Energy Theft in the Smart Grid

Papers

Energy Theft in the Advanced Metering Infrastructure

Evaluating Electricity Theft Detectors in Smart Grid Networks

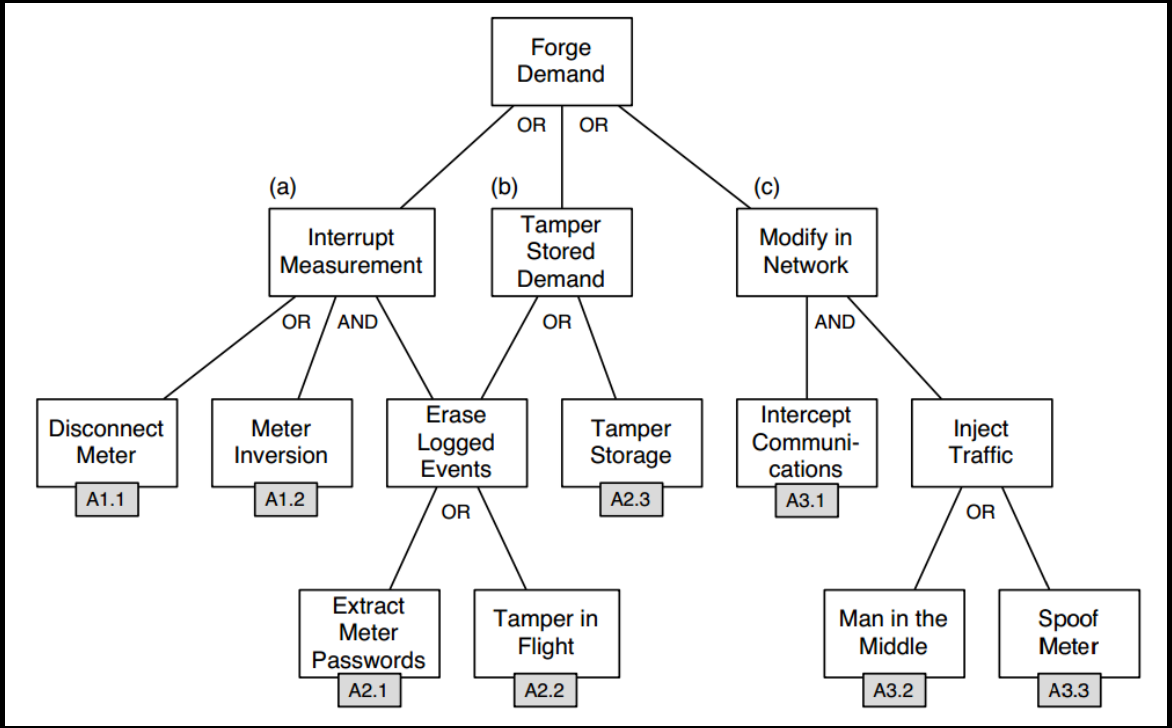
Energy Theft in the Advanced Metering Infrastructure

Stephen McLaughlin, Dmitry Podkuiko, and Patrick McDaniel

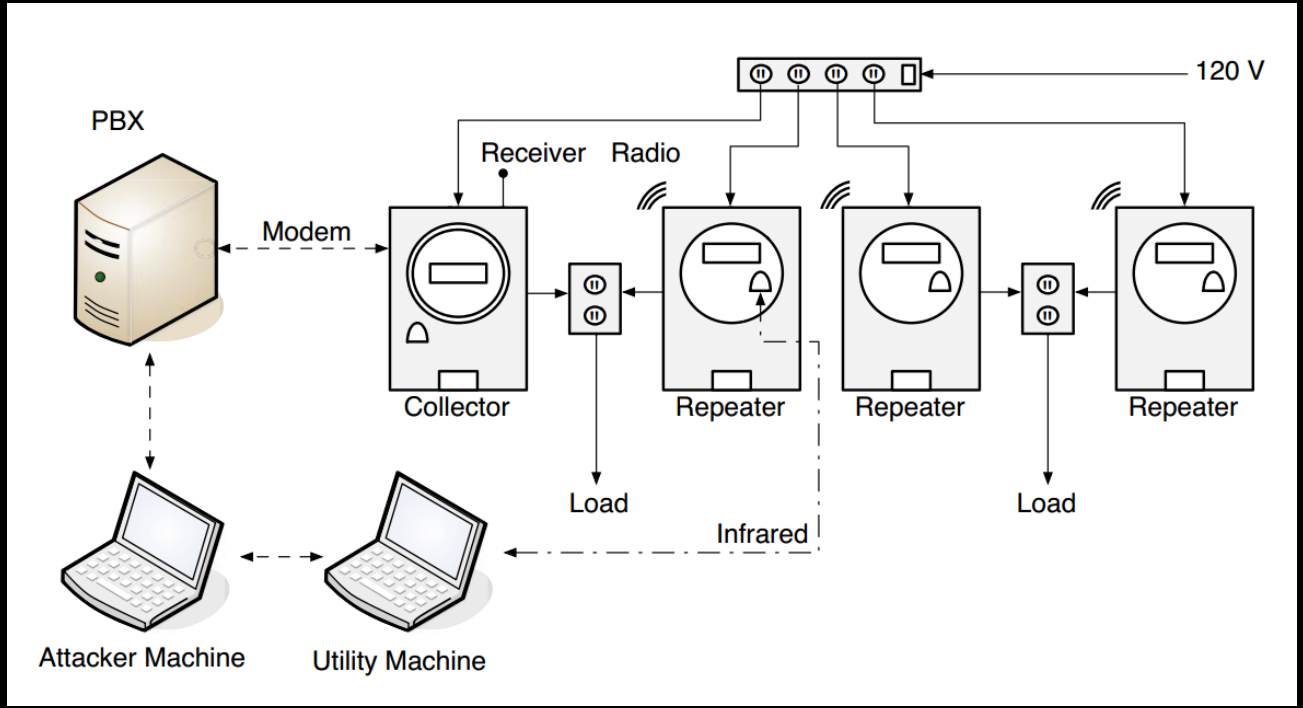
Contents

- Energy Theft Attack Tree
- Test system
- AMI Security Analysis
- Conclusions

Energy Theft Attack Tree



Test System


120 V
PBX
Receiver
Radio
Modem
Collector
Repeater
Repeater
Repeater
Load
Load
Infrared
Attacker Machine
Utility Machine

AMI Security Analysis

- Physical Tampering
- Password Extraction
- Eavesdropping
- Meter Spoofing

Conclusions

Attack Number & Description	Vulnerability	Design Assumption
(A1.1, A1.2) Measurement interruption	Inadequate physical tamper protections	1. Physical limitations
(A2.1) Password extraction	Insecure optical communication	2. Near field security
(A2.3) Meter storage tampering	No Firmware Integrity Protections	3. Physical integrity of meter
(A3.1) Communication interception	Insufficient intrusion detection	4. Trusted backhaul nodes
(A2.2, A3.2, A3.3) Communication tampering	Failure to check for replay	5. Trusted endpoint node

Evaluating Electricity Theft Detectors in Smart Grid Networks

Daisuke Mashima and Alvaro A. Cárdenas

Contents

- Adversarial Classification and Learning
- Electricity-Theft Detectors and Attacks
- Method & Results
- Future work

Adversarial Classification/Learning

Generate worst-case attack

Cost function

Contamination attacks

Theft Detectors and Attacks

Average Detector

ARMA-GLR

(EWMA, CUSUM and LOF)

Method

6 months real, anonymized meter data

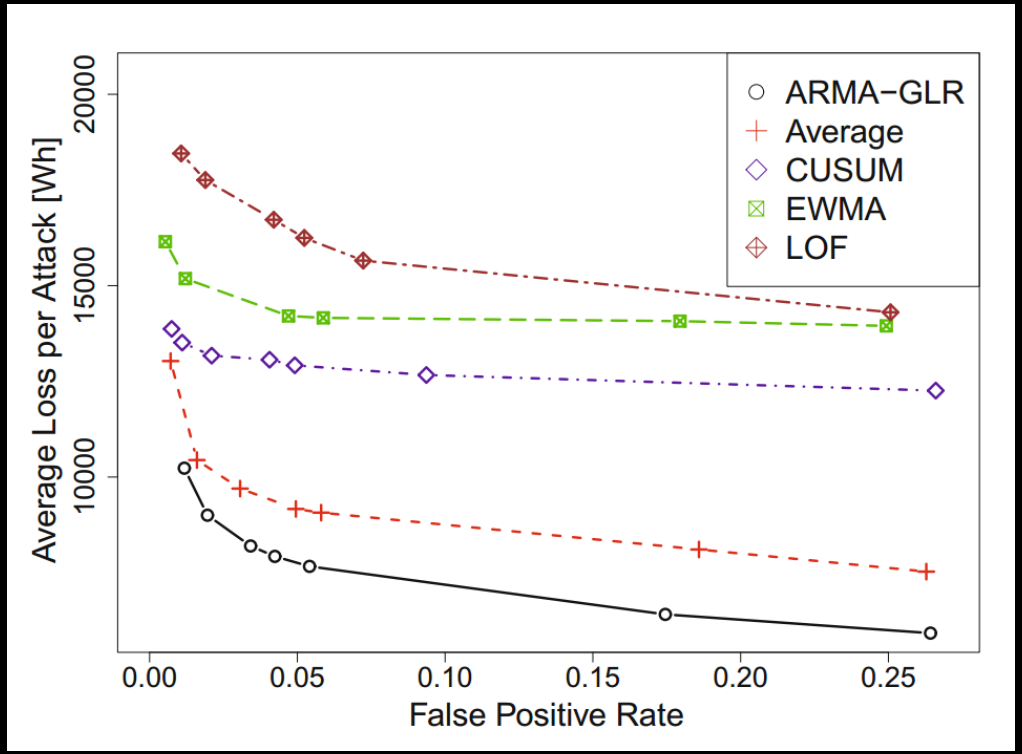
4 week training period

Compute alarm threshold

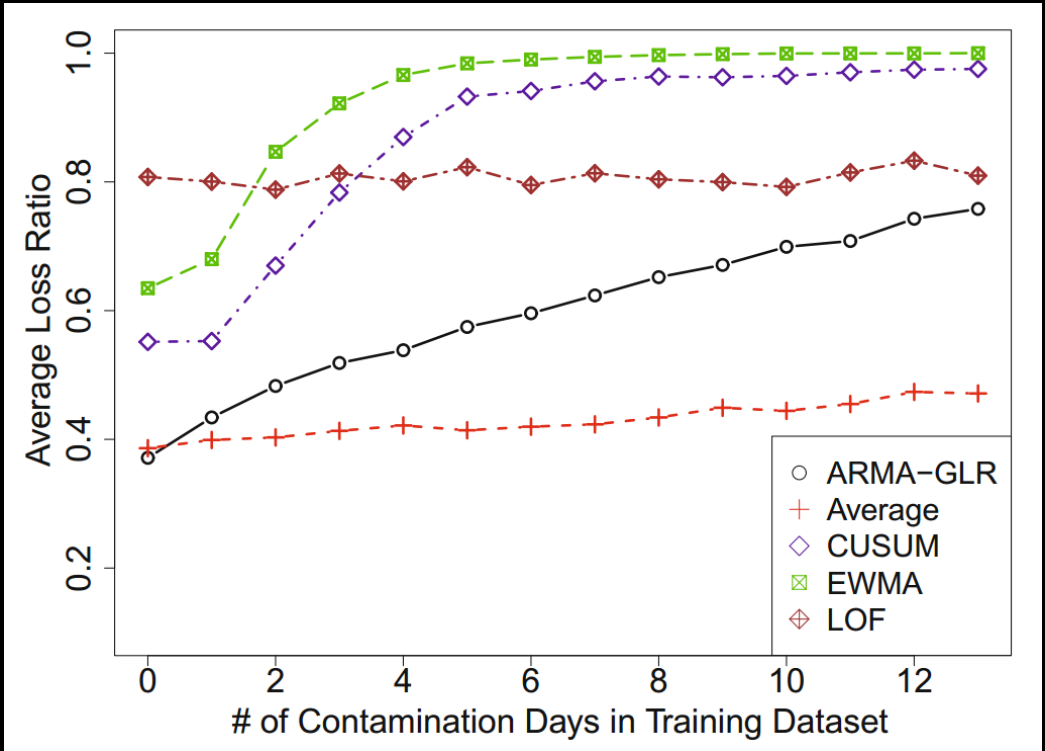
Test following data

Calculate cost if needed

Results


ARMA−GLR
Average
CUSUM
EWMA
LOF
Average Loss per Attack [Wh]
10000
15000
20000
0.00
0.05
0.10
0.15
0.20
0.25
False Positive Rate

Results


Average Loss Ratio
0.2
0.4
0.6
0.8
1.0
0
2
4
6
8
10
12
# of Contamination Days in Training Dataset
ARMA−GLR
Average
CUSUM
EWMA
LOF

Future work

Time Of Use

Longer datasets

Cross-Correlation

Paper comparison

Energy Theft in the Advanced Metering Infrastructure

- Broader
- Lacking depth

Paper comparison

Energy Theft in the Advanced Metering Infrastructure

- Broader
- Lacking depth

Evaluating Electricity Theft Detectors in Smart Grid Networks

- Focused
- Too deep for me

The End

Discuss