https://doi.org/10.33778/kcsa.2020.20.5.011

전기차 무선 충전 시스템에서 실시간 탐지를 위한 지능형 Bluetooth 침입 탐지 시스템 연구★

윤 영 훈*, 김 대 운**, 최 정 안**, 강 승 호**

요 약

IoT의 핵심 요소 기술 중 하나인 Bluetooth를 전기차 무선 충전 시스템에 사용하는 경우가 늘어나면서 이에 대한 보안 문제가 큰 이슈로 부각되고 있다. 무선 통신 기술인 Bluetooth에 보안을 강화하기 위한 다양한 기술적 노력이 있어 왔지만 여전히 다양한 공격 방법이 존재한다. 본 논문은 Bluetooth 시스템을 대상으로 대표적인 2가지 공격 방법을 지능적으로 탐지하기 위해 잘 알려진 Hidden Markov Model을 이용한 지능형 Bluetooth 침입 탐지 시스템을 제안한다. 제안 방법은 탐지의 정확성 이외에 실시간 탐지가 가능하도록 Bluetooth 전송 계층 프로토코인 H4의 패킷 타입과 전송 방향을 조합하고 이들의 시간상의 전개를 특징으로 사용한다. 데이터 수집 환경을 구성하고 실험을 통해 얻은 데이터를 대상으로 개발한 시스템의 성능을 분석한다.

An Intelligent Bluetooth Intrusion Detection System for the Real Time Detection in Electric Vehicle Charging System

Young-Hoon Yun*, Dae-Woon Kim**, Jung-Ahn Choi**, Seung-Ho Kang**

ABSTRACT

With the increase in cases of using Bluetooth devices used in the electric vehicle charging systems, security issues are also raised. Although various technical efforts have beed made to enhance security of bluetooth technology, various attack methods exist. In this paper, we propose an intelligent Bluetooth intrusion detection system based on a well-known machine learning method, Hidden Markov Model, for the purpose of detecting intelligently representative Bluetooth attack methods. The proposed approach combines packet types of H4, which is bluetooth transport layer protocol, and the transport directions of the packet firstly to represent the behavior of current traffic, and uses the temporal deployment of these combined types as the final input features for detecting attacks in real time as well as accurate detection. We construct the experimental environment for the data acquisition and analysis the performance of the proposed system against obtained data set.

Key words : Electric Vehicle Charging System, Bluetooth, Intrusion Detection System, Information Security, Hidden Markov Model, Real Time Detection, Bluetooth Attack

접수일(2020년 11월 12일), 수정일(1차: 2020년 12월 11일, 2차: 2020년 12월 16일), 게재확정일(2020년 12월 18일)

★ 본 연구는 한국전력공사의 2018년 선정 기초연구개발 과제 연구비에 의해 지원되었음(과제번호 : R18XA06-48)

* 동신대학교/신재생에너지전공

** 동신대학교/융합정보보안전공

1. 서 론

모든 사물을 하나의 네트워크로 연결해 정보, 자원 등을 공유하기 위해 IoT 기술이 등장하였다. 무선 통신 기술 중 하나인 Bluetooth는 에너지 소비가 중요한 응용 분야에 적합하도록 BLE(Bluetooth Low Energy)로 진화하면서 IoT의 중요한 통신 기술로 사용되고 있고 특히 전기차 무선 충전 시스템에 주요 구성 기술로 사용되고 있다.

Bluetooth 프로토콜의 보안 기술은 버전 상승과 함께 지속적으로 개선되고 있지만 최신 보안 기술이 구현되지 않은 과거 버전의 Bluetooth 장치가 현장에서는 여전히 전개되어 사용되고 있어 많은 잠재적 보안 문제를 안고 있다. 또한 다양한 버전의 Bluetooth 장치를 대상으로 다양한 공격 도구들이 지속적으로 개발되고 있다. 이러한 Bluetooth의 침해 공격을 선제적으로 차단하기 위해 여러 지능형 침입 탐지 시스템이 제안되고 있다.

IoT 기기를 대상으로 한 대부분의 기계학습 기반의 침입 탐지 시스템들은 이상 행위 분석(Anomaly Behavior Analysis) 방법을 사용하였다[1]. 이 방법의 핵심은 수집이 쉬운 정상 트래픽을 이용해 학습시킨 후 정상 트래픽과 다른 특징을 보이는 트래픽을 이상 행위로 간주하는 방법으로 높은 탐지율을 보여 주었다. 하지만 이상 행위 분석 방법의 최대 단점은 정상 데이터만을 이용함으로써 공격의 유무를 판별할 수는 있지만, 공격 방법의 유형을 구분하지 못하는 한계를 가지고 있다. 공격 방법의 종류를 알아야만 적절한 대응 방법을 선택하고 서비스 제공의 연속성과 피해 규모의 최소를 조합할 수 있는 조치가 가능하다는 점에서 기존 방법들은 여전히 많은 한계를 가지고 있다.

기존 기계학습 기반의 침입 탐지 시스템들의 또 하나의 단점은 학습과 판별에 사용하는 특징이 지나치게 복잡해, 이를 추출해서 실시간에 공격 유뮤 및 종류를 판단하는데 많은 제약이 따른 다는 점이다. 특히 공격 성공에 따른 피해 규모가 큰 응용 분야에서 사전적 혹은 실시간적인 공격 탐지가 불가능하다면 이런 침입 탐지 시스템의 사용은 어렵다. 따라서 탐지율의 성능을 보장하면서 실시간에 탐지가 가능한 특징을 개발하는 것도 기계학습 기반의 침입 탐지 시스템의 성공 여부를 가르는 중요한 문제이다.

[2]에서 이러한 문제를 해결하기 위해 Bluetooth HCI 전송 프로토콜인 H4의 패킷 유형과 전송 방법만을 조합하고 이들의 시간적 패턴을 특징으로 이용하는 방법을 제안하였다. 또한 시간적 패턴을 학습하고 판별하기 위해 잘 알려진 히든 마코프 모델을 이용한 지능형 Bluetooth 침입탐지 시스템을 제안한다. 본 논문은 [2]에서 제시된 방법을 보완하고 다양한 실험을 추가하였다. 데이터는 Bluetooth 네트워크을 대상으로 정상 트래픽과 두 가지 공격이 시도했을 때의 트래픽을 이용해 데이터를 획득하였으며 훈련 데이터와 검증 데이터로 분류해 성능을 평가하였다.

논문의 구성은 다음과 같다. 우선 2장에서 본 논문과 관련된 연구들을 기술하고 3장에서 침입 탐지 시스템을 소개한다. 4장에서 데이터를 이용한 실험과 성능 분석을 실시하고 마지막 5장에서 결론을 내린다.

2. 관련 연구

2.1 Bluetooth 통신 기술

Bluetooth는 UHF 라이오파를 이용해 장치 간의 데이터 무선 교환을 위한 표준 무선통신 기술로써 2.4GHz 대를 이용하며 근거리 개인 통신망(PAN: Personal Area Network) 형성에 사용된다[3]. Bluetooth 네트워크에 참여하는 장치들은 마스터/슬래이브 역할을 수행하고 하나의 마스터 노드엔 7개의 슬래이브 노드가 연결될 수 있으며, 이를 피코넷이라한다. 또한 여러개의 피코넷이 연결된 스캐터넷을 구성할 수 있다.

2.2 Bluetooth 공격 방법

2007년에 완성된 Bluetooth 2.1에서 Bluetooth 보안과 관련한 중요한 변화가 이루어졌지만 무선 통신 기술로서 여전히 많은 보안 취약점을 가지고

있다. 여기서는 가장 잘 알려진 공격 방법을 소개한다[4][5].

1) Bluebugging
Bluebugging 방법을 이용하면 해커들이 핸드폰과 같은 장치에 접근해서 엿듣거나 메시지, 메일 등을 전송할 있으며 전화를 걸 수 도 있다.
2) Bluejacking
가장 흔히 사용되는 공격 방법으로 모르는 사람에게 광고 메시지를 보내는 등에 사용되는 공격 방법이다.
3) Bluesnarfing
Bluejacking은 실제 장치에 연결이 없이 시도되는데 반해 Bluesnarfing은 연결된 후 장치에 있는 다양한 개인 정보 및 데이터를 복사할 수 있는 기술로 피해가 심각할 수 있다.
4) Car whisperer
자동차에 내장된 Bluetooth 장치의 PIN이나 비밀번호를 변경하지 않고 사용하는 경우 행할 수 있는 공격 유형으로 자동차안에서 핸즈프리 대화를 감청하는 것 등이 해당된다.
5) Location tracking
웨어러블 Bluetooth 장치 등을 통해 사용자의 이동이나 위치를 추적할 수 있는 공격방법이 해당한다.
6) BlueBorne
공격 대상자의 Bluetooth 장치에 악성코드를 감염시켜 장치를 장악하는 공격 방법이다. 장치의 제어권을 확보한 후 개인 정보 수집과 같은 다양한 피해를 입힐 수 있다.

2.3 침입탐지 시스템

IoT을 대상으로 시그니처 기반 탐지 시스템, 이상행위 기반 탐지 시스템 등의 전통적인 침입 탐지 시스템이 있다. 또한 베이지 분류기, 서포트 벡터 머신, 딥 러닝 등의 기계학습 방법을 이용한 연구들이 진행되고 있다[6]. 하지만 Bluetooth 프로토콜을 대상으로 직접적으로 기계학습 기반의 침입 탐지 시스템을 설계한 연구는 드물며 Satam의 연구가 있다[1]. 이 논문은 이상행위 분석(ABA: Anomaly Behavior Analysis) 기법에 기반한 N-gram 데이터 구조를 특징으로 하여 결정트리, 앙상블, 서포트 벡터 머신 등 전통적인 기계학습을 적용하고 있다.

하지만 서론에서도 언급했듯이 정상 트래픽을 학습 데이터로 사용하는 이상행위 분석에 기반한 지능형 침입 탐지 시스템은 공격 방법을 구분하지 못한다. 또한 특징으로 사용하는 N-gram 데이터 구조는 Bluetooth 패킷으로부터 계산하는데 많은 컴퓨팅 자원과 시간을 요구하고 있어 실시간성을 확보하는데 어려움이 있다.

3. HMM 기반 Bluetooth 침입 탐지 시스템

3.1 Hidden Markov Model

Hidden Markov Model(HMM)은 마코프 프로세스를 가정한 확률 모델로써 음성인식, 서명인식과 같이 순차성, 시간성을 갖는 데이터를 대상으로한 패턴인식 분야에 많은 사용되는 기계학습 방법이다[7].

일반적으로 HMM은 세 가지 변수를 이용해 아래와 같이 정의할 수 있다.

$$\Theta = (A, B, \pi)$$

A : 상태 전이 확률을 나타내며, 특정 상태에서 다른 상태로의 전이 결정에 사용되는 확률이다.
B : 관측 확률로써 특정 상태에서 관측 가능한 사건들의 발생 확률을 나타낸다.
π : 초기 상태 확률이라 하며, 프로세스 진행의 초기에 특정 상태가 선택될 확률을 나타낸다.

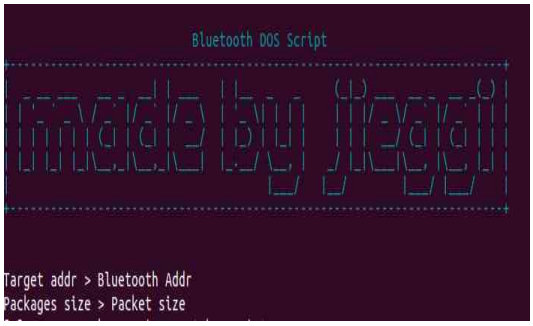
일반적으로 HMM과 관련된 문제는 3가지 있는데 다음 <표 1>과 같다. HMM 기반의 Bluetooth 침입 탐지 시스템 설계는 이 중 학습 문제와 평가 문제에 관련되어 있다. 각각의 클래스를 대상으로 개별 모델을 만들어 학습이 이루어지며 학습된 모델이 동일 유형의 클래스 인스턴스에 대해 최대 확률이 나오도록 학습이 유도된다.

<표 1> HMM과 관련된 문제 유형

문제 유형	내용
평가 문제	주어진 모델 Θ을 대상으로 관찰된 특정 사건들의 연속(sequence)이 발생할 확률을 구하는 문제
디코딩 문제	주어진 모델 Θ을 대상으로 관찰된 특정 사건들의 연속이 발생할 확률을 가장 크게 할 상태의 연속을 구하는 문제
학습 문제	주어진 관측 사건 연속 데이터를 이용해 이러한 사건 연속이 최대로 발생할 수 있게 하는 모델 Θ를 찾는 문제

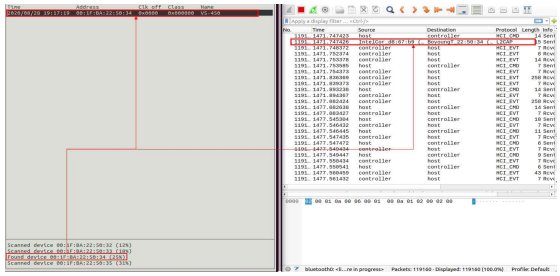
3.2 탐지 대상 공격 방법 및 도구

논문이 제시하는 침입 탐지 시스템은 DoS 공격과 주변 장치를 탐색하는 스캔 공격을 탐지 목적 공격으로 하였다. Bluetooth DoS 공격용 도구는 파이썬으로 구현된 Bluetooth DoS[8]을 사용하였다. 그림 1은 사용한 Bluetooth DoS 스크립트의 첫 화면이다.



(그림 1) Bluetooth Dos script 메인화면

스캔 공격 데이터를 구하기 위해서는 btscanner [9]를 사용하였다. btscanner는 페어링 없이 Bluetooth 기기로부터 다양한 정보를 추출하기 위해 특별히 고안된 도구로써 사용하기도 편하다. HCI, SDP 등에 관한 정보를 수집할 수 있으며 RSSI와 링크 질을 모니터링 할 수 도 있다.



(그림 2) Bruteforce scan 결과 예시

3.3 특징 추출

기계학습에 기반한 침입 탐지 시스템의 성능은 기계학습 고유의 성능뿐 아니라 사용하는 특징에 크게 의존한다. 일반적인 기계학습 기반의 분류 시스템의 성능은 주로 탐지율과 오탐율 측면에서 측정되고 평가되지만 침입 탐지와 같이 사전 탐지나 실시간 탐지가 중요시되는 시스템에서는 이 못지 않게 학습 및 탐지에 드는 시간도 중요한 고려요소 중 하나이다.

본 논문은 이러한 문제점을 해결하기 위해 Bluetooth 규격 중 HCI 전송 계층 프로토콜인 H4(HCI UART Transport Layer)의 패킷 유형과 전송 방향이라는 간단한 패킷 정보를 조합한 특징을 사용한다.

H4 프포토콜은 다음과 같이 4가지 형태의 패킷을 가지고 있다.

- HCI Command Packet.
- HCI ACL Data Packets.
- HCI Synchronous Data Packets.
- HCI Event Packet.

<표 2> 패킷 방향과 타입 표현

hci_h4_direction	'0x00000000', '0x00000001'
hci_h4_type	'0x00000001', '0x00000002', '0x00000003', '0x00000004'

한편, 방향은 호스트와 Bluetooth 하드웨어 사이의 두 가지 방향이 있으므로 총 8가지의 조합이 가능하다. 특징에 시간성을 부여하기 위해 패킷의 시간 순서에 따라 특정 길이의 8가지 조합 시퀀스

를 특징으로 사용한다. 실제 wireshark를 이용해 Bluetooth 패킷을 분석하면 H4 패킷의 방향과 패킷 유형이 표 2와 같이 되어있음을 알 수 있다. 8가지 조합과 그 조합에 부여된 숫자 기호는 다음 표 3과 같다.

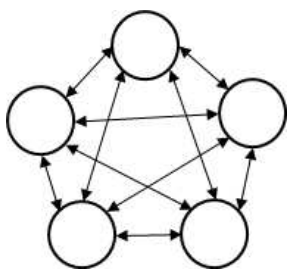
<표 3> 방향과 패킷 유형의 가능 조합

방향	패킷 유형	숫자 기호
'0x00000000'	'0x00000001'	0
'0x00000000'	'0x00000002'	1
'0x00000000'	'0x00000003'	2
'0x00000000'	'0x00000004'	3
'0x00000001'	'0x00000001'	4
'0x00000001'	'0x00000002'	5
'0x00000001'	'0x00000003'	6
'0x00000001'	'0x00000004'	7

따라서 특정 시간 동안의 Bluetooth 트래픽은 8가지 숫자 기호의 연속으로 표현된다. 예를 들어 10개의 패킷으로 구성된 트래픽의 특징은 7, 0, 7, 5, 1, 7, 5, 1, 7, 7로 표현될 수 있다.

3.4 모델 설계

침입 탐지 시스템을 위해 HMM을 설계하기 위해서는 정상 트래픽과 공격 방법 별 모델이 필요하다. 두 가지 공격 방법을 탐지 대상으로 하였으므로 총 3개의 모델이 필요하며 각각의 모델은 자신에게 상응하는 특징 데이터를 이용해 학습한다. 상태는 5개로 지정하였으며 5개의 상태 노드가 완전 연결 그래프 구조인 어고딕(ergodic) 아키텍처를 사용하였다. 모델은 가장 널리 사용되고 있는 Baum-Welch 알고리즘을 사용하여 학습하였다.



(그림 3) 상태 어고딕 아키텍처

주어진 트래픽/특징에 대한 평가는 학습된 3가지 모델을 대상으로 발생 확률을 계산하고 가장 확률이 큰 학습 모델을 따라 분류한다. 즉 정상 트래픽을 학습한 모델의 확률이 가장 큰 경우엔 주어진 트래픽은 정상으로 판별하는 것이다.

4. 실험 및 성능분석

4.1 실험 데이터

Bluetooth 네트워크를 대상으로 한 공개 데이터를 구할 수 없어서 모의 환경을 구축하고 실제 공격 도구를 사용해 데이터를 수집하였다.

사용한 Bluetooth 장비는 Bluetooth 2.0버전이 구현된 이어폰이며 윈도우즈 2000과 음악재생 어플을 이용해 Bluetooth 통신하도록 하였다. 공격자는 리눅스 운영체제에서 두 가지 공격 도구를 사용하여 공격하도록 하였다. Bluetooth 패킷은 네트워크 패킷 분석도구인 wireshark[10]를 사용하여 수집하였다. 패킷 데이터로부터 8가지 숫자 기호된 특징 서열을 추출하는 전처리는 파이썬으로 구현된 pyshark[11] 모듈을 사용하였다.

정상 상태와 두 가지 공격이 행해지는 일정 시간 동안 수집된 패킷은 단일 특징 서열로 변경된 후 크기가 30인 슬라이딩 윈도우를 이용해 크기 30인 서열 특징으로 분할하였다. 수집된 패킷으로부터 획득한 크기 30인 특징 서열 중 70%는 훈련 집합으로 사용하였고 나머지 30%는 검증집합으로 사용하였다. 데이터 집합의 전체구성은 다음과 같다.

<표 4> 데이터 집합의 전체 구성

패킷 유형	훈련 집합	검증 집합	합계
Normal	44382	19022	63,404
DoS attack	39711	17019	56,730
Scan attack	5893	2526	8,419
	89,986	38,567	128,553

4.2 실험 결과

모델 구현에 사용한 HMM 모듈은 파이썬으로 구현된 hmmlearn[12]을 사용하였다. 세 가지 패킷

유형의 검증 집합을 사용해 얻은 혼동 행렬은 표와 같다.

<표 5> 혼동 행렬

		Predicted		
		Normal	DoS attack	Scan attack
Actual	Normal	13752	0	5270
	DoS attack	0	17019	0
	Scan attack	1108	427	991

일반적으로 성능 평가에 사용되는 Accuracy, Precision, Recall, F1 성능 지표는 아래 표와 같이 정의된다.

<표 6> 성능 지표 정의

성능 지표	정의
Accuracy	(TP + TN)/(TP + FP + TN + FN)
Precision	TP / (TP + FP)
Recall	TP / (TP + FN)
F1 score	Precision과 Recall의 조화 평균값

테스트 데이터를 대상으로 한 전체 정확도는 0.82이었고 각각의 데이터를 대상으로 한 기타 성능 지표는 표 7과 같다.

<표 7> 성능 지표 값

	Normal	DoS attack	Scan attack
Precision	0.93	0.98	0.16
Recall	0.72	1	0.39
F1 score	0.81	0.99	0.23

테스트 데이터를 대상으로 시스템의 전체 정확도는 0.82였다. 정상 트래픽을 대상으로 한 정확도 및 기타 세 가지 지표가 모두 높은 것으로 나타났다. 또한 침입 탐지 시스템에서 특히 문제가 되고 있는 정상 트래픽을 공격으로 오인하는 오탐율은 상당히 작았다. 마찬가지로 DoS 공격에 대해서도 정확도를 비롯한 Precision, Recall, F1 score가 매우 높아 H4 패킷의 종류와 방향을 특징으로 사용한 HMM 기반 침입 탐지 시스템의 DoS 공격 탐지는 실시간으로 사용하기에 매우 적합하다고 할 수 있다. 다만 주변 기기를 탐지하는 Scan 공격은 정상 트래픽과 거의 구분하지 못하는 것으로 나타났다. H4 프로토콜의 기본 기능이 주변 기기의 탐지라는 점에서 이해할 수 있는 결과로 보인다. 다만 페어링을 하지 않는 다는 사실을 특징에 포함시킬 수 있으면 이는 개선될 여지가 커 보인다.

5. 결 론

본 논문은 Bluetooth 네트워크에서 두 가지 공격 방법을 탐지하기 위한 HMM 기반 지능형 침입 탐지 시스템을 제안하였다. 빠른 탐지를 위해 H4 프로토콜의 패킷 유형과 방향의 조합을 이용해 시간 서열을 특징으로 사용하였다.

모의 환경을 구성하고 두 가지 공격 도구를 사용하여 데이터를 수집하여 시스템의 학습과 검증에 사용하였다. 검증 결과, 정상 트래픽과 DoS 공격에 대해서는 매우 높은 탐지 성능을 보여 주었지만, scan 공격에 대해서는 정상 트래픽과 거의 구분하지 못하였다.

기존의 기계학습 기반 Bluetooth 침입 탐지 시스템에서 사용된 기계학습은 시간 정보를 고려하지 않은 기계학습 방법만을 사용한 것에 반해 단순한 패킷 정보에 시간성 추가하고 이를 학습할 수 있는 HMM을 사용하여 정상 트래픽과 DoS 공격을 높은 정확도로 탐지할 수 있음을 보여줬다는데 의의가 크다. 다만, scan 공격과 같은 특정 공격을 탐지하는 데는 명백한 한계를 보여 줌으로써 앞으로 다양한 공격들을 종류별로 구분하는 범용의 침입 탐지 시스템으로 발전하기 위해서는 개선해야 할 부분 또한 크다는 사실을 확인하였다.

참고문헌

[1] P. Satam, S. Satam, and S. Hariri, Bluetooth Intrusion Detection System(BIDS), 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), October, 2018.

[2] J. A. Choi, D. W. Kim, and S. H. Kang, "An intelligent Bluetooth Intursion Detection

Systgem using Hidden Markov Model", Proceeding of Cyber Security Conference at Honam, October, 2020.

[3] https://en.wikipedia.org/wiki/Bluetooth

[4] K. Haataja and P. Toivanen, "Two practical man-in-the-middle attacks on Bluetooth secure simple pairing and countermeasures in IEEE Transactions on Wireless Communications", vol. 9, no. 1, pp. 384-392, January 2010.

[5] https://www.essaysusa.com/article/types-of-bluetooth-attacks

[6] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider and A. Wahab, "A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions", Electronics, 9(7), 2020.

[7] L.R. Rabiner, "A tutorialj on hidden Markov models and selectd applications in speech recognition", Proceedings of the IEEE, 77 (2), pp.257-286, February 1989.

[8] https://github.com/crypt0b0y/BLUETOOTH-DOS-ATTACK-SCRIPT

[9] https://packages.debian.org/unstable/btscanner

[10] https://www.wireshark.org/

[11] https://github.com/KimiNewt/pyshark

[12] https://hmmlearn.readthedocs.io/en/latest/

〔저자소개〕

윤 영 훈 (Young-Hoon Yun)
1993년 2월 동신대학교
무기재료공학과 (공학사)
1996년 2월 한양대학교
세라믹공학과 (공학석사)
2001년 8월 한양대학교
세라믹공학과 (공학박사)
2006년 3월 ~ 현재 동신대학교
신재생에너지전공 교수
email : yunh2@dsu.ac.kr

김 대 운 (Dae-Woon Kim)
2016년 3월 ~ 현재 동신대학교
융합정보보안전공 재학
email : i---d@naver.com

최 정 안 (Jung-Ahn Choi)
2016년 3월 ~ 현재 동신대학교
융합정보보안전공 재학
email : yy0099@daum.net

강 승 호 (Seung-Ho Kang)
1994년 8월 전남대학교
전산학과 (이학사)
2003년 2월 전남대학교
전산학과 (이학석사)
2008년 8월 전남대학교
전산학과 (이학박사)
2013년 9월 ~ 현재 동신대학교
융합정보보안전공 교수
email : drminor@dsu.ac.kr