A General Distributed Architecture for Resilient Monitoring over Heterogeneous Networks

Fábio Januário[1,2], Alberto Cardoso[2], and Paulo Gil[1,2]

[1] Departamento de Engenharia Electrotécnica, Faculdade de Ciências e Tecnologia, Universidade Nova de Lisboa, Portugal
[2] Centre for Informatics and Systems (CISUC), University of Coimbra, Portugal
f.januario@campus.fct.unl.pt, alberto@dei.uc.pt, psg@fct.unl.pt

Abstract. The growing developments on networked devices, with different communication structures and capabilities made possible the emergence of new architectures for monitoring systems. In the case of heterogeneous distributed environments, where knowledge, processing devices, sensors and actuators are distributed throughout the network, the design of such systems are challenging in terms of integration and, markedly, in security and state-awareness of the overall system. This work proposes a general distributed architecture, with supporting methods, for building a resilient monitoring system that can adaptively accommodate both cyber and physical anomalies. Its implementation relies on multi-agent systems within a distributed middleware.

Keywords: Resilient systems, distributed computing, embedded systems, multi-agents, wireless sensor and actuator network, heterogeneous networks.

1 Introduction

Modern computing networks that enable distributed computing consist of a wide range of heterogeneous devices, with various levels of resources, which are interconnected using differing networking technologies [1]. These networks may be implemented in industrial environments for connecting large number of subsystems, of different natures, including interactions with humans and supervision platforms.
Distributed heterogeneous environments present inherently some challenges and vulnerabilities. In the context of monitoring systems for fault and failure detection there is the need of efficient information processing and correct assessment of the systems' behaviour. Such endeavours require the development of dedicated methods to identify and recover from faults and failures, or in order to mitigate their impact on the overall system. Regarding the vulnerabilities of these networked systems, the cyber-intrusion is of major importance, as malignant actors can mask the system's degradation or provide fake data to higher management levels, with respect to the current system's status [2].

In this work, a resilient system is regarded as a system that maintains state awareness and an acceptable level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature [3][4]. In the

L.M. Camarinha-Matos et al. (Eds.): DoCEIS 2014, IFIP AICT 423, pp. 129–136, 2014.

case of heterogeneous monitoring systems, this resilience provides the system with security and trust mechanism, thus fixing, mitigating or coping with the aforementioned vulnerabilities.

The implementation of resilient enforcement mechanisms can be accomplished by incorporating dedicated algorithms and heuristics on a distributed architecture based on multi-agents and "chunks" of middleware deployed remotely. One of the most prevalent alternatives in the context of distributed architecture design is the multi-agent system (MAS) paradigm. A distributed agent-based architecture provides flexibility to move functions to where actions or measures are needed, thus obtaining improved responses at execution time, autonomy, services continuity and superior levels of scalability [5].

Middleware architectures are becoming increasingly important as networks, services and applications become more complex. These architectures can deal with coordination, cooperation and interoperability of distributed components by bridging the gap between applications and their underlying low level software and hardware infrastructures. Moreover, they provide tools and methods that can help hiding the complexity and heterogeneity of hardware and network platforms. Also, middleware supports programmer's applications in several ways, such as providing appropriate system abstractions and reusability of code services, while helping in the network infrastructure management [6].

The present work proposes a general architecture for resilient monitoring over heterogeneous networks making use of multi-agents embedded on a distributed middleware framework, where each agent is tailored for executing specific and coordinated tasks, namely for detecting and recovering from physical and cyber malfunctions.

2 Relationship to Collective Awareness Systems

According to the European Commission, collective awareness systems are information and communication technologies (ICT) systems that leverage the emerging "network effect", by combining open online social media, distributed knowledge creation, and data from real environments, in order to create awareness of problems and possible solutions requesting collective efforts, while enabling new forms of innovation [7].

These systems can be adopted in various scenarios, like in social environments, enterprises collaboration, industrial processes and decision methods. In these contexts, a network infrastructure allowing communication and perception is considered necessary to assess the context aware, by making use of a collaborative approach.

The electric power production and distribution is a critical system where monitoring is of major important to prevent or accommodate systems' malfunctions. This is one striking example where resilient systems can contribute to the integrity of the overall system, by preventing cyber and physical attacks to infrastructures. Another field with high security requirements, is that of governmental communications, where intrusion threats in their communication networks are taken

very seriously. Finally with the automation of many industrial processes it is necessary to develop monitoring systems in order to ensure the correctness of operation.

To provide security and dependability mechanisms to this kind of distributed systems, new set of heuristics and algorithms have to be developed, which opens a window of opportunity for new contributions to the field. In this context, the present work intends to give a contribution to the development of collective awareness systems, by proposing a general distributed architecture for enhancing the overall resilience of monitoring systems over heterogeneous networks.

3 Resilient Systems

The research area of resilient systems is a relatively new topic that involves systems design taking into account issues, such as cyber security, physical security, process efficiency and stability, process compliancy and state awareness.

In [8] a hybrid system model is used to address physical layer control design and cyber level security policy making for cyber-physical systems that are subject to cascading effects from cyber attacks and physical disturbances. In [9], the authors propose a hybrid theoretical framework to analyse and design, in a quantitative and holistic way, robust and resilient control systems that can be subject to different types of disturbances, at different layers of the system. The work in [10] presents an intelligent resilient control algorithm for a wireless network control system based on the quantification of the concept of resiliency in terms of the quality of control. The authors developed an intelligent resilient control algorithm that maintains operational normalcy in face of wireless interference incidents, such as radio frequency jamming and signal blocking, while [11] proposes a resilient condition assessment monitoring system, able to dynamically adapt and reconfigure, depending on the assessed conditions.

In literature one can find several works making use of MAS to implement intelligence mechanisms. In [12], it is presented an overview on how to achieve critical infrastructure resilience through advanced control engineering. The authors developed a hierarchical multi-agent dynamic system framework to model distributed control system dynamics and enforce resilience. In [2], a generalized design methodology was suggested for analysing and accommodating anomalies in cyber physical systems. By using computational intelligence techniques it is provided a design method to integrate cyber and physical data and, thus ensuring the appropriate response to both benign and malicious actions. In [13], a distributed multi-agent architecture is presented to implement a resilient supervision system over wireless sensor and actuator network. This system implements resilience enforced mechanisms, by incorporating dedicated algorithms and heuristics in an architecture based on agents, so as to guarantee the state awareness and an acceptable level of operational normalcy, in response to disturbances.

Taking into account previous constrains on resilient systems, this work intends to extend resilience policies to heterogeneous and distributed environments. With the modern computing networks infrastructures and distributed resources these systems

become an important research area to provide security and dependability. Aiming at this purpose, the present work proposes a general resilient architecture based on the MAS paradigm.

3.1 Architecture Overview

The proposed architecture is based on a MAS embedded on a distributed middleware platform, for which issues, such as those of communication, network topologies, routing protocols and integration are assumed to be dealt with elsewhere. Fig. 1 presents a distributed environment comprising three main components, namely applications, middlewares and processes/devices or nodes.

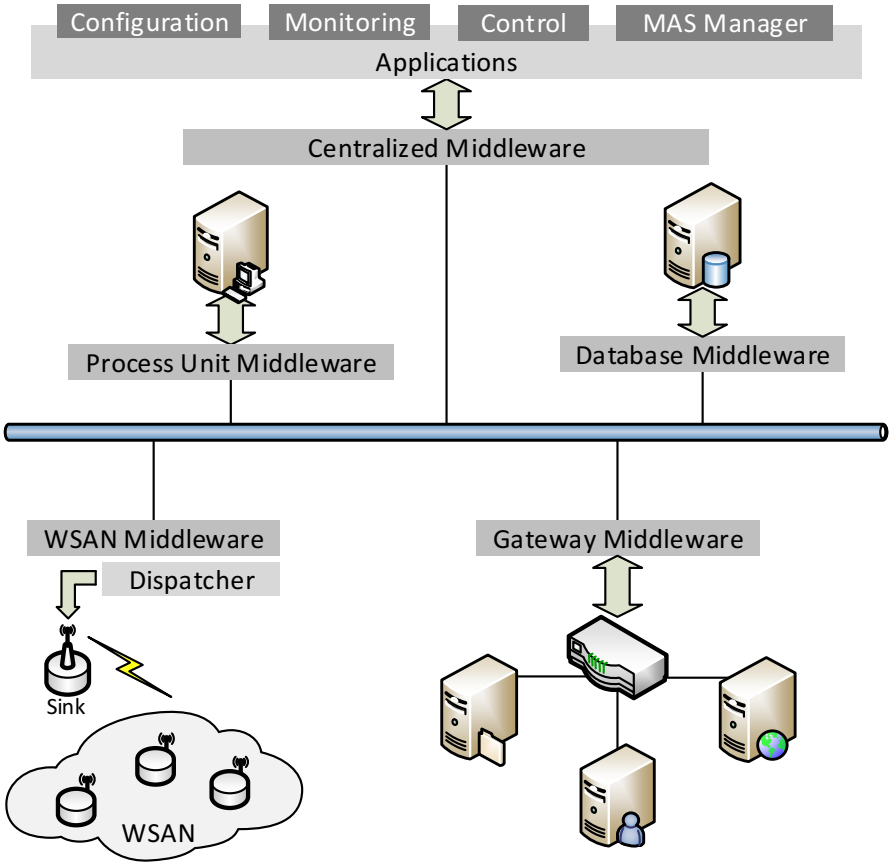

Fig. 1. General distributed architecture

The processes/devices or nodes consist of physical components and the necessary hardware and software infrastructures. These components can be represented by processing units that process data stemming from the network, or from databases that

store and provide information and knowledge regarding the network, gateways interfacing with another network that uses different protocols, and sensor and actuator networks (wireless or not) to interact with the environment, by sensing and actuating on physical infrastructures. Fig. 1 shows a wireless sensor and actuator network (WSAN), where the sink node and the dispatcher are responsible for transferring the data from the WSAN into the middleware and for coordinating the underlying communications.

The application layer provides users with a number of applications allowing, in a transparent way, the interaction with networks, devices and plants in the perimeter of the networks. The monitoring application enables to follow-up the system status, while the control application manages, commands or manipulates the behaviour of the system, using sensors and actuators. The configuration application enables to setting up the system's parameters and available devices. Finally, the MAS manager configures and changes the multi-agent system's attributes.

The middleware layer allows the interaction between the application layer and the plant/devices. The middleware is in this architecture deployed, in a decentralized fashion, on several components in order to bring about the functionalities to the location where they are called out. In heterogeneous networks this topology has the advantage of each "chunk" of middleware could be implemented taking into account the associated hardware or software constrains shown up in the process/device layer.

Fig. 2 presents the main components of the proposed middleware. The integration layer facilitates data exchange between the process/device infrastructures and applications. Data from sensor and distributed devices, as well as additional diagnosis information is fed into the middleware, analysed and forwarded to the corresponding destination. Further, actuation commands and data is passed down from the middleware to actuators or devices, while the monitoring layer evaluates the performance of the middleware at runtime by applying data quality metrics. This element ensures that processing delays are within required bounds. The configuration layer enables the definition of commands to configure the data uploaded and downloaded from the devices, as well as agents in the security and dependability modules.

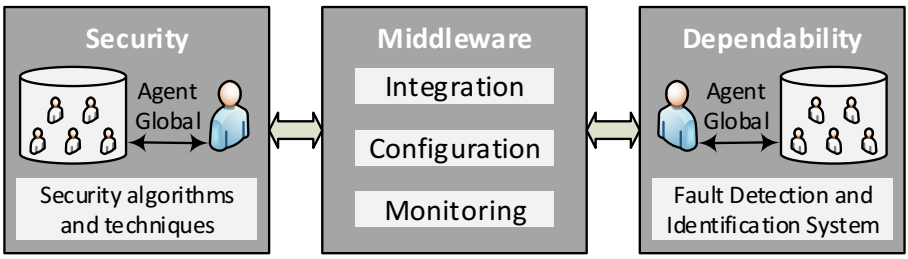

Fig. 2. Resilient middleware based in MAS

Dependability. For enabling the monitoring system to meet dependability targets it is necessary to incorporate fault tolerant and self-healing mechanisms into the resilient design. These mechanisms will ensure end-to-end performance communication in environments where growth, scalability, closed loop stability and performance, are important features.

Security. When sensitive data received from sensors or servers and data sent to actuators or other devices are transmitted through uncontrolled environments, security is inescapably compromised. If not protected, transmitted data may be accessed, corrupted, or even destroyed, by unauthorized users. Consequently, security mechanisms should be developed and implemented in order to be able to adapt to changes in the application environment, to system requirements and system resources.

3.2 Multi-agent System

Agents can be regarded as computing entities in a given environment, presenting a certain degree of autonomy, and possessing the ability to feel and act in order to accomplish a given mission. Some of their inherent features include the following [14]:

- Autonomy: agents are independent entities, able to accomplish a given task, without any programming or direct intervention;
- Reactivity: capability of perceiving their environment and respond quickly and effectively to changes;
- Pro-activity: ability to take initiative goals and behave in order to meet them;
- Cooperation: agents have the ability to interact and communicate with one another for the sake of their own teleonomy;
- Intelligence: in order to evaluate and take over a task, in an autonomous way, an agent should incorporate intelligent techniques;
- Mobility: agents have the ability to move its code from a node to another one in a system, offering mobility properties in distributed computational devices.

Multi-agent systems offer the means to design and implement complex distributed systems. This paradigm extends previous approaches and methodologies, namely object-oriented or distributed computing. The proposed architecture takes into account the use of MAS (Fig. 3), where a master agent is responsible for the management routines related to other dependent local agents, and for coordinating some tasks, such as configuration requests.

Each module (dependability or security) has a master agent that is responsible for all dependent agents, as well as the communication with other agents. Local agents are devoted to monitoring the state of the system with specific methods and algorithms. In the case of heterogeneous distributed systems, subsystems do not possess the same characteristics and vulnerabilities, so these agents have to be configured to provide the necessary functionalities to each subsystem. In the case of a detected event, the agent has the ability to act accordingly, while guaranteeing the maintenance of the system until the problem is completely solved.

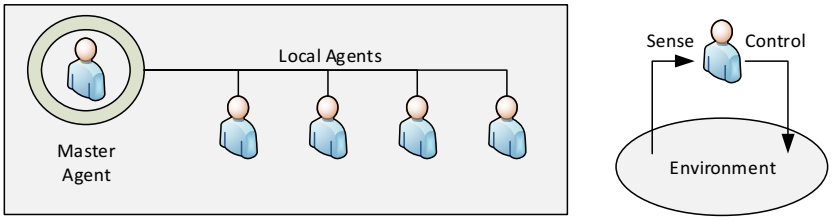

Fig. 3. Multi-agent system architecture

In this architecture, mobile agents have an important role, as their use allows reducing the network traffic. One of the applications for mobile agents deals with communications between middlewares, namely for configurations of distributed agents, with commands sent by the user. With these features MAS allows the implementation of different techniques and show to be a good way so as to provide resilience to heterogeneous networks.

4 Conclusion and Future Work

This paper addressed the problem of resilient monitoring over heterogeneous networks. A general architecture based on multi-agent systems embedded on a distributed middleware framework. The resilience is achieved by combining two main features/resources: *i*) dependability with the implementation of a fault detection and identification system, aiming at maintaining the system in safe operation state; *ii*) security envelope by developing measures to protect the system from cyber and physical attacks.

Finally, it should be mentioned that the present work is still under progress. Further developments will include the exhaustive research in security and dependability areas in order to provide metrics and methods to improve the framework responsiveness.

Acknowledgments. Januário, F. acknowledge Fundacão para a Ciência e Tecnologia (FCT), Portugal for the Ph.D. Grant SFRH/BD/85586/2012. This work has been partially supported by iCIS-Intelligent Computing in the Internet of Services, Project CENTRO-07-ST24-FEDER-002003.

References

1. Tynan, R., O'Hare, G.M.P., Marsh, D., O'Kane, D.: Multi-agent System Architectures for Wireless Sensor Networks. In: Sunderam, V.S., van Albada, G.D., Sloot, P.M.A., Dongarra, J. (eds.) ICCS 2005. LNCS, vol. 3516, pp. 687–694. Springer, Heidelberg (2005)
2. Rieger, C.G., Villez, K.: Resilient control system execution agent (ReCoSEA). In: 2012 5th International Symposium on Resilient Control Systems, pp. 143–148. IEEE (2012)
3. Rieger, C.G., Gertman, D.I., McQueen, M.A.: Resilient control systems: Next generation design research. In: 2009 2nd Conference on Human System Interactions, pp. 632–636. IEEE (2009)

4. Garcia, H.E., Jhamaria, N., Kuang, H., Lin, W.-C., Meerkov, S.M.: Resilient monitoring system: Design and performance analysis. In: 2011 4th International Symposium on Resilient Control Systems, pp. 61–68. IEEE (2011)
5. Alonso, R.S., Tapia, D.I., Bajo, J., García, Ó., de Paz, J.F., Corchado, J.M.: Implementing a hardware-embedded reactive agents platform based on a service-oriented architecture over heterogeneous wireless sensor networks. Ad Hoc Networks 11, 151–166 (2013)
6. Soldatos, J., Pandis, I., Stamatis, K., Polymenakos, L., Crowley, J.L.: Agent based middleware infrastructure for autonomous context-aware ubiquitous computing services. Comput. Commun. 30, 577–591 (2007)
7. Digital Agenda for Europe: Collective Awareness Platforms for Sustainability and Social Innovation, https://ec.europa.eu/digital-agenda/en/collective-awareness-platforms
8. Zhu, Q., Başar, T.: A dynamic game-theoretic approach to resilient control system design for cascading failures. In: Proceedings of the 1st International Conference on High Confidence Networked Systems - HiCoNS 2012, p. 41. ACM Press, New York (2012)
9. Zhu, Q., Basar, T.: Robust and resilient control design for cyber-physical systems with an application to power systems. In: IEEE Conference on Decision and Control and European Control Conference, pp. 4066–4071. IEEE (2011)
10. Ji, K., Wei, D.: Resilient control for wireless networked control systems. Int. J. Control. Autom. Syst. 9, 285–293 (2011)
11. Garcia, H.E., Lin, W.-C., Meerkov, S.M.: A resilient condition assessment monitoring system. In: 2012 5th International Symposium on Resilient Control Systems, pp. 98–105. IEEE (2012)
12. Rieger, C.G., Moore, K.L., Baldwin, T.L.: Resilient control systems: A multi-agent dynamic systems perspective. In: IEEE International Conference on Electro-Information Technology, EIT 2013, pp. 1–16. IEEE (2013)
13. Januário, F., Santos, A., Lucena, C., Palma, L., Cardoso, A., Gil, P.: Resilient Supervision System over WSAN: A Distributed Multi-Agent Architecture. In: 3rd International Conference on Sensor Networks (2014)
14. Paolucci, M., Sacile, R.: Agent-Based Manufacturing and Control Systems: New Agile Manufacturing Solutions for Achieving Peak Performance (2005)