JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 23, No. 4: 477~485, Apr. 2019

드론 네트워크 보안을 위한 해시표 대체 방식의 능동 방어 기법

임성민[1] · 이민우[2] · 임재성[2*]

MTD (Moving Target Detection) with Preposition Hash Table for Security of Drone Network

Sungmin Leem[1] · Minwoo Lee[2] · Jaesung Lim[2*]

[1]Undergraduate Student, Department. of Military Digital Convergence, Ajou University, Suwon 16499, Republic of Korea
[2*]Professor, Department. of Military Digital Convergence, Ajou University, Suwon 16499, Republic of Korea

요 약

드론 산업의 발달로 인해 드론 네트워크의 보안이 중요해졌다. 특히, 드론 네트워크의 무선통신 감청과 이로 인한 불법 드론 공격, 서비스 거부 공격에 대한 방어가 필요하다. 본 논문에서는 드론 네트워크의 보안성 향상을 위해 능동 방어를 위한 네트워크 MTD (Moving Target Defense) 기법을 적용하는 방안을 제안한다. 기존의 네트워크 MTD 기법을 드론 네트워크에 적용하게 되면, 드론 식별을 위한 해시값이 무선통신 중 노출될 위험이 있고, 일대다 군집형 드론 네트워크로의 적용이 제한된다. 본 논문에서는 해시값 노출에 따른 보안 위험을 감소하기 위해 해시표 사전 배치 (PHT, Preposition Hash Table) 방식을 사용하고, 해시값을 별도의 카운터로 대체한다. 드론 네트워크 상에 해시값을 직접 전송하지 않기 때문에 해시값 생성시 사용된 키 값의 노출 위험이 감소되고, 결과적으로 동일한 키의 사용 시간을 연장하게 됨으로써 드론 네트워크의 보안성 향상에 기여할 수 있다. 또한, 비행 중 드론의 키 교환을 하지 않기 때문에 일대다 군집형 드론 네트워크로의 적용이 가능하다. 모의실험을 통해 드론 네트워크 공격시 키 사용량과 패킷 전송 성공률을 확인하여 제안방식이 드론 네트워크의 보안성 향상에 기여할 수 있음을 확인하였다.

ABSTRACT

As the drones industry evolved, the security of the drone network has been important. In this paper, MTD (Moving Target Detection) technique is applied to the drone network for improving security. The existing MTD scheme has a risk that the hash value is exposed during the wireless communication process, and it is restricted to apply the one-to-many network. Therefore, we proposed PHT (Preposition Hash Table) scheme to prevent exposure of hash values during wireless communication. By reducing the risk of cryptographic key exposure, the use time of the cryptographic key can be extended and the security of the drone network will be improved. In addition, the cryptographic key exchange is not performed during flight, it is advantageous to apply PHT for a swarm drone network. Through simulation, we confirmed that the proposed scheme can contribute to the security of the drone network.

키워드 : 드론, 네트워크, 보안, 해시, 능동 방어 기법

Keywords : Drone, Network, Security, Hash, MTD

Received 15 March 2019, **Revised** 18 March 2019, **Accepted** 30 March 2019

***Corresponding Author** Jaesung Lim(E-mail:jaslim@ajou.ac.kr, Tel:+82-31-219-2545)
Professor, Department. of Military Digital Convergence, Ajou University, Suwon 16499, Republic of Korea

Open Access http://doi.org/10.6109/jkiice.2019.23.4.477 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

4차 산업혁명기술을 이용하는 대표적인 서비스 모델인 드론 산업이 급속히 발전하고 있다. 이러한 드론 네트워크는 지상통제국, 비행체, 그리고 무선 통신망으로 구성된다. 드론 산업의 성장에 따라 지상통제국과 드론 간 일대일 형태의 드론 네트워크 보다는 일대다 형태의 군집형 드론 네트워크로 변화되고 있다[1].

드론 네트워크는 무선 통신을 사용하기 때문에 많은 네트워크 공격 위협에 노출되어 있다. 소형, 경량화 된 드론에서 충분히 안전한 암호 통신을 사용하기는 어려워 보인다. 공격자가 획득한 송수신 정보를 이용하게 되면, 불법 드론을 운영하거나 드론 네트워크의 서비스를 방해하는 DoS (Denial of Service) 공격이 가능하게 된다.

따라서, 드론 네트워크에서 무선 통신의 감청 위협을 감내하기 위해서는 공격자가 키 해독을 어렵게 해야 한다. 하지만 드론의 비행 시간이 길어지고 동일한 키를 사용하게 될수록 공격자의 키 해독 가능성은 높아지게 된다[2-4]. 이러한 일이 발생하게 되면, 공격자는 기존에 수집한 정보들을 해독하게 됨으로써 완전 순방향 비밀성 (PFS, Perfect Forward Secrecy)을 지키기 어렵게 된다. 드론 네트워크를 이용해 전송하는 정보가 매우 중요할 경우 치명적인 정보 노출 사고가 될 수 있다.

암호화 해시 알고리즘의 키 노출을 예방하기 위해 키를 자주 바꾸는 방법도 쉽지 않다. 왜냐하면, 비행체가 포함된 드론 네트워크에서 드론의 키를 변경하는 것이 어렵기 때문이다.[1] 이를 보완하기 위해 IPSec (Internet Protocol Security)을 사용하는 종단간 암호화 통신을 사용할 수도 있지만 여전히 상호인증 및 키 설정 절차에 대한 공격 위험이 존재한다[5].

본 논문에서는 드론 네트워크에 대한 무선통신 공격 위협을 감소 시켜 보안성을 향상시키기 위하여 기존의 네트워크 MTD (Moving Target Defense) 기법을 드론 네트워크에 적용하는 방법을 제안한다. 네트워크 MTD 기법은 단말 또는 서버의 네트워크 주소를 해시값으로 변이시켜 공격자가 공격 대상을 특정하기 어렵게 하는 기법이다[6].

1) 공개키를 이용한 암호키 분배 기법도 가능하지만, 본 논문에서는 하드웨어적 제약조건이 까다로운 경량 드론을 대상으로 한다.

하지만, 유선망에서 사용하는 네트워크 MTD 기법을 무선망을 사용하는 드론 네트워크에 적용하게 되면, 역시 송수신간에 해시값이 노출되게 된다. 본 논문에서는 이러한 방법을 구현하기 위해 기존 네트워크 MTD 기법과는 달리 해시 값이 노출되지 않는 방식을 제안한다. 제안 기법은 해시표를 사전에 드론에 위치하게 하고 해시표의 값을 또 다른 값인 카운터로 대체하여 송신하는 해시표 사전 배치 (PHT, Pre-position Hash Table) 하는 것이다. 해시표는 드론에 직접 접근하지 않는 이상 공격자는 확인할 수 없으며, 공격자는 패킷을 감청하여도 해시값이 아닌 카운터만 알 수 있어 해시 표를 추정할 수 없다.

이로 인해 공격자는 제한된 시간 내에서 키 값을 알아내기 어려워지게 되고, 키 노출 위협이 감소된 만큼 키 사용 시간이 늘어나게 되어 드론 네트워크의 보안성이 향상되게 된다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 네트워크 MTD에 대한 관련 연구를 살펴보고, Ⅲ장에서 본 논문의 제안 기법인 PHT 기법을 설명한다. Ⅳ장에서는 모의실험을 통해 PHT 기법의 성능을 분석하여 키 사용량의 감소, 전송 성공률을 통해 PHT 기법의 성능을 확인한다. Ⅴ장에서 결론으로 본 논문을 매듭짓는다.

Ⅱ. 관련 연구

주요 MTD 기법으로 시간 동기화 기법, 해시 함수 기반 동기화 기법, 응답 기반 동기화 기법을 소개한다.

2.1. 시간 동기화 기법

H. Lee 등 [7]이 제시한 시간 동기화 기법은 송신자와 수신자가 동일한 IP/Port를 공유하기 위해 타임 슬롯 (time slot)을 이용한다. 각 타임 슬롯은 시간 τ의 주기로 나누어져 있다. 송신자와 수신자는 슬롯의 값과 공유 함수를 이용하여 타임 슬롯에 동기화된 IP/Port를 계산한다. 이때 슬롯에 동기화 되지 않은 값을 사용하는 패킷이 전송된다면 시스템은 이 패킷을 네트워크 감청에 의한 공격으로 추정할 수 있다.

하지만 드론 네트워크의 무선 통신 환경에서는 통신 장애, 전송 지연의 문제로 인해 시간 동기화 기법을 사용하기 어렵다. 그림1과 같이 통신 오류에 의한 패킷 누

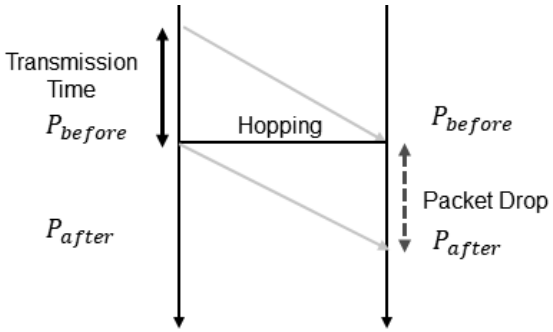

Fig. 1 Example of the packet dropping when a hopping is occurred since the transmission delay.

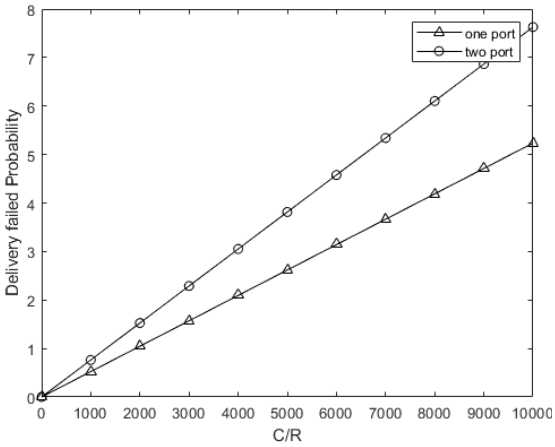

Fig. 2 Compare to the transmission failure rate between with the number of using ports (C : attack strength, R : buffer space).

락, 드론의 동적 이동에 따른 네트워크 구조 변경에 따른 전송 지연이 빈번하게 발생하여 타임 슬롯간에 호핑(hopping)이 발생하기 때문이다.

2.2. 해시 함수 기반 동기화 기법

M. Dunlop 등[8]은 기존 IPv6 체계에 해시 함수를 적용한 새로운 동기화 기법인 MT6D (Moving Target IPv6 Defense)를 제안하였다. MT6D는 IPv6에 있는 Interface Identifier 값을 동적으로 변환하여 공격자가 네트워크 정보를 분석하는 것을 방해한다. 송신자와 수신자는 사전에 공유한 암호키와 타임 스탬프(time stamp)를 입력값으로 하는 암호화 해시 함수를 사용함으로써 보안성을 강화하였다.

하지만, MT6D는 일대일 (point-to-point) 환경에서는 문제가 없지만, 군집 드론과 같은 일대다, 또는 다대대의 다중 클라이언트 환경에서는 암호키 관리와 배정의 어려움이 있다.

Y. Lou 등[9]은 네트워크 노드의 주소를 가상 주소로 대체하기 위해 AHG (Address Hopping Gateway)와 PAHG (Port and Address Hopping Gateway)를 통해 실제 주소와 가상주소를 연결하는 RPAH (Random Port and Add- ress Hopping)를 제시하였다. 가상주소는 공유된 키, 노드 ID, 해시 함수를 사용하여 계산된다. 하지만 RPAH와 같이 무선 환경에서 노출되는 해시 값을 사용하는 경우에는 생일 공격 (Birthday Attack)과 같은 다양한 해시 공격 방법으로 분석되고 공격당할 수 있다. 따라서 해시 값이 노출되지 않도록 다른 방안을 사용해야 한다.

2.3. 응답 기반 동기화 기법

G. Badishi 등[10]은 메시지의 전송과 그에 따른 응답값에 따라 통신 포트를 동적으로 변경하는 호핑 방식을 제안하였다. 응답 기반 호핑 기법에서의 제어 메시지는 송신자와 수신자간의 연결을 동적으로 변화시키기 때문에 제어 메시지를 안정적으로 수신하는 것이 매우 중요하다. 이 때문에 수신 측에서는 항상 2개의 포트를 이용하여 모든 패킷을 수신한다. 이 2개의 포트는 P_{old}, P_{new}로 이루어지며 P_{new}에 값이 정상적으로 수신되면, P_{new}를 사용하고 기존의 P_{new} 값은 P_{old}에 넣어 예비로 사용하는 방식으로 구현되었다.

응답 기반 동기화 방식은 시간 기반 동기화 방식과 달리 패킷 누락을 대비하였기 때문에 더 안정적인 호핑 방식을 사용 할 수 있고 이 때문에 상대적으로 덜 정밀한 시간 동기화가 필요하지 않다는 장점이 있다. 하지만, 동시에 2개의 주소가 활성화되어 있기 때문에 한 번의 공격이 성공할 경우 그 영향을 받는 피해는 2배로 증가하게 된다. 그림2는 공격 대상에서 활성화된 주소의 개수가 각각 1개, 2개일 때를 대상으로 노드의 버퍼 크기에 대한 공격의 강도 (메시지의 양)에 따른 전송 실패 확률을 비교한 것이다.

이를 통해 응답 기반 동기화 기법은 결과적으로 주소당 공격 성공 양이 늘어나게 되는 것을 알 수 있다.

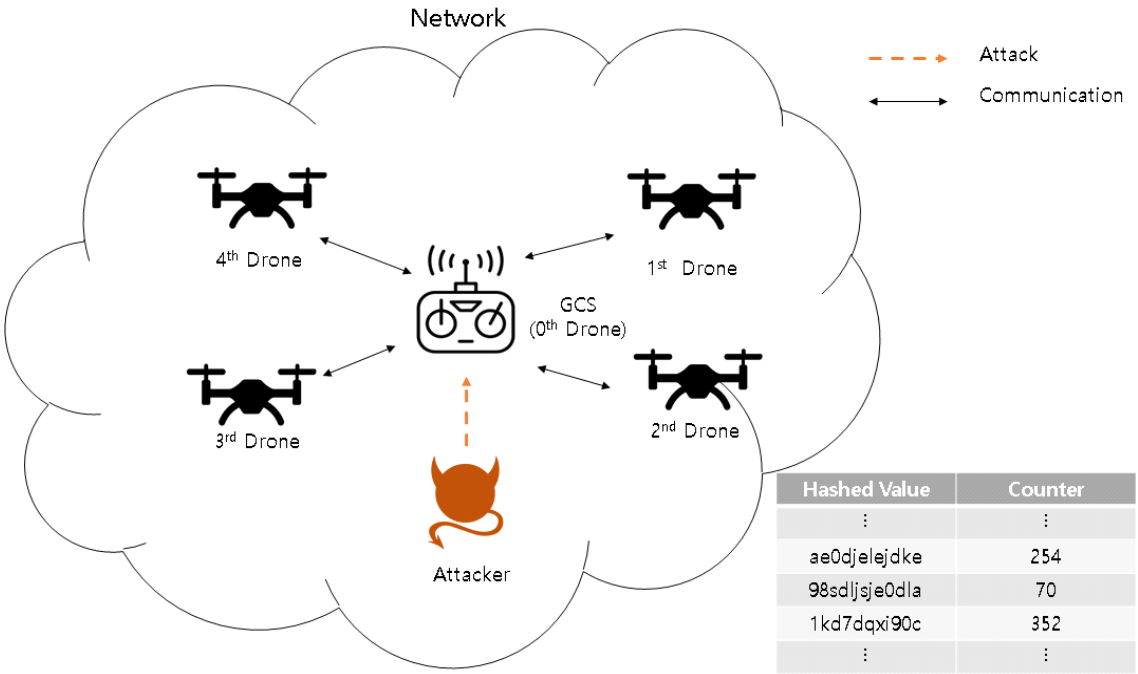

Fig. 3 System model of PHT algorithm

Ⅲ. PHT 알고리즘

PHT 알고리즘은 해시표를 사전에 배치하고, 해시값을 직접 송수신 하지 않고 카운터 (counter)라고 불리는 대체값을 사용한다.

3.1. 해시표 사전 배치 개념

드론은 비행체가 추락하거나 포획될 경우 내장 정보가 공격자에게 노출될 위험이 있다[11]. 본 논문에서 제안하는 PHT 기법은 그림3과 같이 해시값을 직접 노출시키지 않도록 해시표를 미리 배치하는 방법을 사용한다. 이를 위해 모든 드론과 지상통제국 (GCS, Ground Control Server)은 드론의 비행 전 동일한 암호화 키로 만들어진 암호화 해시표를 갖는다. 이 때문에 드론 비행 중에 키를 바꿀 필요가 없다. 드론 탈취 시에도 키를 직접 내장하지 않았기 때문에 공격자는 해시값을 역으로 산출 할 수 없게 된다.

따라서 해시표를 사전 배치함으로써, 키 분배 문제와 드론이 물리적으로 탈취되어 공격자가 키를 해독 하려는 tampering 공격 위험을 감소시킬 수 있다.

3.2. 해시값 대체용 카운터 생성

PHT에서 해시값 대신 카운터를 사용하는 이유는 다음과 같다. 첫째, 해시값을 노출 시키지 않기 위함이다. 무선 통신 특성상 공격자는 통신 내용을 감청할 수 있다. 이 때문에 해시값을 직접 사용하는 것은 PFS를 약화 시키는 요인이 된다. 둘째, 드론의 주소를 매번 변경함으로써 공격 대상을 특정하려는 시도를 무력화시키기 위함이다. 특히, 드론이 할당 받은 주소를 카운터를 이용하여 매번 변경함으로써 공격자는 변경된 주소를 알고 있지 않으면 공격 패킷은 전혀 다른 목적지로 전송되거나 파기된다. 대신 변경된 주소를 아는 정상 드론들은 수신한 카운터와 미리 받은 해시표를 참조하여 변경된 주소를 알 수 있다. 또한, 해시값 보다 짧은 비트열을 갖는 카운터 값을 사용하기 때문에 송수신 정보량이 감소하게 되기 때문에 드론과 같은 경량화 환경에 잘 맞는다. 이러한 카운터의 생성 방법은 식(1)과 같다.

$$counter = \left[\frac{\psi}{k+1}\right] \times x \tag{1}$$

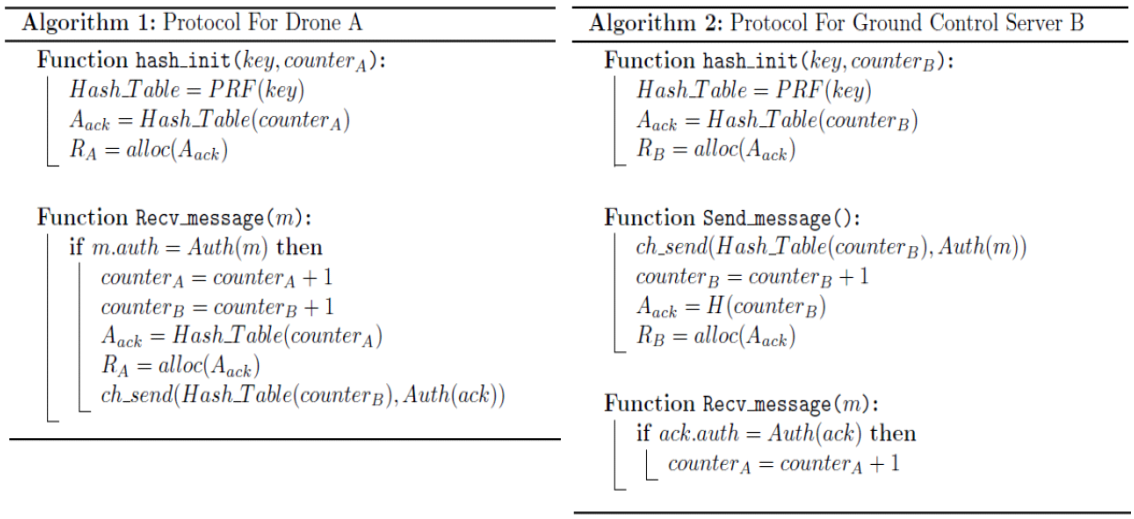

Fig. 4 Pseudo code of PHT algorithm. Algorithm 1: Protocol for a Drone. Algorithm 2: Protocol for GCS.

드론 네트워크에 가입한 각각의 드론들은 모두 자신의 순번을 가지고 있다. 임의의 드론의 순번이 x라면 네트워크에서 사용할 수 있는 주소의 개수 (ψ)를 네트워크에 가입된 드론의 개수 (k)와 지상통제국을 더한 값으로 나눈다. 여기에 자신의 순번 x를 곱하여 나온 값을 카운터라고 정의한다. 따라서 모든 드론과 지상통제국들은 카운터값을 이용해서 해당 해시표에 해당하는 값을 확인함으로써 수신된 메시지를 검증할 수 있게 된다.

여기에서 전체 주소의 값과, 네트워크에 가입된 드론의 수, 그리고 해당 드론의 순번은 공격자에게 알려져 있지 않기 때문에 공격자는 해당 정보를 얻기 어렵다. 또한, 카운터 값만을 가지고서는 공격자가 해시표의 값을 역산하기에도 어렵다.

3.3. 카운터와 해시표 매핑

PHT 기법을 사용하기 위한 전체적인 알고리즘이 그림4에 정리되어 있다. 카운터의 사용법은 다음과 같다. 먼저 그림3과 같이 한 개의 지상통제국과 여러 개의 드론이 연결된 드론 네트워크를 가정한다. 드론과 지상통제국은 사전에 해시표 각각 갖고 있다. 지상통제국은 전체 주소의 개수와 네트워크에 가입된 드론의 수를 각 드론에게 알려준다. 이때 지상통제국의 순번은 0으로 정한다.

그림4의 Algorithm 1은 임의의 드론 A에서 사용되는 알고리즘이다. hash_init(key, counterA)는 비행전 드론에 해시 데이블을 사전 배치 (Hash_Table)하고, 카운터 값을 통해 자신의 값 (Aack)을 찾아 응답값 (RA)를 만드는 단계이다.

Recv_message는 네트워크로부터 받은 메시지 (m)을 검증해서 해시테이블의 값과 일치하는지 여부를 판별한다. 그 값이 일치하면 수신된 메시지는 드론 네트워크에 가입된 합법적인 드론이라고 확인하게 된다. 또한, 동적으로 주소를 변경하기 위해 자신의 카운터와 지상통제국의 카운터 값을 1씩 증가 시킨다.[2] 이것은 해당 메시지를 정상적으로 수신했다는 의미이다.

예를 들어, 어떤 드론이 드론 A와 통신하고 싶다면 수식 (1)을 사용하여 드론 A의 카운터를 계산하고, 계산된 값을 사전에 받은 해시표에서 확인하여 드론 A의 주소를 확인 후 해당 주소로 메시지를 전송한다. 드론 A는 수신 받은 메시지에 있는 주소와 카운터가 일치하는지를 해시표를 통해 확인한다. 일치하면 자신이 가진 카운터를 1씩 증가시키고 응답 메시지를 지상통제국인 서버 B에게 전송한다.

그림4의 Algorithm 2는 지상통제국인 서버 B에서 사용되는 알고리즘이다. 응답 메시지를 수신한 지상통제

2) 카운터를 변경 시키는 값을 1 단위로 한 것은 구현을 용이하기 위함이다. 주파수 도약 방식과 같이 도약 값을 가변하는 방식도 적용 가능하다.

국 서버 B는 드론 A가 보낸 메시지의 카운터 값과 주소를 해시표를 이용하여 그 값을 검증한다. 앞에서와 마찬가지로 카운터 값에 따라 확인한 해시표의 값이 일치하면 응답 메시지가 드론 A로부터 온 것으로 신뢰할 수 있으므로 지상통제국 서버 B는 드론 A의 메시지를 신뢰하고 드론 A의 카운터 변경을 확인한다.

Ⅳ. 모의 실험 및 결과 분석

본 모의 실험에서는 그림3와 같은 드론 네트워크를 대상으로 한다. 성능 평가 기준은 암호화 해시 알고리즘의 키 사용량, 패킷 전송 성공률이다. 모의 실험은 Matlab을 이용하였고, 실험을 위한 값들과 파라메터들은 표1과 표2에 각각 정리하였다.

PHT 기법의 성능을 위한 분석 모델은 응답 기반 동기화 기법[10]을 활용하여 구성하였다.

Table. 1 Parameters and values for simulation

Parameter	Value
Max. number of addresses	65,536
Max. number of drones	20
Max, number of TX message for a drone	1

Table. 2 Parameters and meaning for simulation

Parameter	Meaning
$P_{success}$	Success Probability of TX packet
R	Buffer Size for receiving
a	Message Size for transmitting
C	Message Size for attacking
ψ	Number of address for available
k	Number of drone

4.1. 성능 분석 모델

본 논문에서는 드론 네트워크에서 암호키 탈취를 위한 공격이 발생했을 때 패킷 전송의 성공 확률 ($P_{success}$) 분석을 위해 [10]의 연구를 참고하였다. [10]에서는 사용 가능한 주소의 크기 (ψ)가 고정된 상태에서 송신 메시지의 양 (a), 각 주소에 대한 공격 메시지의 양 (C), 메시지의 수신 버퍼의 총 크기 (R)의 값을 변경하여 패킷 전송의 성공 확률을 구하였다.

PHT의 성능 분석을 위해, 본 논문에서는 드론 네트워크에 연결된 드론의 개수를 반영하도록 [10]의 수식을 보완하였다. 다음은 성능 분석에 사용된 수식들과 각 수식에 대한 설명이다.[3)]

공격자의 드론 네트워크에 대한 공격 환경 속에서 네트워크 MTD 기법의 성능은 패킷 전송에 대한 성공 확률로써 확인하다. 패킷 전송 성공 확률은 다음과 같이 정의된다.

$$P_{\text{success}} = \frac{RXPackets}{TXPackets} \tag{2}$$

먼저 분모 값인 송신된 패킷 (sent Packets)은 드론 네트워크에 보내진 패킷의 총합이다. 각 드론에 1개의 주소가 할당되고, 각 드론에 송신되는 메시지는 한 개의 패킷으로 구성되며 지상통제국을 제외하면, 드론 네트워크에 송신된 전체 패킷의 개수는 공격 패킷을 포함하여 $C+(\psi-k-1)$으로 나타낼 수 있다.

다음으로 분자 값은, 공격 패킷을 제외하고 네트워크에서 수용 가능한 패킷의 개수이다. 즉, 수신된 패킷이란 전체 네트워크에서 수용 가능한 최대 패킷의 개수를 의미한다. 수신 패킷의 값은 드론의 버퍼와 메시지의 크기에 따라 달라 질 수 있다. 우선 드론의 버퍼와 메시지의 크기가 같은 경우 (즉, $R=a$)를 살펴본다.

공격 메시지의 양이 드론 네트워크에서 가용한 트래픽보다 같거나 클 때의 전송 성공 확률은 수식 (3)과 같다.

$$P_{\text{success}} = \frac{(\psi-k-1)a}{C+(\psi-k-1)} \quad (C \geq \psi-k-1) \tag{3}$$

같은 조건에서 공격의 양이 드론 네트워크에서 수용 가능한 양보다 적은 경우의 전송 성공 확률은 수식 (4)와 같이 정리된다[10].

$$P_{\text{success}} = 1 - \frac{C}{(\psi-1-k)(1+a)} \quad (C < \psi-k-1) \tag{4}$$

이번에는 드론의 수신 버퍼의 크기가 메시지의 크기

3) [10]에서는 임의의 노드에 대한 포트 스캐닝 공격 상황에서 패킷 전송 확률을 유도하였다. 본 논문의 식(3)~(7)은 [10]의 결과를 사용한다.

양보다 큰 경우 ($R > a$)를 알아보자. 이때에는 수신 버퍼가 메시지의 양보다 크기 때문에 공격이 효율적으로 이뤄지기 위해서는 사용자들의 전송 성공 확률을 기준으로 공격량을 선정해야 한다. 따라서 유효 공격량 ($C_{effective}$)을 전송 성공 확률의 최소값으로부터 유도한 값을 사용한다[10].

$$C_{effective} = \frac{(\psi - k - 1)a}{\sqrt{\frac{R}{R-a} - 1}} \tag{5}$$

따라서, 수신 버퍼가 메시지의 양보다 큰 경우, 공격의 양이 유효 공격량 보다 적은 경우의 전송 성공 확률은 수식 (6)과 같다.[4)]

$$P_{success} = \frac{(\psi - k - 1)a - C(\sqrt{\frac{R}{R-a}} - 1)}{(\psi - k - 1)a} + \frac{R}{(\psi - k - 1)} \frac{C(\sqrt{\frac{R}{R-a}} - 1)^2}{a^2 \sqrt{\frac{R}{R-a}}}, \tag{6}$$
$$(R > a, \quad C < C_{effective})$$

같은 조건에서 유효 공격량 보다 많은 공격이 이뤄지는 경우의 전송 성공 확률은 수식 (7)과 같다.

$$P_{success} = \frac{(\psi - k - 1)R}{C + (\psi - k - 1)a}, \tag{7}$$
$$(R > a, \quad C \geq C_{effective})$$

4.2. 키 사용량 비교

먼저 암호화 해시 알고리즘의 키 사용량을 비교한다. 키 사용량을 비교하는 이유는, 드론 네트워크의 보안성 수준과 키의 사용량 사이에 연관성이 있기 때문이다. 즉, 공격자가 드론 네트워크에서 획득한 정보를 바탕으로 키를 유추할 것을 대비해 키를 주기적으로 변경하면 그만큼 키를 유추하는 것이 어려워지게 된다. 공격자가 키를 유추하는 것이 어려워지면 그만큼 키를 변경해야 할 주기가 늘어나기 때문에 드론 네트워크의 보안성이 향상되는 것이다. 따라서, 본 논문에서는 키 사용량을 통해 드론 네트워크의 보안성을 평가한다.

이를 구현하기 위해, 응답 기반 동기화 기법에서는 단위 시간 Δ에 대해 전송 시작부터 키 계산이 될 때까지의 시간을 500Δ라 가정하고 이 시간이 지나면 자동으로 키를 변경하는 것으로 가정하였다.[5)] 하지만 해시값이 직접 노출되지 않는 PHT의 경우에는 주기적으로 키를 변경할 필요가 없으므로, 공격 패킷량이 증가하여 전송 성공률이 90% 이하로 감소하는 경우 키를 강제로 교체하는 것으로 가정하였다.

그림5는 응답 기반 동기화 기법과 PHT를 사용했을 때 드론 운영 시간에 따른 키 사용량을 비교한 것이다. 모의 실험 결과, PHT를 사용하는 경우 주기적으로 키를 교체하는 [10]기법 보다 월등히 키 사용량이 감소되었음을 확인할 수 있다. PHT에서는 공격자가 무선 통신에서 해시값을 구할 수 없을 뿐 아니라, 획득한 정보를 이용하더라도 실제 해시표를 추론할 수 없기 때문에 그만큼 키 사용 시간이 늘어난다.

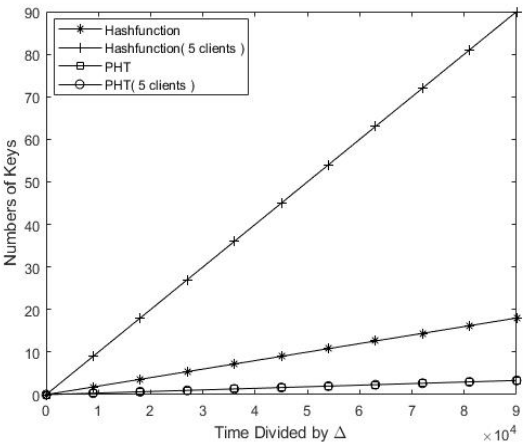

Fig. 5 Comparison of key usage between the hash function and the PHT algorithm for a drone network.

4.3. 드론 개수에 따른 전송 성공 확률

그림6은 응답기반 동기화 방식과 PHT를 사용했을 경우, 드론 네트워크에 가입된 드론 수의 변경에 따른 전송 성공 확률을 나타낸 것이다.

모의 실험 결과, PHT 기법이 응답 기반 동기화 기법에 비해 패킷 전송 성공 확률이 더 증가하는 것으로 나

4) 유효 공격량 보다 적은 공격이 발생하여도 전송이 실패할 수 있기에 성능 분석 모델에 포함한다.

5) 암호화 해시 알고리즘에 따라 키를 구할 수 있는 시간이 다르겠지만 본 연구에서는 경량 드론의 비행 시간(약 1200초)과 생일 패러독스를 고려하여 암호키 해독에 필요한 시간을 600초 미만을 가정하였다.

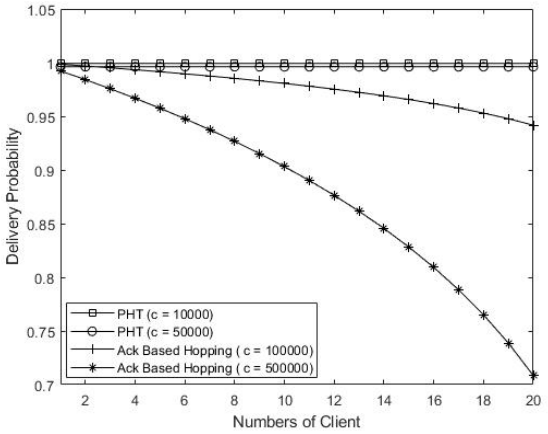

Fig. 6 Comparison of TX success probability for increasing the number of drones

타났다. 또한, 공격의 양이 5배 증가하였을 때에도 PHT에서의 전송 성공 확률은 큰 변화가 없지만, [10]에서는 전송 성공 확률이 급격하게 감소함을 알 수 있다.

이것은 PHT에서 드론의 주소가 카운터 변경을 통해 동적으로 변함으로써 공격자가 정확한 공격양을 예측하기 어려워지므로, PHT에서는 전송 성공 확률이 드론의 개수와 무관하게 높은 값을 유지할 수 있기 때문이다.

Ⅴ. 결 론

본 논문에서는 드론 네트워크의 보안성 향상을 위해 드론의 주소를 동적으로 변경하기 위한 네트워크 MTD 기법을 드론 네트워크에 적용하는 방안을 연구하였다.

본 논문에서 제안한 드론 네트워크를 위한 PHT 알고리즘은 무선통신 기반의 드론 네트워크 환경을 고려하여 해시값의 직접적인 노출 위협을 감소시키기 위해 해시표를 사전 배치하고 카운터로 대체하였다. 이로써 공격자가 키 해독을 더욱 어렵게 되었고 암호화 해시 알고리즘의 키 사용 시간을 연장하는 결과를 제공한다. 또한 키의 교환이 이뤄지지 않으므로 일대다 환경에서 키 관리의 편의성을 제공한다.

모의 실험을 통해 드론 네트워크의 무선 통신 환경에서 PHT의 성능을 확인함으로써, PHT 기법을 드론 네트워크에 적용시 보다 보안성을 향상 시킬 수 있음을 확인하였다.

ACKNOWLEDGEMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2016R1A2A1A05005541).

REFERENCES

[1] M. S. Hyun, K. H. Choi, and J. H. Kim, “Development of Simulation and Test-Bed for Searching Missing People Using Multi-Drone Simulator and LoRa Sensor Network,” *The Journal of Korean Institute of Communications and Information Sciences*, vol. 43, no. 11, pp. 1941-1951, Nov. 2018.

[2] N. Jadeja, and V. Parmar, “Implementation and Mitigation of Various Tools for Pass the Hash Attack,” *Procedia Computer Science*, vol. 79, pp. 755-764, Mar. 2016.

[3] C. Gudla, S. Rana, and A. H. Sung, “Defense Techniques Against Cyber Attacks on Unmanned Aerial Vehicles,” *International Conference Embedded Systems, Cyber-Physical Systms & Applications*. New York, Oct. 2018.

[4] K. Driscoll, “Lightweight crypto for lightweight unmanned arial systems,” *Integrated Communications, Navigation, Surveillance Conference (ICNS)*, 2018.

[5] G. C. Wang, B. S. Lee, K. J. Lim, and J. Y. Ahn, “Technical Trends on Security of Control and Non-Payload Communications Network for Unmanned Aircraft Systems,” *Electronics and Telecommunications Trends*, ETRI, 2017.

[6] H. Okhravi, T. Hobson, D. Bigelow, and W. Streilein, “Finding focus in the blur of moving-target techniques,” *IEEE Security & Privacy*, pp. 16-26, Nov. 2013.

[7] H. Lee, and V. Thing, “Port Hopping for Resilient Networks,” *60th IEEE Vehicular Technology Conference*, pp. 3291- 3295, Sept. 2004.

[8] M. Dunlop, S. Groat, W. Urbanski, R. Marchany, and J. Tront, “MT6D: A Moving Target IPv6 Defense,” *IEEE Military Communications Conference*, pp. 1321-1326, Nov. 2011.

[9] Y. B. Luo, B. S. Wang, X. F. Wang, X. F. Hu, and G. L. Cai, “RPAH: Random port and address hopping for thwarting internal and external adversaries,” *Trustcom/Big-DataSE/ISPA*, vol. 1, 2015.

[10] G. Badishi, A. Herzberg, and K. Idit, “Keeping Denial-

of-Service Attackers in the Dark," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 3, pp. 191-204, Aug. 2007.

[11] K. Hartmann, and C. Steup, "The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment," *5th International Conference on Cyber Conflict*, 2013.

임성민(Sung-min Leem)

2019년 2월 : 아주대학교 국방디지털융합학과 학사
※ 관심분야 : 정보보호, 통신공학

이민우(Minwoo Lee)

1998년 3월 : 한국항공대학교 항공통신정보공학과 학사
2013년 2월 : 아주대학교 NCW공학 박사
2017년 1월 : 국군사이버사령부 핵심기술연구팀장
2019년 3월 : 아주대학교 국방디지털융합학과 대우교수
※ 관심분야 : 사이버전, 위성통신, 국방무기체계보안

임재성(Jaesung Lim)

1983년 2월 : 아주대학교 전자공학 학사
1985년 2월 : KAIST 영상통신석사
1994년 2월 : KAIST 디지털통신 박사
1998년 3월~현재:아주대학교 소프트웨어학과 정교수
2004년 3월~현재:아주대학교 국방전술네트워크 연구센터장
2015년 3월~현재:아주대학교 국방디지털융합학과 학과장
※ 관심분야 : 드론 네트워크, 국방전술통신, 전술데이터링크