Security Challenges for Customer Domain in the Smart Grid

Oct 17, 2011

Myongji University

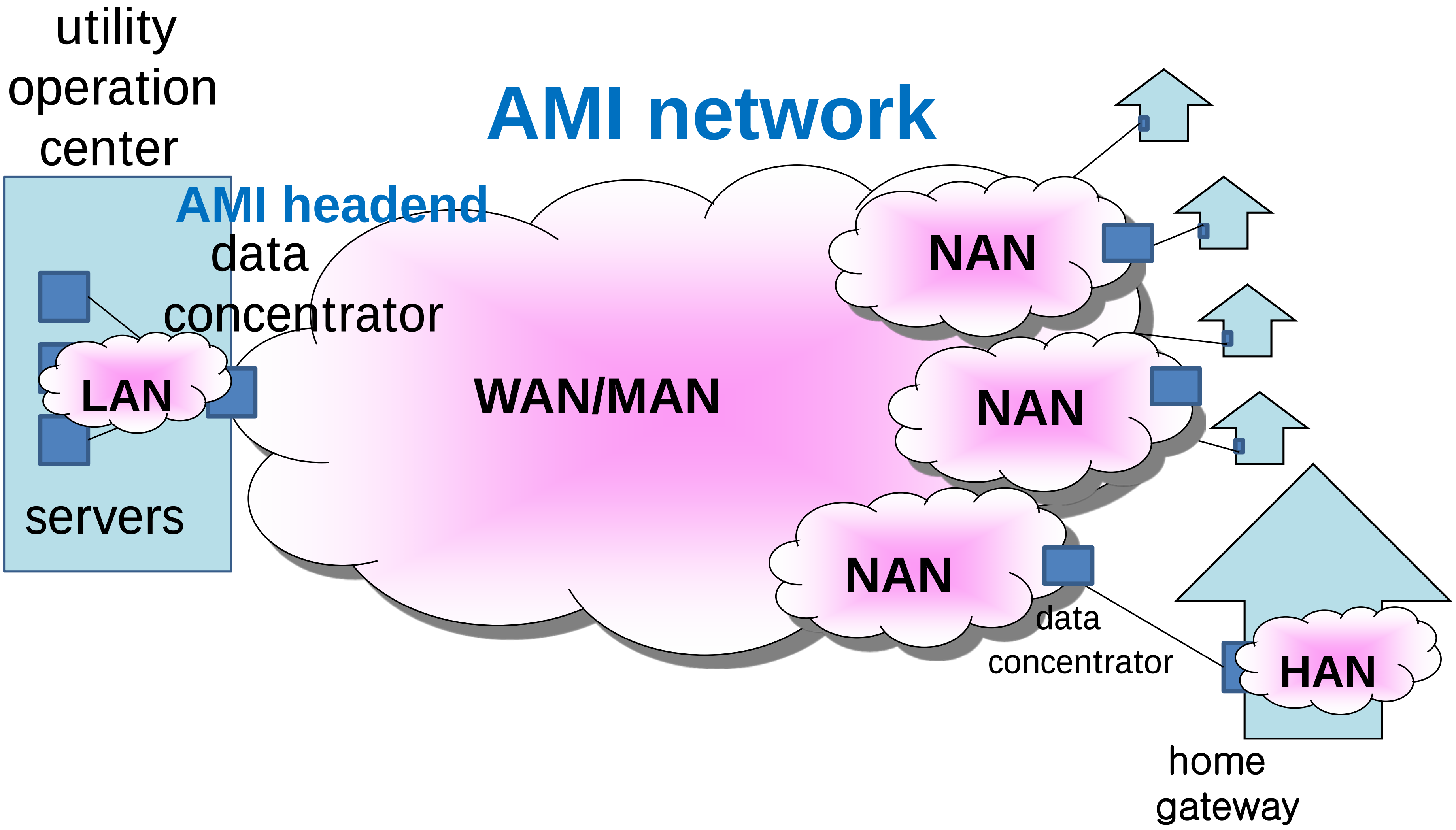
Sugwon Hong

APAP 2011, Special Session: Smart Grid, Beijing

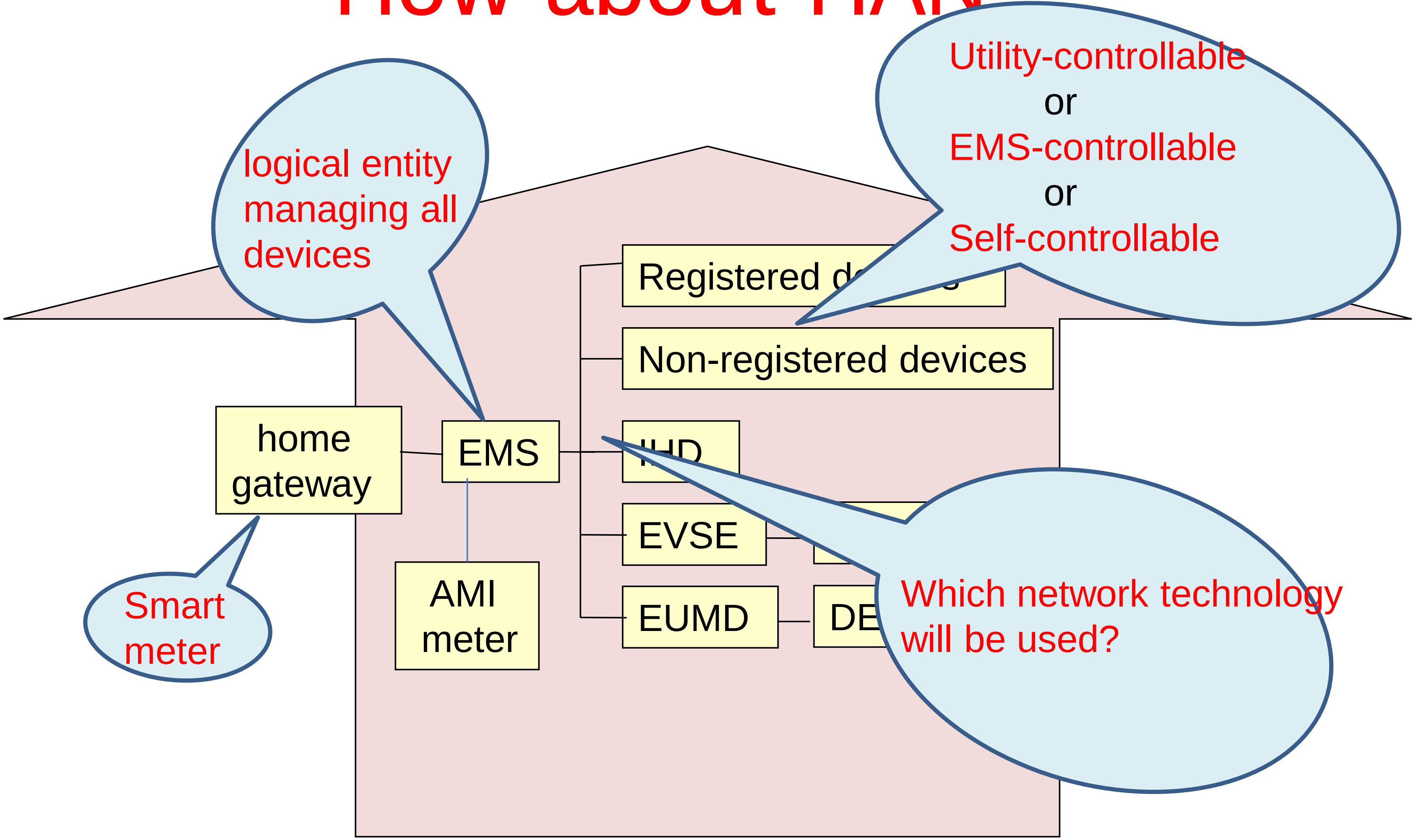
Question

- As AMI is getting interest, security for AMI also have been studied, especially by the UCA AMI-SEC task force.
- I am not going to put a list of security threats and requirements here.
- I want to try to find answers to the following question: “while many network services have confronted similar security challenges and overcome most of them, are there any new security challenges in the AMI service? If any, what will they be?”

It’s a typical network of networks



How about HAN?



logical entity managing all devices

Utility-controllable
or
EMS-controllable
or
Self-controllable

Registered de   s

Non-registered devices

home gateway

EMS

IHD

EVSE

AMI meter

EUMD

DE

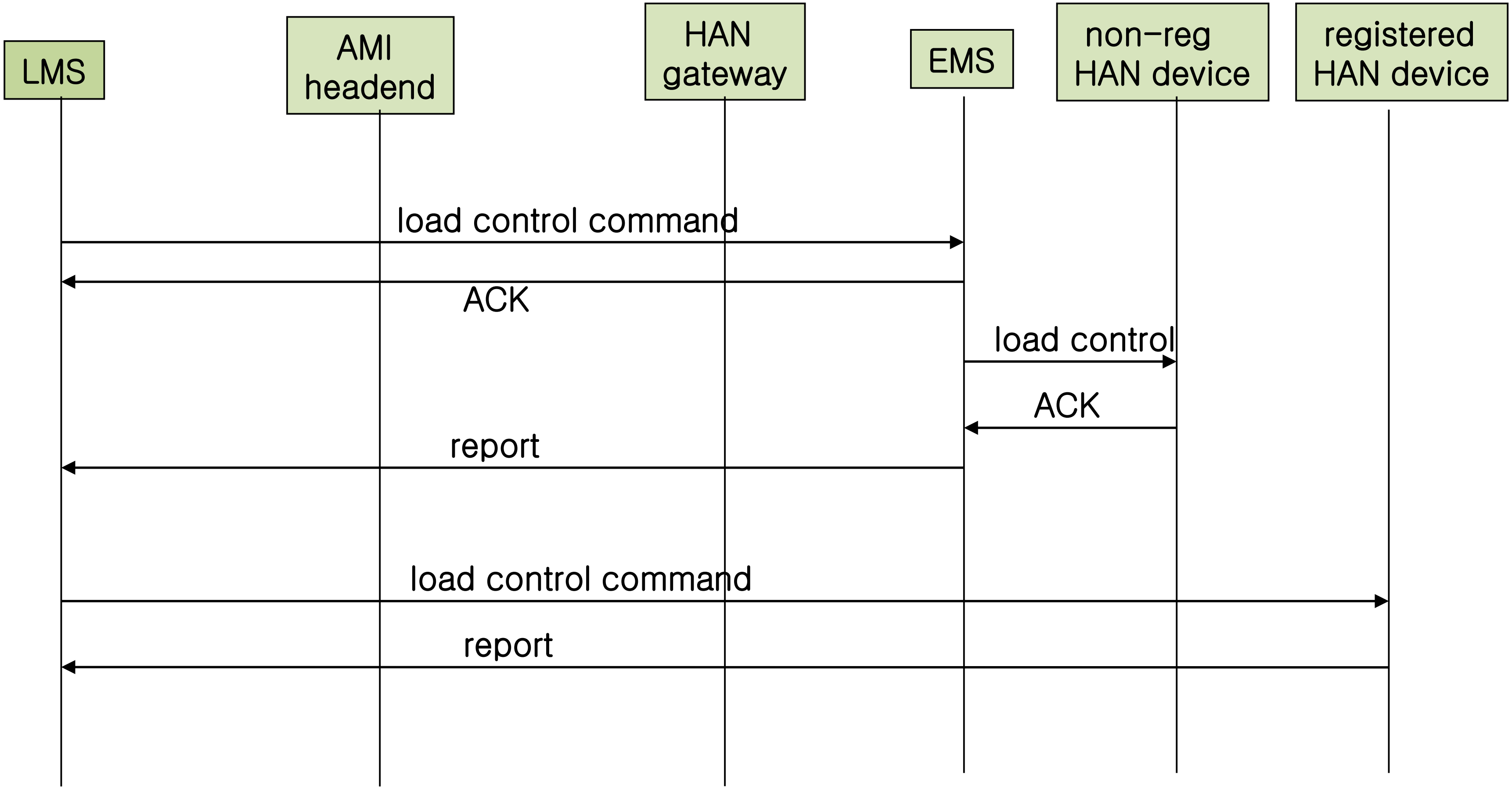
Smart meter

Which network technology will be used?

Information flows, looks familiar

- Over this network, there will be two-way information flows for operation, management, and business. Some typical ones are:
  - Registration/authentication information
  - Demand/response information
  - Energy usage information
  - Load control information
  - Outage information
  - etc.
- New information flows may be added depending on applications (services).

Example: load control information flow



Security Requirements and measures

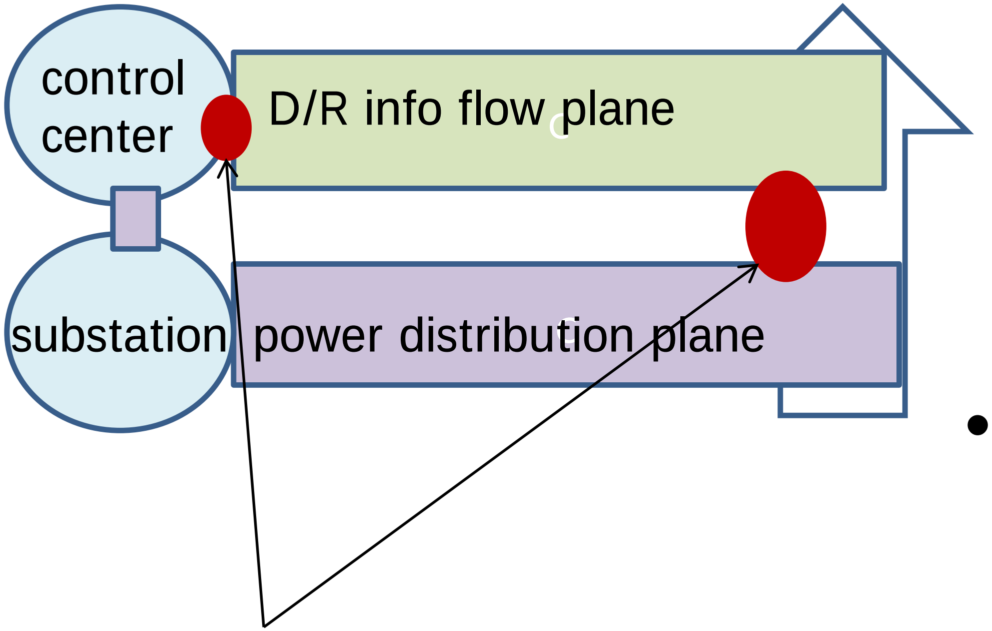
confidentiality	Only authorized users should read data and commands
integrity	Data and commands should be unchanged and replayed
authentication	Users or devices should verify who they are
availability	Data should be accessed when they are needed
authorization	Users/devices should have authority to access data/command
Non-repudiation	Users can not deny their actions later

- Many defensive tools and strategies are available.
- The question is: Are they effective enough?
- Smart grid is entering the roads that other predecessor paved already.
- We can learn a lot of lessons from the financial services in the banking system.

One “worry”

- Can any intruder who is riding on the customer’s network penetrate the power distribution system?
- Can the intruder cause widespread damage to power distribution?
- There are two contact points between two planes: information flow plane and power distribution plane.
- Can we design the system so that any abnormal impact is limited to a single household, or a small group of households.

Two overlay planes



Two contact points:
- AMI headend
- HAN gateway (smart meter)

- Keep the distribution system isolated as possible as you can
  - Don’t be distracted by any fancy buzzword.
- Identify all access points where possible problems happen.
- Design to minimize impact caused by unwanted activities.

A real “headache”

- Some HAN devices may be located at unmanned, unprotected, insecure places.
  - Not to mention physical theft and damage, attackers can access firmware data and read stored data, especially recover crypto keys.
  - With the keys they may understand control messages to devices.
  - At worst they can impersonate authorized users to penetrate the grid.
- So, the minimum requirement is any physical intrusion to devices should be detectable at least, dispatching warning signals to control nodes.

Smart devices

- Devices should be smart enough
  - tamper proof, secure firmware storage, keys, firmware upgrading,
  - intelligent to have monitoring and detection capabilities,
  - security functions: encrypt/decrypt, authentication, authorization, accounting
  - secure communication
  - on top of the basic power-related functions
- And devices may have limited computing power.
- And devices should be cost effective.
- All these requirements come down to the more important task: how to implement.

Privacy, does it really matter?

- The concern is that energy usage pattern is revealed and may be used in unauthorized ways.
- But face up to the world we live where we are willing to agree to reveal much more precious private information to the other party we trust.
- Here is how the private data is used: the data is used for the sole purpose of delivering energy to households, billing, and servicing of that kind. Other than this purpose, the data should not be allowed to use without any consent of users concerned.

Summary

- “while many network services have confronted similar security challenges and overcome most of them, are there any new security challenges in this service. If any, what will they be?”
  - Not really.
  - All hands on deck. Many defensive tools and strategies.
  - We can learn lessons from other network services where security is so concerned.

- We worry about any chance of penetrating the power transmission/distribution system due to the deployment of customer service networks.
  - Identify access points. Preparing for the worst case, we design the system to mitigate impact.
- We need to pay attention to the fact that some devices may be located at unmanned, unprotected places.
- In reality, the more important task is not what to protect and how to protect, but how to implement.
- Don’t make a big deal out of privacy issue.