IoT-Middleware-Gap analysis, 13-16 Dec, 2010

Title: IoT-Middleware-Gap analysis

Company: Tata Consultancy Services Ltd

Purpose: Information

Doc number: 

Meeting: GISFI#3, Pune, India, 13 – 16 Dec, 2010
Requirement of middleware in IoT

 Difficult to define and enforce a common standard among all the diverse devices belonging to diverse domain.

 Middleware acts as a bond joining the heterogeneous components together.

 Applications of diverse domains demand abstraction/adaptation layer

 Middleware provides API (application programming interfacing) for physical layer communications, and required services to the applications, hiding all the details of diversity.
## Existing IoT middleware and their features

<table>
<thead>
<tr>
<th>Name of the middleware</th>
<th>Description</th>
<th>Features</th>
<th>Associated Standard Body</th>
</tr>
</thead>
</table>
| Hydra Middle-ware[1]   | Allows developers to incorporate heterogeneous physical devices into their applications by offering easy-to-use web service interfaces for controlling any type of physical device irrespective of its network technology | • Based on OSGi.  
• Supports various service managements, including context security & Ontology  
• Event management,  
• Easy to use web service interface.  
• Dynamic reconfiguration and self-configuration. | ETSI and European Commission (7th Framework Program) |
| ISMB middleware[2]     | Working with 1:1, 1:many, many : many communication, hierarchical node, device discovery, Internet wide publish/subscribe. | • Mainly for RFID.  
• Multi-sensorial wearable device (wrist watch) for indoor monitoring and context awareness |  |
| ASPIRE [3]             | • Aims at developing and promoting an open-source, lightweight, standards-compliant, scalable, privacy-friendly, and integrated middleware along with several tools for RFID. | • Provides set of tools to deploy RFID solutions without a need for tedious low-level programming. | ETSI and European Commission (7th Framework Program) |
| UbiRoad- Semantic Middleware for Environments [4] | • Operates on top of numerous sensor and access networks. Addresses interoperability between the in-car and roadside devices for seamless and flexible collaboration amongst the smart road devices and services. | • Utilizes semantic languages and semantic technologies for declarative specification of devices' and services' behaviour.  
• Establishes common ontology |  |
## Existing IoT middleware and their features contd.

<table>
<thead>
<tr>
<th>Name of the middleware</th>
<th>Description</th>
<th>Features</th>
<th>Associated Standard Body</th>
</tr>
</thead>
</table>
| SAI Middleware [5]          | A Scalable Grid and Service-Oriented middleware for distributed heterogeneous data and system integration in Context-Awareness oriented Domains.                                                        | • Based on distributed grid architecture  
• Uses message bus infrastructure based on Java based message queuing (JMS), active MQ,  
• Follows service oriented architecture (SOA).                                                                                       |                                                                                |
| UBISOAP middleware [6]      | A Service Oriented Middleware for Ubiquitous Networking                                                                                                                                                     | • SOAP based, a two-layer architecture  
• Network-agnostic connectivity & addressing, QoS aware network link selection.                                                            | ETSI and European Commission (6th Framework Program)                                                                                      |
| UBIWARE [7],[8]             | Facilitates communication between heterogeneous objects using agent core, Reusable atomic Behaviours and set of rules.                                                                                     | • Has an autonomous software agent to monitor the state of the resource, discover, request and utilize external help if needed  
• Has an important central component - agent core.                                                                                 |                                                                                |
| SOCRADES[9]                 | Enables enterprise-level applications to interact with and consume data from a wide range of networked devices using a high-level, abstract interface that features web services standards. | • Has a Query Engine and module for selecting the best possible device  
• OnDemandDiscoveryAndDeployment:                                                                                                         |                                                                                |
## Existing IoT middleware and their features Contd.

<table>
<thead>
<tr>
<th>Name of the middleware</th>
<th>Description</th>
<th>Features</th>
<th>Associated Standard Body</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Sensor Networks (GSN) middleware[10]</td>
<td>Central concept is the virtual sensor abstraction which enables the user to declaratively specify XML-based deployment                                                                                                                                                                                                   • Has a virtual sensor manager (VSM), query manager. • The top three layers deal with access mechanisms, access control, and integrity and security.</td>
<td></td>
<td>ETSI and European Commission</td>
</tr>
<tr>
<td>SMEPP[13]</td>
<td>Secure Middleware for Embedded Peer To Peer System                                                                                                                                                                                                                                                                                     • Specifies a quality oriented P2P service architecture supporting self configurable services and focuses on self-organization, service discovery and delivery.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Extensible Messaging and Presence Protocol (XMPP) is an open-standard communications protocol for message-oriented middleware based on Extensible Markup Language (XML).
Gaps Identified

- Middle-ware are available for respective field separately, for example, to address the RFID domain ASPIRE, WhereX, ISMB etc, for sensor networks in general GSN, for smart vehicular systems UBIROAD, but there **exists no generic middleware which can be applicable across all possible smart environments, including RFID domain**, and that can be customized as per the domain specific requirements.

- To resolve scalability issues IPv6 is proposed but not yet resolved completely.

- Support for context detection and processing has not been achieved fully.

- Support of semantic modelling

- Managing of data volumes.
Security and Privacy Issues in IoT Middleware Design

- Hydra middleware: supports key management and focuses on security-privacy preferences in QoS-aware selection.

- ISMB middleware: developed assistive services to improve patient data security

- ASPIRE middleware: incorporates measures for anonymity, blurring, cleanup, encryption, separation of different data etc.

- Shrink-wrapping in SAI: Shrink-wrapped security mechanism tightly couples the security framework to a user’s situation.

- PLASTIC project: advanced middleware support for service discovery, service composition, security and context management have been done.

- SURPAS: it aims to make a consolidated security framework that will transform security from an obstacle to a driver of large-scale industrial collaboration. The framework has the capability to include new and reconfigure existing security mechanisms.
Security and Privacy Issues in IoT Middleware Design

- **SOCRADES**: Its objective is to set secure communication between and integration of heterogeneous embedded systems and devices; accordingly, it specifies new wireless communication protocols that provide required security.

- **GSN middleware**: Its container architecture deals with access control mechanisms, integrity and security of data.

- **SIERENA**: Its web services specifications have security features such as user authentication, data encryption, etc.

- **SMEPP**: Its central focus is to make the middleware secure, generic and high customizable, allowing for its adaptation to different devices and domains. Objectives include: (i) design and implementation of a security infrastructure for EP2P systems and its integration into the middleware, (ii) design and implementation of secure routing protocols, and (iii) design and implementation of cryptographic protocols and security primitives for EP2P systems.
Gaps Identified: Security & Privacy Issues

- Unified approach to the design of security and privacy mechanisms is missing. Security and privacy sometimes of conflicting interests: user privacy opposes administrators security. An unified approach is in demand.

- Platform and device integrity protection is an unsolved problem.

- Design of robust yet light-weight cryptographic protocols which are adaptive and context-aware is a major unsolved problem.

- Design of privacy-aware data mining protocol with particular focus on security analysis and strength of privacy is required.

- Design of context-aware data privacy preservation protocol is required.
References

[9] “SOA-based Integration of the Internet of Things in Enterprise Services”,
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.73.1088&rep=rep1&type=pdf
Thank You