정 보 보 호 학 회 지
제29권 제1호, 2019. 2

2018 정보보호 R&D 챌린지 – 차량주행 데이터기반 도난탐지 트랙 –

곽 병 일*, 김 휘 강**

요 약

나날이 발전하고 있는 ICT 기술과 차량과의 융합은 차량을 대상으로 하는 사이버 위협과 공격을 더욱 증대시킨다. 그러나 차량 보안을 연구하는 산업계, 학계 연구 그룹들 또한 다양한 접근 방법을 통해 이러한 위협과 공격을 앞서 예방하고 탐지하기 위해 노력하고 있다. 2018 정보보호 R&D 데이터 챌린지에서는 차량주행 데이터기반 도난탐지 트랙을 마련하였다. 이는 운전자별 주행 데이터에 대한 분석을 통해 현재 주행 중인 운전자를 식별하는 챌린지로써 국내 및 해외에서 처음으로 진행된 트랙이다. 이번 2018 정보보호 R&D 데이터 챌린지 중 차량주행 데이터기반 도난탐지 트랙에 참가한 참가자들은 주행 데이터를 통계적 기반으로 분석하여 모델링 하였으며, 분석하는 과정에 있어 의미 있는 분류 결과를 도출해 내었다. 일반적으로, 한 가정이 보유하고 있는 차량이 가족들 이외 다른 이들에게는 잘 공유되지 않는다는 점을 고려한다면, 비록 소수의 운전 참가자이지만 5명을 대상으로 하는 본 실험이 의미가 있다고 본다. 이번 정보보호 R&D 데이터 챌린지를 통해, 운전자 주행 데이터가 도난 탐지를 위한 운전자 분류뿐만 아니라, 운전자에게 특화된 의료와 보험과 같은 맞춤형 서비스를 제공할 수 있는 가능성을 확인할 수 있었다.

Ⅰ. 서 론

네트워크와 연결되는 Connected Car 환경에서의 차량은 Wi-Fi, Bluetooth, Audio, Video, Navigation과 같은 다양한 유무선 인터페이스와 연결이 되고 있다. 이처럼 차량 내부와 인터넷 연결성의 증가는 차량에 대한 공격 벡터로써 사이버 공격의 위협 가능성을 더욱 증대시킨다. 최근에도, 특정 차량의 모듈식 IVI (In-Vehicle Infotainment) 시스템을 원격으로 해킹하여 CAN 버스에 임의의 CAN 메시지를 보내면서 차량 내 스피커, 마이크 등을 원격으로 제어할 수 있는 취약점이 발견되었다 [1][2]. 커넥티드 카에 부착된 TCU (Telemetics Control Units) 디바이스의 취약점이 일부 차량에서는 패치가 이루어지기도 하지만, Keen security lab의 보고에서도 보듯이 여전히 존재하는 다수의 취약점이 차량 내부 네트워크로 들어오는 침투 통로로 활용이 될 수 있다 [3]. 이렇듯, 차량을 대상으로 하는 사이버위협을 보다 앞서 예방하고 탐지하기 위해서는 지속적인 관심과 지원 그리고 다양한 관점에서의 활발한 연구가 필요하다.

2018 정보보호 R&D 챌린지는 지능형 사이버위협에 대응하기 위한 연구의 한 일환으로써, AI 보안 기술개발의 장려와 인력양성을 진작시키기 위한 생태계를 조성하고자 해당 데이터 챌린지를 개최했다 [4]. 본 챌린지에서는 다수의 PC 악성코드와 모바일 악성앱 데이터 그리고 소수이기는 하지만 차량을 대상으로 하는 운전자의 주행 데이터를 제공하였다. 또한, 본 챌린지에 참가한 그룹들은 제공된 데이터를 데이터 마이닝과 머신러닝 기술을 이용하여 분석함으로써, 각 트랙에서 제시한 요건을 달성하는 것이 주된 목표이다.

2018 정보보호 R&D 챌린지 중 본 논문은 운전자의 차량주행 데이터를 기반으로 도난탐지 여부를 분석하는 내용에 중점을 둔 자동차 보안 관련 연구이다. 2장에서는 국내 및 해외의 데이터 챌린지와 차량 도난 탐지 연구들을 소개한다. 3장에서는 차량주행 데이터기반 도난탐지 트랙의 튜토리얼, 문제, 데이터 구성, 그리고 평가방법을 설명한다. 4장에서는 대회 결과를 나타내며, 끝으로 본 논문의 결론은 5장에서 서술한다.

* 고려대학교 정보보호대학원 (kwacka12@korea.ac.kr)
** 고려대학교 정보보호대학원 (cenda@korea.ac.kr)

Ⅱ. 관련 연구

2.1. 국-내외 데이터 챌린지

IoT 환경에서의 기기들을 통해 다양하고 많은 양의 데이터가 지속해서 생성되고 있다. 하지만, 이러한 데이터를 활용하기 위해서는 표준화또는 정규화 등의 데이터 변환, 차원 감소 (Dimension reduction) 같은 진입 장벽이 존재한다. 최근에 산업계와 학계는 데이터의 활용 및 성능 개선을 위해 데이터 챌린지와 같은 데이터 분석 대회들을 개최하고 있다. NIPS competition 및 Kaggle 은 그중 많은 데이터 분석가들에게 잘 알려진 대회로 볼 수 있다.

NIPS는 인지과학과 머신러닝 응용 분야에 있어 최신 연구결과들을 발표하는 국제 학회로써, 현재 세계적으로 이 분야에서 가장 유명한 학회 중 한 곳이다. 2017년부터 개설된 competition track의 데이터 분석 주제는 학회에 제안된 여러 사회 문제와 관련된 주제 중 일부가 선정되며, 이 트랙은 전 세계 많은 데이터 과학자들이 참가하며 진행되고 있다 [5].

Kaggle은 챌린지에 참가한 연구자들이 제시된 과제에 대해 데이터 분석 및 예측 모델링을 수행할 수 있도록 플랫폼을 제공한다 [6]. Kaggle에 등록되는 과제들은 다양한 분야에 걸친 주제들이 제공되며, 참가자들은 해당 문제들을 대한 해결 방식과 결과를 업로드하여 경쟁을 진행한다. 참가자들이 업로드하는 문제 해결 방식은 참가자 뿐만 아니라 사용자들에게 모두 공개가 되며, 이를 튜토리얼로써 참고할 수 있도록 하고 있다.

국내 또한 다양한 분야의 데이터 분석 챌린지가 진행되었다. 그중 산업계와 학계가 공동으로 주관하여 진행한 2017 정보보호 R&D 데이터분석 챌린지의 경우 정보보호 관련하여 차량에서의 이상징후 탐지를 위한 데이터 분석과 악성코드 분류를 위한 데이터 분석 챌린지를 진행하였다. 차량 데이터의 경우 차량 내부 네트워크인 Controller Area Network (CAN) Bus에서의 정상 트래픽과 공격이 이뤄질 때의 비정상 트래픽을 비교 분석하여 이상징후를 탐지하는 트랙을 개최했다 [7].

2.2. 운전자 분류

운전자 분류 연구는 차량에서 나오는 다양한 센서들과 Inertial Measurement Units (IMU)로 수집 분석되는 데이터를 통해 연구들이 진행되었다. Enev et. al.은 차량에서 추출 가능한 피쳐 (feature)들의 클러스터링을 통해 센서들을 4개 그룹으로 분류했으며, 주행 구간과 주차 구간을 11개 피쳐로 설정하여 운전자의 주행 패턴 분석 및 운전자 식별 실험을 수행했다 [8].

Kwak et. al.은 차량에 부착된 다양한 센서들을 추출하여 데이터 분석을 진행했다. 실험 도로를 일반 도심 도로, 자동차 전용 도로, 주차장 3 구역으로 구분 지어 데이터를 분석했으며, 51개 피쳐 중 선정된15개 피쳐와 추가된 통계적인 피쳐 (Statistical feature)를 통해 10명의 운전자에 대한 분류를 수행했다 [9].

Chen et. al.은 주행 시 빈번히 발생하는 좌회전과 우회전 이벤트를 통한 데이터를 이용하여 운전자의 주행 패턴을 분석과 운전자 식별에 적용했다. 주행 패턴 분석에 사용한 피쳐는 좌회전과 우회전 시 가속도, 가속도의 편차, 각속도의 편차이며, 데이터 추출 후 다섯 구간으로 분리하여 위 3개 피쳐에 대한 자기 상관계수 값을 추가하여 실험을 진행했다. 해당 연구에서는 자동차, 주행도로, 운전자들을 교체해 가면서 실험을 진행했으며, 각 주행은 운전자마다 두 번 주행을 통해 IMU 및 차량의 센서 데이터를 수집하여 운전자 분류 실험을 수행했다 [10].

Ⅲ. 2018 데이터 챌린지

2018 정보보호 R&D 데이터 챌린지의 차량주행 데이터기반 도난탐지 트랙은 운전자의 주행 데이터를 분석하여 현재 주행하고 있는 운전자가 인가된 운전자인지를 높은 정확도로 분류해야 하는 트랙이다. 본 장에서는 2018 데이터 챌린지의 차량주행 데이터기반 도난탐지 트랙에 대한 세부 설명을 서술한다. 첫 번째로 3.1절에서는 차량주행 데이터기반 도난탐지 트랙의 튜토리얼에 대해 서술한다. 3.2 절에서는 트랙 문제를 설명하며, 3.3절에서는 데이터 셋을 어떻게 구성하였는지 상세하게 기술한다. 마지막으로 3.4 절에서는 평가 방법을 설명한다.

3.1. 튜토리얼

차량주행 데이터기반 도난탐지 트랙의 튜토리얼에서

는 차량 도난을 효율적으로 탐지하기 위해, 차량에 내장된 센서 데이터들의 주행 패턴을 이용한 운전자 식별을 수행했다. 다양한 센서들로부터 추출된 데이터들을 통해 운전자의 주행 패턴을 구분하고, 운전자 분류 성능 향상과 피쳐 가공 관련 자원 소모를 줄이기 위해 피쳐 선택 (feature selection) 및 통계적인 피쳐를 추가했다. 또한, 통계적인 피쳐 추가 시 슬라이딩 윈도우 (sliding window)의 크기 변화를 통해 운전자의 분류 정확도 평가를 수행했다.

차량에 OBD Scanner를 부착하여 운전자 10명의 주행 중 차량 상태 데이터들을 추출했으며, 각 운전자별로 4번 주행했다. 주행 구간은 고려대학교 자연계 캠퍼스에서 상암 월드컵경기장 (약 17km) 사이의 구간을 두 구간으로 나눌 수 있다. 첫 번째 주행 구간은 신호등, 횡단보도, 이륜자동차 등이 존재하는 일반 도심 도로 구간이고, 두 번째 주행 구간은 신호등이 없고 이륜자동차가 주행할 수 없는 자동차만 주행이 가능한 자동차 전용도로가 포함된 구간이다.

주행 데이터의 51개 피쳐 중 운전자 분류 정확도 향상과 학습 시 계산량 감소를 위해 피쳐 선택 과정을 수행했다. 표 1은 피쳐 선택 과정을 통한 15개의 피쳐를 나타낸 것이다. 피쳐 선택 후 피쳐들의 정규화 과정을 수행했다. 수집된 주행 데이터들의 값의 범위가 다르므로 동일한 범위로 맞춰주는 기능이 필요하다. 해당 튜토리얼에서 진행한 정규화 과정은 최소값과 최댓값을 이용한 다음의 공식을 적용했다.

$$X_i = \frac{x_i - \min(x_i)}{\max(x_i) - \min(x_i)} \quad (1)$$

분류 정확도를 높이기 위한 통계적인 피쳐의 추가 과정에서 슬라이딩 윈도우를 통해 타임 윈도우 (Time window) 동안의 평균, 중간값, 표준편차를 피쳐로 추가한다. 해당 과정을 통해 주행 데이터 셋을 구성하고 일반 도심 도로, 자동차 전용 도로, 주차 지역 3개 구간으로 구분하여 운전자 분류에 적용됐다. 전체 데이터를 10-fold cross-validation 했으며, 분류 알고리즘은 Decision Tree, Random Forest, k-nearest neighbors algorithm, Multi-layer perceptron으로 구성했다. 이 중 Random Forest 알고리즘에서 약 99.3 % 이상의 높은 정확도로 운전자를 분류했다.

3.2. 문제 설명

차량의 기술 발전과 더불어 네트워크 통신을 이용한 원격 접근으로 차량을 탈취하는 도난 사건들이 최근에

〔표 1〕 피쳐 선택 과정을 통한 중요 피쳐 15개

Feature	Type of vehicle data	Range	Description	Feature rank
Long-term fuel trim bank1	Fuel	-100 - 100 (%)	주행에 따른 연료 조절 시스템의 조정 값	1
Intake air pressure	Fuel	0 - 255 (kPA)	엔진 흡기압	4
Accelerator Pedal value	Fuel	0 - 100 (%)	가속 페달 압력의 정도	9
Fuel consumption	Fuel	0 - 10000 (mcc)	엔진의 연료 소모량	11
Friction torque	Engine	0 - 100 (%)	엔진의 마찰 토크	3
Maximum indicated engine torque	Engine	0 - 100 (%)	최대 엔진 토크	5
Engine torque	Engine	0 - 100 (%)	현재 엔진 토크	6
Calculated load value	Engine	0 - 100 (%)	엔진에 대한 부하량의 계산 값	7
Activation of Air compressor	Engine	0 or 1	차량 에어 컴프레셔의 작동 여부	8
Engine coolant temperature	Engine	-40 - 215 (℃)	엔진 냉각수 온도	10
Transmission oil temperature	Transmission	-40 - 215 (℃)	변속기 오일 온도	2
Wheel velocity, front, left-hand	Transmission	0 - 511.75 (km/h)	차량 전방 좌측 휠 속도	12
Wheel velocity, front, right-hand	Transmission	0 - 511.75 (km/h)	차량 전방 우측 휠 속도	14
Wheel velocity, front, left-hand	Transmission	0 - 511.75 (km/h)	차량 후방 좌측 휠 속도	13
Torque converter speed	Transmission	0 - 16383.75 (rpm)	토크 컨버터 속도	15

(a) Driving Course - C1

(b) Driving Course - C2

〔그림 1〕 데이터 셋 챌린지에 사용된 주행 코스

Field of Data (# of features : 51) Trip Time Driver

Feature Name

Fuel_consumption	Accelerator_Pedal_value	Throttle_position_signal	...	Acceleration_speed_-_Lateral	Steering_wheel_speed	Steering_wheel_angle	Trip	Time(s)	Driver
755.2	0	0	...	-10.2	0	-499.9	1	1	A
320	0	0	...	-10.2	0	-499.9	1	2	A
256	0	0	...	-10.2	0	-499.9	1	3	A
230.4	0	0	...	-10.2	0	-499.9	1	4	A
230.4	0	0	...	-10.2	0	-499.9	1	5	A
256	0	0	...	-10.2	0	-499.9	1	6	A
256	0	0	...	-10.2	0	-499.9	1	7	A
268.8	0	0	...	-10.2	0	-499.9	1	8	A
281.6	0	0	...	-10.2	0	-499.9	1	9	A
320	0	0	...	-10.2	0	-499.9	1	10	A
⋮				⋮					
2112	15.2	17.9	...	-10.2	64	-51.8	1	169	A
2252.8	16.4	20.7	...	-10.2	108	32.9	1	170	A
2086.4	12.5	14.1	...	-10.2	100	17.2	1	171	A
857.6	5.5	2.8	...	-10.2	44	58.5	1	172	A
371.2	0	0	...	-10.2	12	57.7	1	173	A
1433.6	20.3	15.5	...	-10.2	32	31.9	1	174	A
537.6	28.5	33.4	...	-10.2	56	8.5	1	175	A
2905.6	28.5	33.4	...	-10.2	4	5.4	1	176	A
2854.4	28.9	33.4	...	-10.2	0	7.4	1	177	A
2841.6	28.5	33.4	...	-10.2	8	12.1	1	178	A
1753.6	10.2	10.8	...	-10.2	12	5.3	1	179	A

Data

〔그림 2〕 주행 데이터 셋 샘플

도 발생하고 있다. 실제 주행 데이터 셋을 기반으로 한 운전자 분류 알고리즘의 개발은 이러한 문제 해결에 도움이 될 것이다. 그러므로 차량 도난 탐지 알고리즘의 주된 목표는 새로운 주행 데이터가 생성되었을 때, 기존에 보유하고 있는 학습된 주행 데이터를 기반으로 자동차를 운전하는 실제 차량 운전자 여부를 정확하게 구분하는 것이다.

3.3. 데이터 셋 구성

차량주행 데이터 기반 도난탐지 트랙에서 사용된 데이터는 KIA Soul (S1), HYUNDAI YF Sonata (S2) 두 대 차량을 운전자 10명이 주행한 데이터로 구성된다. 주행 구간은 그림 1과 같이 고려대학교 자연계 캠퍼스부터 상암월드컵경기장 코스 1 (C1)과 고려대학교 자연계 캠퍼스부터 고대앞사거리, 안암오거리, 용두동사거리, 신설동역, 동묘앞역, 창신역, 보문역, 고려대학교 자연계 캠퍼스와 같이 코스 2 (C2)로 구성된다. 주행 코스의 길이는 자동차 전용도로가 포함된 주행 코스 C1이 약 17km이며, 일반 도심 주행도로로 구성된 주행코스 C2는 약 5.5km이다.

차량주행 데이터 기반 도난탐지 트랙에서는 예선과 본선을 구분하여 데이터 셋을 구성했다. 예선은 S1 차량과 C1 코스로 하는 데이터 셋을 구성했으며, 전체 9명의 운전자가 주행 구간을 4번을 주행했다. 각 데이터 셋은 운전자가 주행했을 시 운전자를 의미하는 A - I 사이의 알파벳으로 나타냈으며, 학습용인 3번의 주행 데이터 셋(약 460km) 과 검증용인 1번의 주행 데이터 셋(약 150km) 으로 구성했다[1]. 추출 데이터는 차량 속도, 스티어링 휠 각도, 연료소모량, 미션오일 온도 등 51개의 피쳐로 구성된다.

주행 데이터 셋의 세부적인 형태는 그림 2와 같으며,

1) http://ocslab.hksecurity.net/Datasets/datachallenge2018/vehicle

데이터의 첫 번째 레코드에 Feature Name이 있으며 순차적으로 주행 데이터가 누적된다. 각 피처는 그림 2의 Feature name과 같이 51개의 피처로 구성되며, 운전자별로 몇 번째 주행인지를 나타내는 Trip, 레코드의 시간을 나타내는 Time (sec), 그리고 운전자 레이블링과 같이 전체 3개의 피처가 추가된다.

데이터 챌린지에서 검증용 데이터는 운전자 레이블링 부분을 삭제하여 제공했으며, 이때 검증용 주행 데이터는 1회의 주행 데이터를 절반으로 나누어 2개의 주행 데이터로 구성했으며, 전체 5명의 주행 데이터를 랜덤하게 배치하여 구성했다.

3.4. 평가 방법

차량 도난 탐지 알고리즘의 평가는 운전자 분류 정확도를 통해 진행했다. 본 트랙에서는 운전자 분류를 Multi-class classification으로 수행했으며, 운전자 분류 정확도는 아래 제시된 정확도 계산식을 이용했다.

$$Accuracy = \frac{T_A + T_B + \cdots + T_N}{D_A + D_B + \cdots + D_N} \quad (2)$$

$D_A, D_B, \cdots, D_N$ 는 운전자별 전체 주행 데이터 수를 의미하며, $T_A, T_B, \cdots, T_N$ 는 해당 운전자를 올바르게 분류한 데이터 수이다. 또한, $F_A, F_B, \cdots, F_N$ 는 해당 운전자를 잘못 분류한 데이터 수이다. 표 2는 각 운전자의 주행 데이터 수, 일치 수, 비일치 수를 나타낸 것이다.

〔표 2〕 분류 정확도 평가 방법

카테고리	운전자	주행 데이터수	실제결과	
			일치	비일치
실험결과	A	D_A	T_A	F_A
	B	D_B	T_B	F_B
	…	…	…	…
	N	D_N	T_N	F_N

Ⅳ. 대회 결과

4.1. 본선 결과

2018 정보보호 R&D 데이터 챌린지 - 차량주행 데이터기반 도난탐지 트랙에는 참가자 팀명 태듕, IMLAB, 차도둑들, 고려대&연세대, 오투랩스 전체 5팀이 참가했다. 참가한 팀들의 정확도는 표 3에 나타냈다. 1st 세션에서는 C2 주행코스와 S2 차량을 이용해 데이터 셋을 구성했으며, 2nd 세션에서는 C1 주행코스와 S2 차량을 이용해 데이터 셋을 구성했다. 1st 세션에서는 운전자의 주행 4회를 학습용으로 1회를 검증용으로 사용하였다. 2nd 세션에서는 9회의 주행을 학습용으로 1회의 주행을 검증용으로 사용하였다. 참가팀들의 분류 정확도는 1st 세션보다 2nd 세션에서 높게 나타났다.

〔표 3〕 본선 참가자별 분류 정확도

참가팀 팀명	1st 세션 분류 정확도(%)	2nd 세션 분류 정확도(%)
태듕	40.832	59.117
IMLAB	31.904	52.995
차도둑들	24.137	48.236
고려대&연세대	40.878	30.48
오투랩스	23.698	40.428

4.2. 차량 도난 탐지 방법론

대회 참가팀들은 주행 데이터의 피처 51개 중 운전자 분류에 영향을 주지 않는 피처들을 제거하기 위해 상관 분석 (correlation analysis)을 수행했다. 상관 분석 결과 피처간에 상관도가 높게 형성되어 있으면 피처에서 제외했으며, 피처의 분산 분포를 통해 분산이 '0'으로 되어 있는 피처들도 제외했다. 이들 참가팀들은 선택된 피처들에 대해 데이터 정규화 과정을 진행하였고, 다양한 머신러닝 알고리즘들을 적용했다. 운전자 분류를 위해 적용한 알고리즘은 Random Forest, XGBoost, SVM, CNN, Boosting Tree 등이다. 그 중 일부 참가팀은 운전자 분류 정확도를 향상시키기 위해 grid search cross-validation을 사용하여 알고리즘의 hyper parameter tuning을 수행했다. 그 외에 운전자 분류 결과를 분류 점수로 활용하여 높은 점수를 받는 운전자를

해당 주행 데이터의 운전자로 분류하는 post processing 방법도 수행했다.

Ⅴ. 결 론

2018 정보보호 R&D 데이터 챌린지 - 차량주행 데이터기반 도난탐지 트랙은 운전자별 주행 데이터에 대한 분석을 통해 현재 주행 중인 운전자를 식별하는 챌린지로써 국내 및 해외에서 처음으로 진행된 트랙이다. 도난탐지 트랙의 예선 및 본선에서 운전자 9명에 대한 분류 정확도는 낮게 나타났으며, 5명에 대해서는 더 높은 분류 정확도를 얻었다. 일반적으로 데이터 분석의 경우, 해당 분야의 전문 지식이 데이터 분석과 패턴 분석에 많은 부분을 차지하지만, 도난탐지 트랙의 주행 데이터는 차량 관련 종사자가 아닐 경우 해당 데이터가 의미하는 바를 자세하게 알기 어려운 제약 사항이 존재한다. 그럼에도 불구하고, 이번 데이터 챌린지에 참가한 그룹들은 통계적 기반으로 데이터를 분석하고 모델링 했으며, 분석하는 과정과 결과에 있어 의미 있는 분류 결과를 도출해 내었다. 또한, 운전자 주행 데이터가 도난 탐지를 위한 운전자 분류뿐만 아니라, 운전자에게 특화된 의료와 보험과 같은 맞춤형 서비스를 제공할 수 있는 가능성을 확인할 수 있었다.

다만, 신속하고 정밀한 차량 도난 탐지를 위해서는 우선적으로 본 대회에서 제공된 데이터 형식 외에 다각도로 접근하여 수집된 운전자 주행 데이터가 필요로 할 것이며, 높은 운전자 분류 정확도를 도출하기 위해 방법론에 대한 꾸준한 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] “Volkswagen Group models vulnerable to hackers”, Computest, last accessed: ‘2019.01.30, http://persberichten.deperslijst.com/84335/press-release-volkswagen-group-models-vulnerable-to-hackers.html

[2] “The Connected Car Ways to get unauthorized access and potential implications”, Computest, last accessed: ‘2019.01.30., https://www.computest.nl/documents/9/The_Connected_Car._Research_Rapport_Computest_april_2018.pdf

[3] “Experimental Security Assessment of BMW Cars: A Summary Report”, Keen security lab, last accessed: ‘2019.01.30., https://keenlab.tencent.com/en/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf

[4] “정보보호 R&D 데이터 챌린지 2018”, last accessed:’2018.01.30., http://datachallenge.kr/

[5] “Kaggle”, last accessed: ‘2018.01.30., https://www.kaggle.com/

[6] “NIPS (Neural Information Processing Systems Conference) Competition Track” , last accessed: ‘2018.01.30, https://nips.cc/Conferences/2018/CompetitionTrack

[7] “정보보호 R&D 데이터 챌린지 2017”, last accessed: ‘2018.01.30, http://datachallenge.kr/challenge17/

[8] Enev, M., Takakuwa, A., Koscher, K., & Kohno, T “Automobile driver fingerprinting”, *Proceedings on Privacy Enhancing Technologies*, 1, pp. 34-50.

[9] Kwak, Byung Il, JiYoung Woo, and Huy Kang Kim “Know your master: Driver profiling-based anti-theft method”, *2016 14th Annual Conference on Privacy, Security and Trust. IEEE*, pp. 211-218.

[10] Chen, Dongyao, Kyong-Tak Cho, and Kang G. Shin “Mobile IMUs Reveal Driver's Identity From Vehicle Turns” *arXiv preprint*, arXiv: 1710.04578

〈저 자 소 개〉

곽 병 일 (Byung Il Kwak)
학생회원

2013년 2월 : 세종대학교 컴퓨터공학과 졸업
2013년 9월~현재 : 고려대학교 정보보호학과 석·박사통합과정
관심분야 : 온라인게임 보안, 데이터 마이닝, 네트워크 보안, IoT 보안

김 휘 강 (Huy Kang Kim)
종신회원

1998년 2월 : KAIST 산업경영학과 학사
2000년 2월 : KAIST 산업공학과 석사
2009년 2월 : KAIST 산업 및 시스템공학과 박사
2004년 5월~2010년 2월 : 엔씨소프트 정보보안실장. Technical Director
2010년 3월~2014년 12월 : 고려대학교 정보보호대학원 조교수
2015년 1월~현재 : 고려대학교 정보보호대학원 부교수
관심분야 : 온라인게임 보안, 네트워크 보안, 네트워크 포렌식