WI-FI FINGERPRINT-BASED APPROACH TO SECURING THE CONNECTED VEHICLE AGAINST WIRELESS ATTACK

Hyeokchan Kwon, Sokjoon Lee and Byung-ho Chung

Electronics and Telecommunications Research Institute,
218 Gajeong-ro, Yoseong-gu, Daejeon, Republic of KOREA
{hckwon, junny, cbh}@etri.re.kr

ABSTRACT

In this paper, we present wifi fingerprint-based approach to securing the connected vehicle against wireless attack. In current connected vehicles such as Tesla EV, Mitsubishi outlander PHEV etc., there is a wi-fi access point on the vehicle to connect to the mobile device which has telematics apps installed. And generally the wi-fi access point is managed by the head unit system in the vehicle. Currently, the headunit in the vehicle utilizes white-list that contain MAC addresses of the pre-registered (i.e authorized) device. However, the white-list based mechanism cannot detect the device that forges its MAC address with authorized one. This paper presents security mechanism to detect rogue telematics device that has a spoofed (i.e, forged) MAC by analysing wi-fi fingerprint. We generate wi-fi fingerprint by analysing radio frequency features such as error vector magnitude (EVM), frequency offset, I/Q offset, sync correlation and so on. And we also utilizing distance information for improving detection ratio. The prototype of the proposed mechanism is implemented in this work, and we provide experimental results.

KEYWORDS

Connected Vehicle Security, Wireless Attack, Wi-Fi Fingerprint, Telematics Device Authentication

1. INTRODUCTION

Recently, various telematics apps for diagnostic the car, setting the configuration, locating the car, locking it remotely etc. are exist and they use wireless network such as wi-fi, Bluetooth etc. to connect to the vehicle. In current connected vehicles such as Tesla EV, Mitsubishi outlander PHEV etc., there is a wi-fi access point on the vehicle to connect to the mobile device which has telematics apps installed. And generally the wi-fi access point is managed by the head unit system in the vehicle.

In recent years, some hacking accidents have occurred with connected vehicles providing wi-fi access. For example, in this year, Mitsubishi outlander PHEV was hacked [1] by cracking wi-fi PSK (Pre-shared key) and analysing binary protocol using MITM (Man in the middle attack). In this case, the hackers were able to disable the theft alarm, unlock the car, turn the light, pop the window/jimmy, turns on pre-heating, pre-cooling and so on. For another example, the Tesla EV was also hacked [2] by using malicious wi-fi hotspot which is connected to a car's web browser. In this case, the hackers were able to remotely unlock the door, take over control of the dashboard

Natarajan Meghanathan et al. (Eds) : NETCOM, NCS, WiMoNe, GRAPH-HOC, SPM, CSEIT - 2016
pp. 211– 217, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.61518

computer screen, open the door, move the seats and activate the indicators and windscreen wipers, as well as fold in the wing mirrors while the vehicle was in motion. And they were also able to take remote control of Tesla's brakes and door locks from 12 miles away.

In this paper, we present wi-fi fingerprint-based approach to securing the connected vehicle against wireless attack. Currently, with regard to wi-fi access, the head unit check MAC address of the device in order to determine whether the device is authorized or not. To do this, head unit use white-list which consists of MAC addresses of the pre-registered device. However, the white-list based mechanism cannot detect the device that forges its MAC address with authorized one. This paper presents security mechanism to detect rogue device that has a spoofed (i.e, forged) MAC by analysing wi-fi fingerprint. We generate wi-fi fingerprint by analysing radio frequency features such as error vector magnitude (EVM), frequency offset, I/Q offset, sync correlation and so on. And we also utilizing distance information for improving detection ratio. The prototype of the proposed mechanism with considering EVM as a radio frequency feature is implemented in this work, and we provide experimental results. So far, security research regard to security vulnerability/threat on connected vehicle has not been conducted.

The rest of the paper is organized as follows. The wi-fi fingerprint-based telematics device authentication mechanism and experiment result is described in section 2. Finally, conclusion is given in section 3.

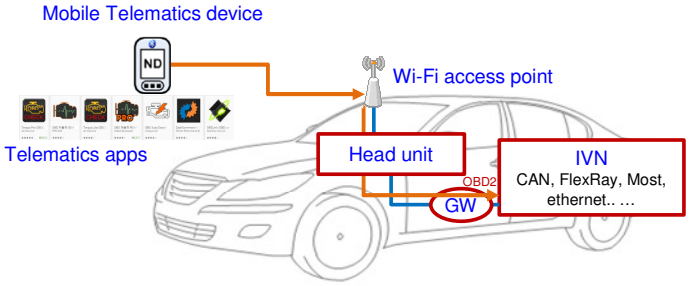

Figure 1. Wi-fi based connected vehicle

2. WI-FI FINGERPRINT-BASED TELEMATICS DEVICE AUTHENTICATION MECHANISM FOR CONNECTED VEHICLE

In order to authenticate telematics device, we utilizes the radio frequency features and distance information (i.e. RSSI). In the wi-fi fingerprint generation phase, the wi-fi access point on the vehicle collects and analysis wi-fi signals of the device by moving the physical location of the device and generates wi-fi fingerprint. In the verification phase, it estimates the distance from device to vehicle by using RSSI value, and it analyses wi-fi fingerprint data with the best nearby radio frequency features in current relative distance with the vehicle. Figure 2 shows the overall architecture of this mechanism.

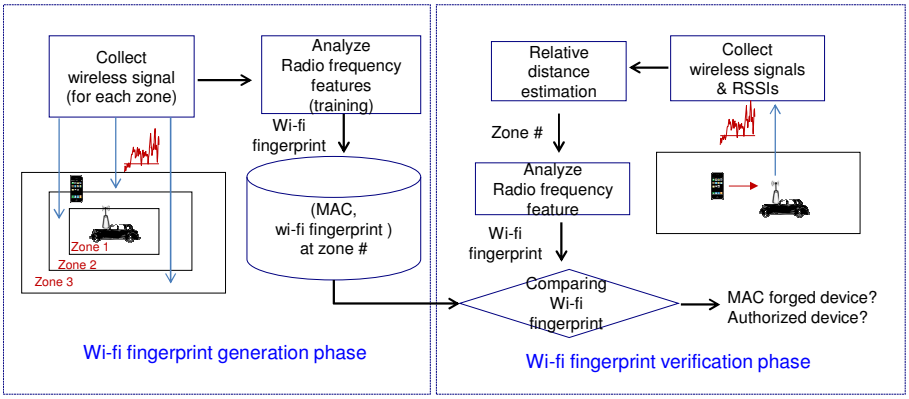

Figure 2. Overall process of wi-fi fingerprint–based MAC verification for telematics device

2.1. Wi-fi fingerprint generation mechanism

In the Wi-fi fingerprint generation phase, the head unit registers MAC address of the authorized device. And it determines a wireless signal collection zone, and moves wireless device to the measurement point and generates wireless wi-fi signals. The head unit collects wi-fi signals from the authorized device, and then analyse them by machine learning algorithm such as K-NN, SVM and so on, and creates wi-fi fingerprint of the authorized device. In this paper, we use K-NNDD (K-Nearest Neighbour Data Description) [5] for training radio frequency of authorized devices. The relative distance and RF fingerprint information is stored in wi-fi fingerprint database.

In this paper, we applied error vector magnitude (EVM) as a RF feature. EVM is a vector magnitude difference between an ideal reference signal and measured signal. Figure 3 shows the concept of error vector magnitude (EVM) and mathematical formula for deriving EVM value.

$$EVM = \sqrt{{Err_I}^2 + {Err_Q}^2} \quad \text{, where} \begin{cases} Err_I = I_{reference} \cdot I_{measured} \\ Err_Q = Q_{reference} \cdot Q_{measured} \end{cases} \quad \text{, (formula 1)}$$

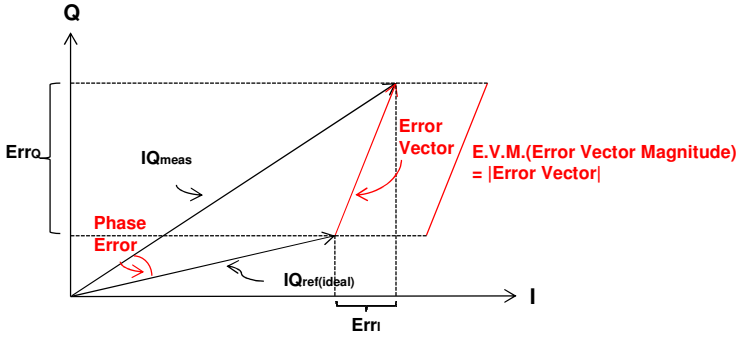

Figure 3. The concept of the Error Vector Magnitude

EVM is calculated by comparing the difference between measured signals with an ideal reference signals for determining the error vector. The EVM value is the root mean square value of the error vector over time at the instants of the symbol clock transitions. There are various reasons of mismatching measured signal with reference ideal signal such as hardware impairment, channel characteristics, noise at the receiver and modulation error. By using modulation error, we can

identify particular wireless devices with different manufacturer or different wifi-chipset or even the same manufacturer/wifi-chipset.

2.2. Wi-fi fingerprint verification mechanism

In the Wi-fi fingerprint verification phase, the head unit collect and analyse RF signals of the device and extracts MAC address, RSSI and radio frequency features. And then it estimates the relative distance from the device to the vehicle by analysing the RSSI value. To calculate distance from RSSI values we used the following formula:

$$RSSI = -12.5Ln(d) - 36.25$$

The correction factors are derived through iterative experiments by minimizing the difference from the value by distance estimation algorithm with real distance. The notation d in this formula is a distance. The head unit then selects the radio frequency features having the highest P(radio frequency features | d) of the MAC of the device. P(radio frequency features | d) means a probability of radio frequency features in a given zone. Then it creates radio frequency signature from the radio frequency features by using machine learning algorithm. Then it determines whether the device having cloned MAC by comparing the wi-fi signature of the device with the device having same MAC in the database. In this paper, we use K-NN(K-Nearest Neighbor) algorithm for comparing measured radio frequency signature with reference radio frequency signature.

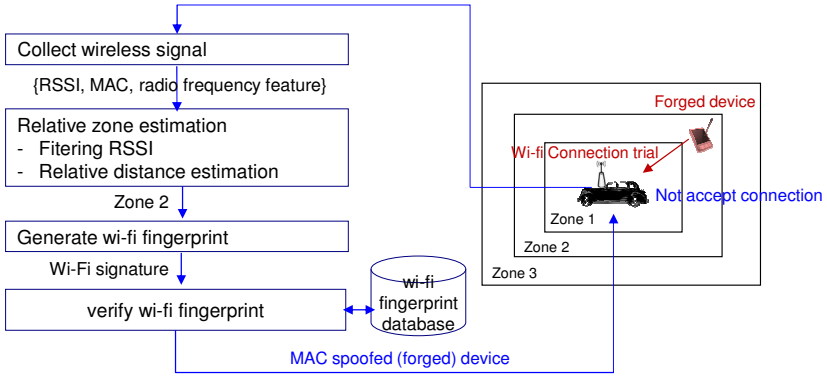

Figure 4. Detection process of rogue device

2.3. Experiments result

We developed hardware platform to collect wi-fi radio frequency signal and extract wireless features. Figure 5 shows the developed HW platform which can be installed to the head unit in the connected vehicle. This hardware platform includes Atheros 9380 WLAN chipset for monitoring wi-fi signals. We developed test platform with related user interface and dashboard, and we developed also wireless attack tool for evaluating developed system. Figure 6 shows the screenshots of our attacking tool to create cloned MAC. Figure 7 shows the UI of test platform for MAC spoofing device through wi-fi signature analysis and verification. Table 1 shows the experiment result.

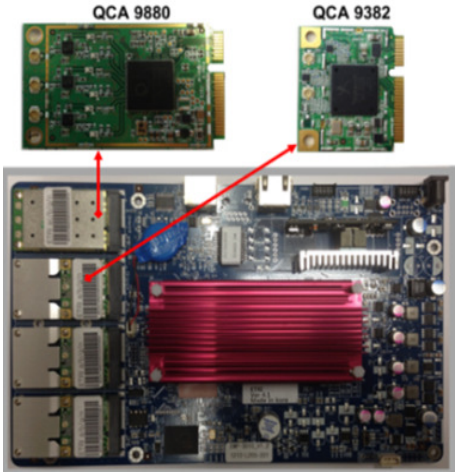

Figure 5. Prototype hardware platform which supporting wireless radio frequency feature extraction

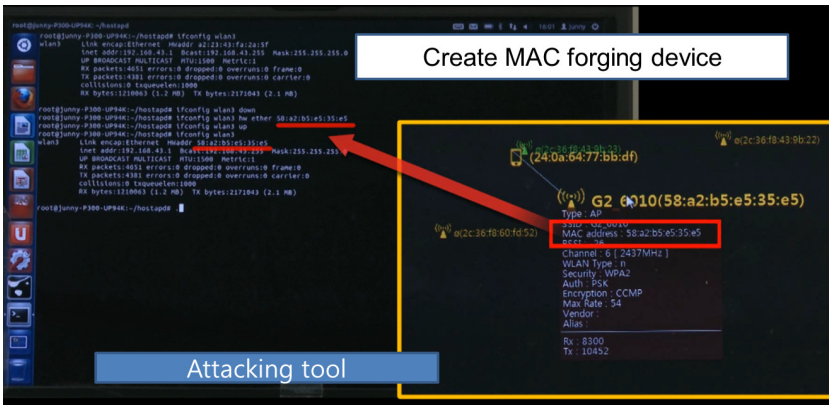

Figure 6. Snapshot of the attack tool, it shows the creation of MAC forging device

Figure 7. Snapshot of the test platform, it shows the MAC verification process in GUI

Table 1. Experiment result (FAR: False Accept Rate, FRR: False Reject Rate, EER: Equal Error Rate)

Test device	threshold	FAR	FRR	EER
Mobile device with different chipset (smart phone w/ Broadcom chipset, laptop computer w/ intel chipset, laptop computer w/ atheros chipset)	0.91	2.7%	0%	0.8%
Mobile device with same wi-fi chipset (iphone4s smart phone w/ broadcom's BCM 4330, iphone4 smart phone w/ broadcom's BCM 4329)	0.86	10.04%	0%	5.34%

3. CONCLUSIONS

In this paper, we present wifi fingerprint-based approach to securing the connected vehicle against wireless attack.

This paper provide the security mechanism to detect rogue device that has a spoofed (i.e, forged) MAC by analysing wi-fi fingerprint. We generate wi-fi fingerprint by analysing radio frequency features such as error vector magnitude (EVM). And we also utilizing distance information for improving detection ratio. The distance information is derived by RSSI value which in included in wi-fi signal. The prototype of the proposed mechanism with considering EVM as a radio frequency feature is implemented and we provide experimental results. The proposed mechanism analyse a characteristics of the wi-fi radio frequency signal of the device for detecting MAC spoofing device. We also developed wireless attacking tool and test platform with GUI.

In our experiments, the FAR is 2.7% in case that test mobile device has different chipsets and 10.4% in case that test mobile device has same chipsets. The detection rate should be improved when rogue device with a same manufacturers and wi-fi chipset with authorized one. Currently, we are designing the algorithm consider additional wi-fi radio frequency features such as IQ offset, sync correlation and so on.

ACKNOWLEDGEMENTS

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.R-20160226-002842, Development of V2X Service Integrated Security Technology for Autonomous Driving Vehicle)

REFERENCES

[1] Hacking the Mitsubishi Outlander PHEV hybrid, https://www.pentestpartners.com/blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/, Pen test partners, 2016

[2] Hackers take Remote Control of Tesla's Brakes and Door locks from 12 Miles Away, http://thehackernews.com/2016/09/hack-tesla-autopilot.html, The Hacker News, 2016

[3] Hao, Peng, "Wireless Device Authentication Techniques Using Physical-Layer Device Fingerprint" (2015). Electronic Thesis and Dissertation Repository. Paper 3440. Western university, http://ir.lib.uwo.ca/etd/3440

[4] H. Kwon, G.An, S.H.Kim and B.H.Chung, "Detecting cloned devices in wireless network using RSSI and RF Features", ICONI, Dec., 2014

[5] J. Son and S. Kim, "kNNDD-based One-Class Classification by Nonparametric Density Estimation," Journal of the Korean Institute of Industrial Engineers, Vol. 38, No. 3, pp. 191-197, Sep. 2012.

[6] JP Hubaux, S Capkun, J Luo, The security and privacy of smart vehicles, IEEE Security & Privacy Magazine, 2004

[7] AirTight Patent, Method and system for monitoring a selected region of an airspace associated with local area networks of computing devices, Patent# US 7,002,943 Feb, 2006

[8] Y. Shi and Michael A. Jensen, Improved Radiometric Identification of Wireless Devices Using MIMO Transmission, IEEE Transactions on Information Forensics and Security, Dec. 2011

[9] R. Beyah and A. Venkataramen, Rogue-Access-Point Detection - Challenges, Solutions, and Future Directions, IEEE Security & Privacy, vol.9, issue 5, pp.56-61 (2011)

[10] Agilent 8 Hints for Making and Interpreting EVM Measurements, Agilent Technologies, 2005

AUTHORS

Hyeokchan Kwon

Received PhD degree in computer science from Chungnam National University in 2001. Since 2001, he is currently a principal researcher in electronics and telecommunications research institute (ETRI) in Korea. His research interests include automotive security, wireless intrusion prevention system and IoT security, etc.

Sokjoon Lee

Received MS degree in computer engineering from Seoul National University in 2000. Since 2000, he is currently a principal researcher in electronics and telecommunications research institute (ETRI) in Korea. His research interests include cryptographic protocol and ICT-Physical convergence security such as medical security, automotive security, etc.

Byung-ho Chung

Received PhD degree in computer science from Chungnam National University in 2004. He joined Agency for Defense Development (ADD) in 1988 where he was a senior researcher for 12 years. Since 2000, he is currently a principal researcher in electronics and telecommunications research institute (ETRI) in Korea. His research interests include automotive security, medical security, wireless security, multimedia security, etc.