FUJITSU

shaping tomorrow with you

Evaluating Electricity Theft Detectors in Smart Grid Networks

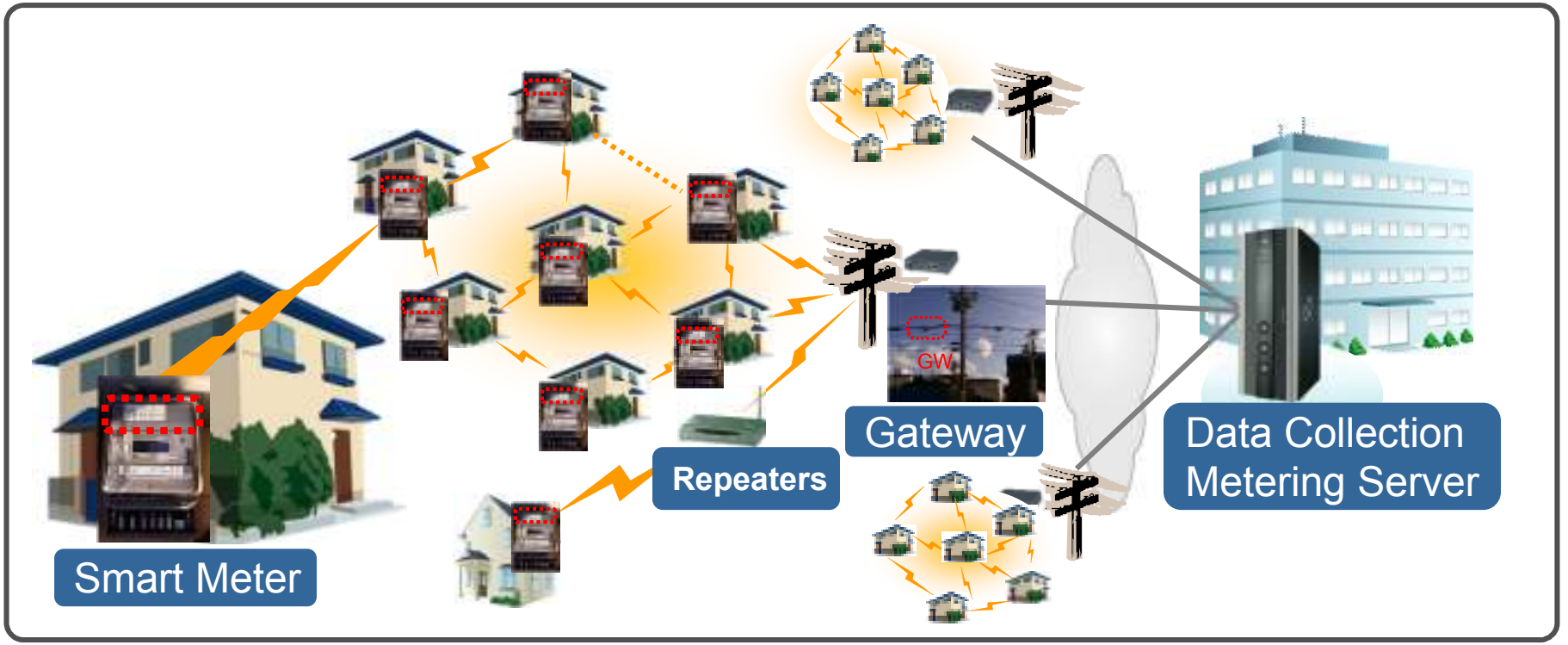
Daisuke Mashima
SEDN (Solutions for Electricity Distribution Networks) Group
Fujitsu Laboratories of America Inc.

Alvaro Cardenas
University of Texas, Dallas

Advanced Metering Infrastructure (AMI)

FUJITSU

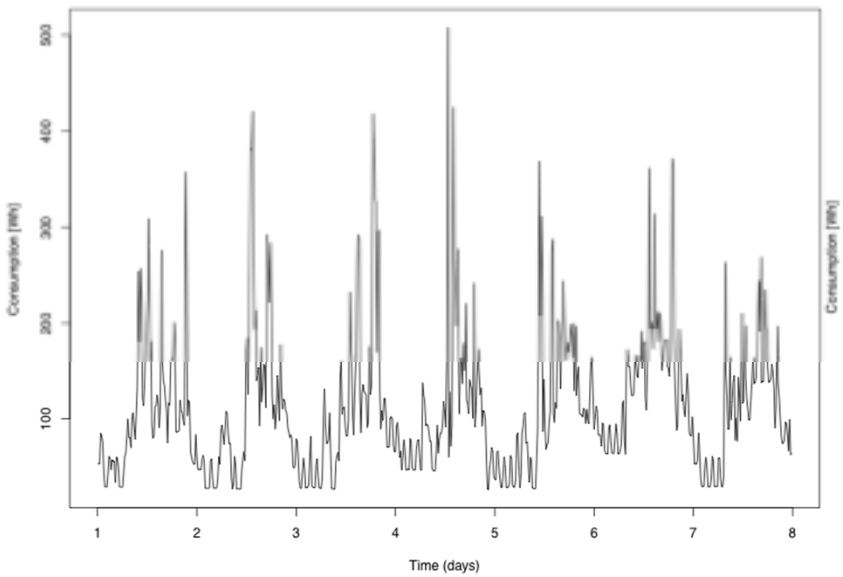
- Replacing old mechanical electricity meters with new digital meters
- Enables frequent, periodic 2-way communication between utilities and homes

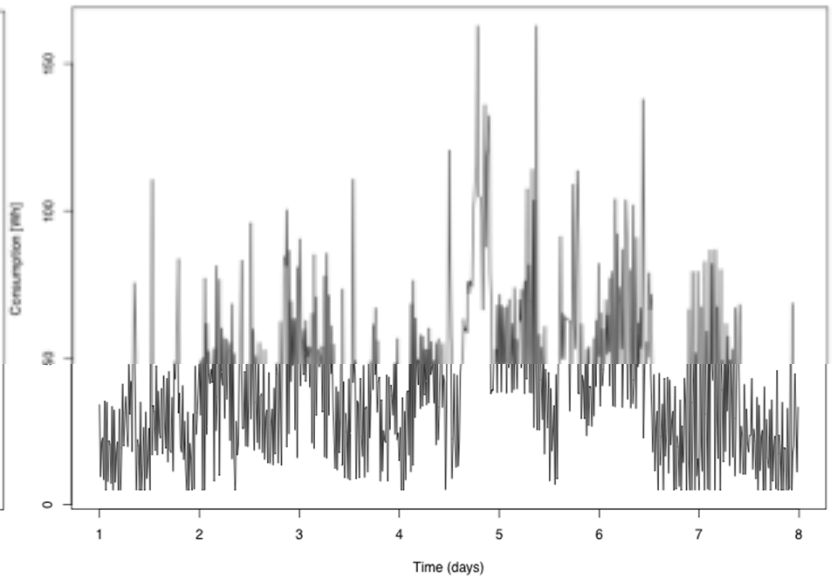


Electricity Consumption Examples

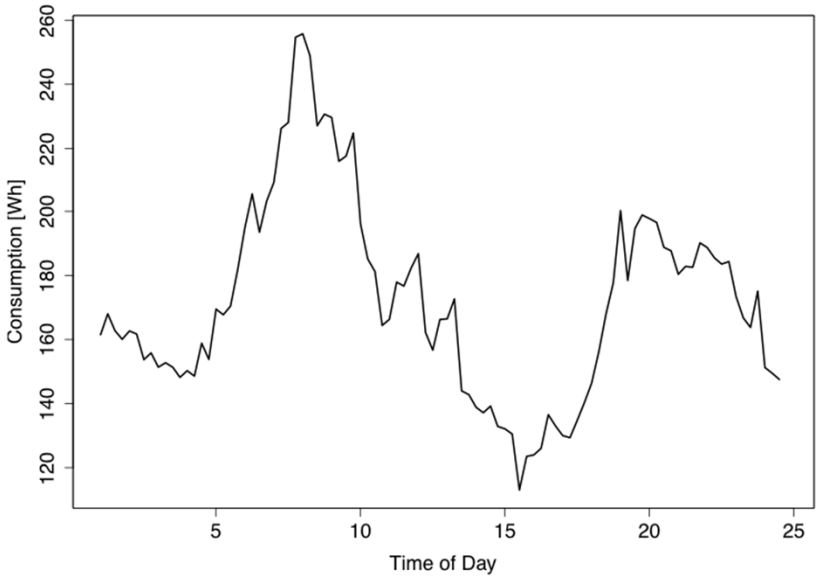
FUJITSU

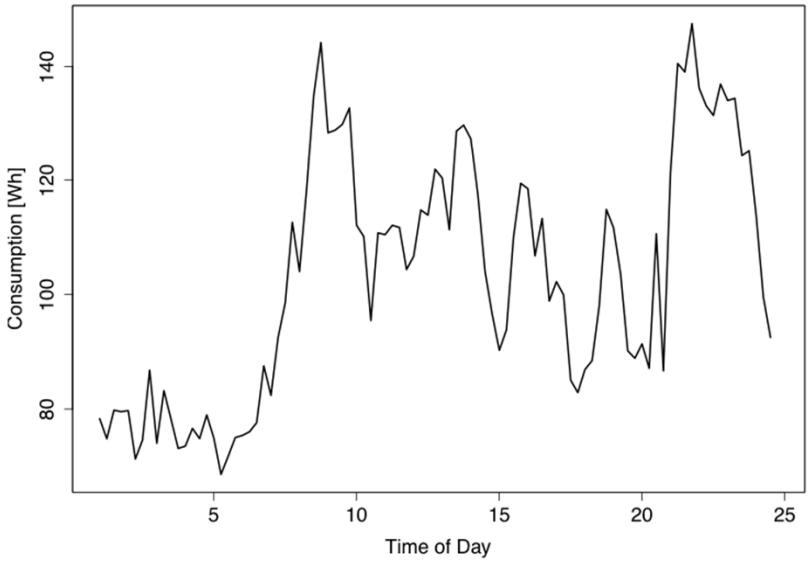
Weekly





Daily





Electricity Theft under AMI

FUJITSU

FBI: Smart Meter Hacks Likely to Spread

39 tweets retweet

A series of hacks perpetrated against so-called "smart meter" installations over th past several years may have cost a single U.S. electric utility hundreds of million of dollars annually, the FBI said in a cyber intelligence bulletin obtained b

FEDERAL BUREAU OF INVESTIGATION
INTELLIGENCE BULLETIN
Cyber Intelligence Section

27 May 2010

(U//FOUO) Smart Grid Electric Meters Altered to Steal Electricity

(U//FOUO) This intelligence bulletin satisfies requirements contained in the FBI's Cyber Intrusions against the US Standing Collection Requirements USA-CYBR-CYD-SR-0085-09, USA-CYBR-CYD-SR-0004-10, and USA-CYBR-CYD-SR-0061-10.

(U//FOUO) Smart Grid electric meters[a] in Puerto Rico are being exploited to under-report the amount of electricity used by consumers and businesses, according to FBI case information.[1] The Puerto Rican utility estimates their losses could reach $400,000,000 annually. This is the first report that criminals have compromised Smart Grid meters and the first time the FBI has investigated meter fraud.

UNCLASSIFIED

(U) Source Summary Statement

(U//FOUO) The information contained in this Intelligence Bulletin is derived from confidential sources with direct access who the FBI judges to be accurate, reliable, and credible, despite the fact that they have not reported previously. We would deem this reporting more reliable, if it could be independently verified.

(U//FOUO) The FBI assesses with medium confidence[b] that as Smart Grid use continues to spread throughout the country, this type of fraud will also spread because of the ease of intrusion and the economic benefit to both the hacker and the electric customer.

(U) Smart Grid meters are intended to improve efficiency, reliability, and allow the electric authority to charge different rates for electricity at different times of the day. The Smart Grid also improves a utility's ability to remotely read meters to determine electric usage.[2]

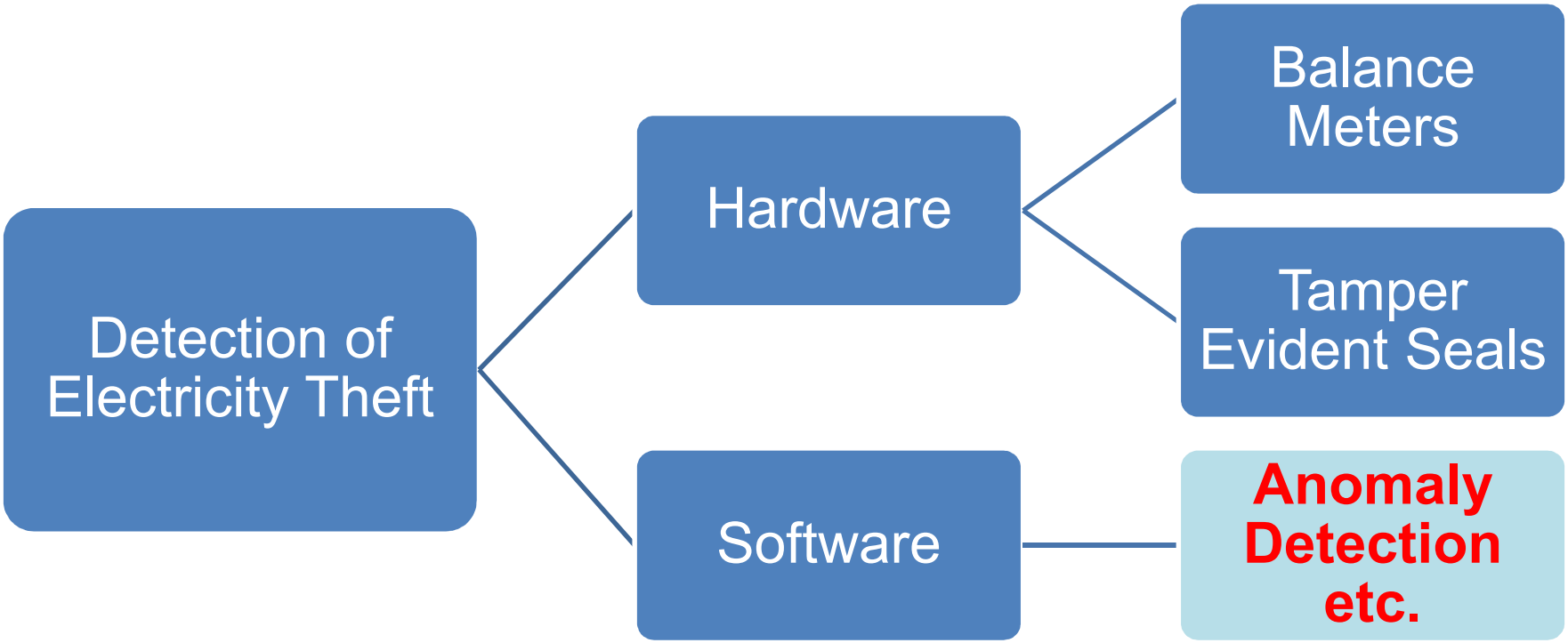
(U//FOUO) Meters are being compromised in the following ways, according to a contact with good access

Attacks will happen, but devices are deployed for 20~30 years.

Strategy and tools for attack could be easily shared and distributed, e.g., through the Internet!

Taxonomy of Detection Mechanisms

FUJITSU

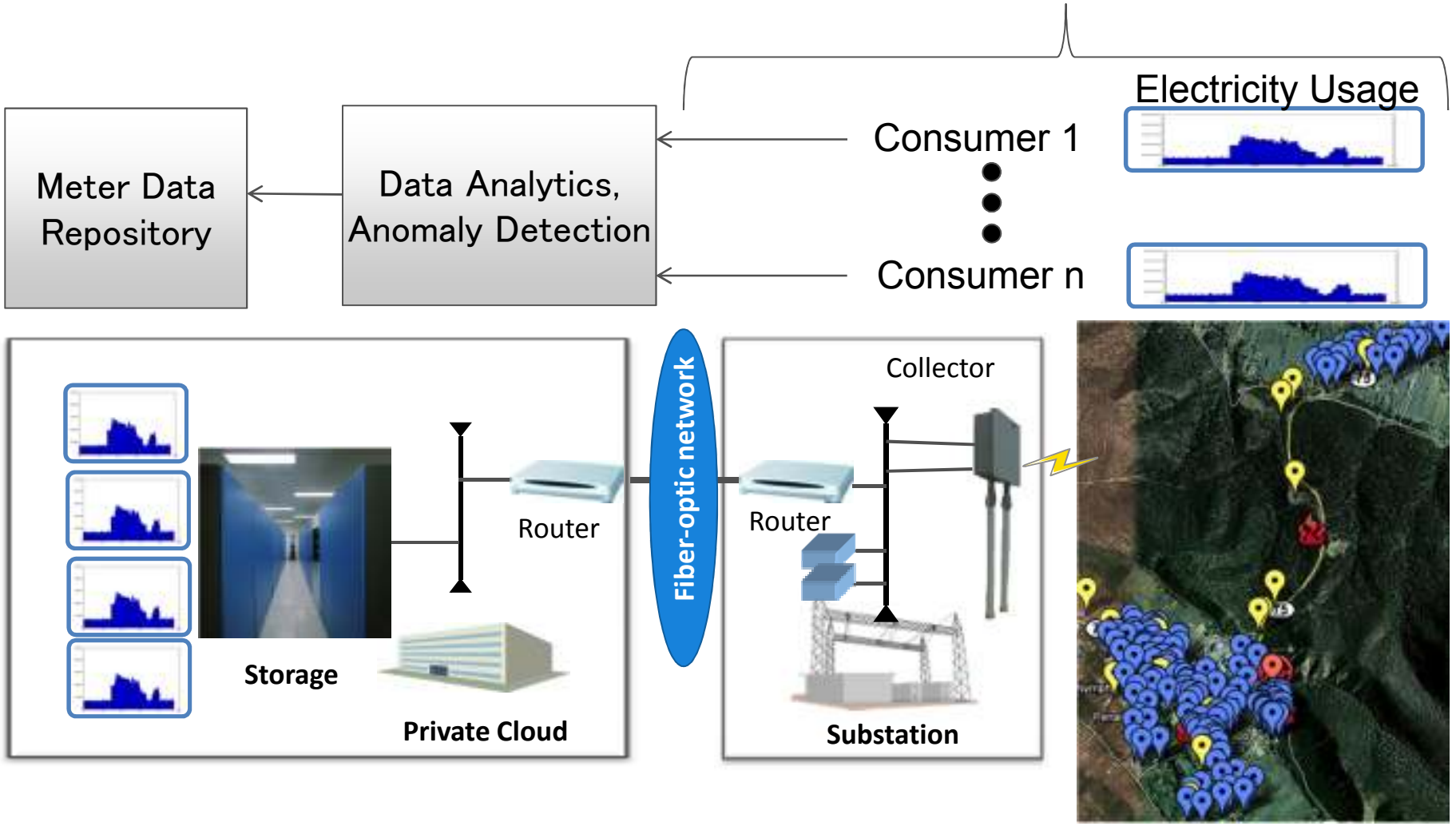


Among software based detection, we focus on anomaly detection schemes because they do not require actual attack samples, which are hard to collect in practice.

Anomaly Detection Architecture in AMI

FUJITSU

Smart Meters send consumption data frequently (e.g., every 15 minutes) to the utility



Our Contribution

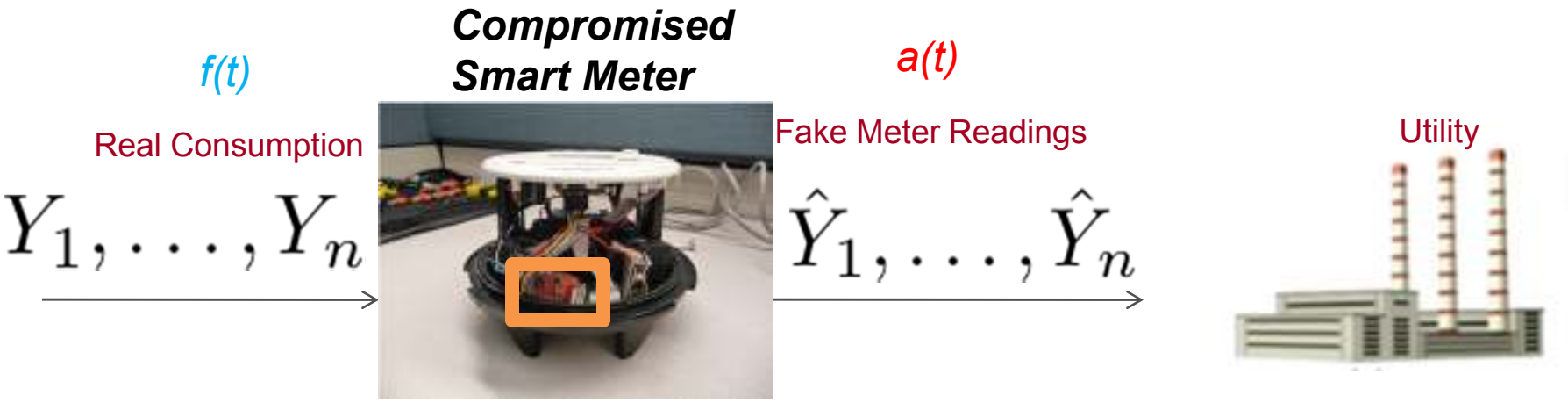
FUJITSU

- Design anomaly-based electricity theft detectors using fine-grained electricity usage data reported by smart meters

- Evaluate such electricity theft detectors
  - Instead of a traditional approach relying on real attack samples, propose new evaluation framework that uses “optimal” gain of attackers
    - I.e. find the worst-possible attack against each detector, and then calculate the cost (kWh stolen without being detected) of such an attack

Adversary Model

FUJITSU



Goal of attacker: Minimize Energy Bill: $\min_{\hat{Y}_1,\ldots,\hat{Y}_n} \sum_{i=1}^{n} \hat{Y}_i$

Goal of Attacker: Not being detected by classifier “C”:

$$C(\hat{Y}_1, \ldots, \hat{Y}_n) = \text{ normal}$$

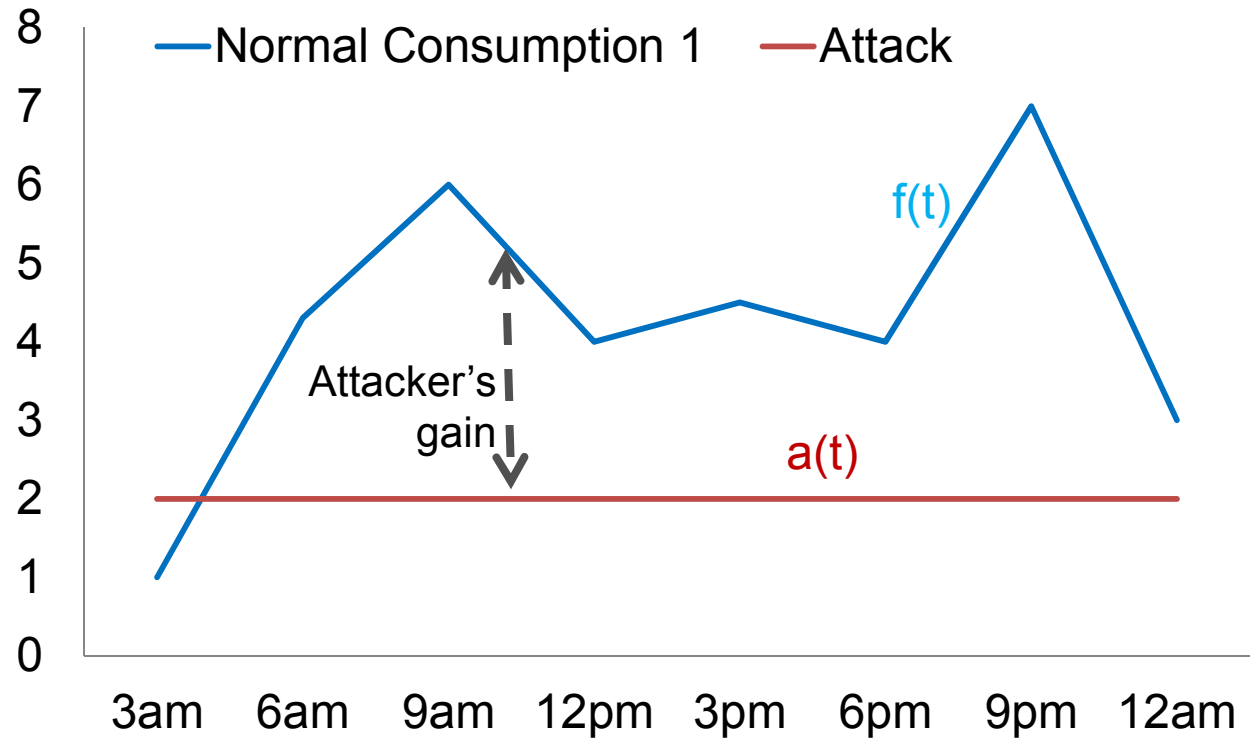
Detector using Simple Daily Average

FUJITSU

- Take average of signal *f(t)* and report any average lower than a threshold as electricity theft
  - E.g. Select threshold as “2”
  - If daily-average of signal is lower than 2 report an alarm

- Problem
  - Attacker, to maximize its gain, selects attack signal as constant *a(t)*=2

  Clearly *a(t)* looks “abnormal”, but it does **NOT** raise an alarm because the average of *a(t)* never went below 2!



Other Electricity Theft Detectors

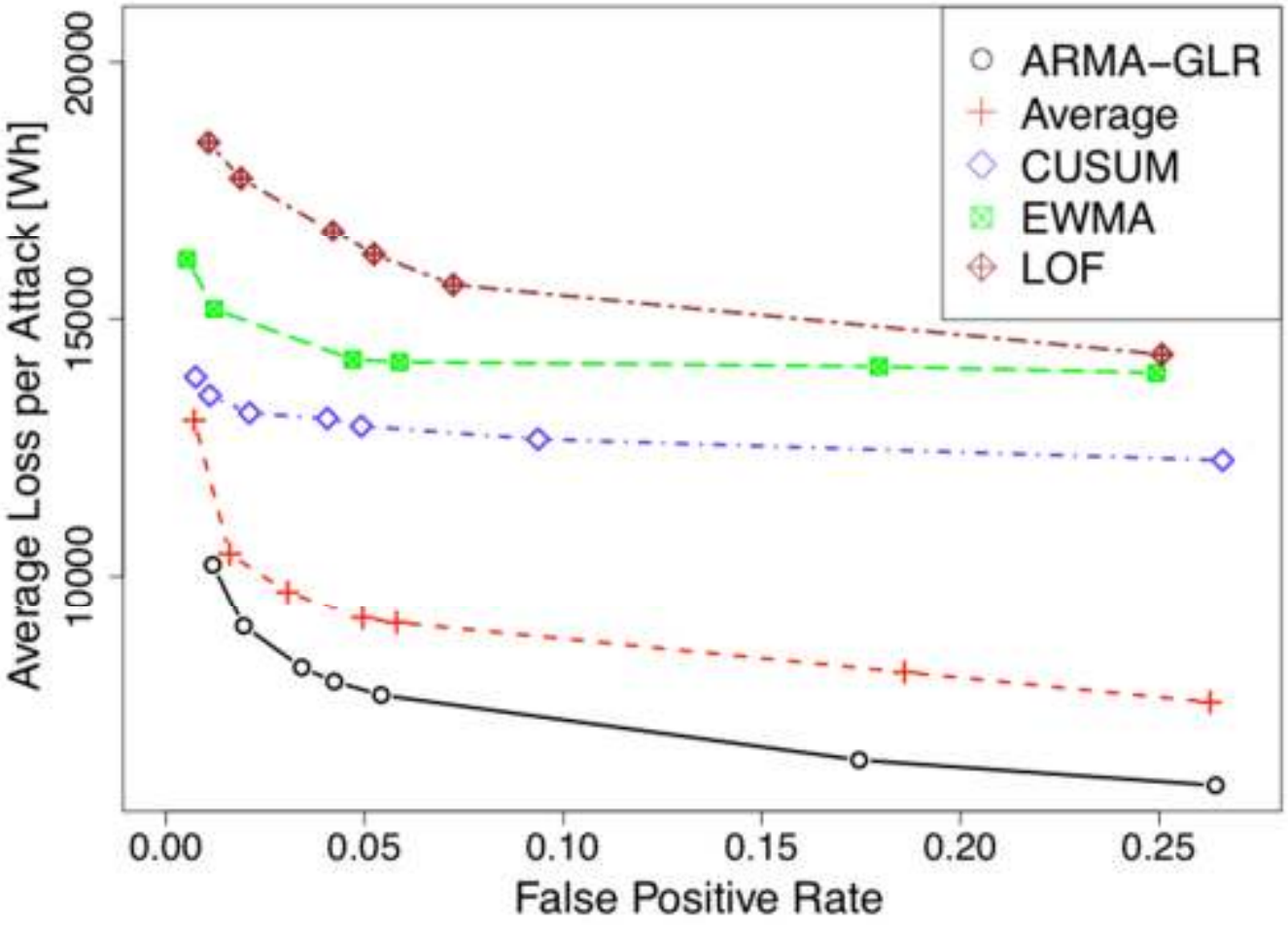
FUJITSU

- ARMA-GLR Detector
  - Use ARMA (Auto-Regressive Moving-Average) model to predict future consumption and evaluate the prediction error
- EWMA (Exponentially-weighted Moving Average) / CUSUM (Cumulative SUM) Chart
  - Common techniques to continuously monitor process state (i.e Control Chart for QC)
- LOF (Local Outlier Factor)
  - Clustering-based approach to identify outlying data points

Tradeoff Curves

FUJITSU

Y-axis: Cost of Undetected Attacks (can be extended to other fields)
X-axis: False Positive Rate



- Each detector is trained by using the last 28-day electricity consumption pattern.
- Real AMI data (6 months of 15 minute reading-interval for 108 customers) is used.

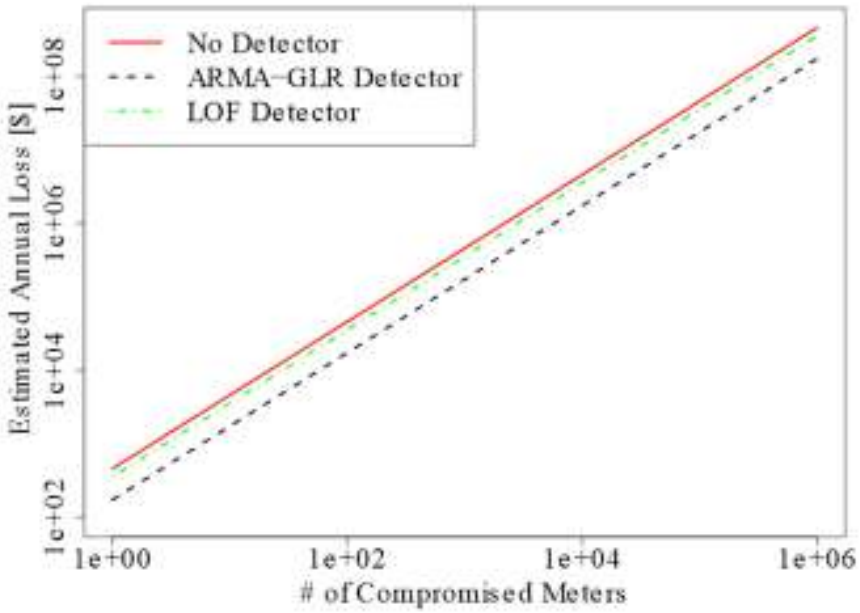
Monetary Loss

FUJITSU

- Loss per customer

Detector	FP Rate	Average Loss	Revenue Lost
Average	0.0495	$0.55	43%
EWMA	0.0470	$0.852	68%
CUSUM	0.0491	$0.775	62%
LOF	0.0524	$0.975	77%
ARMA-GLR	0.0423	$0.475	38%

- What if the attack propagates widely??

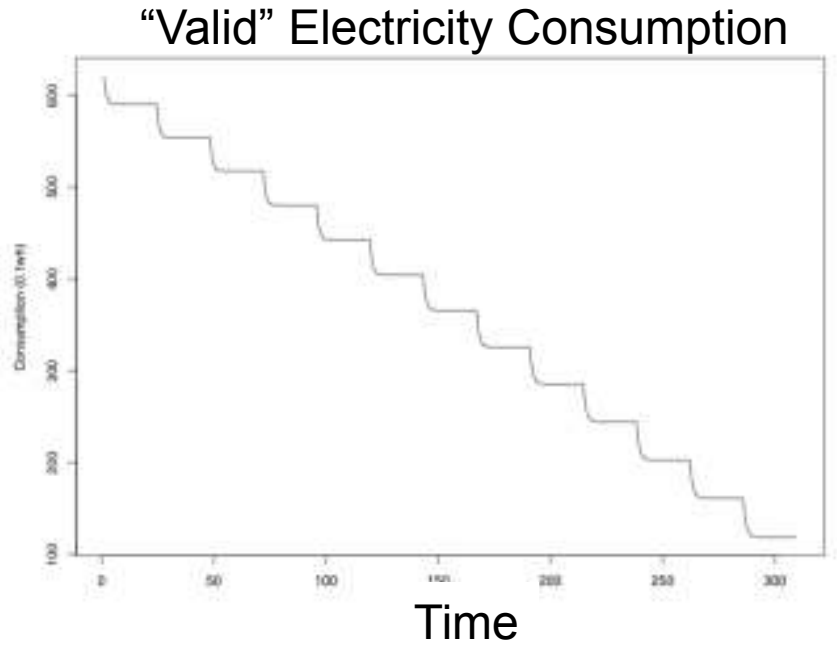


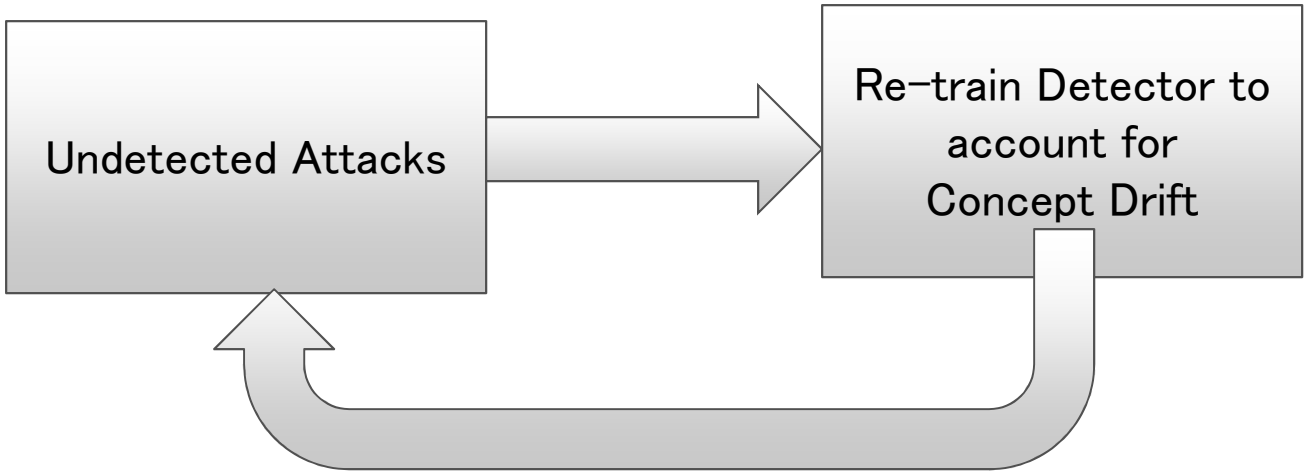
Effects of “Poisoning” Attacks

FUJITSU

- To incorporate changes in normal pattern over time (Concept Drift), detectors need to be **re-trained periodically**.

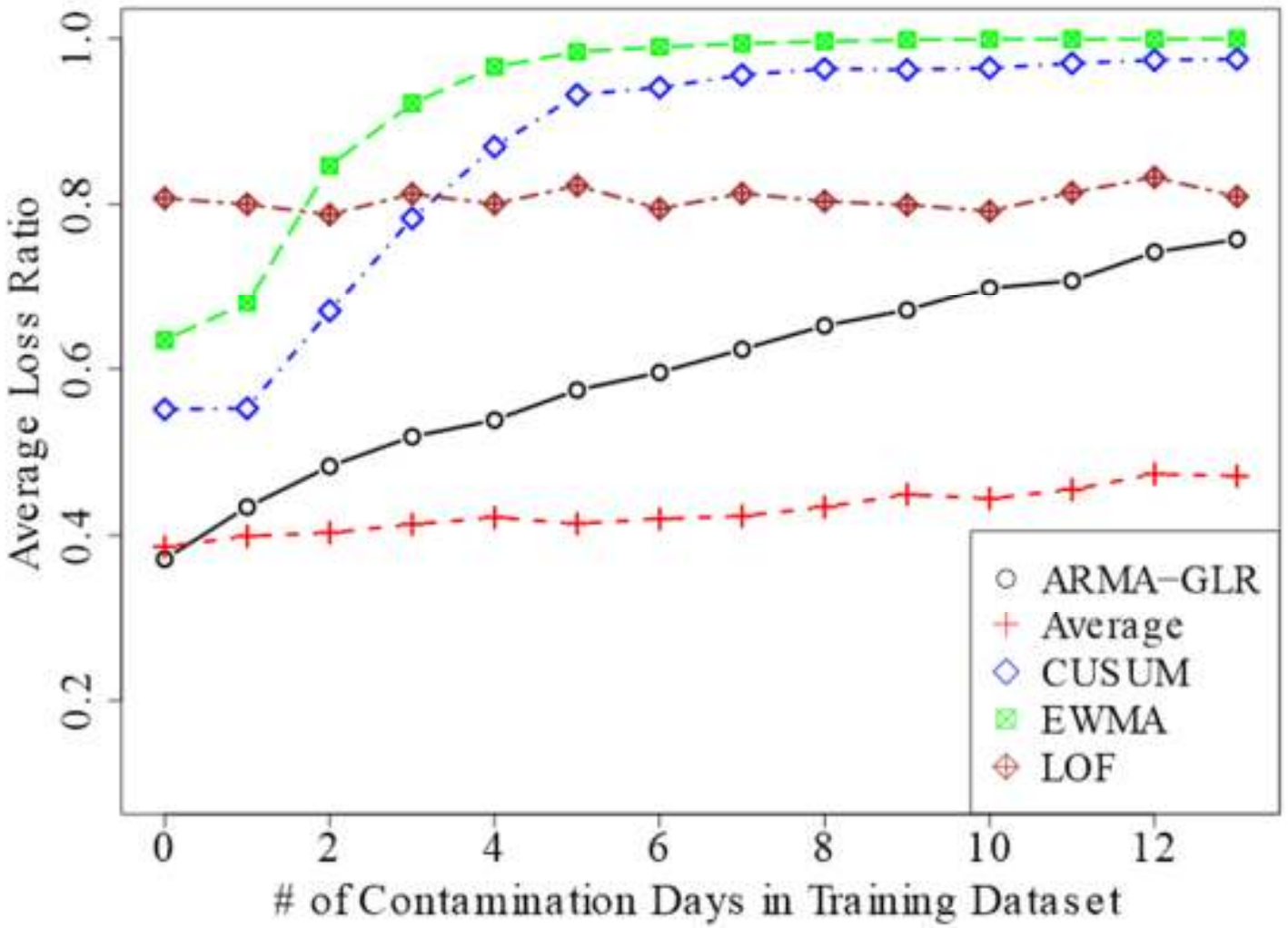
- Attacker can use undetected attacks to ***poison*** training data





Experimental Results of “Poisoning” Attacks

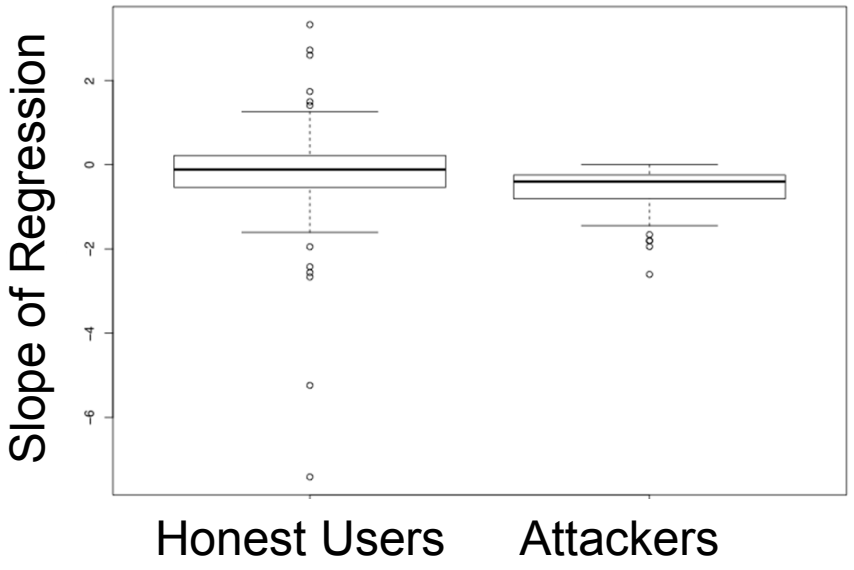
FUJITSU

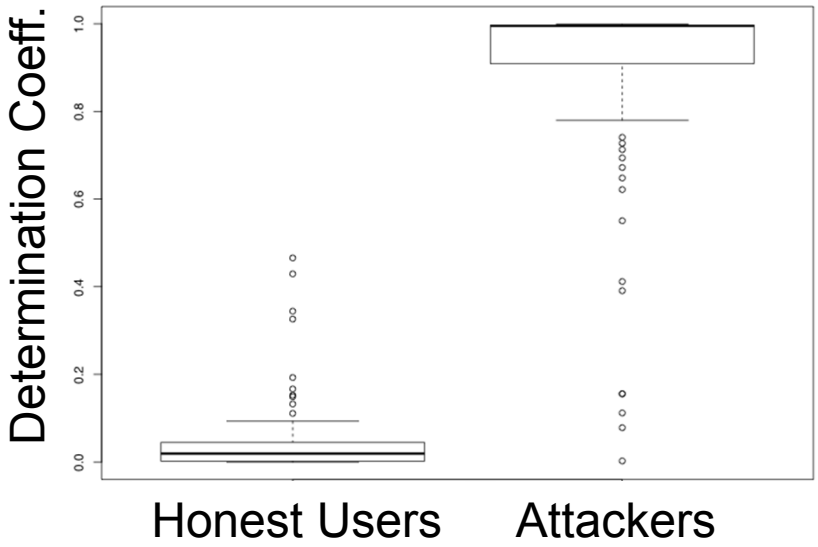


Detecting Poisoning Attacks

FUJITSU

- Identify concept drift trends helping an attacker
  - Continuously lower consumption over time.
- Countermeasure: linear regression of trend
  - Slope of regression was not good discriminant
  - Determination coefficients worked!

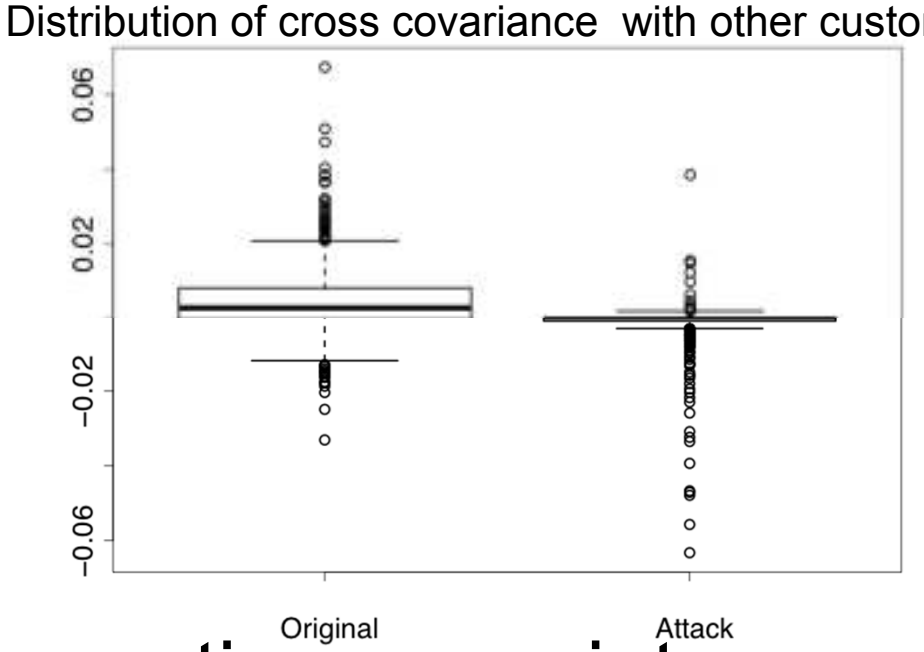




Ongoing Work

FUJITSU

- Use of cross correlation with other customers to detect attacks

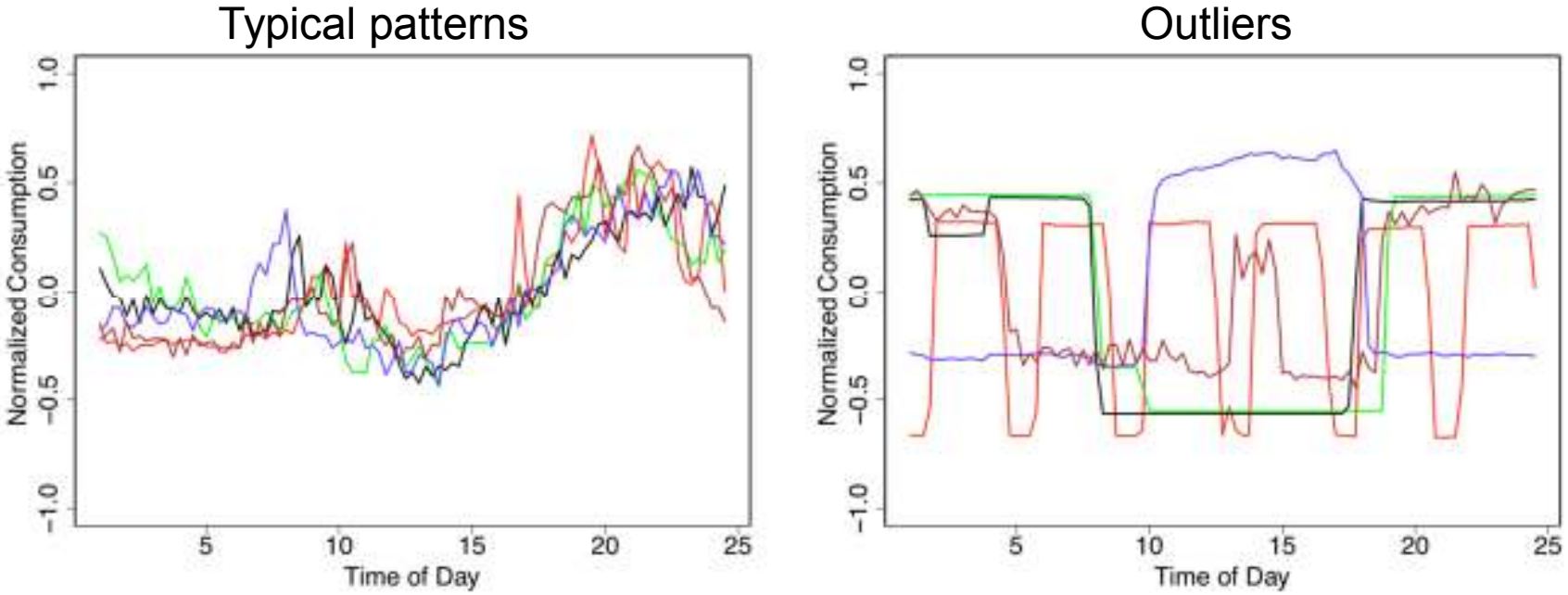


- Take “shape” of consumption curve into consideration?
- Correlation with other factors? (Weather, temperature etc.)
- Design and evaluate other detectors

Ongoing Work

FUJITSU

- Detect other types of anomalies
  - Apply LOF on consumption pattern of different customers on the same day



  - Outliers may be caused by a variety or reasons, such as meter failure etc.

Thank you very much.

FUJITSU

- Reference:
  - *"Evaluating Electricity Theft Detectors in Smart Grid Networks."* Daisuke Mashima and Alvaro Cardenas. In Proceedings of the 15th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2012), 2012.

- Questions?

Contact:
Daisuke Mashima
dmashima@us.fujitsu.com
Fujitsu Laboratories of America Inc.
1240 E. Arques Ave. M/S 345
Sunnyvale, CA 94085