Journal of the KIMST, Vol. 21, No. 6, pp. 817-825, 2018
ISSN 1598-9127
DOI http://dx.doi.org/10.9766/KIMST.2018.21.6.817

Research Paper 정보 · 통신 부문

전술 군집 드론 네트워크를 위한 중앙집권식 그룹키 관리 기법

이종관*,1) · 신규용1) · 김경민1)

1) 육군사관학교 사이버전 연구센터

Centralized Group Key Management Scheme for Tactical Swarming Drone Networks

Jong-Kwan Lee*,1) · Kyuyong Shin1) · Kyung-Min Kim1)

1) *Cyber Warfare Research Center, Korea Military Academy, Korea*

(Received 23 May 2018 / Revised 1 August 2018 / Accepted 5 October 2018)

ABSTRACT

Recently, drones have been used in various field to overcome time and space limitations. However, single drone still has a lot of restriction on transportation wight and travel time. Therefore many studies have been conducted to increase the utilization by swarm of drones. Many things should be additionally considered in order to operate swarming drones securely. Especially the group key management is a challenging research topic in tactical domain due to existence of adversary that has anti-drone skill. In this paper, we proposed an efficient group key management scheme for tactical swarming drone networks where an adversary equipped with anti-drone skills exists. The group key can be updated with a small number of message exchange compared to other convenience schemes. The numerical and simulation results demonstrate that the proposed scheme manages the group key efficiently and securely.

Key Words : Tactical Swarming Drone(전술 군집 드론), Group Key Management(그룹키 관리), Centralized Scheme(중앙집권식 기법), Dynamic Networks(동적 네트워크)

1. 서 론

드론은 군사적 목적 뿐 아니라 물류, 구조, 방송, 통신 등 다양한 분야에서 활용되고 있다. 기존 방식으로는 해결하기 어려웠던 난제들을 드론을 활용하여 극복할 뿐 아니라 새로운 응용 분야를 창출하고 있다. 하지만 개별 드론은 태생적으로 제한된 성능 때문에 그 활용도가 한정적일 수밖에 없다. 따라서 다수의 드론을 군집화하여 보다 효과적으로 다양한 분야에서 드론을 활용하려는 연구가 진행되고 있다[1]. 최근 정밀한 위치 보정 기술을 이용해 사전에 입력된 시나리오에 따라 개별 드론들을 위치시킴으로써 군집 드론을 예술 공연에 활용하는 사례가 많다. 향후에는 이보

* Corresponding author, E-mail: jklee64@kma.ac.kr

다 더욱 진보된 형태로 군집 드론이 군사적 목적으로 활용될 것으로 예상된다.

한편, 드론의 비약적인 성장에 따라 드론에 의한 사생활 침해, 민감한 정보의 노출 등 보안상의 취약점이 새롭게 대두되고 있다. 이에 따라 드론의 비행을 감시, 방해하고 더 나아가 드론의 동작을 정지시키는 안티드론 기술이 자연스럽게 발전하고 있다[2]. 안티드론 기술은 원격으로 드론을 운용하는데 필수적인 전파를 방해, 교란하는 기술과 그물, 레이저, 독수리 등을 이용하여 물리적으로 드론의 운용을 정지 또는 파괴하는 기술 등이 있다.

안티드론 기술에 의해 군집을 형성한 드론들 중 일부가 비인가자의 수중으로 넘어가는 경우 군집 드론 네트워크에서 유통되는 데이터의 유출, 암호키 노출 등의 보안 취약점이 발생된다. 또한 군집 드론은 임무와 목적에 따라 하나의 군집이 다수의 서브 군집으로 분할되거나 다수의 군집이 하나의 군집으로 결합될 수도 있다. 따라서 군집을 형성한 노드들 중 일부가 우발적인 상황으로 네트워크를 이탈하거나 동적으로 네트워크가 급격하게 변경될 때 효과적인 키 관리 기법이 필요하다.

그룹키 관리 기법은 일반적으로 중앙집권식, 비중앙집권식, 분산식 등 3가지 형태로 구분할 수 있다[3,4]. 중앙집권식은 하나의 키분배센터(KDC: Key Distribution Center)가 네트워크 전체의 키를 생성, 분배하는 역할을 한다. 효과적으로 키를 관리할 수 있는 장점이 있지만 KDC가 정상적인 역할을 수행하지 못하는 경우 네트워크 전체에 영향을 미치게 되는 단일 장애 지점(single point of failure) 문제가 발생한다. 비중앙식집권식 방식은 단일 네트워크를 여러 개의 클러스터 또는 계층으로 구분하여 클러스터별 또는 계층별로 키관리를 수행하는 방식이다. 보통 KDC와 네트워크 멤버들 간의 통신거리가 2-hop 이상인 경우 효과적일 수 있다. 또한 중앙집권식의 단일 장애 지점 문제를 완화할 수 있는 장점이 있다. 하지만 네트워크를 서브 네트워크로 분할하고 서브 네트워크별 KDC를 운용해야하는 등 키 관리 절차가 복잡하다는 단점이 발생한다. 마지막으로 분산식 방식은 타 기법과 달리 별도의 KDC를 운용하지 않으며 네트워크 멤버들간의 정보교환을 통해 키를 생성, 분배하는 방식이다. KDC의 기능이 네트워크 멤버들에게 공평하게 분배되었다고 할 수 있다. 따라서 특정 네트워크 멤버의 고장 또는 보안상의 문제가 키 관리에 전체적으로 영향을 미치지 않는다. 하지만 키 관리를 위해 멤버들간의 정보교환이 전제되어야하기 때문에 키 관리 절차가 매우 복잡하고 키를 생성, 분배하는데 많은 시간이 소요된다는 단점이 있다. 정리하면 특정 기법이 다른 기법에 비해 우월하다고 할 수는 없다. 다만, 사용되는 네트워크 환경을 고려하여 최적화된 기법을 선택하는 것이 필요하다.

적합한 키 관리 기법을 설계하기 위해서는 전술 군집 드론 네트워크의 특징과 각 기법들의 장단점이 고려되어야한다. 군집 드론은 상호 근거리에 위치하고 있기 때문에 일반적으로 모두 1-hop 거리에 있으며 매우 큰 이동성을 가지고 있어 네트워크를 세분화하여 관리하는 것이 쉽지 않다. 따라서 비중앙식 방식은 적합하지 않다. 또한 신속하게 키가 분배되어야 하는 전술환경을 고려한다면 키 분배에 많은 시간이 소요되는 분산식 또한 적절하지 않다고 할 수 있다. 반면 1-hop 거리에 있는 지상통제소의 지휘통제에 따라 임무를 수행하는 군집 드론의 네트워크 환경을 고려하면 중앙집권식이 가장 적절하다 할 수 있다. 따라서 본 논문에서는 전술 군집 드론 네트워크를 위한 효과적인 그룹키 관리 기법을 제안한다. 제안하는 기법은 중앙집권식으로 지상통제소(GC: Ground Controller)가 KDC 역할을 수행하며, 간단한 키 생성 알고리즘을 적용하여 전술적인 환경을 고려한 네트워크 변화에도 안전하고 효과적으로 그룹키를 갱신, 분배할 수 있다.

본 논문은 다음과 같이 구성된다. 2장에서 군집 드론 네트워크의 특징과 제한사항에 대해서 살펴보고 3장에서 제안하는 기법에서 고려하는 시스템 모델에 대해 정의한다. 4장에서 제안하는 기법을 상세히 설명하며 5장에서 제안하는 기법의 성능을 분석하고 6장에서 결론을 맺는다.

2. 군집 드론 네트워크

군집 드론 네트워크의 일반적인 특징과 제한사항은 다음과 같다.

- 무선 링크(wireless link): 드론은 기본적으로 무선 링크에 의존하여 지상통제소 또는 이웃 드론들과 정보를 교환한다. 무선 링크의 방송(broadcasting) 형태의 정보 전달 특성으로 스니핑(sniffing)과 같은 수동적인 공격 뿐 아니라 중간자(man-in-the-middle) 공

격, 메시지 재전송(message replay) 공격 등의 능동적인 공격에도 쉽게 노출된다. 따라서 키의 실시간 전달, 갱신, 폐기 등이 유선 링크에 비해 자유롭지 못하다.

- 제한된 성능(limited power): 드론은 비교적 소규모 비행체로 장시간의 비행을 보장하기 위해 드론의 무게와 에너지 사용에 대한 제약이 따를 수밖에 없다. 따라서 비행 외의 기능 구현에 대한 에너지 사용이 최소화되어야 한다. 즉, 낮은 CPU 성능, 적은 메모리 용량, 좁은 대역폭 등의 제한사항이 있다. 따라서 키 관리에 있어서 이러한 점들이 고려되어야 한다.

- 동적 네트워크(dynamics): 드론들은 공중에서 운용되므로 가시선이 쉽게 확보되어 열악한 채널 환경에 의한 네트워크 변경은 많지 않을 것이다. 하지만 군집 드론 네트워크는 필요에 따라 네트워크 멤버가 추가되기도 하고, 일부 멤버가 다양한 이유로 네트워크에서 이탈할 수도 있다. 또한 목적과 임무에 따라 두 개의 네트워크가 결합 또는 한 개의 네트워크가 다수의 네트워크로 분할될 수도 있다. 즉, 매우 동적인 네트워크이다. 따라서 네트워크 멤버십 변경에 따라 자원할당기법 및 키 관리 기법 등도 동적일 수밖에 없다.

- 멤버 유사성(homogeneous): 군집을 형성한 드론들은 여러 가지 면에서 유사성이 높을 수밖에 없다. 군집 드론은 동일한 목표에 군집을 형성하여 비행하기 때문에 비행간 고도, 속도, 방향 등이 유사하다. 또한 네트워크 운용을 위한 자원들도 유사하게 할당될 수밖에 없다. 왜냐하면 대부분의 멤버들이 동일한 임무를 수행하기 때문이다. 이러한 유사성을 비정상적인 멤버들을 식별하는데 활용할 수 있다.

이러한 군집 드론 네트워크의 특징과 제한사항들을 고려하여 키 관리 기법이 설계되어야 한다.

3. 시스템 모델

전술 군집 드론 시스템은 지상통제소(GC)와 n개의 드론으로 구성된다. 지상통제소와 드론은 1-hop 거리에 있어 동일한 그룹키를 소유하고 있다면 전송되는 모든 정보를 GC와 드론들이 공유할 수 있다. 또한 드론은 개별 또는 집단 단위로 계획적으로 군집을 이탈하거나 이탈했다가 다시 네트워크에 가입할 수 있다. 뿐만 아니라 다른 네트워크와의 결합, 분할이 수시로 발생된다.

드론은 개별적으로 개인정보를 내장하고 있으며 이는 유무선의 매체를 통해 외부로 전송되지 않는다. 드론들간에 매체를 예약방식 또는 경쟁방식으로 공유하며 형평성(fairness)을 고려한 MAC(Medium Access Control) 프로토콜 적용으로 모든 드론이 동일한 매체 접근기회를 보장받는다. 드론은 운행 시간 연장을 위한 에너지 소비의 최소화를 위해 제한적인 메모리 용량과 계산능력만을 보유한다. 그리고 군집 내의 드론들은 유사한 행동 패턴을 유지한다. 즉 드론의 속도, 이동 방향, 고도 등의 정보가 비슷하다.

지상통제소는 드론에 비해 채널 접근에 대한 우선권을 가지고 있다. 또한 드론과 달리 충분한 메모리 용량과 CPU 파워, 통신능력을 보유하며, 모든 드론의 개인정보를 저장하고 있다. 그리고 각 드론의 위치 정보를 주기적으로 수신하여 모든 드론의 이동 패턴을 파악할 수 있다[7]. 이를 통해 다수의 드론과 구분되는 행동을 하는 드론을 식별할 수 있다.

한편, 안티드론 기술을 보유한 적(또는 비인가자)의 존재를 가정한다. 적은 안티드론 기술을 이용하여 드론의 물리적인 파괴 없이 드론을 획득할 수 있다. 즉, 드론의 송수신 기능을 활용하여 획득된 드론을 통해 네트워크에 유통되는 정보에 대한 도청 등 수동적 공격 뿐 아니라, 네트워크 교란 목적의 허위 데이터 전송과 같은 능동적 공격도 감행할 수 있다.

Table 1. Notation

표 기	의 미
GK	정상 그룹키
$\widehat{GK}$	허위 그룹키
$\Psi_t^n(x)$	t번째 Type n 다항식
u_i	i번째 멤버 노드
x_i	i번째 멤버 노드의 개인정보
GC	지상통제소(키 분배센터)

4. 제안하는 기법

본 장에서는 다양한 동적인 네트워크 환경에서 제안하는 기법의 그룹키 관리 절차를 상세히 설명한다. Table 1은 제안하는 기법을 설명하는데 사용되는 주요 기호를 나타낸다.

4.1 그룹키 생성 알고리즘

제안하는 기법에서 적용하는 그룹키 생성 알고리즘은 기본적으로 CG가 노드들의 정보와 분배하고자 하는 그룹키를 이용하여 다항식(Ψ)을 만들고 다항식의 계수를 각 노드들에게 전달한다. CG로부터 계수 정보를 수신한 노드는 다항식에 자신의 정보를 입력하여 그룹키를 획득한다.

노드 u_i의 개인정보(또는 개인키)를 xi라 하자. CG는 네트워크의 모든 노드의 개인정보를 저장하고 있다. CG는 전달하고자 하는 그룹키 GK를 포함하여 다음과 같은 다항식을 만든다.

$$\begin{aligned}\Psi(x) &= (x-x_1)(x-x_2)\cdots(x-x_n)+GK \\ &= a_0+a_1x+\cdots+a_{n-1}x^{n-1}+x^n\end{aligned} \quad (1)$$

CG는 다항식의 계수들(a_0, a_1, ... a_{n-1})을 노드들에게 전달한다. 각 노드는 수신한 계수들로부터 다항식을 구성하고 자신의 정보 x_i를 입력하면 식 (1)에서 곱셈항들이 0이 되기 때문에 그룹키 *GK*를 획득할 수 있다. 반면 다항식에 자신의 개인정보가 포함되어 있지 않은 노드의 경우 자신의 개인정보를 다항식에 입력하더라도 곱셈항이 0이 되지 않아 *GK*를 획득할 수 없다.

4.2 네트워크 가입(join) 및 이탈(leave) 식별

네트워크 멤버십의 변동에 대한 판단은 네트워크 가입 및 이탈을 해당 노드가 이웃노드들에게 선언하는 명시적 방법과 명시적 선언 없이 멤버십 변동과 관련된 연관 정보의 분석을 통해 판단하는 암묵적 방법으로 구분할 수 있다.

네트워크 가입은 네트워크 가입 전에 해당 노드에 대한 인증절차가 필수적이기 때문에 통상 명시적인 방법이 사용된다. 네트워크 가입을 희망하는 노드는 MAC에 대한 접근권한을 획득한 후 GC 또는 이웃노드들에게 네트워크 가입 요청을 한다. 이후 상호 약속된 절차를 거쳐 기존 그룹키를 새로 가입하는 노드에게 전달하거나 새로운 그룹키를 모든 노드에게 재분배한다.

반면 네트워크를 이탈하는 경우에는 상황에 따라 명시적 또는 암묵적 방법이 사용된다. 노드가 GC에게 이탈 여부를 명시적으로 선언한 후 네트워크를 이탈하는 경우에는 GC가 그룹키 갱신의 필요성을 바로 인지할 수 있다. 즉, 각 노드는 주기적으로 Hello 메시지 또는 상호 약속된 신호를 전송하여 네트워크에 가입되어 있음을 명시적으로 선언하는 것이다.

반면 의도치 않은 상황으로 노드가 네트워크를 이탈하는 경우에는 그룹키 갱신의 필요성을 암묵적으로 판단하는 별도의 절차가 필요하다. 특히, 전술 환경에서는 적의 의도된 위해행위로 계획되지 않은 네트워크 이탈이 다수 발생할 확률이 높다. 적에게 노획된 노드가 피아식별을 위한 프로토콜을 정상적으로 준용하고 수신모드로 대기하면서 네트워크 내에서 유통되는 정보를 감청하는 경우 해당 노드의 네트워크 이탈을 판단하기 어렵다. 따라서 다른 노드들과 구분되는 특징(위치, 속도, 방향 등)을 기초로 GC가 노드 이탈을 판단해야 한다. 이는 이상점(outlier) 검출 알고리즘을 통해 구현이 가능하다. 본 논문에서는 통계적 거리 기반 이상점 검출 알고리즘을 통해 노드의 네트워크 이탈을 판단할 수 있다고 가정한다[8]. 즉, 적에게 노획되거나 또는 해킹에 의해 다른 노드들과 다른 이상행위를 하는 노드들은 네트워크 이탈로 판단하여 그룹키를 재분배한다.

4.3 네트워크 가입시 그룹키 관리

신규 노드가 네트워크에 가입되었을 때 그룹키를 관리하는 방법에는 ①그룹키를 갱신하는 방법과 ①기존 그룹키를 신규 노드에게만 전달하는 방법이 있다. 신규 노드가 발생할 때마다 그룹키를 갱신하는 것은 전체 네트워크 보안성을 향상시킬 수는 있지만 각 노드가 그룹키 갱신을 위한 CG와의 통신과 추가적인 연산이 필요하다는 단점이 있다. 반면 기존 그룹키를 신규 노드에게 전달하는 방법은 신규 노드와 CG와의 통신만으로 신규 노드가 그룹키를 획득할 수 있다는 장점이 있다. 한편, 그룹키의 안전성을 위해 네트워크 멤버십의 변경이 없더라도 무차별 대입 공격(brute force attack)에 대응하기 위해 주기적으로 그룹키를 갱신하는 것이 필요하다. 따라서 제안하는 기법에서는 *그룹키 갱신시간*이 *TH* 이상이면 그룹키를 갱신하는 방법을 적용하고, *TH* 이하이면 그룹키를 신규 노드에 전달하는 방법을 적용한다.

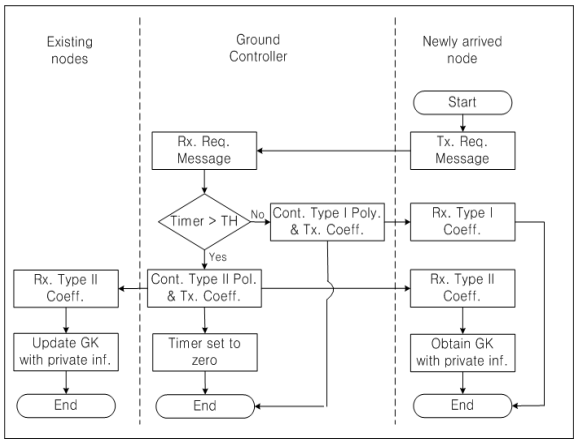

Fig. 1. Procedure of group key management for a newly arrived node

4.3.1 현재 그룹키 전달

네트워크 가입을 희망하는 노드 u_i는 GC에게 네트워크 가입 요청 메시지를 전달한다. u_i로부터 네트워크 가입 요청을 받은 GC는 u_i의 개인정보와 현재 그룹키 GK_t를 이용하여 다음과 같이 다항식을 구성한다.

$$\begin{aligned}\Psi_t^I(x) &= (x-x_i)(x-r_1)\cdots(x-r_{n-1}) + GK_t \\ &= a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + x^n\end{aligned} \quad (2)$$

여기서 r_k ($0<k<n$) 는 GC가 다항식 구성을 위해 랜덤하게 생성한 값이다. 그리고 Ψ_t^I을 t번째 생성되는 그룹키에 대한 Type Ⅰ 다항식이라 정의하자. 다항식의 계수들을 수신한 u_i는 자신의 정보를 다항식에 대입하여 그룹키 GK_t를 획득한다. 기존 멤버들은 그룹키 전달 과정에 참여하지 않는다.

4.3.2 새로운 그룹키 분배

u_i로부터 네트워크 가입 요청을 받은 GC는 u_i와 기존 멤버 노드들의 개인정보, 새로 생성한 그룹키를 이용하여 다항식을 구성한다. n개의 노드로 구성된 네트워크에 새로운 노드 u_i가 가입하는 경우 GC가 생성하는 다항식은 다음과 같다.

$$\begin{aligned}\Psi_{t+1}^{II}(x) &= (\Psi_t^{II}(x) - GK_t)(x-x_i) + GK_{t+1} \\ &= (x-x_1)(x-x_2)\cdots(x-x_{n+1}) + GK_{t+1} \\ &= a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + x^{n+1}\end{aligned} \quad (3)$$

여기서 Ψ_t^{II}는 기존 그룹키 분배를 위해 GC가 구성한 다항식이다. Ψ_{t+1}^{II}은 (t+1)번째 그룹키에 대한 Type II 다항식이다. 다항식 생성 후 GC는 다항식의 계수들을 전 노드에게 전송하고 *그룹키 갱신시간(timer)*을 0으로 설정한다. 새로 진입한 노드를 포함한 모든 노드들은 자신의 개인정보를 Ψ_{t+1}^{II}에 대입하여 새로운 그룹키 GK_{t+1}를 획득한다.

Fig. 1은 새로운 노드가 진입했을 때 기존 그룹키 전달 절차와 새로운 그룹키의 분배 절차를 나타낸다.

4.4 네트워크 이탈시 그룹키 관리

노드 이탈은 크게 계획된 정상적인 이탈과 비계획적인 이탈로 구분할 수 있다. 계획적 이탈인 경우 전방 안전성을 위해 현재의 그룹키를 갱신하는 것이 필요하다. 한편, 비계획적인 이탈인 경우 해당 노드를 비인가자가 악의적인 목적으로 사용할 수 있다. 따라서 잔류하는 노드들의 그룹키를 갱신하는 것 뿐 아니라 이탈된 노드에게는 기만 목적의 그룹키를 전달한다. 이번 절에서는 계획적 이탈과 비계획적 이탈에 대한 그룹키 관리 방법에 대해 설명한다.

4.4.1 계획된 노드 이탈

계획된 노드 이탈의 경우 해당 노드는 명시적으로 GC에게 네트워크 이탈을 보고한다. 계획된 네트워크 이탈을 인지한 GC는 네트워크를 이탈한 노드에 대한 개인정보를 제외한 새로운 Type Ⅱ 다항식을 구성한다. n개의 노드로 구성된 네트워크에 u_n가 이탈한 경우 GC가 생성하는 다항식은 다음과 같이 계산된다.

$$\begin{aligned}\Psi_{t+1}^{II}(x) &= (\Psi_t^{II}(x) - GK_t)/(x-x_n) + GK_{t+1} \\ &= (x-x_1)(x-x_2)\cdots(x-x_{n-1}) + GK_{t+1} \\ &= a_0 + a_1x + a_2x^2 + \cdots + a_{n-2}x^{n-2} + x^{n-1}\end{aligned} \quad (4)$$

GC는 다항식의 계수들을 전 노드에게 전달한다. 잔류하는 노드들은 자신의 비밀키를 식 (4)에 대입하여 새로운 그룹키 GK_{t+1}를 획득한다. 반면 네트워크를 이탈한 u_n이 식 (4)에 자신의 개인정보를 대입하면 무의미한 형태의 값을 얻게 되며 그룹키 GK_{t+1}를 획득할 수 없다. 이는 다항식에 자신의 개인정보가 포함되어 있지 않기 때문이다.

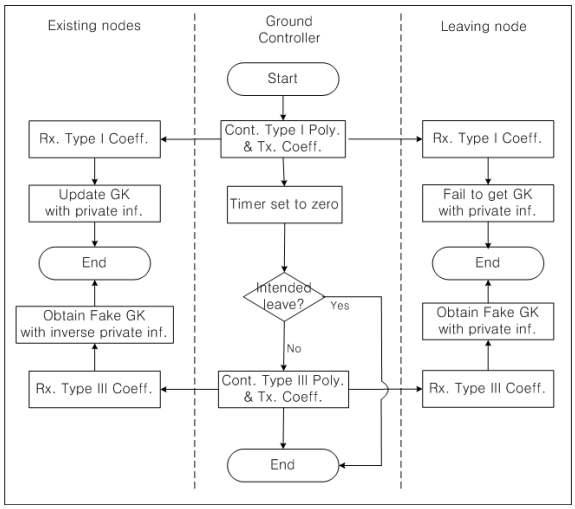

Fig. 2. Procedure of group key management for a leaving node

4.4.2 비계획된 노드 이탈

비계획적인 노드 이탈의 경우 GC는 명시적으로 노드 이탈을 인지할 수 없다. 하지만 3.2절에서 설명한 바와 같이 이상점 검출 알고리즘을 통해 네트워크 이탈을 간접적으로 확인할 수 있다. 비계획적 이탈을 인지한 GC는 3.4.1절에서 설명한 절차와 동일하게 기존 그룹키를 갱신한다. 이후 이탈된 노도 u_i의 개인정보, 잔류 노드의 개인정보, 허위 그룹키 $\widehat{GK}$를 이용하여 다음과 같이 Type Ⅲ의 다항식을 구성한다.

$$\begin{aligned}\Psi_t^{III}(x) &= (x-x_i)(x+x_1)\cdots(x+x_n)+\widehat{GK} \\ &= a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}+x^n\end{aligned} \quad (5)$$

u_i는 자신의 개인정보를 식 (5)에 입력하여 허위 그룹키 $\widehat{GK}$를 획득한다. 반면 잔류하는 노드들이 식 (5)에 자신의 개인정보를 입력하면 정상적인 그룹키를 획득할 수 없으나, 음수의 개인정보를 입력하면 허위 그룹키를 획득할 수 있다. 즉, 잔류 노드들은 개인정보를 이용하여 식 (4)와 (5)로부터 정상적인 그룹키 GK와 허위 그룹키 $\widehat{GK}$를 구분할 수 있다.

4.5 다수의 노드 가입 및 이탈시 그룹키 관리

두 개 이상의 노드가 한 번에 네트워크에 가입 또는 이탈하는 경우에 개별적으로 그룹키를 갱신 또는 전달하는 것은 GC와의 메시지 교환을 비례적으로 증가시켜 매우 비효율적이다. 제안하는 기법에서는 다수의 노드가 네트워크에 가입 또는 이탈시 메시지 교환을 최소화하여 그룹키를 관리한다.

4.5.1 다수의 노드 가입

다수의 노드가 동시에 가입하는 경우 GC는 각 노드들과 개별적인 인증절차를 거친다. 그룹키 갱신시간이 TH 이하인 경우에는 4.3.1절에서 식 (2)을 통해 설명한 바와 같이 새로 진입하는 노드들의 개인정보들과 랜덤값 그리고 현재의 그룹키 정보를 이용하여 Type I 다항식을 구성한다. 반면에 갱신시간이 TH 이상인 경우에는 4.3.2절에서 식 (3)을 통해 설명한 바와 같이 Type II 다항식을 구성한다. 노드들과의 메시지 전달과정과 개별 노드들이 그룹키를 획득하는 절차는 개별 노드가 네트워크에 진입하는 경우와 동일하다. 하나의 다항식에 새로 가입하는 다수의 노드 정보를 포함하고 있어 그룹키 갱신 또는 전달을 위해 필요한 메시지 교환양을 크게 줄일 수 있다.

4.5.2 다수의 노드 이탈

다수의 노드가 동시에 네트워크를 이탈하는 경우 GC는 4.4절에서 식 (4)와 식 (5)에서 설명한 바와 같이 기존의 다항식에서 이탈한 노드들의 개인정보를 제외한 다항식을 구성한다. 따라서 네트워크에 잔류하는 노드들은 자신의 개인정보를 통해 그룹키를 갱신할 수 있으며, 이탈한 노드들은 그룹키 갱신이 불가능하다. 네트워크를 이탈하는 노드별로 다항식을 구성하지 않고 하나의 다항식으로 다수의 노드 이탈을 처리할 수 있어 메시지 교환양을 크게 줄일 수 있다.

5. 성능 분석

본 장에서는 보안성과 통신 효율성 측면에서 제안하는 기법의 성능을 분석한다.

5.1 보안성

제안하는 기법의 보안성을 평가하기 위해 전방안전성(Forward Secrecy), 후방안전성(Backward Secrecy), 공모공격(Collusion Attack)에 대한 안전성을 분석한다.

5.1.1 전방 안전성(Forward Secrecy)

전방 안전성은 네트워크 그룹을 이탈한 멤버가 이

전 그룹키를 이용하여 현재 통신내역에 접근하지 못하게 하는 것이다. 네트워크 그룹을 이탈한 멤버 u_i는 자신의 개인정보, 현재 보유하고 있는 과거의 그룹키들 그리고 GC로부터 수신한 정보를 기초로 현재의 그룹키를 추출하려고 시도할 것이다. 하지만 GC가 송신한 정보에는 이미 u_i에 대한 정보가 제외되어 있기 때문에 u_i의 비밀키로 현재의 그룹키를 추출하는 것은 불가능하다. 또한 그룹키는 GC에 의해서 랜덤하게 생성되므로 과거의 그룹키들을 토대로 현재의 그룹키를 추출할 수 없다. 따라서 제안하는 기법은 전방 안전성을 보장한다.

5.1.2 후방 안전성(Backward Secrecy)

후방 안전성은 네트워크 그룹에 새롭게 가입한 노드가 가입 이전의 통신내역에 접근하지 못하게 하는 것이다. 가입 이전의 통신내역에 접근하기 위해서는 과거의 그룹키가 필요하다. 새로 네트워크에 가입한 노드 u_i가 과거의 그룹키를 획득하기 위해서는 GC가 과거에 전송했던 정보가 필요할 뿐 아니라 과거의 네트워크 멤버들의 비밀키가 필요하다. 하지만 각 노드의 비밀키는 절대 유통되지 않는다. 또한 GC도 과거의 정보를 재전송하지 않을 뿐 아니라 그룹키는 랜덤하게 선택되므로 GC가 전송한 현재의 정보를 통해 과거의 정보를 유추하는 것은 불가능하다. 따라서 제안하는 기법은 후방 안전성을 보장한다.

5.1.3 공모 공격(Collusion Attack)

공모 공격은 네트워크의 합법적인 가입자였던 2개 이상의 노드가 네트워크를 이탈한 이후 협력적인 방법으로 현재의 그룹키를 획득하려는 시도이다. 제안하는 기법에서는 그룹키를 갱신하는 과정에서 그룹을 이탈한 노드의 비밀키 정보가 모두 삭제된다. 또한 노드들의 비밀키는 상호 독립적으로 할당되기 때문에 그룹을 이탈한 노드들의 비밀키의 조합을 통해 다른 노드의 비밀키를 유추할 수 없다. 따라서 제안하는 기법은 공모 공격에 안전하다.

5.2 통신 효율성

통신효율성을 측정하기 전술적 환경에서 그룹키가 갱신되기 위해 필요한 메시지 교환횟수를 분석한다. 또한 *그룹키 갱신시간*이 통신 효율성에 미치는 영향을 살펴본다.

5.2.1 가정 사항

제안하는 기법의 성능을 평가하기 위해 다음과 같은 시나리오를 가정한다. 임무수행을 위해 최초 *n*개의 드론으로 구성된 군집드론은 작전 수행간 목표 및 임무 변경에 의해 일부가 계획적으로 군집을 이탈할 수 있으며, 적의 안티드론 기술에 의해 비계획적으로 이탈할 수 있다. 계획, 비계획적으로 군집을 이탈하는 드론은 다음과 같은 포아송(Poisson) 분포를 따른다고 가정한다.

$$p_i(k) = e^{-\lambda_i}\frac{\lambda^{k_i}}{k!}, \qquad i = 1, 2 \tag{6}$$

여기서 λ_1, λ_2는 각각 계획적인 이탈, 비계획적인 이탈의 경우 단위 프레임당 사건(event)이 발생할 평균을 나타낸다. 계획적, 비계획적 이탈은 서로 독립적인 사건이므로 두 분포의 합도 포아송 분포를 따르게 된다. 따라서 최초의 군집 규모를 유지하기 위해 이탈한 드론의 수만큼 새로운 드론들이 네트워크에 진입한다라고 가정하면 진입하는 드론의 수도 $\lambda_3(=\lambda_1 + \lambda_2)$ 파라미터를 갖는 포아송 분포를 따른다.

한편, 한 프레임 이내에서 요청된 진입 또는 이탈은 GC에 의해서 동시에 처리되며 *그룹키 갱신시간*은 *TH* 프레임이라 가정하고 그룹키가 *TH* 프레임 이상의 시간 이내에 갱신되지 않았다면 자동으로 GC에 의해서 그룹키를 갱신한다.

5.2.2 메시지교환 횟수

제안하는 기법에서 *n*개의 드론이 진입, 이탈하는 경우 GC와 드론간에 교환해야 하는 메시지의 개수는 Table 2와 같다.

Table 2. Number of message exchange

구 분	이 탈		진 입
	계획적	비계획적	
횟 수	$n + 1$	2	$n + 1$

N_1^p, N_2^p, N_3^p를 각각 제안하는 기법에서 계획적 이탈, 비계획적 이탈, 진입시 프레임당 평균 메시지 교환 횟수라 하자. N_1^p과 N_2^p는 다음과 같이 계산된다.

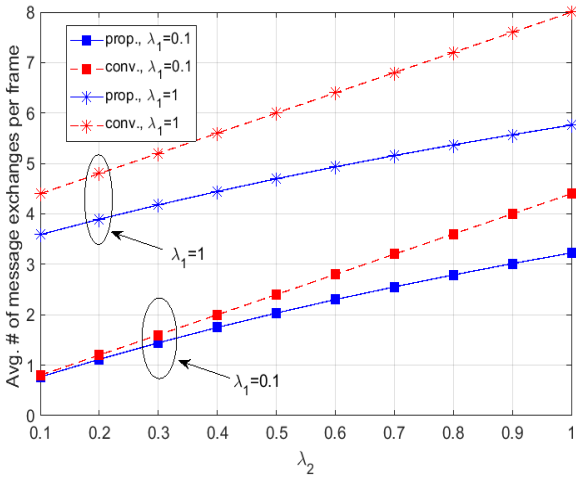

Fig. 3. Average number of message exchanges per frame with different λ_1 and λ_2

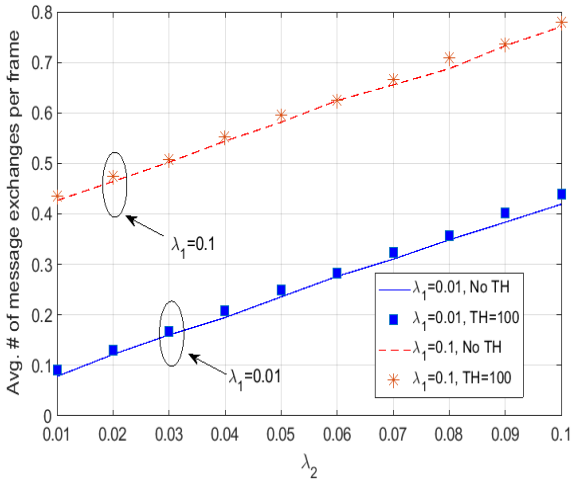

Fig. 4. Average number of message exchanges per frame with different *TH*

$$N_1^p = \sum_{k=1}^{\infty}(k+1)p_1(k) = \lambda_1 + 1 - e^{-\lambda_1} \quad (7)$$

$$N_2^p = 2\sum_{k=1}^{\infty}p_2(k) = 2(1-e^{-\lambda_2}) \quad (8)$$

한편 네트워크 진입은 독립적으로 포아송 분포를 따르는 계획적, 비계획적 이탈의 합이기 때문에 N_3는 다음과 같다.

$$N_3^p = \sum_{k=1}^{\infty}(k+1)p_3(k) = \lambda_3 + 1 - e^{-\lambda_3} \quad (9)$$

따라서 프레임당 평균 메시지 교환 횟수 N_t^p은 다음과 같다.

$$N_t^p = N_1^p + N_2^p + N_3^p = 6 + 2\lambda_1 + \lambda_2 - (2+e^{-\lambda_1})(1+e^{-\lambda_2}) \quad (10)$$

반면, 단일 드론의 진입, 이탈시 마다 그룹키를 갱신하는 기법[5,6]의 프레임당 평균 메시지 교환 횟수 N_t^c는 다음과 같다.

$$N_t^c = N_1^c + N_2^c + N_3^c = 4(\lambda_1 + \lambda_2) \quad (11)$$

Fig. 3은 λ_1과 λ_2의 값에 따른 프레임당 평균 메시지 교환횟수를 나타낸다. λ 값이 작은 경우 제안하는 기법과 기존 기법의 차이가 적은 반면 λ가 증가할수록 기존 기법에 비해 제안하는 기법이 적은 메시지 교환 횟수를 나타낸다. 이는 λ가 증가할수록 프레임당 2개 이상의 드론에 의해 그룹키 변경 소요가 발생할 확률이 높기 때문이다. 따라서 다수의 그룹키 변경 소요를 한 번에 처리할 수 있는 제안하는 기법이 λ가 증가할수록 기존 기법에 비해 우수한 성능을 나타낸다.

5.2.3 *그룹키 갱신시간(TH)*이 성능에 미치는 영향

제안하는 기법에서 그룹키가 일정 시간 이상 갱신되지 않으면 GC에서 자동으로 그룹키 갱신이 이루어진다. 제안하는 기법에서 그룹키 갱신시간은 *TH* 프레임이고, 포아송 분포의 프레임당 평균은 λ이다. 따라서 $TH \cdot \lambda > 1$일 때 평균적으로 자동으로 그룹키가 갱신되지 않는다. 반대로 $TH \cdot \lambda < 1$일 때 평균적으로 자동으로 그룹키가 갱신된다. 한편, 자동으로 그룹키가 갱신되기 위해 요구되는 메시지 교환횟수는 1이다. 따라서 λ의 값에 따라 적절한 *TH*를 선택할 경우 메시지 교환 횟수가 크게 증가하지 않는다. λ가 큰 경우 *TH*의 영향은 미미하다는 것을 직관적으로 알 수 있다. 왜냐하면 λ가 크면 그만큼 그룹 갱신 기회가 잦으므로 그룹

갱신 시간이 *TH*를 초과할 확률이 낮기 때문이다.

Fig. 4는 λ가 0.01 ~ 0.1 사이의 값으로 매우 작을 때 *TH*가 제안하는 기법의 성능에 미치는 영향을 나타낸다. *TH*는 100 프레임으로 설정하였는데 이는 100 프레임 동안 그룹키 갱신이 없으면 GC에 의해 자동으로 그룹키가 갱신되는 극단적인 상황을 조성한 것이다. 그림에서 보는 바와 같이 100 프레임마다 그룹키를 변경하더라도 *TH*가 제안하는 기법의 성능을 크게 훼손하지 않음을 알 수 있다. 이는 GC가 한 번의 메시지 전송만으로 그룹키를 갱신할 수 있기 때문이다.

6. 결 론

본 논문에서 전술 군집 드론 네트워크에서 중앙집권적인 그룹키 관리 기법을 제안하였다. 제안하는 기법은 군집 드론이 운용되는 전술적 환경을 고려하여 드론의 네트워크 집단 이탈, 집단 진입의 경우 메시지 교환 횟수를 최소화하여 그룹키를 갱신한다. 또한 적에 의한 드론 탈취에 대비하여 드론이 비계획적으로 이탈한 경우 가짜 그룹키를 이탈한 드론에게 전송하여 기만의 효과를 달성하고 보안성을 강화하였다.

제안하는 기법을 수학적으로 분석한 결과 개별 드론 단위로 그룹키를 처리하는 기존 기법들에 비해 메시지 교환 횟수를 크게 줄여 안전성을 보장하는 가운데 그룹키 관리의 효율성을 향상시킴을 확인하였다.

후 기

본 논문은 육군사관학교 화랑대연구소의 2018년도 논문출판비 지원을 받아 연구되었음.

References

[1] Q. Cui, P. Liu, J. Wang and J. Yu, “Brief Analysis of Drone Swarms Communication,” 2017 IEEE International Conference on Unmanned Systems(ICUS), Beijing, pp. 463-466, 2017.

[2] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi and J. Chen, “Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges,” in IEEE Communications Magazine, Vol. 56, No. 4, pp. 68-74, APRIL 2018.

[3] N. Renugadevi, G. Swaminathan and A. S. Kumar, “Key Management Schemes for Secure Group Communication in Wireless Networks - A Survey,” 2014 International Conference on Contemporary Computing and Informatics(IC3I), Mysore, pp. 446-450, 2014.

[4] B. Jiang and X. Hu, “A Survey of Group Key Management,” 2008 International Conference on Computer Science and Software Engineering, Wuhan, Hubei, pp. 994-1002, 2008.

[5] Zheng, X. L., Huang, C. T., Matthews, M., “Chinese Remainder Theorem based Group Key Management,” Association for Computing Machinery Proc. 45th Annual Southeast Regional Conf.(ACMSE-07), Winston-Salem, North Carolina, USA, pp. 266-271, 2007.

[6] Zhou, J., Ou, Y.-H., “Key Tree and Chinese Remainder Theorem based Group Key Distribution Scheme,” J. Chin. Inst. Eng., Vol. 32, No. 7, pp. 967-974, 2009.

[7] C. Li, Y. Li, Z. Tian, S. L. Weekes and K. Pahlavan, “Design and Performance Evaluation of a Localization System to Locate Unwanted Drones by using Wireless Signals,” 2018 IEEE International Conference on Consumer Electronics(ICCE), Las Vegas, NV, pp. 1-6, 2018.

[8] Y. Zhang, N. Meratnia and P. Havinga, “Outlier Detection Techniques for Wireless Sensor Networks: A Survey,” in IEEE Communications Surveys & Tutorials, Vol. 12, No. 2, pp. 159-170, Second Quarter 2010.