Electric Vehicle Authentication and Secure Metering in Smart Grids

Yutaka Yamaguchi, Kyushu University, Japan
Email: yamaguchi.yutaka.534@s.kyushu-u.ac.jp

Dirceu Cavendish, Kyushu Institute of Technology, Japan
Koide Hiroshi, Kyushu University, Japan

A short resume of the presenter

Yutaka Yamaguchi

- Fourth year student at Kyushu University
- Japanese national

IoTRC Kyushu Institute of Technology

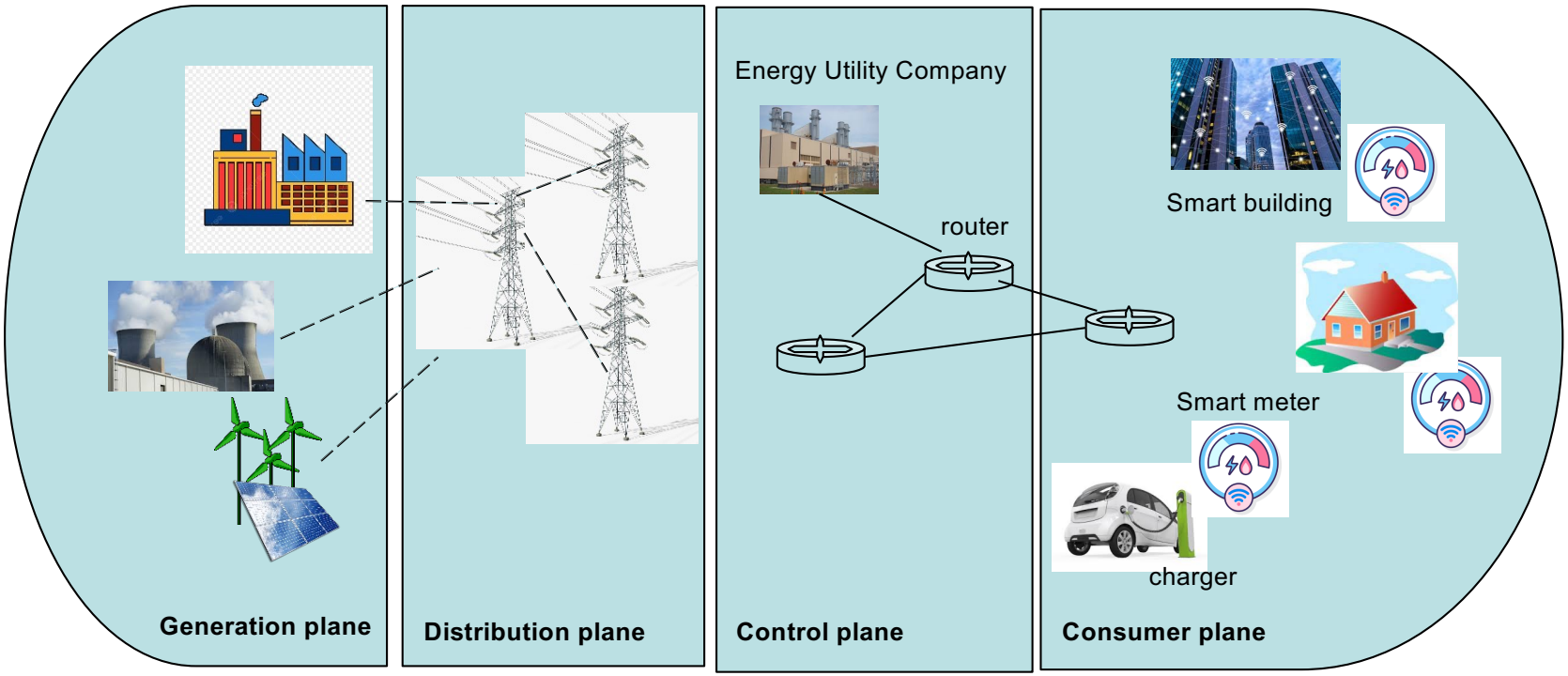
Topics of research

- Moving Target Defense
- Attacks Tracer

IoTRC Kyushu Institute of Technology

Abstract

Leverage SIM card to electric vehicles.



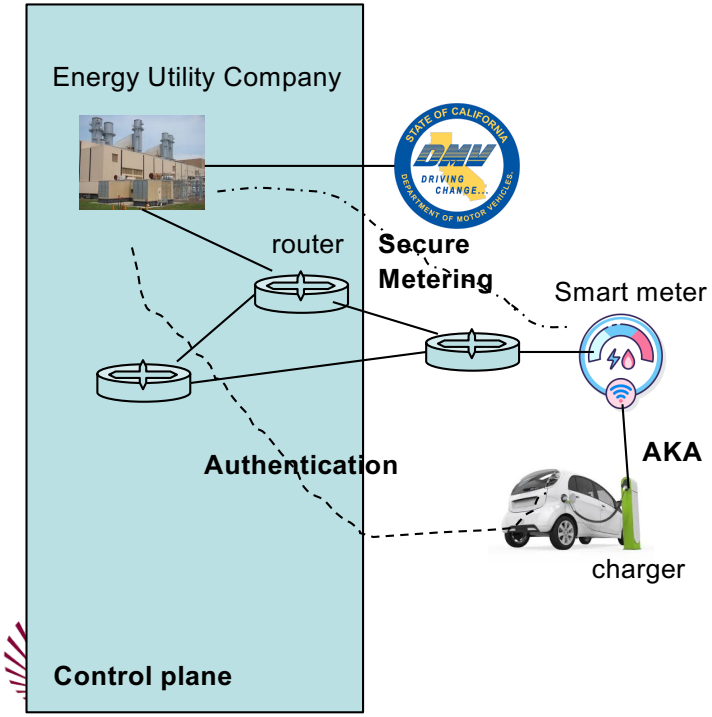
KYUSHU UNIVERSITY

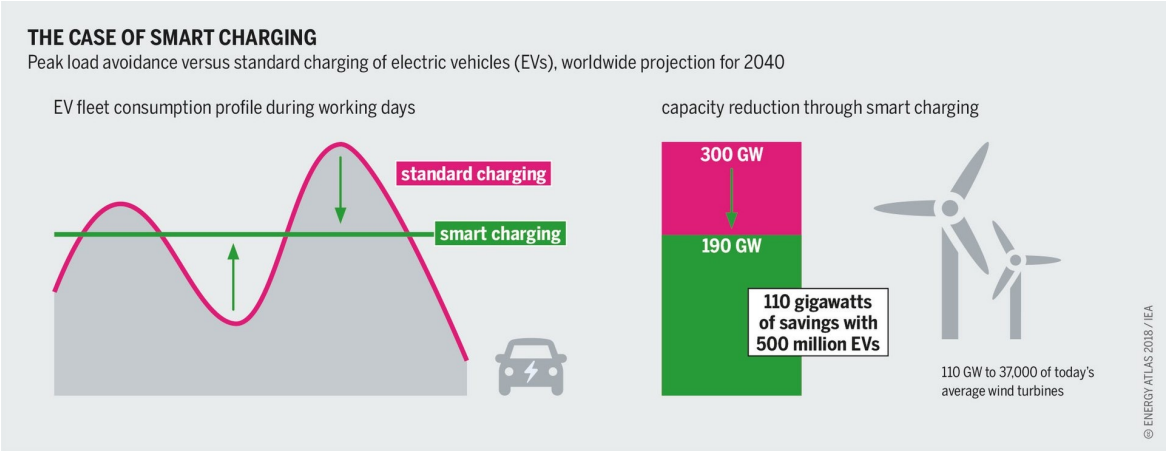
IoTRC Kyushu Institute of Technology

Utility companies and Security

Utility Company Security

- Monitoring/control of regions energy consumption
  - overload/outage monitoring
  - Peak Load EV Charging avoidance(energy aggregators)
- Security:
  - Advanced Metering Infrastructure (AMI) monitors grid resources (e.g. transformers) and energy demand/consumption (smart meters).
  - Consumer subscription reliability/fraud protection
    - EV subscriber authentication protocol (AKA protocol:auth/secure metering)





KYUSHU UNIVERSITY

IoTRC Kyushu Institute of Technology

Safe EV Charging

EV Charging Requirements

- Mutual authentication of service provider (PUC) and consumer/vehicle

- Secure charging metering:

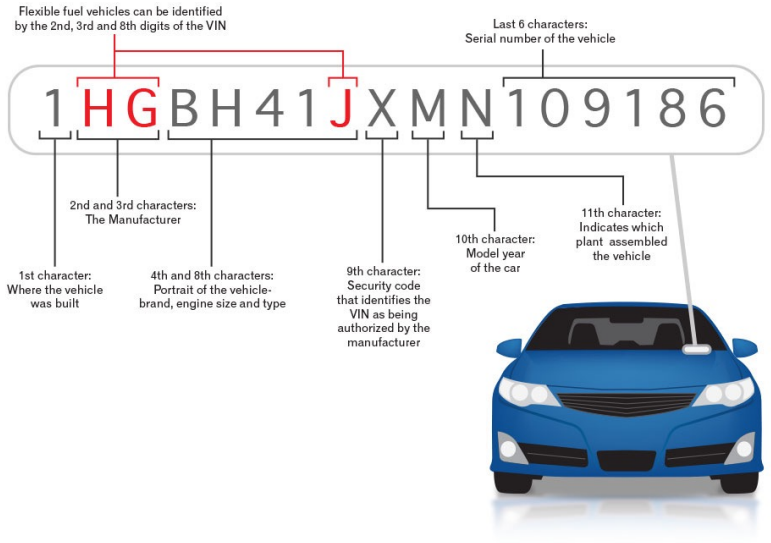
KYUSHU UNIVERSITY

IoTRC Kyushu Institute of Technology

To achieve safe EV charging

・Authentication should be performed using symmetric key authentication.

・Authentication keys should be shared only between users and service providers.

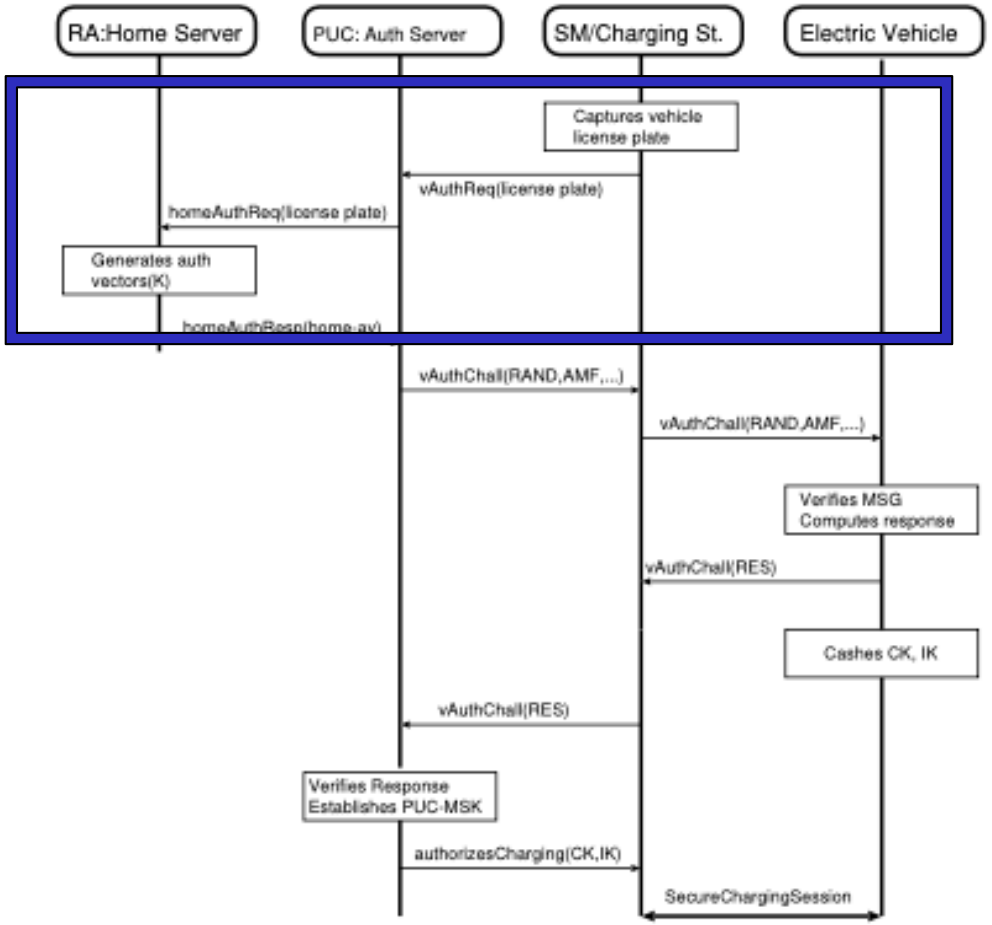


KYUSHU UNIVERSITY

IoTRC Kyushu Institute of Technology

Key Authentication Description

```
SM
home AKA communication initiation

PUC
(Home_AKA)Send_License_Plate

HS
(Home_AKA)Generate_Key
(Home_AKAG)Generate_Authentication_Vector
SQN: 188875110173367
(Home_AKA)Generate_XRES_MAC
XRES: 11665645253085518279
MAC: 10822972401101129059

PUC
(Home_AKA)Extract_RAND_AMF_SN_SQN_XRES_MAC

SM
(Home_AKA)Send_RAND_AMF_SQN_XMAC

EV
(Home_AKA)Generate_RES_AK_CK_IK_MAC
RES: 11665645253085518279
XMAC: 10822972401101129059
AK: 34423461800822
CK: 22491236809316653975152983170713002 81
IK: 22851957903633981703100711352816157 3847
OK! MAC = XMAC
PUC_MSK = 8864995077770743931886362418142198 22

SM
(Home_AKA)Forward_Encrypted_RES

PUC
SQN: 188875110173368
(Home_AKA)Compare_RES_and_XRES
OK! XRES = RES
PUC_MSK: 8864995077770743931886362418142198 22
```



Home Authentication and Key Agreement

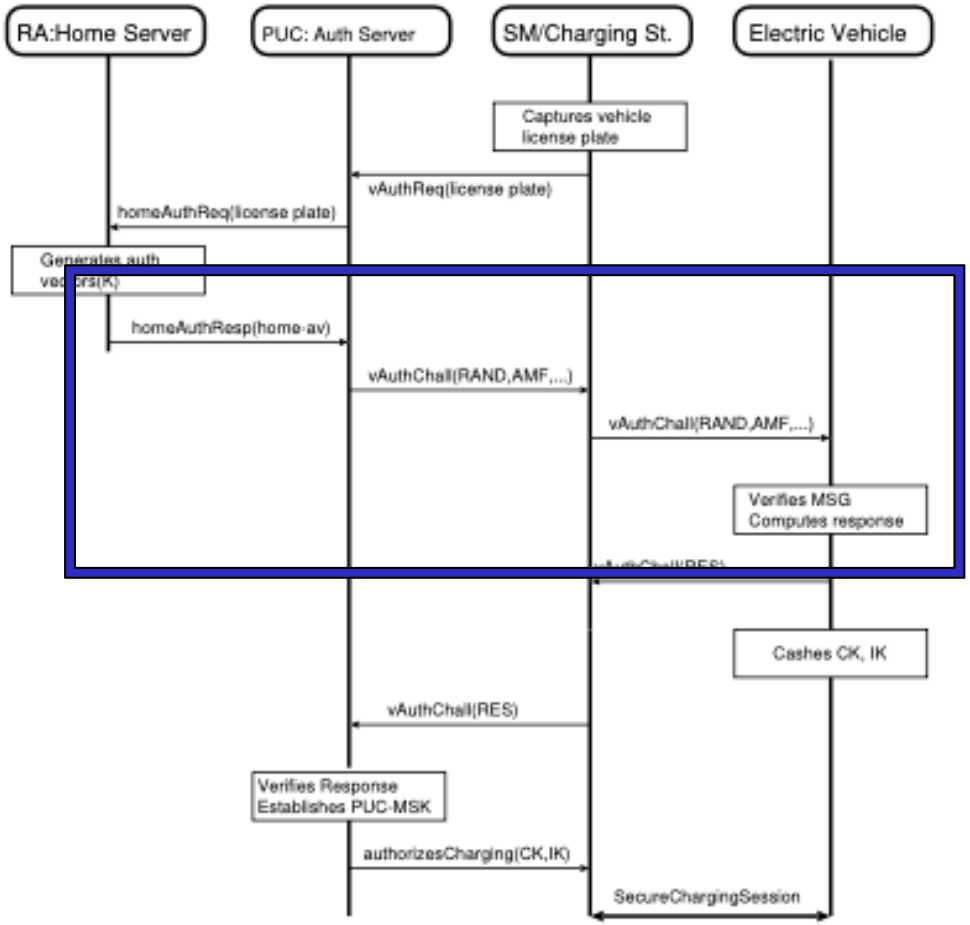
Figure 3: Home Authentication and Key Agreement

KYUSHU UNIVERSITY

IoTRC Kyushu Institute of Technology

Key Authentication Description

```
SM
home AKA communication initiation

PUC
(Home_AKA)Send_License_Plate

HS
(Home_AKA)Generate_Key
(Home_AKAG)Generate_Authentication_Vector
SQN: 188875110173367
(Home_AKA)Generate_XRES_MAC
XRES: 11665645253085518279
MAC: 10822972401101129059

PUC
(Home_AKA)Extract_RAND_AMF_SN_SQN_XRES_MAC

SM
(Home_AKA)Send_RAND_AMF_SQN_XMAC

EV
(Home_AKA)Generate_RES_AK_CK_IK_MAC
RES: 11665645253085518279
XMAC: 10822972401101129059
AK: 34423461800822
CK: 22491236809316653975152983170713002 81
IK: 22851957903633981703100711352816157 3847
OK! MAC = XMAC
PUC_MSK = 8864995077770743931886362418142198 22

SM
(Home_AKA)Forward_Encrypted_RES

PUC
SQN: 188875110173368
(Home_AKA)Compare_RES_and_XRES
OK! XRES = RES
PUC_MSK: 8864995077770743931886362418142198 22
```



Home Authentication and Key Agreement

Figure 3: Home Authentication and Key Agreement

KYUSHU UNIVERSITY

IoTRC Kyushu Institute of Technology

Key Authentication Description

```
SM
home AKA communication initiation

PUC
(Home_AKA)Send_License_Plate

HS
(Home_AKA)Generate_Key
(Home_AKAG)Generate_Authentication_Vector
SQN: 188875110173367
(Home_AKA)Generate_XRES_MAC
XRES: 11665645253085518279
MAC: 10822972401101129059

PUC
(Home_AKA)Extract_RAND_AMF_SN_SQN_XRES_MAC

SM
(Home_AKA)Send_RAND_AMF_SQN_XMAC

EV
(Home_AKA)Generate_RES_AK_CK_IK_MAC
RES: 11665645253085518279
XMAC: 10822972401101129059
AK: 34423461800822
CK: 22491236809316653975152983170713002 81
IK: 22851957903633981703100711352816157 3847
OK! MAC = XMAC
PUC_MSK = 8864995077770743931886362418142198 22

SM
(Home_AKA)Forward_Encrypted_RES

PUC
SQN: 188875110173368
(Home_AKA)Compare_RES_and_XRES
OK! XRES = RES
PUC_MSK: 8864995077770743931886362418142198 22
```

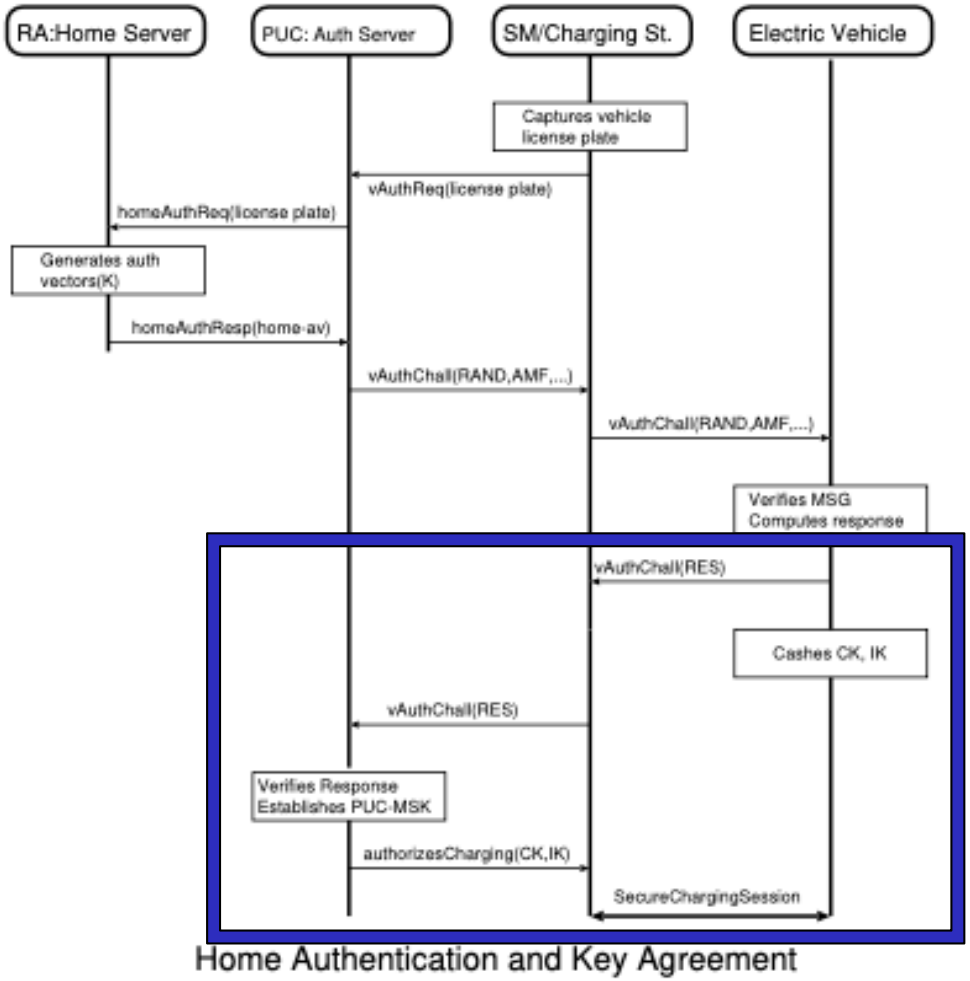


Figure 3: Home Authentication and Key Agreement

KYUSHU UNIVERSITY

IoTRC Kyushu Institute of Technology

IMPLEMENTATION PROOF OF CONCEPT

```python
class HomeServer(pykka.ThreadingActor):
    def __init__(self):
        super(HomeServer, self).__init__()

    def link_class(self, instance_name):
        self.PUC_ref = instance_name

    def on_receive(self, message):
        print("")
        print("HS")
        self.message = message
        self.order = message["order"]

        if(self.order == "Send_License_Plate"):
            print("(Home_AKA)Generate_Key")
            self.license_plate = message["license_plate"]
            self.Generate_Authentication_Vector()

    def Generate_XRES_MAC(self):
        print("(Home_AKA)Generate_XRES_MAC")
        self.XRES = Create_RES(self.key, self.RAND, self.OP)
        self.MAC = Create_MAC(self.key, self.RAND, self.AMF, self.OP, self.SQN)
        print(f'XRES: {self.XRES}')
        print(f'MAC: {self.MAC}')
        self.Send_Authentication_Vector()


    def Send_Authentication_Vector(self):
        self.PUC_ref.tell({"order":"Send_Authentication_Vector", "RAND":self.RAND,
```

Library : pykka, Crypto.Cipher.AES

Communication between HS, PUC, SM, and EV was implemented by sending a dictionary type list with the tell function of pykka.

The ciphers were generated using the library Crypto.Cipher.AES

KYUSHU UNIVERSITY

IoTRC Kyushu Institute of Technology

CONCLUSION AND FUTURE WORK

- A symmetric key based authentication and key agreement protocol.

- There is no need for the smart meter to store authentication information.

- New encryption and integrity keys are used by the smart meter for each charging session.

The framework hence reduces Smart Meter security requirements, as well as its attack surface.

KYUSHU UNIVERSITY

IoTRC Kyushu Institute of Technology