A low-cost authentication technology of car key based SIMO-VLC

Fan Yang\textsuperscript{1,2}, Kui Jiang\textsuperscript{1}

\textsuperscript{1} School of information and Communication engineering, University of electronic science and technology of China, Chengdu, Sichuan, 610022, China

\textsuperscript{2} School of Physics and Electronic Information, Inner Mongolia Normal University, Hohhot, Inner Mongolia, 010022, China

*nmgyangfan@qq.com

Abstract. With the wide application of software radio technology platform, the traditional authentication technology of car key based on radio is no longer reliable. In this paper, a low-cost SIMO-VLC (single input multiple output visible light communication) system is designed to meet the needs of automobile key authentication, which effectively improves the authentication safety performance of automobiles. Furthermore, the hardware platform of the SIMO-VLC system was presented. Finally, we finished the actual test of bit error rate for scenarios with different colours and different distances in the experiment. The experimental results demonstrate that this technology has better communication reliability in the range of 5-180cm with blue light source.

1. Introduction

With the rise of new energy vehicles, the safety certification technology of car door locks has also been greatly developed. The safety performance of the car door lock represents the most basic safety requirements of the car. Without a good security authentication system of the car door lock, the safety of the car’s belongings and passengers cannot be guaranteed. At present, there are mainly three technologies of car key.

(1) Ordinary wireless car keys based on open spectrum is the most commonly used keys on the market by using of 315MHz and 433MHz frequency. It is based on the rolling code for authentication method that has poor security performance, because the car door would be unlocked as long as it was monitored for a certain period of time by using the software radio platform. However, the advantage of this method is that the communication distance is longer and more convenience, and it is generally over 10m.

(2) Bluetooth based on mobile phones is another technology which is widely used in Tesla cars \cite{1}. Compared with technology (1), Bluetooth technology, has a larger communication bandwidth and can realize encryption algorithm, but the disadvantage of this is that the communication distance is relatively small. Similarly, there is a risk of being monitored since the physical layer is radio.

(3) RFID (radio frequency identification devices) is also a kind of technology of car key. \cite{2}. This technology is also being used in Tesla cars, compared with the first two technologies, because the bandwidth of RFID technology is low, its communication distance is so close that it almost needs to put the key on the car to complete the owner authentication. The convenience is poor, but there is no risk of eavesdropping at the physical level.
Based on the three mainstream automobile certification technologies mentioned above, there are trade-offs between communication distance and safety. In this paper, a low-cost automobile authentication technology based on SIMO-VLC is proposed, which utilizes the high directivity of visible light to not only prevent the risk of physical layer being monitored, but also improve the bandwidth of authentication communication by utilizing the abundant spectrum resources of visible light. At the same time, the communication distance can meet the general requirements of automobile certification and finally it has a good robustness under different angles of irradiation measured by experiment.

2. System model

Visible light communication technology is a technology that realize information transmission through modulation and encryption of visible light [3]. The resources of visible spectrum are abundant and the wavelength range of visible light is about from 380nm to 780nm [4]. According to the relationship between wavelength and frequency $\lambda=v/f$. Suppose the lower limit frequency of visible light is $f_1$, and the upper limit frequency is $f_2$, so, $f_1=v/\lambda_1=4\times10^{14}$Hz, $f_2=v/\lambda_2=8\times10^{14}$Hz. The frequency band width of visible light is about 400THz, so the spectrum resources of visible light are very abundant. In addition, it is very difficult to keep being sniffed at the physical layer without affecting the communication because of the high directivity of light [5]. Therefore, VLC technology has great potential in communication bandwidth and security [6, 7], which is suitable for the application of automobile key authentication. As shown in Figure 1, the receivers were placed at the front, back and two sides of the car, and people hold the transmitter to send a beam of light to unlock the car.

![Figure 1. Schematic diagram of system operation](image1)

From Figure 2, we used a low-cost Arduino to encrypt the key, modulated it through Manchester and sent the signal in the form of visible light, after passing through the Gaussian channel, the visible light signal is converted into an electrical signal by photodiode, and then it passes through the automatic gain controller and it is sampled by two channels of AD to enter the Arduino. Because of the cost, the AD adoption rate can only reach 20Kbps, communication bandwidth can reach 1Kbps. And the cost of the whole system can be controlled within 20 dollars.

From the perspective of the system, this is a SIMO system, which receives two signals and puts them together to form a combination. In this way, both of them make a contribution to the whole signal. The received signal $y(t)$ can be expressed as:

\[
\]
\[ y(t) = h_1 x(t) + h_2 x(t) + n(t) \] (1)

In (1), \( h_1 \) and \( h_2 \) are fading coefficients of the channel, and \( x(t) \) is the transmitting signal, while \( n(t) \) is the Gaussian white noise. The signal declines more as the distance increasing and \( n(t) \) reflects the influence of sunlight on the system. Then we propose a security authentication method based on SIMO-VLC.

There is a set of secret key between the transmitter (car key) and the receiver. A secret key of length \( n \) is sent by the transmitter through visible light technology and the range of the secret key is \( m \). After encrypting the information, a frame header of length \( a \) is added before the signal is sent. After the receiver is awakened by the frame header, it receives a signal to verify that the key is correct, and if so, the car door opens. If not, it will continue to wait for the frame header after the \( \Delta t \) delay. The receiver returns another secret key to the car key once the driver enters the car and then the key is updated.

By analyzing the above security authentication methods, we can calculate the average time required for brute force cracking \( t \) is

\[ t = \frac{m}{2} \times \Delta t \] (2)

By designing the range and delay of the secret key, the car can be prevented from being unlocked by exhaustive method theoretically.

3. Experiment and analysis

In this experiment, firstly, it was encoded the information to send a test signal, and it was ensured that the waveform of the output of the light source LED is not distorted. As it was shown in Figure 3, in process of the experiment, it was changed respectively the colour of the LED light, the angle of receiving the PIN photodiode to test the visible light communication system. Distance and bit error rate would be acquired after the experiment.

![Figure 3 Experiment setup](image)

The performance test of visible light digital communication system is mainly about the bit error rate test, \( p_e = N_{\text{error}}/N_{\text{sum}} \). \( N_{\text{error}} \) is the wrong encode element during transmission, \( N_{\text{sum}} \) is the total number of encode element issued during the system test.

The visible light digital communication system would utilize five different colours (blue, white, red, green, and yellow) as the carrier to transmit information. Then, Arduino was used as the processor in both transmitter and receiver, powered by a mobile power source with the voltage of 12V, and the final results are displayed on the Arduino serial port monitor.
After five groups of tests, the error data in the five groups were recorded, and the bit error rate under each light source was calculated, then the corresponding bit error rate distribution curve was plotted by Matlab. Finally, we test the BER in different offset angles with blue colour light source in the distance of 30cm.

4. Discussion

As shown in Figure 4, five curves with different colors represent the bit error rate performance of the visible light digital communication system under different color light sources and different distances. According to the bit-error rate curve, generally the light intensity of the light source will decrease with the increasing distance meanwhile the bit-error rate of the system will also increase with the increasing distance between the transmitter and the receiver. When reaching a certain distance, the error rate of the system increases rapidly and a large amount of error information will appear in the system. The effective communication range of the system is about 5-140cm, with green light, white light and blue light as the sources. In this range, system information transmission is very stable, although there are some messy codes, the proportion is very small. It may be limited by the power of the driving circuit of the light source. When yellow light and red light are the light sources, the brightness of each LED is not high and the light is not far away, and the effective communication distance of the system can reach about 5-30cm, while a few messy codes appear. In the range of 0-5cm, any of the five colors of LED as the light source. There are messy codes in communication systems and account for a large proportion. This indicates that the communication distance is too close and the light range received by the sensor is relatively narrow which will affect the transmission effect of the system and reduce the transmission reliability of the system.
The results can be obtained over the above experiment. The distance between the light source and the sensor device should not be too close. It should be more than 5cm and the furthest distance should not be more than 210cm. When blue LED and green LED are the light sources, the system has the widest effective transmission range and the best transmission effect. The longest effective transmission distance reach 180cm. Secondly, the effective transmission distance can reach 120cm with the white LED as the light source. The worst transmission effect of the system is yellow LED and red LED. The effective transmission distance is very short which can only reach 30cm at the most. Therefore, blue light is used as the light source in the visible light digital communication system and the transmission distance is within a range of 5-180cm.

Finally, it can be found in Figure 5, the system can tolerate the offset angle within 50 degree. If we change the direction of one of the photodiodes, the performance will be better.

5. Conclusion
A low-cost vehicle key authentication technology is presented based on SIMO-VLC in this paper. Compared with the traditional vehicle key authentication method, it eliminates the likelihood of being monitored in the physical layer by using SIMO-VLC technology. Meanwhile, we designed the hardware platform of the SIMO-VLC system to verify the effectiveness of the propose scheme. Finally, we completed the actual test of the SIMO-VLC system and found the communication by using blue light with lower bit error rate in the range of 5-180cm. The technology we proposed in this paper is proved with great potential in vehicle key authentication. In future, this technology can be combined with the concentrator system to increase the communication distance.

Acknowledgments
This work is supported by the Sichuan Province Science and Technology Program Research Project (No.2019YJ0174)

References
[1] Chen J F. (2015). Bluetooth Remote-Control Electronic Lock: U.S. Patent Application 14/055,295[P].
[2] Kulinets J M, Nuytkens P R, Venkatesh A K. (2013). Lock control system using rfid: U.S. Patent Application 13/474,034[P].
[3] Mostafa, A., & Lampe, L. (2015). Physical-layer security for MISO visible light communication channels. IEEE Journal on Selected Areas in Communications, 33(9), 1806-1818.
[4] Hong, Y., & Chen, L. K. (2016). On the performance of adaptive MIMO-OFDM indoor visible light communications. IEEE Photonics Technology Letters, 28(8), 907-910.
[5] Blinowski, G. (2015). Security issues in visible light communication systems. IFAC-PapersOnLine, 48(4), 234-239.
[6] Grobe, L., Paraskevopoulos, A., Hilt, J., Schulz, D., Lassak, F., Hartlieb, F., ... & Langer, K. D. (2013). High-speed visible light communication systems. IEEE communications magazine, 51(12), 60-66.
[7] Elgala, H., Mesleh, R., & Haas, H. (2011). Indoor optical wireless communication: potential and state-of-the-art. IEEE Communications Magazine, 49(9), 56-62.