Sistema de Control de Acceso y Permanencia – PASA

Sabrina A. Pastrana, Pablo J. Vidal, Marta G. Lasso •

Abstract

In the Laboratorio de Tecnologías Emergentes (LabTEm) of the UNPA we are working in "Administration of Intelligent Buildings, by Multi-agents Systems". One of the concerns that affect the people at the moment is the security and protection of their ownership such as the possibility of being recognized by the environment. The objective of this work is to approach the problem that emerge starting from the identification of people that they have access to an office or building, using a Multi-agent system. With this system we pretend to guarantee the protection of all their properties, tangible and intangible, likewise the control and verification of entry and departure through the generation of reports and the maintenance of historical data of all the transactions carried out by the users, providing autonomy to the people by an identification code that they have.

Keyword: Intelligent Buildings, Control and Verification, Multi-agents Systems

• Universidad Nacional de La Patagonia Austral - Unidad Académica Caleta Olivia. Laboratorio de Tecnologías Emergentes (LabTEm). Caleta Olivia – Santa Cruz – Argentina (9011). e-mail: sabrina.pastrana@gmail.com.ar; {pjvidal; mlasso}@uaco.unpa.edu.ar

Resumen

En el marco del Laboratorio de Tecnologías Emergentes (LabTEm), de la UNPA se esta trabajando en la "Administración de Edificios Inteligentes, mediante Sistemas Multiagentes". Una de las preocupaciones que afectan actualmente al hombre, es la seguridad y la protección de sus pertenencias, como así también la posibilidad de ser reconocido por el ambiente. El objetivo de este trabajo es abordar la problemática que surge a partir de la identificación de las personas que tienen acceso a una oficina o edificio, utilizando un sistema Multi-agente. Con este sistema se pretende garantizar la protección de todos sus bienes, tangibles e intangibles, como así también el control y verificación de ingresos y egresos a través de la generación de reportes y el mantenimiento de datos históricos de todas las transacciones llevadas a cabo por los usuarios, brindando autonomía a los individuos mediante el código de identificación que poseen.

Palabras Claves: Edificios Inteligentes, Control y Verificación, Sistemas Multi-agentes.

1. Introducción

Con el correr de los años, los edificios y construcciones habitadas por seres humanos como por ejemplo, casas de familia, oficinas e industrias han incorporado paulatinamente distintas componentes y artefactos basados en muchos casos en tecnologías avanzadas. Es común hoy en día que se hable de sistemas automáticos para vigilancia, prevención y control de incendios, control de ascensores, climatización e iluminación como así también de procesos industriales automatizados y equipamientos o electrodomésticos "inteligentes". La disponibilidad y abaratamiento del hardware necesarios para este tipo de aplicaciones ha llevado a que elementos tales como robots móviles, sensores inteligentes, cámaras para visión ambiental y computadoras con alto poder de procesamiento entre otros, comiencen a formar parte de nuestra vida diaria como partes constituyentes de los edificios donde vivimos y trabajamos.

Si incorporamos a este fenómeno las posibilidades de interconexión que existen actualmente para integrar estas componentes, la idea de lograr edificios inteligentes surge naturalmente, es decir, edificios que permitan realizar las tareas cotidianas de manera más fácil, segura, confortable y eficiente. Basta observar que es posible hoy en día conectar sensores, computadoras y artefactos eléctricos inteligentes o tradicionales mediante Internet para imaginar innumerables aplicaciones prácticas. Algunas de las aplicaciones que podemos identificar a partir de la noción de edificio inteligente son, el ahorro de energía; los servicios, la seguridad y vigilancia entre otros.

Si bien hoy en día muchos de los dispositivos y sistemas utilizados para la automatización de edificios suelen ser referenciados como "inteligentes", la mayoría de las aplicaciones en esta área son más bien elementales y distan significativamente de las características de los sistemas inteligentes que están disponibles hoy en día en un entorno de computadoras. Esto no significa que este dominio no presenta características y requerimientos que harían aconsejable la incorporación de más inteligencia en los procesos de administración del edificio. Entre los aspectos que deben ser contemplados por un edificio inteligente podemos citar, flexibilidad, escalabilidad, robustez, amigabilidad y tiempos de respuestas adecuados.

Es interesante observar que la mayoría de estas características suelen ser encontradas en los sistemas inteligentes que hoy en día se han popularizado con el nombre de sistemas basados en agentes inteligentes y los sistemas multiagente (SMA). Por lo tanto, no es de extrañar que gran parte de las propuestas más recientes para la administración inteligente de edificios hayan adoptado este enfoque [2].

Un agente inteligente es una entidad (de software o hardware) autónoma, conectada directamente al ambiente del problema, y que es capaz de exhibir un comportamiento flexible tendiente a cumplir sus objetivos de diseño.[10,14,8] Al

hablar de comportamiento flexible, queremos referenciar al hecho de que debe ser capaz de reaccionar a tiempo a los cambios en el ambiente (reactividad), tomar la iniciativa cuando sea necesario (pro-actividad) y comunicarse e interactuar con otros agentes humanos o artificiales (sociabilidad).

Cuando varios agentes interactúan en un ambiente compartido, se obtiene SMA. Un SMA puede ser definido como una red débilmente acoplada de resolvedores de problemas (agentes) que trabajan conjuntamente para resolver problemas que superan las capacidades individuales o con conocimiento de cada uno de ellos.

2. Objetivos

Un problema que se presenta en el mundo actual para todos los individuos, tiene que ver con la seguridad. Los sistemas que habitualmente utilizamos los humanos para identificar a una persona, como el aspecto físico o la forma de hablar, son demasiados complejos para una computadora; el objetivo de un sistema de identificación de usuarios no busca solo identificar a una persona, sino autenticar que esa persona es quien dice ser realmente.

Aunque como humanos seguramente ambos términos nos parecerán equivalentes, para un ordenador existe una gran diferencia entre ellos: imaginemos un potencial sistema de identificación estrictamente hablando, por ejemplo uno biométrico basado en el reconocimiento de la retina; una persona mira a través del dispositivo lector, y el sistema es capaz de reconocer esa imagen como válida, ya que pertenece a la retina de un ojo, de esta forma el individuo puede estar identificado, pero no necesariamente autenticado por el sistema, ya que el sistema debe verificar que la imagen observada se corresponda con alguna de las imágenes almacenadas en la base de datos correspondiente y así garantizar que la persona es quien dice ser. [14,7]

El objetivo de este trabajo es implementar un Sistema de Identificación Segura (SIS) que sea capaz de verificar, autenticar, gestionar y almacenar toda la información perteneciente a cada una de las personas autorizadas a acceder a una determinada zona de un edificio, haciendo uso del paradigma SMA.

3. Sistema de Identificación Segura

Para implementar el nivel de seguridad deseado para una aplicación, un SIS debe garantizar las políticas y procedimientos realizados en la supervisión del uso de la forma de identificación, existir un sistema establecido que proteja el acceso a la información del usuario y prevenir el manoseo de la misma, que los sistemas de identificación solo sean emitidas por las organizaciones autorizadas, para la persona correcta y que los individuos tengan pleno acceso a los privilegios indicados en su

identificación, evitando duplicaciones o mecanismo fáciles de falsificar, debe ser fácil de usar, simple e intuitiva, y no debe asustar con impedimentos técnicos confusos, ser rentable para las empresas o entidades, tanto los costos iniciales como los de distribución y mantenimiento, fácil de gestionar, fáciles de distribuir, de renovar, de sustituir en caso de pérdida o cambios.

Los SIS pueden ser implementados para grupos en particular, para varios grupos dentro de una organización o empresa o para múltiples organizaciones o empresas. Independientemente del número o tipo de entidades que se vean involucradas; para que sean, realmente seguros, los sistemas de identificación deben implementar un modelo de confianza. Este modelo institucionaliza principios y políticas aceptadas universalmente, que las operaciones del sistema siempre tengan el mismo resultado, independientemente de donde sean realizados y todos los participantes involucrados pueden confiar que el sistema verificará con precisión y seguridad su identidad. Antes de implementar cualquier sistema, todas las entidades participantes en un sistema de identificación deben definir y acordar un modelo de confianza.

La decisión de crear un SIS es básicamente el resultado de un análisis de las amenazas a la seguridad, que determina como necesidad primaria asegurarle, a un sistema, un alto grado de confianza.

Los sistemas de autenticación se pueden enmarcar en los siguientes grupos: sistemas basados en algo conocido (contraseña), sistemas basados en algo poseído (tarjeta inteligente) [13] sistemas de identificación por radiofrecuencias (RFID) [11] y sistemas biométricos (basados en características del individuo) [12]. Evidentemente un sistema de autenticación puede y debe combinar varios de estos mecanismos para aumentar el nivel de seguridad, sobre todo si se usa una red de telecomunicaciones. Además, cualquier sistema de autenticación debe ser viable (es decir, económicamente rentable) y aceptado por los usuarios.

Si bien en los sistemas basados en algo conocido, la utilización de claves secretas, uso de número de identificación personal (PIN) y/o tarjetas de identificación, uso de máquinas lectoras de tarjetas o códigos de barra no son suficientes en algunos casos, lo importante es lograr un mecanismo de autenticación que consiste en comprobar que un usuario es quien dice ser.

4. Dominio y descripción del problema

La tecnología de agentes/sistemas multi-agente (SMA) está realizando importantes aportes en la resolución de problemas en diversos dominios (comercio electrónico, subastas electrónicas, medicina, bolsa, etc.), donde aproximaciones tradicionales no proporcionan soluciones suficientemente satisfactorias, y en donde los problemas son inherentemente distribuidos.

La aplicación desarrollada ha sido implementada para la oficina del LabTEm, en la UNPA – UACO aplicando tecnologías Orientadas a Objetos (OO) y SMA como base para la resolución de problemas de seguridad y gestión de edificios, obteniendo beneficios tales como saber que personas han ingresado y cuanto tiempo han permanecido. Este proyecto se ha desarrollado básicamente en un módulo que facilita la gestión de usuarios, combinando técnicas de desarrollo hibrida y un módulo mediante un SMA[5] que permite la gestión del ingreso y egreso a los usuarios. Esta combinación ha permitido una mayor flexibilidad en la escalabilidad del sistema.

El sistema esta desarrollado a partir de tres componentes; un Program Logical Cotroller (PLC) encargado de conectar los dispositivos de ingreso de identificación (teclados) con el servidor a través de un puerto serie RS-232, el servidor donde se encuentra la aplicación Web encargada de la gestión de los usuarios, dispositivos y zonas de acceso y la aplicación SMA se encarga de gestionar los accesos e ingresos, si un usuario abandona el ambiente sin hacer su registración de salida, el SMA se encarga de claudicar los egresos. Este SMA está compuesto por diversos dispositivos, donde cada uno representa una entidad, pudiéndose definir reglas o comportamientos específicos de acuerdo a la responsabilidad de cada agente. El sistema también permite ver información en tiempo real y generar reportes correspondientes a los movimientos que se han registrado en forma diaria.

5. Tecnologías utilizadas

Cada tecnología existente en el mercado hoy en día tiene sus ventajas y desventajas. En este trabajo se han implementado las siguientes:

Java Server Faces (JSF) [9] Proporciona un conjunto de componentes para la interfaz de usuario, incluyendo los elementos estándares de HTML para representar un formulario. Estos componentes se obtendrán de un conjunto básico de clases base que se pueden utilizar para definir componentes nuevos.

Persistencia de datos con Java Persistente API y HIBERNATE: Al referirnos a persistencia normalmente nos referimos a los datos que quedan permanentes en nuestra aplicación y que se suelen almacenar en medios tales como bases de datos o ficheros. En nuestro caso se resolvió utilizar Java Persistente API (JPA)[1], la cual es una especificación desarrollada para Java que busca unificar la manera en que funcionan las herramientas que proveen un mapeo objeto-relacional. El funcionamiento de JPA, se basa en Plain Old Java Object (POJOs), los cuales son simples clases que no dependen de un framework o herramienta en especial. En JPA, los datos se llaman entidades representadas por los POJOs, éstas hacen referencia a una colección lógica de datos que pueden ser almacenados y

recuperados como un todo. Las entidades forman el núcleo de JPA con las cuales se maneja y disponen de diferentes características y propiedades.

6. Implementación de los componentes del sistema

6.1 Módulo de Hardware

Todos los datos de los usuarios y los ambientes, deben ser transportados y monitoreados de alguna forma, para ello se han utilizado diversos dispositivos interconectados con un PLC encargado de gestionar los datos, es la placa de hardware utilizada como un controlador capaz de trabajar en forma autónoma, sin requerir de una persona que supervise su trabajo. Cada uno de los dispositivos presenta diversas características y cumple una función específica dentro del sistema. (Figura 1).

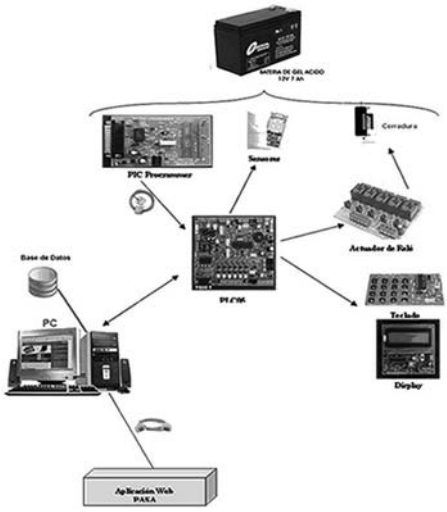

Fig. 1 | **Módulo de hardware**

Los sensores, tienen como función chequear los movimientos que se producen en cada ambiente, mandando un pulso a la unidad a la cual se encuentran conectados.

Los teclados y display se encuentran ubicados en la zona de ingreso/egreso permitiéndoles a los individuos registrarse a través del PIN. En el display se podrá visualizar cualquier error que el usuario haya cometido al momento de ingresar su número de identificación personal.

Las cerraduras eléctricas se encuentran ubicadas en cada una de las puertas de acceso a las habitaciones, las mismas están conectadas a un actuador de relé que se activa enviando un pulso eléctrico que indica que puerta abrir permitiendo asi el ingreso a cada sector.

El PLC es el encargado de recibir la información proveniente de los teclados y sensores y disponer de ella de acuerdo a como se presente el entorno. El PIC Programmer permite programar directamente el PLC.

6.2 Plataforma de desarrollo de agentes JADE

La instrumentación de SMA se ha visto beneficiada en los últimos años por el desarrollo de entornos de programación especialmente adaptados a las características de este tipo de sistemas de software. Entre estos entornos se encuentran aquéllos diseñados de acuerdo con las especificaciones elaboradas por el organismo de estandarización FIPA (Foundation for Intelligent Physical Agents) [3]. Por lo general, los entornos FIPA (JADE [6], ZEUS [4], entre otras.) proporcionan servicios de middleware, así como un conjunto de abstracciones software de carácter básico específicas de los sistemas basados en agentes.

Analizando los entornos, se decidió trabajar con Jade (Java Agent Development Environment), ya que ofrece un ambiente robusto para el control y gestión de SMA. La elección de Jade se debe a que está basado en la plataforma FIPA, siendo esta de fácil de instalación y conexión con el compilador de Java de Sun Microsystems que trabajar con otras plataformas de agentes y facilita la programación y comunicación de los agentes gracias a los esqueletos de agentes y documentación que incluye. Además agrega movilidad a estos entes virtuales dado que pueden ejecutarse en distintas computadoras interconectadas y moverse de una a otra sin problemas.

En este entorno el comportamiento de los agentes JADE se codifica mediante clases de objetos JAVA además Los agentes envían y reciben objetos Java que representan mensajes. Jade proporciona también una librería de protocolos de interacción de agentes. Existe una taxonomía de comportamientos posibles que permiten expresar acciones compuestas (secuenciales, concurrentes e iterativas) o atómicas. La ejecución de los agentes es mediante un hilo de ejecución por agente, no un hilo de ejecución por comportamiento de agente. Cada agente es responsable de la ejecución de su comportamiento.

6.3 Aplicación SMA PASA

Utilizando JADE [6] como base de nuestro SMA que posibilite el control autónomo de los ingresos y egresos, y además, represente en tiempo real el estado

de las zonas con sus respectivos usuarios, se han creado diversos agentes que cumplen una tarea especifica en el SMA PASA.

AgenteEscuchador: Este agente se propone escuchar por el puerto serial de forma de poder enviar y/o recibir información una vez recibida se propone validar la información mandando un mensaje al agente correspondiente para realizar la tarea pedida.

AgenteServicioBD: proporciona los servicios de BD, pudiendo realizar consultas y devolver mensajes.

AgenteCreador: agente encargado de que al inicializar la aplicación SMA, verifica que todos los agentes se creen y que queden en funcionamiento.

AgenteZona: Se encarga de representar la zona, con las reglas definidas particularmente para cada una de las zonas.

AgenteUsuario: Es el encargado de representar la información de un usuario pudiendo informar acerca de sus preferencias.

6.4 Aplicación Web

La aplicación web para el sistema PASA posibilita la gestión de todos los datos que se encuentran almacenados en la base de datos del servidor. Mediante la utilización de tecnología JSF [9] se construyo de forma separada, diversificando el trabajo de diseño de interfaz y asimismo el esquema del mapa de navegación, tomando en cuenta el control de las acciones que podía realizar el administrador Mediante una sesión para un administrador designado es posible acceder a la aplicación. Una vez realizado el login se presenta el menú inicial con las siguientes opciones:

- *Usuarios, Zonas, Dispositivos*: estas opciones permiten que el administrador gestione cada uno de los datos respectos de estas entidades, pudiendo agregar un nuevo objeto usuario, zona o dispositivo, eliminar o modificar alguno ya existente.
- *Reportes:* permite ir al contexto de navegación reportes y en el, generar diversos reportes de acuerdo a la información que se desee tener.
- *Información*: Muestra información en tiempo real sobre el estado de las zonas con los usuarios que se encuentran actualmente en ellas.

6.4.1 Arquitectura en Capas

Siguiendo una arquitectura que separa en contextos para que haya una coherencia y sentido, se decidió trabajar con una arquitectura en capas (Figura 2)

Capa presentación

La misión de esta capa es aislar y facilitar al usuario su interacción con los datos del sistema y con las distintas operaciones que sobre ellos se realizan. Recogerá las

peticiones del usuario, las trasladará hasta la capa de negocio, validará que los datos ingresados son correctos de acuerdo a unas reglas predefinidas y trasladará hasta el usuario los datos proporcionados por las otras dos capas de la aplicación, mostrando esta información de una manera correcta y funcional.

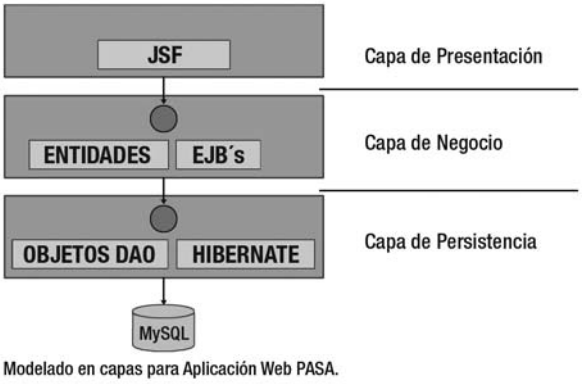

Fig. 2 | **Arquitectura en capas**

Capa negocio

En esta capa es donde se realizan todas las operaciones que verdaderamente dan valor a la aplicación. Este es el núcleo, donde la aplicación realizará las operaciones propias, aportando valor al sistema. Es aquí donde se realizan las operaciones con los datos que son requeridas por la aplicación.

Capa Persistencia

Conjunto de clases encargadas de hacer que la información almacenada en los objetos de negocio, con todos los cambios realizados en cada operación, sea guardado de una manera segura y efectiva. Esta capa proporciona los medios adecuados para acceder la información de una manera rápida y bajo distintos criterios de búsqueda, facilitando, el análisis de los datos independientemente de la forma que sean requeridos.

7. Conclusiones y Trabajos futuros

Con el sistema desarrollado se ha logrado implementar un sistema de identificación segura, la que permite identificar a las personas y una vez generada la autentificación habilitar los recursos configurados para ese usuario utilizando para ello el enfoque multi-agente, a partir de una herramienta con arquitecturas estándares, flexibles y

fáciles de mantener. El mismo es un sistema funcional, que permite controlar el acceso a un ambiente determinado, además con la posibilidad para, agregar, quitar o modificar usuarios, zonas o dispositivos hasta donde el hardware lo permita. Como limitante se reconoce la dependencia del protocolo RS-232 considerado por la distancia física entre el servidor y el PLC.

Siguiendo en esta misma línea, el grupo se encuentra abocada al desarrollo de una aplicación que una vez autenticada la persona, se permita generar condiciones ambientales de iluminación y temperatura de acuerdo a sus preferencias, de manera de ofrecer una mejora laboral y ahorro energético.

8. Agradecimientos

Agradecemos a la Universidad Nacional de la Patagonia Austral por su apoyo al grupo de investigación, la cooperación y las críticas constructivas proporcionadas por el mismo.

9. Referencias

[1] Bauer, C, King, G *Java Persistence with Hibernate*, Manning. 2006

[2] Errecalde M., Lasso M., Villagra A., Pandolfi D., de San Pedro M., “Edificios Inteligentes: el enfoque multi-agente”. WICC 2006.

[3] Foundation for Intelligent Physical Agents.1997. http://www.fipa.org

[4] H.S. Nwana, D.T. Ndumu and L.C. Lee. ZEUS: An advanced Tool-Kit for Engineering Distributed Multi-Agent Systems. In: Proc. of PAAM98, pp. 377-391, London, U.K. 1998.

[5] Honavar V. “Intelligent Agents and Multi-Agent Systems”. IEEE Conference on Evolutionary Computation (CEC), Washington, 1999.

[6] JADE http://www.jade.tilab.com

[7] Lasso M., Vidal P., Villagra A., de San Pedro M., Pandolfi D., Errecalde M., “Identificación de Individuos en Edificios Inteligentes”. WICC 2006.

[8] M. Huhns and L. Stephens, Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence, ch. Multiagent Systems and Societies of Agents, pp. 79–120. The MIT Press, 1999.

[9] P. S. Bhogill. An introduction to Java Server Faces. Java News Brief, Agosto 2003

[10] Poole D., Marchworth A., Goebel R., “Computational Intelligence – A Logical Approach” Oxford University Press, 1998.

[11] RFID Journal: http://www.rfidjournal.com/

[12] “Smart Cards and Biometrics in a Privacy-Sensitive Secure Personal Identification System” Smart Card Alliance report. Mayo 2002.

[13] Tarjetas Inteligentes y Sistemas de Identificación Seguros: Construyendo una Cadena de Confianza” Smart Card Alliance report. Octubre 2006.

[14] Wooldridge M., Jennings N. R., “Intelligent agents: Theory and practice”. 1994.