Communication Encryption Method for Drone Control Using Radio Strength

Yuya HIROTSUJI* and Kenya SATO*

(Received February 2, 2021)

In recent years, with the improvement of drone technology, various demands using drones have been increasing. As a result, security of drones is becoming more and more important. One of the measures is the encryption of drone communication. Since drones need to be lightweight, it is necessary to use secret key cryptography instead of public key cryptography. In related research, the secret key was shared in advance, but this is inefficient. In the proposed method, the secret key is dynamically created and shared using the drone's movement history and radio wave strength. The key match rate under varying SNR is evaluated, and the proposed method is shown to be effective.

Key words : drone, signal strength, encryption

1. Introduction

Drones have become popular in recent years, and the demand for commercial use of drones indoors, such as the movement of goods in warehouses, is increasing in the future[1].Therefore, as the demand for drones has shifted from personal use to commercial use, security measures for drones are becoming more important. There are various perspectives on security measures, and the Secure Drone Council, a general social corporation, has created a security guide[2].This guideline describes the dangers of losing control of a drone. If the signal that controls the drone is hacked by someone with malicious intent and the control of the drone is taken away, or if the communication between the drone and the controller is tapped and various information is taken away, it is extremely dangerous and could result in loss of profit[3].Basically, the communication between the drone and the controller is not encrypted, and only pairing is performed before flight. Therefore, it is possible for someone with expertise to eavesdrop and take control of the drone. Therefore, security must be strengthened by encrypting communications to prevent control of the drone from being stolen or eavesdropped on. However, since the flight time of a drone is determined by how light the weight of the unit other than the flying unit is, it is not possible to prepare large computational resources. For this reason, encryption methods with complex processing and high cryptographic strength are not optimal. From the above, the increase in the overall weight of the drone due to the processing unit for encryption should be minimized. For this reason, it is not possible to encrypt the communication between the drone and the controller using public key cryptography, which is a complex process. Therefore, the secret key cryptosystem is used to encrypt the communication between the drone and the controller. The key to encrypting the communication between the drone and the controller is how to create and share the secret key between the drone and the controller.

* Computer and Information Science, Graduate School of Science and Engineering, Doshisha University, Kyoto, Japan
Email:yuya.hirotsuji@nislab.doshisha.ac.jp, ksato@mail.doshisha.ac.jp

In this study, we aim to improve the security of drones by creating and sharing a secret key between the drone and the controller. There is a method to share the secret key between the drone and the controller in advance, but we propose a method to create and share the secret key without sharing it in advance, and verify its effectiveness.

In Chapter 1, we describe the characteristics and problems of related research. In Chapter 2, the outline of the proposed method and its operation procedure are described based on the problems of related studies. Chapter 3 describes the evaluation of the proposed method and its results. In Chapter 4, we discuss the evaluation results. Finally, Chapter 5 gives a summary of this research.

2. Related Research

2.1 *One tine pad encryption*

There is also an attempt to encrypt the communication between the drone and the controller[4]. The method is to share a sequence of genuine random numbers as a common cryptographic key between the drone and the controller, and to encrypt the control communication packet by packet to prevent control hijacking and information leakage. This method uses a one-time pad cipher, in which a sequence of genuine random numbers is shared secretly between the sender and receiver as a cryptographic key, a ciphertext is generated by exclusive logical or (XOR) of the plaintext with the cryptographic key and sent, and the ciphertext is decrypted by XOR of the shared cryptographic key at the receiver side. The problem with this cryptosystem is that if the cryptographic key is predicted by others, the cipher will be compromised. The problem with this cryptosystem is that if the cryptographic key is predicted by others, the cipher can be broken. This sequence is generated in advance, stored in memory, and passed to the drone.

Light weight, low power consumption, and low cost are important factors for drones, and sharing them in advance is efficient in taking these factors into account. However, this method requires that a genuine random number be generated and shared for each flight. The less frequent the drone flights are, the more work is required in advance. This method is not efficient for operations in warehouses. Another problem is that the true random numbers must be shared safely.

2.2 *Technology for transmission and sharing of secret keys using radio wave propagation characteristics*

Although not a drone, the technique of sharing a secret key in wireless communication between two base stations by utilizing the propagation characteristics of radio waves has been studied[5]. When two base stations communicate, the received signal is affected by fading. However, if the radio waves transmitted by both stations have the same transmission time, frequency, and path, the fading characteristics are the same. Therefore, if both stations transmit at the same time and the received signal has the same transmission power, the strength of the received signal is the same. Therefore, if a secret key is created using the received signal strength, the secret keys created by both stations will match, and the communication can be encrypted.

The important point of this method, however, is that it utilizes the property that the fading characteristics are the same for the same transmission time, frequency, and path, as mentioned earlier. However, since the drone is moving, there is a possibility that the communication between the drone and the controller is not on the same path. If this is the case, the fading characteristics cannot be said to be the same. Therefore, this method cannot be applied to drones.

3. Method

3.1 *Overview*

In this study, we propose a method to encrypt the communication between a drone and a controller using the drone's movement path and radio wave strength.

First, the controller calculates the radio wave strength in the space in advance and creates a radio wave strength map. Since the controller controls the drone, it has a history of the drone's movement path. The controller can predict the strength of the radio wave that the drone will receive by superimposing the history of the drone's movement path and the radio wave strength map.

Next, the controller creates a secret key by quantizing the predicted data. The controller then uses the secret key to perform encrypted communication.

Then, the drone creates a secret key based on the received signal strength and decrypts the communication using the secret key.

The proposed method assumes that the movement path of the drone is secret, so the cipher is not broken even if the radio wave strength map is known.

An overview diagram is shown Fig. 1.

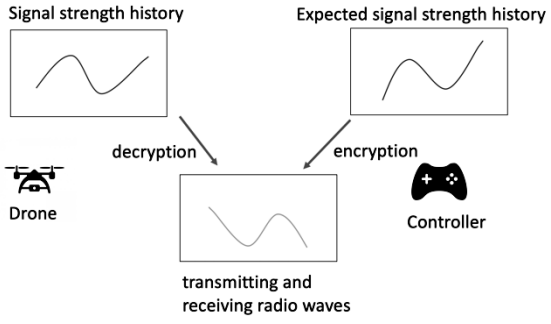

Fig. 1. Overview.

3.2 *Creating a radio wave strength map*

There are three main steps in creating a radio strength map. There are three main steps in creating a radio wave strength map: space dividing, setting the line-of-sight, and calculating the radio wave strength.

3.2.1 *Space Dividing*

The first step is to divide the indoor space into a collection of small spaces, rather than one large space. For each of these small spaces, we calculate the radio wave strength, and the data becomes the radio wave strength map. A small space is assumed to be 6m on a side. The reason for this is that ITU-R m.2412[6] states that shadowing is correlated every 6 meters, and that adjacent spaces are not correlated when they are 6 meters apart.

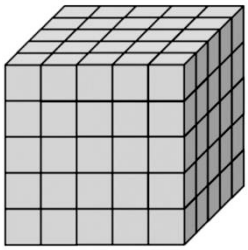

Fig. 2. Space dividing.

3.2.2 *Setting the line-of-sight*

Next, we set up whether the space is within the line of sight (LoS) or the Non line of sight (NLoS) of the controller based on the position of the controller and obstacles in the space. If the space is outside the line-of-sight, the radio wave will be reflected or diffracted and reach the drone, and the radio wave strength will be poor. To determine whether the drone is in or out of line-of-sight, the LoS probability is determined in ITU-R m.2412, and the equation Eq.(1) is used.

$$P_{LoS} = \begin{cases} 1 \ (d_{2d} \leq 5) \\ exp\left(-\frac{d_{2d}-5}{70.8}\right) (5 < d_{2d} \leq 49) \\ exp\left(-\frac{d_{2d}-49}{211.7} * 0.54\right) (5 < d_{2d} \leq 49) \end{cases} \quad (1)$$

Here, P_{LoS} represents the LoS probability and d_{2d} represents the distance between the controller and the drone in a two-dimensional plane without the height dimension.

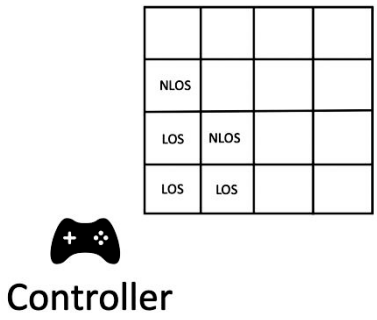

Fig. 3. Setting the line-of-sigh.

3.2.3 *Calculating the radio wave strength*

Finally, we use the radio propagation model to calculate the radio strength in space.

There are three types of calculations for radio wave strength: distance characteristics (distance variation), shadowing (median variation), and multipath fading (instantaneous variation), and we will use distance characteristics and shadowing to perform the calculations[7]. First, for the distance property, we use equation Eq.(2) and equation Eq.(3).

$$\mathrm{L_{LoS}} = 32.8 + \{16.9 * \mathrm{Log10(d_{3d})}\} + \{20 * \mathrm{Log10(f)}\} \quad (2)$$

$$\mathrm{L_{NLoS}} = 11.5 + \{43.3 * \mathrm{Log10(d_{2d})}\} + \{20 * \mathrm{Log10(f)}\} \quad (3)$$

Where L_{LoS} is the distance decay of the radio wave strength within the line-of-sight, L_{NLoS} is the distance decay of the radio wave strength the non line-of-sight, d_{3d} is the distance between the controller and the drone in three dimensions, d_{2d} is the distance between the controller and the drone in two dimensions, and f is the represents the frequency of the radio wave [MHz].Here, f is 2.4[MHz], which is determined by the Ministry of Internal Affairs and Communications [8].

Next, the signal strength variation due to shadowing is lognormally distributed. Therefore, if the standard deviation of the median of the short interval due to shadowing is σ_s, we can simulate shadowing by generating a random variable x according to the probability density function expressed by Eq.(4), which is a normal distribution with mean 0 dB and standard deviation σ_s dB, and adding fluctuations to the signal strength with x as the dB value. Shadowing can be simulated.

Here, σ_s is 4 dB in the line-of-sight and 3 dB outside the line-of-sight based on ITU-R m.2412.

$$P(x) = \frac{1}{\sqrt{2\pi}\,\sigma_s} \exp\left(-\frac{x^2}{2\sigma_s^2}\right) \quad (4)$$

3.3 *Encryption using radio wave strength*

Since the controller is constantly controlling the drone, it knows the drone's movement path. Therefore, by comparing the drone's movement path with the radio wave strength map prepared beforehand, it is possible to predict the radio wave strength history that the drone is expected to receive. We then binarize the signal strength to 0 or 1, using the median value as a threshold. The resulting bit sequence is used as the secret key. Then, the controller sends the encrypted signal to the drone. On the drone side, the secret key is created by performing the same operation as that performed on the controller side based on the radio strength history actually received by the drone. By decrypting the signal using the created secret key, the drone can receive the signal from the controller, and the encrypted communication between the drone and the controller is successful.

3.4 *Operating Procedure*

The operating procedure of the proposed method is described below.

The flowchart is shown in Fig. 4.

(1)Controller Creates Radio Strength Map.

(2)Controller creates a private key based on the drone's movement history and signal strength.

(3)Controller sends a signal to the drone.

(4)Drone receives the signal.

(5)Drone creates a private key based on the signal strength history.

(6)Drone decrypts the signal using the created secret key.

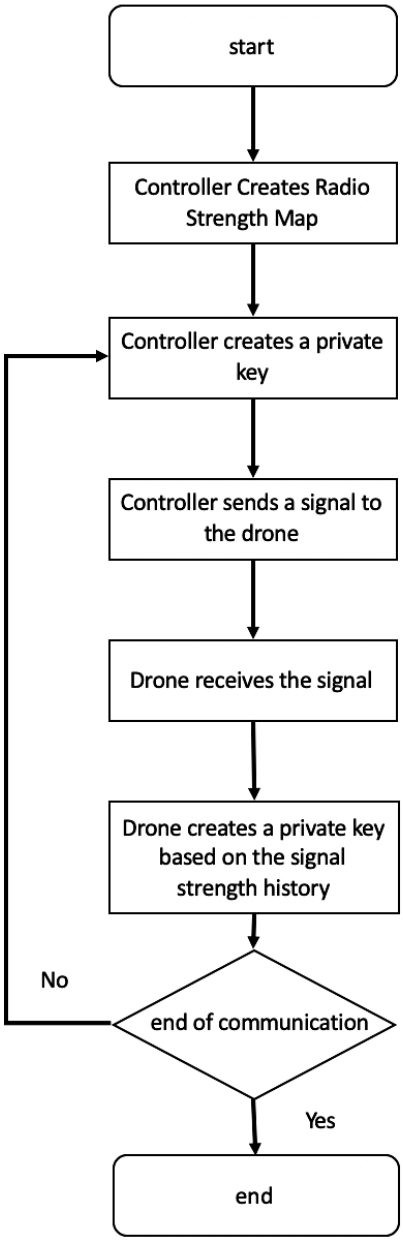

Fig. 4. Flowchart.

4. Evaluation

4.1 *Overview*

The evaluation is performed in a virtual space. The comparison items are the key match rate and the average ratio of matched bits when the SNR is varied. Here, the key match rate is defined as the expression Eq.(5). A key match is defined as a match of all bits of the key.

$$Key\ match\ rate = \frac{number\ of\ key\ matches}{number\ of\ key\ creation} \quad (5)$$

The average ratio of matched bits is the average of the ratio of matched bits out of all the bits in the secret key. The SNR is varied from 0 to 30 in increments of 5, and the secret key is created with 125 bits.

4.2 *Result*

4.2.1 *Key match rate*

The comparison targets are the three bit modifications of the secret key: no bit modification, 3-bit modification, and 5-bit modification.

The graph of the key match rate for each SNR when the secret key was generated 100 times is shown in Fig. 5.

When the SNR is 0, 5, 10, and 15, the key match rate was very low even with bit modification, and the key was not successfully shared. However, when the SNR was 30, the key match rate without bit modification was only 64%, while that with 3-bit modification and 5-bit modification was 100%, indicating that the proposed method was effective.

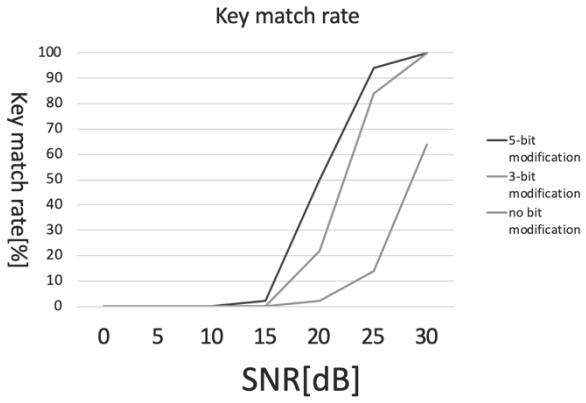

Fig. 5. key match rate.

4.2.2 *Average of the ratio of matched bits*

The graph of the average ratio of matching bits at each SNR for 100 secret key generation is shown in Fig. 6. There was almost no difference when the SNR was 0 and 5, but over this value, the average ratio of matched bits increased as the SNR increases.

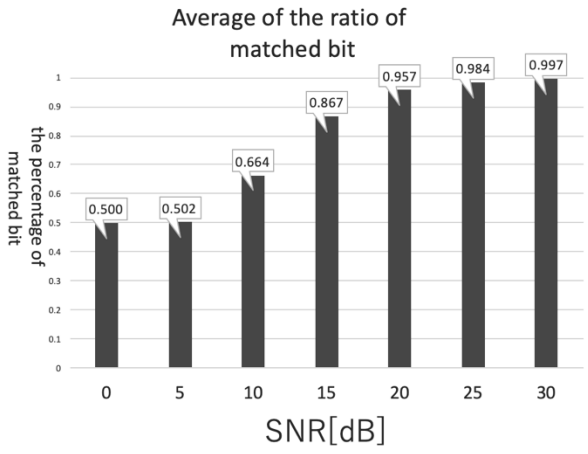

Fig. 6. Average of the ratio of matched bits.

5. Discussion

5.1 *Discussion about key match rate*

In the proposed method, encryption is performed using the drone's movement path and radio wave strength. Therefore, when the SNR is large, i.e., the effect of noise is small, the key match rate is high, but when the SNR is small, i.e., the effect of noise is large, the key match rate is low. However, according to wireless-nets, in some cases, such as in manufacturing plants, a SNR of 25 dB or higher is required [9].Therefore, considering the situation where drones are required, a SNR of 30 dB is practical. Furthermore, since the drone cannot fly stably without a high SNR to begin with, the decrease in the key match rate when the SNR is small is not a problem.

If there is only one controller, there is a possibility that the signal strength will be low locally depending on the shape of the space, which will reduce the key match rate. The solution to this problem is to prepare multiple controllers to supplement the space where the signal strength is low, which will improve the key match rate.

5.2 *Discussion about average of the ratio of matched bits*

At low SNR, 0 and 5, the average ratio of bits that match is almost 0.5, but since the bits are binary (0 and 1), the key is not successfully shared at all.

When the SNR is large, however, the average ratio of bits that match increases, exceeding 0.98 at 25 dB, indicating that if a 125-bit key is created and 5 bits can be modified, a bit match of over 0.96 is sufficient for successful key sharing.

6. Conclusion

Drones will become more widespread in the future as technology develops, and various demands will increase. In addition, security measures for drones are important. This is because if the communication between the drone and the controller is hacked, important information may be leaked by eavesdropping, or a collision may occur by losing control of the drone.

As a countermeasure to these problems, we mentioned that the communication between the drone and the controller should be encrypted. However, drones are required to be lightweight and power-efficient to ensure flight time .This means that public-key cryptography, which is computationally expensive, cannot be used, and secret-key cryptography must be used.

In related research, a method of sharing the secret key in advance has been considered, but sharing the true random number for each flight is inefficient for drones that fly frequently. However, sharing the true random number each time a drone flies is not efficient for drones that fly frequently. Also, sharing the true random number securely is not practical. Another method of sharing a secret key has been considered, but it requires the same transmission time, frequency, and route, and is not applicable to drones.

In this study, we aimed to improve security while reducing the computational cost of the drone by dynamically creating and sharing a secret key by using the drone's movement path and radio wave strength. The controller created a radio wave strength map in advance

based on the shape of the space, and created the secret key using the movement path of the drone controlled by the controller. Then, the drone decrypts the data based on the received signal strength.

The evaluation was done by comparing the key match rate when the SNR was varied, and the bit modification when decrypting with the generated secret key without bit modification, with 3-bit modification, and with 5-bit modification. The evaluation was performed by varying the SNR to 0, 10, 20, and 30.

The evaluation results show that when the SNR is high and is 30 dB, the drone and the controller can successfully share the secret key by performing 3-bit modification.

Acknowledgment

This work was partly supported by JSPS KAKENHI Grant Number JP20H00589.

Reference

1) K. Nonami, “State of the Art and Issue of Drone Technolgy and Business Frontier”, *Journal of Information Processing and Management,* **59**, 755-763(2017).
2) Secure Drone Council, Inc., “Drone Security Guide”, https://www.secure-drone.org/wp-content/uploads/drone¥_security¥_guide¥_201803.pdf(accessed 2019-10-10).
3) G.Vasconcelos, R.S.Miani, V.C.Guizilini, J.R.Souza, “Evaluation of DoS Attacks on Commercial Wi-Fi-Based UAVs”, *IJCNIS*, **11**, 212-223(2019).
4) J. H. Cheon, K. Han, S-M Hong, H. J. Kim, J. Kim, S. Kim, H. Seo, H. Shim, Y. Song, “Toward a Secure Drone System: Flying With Real-Time Homomorphic Authenticated Encryption”, *IEEE Access*, **6**, 24325-24339(2018).
5) H. Iwai, S. Sasaoka, “Transmission and Sharing Technology of Confidential Information Utilizing Radio Wave Propagation Characteristics”, *IEICE TRANSACTIONS on Communications*, **90-B**, 770-783(2007).
6) “Guidelines for evaluation of radio interface technologies for IMT-2020”, Report M.2412-0, 2017.
7) Y. Okumura, “ An Experimental Study of Propagation Characteristics in Land Mobile Communications”, *Report on Practical Application of Research at Research Institute of Electrical Communication*, **l16**, 1705-1764(1967).
8) Ministry of Internal Affairs and Communications, “ Radio equipment used for drones, etc”, https://www.soumu.go.jp/main_content/000528447.pdf accessed 2021-1-10).
9) J. Geier, “How to: Define Minimum SNR Values for Signal Coverage”, http://www.wireless-nets.com/resources/tutorials/define_SNR_values.html(accessed 2021-1-10).