IDENTIFICACIÓN DE INDIVIDUOS EN EDIFICIOS INTELIGENTES

Lasso M., Vidal P., Villagra A., de San Pedro M., Pandolfi D.
Laboratorio de Tecnologías Emergentes (LabTEm)
Universidad Nacional de la Patagonia Austral – Unidad Académica Caleta Olivia
e-mail: {mlasso, pjvidal, avillagra, edesanpedro, dpandolfi }@uaco.unpa.edu.ar

Errecalde M.
Laboratorio de Investigación y Desarrollo en Inteligencia Computacional (LIDIC)
Universidad Nacional de San Luis
e-mail: merreca@unsl.edu.ar

RESUMEN

En el marco del Laboratorio de Tecnologías Emergentes (LabTEm), de la UNPA con la colaboración de la línea de Agentes y Sistemas Multi-agente del Laboratorio de Investigación y Desarrollo en Inteligencia Computacional (LIDIC) se ha comenzado a trabajar en el proyecto de investigación denominado "Administración de Edificios Inteligentes, mediante Sistemas Multiagente". 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 para que se adecue a sus necesidades y gustos. El objetivo de este trabajo es abordar la problemática que surge a partir de la identificación de las personas que tienen acceso a un hogar, oficina o edificio, a través de un sistema Multi-agente, de manera que se puedan garantizar la protección de todos sus bienes, tanto tangibles, como intangibles, como así también la adecuación del ambiente donde ingrese.

1. INTRODUCCIÓN

Un ambiente o edificio inteligente puede ser definido como aquel que utiliza tecnología computacional para controlar en forma automática su funcionamiento permitiendo realizar las tareas cotidianas de manera más fácil, segura, confortable y eficiente.

Un tema muy vigente actualmente y con mucha demanda por parte de la sociedad tiene que ver, principalmente con la seguridad y la protección de sus bienes. Las agresiones, recibidas por las personas no solo suelen ser de tipo física, sino también digitales, todas las personas necesitan confiar en sistemas que les facilite la seguridad tanto de sus bienes materiales tangibles como de sus bienes intangibles, como pueden ser sus sistemas de información o sistemas digitales en general.

Tanto en hogares como en oficinas o edificios en general, cada una de las personas habilitadas para ingresar debe poseer algún sistema de identificación que lo proteja de cualquier tipo de agresión y/o prepare el ambiente de acuerdo a sus necesidades. Un Sistema de Identificación Segura (SIS), debe ser diseñado para responder a un requerimiento fundamental de los individuos, dándole confianza y asegurándole que la persona que se está identificando es realmente quien debe ser.

Certificaciones digitales, firmas electrónicas, tarjetas o PINes (Personal Identification Number) o técnicas biométricas de identificación son algunos de los métodos actuales que brindan en menor o mayor escala algún grado de seguridad a las personas.

Muchos estudios y muchas propuestas han surgido con respecto a cuál de los métodos actuales vigentes para la identificación de personas es la más adecuada para una determinada situación.

Los problemas con estas características han sido abordados usualmente mediante los denominados "sistemas inteligentes", englobando con este término tanto a sistemas de Soft Computing (http://www.ieeecis.org) como a enfoques clásicos de Inteligencia Artificial basados en representaciones y formas de razonamiento de alto nivel [1, 2, 3]. Más allá de las diferencias significativas entre estos enfoques existe un concepto unificador conocido como *agentes*

inteligentes [1, 4, 5, 6, 7, 8, 9, 10]. La problemática vinculada a la creación de la interfaz entre la identificación de personas, la autenticación de la misma y los permisos asignados o condiciones ambientales que deberán sucederse, pueden ser abordadas con un enfoque multi-agentes, como ha quedado reflejado en trabajos recientes vinculados al análisis, desarrollo e implementación de sistemas para la administración autónoma e inteligente de edificios para uso familiar, oficinas y de tipo industrial. A partir de esta tendencia, han surgido un número considerable de desafíos tanto teóricos como prácticos a los cuales el paradigma de los sistemas multi-agente debe dar una respuesta acorde a las particularidades de esta área de aplicación [11].
En este contexto, este trabajo describe en la sección 2 algunos aspectos generales de los edificios inteligentes, en la sección 3 una visión de los sistemas de identificación más comunes y finalmente en la sección 4 se presentan las líneas de investigación y trabajos futuros.

2. EDIFICIOS INTELIGENTES (EI)

Con el correr de los años, los edificios y construcciones habitados 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 necesario 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 las siguientes:
• *Ahorro de energía*: la automatización de edificios permite un menor consumo de energía, controlando de manera flexible y dinámica la calefacción, refrigeración e iluminación de las distintas partes de un edificio. Un ejemplo simple, es el apagado automático de luces en una habitación, cada vez que se detecta que no existe ninguna persona en ella.
• *Servicios personalizados*: es común que en un edificio inteligente sus habitantes puedan expresar sus preferencias respecto a la intensidad de la luz y calor de su oficina. Este tipo de servicios pueden ser muy útiles y placenteros para las personas en la medida que el edificio pueda satisfacer automáticamente dichas preferencias.
• *Seguridad*: este aspecto abarca tanto la seguridad de los habitantes del edificio como así también la del edificio en sí mismo. Como ejemplo del segundo tipo de aplicación podemos mencionar aquellos casos en que el edificio debe mantener una temperatura mínima para las cañerías de un edificio para evitar que éstas se rompan debido al congelamiento.
• *Vigilancia*: en este caso, un sistema de detección de intrusos puede ser establecido que cierre todas las puertas y ventanas automáticamente y dé aviso a los servicios de vigilancia tradicionales.
Si bien hoy en día muchos de los dispositivos y sistemas utilizados para la automatización de edificios suelen ser referenciadas como "inteligentes", la mayoría de las aplicaciones en ésta 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 computadora. 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:* el sistema debe proveer del soporte necesario para permitir extensiones y modificaciones en las políticas que se adoptan en el edificio. Idealmente, el sistema debería tener la capacidad de detectar y adaptarse automáticamente a estos cambios.

• *Escalabilidad:* el sistema debería funcionar adecuadamente en pequeños edificios como así también en edificios con muchos pisos y habitaciones. Las extensiones en la construcción y en la incorporación de nuevos dispositivos, no debería involucrar un costo significativo para la adaptación del sistema de control del edificio a los nuevos requerimientos.

• *Robustez*: las fallas en el sistema, no deberían tener un gran impacto. Sería inaceptable que un error de programación haga el edificio incontrolable.

• *Amigabilidad:* el sistema debería asistir a sus habitantes y facilitarles sus tareas automatizando gran parte de sus actividades rutinarias. Sin embargo, debería ser posible que las personas tomen el control y realicen estas actividades en forma manual cuando lo consideren necesario.

• *Tiempos de respuestas adecuados*: el ambiente es esencialmente de tiempo real y el sistema debería ser lo suficientemente reactivo como para realizar sus decisiones en un lapso de tiempo acotado.

En la sección siguiente se realiza una descripción de los sistemas de identificación que resultan necesarios e imprescindibles para garantizar la seguridad de las personas y vigilancia dentro de un edificio

3. SISTEMA DE IDENTIFICACIÓN SEGURA (SIS)

Dado que una de las aplicaciones identificadas que actualmente preocupan en demasía a los habitantes de hogares, edificios o empresas es su seguridad personal y la posibilidad de que intrusos ocasionen problemas no deseados, es necesario definir algún sistema de identificación.

Cualquier sistema de identificación debe definir las metas de seguridad apropiadas y los atributos dentro de una política de seguridad. Esta política debe identificar el nivel de seguridad apropiado y conmensurado con el valor de cada bien protegido. Una identificación segura debe ser una interfaz entre una forma de acceso individual y la facilidad de acceder a un sistema deseado. Un servicio creíble necesita proveer autenticidad y validación al mismo tiempo. La identificación, una vez autenticada y validada, deberá contener o referenciar información que es usada para verificar no sólo la identidad del individuo sino también sus permisos

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 las credenciales o sistemas de identificación solo sean emitidas por las organizaciones autorizadas, que los individuos tengan pleno acceso a los privilegios indicados en su identificación y que la credencial sea emitida para la persona correcta, evitando duplicaciones o mecanismo fáciles de falsificar, debe ser fácil de usar, para los usuarios 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 de 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 tres grandes grupos: sistemas basados en *algo conocido* (contraseña), sistemas basados en *algo poseído* (tarjeta inteligente), sistemas de identificación por radiofrecuencias (RFID) y sistemas biométricos (basados en características del individuo). 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.
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. La autenticación es el mecanismo más básico, y el primero que existe de protección de un sistema y consiste en comprobar que un usuario es quien dice ser, y comúnmente se basa en nombre de usuario/contraseña. Sin embargo, una autenticación tan simple deja mucho que desear, pues si alguien conoce ambos datos o quién posee la tarjeta no es la persona que debe ser, podría entrar en el sistema falseando la identidad y tendría acceso a todas las aplicaciones para las que está autorizado.
En los sistemas basados en algo poseído, una tarjeta inteligente [12] incluye un chip de computador agregado a la tarjeta, que puede ser un micro controlador con una memoria interna o una memoria interna solamente. La tarjeta puede ser conectada al lector, ya sea directamente por contacto físico o de forma remota, a través de una interfase electromagnética. Al tener un micro controlador agregado, las tarjetas inteligentes tienen la habilidad de almacenar enorme cantidad de datos, realizar sus propias funciones en la misma tarjeta (por ejemplo encriptar y hacer firmas digitales) e interactuar inteligentemente con el lector de la tarjeta. La tarjeta de identificación puede combinar varias tecnologías de identificación, incluyendo el chip, marcas de seguridad visual, tiras magnéticas, códigos de barra y/o tiras ópticas.
Los sistemas de identificación por radiofrecuencias (en inglés *Radio Frequency Identification* o *RFID*) [13] son dispositivos que están sustituyendo poco a poco a las etiquetas de códigos de barras y a las tarjetas magnéticas en todas sus aplicaciones. En el control de accesos se gana en comodidad, no es necesario el contacto físico de la tarjeta con el lector, lo que lo hace más cómodo y más rápido de usar. Este es un sistema en el que el interrogador (el dispositivo que lee los datos) tiene que poder leer muchas tarjetas diferentes, tantas como usuarios haya autorizados.
La biometría es un sistema de reconocimiento humano basado en características físicas (huella dactilar, iris, geometría de la mano, rostro) y de comportamiento (voz, firma, dinámica del tecleo o forma de caminar), cuyas aplicaciones tienen un único propósito y es la autenticación de los individuos para evitar fraudes, dado que valida rasgos únicos e irrepetibles en cada individuo. Los sistemas de identificación basados en biométricos capturan una imagen biométrica, en vivo, y lo compara con la imagen biométrica almacenada que fue capturada al momento en que el individuo se registró en el sistema. Esta equiparación biométrica uno-a-uno, verifica que el portador de la identidad es la mima persona que se registró en el sistema de identificación y que es la persona correcta para usar dicho documento [14].

4. LÍNEAS DE INVESTIGACIÓN Y TRABAJOS FUTUROS.

La discusión no se plantea si un edificio es más o menos inteligente, sino en la forma en que las personas deben interactuar con el mismo sin que les ocasione grandes cambios en sus rutinas. Confort, gestión de energía y seguridad son las principales aplicaciones en un edificio inteligente. En este contexto, el LabTEm , en colaboración con el LIDIC, ha comenzado a trabajar en sistemas

de identificación de individuos que provea la posibilidad de identificar a las personas y una vez generada la autentificación habilitar los recursos configurados para ese usuario utilizando para ello el enfoque multi-agente.

En esta primera etapa se están analizando las distintas tecnologías y evaluando costos y beneficios en el servicio que prestan. Probablemente una única tecnología no sea suficiente o garantice el mayor nivel de seguridad, pero cualquiera de éstas pueden combinarse de manera que el sistema de identificación, refuerce significativamente la confianza de los usuarios reduciendo el riesgo. Esta tarea involucra aspectos teóricos y prácticos y en especial el estudio de las nuevas tecnologías existentes para la implementación en edificios inteligentes. Para esta investigación el grupo cuenta con el asesoramiento técnico de empresas tecnológicas del medio, interesadas en la temática de los edificios inteligentes y en la seguridad no sólo de las personas sino también de sus bienes tangibles e intangibles.

AGRADECIMIENTOS

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

REFERENCIAS

[1] Poole D., Marchworth A., Goebel R., "Computational Intelligence – A Logical Approach" Oxford University Press, 1998

[2] Bratman M. Israel D.J., Pollack M. E., "Plans and resourece-bounded practical reasoning". Computational Intelligence, vol 4, nro. 4. pp 349-355. 1988

[3] Garcia A.J., Simari G.R., "Defeasible logic programming: an argumentative approach". Theory and Practice of Logic Programming. Vol 4, Nro.2 pp. 95-138. 2004

[4] Wooldridge M., Jennings N. R., "Intelligent agents: Theory and practice". 1994.

[5] 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.

[6] S. Russell and P.Norvig, Artificial Intelligence - A Modern Approach. Prentice Hall, second ed., 2003.

[7] S. Kalenka and N. R. Jennings, Cognition, Agency and Rationality, ch. Socially Responsible Decision Making by Autonomous Agents, pp. 135–149. Kluwer, 1999.

[8] M.Wooldridge, Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence, ch. Intelligent Agents, pp. 27–78. The MIT Press, 1999.

[9] M. Wooldridge, An Introduction to MultiAgent Systems. Chichester, England: John Wiley & Sons, 2002.

[10] M.Wooldridge, An introduction to multiagent systems, ch. 4. Practical Reasoning Agents. John Wiley and Sons, LTD, 2002.

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

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

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

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