Effective Verification Method for Origins of Aircraft and Aircraft Authentication Method Required for the Flight of Drones at City

Yun-seok Lee*, Eun Kim, Jong-min Kim and Sung-yun Kim
LKSmart 11-A-213 GuamNam 16Gil 54 MasanHappogu ChangWonSi
Kyungsangnamdo, Republic of Korea
*Corresponding author

***Abstract*—Today, various types of aircraft are being operated within the city. Especially, most users who buy the drone for entertainment are living in the city. Also demand is increasing for drones it can be used in transport logistics, the limit is needed about illegal activity of these drones. Because, there are various problems through the drone like terrorism works of men and money, use on delivery of illegal products and shooting for military important places. In this paper, in order to solve these problems, we propose an effective method to execute the preflight authentication of drones and to verify origin and trajectory of flight at the time of utilization of the aircraft crash and crime.**

Keywords: drone; aircraft; authentication; verification

I. INTRODUCTION

Today, various types of flight called a multi-copter can be often seen. In particular, unmanned vehicle market is being actively utilized in the private sector with the Unmanned Aircraft Vehicle(UAV) market on defense field[1,2,3]. UAV has been developed around the air shooting such as advertising and TV. Especially, there is developing as specialized areas by use such as a crop dusting, forest fire and coast observation, into specialized areas[3,4,5,6,7]. The biggest problem in the operation of drones, it is the intention of the user to operation the vehicle. In general, the airframe called drones can lift a payload of about 10kg and within 1m size. We can say that the damage of men and money is as a natural result, if drones that can lift this size and weight are going down. Especially, if someone uses a drone by purpose of like a terror, he can apply to a particular building or terror to object through the Waypoint flight at long distance. Therefore, it can be happened very worrisome situation[3,4]. In particular, in order to operate the aircraft in certain areas, there are countries that have pre-approval system. However, with improved flight distance and time, there is not a method that illegal action block after takeoff from non-approved areas. And also, there is a problem that airframe identification method is a very limited because the size of an airframe is small[5,6,7].

In this paper, in order to solve these problems, firstly we propose the method to execute the process of purchasing the aircraft at certified companies. Secondly, only registered user through the user registration system must operate the registered aircraft and then, sends a flight and a location information(GPS) through the communication with a server before the flight. And we propose the authentication method that only certified aircraft must be executed the control through the RC or GCS(Ground Control Station) . And if certified aircraft fall in a particular area after breaking away from area of RTH(Return To Home) mode, our method can be traced the operating time and user through the registered information. Thus, it can be prepared for situations such as terror.

II. OUR PROPOSED METHOD

Our proposed method in this paper is divided into three steps for the authentication and verification of the aircraft. There are registration, authentication and verification phase. The third phase among these steps is process to verify when it happen significant event like a crash of aircraft. Thus, it can only be used first and second phase under normal circumstances.

A. Terminology

Terminology	
X_puk	X's Public Key
X_prk	X's Private Key
D_SN	Drone's Serial Number
x	Registration Server Secret Number
h( )	Hash Function
D_RND	Drone's Random Number
RS_RND	Registration Server's Random Number

B. Registration Phase

As shown in Figure 1, user should register own and aircraft information into server at the same time as the purchase of vehicles. Firstly, user sends request for registration to Registration Server. On request for registration, the registration server sends own public key and URL information. User sends encrypted information using by registration server's public key, after checking the serial number of a drone. The registration server stores decrypted information, after decrypting received data. And then, sends a unique secret value of a drone as result

by hash user's password, the serial number of a drone and registration server's secret information. User generates OWNER_INFO and stores into a drone, after receiving the information. At this time, each data is stored separately in the drone.

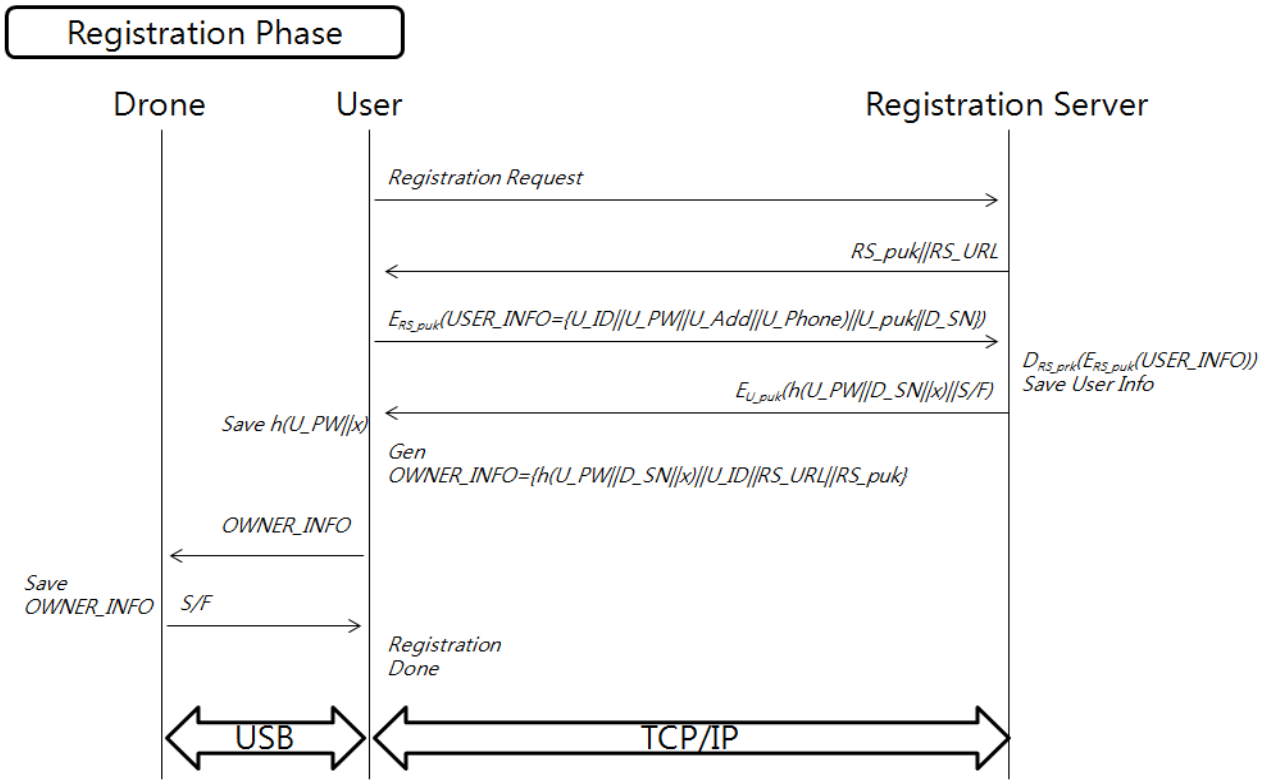

FIGURE I. REGISTRATION PHASE

C. *Authentication Phase*

User must go to the flight space holding their drones. When he turns on the drone in flight space, the drone will automatically perform the authentication process as shown in Figure 2. This authentication phase generates a one-time public key and secret and then, encrypts following information using by server's public key.

D. *Flight_Sch_Info={h(U_PW||D_SN||x)||U_ID||D_SN||D_RND||TimeStamp||GPS Value}*

$$Sign\_Data = EU\_prk(Flight\_Sch\_Info)$$

At this time, the D_RND is nonce value it is generated to defend the replay attacks at every session. TimeStamp is current time information. And flight starting point of the drone is specified through the GPS value.

E. *Verification Phase*

This verification phase has not happened in everyday environments. When aircraft crash or fall by battery problems, it can be used to verify origin of the aircraft. Firstly, stored data in internal memory of the crashed aircraft are as follows.

F. *H(U_PW||D_SN||x), U_ID, D_SN, D_prk, D_puk, RS_URL, RS_puk, TimeStamp, GPS Value*

All this data are respectively stored separately and can also be stored into a file system according to the system. The verifier of the crashed drone mostly handles in investigate agency. We can access to relevant data to connect a drone by using a USB cable. At this point, it provides only access to H(U_PW||D_SN||x) and U_ID, D_SN, RS_URL. And firstly, connects to the recorded URL on U_ID as user's identification, D_SN as identification of the drone and then, checks a path, time and a user. And through this, verification is completed.

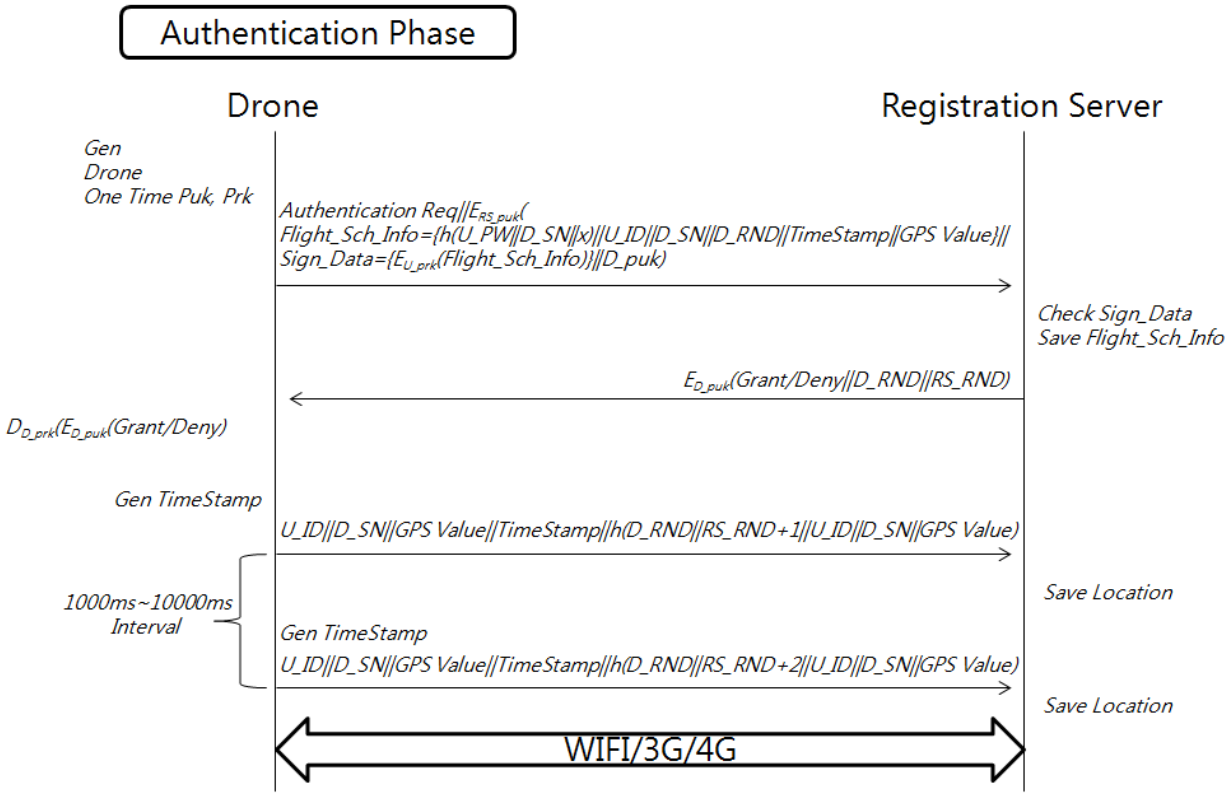

FIGURE II. AUTHENTICATION PHASE

III. ANALYSIS

Our proposed scheme in this paper is an effective drone authentication and verification method for downtown driving. The required basic functions for downtown driving are essential a collision handling method, WayPoint features and like as our proposed authentication method. In this case of authentication method, there is a way to disguise the other owner of drone by illegal user who he has a malicious object. Especially, because drones are operated from anywhere in the city, it can easily obtain the communication information of the drones. Therefore, even if he acquired the communication information, it should be designed that can not be authenticated by using them. The exposed information in communication process using by registration server's public key are an encrypted data as ERS_puk(Flight_Sch_Info||Sign_Data||D_puk), U_ID, D_SN, GPS Value and TimeStamp. Encrypted data by registration server's public key have cryptographic strength, thus it can be seen that it is generally safe. Because it use D_RND as deferent value in every session generates RS_RND and then sends. Such information is stored including nonce in hash value. Therefore the replay attack is impossible. And even if someone U_ID, D_SN, GPS Value and TimeStamp as exposed information modify, it is verified in authentication code in part on the back of message. Because it can determine an error in data, the spoofing attack is not possible.

IV. CONCLUSION

In this paper, we propose a drone authentication system that can be applied and operated various types of UAV in the city. Most drones are difficult to read the radar, because it is small. And also, it can be used drones for like a terror, because it is impossible to tell with the naked eye that drones. Therefore in most cases, there is a case of operating to fly under license by completing a pre-flight declaration of drones. Nevertheless, it has often ignored most of the procedure in case of entertainment or for individual drones. Therefore, authentication process is necessary for safe operation of the drones.

In this paper, we proposed a method to allow the flight of the air using by authentication scheme based on public key and a registration server. In the future, the actual test is required for effective authentication of drones.

ACKNOWLEDGEMENT

This research was supported 2015 area SW convergence commercialization support program funded by Ministry of Science, ICT&Future Planning and NIPA

REFERENCES

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

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

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

[4] R. Mitchell and I. R. Chen, Adaptive Intrusion Detection of Malicisous Unmanned Air Vehicles Using Behavior Rule Specifications, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS:SYSTEMS, 44 (2014) 593-604

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

[6] 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)

[7] 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)