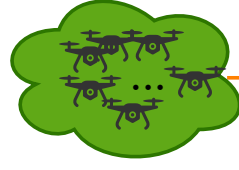


UAVs



M_3
 M_3
...

m different M_3 from
 m different UAVs

GAKA

Step 1

Choose current timestamp T_{cur}^2 and check if $|VT_3 - T_{cur}^2| < \Delta t$?
If yes, then calculate:
 $wt_j^* = H(PID_j || \sigma_j || B_j^* || Ch_1 || \dots || Ch_K || VT_0 || RID_i || VT_3) || H(T_{\rho^{a_i}}(PK_j))$,
 $D_i = T_{\rho^{c_i}}(B_j^*) \bmod q$.
Verify the authenticity of each drone's identity using the following formula:
 $H(T_{\rho^{c_i+wt_1^*}}(VP_1)) || T_{\rho^{c_i+wt_2^*}}(VP_2) || \dots || T_{\rho^{c_i+wt_m^*}}(VP_m) \stackrel{?}{=} H(D_1 || D_2 || \dots || D_m)$

Step 2

ECV_i then calculates the session keys with these m drones:
 $SK_i^j = H(C_i || D_i || wt_j^*)$,
Select partial session key $psk \in \mathbb{Z}_q^*$ and compute:
 $GSK = T_{\rho^{H(D_1 || D_2 || \dots || D_m || psk)}}(\omega) \bmod q$, $VP_i = T_{\rho^{c_i - wt_j^*}}(\omega) \bmod q$
Retrieve the current timestamp VT_4 and broadcast the message to all drones:
 $M_4 = \{VP_i, VT_4\}$

Step 3

After receiving M_4 , each drone selects current timestamp T_{cur}^3 to verify if
 $|VT_4 - T_{cur}^3| < \Delta t$? If yes, then verify the legitimacy of ECV_i :
 $H(T_{\rho^{b_j+wt_j}}(VP_i)) \stackrel{?}{=} H(T_{\rho^{b_j}}(C_i))$, if yes, then calculate:
 $D_i^* = T_{\rho^{b_j}}(C_i)$, $SK_j^i = H(C_i^* || D_i^* || wt_j)$

Procedural explanation

Calculate the share based on the procedure outlined in Algorithm 1,
compute $r(x) = E_0 + E_1x + E_2x^2 + \dots + E_tx^t \bmod q$, $x = Ch_1^j$,
broadcast $[g^{share_1^1} h^{r(Ch_1^1)}, \dots, g^{share_1^m} h^{r(Ch_1^m)}]$,
Retrieve the current timestamp VT_5 and broadcast the message to all
drones (take U_j as an example for illustration):
 $M_5 = \{SEN(SK_i^j)[share_1^j || VT_5]\}$

Shares
computation

Procedural explanation

After receiving M_5 , each drone computes $SDE(SK_j^i)[M_5] = \{share_1^j, VT_5\}$
Selects current timestamp T_{cur}^4 to verify if $|VT_5 - T_{cur}^4| < \Delta t$?
If yes, then choose a polynomial ($z(\cdot)$) of degree $m - t - 2$
Check: $\prod_{j=1}^m v[j]^{z(j) \cdot \lambda_j} \stackrel{?}{=} 1_{\mathbb{G}}$, $v(j) \stackrel{?}{=} g^{share_1^j} h^{r(Ch_1^j)}$

Shares
verifiability

Procedural explanation

$p(x) = \sum_{j=1}^{t+1} [share_1^j] \prod_{k=1, k \neq j}^{t+1} (\frac{x - Ch_1^k}{Ch_1^j - Ch_1^k}) \bmod q$
 $GSK = p(0) = D_0 = T_{\rho^{H(D_1 || D_2 || \dots || D_m || psk)}}(\omega) \bmod q$

Key
recovery

The recovery of GSK requires the participation of no fewer than
 $t + 1$ UAVs, in accordance with the threshold mechanism.