

2nd International Cyber Resilience Conference
1 - 2 August, 2011
Perth, WA, Australia

Gap Analysis of Intrusion Detection in Smart Grids

Nishchal Kush, Dr. Ernest Foo, Dr. Ejaz Ahmed, Dr. Irfan Ahmed, Prof. Andrew Clark
Information Security Institute, Queensland University of Technology
{n.kush, e.foo, e.ahmed, irfan.ahmed, a.clark}@qut.edu.au.



Introduction

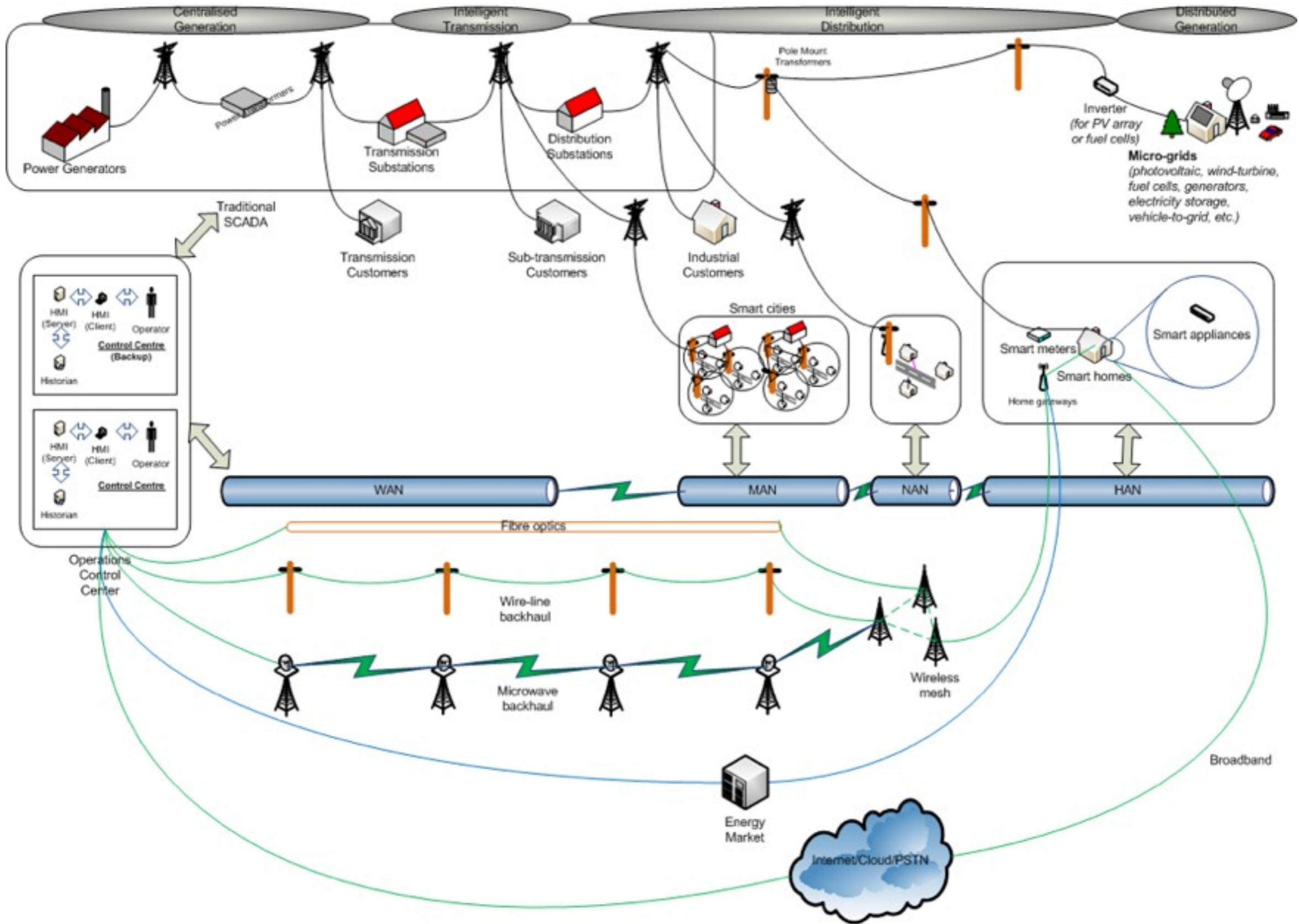
- Background
- Methodology
- Related Work
- Observations
- Conclusion

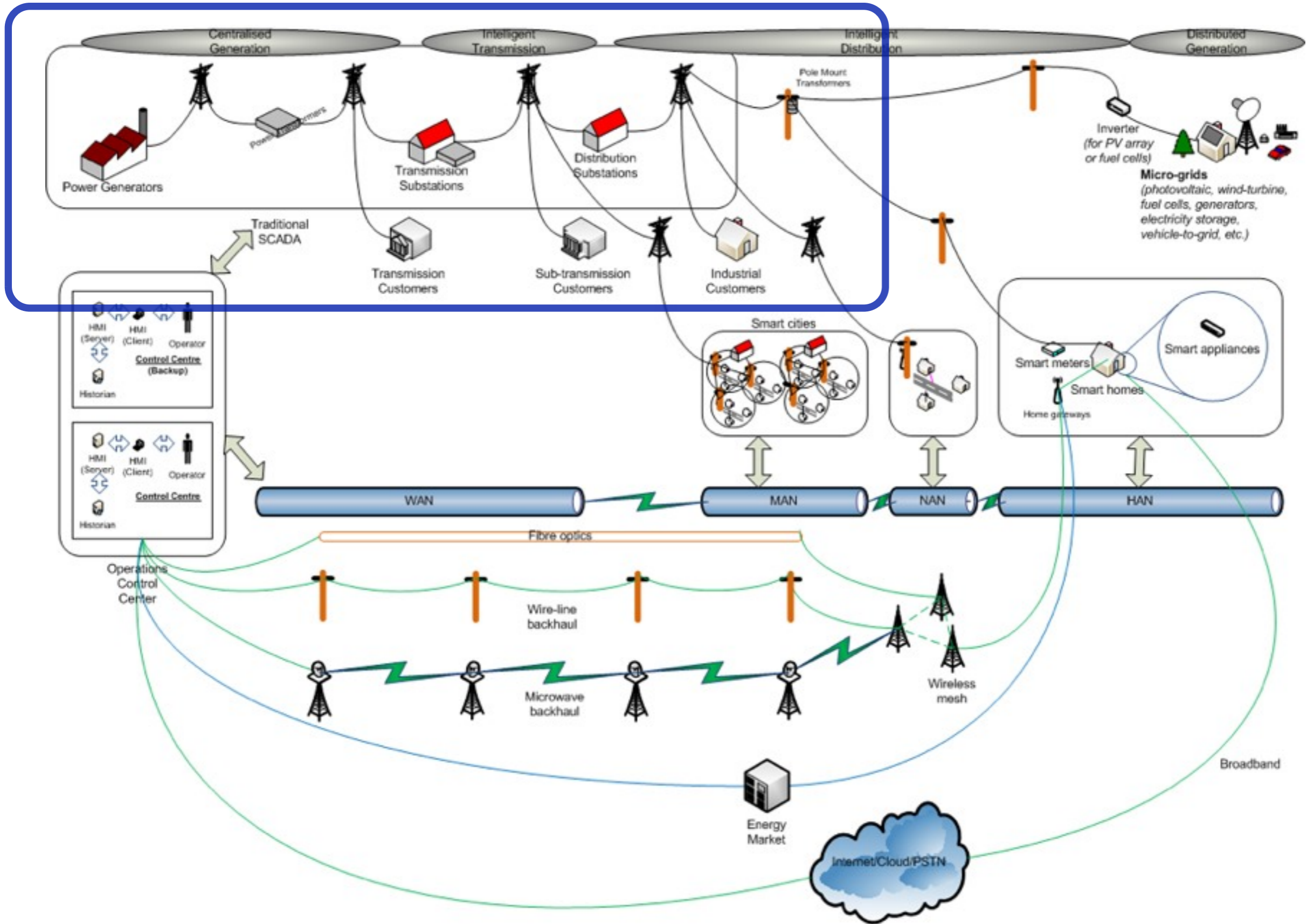
Background

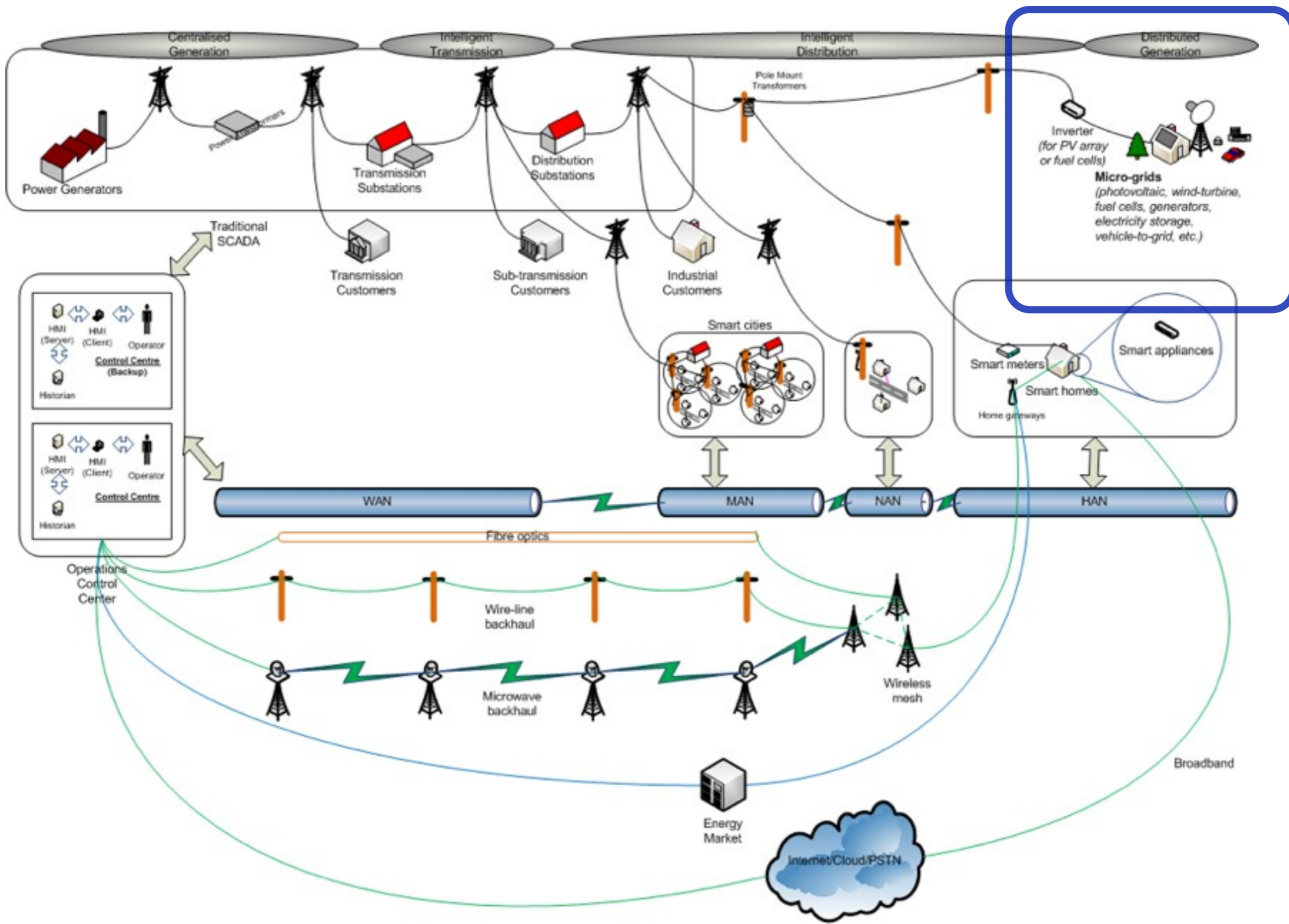
- **What is the Smart Grid?**
 - Different definitions by stakeholders
 - Integration of SCADA and ICT networks
 - Includes SCADA, AMI, PHEV, micro-grids
 - Integrated supply-side and demand-side management

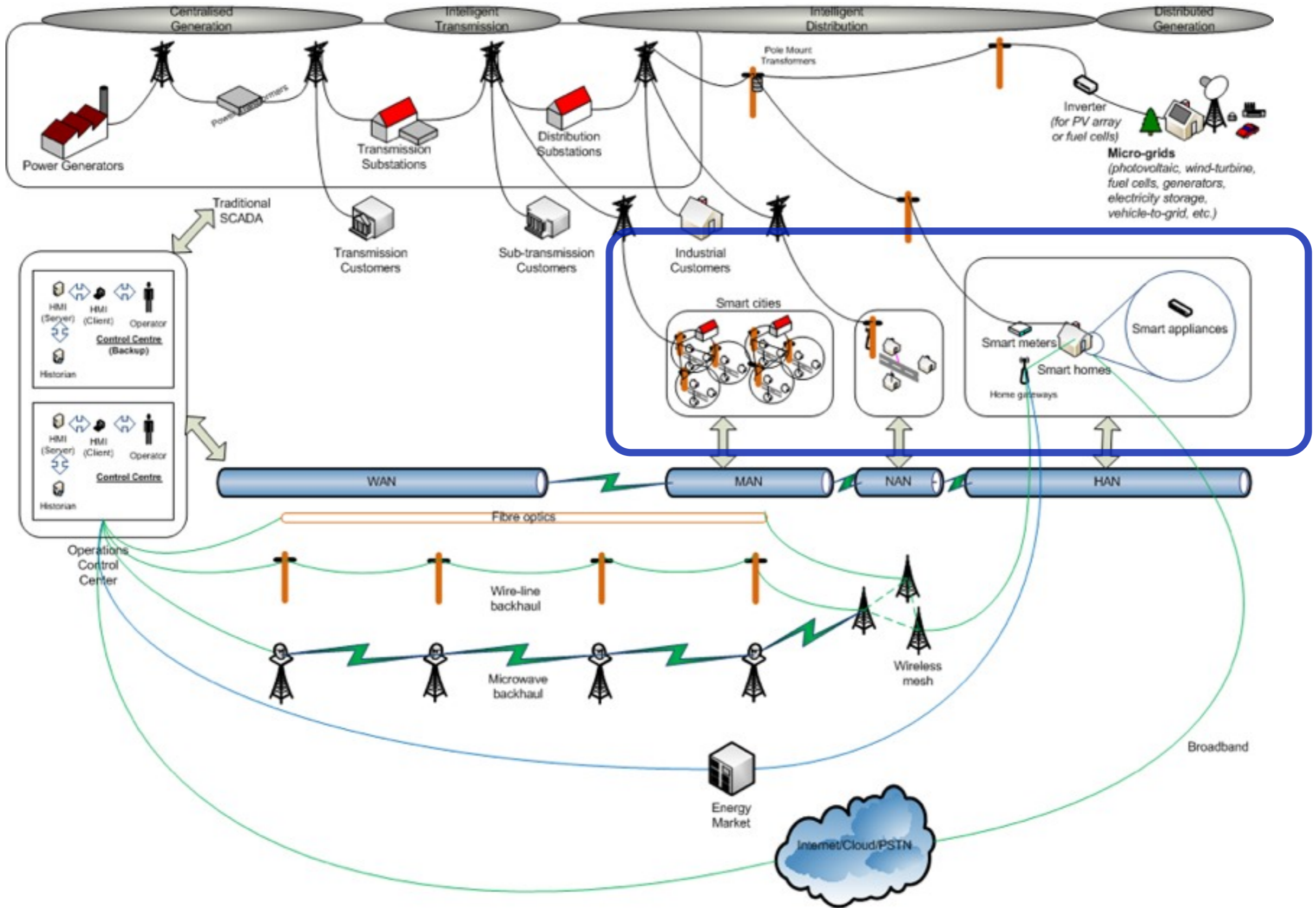
Smart Grid Benefits

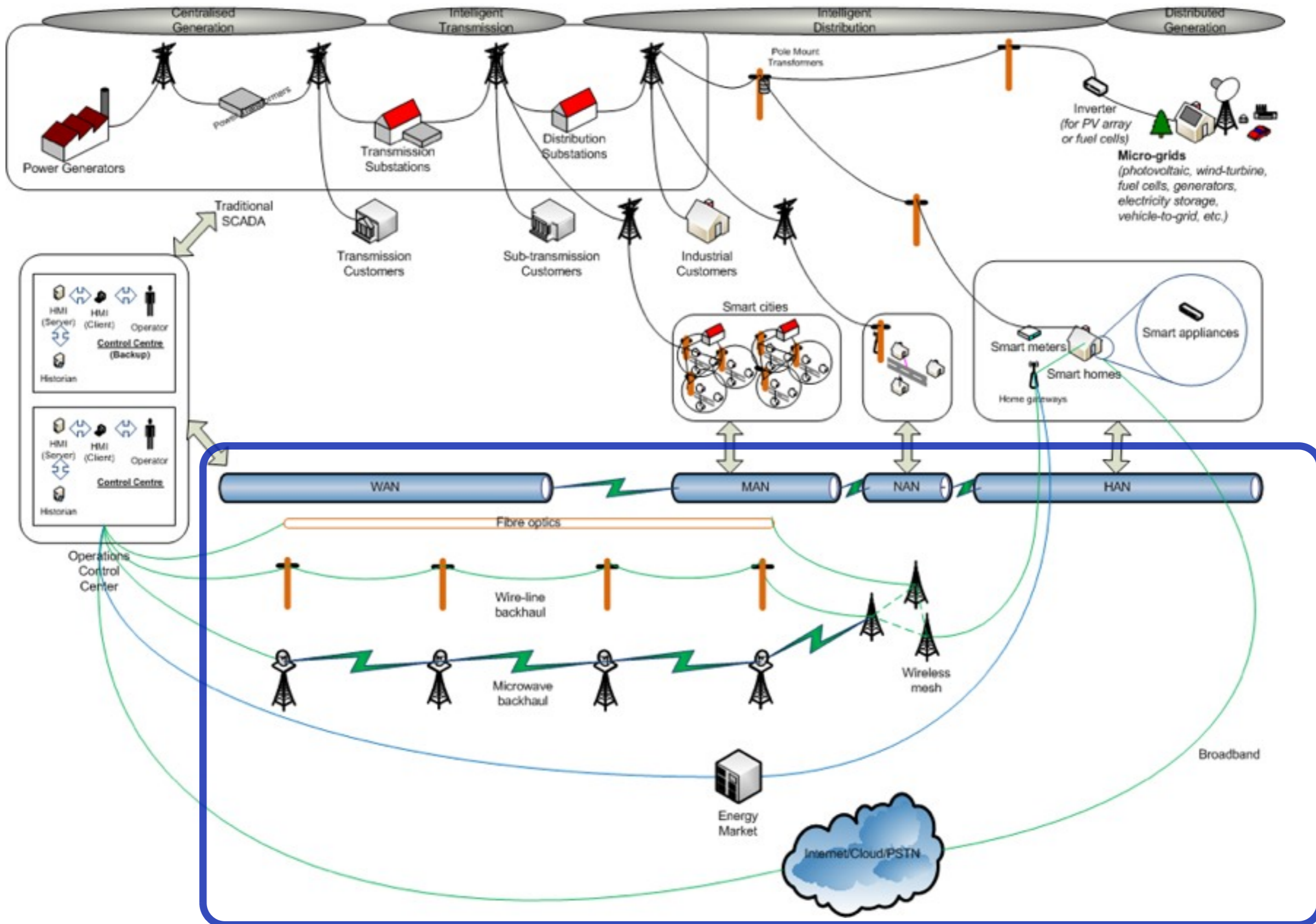
- Greater efficiency in production and consumption
- Higher resistance to disturbances
- Better recovery capabilities from disturbances
- Better control of electrical consumption in distribution networks
- Higher quality of electrical power production
- Integration of micro-grids for distributed generation
- Increase network observability
- (Aggarwal et al., 2010; Hassan & Radman, 2010; Momoh, 2009; Cohen, 2010);



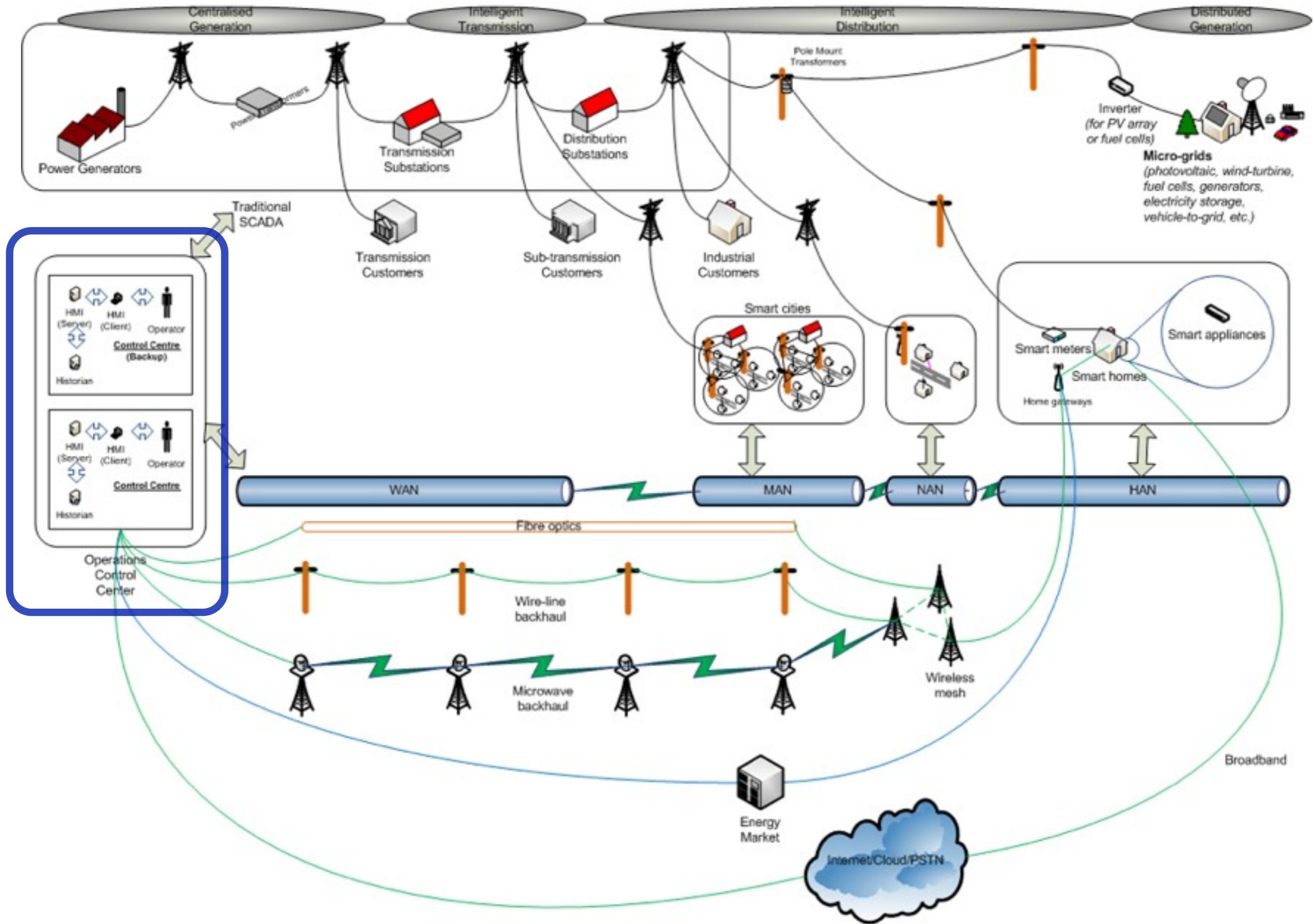








Gap Analysis of Intrusion Detection in Smart Grids



Problem Statement

- Need to protect Critical Infrastructure
- Smart grid introduces additional vulnerabilities
- Cannot rely solely on intrusion prevention
- Defence-in-depth approach

Contributions

- Identified key functional requirements
- Presented gap analysis against these requirements
- Identified limitations of contemporary IDSs

Methodology

- Essential to distinguish Smart Grid from SCADA and ICT networks
- Characterise the environment in which IDS to be deployed
- Formulate operational requirements for Smart Grid IDS
- Compare IDSs against operational requirements

Smart Grid Characteristics

- C1 – Legacy Communication Protocols
- C2 – Scale of Network*
- C3 – Resource Constraints
- C4 – Maintenance Cycle
- C5 – Emerging Standards
- C6 – Topology
- C7 – Data Traffic Patterns
- C8 – Nature of Network*
- C9 – Adaptive*

IDS Operational Requirements

- R1 – Support Legacy Protocols (C1)*
- R2 – Scalable (C2)
- R3 – Support Legacy Hardware (C3,C4)*
- R4 – Standards Compliant (C5)
- R5 – Adaptive (C6,C8,C9)
- R6 – Real-time (C8)*
- R7 – Reliable (C8)

Related Work

- Supply-side IDSs
 - Lauf et al. (2010)
 - Ad-hoc wireless networks
 - Two-stage approach

Barbosa and Pras (2010)

- Data network-flow analysis
- Assumes network is “well behaved”
- Specification-based detection

Valdes and Cheung (2009)

- Motivated by move to COTS
- Multi-layers approach for situational awareness (WholeNetViewer)
- Model-based and signature-based detection

Naess et al. (2005)

- Middle-ware based IDS
- Resource constrained environments
- Application-based security policy for detection

Demand-side IDS

- **Berthier et al. (Berthier, Sanders, & Khurana, 2010)**
 - Focuses on AMI
 - Proposed an architecture of IDS in AMI
 - Recommended specification-based detection

Observations

Req	Lauf	Barbosa	Valdes	Naess	Berthier
R1 - Legacy Protocols	N/A	Y	Y	N/A	N/A
R2 - Scalable	Y	N	Y	N	Y
R3 - Embedded	Y	N	N	Y	N
R4 - Standards	N	N	N	N	N
R5 - Adaptive	Y	N	N	N	N
R6 - Realtime	N/A	N/A	N/A	N/A	Y
R7 - Reliable	N	N	N	N	Y

Summary

- Does not meet requirements
- Used specification-based detection
- Lacked R2 - scalability, R6 - realtime and R7 - reliability
- High false-positives

Limitations

- No quantitative evaluation
- No effective evaluation of realtime suitability
- No suitable evaluation data

Conclusion

- The gap
- Need to improve accuracy
- Need for evaluation data

Research Questions

- How best to perform intrusion detection in the smart grid
- How best to design an IDS for the smart grid
- Where best to deploy the IDS in the smart grid
- What threat models to be considered in the design of the IDS
- How best to train and evaluate the IDS

Future Work

- Refinement of the requirements
- Threat modelling
- Design of intrusion detection framework
- Experimental design and evaluation using test bed

Questions

Thank you