Agentes móviles

Sistemas Multi-Agente y Sistemas Autónomos

Juan A. Botía

Departamento de Ingeniería de la Información y las Comunicaciones, Universidad de Murcia

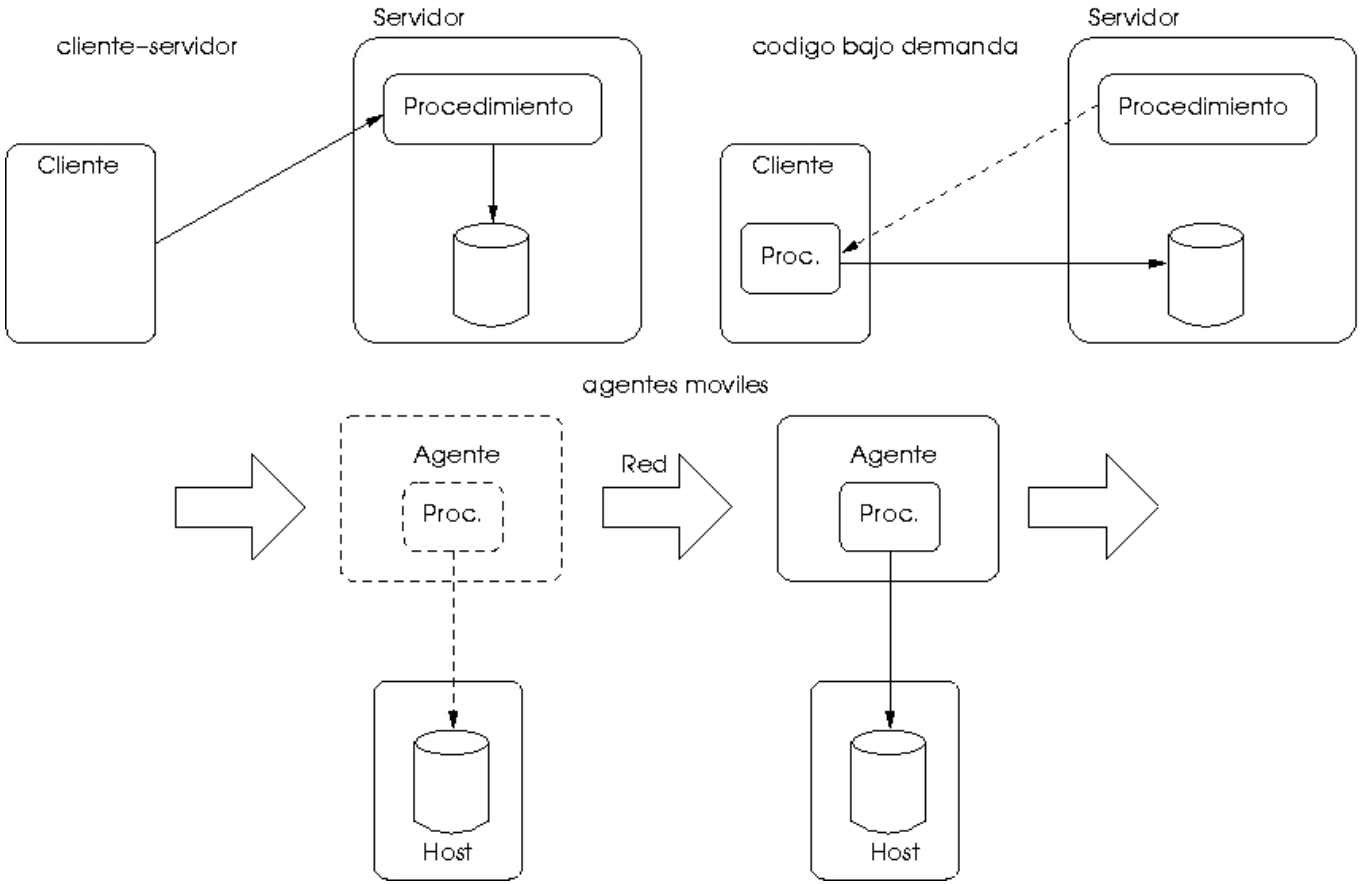
November 14, 2007

1. Agentes Móviles
   - Introducción
   - Motivación
   - Problemas de seguridad

Movilidad en agentes

- La movilidad en los agentes software es una propiedad ortogonal.
- Un agente móvil no está limitado al sistema en el que comienza su ejecución (es libre para moverse entre las máquinas de una red)
- Es capaz de transportar su **estado y código** con él a otro entorno de ejecución

Evolución del paradigma de computación



Evolución del paradigma de computación (y II)

- Paradigma cliente-servidor: el cliente necesita de determinada *inteligencia* para saber qué servicio es el que debe invocar
- Paradigma de código bajo demanda: se obtiene el código justamente cuando se necesita
- Paradigma de agentes móviles:
  - el código no está asociado a un único servidor
  - los agentes móviles deciden cuándo y hacia dónde se van a mover
- La flexibilidad aumenta cronológicamente

¿Para qué agentes móviles?

Razón 1: reducen el tráfico en la red

- En S.D. tradicionales, una interacción entre dos entidades situadas en máquinas distintas necesita, típicamente, de varios pasos de mensajes entre las entidades
- Si la comunicación es segura, la situació se agrava
- Con el paradigma de agentes móviles:
  - El agente iniciador especifica la interacción que ha de tener lugar
  - Cuando el agente móvil llega a su destino, la interacción tiene lugar localmente
  - Tráfico reducido a transportar al agente ida y vuelta

¿Para qué agentes móviles?

Razón 2 : Eliminan la latencia introducida por la red

- Piénsese en un sistema de robots operados en una planta industrial através de una red de telecomunicaciones
  - Cada uno de esos robots debe poder ser controlado en tiempo real
  - la red, en determinados momentos de alto tráfico puede introducir una latencia intolerable
  - El paradigma de agentes permite que, el lugar de enviar las intrucciones por la red, se mande directamente el controlador al robot

¿Para qué agentes móviles?

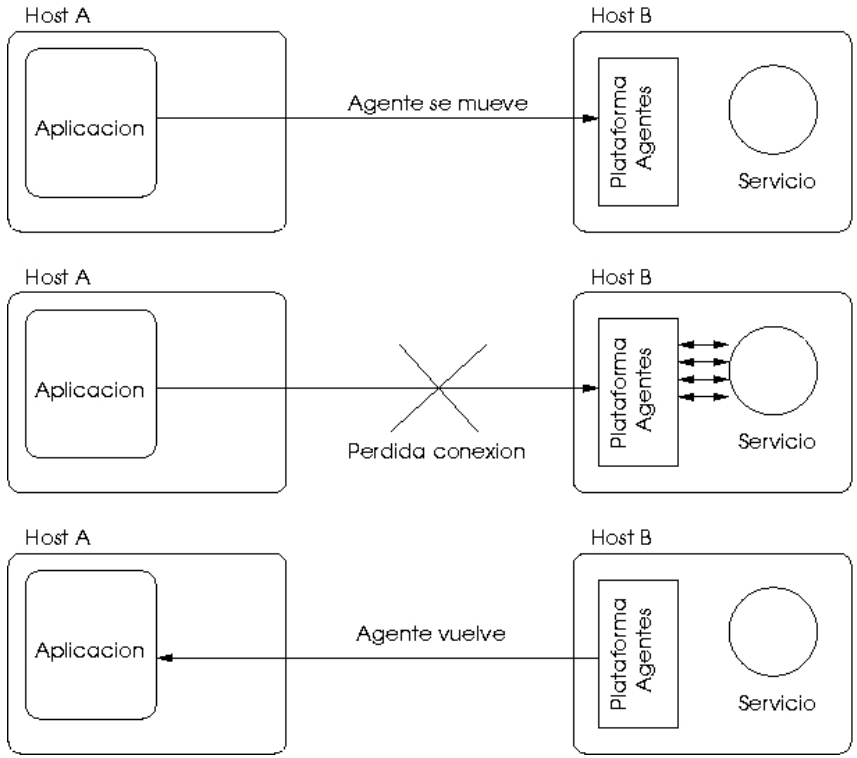
Razón 3: Encapsulan protocolos

- los protocolos de comunicaciones especifican
  1. Mensajes intercambiados
  2. Codificación de datos salientes
  3. Decodificación de datos entrantes
- Mantenimiento de protocolos implica mantenimiento del software de **todo el sistema distribuido**
- Los agente móviles utilizan interacciones locales (i.e. protocolos propietarios)

¿Para qué agentes móviles?

Razón 4: Su ejecución es autónoma y asíncrona

- Conexión permanentemente abierta puede ser un problema tanto técnico como de viabilidad económica
- Si la tarea através de conexión puede encapsularse en un agente software móvil
  - no es necesario el mantener una conexión desde el dispsitivo móvil
  - el agente realiza la tarea disociado del dispositivo



¿Para qué agentes móviles?

Razón 5: Los agentes se adaptan dinámicamente

- Son autónomos y situados
  - tienen la habilidad de sondear su entorno para responder rápidamente a cambios
- si las condiciones de los servidores en donde se ejecutan (e.g. la carga de los mismos) cambian, se pueden distribuir de tal forma que la situación vuelva a ser la idónea para poder resolver el problema que les ocupa

¿Para qué agentes móviles?

Razón 6: Soportan la heterogeneidad de forma natural

- la computación distribuida es heterogénea per se
- Los agentes viven en plataformas homogéneas, por lo tanto superan sin esfuerzo la heterogeneidad

Razón 7: Los agentes son robustos y tolerantes a fallos

- Son autónomos y situados
  - tienen la habilidad de sondear su entorno para responder rápidamente a cambios
- Al poder detectar condiciones desfavorables para su ejecución (o incluso un aviso de shutdown) en el servidor, en cualquier momento pueden llegar a decidir cambiar de host para poder seguir ejecutando su tarea.

Problemas de seguridad en agentes móviles

La computación con código móvil puede sufrir los siguientes tipos de ataques:

- *hijacking*: todas las operaciones, no deseadas, que pueden hacerse con un agente una vez ha llegado a un host malicioso
  - Espiar su estado
  - Espiar su codigo, etc
- *brainwashing*: posibles cambios en el código que pueden alterar la funcionalidad o el estado del agente llevándolo a realizar acciones para las cuales no estaba programado en un principio

En un SMA con agentes móviles se debe garantizar la integridad y la privacidad computacionales (i.e. código intácto y secreto)

Escenario ilustrativo

*Un agente móvil encargado de comprar nuestros billetes de avión es enviado a la red para visitar una lista ordenada de servidores de varias compañías aéreas, con el objeto de buscar un billete de avión adecuado y, una vez que se ha escogido la mejor oferta, reservar el billete. Un ataque simple y provechoso para el atacante consistiría en copiar el código y el estado del agente, modificándolo de tal forma que olvide todos los servidores que ha visitado anteriormente y escoja erróneamente una oferta de la aerolínea con el servidor malicioso. Otro ataque consistiría en aumentar los precios hasta el umbral interno del agente, o simplemente, y si es posible, robar el dinero electrónico del agente. Incluso más problemático sería un escenario en el que el agente no solo reserva el billete sino que además debe firmar la reserva con la firma electrónica del usuario, para ello necesita transportar con él la clave privada del mismo [sería posible suplantar al usuario si el atacante se apropia de su clave privada] [**?**]*

Tareas a cumplir para garantizar seguridad

- el agente móvil debe ser capaz de protegerse así mismo contra copia por parte de un host malicioso (integridad de datos y ejecución),
- el agente móvil debe ser capaz de ocultar a terceros el programa que debe ejecutar para cumplir su tarea (privacidad de código) y
- el agente móvil debe ser capaz de firmar documentos sin exponer la clave privada del usuario (computación en público con secretos).

Solución: servidores confiables + esquemas de criptografía (autenticación de agente y autenticación de host destino)