Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.6, Dec. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.6.1247

Mobile Sink UAV 환경에서 프라이버시를 보장하는 새로운 인증 프로토콜 설계*

오 상 윤,[1†] 정 재 열,[1] 정 익 래,[2] 변 진 욱[3‡]
[1,2]고려대학교 (대학원생, 교수), [3]평택대학교 (교수)

A New Design of Privacy Preserving Authentication Protocol in a Mobile Sink UAV Setting*

Sang Yun Oh,[1†] Jae Yeol Jeong,[1] Ik Rae Jeong,[2] Jin Wook Byun[3‡]
[1,2]Korea University (Graduate student, Professor),
[3]Pyeongtaek University(Professor)

요 약

최근, 무선 센서 네트워크에서 더욱 효율적인 노드의 에너지 관리를 위해 센서 데이터를 대신 수집해주는 모바일 싱크 노드에 관한 연구가 있었다. 대표적인 모바일 싱크 노드로는 UAV (Unmanned Aerial vehicle)가 사용되며, 학계에서는 최적의 UAV 경로를 계산하는 알고리즘을 제시하는 위주로 IoD (Internet of Drones) 환경의 급격한 발전을 만들어냈다. 동시에, 보안 관점에서 다수의 노드와 세션키를 효율적으로 만들어야 하는 IoD의 특성에 맞춰 상호 인증 및 안전한 키 교환을 목표로 하는 기법들이 몇몇 제시되었다. 하지만, 모바일 싱크 노드 환경에서의 안전한 통신을 제안한 대부분 논문은 종단 간 데이터 프라이버시가 지켜지지 않았다. 따라서 본 논문에서는 모바일 싱크 노드와 센서 노드 간 인증부터 모바일 싱크 노드가 센서 데이터를 기지국까지 안전하게 중계하는 통합적 보안 모델을 처음으로 제안한다. 또한, 제안한 프로토콜의 안전성을 비공식적으로 입증하고 알려진 다양한 공격으로부터 안전함을 보인다. 마지막으로 기존에 제시된 IoD 환경에서 안전한 키 교환을 주제로 한 기법들과 통신 오버헤드를 비교해 본 논문에서 제시한 기법이 우수하다는 것을 보여준다.

ABSTRACT

For more efficient energy management of nodes in wireless sensor networks, research has been conducted on mobile sink nodes that deliver data from sensor nodes to server recently. UAV (Unmanned Aerial vehicle) is used as a representative mobile sink node. Also, most studies on UAV propose algorithms for calculating optimal paths and have produced rapid advances in the IoD (Internet of Drones) environment. At the same time, some papers proposed mutual authentication and secure key exchange considering nature of the IoD, which requires efficient creation of multiple nodes and session keys in security perspective. However, most papers that proposed secure communication in mobile sink nodes did not protect end-to-end data privacy. Therefore, in this paper, we propose integrated security model that authentication between mobile sink nodes and sensor nodes to securely relay sensor data to base stations. Also, we show informal security analysis that our scheme is secure from various known attacks. Finally, we compare communication overhead with other key exchange schemes previously proposed.

Keywords: Wireless sensor network, Moblie sink, Node management

Received(10. 20. 2021), Modified(11. 16. 2021), Accepted(12. 07. 2021)

* 이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2020R1F1A1065434)

† 주저자, ohsangyun200@korea.ac.kr
‡ 교신저자, jwbyun@ptu.ac.kr(Corresponding author)

I. 서 론

IoT(사물인터넷)는 물체들에 인터넷을 연결하여 상호연결 기반의 네트워크 환경을 구축하고 사물에 장착된 센서가 다양한 데이터를 받아오는 기술을 의미한다 [1]. 일반적으로 중앙 관제의 역할을 수행하는 서버는 이러한 센싱된 데이터를 종합적으로 관리하고 판단하게 된다. 최근 IoT 기술의 발전으로 인해 서버는 사람의 개입 없이 다양한 기기로부터 받은 센서 데이터를 활용하여 상황 파악 및 필요한 조치를 스스로 수행할 수 있게 되었다. 최근, 이러한 IoT 기술은 다양한 분야에서 실제 응용되어 사용되고 있다 (스마트 창고, 제조업, 지역 감시, logistics). IoT 환경 구성에 주요하게 사용되는 핵심기술 중 하나는 무선 센서 네트워크 기술이며, 이는 유선망에 제약받지 않고 광범위한 필드에서 수집한 센서 데이터를 기지국에 전송할 수 있게 해주는 기법이다. 이러한 무선 센서 네트워크의 특징으로는 노드의 위치를 미리 결정할 필요가 없으며 자가 구성되기 때문에 설치 및 운용이 간편하다는 점이 있다. 하지만, 센서 노드들은 한정된 배터리 용량을 가지며 에너지 효율성을 위해 계산력이 제한되어 있다는 단점도 있다.

최근, 이러한 한계를 극복하고 전체 네트워크의 수명을 늘리고자 다양한 연구들이 제시되었다. 그중에서도 모바일 싱크 임무를 수행하는 UAV를 도입한 드론 기반 무선 센서 네트워크[2] 모델이 대표적이다. 이 모델은 드론이 미리 설정된 경로를 이동하며 모바일 싱크 노드 역할을 수행하고 다양한 센서로부터 데이터를 수집 후 기지국에 전달한다. 이로 인해, 소형 노드들에게 반드시 요구되는 기지국까지의 데이터 전달 비용을 절약할 수 있다는 점에서 에너지 효율적이다.

드론 기반 무선 센서 네트워크는 센서들만으로 데이터를 기지국까지 중계하는 전통적인 기법과는 달리 드론이라는 이동 가능한 새로운 객체가 추가되었기 때문에 이에 따른 보안 요구사항이 더 추가되었으며 각각의 참여자들이 안전@korea.ac.kr하게 관리해야 할 요소들도 (인증서, 비밀 값, 등) 증가하였다. 하지만, 최근에 제시된 인증 기법들은 공격자에 의한 모바일 싱크 노드의 탈취 혹은 포획이 발생했을 때 센서로부터 수집된 데이터를 보호할 수 있는 방법을 전혀 고려하지 않고 있다. 센서로부터 수집된 데이터는 위치와 시간 그리고 이미지 및 영상과 같은 프라이버시에 매우 민감한 정보들을 담고 있지만, 대부분

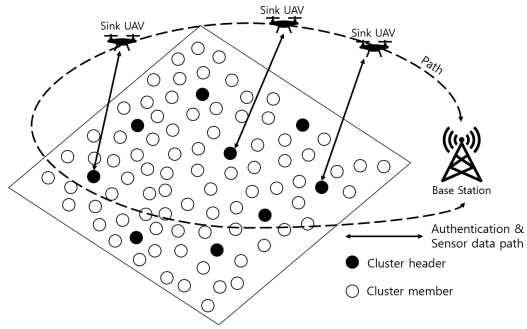

Fig. 1. System architecture of proposed model

의 무선 센서 네트워크에서의 고전적 보안 프로토콜은 센서와 기지국 간의 통신에서 발생하는 채널의 기밀성 및 프라이버시 제공에만 집중하였다. 또한, 드론 기반 무선 센서 네트워크에서도 센서 노드와 모바일 싱크 노드 (드론) 간 혹은 모바일 싱크 노드와 기지국 간의 안전한 보안 채널 형성에만 많은 연구가 수행되었다. 이러한 기존 드론 기반 무선 보안 프로토콜들에서는 공격자가 모바일 싱크 노드를 탈취하여 센서로부터 수집한 데이터를 드론이 먼저 볼 수 있는 매우 심각한 보안 위협이 존재한다. 즉, 데이터가 되어 전달되는 최종 목적지는 기지국인데 중간에서 드론 기반의 모바일 싱크 노드가 이 정보를 먼저 확인하여 프라이버시를 침해 할 수 있는 보안 취약점이 발생할 수 있다. 최근 빈번히 발생하는 드론 관련 보안 이슈 및 사고들의 근본 원인은 드론이 직접 센싱된 정보를 받아서 볼 수 있다는 사실에 기인한다. 이러한 위협 및 취약점을 방어하기 위해 모바일 싱크 노드가 본인의 비밀키로 수집된 데이터를 암호화하는 방안을 고안할 수 있지만, 해당 접근법은 다음의 두 가지 문제점을 지닌다.

- [프라이버시 문제] 모바일 싱크 노드의 탈취는 메모리에 보관된 관련 암호화/복호화 키 모두를 탈취할 수 있음을 가정하므로 공격자는 그 해당 키로 암호문을 복호화할 수 있음을 의미한다. 또한, 모바일 싱크 노드는 언제든지 스스로 암호문을 복호화할 수 있으므로 센싱된 데이터의 프라이버시를 언제든지 침해할 수 있다. 더 나아가, 드론이 직접 센서 노드와 모바일 싱크 노드 간의 협의한 쌍별 키를 이용하여 암호화하는 방법도 여전히 드론이 수집된 데이터를 볼 수 있는 문제를 해결할 수 없다.

- 〔비효율성 문제〕 모바일 싱크 노드가 수집된 데이터를 매번 암호화하는 것은 프라이버시 침해 문제를 막을 수 없을뿐더러 암/복호화로 인한 비효율성을 증가시킨다. 모바일 싱크 노드가 수집된 데이터를 어떠한 키로 암/복호화할 것인가에 대한 키 결정의 문제도 번거로울 뿐 아니라 매번 운행 중에 암/복호화를 처리하는 것은 드론 측면에서 매우 비효율적이다.

따라서 본 논문에서는 이러한 드론의 직접적인 암호화 기법을 통해서 보안 프로토콜을 설계하지 않고 암호화의 주체를 센서 노드와 기지국 간의 비밀키로 수행하게 하여 드론이 전혀 해당 암호문들을 복호화할 수 없도록 하는 프라이버시 보장 및 인증 프레임워크를 처음으로 제안한다. 즉, 센서 노드들은 데이터를 우선 수집하여 곧바로 모바일 싱크 노드에게 전달하지 않고 기지국과 공유된 대칭 키로 먼저 암호화하여 암호문을 모바일 싱크 노드에게 전달하게 되며 결국 모바일 싱크 노드는 암호문을 기지국에게 전달함으로써 모바일 싱크 노드의 프라이버시 침해 문제를 해결하는 것이 본 논문의 주요 아이디어이다. 이러한 프라이버시가 보호되는 프레임워크를 기반으로 하여 센서 노드, 모바일 싱크 노드, 그리고 기지국 간에 기밀성과 인증을 제공하는 보안 프로토콜을 처음으로 설계한다. 이와 관련하여 본 연구의 공헌도는 다음과 같다.

- 〔통합 보안 인증 프로토콜 설계〕 본 논문에서는, Fig. 1.에 나와 있는 것처럼, 센서 노드, 모바일 싱크 노드, 기지국 사이의 통신을 안전하게 보호할 수 있는 통합 보안 인증 프로토콜을 설계한다. 드론 기반 센서 네트워크에서 대부분의 보안 프로토콜들은 센서 노드와 모바일 싱크 노드 사이의 보안 프로토콜 설계에 많은 연구가 이루어졌다. 본 논문에서는, 데이터 전송이 발생하는 모든 구간별로 데이터에 대한 기밀성 및 인증 서비스를 제공할 수 있도록 설계하였으며 이로 인해 센서로부터 수집된 데이터가 모바일 노드를 거쳐 안전하게 기지국까지 전달되도록 설계하였다. 또한, 중간에 위치하는 모바일 싱크 노드가 수집된 데이터를 알 수 없도록 하여 모바일 싱크 노드로부터의 프라이버시 침해를 보장할 수 있는 프로토콜을 처음으로 제안하였다.
- 〔안전성〕 최근에 제시된 드론 기반 센서 네트워크에서의 안전한 인증 기법을 분석 비교하여 제시한 기법이 안전하다는 것을 비공식적으로 보인다. 제시된 방법은 중간자 공격을 막기 위해 개체 간 상호 인증을 고려하여 설계하였다. 또한, Table 2.와 Table 3.에 분석한 대로, 제안한 기법은 기존 보안 요구사항들을 모두 만족하며 동시에 통신 구간별로 기밀성과 인증을 제공한다.

논문의 구성은 다음과 같다. 2장에서는 드론 기반 센서 네트워크가 제시된 배경에 대해 언급한다. 3장에서는 본 논문에서 제시하는 프로토콜에 관해 설명한다. 기존 드론 기반 센서 네트워크에서 안전한 인증을 위해 이전에 제시된 기법들과 본 논문에서 제시한 기법의 안전성 비교를 4장에서 진행하고, 5장에서는 제시한 기법의 성능을 분석 및 비교한다. 마지막으로, 7장에서는 본 논문의 결론을 짓는다.

II. 관련 연구

2.1 드론 기반 센서 네트워크의 등장 배경

무선 ad-hoc 네트워크에서 사용되는 라우팅 프로토콜은 점대점 방식의 통신을 사용하기 때문에, 노드 수가 훨씬 더 많은 무선 센서 네트워크에 적합하지 않았다 〔3〕. 또한, 무선 센서 네트워크는 초소형의 한정된 컴퓨팅 자원을 가진 노드를 대상으로 프로토콜을 설계해야 하기때문에, ad-hoc 네트워크보다 계산력이나 저장공간의 제약사항이 존재한다.

이러한 제약사항을 가진 무선 센서 네트워크의 프로토콜은 크게 평면 기반 라우팅과 계층 기반 라우팅으로 나뉜다. 평면 기반 라우팅은 모든 노드가 같은 역할을 갖고 하나의 라우팅 기법을 사용해 데이터를 기지국까지 전달하는 기법을 의미한다. 대표적인 기법으로는 〔4〕가 있다. 계층 기반 라우팅은 LEACH (Low-Energy Adaptive Clustering Hierarchy) 모델로서 많이 알려져 있다. 이 기법은 모든 센서 노드들이 데이터를 기지국에 전송하는 데에 있어서 에너지 소모를 공정하게 분산시키기 위해 데이터 중계 역할을 하는 클러스터 헤드를 주기적으로 교체하는 방식이다 〔5〕. 계층 기반 라우팅을 사용하게 된다면 평면 기반 라우팅 기법보다 데이터 전송 역할을 맡은 노드의 데이터 전송 부담을 줄일 수

있어 네트워크의 망의 신뢰성이 높아진다. 계층 기반 라우팅은 크게 비대칭 키(공개키) 기법과 대칭 키 기법으로 나뉜다. 대칭 키 기반 기법은 속도가 빠르지만, 네트워크의 확장성이 없고 변질된 노드에 대한 저항성이 없다. 공개키 기법은 대칭 키 기법보다 연산 속도가 느리지만, 네트워크의 확장성을 보장해주며 설계에 따라 생성된 세션의 완전 순방향 비밀성을 보장할 수 있다.

드론 기반 센서 네트워크는 계층 기반 센서 네트워크의 일종으로 센서 노드의 데이터를 기지국까지 중계하는 통신 비용을 줄이기 위해 제시되었다 [6][7]. 이 기법은 센서 노드의 에너지 관리를 더욱 효율적으로 하기 위해 모바일 싱크 노드를 도입하고 싱크 노드가 센서 노드가 배포된 필드를 돌아다니며 데이터를 대신 수집해준다. 이 방식은 센서 노드의 기지국까지 데이터 중계 과정을 건너뛸 수 있기에 센서 노드들의 통신 에너지 소모를 크게 줄일 수 있다.

2.2 모바일 싱크 노드를 도입한 기법 소개

본 절에서는 최근 몇 년간 연구된 모바일 싱크 노드 기반 센서 네트워크에서의 안전한 인증 및 키 교환 프로토콜 [8]-[16]에 대해 살펴본다. 싱크 노드의 이동성 여부에 따라 크게 고정된 싱크 노드와 모바일 싱크 노드로 분류할 수 있다.

2.2.1 고정된 싱크 노드

2015년에, Deebak et al. [8]은 싱크 노드 역할을 하는 게이트웨이 노드를 통해 사용자가 센서 노드로부터 데이터를 받아올 수 있는 기법을 제시했다. 사용자는 소유한 스마트카드를 기기에 삽입해 신분증명을 하고, 게이트웨이 노드와의 인증을 요청한다. 그 후 게이트웨이 노드는 센서 노드와의 인증을 수행하고 세션 키 설립에 필요한 값들을 받아와 사용자에게 넘겨준다. XOR 연산 기반의 경량 기법이지만, 대칭 키 기반이기에 노드 탈취 공격 등에 취약하다. Amin et al. [9]은 [8]을 바탕으로 사전에 서버에 등록한 센서 노드의 가명을 통해 사용자의 익명성을 보장할 수 있는 기법을 제시했다. 하지만, 익명 아이디를 만드는 데 사용되는 랜덤 값이 일회성이기에 가명에 대한 freshness를 보장하지 못한다. 이후, Srinivas et al. [11]은 [9]을 기반으로 사용자, 게이트웨이, 센서 노드가 동일한 대칭 키를 공유할 수 있는 기법을 제시했다. 이 기법은 센서 데이터의 기밀성을 지킬 수 있지만, 여전히 데이터의 프라이버시를 보장할 수 없다. Wazid et al. [12]은 생체정보를 사용해 사용자와 센서 노드 간 세션 키를 만드는 기법을 제시했지만, 싱크 노드는 여전히 중간에서 모든 정보를 볼 수 있는 취약점이 존재하였다. 2020년에 Deebak et al. [14]은 카오틱 맵을 사용해 [8][11][12]에서 제안된 프로토콜들보다 안전하고 계산 효율적인 기법을 제안했다.

Table 1. List of notations

BS	Base Station
CH^j	j-th Cluster Head node
MS^i	i-th Mobile Sink node
C^j	Unique identifier of CH^j
M^i	Unique identifier of MS^i
K^j	Individual key of node C^j
M_{sk}^i	Private key of MS^i
M_{pk}^i	Public key of MS^i
$Cert^i$	Certification of MS^i
$CertList$	Certification list of mobile sink
$Route^i$	Sink movement path and key pair of cluster head node included in path
EK_{BS}^j	Data encryption key of CH^j and BS
TS_n^i, TS_m^j	n-th time stamp of MS^i, m-th time stamp of MS^j
$H(m)$	cryptographic hash function
$E_k(m)$	encryption algorithm to encrypt message m with key k

2.2.2 모바일 싱크 노드

2017년에, Al-Turjman et al. [10]은 페어링 연산을 사용해 모바일 싱크 노드와 센서 노드 간 안전하게 세션 키를 만드는 기법을 제시했다. 이후, Ever et al. [13]은 [10]의 기법보다 안전성 및 연산 효율성을 개선한 기법을 제시하였다. 하지만, [13]은 모바일 싱크 노드가 수집한 데이터를 기지국에 전달해주는 방법을 고려하지 않았다. 2020년에 Alladi et al. [15]는 PUF(Physically Uncloneable

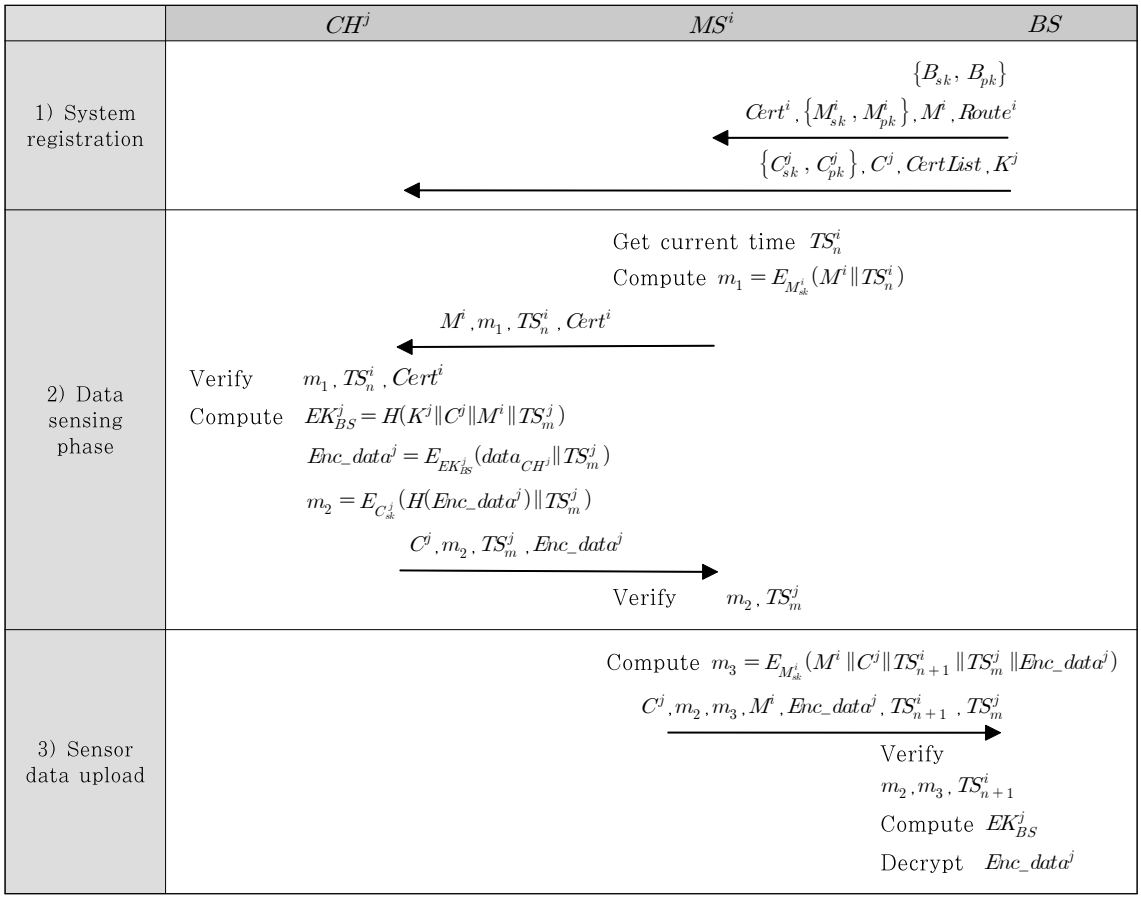

Fig. 2. Proposed protocol

Function)기반의 인증을 사용하는 PARTH를 제시했지만, [10][13] 기법보다 통신 횟수나 통신 비용 측면에서 비효율적이며 모바일 싱크 노드와 센서 노드 간 키 교환 단계가 생략되어 있다. [16]은 certificateless 기법을 사용해 센서 및 드론, 드론과 기지국간 인증을 다룬 모델이며 데이터의 발생부터 BS로의 전달까지 데이터의 암호화 및 안전한 전송을 프로토콜에 고려하지 않았다.

2.3 센서 노드의 공개키 연산 적용 가능성

최근에는 무선 센서 네트워크에서 공개키 기반의 키 관리 기법들이 제안되고 있다. 공개키 기반의 기법은 대칭키 기반의 기법들보다 확장성이 좋고 노드 포획 공격에 대해 저항성을 가진다. 하지만, 공개키 기반 기법은 계산 비용이 더 비싸다는 단점이 있다.

[17]의 연구 결과는 타원 곡선 기반의 공개키 기법을 무선 센서 네트워크의 센서 노드들에게 적용 가능하다는 가능성을 보여주었다. [17]은 8비트 마이크로 컨트롤 유닛인 Atmel ATmega 128에서 160bit의 필드를 갖는 타원곡선의 포인트 곱셈 구현에 1초 미만이 걸린다는 것을 보여줬다.

III. 제안 프로토콜

본 장에서는 논문에서 제안하는 모바일 싱크 기반의 통합적 인증 기법에 관해 설명한다. 이 인증 기법은 4단계로 (시스템 준비, 시스템 등록단계, 클러스터 헤더로부터 데이터 센싱 단계, 센서 데이터 업로드) 구성된다. Table 1.에서는 논문에서 사용되는 주요한 기호들을 간략하게 나타낸다.

3.1 네트워크 모델 설명

드론 기반 무선 센서 네트워크의 궁극적인 목적은 중간 전달자인 모바일 싱크 노드의 효율적인 센서 데이터 수집과 수집한 데이터를 안전하게 기지국에 전송하는 것이다. 본 논문에서는 효율적인 센서 데이터의 수집을 위해 클러스터링 된 센서 네트워크를 도입하고, 모바일 싱크 노드가 센서가 배포된 필드를 돌아다니며 클러스터 헤드에서 데이터를 안전하게 수집하고, 기지국에 안전하게 전달할 수 있는 통합 보안 프로토콜을 제시한다.

3.2 네트워크 모델 설명

기지국 BS는 노드와 통신을 시작하기 전, 시스템 변수(system parameter)를 생성한다. 먼저, BS는 자신의 공개키 개인키 쌍 $\{B_{sk}, B_{pk}\}$을 선택한다. 그리고 암호학적 해시 함수 h_0을 선택한다.

3.3 시스템 등록단계

시스템 등록은 CH와 MS가 실제 지역에 배포되거나 운행되기 전에 발생한다. 따라서 시스템 등록단계에서는 안전한 채널을 활용하여 통신이 이루어짐을 가정한다. 시스템 등록단계는 기지국이 드론과 클러스터 헤드 노드에게 인증에 활용될 값들을 넘겨주는 과정이다. 이 단계에서 기지국은 모든 클러스터 헤드 노드들의 타임스탬프 값을 동기화시키며 각 노드들에게 공개키 개인키 쌍과 인증서 정보를 발급해준다.

3.3.1 모바일 싱크 노드 등록

BS는 모바일 싱크 $MS^i\ (1 \le i \le N_1)$에 대해 각각 키 쌍 $\{M_{sk}^i, M_{pk}^i\}$과 고유 아이디 M^i를 생성한다. BS는 공개키에 대한 인증서 $Cert^i$를 생성한 후, 경로 정보 $Route^i$를 MS^i에게 전달한다. $Route^i$는 MS^i의 이동 경로 및 데이터를 받아와야 할 CH^j의 공개키 및 아이디로 구성된 값이다. 최종적으로 MS^i는 BS로부터 전달받은 내용들 ($Cert^i$, $\{M_{sk}^i, M_{pk}^i\}, M^i, Route^i$)을 내부 저장소에 저장한다.

3.3.2 클러스터 헤드 등록

클러스터 헤드 등록 시 BS가 $CH^j\ (1 \le j \le N_2)$와 $MS^i\ (1 \le i \le N_1)$간에 프로토콜 운영에 필요한 최소한의 비밀 값을 분배하며 CH^j를 등록시킨다. 먼저 BS는 등록할 CH^j의 공개키 개인키 쌍 $\{C_{sk}^j, C_{pk}^j\}$과 CH^j의 고유 아이디 C^j를 생성하고 이후 센서 데이터의 안전한 전송에 사용될 개별 키 K^j를 생성한다. 또한, 모든 MS^i의 인증서 목록을 담고 있는 $CertList$도 CH^j에게 전달한다. $CertList$는 각 MS^i의 아이디, BS의 서명, 등 인증서 정보를 담고 있다.

클러스터 헤드 등록단계 종료 후 최종적으로 CH^j는 $\{C_{sk}^j, C_{pk}^j, K^j\}, C^j, CertList$를 저장하게 된다.

3.4 클러스터 헤더로부터 데이터 센싱 단계

모든 노드가 네트워크에 배포된 이후, MS^i는 시스템 등록단계에서 받은 $Route^i$를 참조해서 이동한다. 경로를 이동하며 MS^i는 CH^j의 연결을 요청하는 연결요청 메시지를 브로드캐스팅한다. CH^j가 메시지를 받고 응답을 보내면 데이터 센싱 단계가 시작된다. MS^i는 정당한 모바일 싱크 노드임을 증명하기 위해 현재시간 TS_n^i 및 아이디 M^i에 대한 인증값 $m_1 = E_{M_{sk}^i}(M^i \| TS_n^i)$을 계산하고 M^i, m_1, TS_n^i를 CH^j에게 전달한다. CH^j는 이 메시지를 수신한 후, 저장되어있는 $CertList$에서 M^i의 정보를 가져오고, M_{pk}^j를 이용하여 받은 m_1을 검증한다. 검증에 실패하거나 타임스탬프가 현재 시간과 오차범위를 크게 벗어날 경우, 인증 실패로 판단하고 세션을 종료한다. m_1 및 타임스탬프가 올바른 값이면, CH^j는 이후 BS와의 데이터 암호화에 사용될 대칭키 $EK_{BS}^j = H(K^j \| C^j \| M^i \| TS_m^j)$를 계산한다. 이후 계산한 대칭키로 센서 노드에서 수집한 데이터 $data_{CH^j}$를 대칭키 암호화 $Enc_data^j = E_{EK_{BS}^j}(data_{CH^j} \| TS_m^j)$하고 생성한 암호화된 데이터값 Enc_data^j에 대한 인증값인 $m_2 = E_{C_{sk}^j}(H(Enc_data^j) \| TS_m^j)$를 계산한다. Enc_data^j 및 m_2에는 재생공격 방지를 위해 현재 시간 값 TS_m^j이 포함된다. CH^j는 최종적으로 $C^j, m_2,$

Table 2. Security analysis of various authentication schemes

schemes	A1	A2	A3	A4	A5	A6	A7	A8
[8]	○	-	○	○	-	○	○	-
[9]	○	○	○	○	-	○	○	×
[10]	○	○	○	○	○	○	○	×
[11]	○	○	○	○	○	○	○	×
[12]	○	○	○	○	-	○	○	×
[13]	○	-	○	○	○	○	○	-
[14]	△	○	×	○	-	×	○	-
[15]	○	×	○	○	○	○	○	-
Ours	○	○	○	○	○	○	○	○

A1: Mutual authentication; A2: Sensor data confidentiality from node capture attack; A3: Resistance to replay attack; A4: Resistance to forgery attack; A5: Multiple node detection; A6: Resistance to Denial of Service; A7: Key freshness; A8: Data ignorance of relaying node

TS_m^j, Enc_data^j를 MS^i에게 전송한다. MS^i는 $Route^i$에 저장돼있는 CH^j의 공개키를 통해 m_2를 복호화 후 Enc_data^j를 검증한다. 검증에 성공하면 수신한 값들을 저장하고 세션을 종료한다. 서명 및 타임스탬프 검증이 실패할 경우, 프로토콜을 종료한다.

3.5 센서 데이터 업로드

센서 데이터 업로드는 이동을 끝낸 MS^i가 받아온 센서 데이터를 BS에게 전달하는 과정이다. $Route^i$를 순회하고 돌아온 MS^i는 서명 $m_3 = E_{M_{sk}^i}(M^i \| C^j \| TS_{n+1}^i \| TS_m^j \| Enc_data^j)$를 계산하고 BS에게 $C^j, m_2, m_3, M^i, Enc_data^j, TS_{n+1}^i, TS_m^j$을 전송한다. 먼저 BS는 타임스탬프 TS_{n+1}^i가 현재 시간과 오차범위 내에 있는지를 검증한다. 이상이 없다면, BS는 MS^i의 공개키 M_{pk}^j를 통해 메시지 m_3를 검증하여 MS^i가 보낸게 맞는지를 확인한다. 그 후 BS는 C^j를 보고 저장된 CH^j의 공개키 C_{pk}^j를 가져온다. 그다음으로 BS는 메시지 m_2를 검증하여 암호문 Enc_data^j를 CH^j가 직접 생성한 것인지 검증한다. 이러한 모든 검증이 올바르면 BS는 TS_m^j를 통해 데이터 암호화 키 $EK_{BS}^j = H(K^j \| C^j \| M^i \| TS_m^j)$를 만들 수 있다. 최종적으로 BS는 Enc_data^j를 복호화해서 센서 데이터를 얻을 수 있다.

IV. 보안성 분석 및 토의

보안성 분석을 위해 모바일 싱크 환경에서 가능한 공격 기법을 분석한 이전 연구들 [13][14][15]을 참고해서 주요한 10가지의 공격 및 보안 성질을 고려하였고 그에 따른 만족도를 분석하여 Table 2.에 나타내었다. '○'는 해당 취약점에 대해 안전하다는 것이며, '×'는 취약하다는 뜻이다. '-' 은 기법이 해당 취약점을 고려하지 않았다는 뜻이다. 본 논문에서는 데이터 암호화 키를 이용하여 종단 간 데이터 프라이버시를 보장하는 것이 목적이기 때문에 완전 전방위 비밀성을 고려하지 않는다. 분석에 앞서 공격자는 싱크 노드 및 클러스터 헤드 노드가 필드에 배포된 이후부터 전체 네트워크를 관찰하며 각 노드가 브로드캐스트 채널을 통해 주고받는 메시지를 모두 기록하며 변조할 수 있다고 가정한다.

4.1 Mutual authentication

제시한 기법에서 참여하는 세 개체들은 공개키 암호기술을 사용할 수 있는 환경이므로 각각 전자서명 값을 생성하여 상호 인증을 수행할 수 있다. 그림 2에 표현된 프로토콜과 같이 CH^j와 MS^i는 상호 한 번씩의 메시지를 주고받아 상호인증을 할 수 있게 설계하였다. MS^i와 BS간에는 MS^i을 인증하는 것이 더욱 실용적이기에 MS^i의 인증만을 고려한 단방향 인증을 설계하였다. BS는 저장된 MS^i의 공개키를 활용하여 MS^i를 인증할 수 있다.

CH^j는 사전등록 단계에서 BS로부터 발급받은 인가된 노드 리스트의 공개키, 아이디가 담긴 $CertList$를 통해 MS^i가 보낸 메시지 m_1에 대한 인증을 통해 MS^i를 인증할 수 있다. 반대로 MS^i는 경로를 출발하기 전 등록단계에서 데이터 수집 대상이 되는 CH^j들의 공개키, 아이디가 담긴 $Route^i$를 BS로부터 전달받는다. $Route^i$에 CH^j들의 공개키가 포함되어 있으므로 MS^i는 CH^j가 보낸 메시지 m_2를 검증할 수 있으며 이를 통해 CH^j를 인증할 수 있다. 공격자는 개인키를 알지 못하므로 서명위조를 할 수 없고 가장 공격을 수행할 수 없다.

4.2 Sensor data confidentiality from node capture attack

클러스터 헤드 노드 CH^j가 수집한 데이터는 BS에 도착할 때까지 기밀성을 유지해야 한다. 제시한 기법에서 CH^j는 사전에 BS에게 분배받은 비밀 값 K^j와 타임스탬프 값 TS_m^j를 사용하여 데이터 암호화 키 EK_{BS}^j를 만들고 해당 키로 센서 데이터를 암호화해 MS^i에게 넘겨준다. MS^i는 암호화된 데이터 Enc_data^j를 받고 BS에게 전달한다. 공격자는 K^j가 없다면 데이터 암호화 키 EK_{BS}^j를 만들 수 없어 복호화가 불가능하다. 또한, 공격자가 MS^i를 물리적으로 탈취하더라도 Enc_data^j만을 알 수 있으므로 평문에 해당하는 수집된 데이터를 알 수 없다. 만약 공격자가 특정 CH^j를 물리적으로 탈취하여 해당 K^j키를 알 수 있다면 해당 CH^j가 수집한 데이터에 대한 기밀성은 보장할 수 없다. 하지만 제안된 프로토콜은 하나의 특정 CH^j의 물리적 탈취를 통해서 다른 모든 CH^j가 수집한 데이터들을 알 수 없도록 설계하였다. 이는 각각의 CH^j가 고유한 대칭키 K^j로 BS와 대칭적으로 공유하도록 설계했기 때문이다. 사실, 대칭키 구조의 암호를 사용하는 프로토콜에서는 해당 대칭키의 노출이 곧 기밀성의 파괴를 의미하게 되므로 이에 대한 완전 기밀성 보장은 한계가 있다.

CH^j에 물리적 복제 방지기술 (physical unclonable function)과 같은 하드웨어 보안 기술을 적용한다면 공격자의 노드 탈취를 통한 관련 공격을 일부 방어할 수 있다. PUF를 사용하는 경우, PUF의 칩에 저장되는 서명을 위한 개인키는 하드웨어 조립 단에서 발급받아야 한다. 또한, PUF 칩은 변조 불가능성(tamper resistance)의 성질이 있어 PUF 칩 안의 개인키를 다른 개체들이 알 수 없다. 이로 인해 개인키를 알고 있는 새로운 CH^j의 복제는 불가능하게 되어 프로토콜 상에서 CH^j 노드의 고유 서명 값을 위조할 수 없게 된다. 이러한 노드의 PUF 적용의 전략은 노드의 위조 불가능성에는 도움이 된다. 하지만 대칭키 K^j에 대해서는 최초 시스템 등록단계에서 BS가 발급하여 전달하는 구조이므로 PUF 칩 내에 발급 보관하는 것이 불가능하다. 위에서 분석하였듯이 현재까지 대칭키 구조의 암호를 사용하는 프로토콜에서는 해당 대칭키의 노출이 곧 기밀성의 파괴를 의미하게 되므로 이러한 취약점을 보완하고자 PUF를 CH^j, MS^i, BS에 적용하여 안전하게 프라이버시를 보장하는 프로토콜을 설계하는 것은 간단하지 않다. 제안한 프로토콜은 비록 능동적인 노드 탈취공격에는 드론의 프라이버시를 보장할 수 없다는 구조적 한계를 지니지만 수동적인 드론 모델에서는 드론으로부터의 프라이버시를 보장할 수 있다. 향후 대칭키 기반의 암호화 구조에서 데이터 기밀성뿐 아니라 능동적 드론으로부터의 프라이버시를 보호할 방법, 더 나아가 개체 간 인증을 유도할 방법에 관한 추가 연구가 반드시 필요하다.

4.3 Resistance to replay attack

공격자는 프로토콜에 사용된 메시지를 도청 후 재전송하여 인증을 통과하거나 프로토콜을 성공적으로 수행할 수 있다. 이를 방어하기 위해 본 프로토콜은 인증 파라미터에 타임스탬프를 추가하여 공격자로부터의 메시지 재사용에 안전하도록 설계하였다. 각 객체는 타임스탬프가 포함된 메시지값 m_1, m_2을 받으면 이를 먼저 검증하고 전송받은 타임스탬프가 현재 시간과의 오차범위 내에 있는지 다시 확인하여 재사용 공격을 막는다. 타임스탬프의 사용은 개체들 간에 반드시 시간에 대해 동기화가 되어있어야 한다는 이슈가 존재한다. 타임스탬프를 사용하지 않고 상대방이 랜덤한 값을 선택하여 보내게 되면 이에 대해 직접 서명한 후 응답하는 방법으로 설계할 수도 있다. 하지만 랜덤한 값의 발생과 전달은 최소 한 번의 통신 횟수를 요구하므로 이는 더 큰 비용을 (에너지, 데이터 손실) 초래할 수 있다. 현재 대부분 IoT 단

말기와 센서는 GPS 등을 활용하여 시간에 대한 동기화가 대부분 되어있으므로 통신 횟수를 추가하는 방법 대신 시간 값을 활용하여 한 번에 서명하여 보내는 전략을 통해 재생 공격을 막도록 하였다.

4.4 Resistance to forgery attack

공격자는 가로챈 프로토콜 메시지를 다른 메시지로 위/변조하여 보낼 수 없어야 한다. 제안된 프로토콜은 CH^j와 MS^i가 메시지 m_1, m_2을 전달하고 검증하여 인증하는 구조이다. 하지만 공격자는 노드들의 개인키를 모르기 때문에 시간 및 관련 메시지에 대한 서명을 위조하여 전달할 수 없으므로 제안된 프로토콜은 위/변조 공격에 강건하다. 메시지 위/변조 공격을 막기 위해 공개키 기반의 전자서명 기술 대신 대칭키 기반의 MAC(message authentication code)을 활용할 수 있다. 하지만 MAC 적용 전략은 CH^j, MS^i들과 BS간에 MAC을 위한 대칭 키들이 기기별로 사전에 각각 분배되어야 하는 사전 작업이 필요하다. 즉, 만약 α개의 CH^j노드와 β개의 MS^i들을 가정했을 때 MAC 생성을 위해 $\alpha \times \beta$개의 대칭 키를 사전에 정의하여 분배해야 하는 번거로움이 있다. 반면에 본 프로토콜에서는 서명 기술의 적용을 통해 총 $\alpha + \beta$개의 선형성질을 만족하는 개인 키 개수가 요구되므로 보다 효율적이다. 또한, 새로운 CH^j, MS^i 노드들의 새로운 추가에 대해서도 제안된 프로토콜은 추가된 노드 수 γ에 선형으로 증가하는 키의 개수를 노드들에게 생성하여 추가하여 프로토콜을 시작할 수 있다. 하지만 MAC 적용 기법은 추가된 CH^j, MS^i 노드들에게 이미 배포된 CH^j, MS^i들과 사용하게 될 새로운 키를 생성하여 각각 생성하여 사전 배포하더라도 이미 배포된 CH^j, MS^i들에 대해서는 그 키들을 분배시킬 효율적인 방법이 존재하지 않는다. 즉, 이미 배포된 CH^j, MS^i를 다시 회수하여 동일한 키들을 갖도록 다시 키 설정을 거쳐야 하는 문제가 발생한다. 이러한 키 관리의 효율성 및 추가 노드들에 대한 효율적 처리를 위해 제안된 프로토콜은 전자서명 기술을 적용해 메시지 위/변조 공격을 막도록 설계하였다.

4.5 Multiple node detection

공격자는 CH^j를 물리적으로 탈취하여 비밀키 값을 구하고 필드 내에서 동일한 키 쌍을 사용하는 다수의 복제된 노드들을 심을 수 있다. 만약, 공격자가 탈취한 비밀 값들을 통해 동일한 여러 노드를 반복적으로 만들어 배포한다고 가정하자. BS는 MS^i로부터 받은 메시지 m_3에서 CH^j의 아이디 C^j를 추출한다. 이후 BS는 여러 다른 지역에서 동일한 아이디 C^j 및 개인키 C_{sk}^j로 암호화된 센서 데이터들이 MS^i로부터 업로드된 것을 식별할 수 있다. 즉, 제안된 프로토콜에서는 BS가 $Route^i$에 포함된 지역정보 및 C^j를 바탕으로 중복되어 수집되는 Enc_data^j를 식별할 수 있고 이를 통해 C^j가 복제되었음을 간파할 수 있는 구조를 지니고 있다. 이후 BS는 MS^i의 $Route^i$에서 C^j를 배제하여 해당 CH^j의 정보를 받아오지 않도록 조치할 수 있다. 더 나아가 PUF를 사용하여 노드의 개인키를 셋업시 보관한다면 복제 불가능하게 되어 메시지를 만드는데 필요한 개인키의 안전성이 물리적으로 보장되게 된다. 제안된 프로토콜은 BS가 최종적으로 CH^j의 메시지를 검증하도록 설계하였다. 그러므로 원래 노드를 악용하여 다중 노드를 가장하는 것은 PUF 칩의 복제 불가능성을 통해 개인키의 안전성을 보장함으로써 해결할 수 있다.

4.6 Resistance to Denial of Service

제안한 프로토콜은 모든 노드가 각자 메시지를 수신 후 곧바로 다음 프로토콜 메시지를 만드는 구조로 설계되지 않았다. 즉, 매 단계마다 수신 노드는 타임스탬프와 서명 값을 검증한 후 올바르면 그다음 프로토콜 메시지를 생성하게 된다. 이로 인해 잘못된 프로토콜 형식인 보거스(bogus) 패킷 및 메시지에 대해서는 1차적으로 걸러서 그다음 연산 및 프로토콜 준비를 하지 않도록 하는 구조로 설계되었다. 일반적으로 DoS 공격에 저항성이 있다고 하는 것은 이러한 최소한의 보거스 데이터들을 필터링할 수 있는 구조를 보유하고 있느냐로 판단한다. 제안하는 프로토콜은 서명 검증 및 확인을 통해 각 개체 모두가 DoS 공격에 강건한 최소한의 필터링 구조를 지니고 있다.

Table 3. Performance analysis of drone based WSN schemes.

	Mo	FC	Communication cost			Computation cost		
			CH	*MS*	*BS*	*CH*	*MS*	*BS*
[8]	×	5	$4M_h+2M_n$	$2M_h+M_n$	$5M_h+M_n$	$5P_h+P_r$	$8P_h$	$14P_h$
[9]	×	4	$4M_h+5M_n$	$4M_n+2M_h$	$5M_h+5M_n$	$9P_h+P_r$	$5P_h+P_r$	$7P_h+P_r$
[10]	○	6	M_h+M_n	$3M_n+2M_h+M_c$	M_h	$2P_h+2P_{bp}$	$7P_h+4P_{bp}+P_{sk}+P_{pk}$	$6P_h+P_{bp}+P_{sk}$
[11]	×	4	$2M_h+M_n$	$3M_n+2M_h$	$7M_h+3M_n$	$6P_h$	$9P_h+P_b$	$13P_h$
[12]	×	3	$4M_h+M_n$	$3M_h+M_n$	$3M_h+M_n$	$16P_h+P_b+P_r$	$7P_h+P_r$	$8P_h+P_r$
[13]	○	5	$M_n+M_{bp}+M_h$	$3M_n+2M_h+M_{bp}+M_c$	M_h+M_c	$P_{bp}+2P_h$	$7P_h+P_r+P_{pk}+P_{bp}$	$4P_h+P_{bp}+P_{sk}$
[14]	×	10	M_n	$3M_h+5M_n+M_c$	$3M_h+M_c+M_n+M_{bp}$	$6P_h+2P_{bp}$	$2P_r+5P_h+P_{bp}$	$5P_h$
[15]	○	10	$2M_n+M_h+3M_p$	$2M_n+5M_p+2M_h+2M_c$	$4M_c+2M_p+M_h$	$3P_h+P_r+P_f$	$3P_f+10P_h+2P_r$	$8P_h+2P_f+2P_{sk}+P_r$
Ours	○	3	$2M_n+M_s$	$4M_n+3M_s+M_h$	-	$2P_{pk}+3P_h$	$3P_{pk}$	$2P_{pk}+2P_h$

Mo: Mobility of sink node. FC: Flow count. M_s: The number of the signature value. M_c: The number of the ciphertext value. M_n: The number of the plaintext (e.g. ID, Timestamp, etc.). M_h: The number of the hash value. M_p: The number of the PUF value. M_{bp}: The number of bilinear pairing values. P_{pk}: The cost of PKC-based encryption/decryption. P_{sk}: The cost of Symmetric key-based encryption/decryption. P_h: The cost of hash operation. P_b: The cost of biometric fuzzy extractor. P_r: The cost of generate random nonce. P_f: The cost of operating PUF IC. P_{bp}: The cost of calculating bilinear pairing function.

4.7 Key freshness

제안된 프로토콜에서 CH^j는 수집된 데이터를 암호화하기 위해 매번 타임스탬프값 TS_m^j을 사용하여 랜덤한 새로운 암/복호화키 EK_{BS}^j를 만든다. 이로 인해 세션마다 암/복호화키가 달라지는 키의 신선도(key freshness)를 유지할 수 있다. 즉, 공격자가 다른 세션에 사용된 암호화 키를 알고 있더라도 이를 활용하여 이후 및 이전의 암호화 키를 알아낼 수 없다.

4.8 Data ignorance of relaying node

데이터를 중계하는 중간 노드 MS^i는 센서 데이터를 알아낼 수 없어야 한다. MS^i가 공격자에게 물리적으로 탈취당하더라도 데이터의 기밀성은 보장되어야 한다. 제시한 프로토콜에서 CH^j는 데이터 전송 요청을 받으면 BS와의 데이터 전송 키 EK_{BS}^j를 만든다. 이 키는 사전에 BS에서 분배받은 비밀 값 K^j가 포함되어 만들어지기 때문에 데이터 중계 노드인 MS^j는 전달받은 데이터를 읽을 수 없다.

V. 성능 분석

5.1 효율성

본 절에서는 제안한 기법의 효율성을 다른 무선 센서 네트워크 환경에서 제시된 인증 기법 [8]-[15]과 비교한다. 본 논문에서는 각 기법의 효율성 비교에 있어서 3가지 항목을 중점적으로 비교했다; 필요한 통신 횟수 (Flow Count), 각 객체가 전송해야 할 통신 비용, 각 객체의 암호 프리미티브 계산 비용. 비교한 결과는 Table 3.에 정리해놓았다. 제시한 기법은 안전한 세션 키 설립부터 데이터의 전송까지 통합적인 시스템이지만, 다른 논문들과의 비교를 위해 센서 데이터 암호화 및 센서 데이터 전송을 제외한 세션 키 설립 과정까지의 연산량을 측정해 비교했다. [8][9][11][12][15]은 대칭키를, [10][13][14]와 본 논문에서 제시한 프로토콜은 공

개키를 사용해 세션키를 설립한다.

하나의 패킷에는 목적지 주소, 데이터 길이 등의 정보가 담긴 프로토콜 헤더가 붙기 때문에 통신 횟수가 많으면 통신 오버헤드가 커진다. 따라서 불필요한 노드의 에너지 소모량을 줄이기 위해 네트워크 통신 횟수는 작을수록 좋다. 제시한 기법은 [12][9]와 더불어 3번의 통신만을 필요로 하는 효율적인 통신 횟수를 가진다.

센서 노드는 한정된 자원을 갖기 때문에 통신 비용과 계산 비용은 낮을수록 좋다. 통신 비용 측면에서 제시한 기법은 [10][14] 다음으로 효율적이었다. 각 노드는 자신의 아이디와 인증서를 전송하면서 통신이 이루어지기 때문에, 상대적으로 낮은 통신 비용으로 세션 키를 만들 수 있었다. 제시한 기법은 인증서를 이용한 상호 인증 단계가 있으므로 다른 공개키 기반 기법들보다 연산량이 조금 더 많다.

5.2 보안 모델 비교

대칭키 기반 기법은 주로 XOR과 해시 연산을 사용하기 때문에 계산 비용이 적지만 네트워크의 확장성이 없으며 완전 순방향 비밀성을 보장하기 힘들다. 드론 기반 무선 센서 네트워크에서 중간 노드로부터 데이터 프라이버시를 지키기 위해서는 *CH*와 *BS*간 보안 서비스를 제공할 수 있어야 한다. 본 논문에서는 Table 4.에 공개키 사용 여부와 보안 서비스 제공 정도를 분석하여 정리해놓았다. 해당 분석에 따르면, 공개키를 사용하면서 모든 객체 간 보안 서비스를 제공할 수 있는 모델은 본 논문에서 제시한 기법이 유일했다.

Table 4. Crypto model & Secure service of each schemes.

	PKC	Security service		
		CH-MS	*MS-BS*	*CH-BS*
[8]	×	○	○	×
[9]	×	○	○	○
[10]	○	○	○	×
[11]	×	○	○	○
[12]	×	○	○	○
[13]	○	○	○	×
[14]	○	○	×	○
[15]	×	○	○	×
Ours	○	○	○	○

5.3 구현 및 비용측정

본 절에서는 MATLAB을 이용해 제안한 모바일 싱크 네트워크를 시뮬레이션하고, 네트워크 통신 비용을 측정한다. 정확한 비교를 위해 본 논문에서 제시한 기법과 네트워크 모델이 비슷한 기법들 [10][13][15]을 대상으로 비교하였다. 실험은 모바일 싱크 노드가 이동하면서 주위의 센서 노드들과 통신할 때 발생하는 메시지를 측정했으며, 논문상의 암호화된 센서 데이터인 Enc_data 및 아래 계층 프로토콜의 오버헤드는 고려하지 않았다. 필드의 총 크기는 500m×500m이며, 센서 노드는 필드에 무작위로 분포된다. 모바일 싱크 노드는 기지국에서 출발하여 정해진 경로에 따라 이동하며 반경 50m 내에 있는 센서 노드와 통신을 시작한다. Fig. 3.은 모바일 싱크 노드가 센서 노드와 통신하며 정해진 경로에 따라 이동하는 것을 보여준다.

본 논문에서 사용한 무선 통신 에너지 소비공식은 [5]에서 제안된 수식인 (1)을 사용한다. [5]에서는 k 비트를 d미터 떨어진 거리에 보낼 때 통신 에너지를 다음과 같이 소비한다.

$$E_j = E_{elec} \times k + E_{amp} \times k \times d^2 \quad (1)$$

E_{elec}는 패킷 전송 회로를 작동시키는데 필요한 에너지이며 $50nJ$로 설정한다. E_{amp}는 증폭 회로를 작동시키는데 필요한 에너지이며 $100pJ$로 설정한다.

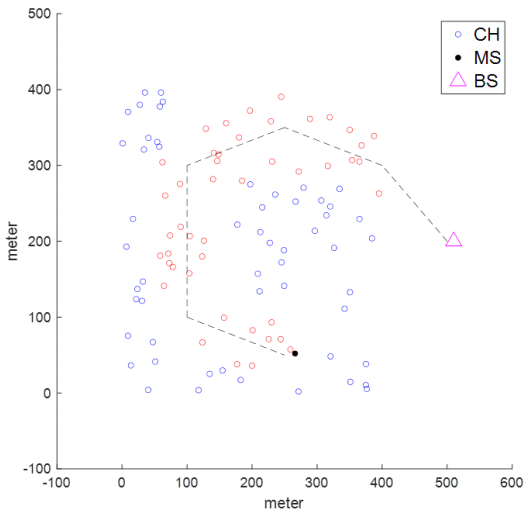

Fig. 3. Network topology

모바일 싱크 노드는 1초마다 근처의 센서 노드들에게 통신 요청 메시지를 보낸다. 실험에 사용한 대칭키 알고리즘은 AES-256이며, 공개키는 타원곡선 암호화의 secp256k1 커브를 사용했다. PUF의 CRP는 128bit로 설정했다. 해시 연산으로는 SHA-256을 사용했다.

5.3.1 네트워크 통신 비용

Fig. 4.는 모바일 싱크 노드가 이동하며 센서 노드와의 양방향 인증을 수행하기까지 소비되는 에너지 소모량을 (1)에 따라 계산한 결과를 보여준다. 실험은 모바일 싱크가 정해진 루트에 따라 이동 후 기지국까지 도착하는 것을 한 라운드로, 1000라운드를 반복하였다. 라운드마다 센서 노드의 위치는 무작위로 배치된다. 제시한 기법은 서명 알고리즘이 쓰이기에 다른 두 기법보다 인증에 필요한 통신 에너지 소모량이 높았다. [15]은 bilinear pairing 연산 기법이 각 인증 단계마다 수행되기 때문에 필요한 통신 에너지 소모량이 가장 높았다. [10]은 해시 연산 기반의 인증을 수행하기 때문에 인증에 필요한 통신 에너지 소모량이 가장 낮았다.

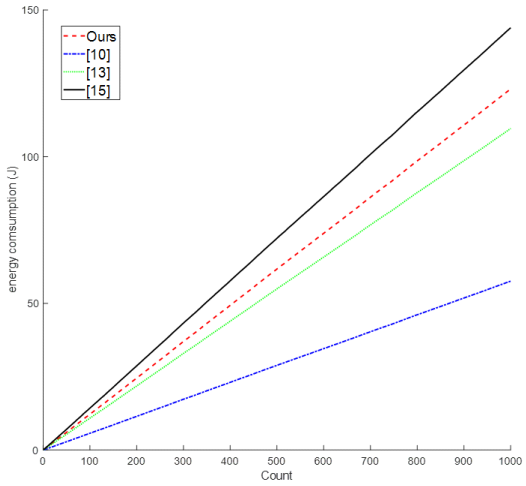

Fig. 4. Energy consumption in data communication

VI. 결 론

본 논문에서는 처음으로 드론 기반 무선 센서 네트워크 환경에서 모바일 싱크 노드로부터 데이터의 프라이버시를 보장할 수 있는 인증 프로토콜을 제시했다. 본 논문은 센서 노드와 기지국 간 안전한 세션 키를 설립하는 과정과 데이터를 기지국까지 안전하게 전송하는 방법을 담고 있다. 제시한 기법은 중간 데이터 전달 노드가 물리적으로 탈취당하더라도 수집된 데이터의 기밀성을 보장할 수 있다. 본 논문에서는 드론 기반 무선 센서 네트워크 환경에서 요구되는 8가지의 보안 요구사항을 정의했으며 우리의 조사에 따르면 최근 제시된 세션 키를 안전하게 만드는 방법을 소개한 프로토콜 중 모든 항목을 만족하는 것은 우리가 유일했다. 또한, 각 항목에 대해 우리 프로토콜의 안전성을 비공식적으로 입증했다. 제시한 기법은 기존 드론 기반 무선 센서 네트워크 환경에서 공개키를 사용한 인증 프로토콜[10][13][14] 보다 효율적이다.

드론 기반 무선 센서 네트워크는 물리적 전송 지연 특성상 여러 대의 모바일 싱크 노드를 이용해 데이터를 중계하는 상황이 나올 수 있다. 하지만, 다수의 싱크 노드가 필드를 돌아다니며 서로 간 인증 및 세션 키를 설립하는 과정에 관한 연구가 부족하다. 따라서 다수의 싱크 노드를 사용하는 환경에서 효율적인 싱크 노드 간 인증, 세션 키 설립, 데이터 중계방법을 후속 연구할 계획이다.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787-2805, May. 2010.

[2] M. Gharibi, R. Boutaba, and S. L. Waslander. "Internet of drones," IEEE Access, vol. 4, pp. 1148-1162, Mar. 2016.

[3] I. Chlamtac, M. Conti, and J. J-N. Liu, "Mobile ad hoc networking: imperatives and challenges," Ad hoc networks, vol. 1, no. 1, pp. 13-64, Jul. 2003.

[4] Y. Yao, and J. Gehrke. "The cougar approach to in-network query processing in sensor networks," ACM Sigmod record, vol. 31, no. 3, pp.

9-18, Sep. 2002.
[5] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," Proceedings of the 33rd annual Hawaii international conference on system sciences. IEEE, Jan. 2000.
[6] R. I. da Silva, and M. A. Nascimento, "On best drone tour plans for data collection in wireless sensor network," Proceedings of the 31st annual ACM symposium on applied computing, Apr. 2016.
[7] J. Tang, H. Huang, S. Guo, and Y. Yang, "Dellat: Delivery latency minimization in wireless sensor networks with mobile sink," Journal of Parallel and Distributed Computing, vol. 83, pp. 133-142, Sep. 2015.
[8] D. B. David, "Secure and efficient mutual adaptive user authentication scheme for heterogeneous wireless sensor networks using multimedia client-server systems," Wireless Personal Communications, vol. 87, no. 3, pp. 1013-1035, May. 2016.
[9] R. Amin, and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," Ad Hoc Networks, vol. 36, pp. 58-80, Jan. 2016.
[10] F. Al-Turjman, Y. K. Ever, E. Ever, and H. X. Nguyen, "Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks," IEEE Access, vol. 5, pp. 24617-24631, Oct. 2017.
[11] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," Ad Hoc Networks, vol. 54, pp. 147-169, Jan. 2017.
[12] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of drones deployment," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3572-3584, Dec. 2018.
[13] Y. K. Ever, "A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications," Computer Communications, vol. 155, pp.143-149, Apr. 2020.
[14] B. D. Deebak, and F. Al-Turjman, "A smart lightweight privacy preservation scheme for IoT-based UAV communication systems," Computer Communications, vol. 162, pp. 102-117, Oct. 2020.
[15] T. Alladi, V. Chamola, and N. Kumar, "PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks," Computer Communications, vol. 160, pp. 81-90, Jul. 2020.
[16] W. Jongho, S. Seung-Hyun, and E. Bertino, "Certificateless cryptographic protocols for efficient drone-based smart city applications," IEEE Access, vol. 5, pp. 3721-3749, Mar. 2017.
[17] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," International workshop on cryptographic hardware and embedded systems. Springer, pp. 11-132, 2004.

〈저자소개〉

오 상 윤 (Sang Yun Oh) 학생회원
2019년 2월: 백석대학교 정보보호학과 졸업
2019년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 프라이버시 향상 기술, 블록체인, IoT

정 재 열 (Jae Yeol Jeong) 학생회원
2010년 2월: 고려대학교 수학과 졸업
2013년 8월: 고려대학교 정보보호대학원 정보보호학과 석사
2013년 9월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 암호 프로토콜, 프라이버시 향상 기술, 생체인증

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

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