Ubiquitous Computing at RTMM LAB: An Introduction

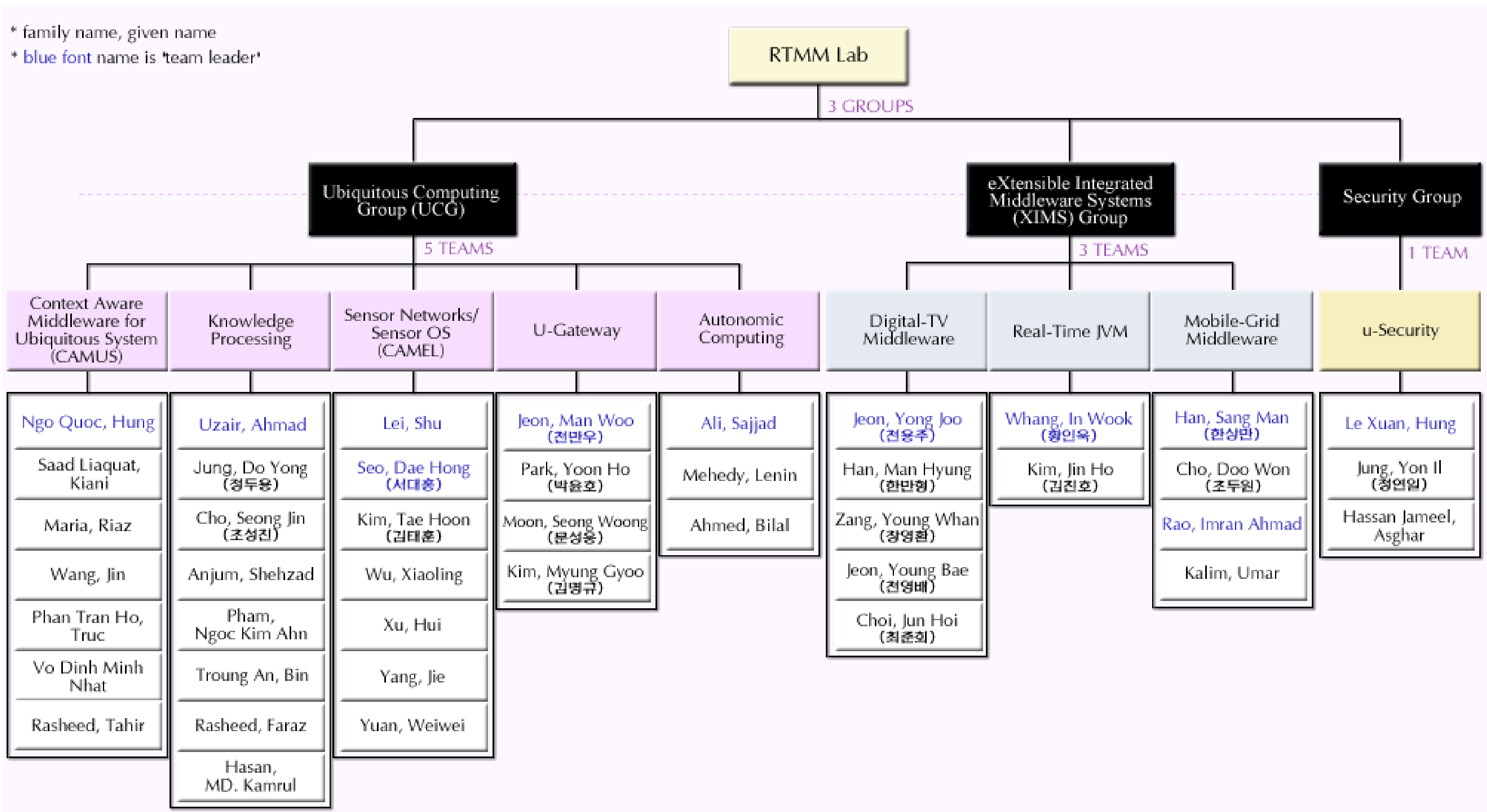
Prof. Sungyoung Lee

Real-time & MultiMedia LAB
KyungHee University, Korea
http://oslab.khu.ac.kr

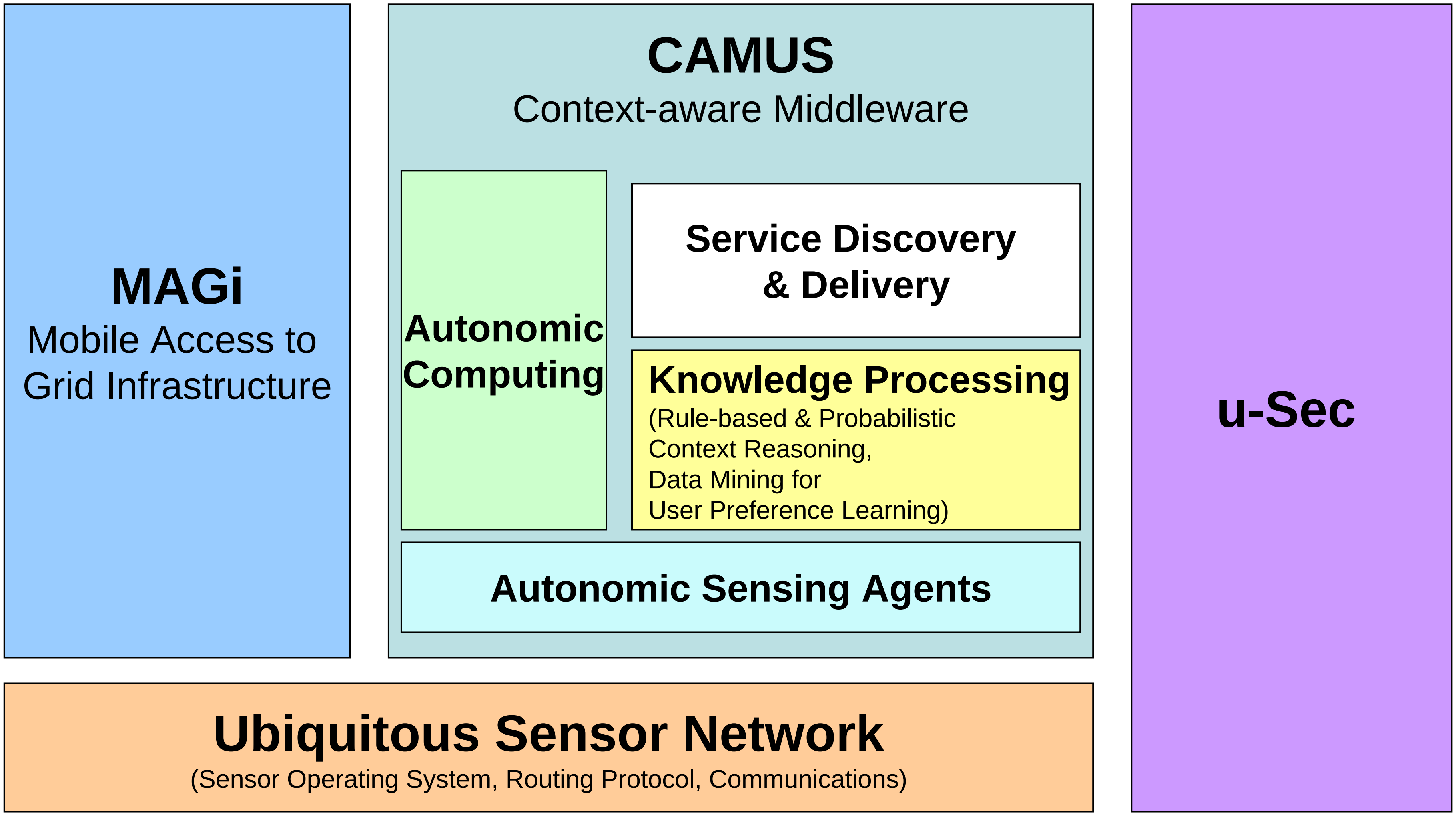
Outline

- **Organization**
- **Major Research Groups**
    - **CAMUS** – Context-aware Middleware for Ubicom Systems
    - **Knowledge Processing**
    - **Service Discovery & Delivery**
    - **Autonomous Computing**
    - **USN** – Ubiquitous Sensor Network
    - **MAGi** – Mobile Access to Grid Infrastructure
    - **Security**

Organization of RTMM LAB



Major Research Groups



… And The Professors …




Prof.
Tae Seong Kim

Dr. Andrey V.Gavrilov.

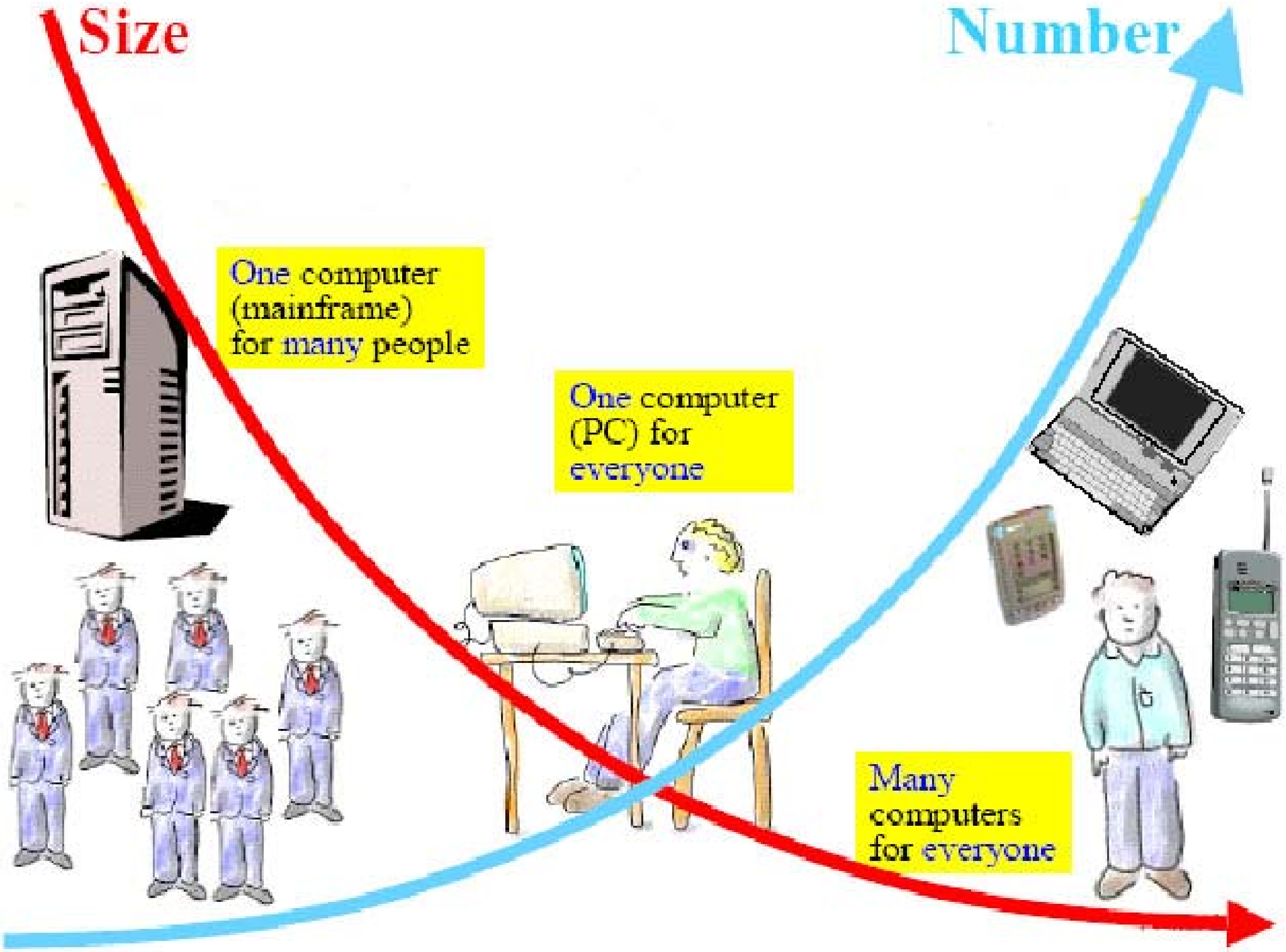
Dr. M. Kaykobad

Dr. Yllias Chali

- **Availability of expertise in fields of**
  - Distributed Systems, Real-time Systems
  - Mobile Wireless Communications, WSN
  - Knowledge Representation and Processing
  - Artificial Intelligence
  - Human Computer Interaction
  - Biomedical Engineering

CAMUS Group

Computing-a clear Trend



Picture from Prof. Mattern, Porquerolles

The Vision

Mark Weiser
(1952 – 1999), XEROX PARC

"In the 21st century the technology revolution will move into the everyday, the small and the invisible…"
Mark Weiser, 1988

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it"
Mark Weiser, 1991

And the key challenge

- **Ubiquitous (Pervasive) Computing**
  - Calm technology: embedded, invisible, seamless, unobtrusive, intelligent.

- **Context-awareness**
  - An important aspect of the intelligent pervasive computing systems
  - Systems that can anticipate users' needs and act in advance by "understanding" their context.

- **Sensing is a key enabling technology**
  - Ubiquity: deployed pervasively in the environment, on daily objs, on body…
  - Heterogeneity: communications, access mechanisms, output data, etc.
  - e.g. in location-sensing techniques: triangulation, proximity, scene analysis
    - ***(Jeffrey Hightower, "Location Systems for Ubiquitous Computing", IEEE Computer August 2001.)***

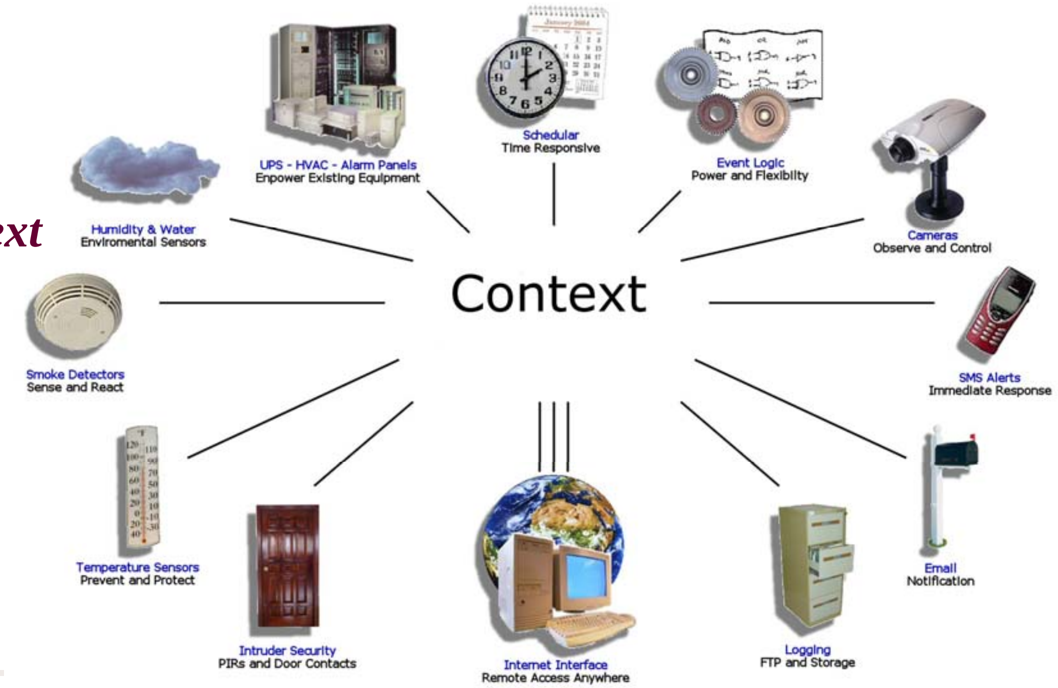
Context

Our definition(*): *The specific conditions, external to the application itself, such as audience, speaker (user), situation (place and its surroundings), time, environmental and network conditions, etc., which determine the application behavior, will be called the 'context' of the application.*

+Sensed Context

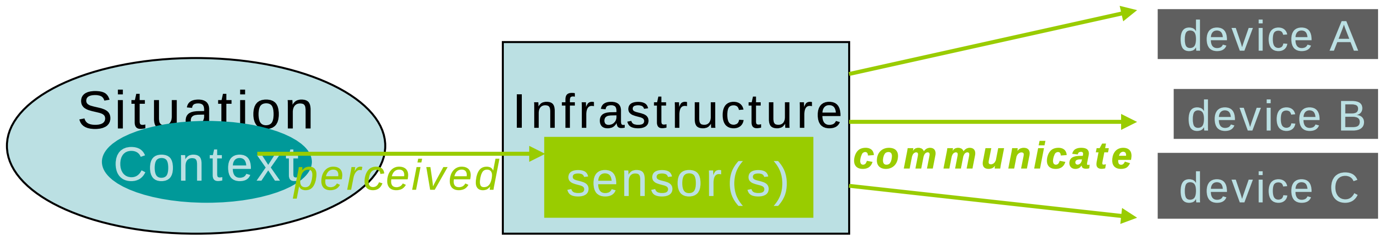
+Predefined Context

+Inferred/Deduced Context

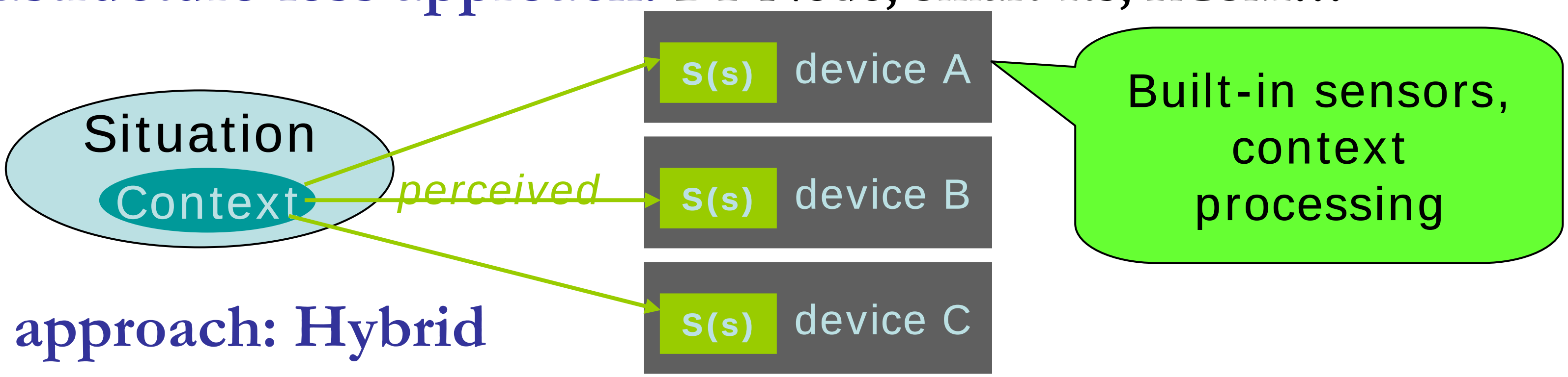


Approaches for Achieving Context-Awareness

- **Infrastructure-based approach:** **Context Toolkit, GAIA, Semantic Web Context Infrastructure (e.g. COBrA)…**

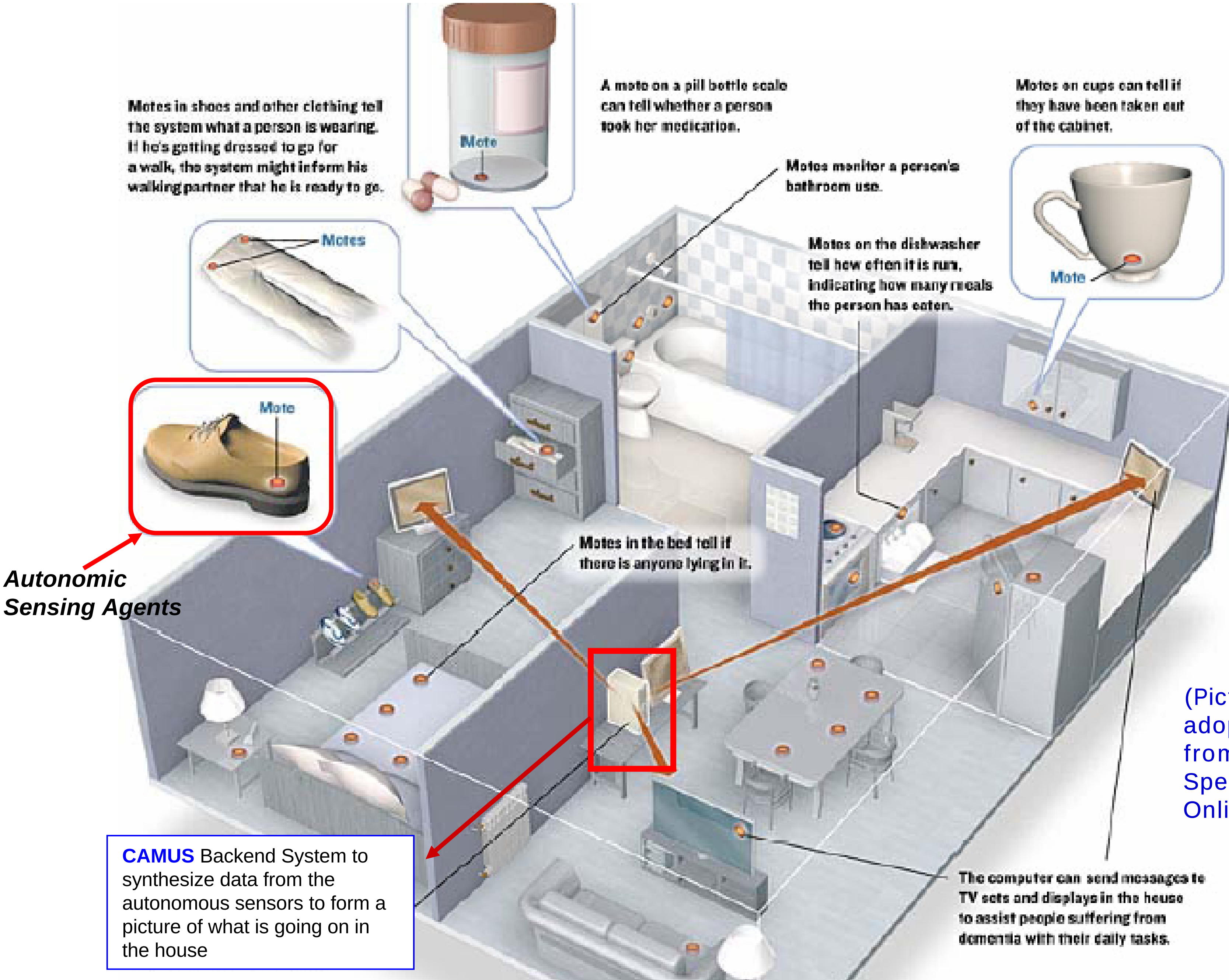


- **Infrastructure-less approach:** **BT Node, Smart-Its, RCSM…**



- **Our approach: Hybrid**
  - to exploit the computational *power* of backend system for realizing context, the autonomy of smart devices (*flexibility* in providing services everywhere), and the convenient interaction with the users (*unobtrusiveness*)

CAMUS - Context-Aware Middleware for Ubicom Systems



CAMUS Backend System to synthesize data from the autonomous sensors to form a picture of what is going on in the house

(Picture adopted from IEEE Spectrum Online)

Context-aware Middleware

- **Steps in processing context (roughly):**
  - sensing technologies, gathering sensed context data, sensor data fusion
  - modeling & storing context data,
  - Reasoning/inferring & learning, and
  - Delivering/disseminating the inferred contexts to applications

- **Designating those steps to Middleware will:**
  - Free the application developer from underlying tasks: Let him focus on implementing application logic
  - Reusability: built once – used by everyone
  - Separation of concerns: Context-aware Middleware decouples application layer with lower layers => more efficient to develop

Key characteristics of CAMUS

- **Support for heterogeneous and distributed sensing agents**
  - Unified Sensing Framework: data structure & access interface
  - Make it easy to incrementally deploy new sensors and context-aware services in the environment
  - Autonomic Sensing Agents are being developed
- **Provide different kinds of context classification mechanisms**
  - Pluggable engines
  - Different mechanisms have different power, expressiveness and decidability properties
  - Rules written in different types of logic (first order logic, description logic, temporal/spatial logic, fuzzy logic, etc.)
  - Probabilistic-based reasoning mechanisms, e.g Bayesian nets
  - Data mining & User Preference Learning are being investigated

Key characteristics of CAMUS (cont)

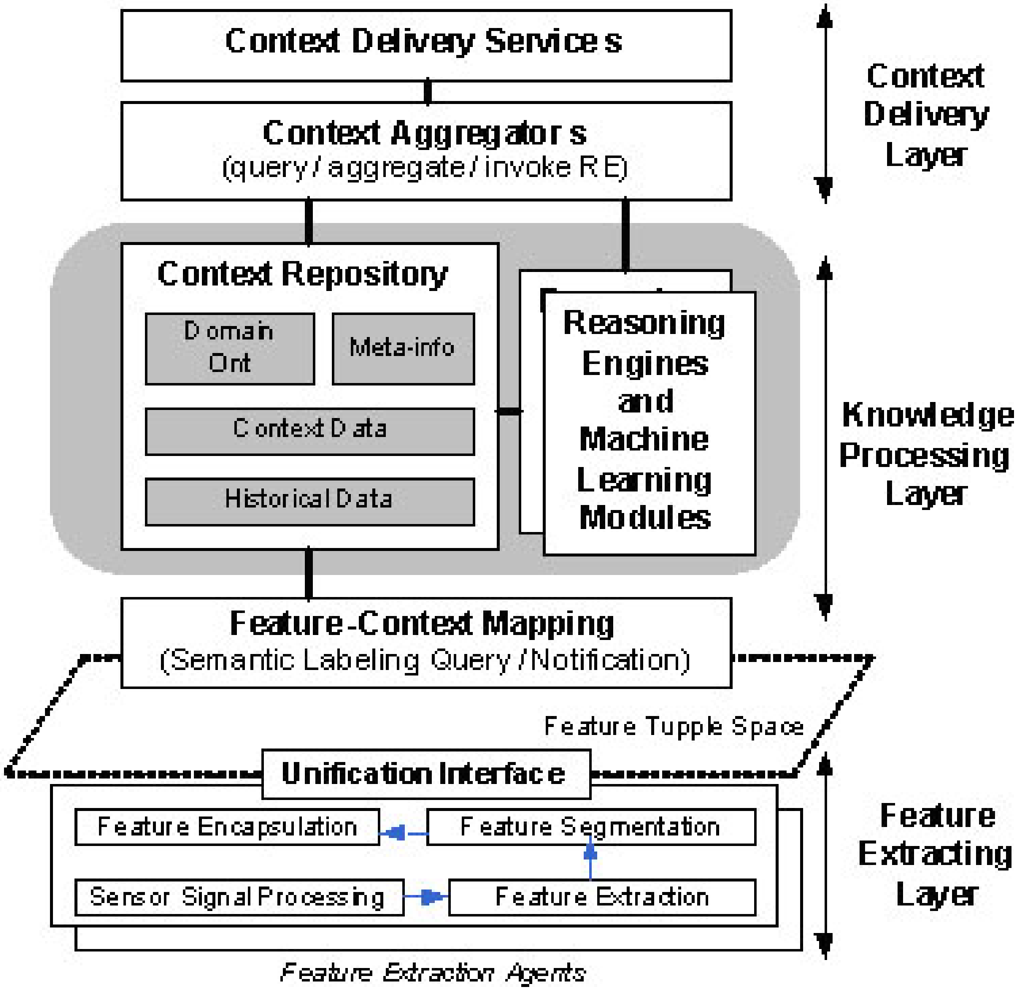
- **Follow a formal context model using ontology**
  - Using OWL
  - To enable syntactic and semantic interoperability, and knowledge sharing between different domains
- **Dealing with uncertainty to enhance the quality of context**
  - A really challenge for system usability
  - We deal with uncertainty in all levels: sensor data (probability attribute associated with feature value), context data (probabilistic reasoners, & modeling uncertainty being developed)

Key characteristics of CAMUS (cont)

- **Service Discovery & Delivery**
  - Semantic Matchmaking & Policy based Autonomic Access Control
- **Facilitate for applications to specify different behaviors in different contexts easily, as well as privacy policy and security mechanism**
  - Graphical development tool to ease developers in writing context-aware app.
  - Will be developed along with the application scenarios (smart spaces)

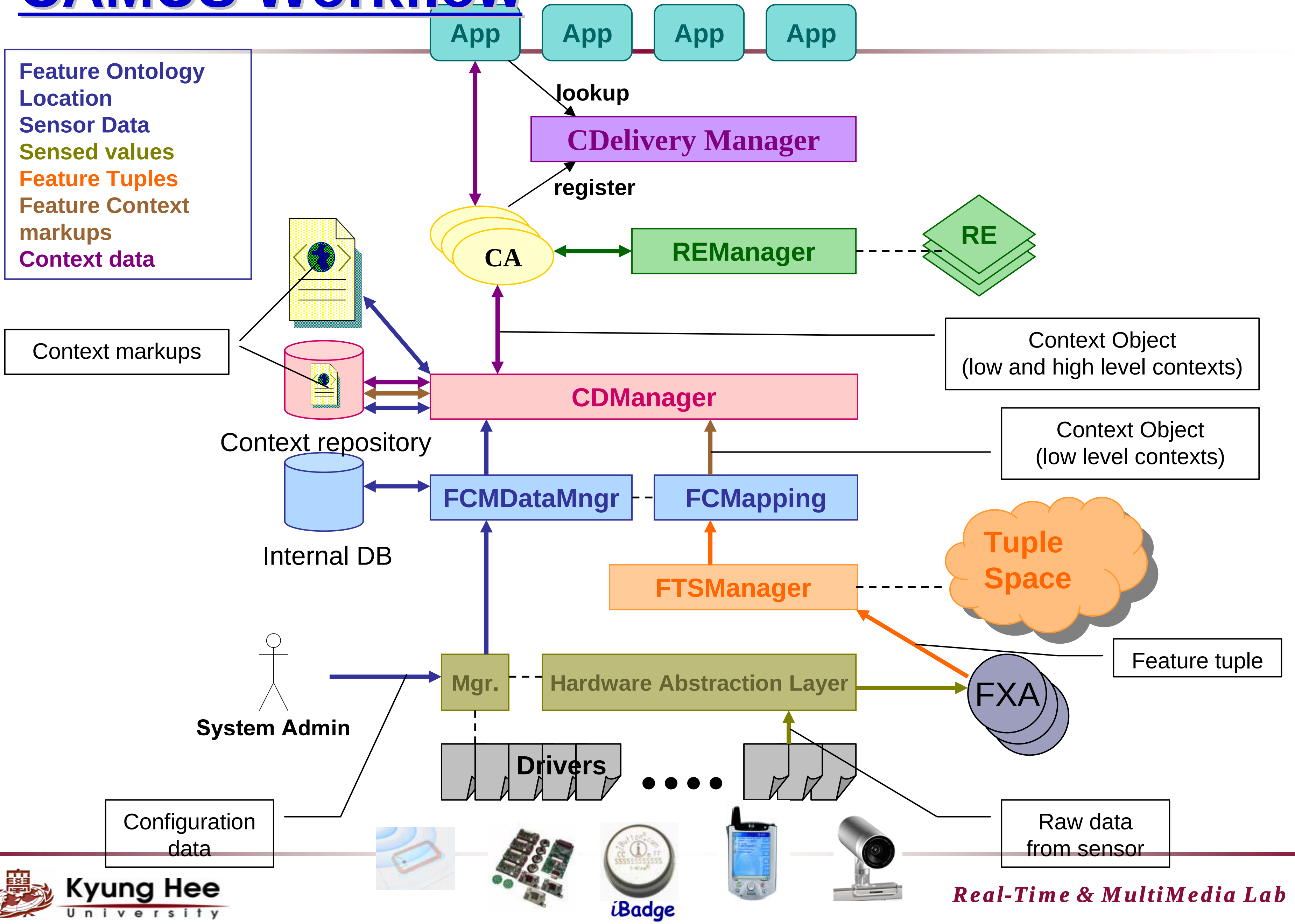
Our proposed Architecture

- **C**ontext-**A**ware **M**iddleware for **U**bicomp **S**ystems



Publication: 8 papers in int'l conferences (LNCS & IEEE), 1 technical report

CAMUS Workflow



Sample Dataflow

- **FEATURE : Unified format of data from sensors**
  - <sensorTypeID, featureTypeID, sensorID, quantizedLevel, value, probability, timestamp>
  - Ex : <6,1,1,null,105,1,20041210120000> → RFIDTagID = 105, from sensor #1, probability=1, timestamp=20041210120000
- **The feature is mapped into context markup**

```
<RFIDTag>
   <value>105</value>
   <probability>1</probability>
   <timestamp>20041210120000</timestamp>
<RFIDTag>
```

- **Combining many kinds of features with the data about users, sensors, places, using some reasoning mechanism, the system can infer the location of user**

```
<Person resource="http://hs.ac.kr/doctors#doctorA ">
   <locatedIn resource="http://hs.ac.kr/rooms#room125"/>
</Person>
```

- **The location info will be saved in the context repository, and can be delivered to the applications/services by Location Context Aggregator**
- **The system can also use reasoning to infer higher-level contexts, such as user's activities, based on location, user's intention and the environment features, then provides some smart services.**

Current Status of CAMUS

- **Finished system designing & prototyping**
- **A smart office scenario has been built**
  - CAMUS showed the usefulness and reusability for application programmers
  - Easily incorporate the specific algorithms from expert domains for extracting context information, e.g. sound/image based pattern recognition
- **However, the constraints in the availability of current sensing devices make it difficult to fully realize the hybrid approach**
  - Autonomic Sensing Agents instead of Software Abstraction of Sensing Devices

Autonomic Sensing Agent

- **The vision: "the real power of the concept [ubicomp] comes not from any one of these devices; it emerges from the *interaction* of all of them" – Mark Weiser**
  - In current smart sensors, the only functionality provided is just to send an identity or raw sensory data to a nearby stationary server to realize services on their behalf.
- **By Autonomic Sensing Agent, we are trying to leverage the interaction & collaboration between smart sensing devices for realizing their own services, improving the accuracy, and providing context data to the back end system.**

Autonomic Sensing Agent (cont.)

- **Why collaboration?**
  - Single agent can only perceive a small subset of its environment with its own local sensors, and therefore needs to cooperate with others for deriving more accurate context data.
- **A *lightweight autonomic communication protocol* is being developed**
  - Ubiquitous Network with thousands of nodes form short-live, ad hoc communications. There must be a common, autonomic yet secure & lightweight *'language'* to leverage the interaction & collaboration among them; & context aggregation of the backend system to draw a complete picture of what's going on in the environment
- **Some initiations**
  - BT Nodes (ETH), Smart-Its, Smart Sensors, RCSM: No collaborative processing & learning, just context-aware communication

Autonomic Sensing Agent (cont.)

- **Where (or to Whom) to send context data?**
  - Group based, Role-based (semantic level)
  - Autonomic Access Mechanisms: Credential, Lightweight Trust Scheme.
- **What to send And How to send**
  - Device ID, feature-signature, Metadata, feature value, security attributes, etc.
  - Broadcast small messages for advertising/discovery, & followed by Uni/Multicast large messages for data exchange
  - ZigBee platform (short range low data rate)
- **When to send context data? (segmented features)**
  - Define some metrics e.g. local context deviation
  - Collaborative learning mechanism for sensor network e.g. Support Vector Machine (SVM)

Knowledge Processing Group

Introduction

- **Previously, Context reasoning has been confined to isolated concepts of context.**
  - Location
  - Environment
  - Application specification
  - Time etc.
- **We define Context in its comprehensive sense and develop**
  - An integrated Context Reasoning Engine to capture the maximum of real situations

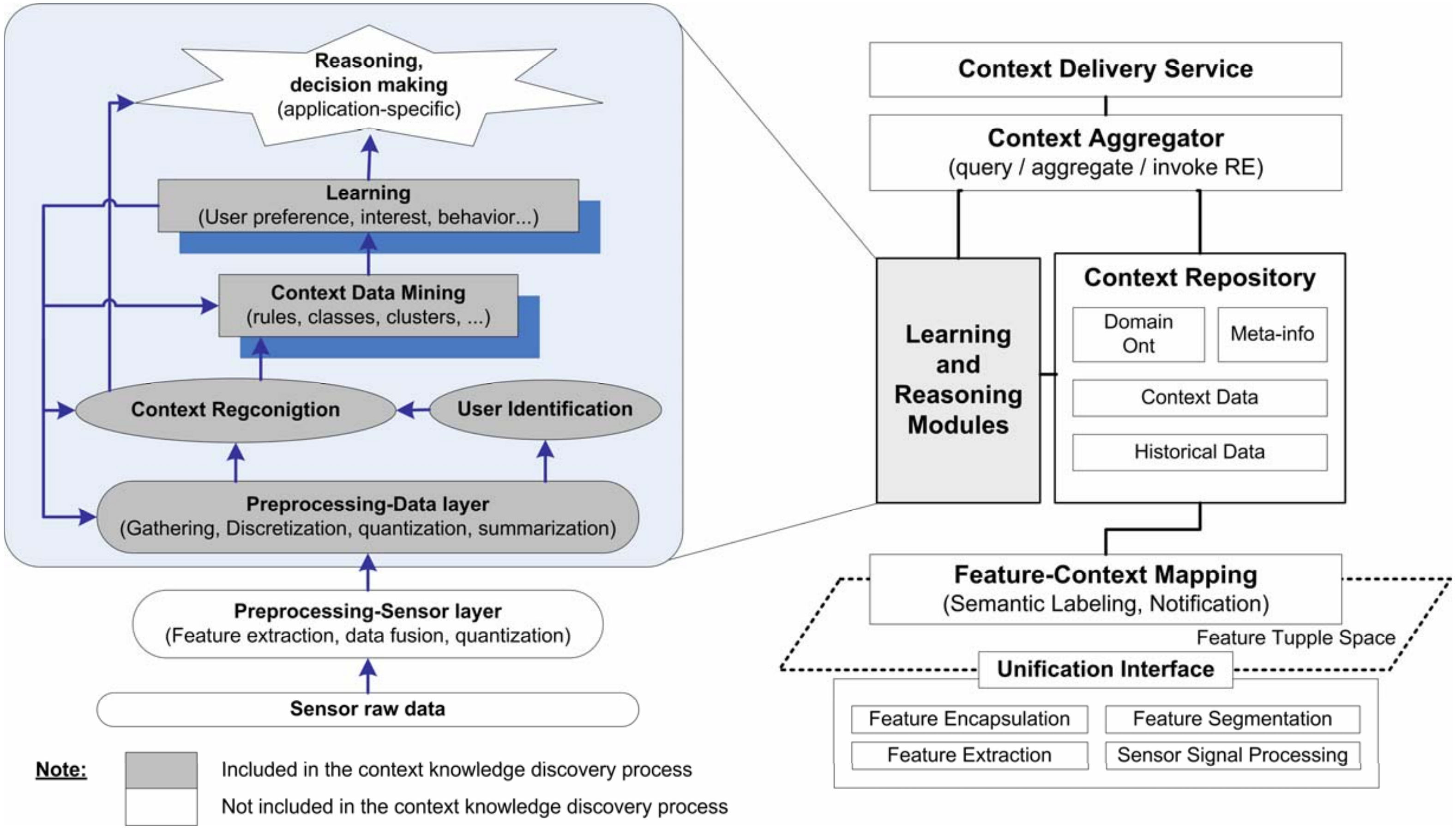
Distinguishing Features

- Converting Low level sensor information into Knowledge of Use's identity, location, situation and environment
- Develop efficient distributed storage and query mechanisms to deal with tons of Context data
- Learning users habits, preferences out of this historical Context data
- Predicting probable future situations based on past evidence

Research Directions

- **Context Modeling**
  - To Represent and Capture the knowledge about **'Context'** using Semantic Web technologies i.e OWL, RDF
  - Knowledge representation: Contel – context ontology model for CAMUS, including the User preference and behavior routine ontology
  - User Modeling: modeling (or learning) of user preference and routine
- **Context Summarization and Garbage Collection**
  - Autonomic Context Knowledge Management
- **Context Reasoning**
  - Inference and prediction of 'Effect' of a certain 'Cause' in the user environment
- **Location Awareness**
  - Probabilistic methods to analyze Radio Signal Strength Indicators (RSSI) of WiFi Access Points.
  - Provision of location awareness in CAMUS

Reasoning Engine



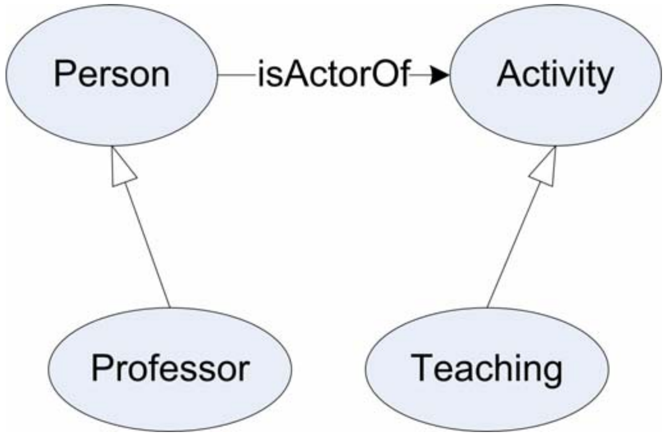
Contel Example

- **Domain Ontology**

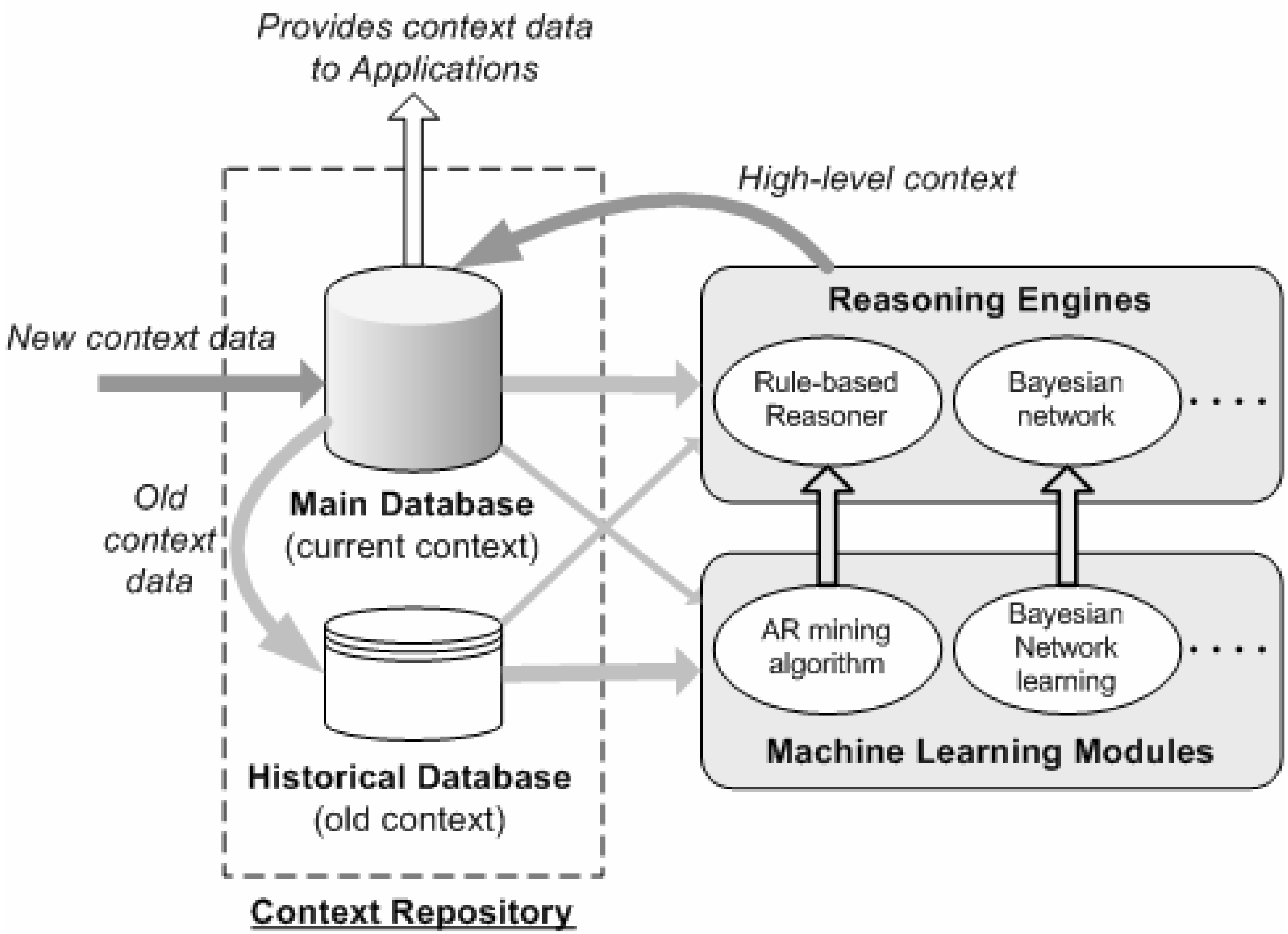
```
<rdf:Class rdf:id="Person"/>
<rdf:Class rdf:id="Activity"/>

<rdf:Class rdf:id="Professor">
        <rdf:subClassOf rdf:resource="#Person"/>
</rdf:Class>

<rdf:Class rdf:id="Teaching">
        <rdf:subClassOf rdf:resource="#Activity"/>
</rdf:Class>

<owl:ObjectProperty rdf:ID="isActorOf">
        <rdfs:domain rdf:resource="#Person"/>
        <rdfs:range rdf:resource="#Activity"/>
</owl:ObjectProperty>
```

- **Context Data**

```
<Professor rdf:id="Professor SY Lee">
        <isActorOf>
                <Teaching rdf:id="Real-Time_System"/>
        <isActorOf>
</Professor>
```

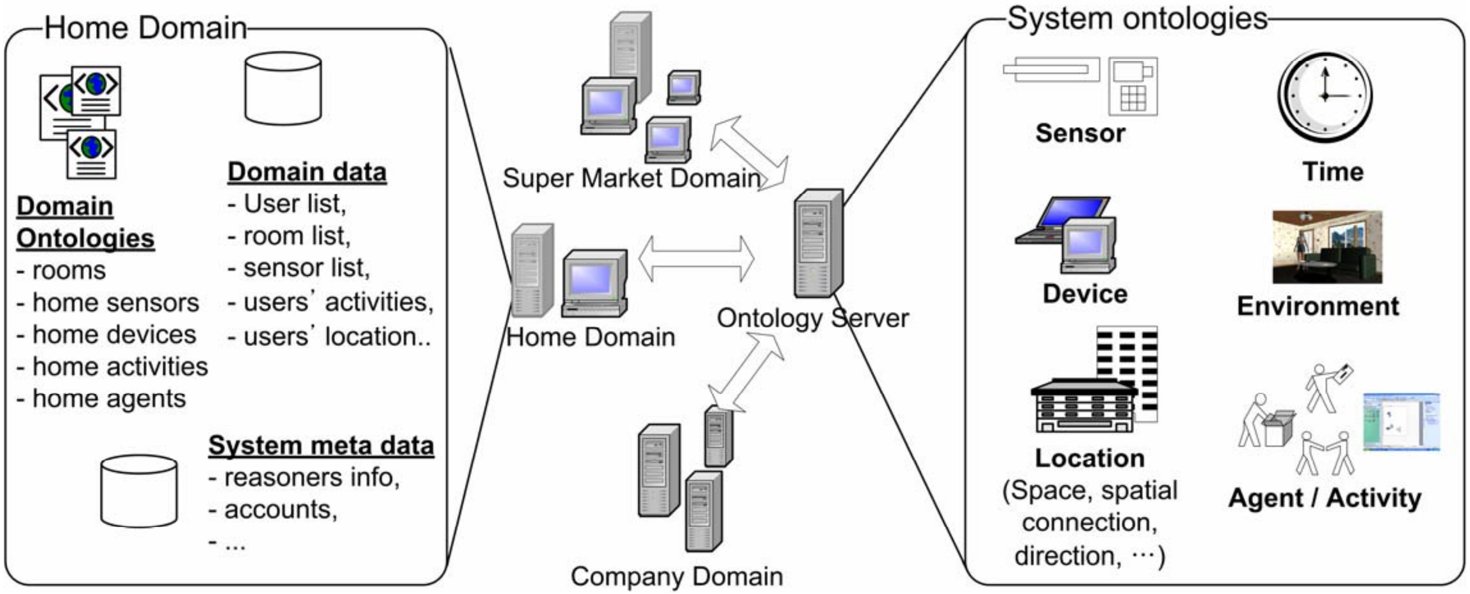


A Learning-Reasoning combination approach



Context Repository

- Include the domain ontology and Context Information
  - **Domain Ontology.** Domain ontology contains the ***domain concepts and properties*** with formal semantics described in OWL.
  - **Context Information.** Context is ***any information saved by the Feature - Context Mapping layer*** gathered from the environment through lower layers of the architecture.

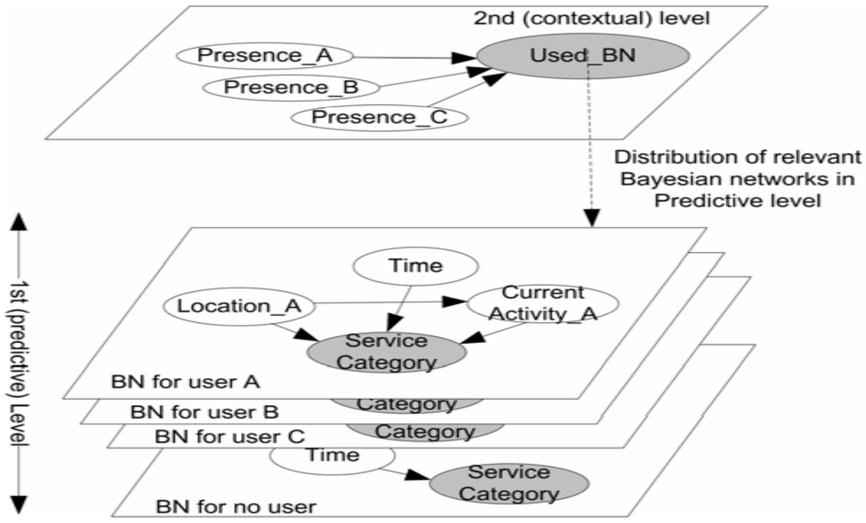


Location Awareness

- **Location: Integral part of Context**
  - In CAMUS Reasoning Engine Location of user is modeled and represented as core Context information
- **WiFi LAN based Location Awareness**
  - Signal Strength of WiFi Access Points are used to estimate the location of a mobile device e.g Laptop Notebooks, Handheld devices.
  - Location Reasoning Module builds a 'Location Probabilistic Model' based on Signal Strength of every WiFi Access Point in CAMUS environment.
  - Location of target Devices is estimated based on real-time Received Signal Strength of the device.

Preference and Priority Learning

- **Using a Bayesian RN-Metanetwork to learn the Preference and Priority of users, as well as resolve the conflicts in a multi-user environment**
  - Example: Modeling of user's Multimedia Service Preference and priority



Context Summarization Module

- **Ubiquitous Computing Environments contains a large amount of data sources in the form of sensors.**
- **These data sources emit a huge amount of contextual data continuously.**
- *Key Idea*
  - *To identify and remove some irrelevant data (garbage collecting context), summarize it and only store the summarized and more meaningful data.*
- Benefits
  - improved performance in query processing, data retrieval, knowledge reasoning and machine learning.

Related works

- **Gaia**
  - Manages uncertain contexts, however no support for distributed environment & query
- **CoBrA**
  - Not support uncertain contexts and distributed environment
- **Context Gateway**
  - Centralized Knowledge Base (KB) & no uncertain contexts
- **Solar**
  - Distributed, but simple sensor data, no KB, no reasoning
- **LiquidQ**
  - Just a distributed query mechanism, no reasoning

Reasoning Algorithms

- **Bayesian net**
  - Learn user preference in TV channel selection, user activity and availability
- **Flexible, Incremental Learning of User Models (FILUM)**
  - To learn user model for mobile state (Intelligent Telephone Assistant project)
- **Hidden Markov Model**
  - To learn and infer a user's daily movements (University of Washington)
- **Classification**
  - Context regcognition and prediction
- **Neural net**
  - Learn the next-2-second occupation of user (Adaptive house)
- **Q-learning, Association Rule mining, etc.**

Future Directions

- **Improve the performance of Bayesian Reasoning Algorithms**
- **Expanding the scope of Location Awareness**
  - In-building Location Awareness suffer from many physical limitations e.g Walls, people, machines.
  - Accuracy of reasoning about location drops as the target area gets bigger.
- **Building Context Negotiation mechanisms**
  - Multiple User's pose conflicting requirements to Context Aware Systems
  - Enabling CAMUS to Negotiate among conflicting Contexts and find a graceful resolution.
- **Context Prediction Model**
  - For preparing situation based on User's previous preferences.

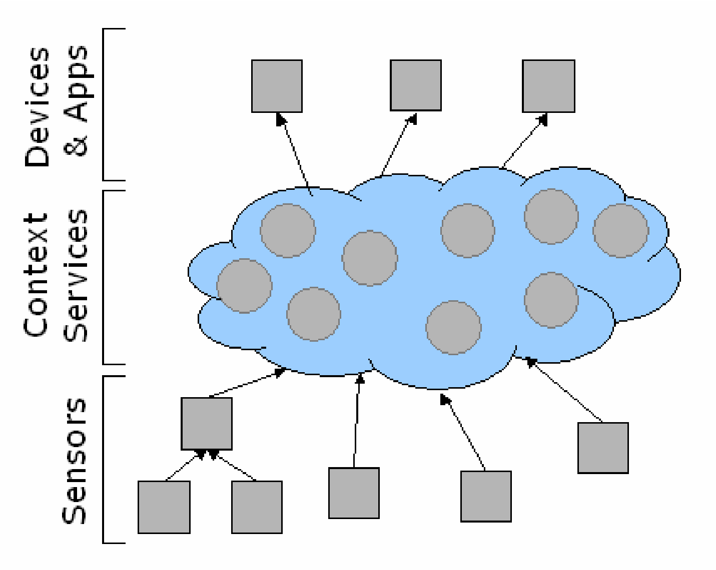
Publications

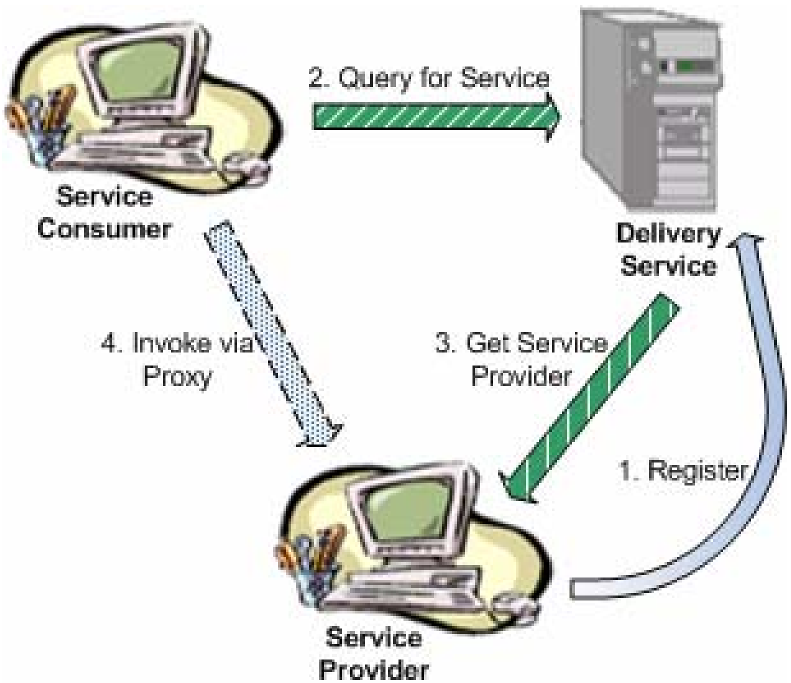
- Uzair Ahmad, S. Y. Lee, Mahrin Iqbal, Uzma Nasir, Arshad Ali, Mudeem Iqbal: Reflective Middleware for Location-Aware Application Adaptation. ICCSA (2) 2005: 1045-1054
- Uzair Ahmad, Sung Young Lee, Young Koo Lee, On Building a Reflective Middleware Service for Location-Awareness, RTCSA 2005, Hong Kong
- Kim Anh Pham Ngoc, Young Koo Lee, Sung Young Lee. OWL-Based User Preference and Behavior Ontology for Ubiquitous System. Accepted to ODBase Conference. Nov 2005.
- Kim Anh Pham Ngoc, Young Koo Lee, Sung Young Lee. Context Knowledge Discovery in Ubiquitous Computing. Accepted to ODBase Conference. Nov 2005.
- Anjum Shehzad, N. Q. Hung, Kim Anh Pham, Sungyoung Lee. Formal Modeling in Context Aware Systems. In proceedings: Workshop on Modeling and Retrieval of Context, CEUR, ISSN 613-0073, Vol-114, 2004.
- Faraz Rasheed, Yong-Koo Lee, Sungyoung Lee, "Context Summarization and Garbage Collecting Context", Ubiquitous Web Systems and Intelligence 2005 http://www.orient-explorer.com/ICCSA/registration.html, Suntec Singapore, 9-12 May 2005, (SCIE)
- Binh An Truong. Modeling and Reasoning about uncertainty in Context-Aware Systems. ICIS 05.

Service Discovery and Delivery in CAMUS

Introduction

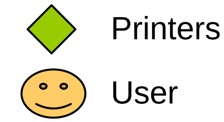
- **As the services become more and more distributed and pervasive, it becomes difficult to find an appropriate service and use it**



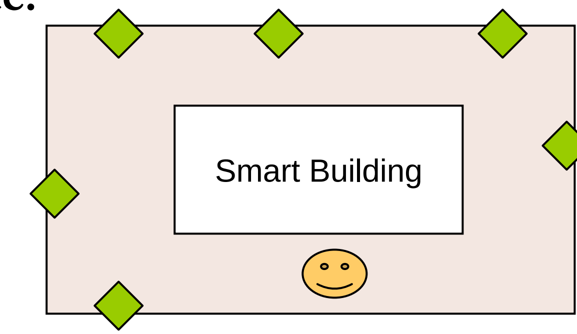


- **A service registration, lookup and delivery mechanism is required**
  - This is the top layer of our CAMUS architecture
  - It searches for the appropriate service
  - It is analogous to search engines in web

Problem Scenario



- **We assume that CAMUS is deployed in a smart academic building**
- **Printers are deployed in various labs and professors offices**
- **CAMUS should provide student, professor, visitors etc.**
  - A printing service, based on
    - **Context**
      - Location (nearest printer)
      - Printer's load (Printer with lower load)
      - Printers which are not out of papers etc..
    - **Access Policy**
      - A guest may be allowed to only one printing service
      - A student should not be allowed to print from a printing service which is available in the professor's office etc.
    - **User Priority**
      - Professor should get higher priority than a student to print from the same printing service.
    - **User preference**
      - User may prefer HP to CANON
      - User may prefer laser printer to bubble jet printer.
      - User may prefer letter size to A4 papers…etc.



Problem Specification

- **Traditional service registration, lookup and delivery services can not satisfy the requirements of context aware environments because**
  - Traditional approaches use 'syntax-based' search
    - Same 'semantic' concept can have different 'syntactic' representations => ***Synonyms*** (e.g., laptop = computer, desktop = computer)

      i.e. RTMM Lab Printer, Network Lab Printer etc for different Printer
    - Different 'semantic' concepts can have same 'syntactic' representation => ***Homonyms*** (e.g. cold = illness, cold = weather)
  - They do not consider the 'context' in which the client makes a service request
    - User at Location 'A' would like to use printer nearby his location

Problem Specification (cont.)

- Do not support access control over services and information
  - Users may have different access to a service
  - User doesn't want everyone to know he is at Location 'A'

- Security requirements change with the changing context
  - Allow people to enter on weekdays but not on weekends

Motivation

- **Our motivation is to provide a model for service delivery in context aware environments**
- **Functionalities:**
  - Provide a discovery and registration mechanism which can utilize syntax as well as semantics in order to make better matchmaking decisions in discovering appropriate services
  - Incorporate dynamic and transparent access-control mechanism in the context delivery process to ensure privacy and overall integrity of the system

Service Search & Matching

- **We use ontologies to create a common understanding of a specific domain to perform Semantic matching**
  - overcomes some problems related to *homonyms* and *synonyms*

- **We use context for filtering out unrelated services**
  - Preemptive Filtering – if a 'Printer Service' status is changed to '*out of paper*' or '*out of toner*' it is
    removed from the search space
  - Post Filtering – basing on user's context e.g., Location, Time, User Preference etc

Matchmaking in CAMUS

Pre-Matchmaking Filtering

If a printer service is out of service or out of paper it is removed from the search space

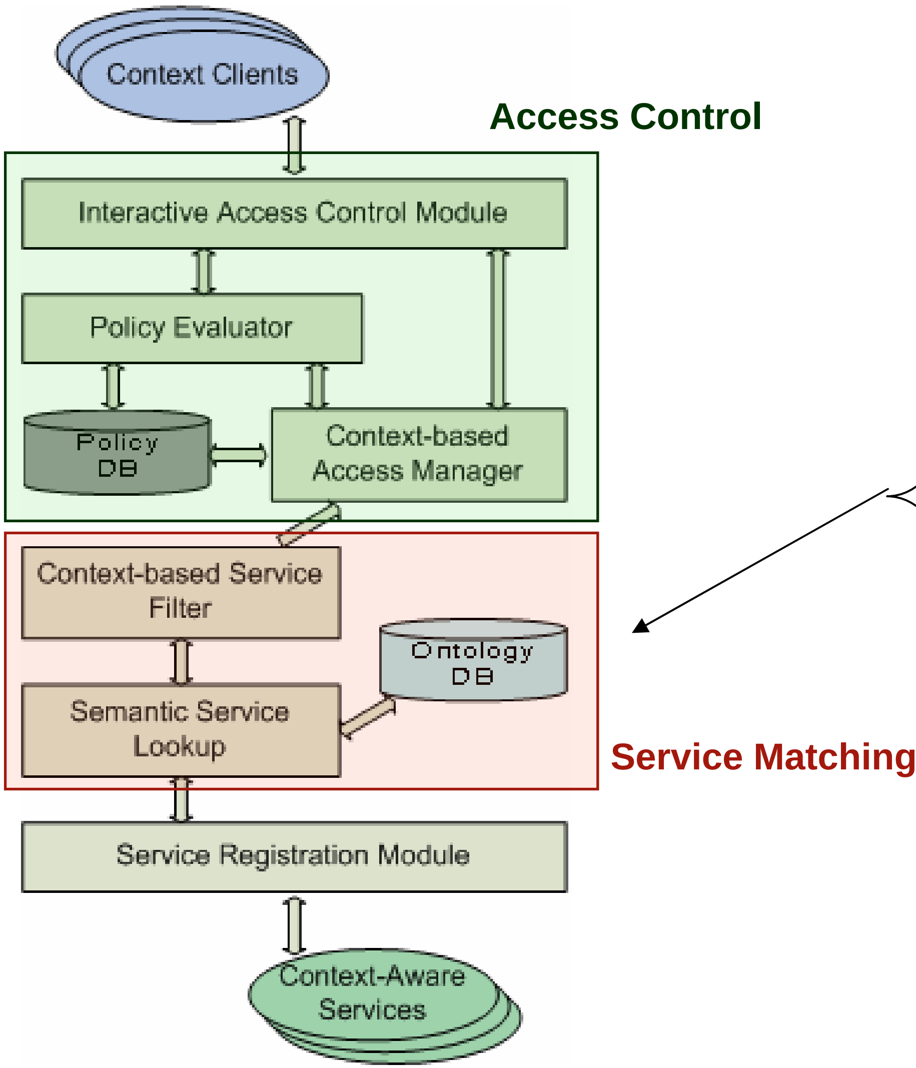
Matchmaking

Matchmaking based on ontology and semantics is performed and all kinds of available printing service are retrieved

Post-Matchmaking Filtering

Depending on the context (i.e. location and printer's load) the appropriate service is provided. Multiple services may be displayed to the user

Service Delivery Architecture



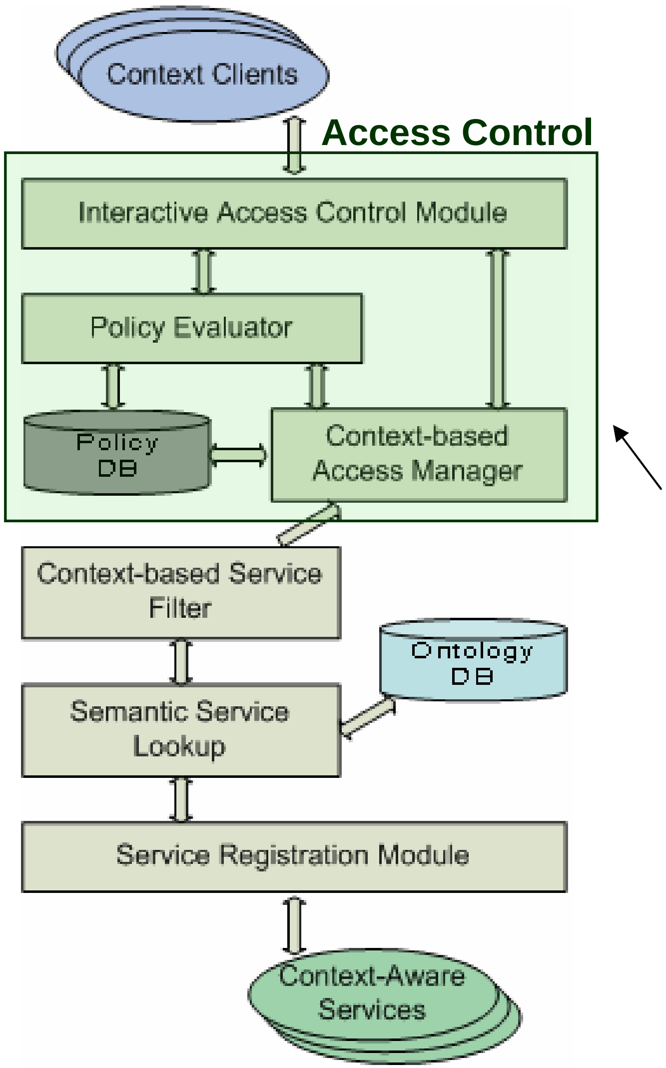
Context-based Service Filter Module performs the Pre-filtering

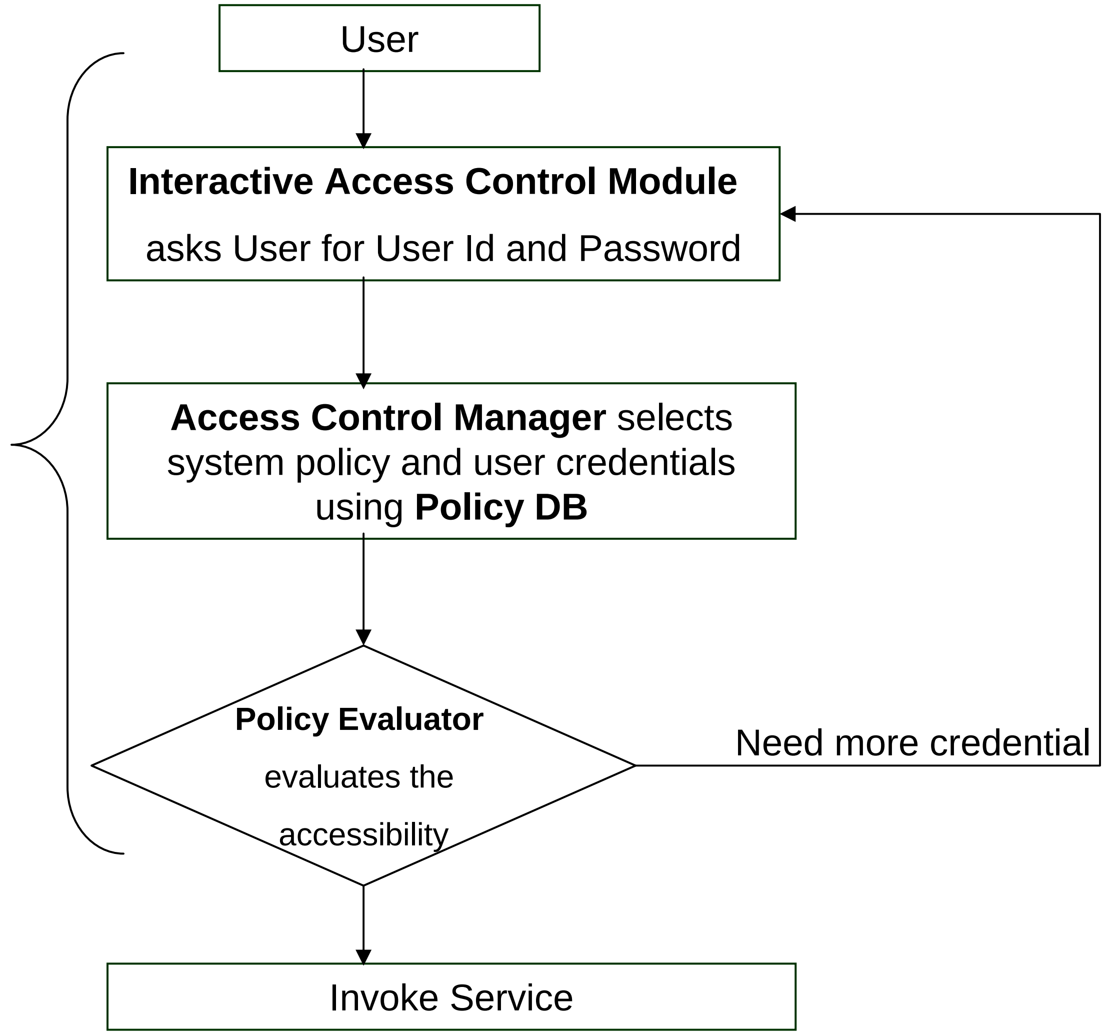
Semantic Service Lookup performs the semantic matching and finds out the services using **Ontology DB** and **Service Registration Module**

Context-based Service Filter Module performs the Post-filtering

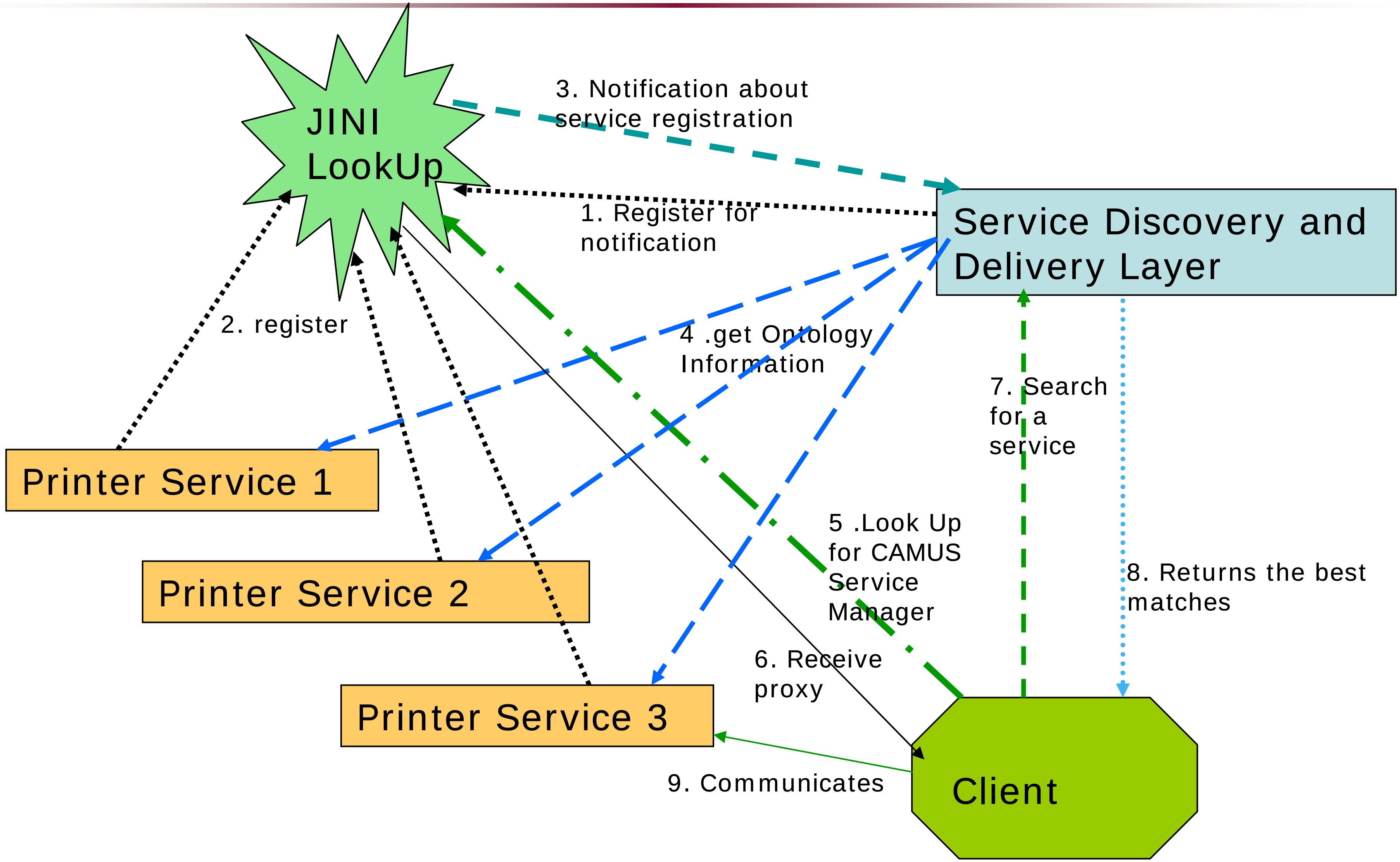
Search result is passed to user

Access Control Approach





Communication Using JINI

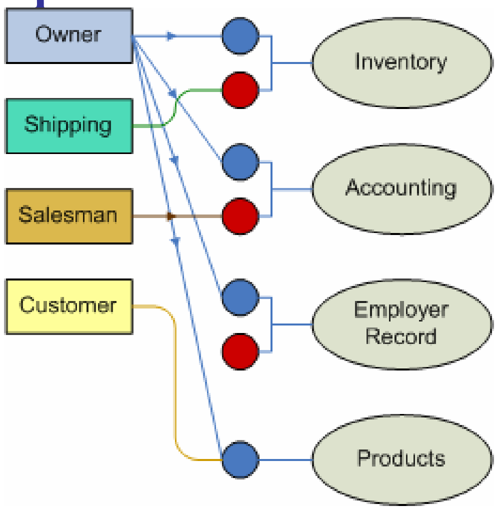


Current Research Direction

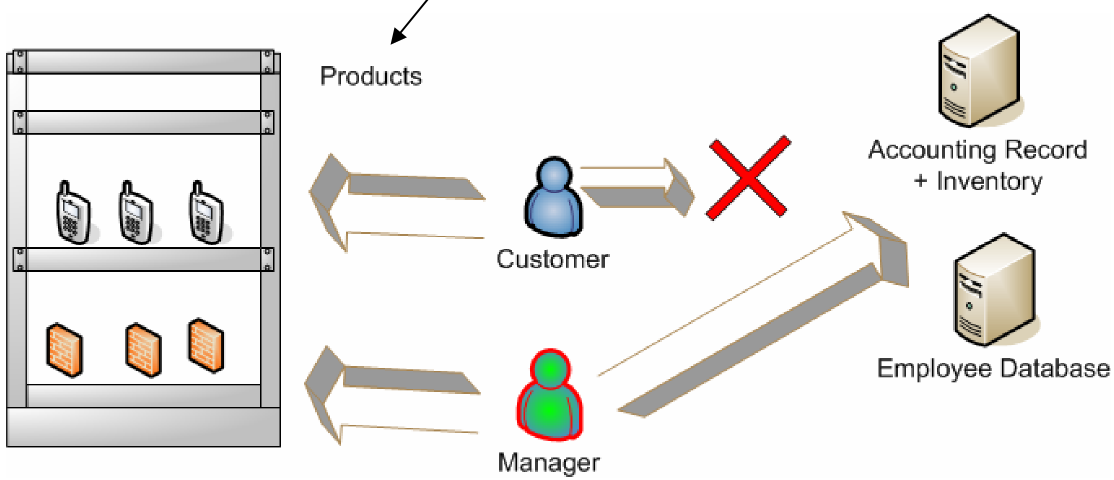
- **We are trying to** personalize our service discovery mechanism **for better user satisfaction in a smart environment.**
- **We found several works regarding** personalization (use of user preference) **of web service discovery. MyYahoo, Amazon.com etc are some examples where an user can enjoy personalized services.**
- **We will adopt**
  - Use of user preference in Service Discovery
  - User Preference Learning in Service Discovery
  - Usage Pattern Detection
  - Privacy and security of user preferences

An Application Scenario

- A market place scenario with various services, clients and policies



In future, an user will be able to find more personalized search result for the products base on his preference using CAMUS



Summary

- **This module presents a solution for service registration, matching and delivery in context aware environments**

- **Functionalities achieved**
  - Improved search relevance and precision by incorporating semantics and context-based filtering
  - Dynamic system policy selection and implicit client credentials for transparent access control

Towards An

Autonomic CAMUS

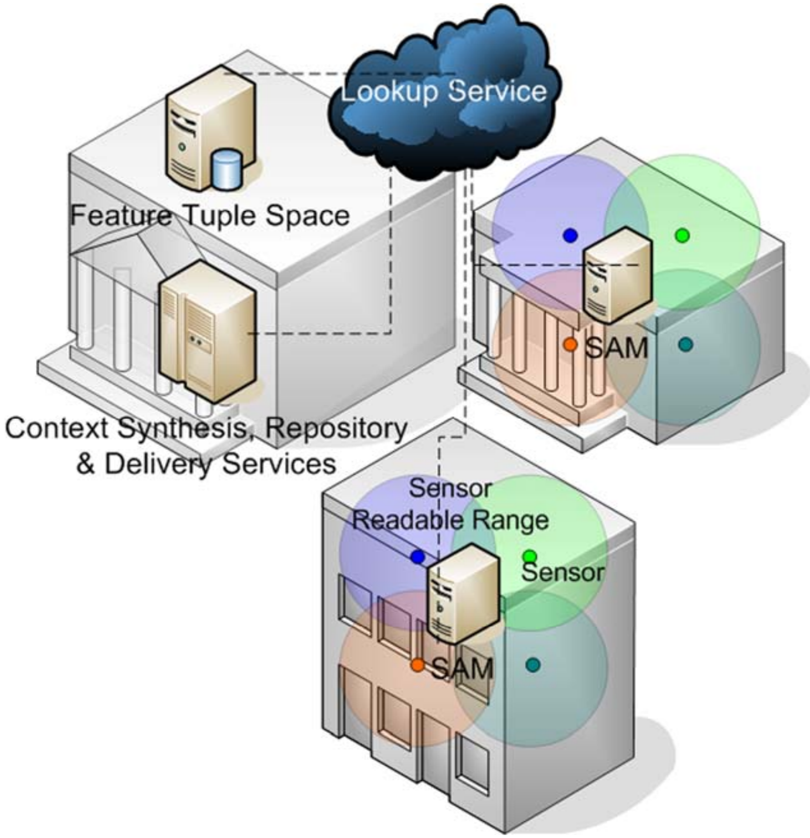
The Vision of Autonomic CAMUS

- **Design, build and manage complex and disparate computing systems capable of**
  - ***Self-configuration***: Automatically configure components to adapt them to different environments
  - ***Self-healing***: Automatically discover, diagnose, and correct faults
  - ***Self-optimization***: Automatically monitor and adapt resources to ensure optimal functioning regarding the defined requirements
  - ***Self-protection***: Anticipate, identify, and protect against arbitrary attacks

- **The union of Autonomic and Ubiquitous computing is highly beneficial in terms of**
  - Management of system complexity and heterogeneity
  - Reduced deployment and maintenance costs
  - Use of context information from Ubiquitous system for policy guidance, optimized configuration etc.

Problem

- **Currently CAMUS uses no mechanisms for fault tolerance or self-healing**
- CAMUS is designed to be deployed over a dynamic network
  - Entities (computers, servers, services) may change their identification or location without prior notice
  - Other inherent network problems like network disconnection, malformed data, buffer overflows, memory constraints, network queues, heterogeneous interfaces, malicious code etc.



- Due to the distributed nature of CAMUS, fault tolerance and self-healing is very important and of great benefit

Motivation

- **To develop an Autonomic CAMUS, with initial focus on Self-healing and fault tolerance**
  - AutoCAMUS should have the capability to anticipate and correct problems before they impact any aspect of its performance
  - Each layer of CAMUS will be embedded with a customized self-healing manager so that we have a specialized self-healing subsystem for each:
    - Feature Extraction layer
    - Reasoning and Learning module layers
    - Context Delivery and Aggregation layer
    - Services layer

Approach

- **Current work on AC systems and ubiquitous systems largely involves reactive healing, based on feedback control i.e.,**
  - On the basis of instantaneous need
  - On the basis of short-term historical measurements
- **Obvious drawbacks of this approach are**
  - Static in nature
  - Potentially large variations in performance
  - Slow response to change (lack of adaptability)
- **Our idea is to incorporate predictive autonomicity for self-healing in CAMUS**

Autonomic CAMUS

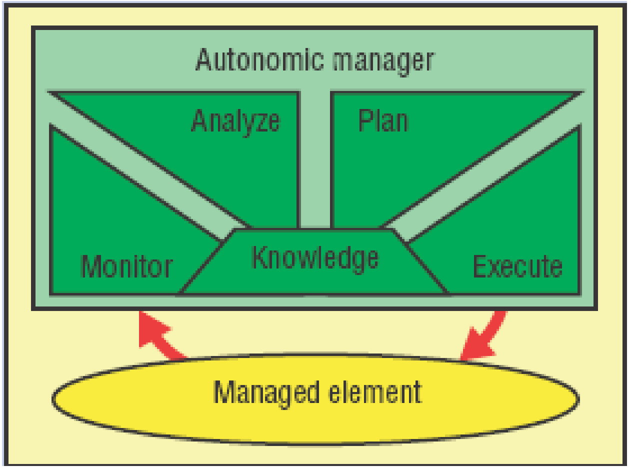
- **Modeling autonomic management in AutoCAMUS using**
  - Resource Modeling
    - A structured model for resource monitoring, analysis, event notification and corrective measures
  - Event Modeling
    - A structured model for maintaining/changing the system state based on context and situation of events and the system policy
- **Catering for uncertainty and fault detection in system state using Fuzzy logic/Bayesian Networks**
- **Catering for predictability using historical data**
- **Goal**
  - Fault-tolerant, self-healing CAMUS using predictive autonomicity

Current Work

- **Detailed analysis of prediction schemes that can be utilized in AutoCAMUS**
  - Step-Wise Regression (SWR)
    - Uses linear regression analysis to determine the relationship between two or more quantitative variables so that one variable can be predicted from the others
    - Good for speed but difficult to incorporate machine learning
  - Rule Induction (RI)
    - Discovers patterns that delineate categories, assemble them into classifiers, and use them to make predictions e.g., ID3 and C5.0 algorithms
    - Better suited for concept learning and context categorization
  - Case-based Reasoning (CBR)
    - utilizes specific knowledge of previously solved cases to solve future ones
    - Good for analogy and reasoning-based systems
  - Artificial Neural Nets (ANN)
    - Uses multilayer perceptrons with a specific back propagation learning algorithm for prediction
    - Speed of convergence is slow
- **Implementation of a test-bed system to analyze requirements for self-healing in AutoCAMUS**

Future Research Directions

- Building truly closed control loops (MAPE loop)



- To cater for issues related with the modeling of uncertainty

- To incorporate predictability and learning behavior

Selected Publication

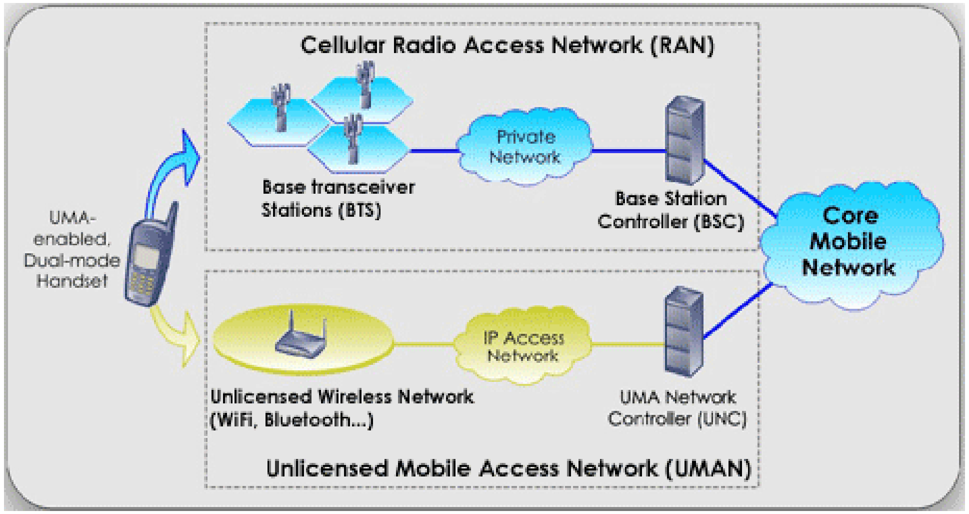
1. *Research Issues in the Development of Context-Aware Middleware Architectures*. Hung Quoc Ngo, Anjum Shehzad, Young-Koo Lee, and Sungyoung Lee. 11th IEEE International Conference on Embedded and Real-time Computing Systems and Applications (*RTCSA '05*).
2. *Service Delivery in Context Aware Environments: Lookup and Access Control Issues*. Maria Riaz, Saad Liaquat Kiani, Sungyoung Lee, and Young-Koo Lee. 11th IEEE International Conference on Embedded and Real-time Computing Systems and Applications. (*RTCSA '05*).
3. *A Distributed Middleware Solution for Context Awareness in Ubiquitous Systems*. Saad Liaquat Kiani, Maria Riaz, Sungyoung Lee, and Young-Koo Lee. 11th IEEE International Conference on Embedded and Real-time Computing Systems and Applications. (*RTCSA '05*).
4. *A Comprehensive Middleware Architecture for Context-Aware Ubiquitous Computing Systems*. Anjum Shehzad, Hung Quoc Ngo, S. Y. Lee, Young-Koo Lee. ACIS International Conference on Computer and Information Science *(ICIS 2005)*.
5. *Context-awareness in large scale ubiquitous environments with a service oriented distributed middleware approach*. Saad Liaquat Kiani, Maria Riaz, Sungyoung Lee, Young Ku Lee. ACIS International Conference on Computer and Information Science *(ICIS 2005)*.
6. *Incorporating semantic-based search and policy-based access control mechanism in context service delivery*. Maria Riaz, Saad Liaquat Kiani, Sungyoung Lee, Young Ku Lee. ACIS International Conference on Computer and Information Science *(ICIS 2005)*.
7. *Formal Modeling in Context Aware Systems* . Anjum Shehzad, N. Q. Hung, Kim Anh Pham, S. Y. Lee. In proceedings: Workshop on Modeling and Retrieval of Context, *CEUR*, ISSN 613-0073, Vol-114, 2004, Germany.
8. *Developing Context-Aware Ubiquitous Computing Systems with a Unified Middleware Framework*. Hung Q. Ngo, Anjum Shehzad, Saad Liaquat, Maria Riaz, Sungyoung Lee. Lecture Notes in Computer Science, Volume 3207, Jan 2004, Pages 672 – 681 *(EUC 04)*
9. Uzair Ahmad, Sungyoung. Lee, Mahrin Iqbal, Uzma Nasir, Arshad Ali, Mudeem Iqbal: Reflective Middleware for Location-Aware Application Adaptation. ICCSA (2) 2005: 1045-1054
10. Uzair Ahmad, Sungyoung Lee, Young Koo Lee, On Building a Reflective Middleware Service for Location-Awareness, RTCSA 2005, Hong Kong
11. Kim Anh Pham Ngoc, Young Koo Lee, Sung Young Lee. OWL-Based User Preference and Behavior Ontology for Ubiquitous System. Accepted to ODBase Conference. Nov 2005.
12. Kim Anh Pham Ngoc, Young Koo Lee, Sung Young Lee. Context Knowledge Discovery in Ubiquitous Computing. Accepted to ODBase Conference. Nov 2005.
13. Faraz Rasheed, Yong-Koo Lee, Sungyoung Lee, "Context Summarization and Garbage Collecting Context", Ubiquitous Web Systems and Intelligence 2005 http://www.orient-explorer.com/ICCSA/registration.html, Suntec Singapore, 9-12 May 2005, (SCIE)
14. Binh An Truong. Modeling and Reasoning about uncertainty in Context-Aware Systems. ICIS 05.
15. *Middleware Infrastructure for Context-aware Ubiquitous Computing Systems* . Technical Reports. February 2005. (153 pages)
16. *AutoMAGI - an Autonomic middleware for enabling Mobile Access to Grid Infrastructure* – Accepted for publication in International Conference on Autonomic and Autonomous Systems *(ICAS '05*)
17. *A Component-based Architecture for an Autonomic middleware enabling Mobile Access to Grid Infrastructure* - Accepted for publication in International Conference on Embedded and Ubiquitous Computing (*EUC '05*)

All the above papers can be found at our homepage http://ucg.khu.ac.kr

Ubiquitous Sensor Networks

Motivation for Virtual – IP Gateway

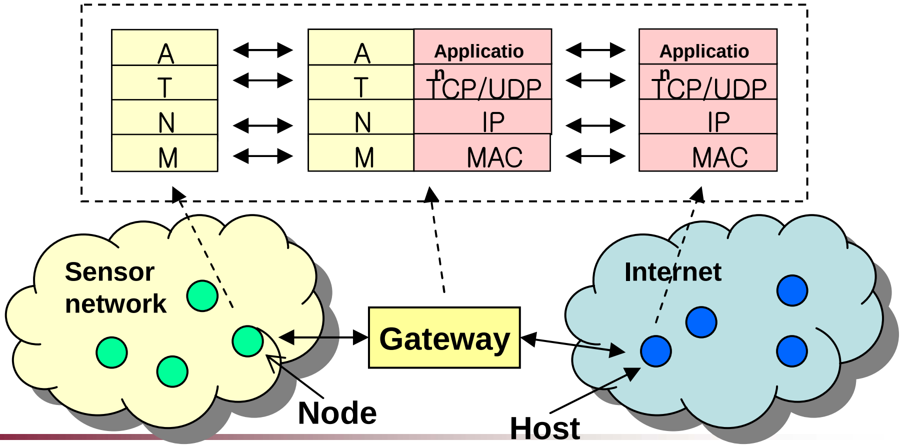
- Wireless sensor networks cannot have meaningful work without connecting with TCP/IP based network, such as Internet.
- Furthermore, in Next Generation Network paradigm all kinds of heterogeneous wireless networks and IP based Internet should be integrated into one network to provide ubiquitous services for users.



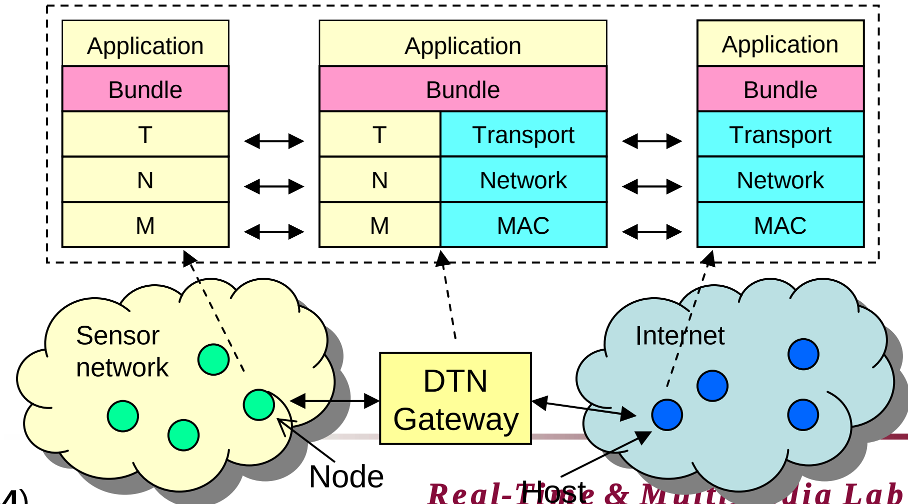
→ We analyze all existing related research work, then based on the analysis result we present the basic design principle and key idea for connecting sensor networks with TCP/IP network.

Related Work: Gateway-based Approach

- Application-level Gateway
  - Different protocols in both networks are translated in the application layer
  - Advantage: the communication protocol used in the sensor networks may be chosen freely.
  - Drawback : Internet users cannot directly access any special sensor node.

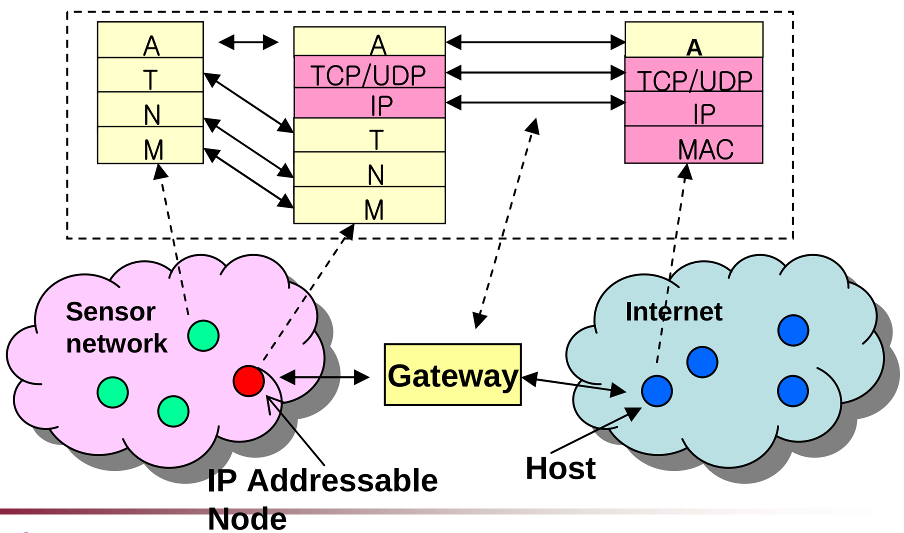


- Delay Tolerant Network
  - A *Bundle Layer* is deployed in both TCP/IP network and non-TCP/IP network protocol stacks to store and forward packets
  - Advantage: very easy to integrate with different heterogeneous wireless networks by deploying this *Bundler Layer* into their protocol stacks.
  - Drawback: comes from the deployment of *Bundle Layer* into existing protocols, which is a cost consuming job.

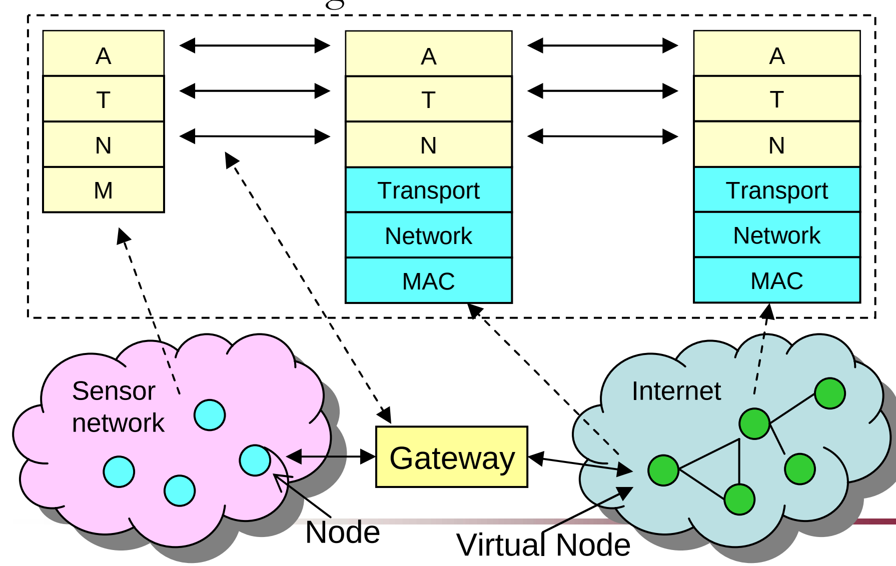


Related Work: Overlay-based Approach

- TCP/IP overlay sensor networks
  - Implement IP protocol stack on sensor nodes
  - Advantage: Internet host can directly send commands to some particular nodes in sensor networks via IP address.
  - Drawback: only can be deployed on some sensor nodes which have enough processing capability



- Sensor networks overlay TCP/IP
  - Sensor networks protocol stack is deployed over the TCP/IP and each Internet host is considered as a virtual sensor node
  - Advantage: Internet host can directly communicate with sensor node
  - Drawback: brings more protocol header overhead to TCP/IP network, loses the consistency with current IP based working model



Major Design Principle

- **Consistency:** The new approach should be IPv6 based, because it should have the consistency with the working paradigm of Next Generation Network.
- **Transparency**: By using IP based approach, non-system-designer users should be able to use services provided by sensor networks without knowing that "these services are provided by sensor networks."
- **Energy efficiency**: Sensor networks should be able to freely choose routing protocol to optimize energy efficiency and performance.
- **Direct accessibility**: Some sensor nodes should be able to be accessed and operated by Internet users directly by using IP address to identify them from others.

Major Design Principle

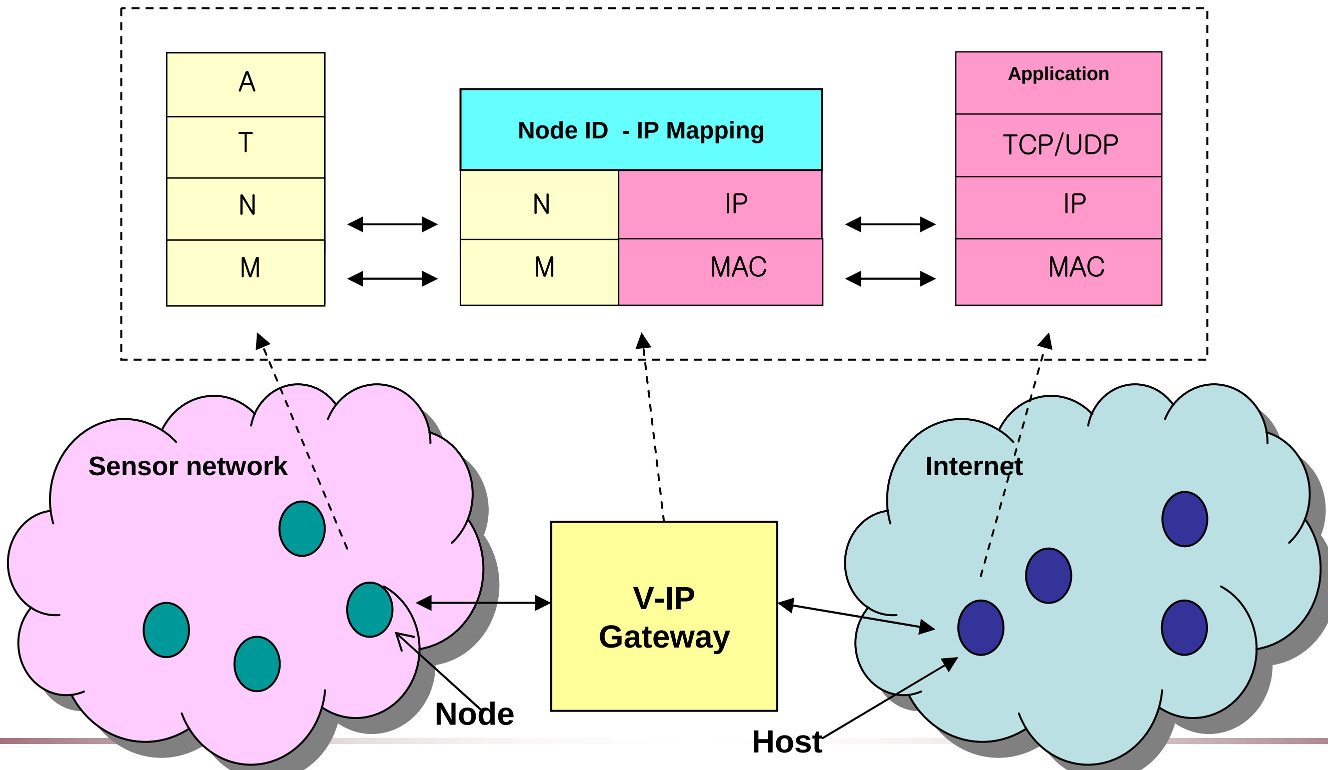
- **No overlay approach**: Because both of *TCP/IP overlay sensor networks* and or *sensor networks overlay TCP/IP* require modification on protocol stacks.

- **Easy integration between different sensor networks:** Several locating in different place's sensor networks should be easily integrated into one virtual sensor networks based on IP addresses.

- **Taking the advantage of knowing sensor node's label (ID) or location address:** Because once we can know the ID or location address of data source node it is very easy to build up the routing path between data source and gateway.
  - Data-Centric cannot provide the consistency with Internet working module

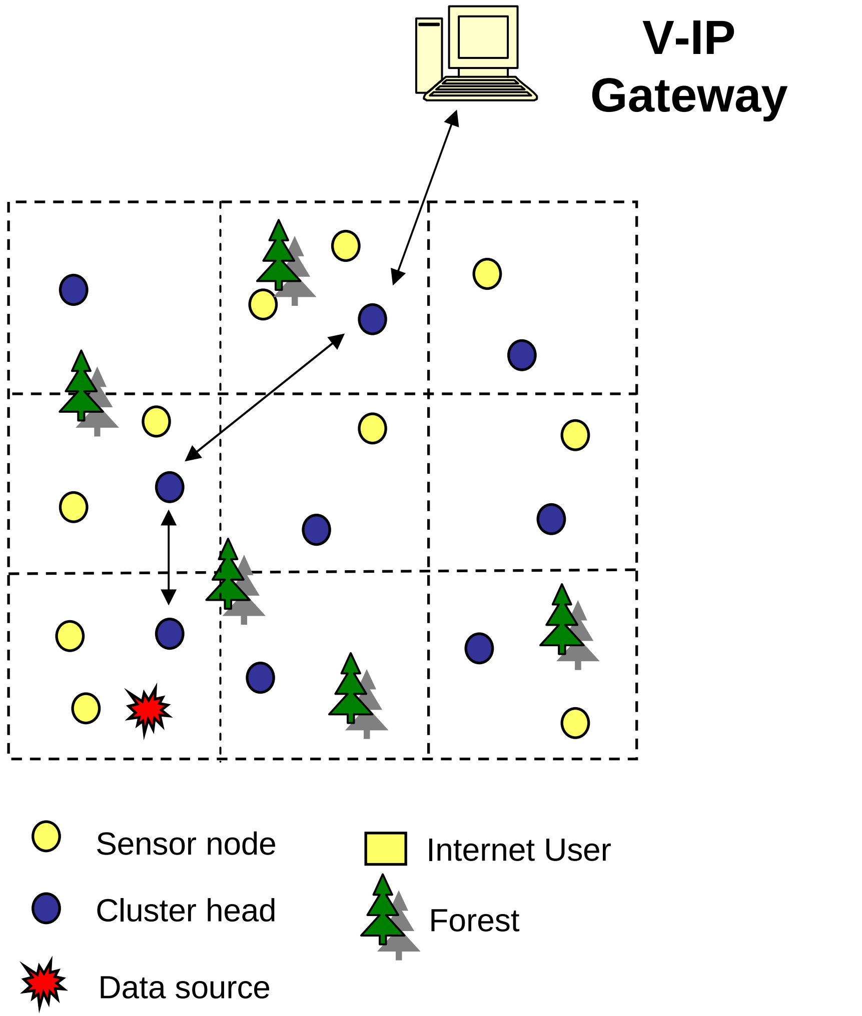
Key Idea of Virtual – IP Gateway

- Basing on Node-Centric or Location-Centric communication paradigm, mapping the node label (ID) or location address with IP address in gateway.
- The IP address will not be physically deployed on sensor node, but just store in gateway as a virtual IP address for Internet users.



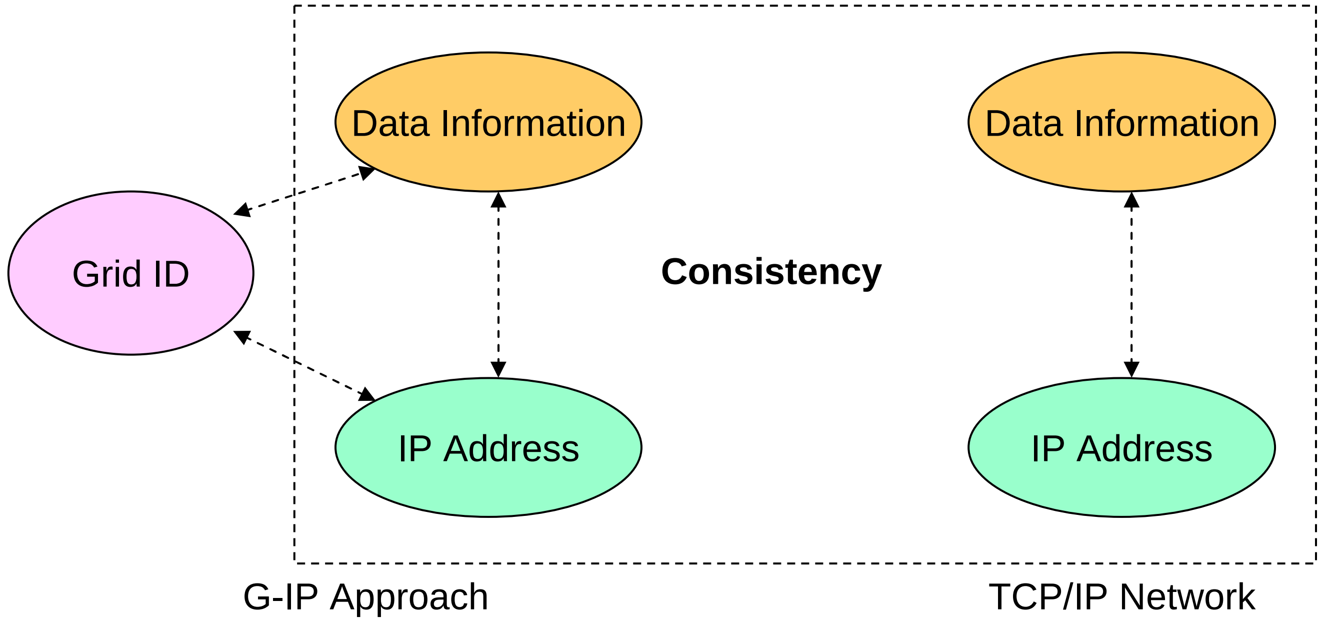
An Example: G-IP Approach(1/3)

- Active Data Discovery and Registration
  - After building up grids, each coordinator actively senses its local environment and registers the *Data Information* about the sensed data to gateway.
- Data Information & Grid ID & IP address Mapping
  - After active data discovery and registration, gateway can have *Data Information* and gird ID for whole sensor networks. In this step, we assign global unique IP address for each grid in gateway.



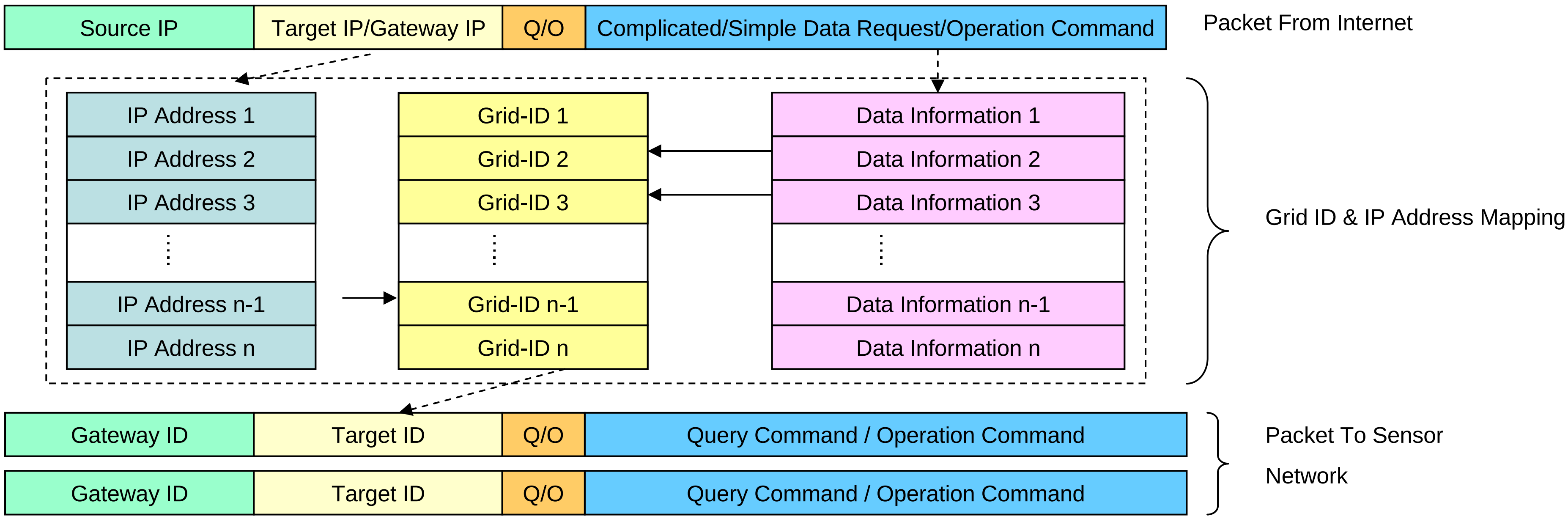
Consistent with Internet (2/3)

- **We are trying to use IP address instead of Grid ID.**
- **Because once we can hide the Grid ID from Internet users, we can** have the consistency between traditional IP based Internet and our G-IP approach.



Packet Translation (3/3)

- Four different kinds packet translations that can be done by *Grid ID – IP Address Mapping Layer.*
  - Directly operate coordinator
  - Directly Query based on IP address
  - Directly Query based on Data Information
  - Complicated Data Request from several coordinators



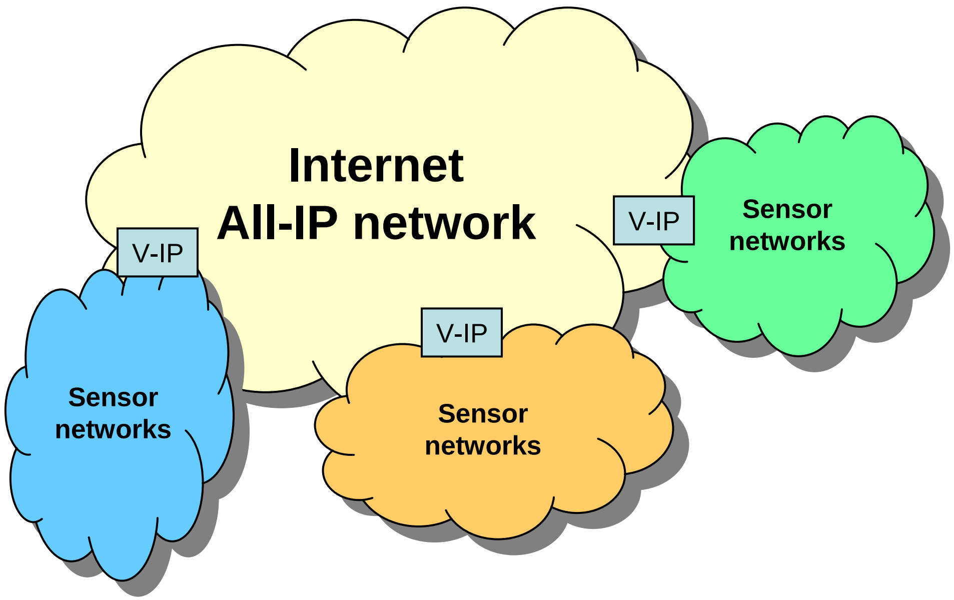
Comparison with Related Work

- Our solution can cover most of the benefits of related researches

Researches / Benefits	Application level gateways	Delay Tolerant Network	TCP/IP overlay sensor networks	Sensor networks overlay TCP/IP	Virtual IP gateway
Consistent with Internet working model	No	No	Yes	No	Yes
Transparent for Internet users	Yes	Yes	Yes	No	Yes
Freely choose routing protocol in sensor networks	Yes	Yes	No	Yes	Yes
Directly accessibility some special sensor node	No	No	Yes	Yes	Yes
Easy to integrate different sensor networks	No	Yes	No	Yes	Yes

Discussion: Integration of Different Sensor Networks

- Several sensor networks deployed in different locations
- These sensor networks may be using totally different routing protocols for their special applications
- All of these sensor networks have gateways which have *virtual IP addresse*s, it is very easy to integrate them into one virtual sensor networks.



Future Research Trend

- Internetworking between Wireless Sensor Networks and Wired TCP/IP network **towards Next Generation Network Paradigm**
- Integration of Heterogeneous Sensor Networks **for building up comprehensive Virtual Sensor Networks over wired/wireless networks**
- Autonomic Routing Service and Query Service **of Sensor Networks for Heterogeneous working situations and environments**
- Cross Layer Design for Energy Efficient & Real Time **Data Transmission over Heterogeneous Sensor Networks**

Publications

- **Shu Lei, Yang Jie**, **Sungyoung Lee,** "ETRI: A Dyanmic Packet Scheduling Algorithm for Wireless Sensor Networks", ETRSI 2004, Lisbon, Portugal, December 5-8, 2004
- **Shu Lei**, **Wu Xiaoling, Yang Jie, Sungyoung Lee,**"Maximizing System Value among Interested Packets While Satisfying Time and Energy Constraints", ICN'05, April 17-21, 2005 - Reunion Island, Springer-Verlag Lecture Notes in Computer Science, (SCIE)
- **Shu Lei, Wu Xiaoling, Yang Jie, Sungyoung Lee, Jinsung Cho,** "Two Ties Buffer and ETRI-PS Packet Scheduling Algorithm for Wireless Sensor Networks", GESTS International Transaction on Computer Science and Engineering, Vol.6 and No.1, ISSN: 1738-6438, http://www.gests.org, (Journal), May, 31, 2005
- **Wang Jin, Shu Lei, Wu Xiaoling, Sungyoung Lee, Jinsung Cho**, "A Load-balancing and Energy-aware Clustering Algorithm in Wireless Ad-hoc Networks", USN'05, Japan, Springer-Verlag Lecture Notes in Computer Science, (SCIE)
- **Shu Lei, Xu Hui, Jinsung Cho, Sungyoung Lee, Youngkoo Lee,** "Virtual – IP: Connecting Ubiquitous Sensor Networks with TCP/IP Network", submitted to ICOIN 2006, Japan, Springer-Verlag Lecture Notes in Computer Science, (SCIE)

CAMEL SensorOS

(Component-based Multi-thread Lightweight Sensor OS)

Introduction

- Sensor OS Research Trend

  - State Machine Based OS
  - Berkeley
  - Hard to portable

  - Distributed Services
  - EU
  - Initial Development Stage

  - Lightweight Multi-thread
  - University of Colorado
  - Hard to reconfiguration

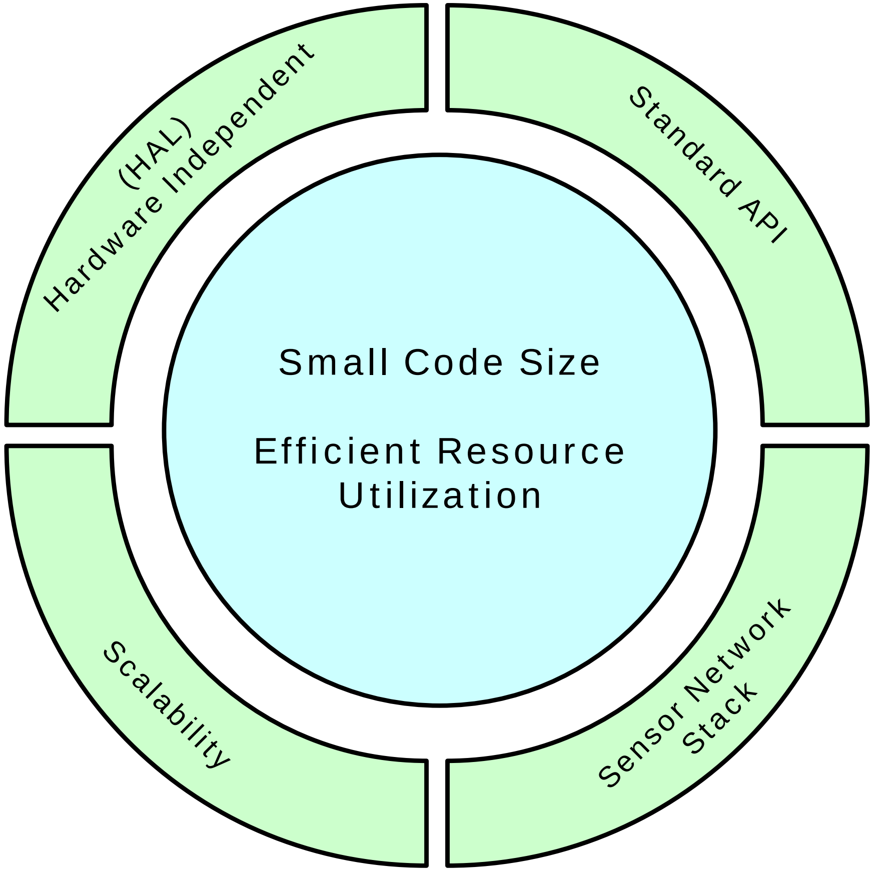
  - Scalability
  - ETRI
  - No component based OS

Introduction

- Common Consideration for Designing SensorOS
  - Efficient Resource Utilization

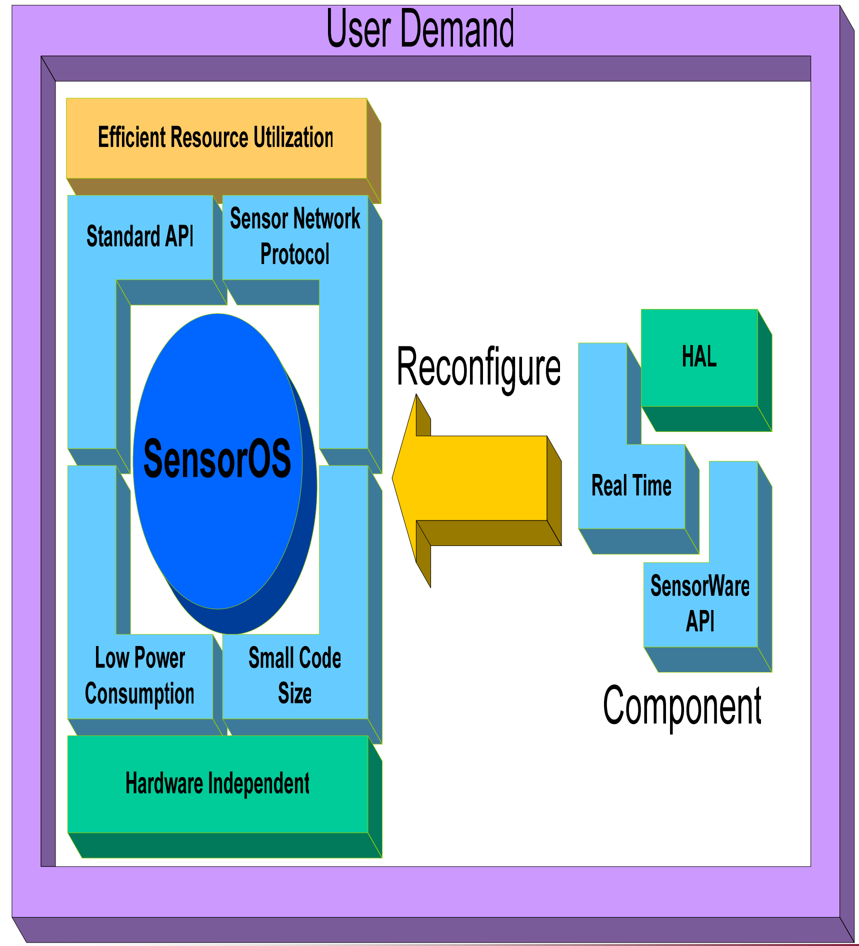
  - Small Code Size
  - Low Power Consumption
  - Standard API
  - Scalability
  - Sensor Network Stack

  - Hardware Independent (HAL)
    - Kernel for various MCU
    - Sensor Driver support



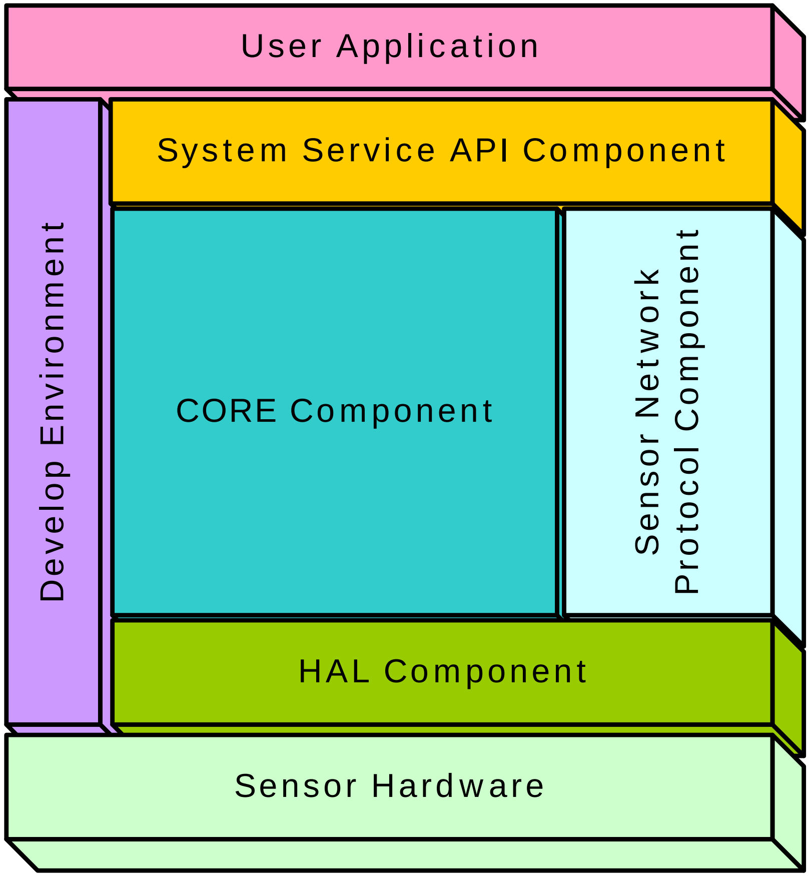
CAMEL SensorOS

- **Why Component-based Kernel ?**
  - Variety Environment
    - Non Risk Environment
      - Home, School, Shop . .
    - Risk Environment
      - Power plant, military . .
  - Variety H/W platform
    - Mote Kit, Nano-24 . .



- **Solution : Reconfigure**

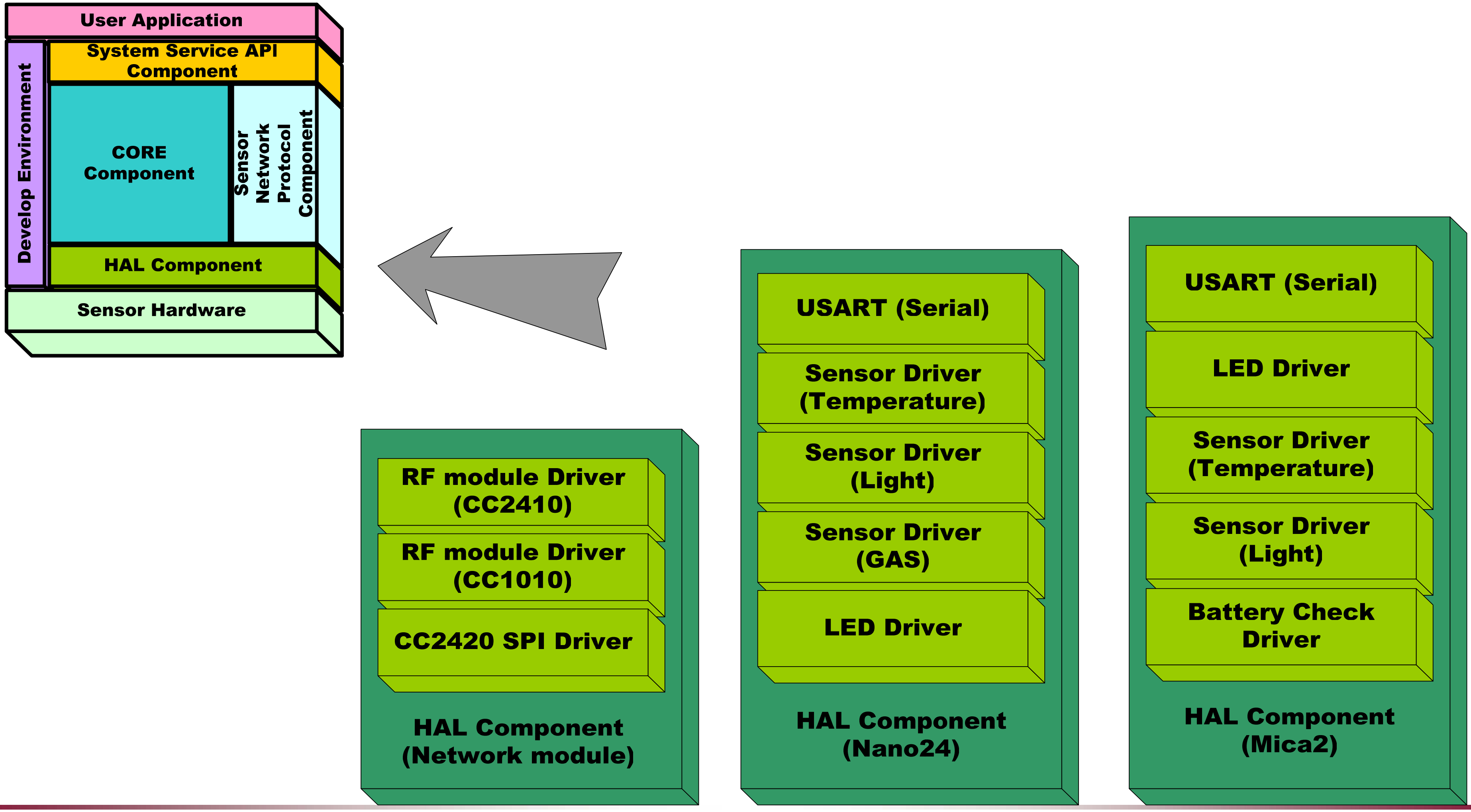
CAMEL Sensor OS Architecture



CAMEL SensorOS

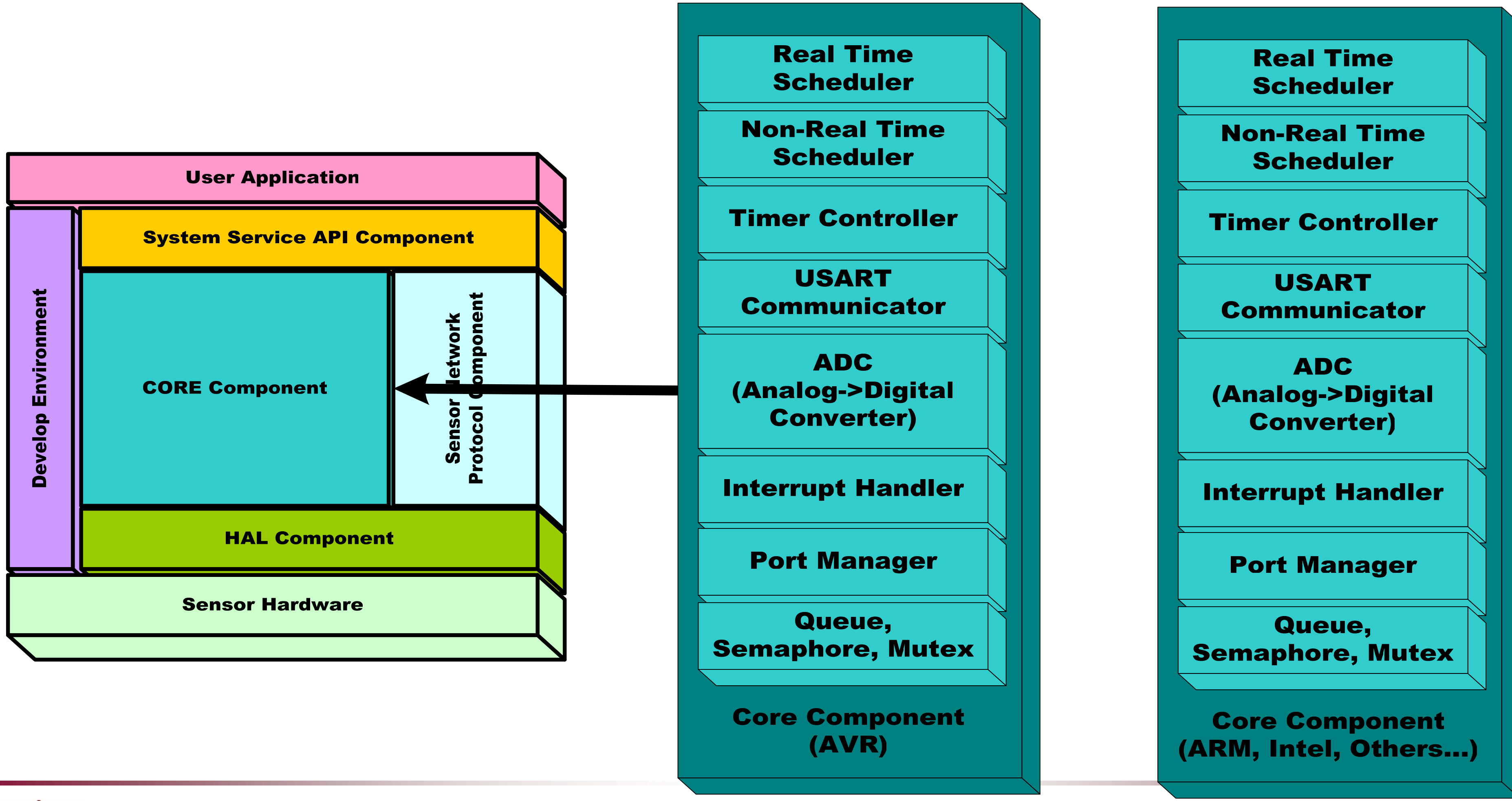
Hardware Abstract Layer Component

- HAL Component for various Hardware



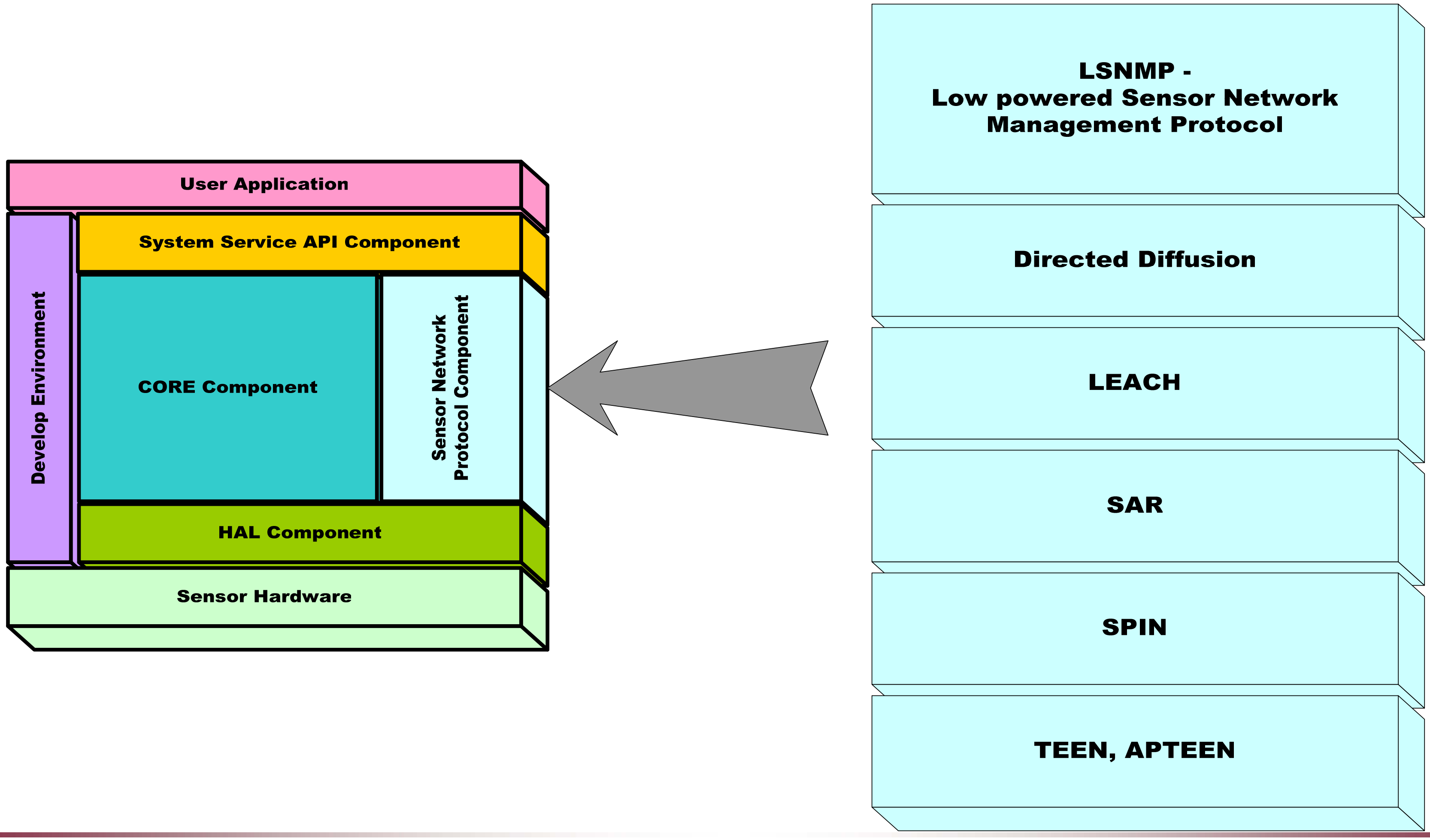
Core Component

- Core Component for various Environment



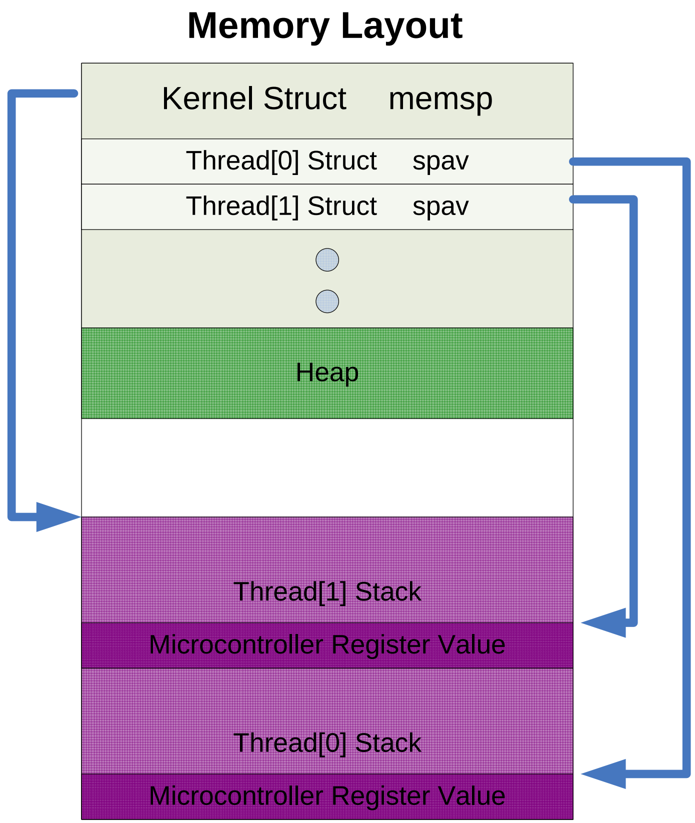
Sensor Network Protocol

- Sensor Network Protocol Component



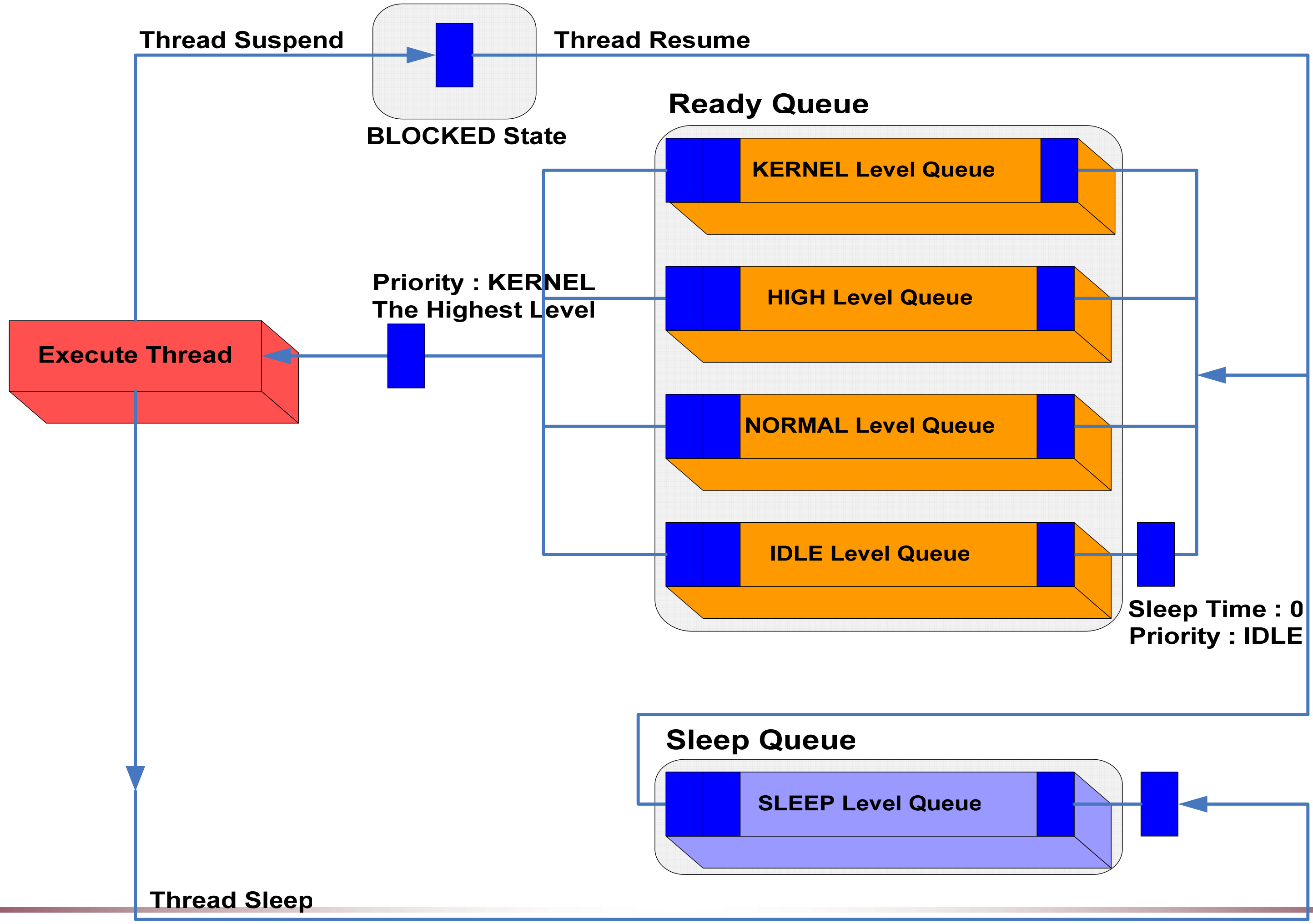
CAMEL - AVR Core Component

- Core Memory Layout
  - Multi-Stack
    - Stack per Thread
  - Variable Stack Size
    - Small stack (64B)
    - Normal stack (96B)
    - Large stack (128B)
  - Maximum 10 Threads
    - For System Safety



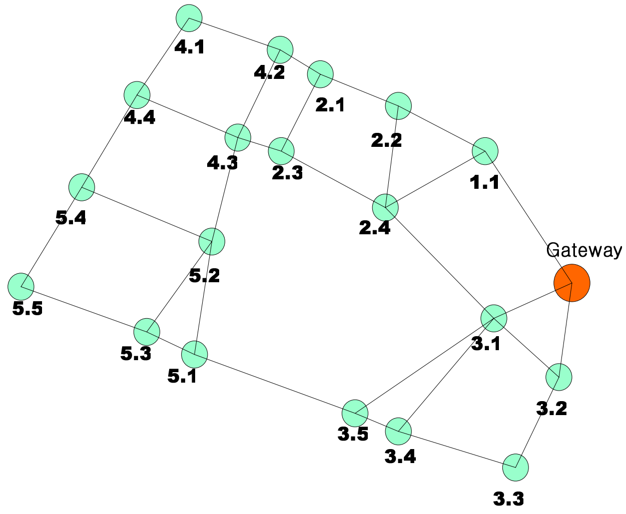
CAMEL - Non Realtime Thread Module

- Multi Level Queue



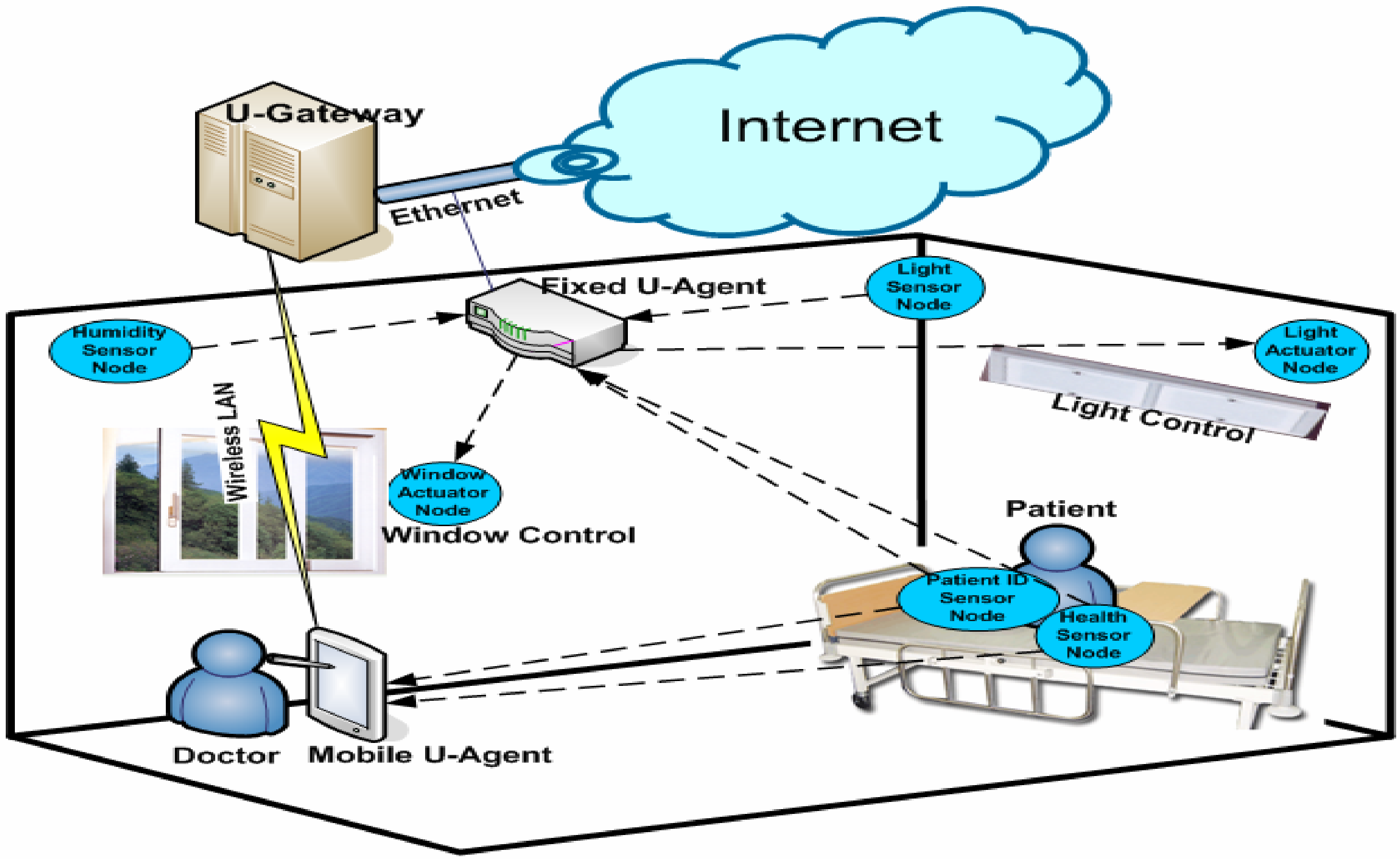
LSNMP

- Low Powered Sensor Network Management Protocol
  - Home Gateway Based Flat Routing
  - Autonomic Network Topology Management
    - Node-position discovery
    - Packet Scheduling
    - Addressing with Node-position
    - Autonomic Routing Tree
  - Message Types
    - Join-Request
    - Join-Accepted
    - Route Change



Applicable Field

- Hostpital Demo Scenario



Conclusion & Future Work

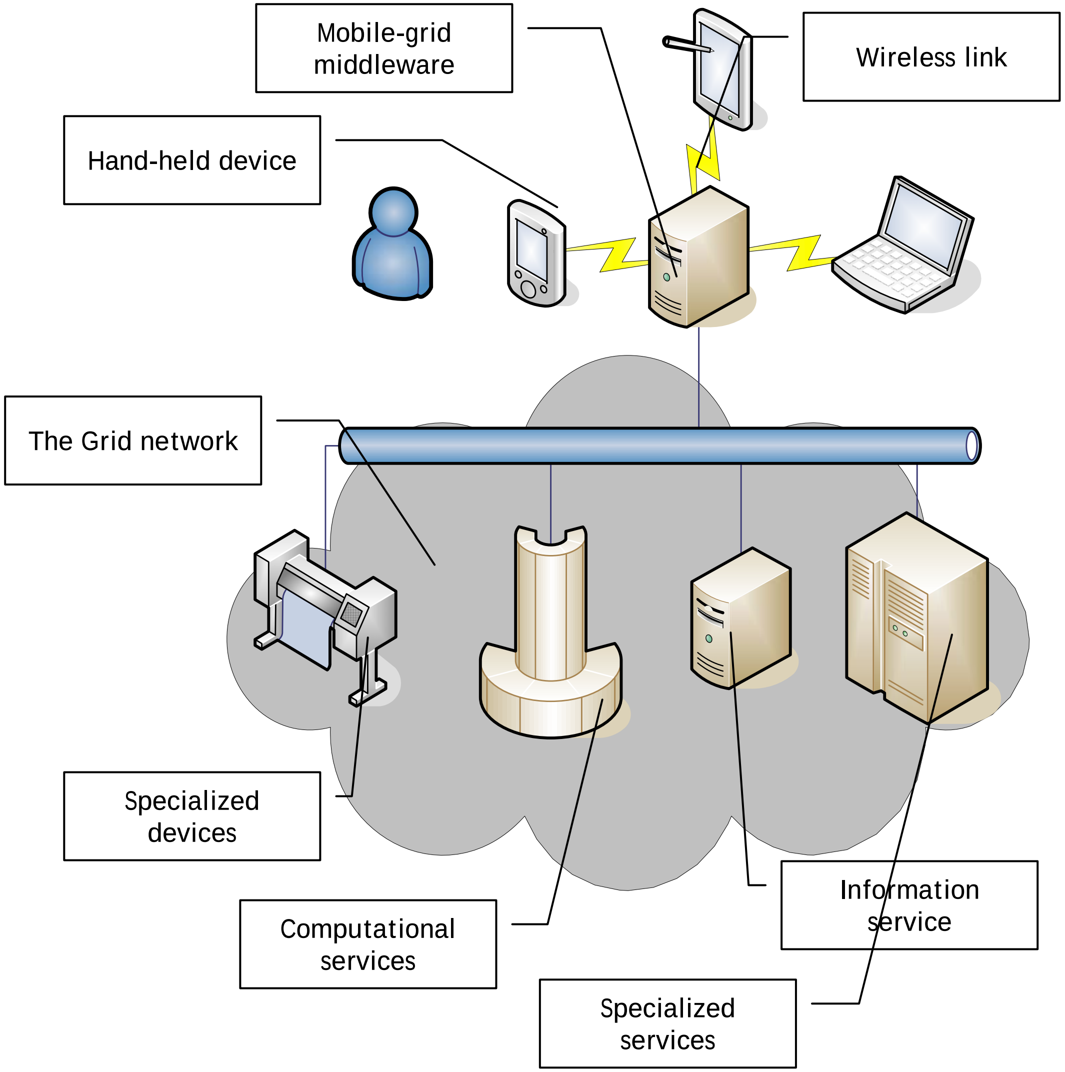
- We support
  - Kernel and Device Drivers for Various Hardware
  - Adaptation of various Sensor-Network environment
  - Low-Power Consumption
  - Standard API for C language

- Future Work
  - Support GUI Development Environment
  - Performance tuning and evaluation

MAGI ~
Mobile Access to Grid Infrastructure

Motivation - Accessing the Grid via a mobile device

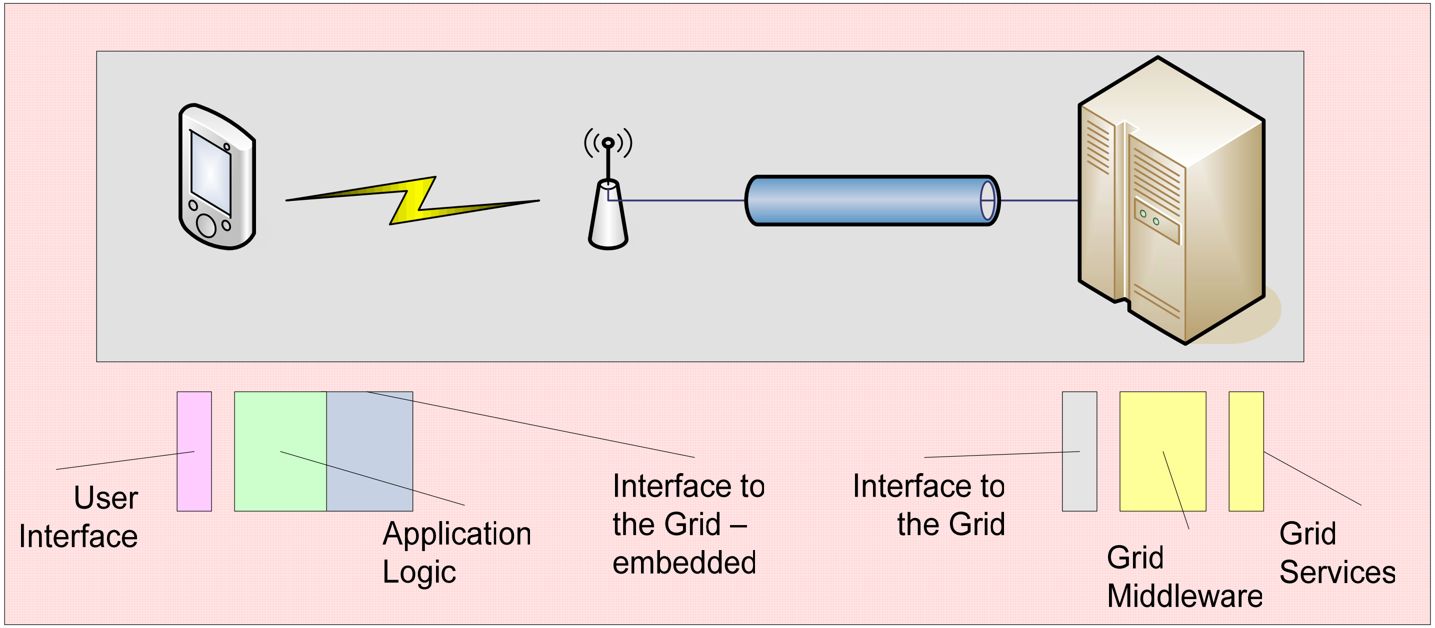
- Combining the benefits of both; the Grid and hand-held devices
  - Availability of resources and services in the Grid
  - Ubiquitous and flexible usage via hand-held devices
- Example
  - Patient Diagnosis
  - Sales Agent



Problem

- **Protocols of the Grid Middleware cannot be accessed directly by practical mobile applications**
  - Computational load on the client (application logic)
  - Communication load (use of the Grid interface)

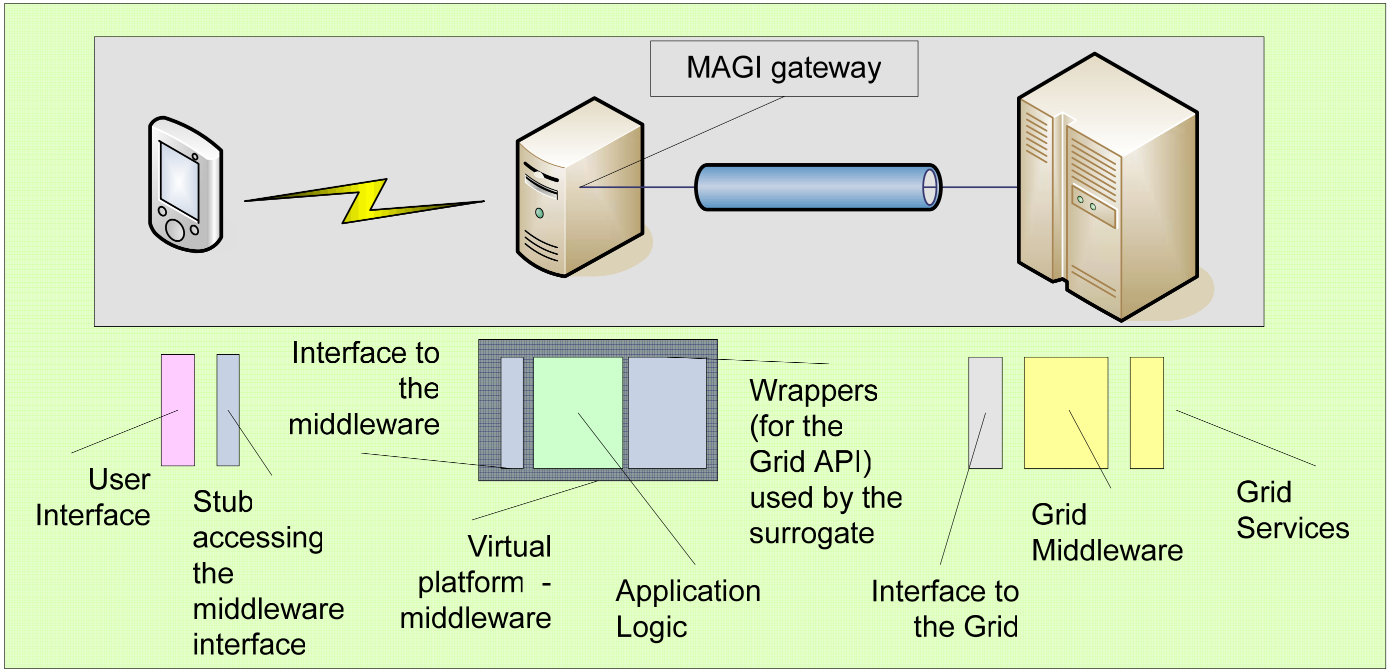
The Client device bears the load



Solution

- The application logic – in the form of a surrogate* - is downloaded to the middleware; a virtual host
- The surrogate via the MAGI gateway, then interacts with the Grid services to accomplish the desired task
- We reduce the computational load on the client and minimize the communication load between the client and the middleware

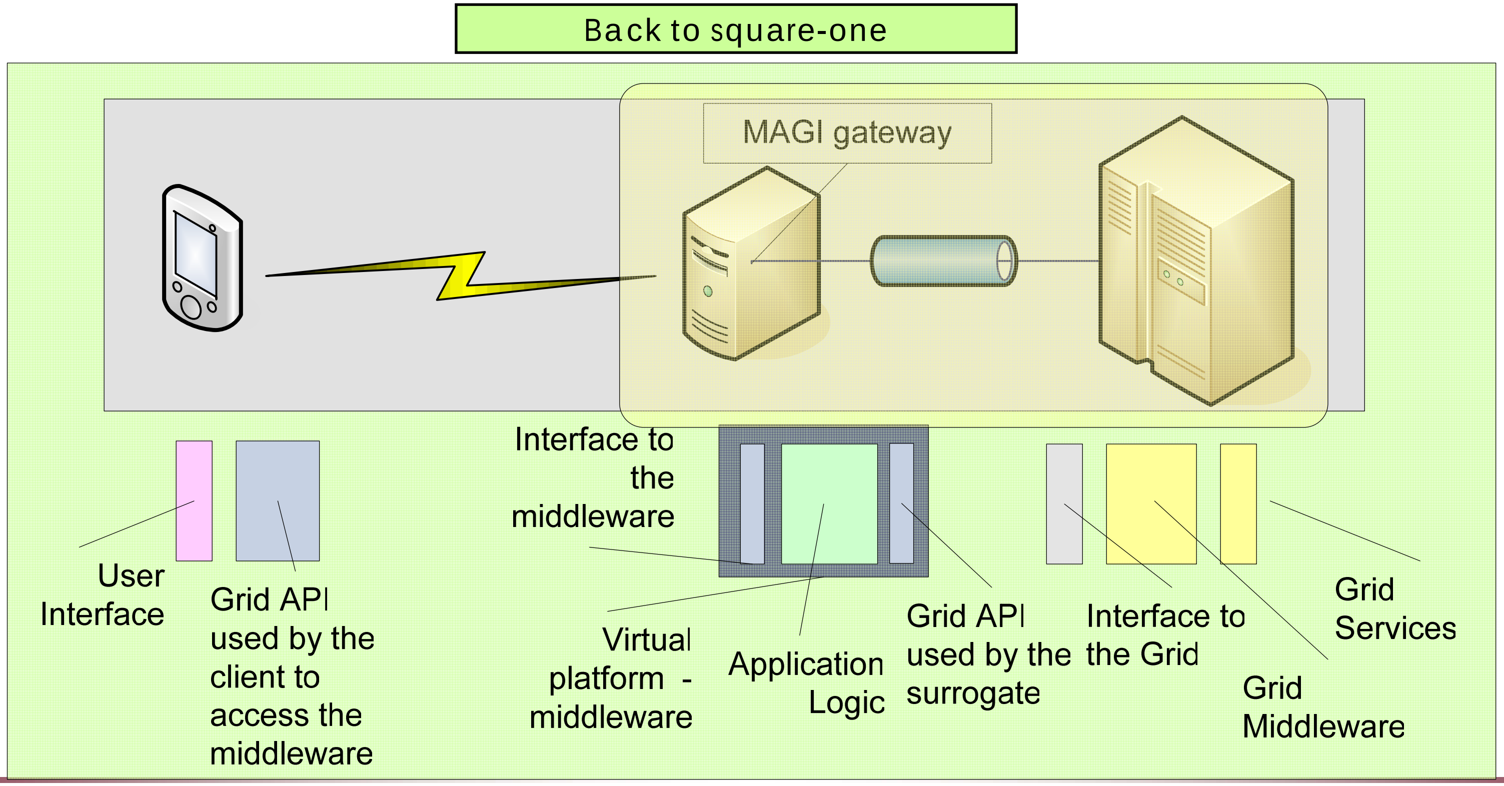
The Middleware bears the load



*Surrogate - One that takes the place of another; a substitute

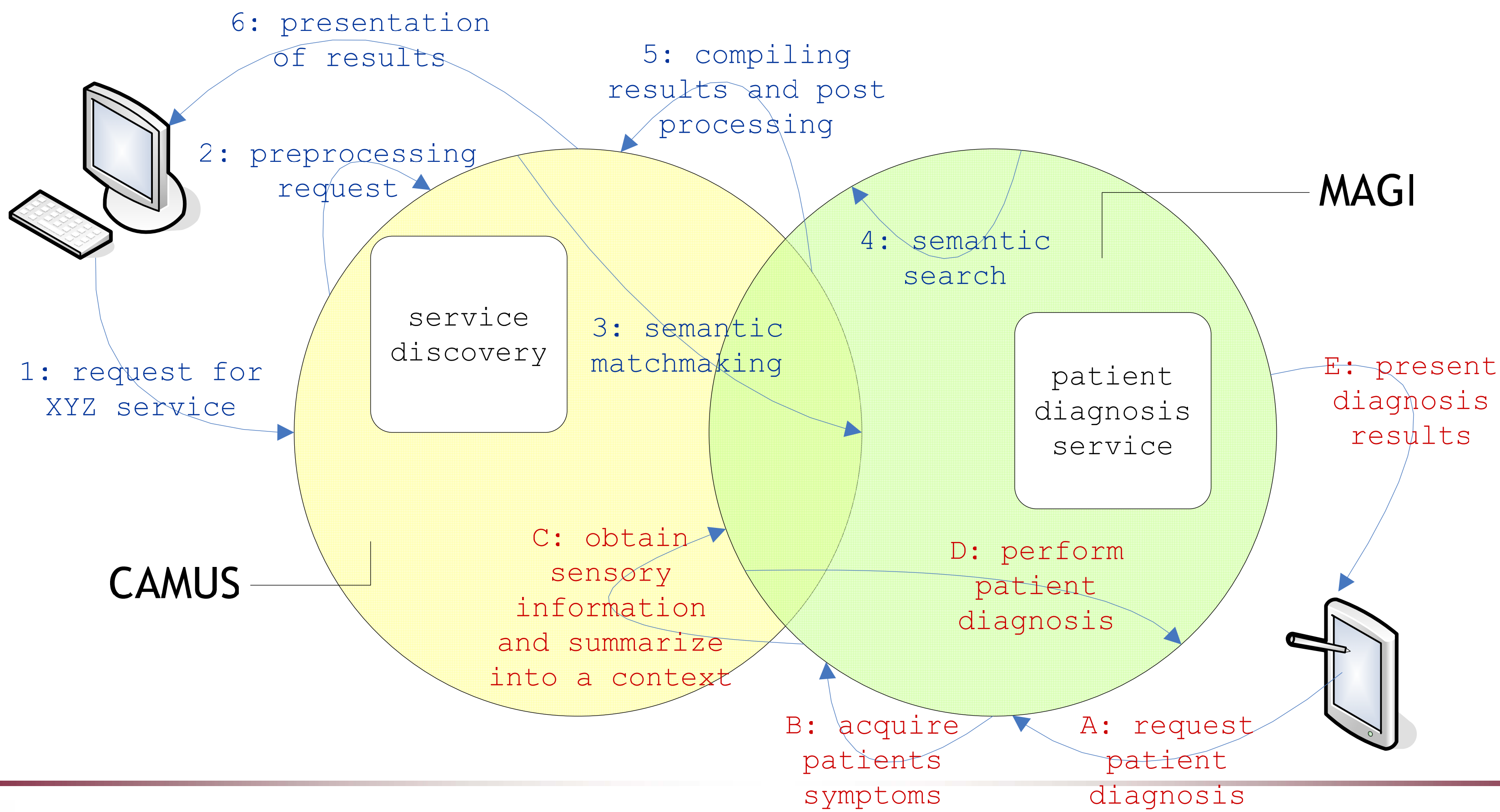
Why not be a part of the Grid?

- The middleware must adhere to the Grid standards
- The client has to use the Grid API to interact with the middleware
- We lose the advantage of minimum communication between the client and the middleware



MAGI & CAMUS

- **Belong to different domains but reinforce each other**
  - CAMUS ~ information gathering and context formation
  - MAGI ~ pooling Grid resources for hand-held devices



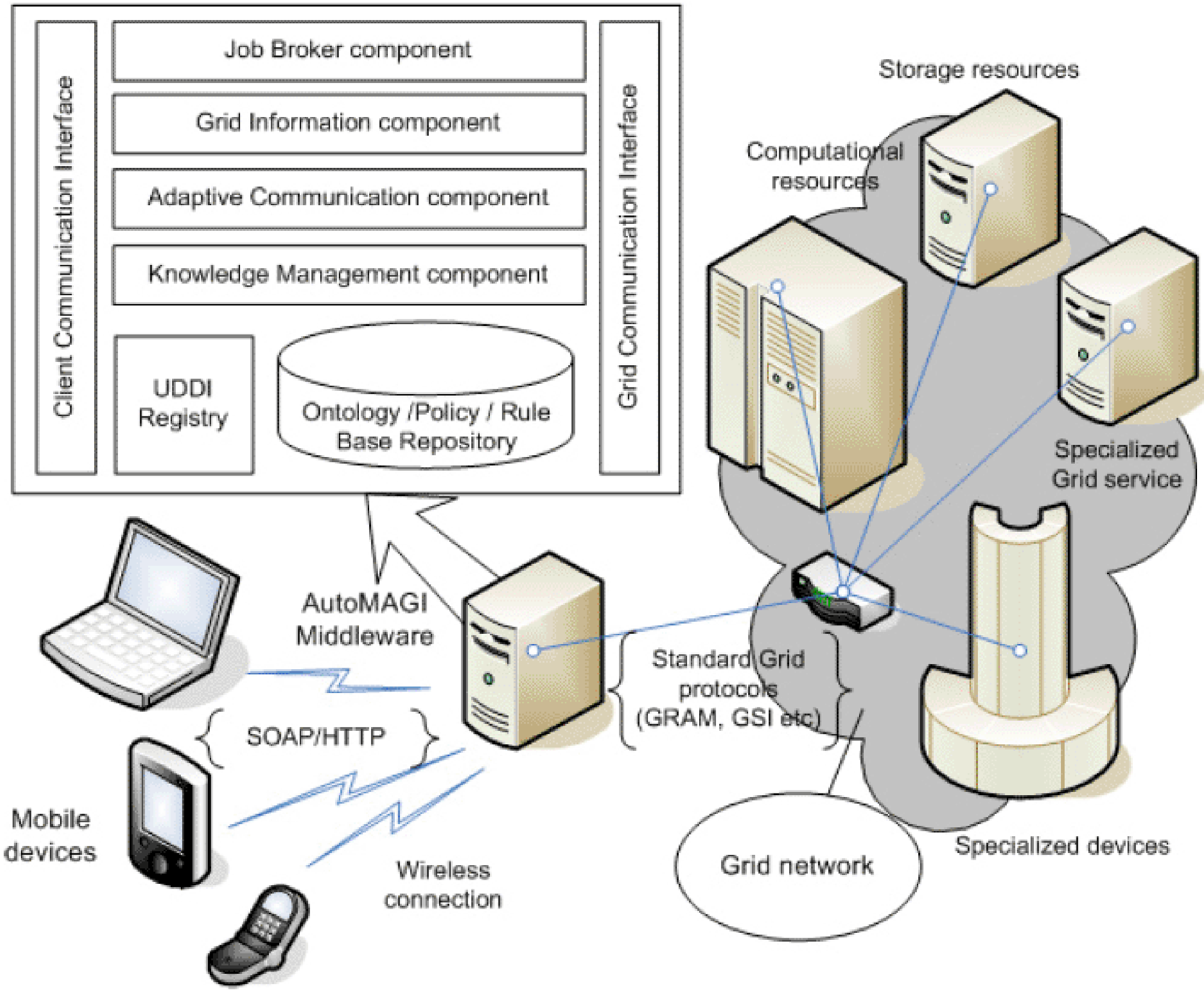
Challenges

- **Traditional client/server approach for Grid environments do not cater for issues of mobile devices**
  - Intermittent connectivity - Quality of service
  - Trust factor – security issues of mobile devices
  - Processes may be initiated by the client as well as the server
- **An application gateway/portal cannot achieve the same results**
  - Does not cater for the aforementioned issues
- **Hence the need of a middleware**

Problem statement

To devise an architecture for a middleware, enabling heterogeneous mobile/hand-held devices access to grid services

Deployment and Architecture



Research challenges

- **Job delegation to the grid**
  - Surrogate model
- **Security**
  - Lightweight trust evaluation model
  - Secure information exchange (encryption with keyword search)
- **Adaptive communication**
  - Programming model for software based fault tolerance
- **Autonomic middleware**
  - Configuration and reconfiguration of itself
  - Resolving anomalies with minimum possible human intervention

Related Work

- **Commodity Grid (CoG) Kits - portals**
  - Rapid application development (RAD)
  - Unlike MAGI, does not cater for Quality of Service (QoS) issues in wireless networks
- **Mobile agent paradigm for a middleware allowing mobile users' access to the Grid**
  - Incurs significant network performance overhead
  - Unlike MAGI, does not consider security aspects
- **Signal; mobile proxy-based architecture**
  - Unlike MAGI, mobile devices become part of the Grid Network
  - Proxy schedules the jobs

Progress to date

- **Conceived the architecture**
  – Research about the mentioned areas [in progress]
- **Implemented a prototype**
  – Tested the feasibility
    - w.r.t network communication overhead
    - Results show that the introduction of the middleware causes negligible overhead
- **Simulation tests for some modules**
  – [in progress]
- **Implementation of the middleware libraries**
  – [in progress]
- **Publicised our research**

Publications

1. Kalim U., Jameel H., Sajjad A. and Lee S.Y**., "Mobile-to-Grid Middleware: An approach for breaching the divide between mobile and Grid environments". In *Proc. 4th International Conference on Networking (ICN '05)*, 2005.**
2. Jameel H., Kalim U., Sajjad A. and Lee S.Y**., "Mobile-to-Grid Middleware: Bridging the gap between mobile and Grid environments". In *Proc. European Grid Conference (EGC '05)*, 2005.**
3. Sajjad A., Jameel H., Kalim U**., et al. "AutoMAGI – An Autonomic middleware for Mobile Access to Grid Infrastructure", In *Proc. of International Conference on Autonomic and Autonomous Systems, 2005.***
4. Sajjad A., Jameel H., Kalim U**. et al, MAGI –"Mobile Access to Grid Infrastructure: Bringing the gifts of Grid to Mobile Computing". In *Proc. 2nd International Conference on Grid Service Engineering and Management (GSEM 2005).***
5. Kalim U., Lee S. Y**., "Framework of an Application-Aware Adaptation Scheme for Disconnected Operations", Submitted for publication in *Proc. of Seventh Annual International Working Conference on Active and Programmable Networks, 2005.***

Summary and future work

- **An architecture for a middleware, enabling heterogeneous mobile/hand-held devices access to grid services**

- **Continue the research work on the aforementioned challenges**
  - Job delegation to the grid
  - Security
    - Lightweight trust evaluation model
    - Secure information exchange (encryption with keyword search)
  - Adaptive communication
    - Programming model for software based fault tolerance
  - Autonomic middleware
    - Configuration and reconfiguration of itself
    - Resolving anomalies with minimum possible human intervention
- **Implementation of the middleware libraries**

U-Security Research Group

Objective

- To develop secure methods for the Autonomic CAMUS system
  - Develop and Implement Security Architecture of Ubiquitous Sensor Networks and Mobile Grid Environment as a first step
- Our Objective is to improve the current state of security in the aforementioned systems through research on the underlying Security and Cryptographic Protocols

Current Research Work

- Security in CAMUS System
- MAGISec- A Security Infrastructure for Mobile-to-Grid Middleware
- Security Architecture for Ubiquitous Wireless Sensor Networks
- Trust Management in Ubiquitous and Autonomous Systems
- Cryptographic Schemes/Protocols
  - Key Management
  - Secret Sharing Schemes
  - Searching on Encrypted Data, etc

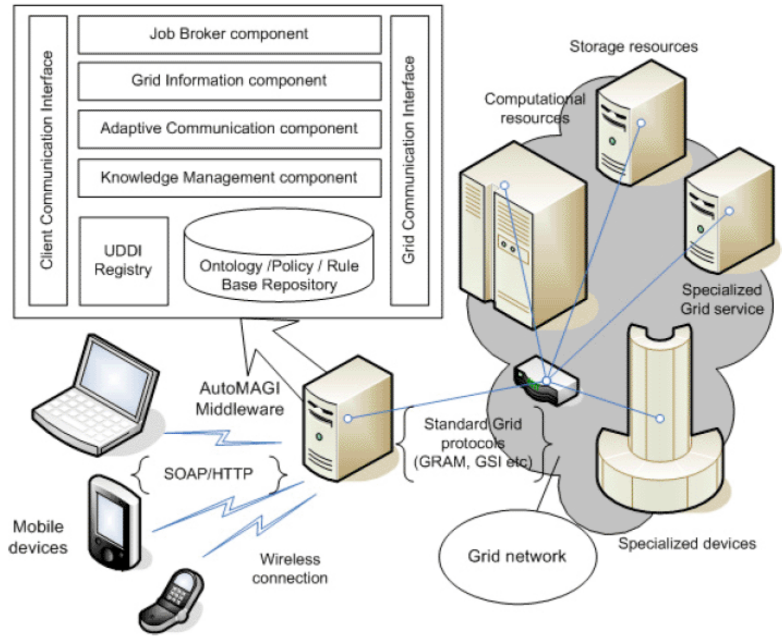
Security in Autonomic CAMUS

- **A large scale deployment of CAMUS requires a complete survey of the security issues involved**
- **At the lower level, we need to deal with the security of the sensors involved in detecting and obtaining raw data**
  - Data privacy should be maintained
- **At higher levels, User Privacy should be maintained**
  - Smart Office/Home Scenario: User does not want his private information to be viewed or monitored by an outsider
  - Communication of the user with the CAMUS system should not be understandable to an unauthorized individual
  - The CAMUS system should be resilient against outside attackers
  - Once Autonomous CAMUS is introduced, we need to deal with self-protection
- **Our goal is to address all these issues one by one to make CAMUS into a highly secure system**

Research Direction

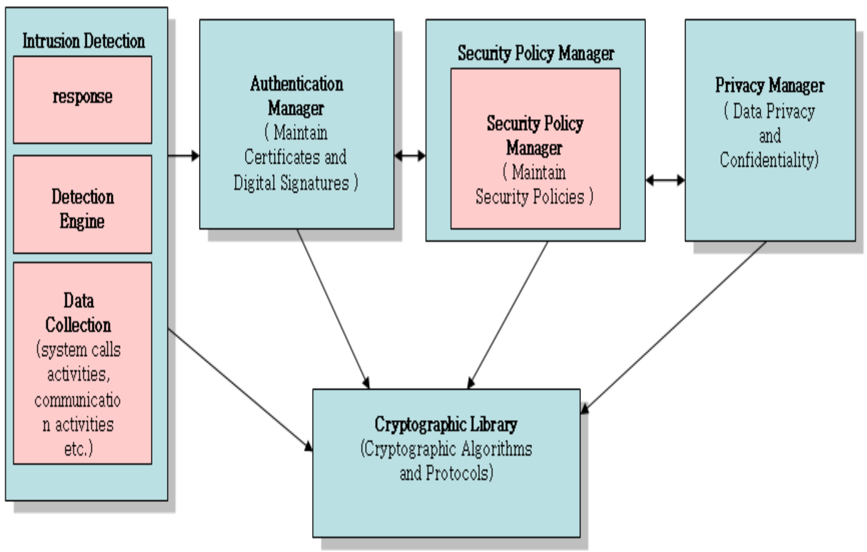
- **As a first step we worked on the security infrastructure of the two systems**
  - Mobile to Grid Middleware
    - Most of the users of CAMUS will be mobile clients interacting with the system
  - Ubiquitous Sensor Networks
    - The security of the underlying sensors layers is of utmost importance in CAMUS
- **Our experience with these systems will help us develop the Security Infrastructure of the CAMUS system**

MAGISec – Security Infrastructure for Mobile Grid(1)



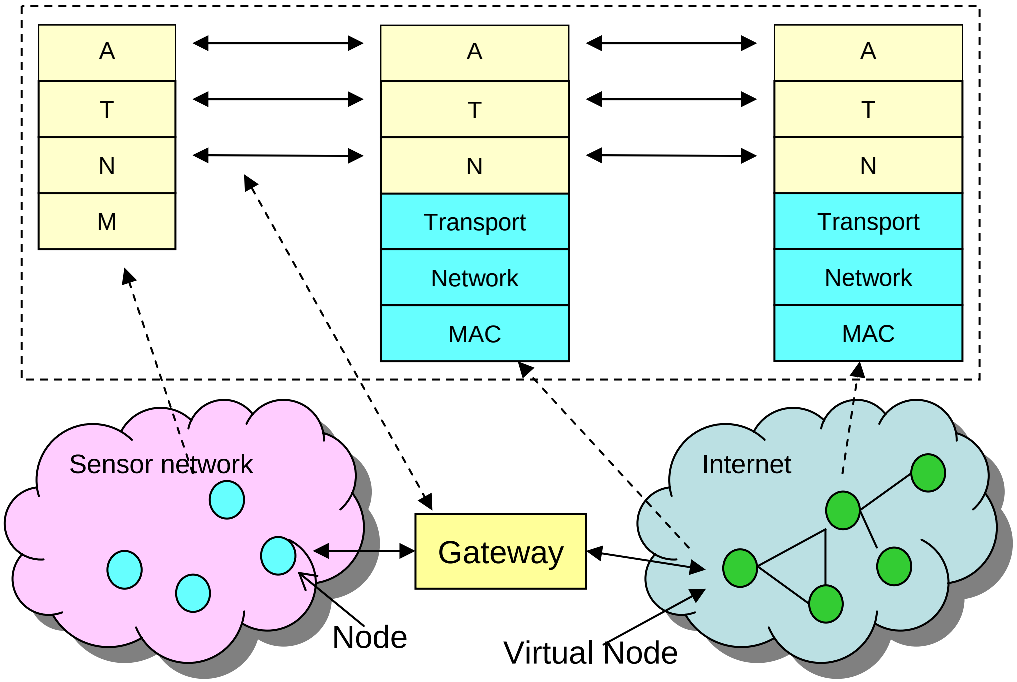
- This project is a part of MAGI, Mobile-to-Grid Middleware project
- The introduction of Grid Services to mobile clients promises enhanced capabilities to the user
  - A middleware brokers the communication between mobile client and the Grid
- Secure Authentication, Data privacy and integrity have the utmost importance
- Current Research Work focuses more on the security of Grid and less on the security of a Mobile-to-Grid Middleware

MAGISec – Security Infrastructure for Mobile Grid(2)



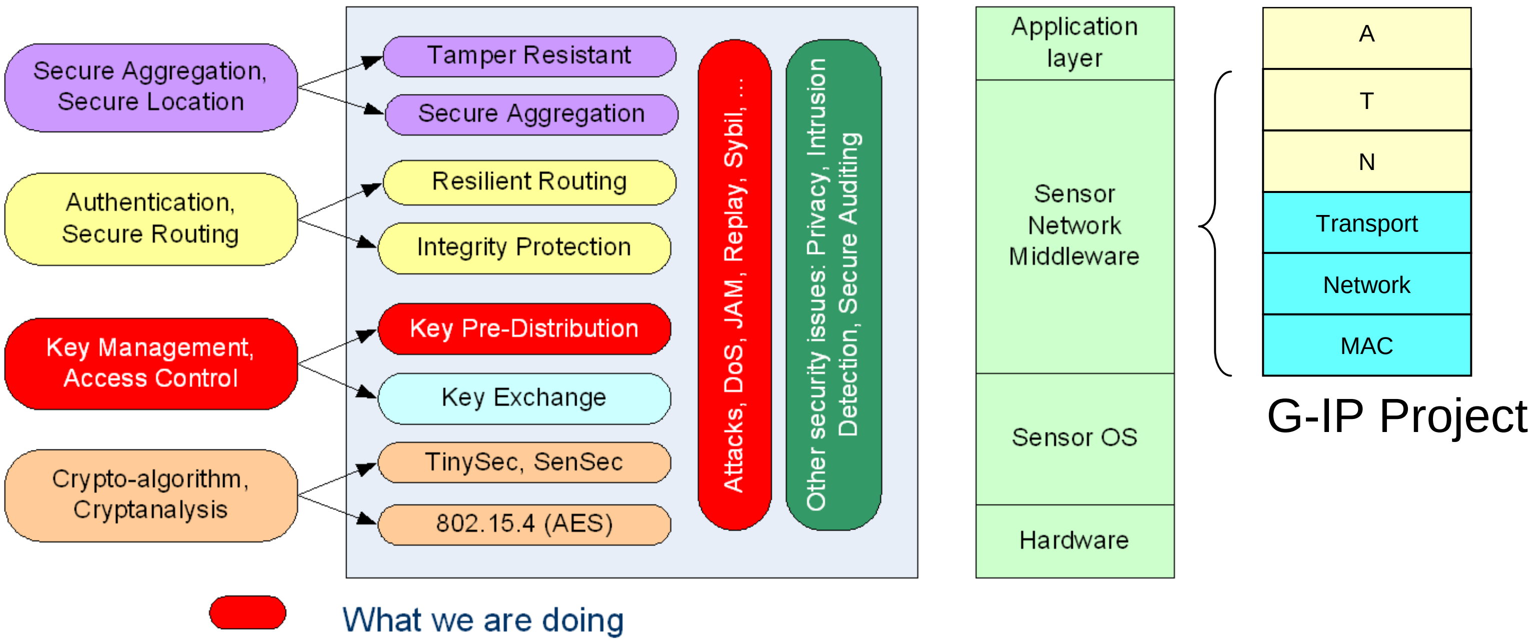
- The Cryptographic Library will contain the basic cryptographic algorithms and protocols
- These will be needed by the Authentication Manager, Security Policy Manager, the Privacy Manager and the Intrusion Detection Module
- The Security Manager and Authentication Manager have to interact as far as trust management is concerned
- For trust establishment the foremost step is authentication
- The Intrusion Detection module will have to interact with the authentication manager to determine the presence of intruders or to prevent intrusion

Security Architecture for Sensor Networks



- This Security Infrastructure supports Security for G-IP Project (Grid ID – IP Address) (Slice 65)
- Provide Secure Aggregation, Secure Location, Authentication, Secure Routing, Key Management, Access Control, and Cryptography for Sensor Networks.
- Currently, we are working on Key Management and Access Control

Security Architecture for Sensor Networks



- Security must be justified and ensured before the large scale deployment of sensors
- Current research on wireless sensor networks does not address this problem completely
  - The systems rectify a limited number of security issues
- Figure shows the security issues rendered in every layer of the protocol stack
- We will deal with the problems one by one and build appropriate security mechanisms

Trust Management in Ubiquitous Systems

- **Trust Management**
  - Trust is needed between participants to support collaborative tasks in ubiquitous and uncertain environments
  - **Example:** Routing Messages in Ad hoc Wireless Networks
    - A sender node must rely on intermediary nodes to send the message to the intended destination
    - Generally the intermediary nodes have no a priori relationship with the sender which they might have never encountered before
    - Forwarding messages causes battery and processing
    - Why should a sender rely on such nodes to help?
    - If multiple path exist, which path should be the most appropriate
    - These decisions are based on the degree of "trust" the sender has on the nodes
      - Based on past experience and observations and their reputations

Trust Management in Ubiquitous Systems

- Mutual Trust is crucial for ubiquitous devices to Share information
- Before interaction, two entities can calculate how much trust they put on each other
  - Decide the access privileges according to this trust value
- Propose a trust evaluation model for collaborative tasks in ubiquitous systems
- Current Trust Models do not discuss a complete modeling of trust characteristics and are too cumbersome to evaluate

Cryptographic Schemes and Protocols

- Every Secure System requires an efficient use of the underlying Cryptographic Algorithms, Schemes and Protocols
- To build a Secure Architecture we need to develop the core Cryptographic Protocols best suited for our Scenarios
- Current Research on Cryptographic Schemes/Protocols
  - Key Distribution and Management in Wireless Sensor Networks
    - Devise a protocol that is secure and energy efficient
  - Secret Sharing Schemes
    - Formulate Robust Secret Sharing Schemes with applications to Sensor Networks and Mobile Grid Environments
  - Search on Encrypted Data
    - Develop efficient schemes to overcome the drawbacks of current protocols on Searchable Encryption

Publication Record

- Hung Le Xuan, Sungyoung Lee and Young-Koo Lee, "A Key-Exchanging Scheme for Sensor Networks", The 2005 IFIP International Conference on Intelligence in Communication Systems (INTELLCOMM'05), Canada. October 17-19, 2005 (to appear on LNCS Springer Verlag)
- Hassan Jameel, Sungyoung Lee and Young-Koo Lee "A Secret Sharing Scheme for Preventing the Cheaters from Acquiring the Secret" submitted to SKLOIS Conference on Information Security and Cryptology
- Hassan Jameel, Sungyoung Lee and Young-Koo Lee "Secure Information Exchange in a Mobile-to-Grid Middleware Environment" submitted to 3rd International IEEE Security in Storage Workshop
- Hassan Jameel, Hung Le Xuan, Sungyoung Lee and Young-Koo Lee "A Vector Space Based Trust Evaluation Model for Ubiquitous Systems"3rd International IEEE Security in Storage Workshop

Future Work and Plan

- Design A Security Infrastructure for CAMUS based on Security Architecture proposed for Mobile Grid and Sensor Networks
- Further Develop and Implement the Mobile Grid Middleware and Sensor Network Security Infrastructure
- Learn from our experience with these secure subsystems and build a highly secure infrastructure for CAMUS
- Research and Design Secure and Efficient Cryptographic Protocols for the aforementioned Systems

Conclusion

Conclusion

- Brief Introduction about RTMM LAB
- Current Research Activities
    - Context-aware Middleware for Ubicom Systems
    - Knowledge Processing
    - Service Discovery & Delivery
    - Autonomous Computing
    - Ubiquitous Sensor Network
    - Mobile Access to Grid Infrastructure
    - Security
- Hope for Collaboration & Inspiration
  – Visit us at: http://oslab.khu.ac.kr

The End

Thank you for your participation!

Prof. Sungyoung Lee

sylee@oslab.khu.ac.kr

RTMM LAB

Computer Engineering Dept.

KyungHee University.