Using Multi-Agent Systems to Increase Privacy and Security in IoT

Andrei Olaru

andrei.olaru@upb.ro

AI-MAS Group, University Politehnica of Bucharest

3rd FIT Europe Seminar

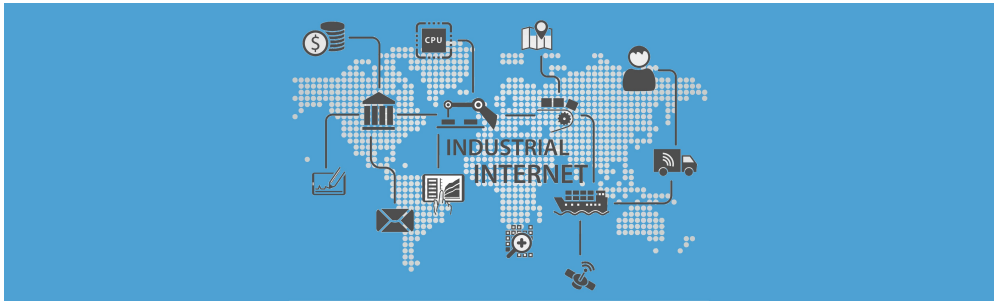
The Internet of Things: the cyber-physical system in which objects and devices are embedded with computing capabilities and are connected to the Internet.

smart home

The Internet of Things: the cyber-physical system in which objects and devices are embedded with computing capabilities and are connected to the Internet.

smart home · smart medicine

The Internet of Things: the cyber-physical system in which objects and devices are embedded with computing capabilities and are connected to the Internet.



smart home · smart medicine · smart industry

Challenges in IoT relate to

- Security
- Privacy
- Compatibility & interoperation
- Connectivity and bandwidth
- Maintenance and management

[Lamba et al., 2017]

Challenges in IoT relate to

- Security ←
  - the devices cannot be accessed by unauthorized parties
  - user data must be secure – cannot be accessed by unauthorized parties

- Privacy
- Compatibility & interoperation
- Connectivity and bandwidth
- Maintenance and management

[Lamba et al., 2017]

Challenges in IoT relate to

- Security
- Privacy ←
  - only the necessary data is shared with other parties
  - users are able to control what data they share and with whom
- Compatibility & interoperation
- Connectivity and bandwidth
- Maintenance and management

[Lamba et al., 2017]

Challenges in IoT relate to

- Security
- Privacy
- Compatibility & interoperation ←
  - difficult interoperation between communication protocols
  - difficulty in heterogeneous systems
  - some smart-* systems are not open to interoperation
- Connectivity and bandwidth
- Maintenance and management

[Lamba et al., 2017]

Challenges in IoT relate to

- Security
- Privacy
- Compatibility & interoperation – difficulty in heterogeneous systems
- Connectivity and bandwidth
- Maintenance and management

[Lamba et al., 2017]

Challenges in IoT relate to

- Security
- Privacy
- Compatibility & interoperation – difficulty in heterogeneous systems
- Connectivity and bandwidth
- Maintenance and management

[Lamba et al., 2017]

Challenges in IoT relate to

- Security
- Privacy
- Compatibility & interoperation – difficulty in heterogeneous systems
- Connectivity and bandwidth
- Maintenance and management

[Lamba et al., 2017]

Challenges in security:

- 1 ensure secure communication between devices
- 2 ensure secure access to devices
- 3 ensure update delivery to the devices
- 4 verify the identity of devices which join an open system
- 5 ensure that devices are able to operate without Internet connection
- 6 ensure security despite devices being resource-constrained

Challenges in privacy:

-  1 ensure only necessary data about users is gathered
-  2 ensure that personal information cannot leak while other data is gathered
-  3 ensure informed user consent for the gathered data
-  4 ensure any personally-identifiable information is anonymized and aggregated

Challenges in heterogeneity, openness, robustness:

-  1 ensure devices from different producers and with different owners can exist as part of the same system
-  2 ensure that new devices can join the system and be integrated
-  3 ensure that the system works when devices leave or become disconnected

What are Agents?

agere (Latin) – to do.

Agents are entities which act autonomously in an environment.

agere (Latin) – to do.

Agents are entities which act autonomously in an environment.

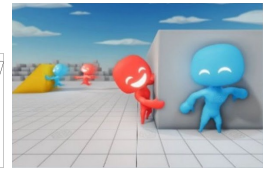
Software agents act autonomously in a socio-technical environment,
interacting with tools, human users, and other agents,
in order to reach their goals.

Multi agent systems are used in a wide range of applications:

- agent-based model simulation

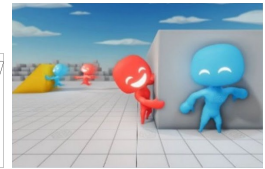
Multi agent systems are used in a wide range of applications:

- agent-based model simulation
- multi-agent learning



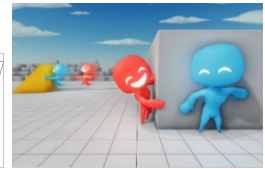
Multi agent systems are used in a wide range of applications:

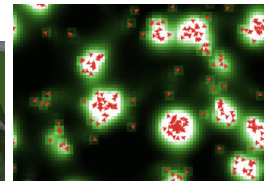
- agent-based model simulation
- multi-agent learning
- multi-robot control



Multi agent systems are used in a wide range of applications:

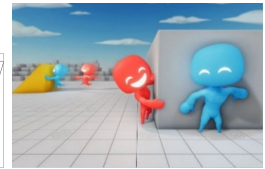
- agent-based model simulation
- multi-agent learning
- multi-robot control
- swarms and self-organizing systems

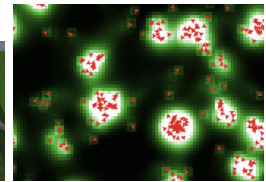


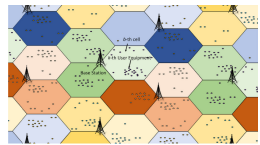


Multi agent systems are used in a wide range of applications:

- agent-based model simulation
- multi-agent learning
- multi-robot control
- swarms and self-organizing systems
- complex problem solving

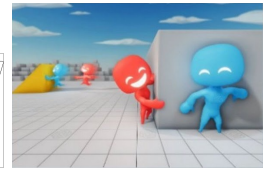


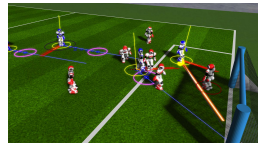


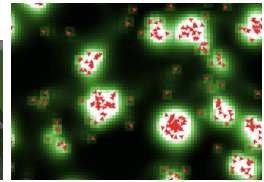


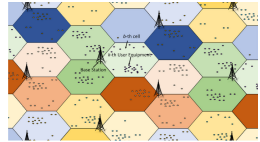
Multi agent systems are used in a wide range of applications:

- agent-based model simulation
- multi-agent learning
- multi-robot control
- swarms and self-organizing systems
- complex problem solving
- games and collaboration







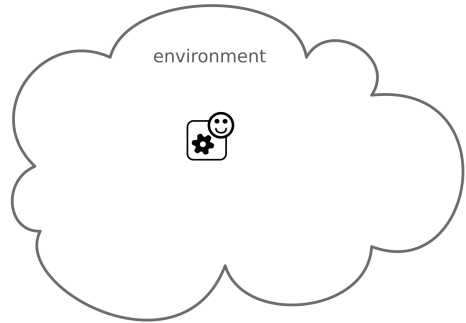


(a) Offensive task

(b) Defensive task

Agents are a programming paradigm – AOP – centered on individual entities and their relationship with other entities in their environment.

- agents are presistent

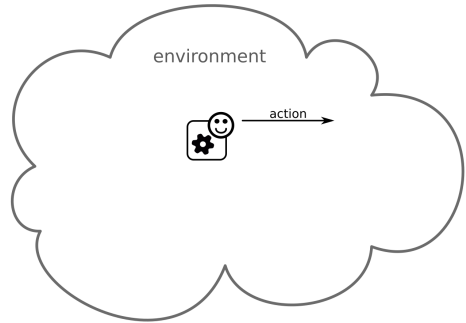


Instead of focusing on the global state of the system, AOP focuses on the state and behaviour of individual entities, each dealing with the other entities in its own way.

⇒ AOP is adequate for open and heterogeneous systems.

Agents are a programming paradigm – AOP – centered on individual entities and their relationship with other entities in their environment.

- agents are presistent
- agents are autonomous

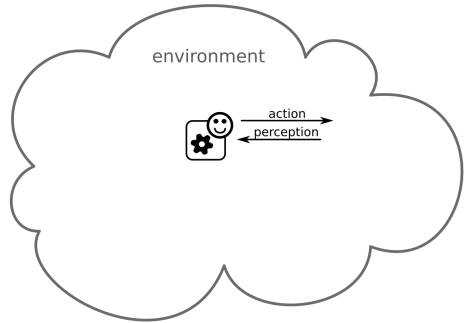


Instead of focusing on the global state of the system, AOP focuses on the state and behaviour of individual entities, each dealing with the other entities in its own way.

⇒ AOP is adequate for open and heterogeneous systems.

Agents are a programming paradigm – AOP – centered on individual entities and their relationship with other entities in their environment.

- agents are presistent
- agents are autonomous
- agents are reactive



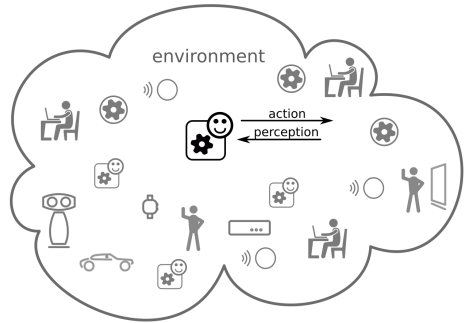
Instead of focusing on the global state of the system, AOP focuses on the state and behaviour of individual entities, each dealing with the other entities in its own way.

⇒ AOP is adequate for open and heterogeneous systems.

Agents are a programming paradigm – AOP – centered on individual entities and their relationship with other entities in their environment.

- agents are presistent
- agents are autonomous
- agents are reactive
- agents are social

Instead of focusing on the global state of the system, AOP focuses on the state and behaviour of individual entities, each dealing with the other entities in its own way.



⇒ AOP is adequate for open and heterogeneous systems.

$$\text{IoT} + \text{MAS} = ??$$

Agents can be very simple or very complex, but they always can be viewed in the same manner:

- they encapsulate an autonomous decision process
- they are able to receive messages from the outside
  - agent communication is standardized by the FIPA-ACL standard.

Agents can be very simple or very complex, but they always can be viewed in the same manner:

- they encapsulate an autonomous decision process
- they are able to receive messages from the outside
  - agent communication is standardized by the FIPA-ACL standard.

⇒ a standardized view of an open, heterogeneous system

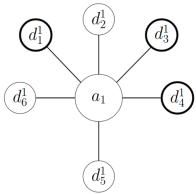
Agents can help with

- managing the data that is coming from sensors and other devices in order to protect privacy 
- managing data aggregation so as to ensure anonymization 
- improving the secure access to IoT devices and protecting them from intrusion 
- manging devices joining and leaving the system 
- management of system heterogeneity in terms of communication protocols 

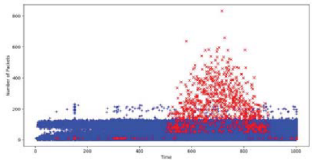
Collaborative agent-based detection of DDoS IoT botnets, 2019 [Giachoudis et al., 2019]

Problem: IoT devices are hijacked as part of botnets and participate in DDoS attacks.

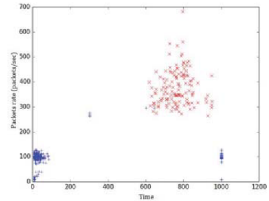
Agent-based solution: use agents that analyze the messages from devices and detect the launching of a DDoS attack.



architecture



message analysis

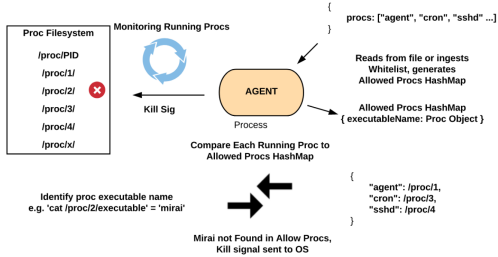


clustering

Cyber physical IoT device management using a lightweight agent, 2019 [Maloney et al., 2019]

Problem: IoT devices are vulnerable to attacks because their software is not up-to-date.

Agent-based solution: use agents to autonomously manage the updates of devices, the applications installed on devices, and the configuration of the devices.

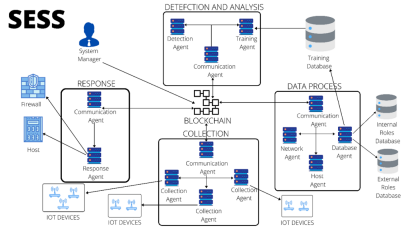


process management

Intrusion detection system for the internet of things based on blockchain and multi-agent systems, 2020 [Liang et al., 2020]

Problem: IoT devices may be corrupted and start working for malicious parties.

Agent-based solution: use agents and blockchain to collect data from the IoT devices; data is stored in a distributed, secure manner by using a private blockchain, protecting all the agents and devices from tampering.

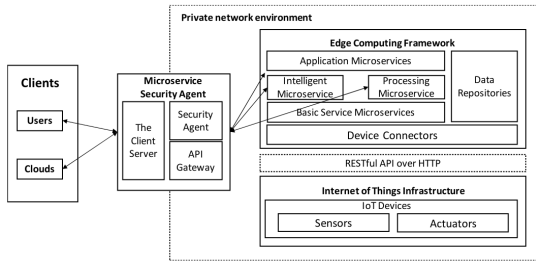


system architecture

Microservice security agent based on API gateway in edge computing, 2019 [Xu et al., 2019]

Problem: Edge computing scenarios need a security approach for edge devices.

Agent-based solution: control access with an agent which is able to decide if access to the edge computing framework is legitimate.

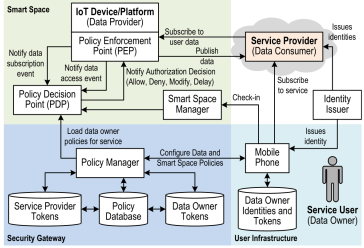


system architecture

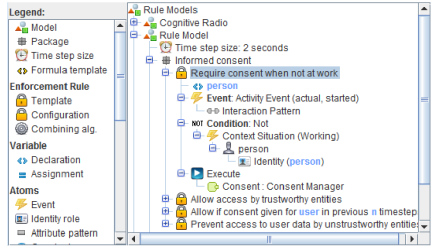
An agent-based framework for informed consent in the internet of things, 2015 [Neisse et al., 2015]

Problem: Users need to give their consent for the information which is gathered by IoT devices.

Agent-based solution: an agent is used to obtain informed consent from users depending on the data and the context.



system architecture

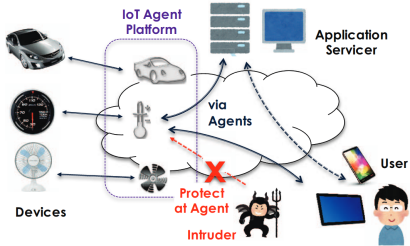


context-based consent

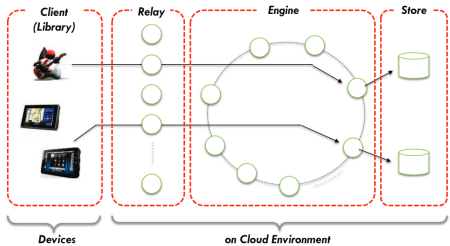
IoT agent platform mechanism with transparent cloud computing framework for improving IoT security, 2017 [Nakagawa and Shimojo, 2017]

Problem: IoT devices may be corrupted and start working for malicious parties.

Agent-based solution: separate IoT devices from the cloud via a series of agentified relay nodes.



system concept



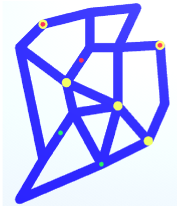
system components

Agent-based IoT coordination for smart cities considering security and privacy, 2019

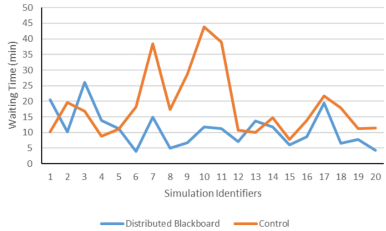
[García-Magariño et al., 2019]

Problem: In a smart city scenario, solutions are needed for large-scale data storage

Agent-based solution: a multi-agent system coordinates distributed blackboards, obtaining decentralized, asynchronous communication.



scenario map



experimental results


FLASH-MAS

FLASH-MAS is *A Fast and Lightweight Agent Shell* to serve as a deployment platform for a variety of agent-based applications, including in IoT.

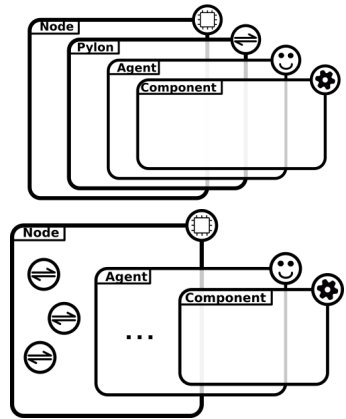
Its aim is to be a modern MAS framework: standard-based · highly modular · very lightweight

[Olaru et al., 2019]

In a FLASH-MAS deployment there is a great variety of entities, which are not all necessarily agents.

- entities inherent to the deployment – nodes, communication infrastructures
- entities based on various MAS models – agents, artifacts, workspaces, groups, organizations, contexts
- entities which facilitate working with the MAS – GUI support, monitoring and control entities

Entities can be placed in the context of one-another flexibly.



Entities have characteristic operations. ←

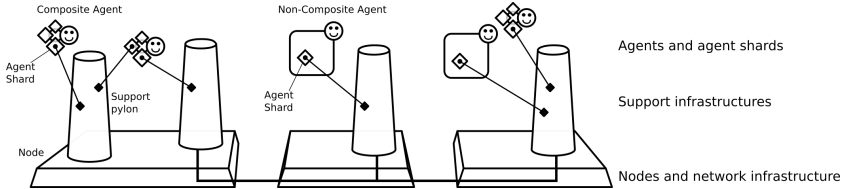
- agents have `receive`
- nodes have `load` and `migrate`
- workspaces have `join`
- communication infrastructures have `route`

etc

Operations can be accessed based on the *context* of the calling entity.

⟨ the *context* is all the entities that an entity is part of in some way ⟩

Some entities in the context may even be *virtual* – they have no operations but they may serve as scope to other entities. E.g. geographic areas, or intervals of time.



agents · shards · pylons · nodes

but also

groups · organizations · artifacts · bridges

Iot devices are notoriously limited on resources and many times need to use specific, constrained protocols.

In the entity-operation model

- all devices are also (first-class) entities
- bridges can exist which translate from one communication protocol to another
- the changes in communication protocol are transparent to the entities

Iot devices are notoriously limited on resources and many times need to use specific, constrained protocols.

In the entity-operation model

- all devices are also (first-class) entities
- bridges can exist which translate from one communication protocol to another
- the changes in communication protocol are transparent to the entities
- FLASH-MAS allows to have all the entities in the deployment as actual entities in the model, with a coherent set of operations, and communicating transparently

- IoT brings a great number of challenges, especially related to security and privacy
- agents are persistent, autonomous entities which enable designing adaptive, open, heterogeneous systems
- agents can be used in IoT architectures in order to make decisions, dynamically, related to access, management, and protection of IoT devices

Thank You!

Questions are welcome!

andrei.olaru@upb.ro

García-Magariño, I., Gray, G., Muttukrishnan, R., and Asif, W. (2019).
Agent-based IoT coordination for smart cities considering security and privacy.
In 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), pages 221–226. IEEE.

Giachoudis, N., Damiris, G.-P., Theodoridis, G., and Spathoulas, G. (2019).
Collaborative agent-based detection of ddos iot botnets.
In 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), pages 205–211. IEEE.

Lamba, A., Singh, S., Balvinder, S., Dutta, N., and Rela, S. (2017).
Mitigating iot security and privacy challenges using distributed ledger based blockchain (dl-bc) technology.
International Journal For Technological Research In Engineering, 4(8).

Liang, C., Shanmugam, B., Azam, S., Karim, A., Islam, A., Zamani, M., Kavianpour, S., and Idris, N. B. (2020).
Intrusion detection system for the internet of things based on blockchain and multi-agent systems.
Electronics, 9(7):1120.

Maloney, M., Reilly, E., Siegel, M., and Falco, G. (2019).
Cyber physical IoT device management using a lightweight agent.
In 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pages 1009–1014. IEEE.

Nakagawa, I. and Shimojo, S. (2017).
IoT agent platform mechanism with transparent cloud computing framework for improving IoT security.
In 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), volume 2, pages 684–689. IEEE.

Neisse, R., Baldini, G., Steri, G., Miyake, Y., Kiyomoto, S., and Biswas, A. R. (2015).
An agent-based framework for informed consent in the internet of things.
In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), pages 789–794. IEEE.

Olaru, A., Sorici, A., and Florea, A. M. (2019).

A flexible and lightweight agent deployment architecture.

In 2019 22nd International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 28-30 May 2019, pages 251–258. IEEE.

Xu, R., Jin, W., and Kim, D. (2019).

Microservice security agent based on API gateway in edge computing.

Sensors, 19(22):4905.

Thank You!

Questions are welcome!

andrei.olaru@upb.ro