드론 데이터 보안을 위한 소형 양자통신암호화장비 제안

김형엽, 이옥연*

국민대학교*

gudduq159@kookmin.ac.kr, oyyi@kookmin.ac.kr*

Proposal for an Compact Quantum Encryptor for Drone Data Security

Hyeong-Yeop Kim, Okyeon Yi*

Kookmin University*

요 약

4차 산업혁명의 전개와 더불어 인공지능(AI), 빅데이터, 양자컴퓨터 등의 첨단 기술이 급속도로 발전하고 있다. 이러한 배경 속에서 6G, 위성통신, 양자암호통신과 같은 차세대 통신 기술에 대한 연구도 활발하게 이루어지고 있다. 특히 양자암호통신은 양자의 불확정성 원리에 기반하여 도청이 불가능하다는 점에서 매우 높은 보안성을 제공할 것으로 기대된다. 그러나 현재 양자암호통신 기술은 크고 무거운 하드웨어 장치를 요구하는 한계가 있기 때문에 드론이나 로봇과 같은 소형 장치에 탑재되기 어려운 실정이다. 본 논문에서는 이러한 문제를 해결하기 위한 방안으로 양자암호통신의 구성에서 암호부를 소형화하여 소형 장치에 적용할 수 있는 구조를 제안한다. 또한, 양자 키 분배를 통해 공유된 키를 사용하여 데이터를 구간 암호화할 때의 스루풋 측정하여 드론 환경에서 가용성을 분석한다.

Ⅰ. 서 론

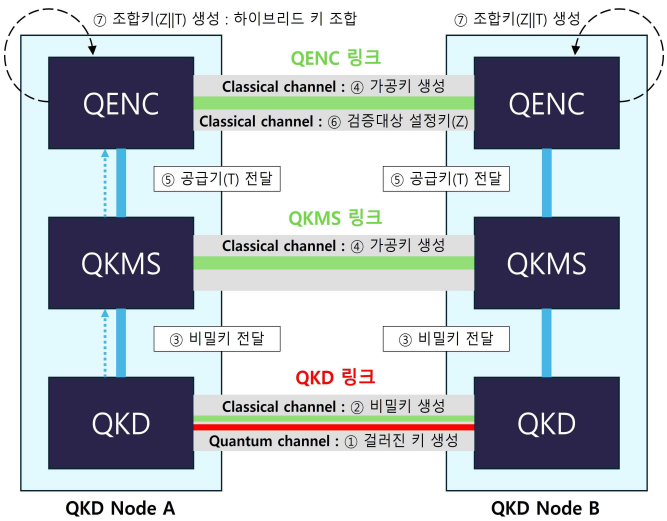
4차 산업혁명이 전개됨에 따라 인공지능(AI), 사물인터넷(IoT), 양자컴퓨터와 같은 첨단 기술의 급격한 발전은 6G, 위성통신과 더불어 양자암호통신 같은 차세대 통신 기술의 연구를 촉진하고 있다. 양자컴퓨팅의 발전은 기존 암호 체계의 안전성을 위협하기 때문에 전 세계적으로 양자내성암호와 양자키분배의 기술 개발 및 표준화 작업이 활발하게 이루어지고 있다.[1] 국내에서는 KT, SKT, 한국과학기술정보연구원(KISTI)을 포함한 여러 기관에서 양자암호통신장비의 고도화 및 상용화를 위한 연구개발에 매진하고 있다. 2023년 4월에는 국가정보원에서 세계 최초로 양자암호통신장비의 보안기능 시험제도를 시행하였다. 해당 제도에서는 양자암호통신장비(QKD Node)를 세 구성요소로 나누어 각각의 보안 요구사항을 정의하며 보안기능 시험 시 해당 보안요구사항을 준수하는지 시험한다.[2]

현재 개발되고 있는 양자암호통신장비는 물리적으로 크고 무거운 하드웨어 장치를 요구하기 때문에 그 자체로 모바일 환경이나 드론과 같은 소형 장비에 적용하기 어렵다는 한계를 갖는다. 이에 본 논문에서는 양자암호통신의 암호부인 양자통신암호화장비(이하 'QENC')를 소형화하여 드론 등의 장비에 탑재하는 구조를 제안한다. 또한, 드론과 지상국 사이에서 전송되는 센서, 영상과 같은 다양한 데이터를 보호하는 기능으로 구간암호화를 수행하여 가용성을 분석한다.

Ⅱ. 관련 연구 - 양자암호통신장비의 구성

본 장에서는 [2]에서 정의한 양자암호통신장비의 구조와 각 요소 장비를 설명한다. 양자암호통신장비는 [그림 1]과 같이 세 개의 계층으로 구성되며 각 계층은 특정한 역할과 기능을 담당한다. 아래층에 위치한 양자키분배장비(QKD, Quantum Key Distribution)는 양자 채널과 클래식 채널을 통해 비밀키를 안전하게 분배하는 역할을 한다. 이 장비는 BB84 프로토콜과 Decoy 방법을 활용하여 키를 공유하며, 이때 전송되는 양자의 물리적 특성에 따라 제 3자에 의한 도청을 원천적으로 차단할 수 있다.

가운데층에는 양자키관리장비(QKMS, Quantum Key Management System)가 위치한다. QKMS는 QKD로부터 전달받은 비밀키를 안전하게 저장하거나 필요한 장비 및 시스템에 비밀키를 공급하는 등의 키 생명주기 전반을 관리한다.



〔그림 1〕 양자암호통신장비 구성도

마지막 윗층에는 양자통신암호화장비(QENC, Quantum Encryptor)가 위치한다. QENC는 QKMS로부터 받은 공급키(T)와 자체적으로 또는 다른 QENC와 공유한 가공키(Z)를 조합하여 최종적인 조합키(Z||T)를 생성한다. 조합키 생성을 위한 키 유도 함수는 검증대상 암호 알고리즘의 KBKDF를 사용한다. 생성된 조합키는 두 QENC 간의 데이터 통신을 암호화하는 데 사용된다. 또한, QENC에서는 양자내성암호(Post-Quantum Cryptography) 키 교환 알고리즘(KEM, Key Encapsulation Mechanism)을 통해 공유된 키도 양자 키로 허용된다.

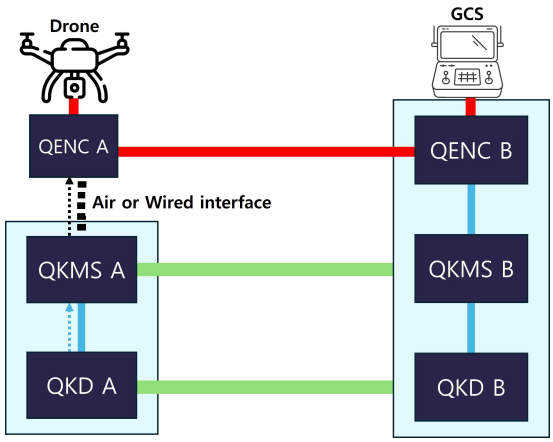
Ⅲ. 소형 양자통신암호화장비의 운영 구조

양자암호통신장비에서 QKD, QKMS 제품의 형태에 따라 서로가 독립적인 장비 혹은 일체형 장비로 구성될 수 있다. [2]에서는 QKMS의 여러 보안 요구사항을 정의한다. 그 중 QENC와 키 공급을 포함한 통신을 위한 보안 요구사항은 [표 1]과 같이 정의되어 있다.

〔표 1〕 양자키관리장비의 보안 요구사항

식별번호	기능명세	보안기능의 구현 강도
1.4.1	제품은 공급키를 QENC에게 안전하게 공급해야 한다.	필수
4.1.1.	제품은 검증필 암호모듈을 이용한 암호통신을 사용하여 데이터를 전송해야 한다.	필수
4.1.2	제품은 QKD 네트워크의 통신상대와 상호 인증을 수행해야 한다.	필수

드론을 위한 소형 양자통신암호화장비의 운영 구조를 [그림 2]와 같이 구성한 경우, QENC와 QKMS 사이에서 [표 1]의 상호 인증 및 데이터 보호를 통해 안전하게 키를 공급한다면 보안 요구사항을 준수하면서 드론과 GCS 구간의 양자 키 기반 데이터 보호를 제공할 수 있다.



〔그림 2〕 드론용 소형 양자통신암호화장비 구성도

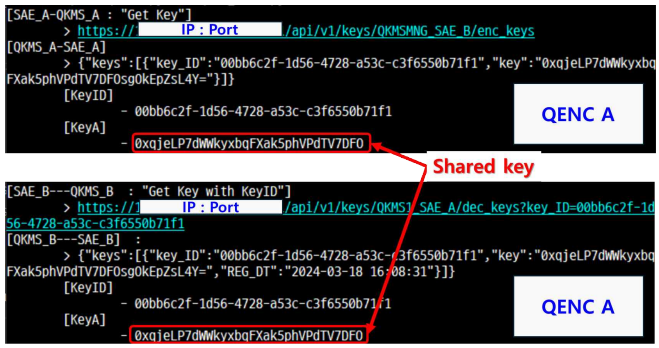
제안하는 드론용 소형 QENC의 운영 구조는 QENC가 드론에 탑재되어 QKMS와 유·무선으로 연결되는 구조로 구성된다. 이때, QENC에서 [표 1]의 보안 요구사항을 준수하여 QKMS와 검증필 암호모듈을 이용하여 상호 인증 및 암호화 통신을 수행하여 안전한 키 교환을 수행해야 한다.

Ⅳ. QENC-QKMS의 양자 키 공유 및 가용성 분석

〔표 2〕 각 개체의 실험 환경 구성

구성 요소	실험 환경
Drond	• 라즈베리파이 B+ (Coretex-A53)
GCS	• Window11 데스크탑 (Intel i7-1065G7)
QENC A	• 라즈베리파이 CM3+ 기반 하드웨어 암호화 장비 (Coretex-A53)
QENC B	
QKMS	• 양자키관리장비
QKD	• 양자키분배장비

[그림 2]에 대한 실험은 제안한 운영 구조에서 각각의 QENC가 QKMS와 연동되어 키를 공유하는 단계와 공유된 양자 키를 사용하여 구간 암호화를 수행할 때의 스루풋을 측정하는 단계로 구성하였다. 실험에 사용된 장비는 [표 2]와 같다. 각각의 QENC에서 [그림 3]과 같이 QKMS로부터 키를 공급 받아 동일한 양자 키가 공유된다.



〔그림 3〕 QKMS-QENC 연동 키 공급 결과

[표 3]은 공유된 양자 키를 이용하여 구간 암호화가 구동될 때, iperf로 양방향의 스루풋을 측정한 결과이다. 5초 동안 1초 간격으로 테스트한 평균 스루풋은 약 36~41Mbps임을 알 수 있다.

〔표 3〕 QENC의 구간암호화 스루풋 측정 결과

Sender	Avg. Transfer	Bitrate	Retransmitted Packets
Drone	4.38 Mbytes	36.76 Mbits/sec	0
GCS	3.87 Mbytes	41.58 Mbits/sec	0

드론은 민간에서 군수 분야까지 폭넓게 운영되면서, 수행하는 임무에 따라 비행 상태, 경로 등의 제어 정보부터 영상, 센서 정보와 같은 비행 데이터가 발생할 수 있다. 실시간으로 드론에서 GCS로 전송하는 영상 정보는 가장 많은 스루풋을 요구하는 서비스 중 하나이다. 이론적으로 1080p의 영상의 경우 H.264 코덱을 사용하는 경우 높은 품질의 영상 전송을 위해 약 20Mbps의 bitrate를 요구하기 때문에 QNEC를 통해 드론과 GCS 간의 송·수신 데이터를 안정적으로 보호할 수 있을 것으로 기대된다.

Ⅴ. 결론

본 연구는 양자암호통신장비를 드론과 같은 소형 장비에 도입하기 위한 운영 방법론을 제시하였다. 현재 시장에 인증받은 양자암호통신장비가 없는 상황에서 [2]의 요구사항에 따라 발전되면 추후 높은 보안성이 요구되는 국가 주요 인프라에 적용되는 QENC 연구의 초석이 될 것이라 기대한다.

ACKNOWLEDGMENT

본 연구는 대한민국 정부 산업통상자원부 및 방위사업청 재원으로 민군협력진흥원에서 수행하는 민군기술협력사업의 연구비 지원으로 수행되었습니다.(과제번호 21-CM-AU-09)

참 고 문 헌

[1] 김동천, 김영범, 서석충. (2023). NIST PQC 공모전 동향 분석 및 표준화 대상 & Round 4 알고리즘 소개. 정보보호학회지, 33(2), 39-48.

[2] 국가정보원, 국가용 보안요구사항V3.0 - 양자암호제품군, 2023년 3월 27일.