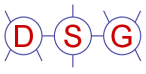
SP2A: a Service-oriented Framework for P2P-based Grids

M.Amoretti, F. Zanichelli, G. Conte


UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione

Distributed Systems Group 

Outline

- Service-oriented Peer-to-Peer Architecture (SP2A)
- SP2A: structure and adopted technologies
- **`STATE`** component
- **`GROUP`** and **`SECURITY`** components
- **`RPS`** component
- Conclusions
- Future work

MGC-05 November 28th, Grenoble, France

Service-oriented Peer-to-Peer Architecture SP2A

SP2A is a framework enabling *Service Host Environments* to form dynamic Grids.

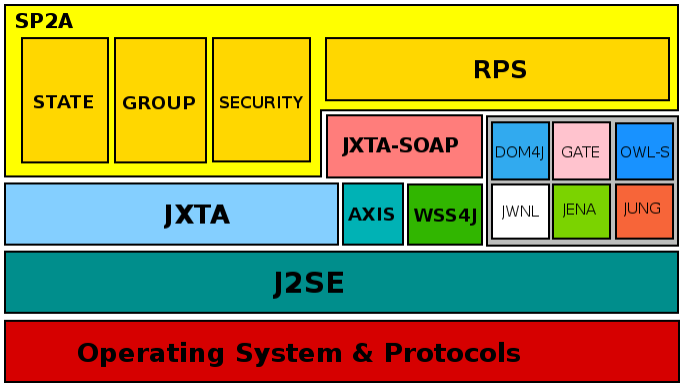
Implemented as a lightweight API for the development of *service-oriented peers* featuring:

- ability to *share* and *consume* Web Services in a P2P overlay network
- responsibilty of routing messages in the P2P overlay network
- semantically enriched service descriptions, semantic discovery of services
- peergroup security, transport security (TLS), message security (WSS)

Temporary project homepage: http://dsg.ce.unipr.it/research/SP2A

UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione
Distributed Systems Group D S G

SP2A: structure and adopted technologies



`STATE` component

Main module: StateManager

- connect to supernode (if leaf peer)
- change state (leaf → supernode, supernode → leaf)
- activate dynamic leaf/supernode switching
- show connected supernode (if leaf peer)
- show connected leaf peers (if supernode)


UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione
Distributed Systems Group D S G

`GROUP` and `SECURITY` components

Main modules: GroupManager and SecurityManager

- create group (with security policy)
- share group
- find group
- join group
- leave group

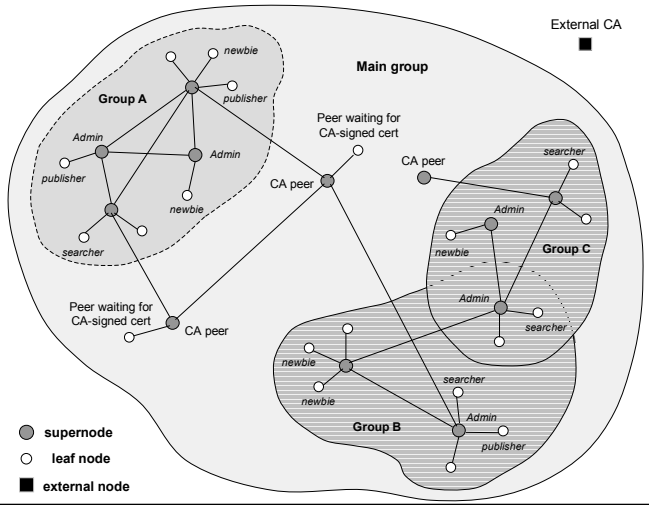
Enforcing security policies

Secure transport
Ex. secure pipe

Certification Authority
Ex. CA peer

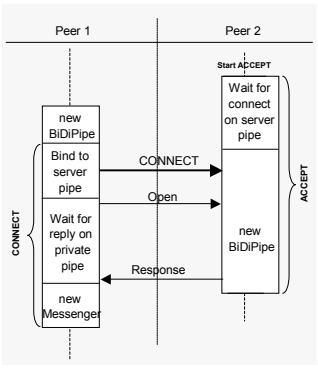
Admission Control
Ex. certificate-based

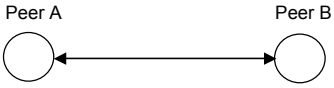
Authorizations
Ex. role-based, with
local and remote control



Secure communication

JxtaBiDiPipe
- Built on basic JXTA Input/OutputPipe
- Reliable bidirectional communication, based on TLS protocol (Transport Layer Security)
  → Cryptographic techniques are used





Handshake process

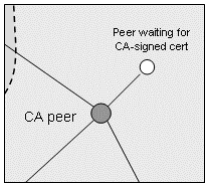
1. Negotiation of security parameters
2. Creation of a *private* secure pipe

Certification Authority peer

JXTA provides *self-signed* certificates → Not suitable for all policies

Solution:

Certificates signed by a trusted entity, such as a peer CA



Peer CA

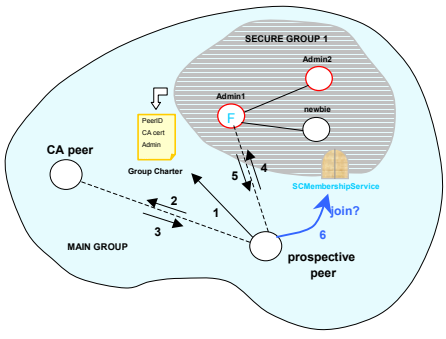
- *multi-threaded* peer, managing multiple connections
  1. Modularity
  2. Efficiency
- mutual authentication between parties and synchronization on a secure pipe
- wait for Certificate Signing Request (CSR) and send signed certificate

UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione
Distributed Systems Group D S G

Admission Control

JXTA provides 3 implementations
- NoneMembershipService
- PasswdMembershipService
- PSEMembershipService

→ unsecure, not flexible



A new service has been realized:
SCMembershipService

1. read the Group Charter
2. interact with CA: send CSR
3. acquire signed certificate
4. find admin peer and request access
5. acquire secure credential
6. join the SCMembershipService

MGC-05 November 28th, Grenoble, France

SC = Secure Credential

Once admitted, the peer receives a credential with the lowest rank.

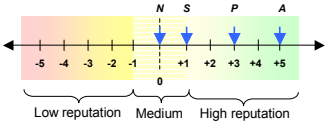
PeerGroupID
PeerID
Admin access Cert
Peer Rank
Permission Table
Reputation

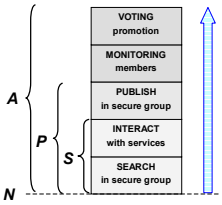
SecureCredential

PeerRank:
current role of the member peer
(*Newbie*, *Searcher*, *Publisher*, *Admin*)

Permission table:
allowed operations (role-based)

Reputation:
current reputation value





Secure group creation

Delegated to an *owner* peer (→admin)

- Service list definition
- Group Charter creation
- Secure group creation

PeerGroup Services
EndpointService
ResolverService
NoneMembershipService
AlwaysAccessService
DiscoveryService
RendezVousService
PeerInfoService

JXTA default services

PeerGroup Services
EndpointService
ResolverService
SCMembershipService
AlwaysAccessService
DiscoveryService
RendezVousService
PeerInfoService

Secure group services

Group Charter:

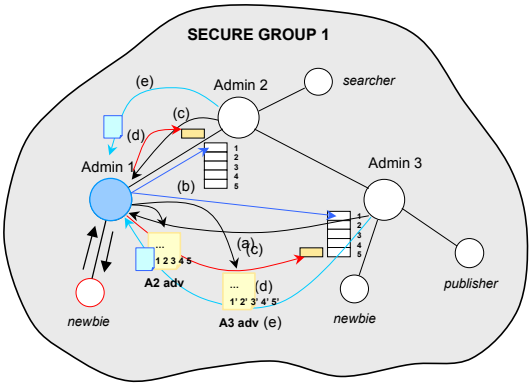
it specifies the policy
adopted by the group

- Group identification
- Trusted CAs
- Admin name

Published in the main group

Distributed voting

Promotion request → admins' voting threads



(a) Search for admins, acquire the PreVoting pipe ID

(b) Connect to discovered admins

(c) PreVoting Response with the private secure pipe ID

(d) Voting Request on the private secure pipe

(e) Voting Response

→ Final decision: majority-based

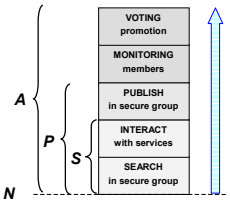
UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione
Distributed Systems Group D S G

Authorization control

The operations which are not allowed by the current role must be *prevented*

Local control
easy to implement, but not very secure
→ *SCDiscoveryService*

Distributed control
difficult to implement, but secure
→ *SCResolverService*

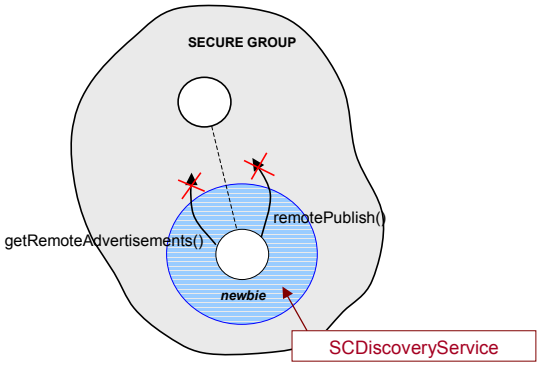


MGC-05 November 28th, Grenoble, France

Authorization control

SCDiscoveryService

Permission table control is perfomed by the sender itself, *before* executing the search/publish operations



Problem:

Service hacking…

Solution:

Remote control

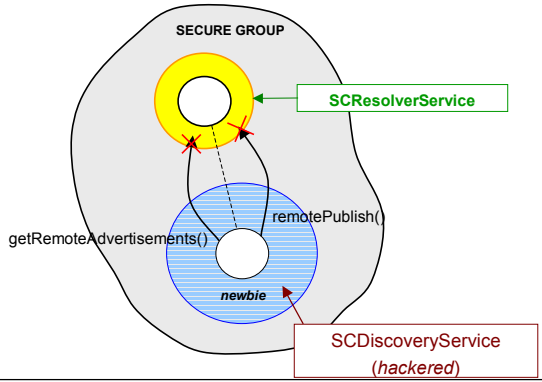
→ *SCResolverService*

UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione
Distributed Systems Group D S G

Authorization control

SCResolverService

Permission table control is performed by routing peers, which read the sender's credential (sent with the message)



Secure Routing

- Each message is coupled with the *secure credential* of the peer
- Propagating peers check the secure credential

MGC-05 November 28th, Grenoble, France

RPS component

Main modules: RPSManager and ResourceProvisionService

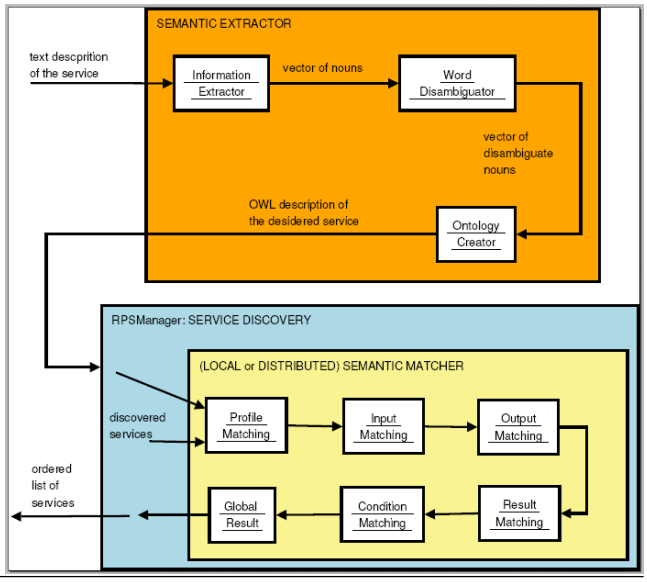
- create RPS
- share RPS
- find RPS by (attribute,value) syntactic query
- find RPS by ontology-based semantic query
- invoke RPS methods

UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione
Distributed Systems Group D S G

Semantic discovery of RPSs

Semantic query construction

Semantic Discovery and Local or Distributed Matching (SDLM or SDDM)



Semantic Extractor

The SE module generates an ontology from a textual description of the desired RPS. The SE module includes:

- *Information Extractor* : based on **GATE**, extracts nouns, adverbs, conjunctions, verbs, etc. (syntactical and structural information)
- *Word Disambiguator* : implements the algorithm proposed by Navigli and Velardi (2004), which creates a semantic graph for each ambiguous word, and tries to connect it to non-ambiguous word graphs (using **WordNet** as the reference dictionary).
- *Ontology Creator* : builds an ontology from the semantic graphs created by the Word Disambiguator, considering hypernimy relations ("is a kind of"), searching for common superclasses.

UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione
Distributed Systems Group D S G

Semantic Matcher

Coarse-grain discovery: syntactic search for classes of the SE-generated ontology.

Fine-grain matching: the SM module (of the query originator, or of each involved supernode) compares discovered services with an OWL-S service profile generated upon user inputs, and returns a list ordered by similarity degree.

SDLM: semantic matching is local to the query originator [implemented]

SDDM: semantic matching is distributed in the supernode network [to do]

JXTA-SOAP

soap.jxta.org

JXTA-SOAP is a package which allows SOAP communication over JXTA Peer-to-Peer networks. The design goals of this project are very attractive:

1) Wrapping Web Services in JXTA services.
2) Using JXTA for Web Service discovery and message transport.
3) Supporting WSS and WSRF.

JXTA-SOAP is an official Sun MicroSystems project, managed by Michele Amoretti (ardarico@jxta.org) of Distributed Systems Group.

Conclusions

- SP2A: a framework for service-oriented peer-to-peer Grids
- Four components for peer state, peer groups, security, and service management.

Future work

- More security policies!
- *Reputation management..*
- SDDM implementation (requires new JXTA services)
- Automatic RPS aggregation and orchestration

Thank you!