Tampere University

Cyber security issues in Smart Grids

Sami Repo

Content

- Background
- Methodology
- Impact scenarios
- Distribution grid impacts
- Conclusions

Background

- Your Lightbulb Might be Too Smart - Assessment of the Emerging Cybersecurity Risks in Electricity Distribution
- To **assess the potential risks for power system**, caused by **cybersecurity vulnerability of home automation**
- Focus on risks which may have wide and impact
  - Compromised cybersecurity in cloud-based automation systems or remote access to devices
  - Relatively high nominal power
  - Almost every household have a such device or will have in near future

Methodology

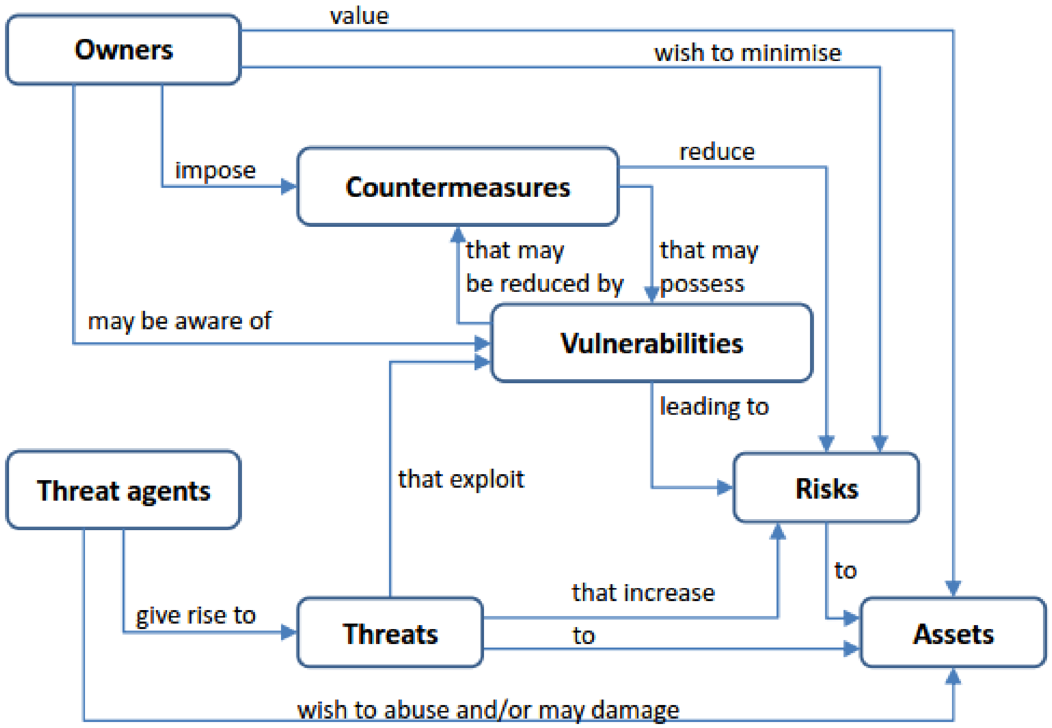
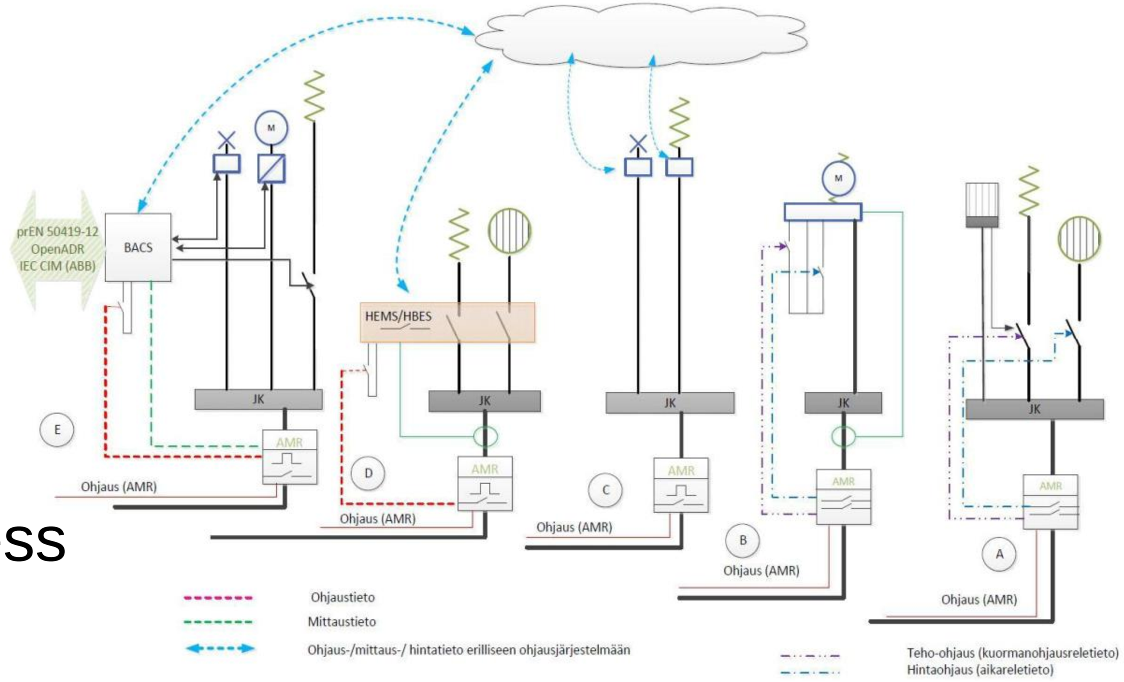


Figure 4: the elements of a risk and their relationships according to ISO 15408:2005

- Instead of recognizing all possible threat and vulnerability combinations, we would first consider the impact scenarios, which may create a significant impact in the system
  - what kind of load is required
  - what kind of devices can cause this
  - what kind of home automation is controlling these
- Estimate how large the impact will be on physical level and what it means as a number/capacity of hacked resources and how many of such resources Finland have today and near future

Simple calculation of 3*25 A house

- Disconnecting building or device by overloading main fuses; 3*25 A fuse (17 kW) will melt in 17 min with ~40 A (27 kW)
- Rated powers
  - Space heating: ~10 kW (direct), ~11+11 kW (heat pump + resistors)
  - Hot water: ~11 kW
  - EV: 3-11 kW
  - Home appliances
  - Lights
- **Possibilities to switch on all/many devices simultaneously**
  - Home automation with cloud / Internet access
  - Device specific remote access



Impact scenarios

- **Local voltage quality challenge**
  - Rural area distribution networks are commonly close to technical limits (system condition)
  - Load or production change by synchronizing the behaviour (attack)
  - Voltage variations in weak network exceeding the limits of the power quality standards leading to customer complains and grid reinforcement need (impact scenario)
  - Rough estimate: 100-500 kW in weak MV grid and 10-100 kW in weak LV grid

Impact scenarios

Local overloading

- Grid is exceptional high loading condition or operated with alternative grid topology (system condition)
- Load or production change by synchronizing the behaviour (attack)
- Current limit of a transformer or a line is exceeded to create thermal damage (impact scenario)
  - 100 kW MV/LV transformer supplies 10 residential buildings
  - 10 EVs are charging with full power (3*16 A ~ 11 kW) = 110 kW
  - Normal loading condition would be remarkable less due to unsynchronized loading
- Rough estimate: 200-500 kW

Distribution grid impacts

- Assume that 50/100 % of customers will invest for air-to-air heat pumps (HPs) or electric vehicles (EVs)
- Attacker has a control of all/many of them
- Calculate the impact of attack by comparing two load flow cases:
  - All HPs or EVs are operated at nominal power during the peak loading of a distribution grid
  - Normal loading conditions of a distribution grid
- Modified load profiles of customer groups:
  - Additional HPs and EVs modify the profiles → How high is a normal peak loading
  - Attack profile: profile of other demand + nominal power of HP or EV
- Peak loading occurs during different hours for primary transformers, MV feeders, distribution transformers and LV feeders → impact area

Distribution grid impacts

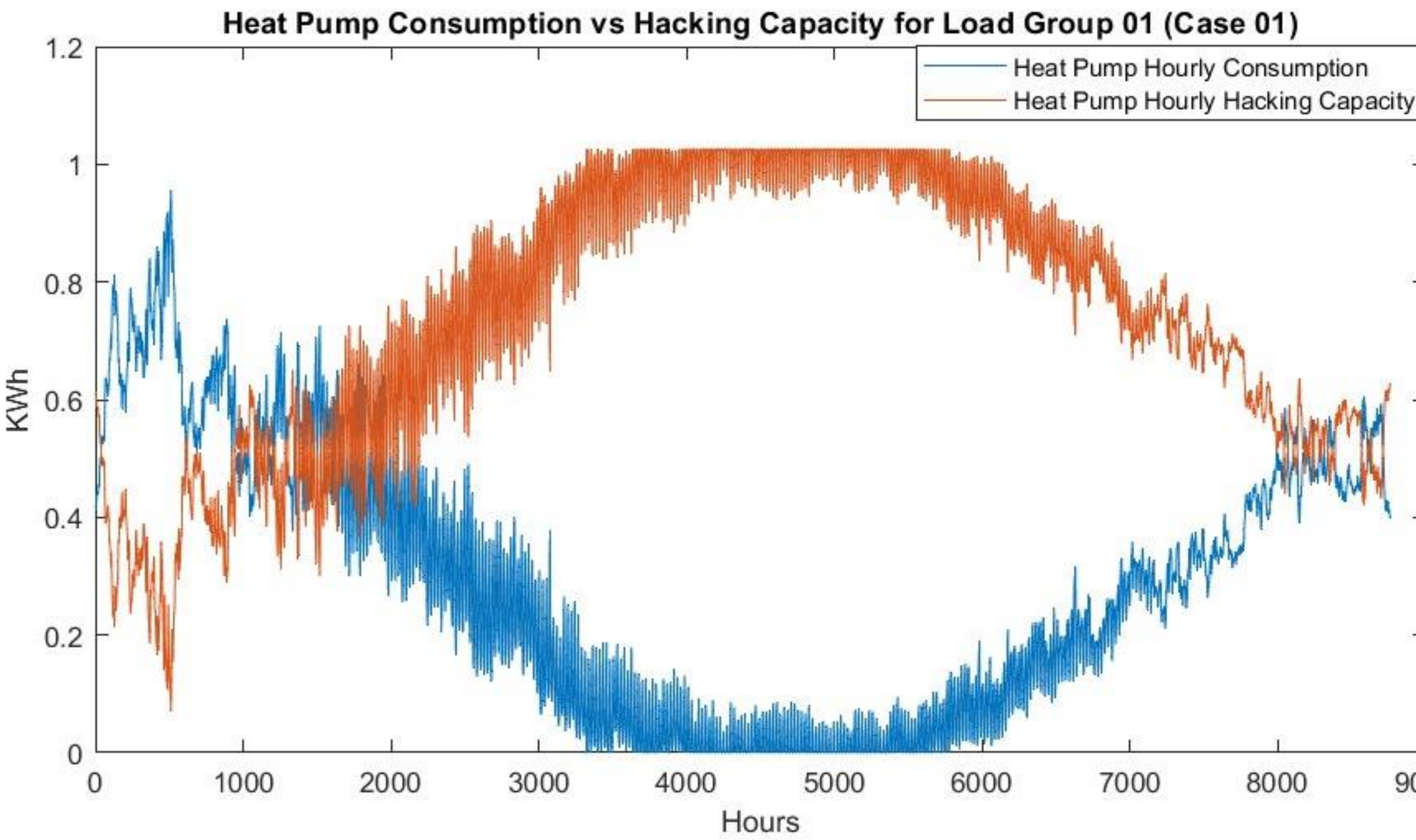
- 1: single family house, electric heating, heat storage <300 l
- 2: single family house, electric heating, heat storage 300 l
- 11: single family house, no electric heating, no electric sauna
- 12: single family house, no electric heating, electric sauna
- 13: row house, no electric heating, no electric sauna
- 14: row house, no electric heating, electric sauna
- 17: row house, electric heating
- 18: vacation home
- 23: (dairy) farming house, electric sauna
- 24: (dairy) farming house, electric sauna, electric heating

Tampere University

Distribution grid impacts

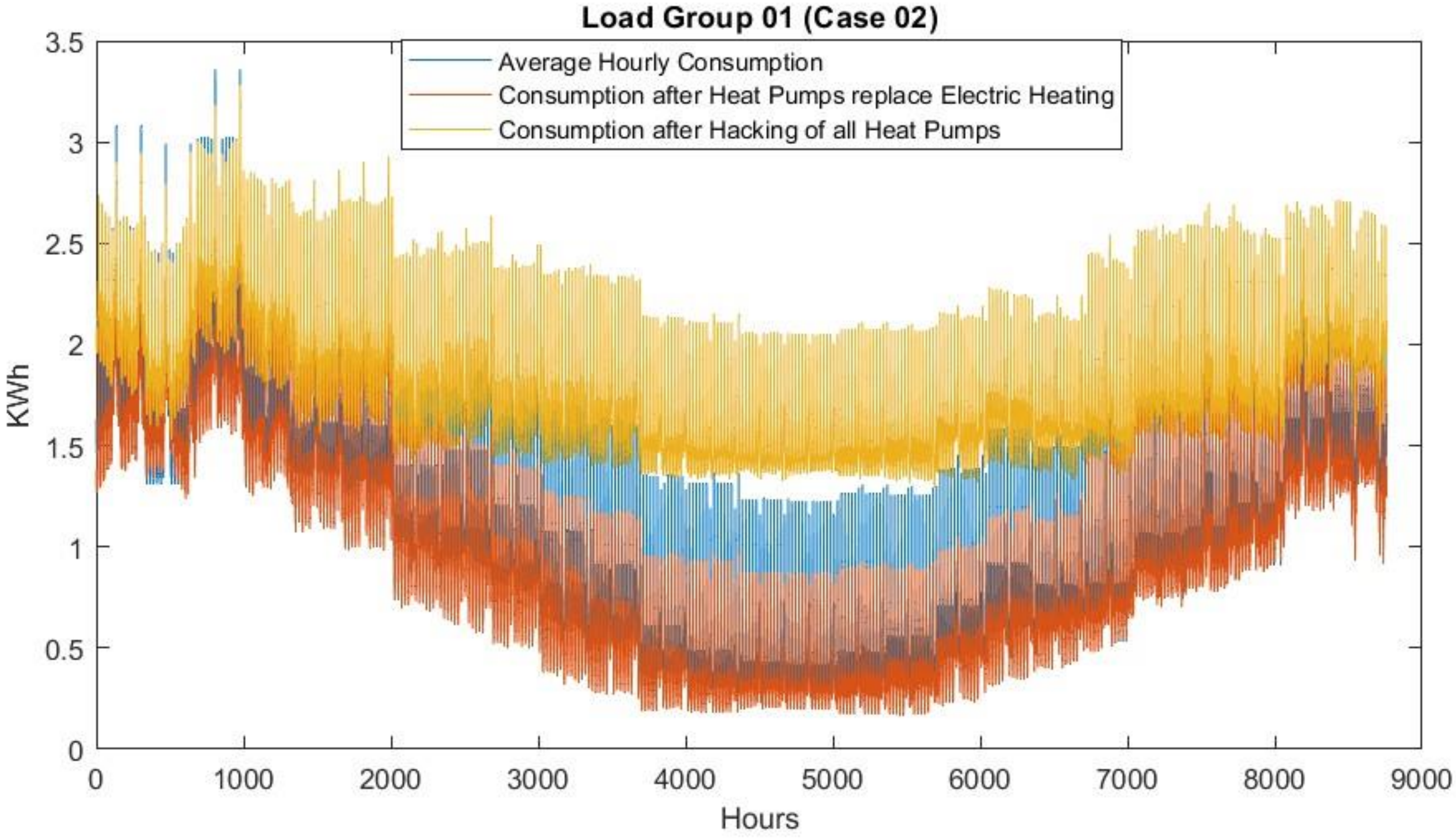
Heat Pump Load Simulation

- Temperature data of year 2022 is used for formulation of heat pump load curve. Data is taken from Partala observation station of FMI.
  - Indoor temperature is set at 17 degree Celsius.
  - Sum of Heating Degree Days is calculated for the region under study
  - Hourly Coefficient of Performance is calculated based on indoor and outdoor temperatures along with consideration of fault factor.
- Assumptions
  - Heating space of each customer is based on their annual energy consumption.
  - Heat pump is then sized to cover complete space heating requirement of each customer throughout the year.
- Heat pump model is then developed specifically for the area

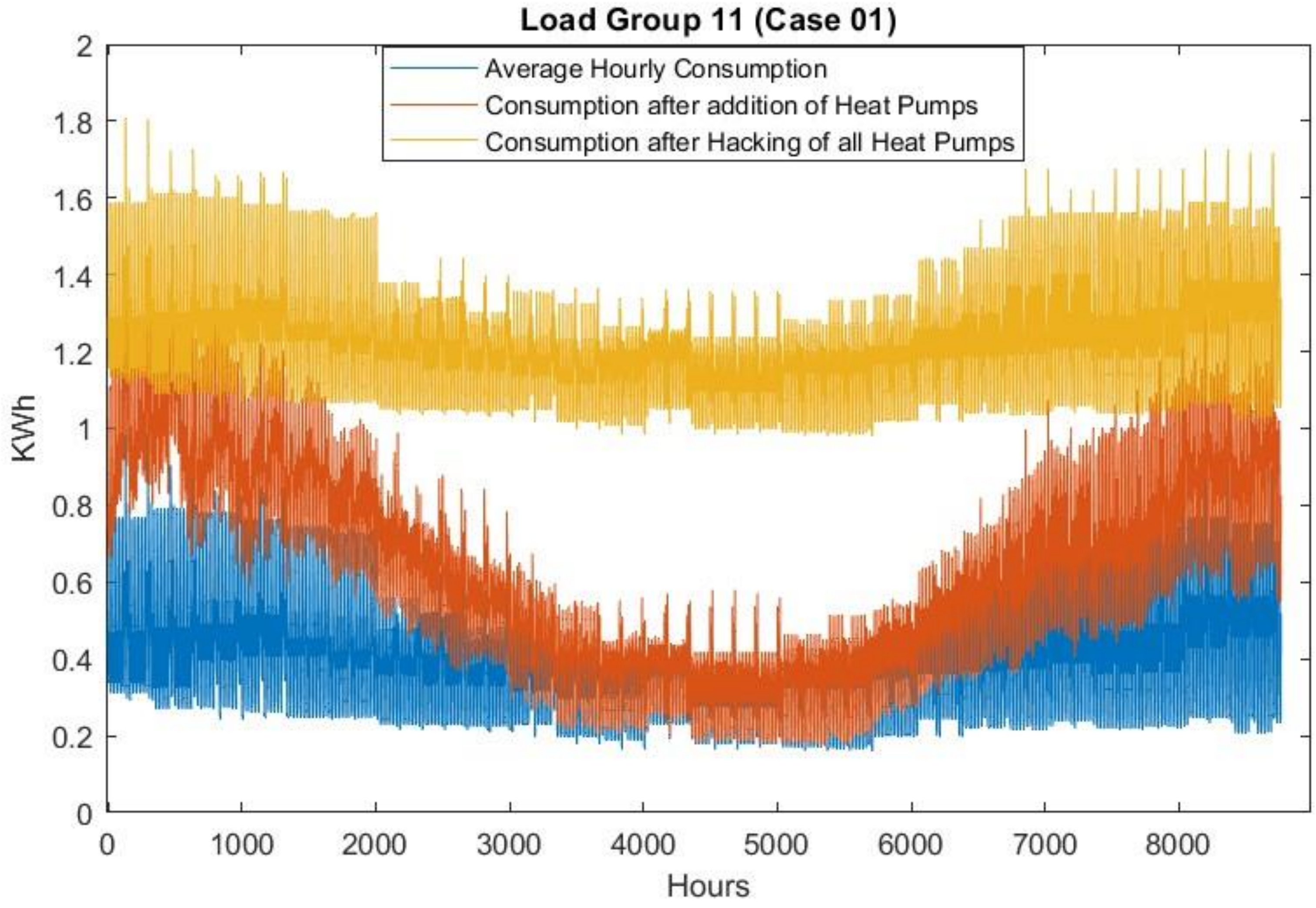

Heat Pump Consumption vs Hacking Capacity for Load Group 01 (Case 01)
Heat Pump Hourly Consumption
Heat Pump Hourly Hacking Capacity
KWh
Hours
0
0.2
0.4
0.6
0.8
1
1.2
1000
2000
3000
4000
5000
6000
7000
8000

Tampere University

Example of scenario 2 for Electric Heated Load Group 01



Example of Scenaio 01 for Non-Electric Heated Load Group 11

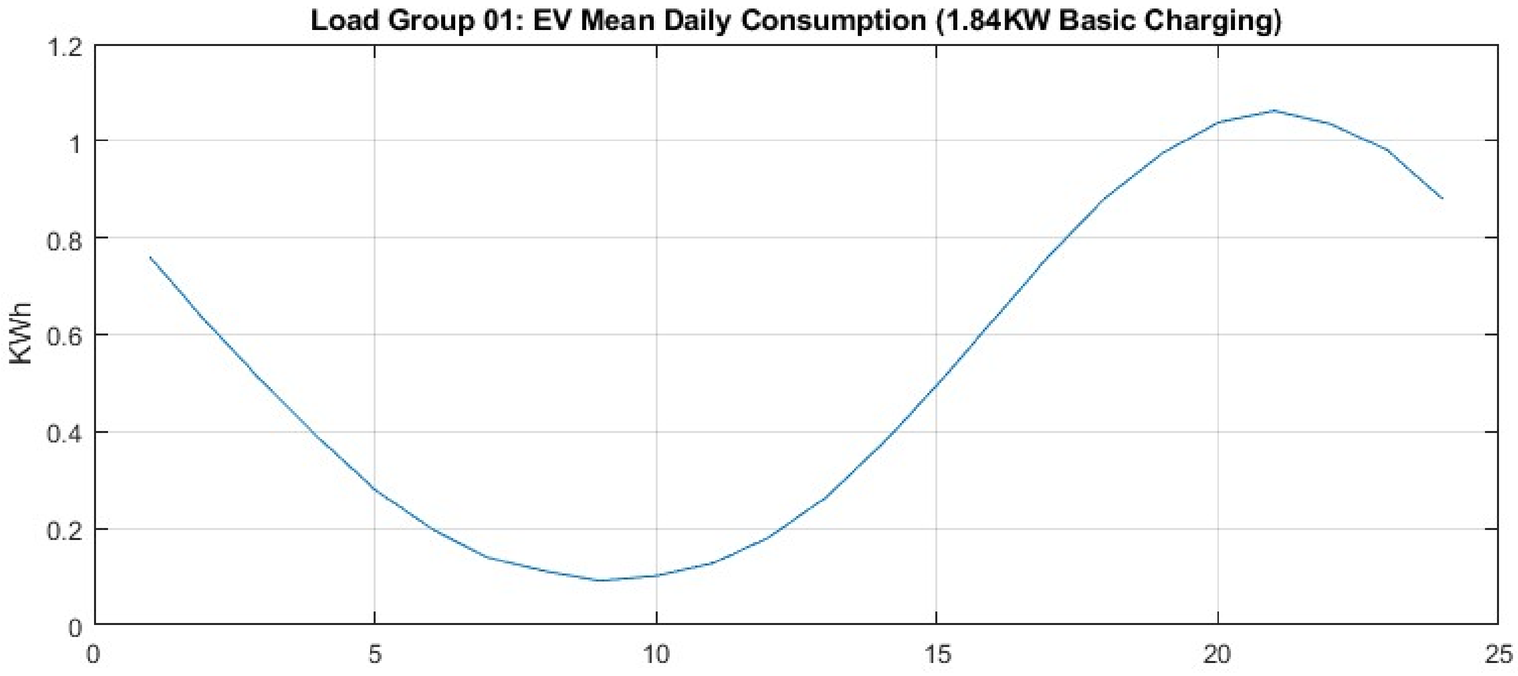


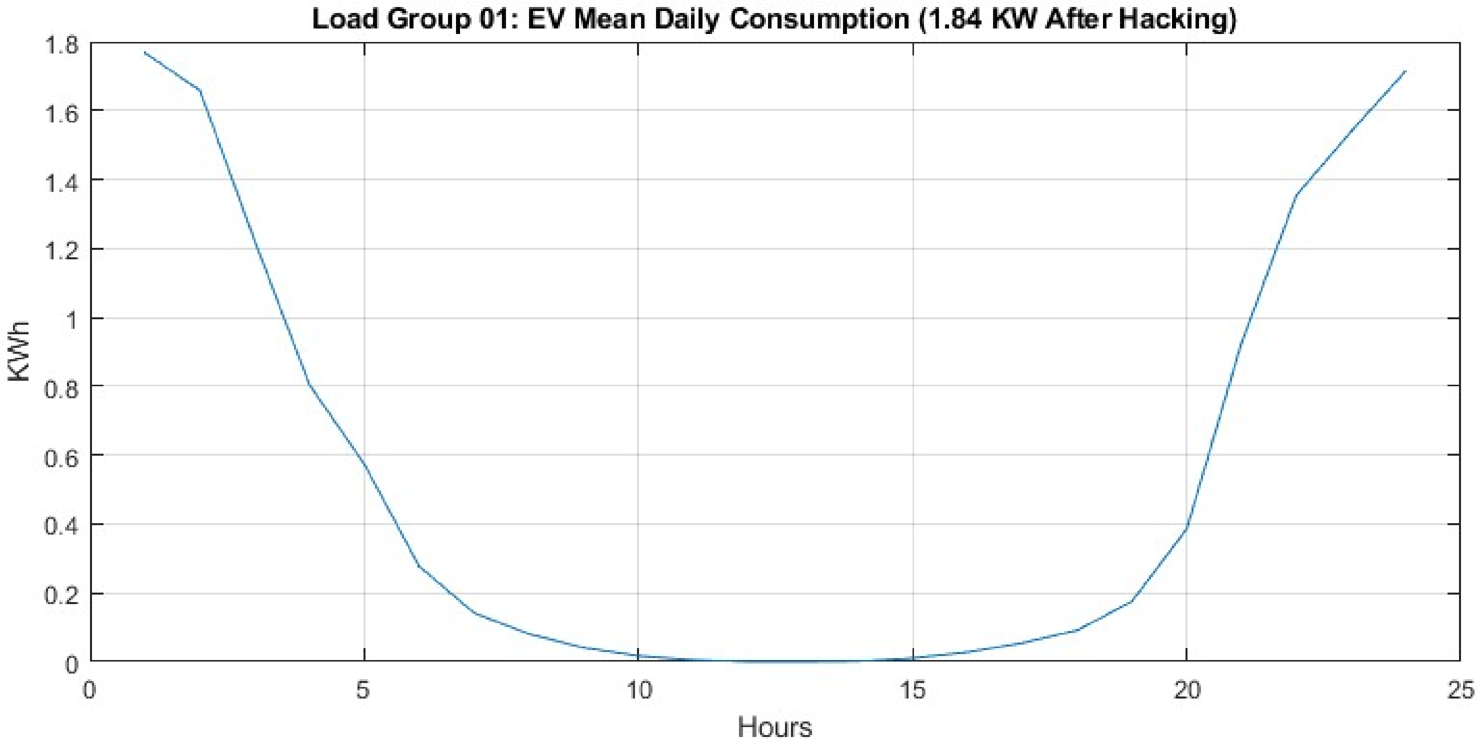
Distribution grid impacts

Electric vehicle charging

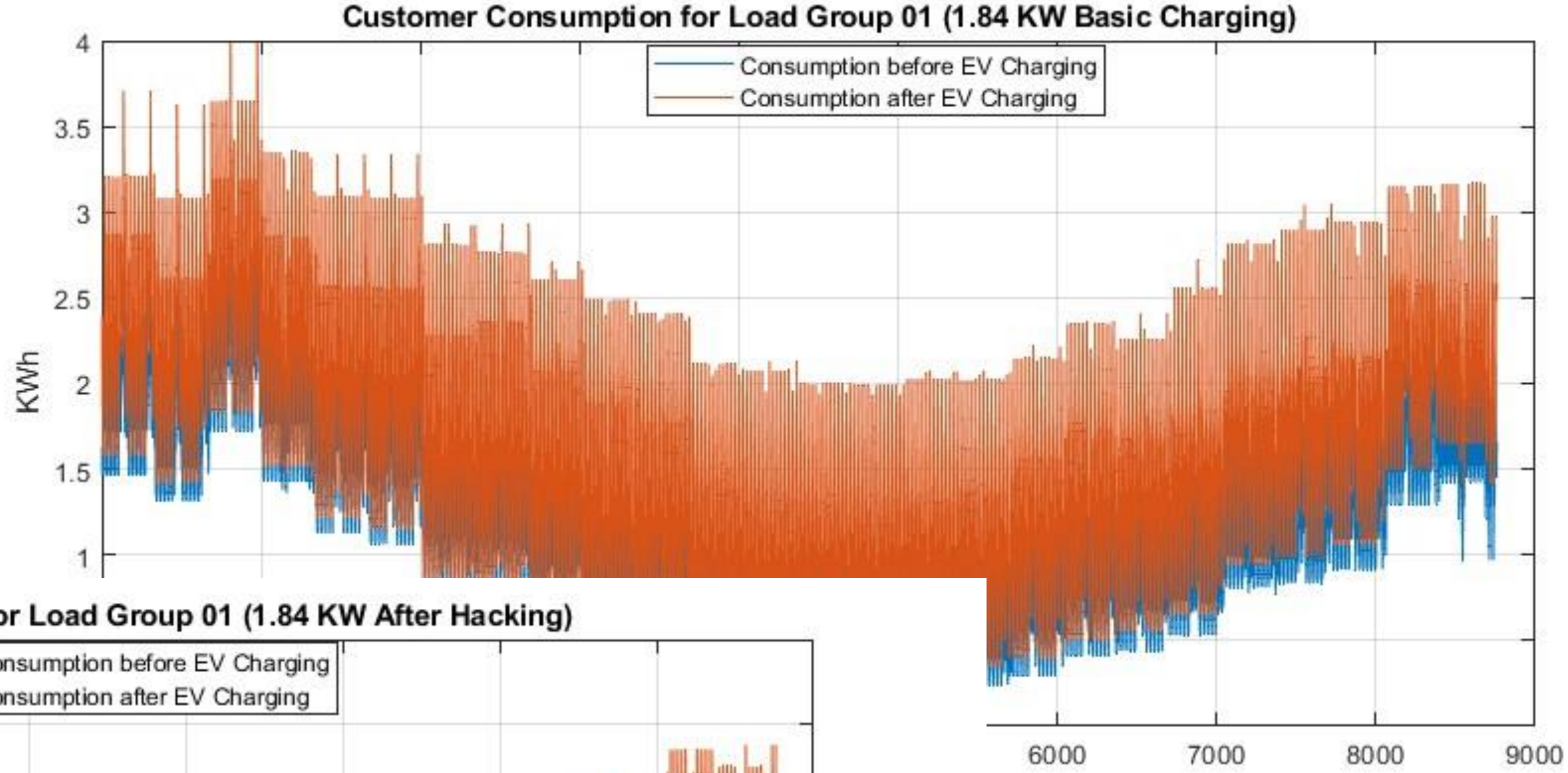
- Mean and standard deviation values for daily arrival time and driving distance are taken from Traficom data.
- Random assignment is done to each customer.
- Charging powers of 1.84 and 11.1 KW are used to model home charging.
- One Electric vehicle is assigned per house.
- Attack is realized on a moment when the most vehicles are available for charging

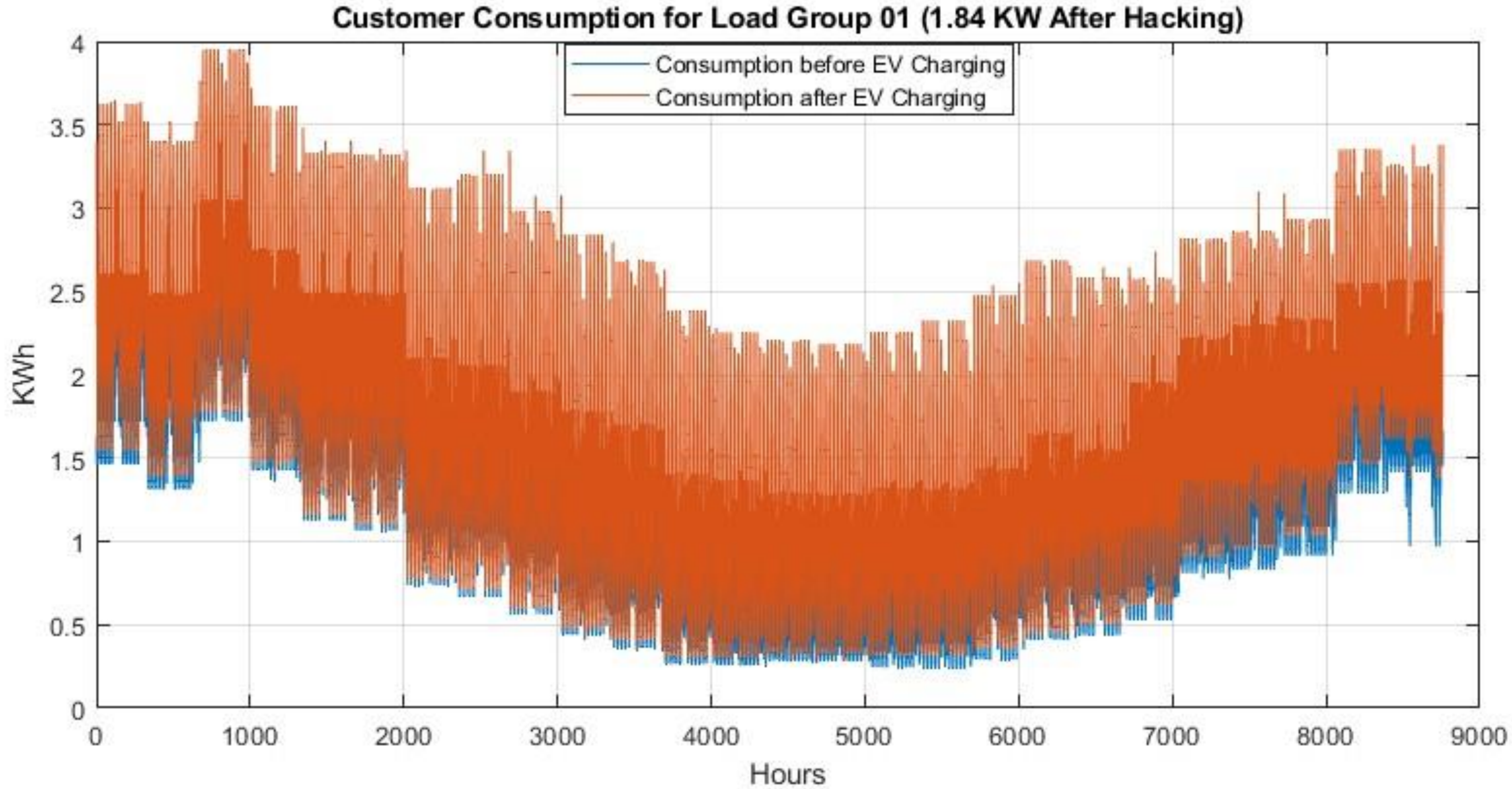
Group1 1.84 kW charging



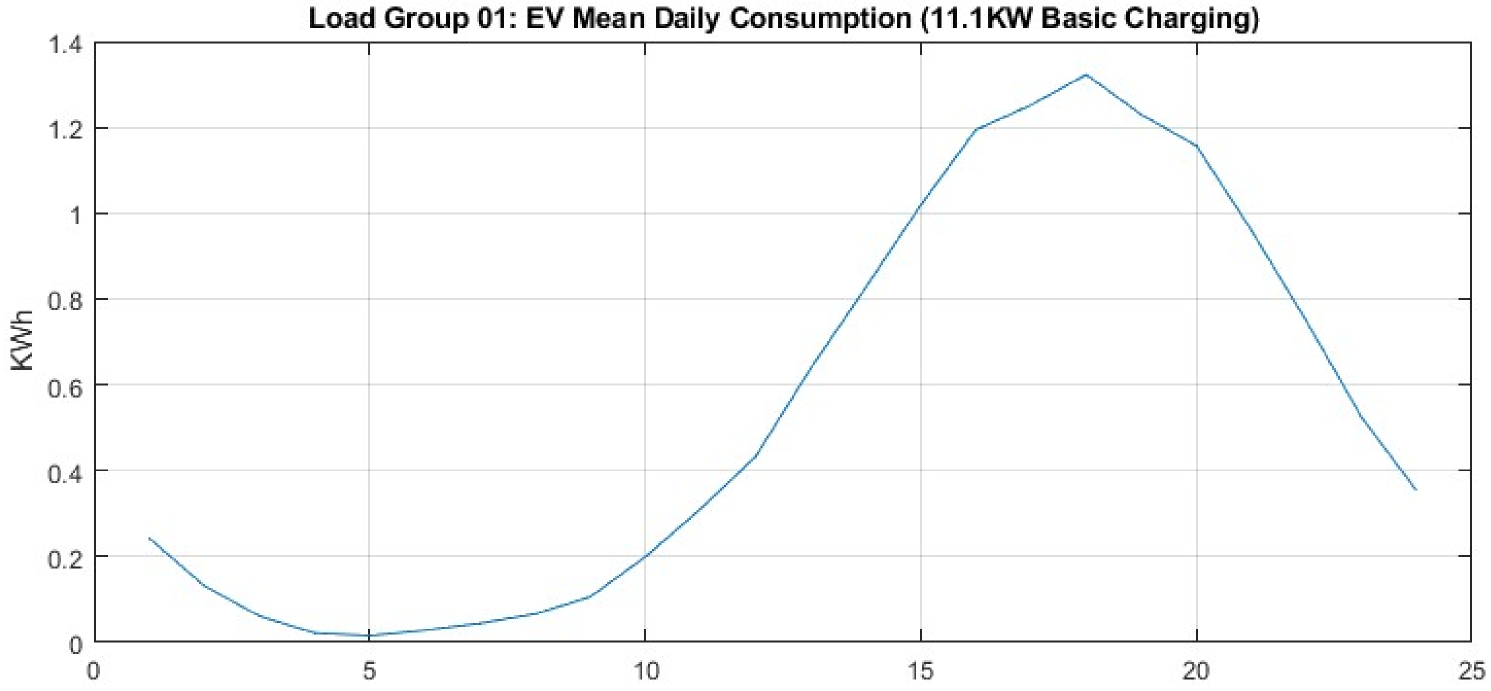


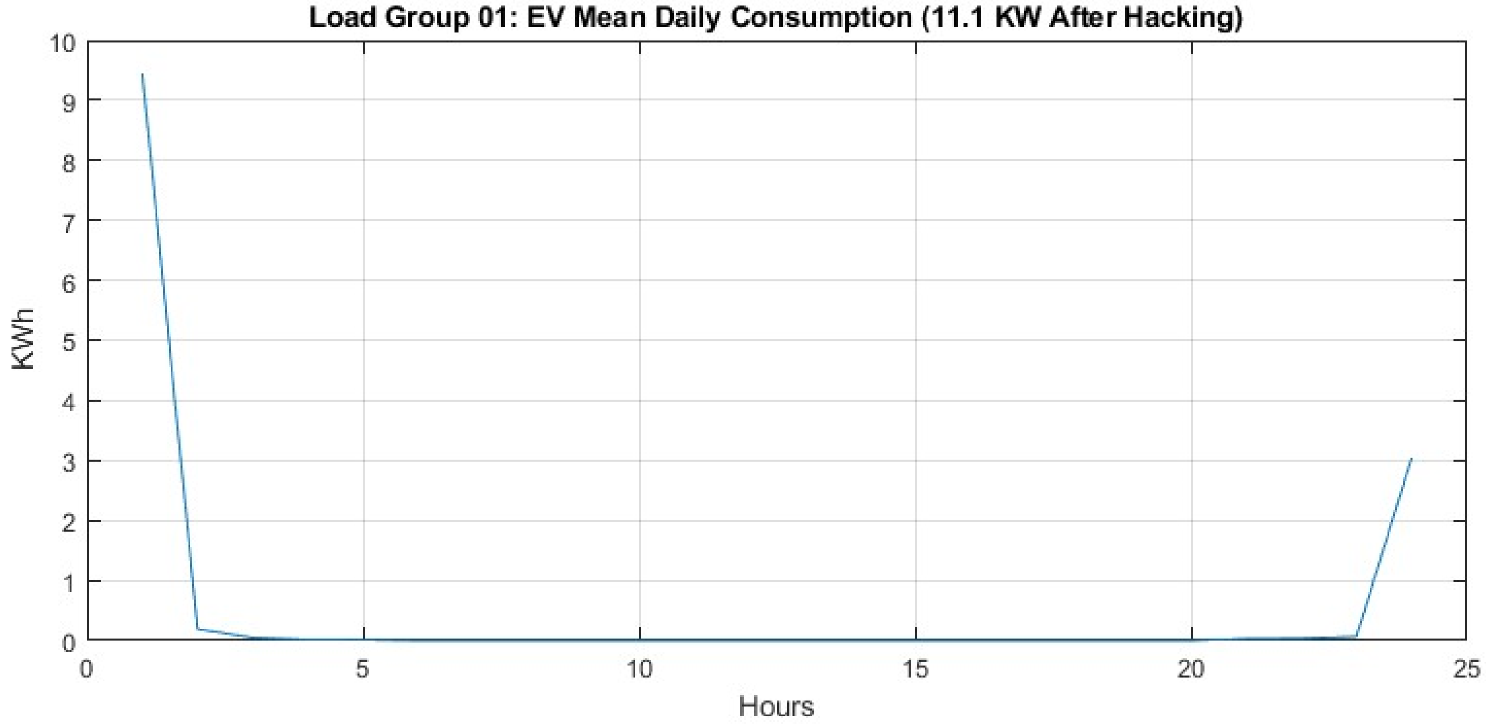
Group1 1.84 kW charging





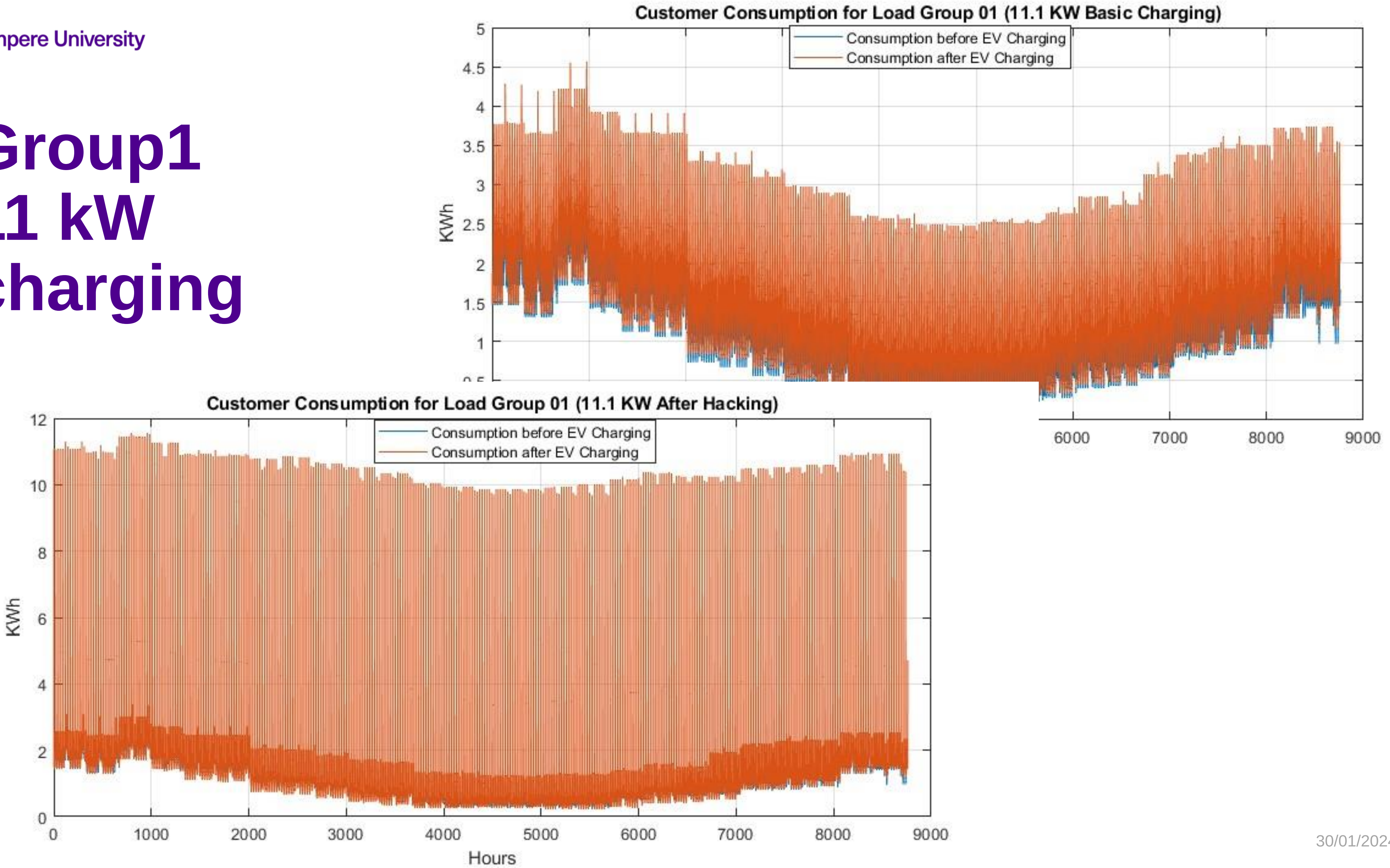
Group1
11 kW
charging



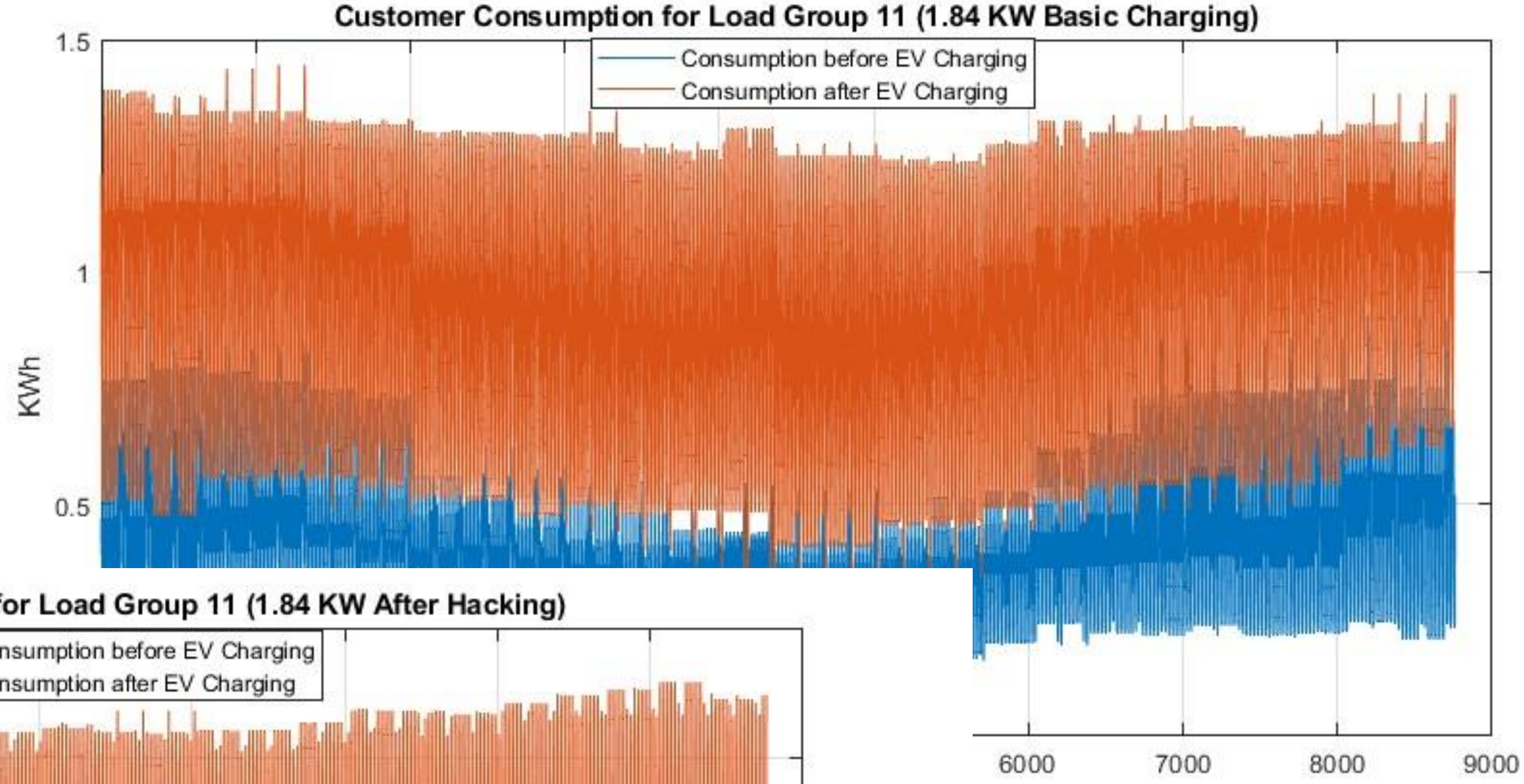


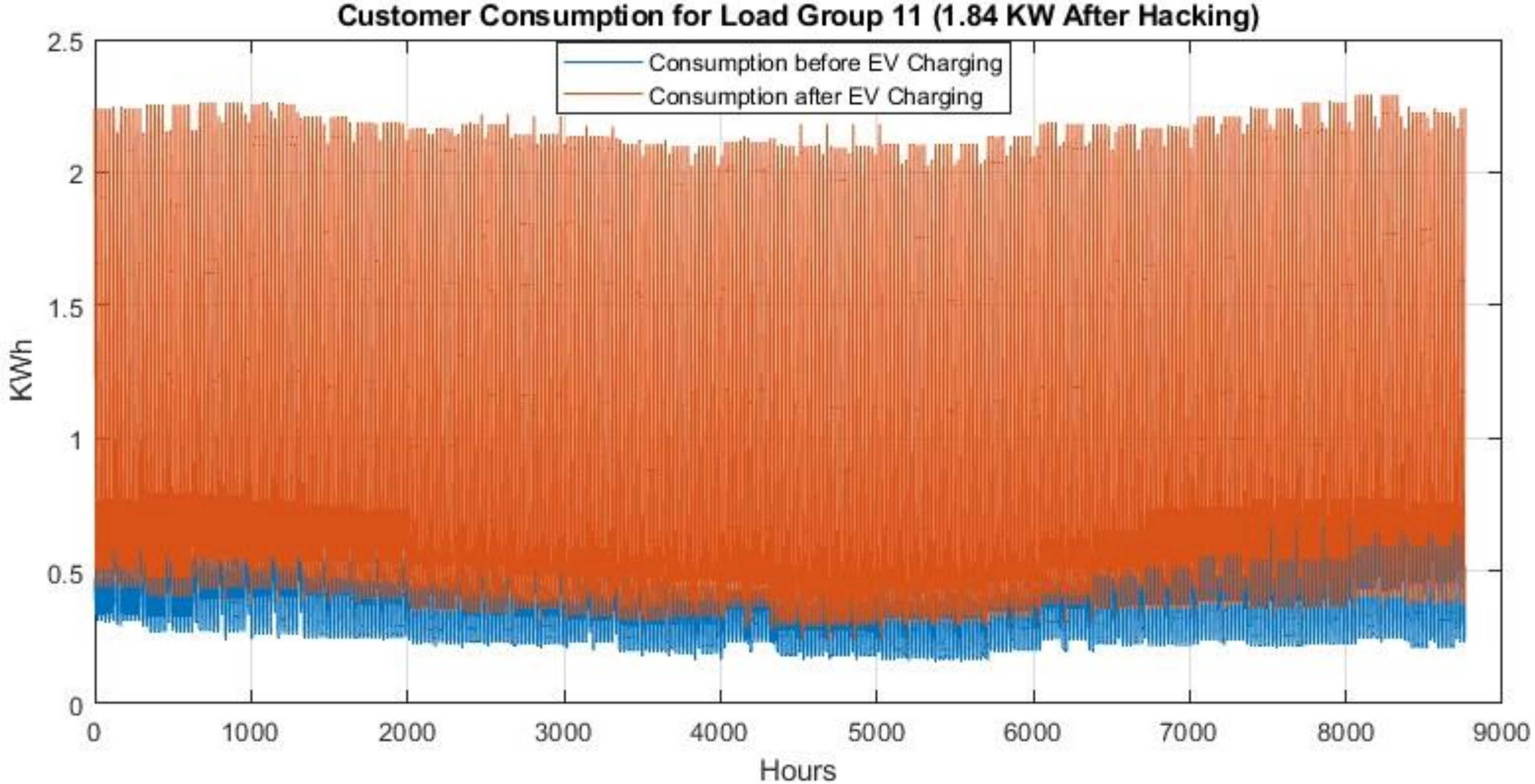
Tampere University

Group1
11 kW
charging



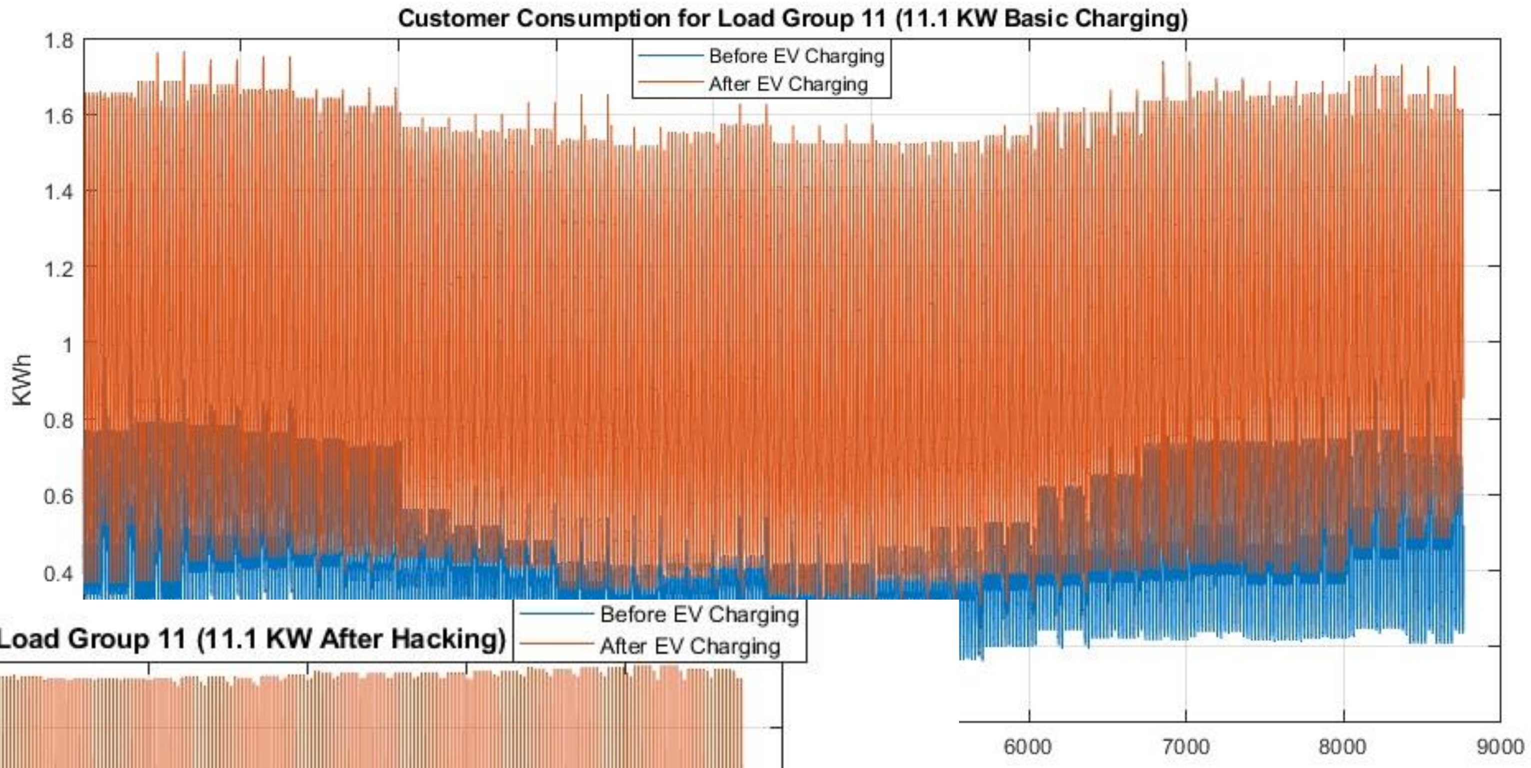
Group11 1.84 kW charging

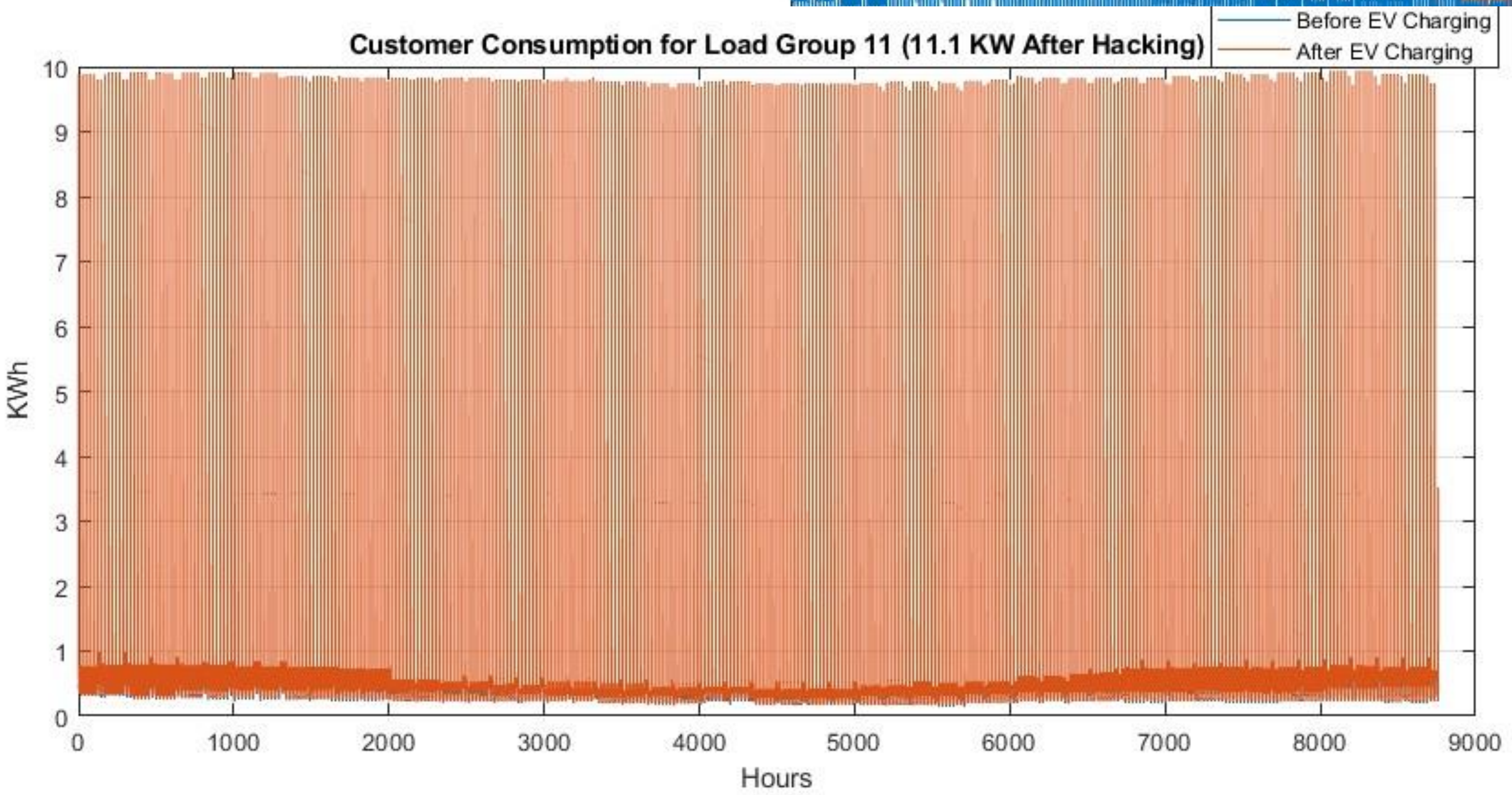




Tampere University

Group11
11 kW
charging





Conclusions

Customer	Energy	Peak load (normal)	Peak load (attack)
Direct electric heating		Q	
+ heat pump	Decrease	<Q	Q
+ electric vehicle 1.84 kW	Increase	~1.2*Q	~1.4*Q
+ electric vehicle 11 kW	Increase	1.2-1.7*Q	3-4.5*Q
Non-electric heating		QQ	
+ heat pump	Increase	~2*QQ	~3*QQ
+ electric vehicle 1.84 kW	Increase	~1.7*QQ	~2.5*QQ
+ electric vehicle 11 kW	Increase	~2*QQ	8-13*QQ

Note! Some peak loads of service points are very high under an attack, when the service point includes multiple appartments (row house, appartment building). This is due to very strong synchronization effect.

Grid impact (transformer and cable loadings and node voltages) calculations are under study at the moment. It is expected that the **strong peak load synchronization of an attack** will create more issues for a grid than for customers.