



I N S P I R E

EC Grant Agreement n. 225553

Peer-to-Peer Systems: Edges constitute the Core

INSPIRE – 2nd Workshop
Rome, January 21, 2011

Daniel Germanus - Technische Universität Darmstadt
- DEEDS Group



TECHNISCHE
UNIVERSITÄT
DARMSTADT

- Introduction: P2P Fundamentals
- Classification of P2P protocols
- P2P protocol & extension overview
- P2P Summary
- Protection enhancements for SCADA systems: An INSPIRE perspective
- Challenges & Future Work

Introduction

- A traditional and prevalent communication scheme for networked systems: (asymmetric) **Client/Server Communication**
- Server system have usually **more resources** than clients, **resources** were located at the **core of the network**
- Resource availability in client systems improved (CPUs, storage)
- Interconnectivity improved: Internet age, adequate bandwidth for millions
- Exploit vast amount of client resources throughout the network

- Exploitation of resources at the “edge” of the network (instead of the core)
- Early and prominent example: Napster
- Napster’s concept:
 - Exchange media (originally for free)
 - Centralized directory service
 - Decentralized media file transfers
- Napster contemplation:
 - **Symmetric communication scheme**: Clients are also servers → “servents”
 - Overlay network is spanned on top of existing IP underlay network
 - Single point of failure: Directory service, which is still centralized.

- More P2P systems followed, can be categorized as follows:
 - **Fully decentralized**: early Gnutella releases
 - **Hierarchical**: Gnutella2, Skype
- **Features** of hierarchical or decentralized systems:
 - Basic service (Message routing among peers, storage/retrieval of data)
 - Fault tolerance (Path redundancy, data replication)
 - Security (Availability, Integrity, Anonymity)
 - Scalability (Protocol dependent)
- **Nowadays, many P2P protocols exist and many extensions are proposed**

- P2P protocol categories: unstructured, structured, hybrid

	Unstructured	Structured	Hybrid
Scalability	Low	High	High
Maintenance Overhead	Low	High	Hierarchically organized, calm leaves
Efficiency	Low	High	Medium
Protocol examples	Freenet, Gnutella 0.4	Chord, Kademia, Pastry, Viceroy	Gnutella 2.0, Skype, JXTA

P2P Protocols : Extensions and Summary

- Several **protocol extensions** surfaced:
 - **Efficiency**, e.g., improved lookup algorithms, peer neighbor selection, reactive overlay adaption
 - **Security**, e.g., secure admission protocols, anonymity features
- P2P technology is applicable for data dissemination and storage:
 - Suitable for **large scale and hostile environments**
 - Can be integrated as **middleware** layer into existing systems
 - Exploits and masks **heterogeneity**
 - **But:** Introduces new threats & generates network overhead
- **How fits P2P into a SCADA context?**



SCADA Protection - Requirements



I N S P I R E

EC Grant Agreement n. 225553

- **Protection enhancement**
 - Mitigate existing failures/cyber threats through monitoring and reaction
 - Quantifiable protection in demand
- **Minimal intrusiveness**
 - Reduce integration efforts
 - No dedicated HW infrastructure required
 - Node access, no source code available/accessible
 - Generic solution (as far as possible)
- **Scalability**
 - Support interconnected & large scale networks
- **Support legacy systems & heterogeneity**
 - Resource frugality to support legacy systems with limited resources
 - Interoperability, i.e., mask heterogeneity of nodes/links

- Node crash → SCADA data loss
 - Underlay network node crashes (e.g., a non-edge router)
 - SCADA communication between RTU(s) and MTU disabled
 - Crashed node possibly recovers (e.g., via reboot)
 - Underlay network possibly adapts routing tables to surround crashed node (e.g., via OSPF)
- Attacks → SCADA data corruption
 - SCADA message data integrity is compromised
 - Attack occurs between source and sink (e.g., on a router)

(Krutz et al.)

- Delay
- Jitter
- Transient loss
- Permanent loss
- Eavesdropping
- Fault injection

→ Critical Status of the SCADA/CI

- ☺ Inherent path redundancy and data replication → **Protection enhancement**
- ☺ Middleware → Mask underlying **heterogeneity**, benefits **minimal intrusiveness**
- ☺ Efficient self-organization → **Scalability**
- ☺ Modest requirements → **Reduce integration efforts**
 - TCP/IP stack
 - Small computational overhead/memory footprint
- ☹ Some new risks, e.g., Sybil attacks & content pollution
- ☹ Network overhead

Overall Objectives:

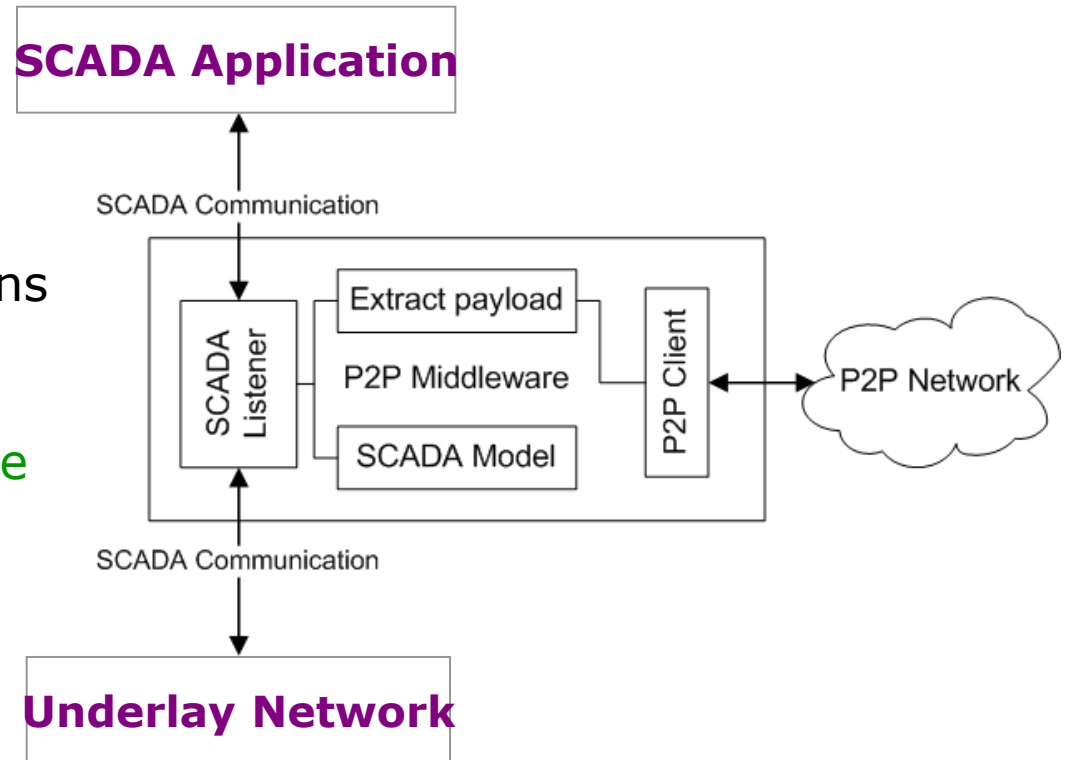
- **Recover** lost messages consequent to crashes
- **Discover** corruptions consequent to fault injections

Approach:

Monitor SCADA data → **store it in P2P overlay** → Detect perturbation → Recover SCADA data

Protection:

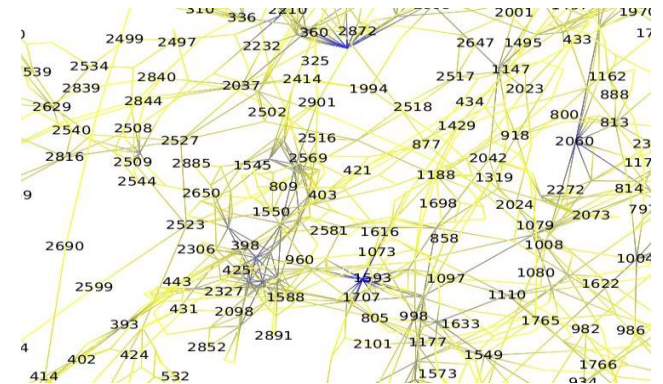
- **Rerouting and data replication** to mitigate SCADA data loss/corruption



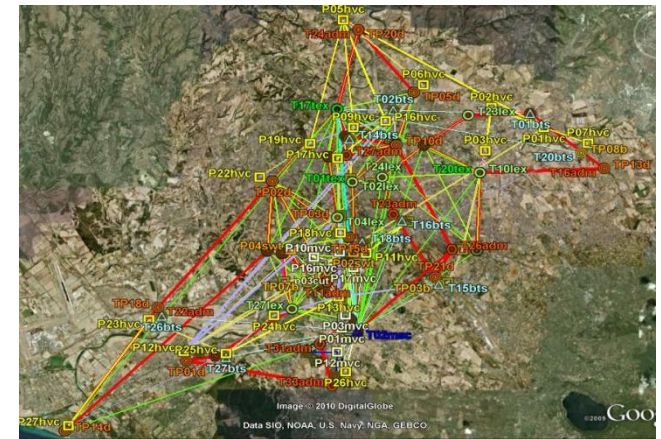
- **Node crash**
 - Request SCADA sensor data from the P2P DHT if the corresponding SCADA message does not arrive via the traditional SCADA channel (connection lost, timeout)
 - Bridge time until traditional connection works again
- **Data corruption**
 - For each received SCADA sensor message copies are requested from the P2P DHT
 - Check for equality

- **Replication degree** – how many copies are produced by the P2P overlay for data redundancy
 - Trade-off between data availability and comm/storage overhead
- **Get request count** – how many requests are sent to the P2P overlay in parallel and along different paths for each data retrieval operation
 - Trade-off between timeliness and comm. overhead
- **Similarity ratio** – how many copies retrieved from the P2P overlay need to be identical with the SCADA value to declare it as correct
 - Trade-off between attack detection accuracy and overhead

- Evaluation on realistic topologies (power grid data, telecommunication, etc.)
- Identification of relevant design parameters for P2P protocols in a SCADA application domain
- Quantifiable P2P Security: What is the security gain compared to other communication paradigms like C/S?



North American Power Grid



Telecom Italia Rome SCADA Network



I N S P I R E

EC Grant Agreement n. 225553

Thanks for your attention!

www.inspire-strep.eu

germanus@cs.tu-darmstadt.de