VU Network Security Advanced
Lecture 05

MANET Security
Smart Grid Security

Tanja Zseby
TU Wien

WS 2018/19

institute of telecommunications

TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

Student Position

- 10h/Week
- Minimum: € 500 brutto (14x/year)
- Student ETIT or Informatics (or similar)
- Knowledge in IP Networks Network Security, data analysis, programming (C/C++, Python)

- See TU Wien Mitteilungsblatt from 18.10.2018
- Apply at sekretariat@nt.tuwien.ac.at

Mobile Ad hoc Network (MANET) Routing Security

Source: Nadeem, Howarth. „A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks“. IEEE Communications Surveys Tutorials, 2013.

MANETs

- Mobile Ad hoc network
  - Each node acts as router and forwards traffic of other nodes
  - Nodes can move, join/leave network
- Topology
  - Static (e.g. urban mesh networks)
  - Dynamic (e.g. vehicular networks)
  - Hybrid (mixture of fixed and mobile nodes)
- Wide varity of routing protocols
  - Proactive
  - Reactive
  - Hybrid

Application Fields

- Military
  - Fast and easy establishment of communication
- Vehicular ad hoc networks
  - Communication among cars
- Urban Mesh Networks
  - Berlin Freifunk, Vienna Funkfeuer
- Personal Networks
  - Connect smartphones, laptops on the fly
- Sensor networks
  - Sensor nodes (with low range) can send data via other sensors
  - Sometimes used for smart meters

MANETs

- Single administration
  - All nodes under one authority
  - Better options to establish security, trust models
  - Nodes share resources
  - Example: military network
- Multiple administrations
  - Nodes administered by different authorities
  - Nodes cannot be trusted
  - Nodes may be selfish (e.g. don’t forward packets of others)
  - Example: urban mesh

MANET Security

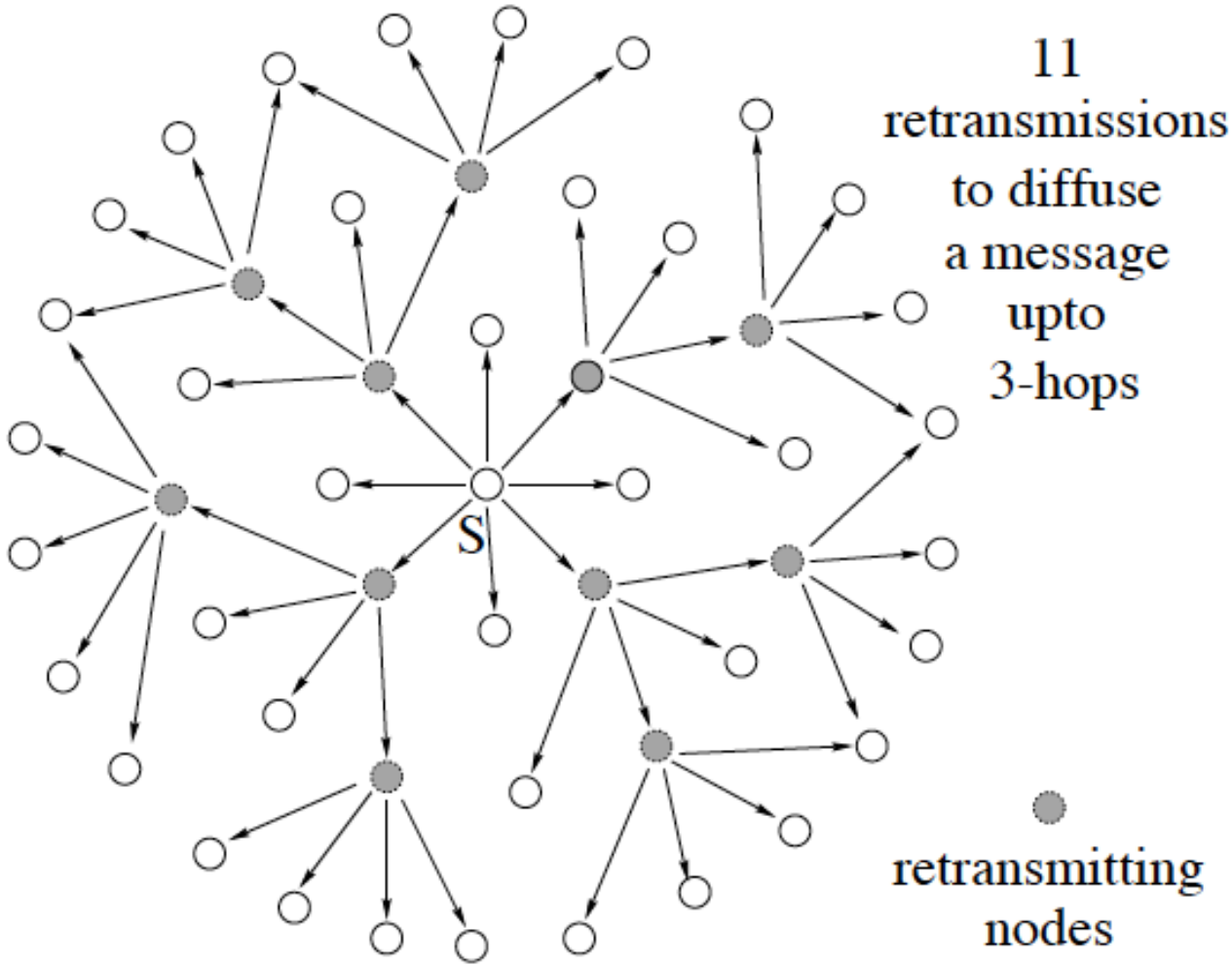
- Cooperative routing
  - Each node participates in routing
  - Each node sees traffic of other nodes
  - ➔ many attacks possible
- Dynamic unpredictable topology
  - Nodes may join/leave
  - Dynamic physical boundaries of network
- Usually limited resources
  - Small devices
  - Battery-powered devices
  - Wireless links

➔ Difficult to deploy classical security measures

Recap: AODV and OLSR

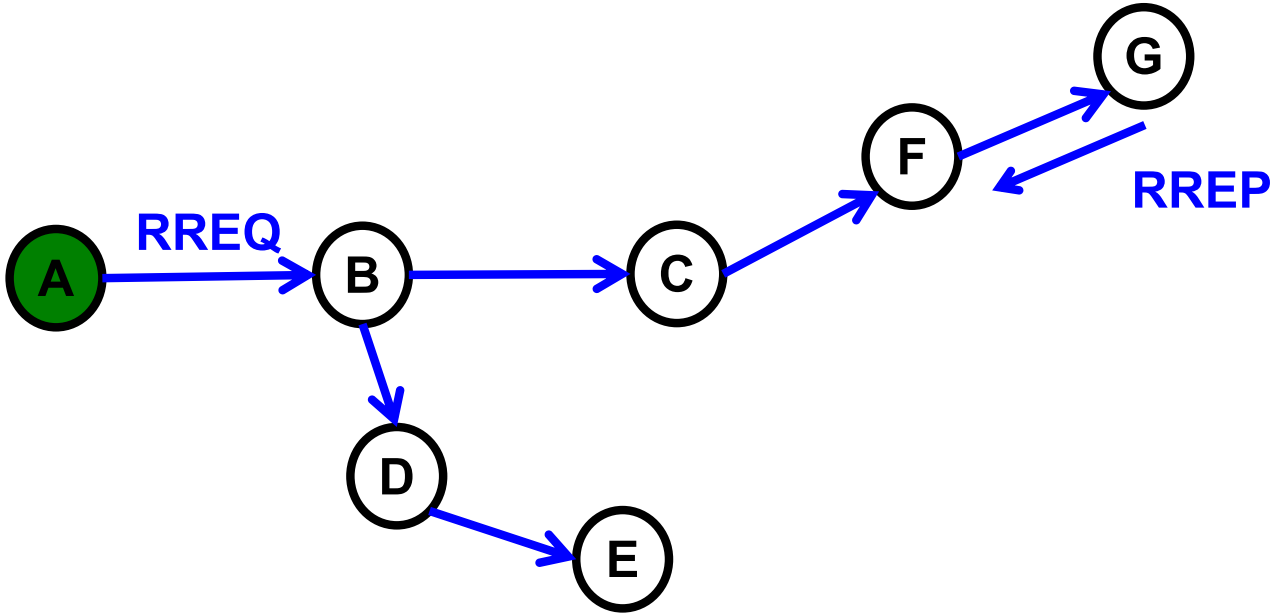
- Optimized Link State Routing Protocol (OLSR)
  - ***Proactive***: nodes maintain table with routes to all other nodes
  - ***Link state*** protocol: Nodes need full topology information
  - MPRs to reduce number of messages
  - Useful in dense environments, slow topology changes (e.g., urban mesh, static sensor networks)
- Ad hoc On-Demand Distance Vector (AODV)
  - ***Reactive***: routes established on demand
  - ***Distance Vector*** protocol: nodes don't need full topology information
  - Useful in high dynamic environments (e.g., vehicular networks, tactical networks)

OLSR



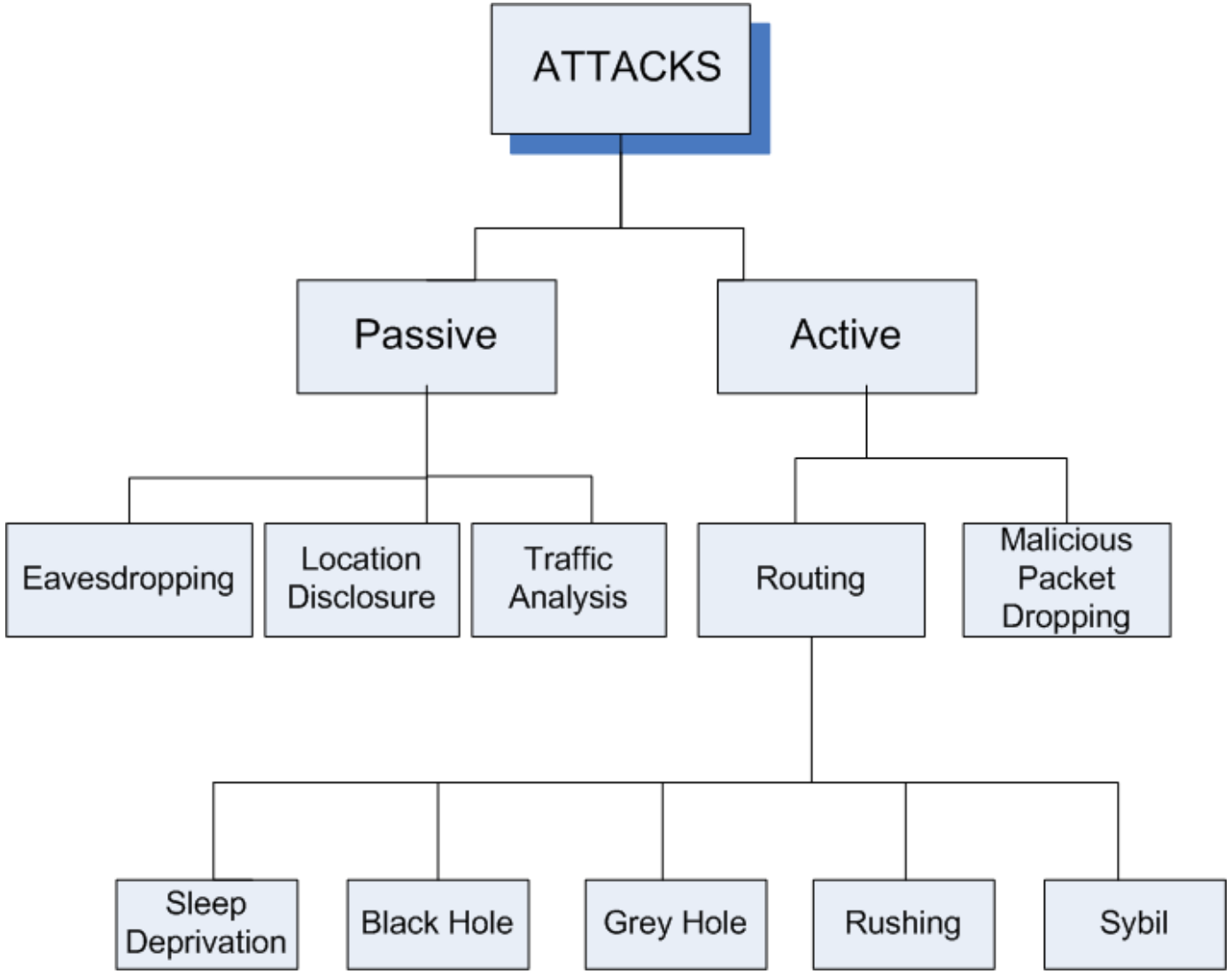
Source: Qayyum, Viennot, Laouiti, “Multipoint relaying for flooding broadcast messages in mobile wireless networks,” i*35th Annual Hawaii International Conference on System Sciences, 2002. HICSS*, 2002.

AODV



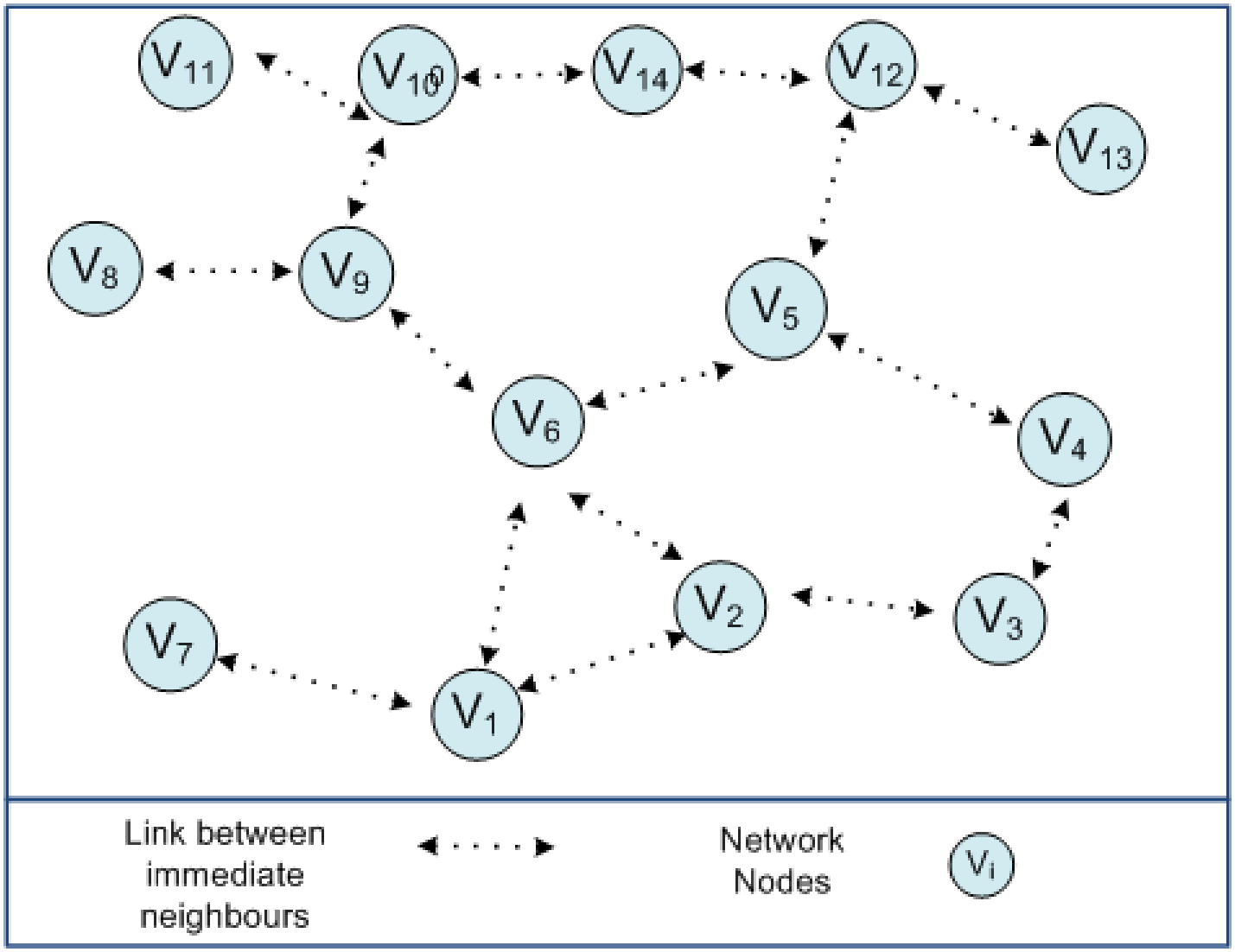
- A wants to send data to G ➔ sends a route request (RREQ)
- Route request (RREQ) is broadcasted in the network
- Intermediate nodes record path back to A
- G receives route request (RREQ) ➔ sends route reply (RREP)
- Route reply is sent on recorded path back to A

MANET Attacks



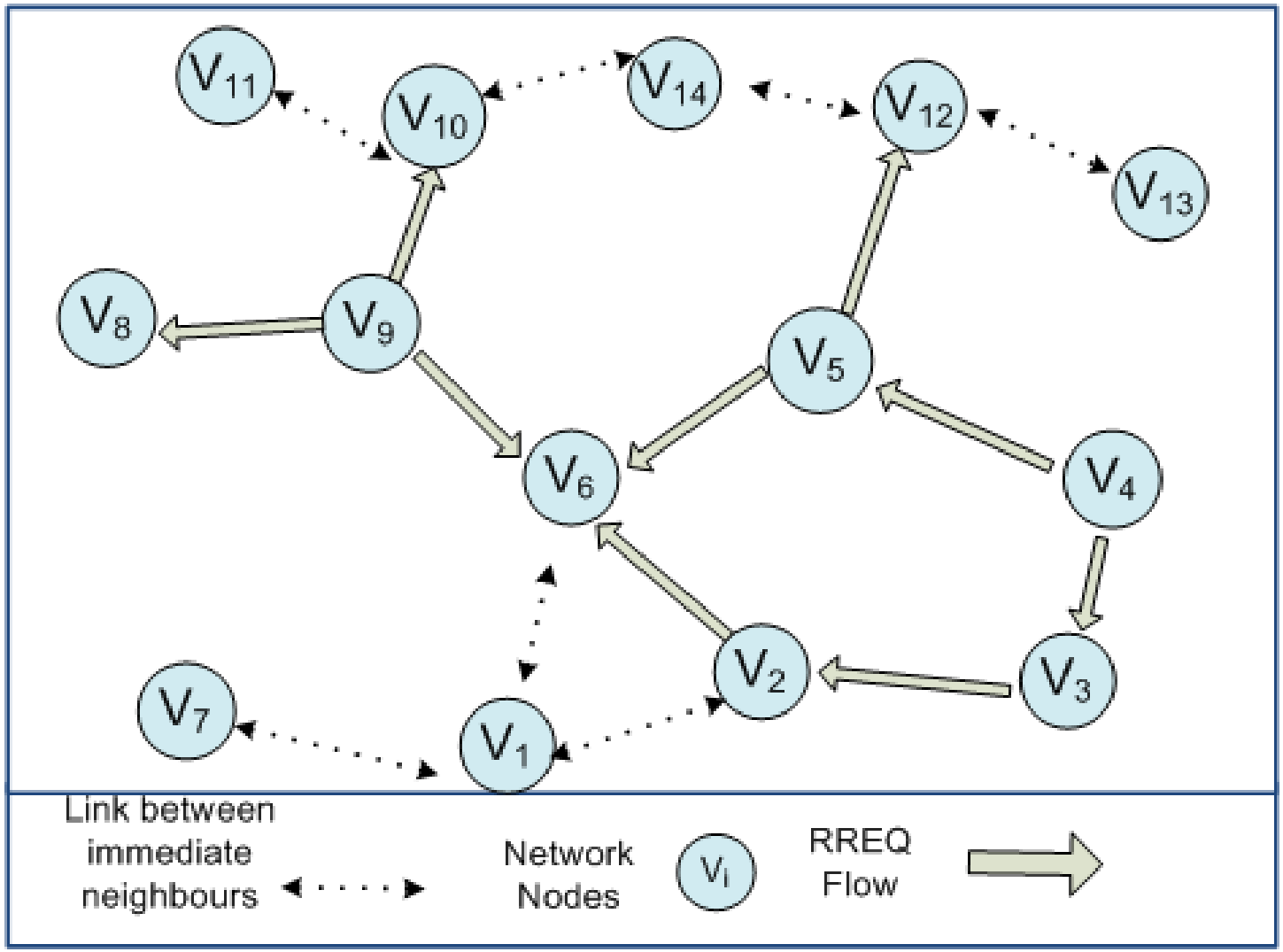
Source: Nadeem, Howarth. „A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks“. IEEE Communications Surveys Tutorials, 2013.

Healthy Network



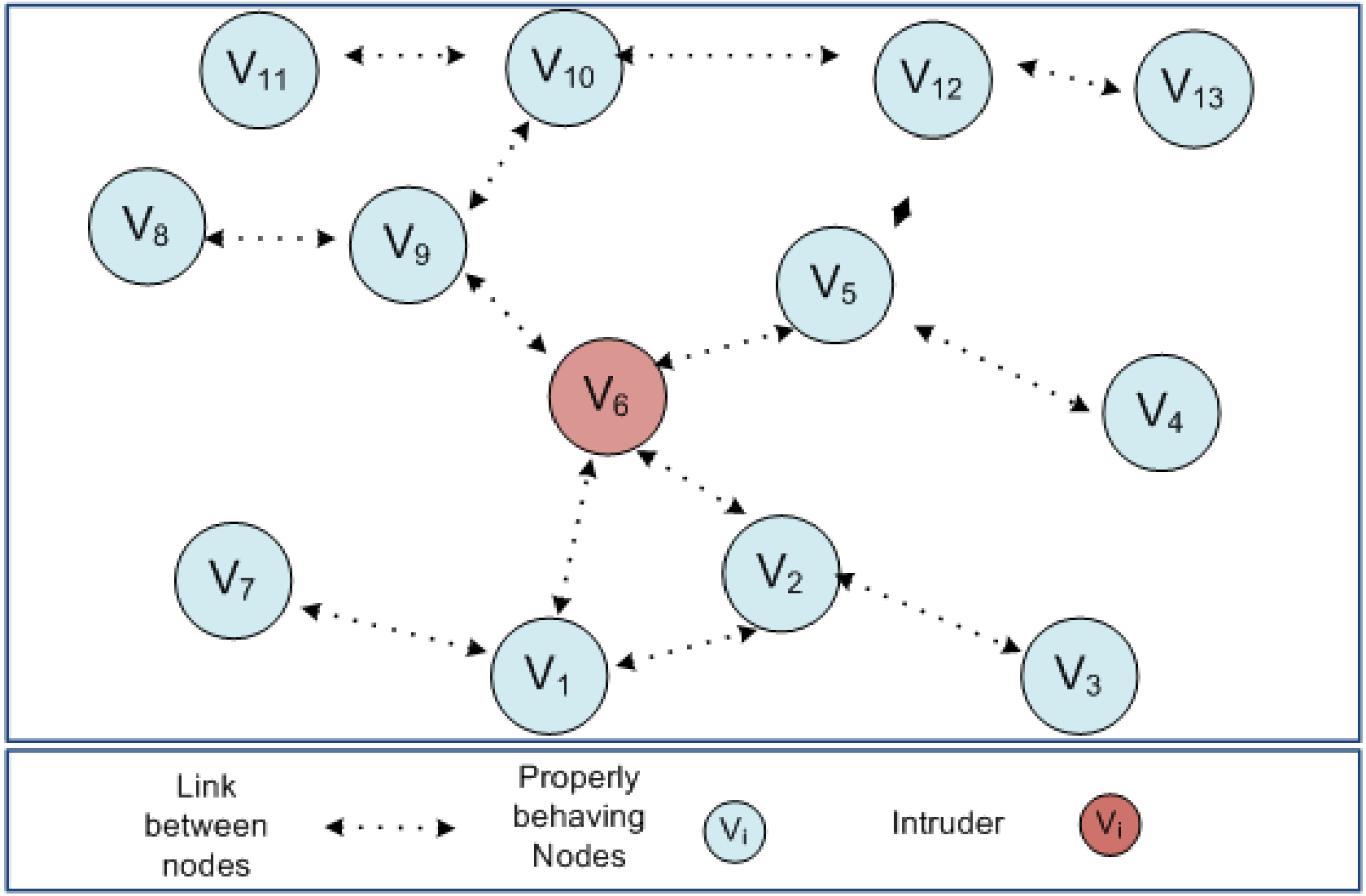
Source: Nadeem, Howarth. „A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks“. IEEE Communications Surveys Tutorials, 2013.

Route Discovery (v9,v4)



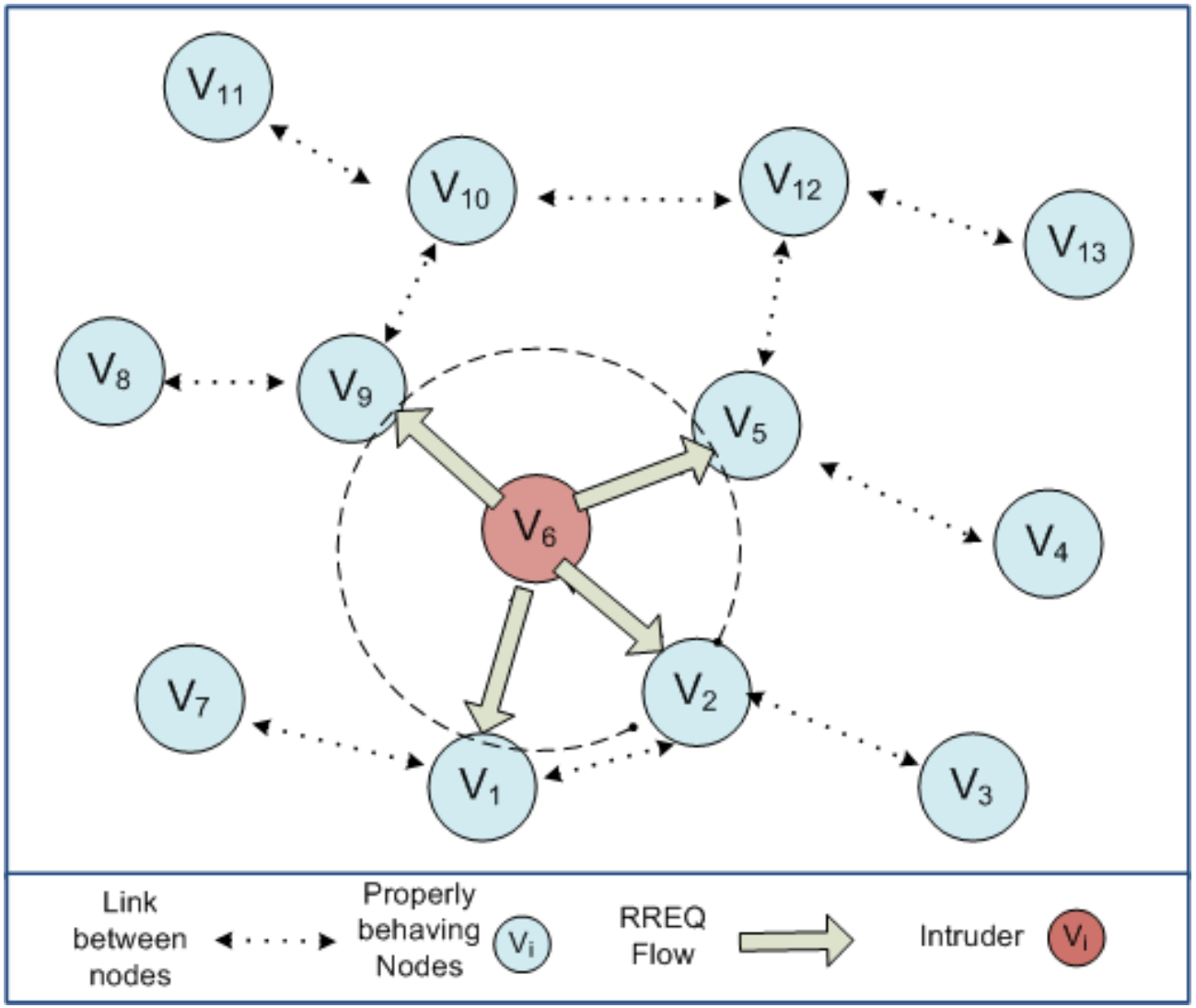
Source: Nadeem, Howarth. „A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks“. IEEE Communications Surveys Tutorials, 2013.

Malicious Node in Network



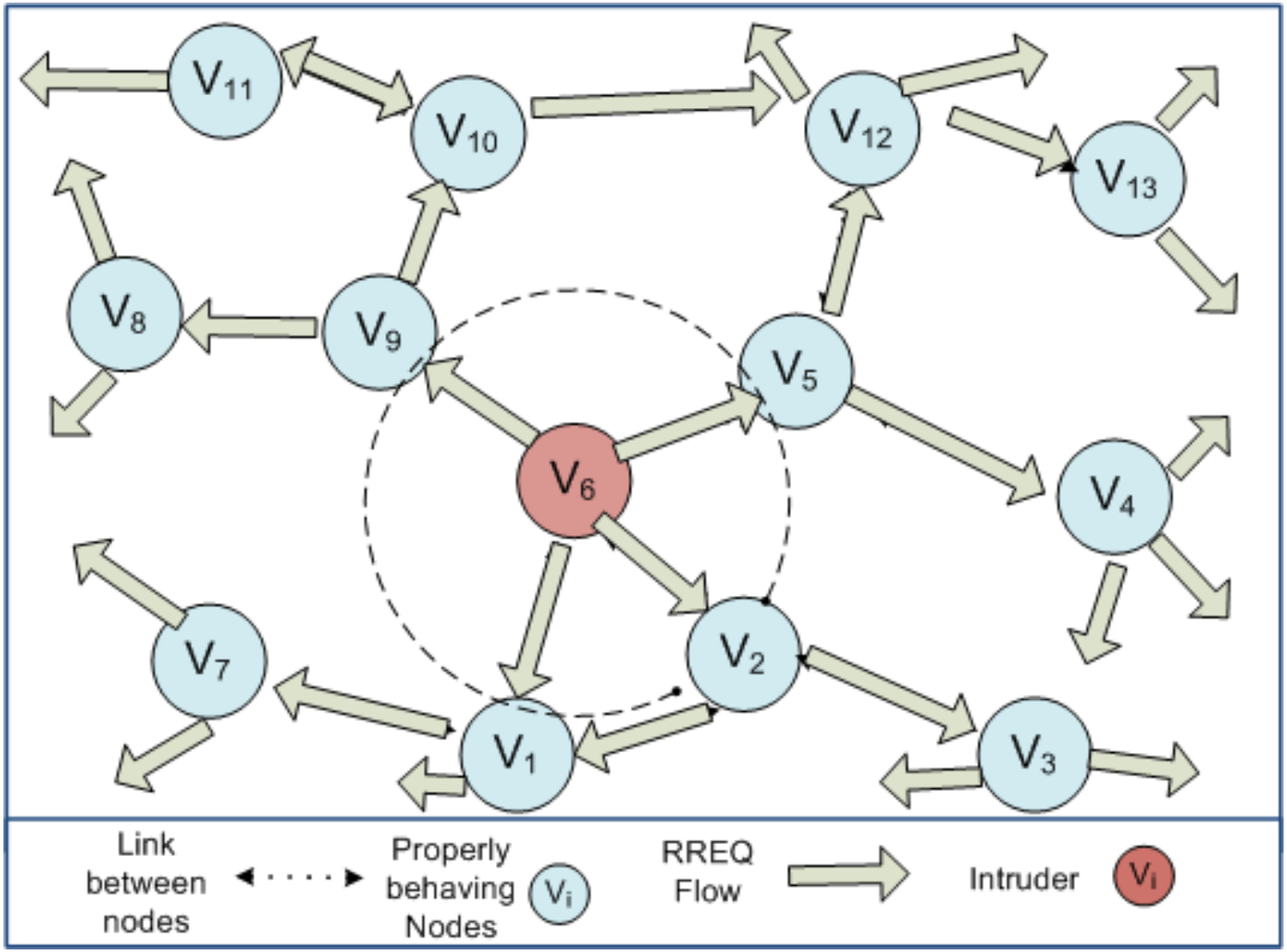
Source: Nadeem, Howarth. „A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks“. IEEE Communications Surveys Tutorials, 2013.

Generating Malicious Routing Requests



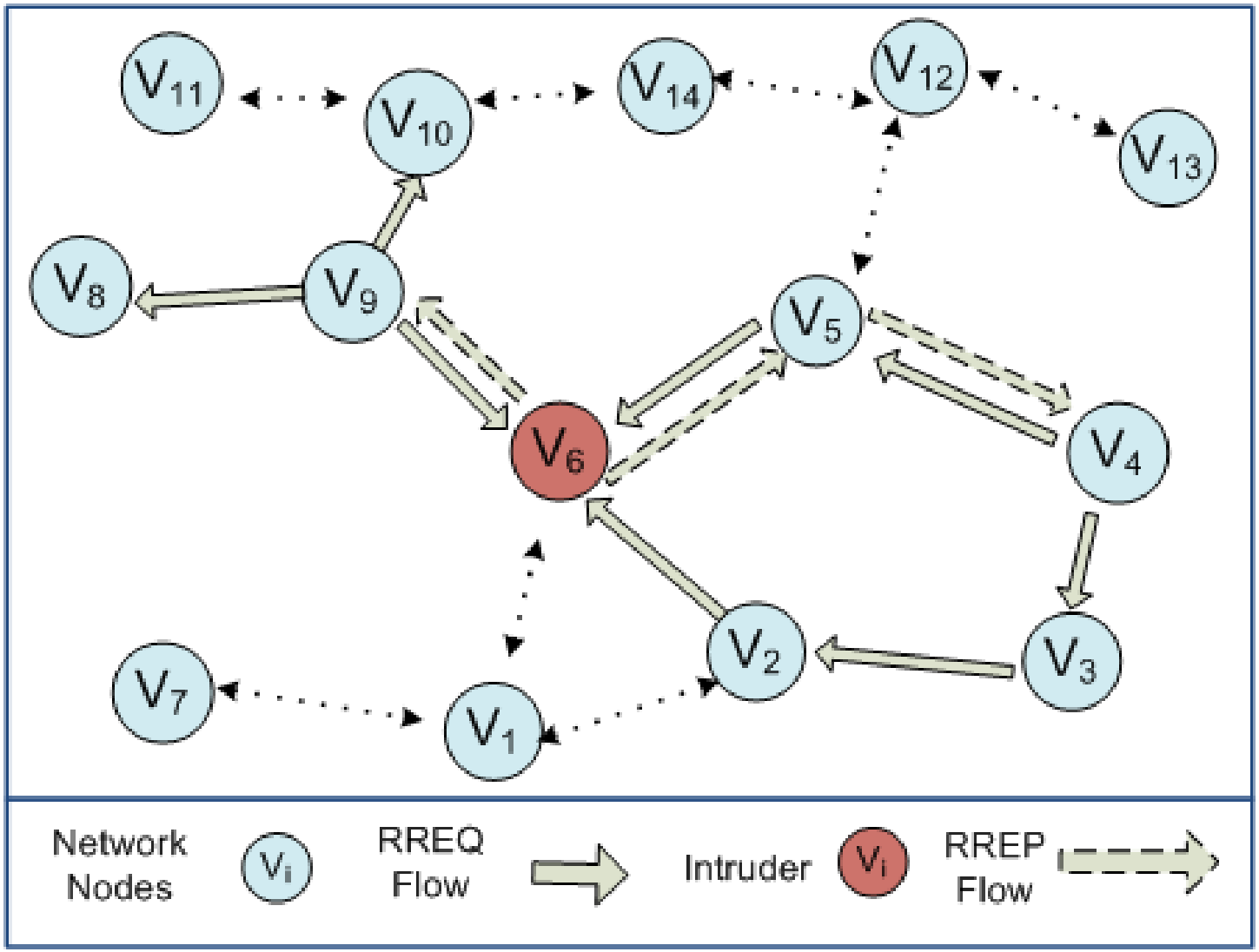
Source: Nadeem, Howarth. „A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks“. IEEE Communications Surveys Tutorials, 2013.

Flooding of Malicious Routing Requests



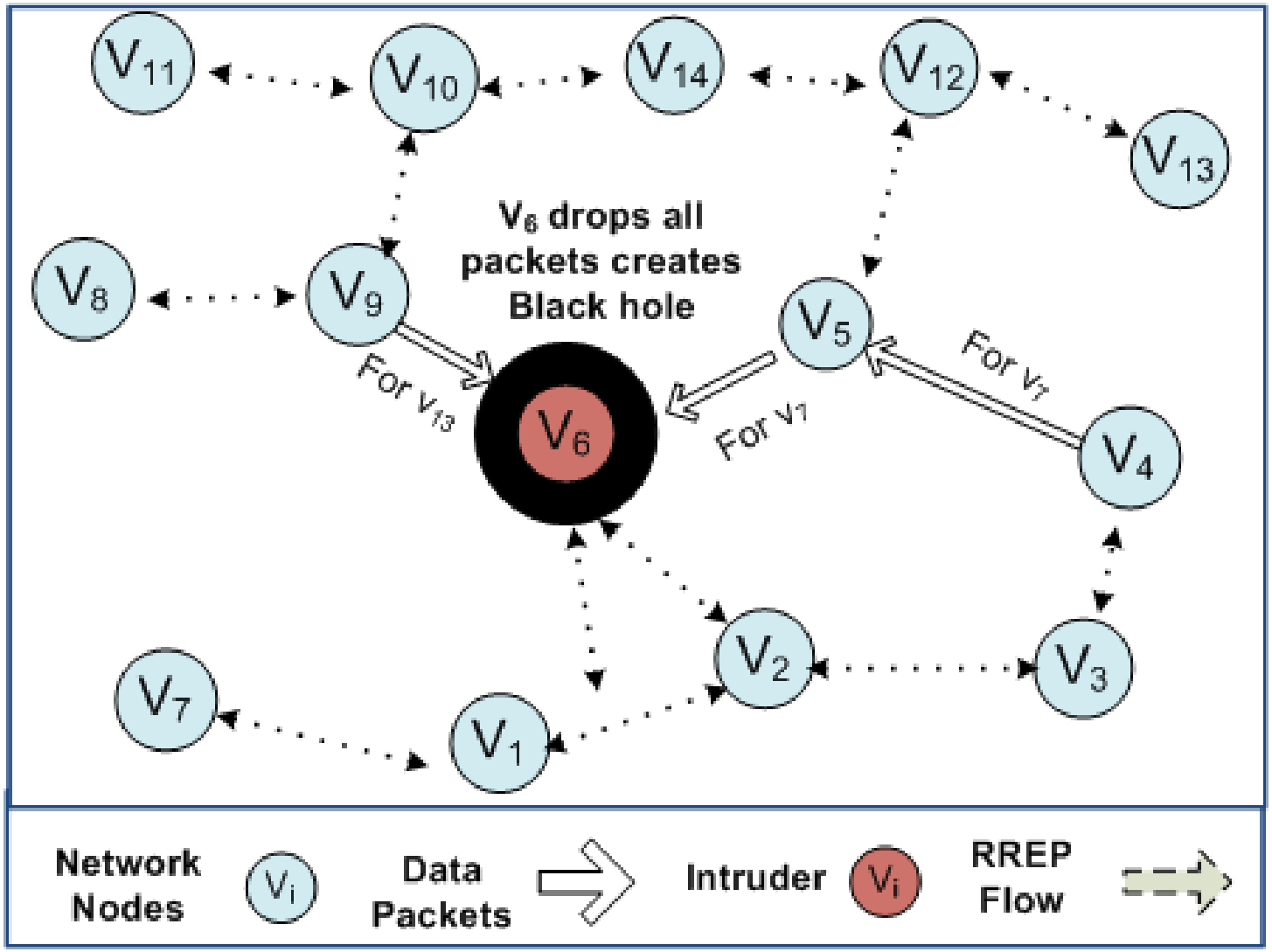
Source: Nadeem, Howarth. „A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks“. IEEE Communications Surveys Tutorials, 2013.

Malicious Node sends False Routing Reply



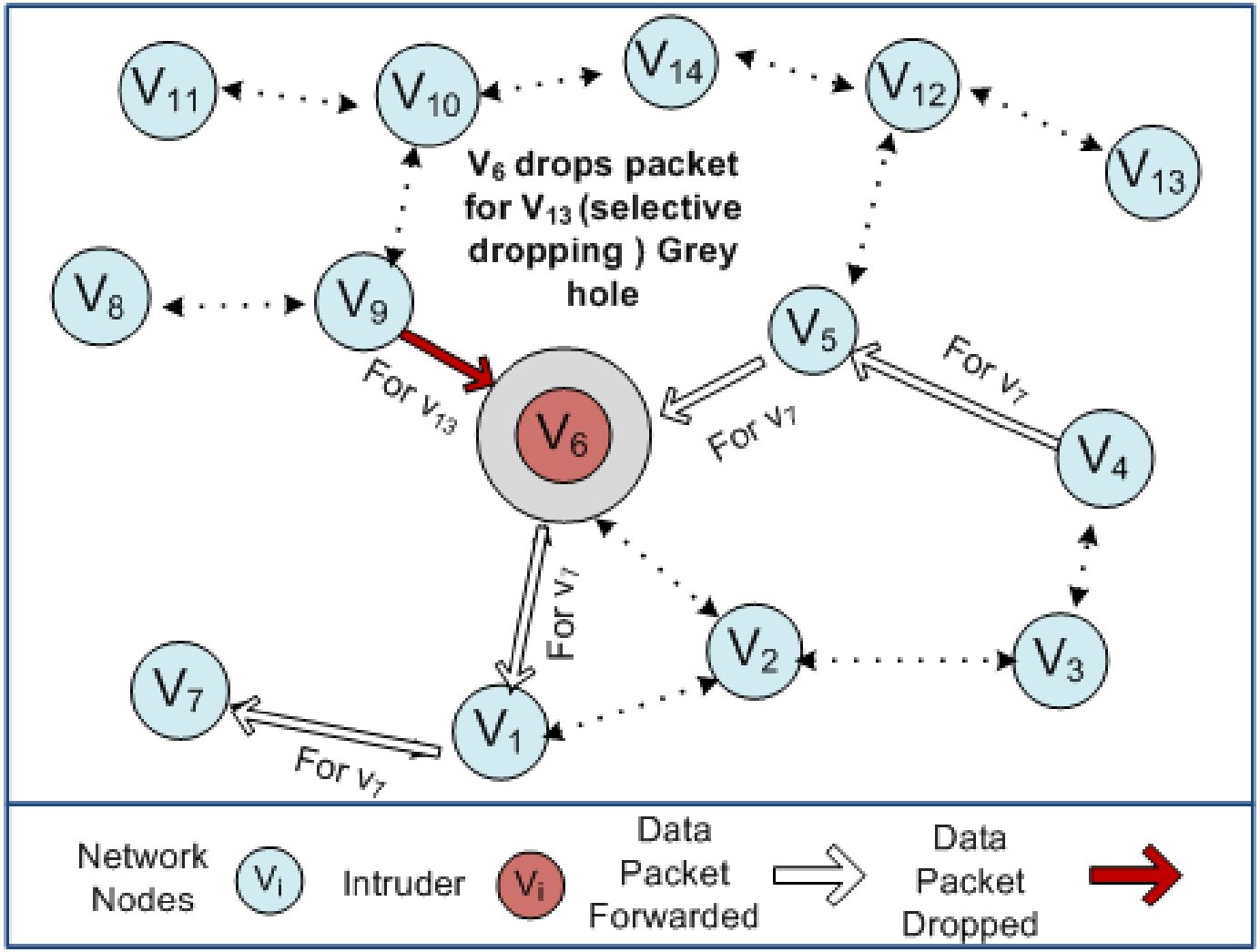
Source: Nadeem, Howarth. „A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks“. IEEE Communications Surveys Tutorials, 2013.

Black Hole established



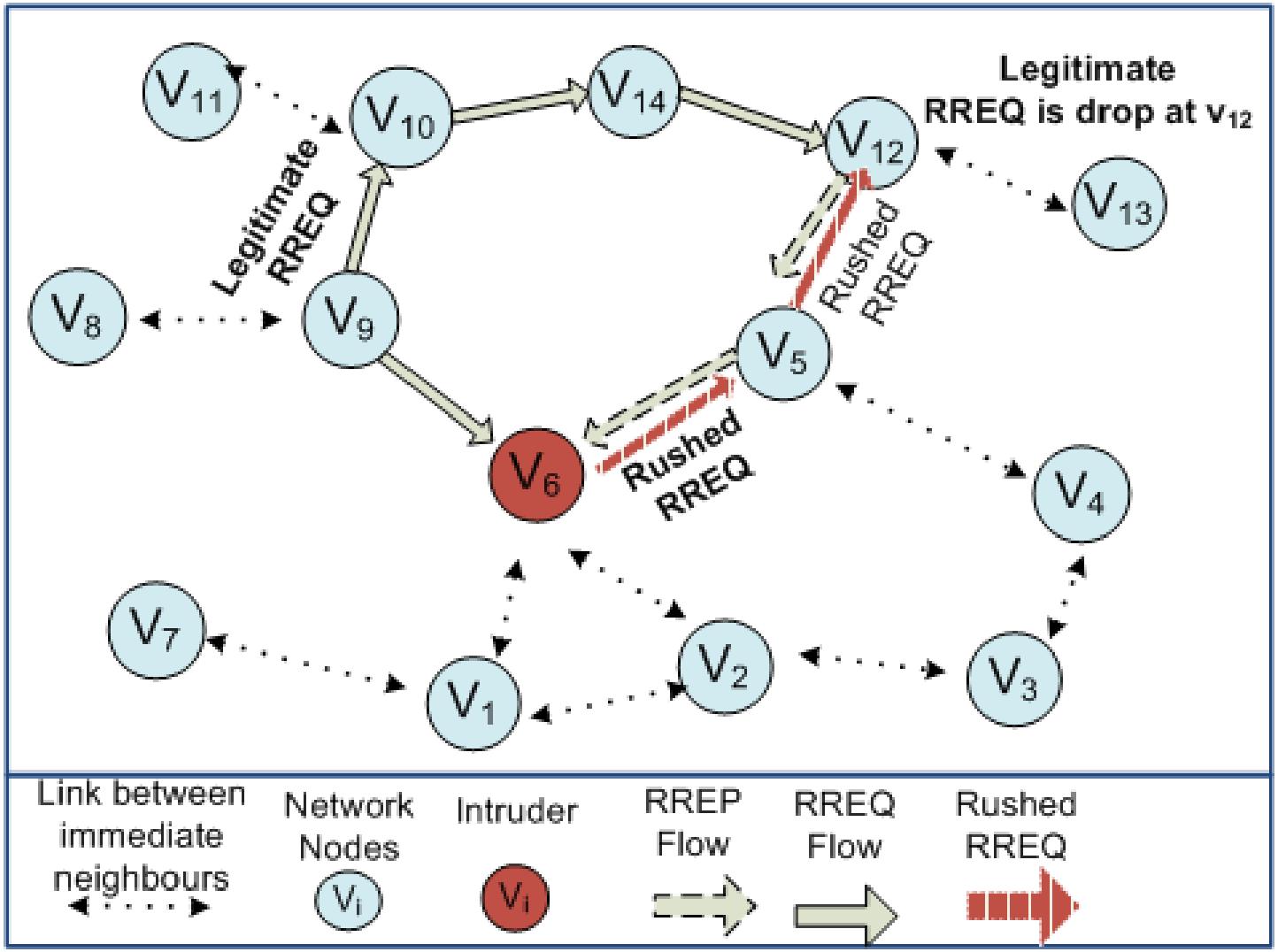
Source: Nadeem, Howarth. „A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks“. IEEE Communications Surveys Tutorials, 2013.

Grey Hole



Source: Nadeem, Howarth. „A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks“. IEEE Communications Surveys Tutorials, 2013.

Rushing Attack



Source: Nadeem, Howarth. „A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks“. IEEE Communications Surveys Tutorials, 2013.

MANET Attack Mitigation

- Trust Establishment
  - Using cryptography (keys, signatures)
  - Problem: highly dynamic networks, no central control, nodes join/leave ➔ key distribution
  - Problem: Computational expensive
- Traffic Observation
  - Observe which packets are forwarded by whom
  - Exchange Information with neighbors
  - Identify malicious or selfish nodes
  - Problem: high effort
  - Problem: Colluding nodes

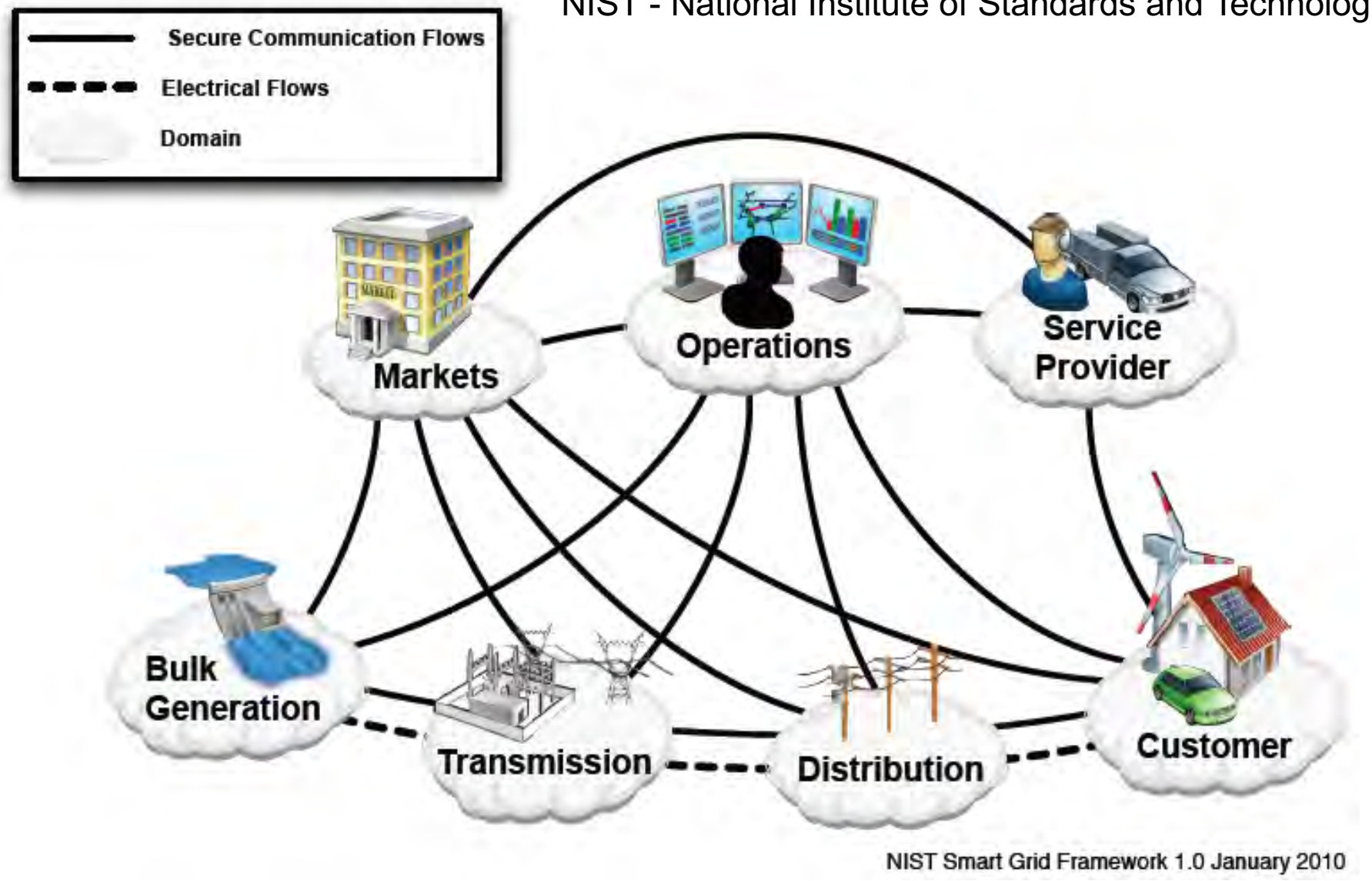
Smart Grid Communication

Smart Grids

- Ensure efficient and reliable energy supply
  - Efficient energy distribution
  - Cope with distributed energy sources
  - Cope with dynamic supply by renewable energy sources
  - Power outage prevention
- Support energy saving efforts
  - Consumer awareness
  - Flexible tariffing
  - Control of home appliances
- SG features ➔ new communication demands
- **Critical infrastructure** ➔ high security demands

US NIST Smart Grid Domains

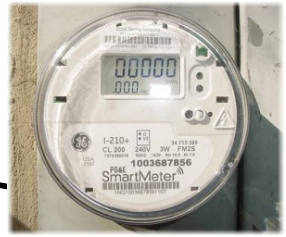
NIST - National Institute of Standards and Technology



Smart Grid Communication

Market

eVehicle



Smart Meters

Data Processing

Utility Providers

Power Plants

Renewables

Home Appliances

ITU

IETF

DIN

NIST

IEC

Smart Grid Communicat

ISO

ETSI

ZigBee™

cen

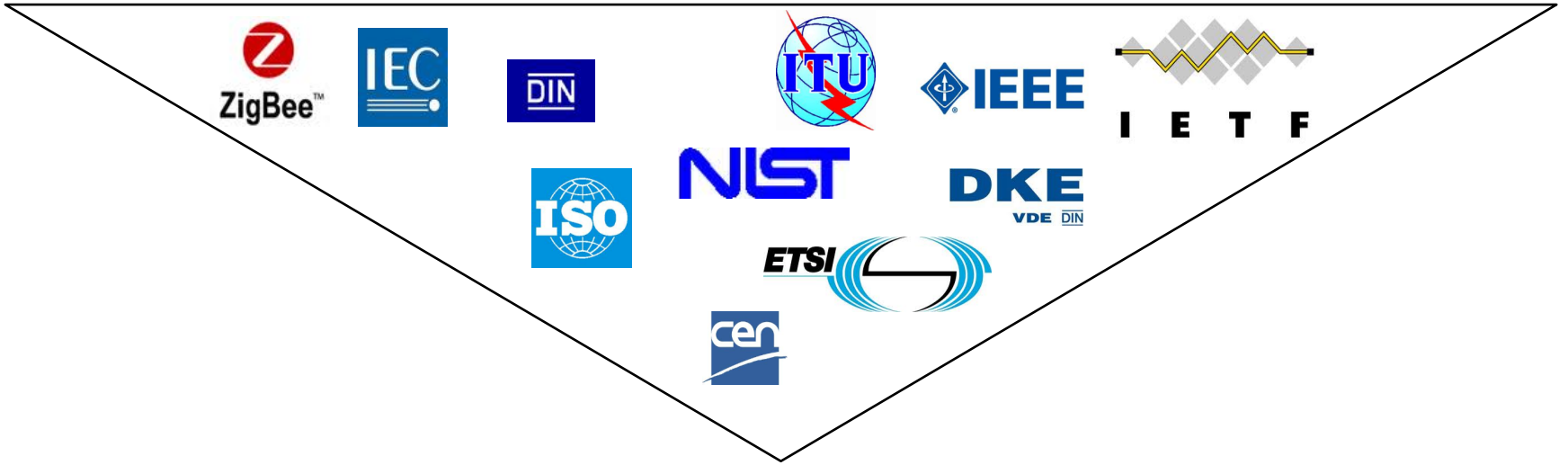
DKE VDE DIN

IEEE

“The nice thing about standards is that you have so many to choose from.”

[Andrew S. Tanenbaum, Computer Networks 2nd Ed.]

IP as Convergence Layer (Hopefully)



Internet Protocol (IPv4, IPv6)

What IPv6 can offer

IPv6 Feature	Applicability in Smart Grid
Huge address space	Addressing millions of smart grid devices Establishment of well-structured hierarchical networks (e.g., meters, concentrators, etc.)
Stateless address autoconfiguration	Simple installation of new meters Use of device identifier as part of address
IPsec support	Establishment of security associations Data encryption, authentication
Quality of Service	Prioritization of messages (e.g. time critical control messages, alarms,)
IPv6 Multicast	Efficient message transmission to a set of devices (e.g., software updates, phasor measurements)
6LoWPAN	IPv6 interoperability in resource constraint environments

Smart Grid Security Challenges

- Cyber Physical System
  - Connects cyberspace with real world
  - Control function manipulation has effects on devices

  ➔ Threat to devices and humans
- Critical infrastructure
  - High incentives for attackers
  - Attracts sophisticated well-equipped attackers

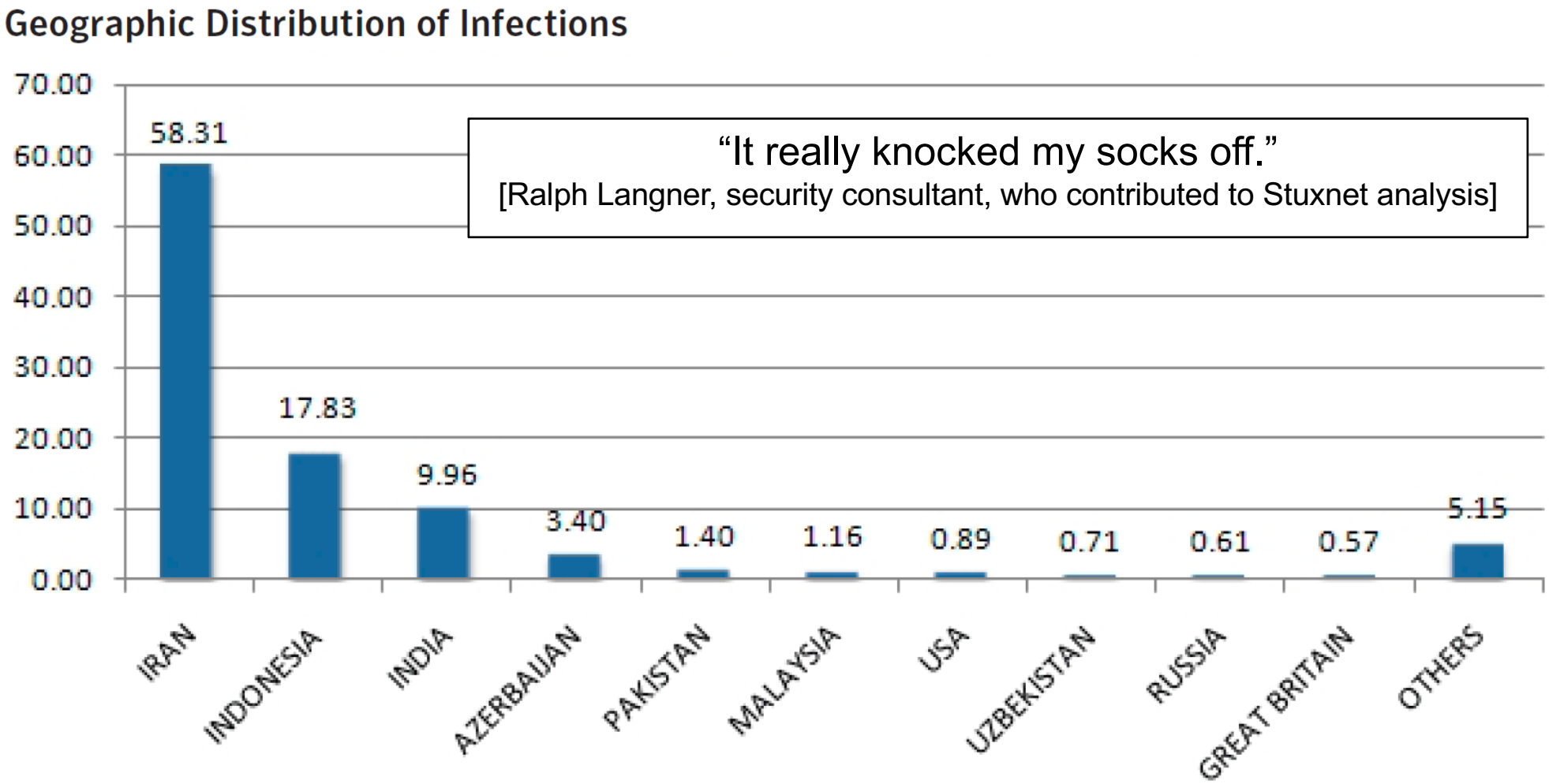
  ➔ Attractive target
- Complex Systems
  - Dependencies Communication/Power Infrastructures
  - Different domains, shared responsibilities

  ➔ Inconsistent security policies, many attack entry points

  ➔ **high security demands**

A Wakeup Call

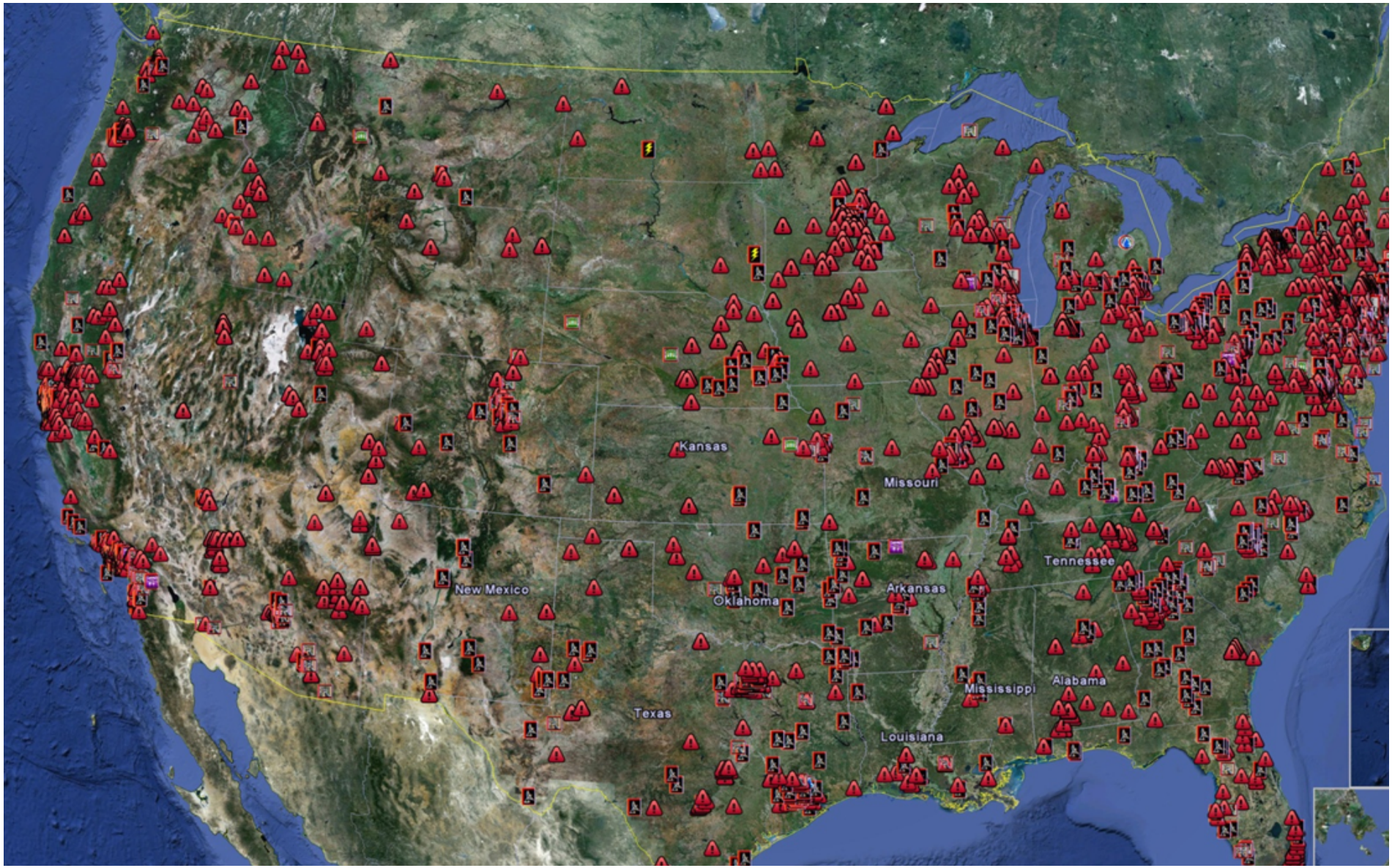
Stuxnet: Attack on Cyber Physical System



"It really knocked my socks off."
[Ralph Langner, security consultant, who contributed to Stuxnet analysis]

Source: Symantec W32. Stuxnet Dossier, Feb. 2011

Internet Connected Control Systems



Source: ICS-CERT Monitor Oct-Dec 2012

A Tempting Target

- Findings from US congressional report in May 2013
  - Based on answers from 113 utility operators

- Frequent cyber attack attempts at several utilities
  - Probing, phishing, malware infections
  - Some report daily, constant or frequent attempted cyber-attacks
- One utility observed 10.000 attempted attacks/month
- Only few own spare transformers

Source: Electric Grid Vulnerability Report, May 2013

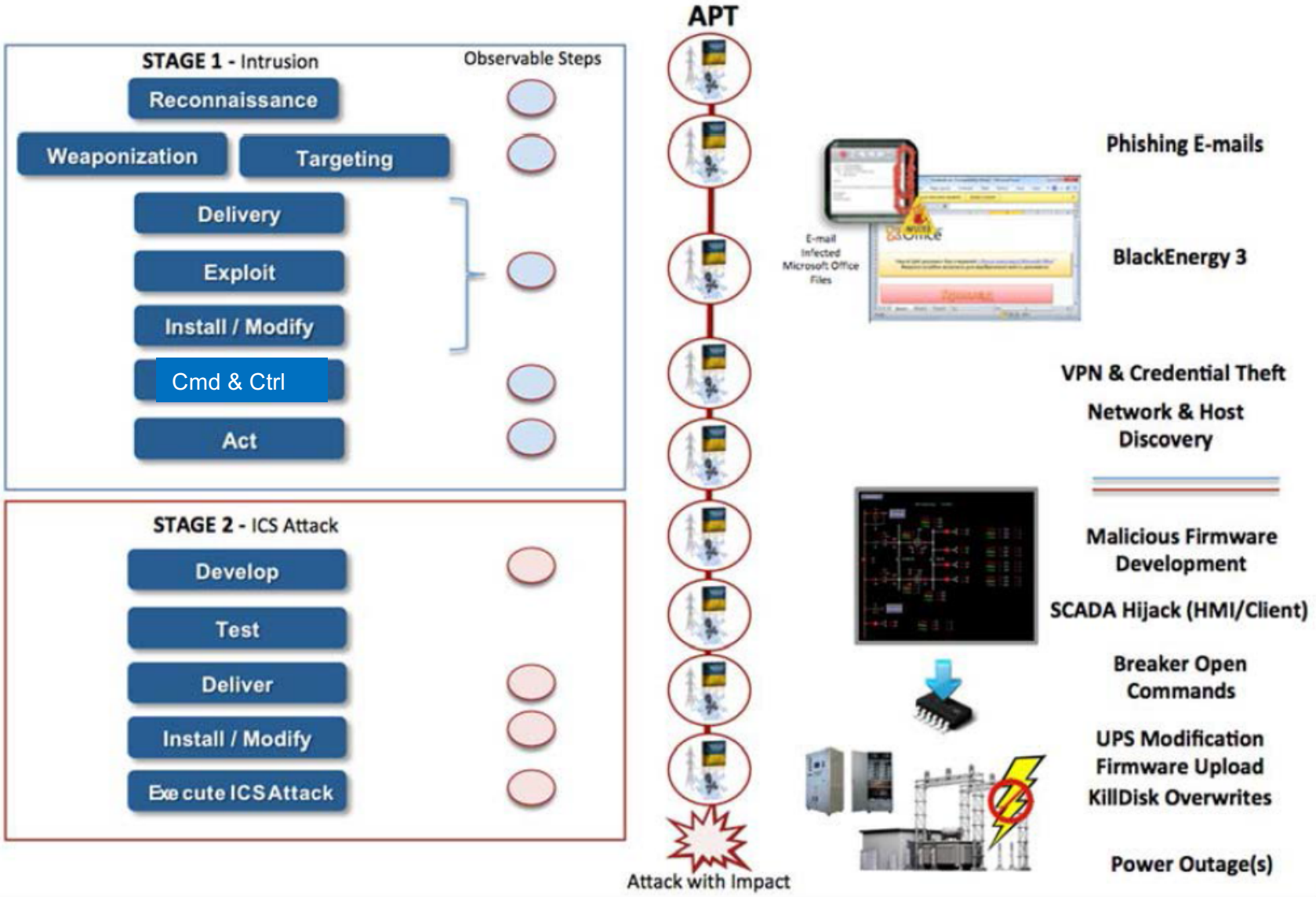
2015 Attack on Ukrainian Power Grid

- Send spear phishing email with infected MS Office documents (BlackEnergy3 botnet) ➔ infect corporate network
- Contact C&C, load further malware
- Steal credentials for VPN connections
- ➔ Establish path from corporate network into Industrial Control System (ICS) network
- Hijack SCADA HMI clients ➔ gain information, develop malicious firmware
- Use remote access to open breakers
- Install malicious firmware to prevent recovery
- Erase critical system data (KillDisk)
- Disable uninterruptible power supplies (UPS) via remote IF
- Phone DoS

➔ Power Outage:

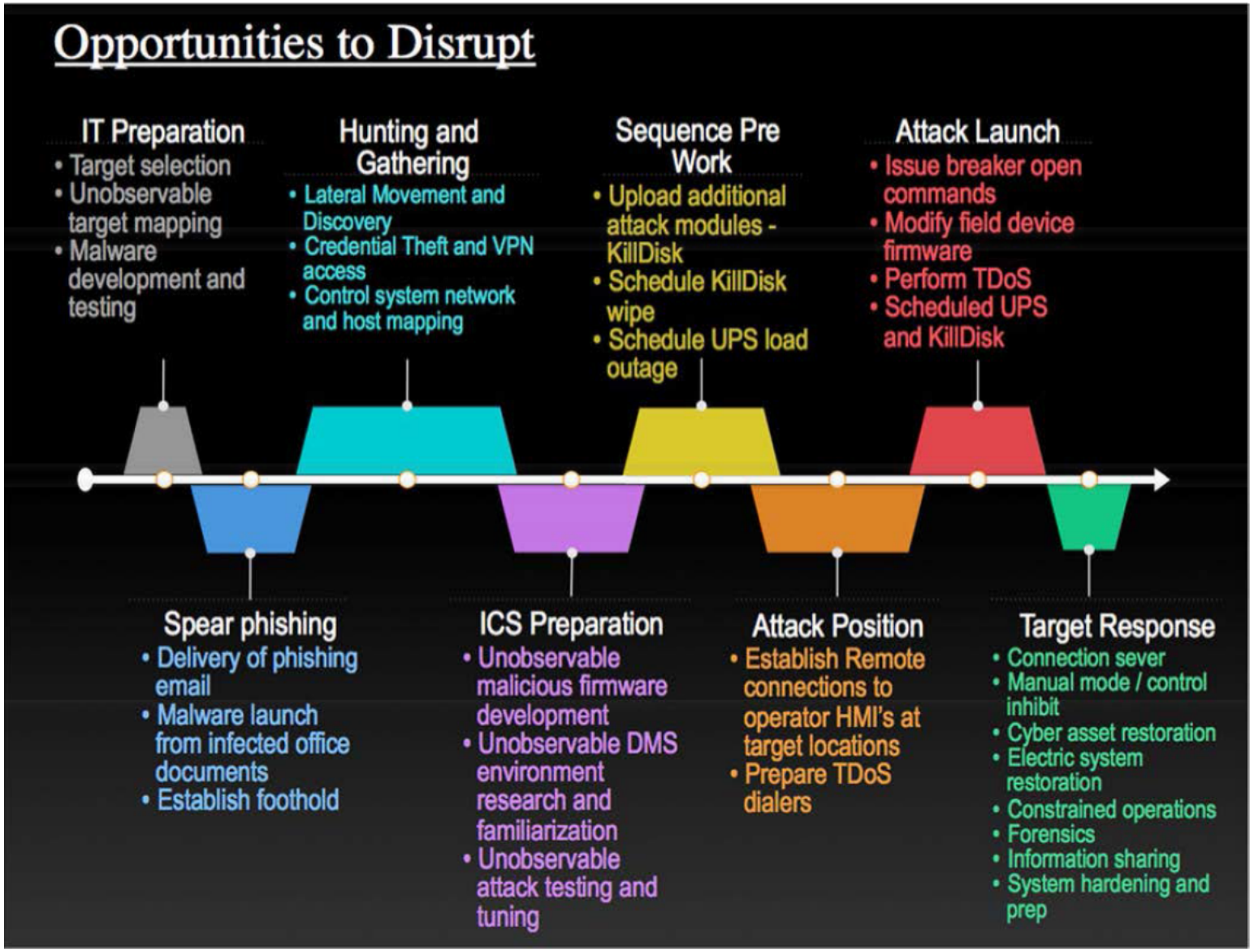
- At least 27 substations offline, 225,000 customers, many hours

Advanced Persistent Threat (APT)



Source: SANS-ICE, E-ISAC, Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case, March 18, 2016

Attack Disruption Possibilities



Source: SANS-ICE, E-ISAC, Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case, March 18, 2016

Visible Activity

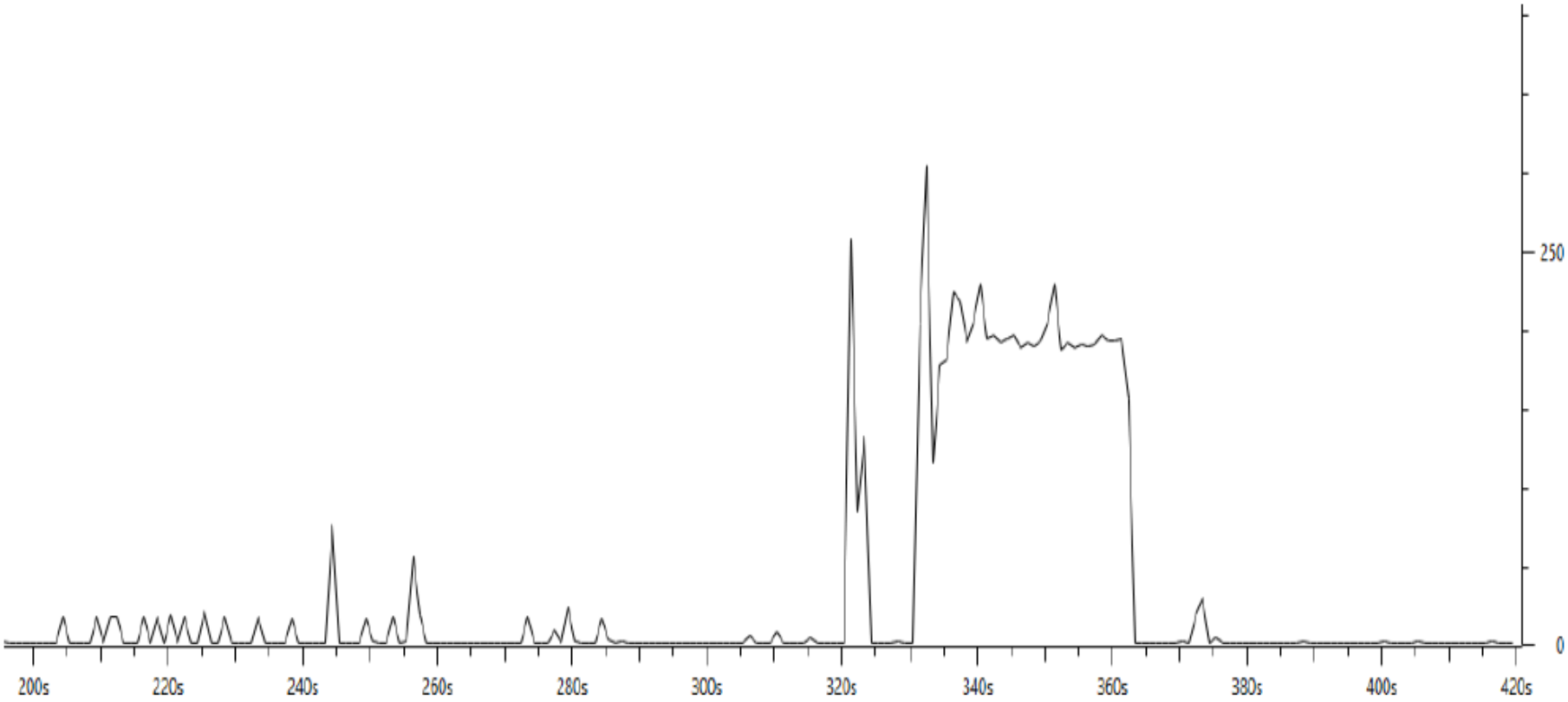


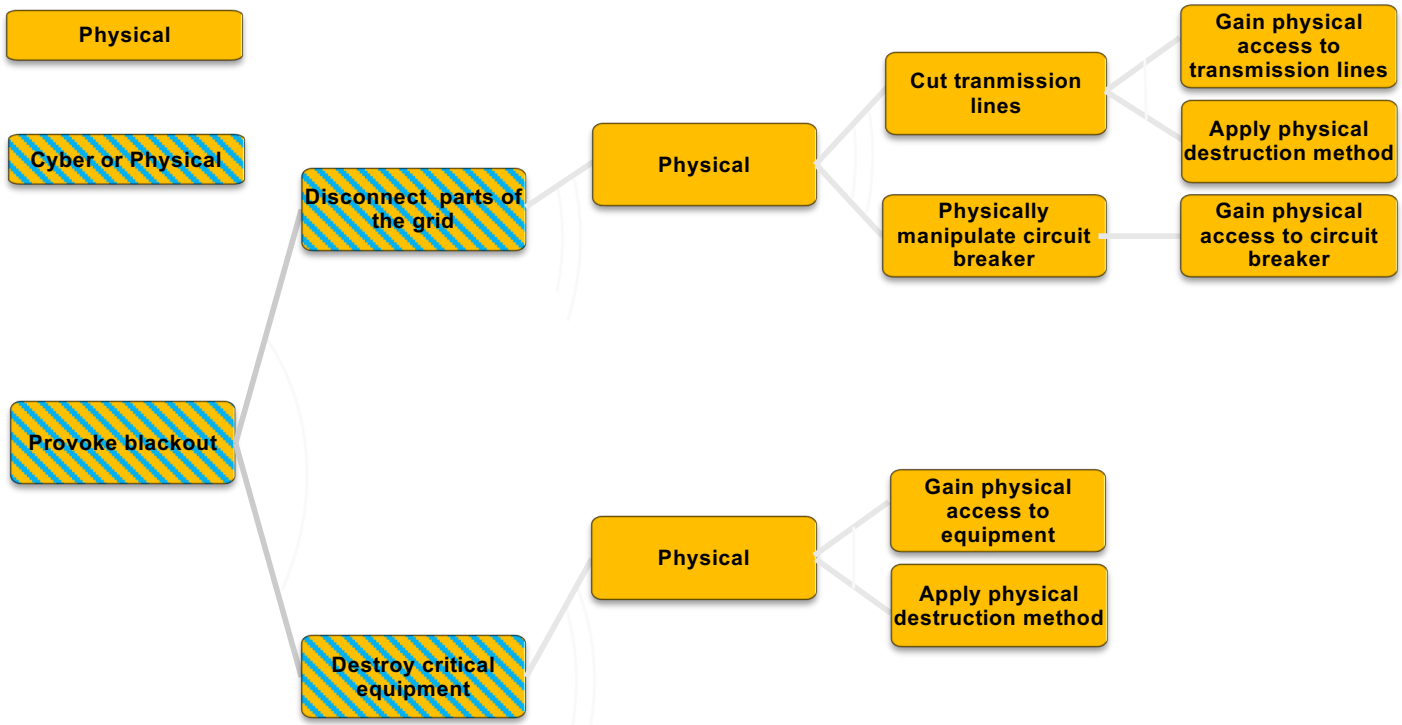
Figure 10: Sample Network I/O Data from a Malicious Firmware Update to an Industrial Ethernet Switch[38]

Source: SANS-ICE, E-ISAC, Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case, March 18, 2016

Smart Grid Protection Efforts

- Europe
  - Big concerns about data protection, privacy
  - Netherlands: Rollout stopped due to privacy concerns
  - Germany: BSI Protection profile, certification required
  - Austria: Smart Grids Austria Group
    - Reference Architecture for Secure Smart Grids in Austria (RASSA)
- US
  - Focus on critical infrastructure protection (sabotage, terror)
  - Less regulation, “market-friendly”
  - Discussions about responsibilities of agencies, vendors, operators

Physical: Attack Options (Attack Tree)



Source: Paudel, Smith, Zseby: Attack Models for Advanced Persistent Threats in Smart Grid Wide Area Monitoring. In *Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids* (CPSR-SG'17).2017

Cyber-Physical: Attack Options (Attack Tree)

Source: Paudel, Smith, Zseby: Attack Models for Advanced Persistent Threats in Smart Grid Wide Area Monitoring. In *Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids* (CPSR-SG'17).2017

Smart Grid Security
Example 1: Advanced Metering Infrastructure (AMI)

AMI Security Challenges

- Resource constraints
  - Hardware costs (e.g., smart meters, gateways)
  - Transmission capacity (e.g. wireless networks)
  - Physical protection (costs)

  ➔ Limitations for security measures
- New communication patterns
  - Machine-to-machine communication
  - New protocols, new traffic patterns

  ➔ Little experience with attack patterns and traffic profiles

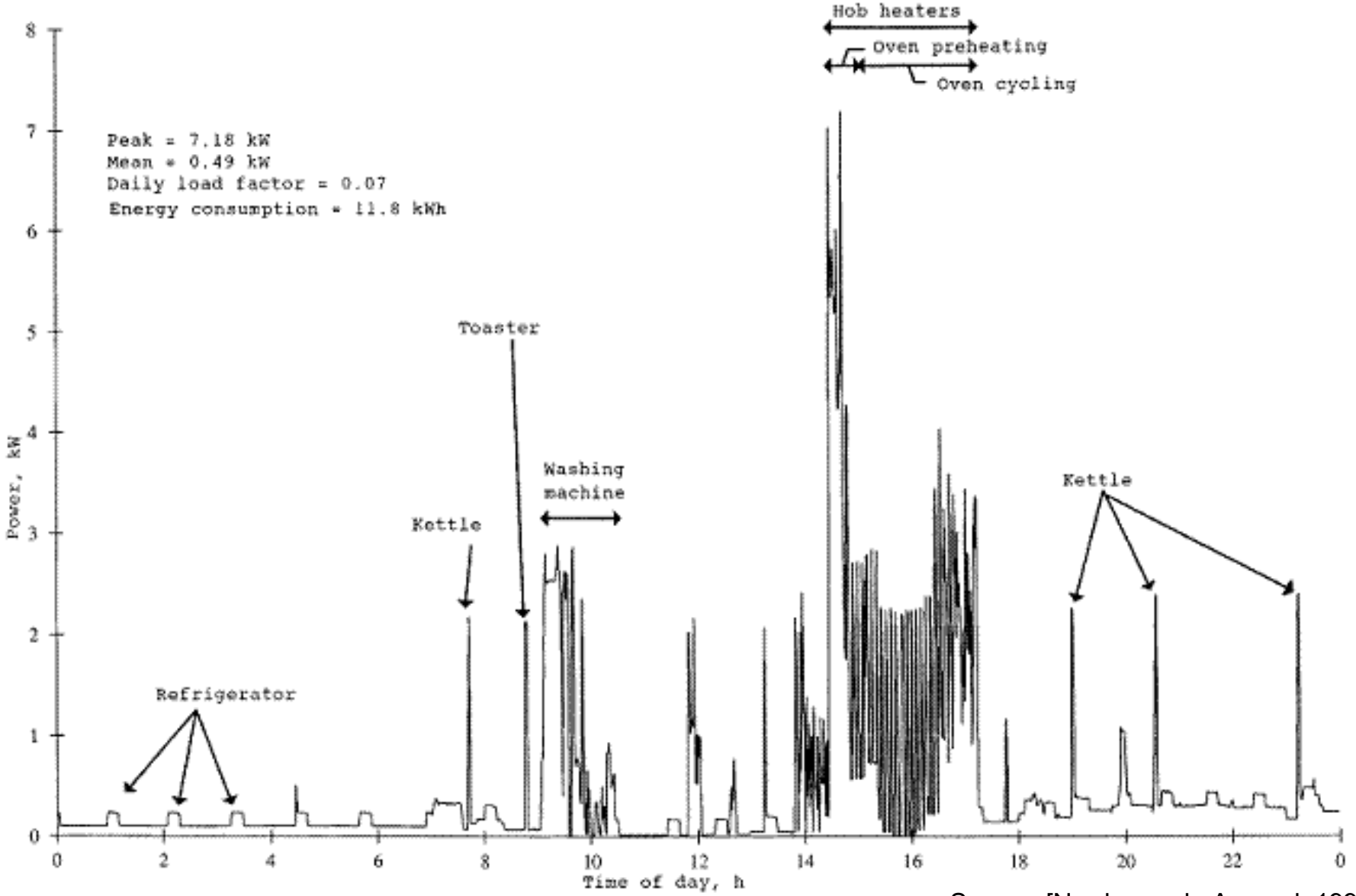
AMI Security Challenges

- Homogeneity of devices
  - large installations with many similar devices

  ➔ Fast spreading of malware
- Equipment Lifecycle
  - Long-term installations (10-20 years)
  - Broadly distributed devices ➔ hardware exchange difficult

  ➔performance difference to attack equipment
    - in 10 years attacker has a 10 years advanced hardware !

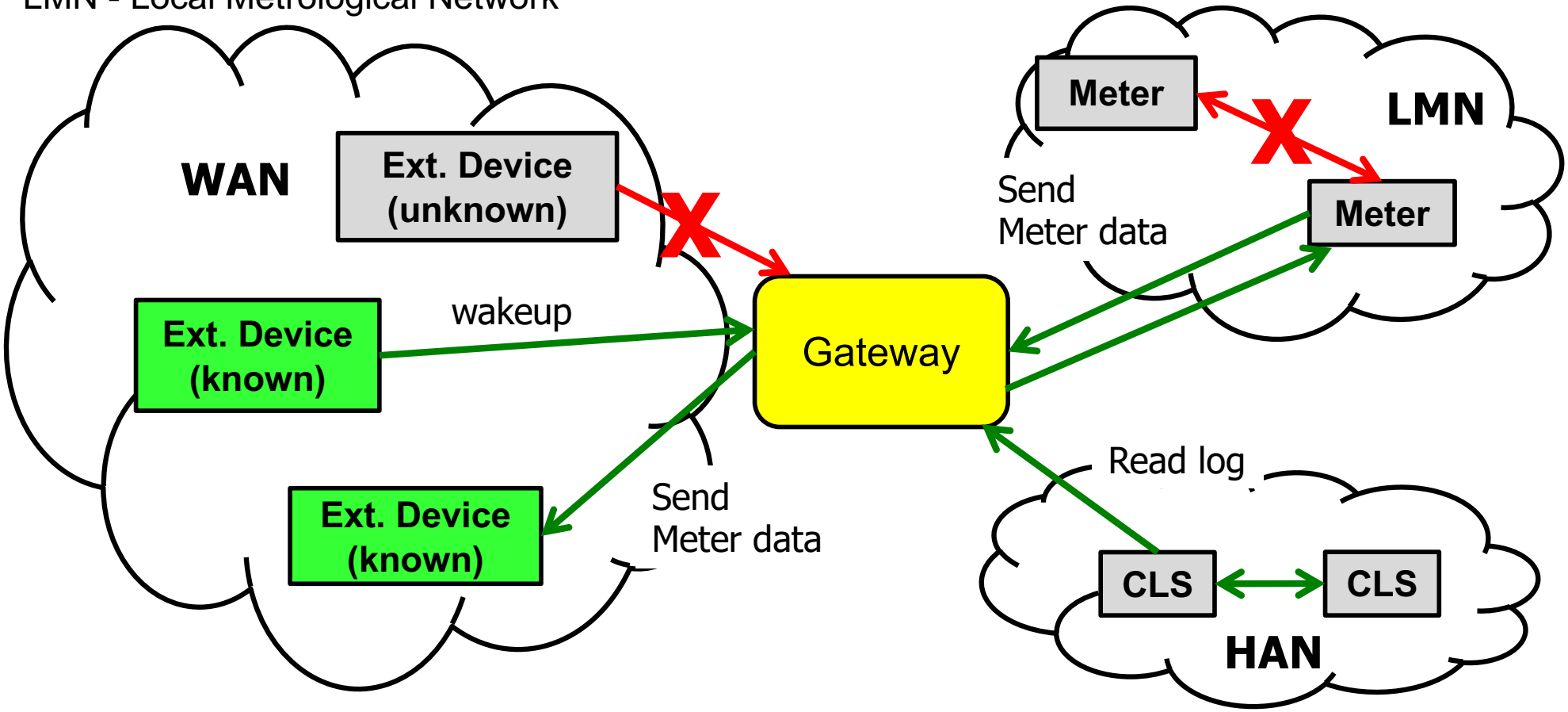
Privacy Concerns



Source: [Newborough, Augood, 1999]

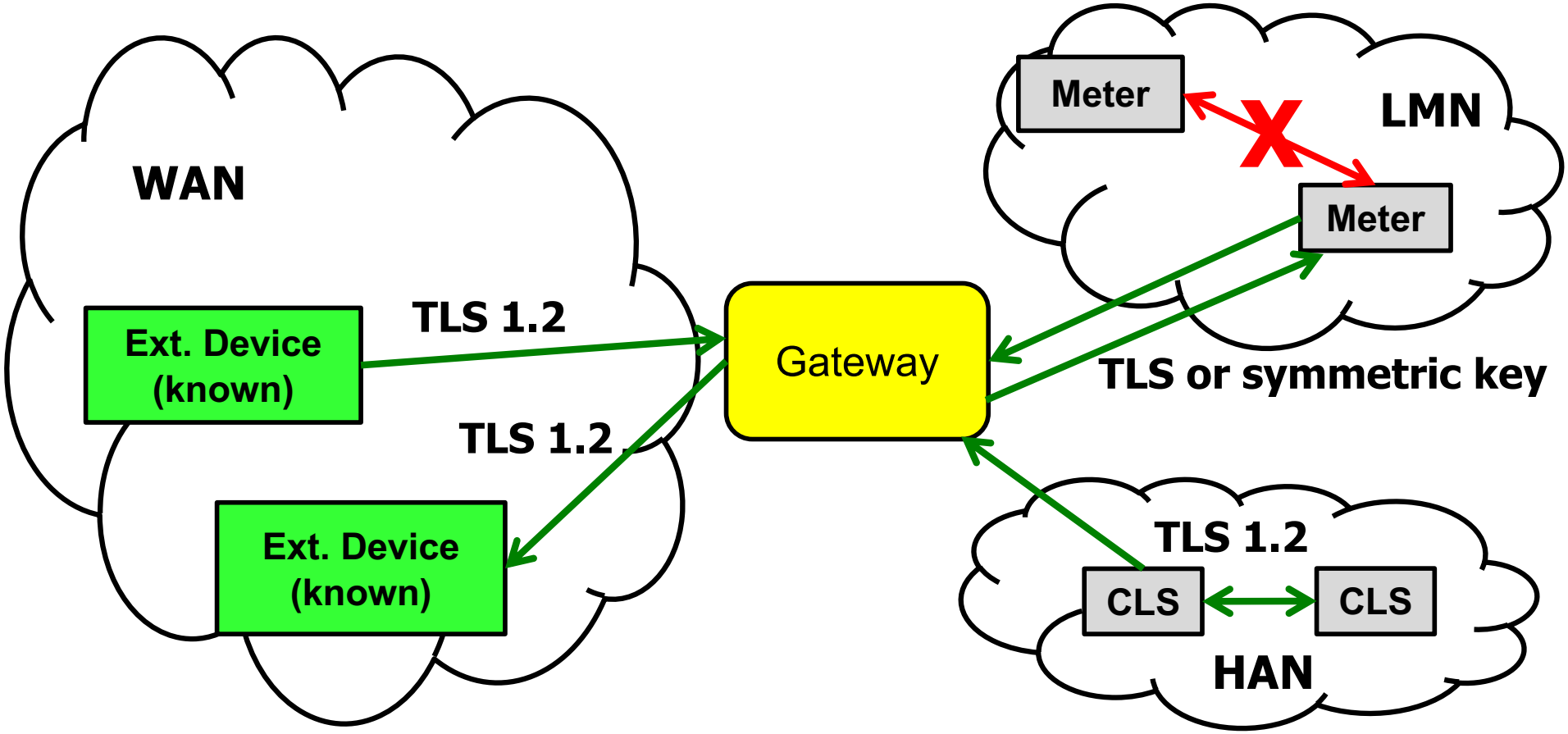
Smart Metering Gateway Protection Profile (BSI)

CLS- Controllable local System
LMN - Local Metrological Network



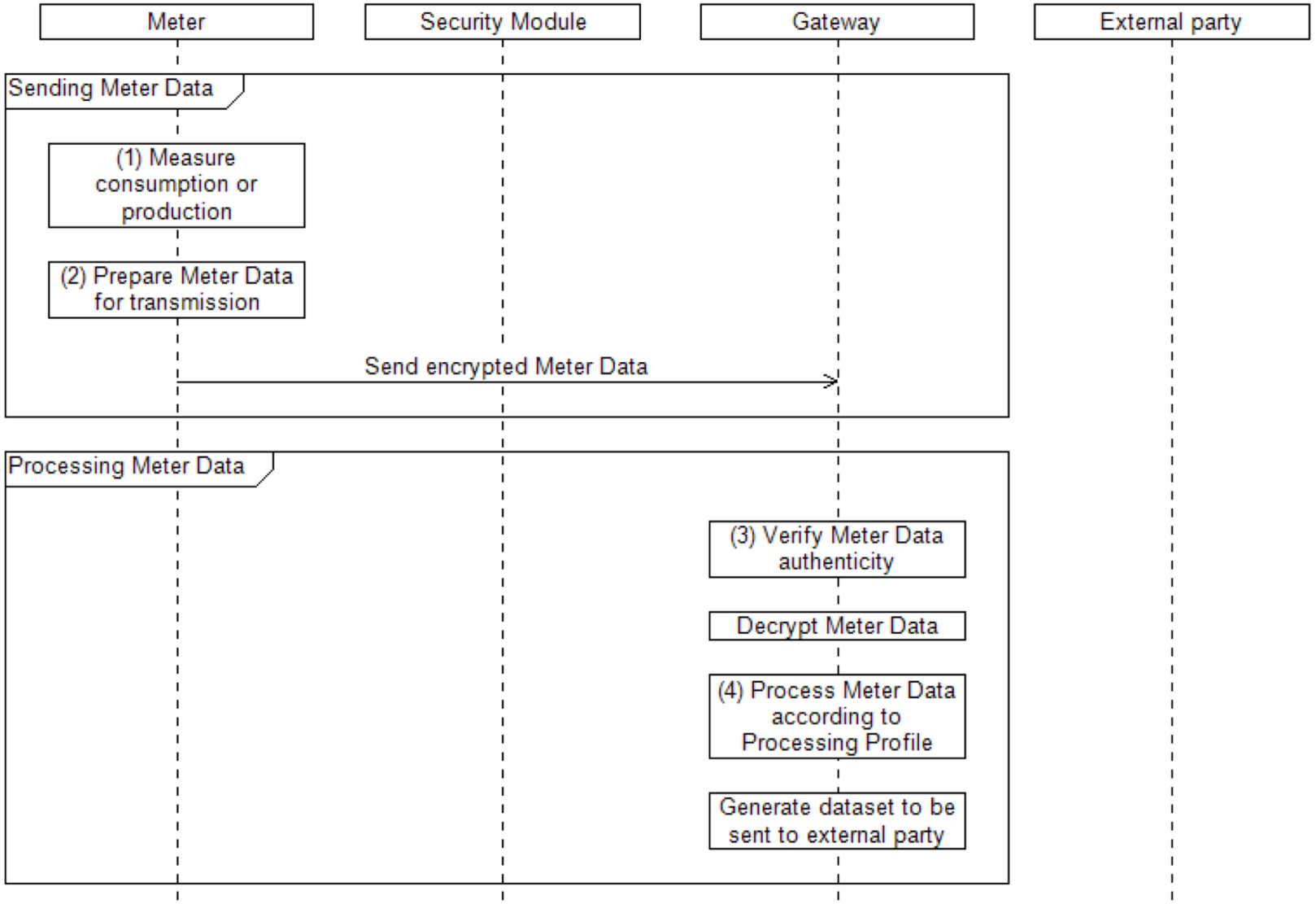
➔ Restricted communication

Smart Metering Gateway Protection Profile (BSI)



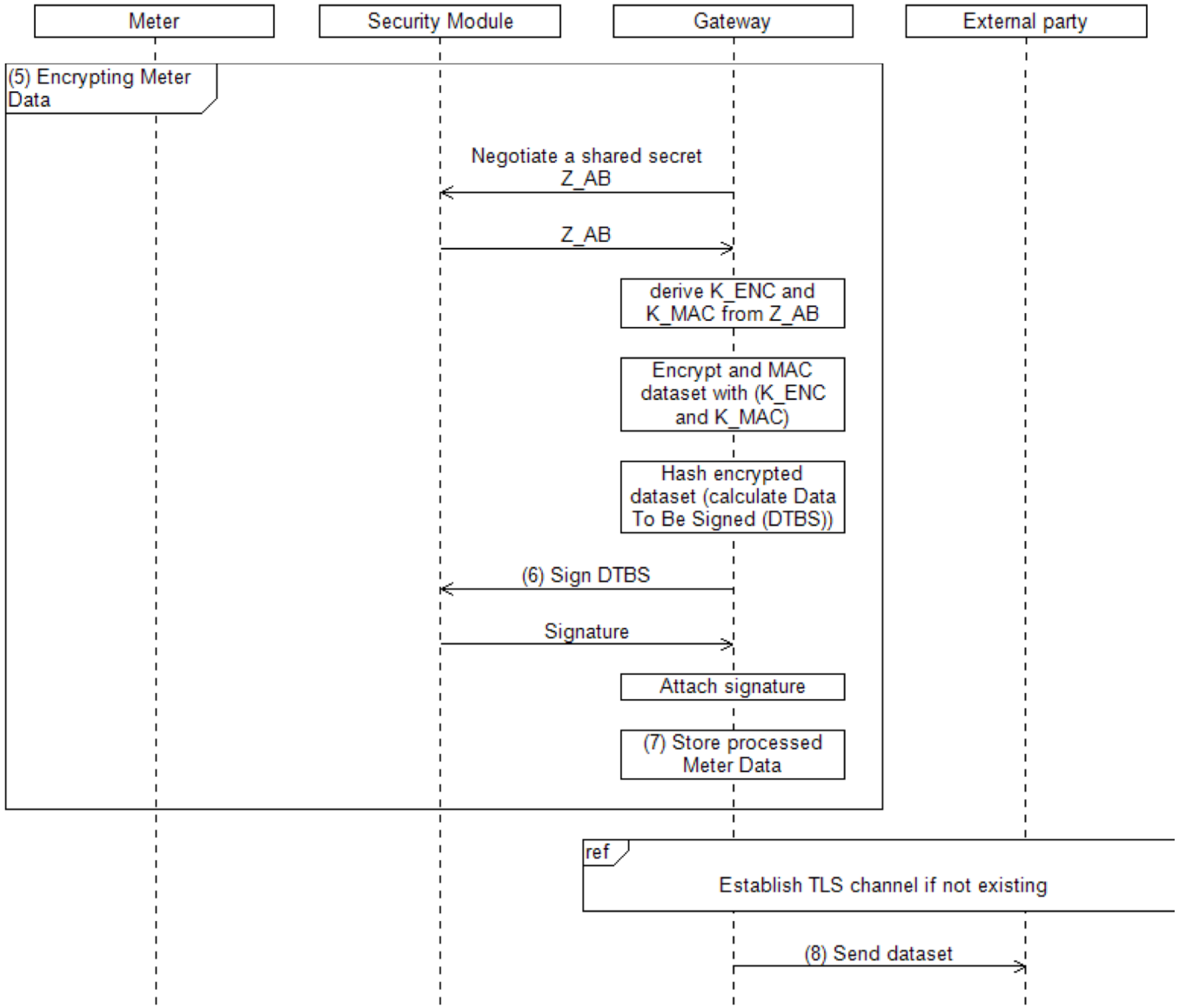
➔ Encryption
➔ Message Authentication

Message Exchange for Meter Data Reporting



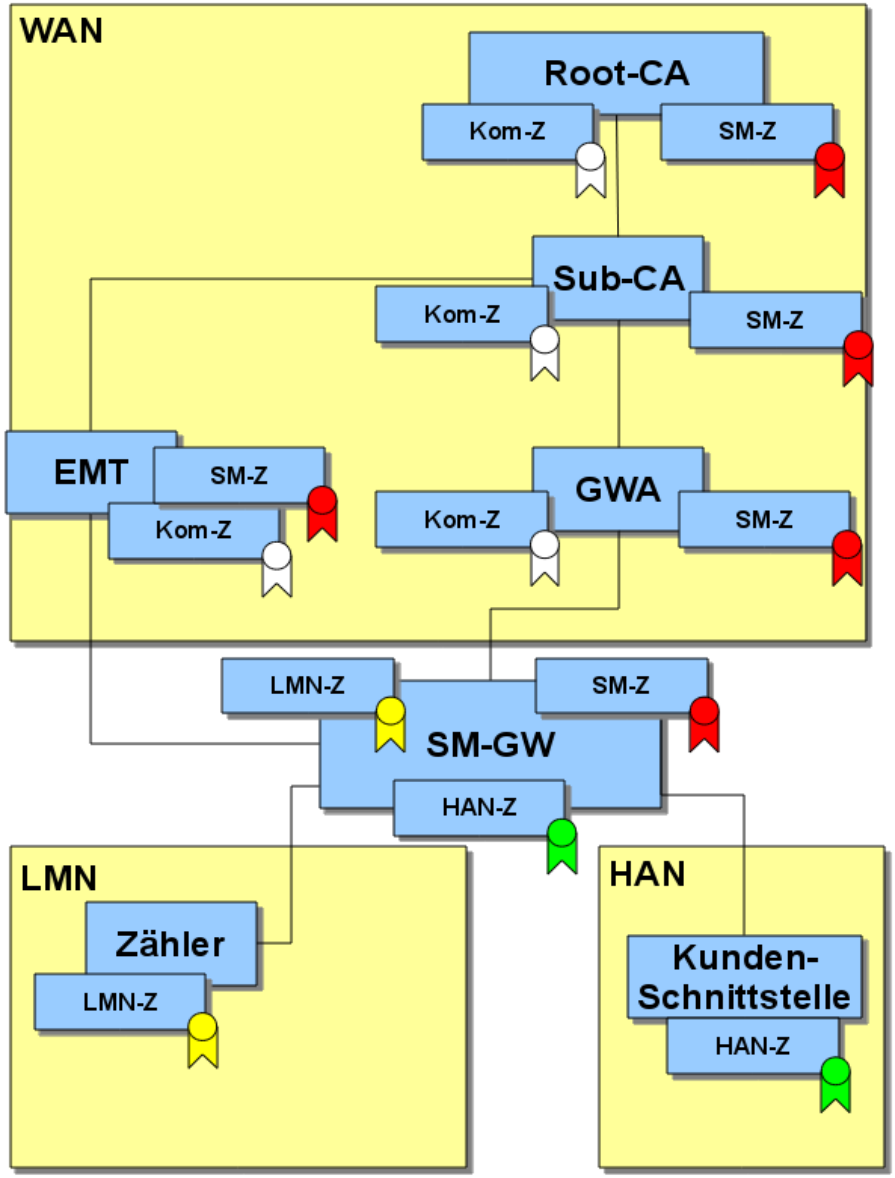
Source: BSI Smart Meter Gateway Protection Profile, Version 1.3, BSI-CC-PP-0073

Message Exchange for Meter Data Reporting



Source: BSI Smart Meter Gateway Protection Profile, Version 1.3, BSI-CC-PP-0073

Public Key Infrastructure (PKI)



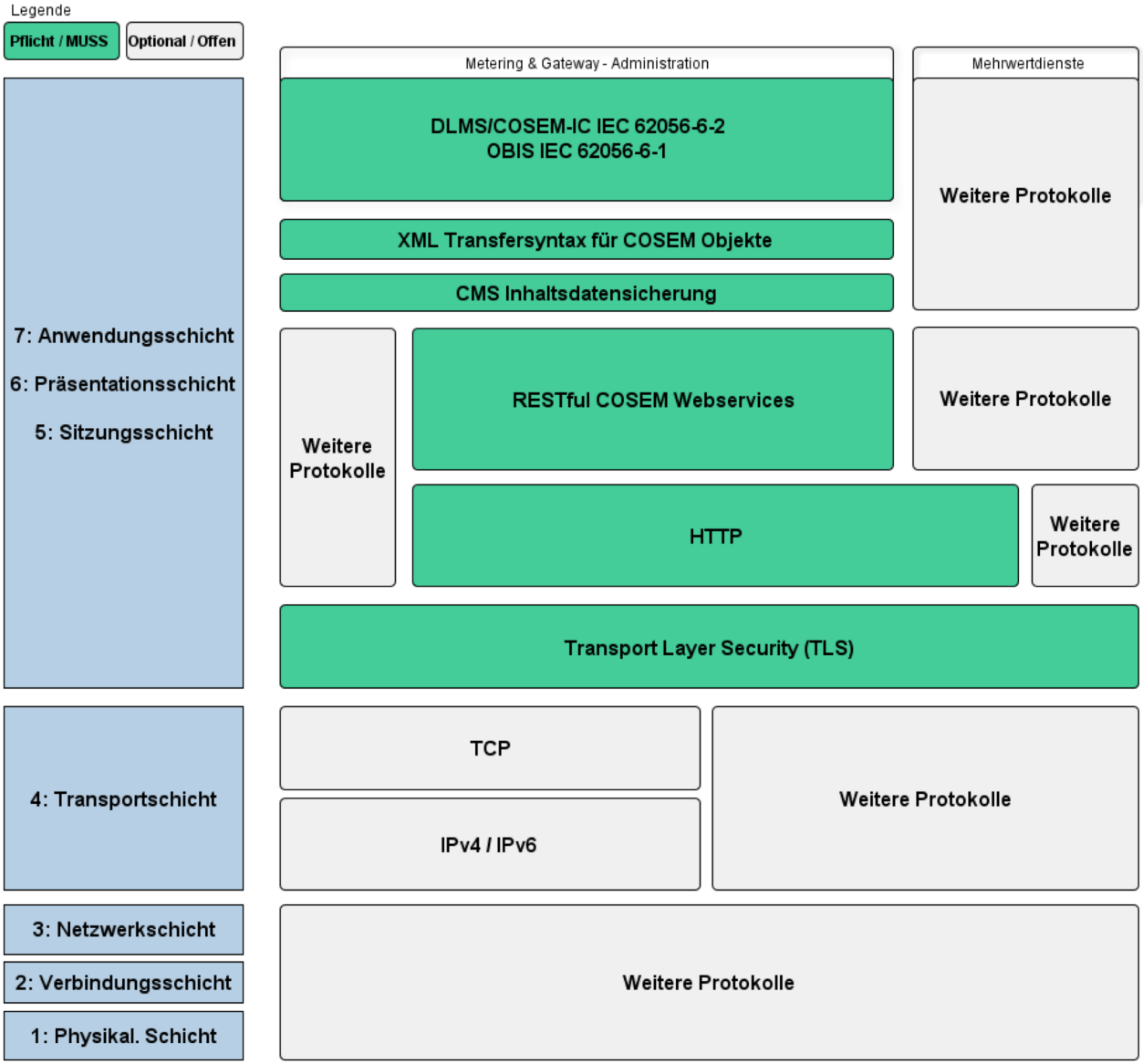
Purpose: ensure authenticity of public keys

EMT – External stakeholders
GWA- Gateway-Administrator
SMGW - Smart Meter Gateway

- smart metering certificates for communication of SMGW over WAN
- certificates for PKI Communication
- optional certificates for authentication of meters in LMN
- optional certificates for authentication of devices in HAN

Source: BSI TR-03109-4, March 2013

Communication Protocols WAN



Source: BSI Technische Richtlinie BSI TR-03109-1, March 2013

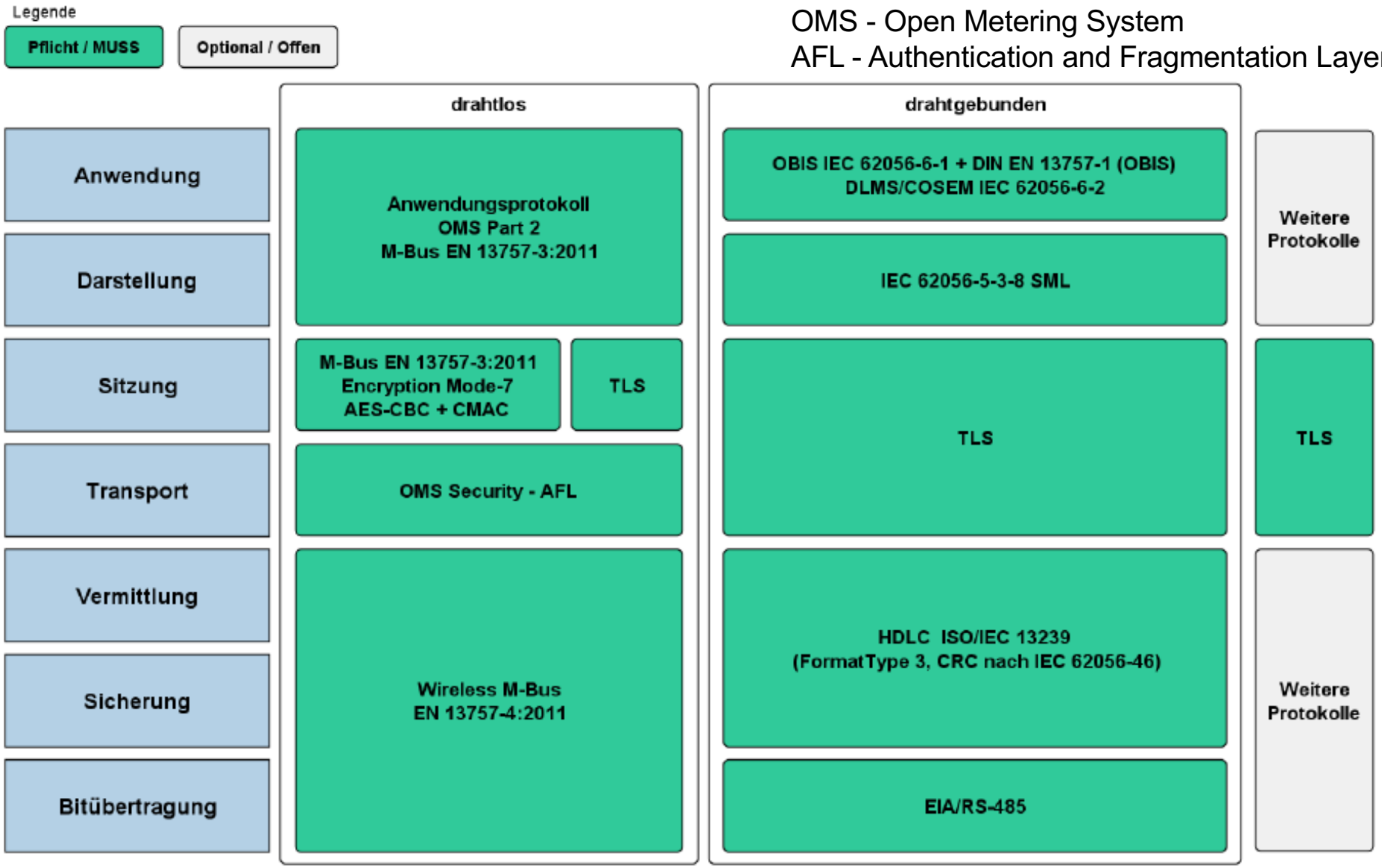
Cryptographic Methods

- Protocol
  - TLS 1.2
- Elliptic Curve Cryptography
  - Elliptic Curve Digital Signature Algorithm – ECDSA
  - Elliptic Curve Key Agreement Algorithm – ECKA
  - Defined in BSI TR-03111
- Block Cipher
  - AES
  - Different modes

TLS Communication in WAN

- Cipher Suites defined in BSI-TR-03116-3
  - Example:
    TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS version 1.2
- Key exchange:
  - ECDHE - Elliptic Curve Diffie-Hellman Ephemeral
- Authentication:
  - ECDSA - Elliptic Curve Digital Signature Algorithm
- Block Cipher
  - AES_128_CBC – AES, 128 bit key, Cipher Block Chaining mode
- Hashfunction
  - SHA256

Communication Protocols LMN



Source: BSI Technische Richtlinie BSI TR-03109-1, March 2013

TLS Communication in LMN

- TLS 1.2 used for
  - Changing keys
  - Reading meter data
  - Selecting data that should be sent
- TLS parameters
  - ECC based (same cipher suites as for WAN)
  - Maximum session duration: 1 month or 5 MB
  - Certificates maximum valid for 7 years
- Meters should be able to
  - Update initial keys
  - Update firmware

  ➔ allow new cryptographic methods

LMN Communication with Symmetric Encryption

- Some meters may not be able to support TLS
  - Support only unidirectional communication ➔ cannot establish TLS channel
  - Limitations regarding bandwidth and availability of suitable communication channel
- ➔ use of symmetric encryption
  - Only allowed if TLS is not possible on meter
  - Meter vendor installs random 128bit key in meter
  - Meter owner sends key to gateway administrator (confidential, authenticated)
  - ➔ meter and gateway have a shared secret key
  - Use key to derive keys for encryption and MAC
  - Key must be changed at least every 2 years

Communication Protocols HAN

- Communication
  - Report data to consumer
  - Report data to service technician
  - Communication between CLS and authorized external market participant
- All communication uses TLS
- CLS can establish connection to external market participant
  - Using the gateway
- If external market participant wants to establish connection to CLS
  - Gateway administrator needs to initiate connection

Smart Meter Gateway

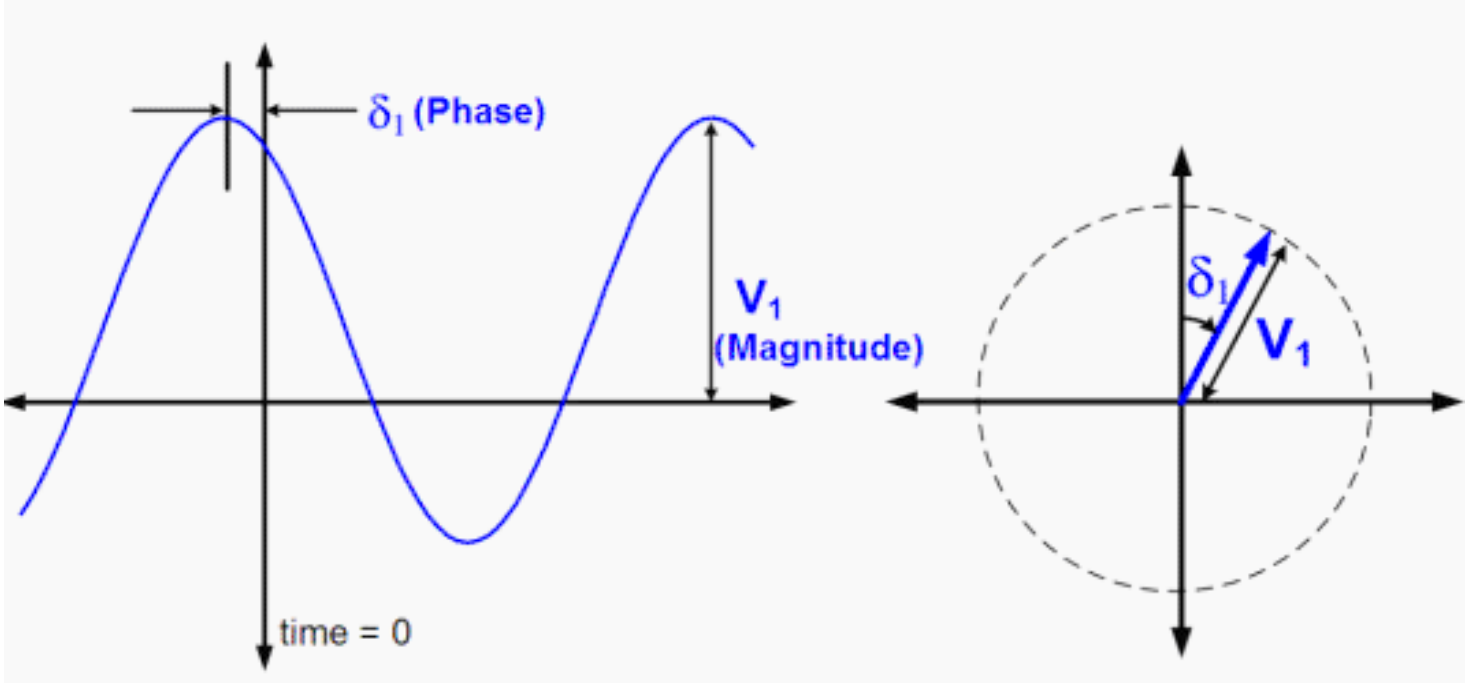
- Protection for Metering Infrastructure
  - Use of TLS
  - Public Key Infrastructure
  - Certification process required

- Several further challenges
  - Only for smart metering environment
  - Cryptographic functions ➔ hardware costs
  - Reactive security, Monitoring functions

Smart Grid Security
Example 2: Wide Area Monitoring Systems (WAMS)

Phasor Measurements

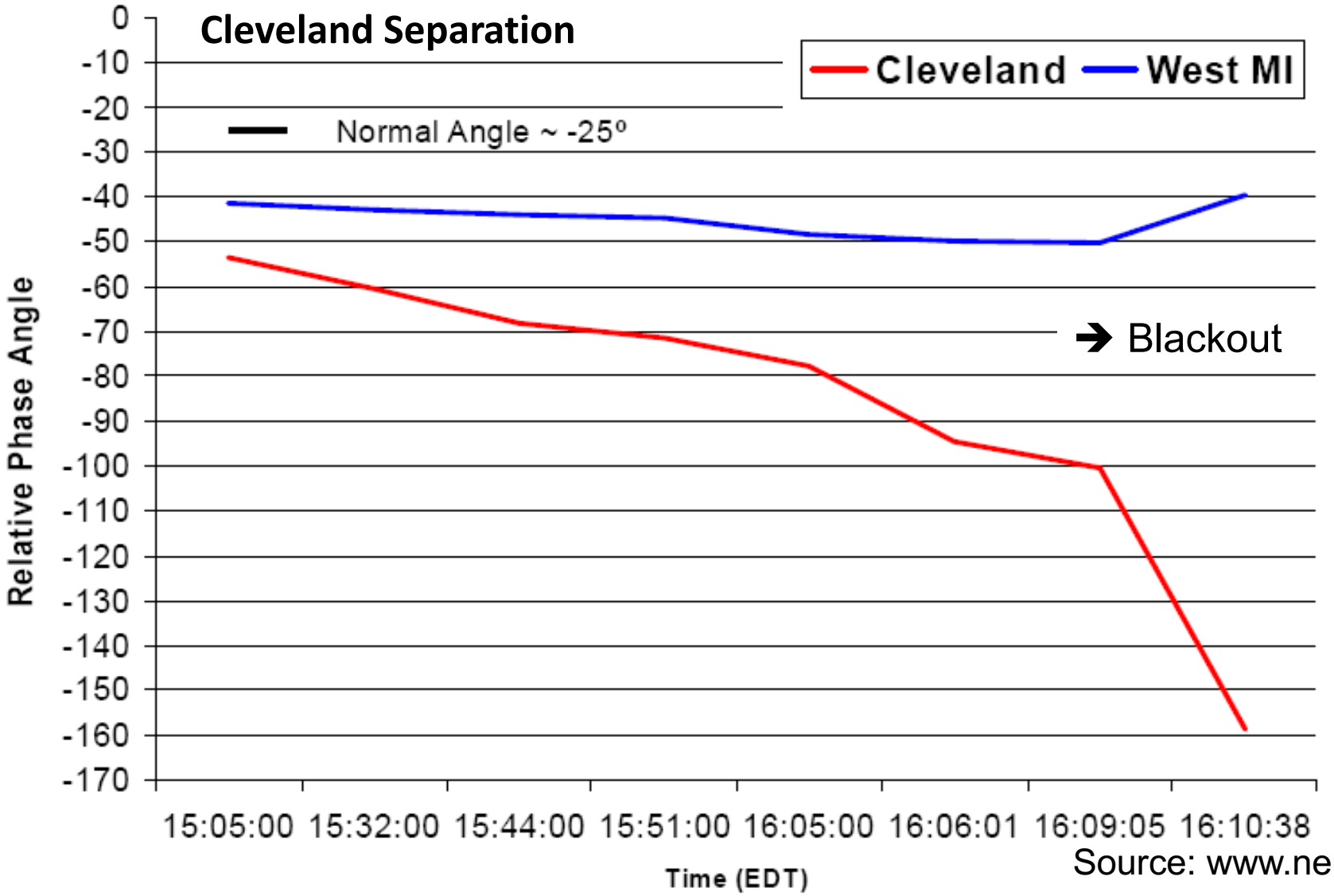
- Phasor Measurement Units (PMUs) measure
  - Voltage phasor
  - Current phasor
  - Frequencies, etc.



Source: NERC, Real-Time Application of Synchrophasors for Improving Reliability, 2010

Motivation

August, 14, 2003



Source: www.nerc.com

Wide Area Monitoring, Protection and Control

- Goal: ***situational awareness*** in electric grid
  - Measure state of electric grid (power quality, substations, etc.)
  - Support existing measurements (e.g. in SCADA)
  - Detect power system events
  - Collect historic data
  - Visualization
  - Take control actions based on observed events

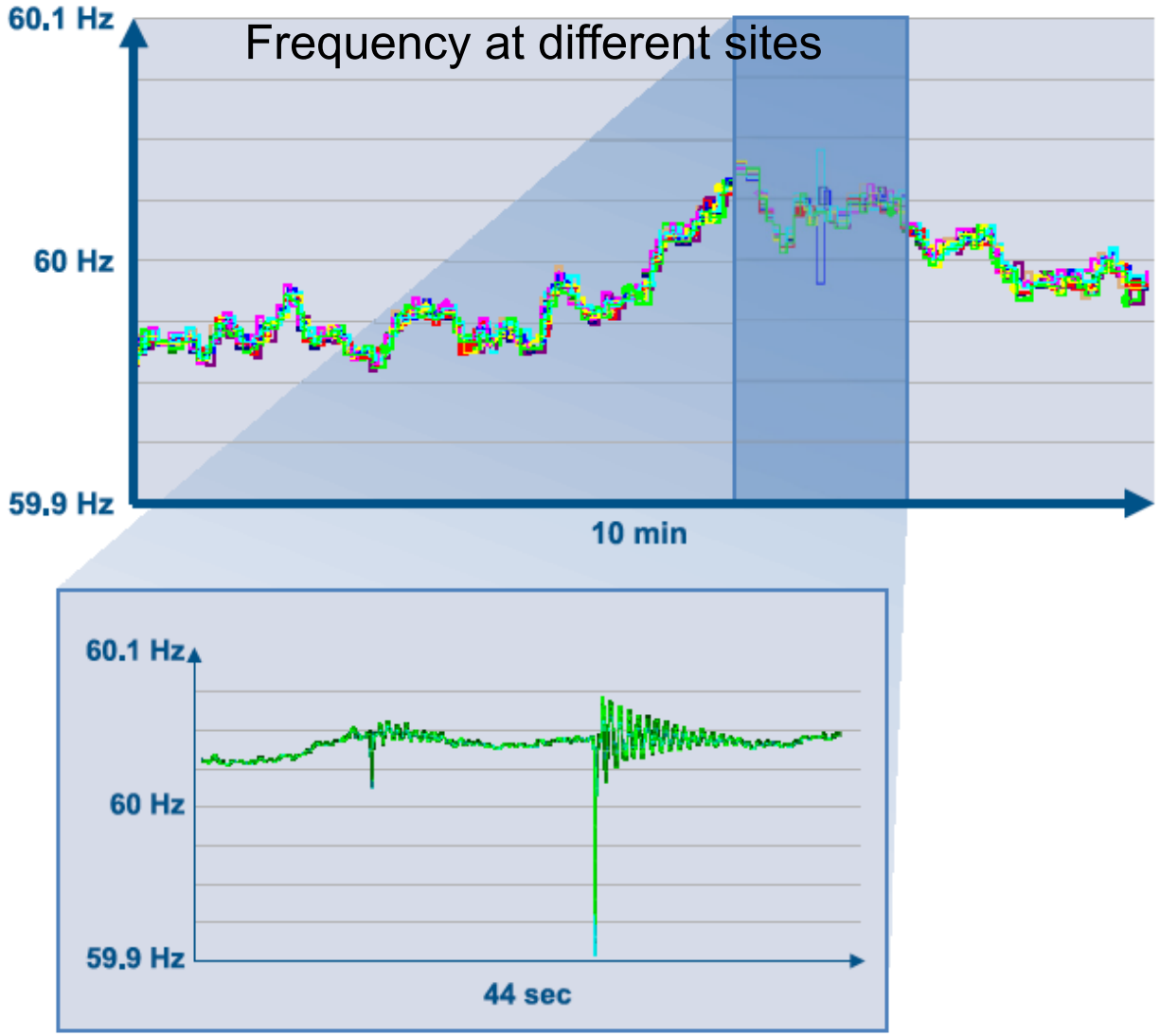
- Application fields: control system stability, load shedding, blackout prediction, post incident analysis..

PMUs in Action: http://www.youtube.com/watch?v=RhAzeyU8RVc

PMU vs. SCADA

SCADA

PMU



Source: NASPI Program Fact Sheet, June 2012

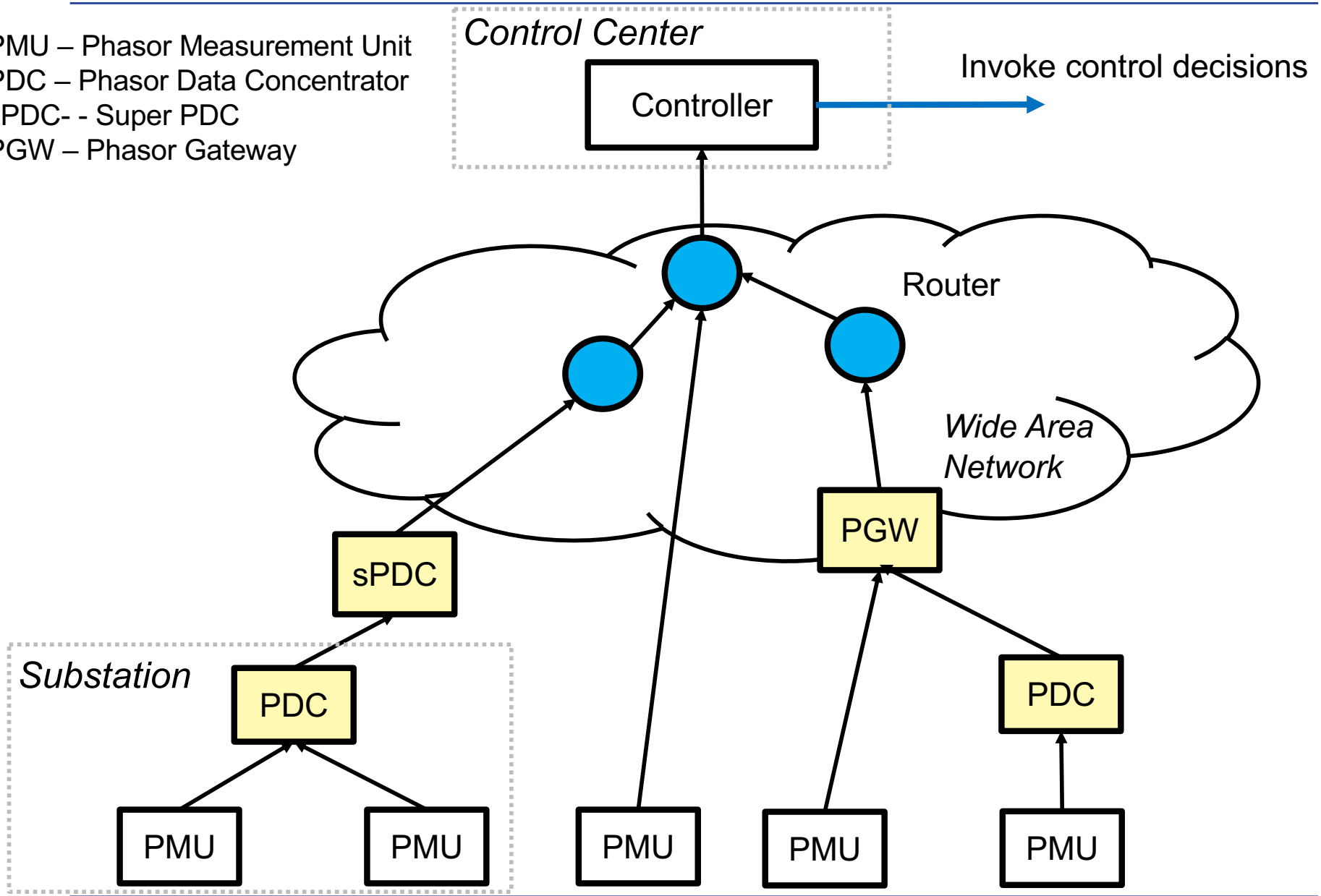
Synchrophasor Measurements

- Collection of data from ***distributed*** measurements

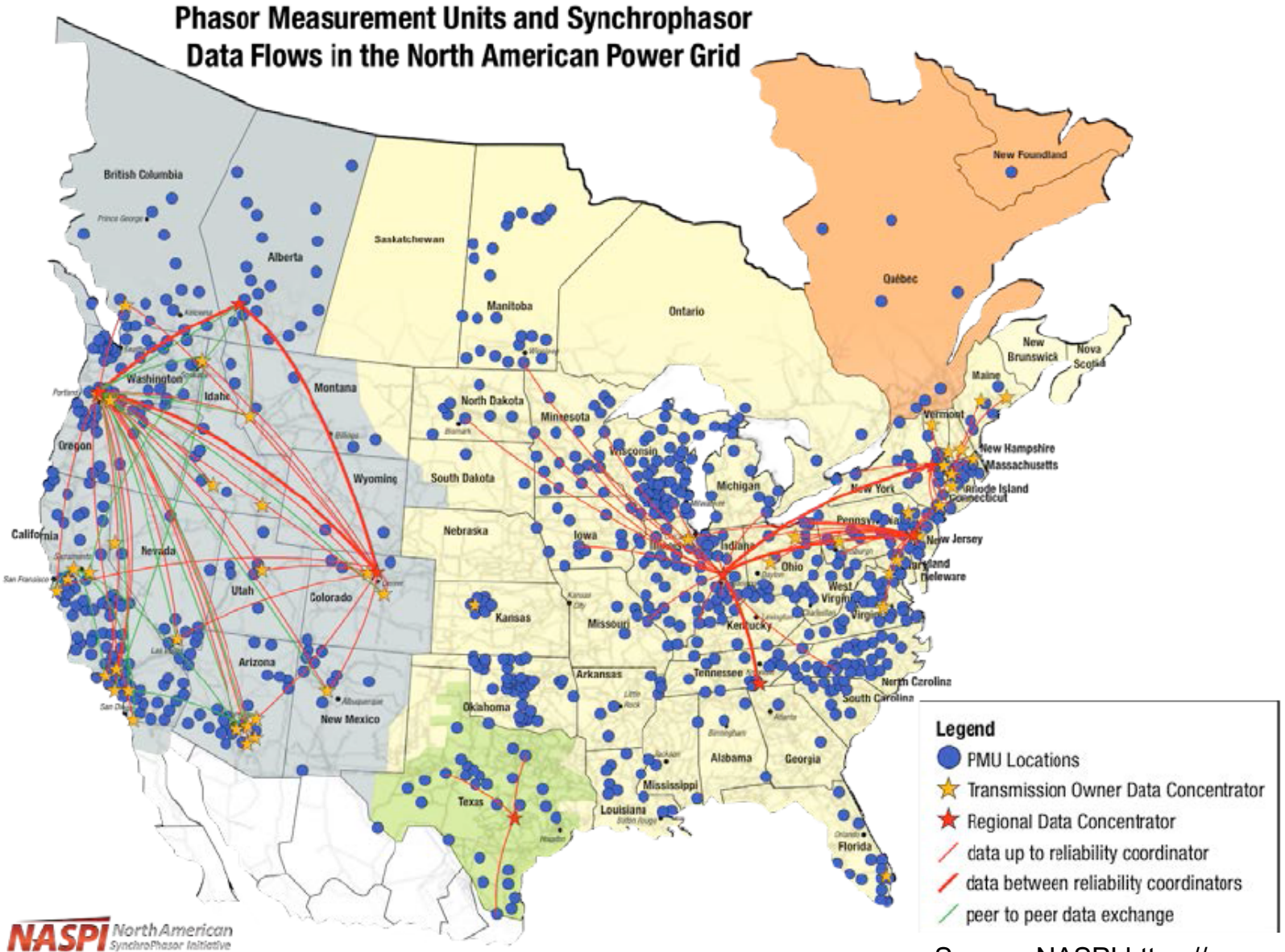
- ***Phasor Measurement Units*** (PMUs)
  - Clock synchronized (GPS signal) measurements
  - Transmit 30-120 measurements per second
- ***Phasor Data Concentrators*** (PDCs)
  - Collect and correlate data from multiple PMUs
  - Discover phase shifts, frequency differences, etc.
  - Report collected/processed data to other applications, storage or human operator
- Are PMUs and PDCs Cyber Critical Assets (CCA)?
  - Still debate

WAMS Variants

PMU – Phasor Measurement Unit
PDC – Phasor Data Concentrator
sPDC- - Super PDC
PGW – Phasor Gateway



Deployment (2014)

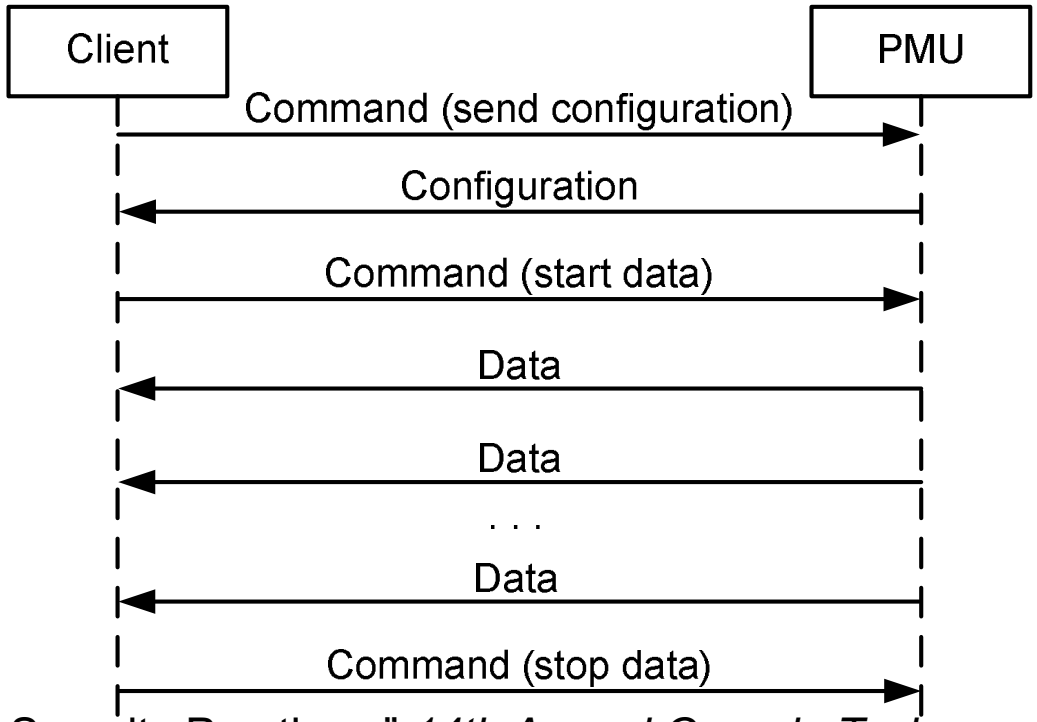


Source: NASPI https://www.naspi.org/

IEEE C 37.118

- Synchrophasor Communication Standard
  - PMUs preconfigured (measurement frequency,etc)
  - PDC/client requests configuration information and data
  - PMU sends configuration frame and data stream

- Communication
  - UDP, TCP or both
  - No encryption
  - No integrity check



Source: J. Stewart, et al. "Synchrophasor Security Practices." *14th Annual Greogia Tech Fault and Disturbance Analysis Conference*. 2011

WAMS Security

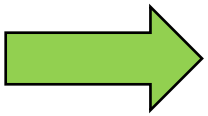
Communication Demands

- Latencies are critical
  - Fast reporting of measurement values (failure detection, automated control)
  - Prioritization for Alarms ➔ QoS
- Highly distributed (wide area) sensors
  - Data Transmission over wide area network
  - Many potential attackers
- Group Communication
  - Transmit the same data to multiple receivers
  - Most efficient by using multicast functions
- High Security demands
  - Wrong state information ➔ wrong control actions

➔ Many challenges for security protocols

WAMS Security

Confidentiality
Integrity
Availability

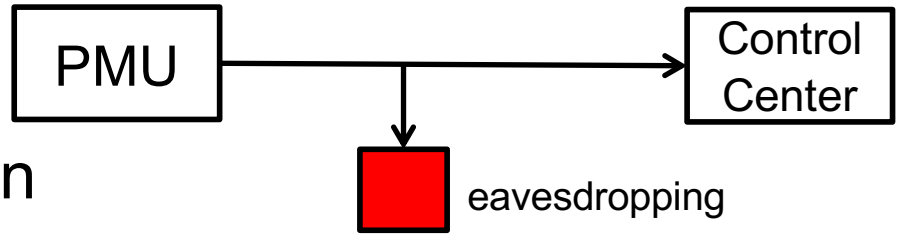


Availability
Integrity
Confidentiality

- Availability
  - No measurements ➔ no situational awareness
  - ➔ ensure that control systems get required input data
- Integrity
  - Wrong measurements➔ wrong control decisions
  - ➔ prevent modification of sensor data
- Confidentiality
  - Transmitted information may be used to prepare attack
  - ➔ prevent eavesdropping

Reconnaissance Attacks

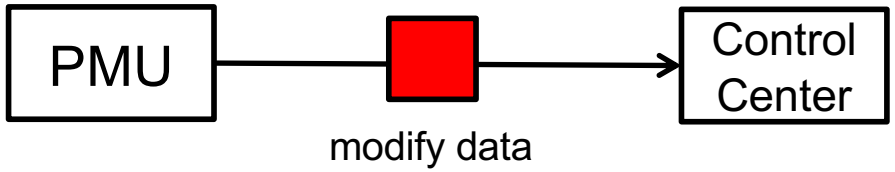
- "Finger print" systems for attack preparation
  - Device ID, operating system, software versions
  - Open ports
- C37.11 frames contain
  - Configuration information
  - Substation names
  - GPS coordinates ➔ location of PMU
- Remote access with password authentication
  - But: passwords transmitted in plaintext…
- Countermeasure: Encryption (IPsec, TLS)
  - But: introduces latencies



Source: Morris et al., Cyber security recommendations for wide area monitoring, protection, and control systems IEEE Power and Energy Society General Meeting, 2012

Packet Injection Attacks

- Sensor measurement Injection
  - Inject false sensor data into control system
  - Can influence control decision
- Command Injection
  - Injects false commands in control system
  - Can trigger incorrect control actions



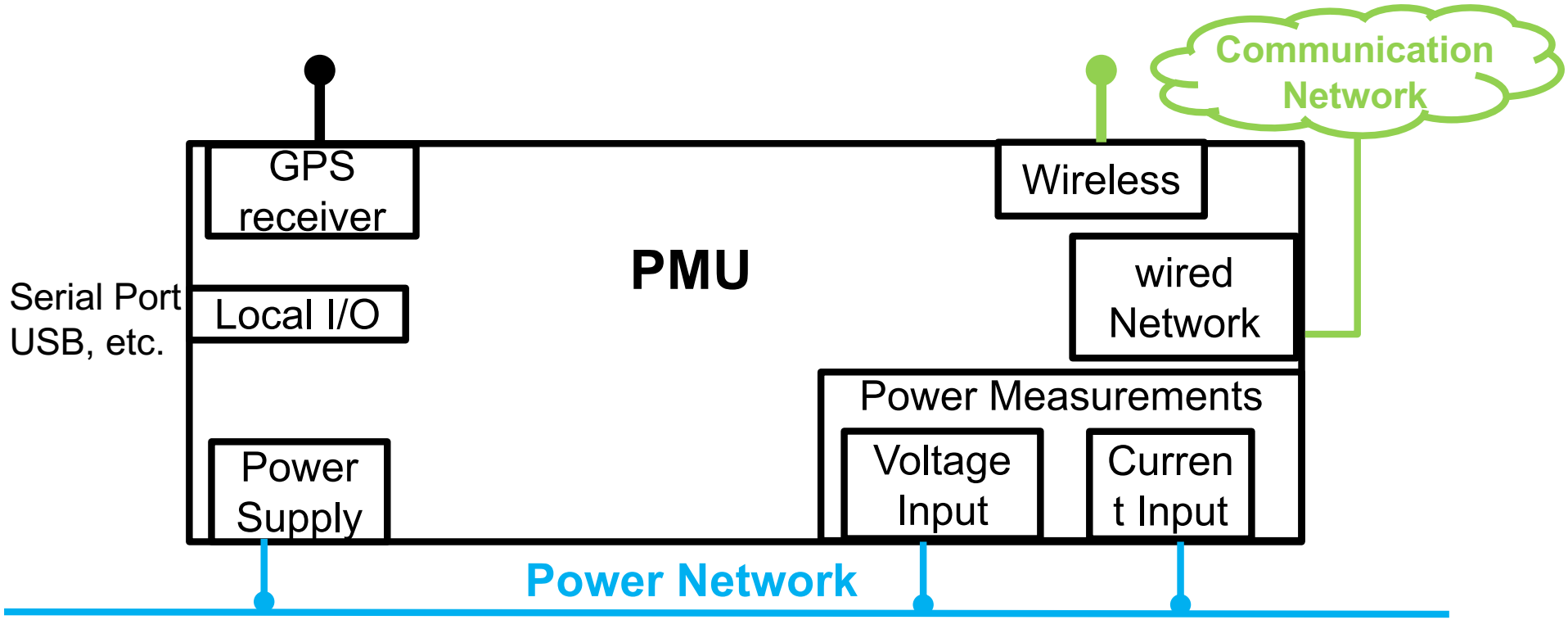
Source: Morris et al., Cyber security recommendations for wide area monitoring, protection, and control systems IEEE Power and Energy Society General Meeting, 2012

Denial of Service Attacks

- Disrupt communication link
  - E.g. overload devices or links
- Control loop does not get required sensor data
  - ➔ disrupts process control

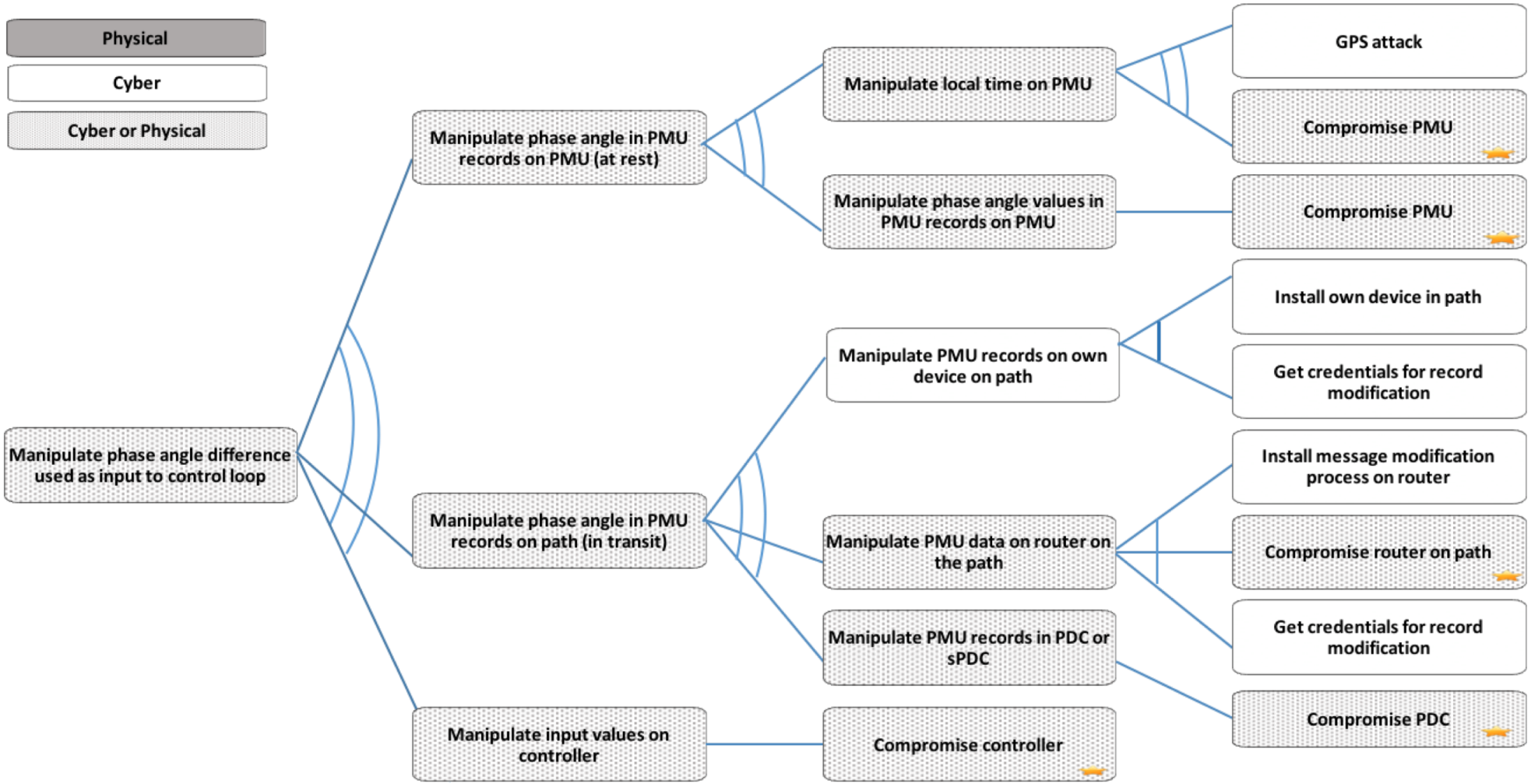
Source: Morris et al., Cyber security recommendations for wide area monitoring, protection, and control systems IEEE Power and Energy Society General Meeting, 2012

Interfaces ➔ Attack Options



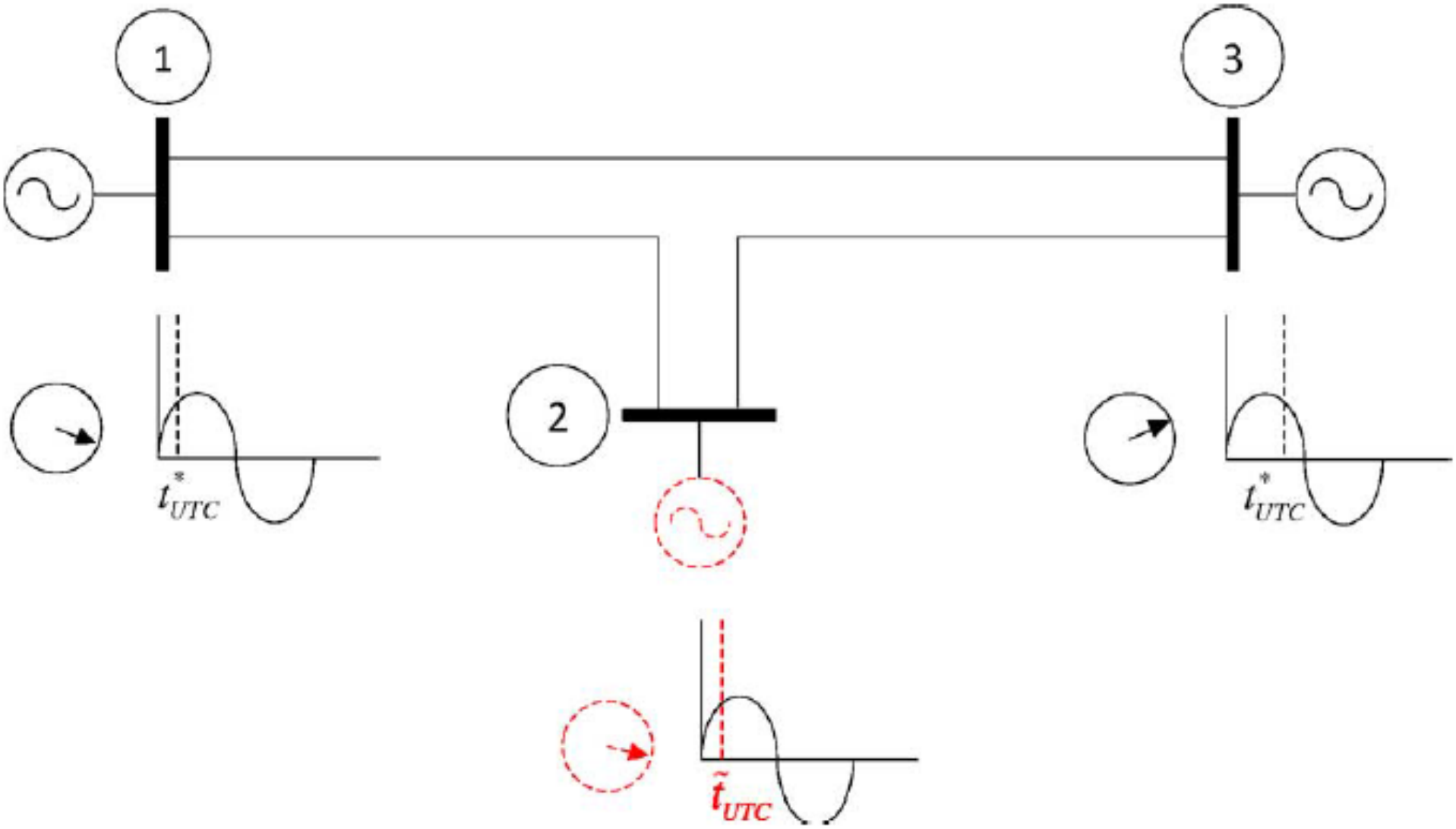
Source: Paudel, Smith, Zseby: Data integrity attacks in smart grid wide area monitoring.
In *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016* (ICS-CSR '16).

Attack Tree



Source: Paudel, Smith, Zseby: Data integrity attacks in smart grid wide area monitoring.
In *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016* (ICS-CSR '16).

GPS Spoofing influence to Phasor Measurements

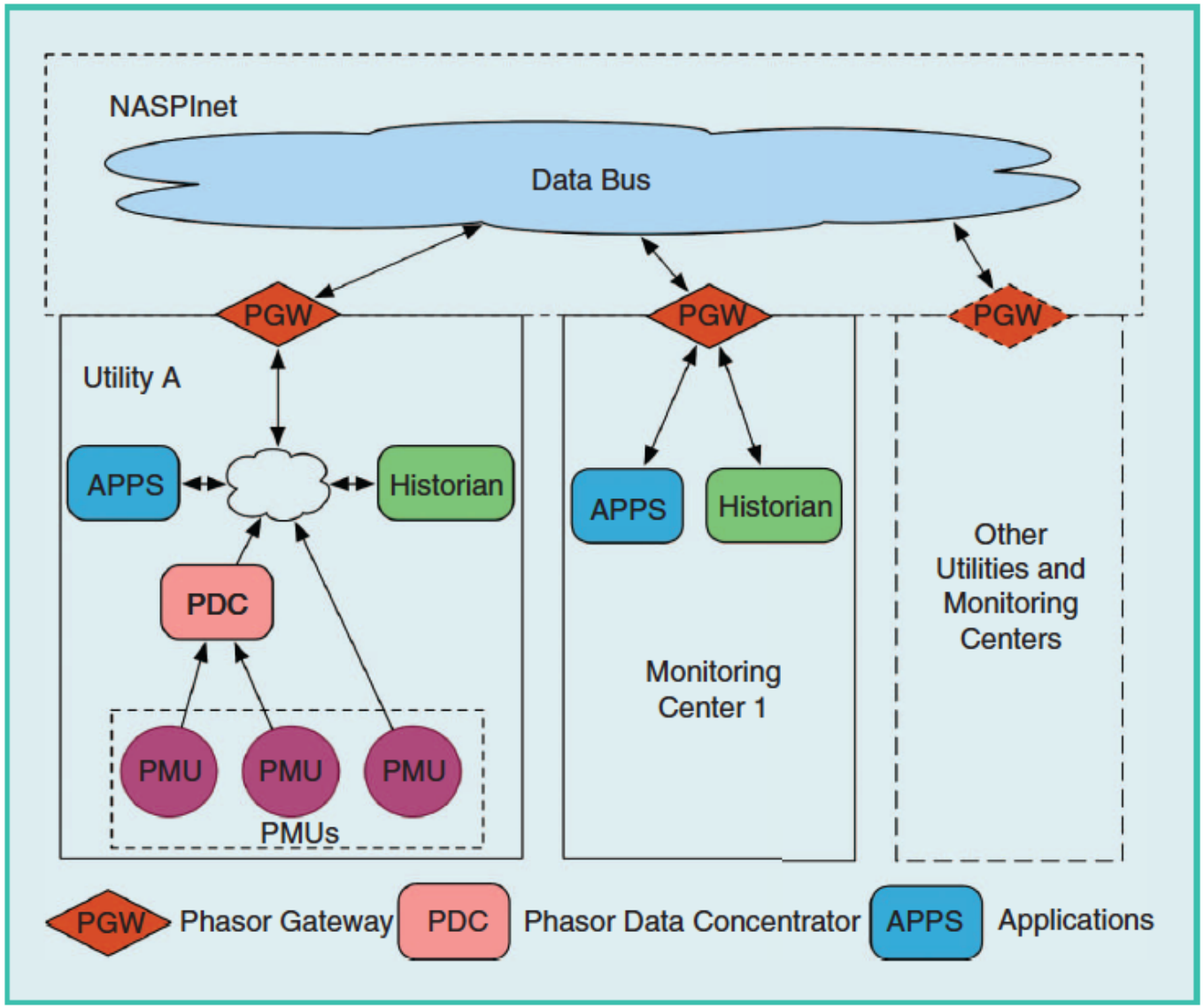


Source: Jiang, et al., Spoofing GPS Receiver Clock Offset of Phasor Measurement Units, IEEE Trans. on Power Systems, VOL. 28, NO. 3, 2013

North American SynchroPhasor Initiative (NASPI)

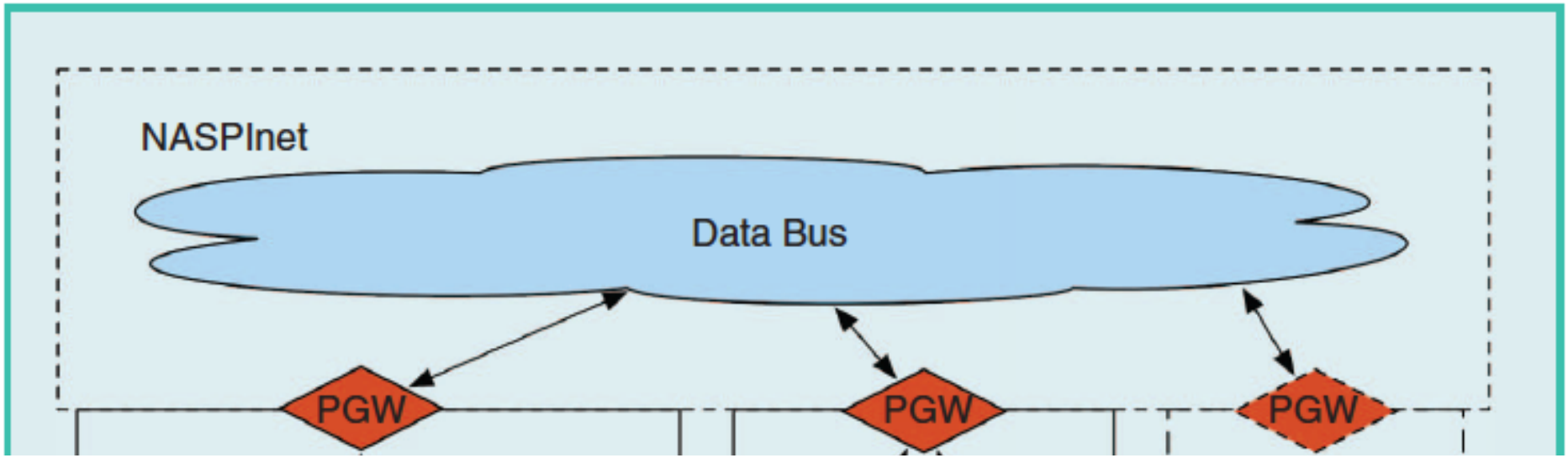
- Goals
  - Improve power system reliability and visibility
  - Wide area measurement and control
  - Use of synchrophasor technology
- Formed in 2007
  - U.S. Department of Energy (DoE)
  - National Electric Reliability Council (NERC)
  - Electric utilities
- Network of PMUs
  - Requires secure high-speed wide area communication ➔ NASPI Network (NASPInet)

NASPInet



Source: Bobba et al. "Enhancing Grid Measurements: Wide Area Measurement Systems, NASPInet, and Security," in *Power and Energy Magazine, IEEE* , vol.10, no.1, pp.67-73, Jan.-Feb. 2012

NASPInet



- Phasor Gateways (PGWs)
  - Publish synchrophasor measurements
  - Subscribe to receive synchrophasor measurements from other PGWs
- Group Communication useful

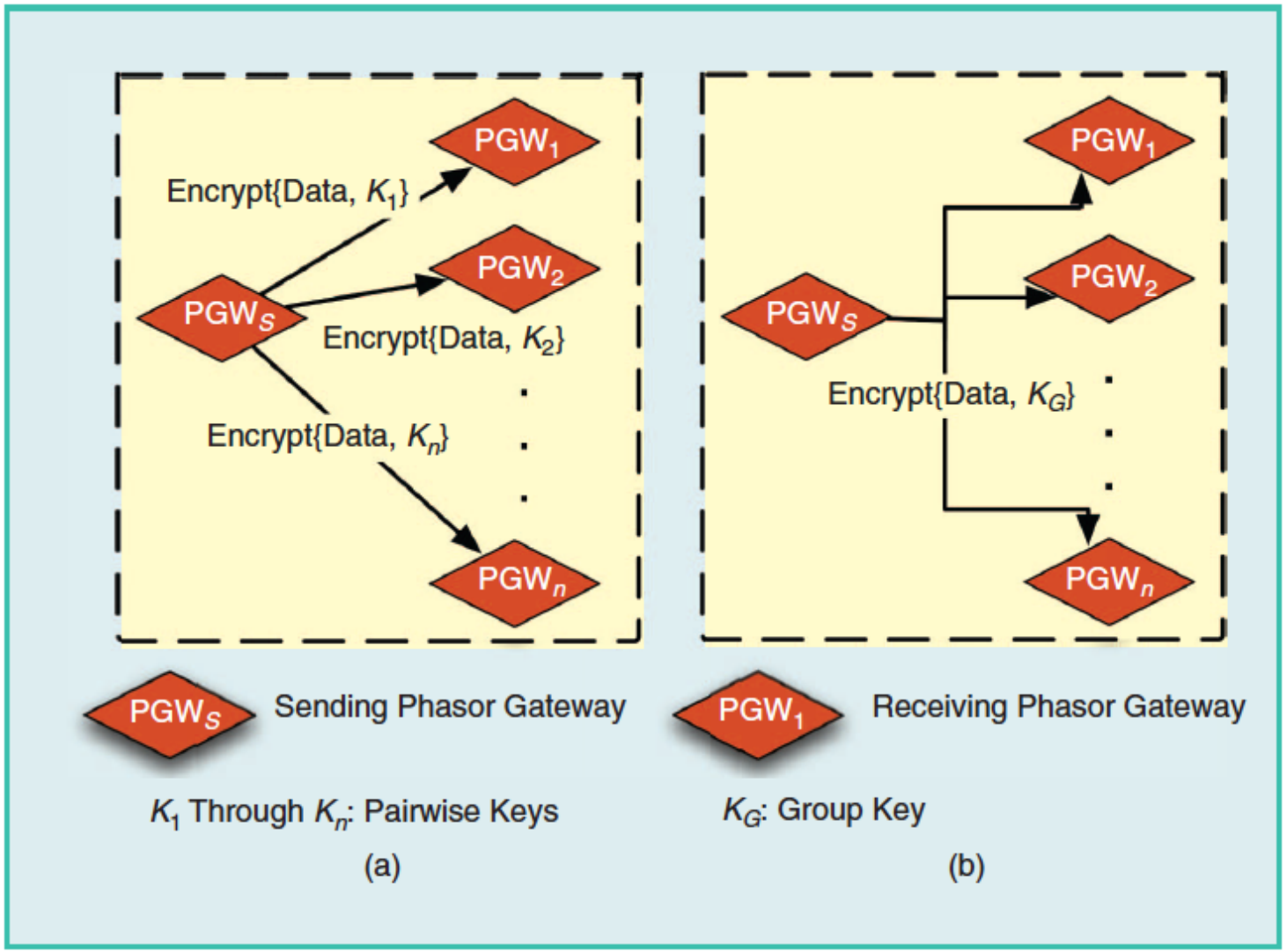
Source: Bobba et al. "Enhancing Grid Measurements: Wide Area Measurement Systems, NASPInet, and Security," in *Power and Energy Magazine, IEEE* , vol.10, no.1, pp.67-73, Jan.-Feb. 2012

Authentication Methods

- Source Authentication
  - Ensures that message originated from source

- Group Authentication
  - Ensures that message originated from a group member
  - Possible if group members work with symmetric key (e.g., no asymmetric crypto available)

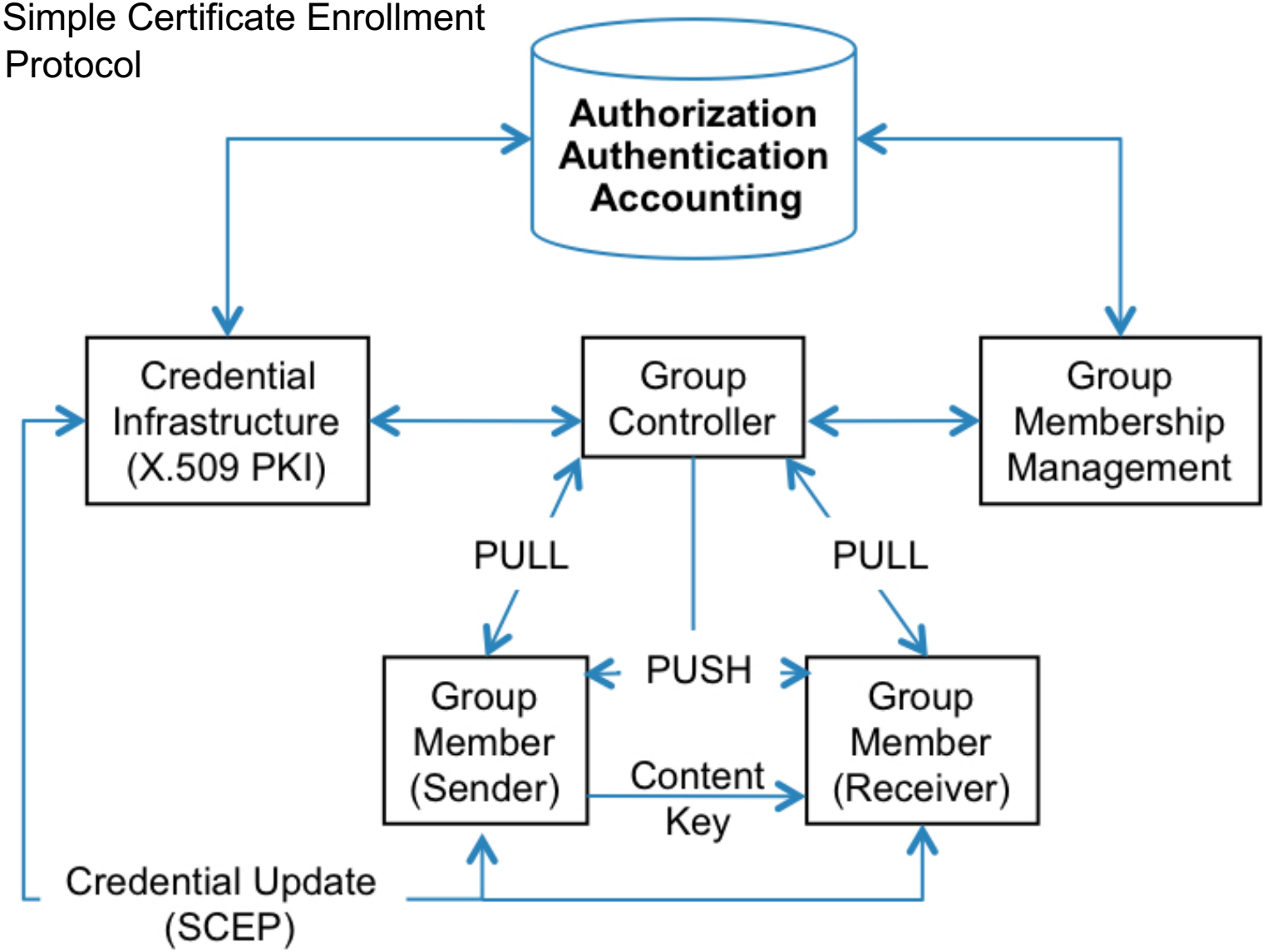
NASPInet: Group Communication



Source: Bobba et al. "Enhancing Grid Measurements: Wide Area Measurement Systems, NASPInet, and Security," in *Power and Energy Magazine, IEEE* , vol.10, no.1, pp.67-73, Jan.-Feb. 2012

Group Domain of Interpretation (GDOI)

SCEP - Simple Certificate Enrollment Protocol



Source: "WikipediaGDOI FBD" by Mbaugher

Smart Grid Security

- Security very important
  - Critical Infrastructure ➔Tempting target
  - Many challenges (homogeneity, hardware lifecycle)
  - Expertise in IT and Energy required
- Plenty of different Standards
  - Coordination just starts
  - Some outdated methods
- National efforts
  - Partial solutions (e.g., gateway)
  - EU/US mandates
- Still Work in Progress
  - Moving Target: Protocols, Architectures
  - Very few security solutions deployed, many mistakes

Thank you!