International Civil Aviation Organization

RPASP-3-WG2-WP/006
../../15

WORKING PAPER

REMOTELY PILOTED AIRCRAFT SYSTEMS PANEL (RPASP)

THIRD MEETING (RPASP/3)

Montreal, Canada – 14 to 18 December 2015

Agenda Item 3.2: Command and control (C2)

RPAS AND C2 LINK SECURITY PROTOCOLS

(Presented by Edward Falkov and Sergey Shavrin, Russian Federation)

SUMMARY

A set of protocols for secure and authenticated multiparty information interchange over radio links are being proposed. The protocols are based on elliptic curves cryptography and are designed to minimize overall traffic over the links.

It is supposed that the given working paper is the subject for consideration within RPASP (WG1, WG2, WG3, WG5, WG6) and ICAO Panels AVSECP, CP, SP.

1. INTRODUCTION

Availability and low cost of radio equipment allows smart terrorists to be able both to intercept coordinates and to identify aircraft in the air under surveillance; at the same time the possibility of precise operative control of RPA greatly complicates the flight security problem.

RPAS information security system should satisfy two contradictive requirements:

- from one side, every air traffic participant should be able to understand (= to get access) the manoeuvres of other participants to avoid collisions;

- from the other side – no one else should get access to this information (= aircraft ID + coordinates).

The two-key cryptography can be used to overcome the problem providing confidentiality and authentication of information interchange. Its practical implementation to C2 Link raises two new problems:

a) as a rule, messages transmitted over C2 link are too short to be easily and reliably protected by common two-key algorithms;

b) the most of two-key algorithms are not especially designed for dynamic multiparty information interchange and can lead to significant traffic increase within this implementation.

A set of protocols for secure and authenticated dynamic multiparty information interchange over radio links are being proposed and described below. The protocols are based on elliptic curves cryptography and are designed to minimize overall traffic over the links.

2. DISCUSSION

Each object should be assigned a pair of keys – a public and a private. All public keys are stored in a common database accessible only to authorized personnel including pilots on duty. Private keys are physically protected inbuilt part of an object equipment inaccessible out of encryption / decryption function.

Elliptic curves encryption and decryption functions are calculated according to the equations as follows:

$$E_{\{pub\_K,pr\_K\}}(DATA) = DATA + pr\_K1 \times pub\_K2 = DATA + pr\_K1 \cdot pr\_K2 \times G \quad (1)$$

$$D_{\{pub\_K,pr\_K\}}(E\_DATA) = E\_DATA - pr\_K2 \times pub\_K1 = E\_DATA - pr\_K2 \cdot pr\_K1 \times G \quad (2)$$

here:

DATA – plaintext;

E_DATA – cypher text;

pub_K1, *pub_K2* – public keys assigned to objects 1 and 2;

G – generic curve point;

pr_K1, *pr_K2* – private keys assigned to objects 1 and 2;

+ - addition function for elliptic curve points;

× - multiplication of elliptic curve point by a number.

DATA, E_DATA, *pub_K1*, *pub_K2* and *G* are elliptic curve points.

Any pair of objects can use (1) and (2) principles to secure and authenticate the mutual traffic. This mechanism is good enough for point – to – point communications, but it excludes broadcast mode and leads to significant traffic increase for multiparty information interchange.

A combined use of symmetric and two-key cryptographic algorithms is proposed to overcome this problem. Broadcast mode security should be organized over a symmetric cryptographic algorithm, and a two-key cryptographic algorithm should be used for group key exchange.

GROUP GENERATION PROTOCOL

- Each object beyond the radio access periodically broadcasts its identifier (e.g. ICAO address) as a plaintext (unencrypted), the message format should be as follows (Fig. 1):

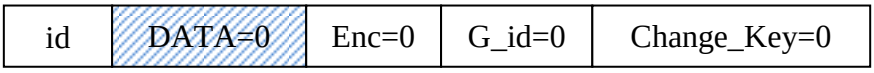


Fig.1 "message №0"

id – object identifier;

DATA – data field;

Enc – cryptographic algorithm type (0 – two-key, 1 - symmetric);

G_id – group identifier, sharing one symmetric key. Time stamp of key generation moment is strongly recommended to use as G_id;

Change_Key – key change flag: 0 - information, 1 - key change.

- When an object comes to radio access zone of another object and receives message of "message №0" type it should check the legality of the received identifier originator object position according to the flight schedule and inform the controller about any incorrectness. Then the object 1 should generate a common key M, encrypt it by its own private key and peer object 2 public key according to (1) and send it to object 2 within the message of "message №1" type (see Fig. 2). Time stamp of key generation moment is strongly recommended to use as G_id1.

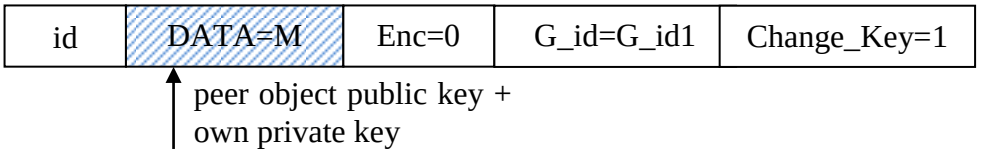


Fig.2 "message №1"

- On reception of this message ("message №1" type) object 2 should also check the legality of the object 1 position, get object 2 public key from the database and decrypt the common key M according to (2). Thus objects 1 and 2 share the key M and group identifier G_id1 and can use them to encrypt and decrypt data (e.g. position report *koords*) in DATA field using symmetric cryptographic algorithm; the message format should be "message №2" as follows (Fig. 3):

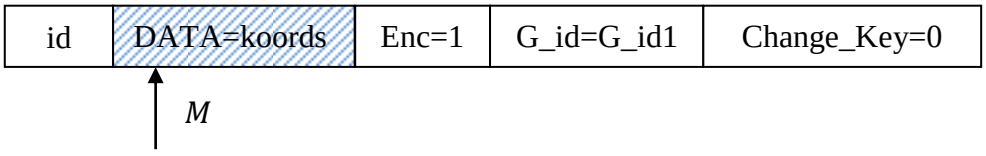


Fig.3 "message №2"

- Thus the group is generated. Fig. 6 illustrates the Group generation protocol.

GROUP ENTRY PROTOCOL

- Each object (e.g. object 1) beyond the radio access periodically broadcasts its identifier (e.g. ICAO address) as a plaintext (unencrypted), the message format should correspond to “message №0” (Fig.1):
- When an object 1 comes to radio access zone of another object (object 2) and object 2 belongs to some group and has already got a key M and a group identifier G_id2, object 2 should check the legality of object 1 position and reply to object 1 by a message of "message №3" type (see Fig. 4).

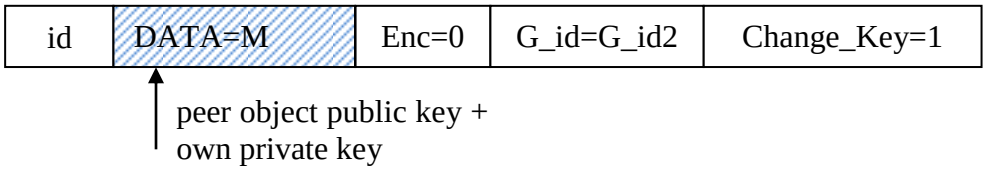


Fig.4 "message №3"

- On reception of this message ("message №3" type) object 1 should also check the legality of the object 2 position, get object 2 public key from the database and decrypt according to (2) and accept the common key M and group identifier G_id2. Thus objects 1 shares the common key M of the object 2 group and group identifier G_id2.
- Thus object 1 gets group entry. Fig. 7 illustrates Group entry protocol.

GROUP UNITE PROTOCOL

- Each object, e.g. object 1, which is the member of a group and shares common key M1 of a group and group identifier G_id1 should broadcast periodically messages of "message №2" type.
- When object 1 comes to radio access zone of another object, e.g. object 2, and object 2 belongs to another group and shares a common key M2 and a group identifier G_id2 of this group than the new

common key M3 and group identifier G_id3 should be generated and shared between all the members of both groups (after mutual check of position legacy).

- Thus two different groups are united into one new group sharing the new common key M3 and group identifier G_id3. Fig. 8 illustrates Group unite protocol.
- The new common key M3 should be calculated as M3 = M1 XOR M2.
- Key M1 should be transmitted by object 1 to object 2 within a message of "message №3" type; the same way key M2 should be transmitted by object 2 to object 1.
- Key M1 should be used by object 1 and key M2 – by object 2 to share the new key M3 between the members of their groups within a message of "message №4" type (see Fig. 5).

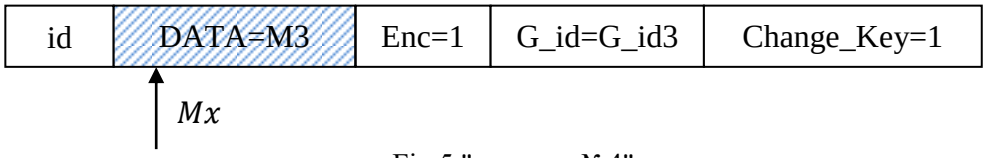


Fig.5 "message №4"

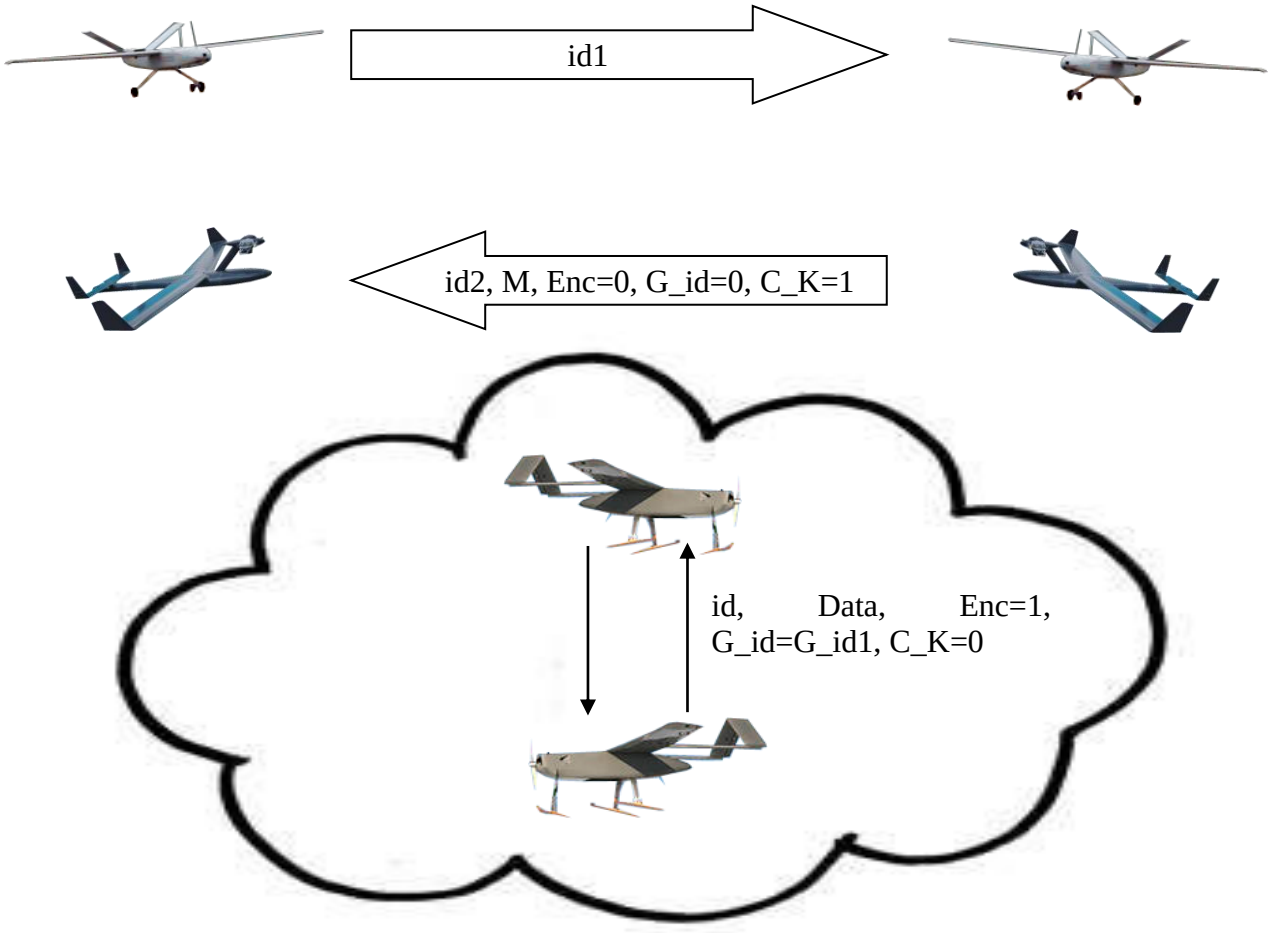


Fig.6 Group generation protocol

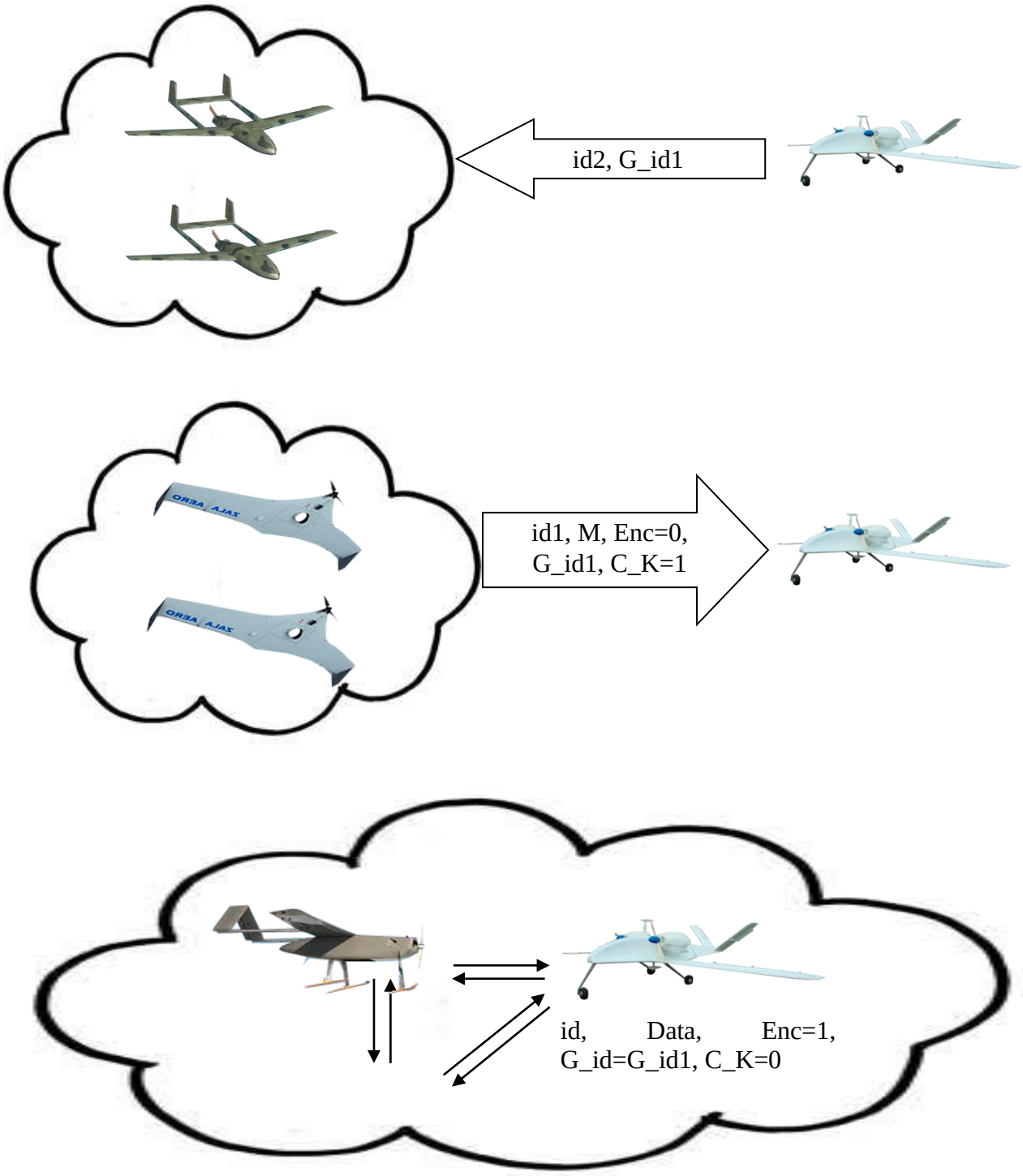
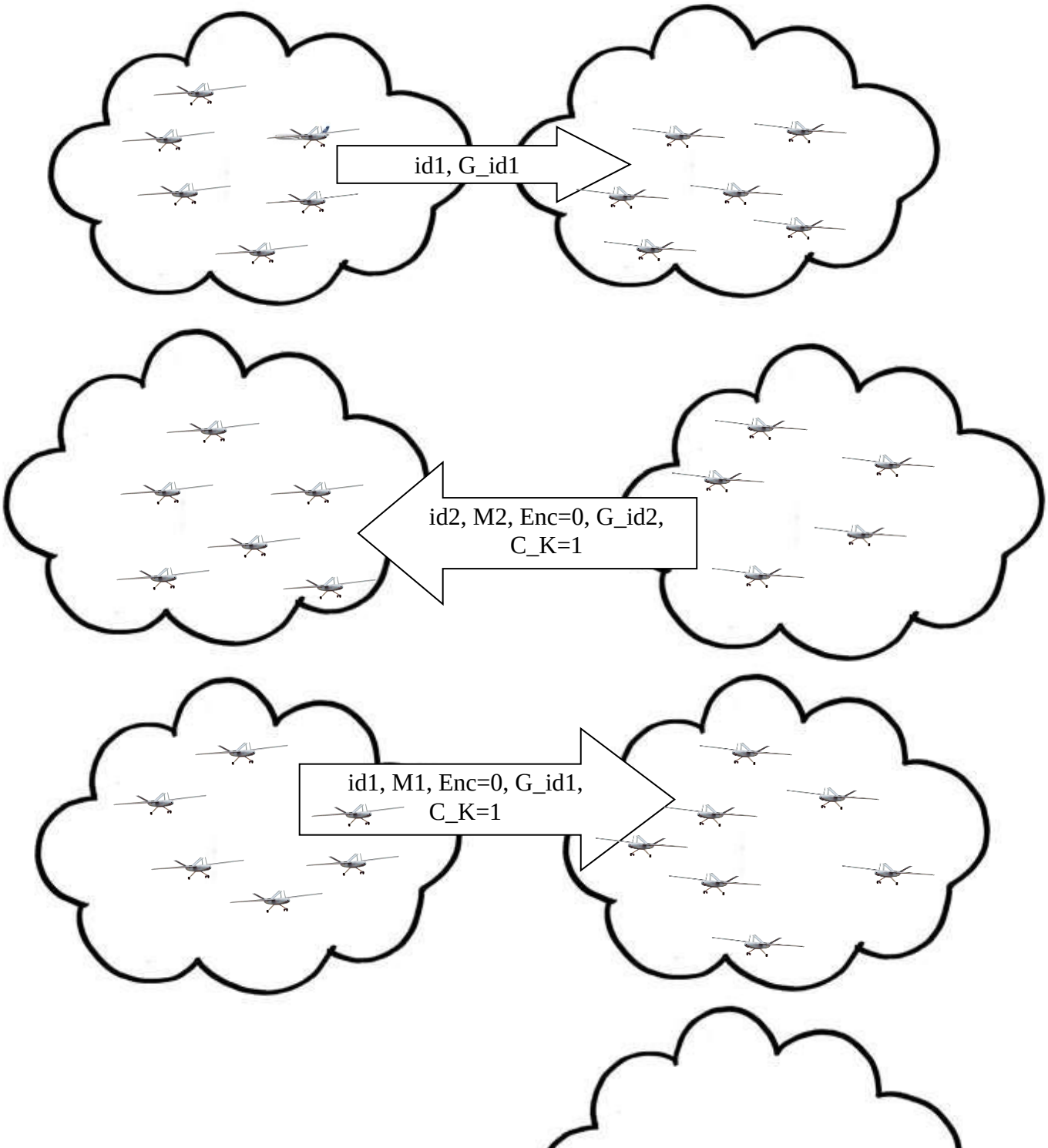
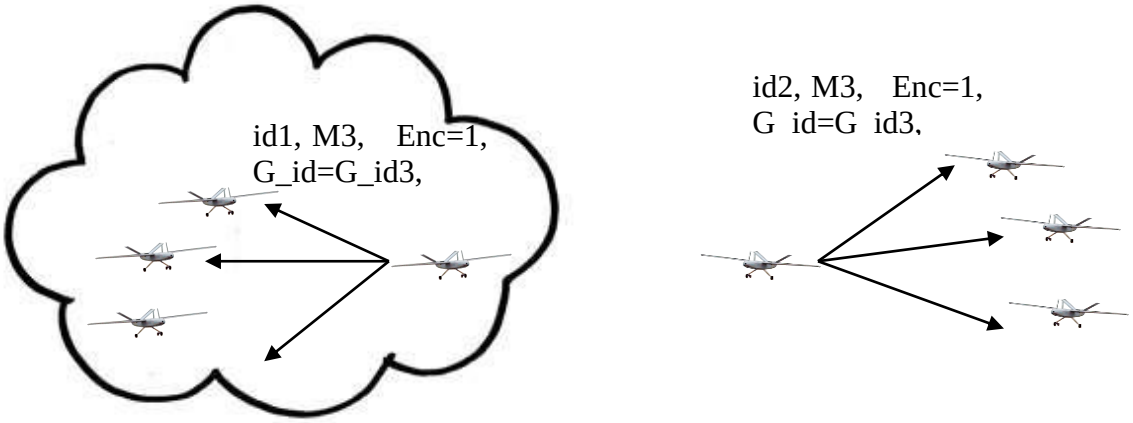


Fig.7 Group entry protocol





3. ACTION BY THE MEETING

The RPASP WG 2 is invited to:

a) note and review the contents of this working paper;

b) agree that WG 2 continue its work on this proposal.

— END —