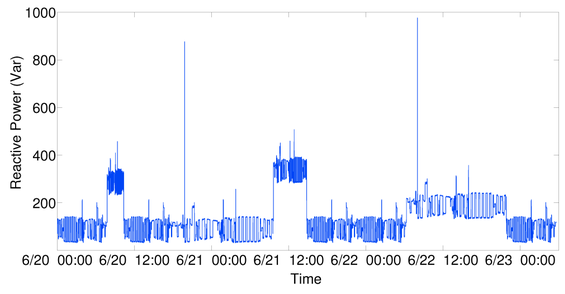
Privacy Disclosure Through Smart Meters: Reactive Power Based Attack and Defense

Jingyao Fan, Qinghua Li and Guohong Cao

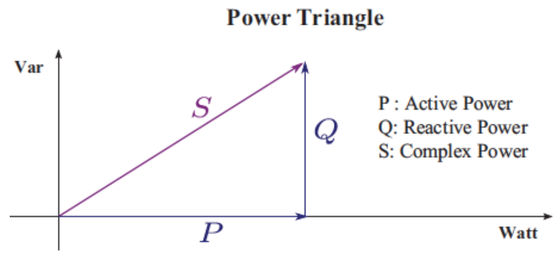
Introduction & Motivation

- **Smart Meters**
  - More and more widely deployed in households in US, EU and Asia
  - Can measure, store and upload richer and more fine-grained power consumption data: both active power and reactive power
  - Provide better energy efficiency and fault tolerance
- **Privacy Concerns**
  - Home appliances may have unique power consumption signatures
  - Fine-Grained power consumption data provided by smart meters can be used to infer home appliance usage
  - Appliances usage can be used to further infer user activities.



Reactive Load Profile

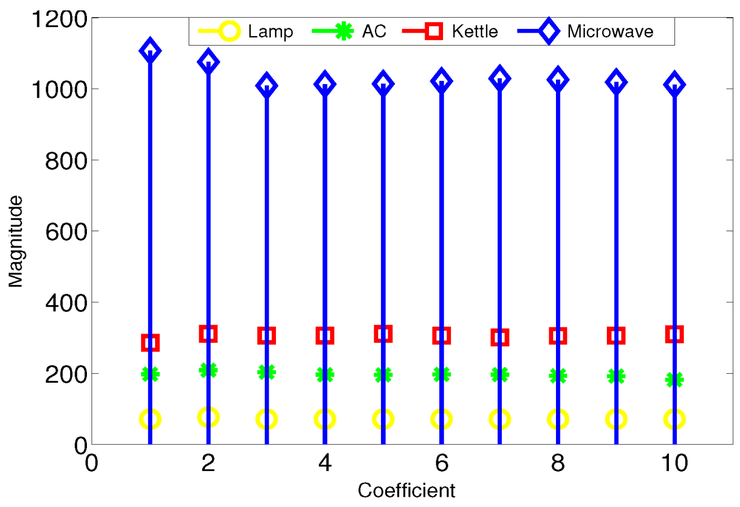
- **Existing solutions**
  - Attack: Use *active power* data to infer appliances usage
  - Defense: use load-controlled rechargeable batteries to mask the active power data from smart meters
- **Open Questions**
  - Smart meters provide both active and reactive power data
    - Active and reactive power are orthogonal
    - Battery-based defense does not affect reactive power
  - Whether the *reactive power data* **alone** can cause privacy leakage?
  - How to prevent such privacy leakage?



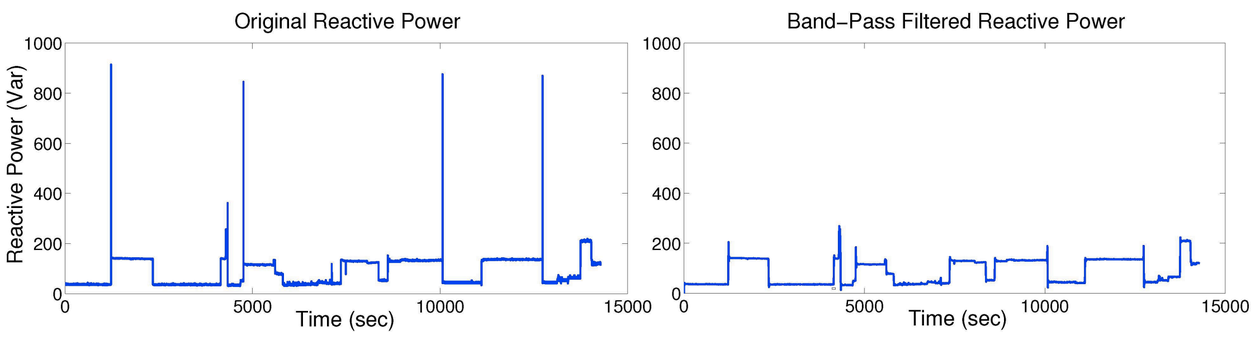
Relationship between active power and reactive power

Reactive Power–Based Attack

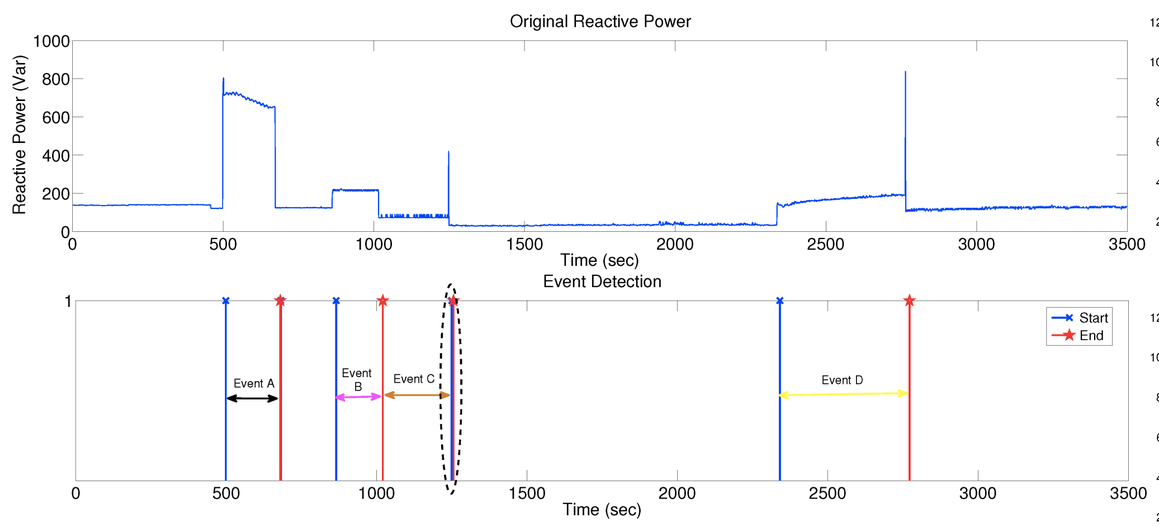
- **Attack Approach**
  - Appliance Signature Extraction: Wavelet transform on 1 min window use wavelet coefficients as signatures

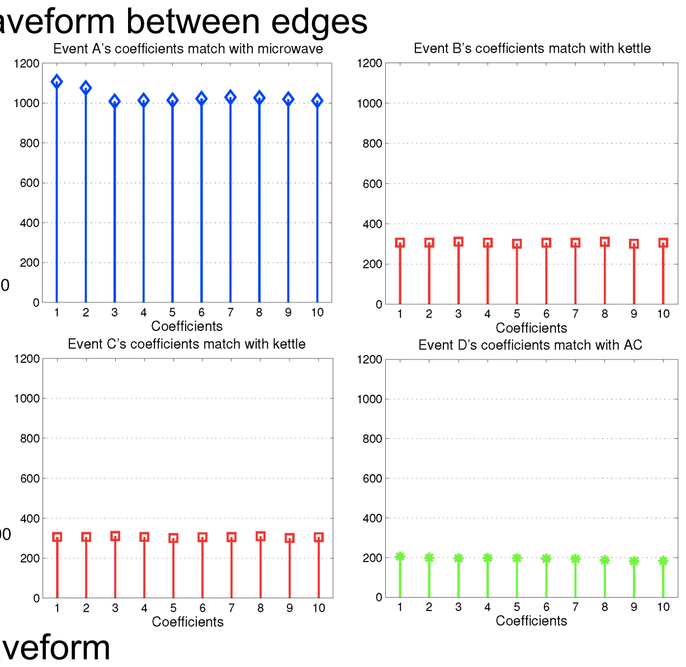


- Filtering:



- Event Detection: extract waveform between edges



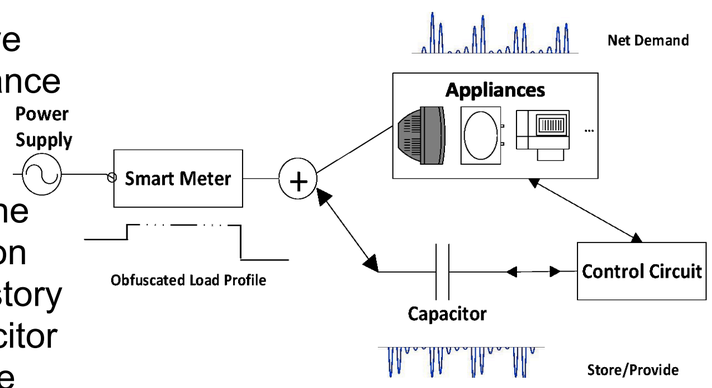


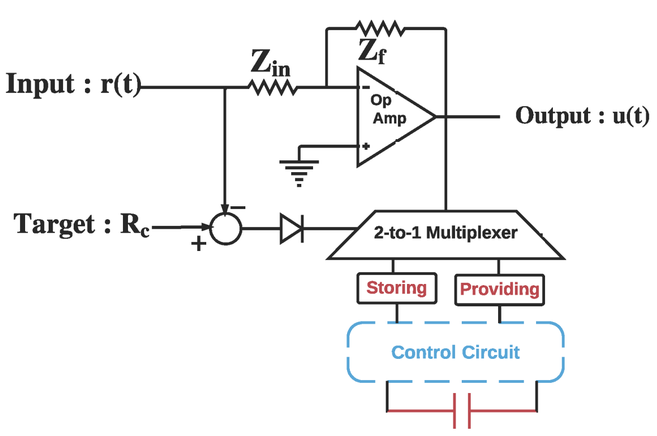
- Identification: Get wavelet coefficients of extracted waveform and match wavelet coefficients with appliance signatures
- **Experiments**
  - Compare identified appliance usage with user logged info
  - False Positive: OFF identified as ON
  - False Negative: ON identified as OFF

Appliances	Apt 1	
	False Positive	False Negative
Lamp	4.2%	5.8%
Refrigerator	11.7%	13.5%
Air Conditioner	14.5%	16.5%
Microwave Oven	1.3%	2.7%
Dishwasher	~0	2.6%
Kettle	1%	1.7%
Laptop	3.9%	5.6%
TV	3.3%	6.7%
Overall	5.8%	7.5%

Reactive Power-Based Defense

- **Reactive Power Obfuscation (RPO)**
  - General Idea: Use capacitors to store/provide reactive power in a controlled manner so that reactive power changes caused by appliance are obfuscated.
- **Design of RPO**
  - Initialization process: initializes the target reactive power *Rc* based on the household's power usage history and the capacitance of the capacitor
  - Maintaining process: maintain the net reactive power at *Rc*
    - Decision making module: store or provide?
    - Storing/Providing module: control the capacitor's action
  - Adjusting process: adjust *Rc* when the capacitor is unable to maintain the current reactive power at *Rc*
    - High demand: decrease *Rc*
    - Low demand: increase *Rc*





- **Experiments**
  - Compare original and obfuscated load profile

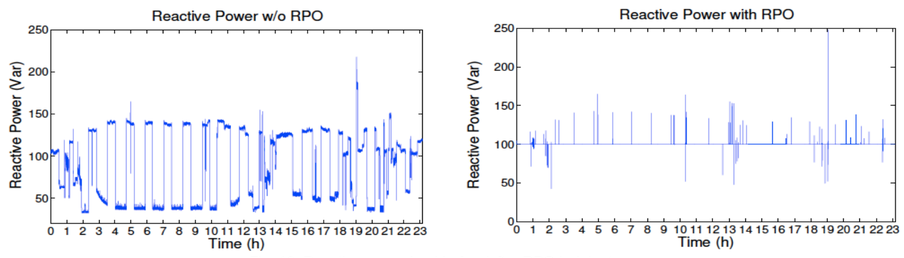


Fig. 10: Reactive power load before/after RPO is Adapte

- Effectiveness of mitigating the proposed attack: launch the attack against the original load profile and the obfuscated load profile

Appliances	detection rate of Apt 1			
	ON		OFF	
	No RPO	RPO	No RPO	RPO
Lamp	95.8%	1.2%	94.2%	1.4%
Refrigerator	88.3%	1%	86.5%	0.9%
AC	85.5%	0.8%	83.5%	0.5%
Microwave	98.7%	1.2%	97.3%	1.6%
Dishwasher	~1	2%	98.4%	1.6%
Kettle	99%	1.3%	98.3%	1.7%
Laptop	96.1%	0.9%	94.6%	1.3%
TV	96.7%	0.7%	93.3%	1%
Overall	94.2%	0.9%	92.5%	1.1%

Related Publications

[1] *"Privacy Disclosure Through Smart Meters: Reactive Power Based Attack and Defense" IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2017*