Scuola Superiore Sant'Anna

Challenges for enabling Cloud Computing over optical networks

Piero Castoldi, Barbara Martini, Fabio Baroncelli

Workshop "Grid vs Cloud Computing and Why This Should Concern the Optical Networking Community"
OFC/NFOEC 2009 – March 22-26, 2009 - San Diego, USA

Outline

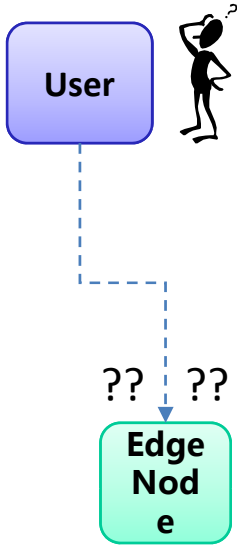
- Introduction and concepts
- Challenges
  - Resource virtualization
  - Service Abstraction
  - User-driven service delivery
  - Security
- Conclusion

The "network as a service" paradigm

- Cloud Computing is a general paradigm of operation where the capabilities of an ICT infrastructure (e.g., computation, storage, servers, connectivity) are consumed "as a service".
- Users are able to access ICT capabilities from the Internet (i.e., "the cloud") without knowledge of and control over the technology infrastructure that supports them.
- According to the "network-as-a-service" (NaaS) paradigm, the network should support user-oriented capabilities

User-oriented network capabilities

- Cloud computing will require dynamic complex service set-up and tear down with strict requirements (e.g. content streaming are with adequate bandwidth, delay and jitter and performance of streaming server)



"Client-Request" Format:
Disney, Wall-E → (Session, Server-Location)
HD Movie → (Bandwidth)
Good Quality → (QoS)

"Network-Directives" Format:

```
mpls {
    traffic-engineering bgp-igp-both-ribs;
    no-cspf;
    label-switched-path to-R2{
      to 10.20.0.1;
      install 10.20.12.0/24 active;
      bandwidth 10m;
    }
```

Triggering of network services in transport network is available via network technology-dependent interfaces (e.g. the User to Network Interface), but

→ network has a different "grain" in service description with respect to an application

→ intimate knowledge of the network technology is required

→ no mechanism is available for coordinating set-up of complex private networks

What is needed: a provisioning framework operating at a level of abstraction suitable for being invoked directly by an application

Concepts (1)

- Network resource
  - a network capability of supporting (set-up, configure, monitor, tear-down) the forwarding of data, possibly across multiple nodes, according to a certain encapsulation (e.g. a MPLS L2 LSP)
- Non-network (or IT) resource
  - a data processing capability over the payload of a data flow, realized in software or in hardware in a network node (e.g. a random access memory)
- Network service
  - a service, described in a technology-independent way that, leveraging on network resources, offers connectivity capabilities, directly or indirectly, to the customers' applications (e.g. a L2 VPN)
- Non-network service
  - a service, described in a technology-independent way, that leveraging on an IT resources offers a data manipulation capability (e.g. a storage service).

Concepts (2)

- Virtualization of resources
  - capability to hide the network resource technology details to an application
- Service abstraction
  - capability to map the set of high-level parameters specified by an application, into a set of specific parameters used by the network for the provisioning of that service.
- The process of service abstraction requires virtualization of resources:
  - Resources on a network are made available as independent services that can be accessed without knowledge of their underlying technical implementation.
  - Services are defined through an ontology language to facilitate their composition.
  - Semantic rules can be defined to compose or orchestrate services

Cloud computing and optical networks

- Cloud Computing can benefit from ultra high-capacity optical network connectivity, if optical networks are adapted to support user-oriented capabilities:
  - Service control signaling, i.e., signaling for session control among end-user applications including message exchange for session state monitoring, resource negotiation and media transfer control.
  - Resource control signaling, i.e., signaling for resource control for the purpose of a consistent end-to-end resource reservation leveraging on the Control Plane, serving for:
    - resource and admission control
    - network attachment functions (e.g., auto-discovery of border network topology)

Challenges

- Resource virtualization
  - Joint virtualization of IT and network resources
  - Network resource discovery and virtualization at the network boundary
- Service abstraction:
  - Service exposition for bridging applications and CP-enabled Optical Network
- User-driven service delivery
  - On-demand service triggering
- Security
  - AAA in multi-operator scenario and distributed environment
  - Advanced mechanisms for user access control

Network resources

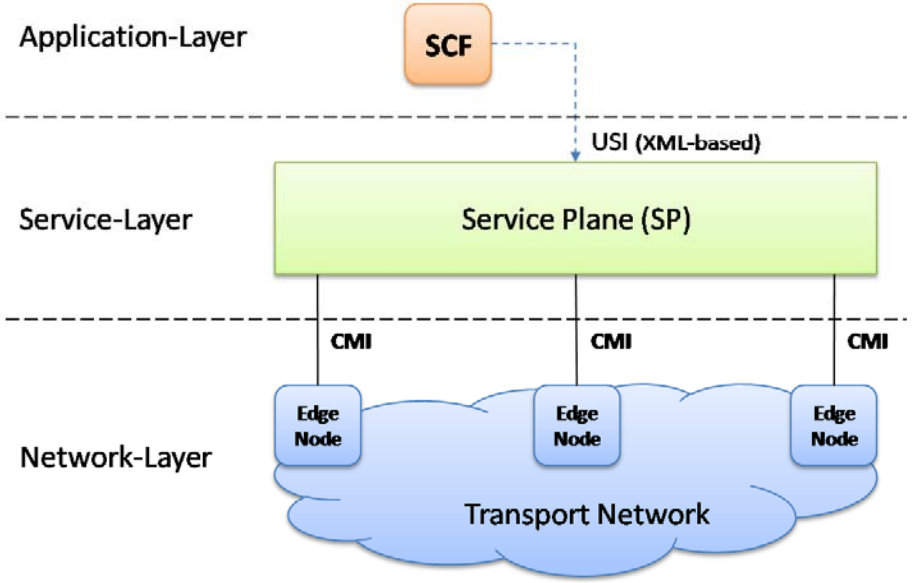
	Grid computing	Cloud computing
Service concept	Capability to transfer a specific type of data traffic generated by a customer network: – Traffic transparency – QoS support – Advanced mesh connectivity (e.g. L1/L2/L3 VPN, VPLS)	Capacity to match application request to network resource availability and accordingly affect network resource status: –Traffic enforcement on per-flow basis – QoS guarantees – End-to-end resource control
Requesting application	E-science applications TE/Management application (OSS)	Multimedia applications Virtual terminal applications
Service request	QoS-enabled connectivity set-up in WAN context	Assured data transfer among end-hosts
Service granularity	Coarse grain (GB up to TB)	Fine grain (100's MB)

Non-network (IT) resources

- IT Resources are more difficult to be described than network resources
  - IT resources are more heterogeneous and may lack of a relation of hierarchy
  - Some virtualization efforts exist but solutions are heterogeneous (e.g. naming for addressing: Universal Unique Identifier, Universal Resource Identifier, etc)
  - An adequate, typically complex, information model is needed to handle IT resource (discover, publish, etc)
  - Some applications, e.g. grid, already have a well established IT resources virtualization mechanism that do not involve provider networks at all.

Virtualization of resources and service abstraction (1)

- Control Plane-enabled optical transport networks
- Approach based on the introduction of a Service Plane:
  - Fill the informational-gap between the Application-Layer (Service Control Function) and the Network-Layer
  - Decouples network technologies from future evolution of the network services
  - Composes and orchestrates the connectivity service provided by the CP at the boundary of the Transport Network via CMI (Control-Plane Management Interface)
  - Defines a technology-independent network service definition at a level of abstraction suitable for being invoked by an application via USI (User-to-

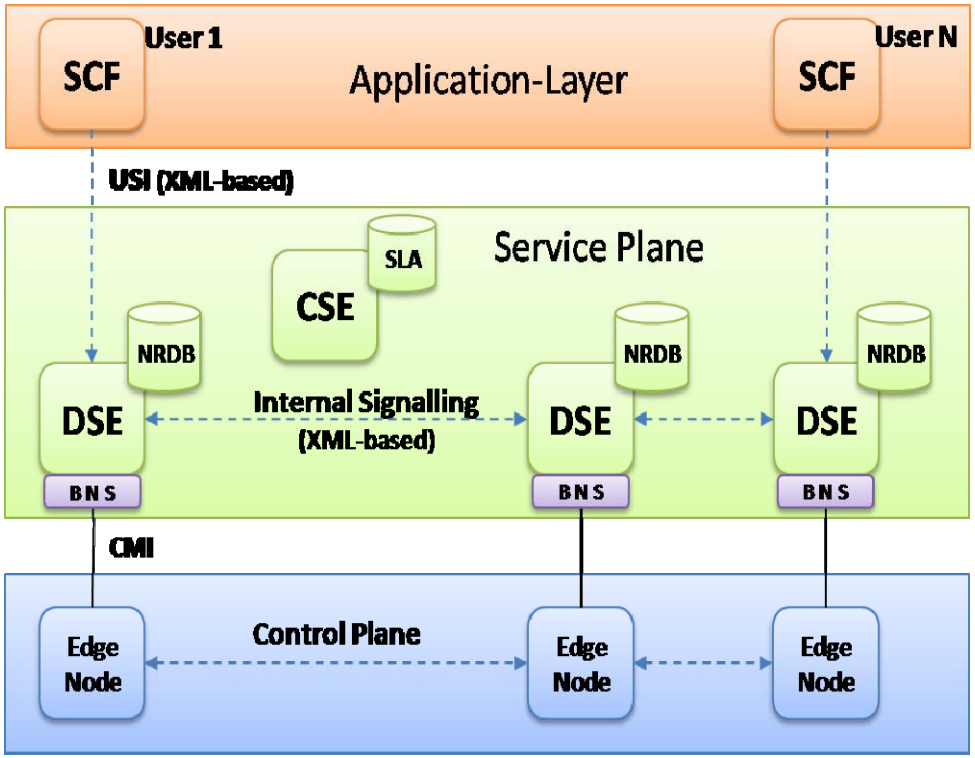


F. Baroncelli, B. Martini, V. Martini, P. Castoldi, "A distributed signaling for the provisioning of on-demand VPN services in transport networks" Proc. of IM 2007, May 2007, Munich, Germany.

B. Martini, V. Martini, F. Baroncelli, K. Torkman, P. Castoldi, "Application-driven Resource Management in Multi-Service Optical Networks", Journal of Optical Communications and Networking, June 2009, to appear

Virtualization of resources and service abstraction (2)

- Fully distributed and technology-independent approach based on a Service Plane that supports on-the-fly invocation of services
- Populated by a set of distributed entities that inter-communicate via dedicate signalling using XML messages



Two main procedures are envisioned:

- The Background Signalling
- The Service Provisioning Signalling

The Service Control Function (SCF)

- Acts as a gateway
- Request Network services

The Centralized Service Element (CSE)

- Verifies the SCF identity (Client Authentication)
- Controls the access (Service Authorization);

The Distributed Service Element (DSE)

- Handles multiple service requests
- Composes the Network-Services
- Performs technology-specific configurations on controlled PEs using the BNS module

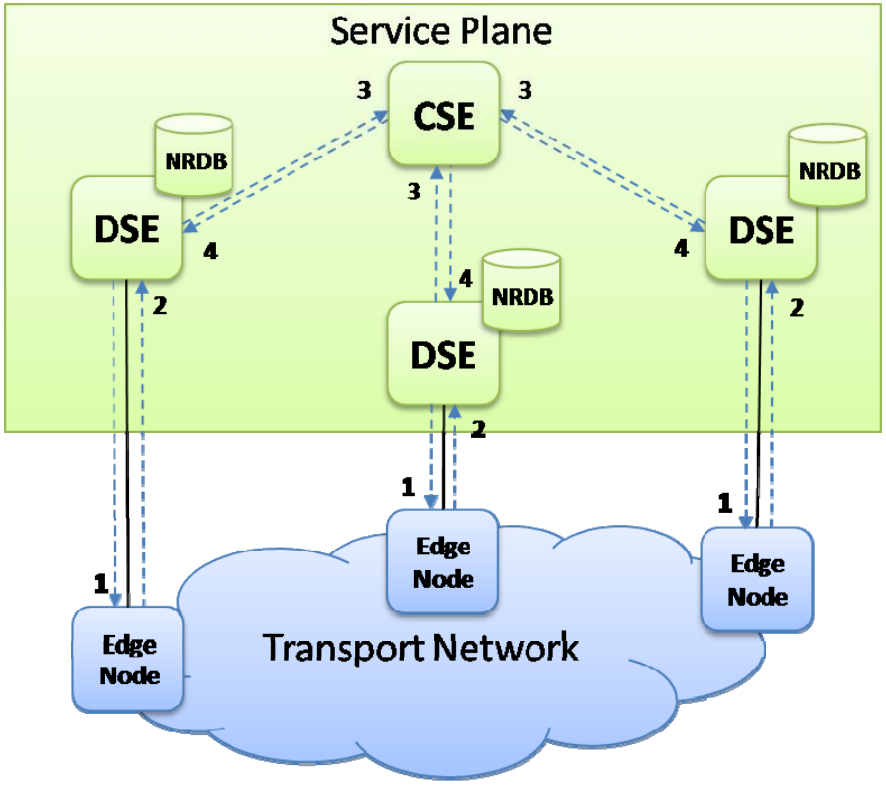
The Broker Network Server (BNS)

- Performs configuration of devices via Control Plane Management Interface (CMI)

Network topology virtualization

Background Signalling:

- Collects and abstracts Network status
- Update the NR-DB within the DSEs
- Is Continuously repeated in background at regular intervals



1 - Network Resource Discovery phase (arrow 1, 2): DSEs gathers at regular intervals the information

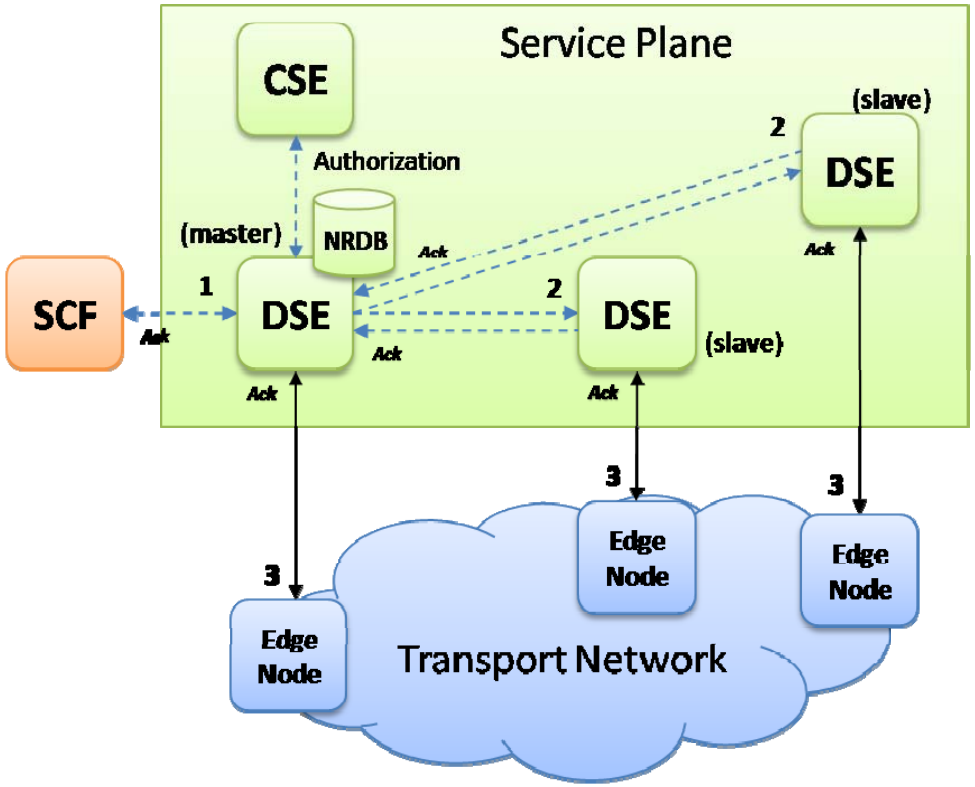
2 - Service Abstraction phase: DSEs map technology-dependent into technology-independent information and stores it in the NR-DB

3 - Information Distribution phase (arrow 3, 4): DSEs distribute information to CSE module
(CSE acts as a Database Reflector of the overall knowledge of Network)

On-demand service triggering

The Service Provisioning Signalling

- is responsible of the actual service provisioning
- is triggered by a service request issued by a SCF to a DSE



1 - The DSE-master receives a Network-Service request from an SCF

[Authorization] A messages exchange occurs between DSE and CSE

2 - The DSE elaborates and distributes directives to the relevant DSEs

[*] DSEs-slave execute service commands coming from a DSE-master.

3 - Each DSE map directive in a set of CMI Network primitives to its controlled PEs (3).

[Ack] Collects and elaborates the response from the PE

[Ack] DSEs-slave send a reply-message to report the established service

[Ack] to SCF

Security

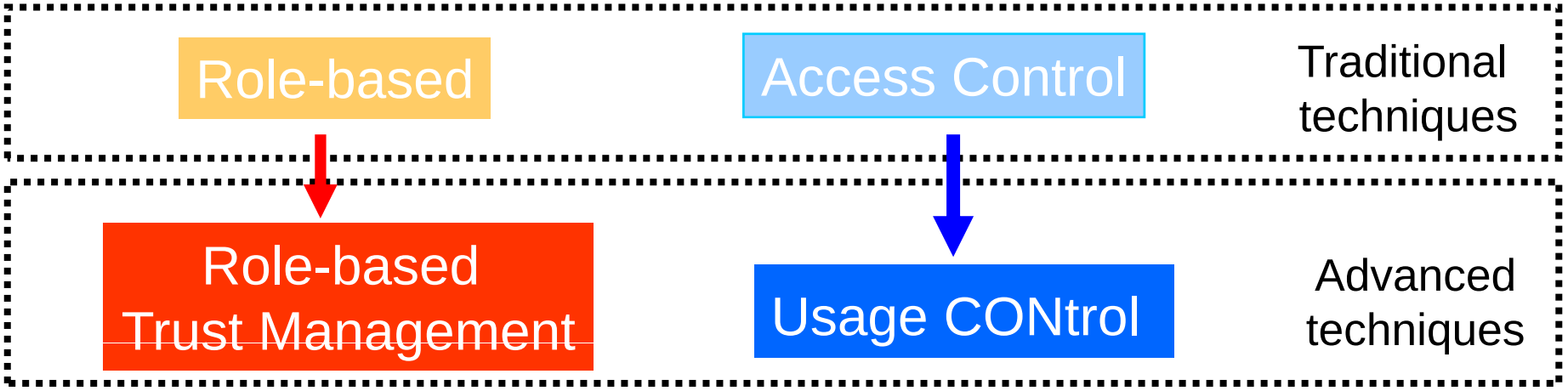
- security at application layer
  - protection against unauthorized access to application platforms (e.g., server, data base or web portal) for corruption of information, interruption of service
- security at service (control) layer
  - protection against unauthorized access to service control element (e.g., SIP proxy, HSS), to subscriber information (e.g., user and service profiles for identity theft), network provider information (e.g., repository with routing, numbering and addressing information)
- security at (transport) network layer
  - protection against unauthorized access to network elements (e.g., IP routers, MPLS nodes), to transport control information (e.g., OSPF, eBGP), to transport user profile information (e.g., DSL subscription data repository, user location information)

Authorization

- Authorization mechanisms are categorized as:
  - Authentication-based mechanisms which assign a set of rights based on the (authenticated) user identity
  - Credentials-based (a.k.a. role-based) mechanisms, which assign a set of rights based on trustworthy information (i.e., credentials) being held by the user
- Role-based Authorization process is composed of two phases:
  - Based on user credentials, the resource provider deduce the level of trust it can place in him and consequently assign a (set of) role(s)
  - Based on the role, the authorization engine identifies and enforces a policy
    - determine the set of actions the user is allowed to perform
    - verify if the user is allowed to perform the required action on the resource

Traditional vs. advanced access control

- In traditional access control
  - The decision process is based on the identity or the role of users that are registered with the Administrative Domain
  - The policy rules are static, i.e., changed only through administrative actions, typically performed by human operator
- In a multi-domain scenario
  - the user may be unknown in the Administrative Domain of the resource provider
  - resource access rights may be revoked or may expire



Trust management

- Trust definition:
  - “Trust of a party A in a party B for a service X is the measurable belief of A in B behaving dependably for a specified period within a specified context in relation to X... ” [Dimitrakos, 2001]
- Trust Management definition:
  - “Technique to make decisions about the dependability of transactions involving risk in a situation of uncertainty”
- Role-Based Trust Management:
  - A subject has (a set of) roles in each Administrative Domain to which he belongs
  - A set of access rules define the relations among Administrative Domains and are used to combine credentials and obtain new roles for the same subject in Administrative Domain to which he does not belong.

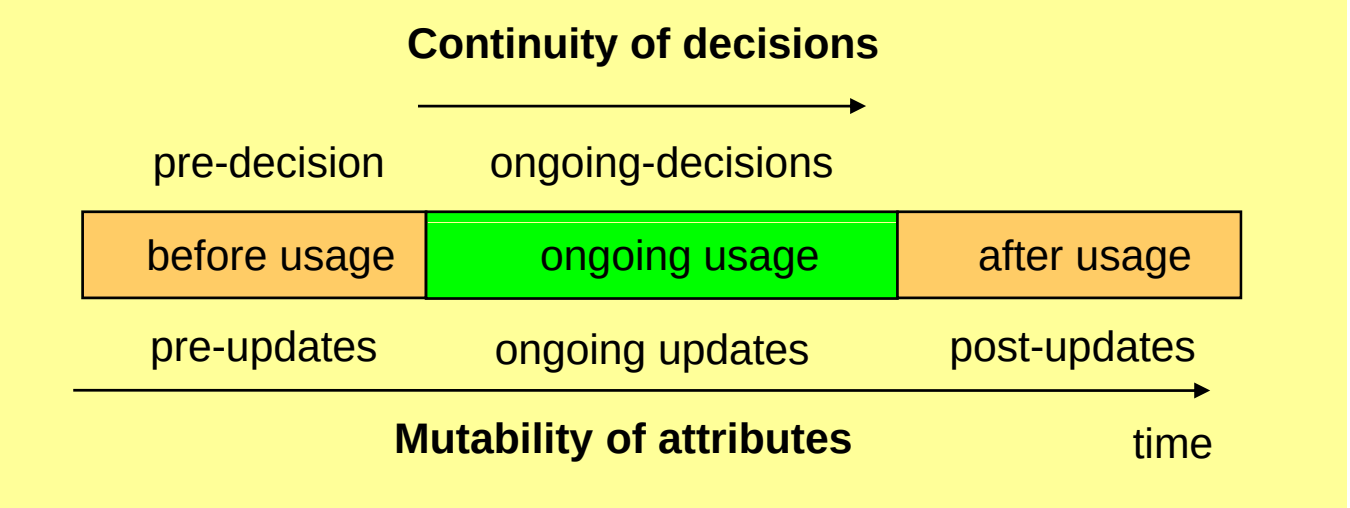
[Blaze96] M. Blaze, J. Feigenbaum, J. Lacy. Decentralized Trust Management. In 17th Symposium on Security and Privacy (pp. 164-173). IEEE Computer Society. 2006

Usage Control Model

- Subjects: entities that perform actions on Objects
  - Characterized by attributes:
    - Identity; Role; Reputation; Credits; …
- Objects: entities that are used by Subjects.
  - Characterized by attributes:
    - Value; Role permission; …

- The decision process is based on:
  - Authorizations
  - Obligations
  - Conditions

after checking subject/object attributes



J. Park, R. Sandhu. "The UCON Usage Control Model", *ACM Trans. On Information and System Security*, 7(1), 2004.

Conclusion

- Re-use of many concepts coming from grid for enabling cloud computing
- Production networks not designed to support cloud computing
- Optical networks can be good candidate because they are CP-enabled
- From security to trustworthiness

Thank you

E-mail: castoldi@sssup.it

ola Superiore Sant' Anna, CNR research area, Via Moruzzi 1, 56124 Pisa, Italy