Privacy and Performance Trade-off in Cyber-Physical Systems

Written by: Zhang, Heng, et al.

Presented by: Dev Shah

IEEE Network (Volume: 30, Issue: 2, March-April 2016)

How is privacy affected in CPS?

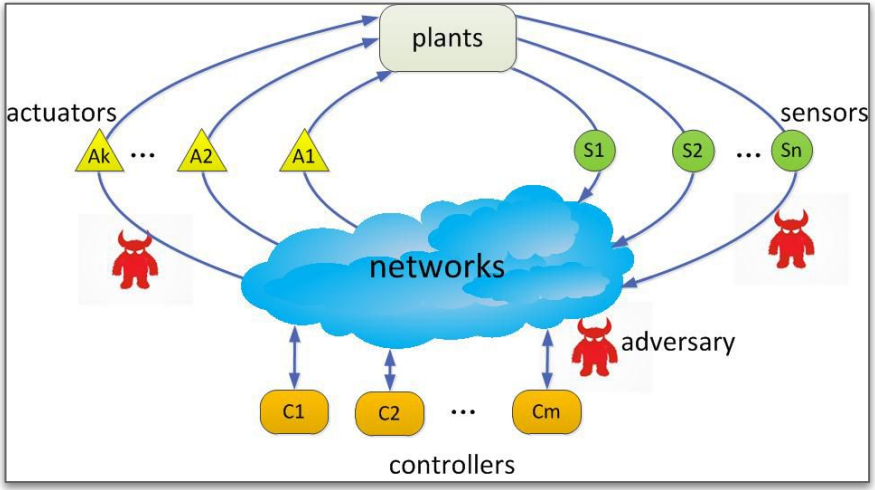
1. Employment of communication networks and heterogeneous IT elements.
2. Attackers can use Non-Intrusive Load Monitoring (NILM) techniques from smart meters.
3. In CPS, Encryption, can be hardly applied due to the limitation of sensors' computing capacity.
4. Brute-force attack can also be used by the adversary against any encrypted data.

What is differential privacy?

- Differential privacy is an effective privacy protection approach which prevent data recovery by adversaries.
- It is, essentially, a perturbation technique that conceals the original data with proper noises.
- Due to its significant advantages including easy realization and mathematical theoretical basis, differential privacy has been widely applied to preserve individual privacy in CPS.
- Individual can also sell his private information to corporations and get rewards when the privacy level of his information is measured by differential privacy.

System Architecture

- Plants - the physical systems
- Sensors - to observe the plants and get the information
- Controllers - to make decisions and issue control commands
- Actuators - to implement the control commands;
- Networks - the communication medium through which the plants, sensors, controllers and actuators exchange information with each other.



Implementation

- xk - state vector of physical plants at time k.
- Si - observes the state
- yi;k - observations sent to the controllers from sensors
- Cj - controller
- uj;k = fu(bxj;k) - control command sent to the actuators, where fu is the designed control law.
- J = J(u) - performance
- (ϵ, δ) - differential privacy is defined by probability inequality. From this definition, the original information is randomly mapped to a subset of the output range, and the adversary cannot infer the original information from the output dataset.
- The parameters ϵ, δ determines the privacy level. More privacy will be achieved when the parameters are closer to 0.

Implementation

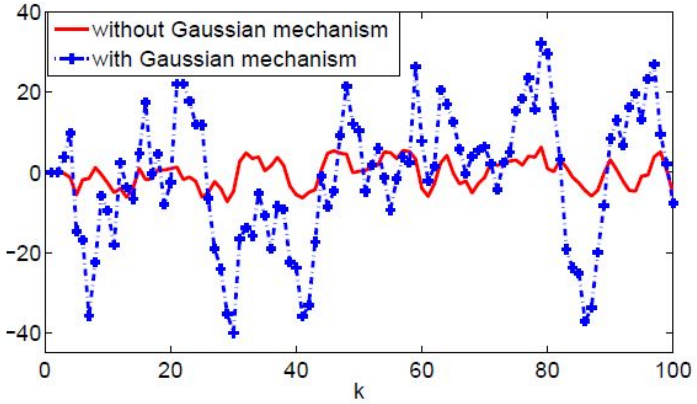
According to the differential privacy approach, we preserve the privacy by adding noises to the sensor's transmitting data and the control data in each time respectively.
Thus, the sensor transmitting data and control data will become -

$$\widetilde{y}_k = y_k + y_k^a, \text{ and } \widetilde{u}_k = u_k + u_k^a$$

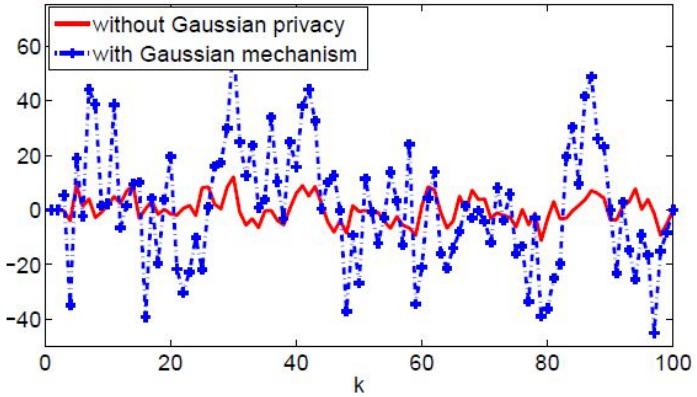
Advantages

- This approach is independent of the acquired background knowledge by the adversaries. It means that this method does not need to update when the new type attack appears.
- Another advantage is the solid mathematical definition which provides a rigorous and self-contained theory basis and quantitative evaluation method for privacy.

Results



(a) State estimate evolution with Gaussian mechanism versus those without Gaussian mechanism.



(b) Control data with Gaussian mechanism versus those without Gaussian mechanism.

Results

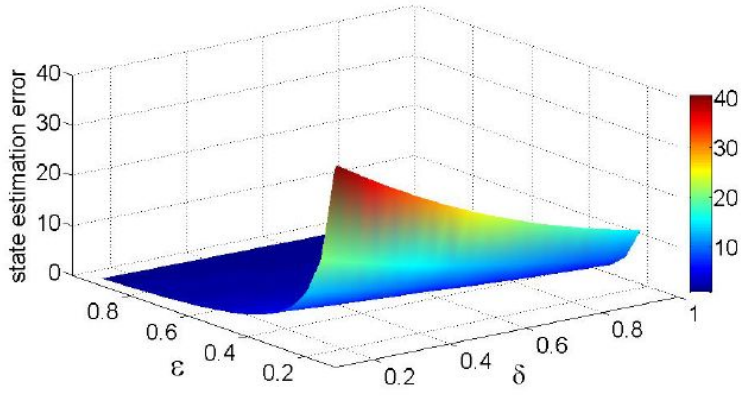
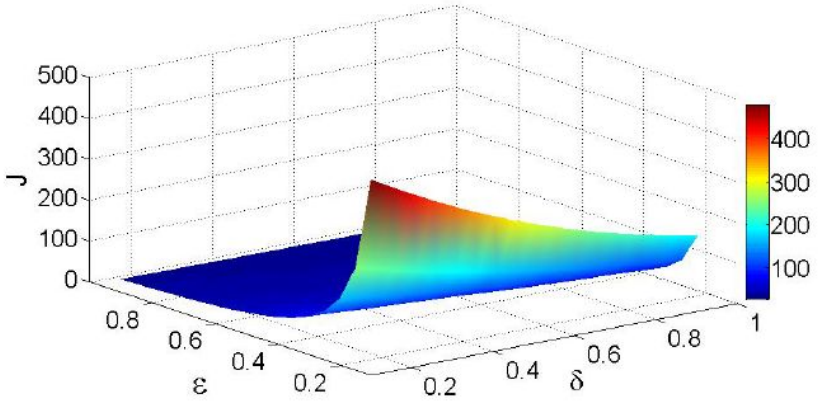
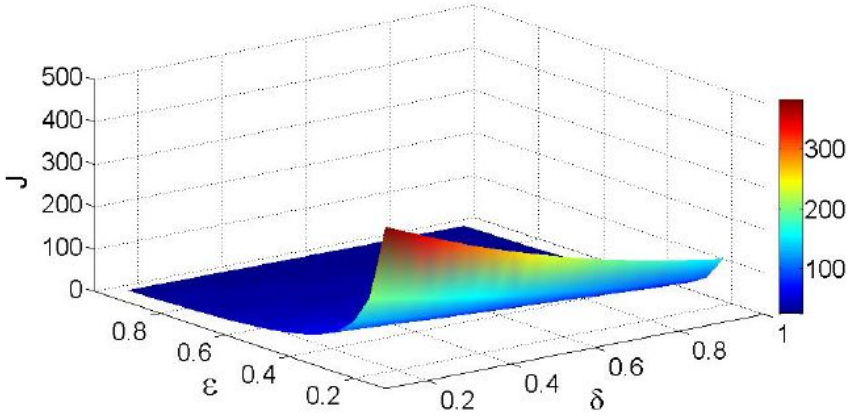


Fig. 3. State estimation errors under different privacy preserving requirements.



(a) The system performance J with Gaussian mechanisms at both sensor side and controller side.



(b) The system performance J with Gaussian mechanism at sensor side.

Future Scope

Here we identify three major challenges in this field in the future research:

- First, investigate the privacy preserving problem on more general system models. They only study the problem on a simple system in this article, and it is more challenging to balance the privacy requirement and system performance on complex CPS system.
- Second, need to further refine the privacy requirements, and design a more efficient privacy preserving mechanism to reduce the system cost.
- Third, jointly exploit feedback control technology and differential privacy mechanism to investigate new challenging issues of privacy in specific CPS systems, e.g., smart grid, social network systems. A challenging problem is how to balance the control performance and multiple privacy preserving requirements.

Questions?