Decentralized group authentication with membership verification in the Smart Grid.

Wilson Daubry

08/11/2022

CyberExcellence

Table des matières

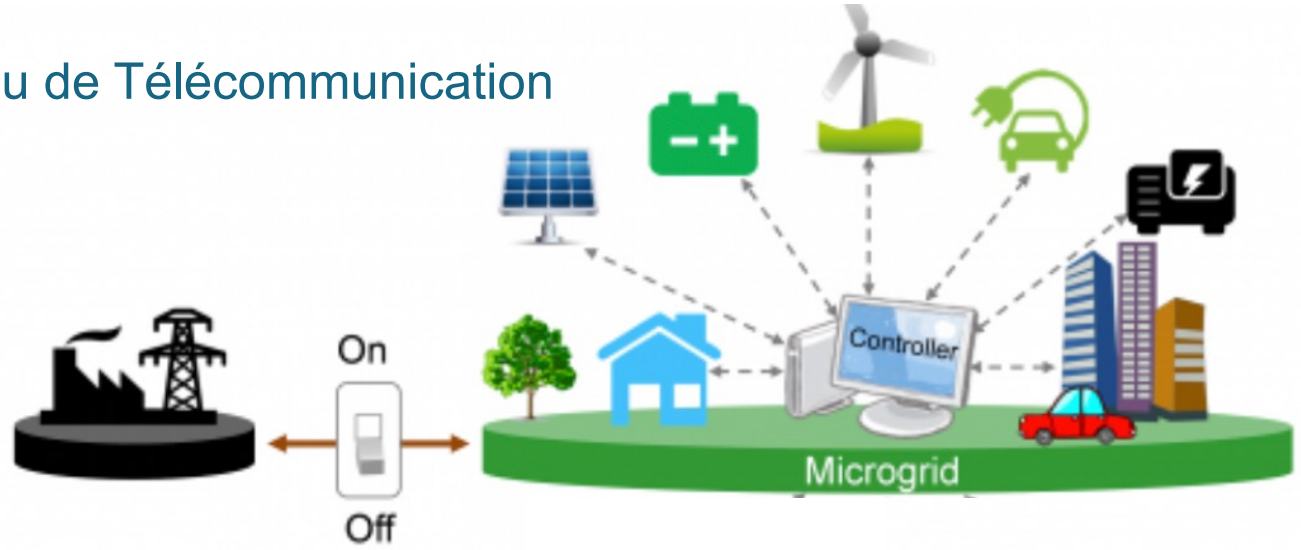
CYPRESS

1. Introduction – Réseau électrique & ilotage

Electrique :

- Réseau de Transmission
- Réseau de Distribution

Réseau de Télécommunication



[1] National Renewable Energy Laboratory. https://www.nrel.gov/. 2022.

CYPRESS

1. Introduction - Ilotage

Objectif :

Permettre une continuité des opérations en ilotage

Problème :

Autorité de Certification inaccessible -> Plus de serveur central

Défis principaux :

(I) Comment assurer l'authentification des nœuds du réseau ?

(II) Comment détecter et prévenir des tentatives de connexion malicieuses ?

CYPRESS

2. Preliminaires

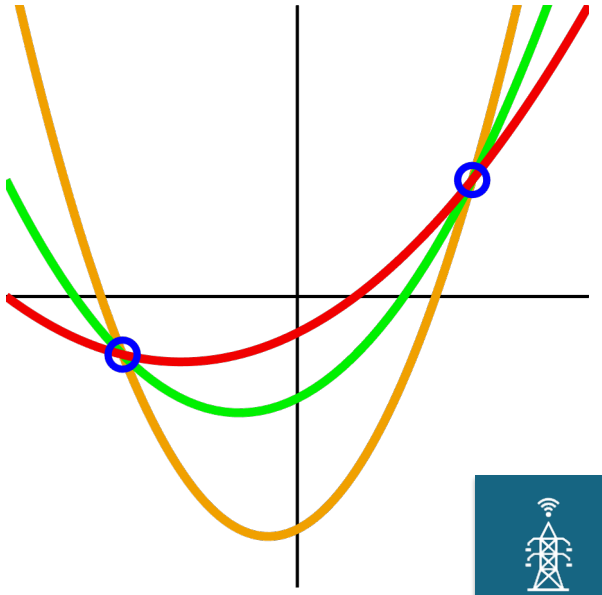
- Shamir's Secret Sharing [2]

Comment partager un secret, et protéger sa reconstruction ?

$$f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \; mod \; p$$

Chaque membre : $M_i \rightarrow f(x_i)$

$$s = f(0) = \sum_{i=1}^{t} f(x_i) \prod_{r=1, r \neq i}^{t} \frac{-x_r}{x_i - x_r} mod \; p$$



[2] Adi Shamir. 1979. How to share a secret. Commun. ACM 22, 11 (1979), 612–613.

CYPRESS

2. Préliminaires

- Authentification de groupe proposée par Harn [3]

Construction basée sur Shamir avec des propriétés supplémentaires :

(I) Partage asynchrone des secrets partiels possible.

(II) Les secrets partiels sont camouflés avant d'être partagés.

(III) La connaissance du secret reconstruit n'est pas suffisante pour forger des secrets partiels

$$s = \sum_{j=1}^{k} d_j f_j(w_j)$$

Secret = Combili de plusieurs points de fonction polynomiales

$$c_i = \sum_{j=1}^{k} d_j f_j(x_i) \prod_{r=1, r\neq i}^{m} \frac{w_j - x_r}{x_i - x_r} \bmod p$$

Un coefficient de Lagrange est produit et partagé par les nœuds

$$s' = \sum_{r=1}^{m} c_r \bmod p$$

Le secret global est reconstruit grâce aux coefficients de Lagrange

Tout membre ayant donné un coefficient c_r valide est authentifié.

Quid si c_r incorrect ?

[3] L. Harn. "Group authentication". In: IEEE Transactions on computers 62.9 (2012), pp. 1893–1898.

CYPRESS

2. Préliminaires

- Lightweight Verifiable Secret Sharing [4]

  Basé sur les propriétés du '*Nyberg's one-way accumulator for one-way hash function*'

  (I) Quasi-commutativité : $H(H(\alpha,\beta),\gamma) = H(H(\alpha,\gamma),\beta)$

  (II) Absorbance : $H(H(\alpha,\beta),\beta) = H(\alpha,\beta)$

  On peut donc créer un vérificateur tel que :

$$V = H(\dots H(H(k,s),s_1)\dots,s_n)$$

  Avec s : le secret, s_i un secret partiel et k une constante.

Si pour un secret $s_m \rightarrow V = H(V,s_m)$, alors le secret partiel testé appartient au secret global.

[4] Likang Lu and Jianzhu Lu. 2022. A Lightweight Verifiable Secret Sharing in Internet of Things. International Journal of Advanced Computer Science and Applications 13, 5 (2022)

CYPRESS

3. Protocole proposé

- Trois phases principales

  (I) Préparation

  En opération normale. Préparation et distributions des secrets partiels, secret hashé, moyens de vérifications aux différents membres.

  (II) Restauration

  Quand l'ilotage survient. Tentative de reconstruction du secret avec la participation d'un maximum de noeud de l'ilot.

  (III) Identification des noeuds malicieux

  Détermination sur base de la théorie des graphes.

CYPRESS

3. Protocole proposé

- Trois phases principales

(I) Préparation

En opération normale.

Préparation et distributions des secrets partiels, secret hashé, moyens de vérifications aux différents membres authentifiés.

(II) Restauration

Quand l'ilotage survient.

Tentative de reconstruction du secret avec la participation d'un maximum de noeuds de l'ilot.

CYPRESS

3. Protocole proposé

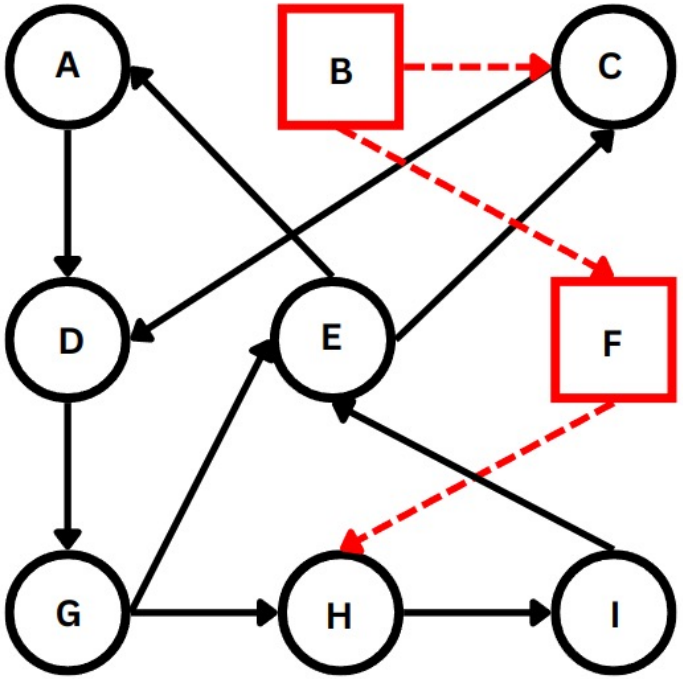
- Trois phases principales

(III) Identification de nœud(s) malicieux.

Processus itératif. Les nœuds choisissent aléatoirement un autre nœud et vérifient son authenticité. Il propage son résultat ensuite.

Construction d'une chaine de confiance.
$Si\ A \rightarrow B\ et\ B \rightarrow C\ alors\ A \rightarrow C$

Les membres authentifiés font ensuite partie d'une même boucle.



4. Conclusion et évolution

Un mécanisme d'authentification décentralisée est proposé.

Il permet d'authentifier les nœuds dignes de confiances.
Il permet d'identifier et d'écarter les nœuds malicieux.

Pistes à explorer :

* Utilisation de *Physical Unclonable Function* pour créer les secrets de groupe.
* Dérivation de clés de groupe en parallèle de l'authentification des messages.
* Analyse de l'efficacité d'une implémentation du système.

CYPRESS

CYPRESS