Green Multi Service IoT

Sécurité et Technologies Informatiques

Année 2021

Option : ……4AS……

Nom du stagiaire : …Ramy Chemak……

Tuteur(s) laboratoire : Hicham Lakhlef **Tuteur Ecole:** Pascal Berthome

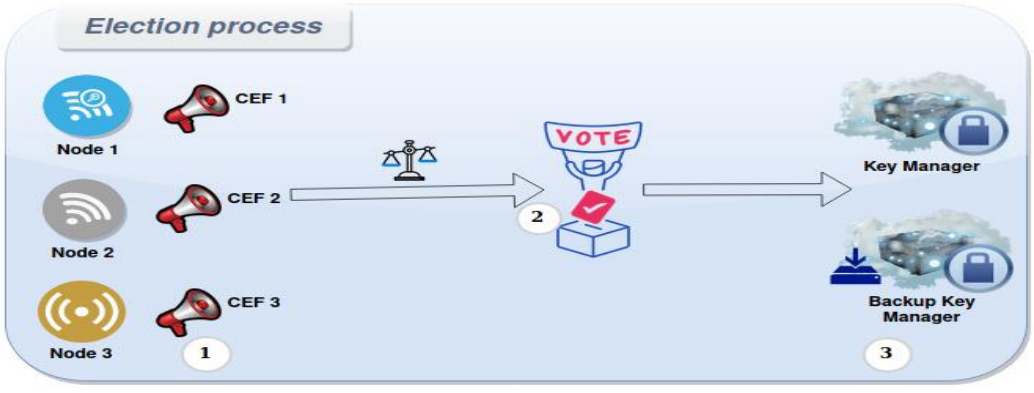
Problem description

Group Key Management (GKM) infrastructure is largely used in IoT networks to safeguard exchanged data between different Things. Network members are subdivided into different logical groups. The Key Manager (KM) provides each node its secret cryptographic keys, which will be used to encrypt the node's communications. The KM is regarded as the backbone component of the whole GKM architecture. In case of its breakdown or compromise, the whole security infrastructure is jeopardized.

Election-based scheme

Election process

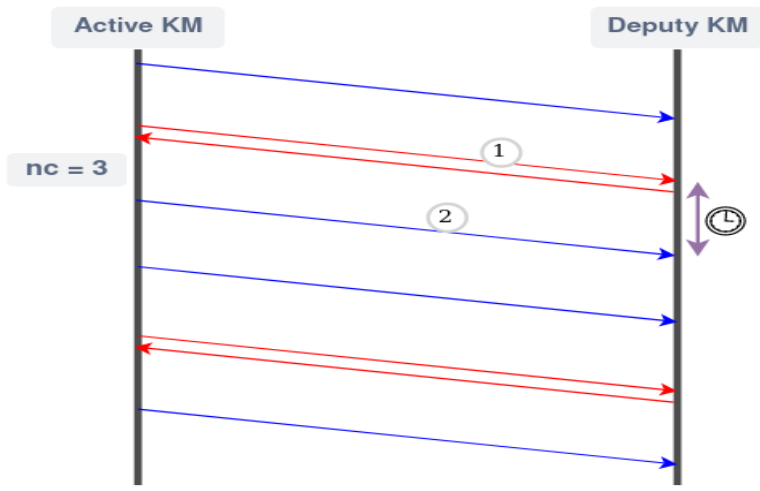
We define the capacity evaluation function (CEF) score. It aggregates the node's storage, networking, processing and energy capacities. Based on the CEF score, each group elects a Key Manager and a Deputy KM. Which means that instead of having a single KM managing the while network, we get one capable KM for each group, and a deputy ready to take over in case of an emergency. Thus makes the solution more decentralized and scalable.



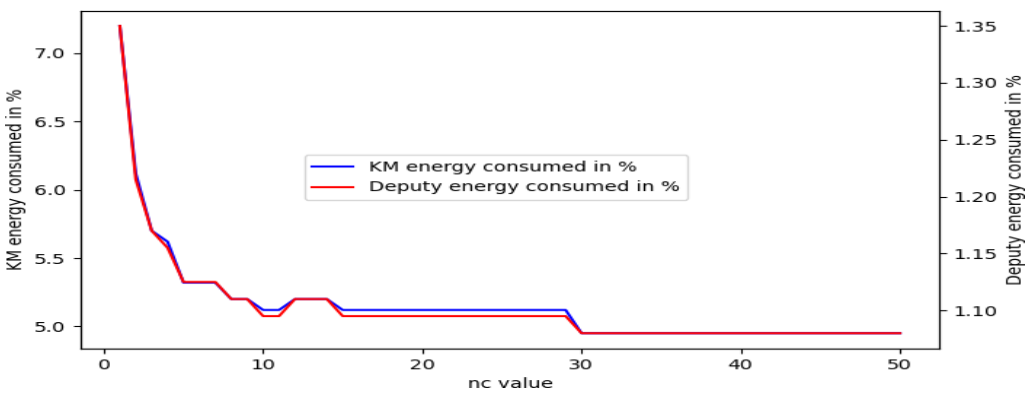
The election process takes place every time the current KM has to be substituted.

Failure recovery process

To ensure the permanent availability of a KM, we introduce the check-over process. This process unfolds through a simple check-over to guarantee availability (more performing), or a double check-over to guarantee availability and integrity (more secure). The checks occurs regularly, and the energy-security compromise is also configurable via a parameter *nc*.



Simulations



Tests simulating the solution's algorithmic behavior were carried out. Simulation results show a fast energy gain between *nc=5* and *nc=10*. Hence, the solution can quickly reach a satisfactory performance-security compromise for the KM.