각각의 망에 맞는 별도 변환방식의 문제점을 해결하고자한다. 또한, 게이트웨이 구간의 복호화 후 재암호화에 따른 도청, 데이터 무결성 등의 보안 취약점 및 각 구간별 별도 정보보호방식 적용에 따른 비효율성에 대한 문제점은 이기종 망에 적합한 단일의 정보보호방식을 채택하여 적용함으로써 종단간 단대단 암호화 통신을 제공한다. 망

연동 게이트웨이에서의 추가적인 통신 관련 데이터 변환을 없애기 위해 통신채널은 음성채널을 사용하여 통신을 수행한다. 추가적으로 각각 분리되어 있는 음성용 통신장치와 데이터용 통신장치를 하나로 통합하고 단일의 통신장치로 이기종 망에 적용하여 시스템 상호 운용성에 대한 효율성을 높였다.

본 논문에서는 제안한 방식을 E2E Equipment라는 단대단 통신장치를 구현하여 PSTN과 UHF망 간 음성 및 데이터에 대한 종단한 암호화 통신을 수행한다. 기존 통신 메커니즘에서 설명한 바와 같이 통신 구성요소에서의 변환 요소 및 다양한 정보보호 방식의 적용에 따른 단점을 보완하고자 Fig.3.의 구성도를 이용하여 설명하기로 한다.

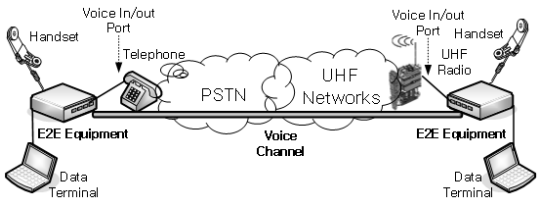


Fig. 3. Proposed network configuration

Fig.3.은 PSTN망과 UHF망의 이기종 망간 음성/데이터 단대단 통신 및 단대단 통신시 정보보호 방식을 적용 할 수 있는 구성도이다. 기존 방식의 장치는 PSTN의 경우 전화기에서 디지털화, PSTN용 보코더 적용, 정보보호 방식 적용, PSTN망에 적용을 위한 모뎀으로 구성된 통신장치를 이용하고 PSTN을 이용하여 게이트웨이를 거쳐 UHF망에 전달된다. UHF 망의 경우 게이트웨이에서 변환되어 전달된 데이터를 무전기의 모뎀을 거쳐 정보보호 방식 적용, 보코더를 거쳐 디지털화된 데이터를 아날로그로 변환하여 송수화 핸드셋으로 전달된다.

제안한 메커니즘을 적용한 통신장치는 음성 및 데이터를 직접 적용하는 통신하는 방식이 아닌 PSTN 전화기의 음성 입력출단(송수화기)에 연결하고 UHF 망에서는 무전기의 음성입출력단(핸드셋)에 연경하여 이기종 망의 통신장치의 음성채널을 통해 통신을 하게 된다. PSTN과 UHF망에서는 음성채널을 단순 연결하기 위한 시스템만 존재한다.

음성의 단대단 통신의 경우 PSTN 단대단 통신용 장치의 송수화기로 음성신호를 받아 음성처리부 보코더 코덱을 통해 디지털신호로 변환하여 단대단 통신용 장치 내 아날로그 모뎀을 거쳐 전화기의 음성채널을 통해 아날로그 신호가 PSTN망으로 전송된다. 전송된 아날로그 신호를 무선(AM)으로 무전기에 전송하고 무전기로 전송된 아날로그 신호는 단대단 통신용 장치 내 모뎀부를 통해 음성 디지털 데이터로 복조되고 음성처리부 보코더 코덱을 통해 아날로그 음성으로 변환되며 음성신호는 단대단 통신용 장치의 송수화 핸드셋을 통해 음성 통신하게 된다. 음성의 단대단 암호통신은 PSTN 단대단 통신용 장치에서 디지털 음성신호를 암호처리부내에서 정보보호방식을 적용하여 전송하면 중간의 시스템에서 별도의 변환 없이 UHF망 단대단 통신용 장치에서 동일한 정보보호방식을 적용하여 종단간 암호화 통신을 수행 할 수 있다.

데이터의 단대단 통신의 경우 PSTN 단대단 통신용 장치로 사용자 단말기의 데이터를 입력 받아 단대단 통신용 장치 내 모뎀부를 통해 전화기의 음성채널을 통해 PSTN망에 전송된다. 데이터는 중간에 재가공 없이 무선(AM)으로 무전기에 전송되고 무전기로 전송된 데이터는 단대단 통신용 장치에 연결된 사용자 단말을 통해 단대단 데이터 통신을 수행한다. 데이터의 단대단 암호통신은 단말기에서 입력 받은 데이터를 PSTN 단대단 통신용 장치에서 정보보호방식을 적용하여 전송하면 중간의 시스템에서 별도의 재암호화 없이 UHF망 단대단 통신용 장치에서 동일한 정보보호 방식을 적용하여 단대단 암호통신을 수행 할 수 있다.

Fig.4.는 종단간 암호화 통신장치에 대한 블록도이다.

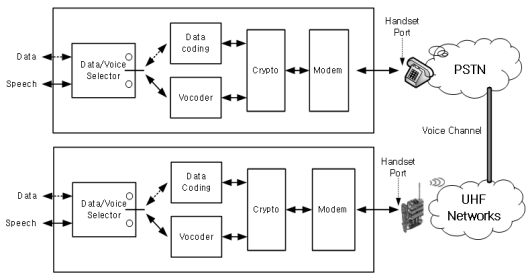


Fig. 4. Block Diagram for end-to-end Equipment

단대단 통신장치에서 Data/Voice Selector는 입력신호(음성/데이터)를 선택하는 기능으로 선택에 따라 데이터 처리 경로가 선택된다. Data Coding은 입력된 데이터를 패킷 처리하는 기능을 수행하고 Vocoder는 입력 받은 음성을 보코더와 코덱을 이용하여 디지털 데이터로 변환한다. Crypto는 단대단 암호통신시 암호화 방식을 처리하는 기능을 수행하며 일반통신시 통과(bypass)된다. Modem은 전송하고

자 하는 디지털 데이터를 PSTN 전화기의 음성채널에 실기 위해 아날로그 변조기능을 수행한다.

단대단 통신장치의 하드웨어 구성은 전체기능 제어 및 Data/Voice Selector, Data Coding 등의 기능을 수행하는 제어처리부와 음성처리 기능을 수행하는 Vocoder부 및 Crypto 기능을 처리하는 암호처리부, Modem 기능을 수행하는 모뎀부로 구성된다. 통신장치 기능별 특징은 다음 절의 '제안한 방식의 분석결과' 절에서 기술한다.

IV. 시험결과

4.1 통신시험 시스템 구성

본 논문에서 기존 운용방식의 문제점 해결에 대한 제안 방식의 장점 분석과 효율성, 음질, 전송지연 시간 등을 분석하기 위해 단대단 통신장치를 이용하여 이기종 망간 종단간 암호화 음성통신을 통해 PESQ (Perceptual Evaluation of Speech Quality) 테스트[15]을 진행하였다. 음성통신은 실시간성을 바탕으로 통신을 해야 하므로 지연시간 및 신뢰성 분석이 가능하다. 또한 종단간 데이터 통신을 통해 데이터 통신에 대한 전송시간도 측정하였다.

시험 장치의 구성은 다음과 같다. 기존 방식 PSTN용 장치의 제어처리부는 freescale사의 MPC계열의 프로세서를 사용했으며 보코더는 TI(Texas Instruments)사의 DSP를 사용하여 AMBE (Advanced Multi-Band Excitation) 코덱[16]으로 구성했으며 모뎀은 PSTN의 아날로그 전송을 위해 V.22bis 모뎀[17]으로 구성하였다. 기존 방식 UHF망 장치의 제어처리부는 삼성의 S3Cxxxx 계열의 프로세스를 사용했으며 보코더는 TI사의 DSP를 사용하여 MELP(Mixed Excitation Linear Prediction) 코덱을 적용하여 구성하였으며 아날로그 무선전송을 위해 MIL-STD188-110B 모뎀[18]으로 구성하였다.

암호화 방식은 PSTN은 AES(Advanced Encryption Standard)[19]를 UHF 망은 ARIA (Academy Research Institute Agency)[20]를 적용하였다.

제안한 방식에서의 단대단 통신장치의 시스템 구성은 제어처리부의 경우 삼성의 S3Cxxxx 계열의 프로세스를 사용했으며 보코더의 경우 TI사의 DSP를 사용하고 음성 코덱은 MELP를 적용하였고 모뎀은 TI사의 DSP를 이용하여 speech-like wave 폼의 QAM 모뎀[5]을 적용하여 시험하였다. 암호화 알고리즘은 ARIA를 적용하였다.

Table1.은 시스템 구성시 적용되어 있는 코덱 및 모뎀라이브러리, 정보보호 알고리즘을 나타내었다.

Table 1. System Configuration

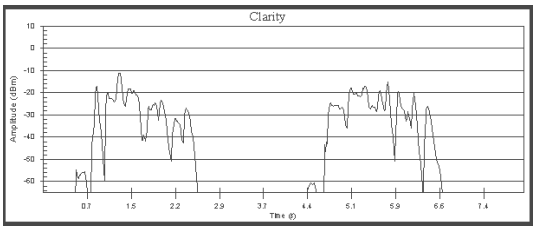
mechanism	Conventional		Proposed
	PSTN	UHF	E2E
Vocoder codec	AMBE	MELP	MELP
modem	V.22bis	MIL-STD 188-110B	QAM
security	AES	ARIA	ARIA

통신 시험망은 기존 방식의 경우 PSTN용 장치를 이용하여 상용의 일반전화망(KT)에 연결하였고 UHF망은 KGRC-2002 V/UHF 무전기를 통신장치와 연결하여 Narrow Band를 이용한 통신망을 구성하였다. 기존 운용방식의 통신시험시 망연동 게이트웨이의 구성은 는 일반 전화망에 연결된 PSTN 통신장치와 UHF망의 통신장치와 연결하여 망연동 게이트장치를 구성하였다.

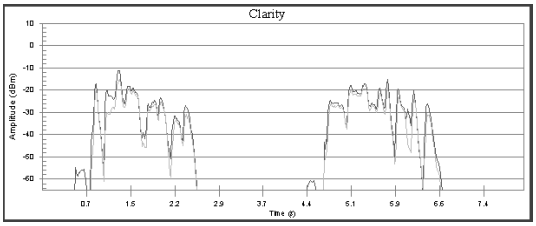
제안한 방식의 통신 시험망은 PSTN 측은 단대단 통신장치를 일반전화기의 송수화기 입출력 단자에 연결하여 전화기를 일반전화망(KT)에 연결하였으며 UHF망 측은 KGRC-2002 V/UHF 무전기의 송수화기셋의 입출력 단자에 단대단 통신장치를 연결하여 Narrow Band로 설정하여 통신망을 구성하였다.

4.2 시험 결과 및 분석

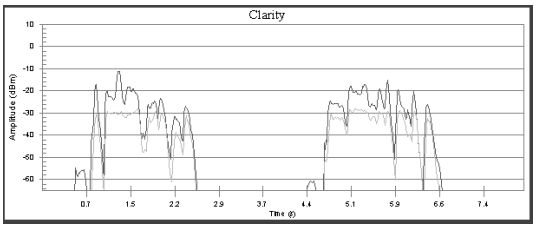
통신시험 시스템을 구성하여 음성 암호화 통신 시험결과 음성신호에 대한 신호 선명도 스펙트럼은 Fig.5.와 같다.



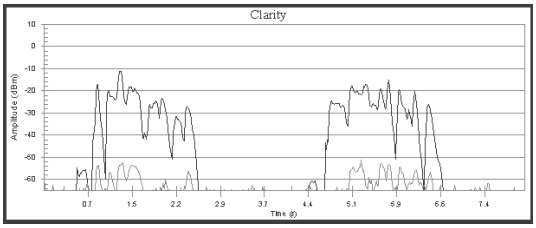
(a) Original voice signal



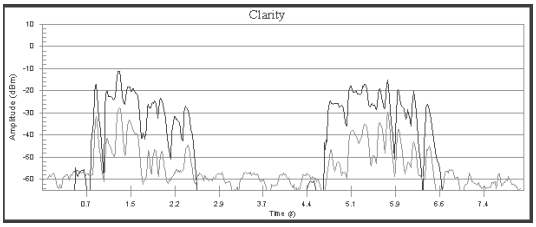
(b) PSTN to PSTN signal using conventional mechanism



(C) UHF to UHF networks signal using conventional mechanism



(d) Comparative signal using conventional mechanism



(e) Comparative signal using proposed mechanism

Fig. 5. Signal of original and comparative voice according to proposed mechanism

Fig.5.에서 원래의 음성신호는 검정색 실선이며 수신한 파형은 회색 실선이다. (a) 음성신호는 송신하기 위한 원래의 음성 신호 스펙트럼이다. (b)는 기존방식의 통신장치로 PSTN 망간 암호화 통신 결과를 나타낸다. 원 음성신호와 큰 차이가 없음을 알 수 있다. (c)는 기존 방식의 UHF 망간 암호화 통신 시험결과이며 MELP 보코더 및 무선망의 특성으로 인해 음성 선명도가 약간 떨어짐을 알 수 있다. (d)는 기존 방식으로 망연동 게이트방식가 PSTN의 AMBE 음성신호를 복호화 후 다시 UHF 망의 MELP 음성신호로 암호화 후 수신단에서 복호화한 결과를 나타내었다. 이 음성신호에서는 선명도가 크게 떨어짐을 알 수 있다. 이는 채널 환경이 좋은 PSTN 보코더에서 UHF 망의 보코더로 변경시 보코더 특성상 음질 열화, 전송망에 대한 효율성으로 인해 음성의 선명도가 많이 떨어진 것이다. 추가적으로 망연동 게이트웨이 구성시 음성신호 연동 과정에서 PSTN 장치와 UHF망 장치의 신호 임피던스 매칭 등이 이루어지지 않아 복호화한 음성 전달이 명확하지 못하여 선명도가 더 떨어진 것으로 추측된다. (e)는 제안된 방식으로 종단간 암호화 통신시 음성신호를 나타낸 음성신호 스펙트럼이다. 원래의 음성신호와 단대단 통신장치에서 수신된 음성신호가 유사하며 음성 선명도도 크게 떨어지지 않음을 알 수 있다. 제안한 방식에서 암호화된 음성을 단대단 통신장치의 QAM 모뎀을 거쳐 망연동 게이트웨이에서 변환없이 그대로 음성신호로 전달되고 음성신호를 음성채널로 그대로 전송하기 때문에 원래의 음성신호와 유사함이 나타남을 알 수 있다. 스펙트럼 중간 부분의 잡음은 신호 임피던스 매칭이 이루어지지 않아 나타났다.

Table 2.는 암호화 통신 시험결과 평균적인 MOS 값의 음질 비교 및 음성 신호 송수신에 대한 지연시간을 비교하였다.

기존 방식의 음성 암호화 송수신에 대한 시험 결과 PSTN간 송수신시 일반 전화망에서 약간 떨어지는 MOS 값은 평균 3.41을 나타났으며 지연은 평균 583.85ms 이다. 도표의 지연시간 중 괄호의 수치는 음성 연결시 V.22bis 모뎀의 호 설정 시간으로 평균 5.1초 정도가 소요되어 표시한 시간이다. UHF 망간 기존방식의 종단간 음성 암호화 통신도 대체로 양호한 MOS 값을 나타냈다.

망연동 게이트웨이를 적용한 기존 방식의 시험에서는 PSTN에서 송신 후 UHF망에서 수신시 MOS 값은 평균 1.96이며 반대의 경우로 송수신시 MOS값은 1.77이다. 또한 송수신 지연시간의 경우 사전에 PSTN의 호가 연결되어 통신시 음성 신호에 대한 지연시간이 약 1,200 ms 정도가 발생하며 호 설정 시간까지 포함되어 지연시간을 측정하면 약 6,300ms 정도의 지연이 발생함을 알 수 있다.

Table 2. PESQ of the comparative voice and end-to-end secure communication delay between PSTN and UHF networks

Mechanism		MOS	Delay time(ms)
conven-tional	PSTN↔PSTN	3.41	583.85 (5683.85)
	UHF망↔UHF	2.76	600.02
	PSTN→UHF	1.96	1221.13 (6332.23)
	UHF→PSTN	1.77	1273.89 (6384.88)
Proposed	PSTN↔UHF	2.81	586.44

제안한 방식으로 시험시 MOS 값은 평균 2.81로 기존 망연동 게이트웨이 방식에 비해 60%정도의 음질 향상이 있음을 알 수 있다. 지연시간은 기존 방 식에서 사전에 PSTN 호 설정이 되어 있을 경우와 비교시 580ms 정도 단축되며 50% 정도 지연시간이 감소함을 알 수 있으며 모뎀 호 설정시간을 포함할 경우 5,600 ms 정도의 시간이 단축됨을 알 수 있다. 제안한 방식에서 PSTN 전화는 전화 다이얼링 후 바로 음성 호가 연결되어 음성채널로 암호화된 신호를 전송하므로 모뎀 호 설정이 필요하지 않다.

위와 같은 결과는 단일의 전술통신망에서에서 단일의 장치를 이용시 종단간 암호통신시 음질 및 지연시간이 별 차이가 없으나 이기종 망 통신시 망연동 게이트웨이가 적용되었을 경우 음성 코덱의 변경, 암호화 방식의 차이로 인한 재암호화, 보코더의 차이로 인해 음질저하, 모뎀에 따른 데이터 재가공에 의한 지연시간, 모뎀 종류에 따른 호 설정시간 등이 크게 차이가 남을 시험결과로 알 수 있다.

Table 3.은 데이터 전송에 대한 평균 전송시간을 기존 방식과 제안한 방식을 비교한 도표이다.

이기종 망간 데이터 통신은 외부 단말에서 통신장치로 입력하여 암호화 후 모뎀을 통해 전송되며 수신측에서 통신장치의 모뎀으로 데이터를 받아 복호화 후 외부 단말로 수신하게 된다.

기존 방식에서 통신장치는 PSTN 통신장치의 경우 데이터 암복호 속도는 평균 687us이며 UHF망 통신장치의 평균 암복호 속도는 592us이다. 제안된 단대단 통신장치도 데이터 평균 암복호 속도는 592us이다. 기존 방식과 제안한 방식 모두 통신장치 모뎀은 2400bps의 전송속도를 갖는다.

Table 3. Transfer time of end-to-end secure communication between PSTN and UHF networks

Mechanism		Transfer time(ms) (1kbytes)
conven-tional	PSTN↔PSTN	3414.02 (8514.02)
	UHF망↔UHF	3415.92
	PSTN↔UHF	3416.61 (8516.61)
Proposed	PSTN↔UHF	3415.89

위 도표에서 기존 방식에서 괄호 부분의 수치는 음성 암호화 통신과 마찬가지로 사전 호 설정 여부에 따른 시간을 표시하고 있다. 통신시험에서 1Kbytes 송신기준 전송시간은 기존 방식의 호가 사전에 설정되어 있을 경우 기존방식과 제안된 방식에 있어 큰 차이를 보이지 않는다. 이는 암호연산 시간과 모뎀의 전송속도 차이가 크지 않고 UHF 망의 경우 평균 1ms 정도의 지연시간으로 인해 큰 차이가 없는 것으로 판단된다. 망연동 게이트웨이에서 재암호화에 의한 연산시간 외에는 큰 차이를 보이지 않는다.

그러나, PSTN 모뎀이 전송속도가 높을 경우 데이터에 대한 단편화 작업과 망연동 게이트웨이에서 UHF 망의 무선 환경에 따른 무선지연시간, 도플러 주파수 영향, 신호대잡음비(SNR: Signal to Noise Ratio), 인터리빙 적용, 채널부호화, 동기화 방식, waveform 등의 설정이 실시간으로 적용해야 할 경우 처리 지연시간이 늘어날 가능성은 있다. 데이터 통신의 경우 호 설정 시간까지 포함한다면 기존 방식 대비 제안한 방식이 효율적이다.

정보호호 측면에서도 기존 방식은 전술통신망의 특성상 망연동 게이트웨이에서 재암호화에 의한 도청 및 데이터 무결성 등의 보안취약점을 제안한 방식을 통해 종단간 사용자 단말에서 암호화하여 전송이 가능하므로 보안 취약점을 제거 할 수 있다.

제안한 방식은 기존방식 대비 이기종 망에서 다른 네트워크별 이기종의 통신장치 보다는 제안된 방식의 이기종 망에 단일의 단대단 통신장치를 적용함으로써 상호 운용성 측면에서 효율적이라 할 수 있다. 또한,

제안한 방식은 기존의 망연동 게이트웨이에서 복호화 및 재암호화에 대한 과정이 없어 도청 및 데이터 무결성에 대한 보안취약점을 없앨 수 있다는 장점과

이기종 망 구축시 데이터 재가공을 위한 망연동 게이트웨이 없이 네트워크 구축이 가능하다는 장점이 있다.

V. 결 론

본 논문의 이기종 전술통신망간 단대단 통신 및 암호통신을 위한 신규 통신 방식을 제안하고 통신장치를 구현하여 이를 실제 운용중인 망에 적용하여 시험하였다. 이를 통해 음성 암호화통신에 대한 음질 선명도 및 통신지연 시간을 비교하였고 데이터 암호화 통신시 1Kbytes 데이터 전송을 기준으로 전송시간을 측정, 비교하였다.

비교 결과 제안된 메커니즘은 종래의 장치와 비교하여 음질, 전송 지연 및 선명도 스펙트럼 특성 관점에서 더 나은 성능을 나타내었으며 MOS 1.04~0.85 정도의 음질 향상과 종래의 장치 대비 최대 50%정도의 전송 지연을 감소시킬 수 있었다. 또한 데이터 암호화 통신시 통화 호 설정시간을 단축했으며 망연동 게이트웨이에서의 재암호화 및 데이터 재가공에 대한 도청, 무결성 등의 보안취약점을 제거하고 시스템 효율성을 높일 수 있었다.

이상의 결과에서 보는 바와 같이 제안한 방식은 이기종 전술통신망 단대단 통신 방법 및 정보보호 방식은 기존 통신망의 음성 및 데이터 전송 효율을 향상시키고 단대단 암호통신에 대한 보안취약점을 해결하며 이기종 망에서 하나의 통신장치 적용으로 망의 효율성, 시스템 상호운용성을 증대시킬 수 있다.

이 논문은 이기종 망의 종단간 암호화에 대한 광범위한 제안 및 분석에 대한 논문이다. 이러한 방식의 메커니즘 적용은 이기종 망에서의 종단간 암호방식을 제공하고 향후 다른 이기종 망의 네트워크 종단간 직접적인 통신에 대해 다양하게 확장될 수 있다.

References

〔1〕 J. Ingerski and A. Sapp, "Mobile Tactical Communications, The Role of The UHF Follows-on Satellite Constellation and Its Successor, Mobile User Objective System," IEEE MILCOM '02, pp. 302-306, 2002.

〔2〕 Park Sang Young, "Cryptanalysis of analog Scambler using the FFT," Journal of Korea Information and Communications Society Vol. 5, pp. 25-29, Jan. 1995.

〔3〕 "Analog to Digital conversion of voice by 2400bps mixed excitation linear prediction(MELP)," MIL-STD-3005, Dec. 1999.

〔4〕 "Mil. Std. Inter- operability and performance standards for data modem," MIL-STD-188-110B, draft ver. revised 7, Mar. 2000.

〔5〕 N. N. Katugampala, K. T. Al-Naimi, S. Villette, and A. M. Kondoz, "Real-Time End-to-End Secure Voice Communications over GSM Voice Channel," EURASIP EUSIPCO '05, 2005.

〔6〕 S. Islam, F. Ajmal, S. Ali, J. Zahid, and A. Rashdi, "Secure End-to-End Communication over GSM and PSTN Networks," IEEE IET '09, pp. 323-326, 2009.

〔7〕 Y. Yang, S. Feng, W. Ye, and X. Ji, "A Transmission Scheme for Encrypted Speech over GSM Network," IEEE ISCSCT '08, pp. 805-808, 2008.

〔8〕 T. Chmayssani, G. Baudoin, and G. Hendryckx, "Secure Communications through Speech Dedicated Channels Using Digital Modulations," IEEE ICCST '08, pp. 312-317, 2008.

〔9〕 C. K. Wong and P. C. Ching, "Digital Speech Transmission for Highly Encrypted and Paramilitary Operated Land Mobile Radio Communications over a Narrowband UHF Channel," IEEE MILCOM '08, pp. 47-52, 1991.

〔10〕 J. M. Alvermann and M. T. Kurdziel, "The Secure Communication Interoperability Protocol (SCIP) over a VHF/UHF Radio Channel," IEEE SSST '10, pp. 1-6, 2008.

〔11〕 K. Kim and J. Hong, "Evaluation of Transmission and Quality Performance of Digital Secure Voice Communications in an HF Network," IEEE ICDT '09, pp. 20-25, 2009.

〔12〕 N. M. Anas, Z. Rahman, A. Shafii, M. N.

A. Rahman, and Z. A. M. Amin, "Secure Speech Communications over Public Switched Telephone Network," IEEE Asia-Pacific Conference on Applied Electromagnetics '05, pp. 336-339, 2005.
〔13〕 L. Diez-del-Rio, "Secure Speech and Data Communication over the Public Switching Telephone Network," IEEE ICASSP '94, pp. II-425-428, 1994.
〔14〕 Ki Hong Kim, "End-to-End Digital Secire Speech Communication over UHF and PSTN," Journal of the Korea Academia-Industrial Cooperation Society, Vol.13, pp. 2313-2318, 2012
〔15〕 "Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs," ITU-T Recommendation P.862, 2002.
〔16〕 http://www.dvsinc.com/products/software.htm.
〔17〕 "2400 bits per second duplex modem using the frequency division technique standardized for use on the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits," ITU-T Recommendation V. 22 bis, 1993.
〔18〕 US DoD, "MIL-STD-188-110B, Military Standard - Interoperability and Performance Standards for Data Modems," 2000.
〔19〕 "Advanced Encryption Standard (AES)," FIPS PUBS 197, 2001.
〔20〕 "A Description of the ARIA Encryption Algorithm," IETF RFC 5794, 2010.

〈저자소개〉

사 진

박 철 용 (Cheol-Yong Park) 정회원
1999년 2월: 광운대학교 전자공학과 졸업
2001년 2월: 광운대학교 전자공학과 석사 졸업
2006년 9월~현재: 충남대학교 컴퓨터공학과 박사과정
2000년 11월~현재: 한국전자통신연구원 부설연구소 선임연구원
〈관심분야〉 통신 정보보호, 시스템 보안

사 진

김 기 홍 (Ki-Hong Kim) 정회원
1998년 2월: 경북대학교 전자공학과 졸업
2000년 2월: 경북대학교 전자공학과 석사 졸업
2007년 8월: 고려대학교 정보보호학과 박사 졸업
1999년 12월~2000년 9월: LG 전자 연구원
2000년 9월~현재: 한국전자통신연구원 부설연구소 선임연구원
〈관심분야〉 통신 정보보호, 신호처리

류 재 철 (Jae-Cheol Ryou) 종신회원
1985년 2월: 한양대학교 산업공학과 졸업
1988년 2월: Iowa State University 전산학과 석사 졸업
1990년 2월: Northwestern University 전산학과 박사 졸업
1991년~현재: 충남대학교 전기정보통신공학부 교수
〈관심분야〉 인터넷 보안