Optimised Test and Security Solution for P2P-based M2M Applications

22. ITG Fachtagung Mobilkommunikation

Besfort Shala
shala@e-technik.org

Frankfurt University of Applied Sciences, Germany
Research Group for Telecommunication Networks

Kleiststraße 3, D-60318 Frankfurt a.M.
E-Mail: shala@e-technik.org
Outline

1. M2M Application Provision

2. Motivation

3. Testing
   - Challenges and problems
   - Test Framework

4. Security
   - Risks
   - Trust concept
   - Integration of trust

5. Conclusion
1 M2M Application Provision

• Various application fields in M2M
  o Energy management
  o Building surveillance
  o Smart Home
  o Traffic management

• Centralised and decentralised approaches for application and service provisioning

<table>
<thead>
<tr>
<th>Features</th>
<th>Centralised</th>
<th>Decentralised</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexibility</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Efficiency</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>No single point of failure</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>End-User Integration</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>
M2M Application Provision – Decentralised

P2P-based M2M Community

Application A

Service 1
Peer 1

Service 2
Peer 2

... ...

Application B

...
- Services are realised by one or more peers
- Application is a combination of one or more underlying services
- Peers are networked using P2P mechanism
- No centralised authority
- Participating peers form a social network of peers – M2M community

![Diagram of M2M Application Provision – Decentralised]
2 Motivation

Relevance for optimising test and security solutions:

- Volatility of peers
- Cooperativeness and collaboration of peers
- Correct functionality of services
- Trustworthy peers
3 Testing – Challenges

Special challenges for testing P2P-based M2M applications

- Decentralised architecture
- Distribution of service and application descriptions
- Observability and controllability
- Service quality
Testing – Different scenarios

Scenarios

- Test a service after it enters the M2M community
- Test a service after the composition of an application
- Test a composed application

![Diagram]

M2M Community

Service 1 → Service 2 → Service 3

Service 4 → Service 5 → Service n

M2M Application

Entering the Community

Service m
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collaboration</td>
<td>Between Application Creator, Peers and Test Environment</td>
</tr>
<tr>
<td>Deployment</td>
<td>Ability to deal with a high number of peers and volatility</td>
</tr>
<tr>
<td>Test Automation</td>
<td>Test process needs to be automated</td>
</tr>
<tr>
<td>Test Derivation</td>
<td>From gathered information test suites need to be derived</td>
</tr>
<tr>
<td>Verification</td>
<td>Test process should deliver results about the functionality of the SUT</td>
</tr>
<tr>
<td>P2P and M2M capability</td>
<td>Support for P2P and M2M technologies</td>
</tr>
<tr>
<td>Trust Management System support</td>
<td>Shall be integrated within the test architecture</td>
</tr>
</tbody>
</table>
Testing – Existing Test Architectures

• Global tester

![Diagram showing Global tester architecture]

• Disadvantages:
  1. No usability for large-scale systems
  2. Single point of failure
  3. No P2P capability
Testing – Existing Test Architectures

- Distributed testers

![Diagram of System under Test with testers A and B connected]

- Disadvantages:
  1. No effective test derivation mechanism
  2. High effort for synchronisation events for coordination between the testers
Testing - Test Architecture for P2P-based M2M Applications

Diagram:
- Test Master
- Test Agent A
  - Application
- Test Agent 1
  - Service 1
  - Peer 1
- Test Agent 2
  - Service 2
  - Peer 2
- Test Agent 3
  - Service 3
  - Peer 3
4 Security - Model for security considerations

M2M Community

M2M Application

M2M Communication Protocol

Service 1   Service 2   Service N

P2P Overlay

IP Network

Peer 1   Peer 2   Peer N
Security – Risks

- Attacks on the Community and the Overlay
- Attacks on the Services and the Applications
Security – Concept of trust (I)

• Trust as a tool for preventing attacks

• According to the ITU-T CG-Trust working group:
  
  o „Trust is an accumulated value from the history and the expecting value for the future.“

  o „Trust is quantitatively/ qualitatively calculated and measured which is used to evaluate values of physical components, value chains among multiple stakeholder and human behaviours including decision making.“

  o „Trust is broader concept that can cover security and privacy“
Security – Concept of trust (II)

- Trust - data collection
- Trust - data analysis
- Trust - decision

### Required elements

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust metric</td>
<td>Measure to evaluate trust level</td>
</tr>
<tr>
<td>Trust model</td>
<td>Method to build trust relationships among peers</td>
</tr>
<tr>
<td>Trust level</td>
<td>Level of confidence between peers</td>
</tr>
<tr>
<td>Trust profile</td>
<td>Profile for storing and updating trust related information</td>
</tr>
</tbody>
</table>
Security – Trust in P2P-based M2M applications

- Trust in P2P-based M2M Applications can be applied to:
  1. Peers
  2. Services
  3. Applications

- Two cases for trust evaluation:
  1. Trust for new provided services
  2. Trust for existing services

- Integration of a trust management system inside the testing framework
Security – Example with an entering service

No Profile
SMF
Peer 1

Service 1

Test Agent 1

New entering service
Update of trust profile after trust computing

Trust computing

Service 2

Trust Profile 2
SMF
Peer 2

Test Agent 2

Service 3

Trust Profile 3
SMF
Peer 3

Test Agent 3
Security – Example with existing services
5 Conclusion

- Test Framework
- Security Evaluation
- Trust concept
- Integration of a Trust Management System
Optimised Test and Security Solution for P2P-based M2M Applications

22. ITG Fachtagung Mobilkommunikation

Besfort Shala
shala@e-technik.org

Frankfurt University of Applied Sciences, Germany
Research Group for Telecommunication Networks

Kleiststraße 3, D-60318 Frankfurt a.M.
E-Mail: shala@e-technik.org