論文 J. of The Korean Society for Aeronautical and Space Sciences 46(7), 602-609(2018)
DOI:https://doi.org/10.5139/JKSAS.2018.46.7.602
ISSN 1225-1348(print), 2287-6871(online)

하이브리드 암호시스템을 이용한 군집 UAV 영상의 고속 암호화

조성원*, 김준형*, 채여경*, 정유민*, 박태규**

Fast Video Data Encryption for Swarm UAVs Using Hybrid Crypto-system

Seong-Won Cho*, Jun-Hyeong Kim*, Yeo-Gyeong Chae*, Yu-Min Joung* and Tae-Kyou Park**
Department of Aerospace Software Engineering, Hanseo University*,**

ABSTRACT

This paper proposes the hybrid crypto-system for fast video data encryption of UAV(Unmanned Aerial Vehicle) under the LTE(Long-Term Evolution) wireless communication environment. This hybrid crypto-system is consisted of ECC(Elliptic Curve Cryptography) public key algorithm and LEA(Light-weight Encryption Algorithm) symmetric key algorithm. ECC is a faster public key algorithm with the same security strength than RSA(Rivest Shamir Adleman), and Korean standard LEA with the same key size is also a faster symmetric key algorithm than AES(Advances Encryption Standard). We have implemented this hybrid crypto-system using OpenSSL, OpenCV and Socket programs under the Swarm 8-UAV. We have shown the efficient adaptability of this hybrid crypto-system for the real-time swarm UAV through the experiments under the LTE communication environment.

초 록

본 논문은 LTE 통신망 환경에서 군집 UAV의 비디오 영상 데이터를 고속으로 암호화하기 위한 하이브리드 암호시스템을 제안한다. 이 암호시스템은 ECC 공개키 알고리즘과 LEA 대칭키 알고리즘으로 구성된다. ECC는 RSA보다 빠르면서 동일한 보안성을 가지며, LEA는 동일한 키로 AES보다 빠른 국내 표준 알고리즘이다. 본 논문은 OpenSSL과 OpenCV를 활용하여 Socket 프로그램으로 8개의 군집 UAV 환경에서 하이브리드 암호시스템을 구성하여 구현하였다. 실험을 통하여 본 하이브리드 암호시스템이 실시간 환경에서 효율적으로 적용이 가능함을 보인다.

Key Words : Swarm UAV(군집 무인항공기), Hybrid Crypto-system(혼합 암호시스템), ECC(타원곡선 암호), LEA(경량급 암호), Video Encryption(비디오 암호화)

Ⅰ. 서 론

UAV의 활용은 군사용에서부터 취미용에 이르기까지 매우 다양하며, 정보통신기술과의 결합으로 더욱 다용도화, 다기능화 되고 있다. 그러나 UAV 활용의 확산에 따라서 GPS 스푸핑, 신호

† Received : February 28, 2018 Revised : June 5, 2018 Accepted : June 21, 2018
** Corresponding author, E-mail : tkpark@hanseo.ac.kr

재밍, 데이터와 영상 해킹, 기체 탈취, 바이러스 감염 등의 사이버 보안 문제가 발생되고 있다[1,2]. 한 예로, 미군용 Predator UAV의 중요한 비디오 영상이 이라크에서 해킹된 사실이 밝혀진 바 있다. 이 사건은 영상 정보가 암호화되지 않았기 때문에 통신 링크를 통해서 단 $26의 SkyGrabber SW[3]에 의해 다운로드 해킹된 것으로 분석되었다[19,20]. 이처럼 UAV의 눈 역할을 하는 카메라를 부착하고 임무를 수행하는 군사용이나 특수 목적용 UAV에서는 영상 보안 기능이 꼭 필요하다는 것을 시사한다. 그리고 최근 UAV의 발전은 군집 UAV(Swarm UAV) 형태로 운용과 활용의 효율화를 추구하고 있으며, LTE 망[4]을 활용하여 비행거리의 제한을 탈피하여 원격으로 실시간 조종 및 영상 정보 전달을 가능하도록 하는 추세이다.

그러나 이러한 LTE 망 환경에서 실시간으로 UAV의 영상 정보를 암호화하는 기존의 연구가 없으며, 많은 수의 군집 UAV 환경에서 영상 보안을 위한 연구도 전무한 실정이다.

따라서 본 연구에서는 LTE 무선 통신 환경에서 지상의 GCS(Ground Control Station)가 군집 UAV로부터 촬영한 영상 데이터를 실시간으로 원격 수신하여 UAV를 제어하며 통신할 때, 전송 영상의 안전한 보안 기능(공개키 교환, 공개키 검증, 비밀키 생성, 영상 암호화)을 제공하기 위해서, 하이브리드 암호시스템을 구성하여 고속으로 처리하는 방법을 제안한다.

본 논문은 2장에서 군집 UAV의 구성 환경에 적용할 암호시스템을 소개하며, 3장에서는 공개키 방식의 ECC와 대칭키 방식의 LEA 알고리즘을 혼합하여 설계한 하이브리드 보안 프로토콜을 제시한다. 4장에서는 OpenSSL, OpenCV를 이용하여 Socket 프로그램으로 8개의 군집 UAV 환경에서 구현한 내용을 설명한다. 5장에서는 ECC-AES(128비트 키) 혼합 방식과 ECC-LEA(128비트 키) 혼합 방식(본 논문 제안 방식)에서의 처리 성능의 비교를 통하여 본 제안의 적용성과 효율성을 보인다.

II. 군집 UAV와 적용 암호시스템

단순 무선 조종기(예, RF 2.4GHz, 915MHz, 433MHz)로 UAV와 송수신 할 수 있는 거리는 시계 거리와 비슷한 2Km 내외로 매우 제한적이다. 따라서 거리 제한 없이 통신망이 구축되어 있는 곳이라면 어디든 UAV 조종이 가능하도록 LTE 통신망을 기반으로 하는 제어 방식으로 최근 진화하고 있다[7,8]. 이를 통하여 원격으로 육지나 해상 조난, 정찰, 화재, 택배, 촬영 등의 임무 수행이 가능하게 된다. 군에서도 별도의 통신망을 통해서 이와 유사하게 임무를 수행할 수 있다. 또한 최근 군집 UAV는 소수의 숙련된 조종 인원으로 많은 UAV를 동시 운용함으로써 협업하거나 역할을 나누어 최대의 업무 효율을 기대할 수 있다[9]. 이때 GCS와 군집 UAV 사이, 혹은 군집 UAV끼리(Intra-swarm)에서 주고받는 정보 및 GCS로 전송하는 중요 영상 정보는 암호화가 필요하게 된다. 따라서 교환 정보의 암호화 시 많은 노드(GCS와 UAV)에서 많은 키가 필요하게 되는데, ECC 공개키 방식을 적용하면 키 생성, 키 전송, 인증, 서명 등 보안 측면에서 많은 이점이 있으며, 추후 군집 UAV의 수를 확장할 때에도 키 관리가 용이하게 된다[14]. 따라서 본 논문에서는 안전하며 빠른 ECC 공개키 방식과 국내에서 개발된 빠른 표준 LEA 대칭키 방식을 혼합한 하이브리드 방식을 적용하여, 다수의 군집 UAV와 GCS 간에 전송하는 큰 용량의 영상 데이터를 낮은 오버헤드로 고속 암호화가 가능함을 보인다.

Figure 1은 적용하는 LTE 환경에서 운용되는 군집 UAS(Unmanned Aerial System)를 보여준다. LTE 환경에서 UAS는 MAVLink[4,5] 통신 프로토콜이 적용되며 GCS에서 UAV로의 제어 명령어 전송과 UAV에서 GCS로의 Telemetry 정보가 MAVLink 프로토콜에 의해 전송된다. 각 UAV는 Satellite를 통해 GPS 정보를 수신한다. 필요에 따라 하나의 UAV(Leader UAV) 혹은 여러 UAV에서 촬영한 카메라 영상 데이터도 LTE 환경 하에서 전송된다. 따라서 상호 암호 통신을 위해서 Fig. 1과 같이 모든 참여 노드에 ECC 공개키와 개인키가 한 쌍씩(Q, d) 생성되어야 한다.

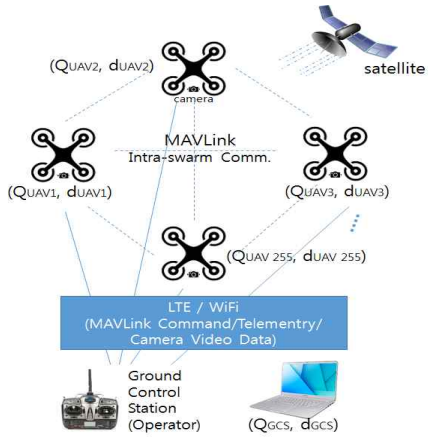

Fig. 1. LTE Swarm UAS Architecture

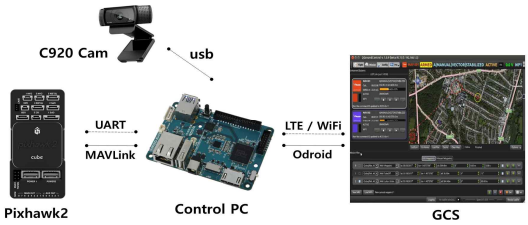

Fig. 2. GCS-UAV Communication

향후 군집 UAV의 수를 확장할 시에도 본 ECC 암호시스템을 적용하게 되면 키 관리와 암호화가 용이하게 된다. Fig. 2는 GCS와 UAV 간의 통신 환경으로 각 UAV에 탑재되는 Control PC는 Odroid Board(Octacore)[10], Flight Control Board는 Pixhawk2[11]로 구성하였다. 소프트웨어 스택은 Ubuntu 14.04 LTS(Linux), OpenSSL, OpenCV, Socket 프로그램으로 구성하였다. 카메라 비디오 영상은 스트림 방식으로 Codec(JPEG 혹은 MPEG)을 선택하여 프레임 수를 조정할 수 있다.

III. 하이브리드 암호시스템 설계

3.1 ECC 공개키 암호알고리즘

ECC는 최근 대두된 IoT(Internet of Things) 환경에서 가장 유용하게 사용되는 타원곡선 상에서 이산 대수 문제의 어려움에 기반한 공개키 암호 알고리즘이다[13]. ECC는 RSA 공개키와 비교하여 더 짧은 키로 동일한 보안성을 제공할 수 있으며 빠르게 처리되는 장점이 있다[15]. 예로 Table 1에서 보는 바와 같이 256비트 키의 ECC의 보안 강도는 128비트 키의 AES와 동일하며, 3072비트 키의 RSA와 동일하다[12]. 또한 ECDH는 Diffie - Hellman 키 교환 방식에 기반을 두고 있어 안전하게 비밀키의 생성이 가능하다. 따라서 기존의 표준 대칭키 암호 알고리즘(AES, LEA 등)과 결합하여 하이브리드 암호시스템으로 구성하기에 적합하다. ECDSA는 전자서명 방식인 DSA(Digital Signature Algorithm)에 기반을 두고 있어 공개키 교환 시에 키의 서명과 검증이 용이하다. 이러한 장점으로 ECC는 최근 IoT 등의 임베디드 시스템에서 키 교환 및 인증, 전자서명, 난수 생성 등의 업무에 적용되고 있다. 본 논문에서는 Table 2에서 보는바와 같이, OpenSSL의 Library를 통해 보안 강도가 Good 수준인 128비트의 ECC 256비트 개인키(Private Key)와 Prime 256v1 커브를 사용하여 설계하였다[17,18].

Table 1. Comparable Security Strengths

Security Strength	Symmetric Key Alg.	RSA Key(bit)	ECC Key(bit)
80 bit	DES(2K)	1024	160-223
112 bit	DES(3K)	2048	224-255
128 bit	**AES-128**	**3072**	**256-383**
192 bit	AES-192	7680	384-511
256 bit	AES-256	15360	512+

Table 2. ECC and OpenSSL curve name

Security Strength	ECC (bit)	NIST curve name	OpenSSL curve name	Recommend-ation (security)
96 bit	192	p-192	prime192v1	Low
112 bit	224	p-224	secp224r1	Medium
128 bit	**256**	**p-256**	**prime256v1**	**Good**
192 bit	384	p-384	secp384r1	Top Secret

Table 3. Speed of LEA-128 and AES-128

Algorithm	Speed (cycles/byte)	CPU
LEA-128	4.51	Intel Core2 Quad Q6600
AES-128	9.32	Intel Core2 Quad Q6600

3.2 LEA 대칭키 암호알고리즘

LEA는 2012년 국내에서 개발된 128비트 경량 고속 블록 대칭키 암호 알고리즘으로 128비트 블록 크기로 처리하며 128, 192, 256비트 키 중 하나를 선택할 수 있다. LEA는 특히 소프트웨어와 IoT에 적합하도록 개발되었으며, 현재 정보통신협회 표준 암호 알고리즘으로 등록되었다[16]. 또한 LEA는 Table 3과 같이 미국 표준인 AES보다 1.5~2배가 빠른 것으로 알려져 있다[6].

3.3 하이브리드 암호화 프로토콜

불특정 다수가 사용하는 패킷 통신 기반의 LTE 네트워크에서 UAV의 영상 데이터가 전달되기 때문에 본 논문에서는 2가지 요소를 고려하여 설계하였다. 첫째는 영상 소스인 UAV에서 암호화되어 최종적으로 GCS에 전달될 때까지 복호화가 되지 않는 종단 간 암호화(end-to-end encryption)이고, 둘째로 군집 UAV 환경에서 GCS와 UAV 간의 통신이 실시간으로 이루어지기 때문에 고속 암호화 또한 매우 중요한 요소이다.

본 논문에서는 우선 카메라 영상 데이터를 안전하고 빠르게 처리할 수 있도록 암호화 프로토콜을 Fig. 3과 같이 설계하였다. 이 프로토콜은 ① 각 노드에서 개인키를 임의로 선택하고 공개키를 생성한다. ② 자신의 공개키에 대해 해시

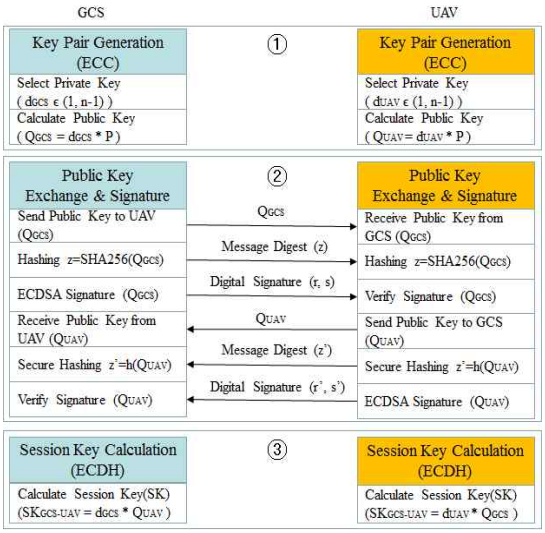

Fig. 3. Security Protocol for GCS-Swarm UAV

(해시 함수 SHA256) 값을 산출하고 전자서명(ECDSA)을 수행한 후, 상대 노드에 공개키와 함께 전송한 후, 각자 상대 노드에서 상대의 공개키를 검증한다. ③ ECDH를 이용하여 수령한 상대의 공개키를 통해 세션키로 사용할 LEA 알고리즘의 비밀키(SK)를 생성한다.

Figure 4는 세션키(SK)로 비디오 영상 데이터를 대칭키 알고리즘인 LEA로 암호화하여 GCS로 전송하는 방식을 보여준다. 따라서 이 하이브리드 암호화 프로토콜을 이용하면 대칭키 알고리즘의 고속성과 공개키 알고리즘의 키 관리 용이성이 결합되기 때문에 다양한 보안 서비스 환경에서 대용량 데이터를 빠르게 처리하거나 스마트폰 보안 등 저 전력 암호화에 적합하다. 실시간 환경에서 동작하는 UAV의 영상 암호화는 계산량이 많고 전력 소모가 큰 기존의 RSA 알고리즘이나 AES와 같은 암호화 알고리즘의 사용이 적합하지 않다. 또한 대칭 암호만을 사용할 경우 n이 UAV의 수라면, n(n-1)/2의 키 개수가 필요한 반면 공개키의 사용은 2n의 키 개수를 가져 n의 수가 증가할수록 전체 시스템의 키 관리가 용이하다. 따라서 본 논문에서는 IoT 환경에 적용하기에 적합한 ECC와 빠르면서도 안전한 것으로 검증된 경량급 암호화 알고리즘인 LEA를 결합한 하이브리드 암호시스템을 군집 UAV 환경을 고려하여 설계하였다.

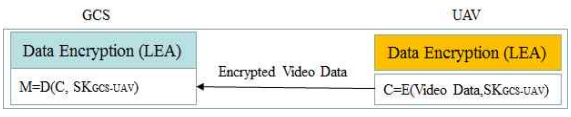

Fig. 4. Video Data Encryption with Group Session Key(SK)

Ⅳ. 영상 암호화 시스템 구현

4.1 OpenSSL에 LEA 추가 구현

OpenSSL은 네트워크를 통한 데이터 통신에 쓰이는 프로토콜인 TLS와 SSL의 open source 구현판으로, C 언어로 작성되어 있는 중심 라이브러리 안에는, 기본적인 암호화 기능 및 여러 유틸리티 함수들이 구현되어 있다. 본 논문에서는 OpenSSL을 기반하여 ECC 암호를 사용하면서 설계한 LEA의 구현을 위해서 OpenSSL이 지원하는 라이브러리에 대칭키 암호 통합 방법[21]에 따라서 LEA 암호 알고리즘 관련 함수를 추가하여 이를 활용하였다. 한국인터넷진흥원(KISA)에서 배포하는 OpenSSL용 오픈소스 모듈 라이브러리를 추가시켜 일련의 작업[22] 후에 컴파일을 하면 LEA 암호화 라이브러리를 OpenSSL에서 확장할 수 있게 된다.

4.2 Socket 프로그램을 활용한 구현

본 논문에서는 설계한 하이브리드 암호 시스템을 OpenSSL 환경에서 Socket 기반(C, C++ 언어)으로 8개로 구성한 군집 UAV 환경(Fig. 5)에서 구현하였다. 이는 설계한 보안 프로토콜 Fig. 3의 ①, ②, ③의 과정을 다중 스레드 프로그램으로 구현한 것으로 Fig. 5에서 보는 바와 같이 그 절차는 다음과 같다. 첫째, 각 참여 노드에 ECC 공개키(Q_{UAV}), 개인키(d_{UAV}) 한 쌍씩을 생성하는데 이때 prime256v1 커브를 사용한다. 둘째, GCS와 각 UAV 간에 공개키를 교환하고 ECDSA를 통하여 전자서명과 검증을 거친다. 셋째, GCS와 각 UAV는 상호 간에 사용할 세션키(K_1~K_8)를 추출한다. 넷째, 군집 UAV에서 공통적으로 사용할 대칭키인 Group Session Key(SK)는 Server GCS에서 별도로 임의(PRNG 함수 사용)로 생성

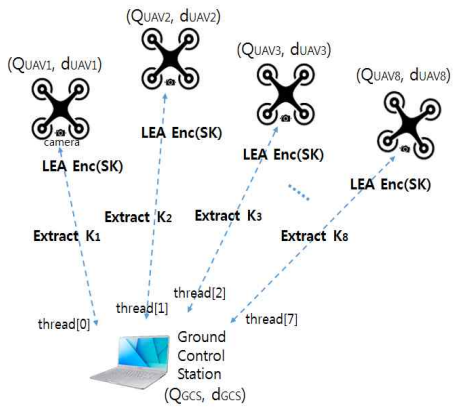

Fig. 5. Group Session Key(SK) Distribution

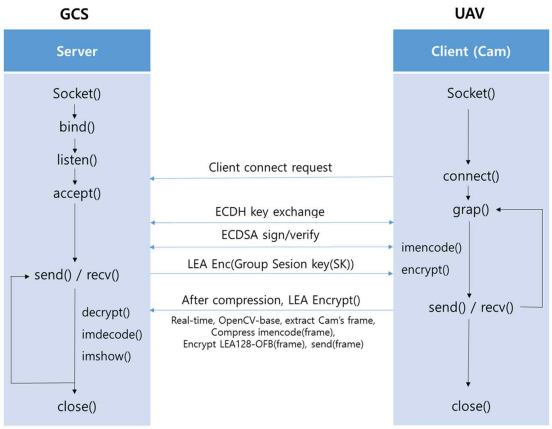

Fig. 6. Socket Programing for Security Protocol

하여 LEA로 앞서 추출된 각 UAV의 대칭키(K_1~K_8)로 암호화하여 각 Client UAV에 배포한다. 이러한 SK의 배포는 GCS Server에서 다중 스레드를 통해서 분리, 할당 방식으로 동시에 처리된다. 이제, Fig. 6에서 보는 바와 같이 UAV Webcam으로부터 입력되는 영상 데이터를 LEA(128비트 SK 키 사용) OFB 모드로 암호화하여 GCS로 송신하게 된다. 이 과정은 LEA가 추가된 OpenSSL과 영상 처리를 위한 OpenCV의 라이브러리(MPEG, JPEG codec)를 사용하여 리눅스 Socket 프로그래밍으로 구현하였다. 여기에서 Client는 캠을 연결한 UAV이며, GCS는 Server로 구현된다. UAV의 카메라는 Logitech-c920 Webcam을 사용하였고, 컬러 프레임(921,600pixel)으로 실시간 스트리밍이 가능하며, 빠른 처리를 위해서 압축 후 암호화(after-compression) 방식으로 처리된다. 이러한 환경에서 구현된 본 하이브리드 암호 시스템의 SK 키 배포 메커니즘은 ECC의 짧은 256bit 키로 다중 스레드를 통해 모든 UAV에서 동시에 키교환, 인증, 전자서명을 수행한다. 또한 SK를 이용한 LEA로 모두 경량화된 고속 암호화가 가능하기 때문에 기존의 군집 UAV 환경에서 요구하는 낮은 처리 오버헤드를 가지면서도 높은 보안성과 고속화를 충족해야 한다는 어려움을 해결한다.

Figure 7과 8은 GCS Server와 UAV client에서 자신의 공개키 생성 후, 상대 노드와의 공개키 상호 교환, 서명 및 검증 그리고 LEA를 위한 공통 세션키 계산 과정을 각각 보여준다. 끝부분의 "ret : 1"은 서명의 성공적 검증을 나타낸다.

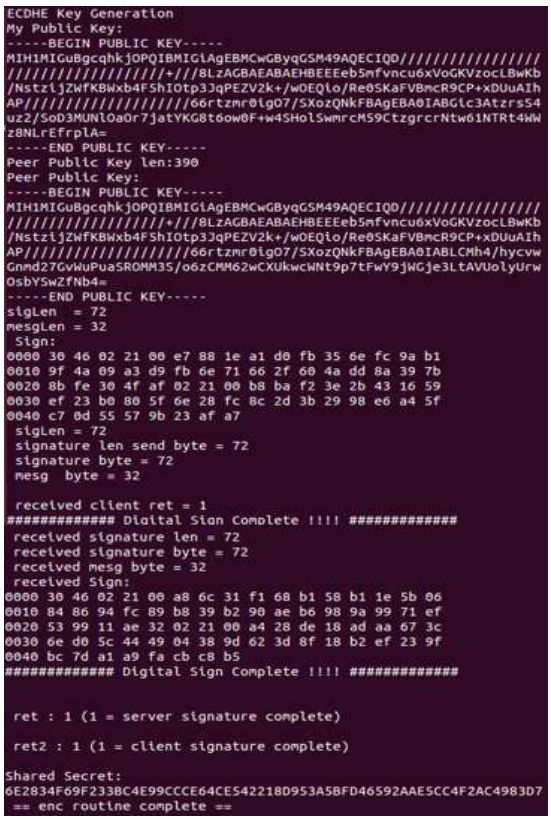

Fig. 7. Generate, exchange, sign and verify public key. Calculate session key for GCS server.

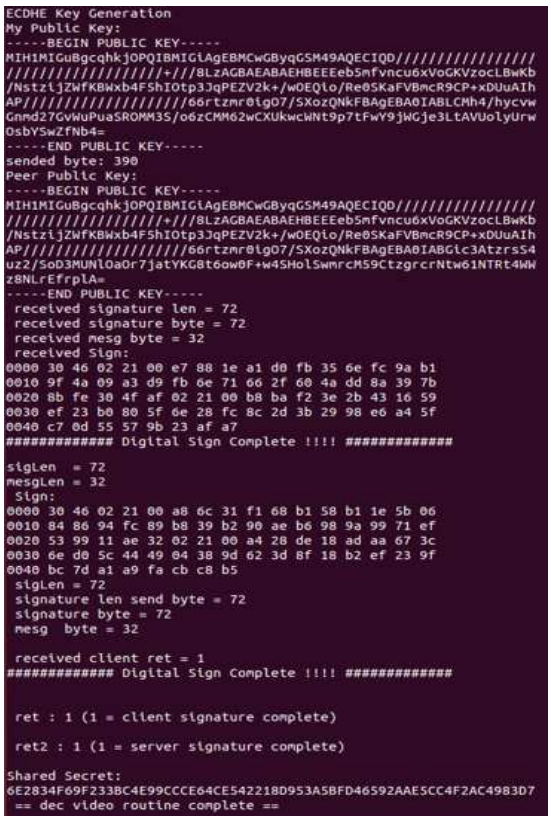

Fig. 8. Generate, exchange, sign and verify public key. Calculate session key for UAV client.

Ⅴ. 실험 결과 및 평가

구현된 암호시스템은 실시간 군집 UAS 환경에서 운용되기 때문에 암호화 처리로 인해 발생되는 오버헤드의 최소화가 중요한 요건이다. 따라서 이를 확인하기 위해서 구현 암호 시스템의 오버헤드를 3가지 방법으로 측정하였다. 첫 번째, 다양한 크기의 동영상 파일을 UAV Control PC(Jetson/Odroid)에서 LTE 통신망을 거쳐 GCS 노트북 컴퓨터로 일괄(Batch) 전송하는 방식으로, Table 4와 Fig. 9에서 보이는 바와 같이 ① 비암호화의 경우 ② ECC와 AES(128비트 키)를 결합한 암호화 ③ ECC와 LEA(128비트 키)를 결합한 암호화(본 논문 제안 방식) 경우로 나누어 처리 속도를 측정하였다. 여기에서 RSA의 활용을 배제한 이유는 ECC와 비교할 때 계산량이 현저히 많아 암호화 처리가 매우 늦어 실시간 처리에 적합하지 않기 때문이다. 따라서 암호화 처리 성능을 ECC와 AES를 결합한 경우, ECC와 LEA를 결합한 경우에서 측정하여 비교하였다. 그 결과, 오버헤드는 본 제안 방식이 ECC와 AES를 결합한 방식보다 평균 약 25.2% 낮게 나타났다. 여기에서 LEA와의 결합이 AES와의 결합보다 처리 성능에 있어서 앞서 언급한 Table 3의 1.5~2배[6]까지 빠르지 않은 이유는, 본 구현에서는 암호화 처리뿐만 아니라 송수신 시간이 함께 포함되기 때문이다. 두 번째, UAV 카메라에서 실시간으로 영상을 단위시간 동안 촬영하여 LTE 통신망을 거쳐 GCS 노트북 컴퓨터로 스트림 방식으로 데이터의 전송량을 측정하였다. Table 5와 Fig. 10에서와 같이 ④ 비암호화 ⑤ 암호화의 경우로 측정하였다. 그 결과, 본 데이터 전송량은 본 제한 방식이 비암호화의 경우 보다 약간 작음(분당 0.20MB 차이)을 알 수 있다. 세 번째, 움직이는 한 물체를 두 대의 UAV에서 동시에 촬영하여 실시간으로 하나의 UAV는 ⑤ 비암호화, 또 다른 UAV는 ⑥ 암호화하여 LTE 통신망을 통하여 GCS에 각각 전송한다. 이때 GCS에서 2가지 실시간 영상(비암호화 영상과 암호화·복호화 영상)을 2개의 모니터에 각각 나타나는 영상을 시각적으로 비교하였다. Fig. 11은 좌에서 우로 움직이는 물체의 암호화 여부에 따른 비교 영상으로, 원본(좌측)과 복호화 영상(우측)을 GCS에서 나타낸 것으로 시각적 차이는 매우 미세하다.

Table 4. Speed of Crypto-processing Time

Input file size (MPEG)	① No enc./dec. (second)	② Total = ECC+AES-128 (second) [Overhead (%)]	③ Total = ECC+LEA-128 (second) [Overhead (%)]
1.5MB	0.111	0.176 [58.558]	0.146 [31.531]
15MB	0.779	1.308 [67.907]	1.135 [45.699]
150MB	7.908	13.419 [69.688]	11.569 [46.294]
1.5GB	66.791	116.196 [73.969]	97.379 [45.796]
Average		67.53 %	42.33 %

† Total(sec) = enc(sec) + dec(sec)

† Overhead(%) = [(total − ①) / ①] × 100

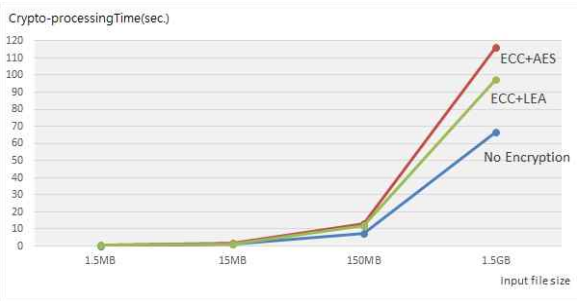

Fig. 9. Speed of Crypto-processing Time

Table 5. Throughput of Video Data Transfer

Duration (minute)	④ No encryption (Mega byte)	⑤ ECC+LEA-128 (Mega byte)
2 min.	28.1	27.9
4 min.	56.7	56.3
6 min.	84.1	83.8
8 min.	112.7	112.2
10 min.	144.7	140.2
Average (per min.)	14.21	14.01

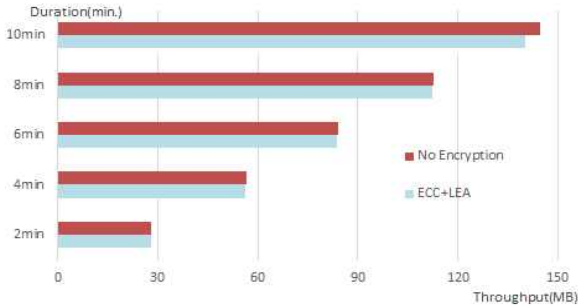

Fig. 10. Throughput of Video Data Transfer

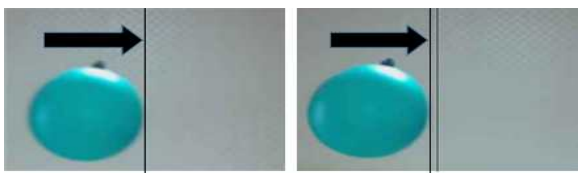

Fig. 11. Two Monitor Displays of a Moving Object

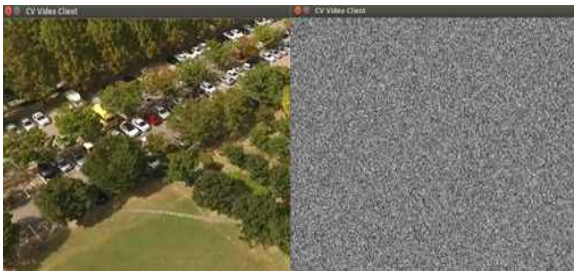

Fig. 12. Video Displays on GCS (Before & After Enc.)

Fig. 13. Swarm UAVs (Agricultural crop-dusting UAVs)

Figure 12는 UAV에서 촬영한 하나의 원본 영상(좌측)과 암호화 영상(우측)이며, Fig. 13은 군집 UAV(농약살포용 UAV 8대)의 모습을 보여준다.

Ⅵ. 결 론

최근의 UAV는 근거리 주파수 통신 방식으로 비행제어 거리가 수 킬로미터로 제한되고, 실시간 영상 전송에 따른 영상 유출 등의 보안 문제가 발생한다. 따라서 LTE 망 환경에서 실시간 군집 UAV를 구성하여 그 운용과 효율을 개선하는 추세이나, 공중망의 사용과 다수의 UAV와 다목적의 활용으로 보안 문제가 더 심각하게 된다. 따라서 본 논문에서는 이러한 환경에서 실시간 시스템에 적합한 빠른 공개키 암호방식인 ECC와 고속의 표준 대칭키 암호방식인 LEA를 결합한 하이브리드 암호시스템 방식으로 군집 UAV 환경에서 영상 암호화시스템을 설계하고 구현하였다. 그 결과로써 본 시스템이 UAV의 실시간 운용에 문제가 없이 낮은 암호화 처리 오버헤드로 그 효율성이 높음을 보였다. 또한 본 논문에서 설계한 하이브리드 암호화시스템은 향후 많은 대수(현재 MAVLink 프로토콜에서는 255대의 UAV까지 운용이 가능함)의 UAV로 군집 UAV 환경을 확대 구성하는 경우에도 본 하이브리드 방식의 적용으로 키 생성, 키 분배, 키 검증 등의 키 관리가 용이하며, 고속 암호화가 가능하여 확장성 측면에서도 중요한 장점을 갖는다.

향후 과제로서는 현재 UAS에서 널리 사용되고 있는 MAVLink 프로토콜의 낮은 보안성을 강화하기 위한 “Secure MAVLink” 연구가 필요할 것이다. 이러한 연구 과제도 본 논문에서 설계한 하이브리드 암호화 방식을 기반으로 한다면 더욱 효율적일 것이다.

References

1) Kim, H., and Steup, C., “The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment,” *Proc. of 5th International Conference on Cyber Conflict*, 2013.

2) Kim, A., Wampler, B., Goppert, J., and Hwang, I. S., “Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles,” *Proc. of AIAA2012*, June 2012.

3) SkySoftware, SkyGrabber, https://www.skygrabber.com, Feb. 2018.

4) Jeon, H. S., “Wireless Communication Technology Developement Trend of Drone,” *Weekly Technology Trend of ETRI*, 2017, pp.2~11.

5) MAVLink Micro Air Vehicle Communication Protocol, http://qgroundcontrol.com, Feb. 2018.

6) Hong, D. J. et al., “LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors,” *Proc. of WISA 2013, LNCS*, vol. 8269, 2014. https://seed.kisa.or.kt/iwt/ko/sup/EgovLeaInfo.do

7) Lin, X. et al., “The Sky Is Not the Limit: LTE for Unmanned Aerial Vehicles,” Ericsson, 2017.

8) Qualcomm Technologies, “LTE Unmanned Aircraft Systems, Trial Report v1.0.1,” Qualcomm Technologies, Inc., May 2017.

9) Weng, L., Liu, Q., Xia, M., and Song, Y. D., “Immune network-based swarm intelligence and its application to unmanned aerial vehicle (UAV) swarm coordination,” *Neurocomputing*, No. 0, 2013.

10) ODROID, ODROID-XU4, http://www.hardkernel. com/ main/products/prdt_info.php

11) Pixhawk2 Autopilot, https://pixhawk.org/modules/pixhawk2#further_info

12) Kumar, A. et al., “Symantec White Paper: Elliptic Curve Cryptography (ECC) Certificates Performance Analysis,” May 2013.

13) Käsper, E., “Fast Elliptic Curve Cryptography in OpenSSL,” *International Conference on Financial Cryptography and Data Security, Springer LNCS 7126*, 2011.

14) Joppe, W. et al., “Elliptic Curve Cryptography,” *Practice Conference on Financial*, Springer, 2014.

15) Mahto, D., and Yadav, D. K., “RSA and ECC: A Comparative Analysis,” *International Journal of Applied Engineering Research ISSN 0973-4562*, Vol. 12, No. 19, Research India Publications, 2017, pp.9053~9061.

16) Korea TTA, *128-bit Block Cipher LEA and its Modes of Operation*, 2014.

17) Perazzo, P., “Security in Networked Computer Systems OpenSSL Lab Session,” Apr. 2015.

18) Brumley, B. B., “Faster software for fast endomorphisms,” *Proceeding COSADE 2015 Revised Selected Papers of the 6th International Workshop on Constructive Side-Channel Analysis and Secure Design*, Vol. 9064, Apr. 2015.

19) Rivera, E., Baykov, R., and Gu, G., “A Study On Unmanned Vehicles and Cyber Security,” 2014.

20) Boettcher, C. et al., “The MILS Component Integration Approach to Secure Information Sharing,” *the 27th IEEE/AIAA Digital Avionics Systems Conference(DASC)*, October, 2008.

21) Openssl, How to Integrate a Symmetric Cipher, https://wiki.openssl.org/index.php/How_to_Integrate_a_Symmetric_Cipher

22) NSR(National Security Research Institute), *Source Code manual of Block Cypher LEA*, ver 1.0, October, 2015.