Effective Message Authentication Method for Performing a Swarm Flight of Drones

Yun-seok Lee*, Eun Kim and Young-sub Kim
LkSmart 11-A-213 GuamNam 16Gil 54 MasanHappogu
ChangWonSi
Kyungsangnamdo, Republic of Korea
*Corresponding author

Dong-chul Seol
GaonSoft 21 BongAmBuk 7Gil MasanHeowonGu
ChangWonSi
Kyungsangnamdo, Republic of Korea

Abstract—**Recently, various types of aircraft are flying in the sky. Especially, Unmanned Aircraft Vehicle (UAV) called drones can operate with from aerial photography to unmanned delivery thus, utilization is very high. Drones are classified as Quad, Hexa and Octa copter depending on the number of rotor. However recently, most drone has to configure and operate the number of such three rotors and two tilt-rotors. The biggest problem of these drones is a short flying time. In general, it is possible a flying about 15~20 minutes. It is highly variable depending on wind influence, nature of the communication environment. Therefore, overall flight distance is inevitably very short. And also shooting or operational area is very limited. To be presented as a solution to this problem is the swarm flight. The swarm flight has the advantage that several drones ensure flying area and execute their mission. Therefore execution of duty is possible in the wider area. In this paper in order to solve this problem, we propose effective message authentication method between aircraft that performs the swarm flight.**

Keywords-drone; swarm flight; authentication; message authentication

I. INTRODUCTION

Today, drones are being used in various fields ranging from aerial photography, entertainment, defense and delivery. Thereby there can take to shooting in far and wide, rather than observing the particular area at a low place, it is possible to obtain more accurate information. Therefore, we judge that its utilization in the field of defense and aviation sector is excellent[1,2,3]. However, the biggest problem of these drones is flying time. The basic structure of the drones is composed of lithium polymer battery, attitude control board with on-board AHRS algorithms, communication board and finally, ESC(Electronic Speed Control) motor. Basically, the battery consumption is a large part of the motor driving immediately[1]. The aircraft is a combination of different types of down to 4~8, and is performed a stable flight. The more the motor can be stable flight and may have a larger payload, however, the flying time can be short due to the large power consumption. In particular, when receiving a course under the influence of the wind, it is much less the flight time to keep the higher the throttle. This can be a great disadvantage that it may not be able to perform the mission through the actual flight. In order to solve this problem, firstly, we can launch a number of the drones. And then it is assigned to a specific area to each drone. Thus, it can be solved by performing a mission in the area at the same time. This method is very effective, because it can be monitored and observed over the wide area. However, there is the financial pressure point because should prepare a number of the aircraft. And also, there may be a direct attack that they can also disable the mission on the massage in mutual communication between aircrafts[3,4,5,6].

In this paper in order to solve this problem, we propose a message authentication algorithm based on hash function. Because the hash function can be a high-speed operation, battery consumption in the operation can be reduced when operating the drone. Especially, our proposed method support message authentication and communication between groups of drone. Therefore, we were removed defect to perform the duties of a swarm flight due to a message forgery.

II. RELATED WORKS

The drones in private sector began in earnest activation in accordance with the flied of aerial photography using by drones. And a new paradigm for the drones is presented that Amazon announced a drone delivery system called PrimeAir in 2013[1]. If the traditional drone industry is properly activates for aerial photography and entertainment, we judged that a new trend it is presented industrial direction on logistics transfer has been born. Amazon aims immediately delivery to the consumer in less than 30 minutes, within 16Km from logistic center, goods of below 2.3kg weight after purchase using the Octa copter Equipped with the 8 wings. And DHL developed a drone called PaketKopter in December 2013. And DHL was a successful the flight test of the drugs shipped to the region of across the river by developing drones called PaketKopter. The PaketKopter can be up to an altitude of 100m with a payload of approximately 3Kg. Next, DHL is researching and developing focuses on entering the PaketKopter in the geographically difficult area. Google and Facebook are also acquired each Titan Aerospace and Ascenta. Both companies are planning to spread the Internet in Africa, South America, etc. by utilizing the drones as wireless communication base station. Actually, Google has conducted and succeeded project Loon. On June 2013, Google began a pilot experiment in New Zealand where about 30 balloons were launched and then 50 local users are connected to the aerial network. Facebook is also working on the project Internet.org to supply the affordable Internet service by launching the 1 million drones in Africa airspace. Teal group as America’s defense industry consulting firm expects to increase to the market size of drones about $ 9.1 billion, by 2025. Considering the television market in the world is the approximately $163 billion, the future market value of the drones has enormous proportions. Therefore, damage of the monetary and non-monetary resources will continue to increase by the collision and crash of the drones in the city. How to respond to this is a pre-registration or prior notification of information on a flight, however, there is no way to respond to the non-reported aircraft, non-reported flight business. And after an accident of drones, how to countermeasures and tracking are also ill-prepared for an emergency[3,4].

III. Our Propose Method

Our message authentication method of aircraft is largely divided as authentication of two types between groups and between aircrafts. This is about the same as in Figure 1. Firstly, GCS(Ground Control Station) has control of the group to perform each swarm flight. In case of the swarm flight, it may perform a mission in a wide area. Thus, it may occur the drones are getting out of the communication area. To secure control through GCS, in other words, that should be done Vehicle to Vehicle communication for communication between a drone and a drone. Each of the drones is to perform the broadcasting when communicating with other aircraft in its communication area. Thus, the mission should be assigned considering the communication area between the drones. And each drone performs the communication according to the own position. At this point, if they need to perform the mission on the wider area, it may be necessary to perform the communication between the two GCS groups. In this case, the drone A3 and B3 are located close to each other as shown in Figure 1. Thus, it should be able to exchange message and information for the mission with each other. As previously mentioned, the biggest problem that may arise in such an environment is that information of wireless communication between drones is very easy to obtain[4,5,6,7].

In solve to this as shown in Figure 2, each of the drones is register in the registration center. And then, they have the secret value hashed with own ID and X as unique secret value of registration center. GCS of the group own the secret value what all of the drones under their control. Firstly, we assume as above. And GCS stores *h(AGCS_ID||x), Gnone* to all drones belonging to their group before flying. Firstly, for the message authentication in communication between GCS and the drone is hashed with information of CM(Control Message), Gnonce and receiver’s secret hash value and secret hash value of receiver. And then, it is broadcasted after junction the result of above operating, sender’s ID and receiver’s ID. Finally, the drone what receive this information can arrive can getting own information, or can broadcasting the data. Therefore, it is possible to reach the end message to the receiver. The broadcasting period of the packet is not more than twice the amount of all the nodes. In other words, the packet unconditionally prevents flooding by operating -1 in their position. And they can send the data to final destination by broadcasting after connection the information that they should inform in case of the communication between the drones is named NM(Notification Message), Gnonce and secret hash value of the GCS. And in case of message authentication between groups, if GCS A is set a Master, GCS A sends group request data, own public key and broadcast data to all nodes. And node A3 sends relevant information to the B3. Then B3 sends relevant information to BGCS, and then BGCS sends BGnonce after encrypting using by a public key of the AGCS. AGCS performs the message authentication between groups.

CM’||h(CM||BGnonce||h(B3_ID||x))||A3_ID||B3_ID

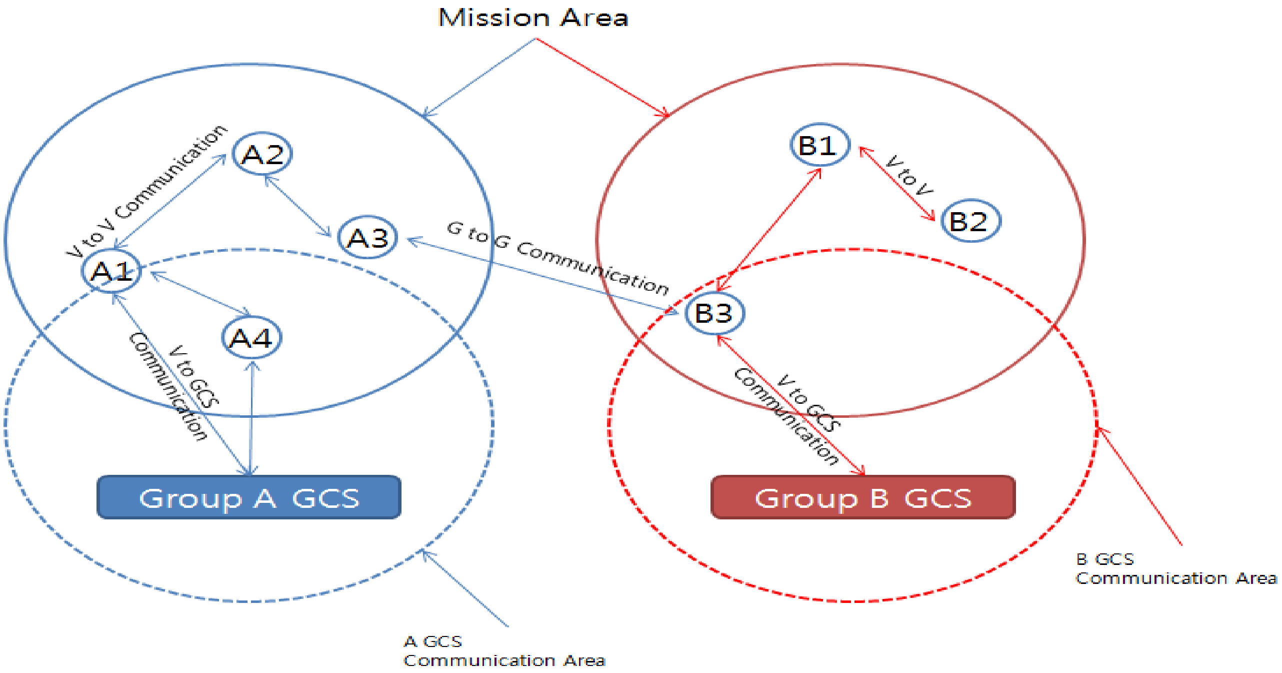

FIGURE I. THE COMMUNICATION AREA AND METHOD OF THE DRONES THAT PERFORMS SWARM FLIGHT

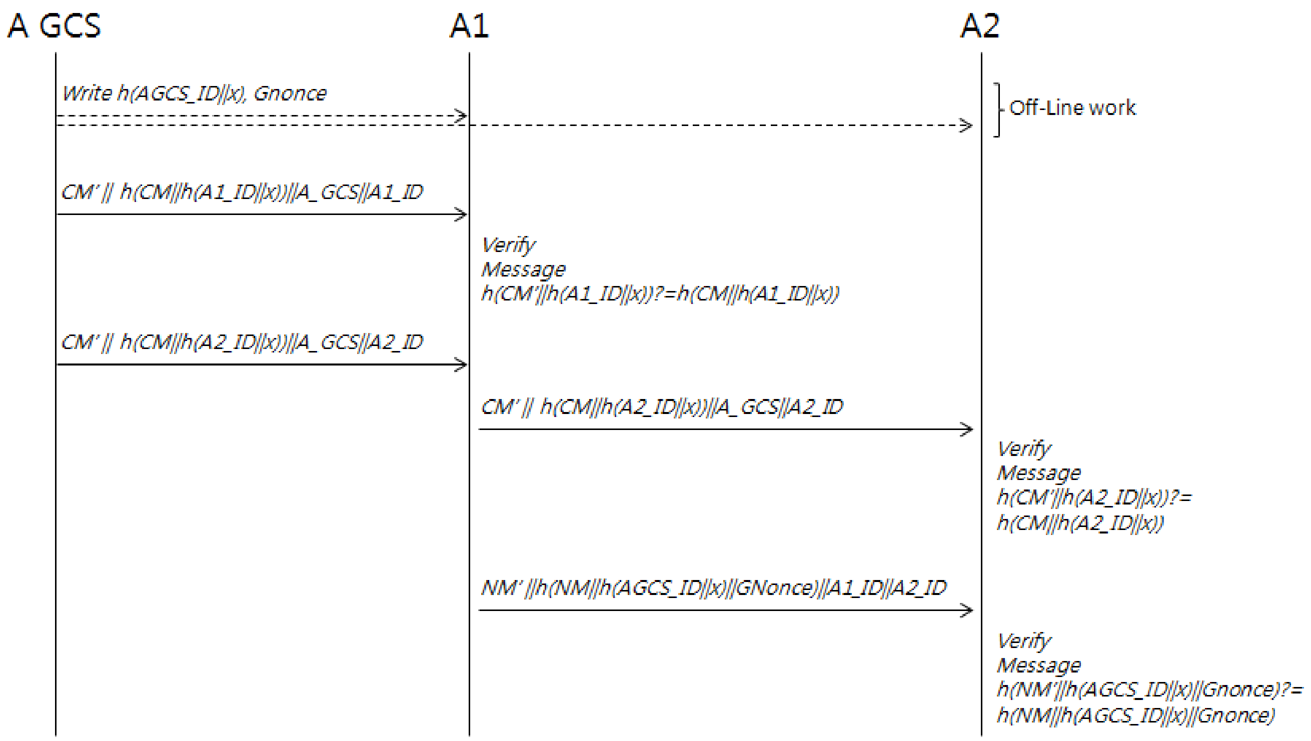
A GCS
A1
A2
Write h(AGCS_ID||x), Gnonce
Off-Line work
CM' || h(CM||h(A1_ID||x))||A_GCS||A1_ID
Verify
Message
h(CM'||h(A1_ID||x))?=h(CM||h(A1_ID||x))
CM' || h(CM||h(A2_ID||x))||A_GCS||A2_ID
CM' || h(CM||h(A2_ID||x))||A_GCS||A2_ID
Verify
Message
h(CM'||h(A2_ID||x))?=
h(CM||h(A2_ID||x))
NM' ||h(NM||h(AGCS_ID||x)||GNonce)||A1_ID||A2_ID
Verify
Message
h(NM'||h(AGCS_ID||x)||Gnonce)?=
h(NM||h(AGCS_ID||x)||Gnonce)

FIGURE II. GCS TO V AND V TO V MESSAGE AUTHENTICATION METHOD FOR SWARM FLIGHT

IV. CONCLUSION

In this paper, we proposed the authentication method for secure message authentication between drones that there are performed the swarm flight. The performance time is improved using by a hash function when all message exchange. And then secret information and nonce as one-time value are pre-distributed and exchanged. Therefore, it is strong in various attacks like a replay, an impersonation and a forgery. In the future, we are planning to conduct research on enhanced message authentication method that can protect against DoS attack, etc.

ACKNOWLEDGEMENT

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

REFERENCES

[1] Ondrej.S., Holub, O., Hanzalek, Z., “Low-Cost Reconfigurable Control System for Small UAVs,” IEEE Tran. on Indu. Elec., 58, (2011) 880-889

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

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

[4] S.W.Kim and S.W.Seo, "Cooperative Unmanned Autonomous Vehicle Control for Spatially Secure Group communications," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, 30(2012)

[5] F.Giulietti, L.Pollini, and M.Innocenti, "Autonomous formation filight," IEEE Control Systems, 20(2000)

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

[7] 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