https://doi.org/10.33778/kcsa.2023.23.4.093

동적 군집 무인체계를 위한 비밀분산법 기반의 그룹키 할당 기법★

이 종 관*

요 약

본 논문은 여러 개의 무인체계 그룹이 하나의 그룹으로 통합되거나 하나의 무인체계 그룹이 여러 개의 그룹으로 분리될 수 있는 동적인 군집 무인체계 환경에서의 그룹키 할당 기법을 제안한다. 제안하는 프로토콜은 그룹키 생성 단계와 그룹키 공유 단계로 구성된다. 그룹키 생성에는 그룹의 대표 노드만이 참여하며, 그룹 대표 노드는 비밀분산기법을 이용하여 그룹키를 여러 조각으로 분할하여 전달한다. 이를 수신한 노드들은 자신이 생성한 그룹키의 비밀 조각과 대표노드로 부터 수신한 조각들을 통해 새로운 그룹키를 개별적으로 추출하고 해시함수를 이용하여 추출된 그룹키의 무결성을 검증하다. 제안하는 기법의 성능을 보안성 및 통신효율성 측면에서 분석하여 네트워크 그룹이 매우 동적으로 변화하는 미래 군집 무인체계 운용에 효과적으로 적용될 수 있음을 확인한다.

Group Key Assignment Scheme based on Secret Sharing Scheme for Dynamic Swarm Unmanned Systems

Jongkwan Lee*

ABSTRACT

This paper presents a novel approach for assigning group keys within a dynamic swarm unmanned system environment. In this environment, multiple groups of unmanned systems have the flexibility to merge into a single group or a single unmanned system group can be subdivided into multiple groups. The proposed protocol encompasses two key steps: group key generation and sharing. The responsibility of generating the group key rests solely with the leader node of the group. The group's leader node employs a secret sharing scheme to fragment the group key into multiple fragments, which are subsequently transmitted. Nodes that receive these fragments reconstruct a fresh group key by combining their self-generated secret fragment with the fragment obtained from the leader node. Subsequently, they validate the integrity of the derived group key by employing the hash function. The efficacy of the proposed technique is ascertained through an exhaustive assessment of its security and communication efficiency. This analysis affirms its potential for robust application in forthcoming swarm unmanned system operations scenarios characterized by frequent network group modifications.

Key words : Group Key Assignment, Secret Sharing Scheme, Swarm Unmanned System, Network Group, Network Merge, Network Split

접수일(2023년 08월 21일), 수정일(2023년 09월 04일), 게재확정일(2023년 10월 08일)

★ 본 논문은 육군사관학교 화랑대연구소의 지원을 받아 수행되었음.

* 육군사관학교 컴퓨터과학과 (주저자, 교신저자)

1. 서 론

국방혁신 4.0에 따르면 우리 군은 안보환경의 변화와 첨단과학기술의 발전에 따라 핵심 첨단전력을 우선적으로 확보하기 위한 세부 과제로 유무인 복합전투체계 구축을 선정하였다. 유무인 복합전투체계 구축은 3단계로 진행될 예정인데 1단계는 원격통제형 중심의 체계 구축이고, 2단계는 반자율형 체계의 시범 운용이다. 마지막 3단계는 반자율형 체계의 확산 및 자율형 전환이다[1].

미래 전장에서는 무인체계가 자율적으로 상황을 인지하고 결심하여 작전을 수행하게 된다. 이때, 무인체계들은 공동의 목표 달성을 위해 다수의 무인체계가 하나의 그룹을 형성하여 운용될 것이다. 휘발성(volatile), 불확실성(uncertain), 복잡성(complex), 모호성(ambiguous)으로 표현되는 전장환경의 특수성을 고려했을 때 최초 형성된 그룹은 작전상황에 따라 매우 다양한 형태로 변화될 것이다[2][3]. 즉, 그룹에 새로운 무인체계가 추가되거나 기존에 소속된 무인체계가 다른 그룹으로 소속이 변경될 수 있다. 더 나아가 다수의 그룹이 하나의 그룹으로 결합되거나, 하나의 그룹이 여러 그룹으로 분리될 수 있다.

본 논문은 이러한 환경을 고려했을 때 그룹 멤버들간의 안전한 브로트캐스팅 전송을 보장하기 위한 효율적인 그룹키 할당 방안을 제안한다. 제안하는 기법은 다수의 그룹이 결합되거나 하나의 그룹이 여러 그룹으로 분리되는 상황에서 그룹키 생성 및 공유가 가능하도록 비밀분산법을 이용한다. 비밀분산법은 비밀을 여러 개의 조각으로 분할하기 위한 암호학적 방법이다. 제안하는 기법은 새롭게 생성한 그룹키(즉, 비밀)를 여러 조각으로 분할하여 그룹 멤버들에게 전달한다. 이를 전달받은 그룹 멤버는 수신한 비밀조각과 본인이 생성한 비밀조각을 결합하여 그룹키를 추출한다. 이를 통해, 군집 무인체계 그룹이 동적으로 변화하는 조건에서도 효과적인 그룹키 할당이 가능하다.

본 논문은 다음과 같이 구성된다. 2장에서 관련 연구 현황을 살펴보고, 3장에서는 본 논문에서 가정하는 시스템 모델과 제안하는 그룹키 할당 기법에 대해 설명하다. 4장에서 제안하는 기법에 대한 성능을 보안성과 통신효율성 측면에서 분석하고 5장에서 결론을 맺는다.

2. 관련 연구

그룹키 할당은 키 분배의 안정성 및 효율성, 확장성, 할당의 간편성, 호환성 등 다양한 요소를 종합적으로 고려해야 한다.

그룹키 할당 기법에 대한 많은 연구 결과가 발표되었으나 전술환경의 특징을 고려한 연구결과는 많지 않다. 그룹키 할당 기법은 일반적으로 중앙집권식, 비중앙집권식, 분산식 등 3가지로 구분할 수 있다[4][5]. 중앙집권식은 하나의 키분배센터(KDC: Key Distribution Center)가 키의 생성, 분배를 담당한다. 반면 비중앙집권식은 다수의 키분배센터를 운용하여 클러스터별 또는 계층별로 키 할당을 수행한다. 분산식은 별도의 키분배센터 없이 네트워크 멤버들간의 정보교환을 통해 키를 관리한다.

군집 드론이 운용되는 전술 네트워크의 특성을 고려하여 중앙집권식의 그룹키 관리 기법이 제안되었다[6]. 제안한 기법은 그룹멤버들의 인증정보들과 현재 그룹키를 이용하여 다항식을 구성하여 전달하고, 이를 전달받은 그룹 멤버들은 자신의 인증정보를 이용하여 다항식으로부터 새로운 그룹키를 추출한다. 그룹키 정보를 그룹 멤버들에게 개별적으로 전송하지 않기 때문에 드론의 집단 이탈 또는 집단 진입의 경우에도 메시지 교환 횟수를 최소화하여 그룹키를 갱신한다. 전방안전성, 후방안전성, 공모공격 등에 안전하며, 그룹키 갱신시 필요한 메시지 교환 횟수가 적어 통신효율성이 우수하다. 하지만 키분배센터가 정상적인 역할을 하지 못할 경우에 전체 네트워크에 영향을 미칠 수 있는 단일 장애 지점(single point of failure) 문제가 있다.

한편, 위치 정보를 활용한 그룹키 할당 기법들

이 제안되었다[7-9]. 이들은 그룹 멤버들간의 양호한 채널 상태를 가정한다. 하지만 전술 네트워크 환경에서는 지형, 기상, 적의 방해 활동 등 다양한 이유로 항상 양호한 채널 상태를 보장할 수 없다. 이러한 제한사항을 극복하기 위해 인접 그룹 멤버가 아닌 채널 환경이 확률적으로 가장 우수한 그룹 리더와 정보교환을 통해 최소 출력으로 그룹키를 할당하는 위치 종속적 그룹키 할당 기법이 제안되었다[10]. 그룹 리더는 지역별 그룹키를 할당함으로써 비밀정보 공유의 신뢰성과 안전성을 동시에 확보할 수 있다. 하지만 제안된 기법은 네트워크의 동적 변화, 즉 그룹 멤버의 가입 및 탈퇴, 다수 그룹의 결합 또는 분리를 고려하지 않았다.

3. 제안하는 그룹키 할당 기법

본 장에서는 제안하는 기법이 가정하는 시스템 모델에 대해서 설명한다. 그리고 제안하는 기법이 다수의 무인체계 그룹이 통합될 때와 하나의 무인체계 그룹이 여러 개의 그룹으로 분리될 때 새로운 그룹키를 생성하고 공유하는 절차에 대해 세부적으로 살펴본다.

3.1 시스템 모델

본 논문에서는 무인체계들이 하나의 그룹을 형성하고 이러한 그룹이 다수 존재하는 전장환경을 가정한다. 그룹에 소속된 무인체계는 하나의 대표노드(*LN: Leader Node*)와 하나 이상의 일반노드(*FN: Follower Node*)로 구분된다. 각 그룹에는 *LN*이 반드시 존재하며 *LN*의 기능이 상실되면 *FN* 중 하나의 무인체계가 *LN*으로 선출된다. 한편, 각 그룹은 필요에 따라 다수의 그룹이 하나의 그룹으로 통합되거나 하나의 그룹이 다수의 그룹으로 분리된다.

모든 무인체계는 공개키(x)와 개인키(y)를 각각 보유한다. 공개키는 그룹내 무인체계들과 공유하며 개인키는 공유되지 않는다. 개인키와 공개키의 관계는 아래와 같다. 이때 소수 p와 q는 무인체계에게 공개된 값이다.

$$x = q^y \bmod p \tag{1}$$

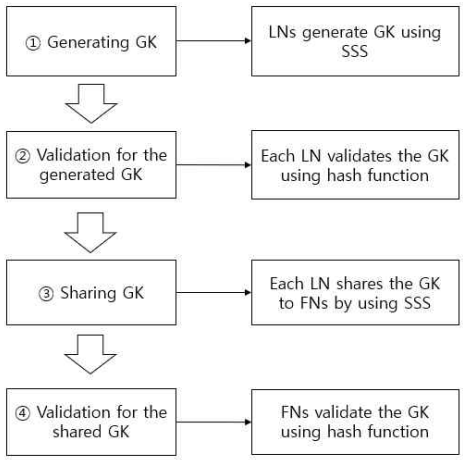
한편, 각 그룹별로 *LN*은 그룹 내에서 사용할 그룹키를 생성한 후 여러 조각으로 분할하여 *FN*에게 전달한다. *FN*은 수신한 그룹키 조각들과 자신만이 보유한 조각을 조합하여 그룹키를 추출한다. 표 1은 본 논문에서 사용하는 기호 및 의미를 나타낸다.

<표 1> 기호 및 의미

기 호	의 미
LN_i	i번째 그룹의 대표노드
$FN_{i,j}$	i번째 그룹의 j번째 일반노드
$x_{i,0}$	i번째 그룹의 대표노드의 공개키
$x_{i,j}$	i번째 그룹의 j번째 일반노드의 공개키
$y_{i,0}$	i번째 그룹 대표노드의 개인키
$y_{i,j}$	i번째 그룹의 j번째 일반노드의 개인키
$f_i(x)$	i번째 그룹의 대표노드가 그룹 결합시 그룹키 생성을 위해 생성하는 다항식
$g_i(x)$	i번째 그룹의 대표노드가 그룹키를 *FN*들에게 공유하기 위해 생성하는 다항식
S_i	i번째 그룹의 그룹키
S_{new}	*네트워크가 결합 또는 분리될 때의 새로운 그룹키*
n_i	i번째 그룹에 소속된 *FN*의 수
k	결합되는 그룹의 수
SSS	Secret Sharing Scheme, 비밀분산법
GK	Group Key, 그룹키

3.2 무인체계 그룹 결합

무인체계 그룹들이 결합될 때 새로운 그룹키의 생성 및 공유 절차는 ① 그룹키 생성, ② 생성된 그룹키 검증, ③ 검증된 그룹키 공유, ④ 공유된 그룹키 검증 등 4개 과정으로 구성된다. 그림 1은 각 단계별 세부 절차를 개념적으로 나타낸다.



(그림 1) 무인체계 그룹 결합시 그룹키 할당

3.2.1 그룹키 생성

네트워크 통합시 그룹키 생성과정은 크게 5단계로 구분된다.

- 1단계 : k개의 그룹이 결합한다고 가정했을 때, i번째 그룹의 대표노드 LN_i는 (0, S_i)와 아래 데이터 포인트들을 지나는 k-1차 다항식 $f_i(x)$를 생성한다.

$$(x_{j,0},\ x_{j,0}^{y_{i,0}}),\ j=1,\ 2,\ \ldots\ k,\ j\neq i \qquad (2)$$

- 2단계 : LN_i는 $f_i(x)$에서 아래와 같이 k개의 데이터 포인트를 추출하여 결합되는 그룹의 모든 LN_j에게 전달한다.

$$(m,\ f_i(m)),\ m=1,\ 2,\ \ldots,\ k \qquad (3)$$

- 3단계 : LN_j는 LN_i로부터 수신한 k개 데이터 포인트와 LN_j가 생성한 데이터 포인터 ($x_{j,0}$, $x_{i,0}^{y_{j,0}}$)를 이용하여 $f_i(x)$를 복원한다.

- 4단계 : LN_j는 $f_i(x)$에서 i번째 그룹의 그룹키 S_i를 다음과 같이 추출한다.

$$f_i(0)=S_i,\ i\neq j \qquad (4)$$

이때, LN_j는 k-1개의 S_i를 추출한다.

- 5단계 : LN_j는 통합 그룹에 대한 그룹키 S_{new}를 다음과 같이 비트단위 연산을 통해 생성한다.

$$S_{new}=S_1\otimes S_2\otimes\cdots\otimes S_k \qquad (5)$$

3.2.2 생성된 그룹키 검증

통합 대상 그룹의 LN들이 생성한 그룹키를 검증하는 단계는 2단계로 구성된다.

- 1단계 : LN_i는 $C_i=H(S_i, x_{i,0})$를 LN_j에게 전달한다. 여기서 H는 일방향 해시함수이다.

- 2단계 : LN_j는 $C_i'=H(f_i(0), x_{i,0})$를 계산하고, $C_i=C_i'$이면 LN_i의 그룹키 S_i는 정당하다고 판단한다.

k-1개의 S_i가 모두 검증되면 식(5)에 의해 계산된 그룹키 S_{new}도 검증된 것으로 간주한다.

3.2.3 검증된 그룹키 공유

통합 대상이 되는 i번째 그룹의 FN의 수는 n_i개라고 가정한다. 검증된 그룹키 공유 절차는 크게 4단계로 구성된다.

- 1단계 : LN_i은 (0, S_{new})와 다음 데이터 포인트들을 지나는 n_i차 다항식 $g_i(x)$를 생성한다.

$$(x_{i,j},\ x_{i,j}^{y_i}),\ j=1,\ 2,\ \ldots\ n_i \qquad (6)$$

• 2단계 : LN_i은 $g_i(x)$에서 아래와 같이 n_i개의 데이터 포인트를 추출하여 모든 $FN_{i,j}$에게 전달한다.

$$(m,\ g_i(m)),\ m = 1,\ 2,\ \ldots,\ n_i \tag{7}$$

• 3단계 : $FN_{i,j}$는 LN_i로부터 수신한 n_i개의 데이터 포인트와 $FN_{i,j}$가 생성한 데이터 포인트 $(x_{i,j},\ x_{i,0}^{y_{i,j}})$를 이용하여 $g_i(x)$를 복원한다.

• 4단계 : $FN_{i,j}$는 $g_i(x)$에서 그룹키 S_{new}를 다음과 같이 추출한다.

$$g_i(0) = S_{new} \tag{8}$$

3.2.4 공유된 그룹키 검증

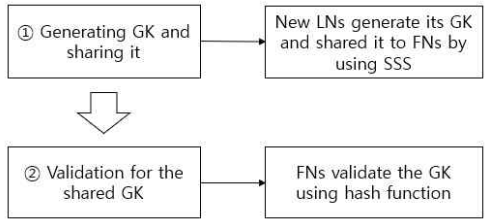
LN_i으로부터 공유된 통합 그룹키(S_{new})를 검증하는 과정은 2개 단계로 구성되며, 3.2.2절에서 설명한 “생성된 그룹키 검증” 과정과 유사하다.

• 1단계 : LN_i는 $C_i = H(S_i, x_{i,0})$를 $FN_{i,j}$에게 전달한다.

• 2단계 : $FN_{i,j}$는 $C_i' = H(g_i(0), x_{i,0})$를 계산하고, $C_i = C_i'$이면 통합된 그룹에 대한 새로운 그룹키 S_{new}는 정당하다고 판단한다.

3.3 무인체계 그룹 분리

무인체계 그룹이 분리될 때 각 그룹별 새로운 그룹키의 생성 및 공유 절차는 ① 그룹키 생성, ② 그룹키 검증 등 2개 과정으로 구성된다. 본 절에서는 그룹이 k개로 분리되고 분리된 하위 그룹에서 FN의 수는 n_i개라고 가정한다. 그림 2는 각 단계별 세부 절차를 개념적으로 나타낸다.



(그림 2) 무인체계 그룹 분리시 그룹키 할당

3.3.1 분리 그룹에 대한 그룹키 생성

그룹 분리시 분리 그룹에 대한 그룹키 생성과정은 크게 4단계로 구분된다. 3.2.3절에서 설명한 “검증된 그룹키 공유” 절차와 유사하다.

• 1단계 : 그룹이 분리되었을 때 i번째 하위 그룹의 대표노드 LN_i는 S_{new}를 임의로 선정하고, $(0,\ S_{new})$와 다음 데이터 포인트들을 지나는 n_i차 다항식 $g_i(x)$를 생성한다.

$$(x_{i,j},\ x_{i,j}^{y_{i,0}}),\ j = 1,\ 2,\ \ldots\ n_i \tag{9}$$

• 2단계 : $g_i(x)$로 부터 아래와 같이 n_i개의 데이터 포인트를 추출하여 모든 $FN_{i,j}$(j=1, 2, … , n_i)에게 전달한다.

$$(m,\ f_i(m)),\ m = 1,\ 2,\ \ldots,\ n_i \tag{10}$$

• 3단계 : LN_i로부터 수신한 n_i개 데이터 포인트와 $FN_{i,j}$가 생성한 데이터 포인터 $(x_{i,j},\ x_{i,0}^{y_{i,j}})$를 이용하여 $FN_{i,j}$는 $g_i(x)$를 복원한다.

• 4단계 : $FN_{i,j}$는 식 (11)과 같이 S_{new}를 추출한다.

$$g_i(0) = S_{new} \tag{11}$$

3.3.2 공유된 그룹키 검증

LN_i으로 부터 공유된 분리 그룹에 대한 그룹키(S_{new})를 검증하는 과정은 2단계로 구성되며, 3.2.2절에서 설명한 “생성된 그룹키 검증” 과정과 유사하다.

- 1단계 : LN_i는 $C_i = H(S_{new}, x_{i,0})$를 $FN_{i,j}$에게 전달한다.
- 2단계 : $FN_{i,j}$는 $C_j^{'} = H(g_i(0), x_{i,0})$를 계산하고, $C_j = C_j^{'}$이면 그룹키 S_{new}는 정당하다고 판단한다.

4. 성능 분석

제안하는 기법의 성능을 보안성과 통신효율성 측면에서 분석한다. 보안성은 전방안전성, 후방안전성 그리고 기밀성과 무결성 측면에서 살펴보고 통신효율성은 그룹키의 완전한 전파에 필요한 메시지 전달 횟수를 통해 분석한다.

4.1 보안성

4.1.1 전방 안전성

전방 안전성(forward secrecy)은 과거의 그룹키로 현재의 그룹키들을 추정할 수 없어야 한다는 것을 의미한다. 따라서 그룹이 결합되었을 때 결합되기 이전의 그룹키를 이용하여 결합된 그룹의 데이터에 접근할 수 없어야 한다. 또한 그룹이 분리되었을 때 분리된 특정 그룹의 무인체계들이 분리되기 이전의 기존 그룹키를 이용하여 자신이 속하는 분리된 새로운 그룹뿐 아니라 자신이 속하지 않은 다른 그룹의 데이터에 접근할 수 없어야 한다.

제안하는 기법은 그룹이 결합되었을 때 결합 대상이 되는 그룹의 LN으로부터 기존 그룹키와 무관하게 생성된 그룹키들의 조합으로 통합 그룹에 대한 새로운 그룹키를 생성한다. 따라서 그룹 결합시에도 전방안전성을 보장한다. 한편, 그룹이 분리되었을 때 분리된 그룹의 LN들이 상호 협력없이 독자적으로 기존 그룹키와 무관하게 그룹키를 생성한다. 따라서 그룹 분리 시에도 전방 안전성을 보장한다.

4.1.2 후방 안전성

후방 안전성(backward secrecy)은 새롭게 할당받은 현재의 그룹키를 통해 과거의 그룹키를 추정할 수 없어야 한다는 것을 의미한다. 따라서 새롭게 생성 및 할당받은 그룹키로 결합 또는 분리되기 이전의 그룹에서의 데이터에 접근할 수 없어야 한다.

제안하는 기법은 그룹 결합시 그룹의 LN들이 현재 사용하고 있는 그룹키와 무관하게 독자적으로 비밀키를 선택하고, 이를 비밀분산법을 이용하여 안전하게 전달한다. 그리고 이들의 조합을 통해 새로운 그룹 비밀키를 생성한다. 즉, 새로운 그룹키를 생성하는 과정에 있어서 각 그룹이 사용하고 있는 그룹키가 전혀 공유되지 않는다. 따라서 제안하는 기법은 후방 안전성을 보장한다. 한편, 그룹이 분리될 때 분리된 그룹의 LN들은 상호 협력없이 독자적으로 기존 그룹키와 무관하게 그룹키를 생성하여 공유한다. 따라서 그룹 분리 시에도 후방 안전성을 보장한다.

4.1.3 기밀성 및 무결성

제안하는 기법에서 LN은 비밀분산법을 이용하여 그룹키를 여러 조각으로 분할하고 이를 FN에게 전달한다. FN은 자신만이 보유하고 있는 개인키를 이용하여 그룹키의 또 다른 조각을 생성한다. FN은 수신받은 조각들과 자신이 생성한 조각을 이용하여 그룹키를 추출한다. 즉, 대외적으로 절대 공개되지 않는 개인키가 없으면 그룹키를 추출할 수 없다. 따라서 제안하는 기법은 기밀성을 보장한다. 한편, FN이 추출한 그룹키는 해시함수를 이용한 검증 절차를 거치기 때문에 무결성이 보장된다.

4.2 통신 효율성

통신효율성을 분석하기 위해 그룹키가 모든 FN에게 전파될 때까지 필요한 메시지 전송 횟수를 살펴본다.

그룹 결합시 모든 무인체계는 1-hop 통신 범위에

있다고 가정한다. 제안하는 기법은 그룹 결합시 그룹별 LN들의 협업을 통해 그룹키를 생성하고 이를 그룹별로 FN들에게 전파한다. 반면, 비교기법은 결합 그룹의 LN이 독자적으로 새로운 비밀키를 생성하고 이를 비밀분산법으로 결합 그룹의 모든 FN에게 전송한다고 가정한다. 이때, 그룹이 결합되기 전의 각 그룹의 노드들은 공개키를 상호 공유하고 있는 상태이다.

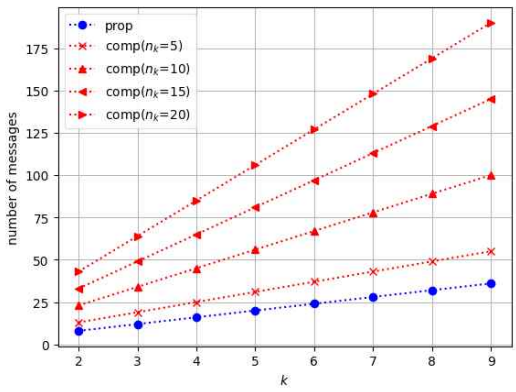
제안하는 기법은 네트워크 결합시 그룹키 생성, 생성된 그룹키 검증, 검증된 그룹키 공유, 공유된 그룹키 검증에 각각 k번의 메시지 전송이 필요하다. 따라서 총 $4k$의 메시지 전송이 필요하다.

한편, 비교기법에서 결합 그룹의 LN은 자신이 속했던 그룹 이외의 무인체계들의 공개키를 보유하고 있지 않다. 따라서 그룹키 할당 전에 공개키들을 추가로 수집하여야 한다. 이후 제안하는 기법과 동일하게 3.2.1에서 설명한 바와 같이 비밀키를 생성하고 결합된 그룹의 FN들에게 전송하며, 3.2.2에서 설명한 것과 같이 전송한 그룹키를 개별 FN들이 검증한다. 따라서 비교기법에서 i번째 그룹의 LN이 결합되는 그룹의 LN이 된다고 가정하면 총 메시지 전달 횟수는 아래와 같다.

$$1+\sum_{\substack{k=1\\k\neq i}}^{m}(n_k+1) \tag{12}$$

그림 3은 그룹 결합시 결합되는 그룹의 수 및 각 그룹에 속한 무인체계의 수에 따라 제안하는 기법과 비교 기법이 발생시키는 메시지 전송횟수를 비교한 것이다. 결합되는 그룹의 수(k)가 크거나 각 그룹별 노드의 수(n_k+1)가 크다면 제안하는 기법이 비교기법에 비해 메시지 전송횟수가 현저히 적다. 한편, 제안하는 기법은 결합되기 이전의 그룹별 리더노드에 의해서 새로운 그룹키가 전파되기 때문에 메시지 전송횟수는 그룹별 노드의 수와 무관하다. 그런데 결합되는 그룹 수의 증가에 따라 전송 횟수도 증가한다. 하지만 비교 기법에 비해 크게 증가하지 않는다.

한편, 그룹 분리시에는 제안하는 기법과 비교 기법의 메시지 전송 횟수가 $2m$으로 동일하다. 제안하는 기법도 그룹 분리시에는 비교기법과 동일하게 하나의 LN에 의해서 그룹키가 생성되고 전파되기 때문이다.



(그림 3) 메시지 전송 횟수 비교

5. 결론 및 향후연구

본 논문은 네트워크 그룹의 동적인 변화를 고려하여 그룹이 결합되거나 분리될 때 그룹키를 할당하는 기법을 제안하였다. 제안하는 기법은 생성된 그룹키를 비밀분산법을 이용하여 여러 조각으로 분할한다. 그리고 그룹키 조각들을 전송하고 이를 수신한 노드들은 수신받은 조각과 자신이 생성한 비밀 조각을 이용하여 그룹키를 추출한다. 공개 채널을 통해 그룹키가 전혀 노출되지 않기 때문에 그룹키의 안전성을 보장할 수 있다. 또한 그룹 결합시 그룹키 생성 절차에 LN들만이 참여함으로써 메시지 전송횟수를 감소시킬 수 있다. 따라서 제안하는 기법은 작전상황에 따라 네트워크 그룹이 매우 동적으로 변화하는 미래 군집 무인체계 운용에 효과적으로 적용될 수 있다.

한편, 제안하는 기법을 적용했을 때의 계산량을 분석하고 최소화하는 방안에 대해 추가적으로 연구할 예정이다.

참고문헌

[1] 국방부, “국방혁신 4.0 기본계획”, 2023.3.

[2] DARPA, Broad Agency Announcement Amendment 2 Collection and Monitoring via Planning for Active Situational Scenarios (COMPASS), Strategic Technology Office, May 2018.

[3] Jongkwan Lee, et. al., "A Study on Research Trends and Future Direction of AI Models for Anomaly Analysis in Military Operations" Journal of Digital Contents Society vol. 24, no. 3 pp. 631-640, March 2023.

[4] Sandro Rafaeli and David Hutchison, "A Survey of Key Management for Secure Group Communication," ACM Computing Surveys, Vol. 35, No. 3, pp. 309-329, Sep. 2003.

[5] Yang Xiao, et. a.l, "A Survey of Key Management Schemes in Wireless Sensor Networks," Computer Communications, Vol. 30 pp. 2314-2341, 2007.

[6] Jongkwan Lee, Kyuyong Shin, and Kyung-Min Kim, "Centralized Group Key Management Scheme for Tactical Swarming Drone Networks", Journal of the KIMST, Vol. 21, No. 6, pp. 817-825, Dec. 2018.

[7] Chang-Oh Kim, Kyungran Kang and Young-Jong Cho, "A Distributed Multicast Group Key Management Scheme for a Hierarchically Structured Network," Journal of KIISE, Vol. 38, No. 1, pp. 22-32, Feb. 2011.

[8] Farooq Anjum, "Location Dependent Key Management in Sensor Networks without Using Deployment Knowledge," Wireless Network, pp. 1587-1600, Oct. 2008.

[9] C. K. Wong, M. Gouda, S. S. Lam, "Secure Group Communications Using Key Graphs," IEEE/ACM Trans. Networking, Vol. 8, pp. 16-31, Feb. 2000.

[10] Jongkwan Lee, Kyuyong Shin, and Kyung-Min Kim, "A Location Dependent Group Key Management Scheme for High Confidential Information in Tactical Wireless Networks", Journal of the KIMST, Vol. 21, No. 5, pp. 658-664, Oct. 2018.

〔저자소개〕

이 종 관 (Jongkwan Lee)
2000년 2월 육군사관학교 전자공학과 학사
2004년 2월 한국과학기술원 전자공학 석사
2014년 2월 아주대학교 NCW 박사
2021년 3월~현재 아주대학교 국방디지털융합학과 객원교수
2017년 12월~현재 육군사관학교 컴퓨터과학과 교수

email : jklee6456@kma.ac.kr