*Message\_1 = E({IDa, IDg, M1, M2, TSi}, KGAi)*

*Where, E is the encryption algorithm*

*KGAi is the ith group key*

*IDa is the unique identity of device, A.*

*IDg is the identity of gateway node, G.*

*M1 = H(IDa || TSi) ⊕ Na*

*M2* ***=*** *H(IDa || IDg || TSi, Na)*

*Message\_2 = E({IDg,IDa,M3,M4,Ng,TSj}, KGA)*

*Where, IDg, IDa, Na, H, ⊕ and || are same as that of Message\_1 components.*

*M3 = H(IDg || TSj) ⊕ Ng*

*M4 = H(IDg || IDa || TSj || Ng ||Na)*

*H is the hash function commonly agreed between A and G.*

*TSi is the Timestamp value when A sends the Message\_1. Na is the nonce value generated randomly by the device, A. ‘⊕’ denotes the XOR operator and ‘||’ denotes concatenation. TSj is the timestamp at which G sends Message\_2 to A. Ng is the nonce generated randomly by the gateway node, G.*