Distributed Artificial Intelligence and Intelligent Agents

Agent Mobility and Trends in Agent technology

Mihhail Matskin

Content

1. What are mobile agents?
2. Remote Procedure Calls vs. mobile agents
3. Security
   - Threats, security of host, security of agent
4. Requirements to Mobile Agents
5. Future trends

References - Curriculum

- Wooldridge: ”Introduction to MAS”,
  - Chapter 9, Section 9.4
- Not in curriculum:
  - White, J. E., Mobile Agents, in Bradshaw, J. (ed.), Software Agents, MIT Press, Cambridge, MA, 1997, p. 437-472.
  - D. M. Chess, C. G. Harrison, A. Kershenbaum. Mobile Agents: Are they a good idea? Research Report, IBM Research Division, T. J. Watson Research Center, 1995, 21 pages.

Examples

Example 1

- Client-Server computing
- A task is to delete from a file server all files which are at least two months old
- Each call to server involves a request sent from user to server and a response sent from server to user
- Deleting n files requires 2(n+1) messages

Example 2

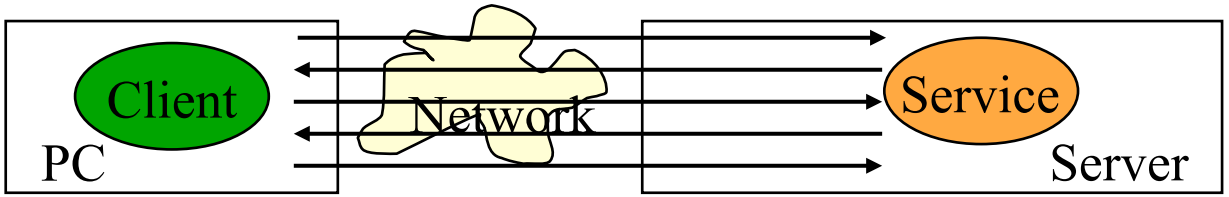
- Portable PC connected to network
- Time of available connection is much shorter than query processing time

What are Mobile Agents 

- Agents that are capable of transmitting themselves – their code and their state – across a computer network, and recommencing execution at a remote site.
- The program chooses when and where to migrate.
- It can suspend its execution at an arbitrary point, transport itself to another machine and resume execution.

➢ *Moving programs while they run!*

Current Approach - Remote Procedure Calls



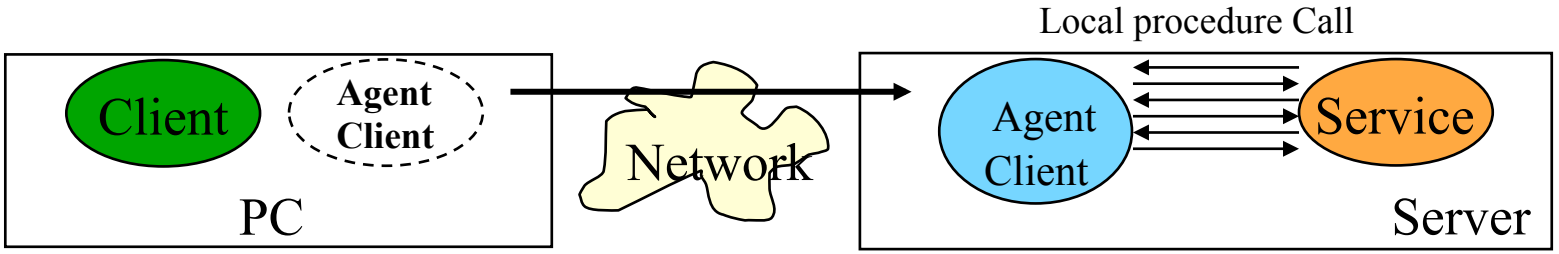
- Enables one computer to call procedures in another.
- The two computers agree in advance upon a **protocol**:
  - The effects of each remotely accessible procedure and the types of its arguments and results.
- Each interaction entails two acts of communication - request & acknowledge

  → ongoing interaction requires ongoing remote communication!

  → e.g.: From a file server, delete all files that are atleast two months old.

  RPC: n files => 2(n+1) messages

New Approach - Remote Executing



- One computer not only calls procedures on another computer, but also provides the procedures.
- Each message contains the procedure + its arguments.
- The two computers agree in advance upon a **language**:
  - instructions and the types of data that are allowed.
- A user agent and a server can interact without using the network once the agent is transported

  → ongoing interaction does not require ongoing remote communication!

New Approach - Remote Executing

- A mobile agent is a program that can migrate from machine to machine in a heterogeneous network
- The program chooses when and where to migrate
- It can suspend its execution at an arbitrary point, transport itself to another machine and resume execution

Some distinctions between approaches to remote execution

- A program which is sent without execution state to remote CPU executes there, possibly communicating with other CPUs and then terminates - remote execution (Java programs would fall into this class)
- A program which carries execution state with it and is sent to a remote CPU executes there, possibly communicating with other CPUs and then moves again to a third CPU or returns to its origin - mobile agent

Advantages of RE over RPC

- **Tactical**
  - Performance - due to less message passing over the network.
  - Less connection time - need network connection only to transport the agent.
- **Strategic**
  - Customization - agents let manufacturers of client s/w extend the functionalities of the server s/w.
  - In a RPC application, the server component needs to be statically installed by the user. In RE, they are dynamically installed by the application itself – which is an agent.
  - New RPC-based applications - decisions by the provider. New RE-based applications - decision by the user.
  - A public network becomes like a platform.

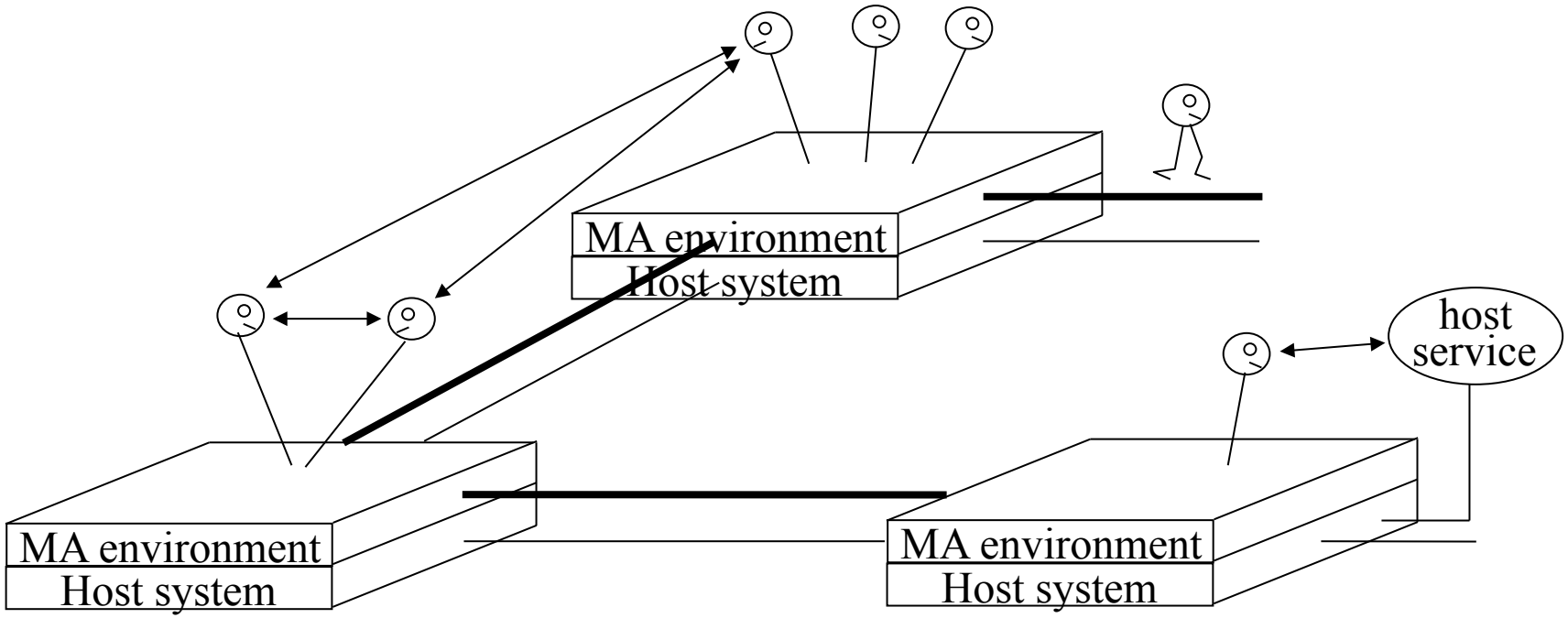
Basic Mobile Agent Environment

- A mobile agent environment is a software system which is distributed over a network of heterogeneous computers.
- Its primary task is to provide an environment in which mobile agents can execute.
- It implements the majority of models which appear in the mobile agent definition.

Basic Mobile Agent Environment

- supports services related to the mobile agent environment itself
- supports services pertaining to the environments on which the mobile agent environment is built,
- provides services to support access to other mobile agent systems
- provides support for openness when accessing non-agent-based software environments

Basic mobile agent environment



Mobile Agents

Security is a significant concern with mobile agent-based computing

Security in Using Agents 1

- Some general issues in using agents:
  - **Delegation**: you are delegating to the agent some of your authority. This means that agents are doing things that you cannot always see.
  - **Mobility**: they may be doing it on the other side of the planet. Or, an agent from the other side of the planet may be doing it on your server.

Security in Using Agents 2

- Some general issues in using agents, contd.:
  - **Viruses**: mobile agents share many characteristics with viruses. In creating an environment for agents, there is the additional risk that we expose weaknesses that may enable viruses to breed.
  - **Trust**: humans have classified their co-workers into those who are reliable and those who are not.

Mobile Agents and Viruses

- It's impossible, in principle, to verify with complete certainty if an arbitrary program is a virus or not.
- In practice, the problem of writing a program that can verify the correct behavior of another program is unsolved.
- It's difficult to define the necessary and sufficient tests that an agent must pass in order to determine its intentions.
- Some precautions:
  - Restriction of access to critical resources.
  - Restriction on altering other programs.

Delegation

- The purpose of an agent is to perform some tasks that would otherwise be performed by its user.
- The agent may need many, if not all, of the access rights of the user.
- In a security environment, this can be readily achieved by passing the copy of the user's certificate to the agent.
- In this regard, the agent is indistinguishable from any other applications employed by the user.
- The certificates are valid for a finite period, defined by the security administrators.

Delegation for agents

- performing the full delegation is not a big problem
- a problem is to limit delegated authority
- agent is more flexible and unpredictable than a traditional application

Security for Hosts

- **Limiting delegation**:
  - Give the agent and the user separate identities
  - Secure co-processors: have a physically separate processor on which the agent runs, execute the agent in a ”padded cell”
  - Allow the agent to interact with the system environment only in a language with limited system level expressiveness
- **Limiting resource consumption**:
  - Limit the amount of each resource that an agent is permitted to consume
  - Limit the amount of e.g. money and CPU time an agent can access (e.g. Telescript)

Security for Agents

- We need to protect mobile agents from malicious hosts because:
  - Agents have a right to privacy!
  - We often do not want to send our programs to a remote host, as to do so might enable the recipient to determine its purpose, and hence our intent.
  - The agent might be modified (sabotaged) in some way, without the owner's knowledge or approval.

Protection of mobile agents from malicious hosts

- current consensus is that it is computationally impossible to protect a mobile agent from a malicious host
- authentication of the executing server
  - easy for a single host
  - difficult for multiple hosts
- agent privacy
  - execution in a highly trusted environment
  - encapsulating all methods and data and high protection in MA environment

Security for Agents

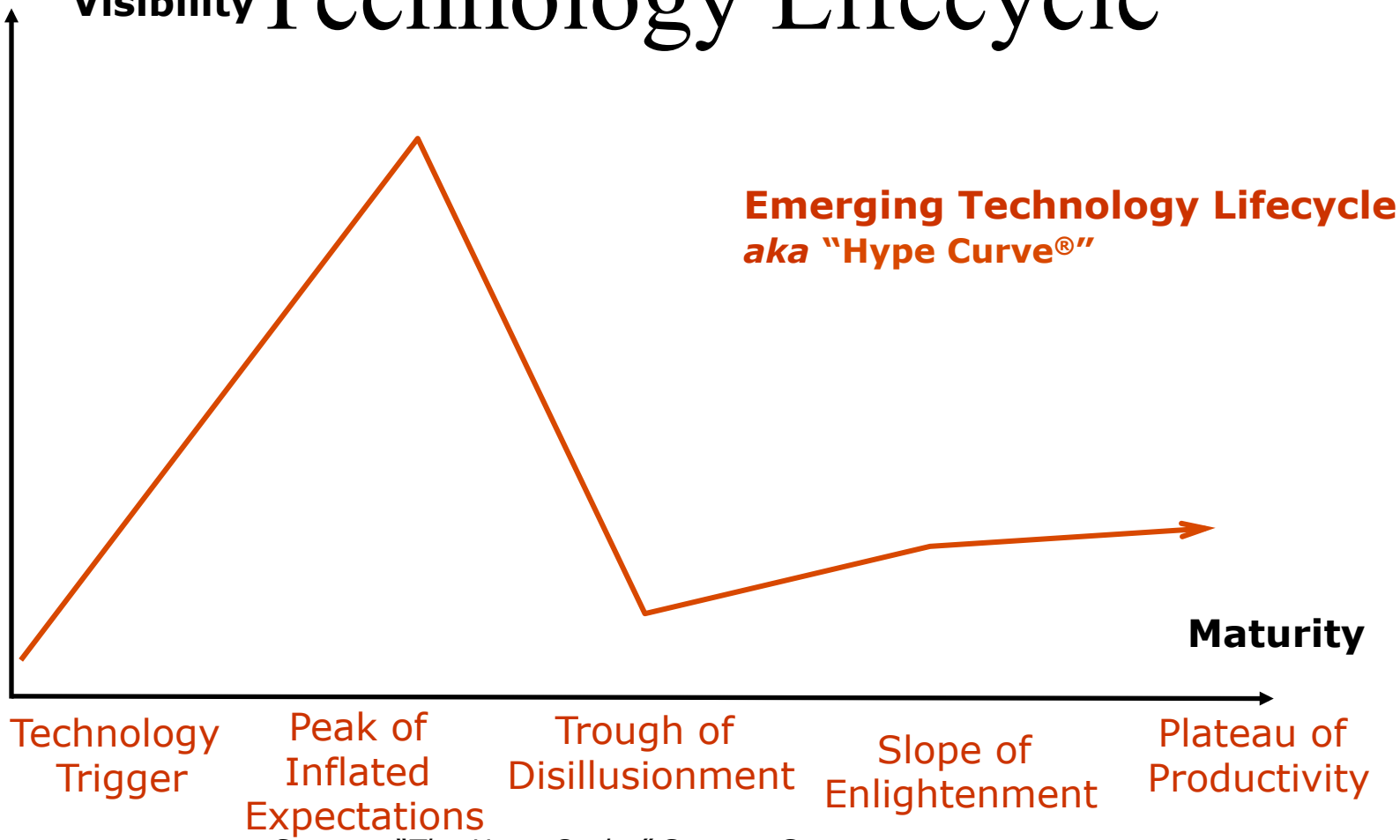
- Some possibilities for protection:
  - Data integrity - an agent can be protected in transit by using conventional encryption techniques.
  - Origin authentication – certification.
  - Access itinerary control – restriction on visiting some environments.
  - Privacy and integrity of gathered information
    - Stateless gathering
    - Stateful gathering

General Requirements to Mobile Agent Environments

- Expressiveness as a programming language
- Ability to execute remotely or to transport state
- Support for agent communication language
- Security support
- Management support

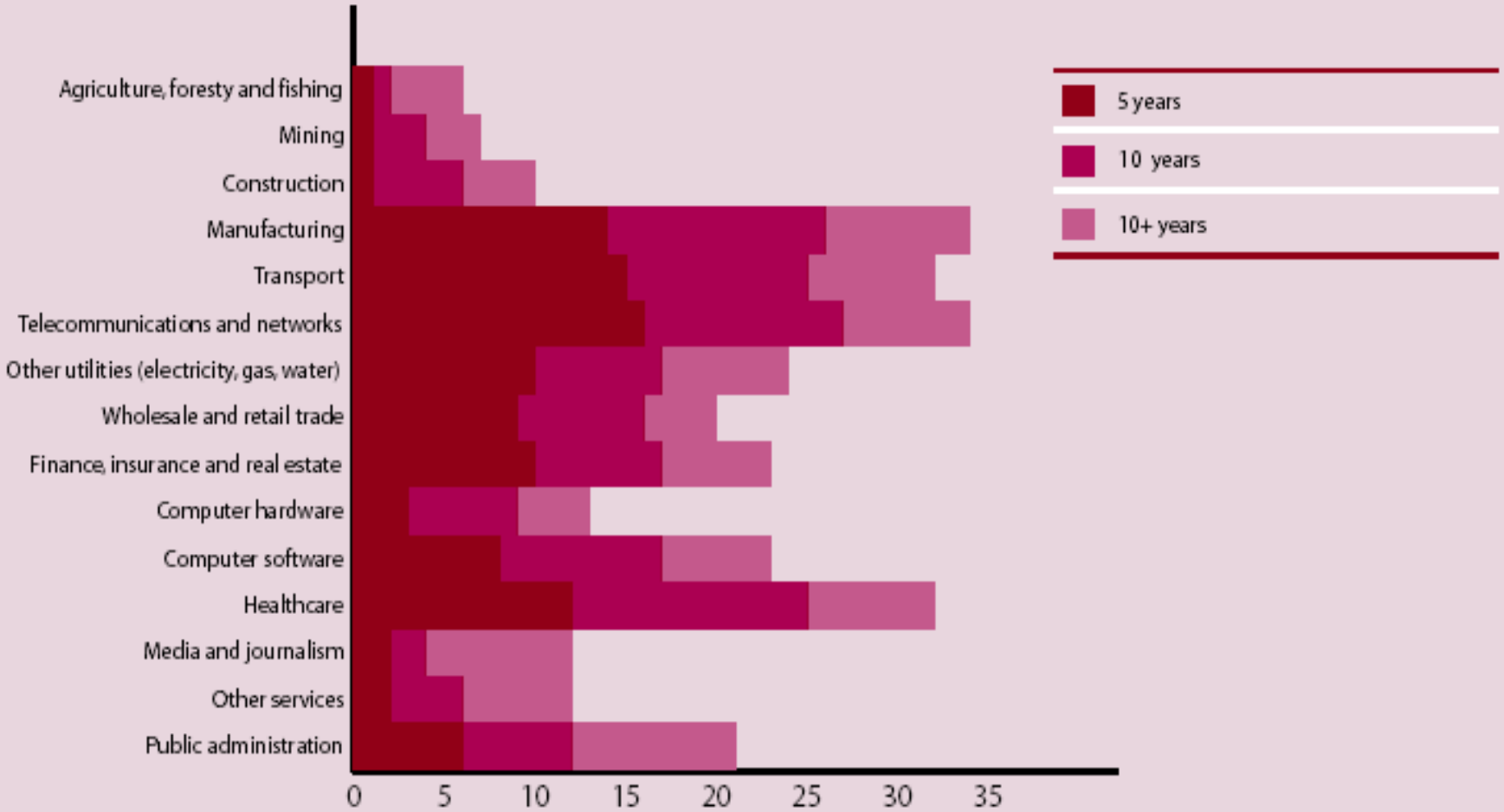
Trends in Agent Technology

Remember the Emerging Technology Lifecycle



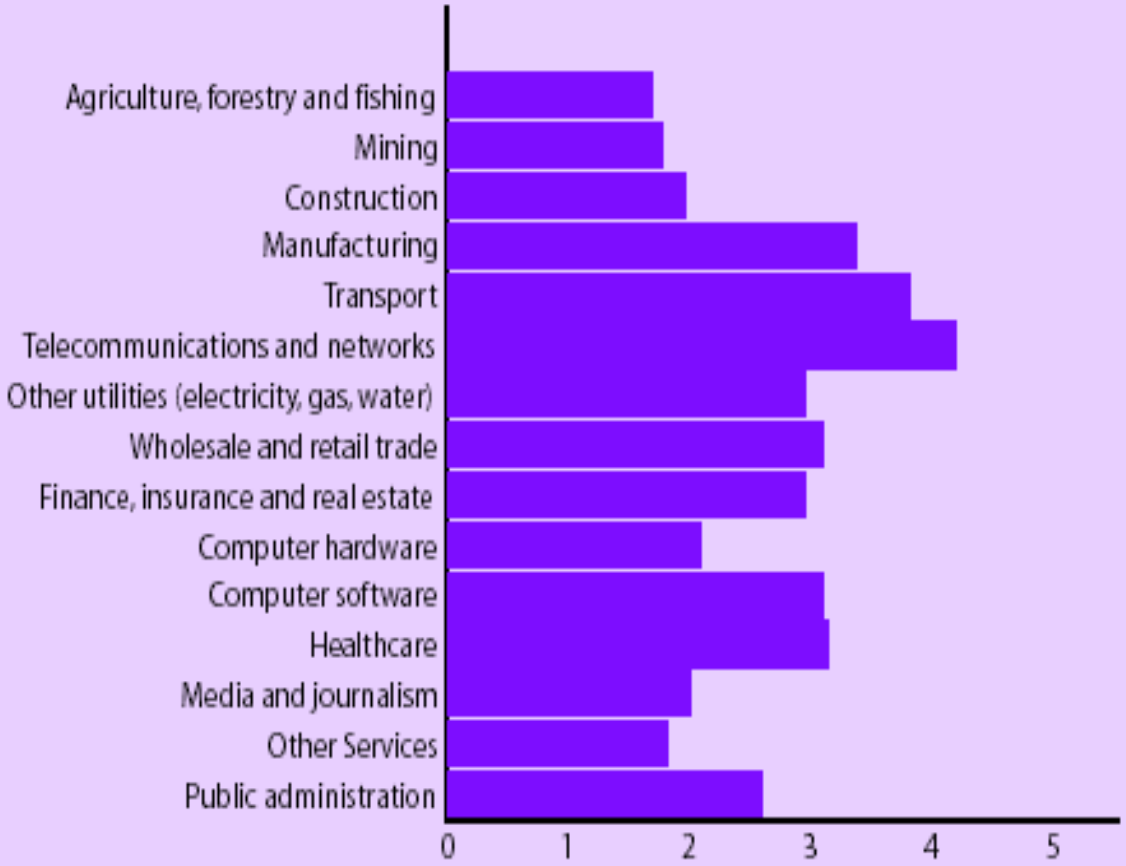
Source: *"The Hype Cycle,"* Gartner Group, ©1995-2004

Figure 6.1: Manufacturing, transport, telecoms and healthcare will encourage agent deployment



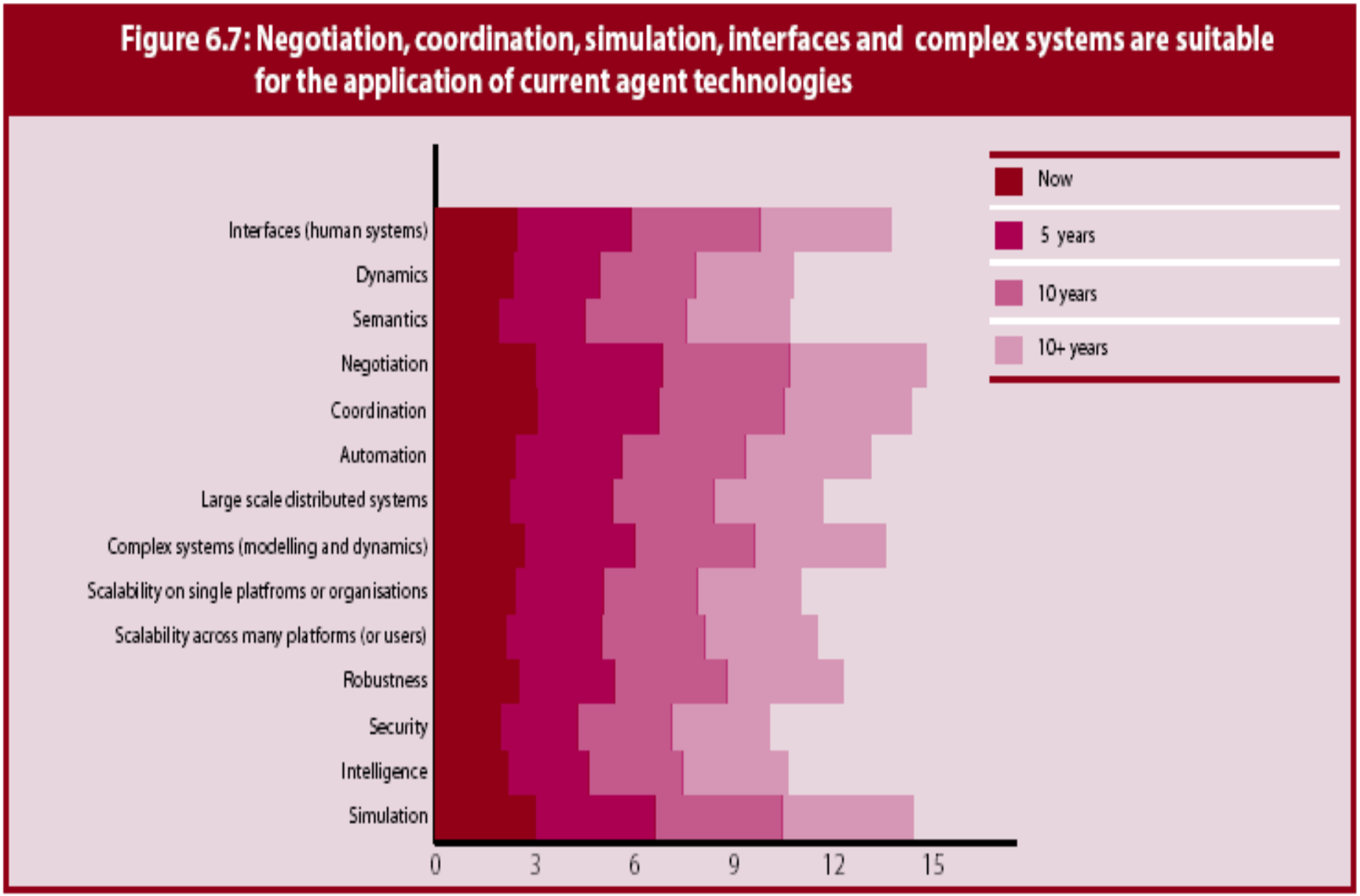
From: Agent Technology: Computing as Interaction. A Roadmap for Agent Based Computing. AgentLinkIII

Figure 6.2: Agents will make the greatest impact in telecoms, transport and manufacturing



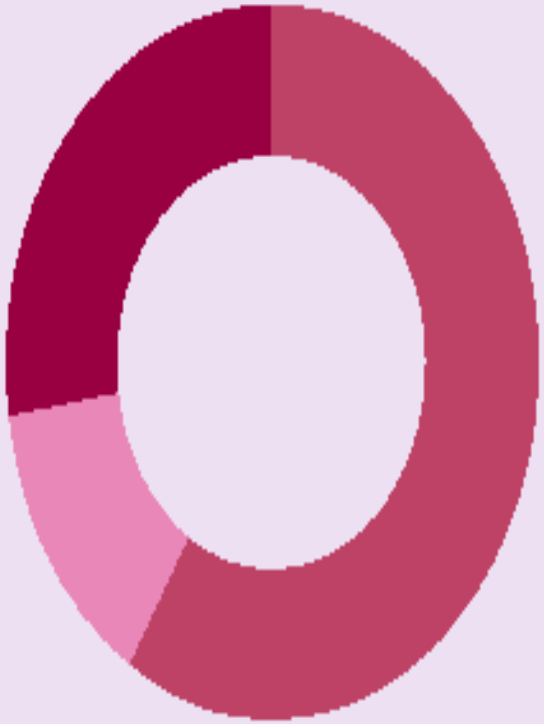
From: Agent Technology: Computing as Interaction. A Roadmap for Agent Based Computing. AgentLinkIII

Figure 6.7: Negotiation, coordination, simulation, interfaces and complex systems are suitable for the application of current agent technologies



From: Agent Technology: Computing as Interaction. A Roadmap for Agent Based Computing. AgentLinkIII

Figure 6.10: Most believe that agent technology will not replace object technology but complement it instead

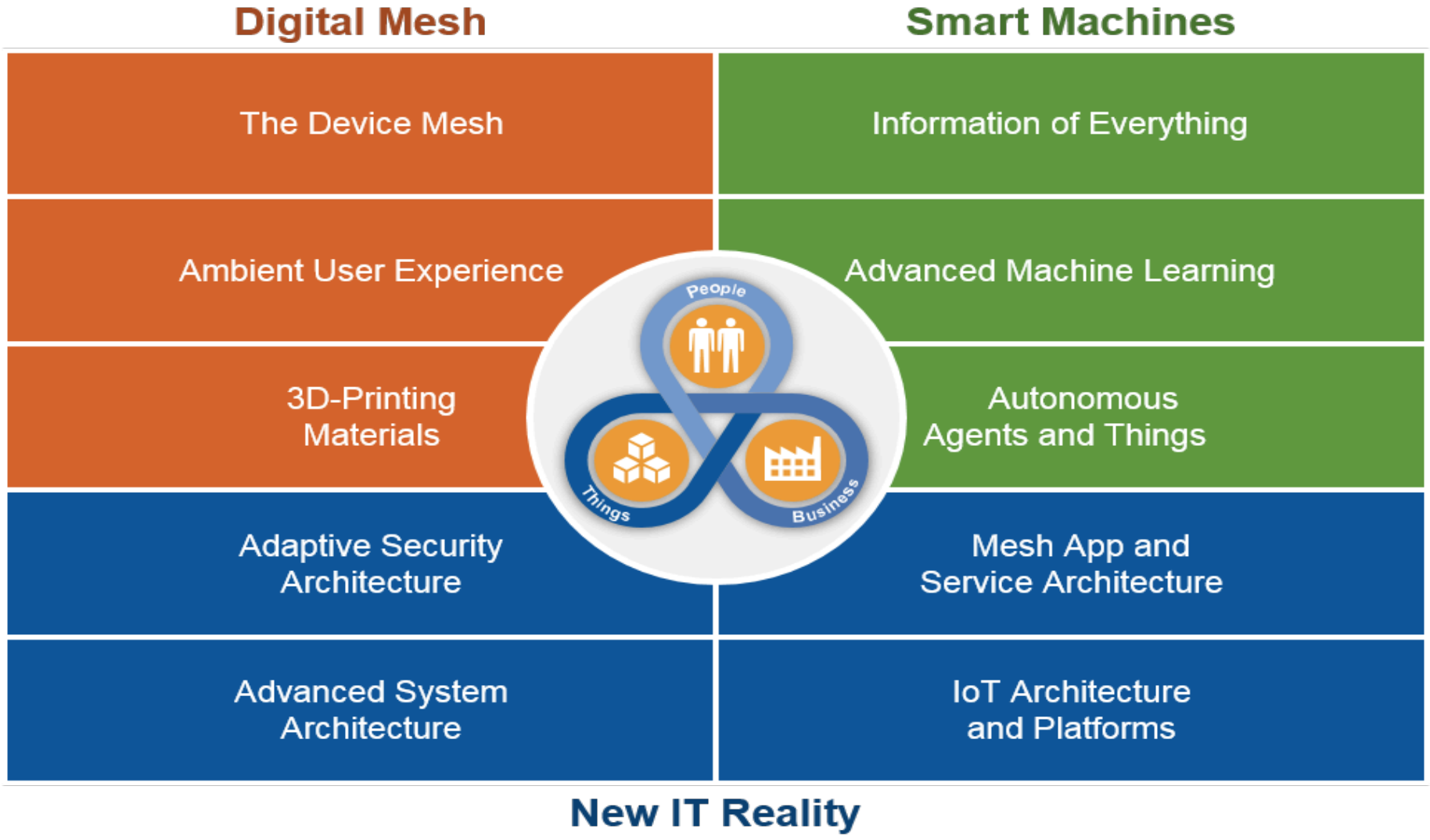


When will agent technology replace object technology?

2010-2020	27%
Now-2010	14%
Never	59%

From: Agent Technology: Computing as Interaction. A Roadmap for Agent Based Computing. AgentLinkIII

Gartner Identified Top 10 Strategic Technology Trends for 2016:



From Source: Gartner (October 2015)
Gartner, Inc. | G00291818

“Trend No. 6: Autonomous Agents and Things

Advanced machine learning gives rise to a spectrum of smart machine implementations — including robots, autonomous vehicles, virtual personal assistants (VPAs) and smart advisors — that act in an autonomous (or at least semiautonomous) manner. VPAs such as Google Now, Microsoft's Cortana and Apple's Siri are becoming smarter and are precursors to autonomous agents. The emerging notion of assistance feeds into the ambient user experience in which an autonomous agent becomes the main user interface. Instead of interacting with menus, forms and buttons on a smartphone, the user speaks to an app, which is really an intelligent agent. These intelligent agents may be associated with an individual app or act across multiple apps. IT leaders should explore how they can use autonomous things and agents to free people for work that only people can do.

However, they must recognize that smart agents and things are a long-term phenomenon that will continually evolve and expand their uses for the next 20 years.”

Gartner Gartner (October 2015)

Gartner, Inc. | G00291818