JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 9, pp. 81-90, September 2020
https://doi.org/10.9708/jksci.2020.25.09.081

PUF-based Secure FANET Routing Protocol for Multi-Drone

Yoon-Gil Park*, Soo-Jin Lee*

*Student, Dept. of Computer Science and Engineering, Korea National Defense University, Nonsan, Korea
*Professor, Dept. of Computer Science and Engineering, Korea National Defense University, Nonsan, Korea

[Abstract]

In order to operate multi drone efficiently, existing control methods must be improved, and drones must be able to construct communication networks autonomously. FANET(Flying Ad-Hoc Network), which is being considered as an alternative to solving these problems, is based on ad hoc network technology and can be exposed to a variety of security vulnerabilities. However, due to the limited computational power and memory of FANET nodes, and rapid and frequent changes in network topology, it is not easy to apply the existing security measures to FANET without modification. Thus, this paper proposes lightweight security measures applicable to FANET, which have distinct characteristics from existing ad hoc networks by utilizing PUF technology. The proposed security measures utilize unique values generated by non-replicable PUFs to increase the safety of AODV, FANET's reactive routing protocol, and are resistant to various attacks.

▸ **Key words**: Routing Protocol, PUF, FANET, Drone, Authentication, AODV

[요 약]

군집 드론을 효율적으로 운영하기 위해서는 기존 통제방식이 개선되어야 하며, 드론들이 자율적으로 통신망을 구성할 수 있어야 한다. 이러한 문제를 해결하기 위한 대안으로 검토되고 있는 FANET(Flying Ad-Hoc Network)은 애드혹 네트워크 기술을 기반으로 하고 있어 다양한 보안취약점에 노출될 수 있다. 그러나 FANET 노드들의 제한적인 연산능력과 메모리, 급격하고 잦은 네트워크 토폴로지 변화 등으로 인해 애드혹 네트워크에 제안되었던 보안대책을 수정 없이 FANET에 그대로 적용하는것은 쉽지 않다. 이에 본 논문에서는 PUF 기술을 활용하여 기존 애드혹 네트워크와는 차별화된 특성을 가지는 FANET에 적용 가능한 경량화된 보안대책을 제안한다. 제시된 보안대책은 복제 불가능한 PUF에서 생성되는 고유한 값을 활용하여 FANET의 Reactive 라우팅 프로토콜인 AODV의 안전성을 높이며, 다양한 공격에 대한 내성을 가진다.

▸ **주제어**: 라우팅 프로토콜, PUF, FANET, 드론, 인증, AODV

• First Author: Yoon-Gil Park, Corresponding Author: Soo-Jin Lee
*Yoon-Gil Park (qkrdbsrlf@gmail.com), Dept. of Computer Science and Engineering, Korea National Defense University
*Soo-Jin Lee (cyberkma@gmail.com), Dept. of Computer Science and Engineering, Korea National Defense University
• Received: 2020. 07. 24, Revised: 2020. 09. 15, Accepted: 2020. 09. 15.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

환경 모니터링, 재난지역에서의 상황파악, 수색 및 구조, 주둔지 경계 및 감시 등 다양한 분야에서 핵심적인 역할을 수행하고 있는 드론은 대부분 1대의 드론을 지상 통제시스템(Ground Control System, 이하 GCS)을 이용하여 통제하는 방식으로 운용되고 있다. 그러나 최근 들어서는 다수의 드론으로 구성된 군집 드론 운용의 필요성이 증대되면서 다수의 드론을 동시에 효율적으로 통제하는 방안에 대한 연구가 활발하게 진행되고 있다. 국방 분야에서도 드론 Bot 전투단을 창설하고 군집 드론의 전술적 운용 방안을 연구하고 있다.

군집 드론의 운용을 위해 필수적으로 고려해야 할 요소는 바로 통신이다. 일반적으로 드론은 위성 또는 GCS 간의 무선통신을 기반으로 운용되기 때문에, 사전에 통신을 위한 기반 인프라가 갖추어져 있어야만 한다. 그러나 재난상황 및 전장 환경에서 긴급하게 군집 드론을 운용해야할 경우 통신을 위한 기반환경을 신속하게 구축하는것은 쉽지 않다. 위성의 경우에는 통신 범위의 제약을 적게 받지만 GCS와의 무선통신을 기반으로 하는 드론은 통신 범위에 심각한 제한을 받기 때문에 통신 범위를 벗어난 원거리 임무 수행은 불가능하다. 따라서 군집 드론을 다양한 상황에서 효율적으로 운용하기 위해서는 통신 범위와 기반구조에 영향을 받지 않고 드론들이 자율적으로 통신할 수 있는 기술의 적용이 반드시 고려되어야 한다.

군집 드론 운용에 적합한 자율 네트워크 구성을 위해 최우선으로 고려해 볼 수 있는 대안은 Flying Ad-Hoc Networks(이하 FANET) 기술이다. FANET은 모바일 애드혹 네트워크(Mobile Ad-Hoc Network 이하 MANET)를 기반으로 만들어진 통신기술로서, 사전에 구축된 통신 기반구조가 없더라도 다수의 드론이 동시에 상호 데이터를 전송할 수 있게 해준다. 그러나 FANET은 MANET과 기본적인 특성을 공유하기 때문에 다양한 보안취약점에 노출될 수 있다. 따라서 다양한 분야에서 활용 가능성이 증대될 FANET을 보다 안전하게 운용하기 위해서는 보안대책에 대한 연구도 반드시 병행되어야 한다.

FANET을 위한 보안대책을 수립함에 있어서는 MANET 및 VANET(Vehicle Ad-Hoc Network)과는 차별화되는 FANET만의 고유한 특성을 반드시 고려해야만 한다. 노드들의 높은 이동성으로 인한 잦은 토폴로지 변화, 적은 메모리와 낮은 연산능력, 제한된 배터리 등으로 요약할 수 있는 FANET만의 고유한 특성은 많은 연산을 필요로 하는 보안대책의 적용을 어렵게 만든다. 또한, 이륙 중량의 제한으로 인해 보안의 구현을 위한 추가적인 하드웨어 탑재도 쉽지 않다. 따라서 FANET에서 효율적으로 보안대책을 구현하기 위해서는 잦은 토폴로지 변화와 자원의 제약에 능동적으로 대응할 수 있도록 보다 경량화된 형태를 가져야만 한다.

이에 본 논문에서는 칩 수준에서 발생하는 물리적 특성을 활용하여 보안을 구현하는 PUF를 기반으로 군집 드론으로 구성된 FANET 환경에 적용 가능한 경량화된 라우팅 프로토콜 보안대책을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 FANET의 개념과 특징, 라우팅 프로토콜 및 보안대책, PUF 기술 등에 대해 살펴본다. 3장에서는 PUF 기술을 활용하여 FANET의 AODV 라우팅 프로토콜의 안전성을 강화할 수 있는 방안을 제안한다. 4장에서는 기존의 안전한 라우팅 프로토콜들과의 비교를 통해 제안한 방안의 효율성을 검증하고, 마지막으로 5장에서 결론을 맺는다.

II. Preliminaries

1. Related works

1.1 Flying Ad-Hoc Network(FANET)

FANET은 UAV 및 드론과 같은 공중노드로만 구성되는 애드혹 네트워크 구조이기 때문에 애드혹 네트워크가 가지는 기본적인 특성을 그대로 가진다. 그러나 MANET 및 VANET 등과는 차별화되며 보안대책의 구현을 어렵게 만드는 특성들도 존재한다. 우선 FANET은 네트워크를 구성하는 노드들의 이동성이 상대적으로 높아 토폴로지가 자주 변경되고, 노드 간 이격거리는 다른 형태의 애드혹 네트워크에 비해 더 멀다. 통신 범위도 기존 MANET 및 VANET보다 길며, 물리적인 노드의 크기가 작아 이륙 중량이 제한된다[1]. 연산능력, 전력, 메모리 등에서도 기존 애드혹 네트워크들에 비해 더 큰 제약을 받는다.

FANET의 라우팅 방법은 기존 애드혹 네트워크의 라우팅 방식과 유사하다. FANET의 주요 라우팅 방법은 크게 Static, Proactive, Reactive, Hybrid 등 4가지 방법으로 구분할 수 있다. ① Static 방식 : 임무 전 드론에 정적인 라우팅 정보를 입력하며, 비행하는 동안 라우팅 정보 업데이트가 이루어지지 않는다. ② Proactive 방식 : 테이블 중심(Table-driven)의 라우팅 방식으로 드론들의 토폴로지가 바뀌면 라우팅 테이블이 업데이트된다. 그러나 노드 들의 높은 이동성으로 인해 토폴로지가 자주 바뀌는 FANET에서는 적용하기 쉽지 않은 방식이다. 대표적으로 DSDV와 OLSR이 있다. ③ Reactive 방식 : On-Demand 방식의 프로토콜

로 두 노드 사이에 통신이 없으면 경로 정보를 저장할 필요가 없고 통신 요구가 있을 때만 경로를 설정한다. 대표적인 프로토콜로는 DSR과 AODV가 있다. 마지막으로 ④ Hybrid 방식 : Proactive 방식과 Reactive 방식을 결합한 형태로 대표적인 프로토콜은 ZRP와 TORA가 있다[2].

1.2 AODV routing protocol and Security measures

C.Perkins에 의해 '99년에 제안된 AODV는 DSDV를 On-Demand 방식으로 적용하기 위해 DSR의 장점을 결합한 프로토콜로써, 경로획득을 위하여 경로 발견, 경로설정, 경로 유지관리의 3가지 단계를 수행하여 경로획득 후 통신을 수행한다[3-4]. 애드혹 네트워크에서 가장 효율적 프로토콜로 알려져 있기는 하지만, 보안 메커니즘이 존재하지 않아 다양한 공격에 취약하기 때문에 이를 해결하기 위한 연구들도 진행되었다.

ARAN(A secure routing protocol for ad hoc networks)[6]은 공개키 암호 기반의 전자서명과 인증서를 통해 각 노드가 매 홉(hop-by-hop)마다 인증을 수행한다. 따라서 강력한 라우팅 보안을 제공할 수 있지만, 공개키 연산의 반복적인 수행으로 인해 배터리 소모가 증가할 수 있다. 또한, 인증서를 발급하는 신뢰할 수 있는 서버가 항상 온라인상에 존재해야 한다.

SAODV(Securing Ad Hoc routing protocol)[7]는 경로획득과정에서 RREQ(Route Request) 및 RREP(Route Reply) 패킷이 변조되는 것을 방지하기 위해 전자서명 및 해시 체인을 사용한다. 따라서 ARAN과 유사하게 공개키 연산으로 인한 오버헤드가 발생할 수 있다. 그리고 공격자가 패킷 내 정상 IP 위조 및 DoS 공격과 같은 유효하지 않은 서명이 있는 패킷을 생성 및 전송하여 정상 경로설정을 방해할 수도 있다[5][9].

SEAR(A secure efficient ad hoc on demand routing protocol for wireless networks)[8]는 공개키 연산에 의한 오버헤드를 줄이기 위해 초기 부트스트래핑 단계에서만 공개키 암호를 사용하고, 이후에는 대칭 키 암호를 사용한다. 따라서 ARAN[6]과 SAODV[7]에 비해 연산량이 감소하여 전체적인 오버헤드 측면에서는 우수하다. 그러나 RERR(Routing Error) 패킷을 보호하기 위해 TESLA[10] 인증체계에서 공개키 암호화 방식을 사용하여 네트워크 오버헤드가 증가하며, 느슨한 시간 동기화를 요구하는 TESLA의 특성으로 인해 DoS 공격에 취약하다는 단점을 가진다[9].

SEAODV(Secure Efficient AODV routing protocol for MANETs networks)[9]는 AODV의 시퀀스 번호와 홉수 및 라우팅 패킷을 보호하기 위해서 단방향 해시함수와 HEAP(Hop-by-hop authentication protocol) 인증체계를 사용한다[9]. 대칭 키 암호를 기반으로 하기 때문에 이전에 제시되었던 접근방법들에 비해 연산 수행에 의한 오버헤드가 크게 감소하고, 보안성 측면에서 향상되었다고 평가를 받는다. 그러나 AODV에 비해 7.5%의 오버헤드가 발생하였고, 패킷 전송률 또한 0.9%가 감소하는 문제가 발생하였다[9].

이상에서 살펴본 AODV 라우팅 프로토콜을 위한 보안 대책들은 대부분 암호연산 수행에 따른 오버헤드가 커서 낮은 연산능력과 배터리 성능을 가지는 소형 드론에 적용하기는 어렵다. 또한, 전자서명이나 인증서를 통한 검증을 수행하기 위해서는 중앙집중방식으로 GCS에 의존할 수밖에 없어 임무 수행범위가 제한되며, 통신 범위 밖에서의 임무 수행 간에는 상호인증이나 안전한 경로획득단계 절차 수행이 불가능해진다.

1.3 Physical Unclonable Function(PUF)

PUF는 물리적으로 복제 불가능한 반도체를 개발하기 위해 창안된 기술로서, 반도체 제조 공정상에서 발생하는 미세한 공정 편차를 이용하여 반도체 칩 내부에서 예측하기 어려운 무작위 값을 생성하는 시스템을 의미한다[11][12]. 각각의 PUF는 'Challenge' 라고 불리는 입력값이 동일해도 서로 다른 'Response' 라는 출력값을 생성한다. 생성되는 출력값에 대해서는 예측 불가능성, 무작위성, 신뢰성이 보장되며, 이러한 특성들을 기반으로 물리적 복제 불가능성을 만족시킨다. PUF는 지연기반의 PUF(Mismatch-based PUF)와 물리적 특성기반의(Physical-based PUF)로 구분된다. 지연기반 PUF는 제작되는 소자 또는 회로의 특성이 반도체 제조 공정 과정에서 발생하는 공정 편차에 의해 각각의 고유한 특성을 갖게 되는 점을 이용한 PUF로 대표적으로는 Arbiter PUF가 있다. Arbiter PUF의 동작 방식은 <그림 1>에서 보는 바와 같다[11]. 이러한 지연기반의 PUF는 외부 환경 및 전압, 온도 등으로 지연시간이 달라질 수 있다는 단점을 가지고 있으며, 이를 보완하기 위해 오류정정 코드(Error Correction Code)에 대한 후처리 작업을 수행한다[13].

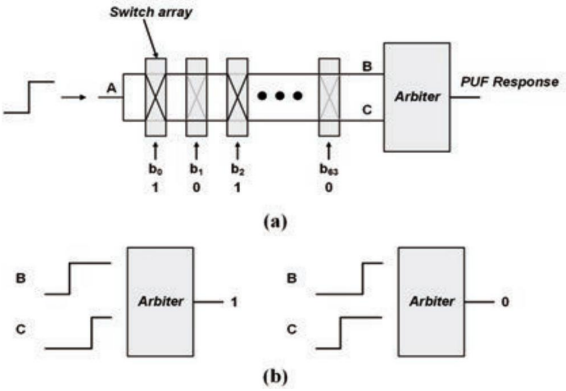

Fig. 1. Mismatch based Arbiter PUF

물리적 특성기반의 PUF는 출력값이 반도체 내 전도성 계층의 물리적 상태에서 결정되는 PUF를 말하며, 반도체 제조 공정에서 인접한 두 전도성 계층 간 연결 상태가 Open이면 0, Short이면 1의 출력값을 가진다. 대표적으로 VIA PUF가 있다. 여기서 VIA는 두 Metal 계층을 수직으로 연결하는 역할을 하며, VIA Hole 크기에 따라 VIA 형성 확률이 달라지며, 노이즈와 환경에 의해 상태가 변하지 않아 별도의 Error Correction Code와 같은 후처리 작업이 불필요하다. VIA PUF 회로 구성은 <그림 2>에서 보는 바와 같다[12].

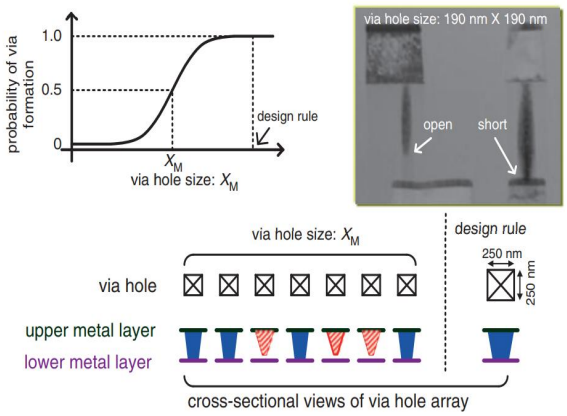

Fig. 2. Physical-based VIA-PUF circuit composition

III. The Proposed Scheme

1. PUF-based Secure Routing Protocol

본 논문에서 제안하는 드론 간 상호인증 및 경로획득절차는 AODV 라우팅 프로토콜에 PUF 기술을 적용하여 GCS에 의존하지 않고 드론 간 자체적인 통신을 수행한다. 경로획득 절차 간 사용되는 표기법은 <표 1>에서 보는 바와 같다.

Table 1. Notation

S	IP address of source drone
D	IP address of destination drone
BC_{id}	Specific number of RREQ (RREQ ID)
D_i	ID of the drone
$C_i^{D_i}$	Input (Challenge) value of D_i
$R_i^{D_i}$	Output(Response) value of D_i
s_n	Sequence number of source drone
d_n	Sequence number of destination drone
h	Hop Count
life-time	Valid time of generated path
Key_{D_i, D_j}	Temporary session keys generated between D_i and D_j
ACK	Confirmation messages
CRP_{pre}	CRP Table saved by existing drone group
CRP_{New}	CRP Table including CRP of new drone

1.1 Small Multi-Drone Registration Phase

생산업체는 생산 과정 중 드론 내부 IC에 PUF 칩을 장착하고, 해당 드론들을 군 인증센터로 납품한다. 인증센터는 납품된 모든 드론에 대해 고유의 ID를 부여하고, 각 드론 내 PUF 칩을 이용하여 Challenge 값에 대한 Response 값의 쌍을 1,000~10,000개 정도 생성하여 CRP(Challenge-Response Pair) 테이블을 구성하고 ID와 함께 안전한 서버에 저장한다. 인증센터 내 서버에 저장될 CRP 테이블의 형태는 <표 2>에서 보는 바와 같다.

Table 2. CRP Table Contents

Drone #1 (ID : D_1)	$C_1^{D_1} - R_1^{D_1}$
	$C_2^{D_1} - R_2^{D_1}$
	$C_3^{D_1} - R_3^{D_1}$
	⋮
Drone #2 (ID : D_2)	$C_1^{D_2} - R_1^{D_2}$
	$C_2^{D_2} - R_2^{D_2}$
	$C_3^{D_2} - R_3^{D_2}$
	⋮
⋮	⋮

운용부대는 인증센터로부터 드론들을 인수받으면서 각 드론의 ID와 CRP(Challenge-Response Pair)를 함께 전달받아 GCS 내의 관리 서버에 저장한다. 이 때 관리 서버 내에 저장된 CRP는 안전하다고 가정한다.

1.2 Multi-Drone CRP Table Generation Phase

운용부대는 군집 드론에 편성되어 작전에 참여할 드론들이 결정되면, 모든 드론에 대해서 필드에 배치되기 전에 <표 3>에서 보는 바와 같은 CRP 테이블을 작성하여 드론에 장착된 비휘발성 메모리(NVM)에 저장한다. 작전에 참여하는 각 드론은 자신의 CRP만 제외하고 나머지 드론들에 대해서 관리자가 임의로 선택한 CRP를 저장하게 되며, 자신에 대해서는 다른 드론들과의 인증에 사용할 Response 값을 생성하기 위한 Challenge 값만을 저장한다. <표 3>은 D_1이라는 ID가 할당된 드론에 저장될 CRP 테이블의 예를 보여주고 있으며, D_1을 제외한 나머지 드론들은 D_1에 대한 CRP를 저장한다.

Table 3. Example of CRP Table for Drone D_1

ID	CRP
D_1	$C_{35}^{D_1}$
D_2	$C_{107}^{D_2} - R_{107}^{D_2}$
⋮	⋮
D_i	$C_{200}^{D_i} - R_{200}^{D_i}$
⋮	⋮

1.3 Route Discovery Phase

AODV 라우팅 프로토콜은 경로 발견단계에서 다음과 같은 RREQ 패킷을 네트워크로 브로드캐스트하여 목적지까지의 최적 경로를 탐색한다.

$$\{S, D, BC_{id}, s_n, d_n, h\} \quad (1)$$

S는 경로설정을 요청한 출발지 드론의 IP주소, D는 목적지 드론의 IP주소를 의미하며, BC_{id}는 RREQ 패킷의 고유번호로서 RREQ 패킷을 전송할 때마다 순차적으로 증가시킨다. s_n과 d_n은 출발지 및 목적지 드론의 시퀀스 번호, h는 홉 수를 의미한다[14]. 수식 (1)에서 보는 바와 같이 AODV의 RREQ 패킷은 보안성을 고려하지 않아 다양한 공격에 취약하다.

본 논문에서 제안한 PUF 기반의 라우팅 프로토콜에서는 군집 드론 운용에 참여하는 각각의 드론이 전체 드론에 대한 CRP 테이블을 가지고 있으므로 출발지 드론은 ID (D_s)와 함께 자신의 Response 값($R_i^{D_s}$)으로 s_n, d_n, h을 암호화한 RREQ 패킷을 네트워크로 브로드캐스트한다. 제안된 기법의 RREQ 패킷 구조는 다음과 같다.

$$D_s, \{S, D, BC_{id}, E_{R_i^{D_s}}(s_n, d_n, h)\} \quad (2)$$

RREQ 패킷을 수신한 중간드론(D_k)은 비휘발성 메모리(Non-volatile memory, 이하 NVM)에 저장된 CRP 테이블에서 출발지 드론의 Response 값을 확인 후 해당 Response 값을 이용하여 암호화된 패킷을 복호화하고 시퀀스 번호 및 홉 수 위조 여부를 검증한다. 이상이 없으면 h를 1 증가시켜 수식 (3)과 같은 RREQ 패킷을 만든 후 자신의 Response 값($R_i^{D_k}$)으로 암호화하여 자신의 ID와 함께 다시 브로드캐스트한다.

$$D_k, \{S, D, BC_{id}, E_{R_i^{D_k}}(s_n, d_n, h+1)\} \quad (3)$$

만약 검증 과정에서 시퀀스 번호 및 홉 수의 위조가 확인되었다면 해당 RREQ 패킷을 무시한다.

1.4 Route Setup Phase

경로설정 단계에서는 RREQ 패킷을 수신한 목적지 드론이 출발지 드론에게 RREP 패킷을 유니캐스트 하여 통신 경로를 설정한다. 출발지 드론이 RREP 패킷을 수신하면 통신을 위한 경로설정 단계가 완료된다. RREP 패킷 구조는 다음과 같다.

$$\{S, D, d_n, h, lifetime\} \quad (4)$$

RREP 패킷은 경로상의 드론들에게 유니캐스트로 패킷을 전송하므로 이전 홉 드론의 ID를 RREP 패킷에 추가하여 전송할 필요가 없으며, RREQ 패킷의 BC_{id}와 출발지 드론의 시퀀스 번호를 제외하고 RREP 패킷에서 생성된 경로의 유효한 시간을 결정하기 위해서 life-time을 추가하여 전송한다[12]. 그러나 AODV는 목적지 드론에서 RREP 패킷을 전송할 때 보안 메커니즘을 사용하지 않아 위조 공격에 취약하다.

제안된 PUF 기반의 라우팅 프로토콜에서는 각 드론이 자신의 NVM에 저장된 전체 드론의 CRP 테이블을 이용하여, 홉 바이 홉 간 무작위로 선택된 3개의 Challenge 값에 대한 Response 값으로 임시 세션 키를 생성하여 d_n, h을 암호화 후 전송한다. 제안기법의 RREP 패킷 구조는 다음과 같다.

$$\{S, D, E_{Key_{D_s, D_k}}(d_n, h), lifetime\} \quad (5)$$

S→A→B→D의 경로를 설정한다고 가정하였을 때, D는 S에게 RREP 패킷을 전송하기 위해 B와 임시 세션 키 생성절차를 수행한다. ① D는 B에게 CRP 테이블에 있는 전체 드론의 CRP 중 3개의 Challenge 값을 무작위로 선택하여 B에게 전송하고, ② B는 수신한 3개의 Challenge 값에 대한 Response 값을 XOR 연산하여 임시 세션 키 $E_{key_{D_b, D_d}}$를 생성한다. ③임시 세션 키 생성을 완료한 B는 D에게 ACK를 임시 세션 키로 암호화하여 전송한다. ④ D도 B와 같은 임시 세션 키 생성절차를 수행 후 암호화된

ACK 메시지를 복호화하여 상호인증이 완료되면, 임시 세션 키로 d_n, h을 암호화 후 B에게 RREP 패킷을 전송한다. 임시 세션 키 생성절차는 RREP 패킷이 출발지 드론에 도착할 때까지 반복된다.

세부 경로설정 단계는 <그림 3>과 같다.

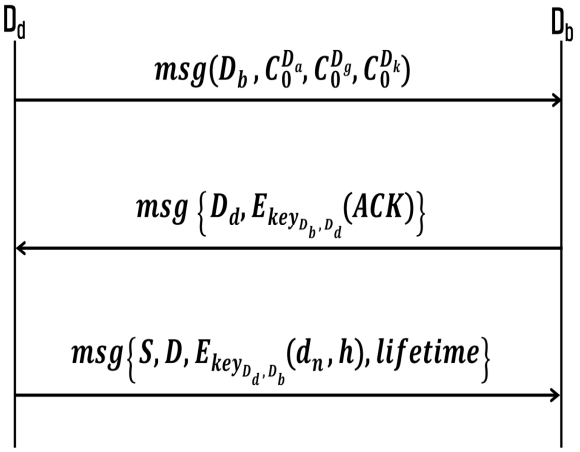

Fig. 3. PUF-based Routing setup phase

1.5 Route Maintenance Phase

RERR 패킷은 연결된 통신 경로가 단절되는 경우 해당 경로가 사용 불가하다는 정보를 알리기 위해서 사용되며, 경로에 포함된 드론들에게 유니캐스트로 전송되며, 패킷의 구조는 다음과 같다.

$$\{D, d_{n+1}, h\} \quad (6)$$

단절된 목적지 드론의 주소 D와 증가된 목적지 시퀀스 번호 d_n이 포함된다. 그러나 패킷이 보호되지 않은 상태에서 전송되기 때문에 위조 공격에 취약하여 공격자가 정상 드론의 연결을 강제로 단절시킬 수 있고 경로획득 절차를 수행하도록 강요할 수 있다. 이러한 공격을 방지하기 위하여 변경된 RERR 패킷의 구성은 다음과 같다.

$$\left\{E_{key_{D_b,D_a}}(D, d_{n+1}, h)\right\} \quad (7)$$

S←A←B 경로로 RERR 패킷을 전송한다고 가정할 때, B는 A와 상호 임시 세션 키를 생성한다. 임시 세션 키 생성절차는 3, 4절에서 기술한 절차와 동일하다. 임시 세션 키가 생성된 후 RRER 패킷을 전송할 B는 D, d_{n+1}, h을 생성한 임시 세션 키로 암호화 후 전송한다. 이를 수신한 A는 임시 세션 키를 활용하여 복호화 후 무결성을 검증한다. 해당 절차는 RERR 패킷이 출발지 드론에 수신될 때까지 반복하여 수행한다. RERR 패킷의 전송 절차는 <그림 4>에서 보는 바와 같다.

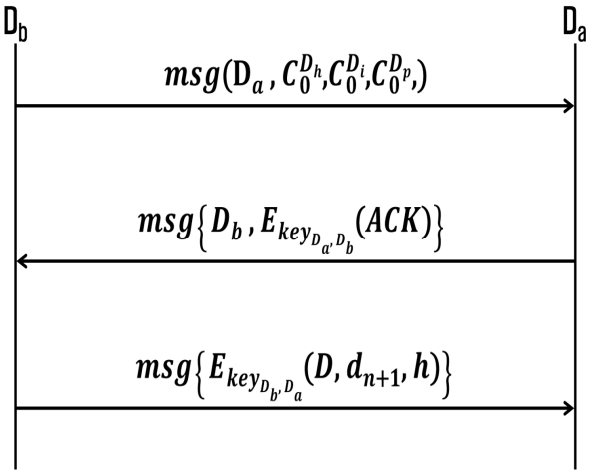

Fig. 4. PUF-based Routing Maintenance phase

1.6 New Drone Join Phase

소형 군집 드론은 자원 제한적인 특성들로 인하여 임무 도중 많은 문제가 발생할 수 있다. 이러한 문제들은 임무 수행에 지대한 영향을 미칠 수 있으며, 통신단절의 원인이 될 수 있다. 본 절에서는 크게 물리적 결함(배터리 문제, 시스템 결함)과 공격자에 의한 격추 및 탈취 상황만을 고려한다.

임무 수행 도중 드론이 갑작스럽게 그룹에서 이탈하였을 시 필요에 따라 단절된 드론의 임무를 대체할 새로운 드론을 투입해야 한다. GCS 기반의 중앙집중식 통제방식은 새로운 드론이 드론그룹에 참가할 경우 기존 드론들은 지상 서버와의 통신을 통해 새로운 드론이 정상 드론이 맞는지를 검증해야 한다. 그러나 이러한 검증방식은 기반시설이 없거나 서버와의 통신이 제한되는 상황에서는 드론그룹이 신규 드론을 검증할 수 없어 드론그룹이 GCS와 통신을 정상적으로 수행할 수 있을 때까지 신규 드론의 그룹 참가는 불가능하다.

이를 보완하기 위해 제안된 PUF 기반의 안전한 라우팅 프로토콜에서는 드론 내 저장된 CRP 테이블을 이용하여 GCS와의 통신 없이도 신규 드론과 드론그룹이 자율적으로 인증 및 가입절차를 수행할 수 있다. 최초 군집 드론은 소형 드론 40대로 구성하며, 모든 드론은 각 NVM 내에 나머지 39대에 대한 CRP_{pre}을 안전하게 저장하고 이륙 이후 정상적으로 동작한다고 가정한다. 신규 드론의 가입절차는 다음과 같이 진행된다. ① 임무 수행 중 갑작스러운 기체결함 및 공격자의 탈취 및 격추 행위로 D_d가 드론그룹에서 이탈한다. ② D_d의 인접 드론 D_3이 경로단절을 식별하여 RERR 패킷을 경로 내 모든 드론에게 전송한다.

③ 지상에서는 D_d를 대체할 D_{41}을 준비하고 드론 간 자율적인 인증절차 수행을 위해 드론그룹이 저장한

CRP_{pre}에 D_{41}의 CRP를 추가한 CRP_{New}을 NVM 내 저장 후 드론그룹으로 이동한다. 이때, CRP_{New}에는 향후 D_d의 복귀 후 재 가입절차를 수행하기 위해 D_d의 CRP까지 저장한다.

④ D_{41}은 CRP_{pre}의 모든 Response 값을 XOR 연산하여 암호키 $E_{key_{41}} = R_{20}^{D_S} \oplus R_7^{D_1} \oplus \cdots R_1^{D_{40}}$을 생성하고 CRP_{New}을 $E_{Key_{41}}(CRP_{New})$로 암호화하여 전체 드론에 브로드캐스트 한다. ⑤ 이를 수신한 드론그룹은 자신의 CRP Table 내 모든 Response 값을 XOR 연산하여 암호키를 생성 후 $D_{Key_{40}} = [E_{Key_{41}}(CRP_{New})]$로 복호화 후 $CRP_{pre} \equiv CRP_{New-D_{41}}$이면 CRP_{New}로 업데이트한다. 신규 드론 가입절차는 <그림 5>와 같다.

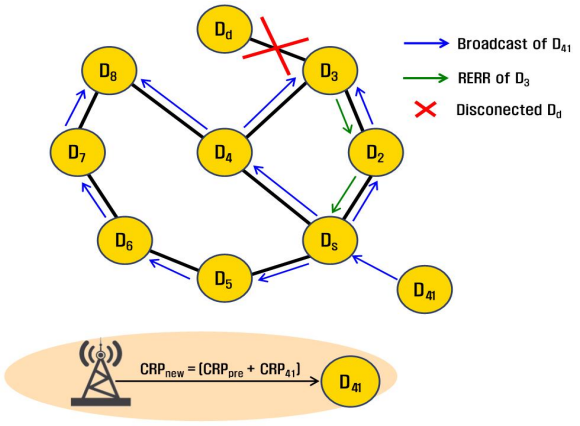

Fig. 5. New Drone Join Phase

1.7 Secure CRP Table Protection Plan

제안한 PUF 기반의 라우팅 프로토콜은 GCS에 의존하지 않고 드론 간 자율적인 통신을 수행하기 위해 고유한 각 드론의 PUF 칩에서 생성된 CRP가 필요하다. CRP는 기본적으로 지상 서버에 안전하게 저장되어 관리된다고 가정하나, 문제는 임무에 투입되는 드론의 NVM에 저장된 CRP 테이블이 공격자로부터 어떻게 안전하게 보호할 것인지에 대한 부분이다.

특정 기기 혹은 장비에 저장된 중요 정보나 암호키 등을 안전하게 보호하기 위해 하드웨어 및 소프트웨어 측면에서의 보안대책이 다수 제안되었다. 그러나 기존에 제안되었던 보호 대책 중 보안 모듈을 활용하는 하드웨어적 보호대책은 소형 군집 드론의 이륙중량 제한으로 인해 적용하기가 쉽지 않다. 또한, AES, DES, RSA 등의 다양한 암호화 알고리즘을 기반으로 정보를 보호하고자 시도했던 소프트웨어 기반의 보호 대책은 암호연산의 수행으로 인해 큰 오버헤드가 발생한다. 따라서 낮은 연산능력과 제한된 배터리를 가지는 소형 군집 드론에 적용하기는 어렵다.

본 연구에서는 소형 드론의 자원 제약적 특성에 영향을 받지 않으면서 CRP 테이블을 안전하게 보호하기 위해 PUF를 활용한다. 각 드론은 이륙 전 지상에서 전체 드론에 대한 CRP를 테이블 형태로 NVM에 저장하는 과정에서 각 드론의 특정 Challenge 값에 대한 고유한 Response 값과 전체 드론의 CRP를 XOR 연산하여 암호화된 상태로 각 드론의 NVM에 저장한다. 암호화에 사용된 Response 값 생성을 위한 임의의 Challenge 값은 NVM에 저장되나, Response 값은 NVM에 저장되지 않고 다시 물리적 상태로 돌아가므로 공격자는 드론을 탈취해도 암호화되지 않은 특정 Challenge만을 획득하게 되고, 암호화에 사용된 고유한 Response 값은 알지 못해 암호화된 CRP 테이블을 복호화할 수 없다. PUF 칩의 고유한 CRP값을 활용한 안전한 CRP 테이블 보호 방안은 <그림 6>과 같다.

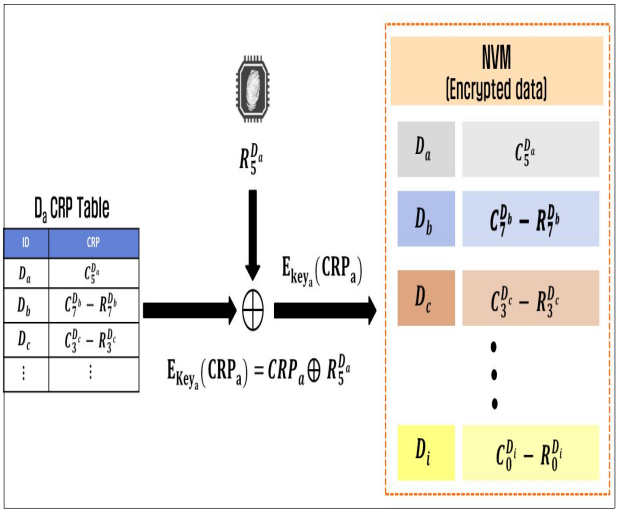

Fig. 6. PUF based CRP Table protection plan

IV. Comparison to Performance and Attack Resistance

1. Performance

본 절에서는 기존 AODV 라우팅 프로토콜들 보안대책들과 제안하는 기법을 인증방식, 연산량, 네트워크 오버헤드, 사전 키 공유측면에서 비교한다.

① 인증방식 : ARAN[6]에서는 공개키를 이용한 디지털 서명과 인증서를 통해서 매 홉 간 인증을 수행한다. SAODV[7]도 공개키 기반의 디지털 서명과 해시 체인을 통

해서 인증절차를 수행한다. SEAR[8]는 초기 부트스트래핑 단계에서만 공개키 인증방식을 사용하며, RERR 패킷의 인증을 위해 공개키기반의 TESLA 인증체계를 활용한다. SEAODV[9]은 대칭 키 방식으로 단방향 해시함수와 HEAP 인증체계로 인증을 수행한다. 제안하는 기법은 별도의 키를 생성하지 않고, 고유한 PUF 칩의 특정 Challenge 값에 대한 Response 값의 CRP로 인증을 수행한다.

② 연산량 : ARAN[6]과 SAODV[5]는 비대칭 암호와 디지털 서명이 사용하여 많은 연산량을 요구한다. SEAR[8]는 RERR 패킷인증에 비대칭 암호화가 사용된다. SEAODV[9]는 단방향 해시함수와 해시 체인으로 인증을 수행한다. 제안하는 기법은 별도의 키 및 암호화 체계를 사용하지 않고 Challenge에 대한 Response 값으로 인증하여 적은 시간과 계산량만이 필요하다.

③ 네트워크 오버헤드 : ARAN[6]은 각 패킷에 대해 인증서와 서명을 추가하여 오버헤드가 높다. SAODV[7]는 각 라우팅 패킷에 디지털 서명과 해시함수가 포함되어 오버헤드가 발생한다[9]. SERA[8]는 해시 체인의 사용으로 디지털 서명보다 오버헤드가 적으나, RERR 인증 간 TESLA 인증체계 적용으로 인해 큰 오버헤드가 발생한다. SEAODV[9]는 해시 키 사용으로 SEAR보다 오버헤드가 적으나 AODV와 비교 시 7.5%의 오버헤드가 증가하였다.

④ 사전 키 공유에 의한 문제점 : 제안하는 보호 대책에서는 오로지 NVM 내 저장된 CRP 테이블만을 활용하므로 오버헤드가 적다. [6-9]의 제안된 기법들은 사전에 키 공유를 수행하며, 이러한 사전 키 공유는 초기 키 노출 등의 문제를 발생시킬 수 있다. 제안기법은 복제 불가능한 PUF의 CRP만을 활용해 사전 키 공유가 불필요하여 초기 키 노출의 위협을 배제할 수 있다. 성능 비교 결과를 요약하면 <표. 4>와 같다.

Table 4. Comparison to previous Protocol

	Authentication	Computation	Over head	Pre-key share
[6]	Digital signature	high[9]	high[9]	O
[7]	Digital signature, MAC	high[9]	medium [9]	O
[8]	one way hash, TESLA	medium[9]	RERR high[9]	O
[9]	one way hash, HEAP	low then [8][9]	7.5% more than AODV[9]	O
Pro posed	PUF's CRP	low	low	X

2. Attack Resistance

2.1 Sequence Number and Hop Count

AODV의 모든 패킷은 시퀀스 번호와 홉 수 자체를 보호하지 않아 공격자에 의한 위조 공격에 취약하였다. 제안기법은 각 드론이 전체 드론에 대한 CRP를 NVM 내 테이블 형식으로 저장함으로 출발지 드론이 RREQ 패킷을 브로드캐스트할 때 자신의 Challenge 값에 대한 Response 값으로 출발지 및 목적지 시퀀스 번호와 홉 수를 암호화 후 전송한다. 따라서 출발지 드론의 CRP를 알고 있는 전체 드론은 출발지 드론의 CRP로 패킷을 복호화하여 시퀀스 번호 및 홉 수의 무결성을 검증할 수 있다. 반면 공격자는 출발지 드론의 CRP 테이블을 알지 못하므로 출발지 드론의 $R_0^{D_i}$를 생성 및 획득할 수 없게 되어 출발지 드론의 Response 값으로 암호화된 $E_{R_0^{D_i}}(s_n, d_n, h)$에서 s_n, d_n, h을 위조하는 것이 불가하다.

2.2 The Same Hop Count

AODV의 RREQ와 RREP 패킷은 홉 수를 보호하지 않아 공격자의 동일한 홉 수를 전달하는 공격에 취약하였다. 그러나 제안기법은 RREQ 패킷 전송 간 출발지 드론의 Response 값으로 암호화하여 홉 수를 $E_{R_0^{D_i}}(s_n, d_n, h)$ 형태로 암호화 후 전송하여 홉 수 필드를 보호할 수 있으며, RREP 패킷 전송 간에도 홉 바이 홉으로 CRP 테이블 내 무작위로 3개의 Challenge 값을 선정 후 해당 Response 값들을 XOR 연산하여 임시 세션 키를 생성하고 생성된 임시 세션 키로 홉 수를 $E_{Key_{D_i, D_3}}(s_n, d_n, h)$형태로 암호화 후 전송하므로 CRP 테이블을 알지 못하는 공격자는 드론그룹과 통신할 수 없다.

2.3 Worm Hole and Black Hole Attack

AODV에서는 공격자가 특정 드론의 ID를 알면 정상 드론인 것처럼 경로에 참가하여 외부의 공격자와 터널인 웜홀을 만들거나 블랙홀 드론을 만들어 정상적으로 전송되어야 할 패킷을 가로채거나 집중되게 하는 공격을 수행할 수 있다. 제안기법은 공격자가 특정 드론의 ID를 알고 있더라도 PUF의 특성으로 각 드론의 CRP를 복제할 수 없고, 공격자가 드론그룹의 CRP 테이블을 획득할 수 없어 RREQ, RREP, RERR 패킷 전송 및 수신 간 활용되는 특정 Challenge에 대한 Response 값을 생성하는 것이 불가하여 정상 드론을 가장하여 웜홀을 만들거나 블랙홀 드론을 만들어 정상 드론들과 통신 경로를 방해할 수 없다.

2.4 DoS Attack

AODV에서는 공격자가 유효하지 않은 많은 양의 RREQ 패킷을 생성하여 전체에게 계속 브로드캐스트 하는 DoS 공격을 수행할 수 있다. 그러나 제안된 기법에서는 출발지 드론이 브로드캐스트 간 출발지 및 목적지 시퀀스 번호와 홉 수를 자신의 Response 값을 이용하여 $E_{R_0^{D_i}}(s_n, d_n, h)$형태로 암호화하여 전송하므로 네트워크 내 전체 드론은 CRP 테이블에 저장되지 않은 CRP를 사용하거나 암호화 없이 전송되는 모든 RREQ 패킷을 전송하지 않고 무시할 수 있다.

2.5 RERR Spoofing Attack

AODV에서는 공격자가 가짜 RERR 패킷을 전송하여 정상 경로를 단절시켜 정상 드론을 네트워크에서 배제 시키거나 경로설정 단계를 반복적으로 강요할 수 있다. 예를 들어 S→A→B→C→D가 있는 경우 B에게 C가 D에서 생성된 것처럼 RERR 패킷을 위조하여 전송할 수 있다. B는 RERR 패킷이 정상인지 확인하는 것이 불가하여 D로 이어지는 경로가 단절되었다고 판단하고 D로 가는 경로를 단절시키거나 경로 발견단계를 반복 수행하게 된다. 제안기법에서는 RERR 패킷에 단절된 목적지 드론의 주소 D와 마지막 목적지 시퀀스 번호에 1을 증가시킨 d_n 등 가변필드를 홉 바이 홉 간 임시 세션 키로 암호화하여 전송하므로 CRP 테이블을 알지 못하는 공격자는 홉 바이 홉 간 임시 세션 키를 생성할 수 없고, 암호화되지 않은 RERR 패킷을 전송하더라도 해당 패킷들은 경로상 드론들에게 무시될 수 있다.

2.6 Sleep deprivation Attack

AODV에서는 RREQ 패킷을 전송하는 출발지 드론이 정상 드론인지를 확인하는 것이 불가능하므로 공격자가 군집 드론의 배터리 전원을 소모 시키기 위해 불필요한 라우팅 패킷을 지속적으로 브로드캐스트 할 수 있다. 이러한 공격은 전력량이 적은 소형 군집 드론에게는 상당한 위협을 초래하며 정상적인 통신과 구별하기가 어렵다. 따라서 많은 양의 RREQ 패킷으로 수면 박탈 공격을 받을 수 있다. 제안기법도 이전 기법들과 마찬가지로 가짜 RREQ 패킷을 브로드캐스트 하는 것이 가능하다. 그러나 전체 드론은 그룹 내 모든 드론의 CRP를 테이블 형식으로 NVM 내 저장하고 있어 RREQ 패킷이 암호화되지 않고 전송되거나 암호화에 사용된 $R_i^{D_i}$이 CRP Table 내 존재하지 않으면 해당 패킷을 무시할 수 있다.

V. Conclusions

향후 드론의 활용은 다방면에 걸쳐 지속적으로 증가할 것이며, 군집 드론의 활용성도 증대될 것이다. 여러 대의 소형 드론들을 군집 드론의 형태로 효율적으로 운용하기 위해서는 GCS에 의존하는 방식이 아닌 자율적인 통신 네트워크 구축을 모색해야 한다. 그러나 현재까지도 군집 드론 운용을 위한 보안성이 강화된 자율적인 통신 네트워크 기법은 뚜렷하게 제시되지 않았다.

이에 본 논문에서는 GCS에 의존하는 중앙집중방식에서 벗어나 FANET을 기반으로 안전한 자율 통신 네트워크를 구축할 수 있는 기법을 제안하였다. 제안된 기법은 자원 제약적인 소형 드론에 보다 적합한 경량화된 기법임을 확인하였으며, 다양한 공격유형에 대해서도 내성을 가질 수 있음을 검증하였다.

REFERENCES

[1] Bekmezci, Ilker, O. K. Sahingoz, and Ş. Temel, "Flying Ad-Hoc Networks (FANETs): A survey," Ad Hoc Networks, Vol. 11, No. 3, pp. 1254-1270, May 2013. DOI: 10.1016/j.adhoc.2012.12.004

[2] Ha, Il-Kyu, "Analysis of Efficient Health Data Transmission Methods based on the Fusion of WBAN and FANET," Journal of the Korea Institute of Information and Communication Engineering, Vol. 21, No. 2, pp. 386-394, Feb 2017. DOI: 10.6109/jkiice.2017.21.2.386

[3] C. E. Perkins, E. M. Royer, "Ad-hoc on-demand distance vector routing," Proc. of the WMCSA'99 Second IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100, New Orleans, LA, USA, 1999. DOI: 10.1109/MCSA.1999.749281

[4] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks", IEEE Personal communications, Vol. 8, No. 1, pp. 16-28, Feb 2001. DOI: 10.1109/98.904895

[5] V. Mulert, J. I. Welch, and W. K. Seah, “Security threats and solutions in MANETs: A case study using AODV and SAODV,” Journal of network and computer applications, Vol. 35, No. 4, pp. 1249-1259, July 2012. DOI: 10.1016/j.jnca.2012.01.019

[6] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. B. Royer, "A secure routing protocol for ad hoc networks," Proc. of the 10th IEEE International Conference on Network Protocols, pp. 78-87, Paris, France, Nov 2002. DOI: 10.1109/ICNP.2002.1181388

[7] M. G. Zapata, N. Asokan, "Securing ad hoc routing protocols," Proc. of the 1st ACM workshop on Wireless security, pp. 1-10,

Atlanta GA USA, Sept 2002. DOI: 10.1145/570681.570682

[8] Q. Li, M. Zhao, J. Walker, Y. C. Hu, A. Perrig and W. Trappe. "SEAR: a secure efficient ad hoc on demand routing protocol for wireless networks", Security and Communication Networks, Vol. 2, No. 4, pp. 325-340, Sept 2008. DOI: 10.1002/sec.60

[9] M. Mohammadizadeh, A. Movaghar, S. M. Safi "SEAODV: Secure efficient AODV routing protocol for MANETs networks", Proc of the 2nd International Conference on Interaction Sciences : Information Technology, Culture and Human, pp. 940-944, Seoul Korea, Nov 2009. DOI: 10.1145/1655925.1656096

[10] A. Perrig, R. Canetti, J. D. Tygar, D. Song,"The TESLA broadcast authentication protocol", Rsa Laboratories Cryptobytes, Vol. 5, No. 2, pp. 2-13, Fall 2002. DOI: 10.1007/978-1-4615-0229-6_3

[11] Baek. Jong-Hak, Sin. Gwang-Jo, "Development and Application of Security Chip Technology Using PUF Technology", The Magazine of the IEIE, Vol. 43, No. 7, pp. 59-67, July 2016.

[12] Sumin Kim, "A Study on the Development of Secure Communication Channel Using PUF Technology in M-IoT Environmen," Jouranl of Information and Security, Vol. 19, No. 5, pp. 107-118, Dec 2019.

[13] T. W. Kim, B. D. Choi and D. K. Kim, "Zero bit error rate ID generation circuit using via formation probability in 0.18 μm CMOS process", Electronics letters, Vol. 50, No. 12, pp. 876-877, June 2014. DOI: 10.1049/el.2013.3474

[14] Ahn Hyo min, "Destination-initiated Fast Route Acquisition Scheme for AODV", Dept. of Electrical and Electronic Engineering, The Graduate School Yonsei University, 2003

Authors

Yoon-Gil Park received the B.A. degree in Economics from Korea Army Academy at Yeongcheon, Korea, in 2014. He is now working toward a M.S. degree at Department of Computer Science and Engineering, Korea National Defense University. He is interested in Cyber Warfare Policy, Drone Security Routing Protocol Security, FANET.

Soo-Jin Lee received the B.S. degree from Korea Military Academy in 1992, M.S. degree in Computer Science from Yonsei University in 1996, and Ph.D. degree in Computer Science and Engineering from Korea Advanced Institute of Science and Technology in 2006. Dr. Lee is currently a Professor in the Department of Computer Science and Engineering at Korea National Defense University, Nonsan, Korea, from 2006. He is interested in Cyber Warfare and Cyber Security Policy, Intrusion Detection System, Mobile Network Security, Encryption theory and applications.