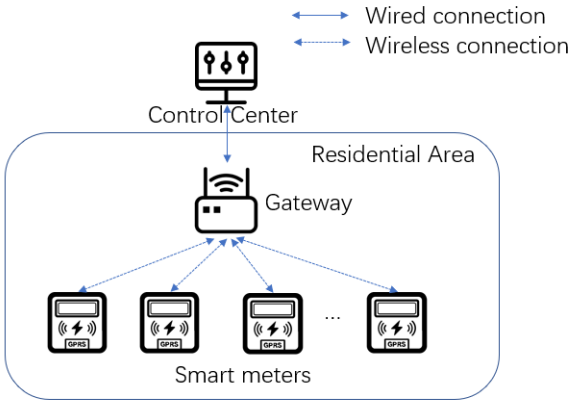
MSDA：Multi-subset Data Aggregation Scheme without Trusted Third Party

Zhixin ZENG, Xiaodi WANG, Yining LIU, Liang CHANG

Frontiers of Computer Science, DOI: 10.1007/s11704-021-0316-x

Problems & Ideas

- Problems of privacy-preserving data aggregation protocol in the smart grid
  - only obtain the sum or average in an area while more fine-grained data brings more value for data consumers
  - depend on a trusted third party to initialize system parameters which is hard to resist denial of service attacks
- Ideas: Multi-subset Data Aggregation Scheme without Trusted Third Party
  - users negotiate some secret keys for encryption using HMQV protocol
  - two super-increasing sequences are used for multi-subset aggregation
  - multi-subset aggregated data can be computed by Algorithm 1



- **System model**

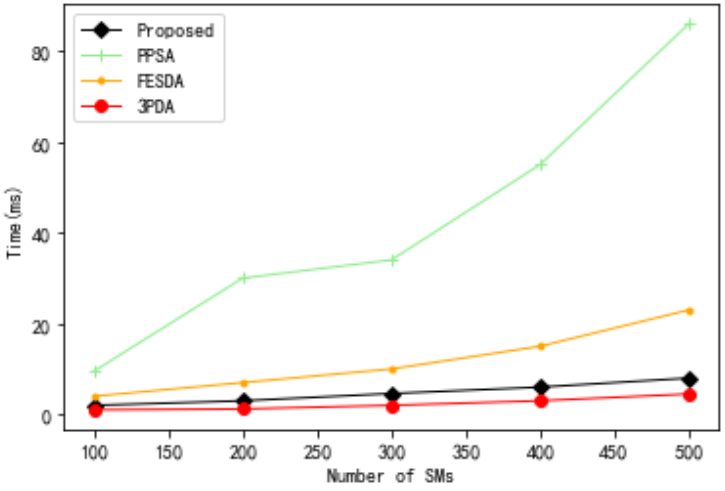
Algorithm 1: Deconstruction D at Control Center (CC)

procedure
Input: D, $\{b_1, b_2, \ldots, b_k\}$, $\{a_1, a_2, \ldots, a_k\}$, $\{R_1, R_2, \ldots, R_k\}$
Output: $\{|U_1|, |U_2|, \ldots, |U_k|\}, \{M_1, M_2, \ldots, M_k\}$
for (i = k; i > 0; i − −) **do**
    $|U_i| = (D - D \bmod b_i)/b_i$
    $D = D - (b_i \cdot |U_i|)$
end for
for (i = k; i > 0; i − −) **do**
    $M_i = (D - D \bmod a_i)/a_i$
    $D = D - (a_i \cdot M_i)$
    $M_i = M + R_i \cdot |U_i|$
end for
end procedure

- **Algorithm 1**

Main Contributions

- **Aggregation cost at GW**



- **Decryption cost at CC**