Hidden Electricity Theft By Exploiting Multiple-Pricing Scheme In Smart Grids

HARISANKAR A
S7 E2
ROLL NUMBER: 32

Department of Electrical Engineering
College of Engineering Trivandrum

8 November 2021

OBJECTIVES

- Present a general billing model to study existing pricing schemes in electricity markets.
- Develop an HET(hidden electricity theft) model to maximize attacks and algorithms for the same
- Propose countermeasures to detect the energy theft.
- Study HET attack and countermeasures on a real world data set.

INTRODUCTION

- FP(Fixed Pricing) and MP(Multiple Pricing) scheme.
- Demand Response technologies fail to benefit honest users in such a case and it is difficult to detect under ETD(electricity theft detection) methods.

METHODOLOGY

- Understand Data-driven and consistency-based methods employed in Electricity theft detection.
- Analysis of a working example based on pricing scheme in Shanghai, China.
- A generalized billing scheme and attack assumptions
- ETD based on Consistency-based methods.

DATA-DRIVEN METHODS

- It trains a classifier model which captures the electricity consumption pattern based on consumption data.
- ELM(extreme learning machine) methods, SVM(support vector machines) etc. are used with top-down schemes, which could detect real-time electricity theft.

CONSISTENCY-BASED METHODS

- It uses physical laws, devices and additional measurements to detect inconsistency.
- The users are assumed to steal electricity, and honest users are filtered out, narrowing the detection range.
- To reach better performance, data driven methods are combined with consistency based solutions.

WORKING EXAMPLE

- Assumption 1- If the amount of electricity usage is unchanged, the revenue of utility company will not be affected.
- Assumption 2- Utility company collects the electricity usage data and calculates the bills once per year.

TABLE I: Multiple-pricing scheme in Shanghai, China.

Stage #	Consumption (kWh/Year)	Time	Unit Price (CNY/kWh)
I	0-3120	Peak	0.617
		Off-Peak	0.307
II	3120-4800	Peak	0.677
		Off-Peak	0.337
III	>4800	Peak	0.977
		Off-Peak	0.487

Figure: MP Scheme example

HET EFFECT ON BILLS

TABLE II: Electricity consumption and bills in the HET attack example.

Stage #	Time	Before Attack (kWh)		Attack I (kWh)		Attack II (kWh)	
		user A	user B	user A	user B	user A	user B
I	Peak	1000	1560	1560	1560	750	2320
	Off-Peak	1000	1560	1560	1560	1500	800
II	Peak	0	840	840	840	0	1240
	Off-Peak	0	840	840	840	0	440
III	Peak	0	1400	0	0	0	490
	Off-Peak	0	1400	0	0	0	2060
Electricity consumption (kWh)		2000	7600	4800	4800	2250	7350
Bills (CNY)		924	4342.8	2293.2	2293.2	923.25	4146.75
Total electricity consumption (kWh)		9600		9600		9600	
Total bills (CNY)		5266.8		4586.4		5070	

Figure: Constraint- Total electricity consumption should be unchanged

BILLING MODEL

- There are m prices ($m \geq 1$) in billing system in the form of P= $[P^1 p^2 p^3 p^m]$
  where $P^1 > p^2 > ..$
- The cumulative electricity consumption vector is given by Ui(t) = $[ui^1(t) + ui^2(t) + ui^3(t) + .]$

HIDDEN ELECTRICITY THEFT

- One gateway meter is employed at the supply side to measure overall electricity to n_0 consumers.

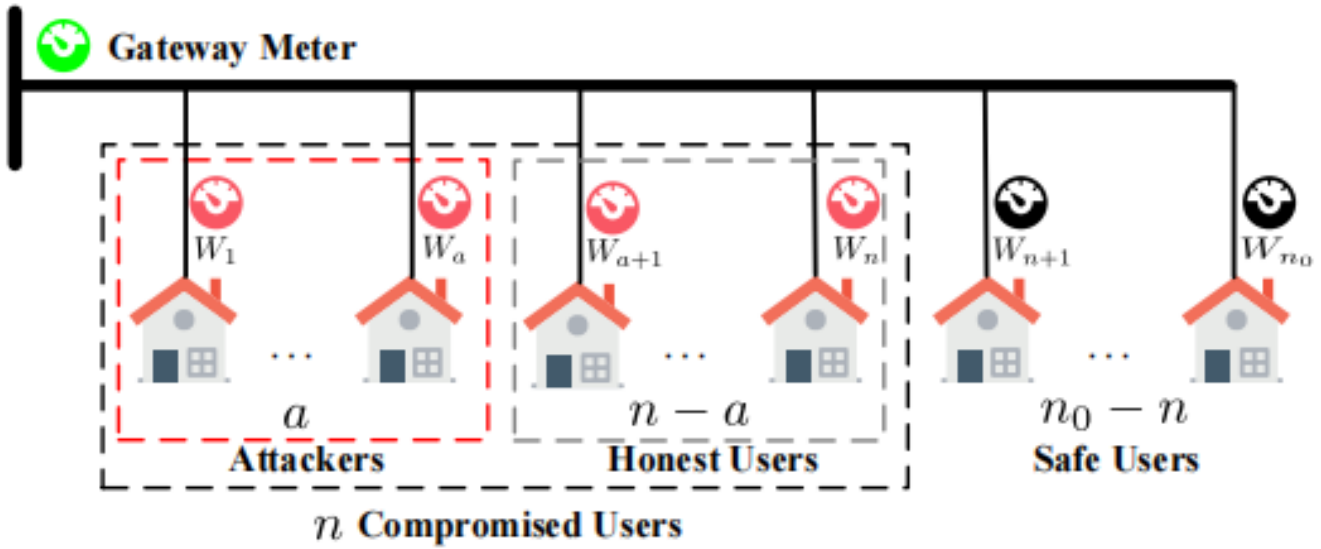

Figure: HET Attackers, victims and safe users

ETD based on CONSISTENCY METHOD

- The detection constraints are

$$\theta * W_0 \geq W_0 - \sum_{j=1}^{m} \sum_{i=1}^{n} W_i^j - \sum_{j=1}^{m} \sum_{i=1}^{n_0}$$

where

- W_0 -Total supplied electricity
- θ-error factor
- W(1<i<n) is the reported consumption of user i, corresponding price j
- W(1<i<n_0)is the consumption of safe users which cannot be accessed by attackers.

CONSISTENCY METHOD contd.

- There exists a unique solution if and only if a=1 and m=1.
- The reported electricity usage cannot be manipulated if and only if there is only one attacker(a=1) under the FP scheme(m=1).
- The total calculated electricity cost for n compromised users could not be changed by attackers if m=1.

HET Attack

- Assumption 1- Among n_0 consumers, n energy meters have been compromised.
- Assumption 2- Measurement data of compromised smart meters can be manipulated.
- Assumption 3- Attackers ultimate aim is to obtain economic gain by paying less money for the same amount of electricity consumed

HET under ToU scheme

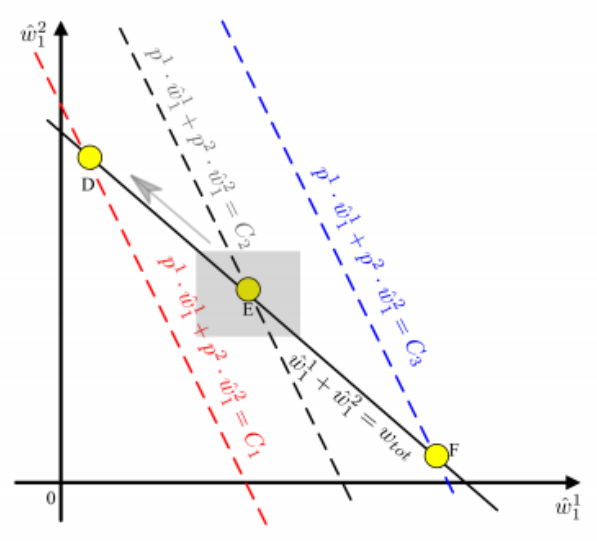

Figure: HET of a user under ToU mode

- One compromised user with two different prices
- Point E denotes real consumption data before attack.
- To reduce the bill from C_2 to C_1, the consumption data should be moved from point E to D.

HET under tiered pricing scheme

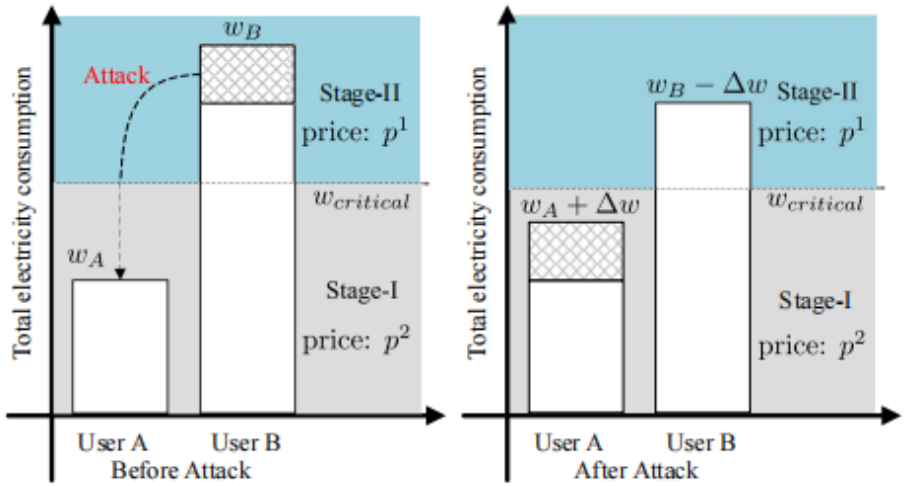

Figure: HET of a user under tiered pricing

- When the total electricity consumption exceeds $W_{critical}$, the excess price is p^1.
- The total bill is reduced by $(p^1 - p^2)w$.
- The total electricity consumption remains the same.

ETD based on data driven methods

- A classifier is trained by normal consumption data samples. When the pattern shows an irregularity, it can raise alarms.
- The electricity consumption of a single user is highly uncertain and hard to predict.
- Attackers could evade the ETD by restricting data modification within a reasonable range.

HET Model

- HET attack starting from time t to t+Δt can be regarded as an optimization problem:

$$Min_w C^M$$

- Wi,j are the reported electricity usage for user i and price p_j.
- The bills of honest users remain unchanged.

HET Model contd.

- Special constraints applied only for ToU pricing-
- The total energy consumed during peak hours and non-peak hours by compromised users and honest users remains the same.

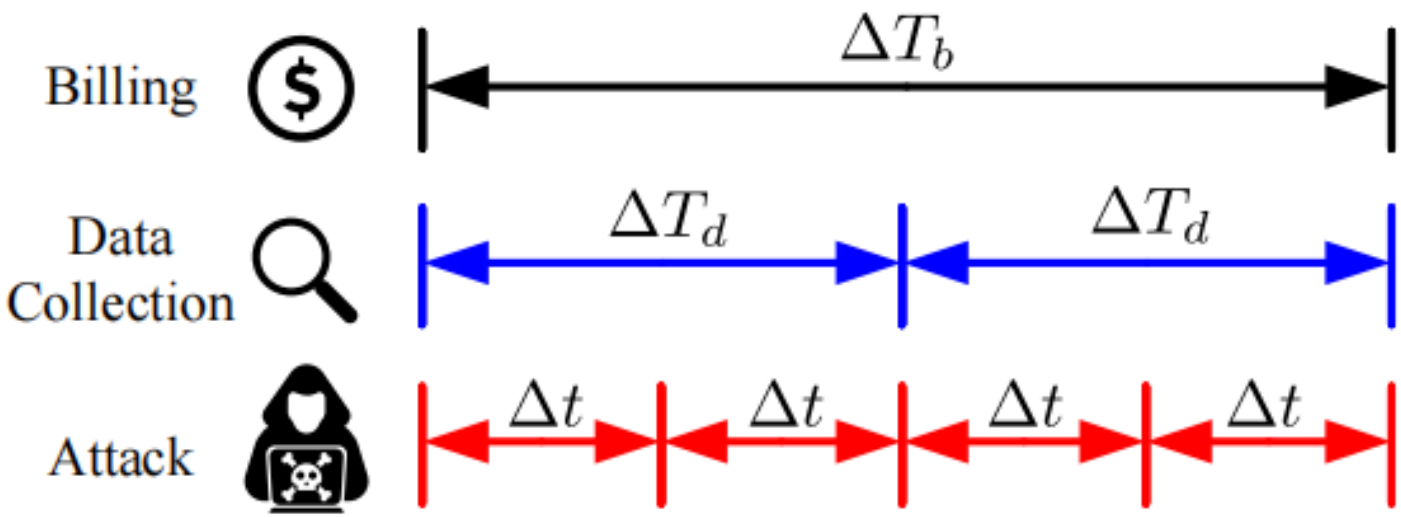

Figure: Billing, Data Collection and Attack cycle

ALGORITHM

- Method 1- Tamper with the electricity consumption data stored in smart meters directly, or jam and inject false data by attacking communication protocols.
- Method 2- Change critical parameters such as CT/PT ratio to change the measurements indirectly.

TAMPERING WITH MEASUREMENTS

- It changes meter measurements directly.
- At the end of each cycle($t+\Delta t$), the target consumption is determined.
- The original consumption is obtained and is replaced by the target consumption.
- If the new price is lesser than the original bill, the process is repeated.

TAMPERING WITH PARAMETERS

- Two of the most common and essential parameters are the ratio settings for CT(Current Transformer) and PT(Potential transformer).
- Since voltage level for a residential consumer is almost fixed, the CT parameters are changed.
- The scaling ratio of current measurement is

$$\lambda = \mathrm{CT(t)} \ / \ CT_i(\mathrm{t})$$

TAMPERING WITH PARAMETERS contd.

- The relation between CT ratio and metered current is obtained as
$$I(t+\Delta t)= \lambda * I(t)$$
- Manipulation of CT ratio will change all measurements from t to $t+\Delta t$
- Only a limited range of tampering is possible.

PARAMETERS

Attack Cycle	Bills after Attack (CNY)	Loss Rate
1 month	38383.26	6.551%
1 day	38409.20	6.488%
1 hour	38413.11	6.479%
15 minutes	38419.23	6.464%

Figure: Original Bill=41074.21 CNY

- The relative error that can be tolerated without detection is 'e'

$$e = (W_{attack} - W_{real})/W_{real}$$

- The relation between scaling ratios of CT and relative error can be defined as

$$\lambda \text{ min} \leq \lambda\ (1+\text{e}) \leq \lambda max$$

SMART METER TESTING

- All smart meters supports Modbus protocol.
- There are 3 Modbus registers in GE EPM5500P- Input, Export and Net energy. All three are R/W accessible.

Name	Address	Range	Access
Import Energy	0x0156	0 to 99,999,999.9	R/W
Export Energy	0x0158	0 to 99,999,999.9	R/W
Net Energy	0x0160	0 to 99,999,999.9	R/W

Figure: Registers in GE EPM5500P

SMART METER TESTING contd.

- During PS(Programmable settings) update mode and the firmware update process(PAC4200 only), the meter can be compromised

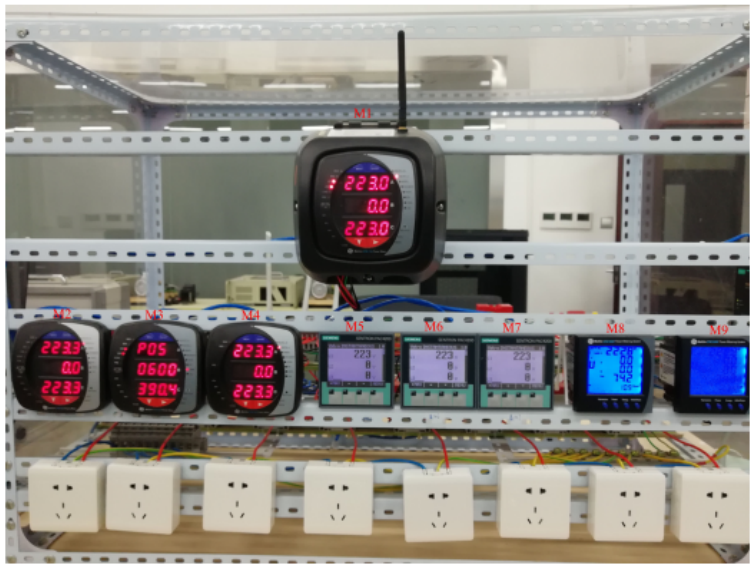

Figure:

M1 (GE EPM7100), M2 (GE EPM7000), M3 (GE EPM6000), M4 (GE EPM2200), M5-7 (Siemens PAC420) and M8-9 (GE EPM5500P)

COUNTERMEASURES

- Two patches can be applied on smart meters registry groups
  a. Patch on Access control
  b. Patch on Writing operation record.

Name	Address	Range	Access
Primary Voltage	0xC355	1 to 999,999	R/W
Secondary Voltage	0xC357	1 to 690	R/W
Primary Current	0xC35B	1 to 999,999	R/W
Secondary Current	0xC35D	1 or 5	R/W

Figure: REGISTERS RELATED TO CT AND PT in Siemens PAC4200

COUNTERMEASURES contd.

- The two strategies to enhance current ETD models are
  a. Random Consistency checking
  b. Charging rebating model

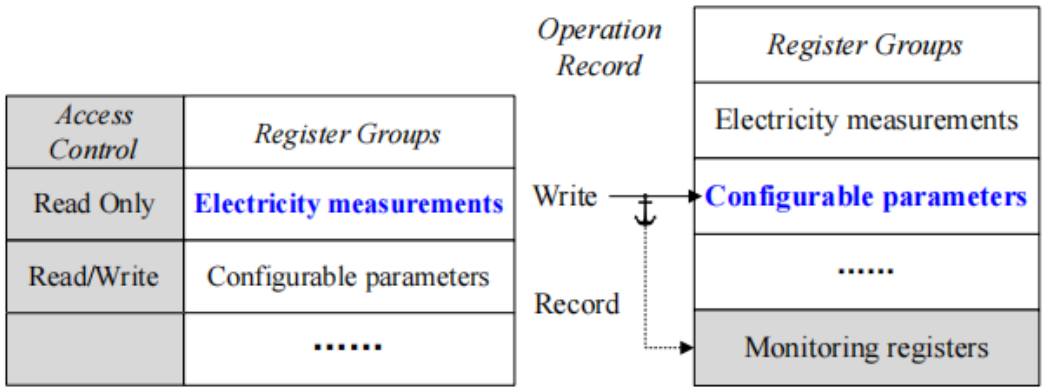

Figure: Protection by altering Smart Meter firmware

COUNTERMEASURES contd.

- The data collection cycle is limited by cost of communication, storage and communication.
- One fundamental assumption by attackers is that innocent users only care about their bills and ignore the details of consumption.

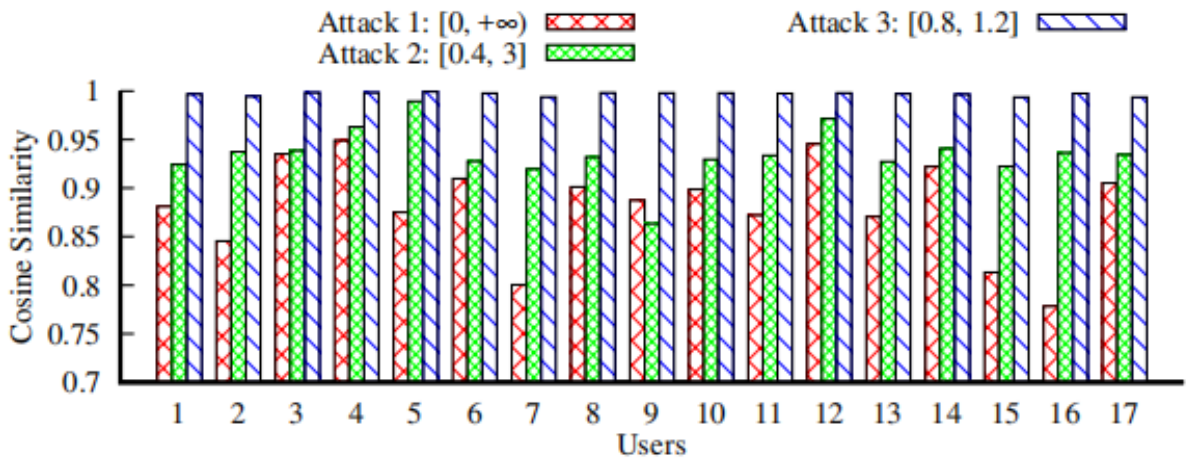

Figure: Cosine similarities between manipulated data and original data

SIMULATION AND ANALYSIS

- The data set obtained from electricity consumption benchmarks project of Australia, which contains the energy consumption data of 25 households from 2012 to 2014.

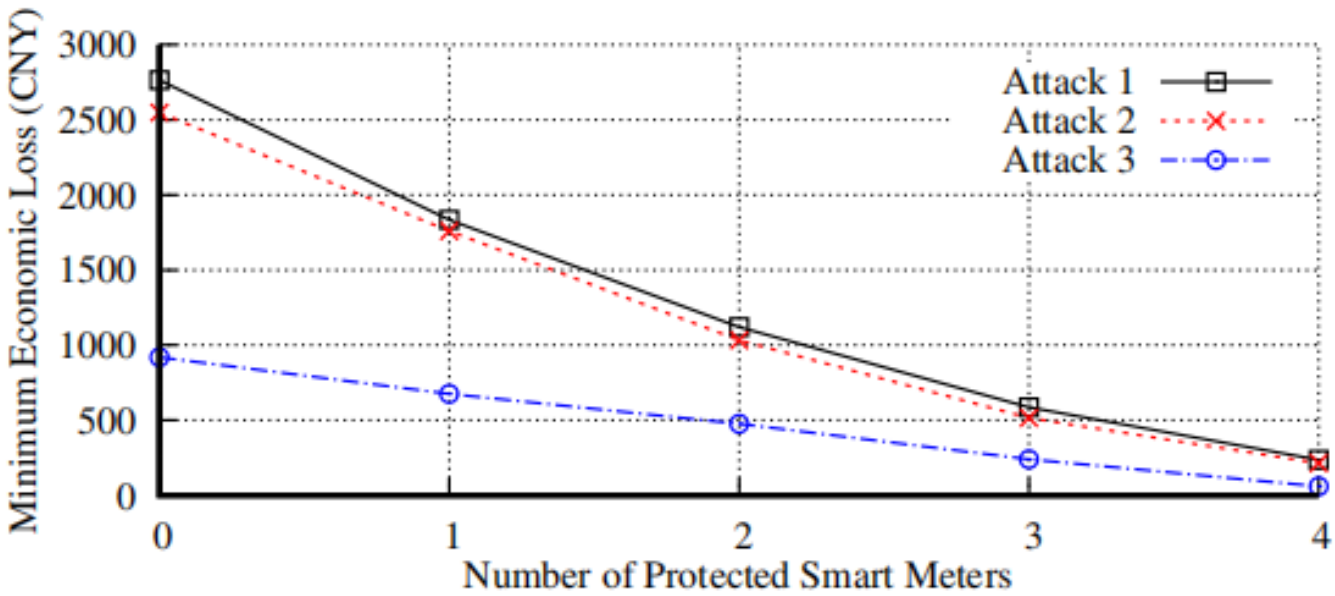

Figure: Smart meter protection and economic losses

DATA

User	Original Data		Data Variation after Attack 1 Attack Range: $[0, +\infty)$		Data Variation after Attack 2 Attack Range: $[0.4, 3]$		Data Variation after Attac Attack Range: $[0.8, 1.2$	
	Energy	Bill	Energy	Bill	Energy	Bill	Energy	Bill
1	2680.84	1547.82	1547.70	845.09	1141.35	626.22	244.13	161.34
2	6683.14	4272.36	-2062.26	-1712.65	-2068.13	-1914.29	-702.36	-720.64
3	4170.32	2392.83	-66.60	-39.19	-62.42	-152.21	234.18	155.34
4	3782.69	1950.45	-64.72	17.74	198.41	115.12	190.18	121.88
5	2854.32	1522.90	1823.16	1050.70	1326.25	1789.85	196.99	235.7
6	2609.16	1487.81	1286.58	668.40	1230.92	698.04	268.55	174.85
7	8009.25	5606.87	-3710.87	-3108.56	-2821.79	-2771.22	-943.57	-929.12
8	4047.20	2106.16	-221.70	4.80	-2.49	16.31	235.73	146.33
9	3550.78	2000.79	210.91	135.53	907.51	468.71	309.32	207.27
10	2510.72	1448.68	1283.87	652.30	1230.06	721.25	275.74	176.33
11	2125.78	1168.43	1637.68	886.17	1401.84	795.41	223.34	135.65
12	4354.37	2453.02	-464.07	-265.97	-368.14	-261.52	57.06	41.32
13	2047.04	1164.68	1783.19	958.42	1330.11	770.01	203.58	129.57
14	4565.71	2425.29	-794.15	-298.46	-794.9	-446.82	107.71	81.96
15	7490.31	5227.63	-3019.89	-2583.62	-2190.05	-2361.46	-729.57	-774.19
16	1198.25	646.23	2244.36	1221.93	2122.45	560.13	130.28	79.46
17	5791.37	3652.26	-1413.19	-1123.58	-1301.33	-1259.37	-301.29	-372.57
Total	68471.25	41074.21	0	-2690.95	0	-2605.84	0	-949.52

Figure: Energy and bills before and after the attack

ANALYSIS

- The profit obtained is 6.5.If a single person is the attacker, it reduces even further.

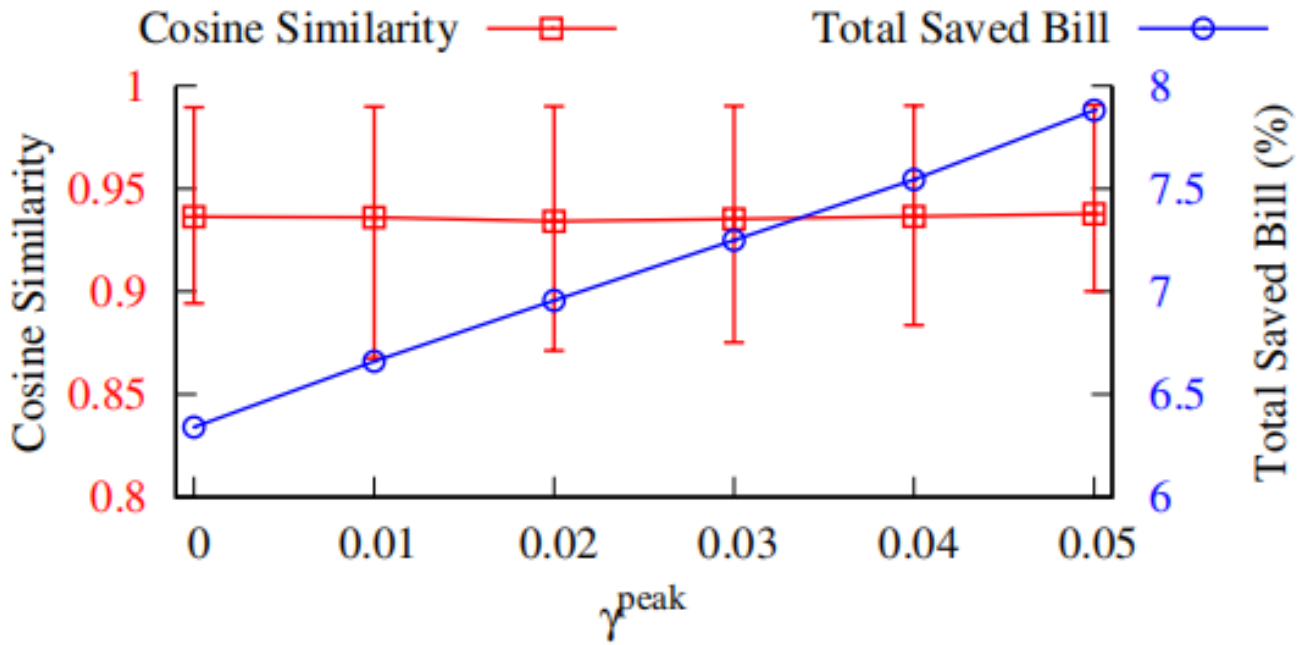

Figure: All users cosine similarity and % of the total saved bill vs peak price

CONCLUSION

- Security of both FP and MP schemes were discussed.
- HET attack model was developed.
- Two algorithms for conducting HET attacks were discussed.
- Feasibility on smart meters were analyzed.
- Countermeasures were also discussed.
- HET attacks and countermeasures were analyzed on a real world data set.

REFERENCES

[1] US Dept. Energy, "Benefits of demand response in electricity markets and recommendations for achieving them," Tech. Rep., 2006.

[2] F. M. Cleveland, "Cyber security issues for advanced metering infrastructure (AMI)," in Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008IEEE. IEEE, 2008, pp. 1–5.

[3] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," in International Workshop on Critical Information Infrastructures Security. Springer, 2009, pp. 176–187.

[4] M. R. Asghar, G. Dn, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," IEEE Communications Surveys Tutorials, vol. 19, no. 4, pp. 2820–2835, Fourth quarter 2017.

[5] Y. Hong, W. M. Liu, and L. Wang, "Privacy preserving smart meter streaming against information leakage of appliance status," IEEE Transactions on Information Forensics and Security, vol. 12, no. 9, pp. 2227–2241, Sep. 2017.

[6] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P. H. Ha, "Anonymous secure framework in connected smart home environments," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 968–979, April 2017.

Thankyou!