Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.5, October 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.5.919

운전 패턴을 이용한 운전자 보조 인증방법*

정 종 명,† 강 형 철, 조 효 진, 윤 지 원, 이 동 훈‡
고려대학교 정보보호대학원

The Sub Authentication Method For Driver Using Driving Patterns*

Jong-myoung Jeong,† HyungChul Kang, Hyo Jin Jo, Ji Won Yoon, Dong Hoon Lee‡
Graduate School for Information Security, Korea University

요 약

최근에 많은 IT기술들이 자동차에 적용되고 있다. 하지만 일부 자동차 IT 기술들은 보안에 대한 적절한 고려 없이 자동차에 적용되어 보안 사고를 야기할 수도 있다. 특히 최근의 연구 결과들은 차량 소유자 인증을 해주는 특정 모델의 스마트키가 무선 신호를 재전송하거나 이를 위조하는 공격으로부터 안전하지 않고, 이를 통해 차량을 탈취할 수 있음을 실험을 통해 증명하였다. 따라서 본 논문에서는 스마트키의 무선 신호 조작 공격을 이용한 차량도난으로부터 안전한 차량 운전자 인증 방법을 제안한다. 오늘날 차량에 구축된 전자장치간의 네트워크에서는 운전자의 운전 패턴에 대한 정보를 얻을 수 있다. 본 논문에서는 이러한 차량 소유자의 운전 패턴 정보를 학습시켜 이를 표준 정규분포화한 후, 운전자에 대한 인증이 가능한 인증 모델을 설계하였다. 또한 제안하는 인증 모델을 검증하기 위해 k-묶음 교차 검증을 수행하였고, false positive rate가 0.35일 때 true positive rate 0.7 로 운전자 인식이 가능함을 확인하였다. 제안하는 인증모델은 차량 소유자에게 연락할 수 있는 모듈(eg. 3G/4G 통신 module)과 함께 사용된다면 기존의 소유기반(스마트 키)의 인증 방식 보다 더 안전하게 차량을 보호할 수 있다.

ABSTRACT

Recently, a variety of IT technologies are applied to the vehicle. However, some vehicle-IT technologies without security considerations may cause security problems. Specially, some researches about a smart key system applied to automobiles for authentication show that the system is insecure from replay attacks and modification attacks using a wireless signal of the smart key. Thus, in this paper, we propose an authentication method for the driver by using driving patterns. Nowadays, we can obtain driving patterns using the In-vehicle network data. In our authentication model, we make driving ppatterns of car owner using standard normal distribution and apply these patterns to driver authentication. To validate our model, we perform an k-fold cross validation test using In-vehicle network data and obtain the result(true positive rate 0.7/false positive rate is 0.35). Considering to our result, it turns out that our model is more secure than existing 'what you have' authentication models such as the smart key if the authentication result is sent to the car owner through mobile networks.

Keywords: Vehicle Security, Driver Authentication, Driving pattern Authentication

접수일(2013년 8월 7일), 수정일(2013년 9월 26일), 게재확정일(2013년 9월 28일)
* 본 연구는 산업통상자원부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)의 일환으로 수행하였음.[KI002113, Car-헬스케어 보안 기술 개발]
† 주저자, jmjeong.in.korea@gmail.com
‡ 교신저자, donghlee@korea.ac.kr(Corresponding author)

I. 서 론

초기의 자동차는 대부분의 장치가 기계식으로 제어되었지만, IT 기술의 발전과 함께 최근 출시되는 자동차는 전자적인 신호의 송수신으로 제어된다. 이를 위하여 ECU(Electronic Control Unit)라는 전자제어장치가 자동차에 도입되었고, 자동차에 설치된 ECU들은 자동차내부의 각 부품에서 발생하는 신호를 감지하고 운전자의 조작에 따라 신호를 발생시키는 방식으로 자동차를 제어한다. 자동차 한 대에는 차종에 따라 적게는 10개에서 많게는 100여개의 ECU가 장착된다. ECU는 자동차의 각 장치를 제어하고 서로 다른 ECU와 상호작용하면서 전체 시스템을 작동시킨다. 많은 수의 ECU들의 원활한 통신을 위해 CAN(Controller Area Network) 프로토콜이 도입되었으며, 이 프로토콜은 국제표준화기구(ISO)와 미국의 자동차엔지니어협회(SAE)에 의해서 국제 표준으로 등록되었다[1][2].

최근에는 IT 기술의 발전과 함께 자동차의 무선 도어 잠금장치가 개발 되었고, 이로 인해 자동차와 운전자의 편리한 근거리 인증이 가능해졌다. 또한 스마트폰과 무선 통신 기술이 연동되면서 원거리에서도 차량 개폐 및 시동 등 다양한 기능을 수행 할 수 있다. 하지만, R. Verdult 등[3]은 현재 자동차에 적용되고 있는 무선 RF 통신을 이용한 스마트키 공격 시나리오에 대해서 소개하였다. 공격에 사용된 스마트키는 RF 통신을 통하여 열쇠와 시동장치 사이에 데이터를 주고받으며, 이 과정에서 Hitag2 [1]프로토콜을 사용한다. Hitag2프로토콜은 NXP사에서 개발된 인증 프로토콜로 2012년에 전 세계의 많은 차량 제조사에서 자동차 키의 인증 프로토콜로 사용되었다. 공격자는 이 Hitag2 프로토콜의 취약점을 이용하여 자동차와 스마트키의 데이터를 도청 및 분석함으로써 짧은 시간(360초)내에 비밀키를 획득할 수 있음을 보였다. 즉, 소유기반(what you have) 인증 기법에서 발생하는 분실 위협 이외에 다른 위협이 존재함을 보여주었다.

보험개발원에서 발표한 자료[4]에 따르면 2011년 한 해 동안 국내에서 발생한 도난건수는 715건에 이르며 도난으로 인해 지급된 보험금은 87억원으로 사상 최고치를 기록하였다. 도난 건수에 비해 보험금이 높은 까닭은 차량 한 대 당 도난에 의한 피해액이 늘어나고 있음을 의미하며 이러한 상황은 스마트키 이외에 새로운 도난 방지 시스템의 필요성을 대두시켜주고 있다.

본 논문은 운전 패턴을 이용한 자동차 소유자의 인증 방법을 제안한다. 액셀을 이용한 가속 페달을 누르는 패턴은 운전자의 운전 습관에 따라 다르므로, 이러한 특성을 미리 분석 및 저장한다면 현재 운전자와 자동차 소유자의 운전 패턴을 비교하는 방법으로 자동차의 실제 소유자를 구별할 수 있다. 제안하는 기법은 학습단계과 검증단계로 나뉜다. 학습단계에서는 자동차의 속성값 즉 RPM(Revolutions Per Minute), 속도, 쓰로틀(throttle)[2]의 현재 상태에 대한 정보를 OBD PID[3](On-Board Diagnostics Parameter IDs)를 통해 일정 주기로 받아온다. 그리고 이를 학습하여 자동차 소유자의 운전 패턴에 대한 분포를 구성한다. 검증단계에서는 기 학습된 자동차 소유자의 운전 패턴을 이용하여 현재 자동차 운전자가 소유자인지를 검증한다. 제안하는 기법은 SAE J1979 표준인 OBD PID를 사용함으로써 자동차 제조사가 아닌 제3의 제조사에서도 설계 가능하다[5].

본 논문의 구성은 다음과 같다. 먼저, 2절에서는 배경 지식에 대해서 소개한다. 3절에서는 자동차 운전자 인증 방법에 대해 소개한 후, 4절에서는 해당 인증 방법의 설계를 제시한다. 마지막으로 5절에서는 제안하는 방법을 실험하고 그 결과의 효율성 분석을 한다.

II. 배경 지식

본 장에서는 제안하는 기법에 필요한 배경지식과 기존 연구의 동향에 대해 설명한다.

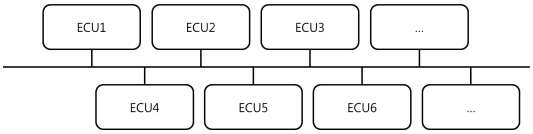
2.1 운전 패턴 인식

2004년, C. Lin 등[6]에 의해 하이브리드 전기 트럭의 연료소비율을 개선하기 위한 운전 패턴 인식 연구가 진행 되었다. 해당 연구는 트럭으로부터 입력받은 일정 기간의 운전 데이터를 6가지 운전습관들로 분류하여 현재 트럭이 최소한의 연료소비를 하도록 제어하는 실험을 진행하였다. 하지만 해당 실험은 분류

1) Hitag2 : 선형 피드백 시프트 레지스터 암호화 방식을 사용한 인증 프로토콜로 카드와 자동차 키에 사용.

2) 쓰로틀 : 자동차 배기가스를 배출하기 위해 흡입하는 공기의 양을 조절하는 장치.

3) OBD PID : 자동차의 고장여부를 진단하기 위해 사용되는 자동차 용 진단기기가 자동차 내의 정보를 가져오기 위해 보내는 정보 요청 패킷.



〔그림 1〕 CAN 프로토콜 BUS 모형

할 운전 패턴이 6가지 밖에 되지 않으므로 차선 변경이나, 곡선 구간을 운행하는 상황을 구별할 수 있지만 운전자를 구별할 수 없기 때문에 운전자 인증에 사용할 수 없다.

2010년, Y. Zhang 등[7]은 잘 훈련된 운전자의 핸들 데이터를 입력 받아 능숙한 운전자와 미숙한 운전자를 구분하는 실험을 수행하였다. 해당 논문은 곡선 주행 혹은 차선 변경 시 입력된 핸들 데이터를 푸리에 변환을 통해 주파수 영역으로 변형하고 그 결과에 분류기법을 적용하여 운전자들을 분류하였다. 하지만 해당 실험은 자동차 내부 ECU의 성능을 고려하지 않았고, 각 운전자 고유의 운전 패턴을 분류하지 않기 때문에 인증방법으로 사용할 수 없다.

2011년, D. Johnson 등[8]이 제시한 연구는 휴대하기 편한 스마트폰의 센서를 이용하여 스마트폰을 차안에 거치하면 운전자의 안전하지 못한 운전 행위를 탐지하여 알려주는 운전 보조 시스템을 구현하였다. 하지만 해당 연구에 사용된 스마트폰은 Apple의 IPhone으로 특정되어 있기 때문에 범용적으로 사용하기 어렵고, 운전 행위를 인식할 수는 있지만 운전자를 구별할 만큼 세밀하게 분류해주지 않는 단점이 있다.

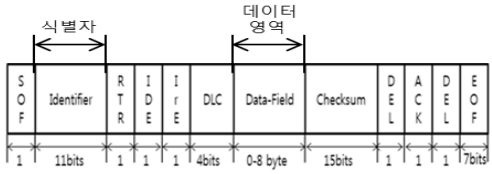
따라서, 본 논문에서는 직선주로에서 운전자가 제어하는 속도에 기반하여 운전자별로 나타나는 특성을 학습하여 이를 통해 운전자를 인증하는 방법을 제시하고 실험하였다.

2.2 CAN 프로토콜

CAN 프로토콜은 지능형 디바이스 네트워크 구축을 위한 높은 신뢰성을 가진 시리얼 버스 시스템으로, 차량용 네트워크의 표준(ISO11898)[1]이며 ECU 통신이다. CAN 프로토콜 네트워크 구조는 〔그림 1〕과 같이 버스형으로 되어있으며, 각 ECU는 네트워크에 메시지를 브로드캐스팅하는 방식으로 데이터를 송수신한다.

2.3 CAN 프로토콜 메시지 구조

〔그림 2〕는 CAN 프로토콜 메시지의 구조를 나타



〔그림 2〕 CAN 프로토콜의 메시지 구조

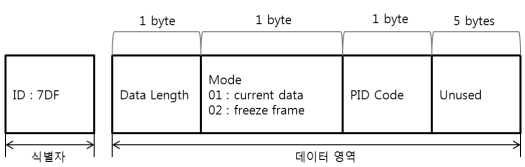
낸다. 〔그림 2〕에서 볼 수 있듯이 CAN 프로토콜의 메시지 구조는 어떤 ECU가 메시지를 생성했는지 명시하는 식별자(Identifier) 영역과 8 byte의 데이터 영역(Data-Filed)이 존재한다. 각 ECU가 서로 통신 할 경우, 송신 ECU는 자신의 ID를 식별자 영역에 기입하고, 자신의 상태 정보에 대한 값을 데이터 영역에 저장하여 CAN을 통해 브로드캐스팅 한다. 수신 ECU는 브로드캐스팅 된 메시지 중에서 자신에게 필요한 정보를 식별자를 통해 필터링하여 메시지를 수신한다.

2.4 OBD PID

2005년 1월부터 국내에서 판매되는 자동차에는 OBD 단자의 장착이 의무화 되었다[9]. OBD 단자는 자동차의 고장 진단을 위하여 자동차 정비소에서 사용되는 자동차 진단장비의 접근 경로이다[10]. 자동차 진단장비는 OBD PID 방식을 이용하여 차량의 고장 및 상태 정보를 받아온다.

OBD PID는 SAE J1797 표준[5]으로 자동차 진단 장비가 〔그림 3〕과 같이 CAN 데이터 영역에 자동차 정비에 필요한 상태 값을 요청하는 PID Code를 넣어 CAN을 통해 브로드캐스팅하고 요청한 값을 받아오는 방식이다. 요청받은 상태 값을 담당하는 ECU에서는 수신한 OBD PID의 Mode값을 확인하여 현재 상태값(current data frame) 혹은 고장 당시의 상태값을(freeze frame) 응답으로 결정하고 해당 상태 값을 CAN을 통해 브로드캐스팅한다.

OBD PID 방식은 기본적으로 CAN 프로토콜 메시지의 식별자 영역에 0x7DF를 넣고 데이터 영역



〔그림 3〕 OBD PID 요청 구조

〔표 1〕 RPM, 쓰로틀, 속도에 대한 OBD PID값

PID	Return	Description	Units
0C	2	Engine RPM	rpm
11	1	Throttle position	%
0D	1	Vehicle speed	km/h

3bytes를 이용하게 된다. 해당 데이터 영역에는 길이, 모드, PID가 기입된다. 본 인증모델에서 사용할 속성인 RPM, 쓰로틀, 속도에 대한 PID 정보는 〔표 1〕과 같다. 따라서 본 인증 모델에서 사용하는 OBD PID 방식의 데이터 영역에 들어가는 값은 〔그림 3〕에서 명시되어 있듯이 첫 번째 byte에는 뒤따라오는 데이터의 길이를 의미하는 0x02가 들어가게 되고, 두 번째 byte에는 현재 상태의 속성값을 받을 수 있도록 0x01 값을 넣어주며, 세 번째 byte에 〔표 1〕에는 기입되어 있는 RPM, 쓰로틀, 속도에 해당하는 PID 값을 넣어준다. 〔그림 3〕의 예와 같은 CAN 프로토콜 메시지를 CAN을 통해 브로드캐스팅 하면 차량으로부터 해당 PID에 대한 정보를 받을 수 있다.

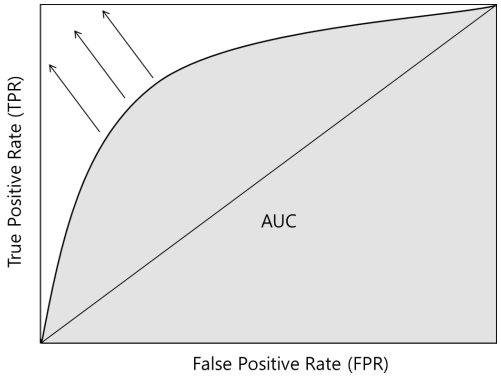
2.5 K-묶음 교차 검증법

통계를 이용한 인증 방식 도입의 신뢰도를 위하여 K-묶음 교차 검증법(K-fold cross validation)을 수행한다〔11〕. 해당 방법은 전체 데이터를 K개의 집합으로 나누어 K-1개의 집합으로 학습을 시키고 남은 1개의 집합으로 테스트를 진행한다. 그리고 이러한 절차를 테스트 집합을 변경해가며 총 K번 반복 수행하는 방법이다. 따라서 특정 데이터에서만 발견되는 결과를 일반화시키지 않는 검증절차로 사용할 수 있다.

2.6 ROC 커브

ROC(Receiver Operating Characteristic) 커브는 검증하고자 하는 특정 모델의 정확도를 평가 할 수 있는 방법이다〔12〕. ROC 커브를 표현하기 위해서는 검증하고자하는 모델의 FP(False Positive), TP(True Positive), FN(False Negative), TN(True Negative)를 계산하여 FPR(False Positive Rate)과 TPR(True Positive Rate)을 구해야 한다.

FPR과 TPR은 다음과 같이 계산할 수 있다.



〔그림 4〕 ROC 커브 예시

$$TPR = TP/(TP+FN)$$
$$FPR = FP/(FP+TN)$$

TPR, FPR 계산을 한 후, X축은 FPR, Y축은 TPR로 지정하여 〔그림 4〕와 같은 ROC 그래프로 나타낼 수 있다. 이 ROC 커브를 적분한 AUC(Area Under Curve)가 0.5 이하일 경우는 해당 모델의 인증이 제대로 되지 않음을 의미하며 AUC가 1에 가까울수록 TPR이 높고 FPR이 낮으므로 인증 실패가 적고 인증 성공이 많은 모델이 된다.

III. 제안하는 운전자 인증방법

본 절에서는 자동차의 CAN 프로토콜 메시지를 이용하여 현재 자동차 운전자가 자동차의 실제 소유자인지 구별하는 인증 방법에 대해서 소개한다.

3.1 개념

운전자가 차량을 운전 할 경우에는, 운전자의 성격에 따라 드러나는 많은 습관들이 있다. 속도를 감속할 때 브레이크를 밟는 정도, 브레이크를 밟을 때 끊어서 밟는 습관, 가속 할 경우 RPM을 유지하는 정도, 액셀러레이터를 밟는 정도 등 이러한 습관들은 운전자마다 다른 패턴을 보이고 있다. 따라서 이러한 습관들을 이용하여 현재 운전하고 있는 차량의 운전자의 패턴을 차량 소유자의 패턴과 비교하게 되면 현재 운전자가 차량의 소유자인지에 대한 인증이 가능하다. 또한 차량 도난 시에는 텔레매틱스 서비스를 활용한 2차 인증을 통해 차량 소유자에게 알람을 주도록 만들 수도 있다.

제안하는 인증 기법은 차량 소유자가 키를 분실하

거나 혹은 키가 해킹되더라도 악의적인 목적의 공격자로부터 차량 도난을 방지한다. 차량의 ECU는 많은 연산을 수행하는데 적합하지 않으므로 본 논문에서는 복잡한 학습 알고리즘을 사용하지 않고 간단한 확률 분포 함수를 이용한 인증 방식을 제안한다.

3.2 공격자 모델

공격자는 차량을 도난하려는 목적을 가지며 일반적으로 차량을 도난하기 위하여 다음과 같은 방식으로 차량의 키가 없는 상태에서 도난을 시도 한다[13].

- 차량 내에 소유자가 숨겨 둔 보조키 탈취,
- 차량 소유자가 잠시 내린 틈에 차량 탈취,
- 주차 혹은 정비를 위해 맡긴 차량키 탈취,
- 차량 키를 차량 소유자 모르게 복사

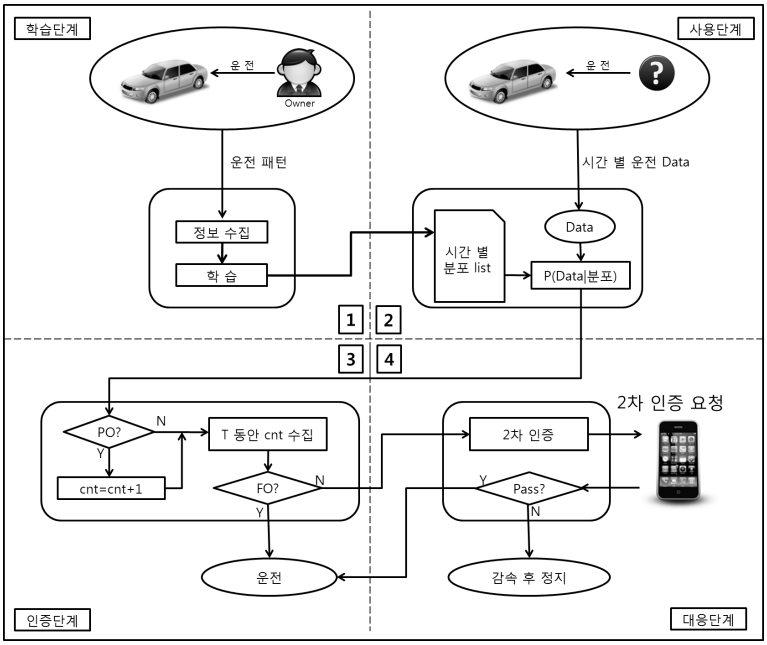
일반적으로 차량키를 탈취하는 방식은 차량 소유자가 탈취가 되었음을 빠른 시간 내에 깨달을 수 있어 신고로 이어지지만 차량의 키가 복사 될 경우에 그 위협에 대해 차량 소유자가 인지하기 힘들다. 특히 스마트키의 보급과 함께 차량의 키를 해킹하여 복사하는 방법이 2012년 R. Verdult 등에 의해 공개되었다[3]. 따라서 본 논문에서 공격자는 현재 자동차에 적용되고 있는 무선 RF 통신을 이용한 스마트키에 대한 공격이 가능하다고 가정한다.

3.3 운전자 인증 모델

본 연구에서는 차량 소유자와 타인의 차량 내부 상태 메시지(OBD PID에 대한 응답메시지)를 통해서 현재 자동차 운전자가 자동차의 실제 소유자인지를 인증한다. 제안하는 인증 모델을 설명하기 위해 사용하는 표기법은 [표 2]와 같다.

[표 2] 인증 모델 표기법

표기	설명
PO	부분적 소유자 운전패턴(partially owner)
FO	전체적 소유자 운전패턴(fully owner)
T	PO를 판단하는데 필요한 기간 (s)
t	데이터를 수집한 시간구간 (ms)
ID	속도, RPM, 쓰로틀
μ	평균.
σ	표준편차.
y	각 시간 구간별 수집된 테스트 데이터.
γ	y가 인풋으로 들어갈 때 정규분포에서의 확률
TH	운전자로 인증할 γ의 기준값(threshold)
cnt	TH 보다 높은 γ의 개수(count)
y_{ID}^{t}	t 시간구간에 해당 ID에 대하여 수집된 테스트 데이터
μ_{ID}^{t}	t 시간구간에 해당 ID에 대해 구성된 정규 분포의 평균
σ_{ID}^{t}	t 시간 구간에 해당 ID에 대해 구성된 정규분포의 표준편차



[그림 5] 차량에서의 소유자 인증방식 절차

〔그림 5〕는 실제 차량에 적용될 경우 인증을 위한 전체 절차를 간략하게 도식화 한 것으로 크게 학습, 사용, 인증, 대응과 같이 4가지 단계로 나누어져 있다. 차량 소유자는 첫 번째 학습 단계에서 차량에 본인의 운전패턴을 학습 시킨다. 본 모델은 입력된 학습 패턴에서 평균과 편차만을 계산하기 때문에 차량 내에 존재하는 ECU들의 평균적인 성능으로도 충분히 연산이 가능하다.

사용 단계에서는 차량 운행 시에 실시간으로 생성되는 차량 내 운전 데이터를 학습 단계에서 구성한 운전패턴분포에 적용하여 유사도 확률을 계산한다. 이 단계에서 구하는 확률은 표준정규분포에서의 확률이기 때문에 표준정규분포 표를 이용하여 구할 수 있다.

인증단계에서는 인증을 위한 계산을 수행한다. 본 모델에서 인증은 두 번의 비교 절차를 통해 PO(Partially Owner)와 FO(Fully Owner)를 판단한다. PO는 순간적으로 소유자와 유사한 운전패턴이 뜨는 경우에 카운트 되는 값으로 이 값이 전체 운전 구간 중 많은 부분을 차지하게 되면 FO로 판정된다.

대응 단계에서는 현재 운전자가 차량 소유자가 아닐 경우, 차량의 텔레매틱스 장치를 통한 차량 소유자의 핸드폰 연결이나 기타 추가적인 인증방식을 사용하여 2차 인증으로 유도하며, 2차 인증을 통과하지 못했을 경우, GM OnStar의 slowdown[4] 서비스와 같이 차량을 서서히 감속 시켜 정지시키는 기술로 연계될 수 있다.

IV. 제안하는 인증 기법 설계

본 절에서는 제안하는 인증 모델의 구조를 제시한다. 제안하는 인증모델은 크게 데이터 수집단계와 학습단계, 인증단계로 구성된다.

4.1 데이터 수집 단계

직선 주로에서 차량을 운전할 때, 운전자는 가속 및 감속을 하게 된다. 이러한 가속 및 감속을 하는 습관은 개인의 운전습관이나 RPM을 유지하려는 습관, 차량의 기계적 파손을 막으려는 습관에 의해 차이가 발생하게 된다. 이러한 차이는 속도와 RPM, 그리고 액셀러레이터가 밟히는 정도에 따라 변화하는 쓰로틀의 값의 변화를 분석하여 구분할 수 있다.

데이터 수집 단계에서는 차량 소유자가 운전할 때 OBD PID를 10ms 주기로 전송하여 자동차의 현재 상태, 즉 RPM, 속도, 쓰로틀의 상태 정보를 수집한다.

4.2 학습 단계

차량의 ECU는 많은 연산을 수행하게 될 경우, 그 성능의 제약으로 인하여 처리속도가 느려질 수 있으므로 연산량이 적은 확률 분포 함수를 이용하여 모델을 구성한다. 제안하는 인증기법의 학습 단계에서는 데이터 수집 단계에서 동일한 코스 운전을 반복하며 수집한 RPM, 속도, 쓰로틀의 상태정보 중 동일한 시간구간들의 값들을 분리해낸 후 분리 된 상태 값들이 평균값을 기점으로 정규분포에 근사한다고 가정하여 표준정규분포를 구성한다.

따라서 수집된 데이터를 이용하여 정규분포를 형성하는데 필요한 각 시간 구간당 평균 μ_{ID}^{t}와 표준편차 σ_{ID}^{t}를 구하여 인증단계에서 사용한다. OBD PID의 결과를 10ms 주기로 받아오므로 이에 해당하는 평균과 표준편차는 다음과 같이 구할 수 있다.

$$\mu_{ID}^{t} = E(y_{ID}^{t}) = \frac{1}{100}\sum_{i=\lfloor t \rfloor}^{\lceil t \rceil} y_{ID}^{i}$$

$$\sigma_{ID}^{t} = \sqrt{E(y_{ID}^{t} - \mu_{ID}^{t})^{2}}$$

4.3 인증 단계

〔그림 6〕은 인증 순서를 나타낸다. 실시간으로 수집되는 운전자의 RPM, 속도, 쓰로틀의 상태 정보를 이용하여 기 학습된 표준정규분포를 통해 유사도 확률을 계산한다. 유사도 확률 γ가 TH 보다 클 경우, 운전자를 PO로 판단하여 해당 cnt를 증가시키고, TH보다 작으면 cnt를 증가시키지 않는다. 일정 시간이 지난 후 PO로 판단된 cnt 값의 크기를 이용하여 현재 차량의 운전자가 소유자 인지를 판단하게 된다.

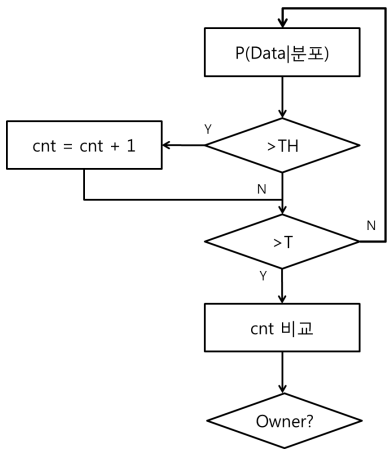
학습단계를 통해 생성된 분포들은 〔그림 7〕과 같이 각자 고유의 평균과 표준편차로 다른 분포를 나타내게 되므로 차량 소유자를 판별하기 위한 기준값 TH가 시간 구간별로 달라진다. 따라서 이러한 기준값을 일괄적으로 적용하기 위하여 초당 생성된 분포를 정규화하여 〔그림 8〕과 같이 동일한 기준값 TH이 사용 가능하도록 설계하였다. 아래 식은 생성된 분포를 표준정규

4) OnStar Slowdown Service : 도난당한 차량이 운행 중일 때 차량을 서서히 감속시키고 기능을 정지 시키는 서비스

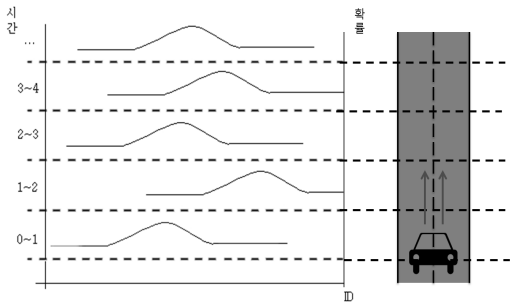
분포로 변환하는 식이다.

$$Z_{+} = \frac{y_{ID}^{t} - \mu_{ID}^{t}}{\sigma_{ID}^{t}} \quad : \text{표준화 과정}$$

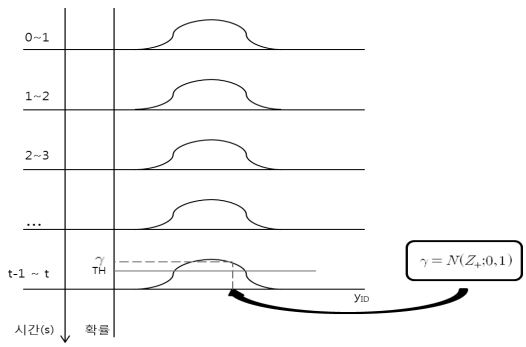
$$\gamma = N(Z_{+};0,1)$$



〔그림 6〕 인증 절차 순서도 : T 시간이 될 때까지 차량의 Data를 받아와 TH와 비교하여 PO를 판단한 뒤 T 시간이후에 PO의 개수를 이용하여 FO를 판정한다.



〔그림 7〕 시간 구간 별 정규 분포

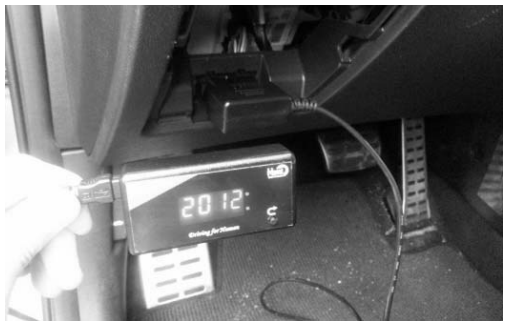


〔그림 8〕 표준정규분포로 변경된 모델에서의 비교

V. 실험 및 평가

5.1 실험 환경

자동차로부터 CAN 메시지를 수집하기 위해 차량의 OBD II 커넥터에 〔그림 9〕와 같이 ECU Data Logger 장비를 부착하였다. ECU Data Logger는 OBD II 커넥터로부터 들어오는 CAN 메시지를 기록함과 동시에 10 ms 주기로 OBD PID를 이용하여 속도, RPM, 쓰로틀에 대한 값을 차량에 요청하여 기록한다. 실험에 사용한 차량은 H사의 A모델이다.

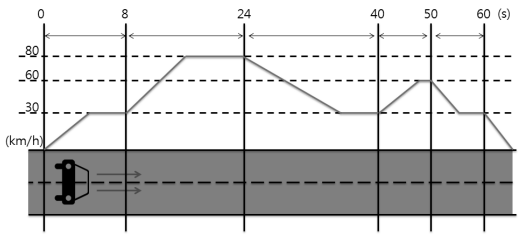


〔그림 9〕 OBD 포트와 ECU Data Logger의 연결

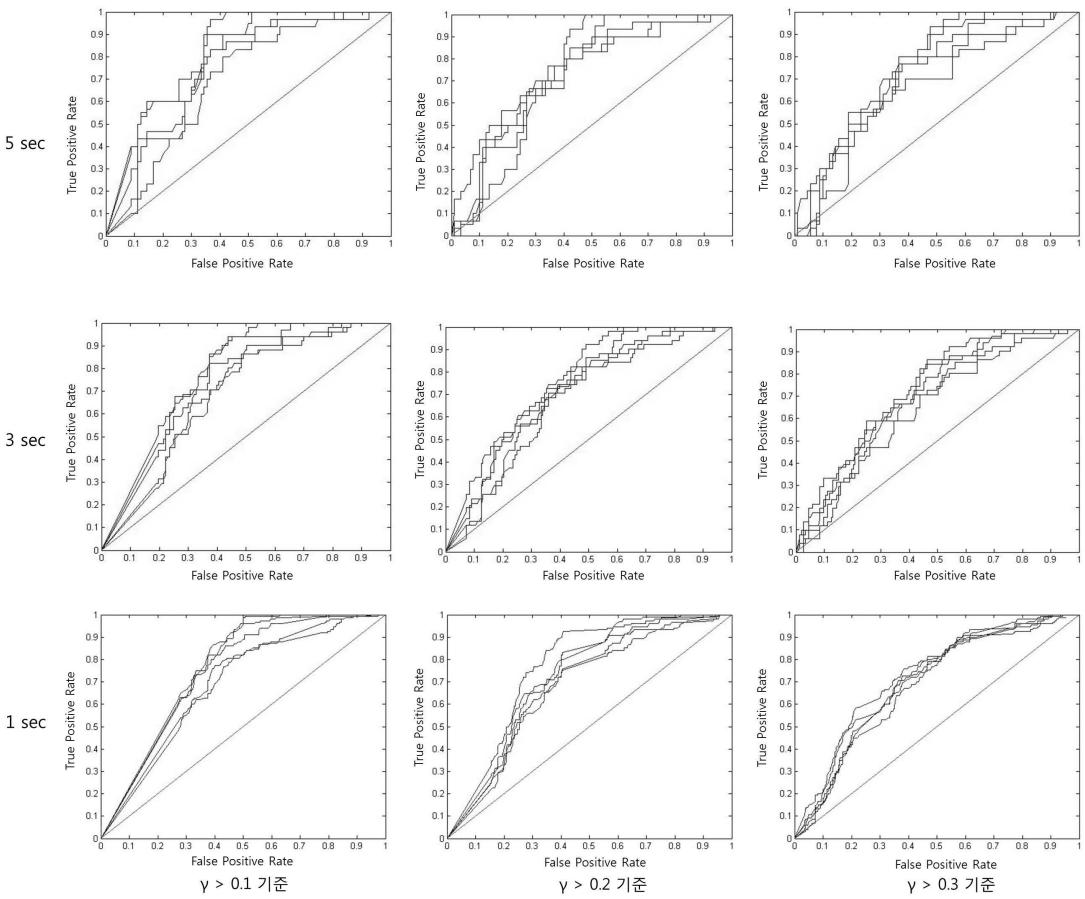
본 실험에서는 데이터 수집을 위해 차량 소유자 1인과 소유자가 아닌 다른 운전자 3인이 동일한 트랙을 반복적으로 운전하였다. 실험 차량 이외의 다른 차량이나 보행자 등과 같은 다른 환경을 배제하고 운전자가 가진 습관에 대한 데이터를 얻기 위해 자동차 부품연구소의 1km 주행 트랙에서 〔그림 10〕과 같이 실험을 진행하였다.

〔그림 10〕은 1km 직선 구간에서 가속과 감속에 대한 목표속도이다. 해당 실험에서는 가속 및 감속을

시간(초)	0~8	8~24	24~40	40~50	50~60
목표속도(km/h)	30	80	30	60	30



〔그림 10〕 1km 직선구간에서의 목표 속도



〔그림 11〕 γ와 T의 변화에 따른 ROC 커브 비교 : T를 1초, 3초, 5초로 했을 때, TH를 0.1, 0.2, 0.3으로 했을 때를 기준으로 9개의 그래프를 나타내었다. 각 그래프는 5-묶음 교차 검증법에 의해 생성된 5개의 결과를 표시하고 있다.

하는 과정에서 운전자가 RPM을 유지하는 정도 및 페달을 밟는 정도 등에서 자신의 특성을 보일 수 있도록 목표속도를 설정하여 반복적인 가속 및 감속이 가능하게 설계하였다. 또한 해당 실험에서 운전자가 가속 및 감속 시간을 미리 알게 되면 평소 습관이 아닌 해당 시간에 맞추어 가속 및 감속을 할 수 있으므로, 차량 조수석에 앉은 동승자가 목표 속도만을 지정해주고 시간은 알려주지 않은 채 실험을 수행하였다. 해당 실험에서 수집한 데이터 중, RPM에 대하여 그래프를 그려보면 〔그림 11〕과 같이 소유자와 다른 운전자 사이에 차이가 존재하는 것을 알 수 있다. 이를 효과적으로 판별하기 위하여 제안하는 인증 기법을 통해 실험 결과를 측정하였다.

5.2 실험 결과 분석

속도, RPM, 쓰로틀 상태 정보를 기반으로 기 학습된 표준정규분포를 이용하여 실시간으로 계산되는 유사도 확률 γ값이 TH값보다 낮은 경우를 PO로 판단하고 T 기간 동안의 PO의 개수를 세어 기준 개수에 이르지 못하면 차량 소유자가 아니라고 판단하여 차량 소유자 인증 결과를 도출 하였다. 우리는 TH값을 각각 0.1, 0.2, 0.3으로 변경하고 5-묶음 교차 검증법을 적용하여 반복 테스트를 한 후, 차량 소유자 인증 결과를 ROC 커브로 표현하였다.

좀 더 정확한 평가를 위해, 차량 소유자 인지를 판단하는데 필요한 시간 T를 1, 2, 3초로 변경하면서, T 동안 계산된 유사도 확률 γ 값이 0.1, 0.2, 0.3 으로 설정된 TH보다 큰 경우의 횟수를 세어서 TP(True Positive)와 FN(False Negative),

FP(False Positive), TN(True Negative)을 판단하였다.

제안하는 인증 기법의 ROC 커브는 〔그림 12〕와 같다. 5-묶음 교차 검증법에 의하여 각 그래프 마다 5개의 ROC 그래프가 그려져 있다. 세로로 나열된 그래프는 각각 좌측에 표시된 시간 동안에 계산된 유사도 확률 γ값이 0.1, 0.2, 0.3보다 클 때의 개수를 이용하여 ROC 그래프를 생성한 것이다.

ROC 그래프 상에서 볼 수 있듯이 γ가 0.3일 때보다는 0.1일 때, 또 T가 1초일 때에 비해 5초일 때의 ROC 그래프들이 좌측 상변에 나타나면서 FPR(False Positive Rate) 대비 TPR(True Positive Rate)의 비율이 더 높게 나오는 것을 확인할 수 있다. 이를 정확히 확인하기 위하여 각 ROC 그래프 별 AUC값을 계산하여 〔표 3〕의 결과를 얻었다. 〔표 3〕과 같이 γ의 기준점 TH를 0.1로 했을 때가 0.2 혹은 0.3을 TH로 설정했을 때보다 AUC가 높았다. T가 1초일 때 5 fold의 값을 보면 TH를 0.1로 했을 때의 AUC 값이 0.7403인 반면 0.2일 때는 0.7021, 0.3일 때는 0.6555값으로 계산되었다. 또한 T 값을 1초로 하여 1초 동안 차량 소유자 인지 여부를 인증하였을 경우 보다 5초 동안 인증하였을 때 AUC 값이 큰 것을 확인할 수 있다.

제안하는 방법은 결과 그래프에서 확인할 수 있듯이 T를 5초로 설정하고 TH를 0.1로 인증 모델을 수행할 경우 FPR은 0.35 수치를 유지하면서 TPR이 0.7 수치가 나오는 것으로 확인 되었다. 이는 기존의 지문인식기에 비해 높은 인증결과를 보장하지는 못하지만 차량에 추가적인 HW 설치가 필요 없고 제한된 성능을 가진 차량 내 ECU에서도 연산 가능하다는 점을 볼 때 현존하는 차량에 적용 가능한 방법이다.

〔표 3〕 5-묶음 교차 검증법 결과에 따라 적용된 AUC

		TH		
T	γ	〉= 0.1	〉= 0.2	〉= 0.3
1sec	1 fold	0.6746	0.6762	0.6583
	2 fold	0.6790	0.6595	0.6482
	3 fold	0.7335	0.7060	0.6375
	4 fold	0.7545	0.7502	0.6823
	5 fold	0.7403	0.7021	0.6555
3sec	1 fold	0.6836	0.6742	0.6508
	2 fold	0.6801	0.6820	0.6649
	3 fold	0.7551	0.7254	0.6633
	4 fold	0.7642	0.7564	0.7049
	5 fold	0.7464	0.7099	0.6606
5sec	1 fold	0.7033	0.6989	0.7063
	2 fold	0.7254	0.7141	0.7170
	3 fold	0.7992	0.7533	0.7011
	4 fold	0.8019	0.7859	0.7546
	5 fold	0.7931	0.7348	0.6972

VI. 결 론

본 논문에서는 자동차 소유자의 운전 패턴을 이용한 운전자 인증 방법을 제안하였다. 제안하는 방법은 차량의 OBD 단자를 통하여 차량의 현재 상태(속도, 쓰로틀, RPM)를 요청해 그 결과를 받았고, 해당 결과를 기반으로 차량 소유자의 운전패턴을 학습시켜 현재 운전하는 운전자를 인증하는 방식을 제안하였다. 이러한 인증방식은 차량의 도난 시에 유용하게 사용될 수 있다.

또한 제안하는 인증 방식은 자동차 제조사에 독립적인 국제 OBD PID 표준을 이용하여 운전 패턴을 분석하였기 때문에 제조사마다 각각 다른 CAN 프로토콜 메시지에 대한 명세를 확인할 필요가 없다. 따라서 차량제조업체가 아닌제 3의 공급업체에서도 설계가 가능하고 다른 특별한 장치가 필요 없기 때문에 차량 내부에 ECU 장비의 펌웨어 업데이트 만으로 적용이 가능하다.

하지만 제안하는 인증 방식은 FP(False Positive)와 FN(False Negative)가 존재하는 한계를 가지고 있다. 따라서 본 방식만을 이용하여 차량이 도난당했는지를 판별하는 것보다 자동차의 운전자가 차량 소유자인지를 확인한 후, 운전자에게 2차 인증을 요구하는 과정을 거치는 방법으로 확장되어 사용 될 수 있다.

향후 연구에서는 제안하는 인증 기술에 대한 오탐율을 줄이고 직선도로가 아닌 실제 도로상황에서 사용가능할 수 있는 개선된 인증모델에 대한 연구가 필요하다.

참고문헌

〔1〕 ISO Standard, "Road vehicles -- Controller area network (CAN) — Part 1: Data link layer and physical signalling," ISO 11898:1, 2003.

〔2〕 SAE Standard, "Vehicle Application Layer," SAE J1939/81. 1997.

〔3〕 R. Verdult, F. Garcia and J. Balasch, " Gone in 360 seconds: Hijacking with Hitag2," 21st USENIX Security Symposium, 2012.

〔4〕 이재원, "FY2011 수리비 지급현황 분석," KIDI, pp. 3-12, 2011.

〔5〕 SAE Standard, "E/E Diagnostic Test Modes," SAE J1979, Apr. 2002.

〔6〕 C. Lin, J. Sooil, P. Huei and L. Jangmoo, "Driving Pattern Recognition for Control of Hybrid Electric Trucks," Vehicle System Dynamics, vol. 42, no. 1-2, pp. 41-58, Dec. 2004.

〔7〕 Y. Zhang, W.C. Lin and C.S. Yuen-kwok, "A pattern-recognition approach for driving skill characterization," Intelligent Transportation Systems, IEEE Transactions, vol. 11, no. 4, pp. 905-916, Dec. 2010.

〔8〕 D.A. Johnson and M.M. Trivedi, "Driving style recognition using a smartphone as a sensor platform," 14th IEEE Intelligent Transportation Systems Conference, pp. 1609-1615, Oct. 2011.

〔9〕 배출가스자기진단장치(OBD) 인증 안내문, http://www.nier.go.kr/eric/portal/tprc/nf/tprc-nf-01.page?boardId=TPRCNF01&bltnNo=1285570000146&command=READ

〔10〕 OBD-II PIDs, http://en.wikipedia.org/wiki/OBD-II_PIDs

〔11〕 R. Kohavi, "A study of cross-validation and bootstrap for accuracy estimation and model selection," In Proceedings of the Fourteenth International Joint Conference on Artificial Intelligence, vol. 14, no. 2, pp. 1137 - 1143, Aug. 1995.

〔12〕 A.P. Bradley. "The use of the area under the ROC curve in the evaluation of machine learning algorithms," Pattern Recognition., vol. 30, no. 7, pp. 1145 - 1159, Jul. 1997.

〔13〕 C. Pardilla, "Top 10 Ways to Steal a Car (and how to defend against them)," Edmunds.com, Jul. 2004.

〈저자소개〉

정 종 명 (Jong-myoung Jeong) 학생회원
2012년 2월: 서울시립대학교 전자전기 컴퓨터 공학부 학사
2012년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 In-Vehicle Security, Fuzzing, 임베디드 펌웨어 분석

강 형 철 (HyungChul Kang) 학생회원
2010년 2월: 고려대학교 산업시스템정보공학과 학사
2010년 3월~현재: 고려대학교 정보보호대학원 석박사통합과정
〈관심분야〉 블록 암호와 해쉬 함수 설계 및 분석

조 효 진 (Hyo Jin Jo) 학생회원
2009년 2월: 고려대학교 산업시스템 정보공학과 학사
2009년 3월~현재: 고려대학교 정보보호대학원 석·박사 통합과정
〈관심분야〉 VANET, In-vehicle Security, Secure Roaming

윤 지 원 (Ji Won Yoon) 정회원
2003년 2월: 성균관대학교 정보공학사 졸업
2005년 2월: University of Edinburgh, 정보학과 석사 졸업
2008년 11월: University of Cambridge 전자공학과 박사 졸업
2008년 2월~2009년 5월: University of Oxford, 로봇연구소 박사후과정
2009년 5월~2011년 5월: University of Dublin 통계학과 연구원 및 강사
2011년 7월~2012년 8월: IBM 연구소 정규 연구원
2012년 9월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 신호정보처리, 응용통계, 빅데이타 분석 기술, 도감청 탐지기술

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학사 졸업
1987년 12월: Oklahoma University 전산학과 석사 졸업
1992년 5월: Oklahoma University 전산학과 박사 졸업
1993년 3월~1997년 2월: 고려대학교 전산학과 조교수
1997년 3월~2001년 2월: 고려대학교 전산학과 부교수
2001년 3월~현재: 교려대학교 정보보호대학원 교수
〈관심분야〉 암호프로토콜, 암호이론, USN이론, 키 교환, 익명성 연구, PET기술