Available online at http://www.ssstj.sci.ssru.ac.th

Suan Sunandha Science and Technology Journal

Guidelines for Vehicle Robbery Prevention using Remote Blocking Signals

Narong Sangwaranatee[1*], Teerat Klangkanasub[2], Narong Kulnides[2]

[1]Department of Applied Physics, Faculty of Science and Technology, Suan Sunandha Rajabhat University,
[2]Department of Forensic Science, Faculty of Science and Technology, Suan Sunandha Rajabhat University,
U-thong Nok Road, Dusit, Bangkok 10300, Thailand
Corresponding author E-mail: *Narong.sa@ssru.ac.th

Received / Accepted

Abstract: In this paper, the radio signal remote sensing device was used to control the vehicle door switching control, which was the field trials experiment. The switching "On" and "Off" of the switching signals were used to control the vehicle door and investigated. In application, the blocking signal from the commit the remote vehicle crime in the venerable place can be protected. The results obtained have shown that the signal blocking by using another remote control over 5 meters, 10 meters and 15 meters could be achieved. The proposed models and tested results have shown that the Vehicle Brand A Model No. 1 could be blocked by 83.33 percent, while Brand A Model No.2 by 83.33 percent, Brand B Model No.1 by 40 percent, Brand B Model No.2 by 60 percent, Brand C Model No. 1 by 83.33 percent, Brand C Model No. 2 by 83.33 percent, meanwhile, the remote control for general vehicle are used radio waves with frequency 315 and 433 MHz, where the criminal will use the interference signals to form the blocking (jamming) signals, the vehicle can be robbed.

Keywords: Vehicle robbery prevention, remote sensing, Remote control, Radio signal transmission.

1. Introduction

Security is one of the most factors that is needed in all societies, where the crimes can be prevented and the societies secure. One of the items that are required to prevent and be secure is the vehicle (car), which is actually parked within the parking places. The vehicle robbery has been the important problem of world society, which is required the key issue to solve and manage, which are many concern techniques reported, for instance, closed circuit television (CCTV) (Wilson., 2005), security person and service, global positioning system (GPS) and general packet radio service (GPRS) (Satyanarayana et al., 2013) tracking systems and Ad hoc networks [Zhou et al., 1999], etc. Although, there are many techniques available today, the committed crime of cars is still increased, especially, in the parking place that assumes to be the best secure place. Thus, the searching of the reliable techniques that can be applied efficiently and cost effectively is needed. In this work, we have proposed and investigated the simple technique that can be used for vehicle robbery prevention by the remote blocking signal, where the other radio signals from the different sources can be blocked and not access the active vehicle remote control, therefore, the committed crime cannot be done. The operation system was formed and tested by a simple arrangement, where the field trials and tests were investigated and data recorded, from which the results obtained have shown that such a proposed system can be used to prevent the vehicle commit crime, especially, in the certain area, for example, within the 15 meter range in the parking area, in which the interference signals can be blocked and the vehicle secure. Where more details are given in the following sections.

2. Operating System

In the case of blocking signals is applied to commit the crime, where the criminals often aim for spacious parking lots in the public places, for example, department stores and public streets, where they are not very common car access functions, which are the immobilizer and the remote keyless entry system. For more advanced systems passive entry and passive start, functions are implemented that allow unlocking or starting of the car by simply getting close to it. Figure 1 shows the remote blocking signal prevention system using the radio

Suan Sunandha Science and Technology Journal

frequency (RF) signal transmission basis. The TI RFID (radio frequency identification and detection) automotive products offer market unique features and performance. All car side products are optimized for full integration into the Central Body Control Module (BCM). The Immobilizer LF (low pass filter) antenna could be easily connected to the LF base station with a flexible cable length up to 13 feet (4m). The cable length could be varied without changing the adaptation to the base station. The integration of the base station reduces system component count and space requirements.

The Controller Entry Device manages the Immobilizer communication and pushes button interaction. During sleep state the devices enters a special low power mode with only 60nA current consumption. By pressing a push button the device wakes up and controls an external UHF (ultra-high frequency) transmitter or transceiver. Security keys and rolling codes could be stored in the integrated EEPROM memory. This memory is accessible over the LF interface without support from the battery in the key fob. The Controller Entry Device offers a special battery charge mode; to achieve faster charging it's recommended to add a charging amplifier device on the base station side. The external resonant circuit with an LF coil and a resonant capacitor could be trimmed to the correct resonant frequency with the integrated trimming capability achieving an easy way to eliminate part tolerances.

The pin-to-pin and software compatible devices are available offering an easy way of scalability from standard one-way communication to high-end bi-directional communication. The UHF device family comes with an easy to use SPI interface where all parameters of a UHF link could be configured. All building blocks of a UHF system are integrated into the devices requiring only one external oscillator, a matching network and the UHF antenna itself. The receiver and transceiver come with an integrated polling mode (wake on radio).

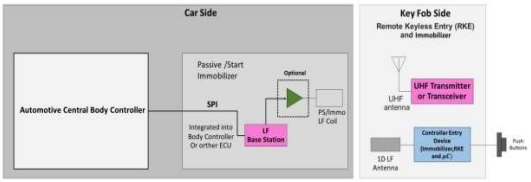

Figure 1. Schematic diagram of a remote blocking system prevention

The power supply is connected to the 12V or 24V board net and regulates down/up to voltages for DSP(digital signal processing), µC, memory and ICs (integrated circuits) and functions DVD drive, communication interfaces, display biasing and backlighting. The need for many different power rails makes the design of the power supply a critical task when trying to design for size, cost, and efficiency. Linear regulators with low quiescent current help reduce battery leakage current during standby operating modes (ignition off), are load dump voltage tolerant for directly battery connected devices, and need low drop out and tracking for low battery crank operation. Beyond providing increased conversion efficiencies, switching power supplies provide EMI (electromagnetic immune) improvement with slew rate control of the switching FET(field effect transistor), Frequency hopping, spread spectrum or triangulation method for attenuation of peak spectral energy, Low current (Iq), soft start for power sequencing and inrush current limitation, Phased switching for multiple SMPS's regulators to minimize input ripple current and lower input capacitance, higher switching frequency for smaller components (L and C's), and SVS functions for brown out indications.

The allowed data exchange between independent electronic modules in the car as well as the remote sub-modules of the BCM and RFID system. High-Speed CAN (up to 1Mbps, ISO 119898) is a two wire, fault tolerant differential bus. With a wide input common mode range and differential signal technology, it serves as the main vehicle bus type for connecting the various electronic modules in the car with each other. LIN supports low speed (up to 20 kbps) single bus wire networks, primarily used to communicate with remote sub-functions of the BCM system.

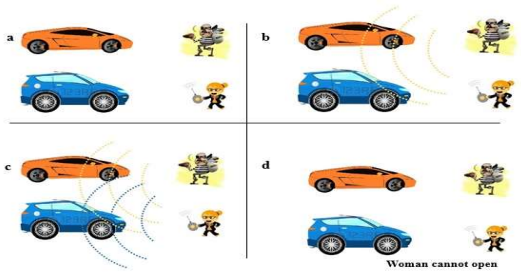

Figure 2. The blocking signals that use to commit the remote vehicle crimes

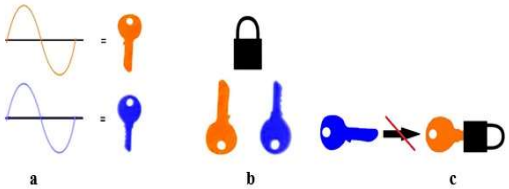

Figure 3. The blocking signal details

Suan Sunandha Science and Technology Journal

Figure 2, firstly, the criminal stands by and waits for the victim to bring a car to parking radius that can be blocked by the remote signal (Figure 2a). The criminal presses the remote control to send a signal to the car before the victim presses the remote control to lock the car (Figure 2b). The second signal is jammed (interfered) (Figure 2c).The victim cannot open and close the doors herself (Figure 1d). When the victim is leaving the car, she presses the remote control to lock the car, which can be seen that the two signals of the car are now jamming. So, the victim is not able to both lock and unlock the car. The first signal was already jamming as shown in (Figure 2d). Even though remote virtual keys are in the same size, the size of each tooth is different (Figure 3a).The car is like a lock, so both keys can be plugged into a lock. But there is only one key that can be unlocked (Figure 3 b) as a key inserted into a compatible across key (Figure 3c). From Jamming Remote, we will explain this principle simply by metaphor with key and lock; the key with the tooth as a signal, the key without tooth as a wiretapping signal and the lock as a car. Firstly access, the criminal has inserted the key, without the tooth, in the lock. So the victim cannot use his key. In this process we cannot see in our owned eyes because it is a wave, in the same way, the toothless key from criminal are not proper for the lock because it is not a type of key which can be unlocked. We will be unlocked when we using the right one, key with a tooth. But we cannot do like that causes the other key are already inserted in the keyhole. (Figure 3c).From testing by using the sample car, we try to press the lock button on the remote control which is not matching with this car and holds this button in different area 5, 10, and 15 meters for a tapping remote control signal, from which the experiment was observed and data recorded, from which the testing distance used is as shown in Figure 4.

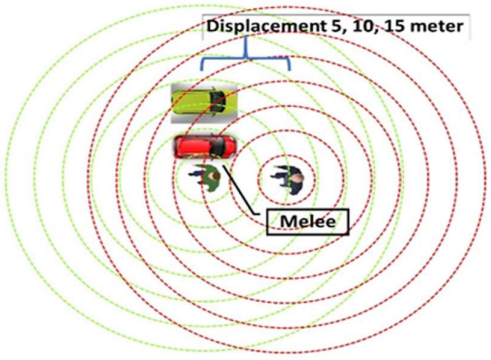

Figure 4. The remote blocking and tapping signals from the vehicles over 5 m 10 m and 15 m.

3. Experiments and Results

From experimental results, as shown in Table 1, in order to detect the blocking signals with a wiretap from remote vehicles over 5 meters, 10 meters, and 15 meters, it was found that the experiment Brand A Model 1 can be blocked 83.33 percent, where Brand A Model 2 can be blocked 83.33 percent. Brand B Model 1 can be blocked by 50 percent, where Brand B Model 2 can be blocked by 50 percent. Brand C Model 1 can be blocked by 83.33 percent, where Brand C Model 2 can be blocked by 83.33 percent. From assumption between car models and signal disturbance, their relationship was assign as follows. H0: Disturbance signal has effect to car model (Priority $\alpha = 0.05$), H1: Disturbance signal has not effect to car model (Priority $\alpha = 0.05$). In Table 2, the result shown Pearson Chi-Square = 6.0, df = 5, Sig = 0.306. This means car A Model 1 related to the remote controls. The disturbance signal> α (0.05) → sig, which reject the null hypothesisH1 (bolt parameters are related). In Table 3, the result shown Pearson Chi-Square = 6.0, df = 5, Sig = 0.306. This means car A Model 2 related to the remote controls. The disturbance signal >α (0.05) → sig, which reject the null hypothesis H1 (bolt parameters are related). In Table 4, the result shown Pearson Chi-Square = 6.0, df = 5, Sig = 0.306. This means car B Model 1 related to the remote controls. The disturbance signal >α (0.05) → sig, which reject the null hypothesisH1 (bolt parameters are related). In Table 5, the result shown Pearson Chi-Square = 6.0, df= 5, Sig = 0.306. This means car B Model 2 related to the remote controls. The disturbance signal >α (0.05) → sig, which reject the null hypothesisH1 (bolt parameters are related). In Table 6, the result shown Pearson Chi-Square = 6.0, df = 5, Sig = 0.306. This means car C Model 1 related to the remote controls. The disturbance signal >α (0.05) → sig, which reject the null hypothesisH1 (bolt parameters are related). In Table 7, the result shown Pearson Chi-Square = 6.0, df = 5, Sig = 0.306. This means car C Model 2 related to the remote controls. The disturbance signal >α (0.05) → sig, which reject the null hypothesisH1 (bolt parameters are related).

Table1. Shows the results of the interference of the remote control of the car Brand A, B, and C.

The remote control of cars for blocking signal		Brand A		Brand B		Brand C	
		A1	A2	B1	B2	C1	C2
Brand A	A1	✓	✓	×	×	✓	✓
	A2	✓	✓	×	×	✓	✓
Brand B	B1	✓	✓	✓	✓	✓	×
	B2	✓	✓	✓	✓	✓	✓
Brand C	C1	✓	✓	×	×	✓	✓
	C2	×	×	✓	✓	×	✓
Total		5	5	3	3	5	5

Table 2. Results of Chi–Square Tests car A model 1

	Value	df	Asymp.Sig (2 sided)
Pearson Chi-Square			
Likelihood Ratio			
Linear – by – Linear Association			
N of Valid Cases			

Table 3. Results of Chi–Square Tests car A model 2

Table 4. Results of Chi–Square Tests car B model 1

Table 5. Results of Chi–Square Tests car B model 2

Table 6. Results of Chi–Square Tests car C model 1

Table 7. Results of Chi–Square Tests car C model 2

4. Conclusion

We have reported the investigations of vehicle crime prevention using the remote blocking signal prevention. From the experiment of blocking signal of the remote control with radio wave tapping, the various different results were obtained. The vehicle remote control device used was obtained from the factory, with 315 and 433 MHz frequencies. The working process of each car was performed by the same situation. In which the signal from source was transmitted to the receiver attached in the car for lock / unlock program, which was found that that the signal was blocked by the jamming signals because the remote control signal on the same wavelength was interfered and cancelled. Moreover, the tapping signal of each remote control signal is different because the signal is not matched, in which the tapping signal is not working and caused the signals with different frequencies have different wavelengths and amplitudes.

References

Wilson, D. (2005). Behind the Cameras: Monitoring and Open-street CCTV Surveillance in Australia, *Security Journal*, Vol.18, 43-54, doi: 10.1057/palgrave.sj.8340190.

Satyanarayana, K., Sarma, A. D., Sravan, J., Malini, M., and Venkateswarlu, G. (2013). GPS and GPRS Based Telemonitoring System for EmergencyPatient Transportation, *Journal of Medical Engineering,* Vol.2013, 1-9, doi:10.1155/2013/363508

Zhou, L., Haas, Z. J. (1999). Securing Ad Hoc Networks, *IEEE Network,* Vol.13, 24-30, doi: 10.1109/65.806983.

Alchekh Yasin, S.Y., Yrfanean, A.R., Mosavi, M.R., Mohammadi, A. (2014). An effective approach for simulating the two-color infrared seekers, *Infrared Physics & Technology,* Vol.67,73–83,doi:10.1016/j.infrared.2014.05. 004.

Ishibashi, Y., Fukui, M, Mechanism of the jamming transition in the two- dimensional traffic networks, *Physica A: Statistical Mechanics and its Applications*, Vol.391,6060–6065,doi:10.1016/j.physa.2012.06.049.

Xiaoqi, L., Baohua, Z., Ying, Z., He, L. and Haiquan, P. The infrared and visible image fusion algorithm based on target separation and sparse representation, *Infrared Physics & Technology,*Vol.67,397-407, doi:10.1016/j.infrared.2014.09.007.

Olmos, P. M., and Murillo-Fuentes, J. J. (2012). Remote Detection of a Frequency Jammer Operating in the Down Link of a Cellular System, *Wireless Pers Commun*, Vol 63, 861–870, doi:10.1007/s11277-010-0171-9