Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.1, Feb. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.1.11

IoD 환경에서 MEC를 활용한 U2U 인증에서 보안 취약점 분석*

최 재 현,[1†] 이 상 훈,[2] 정 익 래,[3] 변 진 욱[4‡]
[1,3]고려대학교 (대학원생, 교수), [2]삼성 SDS, [4]평택대학교 (교수)

Analysis of Security Vulnerability in U2U Authentication Using MEC in IoD Environment*

Jae Hyun Choi,[1†] Sang Hoon Lee,[2] Ik Rae Jeong,[3] Jin Wook Byun[4‡]
[1,3]Korea University (Graduate student, Professor),
[2]Samsung SDS, [4]Pyeongtaek University(Professor)

요 약

최근 사물인터넷(IoT)의 발달과 드론을 활용한 서비스의 증가로 인해 IoD에 대한 연구가 활발히 진행 중이다. 드론은 연산능력이 약하고 저장소의 크기가 작은 자원적인 한계를 갖고 있으며 드론 간 통신 시 정당한 개체 간 인증을 거친 후 데이터를 주고받는다. 드론은 위치, 이동 경로와 같은 민감 정보를 포함하기 때문에 추적성으로부터 안전해야 한다. 본 논문에서는 기존 IoD 연구에서 가명 및 인증서 사용으로 발생할 수 있는 치명적인 보안 취약점을 지적하고 해결책을 제안한다.

ABSTRACT

Due to the recent development of the Internet of Things (IoT) and the increase in services using drones, research on IoD is actively underway. Drones have limited computational power and storage size, and when communicating between drones, data is exchanged after proper authentication between entities. Drones must be secure from traceability because they contain sensitive information such as location and travel path. In this paper, we point out a fatal security vulnerability that can be caused by the use of pseudonyms and certificates in existing IoD research and propose a solution.

Keywords: Internet of Drone, MEC, Authentication, Pseudonym

I. 서 론

최근 항공기술의 발달로 무인 항공기, UAV (Unmanned Aerial Vehicle)에 대한 관심이 전 세계적으로 증가하고 있다. UAV는 레저용 드론, 산업용 드론, 화재 상황 등 안전문제로 인해 사람이 접근하기 힘든 장소에 투입되는 재해용 드론 등이 있다[1][2]. 드론을 통해 데이터를 주고받는 과정에서 정당한 대상만 드론과 데이터를 교환해야 한다. 따라서 드론과의 상호 인증을 마친 후 비밀통신을 형성하는 것이 중요한 보안 요구사항이다. 그러나 현실적으로 드론의 연산능력, 저장소 크기 등 안전한 통신 채널을 형성하는 과정에 한계가 존재한다.

IoD(Internet of Drone)에 관하여 드론의 제한된 자원을 가진 환경에서 보안을 보장하기 위한 연구는 활발히 진행되고 있다. 그 중 Tian et al.[3]

Received(11. 06. 2020), Modified(01. 27. 2021), Accepted(01. 27. 2021)
* 이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구 임 (No. 2020R1F1A1065434).
† 주저자, 93jamie@korea.ac.kr
‡ 교신저자, jwbyun@ptu.ac.kr(Corresponding author)

은 IoD의 인증 및 보안 문제를 해결하기 위해 MEC(Mobile Edge Computing)[4]의 도움을 받아 효율적인 개인정보 보호 인증 체계를 제안했다. MEC를 사용한 개인정보 보호 인증 체계는 빠른 인증, 부인 방지 및 조건부 개인정보 보호를 보장한다. 온/오프라인 서명 체계[5]를 보완하여 IoD에서 각 UAV의 개인정보를 보호하는 UAV의 가명 및 서명 키의 비대화형 업데이트를 제공한다.

본 논문에서 Tian et al.의 연구는 인증기관으로부터 인증서를 받지 않은 공개키 사용, 공개키 간 연결가능성으로 인한 추적 가능한 문제 등 보안 문제를 지적하고 해결책을 제시한다.

II. 배경 지식

2.1 MEC(Mobile Edge Computing)

MEC는 사용자에게 네트워크 에지에서 분산 클라우드 컴퓨팅 기능과 IT 서비스를 제공한다. 특히 응용 애플리케이션에 대해 낮은 지연과 대용량의 대역폭을 제공하고 실시간으로 네트워크 정보 접근이 가능하도록 한다. 클라우드 컴퓨팅과 비교하여 MEC는 사용자의 네트워크 지연율을 크게 줄여 효율적인 네트워크 서비스 제공을 보장한다.

2.2 온/오프라인 서명 체계

온/오프라인 서명[6]은 Even et al.에 의해 처음 제안된 서명 체계이다. 서명 생성 과정에서 온라인, 오프라인 단계로 나누어 진행한다. 오프라인 단계는 서명할 메시지가 주어지기 전에 수행되며 상대적으로 연산 비용이 큰 과정이고 결과로 얻은 값은 중간값으로써 저장된다. 메시지가 주어진 이후, 온라인 단계가 수행된다. 오프라인 단계에서 수행된 값을 사용하여 간단하게 이뤄진다. 온라인 단계는 일반적으로 단순한 연산과정이어서 연산력이 약한 프로세서에서 효율적으로 사용된다.

2.3 Tian et al.의 연구

이 장에서는 Table 1을 통해 Tian et al.의 연구에서 정의하는 표기를 설명하고 Tian et al.에서 제안하는 모델에 대하여 설명한다.

Table 1. Summary of notation at Tian et al.

Notation	Definition
V_i	the ith UAV
R_j	the jth MEC
$Sig_{V_i}(.), Sig_{R_j}(.)$	the signature of the ith UAV and the jth MEC
$cert_{V_i}, cert_{R_j}$	the certificate of the ith UAV and the jth MEC
tpk, tsk	the public and private key of the TA
vpk_i, vsk_i	the public and private key of the ith UAV
spk_j, ssk_j	the public and private key of the jth MEC for signature
epk_j, esk_j	the public and private key of the jth MEC for dec/encryption
id_j	the id of the jth MEC
$pid_{i,k}$	the kth pseudonym of the ith UAV
$VT_{i,k}$	the valid time period of $pid_{i,k}$
T, T_{expire}	the current and expiration timestamp
r_{V_i}, r_{R_j}	the nonce generated by V_i, R_j
UTR	update trigger time range
PBL	public broadcast list
FL	forwarding list
EAT	the estimated arrival time of V_i to neighbor MEC

2.3.1 시스템 모델

Tian et al.가 제안하는 모델은 〈Fig. 1.〉처럼 3가지 개체 (TA, MEC, UAV)로 구성되며, TA와 MEC는 완전히 신뢰하는 개체로 가정한다. TA는 등록을 희망하는 MEC와 UAV에게 인증서를 발급한다. IoD에서 통신하는 동안 각 UAV의 신원은 보호된다. 그러나 TA는 UAV가 이상 행동을 할 때 실제 신원을 공개할 수 있다. MEC는 UAV 간 효율적인 통신을 지원하고 TA 및 각 MEC는 서로 안전한 채널을 형성하고 있다.

IoD 네트워크에 대한 위협은 크게 내부, 외부 공격자로 나눈다. 내부의 공격자는 가짜 정보를 전송하거나 오작동을 일으키는 악의적인 UAV이다. 외부의 공격자는 통신을 도청하거나 위변조할 수 있다. 공격

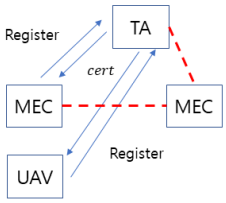

Fig. 1. System architecture

자는 IoD 네트워크에 정당한 UAV로 등록 가능하며 정당한 신원을 이용하여 다른 유효한 개체와 통신할 수 있다. 공격자는 공격대상이 될 UAV의 신원을 파악하고 비행경로 및 위치를 추적하려 한다.

2.3.2 세부 구조

Tian et al.에서 제안하는 모델은 크게 4가지 단계로 구성된다. 각 단계에 대한 설명은 다음과 같다.

(1) 시스템 초기화 : TA가 보안 매개변수를 선정하고 UAV와 MEC를 등록하는 단계이다. 보안 매개변수 λ가 주어지면 TA는 소수 p,q와 $g \in Z_p^*$ 그리고 해시함수 $h_1, h_2 \rightarrow Z_q^*$를 선택한다. TA는 인증기관 역할 수행을 위해 공개키, 개인키 쌍 (tpk, tsk)를 생성한다. 이후 IoD의 공개 정보로써 $\{p,q,g,h_1,h_2,tpk\}$를 게시한다. IoD에 참여 요청하는 MEC(R_j)에 대해 TA는 서명키 쌍 (spk_j, ssk_j)와 암호화 키 쌍 (epk_j, esk_j)를 생성하고 각 키 쌍에 해당하는 인증서 $cert_{R_j}(id_j \| spk_j \| epk_j)$를 발급한다. UAV($V_i$)는 등록 과정에서 키 쌍 $vsk_i = \alpha_i \in Z_q^*, vpk_i = g^{-\alpha_i}$와 오프라인 서명 (r, dr)을 생성한다. 이때, r은 난수이며, $d = h_2(g^r \bmod p)$이다. 이후에 V_i는 오프라인 서명을 활용하여 메시지에 신속하게 온라인 서명을 할 수 있다. V_i는 TA가 서명한 인증서 $cert_{V_i} = cert\{vpk_i \| (pid_{i,1}, VT_{i,1}) \| ... \| (pid_{i,k}, VT_{i,k})\}$를 얻는다. 이 과정에서 TA는 필요 시 추적하기 위해 각 UAV의 실제 신원과 가명 쌍을 저장하고 관리한다.

(2) IoD 합류 : 해당 과정은 〈Fig. 2.〉에서 보듯 Level 1, Level 2가 존재한다. Level 1은 등록단계로써 메시지를 받거나 보내려는 모든 UAV가 수행한다. UAV가 IoD 네트워크에 참여하기로 하면 인근 MEC가 브로드캐스트하는 최신 인증정보를 확인한다. MEC가 브로드캐스트하는 내용은 MEC의 신원, 현재 타임스탬프 및 만료 기간, 공개키 및 인증서, 난수, 공개 브로드캐스트 목록(PBL) 그리고 서명이다. UAV는 TA의 공개키 tpk를 이용하여 MEC가 브로드캐스트하는 내용을 검증한다. Level 2에서는 UAV(V_i)가 MEC에게 Join 요청을 전송한다. 이 요청은 Level 1에서 획득한 epk_j로 암호화된다. 요청 내의 메시지에는 현재 타임스탬프와 만료기간, 난수 r_{V_i}, UAV의 위치와 업데이트 트리거 시간 범위(UTR) 등을 포함한다. MEC는 암호화되어 전달된 vpk_i를 활용하여 $vpk_{i,1}$을 계산하고 PBL에 $(pid_{i,1}, vpk_{i,1})$쌍을 업데이트하고, V_i는 $vsk_{i,1}$를 계산한다. 이후 MEC가 브로드캐스트하는 난수 r_{R_j}'를 사용하여 UAV는 키 쌍을 $vsk_{i,2} = vsk_{i,1} - r_{R_j}'$, $vpk_{i,2} = vpk_{i,1} \cdot g^{r_{R_j}'}$로 업데이트 한다.

(3) 빠른 U2U 통신 인증 : UAV 간 통신에서 빠른 인증을 지원하기 위해 각 MEC는 자신의 통신 범위에 존재하는 IoD Join을 마친 UAV의 $(pid_{i,k}, vpk_{i,k})$을 PBL을 통해 유지하고 브로드캐스트 한다. PBL은 IoD Join의 Level 2 과정으로 업데이트되거나, R_j의 이웃 MEC로부터 전달 목록(FL)을 받아 형성된다. FL은 $\{(pid_{i,1}, VT_{i,1}) \| ... \| (pid_{i,k}, VT_{i,k}), vpk_{i,k}, EAT\}$ 이고 $pid_{i,k}, vpk_{i,k}, VT_{i,k}$는 UAV($V_i$)의 k번째에 해당하는 가명, 공개키, 유효시간이다. EAT는 UAV(V_i)가 이웃 MEC의 적용 범위로 이동하는데 예상되는 소요시간이다. 빠른 인증을 수행하기 위해 발신자 UAV는 사전에 계산해 두었던 오프라인 서명을 기반으로 온라인 서명 $(d,z), z = dr + vsk_{i,k} h_1(m)$을 계산한다. 이때 메시지 $m = (T, T_{expire}, pid_{i,k}, content)$이다. 수신자 UAV는 MEC가 브로드캐스트한 PBL에서 송신자 UAV의 $pid_{i,k}$를 토대로 $vpk_{i,k}$를 찾아 온라인 서명 검증에 사용하며 서명 검증 과정은 다음과 같다.

- 서명 검증 : 메시지 m에 대한 서명 (d,z)가 주어지고 $vpk_{i,k}$로 검증식 $d = h_2(g^{z d^{-1}} vpk_{i,k}^{d^{-1} h_1(m)})$를 만족하면 V_i의 정당한 서명으로 간주한다.

(4) 가명 및 키 업데이트 : 공격자가 가명 및 공개키를 통해 UAV를 식별하고 추적하는 것을 방지하기 위해 각 UAV는 가명 및 서명키를 주기적으로 업데이트한다. UAV는 IoD Join 과정에서 MEC와 합의된 UTR이 존재한다. $VT_{i,k}$와 현재 시간의 차이가 UTR보다 작을 때 수행된다. 이후 PBL의 가명과 서명 검증키가 $pid_{i,k+1}$, $vpk_{i,k+1}$로 업데이트 된다.

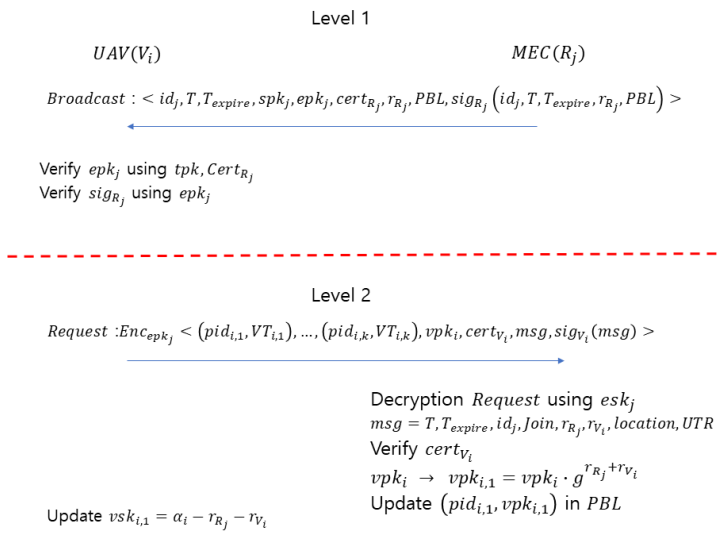

Fig. 2. IoD Join

서명키 업데이트 과정은 다음과 같다.

● 실시간 서명키 업데이트 : 가명과 서명키 업데이트가 실행되면 MEC는 새로운 난수 r'_{R_j}를 브로드캐스트 하고 V_i의 현재의 공개키 $vpk_{i,k}$를 $vpk_{i,k+1} = vpk_{i,k} \cdot g^{r'_{R_j}} \bmod p$로 업데이트한다. UAV는 MEC가 브로드캐스트한 난수 r'_{R_j}를 사용하여 현재의 개인키 $vsk_{i,k}$를 $vsk_{i,k+1} = vsk_{i,k} - r^{'R_j}$으로 업데이트한다.

III. 취약점 분석

Tian et al.은 IoD 환경에서 MEC를 활용하여 프라이버시를 유지하면서 빠른 인증이 가능한 프레임워크를 제안한다. 그러나 해당 연구는 보안 취약점이 존재한다. 이번 장에서는 Tian et al.의 연구에서 찾을 수 있는 보안 취약점을 제시한다.

3.1 인증받지 않은 공개키 사용

IoD Join 단계에서 MEC는 등록되는 UAV(V_i)의 인증서를 검증하고 PBL에 vpk_i를 활용하여 $(pid_{i,1}, vpk_{i,1})$쌍을 업데이트한다. 다음 UTR 전까지 $vpk_{i,1}$은 UAV(V_i)의 공개키로 사용이 된다. 그러나 공개키 $vpk_{i,1}$는 인증기관으로부터 인증서가 발행되지 않은 공개키이다. 즉 $vpk_{i,1}$에 대하여 V_i의 가명 $pid_{i,1}$에 해당하는 정당한 공개키라고 판단할 수 없다. 이후 UTR에 따라 MEC는 난수 r'_{R_j}을 사용하여 $vpk_{i,1}$를 $vpk_{i,2}$로 업데이트한다. $vpk_{i,2}$ 역시 MEC를 통해 $vpk_{i,2}$의 업데이트가 이루어지고 인증기관의 인증서를 발급받지 않았다. MEC가 임의로 생성한 난수를 기반으로 업데이트한 UAV(V_i)의 공개키 $vpk_{i,k}$는 인증기관으로부터 정당한 V_i의 k번째 공개키라는 인증서가 존재하지 않는다. 일반적으로 PKI(Public Key Infrastructure)에서 공개키는 인증기관에 등록을 마친 후 인증기관으로부터 인증서를 발급받아 사용하는 구조다. 따라서 인증서가 존재하지 않는 $vpk_{i,k}$는 UAV(V_i)의 가명 $pid_{i,k}$에 대응하는 공개키라고 신뢰할 수 없는 문제가 발생한다.

이동 경로, 위치 등 민감 정보를 포함하는 UAV에 대해 추적성에 대한 문제를 해결하고자 가명과 각 가명에 대응하는 공개키를 갱신하여 사용하였으나 공개키에 대한 인증서가 존재하지 않아 보안적 취약점이 발생한다. 추적성에 대하여 안전하면서 인증서가 포함된 공개키를 사용하기 위해서는 각 가명 및 이에 대응하는 공개키를 인증기관으로부터 받은 익명인증서와 함께 사용해야 한다. 그러나 Tian et al.의 연구에서 가명 및 공개키에 대한 인증서는 인증기관으로부터 발급받은 인증서가 아니기 때문에 각 인증서에 대응된 공개키를 정당한 공개키라고 신뢰할 수 없고 인증과정에서 공개키를 인증요소로 활용할 수 없다.

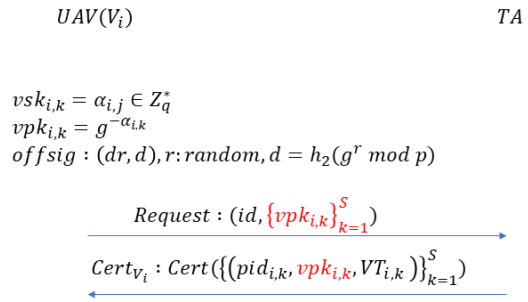

Fig. 3. Proposed UAV update

3.2 공개키 간 연결가능성

드론은 이동 경로, 위치와 같은 민감 정보를 다루기 때문에 추적성으로부터 안전해야 한다. Tian et al.이 제안한 모델에서 공격자의 UAV 추적을 방지하기 위해 가명을 사용하고 이에 대응하는 공개키를 가명과 함께 주기적으로 업데이트한다. MEC는 영역에 포함된 UAV의 UTR에 따라 공개키를 업데이트하기 위해 난수 r'_{R_j}를 생성하고 브로드캐스트 한다. 악의적인 공격자는 공격 대상 UAV가 소속된 MEC가 브로드캐스트하는 내용을 관찰하여 모든 공개키와 업데이트에 사용되는 난수 쌍을 얻을 수 있다. 이 과정에서 공격자는 추적 대상 UAV의 s번째 공개키 $vpk_{i,s}$와 브로드캐스트 하는 난수 r'_{R_j}를 사용하여 다음 공개키 $vpk_{i,s+1} = vpk_{i,s} \cdot g^{r'_{R_j}}$를 계산할 수 있다. 이는 추적성과 관련한 보안문제를 일으킨다. 추적성을 방지하기 위해 Tian et al.는 UAV의 가명을 사용하였으나 각 가명과 쌍을 이루는 공개키는 연결가능성을 갖는다. 따라서 UAV의 가명 사용여부와 관계없이 공격자는 공개키만을 이용하여 특정 UAV를 추적할 수 있어서 Tian et al.이 제안한 프레임워크는 추적성에 대한 보안을 기대할 수 없다.

마찬가지로 만약 공격자가 UAV(V_i)의 s번째 개인키를 알아낼 경우 큰 보안문제가 발생할 수 있다. 공개키 $vpk_{i,s}(=g_{i,s}^{-vsk_{i,s}} \bmod p)$에 대응하는 개인키는 $vsk_{i,s}$이다. 이후 업데이트 된 $vpk_{i,s+1}$에 대응하는 개인키를 $vsk_{i,s+1} = vsk_{i,s} - r'_{R_j}$ 과정을 통해 얻을 수 있다. 즉, $vsk_{i,s+1}$을 생성할 때 사용되는 이전 개인키 $vsk_{i,s}$와 브로드캐스트 되는 난수 r'_{R_j}를 모두 공격자가 알게 된다. 일반성을 잃지 않고 $vsk_{i,s}$ 이전에 브로드캐스트 된 난수 값을 모두 저장하고 있었다면 이전까지 사용되었던 개인키 $\{vsk_{i,k}\}_{k=1}^{s-1}$ 모두에 대한 정보도 쉽게 복원 가능하다.

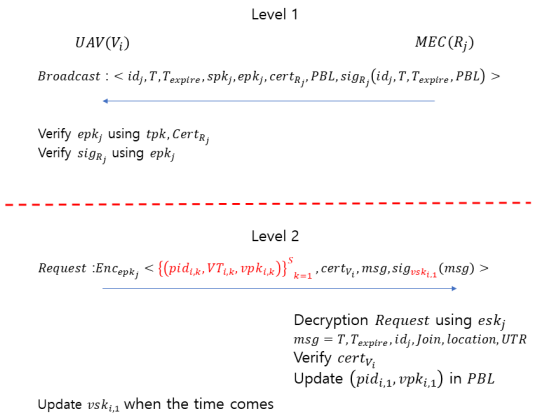

Fig. 4. Proposed IoD join

이는 현재의 사용 중인 개인키가 노출되더라도 이전에 사용되었던 혹은 이후의 사용될 개인키가 노출되지 않아야 하는 완전 기밀성(perfect secrecy)을 위반하는 것이다. 완전 기밀성이 위배될 경우 공격자는 모든 공개키에 해당하는 개인키를 복구 가능하기 때문에 모든 공개키에 대한 임의의 위조 서명을 생성할 수 있다. 따라서 각 공개키, 개인키 쌍에 대한 완전 기밀성을 유지하면서 키 쌍을 업데이트하는 방법이 필요하다.

IV. 대처 방안

본 논문에서 지적한 바에 따르면, Tian et al.이 제안한 프레임워크는 크게 두 가지 보안문제가 발생한다. 인증받지 않은 인증서의 사용과 공개키간 연결가능성이 발생하여 가명을 사용함에도 불구하고 추적이 가능하다. 두 가지 보안문제를 해결하기 위해 가명과 이에 대응하는 공개키를 사용하더라도 공개키에 대한 신뢰도를 갖기 위해 인증기관으로부터 발급받은 인증서를 사용해야 한다. 또한 추적 불가능성을 갖기 위해 각 유효시간에 사용하는 가명 및 공개키에 대해 연결가능성이 존재하지 않아야 한다.

기존 시스템 초기화 과정의 각 UAV는 등록 단계에서 1개의 개인키 및 공개키 쌍을 생성한 후 TA에 등록한다. 그러나 본 논문에서 제안하는 대응 방안은 〈Fig. 3.〉에서 보듯 각 UAV는 여러(S)개의 개인키 및 공개키 쌍을 생성하여 등록과정 진행 시 모든 키 쌍을 등록한다. TA는 UAV에게 등록한 S개의 공개키에 대응하는 가명이 포함된 인증서 $Cert_{V_i}$를 발급

해준다. 이후 Tian et al이 제안한 방법은 IoD 합류 과정에서 가명 및 공개키를 업데이트 하기 위해 MEC가 난수를 생성 후 브로드캐스트 하였으나 본 논문의 대응 방안에서는 UAV가 유효시간과 함께 사용될 공개키값들($\{vsk_{i,k}\}_{k=1}^{S}$)을 미리 생성해 두었기 때문에 MEC로부터 업데이트에 사용되는 인자를 받지 않는다. 〈Fig. 4.〉에서 보듯 MEC는 IoD 합류 단계의 Level 2에서 각 UAV의 합류 요청 시 V_i의 가명, 유효시간, 공개키 쌍을 전달한다($\{pid_{i,k}, VT_{i,k}, vpk_{i,k}\}_{k=1}^{S}$). 이 값을 기반으로 MEC는 각 UAV의 유효시간이 지날 때 마다 가명과 공개키를 업데이트한다.

본 논문에서 제안하는 대처 방안을 사용하는 경우 인증기관으로부터 발급받은 인증서를 사용하기 때문에 인증서에 대한 신뢰도가 있다. 또한 UAV가 생성한 난수를 기반으로 각 가명 및 유효시간에 대응하는 공개키 개인키 쌍을 만들기 때문에 각 공개키간 연결가능성이 존재하지 않아 추적성으로부터 안전하다.

V. 결 론

최근 드론에 대한 사용과 활용범위가 증가함에 따라 효율적으로 드론을 운용하는 연구가 진행되고 있다. Tian et al.의 연구는 IoD 환경에서 MEC를 활용하여 UAV의 연산 부담을 줄이고 UAV간 빠른 인증을 지원한다. 위치, 경로 정보와 같은 민감정보 노출로부터 안전하기 위해 UAV 운용 시 가명을 사용하여 프라이버시를 보장하는 방안을 제안했다.

본 논문에서는 Tian et al.이 수행한 연구가 인증기관으로부터 인증서를 발급받지 않은 공개키를 사용함으로 인한 공개키에 대한 신뢰성의 문제를 지적했다. 또한 가명과 함께 사용되는 공개키들 사이의 연결가능성을 보여 기존 연구가 가명 사용에도 불구하고 추적성에 대하여 안전하지 않음을 보였다. 나아가 가명과 함께 사용되는 공개키에 대응하는 개인키가 한번 노출될 경우 노출 당시 상황 이전, 이후의 개인키가 모두 노출되기 때문에 완전 기밀성에 위배되는 것을 보였다.

본 논문에서는 Tian et al.에서 발생한 취약점에 대해서 UAV의 저장공간을 사용하더라도 인증기관으로부터 발급받은 인증서를 사용한다. 그리고 각 가명 및 공개키가 UAV와의 연결불가능성을 가지면서 공격자의 추적으로부터 안전한 해결책을 제안했다.

References

[1] T. Tomic, K. Schmid, P. Lutz, A. Domel, M. Kassecker, E. Mair, I.L. Grixa, F. Ruess, M. Suppa and D. Burschka," Toward a fully autonomous UAV: research platform for indoor and outdoor urban search and rescue," IEEE robotics & automation magazine, vol. 19, no. 3, pp. 46-56, Sep. 2012.

[2] L. Merino, F. Caballero, J.R. Martinez-de-Dios, I. Maza and A.Ollero, "An unmanned aircraft system for automatic forest fire monitoring and measurement," Journal of Intelligent & Robotic Systems, vol. 65, no. 1, pp. 533-548, Aug. 2011.

[3] Y. Tien, J. Yuan and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted internet of drones," Journal of Information Security and Applications, vol. 48, Oct. 2019.

[4] Y.C. Hu, M. Patel, D. Sabella, N. Sprecher and V. Young, "Mobile edge computing—a key technology towards 5G," ETSI white paper, pp. 1-16, Sep. 2015.

[5] A.C.C. Yao and Y. Zhao, "Online/offline signatures for low-power devices," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 283-294, Feb. 2012.

[6] S. Even, O. Goldreich and S. Micali, "On-line/off-line digital signatures," Journal of Cryptology, vol. 9, no. 1, pp. 35-67, Mar. 1996.

〈저자소개〉

최 재 현 (Jae Hyun Choi) 학생회원
2019년 2월: 인천대학교 수학과 졸업
2019년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 프라이버시 향상 기술, 블록체인

이 상 훈 (Sang Hoon Lee) 정회원
2010년 2월: 서울시립대학교 수학과 졸업
2013년 2월: 고려대학교 정보보호대학원 석사
2020년 8월: 고려대학교 정보보호대학원 박사
2020년 10월~12월: 고려대학교 정보보호대학원 연구교수
2021년 1월~현재: 삼성 SDS IAM 보안 그룹
〈관심분야〉 프라이버시 향상 기술, 생체 인증

정 익 래 (Ik Rae Jeong) 종신회원
1998년 2월: 고려대학교 전산학과 졸업
2000년 2월: 고려대학교 정보보호대학원 석사
2004년 8월: 고려대학교 정보보호대학원 박사
2008년 3월~현재: 고려대학교 정보보호대학원 조교수, 부교수, 교수
〈관심분야〉 프라이버시 향상 기술, 데이터베이스 보안, 생체인증, 블록체인

변 진 욱 (Jin Wook Byun) 종신회원
2001년 2월: 고려대학교 전산학과 졸업
2003년 2월: 고려대학교 정보보호대학원 석사
2006년 8월: 고려대학교 정보보호대학원 박사
2006년 11월~2007년 12월: Royal Holloway University of London 박사 후 연수
2008년 3월~현재: 평택대학교 정보통신학과 조교수, 부교수, 교수
〈관심분야〉 사용자 인증, 암호 프로토콜, 데이터베이스 보안, 프라이버시 보호 기술