Journal of Korea Multimedia Society Vol. 21, No. 8, August 2018(pp. 897-908)
https://doi.org/10.9717/kmms.2018.21.8.897

군집 드론망을 통한 IoT 서비스를 위한 보안 프레임워크 연구

신민정†, 김성운††

A Study on the Security Framework in IoT Services for Unmanned Aerial Vehicle Networks

Minjeong Shin†, Sungun Kim††

ABSTRACT

In this paper, we propose a security framework for a cluster drones network using the MAVLink (Micro Air Vehicle Link) application protocol based on FANET (Flying Ad-hoc Network), which is composed of ad-hoc networks with multiple drones for IoT services such as remote sensing or disaster monitoring. Here, the drones belonging to the cluster construct a FANET network acting as WTRP (Wireless Token Ring Protocol) MAC protocol. Under this network environment, we propose an efficient algorithm applying the Lightweight Encryption Algorithm (LEA) to the CTR (Counter) operation mode of WPA2 (WiFi Protected Access 2) to encrypt the transmitted data through the MAVLink application. And we study how to apply LEA based on CBC (Cipher Block Chaining) operation mode used in WPA2 for message security tag generation. In addition, a modified Diffie-Hellman key exchange method is approached to generate a new key used for encryption and security tag generation. The proposed method and similar methods are compared and analyzed in terms of efficiency.

Key words: GCS (Ground Control Station), Unmanned Aerial Vehicle (UAV), Flying Ad-hoc Network (FANET), Micro Air Vehicle Link (MAVLink), Diffie-Hellman Key Exchange, Lightweight Encryption Algorithm (LEA), Encryption/Decryption, Security Tag

1. 서 론

무인항공기(UAV: Unmanned Aerial Vehicle)는 원격으로 조정이 가능하여 여러 가지 응용 즉, 군사, 지역 감시, 산불 진화, 풍향 예측, 재난 모니터링, 원격 센싱, 트래픽 모니터링, 애드혹 네트워크의 릴레이 역할 등 다양한 응용에 적용되고 있다[1]. 일반적으로 단일 무인항공기 사용으로 응용에 활용되어 왔지만, 소 용량의 무인항공기들이 그룹으로 공동 작업에 임하면 더욱 다양한 IoT(Internet of Things) 서비스를 구현할 수 있어 비용이나 응용 측면에서 융통성을 가진다[2].

단일 무인항공기 응용의 예로 대표적인 무인 항공기인 드론을 인터넷을 통해 원격 활용하기 위해 지상제어장치(GCS: Ground Control Station)와 UAV간의 데이터 송수신을 UDP/IP 기반의 MAVLink

※ Corresponding Author : Sungun Kim, Address: (48513) Yongso-ro 45, Nam-gu, Busan, Korea, TEL : +82-51-629-6235, FAX : +82-51-629-6229, E-mail : kimsu@pknu.ac.kr
Receipt date : Jul. 3, 2018, Approval date : Jul. 12, 2018

† Master's degree, Dept. of Information & Communication Eng., Graduate School, Pukyong National University (E-mail : minjung3373@pukyong.ac.kr)
†† Professor, Dept. of Information & Communication Eng., Pukyong National University
※ This research work was supported by the Research Grant of Pukyong National University(C-D-2017-1214).

(Micro Air Vehicle Link) 응용 프로토콜을 사용하는 방법이 소개되었다[3]. 그리고 데이터 전송 과정에서 정보 보호를 위해 AES(Advanced Encryption Standard) 기반의 암호화 기술도 연구 되었다[4].

한편으로 군집된 형태의 UAV들로 망을 구성한 예에서는 군집에 속한 개별 UAV들의 이동성과 토폴로지 변화 등에 대처하는 망 기술이 요구된다. 또한 서비스 과정에서 전달되는 데이터의 안전성을 보장하기 위해 효율적이면서 강화된 보안 방법이 필요하다[4]. 본 논문에서는 원격 센싱 또는 재난 모니터링 등의 IoT 서비스를 제공하기 위해 다수의 드론이 애드혹 네트워크(Ad-hoc network)로 구성된 FANET (Flying Ad-hoc Network)에 기반하고 MAVLink 응용 프로토콜을 사용하는 군집 드론 망의 보안 프레임워크에 대해 연구한다.

먼저 군집에 속한 드론들이 링 형태의 토폴로지로 토큰을 활용하여 동작하는 무선 토큰링(WTRP: Wireless Token Ring Protocol) 개념을 적용하여 FANET 망을 구성한다. 이는 토폴로지 변화가 심한 군집 환경에서 상대적으로 쉽게 망을 구성할 수 있고 또한 잦은 통신 오류 등에 장점이 있기 때문이다. 그리고 링으로 구성된 FANET 망에 대표드론을 두고 이를 통하여 지상제어장치와 통신을 수행한다. 여기서 대표드론을 통한 지상제어장치와 군집 드론들 간의 통신은 다양한 무선구간을 거치게 되어 응용에 따른 전달 데이터의 보호 및 보안에 세심한 주의가 요구된다[4].

본 논문에서는 MAVLink 응용 프로토콜에 기반하고 전송되는 데이터들의 암호화를 위해 WPA2(WiFi Protected Access 2)의 CTR(Counter) 운용모드에 경량 암호 알고리즘(LEA: Lightweight Encryption Algorithm)을 적용한 효율적인 알고리즘을 제안한다. 그리고 메시지 보안 태그 생성을 위해 WPA2에서 사용하는 CBC(Cipher Block Chaining)모드에 기반하고 LEA를 적용한 방법에 대해 연구한다. 또한 암호화 및 보안 태그 생성 과정에서 새로운 키 생성을 위해 RADIUS(Remote Authentication Dial In User Service) 서버와 같은 인증 서버를 사용하지 않고, 디피-헬만 키 교환(Diffie-Hellman Key Exchange) 방법을 적용하여 자체적으로 키 생성 및 분배 방법을 제안한다[5].

본 논문의 2장에서는 군집 드론 통신망 구성에 관계된 효율적인 망 프레임워크를 제시한다. 3장에서는 관련 연구에 대한 분석을 통해 새로운 보안 프레임워크의 필요성을 기술한다. 4장에서는 제안한 군집 드론 망에서의 보안 프레임워크를 상세히 설명하며, 5장에서는 제안된 방법과 유사 방법들을 효율성 측면에서 비교 분석한다. 마지막으로 6장에서는 제안된 프레임워크의 현장 적용 및 확장 방안으로 결론을 맺는다.

2. 드론 망 관련 연구

드론으로 구성된 망의 효율적 제어를 위해서는 지상제어장치와 드론간의 통신망 구조와 군집드론 간의 망인 FANET의 구성 방식의 두 가지 측면이 중요하다. 본 장에서는 이것들을 분석한 후 이를 바탕으로 군집 드론들을 위한 효율적인 망 프레임워크를 제시한다.

2.1 지상제어장치와 드론간의 통신망 구조

Fig. 1은 드론을 활용한 IoT 서비스를 위한 통신망 구조이다. Fig. 1-(a)는 일반적으로 사용되어온 하나의 UAV를 활용하는 구조로 서비스 범위가 한정되어 응용측면에서 효율성 및 신뢰성이 떨어진다[2].

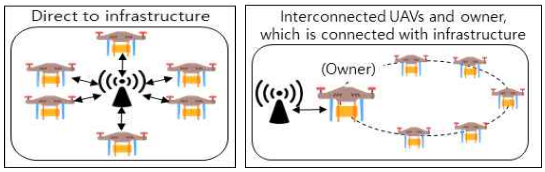
반면에 Fig. 1-(b)와 같이 FANET 형태로 군집 드론 통신망을 구성하면, 다양한 IoT 응용을 위해 멀티 홉(Multi-hop) 통신 및 분산처리 등의 장점으로 서비스 범위의 확장과 작업 시간 단축, 그리고 높은 효율성 및 신뢰성을 기대할 수 있다[2].

2.2 FANET 구조

Fig. 1-(b)에서 제시된 FANET 구현에 있어 일반적으로 두 가지 방법으로 애드혹 네트워크를 구성한다[2]. 먼저 Fig. 2-(a)는 지상 통신 인프라인 지상제어장치와 군집으로 활용되는 드론들이 서로 상호 연동성이 없이 직접 통신하는 방법이다. 즉 드론 간의

(a) (b)

Fig. 1. UAV network architectures for IoT services. (a) Single architecture, (b) Multiple architecture.



(a) (b)

Fig. 2. FANET network configurations. (a) Non-interconnected, (b) Interconnected.

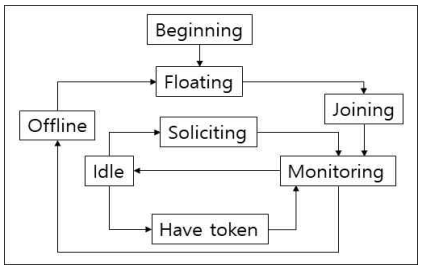


Fig. 3. Finite state machine for WTRP.

통신을 위해서도 항상 지상제어장치를 거쳐야하므로 각 UAV는 상대적으로 고용량의 통신 H/W가 필요해 비행 허용고도 및 이동범위가 한정될 수 있다.

반면에 Fig. 2-(b)와 같이 다수의 드론 중 한 대가 지상제어장치와 연결되고 나머지 드론들은 상호 애드혹 네트워크 형태로 연동되는 방법이 있다. 이 경우 지상제어장치와 통신하는 FANET의 대표 드론(UAV(Owner))을 제외한 드론들은 상대적으로 저용량의 통신 H/W를 활용하여 고도 및 이동 범위의 확장이 가능하다. 즉 통신 공간 확대와 유연한 망 구축, 상호 드론 간의 미션 협력 및 분산 수행 등의 효율성을 가지므로 군사, 지역 감시, 산불 진화, 풍향 예측, 재난 모니터링, 원격 센싱, 트래픽 모니터링, 애드혹 네트워크의 릴레이 등 다양한 응용에 활용이 가능하다[2].

FANET 구성을 위해 기존의 IEEE 802.11(CSMA/CA)에 기반한 MAC 프로토콜의 사용은 강한 이동성과 토폴로지의 빈번한 변화 등의 대처에 문제가 있다[6]. 반면에 WTRP의 적용은 숨은 단말기 문제 해결 및 고 네트워크 부하에도 안정된 성능으로 통신 지연과 에러율 및 전송률 측면에서 효율적이다[6].

Fig. 2-(b)에서 FANET의 대표 드론은 지상제어장치와 직접 무선통신하며 링으로 구성된 FANET에 소속된 드론들에게 데이터를 전달하거나 센싱 데이터를 받아 지상제어장치로 전송하는 중계역할을 한다. 일반적으로 WTRP 형태의 링으로 동작하는 군집 드론으로 구성된 FANET의 동작은 Fig. 3과 같이 총 8가지 상태, 즉 시작(Beginning), 합류대기(Floating), 탈퇴(Offline), 휴지(Idle), 초대(Soliciting), 참여(Joining), 토큰소유(Have token), 모니터링(Monitoring) 상태들로 구성된다.

Fig. 3에서 WTRP 링의 구성을 위해 먼저 대표 드론이 시작 상태를 출발하여 링을 구성하기위해 합류대기상태로 이동한다. 이때 링에 소속된 드론이 없으므로 어느 누구로부터도 초대 프레임(Solicit successor frame)을 받지 못하므로 참여상태를 건너뛰고 단일 드론 링을 구성한 후 모니터링상태에 머문다. 모니터링 상태에서는 3가지 일들을 수행하는데 첫째 합류대기상태에서 제어 토큰을 기다리다 차례가 되면 데이터가 있는 경우는 전송할 데이터를 전달하고 이 토큰을 후임 드론에게 넘겨주는 과정을 수행한다. 둘째 링으로 합류대기상태에서 새로이 가입을 원하는 드론에게 링에 참여시키는 과정이다. 이 과정에서는 휴지상태로 이동한 후 해당 드론이 가입을 기다리는 드론에게 초대 프레임(Solicit successor frame)을 브로드캐스트 통신으로 전달하고, 이를 수신한 드론은 참여 상태로 이동한 후 그 프레임을 준 드론을 선임 드론으로 설정하기 위해 선임 설정 프레임(Set predecessor frame)을 보낸다. 이에 대한 응답으로 후임 설정 프레임(Set successor frame)을 송신하여 링에 가입시킨 후 모니터링상태로 이동한다. 셋째 링 탈퇴과정으로 모니터링상태에서 현재 드론의 후임드론을 선임 드론의 후임으로 정하고 그리고 현재 드론의 선임드론이 이에 대해 응답하여 링에서 제외되는 과정이다. Fig. 5는 위에서 설명된 내용에 기초해 군집 드론으로 구성된 WTRP 링에 합류 및 탈퇴 과정과 데이터 전송에 대한 동작 과정을 도식화

FC 1byte	RA 6byte	DA 6byte	SA 6byte	NON 2byte	GenSeq 4byte	Seq 4byte

(a)

FFMMMPPP 1byte	RA 6byte	DA 6byte	SA 6byte	Data N byte

(b)

Fig. 4. MAC frame structures of WTRP. (a) Control frame structure, (b) Data frame structure.

한 것이다.

WTRP의 MAC 프레임은 제어 프레임과 데이터 프레임으로 구성되며, Fig. 3에서 설명한 동작을 위해 Fig. 4-(a)에서 FC(Frame Control) 필드로 제어 프레임(Token, Claim, Solicit Successor, Set Successor, Set Predecessor, Token Deleted)들을 구분하여 사용한다. 그리고 Fig. 4-(b)는 데이터 전달을 위한 프레임(FF: Data, MMM: 응답 요구 유무, PPP: 우선순위)들로 구성된다. 여기서 RA(Ring Address)는 링 대표 노드의 주소, DA(Destination Address)는 목적지 주소, SA(Source Address)는 송신지 주소, NoN(Number of Nodes)은 링 구성 노드의 수, GenSeq(Generation Sequence Number)는 링을 한 바퀴 순환할 때 마다 증가하는 필드, Seq(Sequence Number)는 매 홉마다 증가하는 필드이다. 자세한 설명은 논문[6]을 참조한다.

2.3 MAVLink 응용 프로토콜

지상제어장치와 UAV가 인터넷을 통해 원격으로 데이터를 송수신하기 위한 양방향 무선 통신으로 동작하는 MAVLink 응용 프로토콜은 UDP/IP 기반에서 동작한다[4]. 응용 프로토콜의 메시지 구조는 Fig. 6과 같이 구성되고 각 필드의 기능은 다음 설명과 같다. 먼저 Stx(Packet Start Sign)는 메시지의 시작을 알리고 Len(Payload Length)은 Msg data(실제 응용 데이터)의 길이이며, Seq(Packet Sequence)는 메시지의 순서번호이다. 그리고 Sys ID(System ID)는 송신 시스템 구분자이며, Comp ID(Component ID)는 송신 시스템 내부 구성 장치에 대한 구분자이다. Msg ID(Message ID)는 메시지 종류를 정의하며, Msg data(Payload)는 실제 응용 데이터이고, CRC(Checksum Code)는 오류검출코드이다.

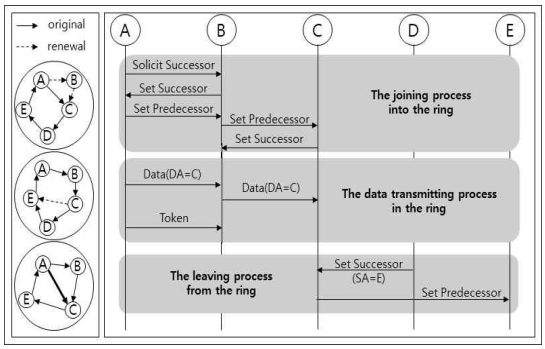


Fig. 5. Procedure of WTRP operations.

Stx (1byte)	Len (1byte)	Seq (1byte)	Sys ID (1byte)	Comp ID (1byte)	Msg ID (1byte)	Msg data (0~255byte)	CRC (2byte)

Fig. 6. The structure of MAVLink message.

이중 Msg ID 필드는 0부터 255까지 총 256가지의 응용이 가능하며, 일부(0~149)는 표준에 의해 미리 정의되고 나머지(150~255)는 필요에 따라 사용자가 정의한다. 대표적인 Msg ID로는 드론의 작동 유무 등 상태 판별을 위한 'Heartbeat' 메시지(Msg ID=0), Ping을 요청하거나 응답하여 대기시간을 측정하는 'Ping' 메시지(Msg ID=4), 그리고 비밀 키를 보내는 'Auth Key' 메시지(Msg ID=7) 등이 있다. Msg data에는 Msg ID가 정의한 메시지 종류에 관계된 데이터가 포함된다. 본 논문에서는 응용 데이터의 안전한 전달을 위해 제안된 보안 메커니즘을 위해 필요한 메시지들을 정의하고 그에 대한 설명은 4.1 소절에서 기술한다.

2.4 제안된 군집 드론 망

Fig. 7은 군집 드론들로 구성된 WTRP 기반의 FANET 망구조에서 인터넷을 통한 IoT 응용 서비스를 위해 본 논문에서 제안하는 FANET 망 구성과 이에 관련된 프로토콜 스택을 도식화한 것이다.

동작에 대한 설명으로, 먼저 지상제어장치와 FANET의 대표 드론은 와이파이(WiFi)로 통신하며, FANET의 WTRP 구성 드론들은 주파수 도약 확산 스펙트럼(FHSS: Frequency Hopping Spread Spectrum) 방식을 사용하는 것으로 가정한다[7]. FHSS 방법은 통신 과정에서 차단 및 통신 장애 등의 간섭에 영향을 덜 받고 도청 등에 대응하는 능력을

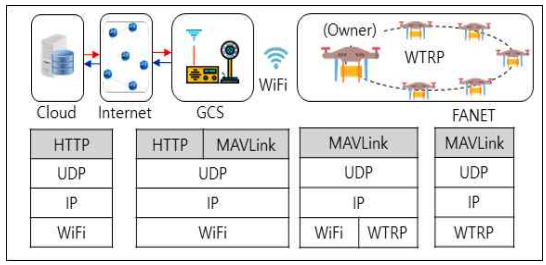


Fig. 7. WTRP-based FANET structure for drone IoT services.

가진다. 다음으로 지상제어장치와 대표 드론 그리고 군집 드론들 간에는 MAVLink 응용 프로토콜로 UDP 기반의 IP 프로토콜로 해당메시지를 전달한다. FANET의 드론들은 응용관련 탐지 데이터들을 MAV Link 메시지 화하여 WTRP MAC 프로토콜로 동작하여 대표 드론에게 전달한다. 이를 성공적으로 수신한 대표 드론은 WiFi 통신으로 지상제어장치에게 전송하여 인터넷을 통한 클라우드 컴퓨팅 기술 등을 활용하여 응용 서비스된다.

3. 관련 연구

본 논문의 저자들은 공장자동화나 생산자동화 환경에서 IoT 장치들과 AP(Access Point)사이 무선구간의 안전한 데이터 전송을 위해 IoT 보안 프레임워크를 제안하였다[8]. 이 방법을 SCM1(보안 검사 메커니즘1: Security Check Mechanism1)이라 명명하고, 보안 태그 생성 및 부착과 암호화를 통해 보안성을 강화하였다. 사용 환경은 사물 인터넷을 위한 사설망으로 서비스의 실시간성과 전송 효율성을 고려하여 AES 기반으로 간략화 된 WPA2 개념을 적용하였다.

또한 논문[4]에서는 지상제어장치와 UAV간의 주고받은 데이터를 인터넷을 통해 원격 활용하기 위한 UDP/IP 기반의 MAVLink 응용 프로토콜의 정보 보호를 위해 AES 기반의 암호화 기술을 제안하였다. 본 장에서는 위에서 언급된 두 가지 선행연구의 문제점 분석을 분석하고 이를 해결하는 보안 프레임워크의 접근 방법을 모색한다.

3.1 기연구된 IoT 보안 프레임워크

Fig. 8은 본 논문의 저자들이 이미 발표한 논문[8]에서 제시한 공장자동화나 생산자동화 환경에서 활용되는 사물 인터넷과 포그 및 클라우드 컴퓨팅 개념이 융합된 망구조이다.

Fig. 8과 같이 많은 IoT 장치들로부터 생성되는

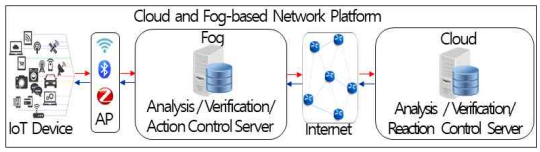


Fig. 8. Network architecture for Cloud and Fog-based M2M IoT services.

엄청난 양의 짧은 길이의 데이터들의 무선 LAN을 통한 전송 과정에서 WPA2 방법을 적용하는 것은 효율성에 문제가 있다. 그래서 시간과 효율성을 고려하여 간략화 된 WPA2 개념을 적용한 방법으로 Fig. 9와 같은 SCM1 보안 프레임을 제안하였다[8].

SCM1은 Fig. 9와 같이 보낼 프레임에 보안 태그를 생성하여 부착한 후 데이터와 보안 태그 필드를 암호화하여 데이터의 무결성 및 기밀성을 보장하는 방법이다. 먼저 키 생성을 위해, 데이터를 전송하는 날짜와 시간을 활용하여 4 바이트(첫 번째 바이트: 해당 월의 2진화된 값, 두 번째 바이트: 해당 일의 2진화된 값, 세 번째 바이트: 해당 시의 2진화된 값, 네 번째 바이트: 해당 분의 2진화된 값)를 얻은 후, 이것을 활용하여 간략화 된 AES의 S-box(Substitution-box) 치환 및 Rcon(Round constant) 연산 과정을 거쳐 키를 생성한다.

SCM1에 의한 보안 태그 생성 과정(Fig. 10-(a))은 송신할 데이터를 4 바이트 배수로 구성하여 생성된 키와 XOR 연산을 통해 OUT을 생성 한 후, 이것을 마지막 데이터 블록까지 XOR 연산하여 최종 결과로 4 바이트 블록을 생성한다. 여기서 송신 데이터가 4 바이트의 배수가 되지 않으면 모든 값이 0인 빈 바이트로 채워서 위의 계산을 수행한다.

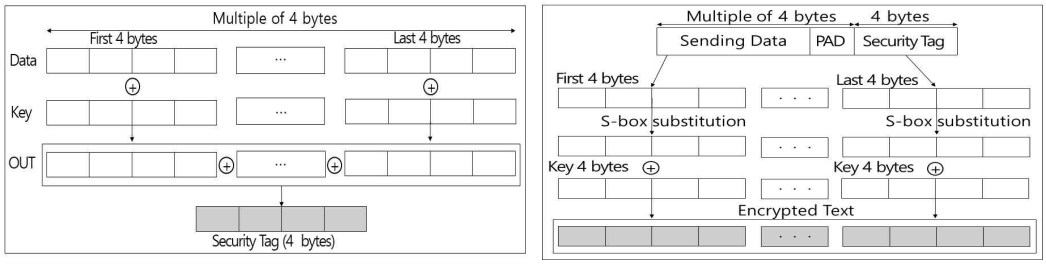
암호화 과정(Fig. 10-(b))은 Fig. 9와 같이 완성된 암호화 대상 필드를 4 바이트로 분리한 후 각각 S-box로 치환하고, 키와 XOR 연산하여 그 결과를 암호문으로 사용한다. 그러나 다양한 무선 환경과 여러 가지 형태의 포그 및 클라우드 컴퓨팅 기술들이 적용되는 환경에서 보안성 강화를 위해 키 교체 및 전달과 보안 태그 생성 및 암호화 방법의 효율성에 대해서는 다소 문제가 있다. 따라서 본 논문에서는 이러한 문제점을 개선하는 LEA 및 디피-헬만 키 교환 방법을 활용하여 새로운 보안 프레임워크를 제안한다.

3.2 기 연구된 MAVLink 관련 보안 프레임워크

MAVLink 프로토콜 보안 방법으로 WPA2의 CTR 운용모드에 AES 알고리즘을 적용하여 암호화하고,

Frame Control	Duration ID	Addr1	Addr2	Addr3	Sequence Control	Addr4	Data	Security Tag	FCS
2 byte	2 byte	6 byte	6 byte	6 byte	2 byte	6 byte	N byte	4 byte	4 byte
802.11 MAC Frame							Encryption		

Fig. 9. SCM1 frame structure.

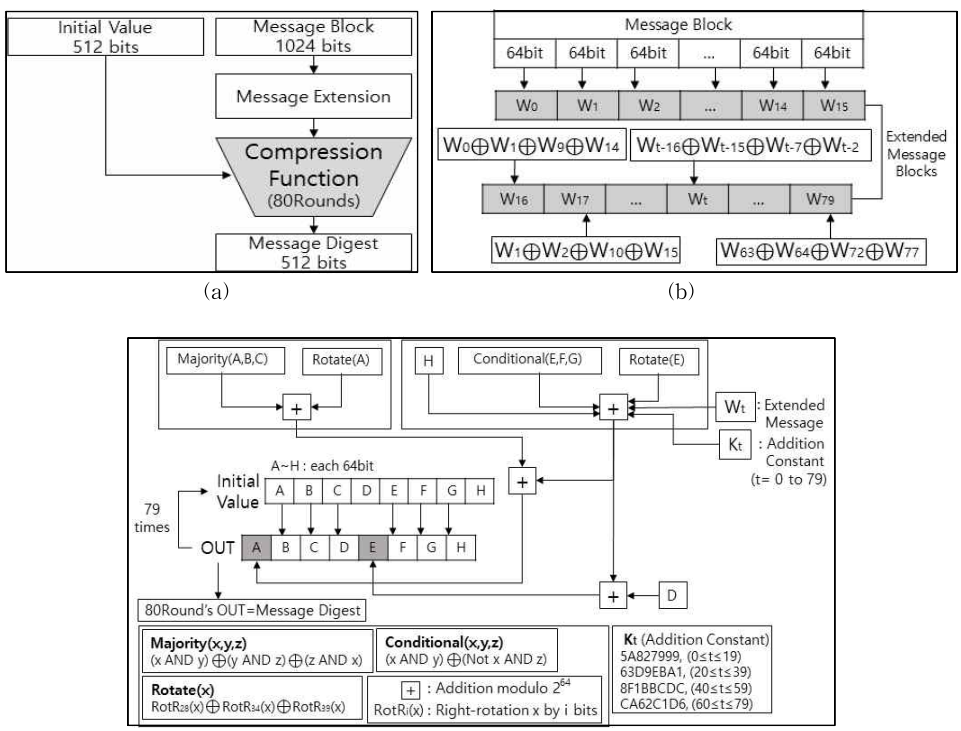


(a) (b)

Fig. 10. Security mechanism of SCM1. (a) Security tag generation method, (b) Encryption method.

메시지 무결성 검정을 위해 SHA-512(Secure Hash Algorithm) 해시함수를 적용한 방법이 소개되었다[4]. 이 방법은 AES 알고리즘으로 카운터 블록을 암호화한 값과 데이터를 XOR연산하여 암호화하여 보안성을 향상시키며 역과정인 복호화는 암호문을 그대로 사용하여 수행하는 방법이다.

그리고 보안 태그 생성을 위해 SHA-512 해시 함수를 사용하는데, Fig. 11은 전체 과정과 메시지 확장(Message Extension) 및 80 라운드로 구성된 압축 함수(Compression Function)의 한 라운드를 도식화한 것이다. 메시지 확장 방법(Fig. 11-(b))은 입력된 메시지 블록(Message Block)을 SHA-512에 적용하기에 알맞은 형태로 확장하는 과정으로, 64비트의 블록(Wt)을 총 80개 생성한다. 압축 함수(Fig. 11-(c))는 각 라운드마다 확장된 메시지 블록(Wt)과 초기 값(Initial Value, A~H) 및 덧셈 상수(Kt)로 512 비트의 결과(OUT)를 생성한다. 여기서 압축 함수에 사용되는 덧셈 상수 및 1라운드에 적용되는 초기 값은 SHA-512에서 정해진 값이다. 각 라운드의 결과는 다음 라운드의 초기 값으로 사용되며, 마지막 80라운



(c)

Fig. 11. Procedure of SHA-512. (a) Total configuration, (b) Message extension method, and (c) Compression function.

드의 결과는 보안 태그(Message Digest)로 활용된다.

3.3 제안된 망에 연구된 보안 프레임워크를 적용함에 있어 문제점

Fig. 7과 같은 군집 드론 망에서는 응용에 따라 많은 양의 데이터를 실시간적으로 전송하는 환경으로 효율성 보장이 필수적이다. 앞에서 기술한 SCM1 및 MAVLink 관련 보안 프레임워크를 적용할 때 다음과 같은 비효율성이 고려된다.

먼저 3.1절에 기술한 SCM1 방법은 WPA2의 복잡성을 간소화시켜 시간적으로는 효율성이 있지만 보안성과 실용성 측면에서 문제가 있다. 키 생성 방법은 시간 정보의 활용으로 송수신자간의 동기 및 오차에 문제가 있고, 암호화와 보안 태그 생성 방법은 간략한 연산으로 인해 보안성이 떨어진다. 이를 개선하기 위해 암호화를 위해서 LEA와 자동 키 생성 및 교환은 디피-헬만 키 교환 방법 혹은 Merkle-Damgard 방법 등을 적용할 수 있다[5,9,10]. 그러나 Merkle-Damgard 방법은 해시 함수이므로 위조에 대처할 수 없으므로 LEA와 디피-헬만 키 교환 방법을 적용한 보안 프레임워크를 제안한다.

그리고 3.2절의 MAVLink 관련 보안 프레임워크에서는 암호화를 위해 AES 방법을 적용하였다. 이 방법은 S-box 치환과 열 혼합 등 복잡한 연산 과정을 10회 수행함으로써 보안성과 실용성은 뛰어나지만 실시간 데이터 전송 환경에서는 효율성이 떨어진다. 본 연구에서 제시한 Fig. 7과 같은 망 응용에서는 많은 양의 데이터를 주고받기 때문에 간단하며 효율적인 보안 방법이 필요하다. 또한 보안 태그 생성을 위한 SHA-512 방법은 큰 블록을 대상으로 하므로 본 연구에 적용하기에는 실용성이 떨어지고 위조에 대한 대응에 한계가 있다.

4. 보안 프레임워크 제안

본 장에서는 MAVlink 응용 프로토콜로 전송되는 데이터들의 암호화와 보안 태그 생성 및 검정을 위해 각각 WPA2의 CTR과 CBC 운용모드를 활용하고 LEA를 적용한 방법을 제안한다. 그리고 암호화 및 보안 태그 생성 과정에서 새로운 키 생성을 위해 인증 서버를 사용하지 않고 디피-헬만 키 교환 방법을 적용하여 자체적으로 키 생성 및 분배하는 방법을 제안한다.

4.1 MAVLink 응용 프로토콜 보안 프레임워크

Fig. 12는 지상제어장치와 대표 드론이 키를 생성하여 FANET의 모든 드론으로 순차적으로 키를 전달하는 과정으로, 주고받는 메시지에 대하여 암호화 및 보안 태그로 보안성을 보장한다. 본 논문의 4.2절에서는 키 생성 방법을 설명하고 4.3절에서는 암호화 및 보안 태그 생성 방법을 제시한다.

Fig. 12에서는 MAVLink 메시지 4개(7번: 비밀 키 상수 및 키 전송, 200번: 재전송 요청, 201번: 키 생성 명령/응답, 202: 키 분배 응답, 키 분배 완료 알림/응답)를 정의하여 키 생성 및 분배 과정에 적용하며, 메시지의 중요성에 따라 보안 태그만 활용하거나 암호화도 같이 적용하는 방법으로 구현된다. FANET에 속한 모든 드론들은 WTRP의 MAC동작으로 키를 분배한다.

비밀 키 생성과 분배가 완료되면 Fig. 13과 같이 다양한 응용 데이터를 포함한 메시지를 주고받는다. 이 과정에서 MAVLink 메시지 2개(204번: 지상제어장치에서 FANET의 대표 드론을 통한 모든 드론으로 메시지 전송, 205번: 지상제어장치에서 FANET의 대표 드론을 통한 특정 드론으로 메시지 전송 혹은 반대 경우)를 정의하고 이를 활용하여 안전한 메시지 전송 과정을 수행한다. 이때 해당 메시지들에 대하여 암호화와 보안 태그 적용으로 보안성을 유지한다.

지상제어장치에서 FANET의 모든 드론으로 데이

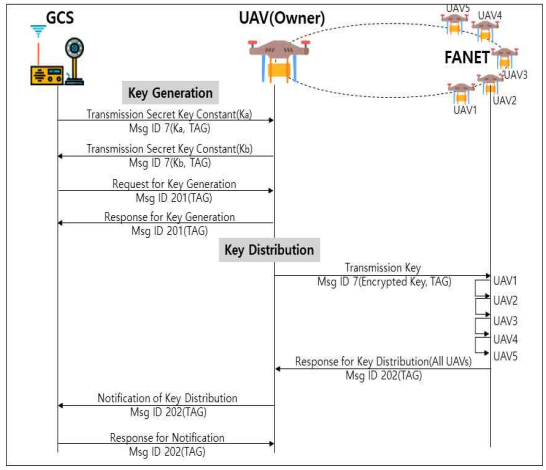


Fig. 12. Procedure for key generation and distribution.

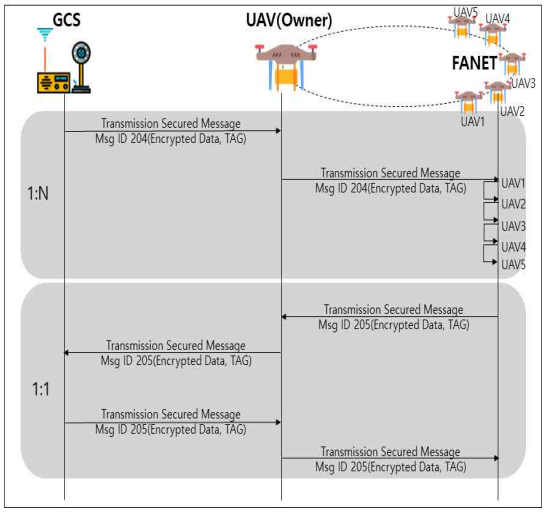


Fig. 13. Procedure for data transmission between GCS and FANET.

터를 순차적으로 전달하는 1:N 통신은 WTRP 토큰링 MAC동작으로 수행된다. 그리고 메시지 전달과정에서 보안성이 위배될 경우는 메시지 200번을 사용하여 재전송과정을 거친다.

4.2 키 생성

본 논문에서는 키 생성을 위해 디피-헬만 키 교환 방법을 활용하였다. 즉 지상제어장치와 대표 드론은 두 가지의 상수(x: 공유 비밀 상수(밑), y: 공유 비밀 상수(모듈러스))를 공유하고 각자의 개인 비밀 상수(a: 지상제어장치의 개인 비밀 상수, b: 대표 드론의 개인 비밀 상수)를 선택해 식(1)을 통해 계산된 비밀키 상수(K_a:지상제어장치의 비밀 키 상수, K_b: 대표 드론의 비밀 키 상수)를 보안 태그를 활용하여 안전한 교환을 달성한다.

$$K_a = x^a \% y, \quad K_b = x^b \% y \tag{1}$$

안전한 비밀 키 상수의 교환 후 식(2)에 따라 키의 첫 번째 바이트를 생성한다. 이 과정에서 지상제어장치와 대표 드론은 서로 다른 개인 비밀 상수(a 혹은 b)를 사용하지만 이산 대수의 원리로 동일한 값이 생성된다[5].

$$\text{Key} = K_b^a \% y\,(GCS) = K_a^b \% y(\text{UAV(Owner)}) \tag{2}$$

위에서 생성된 첫 바이트와 비밀 상수를 활용하여 16 바이트의 비밀 키를 완성한다. 키를 재생성할 경우에는 현재의 키로 새로운 공유 비밀 상수 x와 y를 만든 후 위의 과정을 반복한다. 이렇게 주기적으로 새롭게 생성된 키는 암호화 및 보안 태그 생성에 사용된다.

4.3 암호화 및 보안 태그 생성

암호화 방법은 WPA2의 CTR 운용모드에 LEA를 적용하고 또한 보안 태그 생성은 WPA2의 CBC 운용모드에 LEA를 활용하여 제안된다. Fig. 14는 MAV Link 메시지에 보안 방법을 적용한 구조이다.

LEA는 암호화를 위한 모든 라운드가 ARX(Addition, Rotation, XOR) 연산으로만 구성되어 DES(Data Encryption Standard) 또는 AES에 비해 연산 과정이 간단하여 훨씬 효율적이다[9]. LEA의 암호화 과정은 Fig. 15와 같다. 상세한 설명은 논문[9]를 참조한다.

라운드 키 생성(Fig. 15-(a))은 4.2절에서 생성된 비밀 키를 입력하여 암호화를 위한 라운드 키(총 24 라운드)를 생성한다. 이렇게 생성된 라운드 키를 활용하여 암호화(Fig. 15-(b)) 과정이 수행된다.

그리고 암호화 방법으로서 LEA를 CTR 운용모드로 활용한 Fig. 16-(a) 방법을 제안한다. 본 논문에서 제안하는 방법은 기존 CTR 운용모드에서 이용하는 카운터(Counter) 블록을 대신하여 비밀 값(SV: Secret Value)을 적용한다. SV는 WPA2의 CTR 및 CBC 운용모드 적용에 필요한 값으로 매번 새로운 키를 생성할 때 마다 정하여 안전하게 교환한다.

보안 태그 생성(Fig. 16-(b))은 SV와 입력 블록(암호문) 및 키를 적용하여 생성된 결과를 전송 대상 데이터의 길이에 따라 필요한 바이트만큼 취하여 메시지의 무결성을 검정한다.

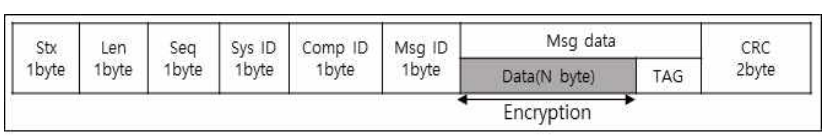


Fig. 14. Structure of secured MAVLink message.

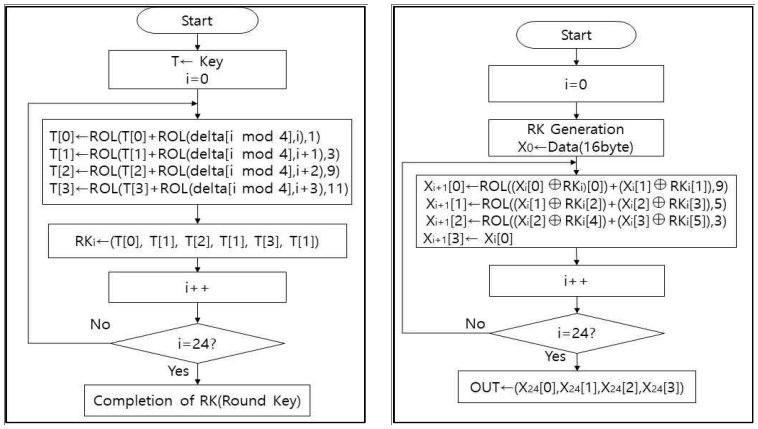


Fig. 15. Flow chart of LEA process. (a) Round key generation, (b) Encryption.

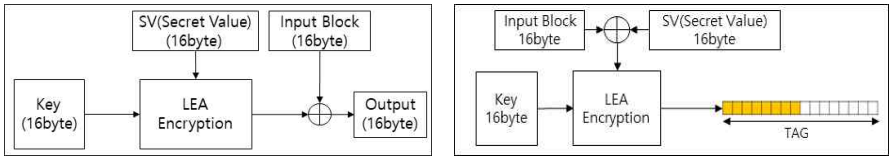


Fig. 16. Proposed security mechanism based on LEA. (a) Encryption(CTR-based), (b) Security tag generation(CBC-based).

5. 타방법과의 비교분석

효율성 분석을 위해 본 논문에서 제시한 방법과 3.1절에 기술한 SCM1 방법 및 3.2절에 기술한 MAV Link 방법의 암호화 및 보안 태그 생성 과정에서 소요되는 계산 유닛의 정의와 이를 비교한다.

먼저 효율성 비교에 사용되는 세 가지 계산유닛(t_0, t_1, t_2)을 정의한다. 먼저 t_0는 XOR 혹은 AND 또는 바이트 곱 등 한 바이트 연산에 대한 유닛이다. 연산 속도가 빠른 시프트 연산에 대한 계산 유닛 $t_1 = 0.1t_0$로 정의한다. 그리고 다른 연산에 비해 복잡한 과정을 거치는 계산 유닛인 S-box 치환은 한 바이트 당 $t_2 = 5t_0$으로 가정한다. 참고로 각 계산 유닛의 정확한 처리 시간에 대한 접근보다는 처리 유닛에 대한 상대적인 비교로 접근한다[9].

먼저 AES 방법은 각 라운드가 16 바이트의 S-box치환($16t_2$)과 행 이동($3t_1$) 그리고 16바이트의 열 혼합($16(4t_0+3t_0)$) 과정과 16바이트의 Rcon과의 XOR 연산($16t_0$)등으로 총 10라운드로 구성된다. 마지막 10라운드에서는 열 혼합과정이 생략되므로 아래 식 (3)과 같이 계산된다.

LEA 방법(Fig. 16-(b))은 16바이트의 암호화 대상 데이터를 4바이트 크기의 네 블록으로 나누어 세 블록을 대상으로 라운드 키와 XOR 연산 2번($2\times4t_0$) 및 그 결과의 4바이트 ADD연산($4t_0$)과 시프트 연산(t_1)을 총 24 라운드 반복 수행하므로 그 결과는 식 (4)로 정리된다.

$$\text{AES} = 10\times(16t_2+3t_1+16\times(4t_0+3t_0)+16t_0)-16\times(4t_0+3t_0) = 1971t_0 \quad (3)$$

$$\text{LEA}=24\times(3\times(8t_0+4t_0+t_1))=871.2t_0 \quad (4)$$

그리고 WPA2의 CTR 모드로 암호화하므로 AES와 LEA에 대한 계산 유닛(식(3)과 식(4))에 16 바이트의 XOR 연산에 해당하는 계산 유닛을($16t_0$)을 더하고 암호화 대상 블록의 크기(L)를 고려한 블록 수(L/16)를 곱하면 식(5)와 식(6)으로 정리된다.

한편 SCM1의 암호화 방법(Fig. 10-(b))은 4바이트의 S-box치환($4t_2$)과 4바이트의 XOR연산($4t_0$)을 수행한다. 그리고 LEA와 동등한 조건에서 비교하기 위하여 라운드마다 4 바이트 크기의 네 블록에 대하

여 수행(총 16바이트)하는 것으로 계산되고 결과적으로 총 24라운드 반복 수행되므로 4와 24를 곱한 후 블록 수(L/16)를 곱하면 식(7)과 같이 정리된다.

$$\text{AES(CTR Mode)}=(\text{AES}+16t_0)\times(L/16)=1987t_0\times(L/16) \quad (5)$$

$$\text{LEA(CTR Mode)}=(\text{LEA}+16t_0)\times(L/16)=887.2t_0\times(L/16) \quad (6)$$

$$\text{SCM1(Enc and Dec)}=(4t_2+4t_0)\times4\times24\times(L/16)=2304t_0\times(L/16) \quad (7)$$

동일한 조건에서 식(5), 식(6), 그리고 식(7)의 계산 유닛에 대한 비교를 그래프로 나타내면 Fig. 17과 같고 제안한 LEA 활용 방법이 더 효율적임을 알 수 있다.

그리고 보안 태그 생성에 관계된 3가지 방법(SHA 512, LEA-CBC, SCM1)들의 계산 유닛은 다음과 같이 분석된다. SHA-512는 512비트 단위의 연산이 총 80라운드 수행된다. 먼저 입력된 메시지를 확장하는 과정(Fig. 11-(b))로서 확장된 블록($W_{16}\sim W_{79}$)마다 총 3번의 XOR연산($3t_0\times8\times64$)을 수행한다. 그리고 각 라운드(Fig. 11-(c))는 초기 값의 시프트 연산 6회($6t_1$), 초기 값(A)을 갱신하기 위한 Majority(8바이트 AND연산 3회($3\times8t_0$) 그리고 8바이트 XOR연산 2회($2\times8t_0$)), Rotate(A)(시프트연산 3회($3t_1$)와 8바이트 XOR연산 2회($2\times8t_0$))과 2번의 AND연산($2\times8t_0$)을 수행한다. 또한 초기 값(E)를 갱신하기 위해 Conditional(8바이트 AND연산 2회($2\times8t_0$)), Rotate(E) (시프트연산 3회($3t_1$)와 8바이트 XOR연산 2회($2\times8t_0$)), 그리고 5번의 AND 연산($5\times8t_0$)을 수행한다. 여기에 처리할 데이터 블록 수(L/64) 및 라운드 수(80)를 곱하면 식 (8)과 같이 정리된다.

LEA-CBC 방법(Fig. 18-(b))은 식(4)에서 SV와 입력 블록의 XOR연산의 계산 유닛($16t_0$)이 추가되어 여기에 처리할 데이터 블록 수(L/16)를 곱하면 식(9)로 정리된다.

SCM1 방법(Fig. 10-(a))은 4바이트 단위로 수행되지만 LEA-CBC와 동등한 조건에서 비교하기 위해 16 바이트 단위의 수행으로 4 바이트의 네 블록(총 16바이트)에 대해 고려한다. 각 라운드에서 키와 XOR연산($4\times4t_0$)을 하고 각 블록에 대해 XOR 연산($3\times4t_0$)하는 과정을 24라운드 반복수행하며 처리할 데이터 블록 수(L/16)를 곱하면 식 (10)으로 정리된다.

$$\text{SHA512}=80\times(1536t_0+(24t_0+16t_0+3t_1+16t_0+16t_0)+(16t_0+3t_1+16t_0+40t_0))\times(L/64)=134664t_0\times(L/64) \quad (8)$$

$$\text{LEA(CBC mode)}=(\text{LEA}+16t_0)\times(L/16)=887.2t_0\times(L/16) \quad (9)$$

$$\text{SCM1(Security Tag)}=(4\times4t_0+3\times4t_0)\times24\times(L/16)=6722t_0\times(L/16) \quad (10)$$

보안 태그 생성의 효율성에 대한 Fig. 18의 그래프는 다음과 같이 분석된다. 동일한 조건에서 식(8), 식(9), 그리고 식(10)의 계산 유닛에 대한 비교 결과로 LEA-CBC 방법이 SHA-512 방법에 비해 빠르지만 SCM1 방법에 비해서는 비교적 느리다. 하지만 SCM1

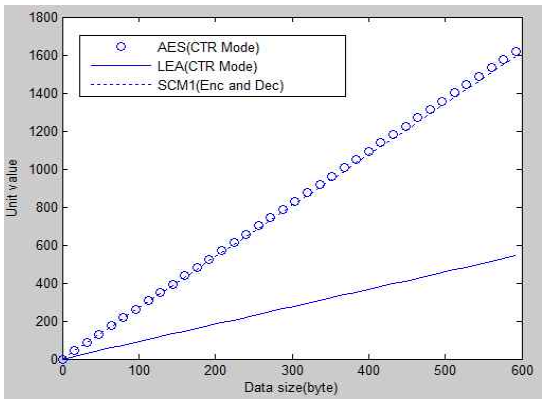


Fig. 17. Processing unit comparison for 3 encryption methods (AES-CTR, LEA_CTR, SCM1).

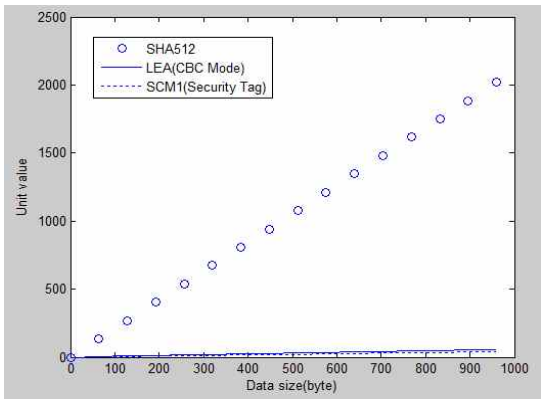


Fig. 18. Processing unit comparison for 3 security tag generation methods (SHA512, LEA-CBC, SCM1).

은 XOR 연산을 여러 번 반복하여 같은 값이 생성될 수도 있어 보안성이 떨어지지만, 반면에 LEA- CBC를 활용한 방법은 LEA 알고리즘 자체의 보안성과 SV 등의 적용으로 상대적으로 뛰어난 효과를 가진다.

6. 결 론

본 논문에서는 군집 드론 망을 활용한 다양한 IoT 응용 서비스 구현에 관계된 망 개념과 보안 메커니즘을 제안하였다. WTRP 링으로 구성된 FANET의 드론들은 잦은 통신 오류에 유연하게 대처하고 대표 드론을 통해 지상제어장치와 효율적으로 통신한다. 그리고 응용 데이터들은 MAVLink 응용 프로토콜로 전달되어 인터넷을 통한 클라우드 컴퓨팅 환경과 연동될 수 있어 서비스 범위의 확장이 가능하다.

보안성이 강화된 드론 IoT 서비스 제공을 위해 새로운 MAVLink 메시지 정의를 통한 보안 메커니즘 제시와 암호화 및 보안 태그 생성 방법이 보안성이 강화된 드론 IoT 서비스 제공을 위해 효율적임을 보였다. 또한 디피-헬만 키 생성 및 교환 방법을 적용하여 외부서버의 도움 없이 자체적으로 키를 생성하고 분배하는 편리한 방법도 제시되었다. 마지막으로 타 방법과의 소요 계산 유닛 비교 분석을 통해 제안된 보안 메커니즘의 효율성을 확인하였다.

향후 보안성 강화를 위해 기밀성이 강화된 SV의 생성 및 갱신 방법과 또한 제안된 보안 방법의 유연성 및 실용성 측면에서 확장과 더 나아가 구현된 프로토타입을 실제 현장 환경에서 적용하는 연구가 요구된다.

REFERENCE

[1] A. Restas, “Drone Application for Supporting Disaster Management,” *World Journal of Engineering and Technology,* Vol. 3, No. 3, pp. 316-321, 2015.

[2] I. Bekmezci, O.K. Sahingoz, and S. Temel, “Flying Ad-Hoc Networks (FANETs): A survey,” *Ad Hoc Networks,* Vol. 11, No. 3, pp. 1254-1270, 2013.

[3] A.J. Marty, *Vulnerability Analysis of the MAV Link Protocol for Command and Control of Unmanned Aircraft*, Master’s Thesis of Air Force Institute of Technology, 2013.

[4] N. Prapulla, S. Veena, and G. Srinivasalu, “Development of Algorithms for MAV Security,” *Proceeding of IEEE International Conference On Recent Trends In Electronics Information Communication Technology*, pp. 799-802, 2016.

[5] IETF, *Diffie-Hellman Key Agreement Method*, RFC 2631, 1999.

[6] M. Ergen and D. Lee, “WTRP-Wireless Token Ring Protocol,” *IEEE Transactions on Vehicular Technology*, Vol. 54, No. 6, pp. 1863-1881, 2004.

[7] Y. Shiu, S. Y. Chang, H. Wu, S. C. H. Huang, and H. Chen, “Physical Layer Security in Wireless Networks: A Tutorial IEEE Wireless Communications,” *IEEE Wireless Communication*, Vol. 18, No. 2, pp. 66-74, 2011.

[8] M. Shin and S. Kim, “A Study on the Security Framework for IoT Services Based on Cloud and Fog Computing,” *Journal of Korea Multimedia Society*, Vol. 20, No. 12, 2017, pp. 101-112.

[9] D. Lee, D. C. Kim, D. Kwon, and H. Kim, “Efficient Hardware Implementation of the Lightweight Block Encryption Algorithm LEA,” *Sensors,* Vol. 14, No. 1, pp. 975-994, 2014.

[10] J.S. Coron, Y. Dodis, C. Malinaud, and P. Puniya, “Merkle-Damgård Revisited: How to Construct a Hash Function,” *Proceeding of Annual International Conference on Advances in Cryptology*, pp. 430-448, 2005.

신 민 정

2017년 2월 부경대학교 정보통신공학과(공학사)
2017년 3월～현재 부경대학교 정보통신공학과 석사과정
관심분야 : 무선네트워크 보안기술, IoT, 포그컴퓨팅, 클라우드컴퓨팅

김 성 운

1982년～1985년 한국전자정보통신 연구소 연구원
1985년～1995년 한국통신연구개발원 선임연구원 실장
1989년～1993년 프랑스 파리 7대학 석·박사
1995년～현재 부경대학교 정보통신공학과 교수
관심분야 : 무선네트워크 보안기술, 센서네트워크, 전송망 및 액세스망 기술, IoT, 포그컴퓨팅, 클라우드컴퓨팅