Do Not Snoop My Habits

Preserving Privacy in the Smart Grid
Outlines

- Introduction
- Motivation
- Privacy-preserving protocol for smart metering.
- Conclusion
Introduction

- The smart grid is promising upgrade for the electrical energy grid.
- Electricity suppliers receive more precise information about the state of their networks.
- Consumers are enabled to adapt their consumption behaviour according to the current supply situation.
Introduction

- More information about consumption patterns of energy consumers may contribute to forecasting about demand in the near future

- Smart meters are used to transmit up-to-date information to the electricity supplier in certain intervals, typically 15 minutes.
Motivation

But this approach threatens privacy. Even if assuming that all data transmitted from the consumer’s home is sent using a secure channel, the electricity supplier will receive much more personal data about the customers.

The paper focus on providing up-to-date and accurate aggregated information about the electricity consumption of a specific area to electricity supplier, without revealing information about individual customers.
Privacy-preserving protocol for smart metering

- Using homomorphic encryption mechanism, the energy supplier will decrypt the aggregated measurement value without being able to decrypt individual smart meter's measurement.

- Homomorphic encryption is a form of encryption which allows specific types of computations, addition or multiplication, on plaintexts to be carried out on ciphertext.

- Suppose we have plaintext messages $x_1, x_2$, then $E(x_1) + E(x_2) = E(x_1 + x_2)$

- So one person could add two encrypted numbers, and another person could decrypt the summation without being able to find the value of the individual numbers.
Privacy-preserving protocol for smart metering

- Groups of smart meters are formed, smart meters in the same building, or in the same street or neighbourhood.

- Each smart meter creates its private key to encrypt its measurement

- One smart meter per group is assigned to be the key aggregator
Privacy-preserving protocol for smart metering

- The key aggregator has received all the group members’ keys. It aggregates the keys to obtain key $K$ and sends it to the electricity supplier ES through a secure channel.

- Nobody except the key aggregator knows other members’ keys

Key $K$ is sent to the ES only once when the system established.
Privacy-preserving protocol for smart metering

- Each smart meter encrypts its consumption measurement using its current key and sends it directly to the ES through a secure channel.

- The ES aggregates the encrypted consumption values.

- Using the aggregated key $K$, the ES decrypts the aggregated measurement (subtract $K$ from the aggregated encrypted value).
Privacy-preserving protocol for smart metering

- Each smart meter uses a different random key per period. However, the aggregated key $K$ remains constant.

- Every period, a smart meter in the group selects a random value. It subtracts this random value from its own key and sends that random value to its successor through a secure channel.

- This random value is added to the received smart meter’s key.

- Each random value added to one smart meter’s key is therefore subtracted from another. So, the aggregated key remains constant.
Privacy-preserving protocol for smart metering

- Each smart meter, updates its key, sends the new one to the key aggregator.

- The key aggregator checks that the aggregation of received keys is equal to $K$ every round, for consistency.
Figure 2. Privacy enhanced architecture for smart metering.
Privacy-preserving protocol for smart metering

- If a smart meter within a group fails, or acts maliciously, sends its key without sending the corresponding encrypted measurement (or vice versa), the ES would not be able to decrypt received encrypted aggregation.

- To solve this problem, the authors propose an additional mechanism called “tokens solution” that would be enabled in the round where this threat is detected.
Privacy-preserving protocol for smart metering

- After the aggregator receives the keys for each smart meter, it generates a token for each key and sends them back to the corresponding smart meters.
- Each smart meter reports its encrypted measurement with its token to ES. The ES sends an acknowledgement message for each measurement received with a token to the aggregator.
- The aggregator aggregates only the keys acknowledged by the ES to obtain the key $K$. 
Conclusion

- This article proposes a privacy-aware protocol based on homomorphic encryption.
- The protocol allows the electricity supplier to access the aggregated consumption information, but hides the individual measurements.
- The proposed solution enables the direct communication between smart meters and the supplier while preserving the privacy of the smart meter users.
- The scheme is better compared to the previous schemes, because it guarantees the privacy despite whether the aggregator is exposing the smart meters’ keys to the supplier or not.
Conclusion

• The scheme can deal with different group size large or small
• It can work well in case of missing reading.
• It does not cause a computation or communication overhead.
• As future work, the authors will perform a security analysis and evaluation of scalability for their suggested protocol.