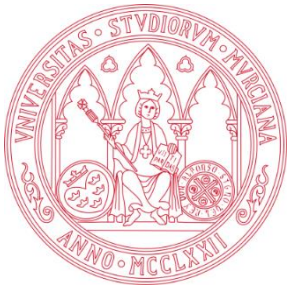


UNIVERSIDAD DE MURCIA
Facultad de Informática

A Proposal for User's Privacy Management in Context-Aware Systems

Propuesta para la Gestión de la Privacidad de los Usuarios en Sistemas Sensibles al Contexto

PhD Thesis

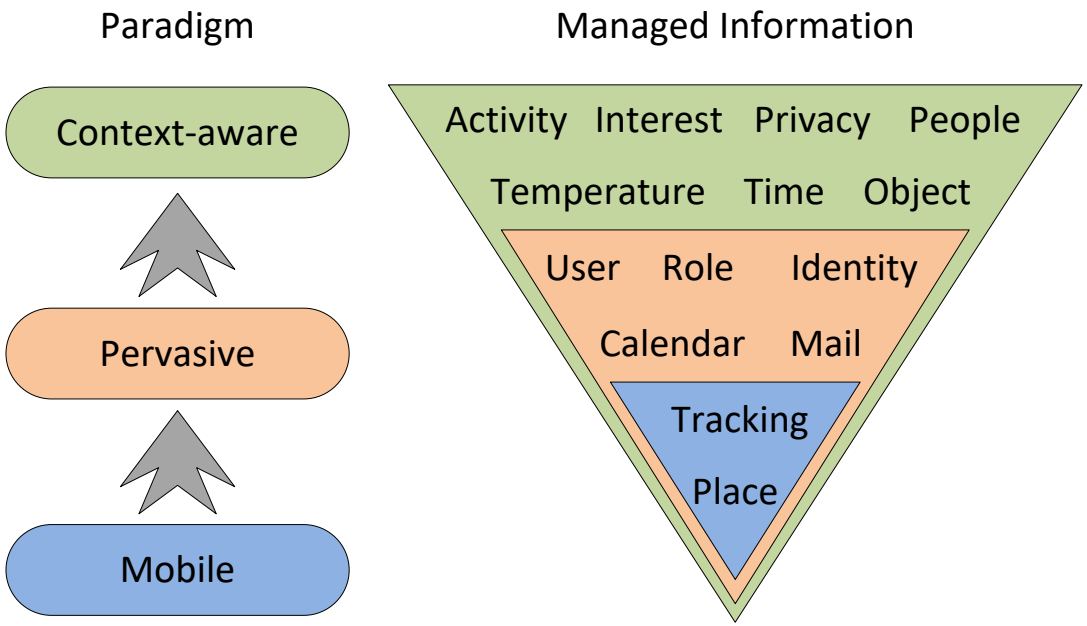
Author
Alberto Huertas Celdrán

Advisors
Dr. Félix J. García Clemente
Dr. Gregorio Martínez Pérez
Dr. Manuel Gil Pérez

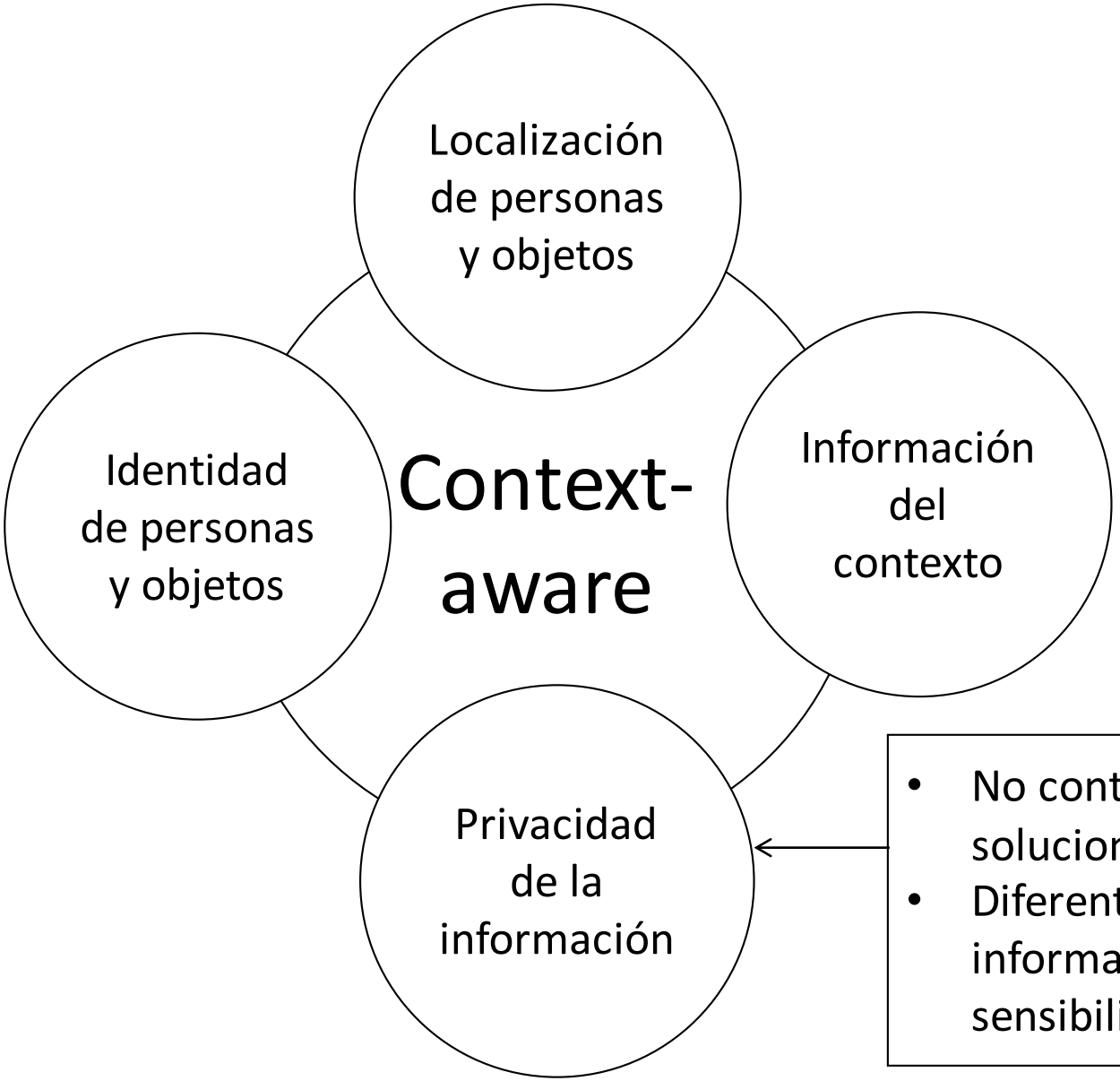
Murcia, February 2017

Introducción y motivación

- La evolución de las tecnologías ha incrementado la **complejidad** de los Sistemas de Gestión de la Información (IMS):
  - Gestionar gran cantidad de información heterogénea
  - Evaluar y proteger la privacidad de la información sensible
  - Considerar la existencia administradores independientes
  - Gestionar diversos componentes con diferentes localizaciones



Introducción y motivación



- No contemplado por muchas soluciones → Objetivo
- Diferentes tipos de información y niveles de sensibilidad

Introducción y motivación

Incremento de la complejidad de la gestión de la información → Automatizar los procesos de gestión

- Automatización de los sistemas sensibles al contexto para la ayuda, entre otras cosas, a:
  - Reducir la complejidad de la gestión de componentes heterogéneos
  - Proteger la seguridad y privacidad de los sistemas y usuarios
  - Reducir retardos en los procesos de gestión
  - Evitar posibles fallos humanos o mal configuraciones

Objetivo y retos de investigación asociados

Objetivo: Definición de sistemas sensibles al contexto que permitan proteger la información de los usuarios y controlar el comportamiento de los recursos de los sistemas

- Subobjetivos planteados en la tesis:
  - Gestión de la privacidad de la información de los usuarios
  - Gestión del comportamiento de los recursos de red
- Retos
  - Gestión automática de la privacidad en sistemas sensibles al contexto
    - Compartir información entre usuarios y servicios
    - Considerar privacidad en escenarios intra- e inter-contexto
    - Políticas sensibles al contexto para gestionar la privacidad
    - Permitir a los usuarios gestionar sus políticas de privacidad
    - Ayudar a los usuarios recomendando políticas de privacidad

Objetivo y retos de investigación asociados

Objetivo: Definición de sistemas sensibles al contexto que permitan proteger la información de los usuarios y controlar el comportamiento de los recursos de los sistemas

- Subobjetivos planteados en la tesis:
  - Gestión de la privacidad de la información de los usuarios
  - Gestión del comportamiento de los recursos de red
- Retos
  - Gestión eficiente y automática de los recursos de red teniendo en cuenta la información del contexto
    - Localización de la infraestructura, el estado de la red o el número de usuarios activos para garantizar consumos eficientes
    - Movilidad de los usuarios y estadísticas de red para garantizar la calidad de la experiencia (QoE) de los usuarios
  - Integrar técnicas de virtualización y redes definidas por software

Estructura de la tesis

Privacidad intra-contexto

Protección de la privacidad en escenarios intra-contexto

Control de la localización e identidad de usuarios con respecto a otros usuarios y servicios

Privacidad inter-contexto

Protección de la privacidad en escenarios inter-contexto

Perfiles para proteger la privacidad de la información de los usuarios cuando éstos se mueven por diferentes contextos

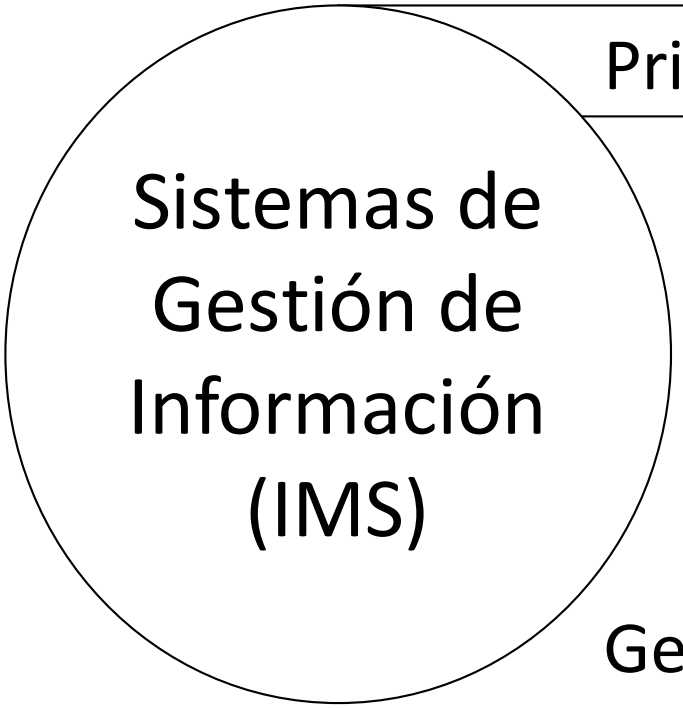
Gestión comportamiento

Reconfiguración de elementos de red

Configuración dinámica de los recursos e infraestructura de red teniendo en cuenta la información del contexto

Usuarios | Servicios | Perfiles | Eficiencia energética | Calidad de experiencia | Conclusiones | Publicaciones

Líneas de investigación



Privacidad intra-contexto

Privacidad inter-contexto

Gestión comportamiento

Proteger la localización de los usuarios

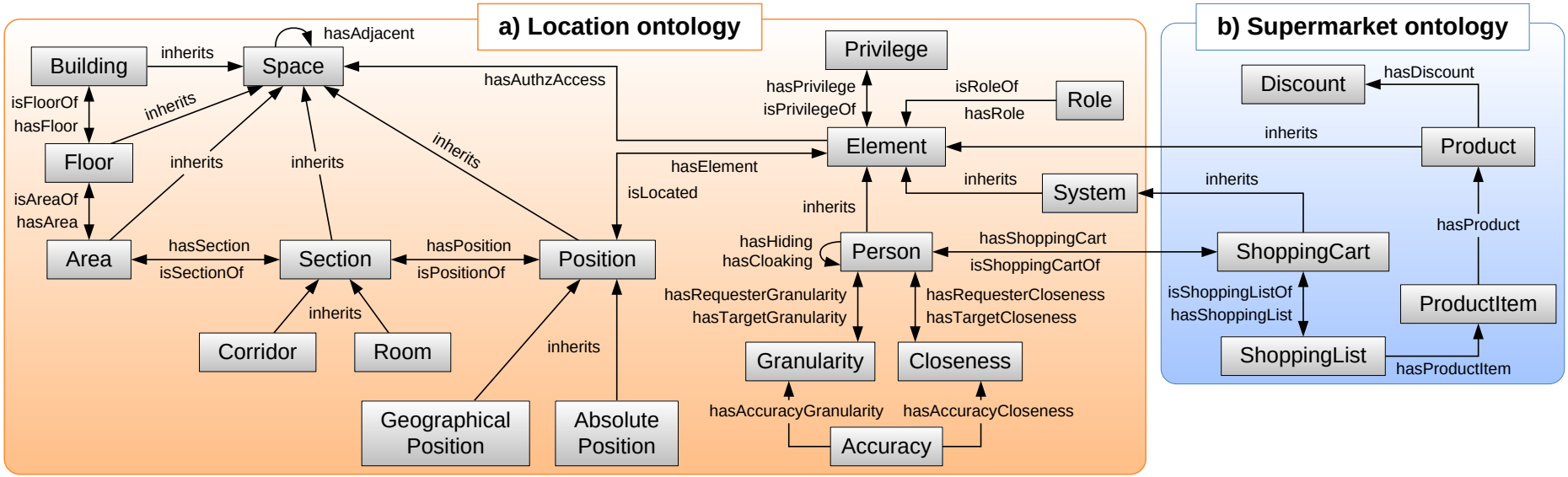
- Necesidad de proteger la localización de los usuarios con respecto a otros usuarios

Framework que permite desarrollar aplicaciones sensibles al contexto teniendo en cuenta la privacidad de la localización los usuarios

- Localización de personas y objetos cercanos
- Rutas hacia determinadas personas, objetos o lugares
- Autorización para permanecer en determinados lugares
- Información del contexto en el que está el usuario

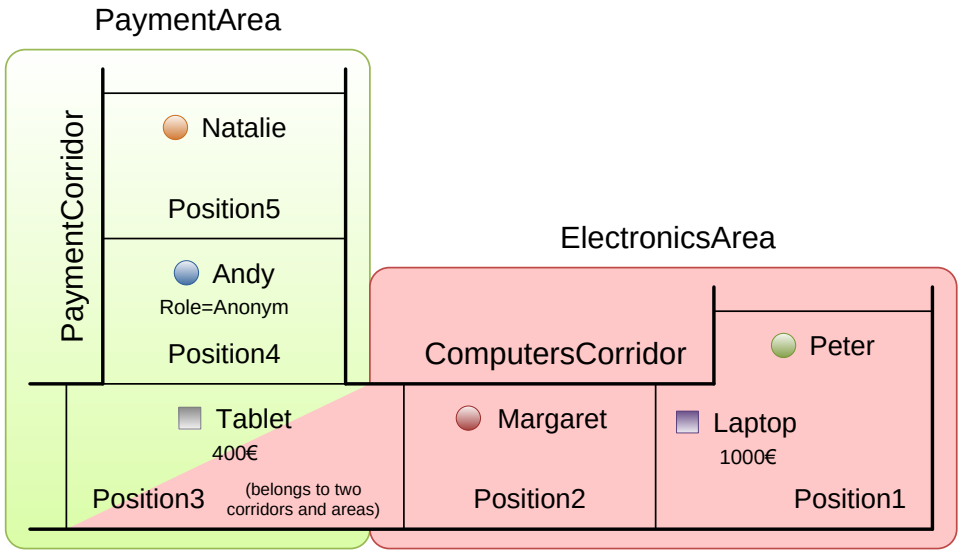
Proteger la localización de los usuarios

- **Location Ontology**
  - Modela información del espacio y la información común para todas las aplicaciones o contextos
- **Supermarket Ontology** (ejemplo como prueba de concepto)
  - Modela los elementos que componen el contexto de los supermercados



Proteger la localización de los usuarios

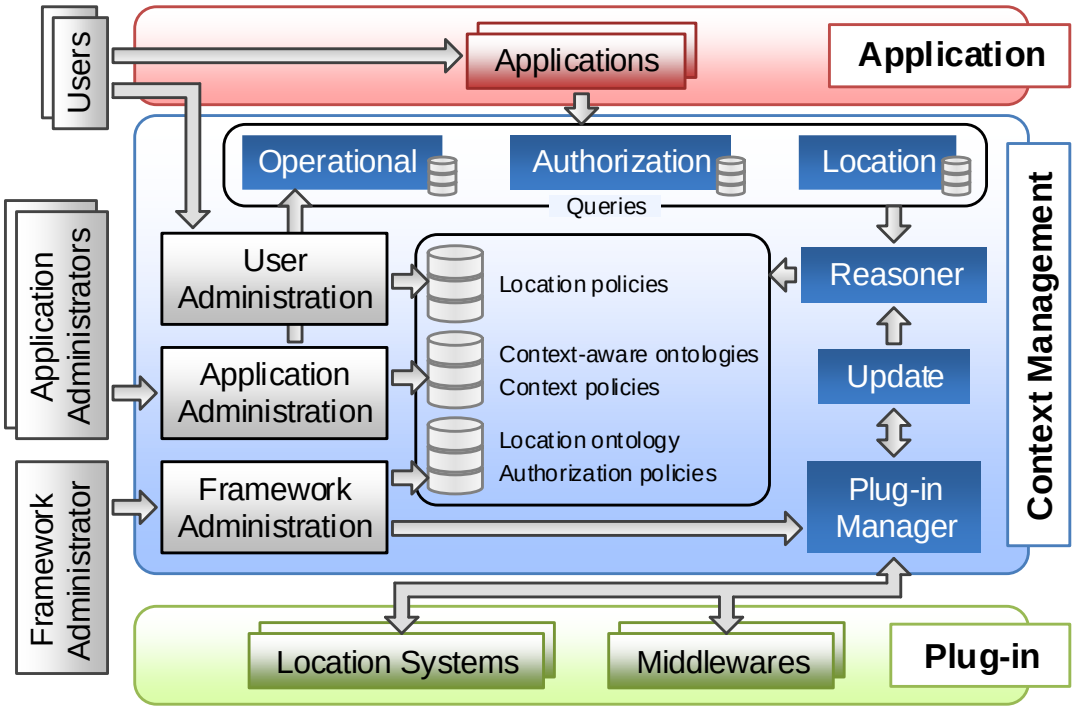
- Caso de uso



- Políticas
  - **Localización** (definidas por los usuarios)
    - Cloaking, Hiding, Granularity, Closeness

Person(#Andy) ^ hasRole(#Andy, #Anonym) ^ isLocated(#Andy, #Supermarket) ^ Person(?requester) → hasCloaking(#Andy, ?requester)

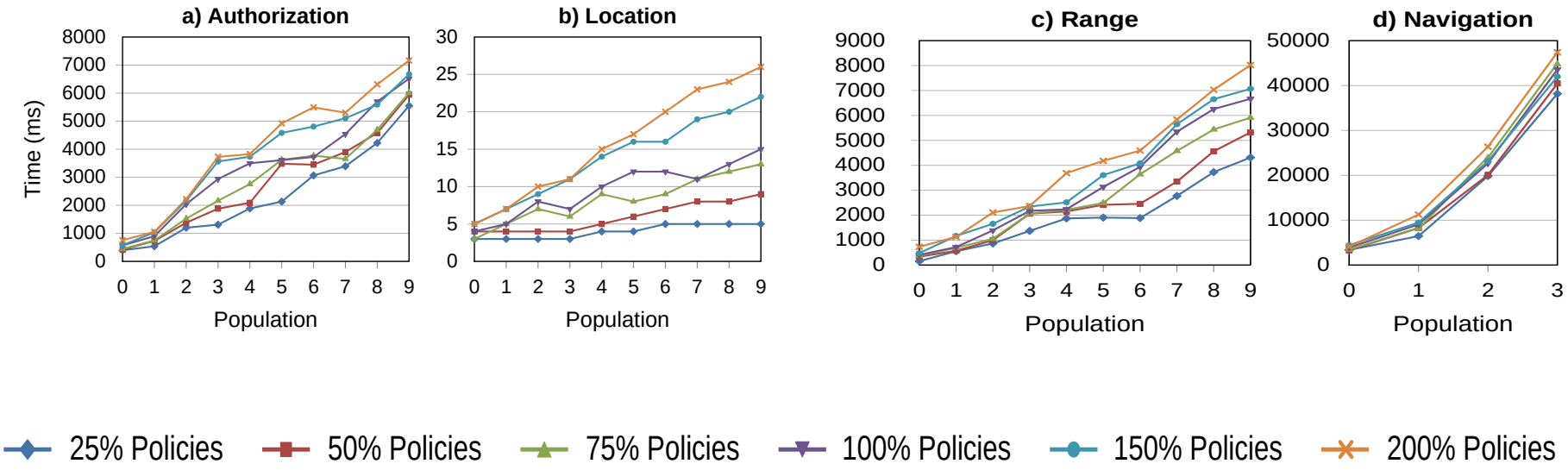
Proteger la localización de los usuarios



- **Capas**
  - **Plug-ins:** obtención de información del contexto y de los usuarios
  - **Context Management:** gestión y protección de la información
  - **Applications:** provisión de servicios sensibles al contexto

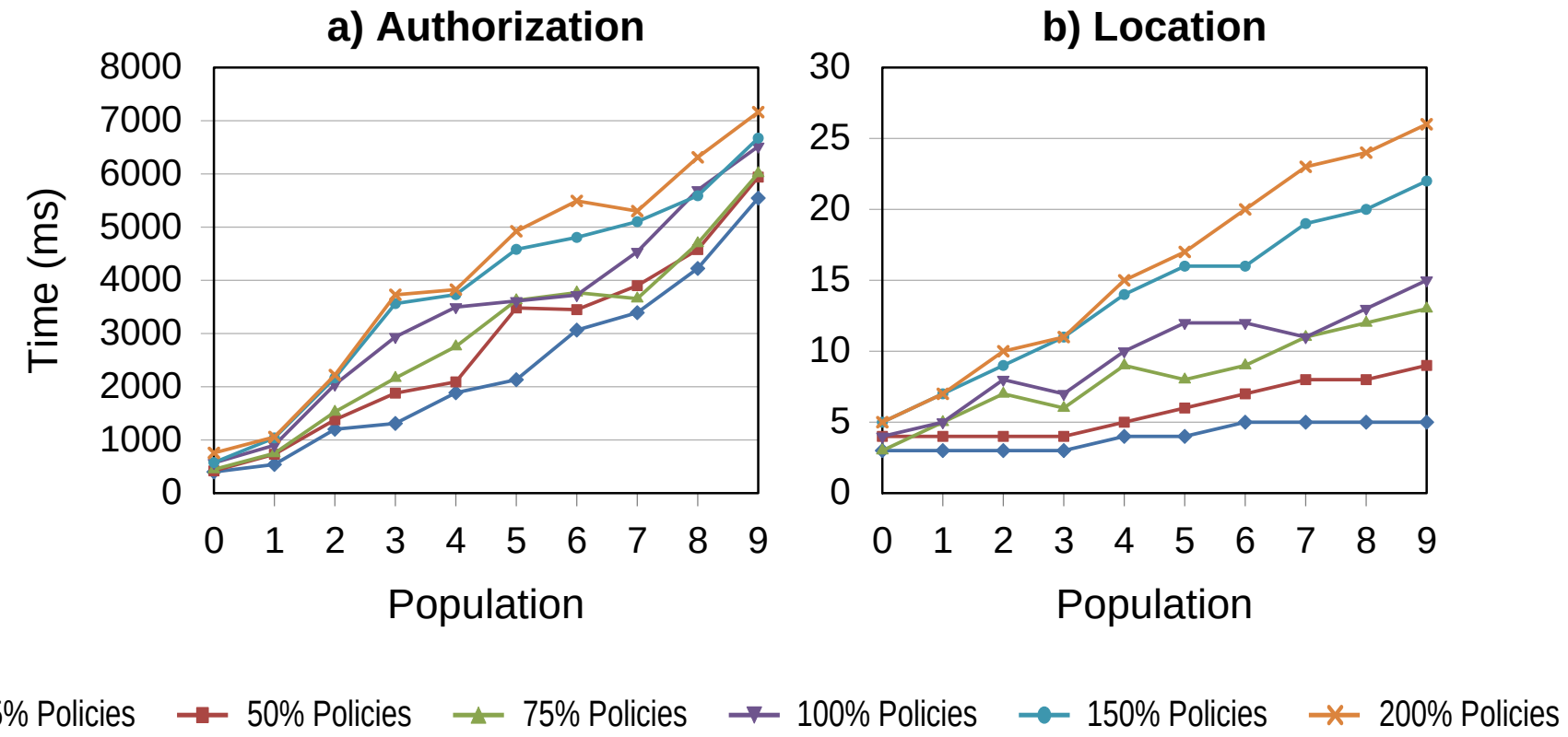
Proteger la localización de los usuarios

- **Implementación prototipo**
  - Ontologías -> OWL 2
  - Políticas -> SWRL
  - Modelos Ontológicos -> Jena
  - Razonador semántico -> Pellet
  - Queries -> SPARQL

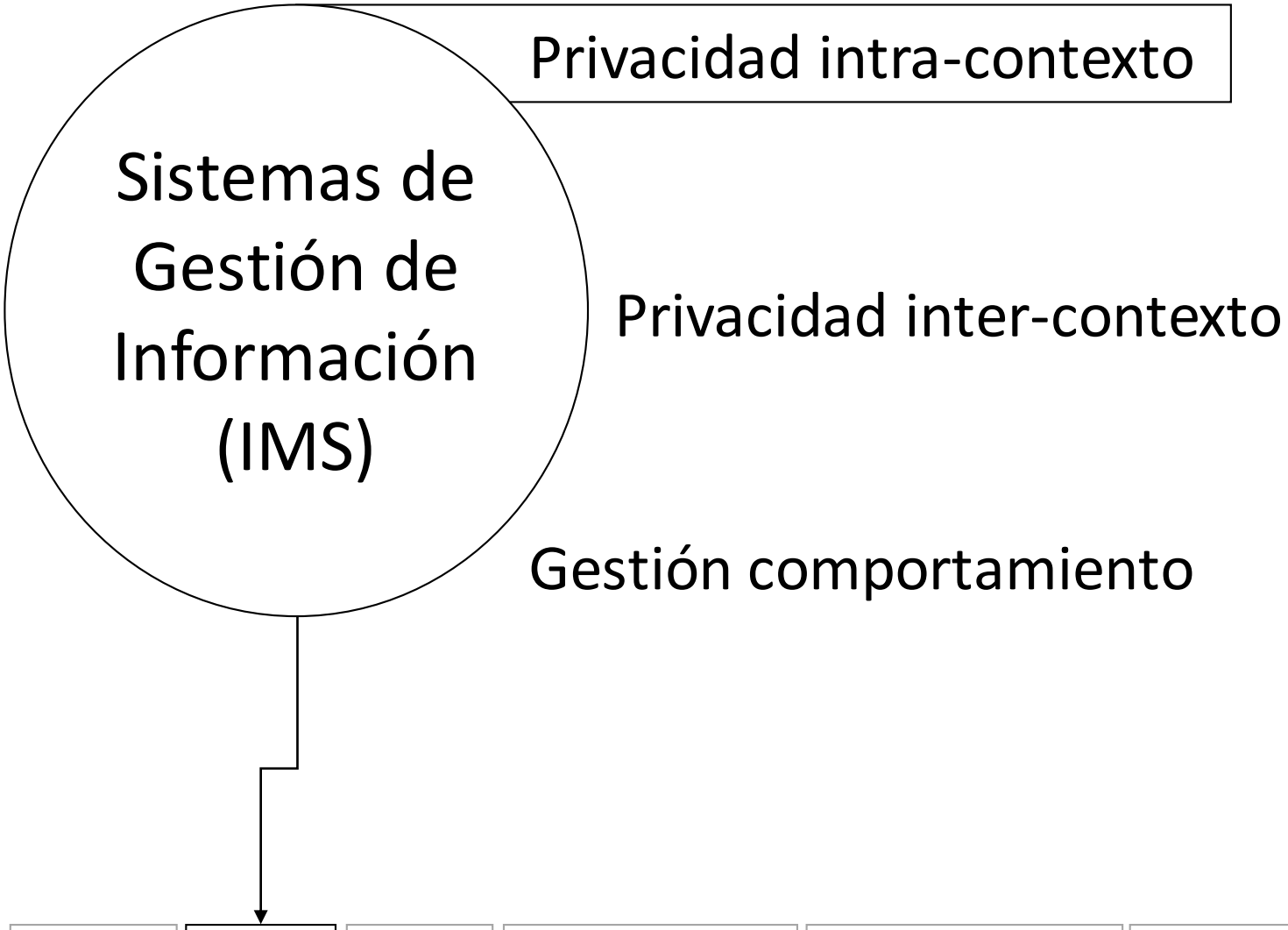


Proteger la localización de los usuarios

Population	0	1	2	3	4	5	6	7	8	9
Individual	15k	30k	45k	60k	75k	90k	105k	120k	135k	150k
Statements	130k	260k	390k	520k	650k	780k	910k	1,040k	1,170k	1,300k



Líneas de investigación



Proteger la información de los usuarios

- Necesidad de proteger no solo la localización de los usuarios con respecto a otros usuarios, si no también otras piezas sensibles de información con respecto a servicios

Middleware orientado al mundo del Cloud Computing que ofrece recomendaciones sensibles al contexto considerando la privacidad de los usuarios

- Las recomendaciones tienen en cuenta:
  - Información del contexto
  - Localización de los usuarios
  - Patrones de comportamiento de los usuarios
  - Perfiles con las preferencias de privacidad de los usuarios

Proteger la información de los usuarios

- Aspectos de privacidad
  - Proteger la identidad de los usuarios con respecto a usuarios y servicios
  - Liberar la localización de los usuarios a servicios concretos
  - Proporcionar posiciones falsas a ciertos usuarios
  - Establecer la precisión y cercanía a la que los usuarios quieren liberar sus localizaciones a usuarios y servicios

- Políticas para definir las preferencias de privacidad:
  - Localización
    - Release, Hiding, Cloaking, Granularity, Closeness
  - Anonimato
    - Revealing

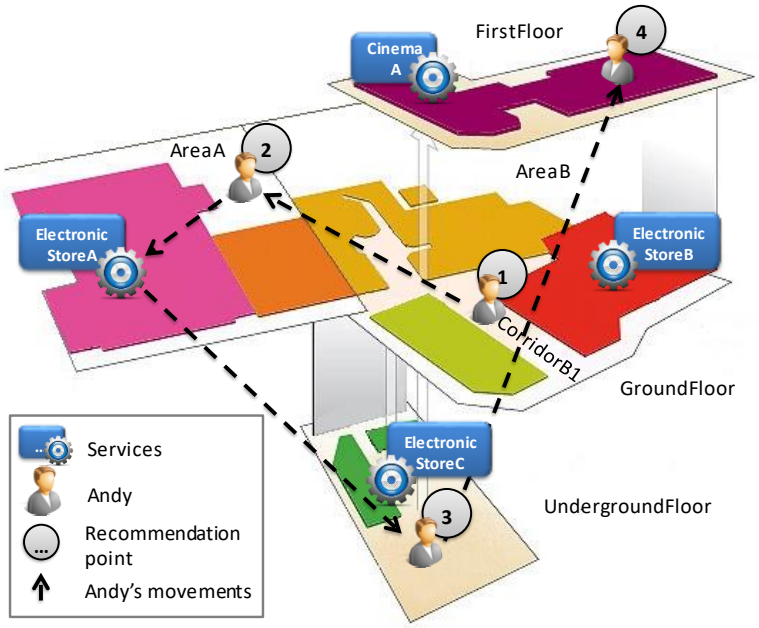
Proteger la información de los usuarios

- Caso de uso: Centro comercial

Person(*#Andy*) ^ *isLocated*(*#Andy*, *#Mall*) ^ *Service*(*?Requester*) *hasType*(*?Requester*, *#ElectronicType*) → ***hasRelease***(*#Andy*, *?Requester*)

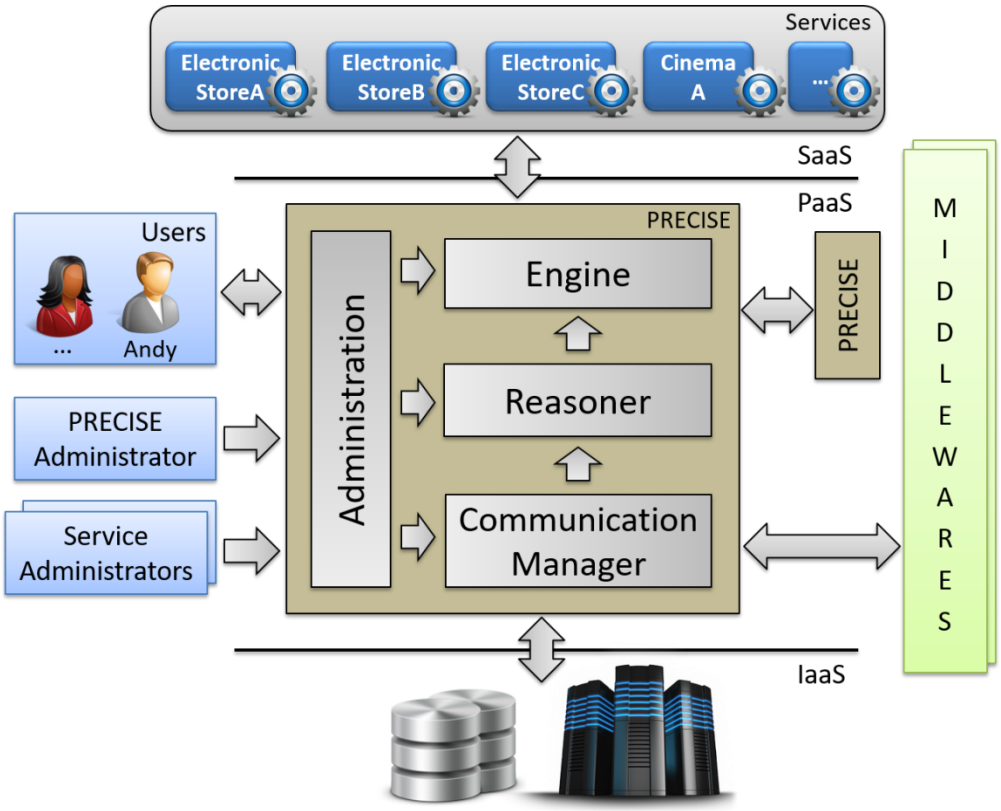
Person(*#Andy*) ^ *isLocated*(*#Andy*, *#UndergroundFloor*)
→ ***hasRevealing***(*#Andy*, *#ElectronicStoreC*)

Person(*#Andy*) ^ *isLocated*(*#Andy*, *#AreaA*)
→ ***hasGranularity***(*#Andy*, *#Floor*)



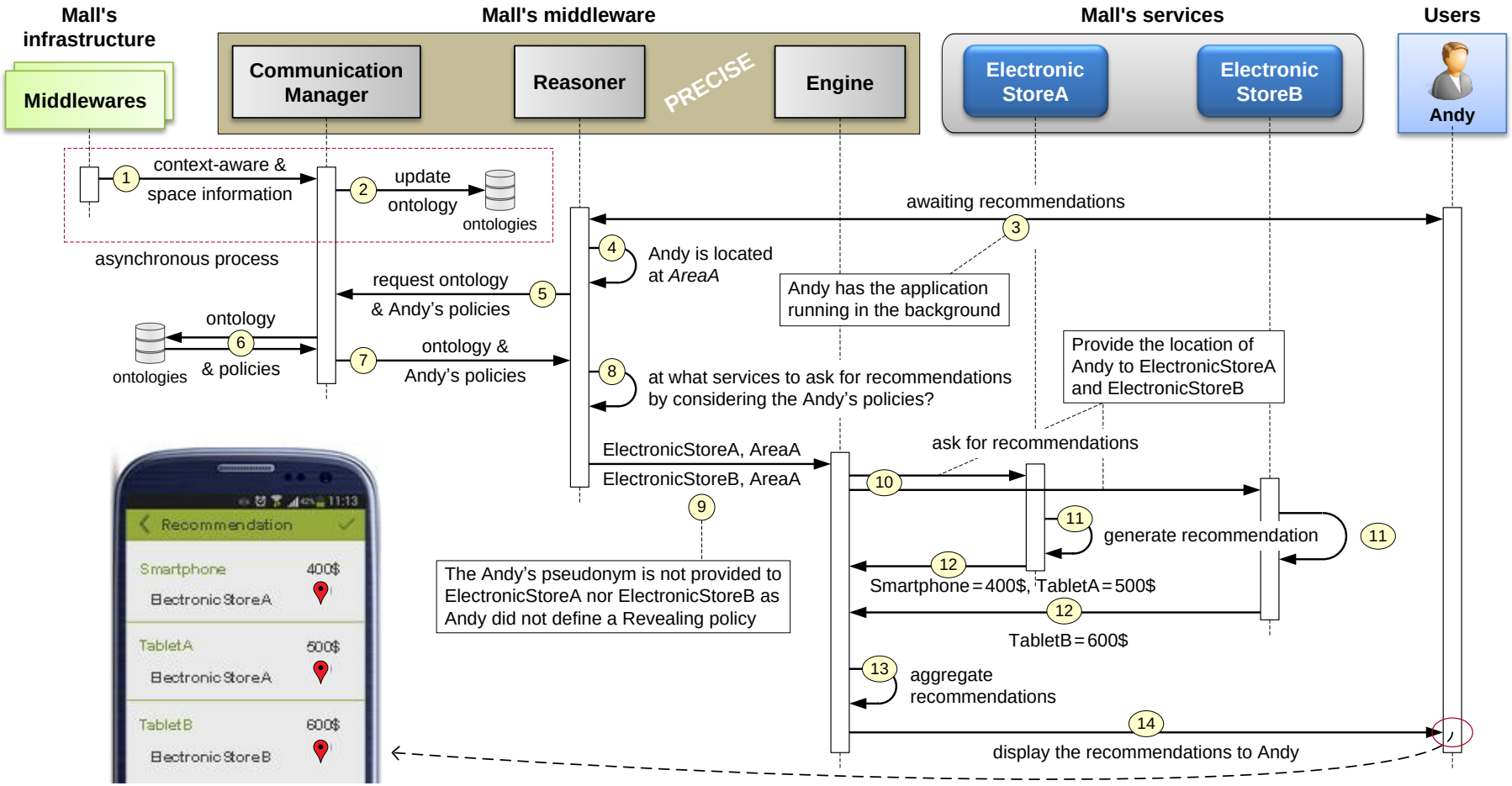
Proteger la información de los usuarios

- Arquitectura para proteger la privacidad de la localización e identidad de los usuarios con respecto a servicios



Proteger la información de los usuarios

- Diagrama de secuencia del caso de uso



Líneas de investigación

Sistemas de Gestión de Información (IMS)

Privacidad intra-contexto

- Localización con respecto a usuarios
- Identidad y localización con respecto a servicios

Privacidad inter-contexto

Gestión comportamiento

Privacidad Inter-contexto

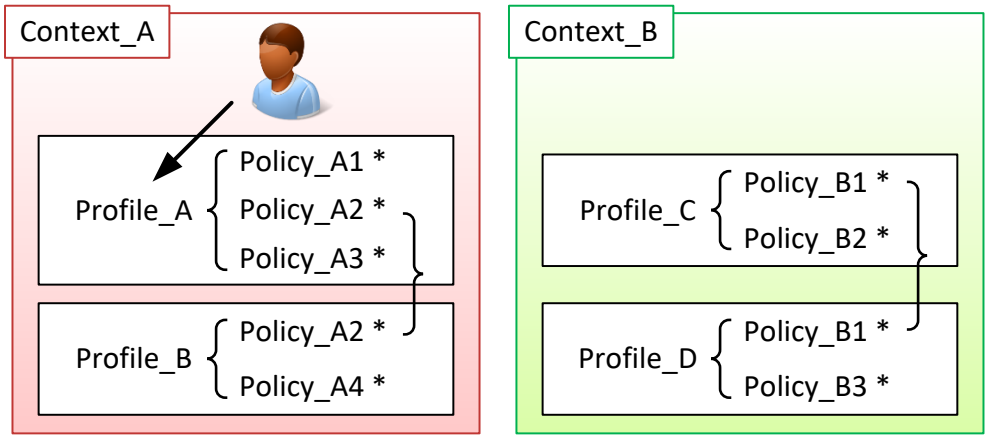
- Necesidad de proteger la información de los usuarios cuando estos se mueven entre diferentes contextos

Sistema que proporciona perfiles (conjuntos de políticas) que protegen la privacidad de los usuarios en los entornos o contextos donde el usuario está localizado

  - El usuario elige el perfil que más encaja con sus preferencias
    - Se evita tener que definir o gestionar sus políticas de privacidad
  - Los usuarios protegen
    - Localización, información personal, actividades e información del contexto
  - Los usuarios consienten liberar su información en tiempo real

Privacidad Inter-contexto

- Perfiles diferentes para cada contexto cuyas políticas pueden ser compartidas entre perfiles del mismo contexto



- Políticas
  - Disclosure (definida por el origen): qué información es liberada y a qué contexto se libera.
  - Reveal (definida por el destino): cuándo y dónde es liberada

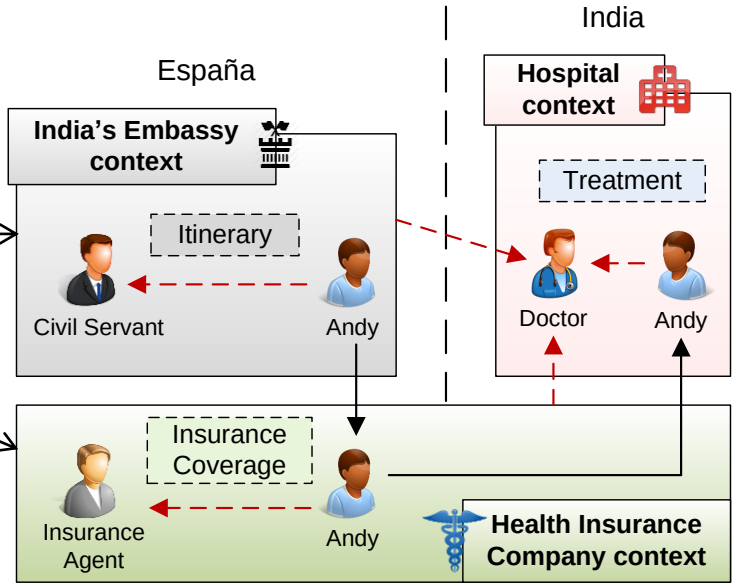
Privacidad Inter-contexto

Inter-Disclosure policies

When Andy is at the India's Embassy & Health Insurance

Id: EmbassyInterD & Type: InterDisclosure[Hospital] & Maker: CivilServant & Target: Andy & Requester: HospitalStaff & What: Itinerary → Result: Disclosure

Id: InsuranceInterD & Type: InterDisclosure[Hospital] & Maker: InsuranceAgent & Target: Andy & Requester: HospitalStaff & What: InsuranceCoverage → Result: Disclosure

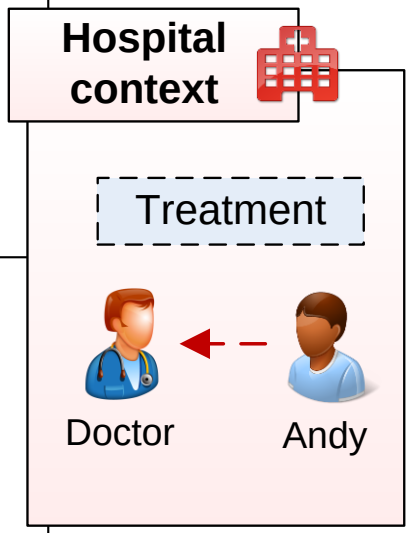


Inter-Reveal policies

When Andy is at the Hospital

Id: 1HospitalInterR & Type: InterReveal[HealthInsuranceCompany] & Maker: HospitalAdmin & Target: ForeignPatient & Requester: Doctor & Where: ConsultingRoom → Result: Reveal

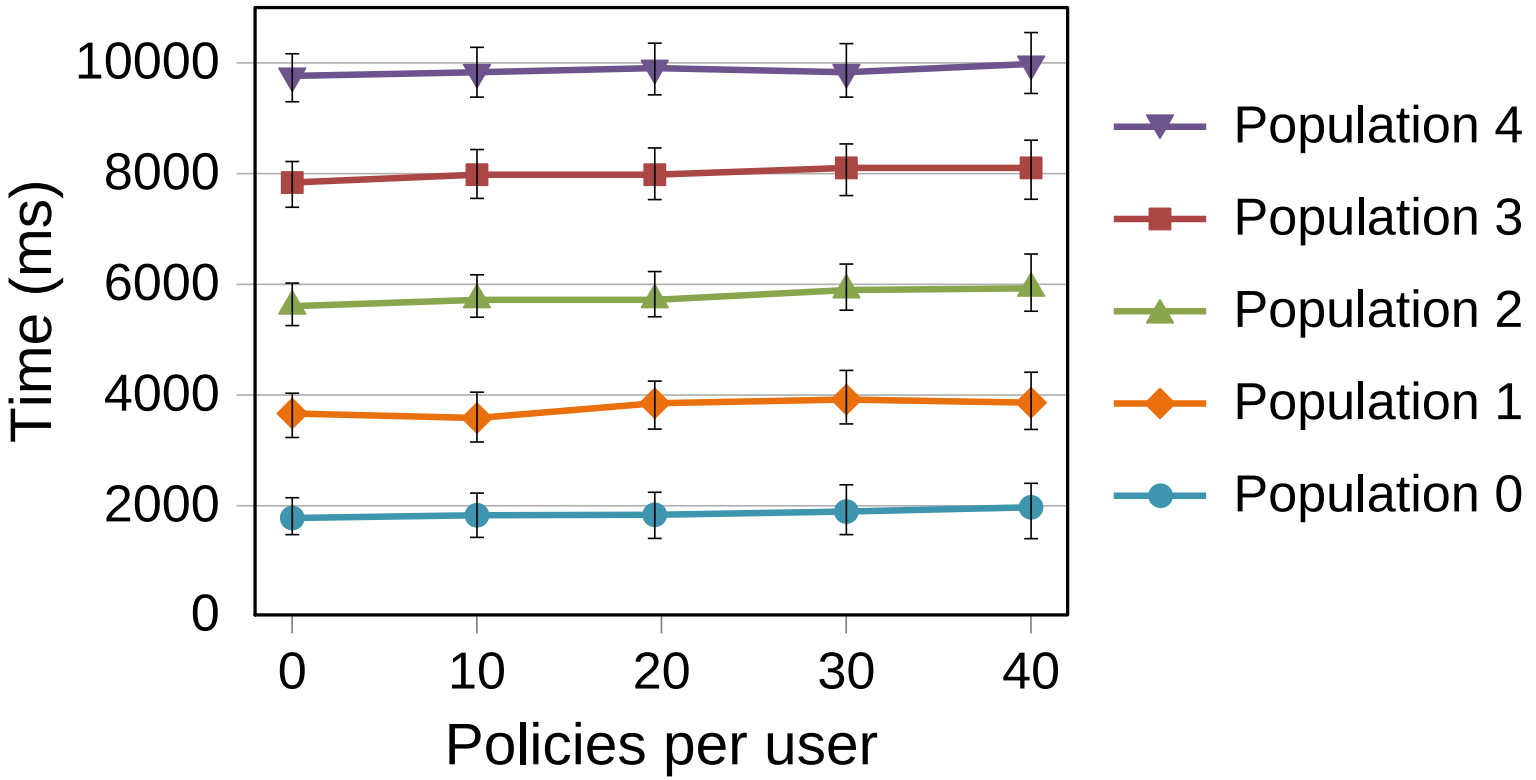
Id: 2HospitalInterR & Type: InterReveal[CountryAEmbassy] & Maker: HospitalAdmin & Target: ForeignPatient & Requester: Doctor & Where: Hospital → Result: Reveal



Privacidad Inter-contexto

- Tiempo de razonamiento

Population	0	1	2	3	4
Individual	30k	60k	90k	120k	150k
Statements	244k	487k	734k	971k	1,203k



Líneas de investigación

Sistemas de Gestión de Información (IMS)

Privacidad intra-contexto

Privacidad inter-contexto

- Perfiles para proteger la información de usuarios
- Decisión en tiempo real de los usuarios

Gestión comportamiento

Policies for green mobile networks

- Necessity to manage at real time and on demand the network infrastructure taking into account the status of the context to reduce the energy consumption

Context-aware policy-based solution in charge of reducing the energy consumption in networks oriented to the SDN paradigm.

- Policies to manage the SDN at run-time and on demand
- Policies consider contextual information:
  - Location of infrastructure, energy consumption, network statistics, and number of active users
- Switching policies and virtualization policies

Policies for green mobile networks

- Policies structure

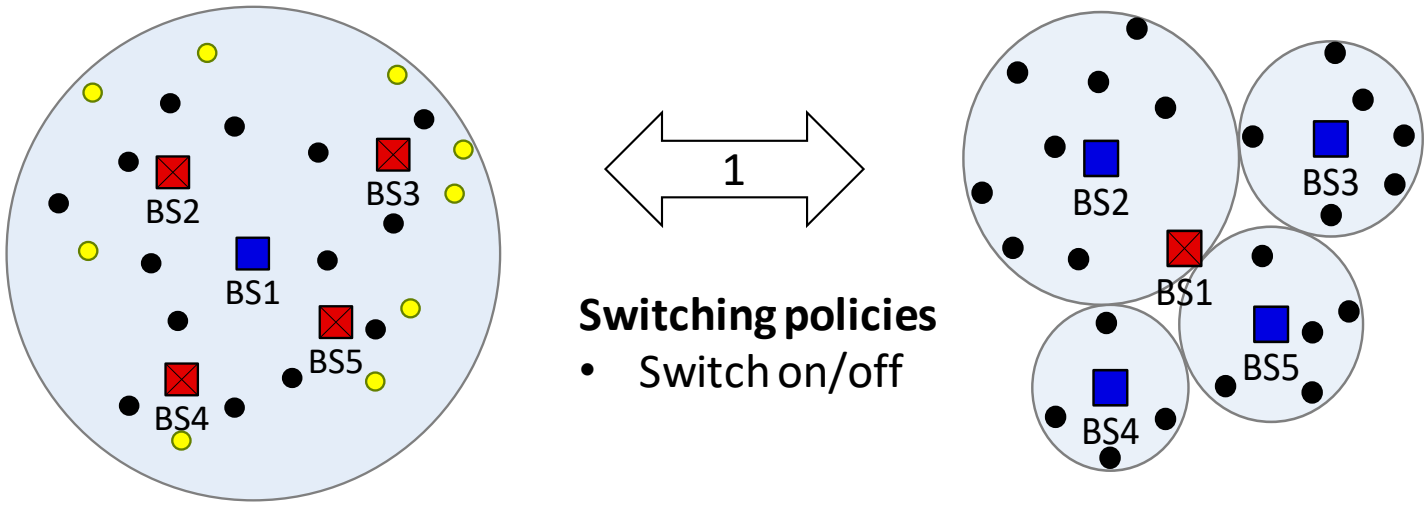
Type ^ Resource ^ Metric ^ Location ^ Date → Result

Element	Values	Description
Type	Switching, Virtualization	Indicate the kind of policy
Resource	Base station, Switch, Service, Intrusion Detection System, etc.	Network element whose information is being managed
Metric	Average of Bytes per flow (ABf), Average power consumption in peak hour (PIUrban), etc	Define the term that encompasses the different parameters that can be used to evaluate the network state
Location	Geographic position, Area, etc.	Position or region where the policy will be enforced
Date	Date, Hour, Timestamp, etc.	Moment or period of time at which the policy will be applied
Result	Switch, CreateProxy	Action performed over the network when the policy is applied

Policies for green mobile networks

Metric	Average power consumption in peak hour (PIUrban)

- Virtualization policies: Create or dismantle virtual network resources to reduce the load of traffic
- Switching policies: Switch on/off network resources when they are consuming energy in an inefficient way

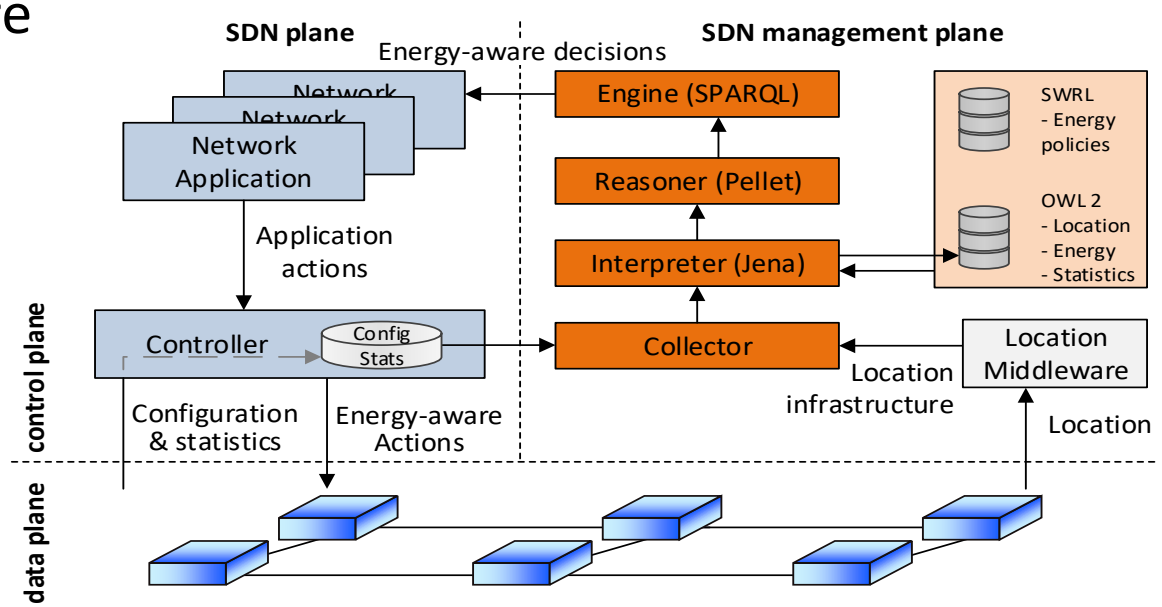


Switching policies
- Switch on/off

Type(#Switching) ∧ BaseStation(?bs) ∧ Location(?bs,?area) ∧ locatedBS(?area,?neighborBs) ∧ integer[PIUrban in #AlarmA] hasPIUrban(?bs) → hasStatus(?neighborBs, #ON) ^ hasStatus(?bs,#OFF)

Policies for green mobile networks

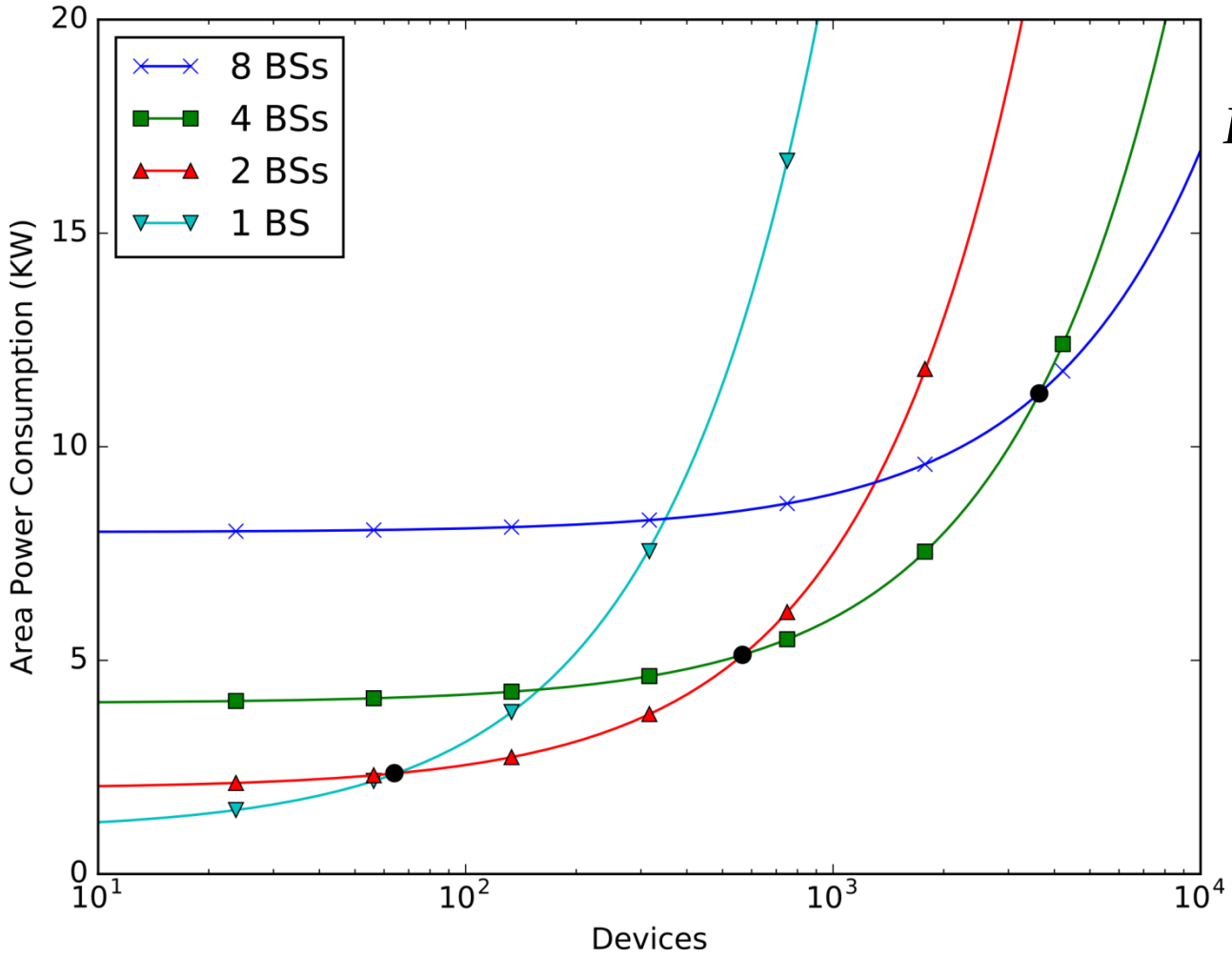
- Architecture



- Implementation
  - SDN Controller: OpenDaylight & OpenVSwitch
  - Southbound: OpenFlow
  - Network Virtualization: OpenStack
  - SDN Northbound: REST API

Policies for green mobile networks

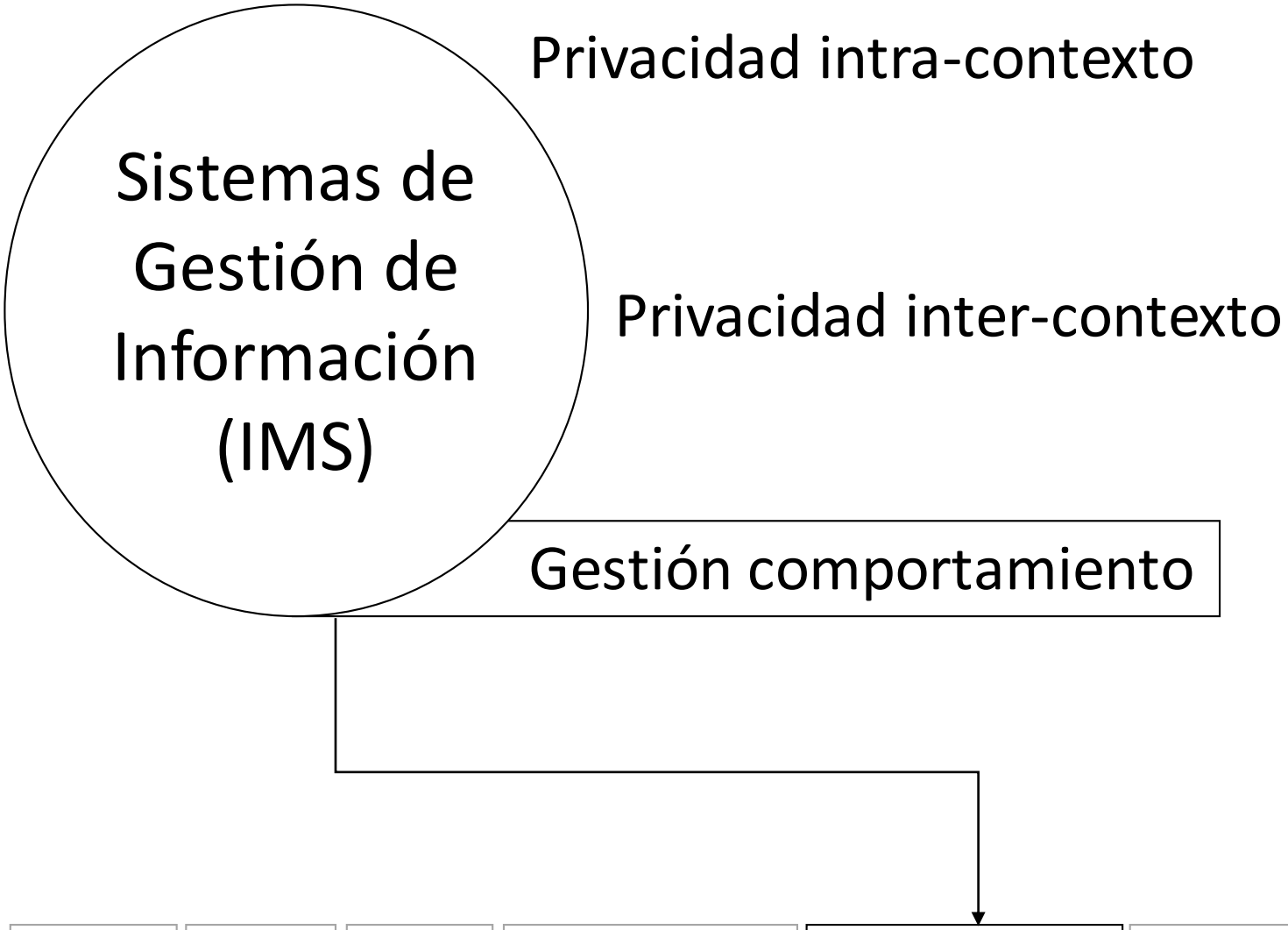
- Experiments



$$P_{total} = c_1 \cdot N_{bs} + c_2 \cdot Nd \cdot d^e$$

Different curves represent the number of base stations when c1 = 1000W and c2 = 0.5mW

Líneas de investigación



Policy-based dynamic mobile scenarios

- Need to manage at real time and on demand the network infrastructure taking into account the mobility of users and the network statistics

Mobility-aware and policy-based on demand control network solution to ensure the QoE by managing at run-time services and/or system state

- Policies consider the mobility of users, the infrastructure location, and the network statistics
- Load balancing, Infrastructure, Restriction policies

Policy-based dynamic mobile scenarios

- Policies to ensure the QoE

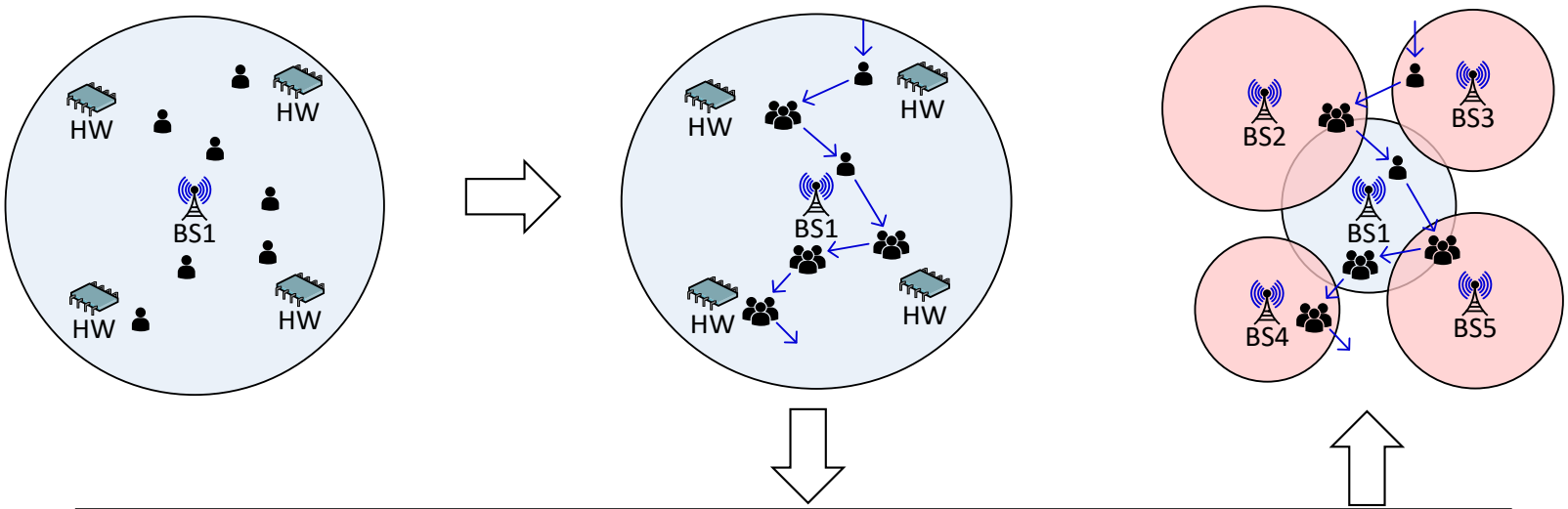
Type ^ Resource ^ Metric ^ Location ^ Date → Result

Element	Values	Description
Type	Load balancing, Infrastructure, Restriction	Indicate the kind of policy
Resource	Base station, Switch, Service, Intrusion Detection System, etc.	Network element whose information is being managed
Metric	Average of Bytes per flow (ABf), Average Number of Packets per Flow (ANPPF), Average of Duration per flow (ADf), etc.	Define the term that encompasses the different parameters that can be used to evaluate the network state
Location	Geographic position, Area, etc.	Position or region where the policy will be enforced
Date	Date, Hour, Timestamp, etc.	Moment or period of time at which the policy will be applied
Result	Balance, Create, Dismantle, Disable, Limit	Action performed over the network when the policy is applied

Policy-based dynamic mobile scenarios

Metric	Average Number of Packets per Flow (ANPPF)

- Restriction policies: disable or limit the traffic of given network resources or services in case of traffic overload
- Infrastructure policies: create or dismantle virtual network resources located at specific locations



Type(#Infrastructure) ^ BaseStation(?bs) ^ Location(?bs,?area) ^ locatedResources(?area,?resource) ^ hasANPPF(?bs,?anppf) ^ inRange(?anppf,#Orange) → create(?resource,#BaseStation)

Líneas de investigación

Sistemas de Gestión de Información (IMS)

Privacidad intra-contexto

Privacidad inter-contexto

Gestión comportamiento

- Gestión dinámica de los recursos de red teniendo en cuenta la información del contexto

Conclusiones

- Gestión automática de la privacidad de la información
  - Escenarios Intra-contexto
    - Protección de la localización de los usuarios
    - Control de la identidad y localización de los usuarios con respecto a servicios y usuarios
  - Escenarios Inter-contexto
    - Perfiles para proteger la información de los usuarios
- Gestión automática del comportamiento de los recursos de red
  - Control dinámico y eficiente de los recursos de red
  - Información del contexto (ej. el uso de los recursos y la localización de la infraestructura) para garantizar QoE y eficiencia energética

Vías futuras

- Gestión de conflictos de políticas de privacidad en escenarios intra- e inter-contexto
- Privacidad de los usuarios en el control del comportamiento de los sistemas
- Network Slicing para la gestión de los recursos de red
- Gestión de los usuarios y recursos de red en nuevos escenarios 5G

Publicaciones relacionadas

Alberto Huertas Celdrán, Félix J. García Clemente, Manuel Gil Pérez, and Gregorio Martínez Pérez, "**SeCoMan: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications**," *IEEE Systems Journal*, Special Issue on *Intelligent Internet of Things* 10(3):1111-1124, 2016.

Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J. García Clemente, and Gregorio Martínez Pérez, "**PRECISE: Privacy-aware recommender based on context information for Cloud service environments**," *IEEE Communications Magazine*, Feature Topics Issue on *Context-Aware Networking and Communications* 52(8):90-96, 2014.

Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J. García Clemente, and Gregorio Martínez Pérez, "**What private information are you disclosing? A privacy-preserving system supervised by yourself**," in CSS'14: *Proceedings of the 6th International Symposium on Cyberspace Safety and Security*, pp. 1221-1228, Paris (France), 2014.

Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J. García Clemente, and Gregorio Martínez Pérez, "**MASTERY: A multicontext-aware system that preserves the users' privacy**," in NOMS'16: Proceedings of the *IEEE/IFIP Network Operations and Management Symposium*, pp. 523-528, Istanbul (Turkey), 2016.

Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J. García Clemente, and Gregorio Martínez Pérez, "**Policy-based management for green mobile networks through Software-Defined Networking**," *Mobile Networks and Applications*, Published online 05 December 2016.

Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J. García Clemente, and Gregorio Martínez Pérez, "**Enabling highly dynamic mobile scenarios with Software Defined Networking**," *IEEE Communications Magazine*, Feature Topics Issue on *Use Cases For Service Provider Networks*, Accepted, 2017.