WIRELESS DEVICE AUTHENTICATION MECHANISM FOR SECURE CONNECTIVITY SERVICE OF SMART CAR

[1]HYEOKCHAN KWON, [2]SOKJOON LEE, [3]JUNGYONG CHOI, [4]BYUNG-HO CHUNG

Electronics and Telecommunications Research Institute
E-mail: {hckwon, junny, choijy725, cbh}@etri.re.kr

Abstract – In this paper, we propose a technology to prevent unauthorized wireless access by identifying and authenticating an attack device based on device fingerprint for smart car. This mechanism detects the attack device with forged MAC address of the normal device. To generate device fingerprint, it extracts and analyzes unique characteristics from wireless signals of the device. Such a characteristics of the signal include error vector magnitude, frequency offset, IQ offset, sync correlation and so on.The physical distance information between device and smart car is also considered to generate device fingerprint to improve detection accuracy.

Index Terms - Device fingerprint, malicious device detection, smart car security, wireless device authentication,

I. INTRODUCTION

Reports of hacking cases and vulnerabilities of smart cars are continuously reported. Especially, as the telematics service through wireless connection of the user terminal is activated, the number of cases of smart car attack by hacking of the wireless communication has been increased.

Here are two examples of wireless hacking reported in 2016[1,2]: First, in the case of a Mitsubishi outlander PHEV vehicle, an attacker hacks a pre-shared key for Wi-Fi communication, attempts to access a wireless AP of the vehicle, collects a packet through a man in the middle attack and then finds control command by reverse engineering [1].

In the case of the Tesla electric car, an attacker installed a malicious Wi-Fi hotspot to induce access to the vehicle's web browser and then attempted to hack it. This attack allowed remote control of the vehicle's doors, wipers, dashboard screens, etc., as well as the ability to remotely control the brakes of vehicles that were traveling 12 miles away. Thus, the wireless connection of the attacker terminal with the vehicle can be regarded as the first step of a hacking attack.

In this paper, we propose a mechanism to detect and block illegal access to vehicle's AP based on device fingerprint. For accessing the WiFi AP of the current user device, the head-unit determines the access permission by checking the MAC address of the device. To do this, the head-unit stores and manages MAC addresses of the pre-registered authorized devices in a white-list form. However, this method has a problem that an attacker cannot detect if the MAC address of the device is forged with the MAC address of the allowed device. In this paper, we propose a device fingerprint-based mechanism to detect MAC-forged devices.

II. SECURE WIRELESS DEVICE AUTHENTICATION MECHANISM FOR SMART CAR

To generate device fingerprint, it extracts and analyzes unique characteristics from wireless signals of the device. Such a characteristics of the wireless signal include error vector magnitude, frequency offset, IQ offset, sync correlation and so on. In this paper, physical distance information between device and vehicle is also considered to generate device fingerprint to improve detection accuracy. Figure 1 shows the structure of a vehicle that provides Wi-Fi-based smart car services.

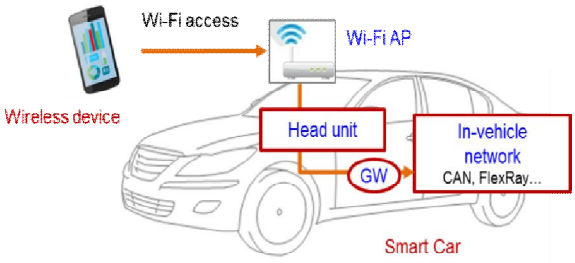
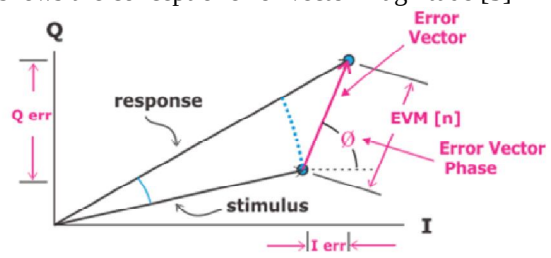


Fig.1. Smart car with wi-fi access point

Figure 2 shows detection process of malicious device with forged MAC address. It consists of two steps. The first step is device fingerprinting generation phase. At this phase, the head-unit of the smart car collects wireless signals of normal device, extracts unique characteristics, and generates device fingerprint. The MAC address and the device fingerprint are stored in the fingerprint database. We use the learning algorithm as K-Nearest Neighbor Data Description to create device fingerprint.

In this paper, we use error vector magnitude value as a unique characteristics from wireless signals of the device. The error vector magnitude (EVM) is the mean square root of the error vector over time at the instant of symbol clock transition. Even in a device of the same manufacturer and a device equipped with the

same modem chipset, there is a fine difference in characteristic of signal between each device. The reasons for this difference are minor damage to the hardware, channel characteristics, noise at the receiver, and modulation errors. This fine difference is used in learning and generating device fingerprint. The figure 2 shows the concept of error vector magnitude [3]



$$\Delta EVM\ (\%) = \sqrt{\frac{1}{N}\sum_{n=0}^{N-1} Ierr[n]^2 + Qerr[n]^2} \times 100\%$$

where: n = symbol index
N = number of symbols
Ierr = I resp - I stim
Qerr = Q resp - Q stim

Fig.2.Error vector magnitude

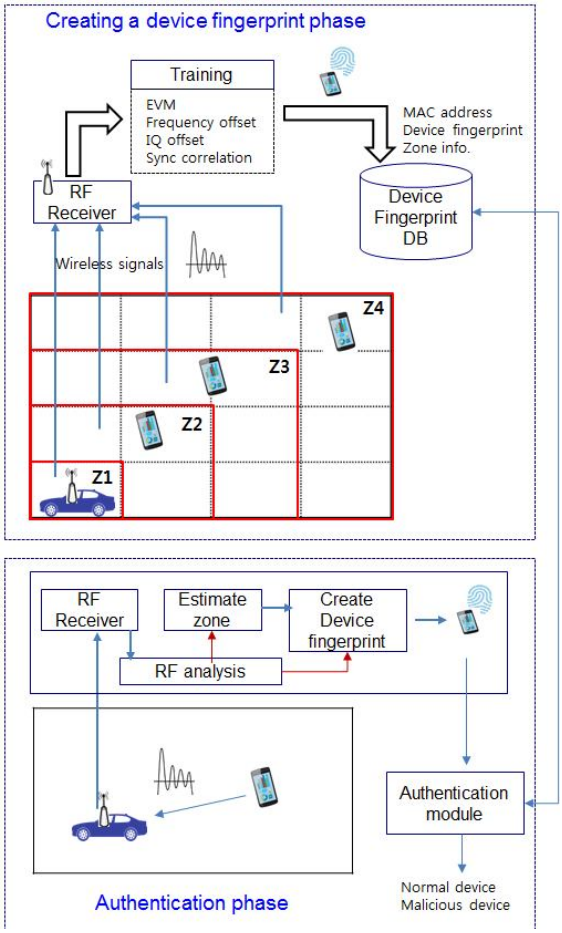


Fig.3.The process of access control of the wireless device

The second step is the Wi-Fi fingerprint verification phase. If there is a device attempting to access the AP in the smart car, the wireless signal of the device is extracted and analyzed to create a device fingerprint. It also predicts the relative physical distance (area) based on the wireless signal RSSI. Then, the device fingerprint corresponding to the MAC address and the area of the wireless fingerprint database is fetched and compared with the fingerprint extracted from the device to determine whether the MAC address is forged or not. In this work, we designed and developed hardware platform prototype for Wi-Fi signal analysis and fingerprint generation. In future, it will be possible to use it in the AP module of the head unit of the vehicle. Figure 4 shows the hardware platform.

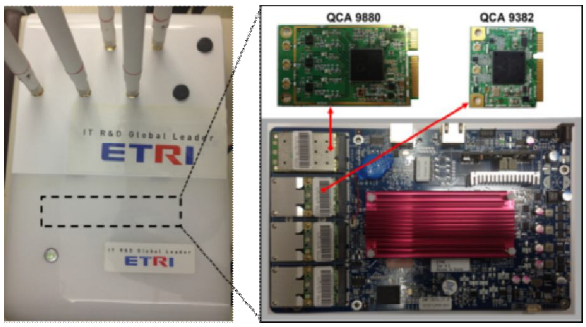


Fig.4. Wi-Fi AP Hardware platform with device fingerprint generation module

The experiment was conducted with the iPhone4S and the threshold was set at 0.9. Experimental results show that detection rate is over 97% when device using different Wi-Fi chipsets with forged MAC address, and detection rate is 85% when devices of same model, same Wi-Fi chipset with forged MAC addresses.

CONCLUSION

Through this research, it is possible to secure and safe smart car service against wireless hacking. Currently, only error vector magnitude is considered among the characteristics of wireless signal, and further study is needed to increase detection accuracy by applying additional parameters. In addition to Wi-Fi, there is a need for hacking countermeasures against various wireless protocols for vehicle access such as Bluetooth.

ACKNOWLEDGMENTS

This work was supported by Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. B0717-16-0097, Development of V2X Service Integrated Security Technology for Autonomous Driving Vehicle)

REFERENCES

[1] Pen test partners, Hacking the Mitsubishi Outlander PHEV hybrid, 2016
[2] Hackers take Remote Control of Tesla's Brakes and Door locks from 12 Miles Away, The Hacker News, 2016
[3] Keysight, Error Vector Magnitude, 2017

[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] Timo van Roermund(NXP), Securing the In-Vehicle Network-Trends, challenges, and solutions, 14th escar Europe, Munich, Nov. 17, 2016

[6] Cyber Security and Resilience of smart cars Good practices and recommendations, ENISA, Dec. 2016

★★★