EFFICIENT POST PAYMENT METHOD USING THE DRONES

[1]YUN-SEOK LEE, [2]EUN KIM, [3]SUNG-YUN KIM

LKSmart
E-mail: lysis2jt@naver.com, sil7777@nate.com, junghuning@naver.com

Abstract— Today, various types of drones are flying in the sky even now. The railway and automotive industry that brought about innovation of logistic transfer will be quite a change through drones. Drones go beyond the constraints of space with the existing railways and cars. Namely, they can be moved to anywhere in the path through which the flight. Like this, utilization of the movable drones will be more increased by combining with a variety of future service contents. Especially, it will be grafted and utilized primarily in delivery of small goods. At this time, the biggest problem is the post-pay payment method. Currently, the verification for the addressee by using the drones is not possible. I mean, it cannot be responsible for lost items because the ships are possible as putting down the delivery item and returning at the place of delivery. And secondly, there is no corresponding method for damaged goods delivered such as breakage can be occur in delivery process. This, customer can not perform a test of whether their own received the correct things. Finally, we can not select a payment method in accordance with the user's situation. Typically, the pre-payment method is usually done, however, post-paid payment method is also valid. Thus, post payment method should be also provided. In this paper, to solve these problems, we proposed the NFC based payment method and be progressing the effective user verification for post payment.

Index Terms— Drone, Payment System, Drone Post Payment.

I. INTRODUCTION

Today, various types of drones are being used with many missions. Especially, drone industry it has developed around the defense sector are growing more use of the private sector by providing and having an affordable price and a high level of control capability of flight[1]-[3]. The priority areas that were utilized are as a field of aerial photography. The aerial photography like this was the implementation area of the experts in the early days. Today, however, drones are being used by self-camera applications when it began to be utilized from the general public gradually. As well as entertainment sector, research that to apply for logistics system such as a parcel service is being actively studied in the private sector[3]-[8]. Especially, it is continuously expanding for the drone courier industry around the Amazon. Drones are studied in various areas. Among that research, it is one of the biggest problems by drones that they cannot proceed the verification of addressee at the time of transfer logistics. And also, the main problem of this method is that it may lead to incorrect delivery. And shipping via drones are many factors to consider like the strong winds, rain, tree branches, wires and etc. The breakages of goods can occur during shipment due to natural problems. And this time, accountability problem arises for the defect, if recipient does not validate the product on the spot. Finally, the current payment system is very familiar to secure by a post-paid method that to complete the transaction after receiving the goods. And in case of pre-paid method, there is no way to effectively cope with the accidents that may occur during shipping. Thus, in the delivery via drones even more requires post-paid transaction. Therefore, in this paper to solve this problem, we propose a validated method for the addressee and also propose a NFC based payment method for post-paid.

II. RELATED WORKS

Drone is unmanned air vehicle to perform a flight by having multiple rotors. These air vehicles are increasing the possibility lin various fields due to provide the stable flight and an easy control method[1][2]. Especially, the private sector has been rapidly developing, since the fused on to camera called Helicam into the field of aerial photography[3][4]. And recently, various studies and experiments for logistic transport using by drones have been progressed. Firstly, the Amazon began the development of drones for delivery service in 2013. And then, they are working to commercialize the drones that can be possible the delivery to the downtown area. And also currently, the PRIME service that can be delivered to the goods within 30 minutes using by drones is operated on a trial basis[2]. And the Walmart is also underway to test delivery through the drone. The Suning as China distributor was announced that it had succeeded delivery by drone. And recently, the Firstey as start-up company also announced that it had succeed that aid box containing bottled waters and emergency foods were shipped to the residential areas following the delivery path via GPS. Like this, goods delivery by drones has advanced to inside of the city with starting a difficult delivery area. However, the biggest problem in this is the human and material damage that may occur through the drones. The terms of these human and material damage about the rotor blades is studied in earlier papers. And also, it has been studied for the technology to prevent the damage that will be occurred when drones crashed. This method is an important issue in term of safety of the flight, however, it is also a separate issue not related to the logistic transport. The first goal that drone should perform in the logistics transportation is correct delivery for goods.

This means that not only will keep dropping things in the proper place, should be forwarded to the actual recipient. It comes with a fixed position on the just released issue that may not be delivered to the recipient entity. Therefore, it should accurately deliver to the recipient, and the recipient must be confirmed by the drones that accurately receive it. The second goal is to secure delivery of the goods. That it will be able to cope with such damage or deterioration of the goods. It must prove that there are no problems at the time of delivery or shipment of the products to be destroyed spoilage during shipping. When the next delivery is complete verify that the recipient must be accurate and safe delivery to verify this.

II. OUR PROPOSE DEVICE

In this paper, the authentication proceeds to the delivery using a smart phone to the user with a safe and accurate delivery of the drone, and also proposes a system that can be completed by the settlement by using the NFC function.

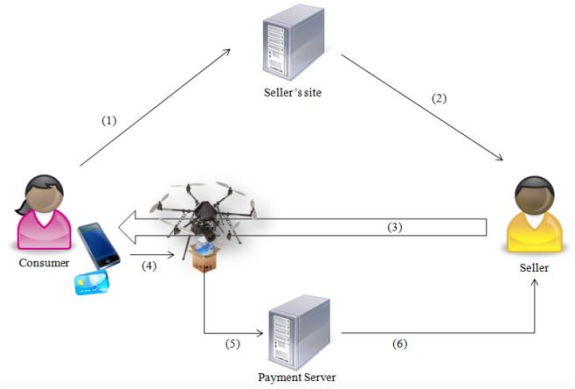


Fig 1. Our proposed method

The process of our proposed drone post payment method in this paper same as following Fig.1.

(1) Firstly, a buyer orders from the provider's website.
(2) A provider(seller) gets buyer information from own website.
(3) A provider delivers goods by the drone.
(4) A buyer checks goods and then, make progress the payment request through NFC onto own smartphone.
(5) The drone completes payment by sending the payment information to payment server.
(6) If payment completes, sends corresponding data to provider.

It will make payments in this order. At this time, a buyer must sign up in advance on two servers. This is the registration phase.

A. Registration phase

As shown in Fig.2, a customer sends an own ID, a password and a secure number SNCS onto Payment Server. Payment server safely stores corresponding data and then, sends own Temporary Key TK and Secure Number SNPS that can be used when trading. A customer can safely store own information onto the Payment Server through this.

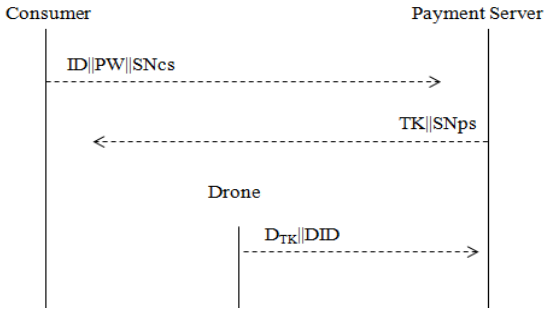


Fig 2. Regisatration phase

Drone sends and also stores an own Temporary Key D_{TK} and an own ID D_{ID} to Payment Server. And like this, whole process is not to continue to occur with every purchase. Thus, it may continue to be used with once registration step. If a customer want to be issued a new ID, PW and TK, can request a re-registration. And also, registration phase like this is assumed to be progressed via a Secure Channel. And this, general how to join in other website is the same. However, provider's website should safely send an own session key to a customer. These steps are referred to the registration phase and then, the transaction can proceed with subsequent transactions.

B. Trade phase

In the trade phase, as shown Fig.3, a customer encrypts E_{SS}(ID||PW) an own ID and a PW that was registered in provider's website by provider's session key. And a seller provides TPN as a temporary product number after performing E_{SS}(TPN). Since then, a seller inputs TPN as a temporary product number, the value of GPS and a price onto the drone. Drone proceeds to fly on the basis of the inputted information. After landing in the correct position, it proceeds to deal with customers. Firstly, a customer runs the transaction application onto own smartphone. And then, inputs the received APN as issued from the provider's website. And it is sent it to the drone through NFC. Drone sends a product number PN and a price to a customer. A customer generates the following cipher text after checking a corresponding product name and a price.

$$E_{TK}(TS||PN||price||ID||PW||Nonce||h(SN_{CS}||SN_{PS}||Nonce||TS))$$

This cipher text is sent to the drone. And then, drone sends a corresponding information combined with DID as an own ID. Payment Server proceeds to verify decrypted data, after decoding received information. The verification about the data uses the customer's ID and PW. Thus it ensures registered the value of SN_{CV} onto the Payment Server. And also performs a hash using by a Nonce value, a product price and finally own SN_{PS}. If the result is the same as the decrypted information, this transaction may be determined to be useful. Thus, it can be progressed the transaction. And

then, Payment Server progress a credit transaction for that price. If accurate credit transaction is completed, encrypts using by D_{TK} as a key of the drone. And then, sends data about success or failure to the drone. Drone performs to decrypt received data. And if success, puts down the product and then, flies again to move to the specified area.

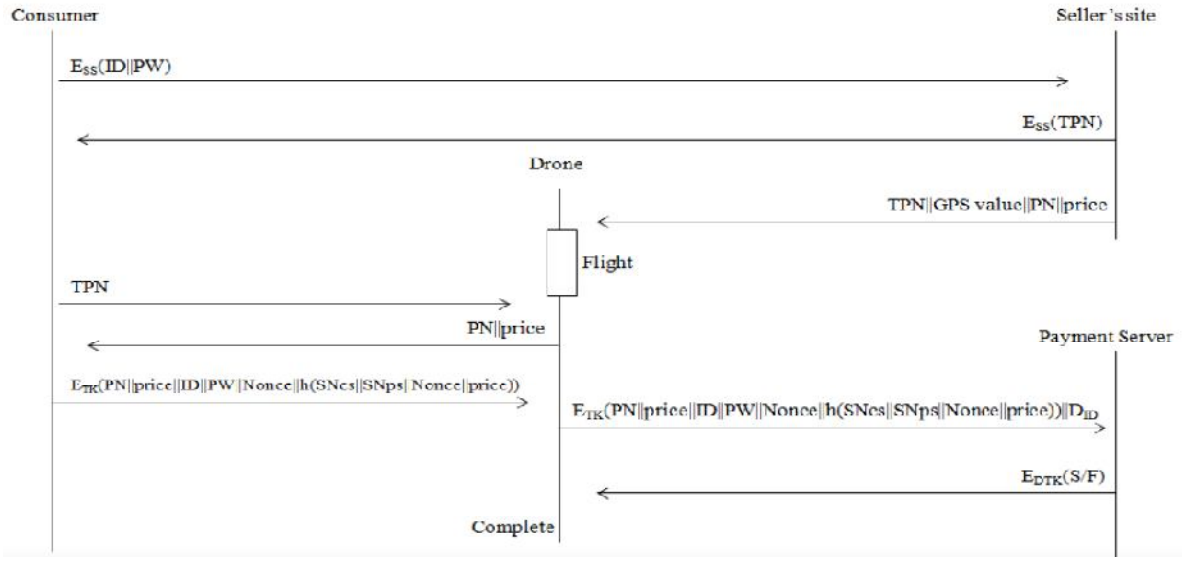


Fig 3. Trade phase

III. ANALYSIS

In this paper, we propose a new system that is possible safe post payment using by a drone. We assume that a user and a drone could be securely stored and managed information via a secure channel.

A. *Safety Analysis*

Our proposed method in this paper is achieved to connect through the actual billing information, after the arrival of drones. After arrival the drones, if someone else would like to camouflage the actual buying customer, because other customer will not know the TPN. Thus, it cannot be made a payment. And if disguised drone try to make payment by carrying an illegal products, a customer confirms the goods and then, proceed the payment, thus, it is possible to prevent the for the wrong product. And if the drone attacks have changed by modifying the high amount of price data to be transmitted after verifying TPN PN || price to the customer, so the actual user displays the price value in the mobile application, it is more than the purchase price It may prevent attacks for the case of high. And communication between the user and the drone is in progressed through the NFC. NFC is not possible a man-in-the-middle attack, due to perform the communication within 10cm. If drones and Payment Server between the communication section from information obtained if the case exposed that information E_{TK} (TS | | PN | | price | | ID | | PW | | Nonce | | h (SN_{CS} | | SN_{PS} | | Nonce | | price || TS)) || D_{ID} inde if the proceeds if the data sent back to replay attacks TS Time Stamp words have different values, so cannot make a payment. and have a different Nonce values every session, the safety is secured by a secret Jung SN_{CS} SN_{PS} between customers and is not exposed through the hash function and the Payment Server. In other words, if a user with business experience knows that security there is TK's Payment Server is secure, even if you want to decrypt and modify the price and trading information to obtain the information it finds the Payment Server SN_{CS} have an ID and password. The find Jean SN_{CS} the basis of its hash value that is h (SN_{CS} | | SN_{PS} | | Nonce | | price | | TS) to perform in if the other exposed a value price, TS, Nonce and they know that SNPS to have a hash value if you try to create a SN_{CS} not know anyone else with an attack that data is not possible. Encryption algorithm used in this paper uses a symmetric key encryption method is fast, so fix the number of communications with the Payment Server in the transaction process with only two times can be high in efficiency. Also use the applications of the smart phone users have the advantage that they are available to determine whether the articles purchased, it can proceed with the secure payment via the NFC.

CONCLUSION

Our proposed scheme in this paper is a post payment method by using a drone. Increasing the utilization of drones, the study of logistic transfer by using a drone has been made actively. In this environment until now, there are being offered a method that how to send drones with corresponding goods, after prepayment. However, in order to cope with the hands or deterioration and loss of goods occurring during the transfer through the drone buyer may wish to proceed with the payment in arrears in their own right. This a secure and efficient payment method vulnerability that

occurs in that case papers offered. Buyer delivered using a smart phone that you own your payment information to effectively secure drones and drones, and NFC communication is sent to the Payment Server without the interference of the information. And therefore it receives only the consequences drones inside do not leave the customer's billing information for the customer. This may proceed in the same secure way post-paid payment by drones.

ACKNOWLEDGMENTS

This paper has received the support of the Research and Business Development(R&BD), Ministry of Trade, Rupublic of Korea(C0332683).

REFERENCES

[1] Z. Mustapa, S. Saat, S.H. Husin, and N. Abas, "Altitude Controller design for multi-copter UAV," Computer, Communications, and Control Technology(I4CT), pp.382-387, 2014.

[2] Y. S. Lee, E. Kim, D. C. Seol, and Y. S. Kim, "Effective Message Authentication Method for Performing a Swarm Flight of Drones," International Conference on Environmental Engineering and Remote Sensing, 2015.

[3] D. G. Ggziabher, R. C. Hayward, and J. D. Powell, "A low-cost GPS/inertial attitude heading reference system(AHRS) for general aviation applications", pp.518-525,1998.

[4] M. Peacock and M. N. Johnstone, "Towards Detection and Control of Civilian Unmanned Aerial Vehicles," Australian Information Warfare and Security Conference, 2013.

[5] R. Mitchell and I. R. Chen, "Adaptive Intrusion Detection of Malicisous Unmanned Air Vehicles Using Behavior Rule Specifications," IEEE TRANS. ON SYSTEMS, MAN, AND CYBER. SYSTEMS, vol. 44, pp. 593-604, 2014.

[6] M. Buehler, K.Iagnemma, and S.Singh, "The DARPA Urban Challenge:Autonomous Vehicles in City Traffic," Springer, 2009

[7] D.F.Pigatto, G.F.Roberto, L.Goncalves, J.F.R.Filho, A.S.R.Pinto and K.R.L.J.C.Branco, "HAMSTER-Healthy, Mobility and Security-based Data Communication Architecture for Unmanned Aircraft Systems," ICUAS, 2014.

[8] K. Mansfield, T. Eveleigh, T. H. Holzer and S. Sarkani, "Unmanned Aerial Vehicle Smart Device Ground Control Station Cyber Security Threat Model," IEEE International Conference on Technologies for Homeland Security, 2013.

★★★