Reputation based Dynamic Responsibility to Agent Assignment for Critical Infrastructure

Guemkam, Guy; Feltus, Christophe; Bonhomme, Cédric; Schmitt, Pierre; Khadraoui, Djamel; Guessoum, Zahia

Published in:
Proceeding of the Tenth IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT 2011), Lyon, France.

DOI:
10.1109/WI-IAT.2011.194

Publication date:
2011

Document Version
Early version, also known as pre-print

Reputation based Dynamic Responsibility to Agent Assignement for Critical Infrastructure

Guy Guemkam*†, Christophe Feltus*, Cédric Bonhomme*, Pierre Schmitt*, Djamel Khadraoui* and Zahia Guessoum†
* *Service Science and Innovation*
Centre de Recherche Public HENRI TUDOR
Luxembourg, G.D. of LUXEMBOURG
{*firstname.lastname*}*@tudor.lu*
† *Laboratoire d'Informatique de Paris 6*
Université Pierre et Marie Curie
Paris, FRANCE
zahia.guessoum@lip6.fr

***Abstract*—Power distribution constitutes a critical service for our economy. To foreseen electricity overload and risks of power blackout according to external perturbations such as the weather, the temperature or the barometric pressure in real time is a crucial challenge. In order to face those problems, research tends to involve consumers in the utilization of the electricity based on weather conditions. Our previous works had proposed an agent based architecture to support this alert mechanism. The architecture exploited a static assignment of functions to agents. That static assignment was a weak point because isolating an agent or breaking the communication channel between two of them created serious damage on the crisis management. In this paper, we complete our previous works and make mobile the assignment of functions mobile for agents. Our approach exploits the concept of agent responsibility that we dynamically assigned to the agent taking into consideration the agent reputation.**

I. Introduction

All around the globe, many regions keep suffering electric power blackout [1] when temperature is significantly decreasing [2] [3]. E.g. Brittany in France recently had to face such problems [4]. Brittany is a geographic and administrative region of 13.136 square miles in the northwest of France that, for some years, suffers from problems in the power distribution especially during very cold weather. For instance, in the week from the 14th to the 18th of December 2009 the region was subject to an important electric load forecast. The expected load for Monday the 14th was about 85200 Mega Watts (MW) and during the evening (around 7PM), the load was expected to raise the historical level of 92400 MW. The influence of the weather conditions on the electric load is estimated at2100MW by 1F°. This rate is important especially since we know that the temperature of the current winter is between 6 and 8F° higher that the average.

As electricity is a not storable good, its production has to precisely fit to its consumption. To maintain and guarantee the balance, electric companies supervise the transport of the power and manage the electric network. They keep watching in real time both production and consumption values to maintain the safety of the system. In case of a productivity problem, solutions are deployed like the importation of power from adjoining countries or the counseling of users request, made via TV and newspapers, to adapt the usage of electric machines (e.g. washing machine or dryer).

Our state of the art in this field [5] has highlighted that many architectures have already been elaborated to support the reaction after the problem's detection. Those architectures are mostly elaborated based on a multi-agent system (MAS) approach which offers the possibility to work in a decentralized and heterogeneous environment. However, we have observed that those architectures are based on a static assignment of functions to agents and that, as a consequence, isolating an agent or breaking the communication channel between two of them could create serious damage to the management of the crisis. In this paper, we propose an innovative approach for making the assignment of functions dynamic to agents. Our approach exploits the concept of agent responsibility that we dynamically assign depending on the crisis situation. Additionally, the crisis context makes vary the agent ability to react (e.g. the agent is momentarily isolated or has a decreased capability to react quickly). In order to consider that constraints, we introduce the agent reputation as a parameter that influences the assignment.

The remainder of this paper is composed as follows. Section II depicts the broadcasting mechanism. Section III presents the responsibility model and section IV introduces the reputation calculus method. Finally, the section V shows how the reputation is used to the dynamic assignment of responsibilities to agents and section 6 concludes the paper.

II. Broadcasting mechanism case study

The broadcasting mechanism (Fig. 1) aims at sending alerts to the population using media such as a SMS whenever a weather alert occurs. This section presents the core components of the broadcasting mechanism. The solution relies on a MAS technology on the top of the JADE framework

[6]. Agents are disseminated on three layers corresponding to the geographical region (city, region or country) and they retrieve information from probes located in weather station and on the electric networks and representing with different values: Pressure, temperature and electric voltage.

The agents that compose the architecture are the following:

The Alert Correlation Engine (ACE) collects, aggregates and analyses weather informations coming from probes deployed over the network and weather stations. Confirmed alerts are sent to the Policy Instantiation Engine (PIE).

The PIE receives confirmed alert from the ACE, sets the severity level and the extent of the geographical response. The PIE instantiates high level alert messages which have to be deployed. Finally the high level alert messages are transferred to the Message Supervising Point (MSP).

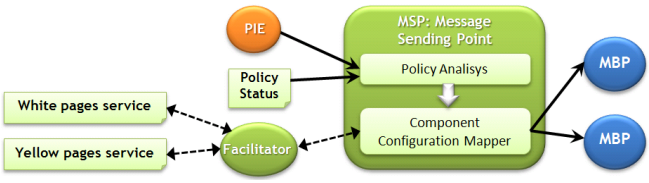

Figure 2. MSP architecture

The MSP (Fig. 2) is composed of two modules. The Policy Analysis (PA) is in charge of analyzing the policies previously instantiated by the PIE. Therefore, the Policy Status database stores all communication policies and their current status (in progress, not applicable, by-passed, enforced, removed...) so that the PA module can check the consistency of the newly received message to be deployed. The second module is the Component Configuration Mapper that selects the appropriate communication channel.

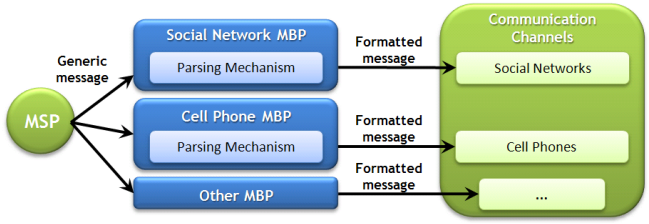

Figure 3. MBP architecture

Fig. 3 presents two different kinds of Message Broadcasting Point (MBP). Indeed, another advantage of MAS is that it is easy to implement from a model, specific agents in order to perform specific tasks. Concretely it enables us to use a different channel of communication (e.g. SMS, e-mail, micro-blogging) to send alerts to citizens, hospitals, etc. By this way our electric blackout prevention system is easily extensible for future communications facilities. MBPs receive generic alert messages from the MSP. Then a specific parser converts the incoming alert message to the appropriate format according to the channel.

In order to consider the mutual trust between agents, each agent maintains within it a database of levels of trust towards its pairs. This means e.g. that the MBP has a dedicated level of trust for the ACE and the MSP.

The broadcasting alert architecture presented in this section is based on the ReD project [7]. The ReD (Reaction after Detection) project defines and designs a solution to enhance the detection/reaction process and improves the overall resilience of critical infrastructures. Fig. 4 introduces the developed architecture illustrated with our weather broadcast alert system. The flow is supposed to begin with an alert detected by a probe.

This alert is sent to the ACE agent (City layer) that does or does not confirm the alert to the PIE. Afterwards, the PIE decides to apply new policies or to forward the alert to an ACE of a higher layer (Region Layer). The PIE agent sends the policies to the MSP agent, which decides which MBP is able to transform the high level alert message into an understandable format for the selected communication channel. In order to manage access rights, we have incorporated to ReD a Context Rights Management module (CRM). Block on the right on Fig. 4. The CRM is in charge of providing access rights to agents (E.g. MBP to the probes and Logs File database, MSP to the Policy Rules Status database). The CRM uses the rights and the crisis context database. The first database includes the access rights corresponding to the responsibilities and the second database includes a set of crisis contexts. Thanks to these databases the CRM agent is able to provide adequate rights at operational layer to an agent depending on the context.

III. Agent Responsibility Model

In a non-crisis context, agents are assigned to responsibilities like MSP, PIE, MBP, etc. Those assignments of responsibilities to agents require specific access rights. By analyzing for instance the activity of monitoring the power network (Fig. 4), we can e.g. observe that the MBP's have the responsibility to collect the voltage on the power line or the weather parameters, to make a basic correlation between the values and the antecedent values records (stocked in the Logs File database) and to report this analysis to the ACE in case of suspected alert. To perform the monitoring activity, the MBP are assigned to precise obligations and gain corresponding access rights recorded in the access right database. Those rights are e.g.: access to temperature or voltage values. When a crisis occurs, for instance if a hurricane isolates some MBP agents from the rest of the network, the normal monitoring rules and procedures do no longer work as usual and it is requested to change the responsibility of the agents. In the above case, other agents have to assure the responsibilities of the isolated MBP. To assure their new responsibilities the agents request additional

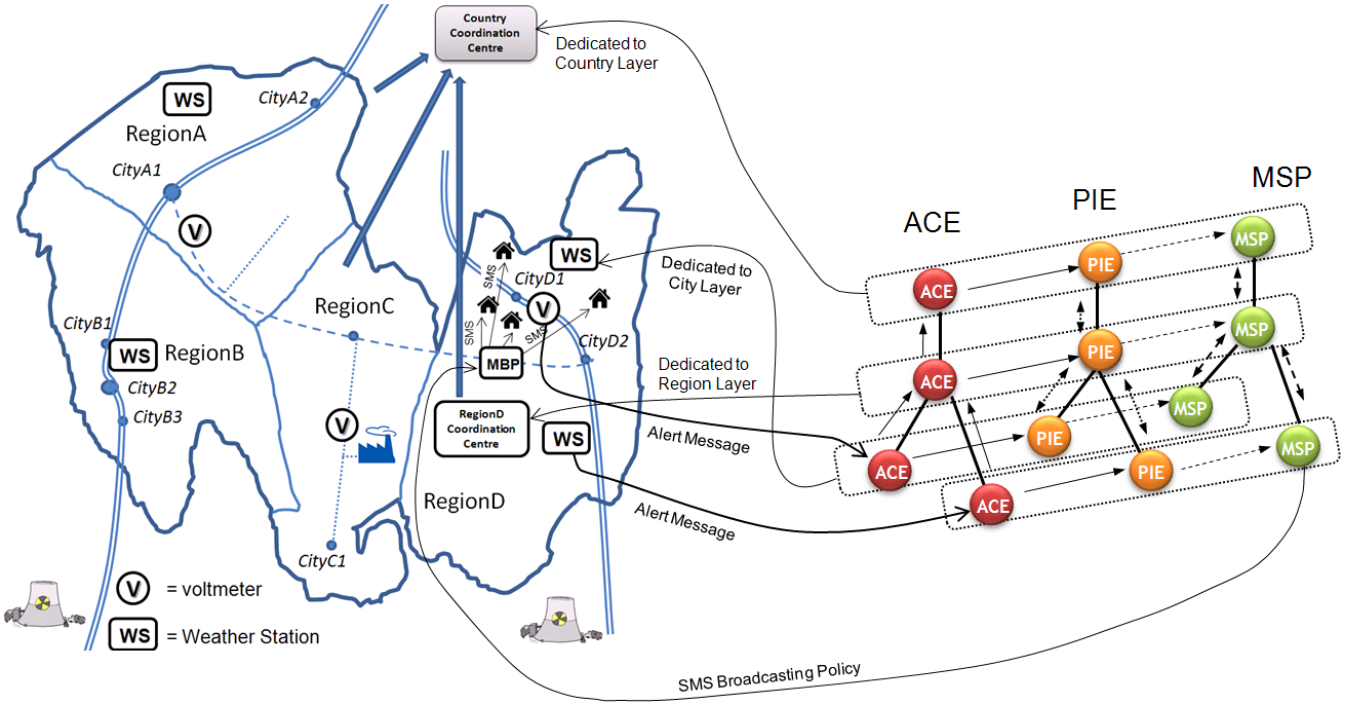

Figure 1. Broadcasting Mechanism inside

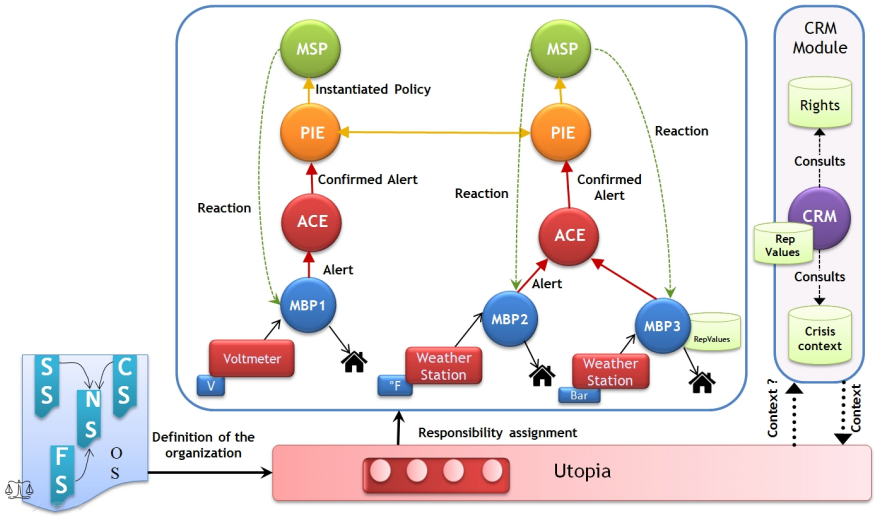

Figure 4. Detailed reaction architecture for power distribution adaptation based on weather parameters

access rights e.g. monitoring probes related to the isolated power line.

In practice, the automatic assignment of rights to agents depending on their responsibilities is not immediate and this contradicts the need to react promptly to the attack or to the problem (e.g. hurricane). To tackle the weakness, our approach is based on the refinement of the agent responsibility and on the granting of access rights based on responsibility. The right management module exploits two databases accessed by the CRM agent. The first database includes the rights corresponding to the responsibilities and the second includes a set of crisis contexts. Each crisis context defines, depending on the type of crisis, which agent is assigned to which responsibility.

The review of the literature highlights that the definition of the agent responsibility is mostly incomplete and that most of the architecture only considering the agent regarding the outcome that it has to produce. Sometimes, advanced

solutions integrate the inputs that those agents request to perform the outcome. We define responsibility as a state assigned to an agent to signify him its obligations concerning the task, its accountabilities regarding its obligations, and the rights and capabilities necessary to perform it.

In order to integrate a dynamic re-assignment of the responsibility from one agent working in normal conditions to one agent working in a crisis environment, we consider all the concepts which compose the responsibility. In [8] we have proposed a responsibility model that can be used to depict the agent responsibility. This model integrates the main following concepts:

Obligation is a duty which links a responsibility with a task that must be performed.

Accountability is a duty to justify achievement, maintenance or avoidance of some given state to an authority under the threat of sanction [9]. Accountability contribute to generate trust or to remove trust depending of the accountability outcomes.

Right encompasses facilities required by an agent to fulfill his obligations, e.g. the access right that the agent gets once it is assigned responsible.

Capability describes the requisite qualities, skills or resources necessary to perform a task. Capability may be declined through knowledge or know-how, possessed by the agent such as ability to make a decision, its processing time, its faculty to analyze a problem, and its position on the network.

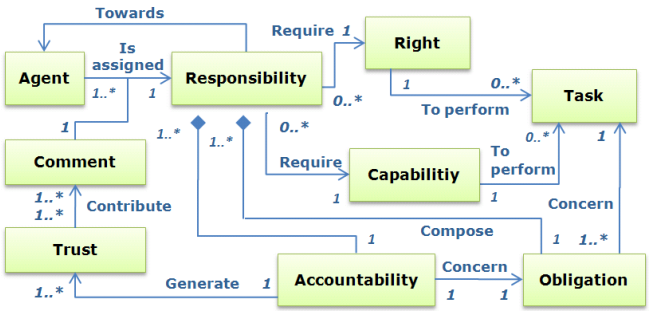

Figure 5. Agent responsibility model

Commitment pledged by the agent represents its engagement to fulfill a task and the assurance that it does it in respect of good practices. The commitment in MAS has already been subject to many researches as explained in [10].

Based on the agent responsibility model of Fig. 5, we define the responsibilities for each agent of the architecture. Table I summarizes the MBP and the ACE responsibilities used in practice for the dynamic assignment (section V). Due to the extent of this paper, only the responsibility for two of them is presented: the MBP and the ACE, and only the 4 most significant components of the responsible are exploited: Obligations, Trust, Capabilities and Rights. For the MBP, we observe that responsibility includes obligations such as the obligation to retrieve logs from the component it monitors, to provide an immediate reaction if necessary, to report the incident to the MSP, etc. To perform this obligation, it needs the capabilities to be on the same network as the component it controls and to communicate with the ACE and the facilitator agent. It also must have the right to read the weather and power line parameters on the concerned network component and to write the values down in a central logs database.

IV. Trust and Reputation Management

The semantic analyzes commitment [11], [12] and advocates to consider the mutual **trust** between agents as a pragmatic commitment antecedent [13] (Fig. 6). The trust component signifies the lower trust value that is necessary for an agent to be assigned responsible and is determined by the importance of the obligation that is to be achieved.

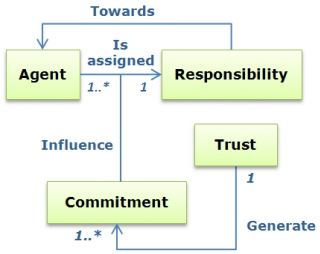

Figure 6. Trust and commitment relationships

The trust and reputation model (TRM) evaluates the role fulfillment of each component involved in the architecture. A large review of computational trust models can be found in [14] and more details for cognitive aspects of trust is presented in [15].

The proposed reputation-based trust management scheme is used to predict the future behavior of a component in order to establish trust among agents and hence to improve security in the system. The way trust information is quantified depends on the application field. Some authors used probabilistic approaches [16] [17] [18] to quantify trust. This approach is used in several fields such as Mobile Ad-hoc Networks, Social Networks or e-commerce. Other approaches such as Fuzzy approaches or Bayesian networks [19][20][21] are also exploited to quantify trust with some differences, if a ageing factor is used or not, the way reputation parameters are aggregated. The information needed to evaluate the trustworthiness of a component is provided by the MBP's probe.

As mentioned in the agent responsibility specifications, if one of the MBP's agents is not trustworthy because for instance it has been corrupted, it has to be removed and replaced. The assignment of a new responsibility to another MBP (MBP1 or MBP2 in Fig. 7) is done based on the trust value of that agent.

	Obligations	Trust	Capabilities	Rights
SAVP	• Retrieve the logs from the component he monitors; • Provide an immediate reaction if necessary; • Communicate with the facilitator to get the address of the other components (ACE, CRM); • Report the incident to the ACE.	0.8	• SAVP must be on the same network as the parameter (browser, ATM, shop, etc.) he monitors; • SAVP must be able to communicate with the ACE and the facilitator agent.	Read parameter value on the concerned network component Write parameter value in the central logs database
ACE	• Decide which keys are appropriated to be deployed by the SAVP; • Confirm the alert to the PIE; • Communicate with the facilitator to get the address of the other components (SAVP, CRM).	0.9	• Fast bandwidth; • High CPU resources; • Central position on the network.	• No specific right.

Table I
AGENTS RESPONSIBILITIES SPECIFICATIONS

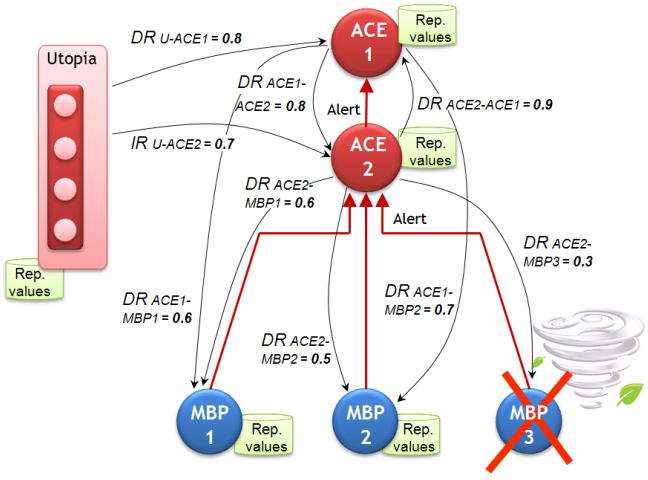

Figure 7. Reputation Repartion Schema

The trust (T) and reputation (R) of each component is provided by trust assessment regarding an MBP agent based on direct information collected by the MBP agents himself and by second hand-information coming from other ACE to which it belongs. This trust based reputation is calculated at time t as follows:

$$T_{ACE1-MBP2} = R_{ACE1-MBP2} = DR_{ACE1-MBP2} \quad (1)$$

Where $DR_{ACE1-MBP2}$ is the reputation derived from the direct reputation of MBP2 in the view of ACE1. The scenario depicted in Fig. 7 shows that ACE1 has no direct connectivity with MBP2 and has to rely on information coming from ACE2. In this case (1) leads to (2):

$$T_{ACE1-MBP2} = R_{ACE1-MBP2} = DR_{ACE1-MBP2} + \lambda * IR_{ACE1-MBP2} \quad (2)$$

Where λ is the weighted factor associated to the reputation value and $IR_{ACE1-MBP2}$ is the indirect reputation value provided by other agents regarding agent MBP2. In the followings we presented how the direct reputation (DR) and the indirect reputation (IR) are calculated. The direct reputation is defined as the probability evaluated by ACE1 that ACE2 will achieve his goal at the next solicitation. Several approaches can be used to deal with reputation information such as Beta, Gaussian, Poisson, binomial. [20] prooves that the Beta distribution system is the most promising due to its flexibility and simplicity as well as its strong foundation on the theory of statistics.

Our model used the Beta probability density function $Beta(\alpha, \beta)$ as shown in equation (3) to represent direct reputation.

$$p(\theta) = Beta(\alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\theta^{\alpha-1}\theta^{\beta-1} \quad (3)$$

Where θ represents the probability that the next event will occur. This Beta function is indexed with two parameters α and β, which represent the sum of positive and negative assessment, respectively that ACE1 has for ACE2. We consider that ACE1 rates ACE2 during an assessment in a binary scale (positive (1), negative (0)). The direct reputation value is the mean of the Beta distribution between ACE1=A and ACE2=B. Reputation value for agent ACE2 about agent ACE1 is calculated as the expectation value of $Beta(\alpha, \beta)$ with E equal the standard deviation :

$$R_{ACE1-ACE2} = E(Beta(\alpha, \beta)) \quad (4)$$

An agent ACE1 is trusted by agent ACE2 if and only if $R_{ACE1-ACE2} \geq \tau$ where τ is a threshold value from which the agent is considered trustworthy. This threshold is defined by the responsibilities specifications. For instance, the trust threshold for MBP agents is set to 0.8. Initially, $\alpha = \beta = 0$, which corresponds to uniform distribution and indicates absence of knowledge.

$$R_{ACE1-ACE2} = E(Beta(\alpha, \beta)) = \frac{\alpha + 1}{\alpha + \beta + 2} \quad (5)$$

The update of this reputation value is done with respect to the Beta function. This trust represents the trustworthiness of one agent to another. In order to highlight the impact of recent behavior, the ageing factor is introduced. We assume that this ageing factor g depends on the context. This value is update in (6) as follows:

A small value of g gives more weight to recent trust values. However choosing the right value of g is not straightforward. For this purpose, we assume that the value of g is chosen by a Human at the initialization of the system. Unlike the components weights which represents the personal view that an agent has to another.

Our solution for setting components weights is based on the similarity beliefs between two agents. This similarity is based on the assumption that if two agents rate a third agent in the same way, this means that they have similar beliefs and views of this agent. Given two agents ACE1 and ACE2, let the set $(ACE1, ACE2)$ be the set of all mutual agents, that both ACE1 and ACE2 have interacted with and hence have a direct reputation with those agents in (7) as follows:

$$Set(ACE1, ACE2) = \{c, d, e, ..., n\} \quad (7)$$

The similarity belief (Λ) between those two agents is given in (8).

$$\Lambda = Sim(ACE1, ACE2) = 1 - Dis(ACE1, ACE2) \quad (8)$$

Where the distance function between 2 agents ACE1, ACE2 is calculated in (9) based on the Euclidian method.

By doing that, an agent can have no common direct history with another and in the same time have a trustworthy (or not) view of that agent.

Table II represents the reputation value that the agents have for each other based on their common past interaction history. The grey boxes represent the reputation that agent has about itself. This is not possible since we assume that reputation is not reflexive. The unknown value means that CRM has no common history with that agent.

Agents	ACE1	ACE2	λ CRM	CRM
MBP1	*unknown*	0.6	*unknown*	0.8
MBP2	*unknown*	0.8	*unknown*	0.9
MBP3	*unknown*	0.1	*unknown*	0.16
ACE1		0.8	0.6	0.8
ACE2	0.9		0.7	0.7

Table II
EXAMPLE OF REPUTATION CALCULATION

V. EXAMPLE OF RESPONSIBILITY ASSIGNMENTS BASED ON REPUTATION.

In this section, we introduce a simple use-case allowing to show how the reputation (see Section IV) impacts the responsibilities yield to the agents (see Section III) thanks to the Context Right Management (CRM) module.

To assign responsibilities to agents, we have associated our architecture with $\mathcal{U}$TOPIA [22] an ins*T*itution *O*riented *P*rogramm*I*ng fr*A*mework which aims at simplifying agent-based institutions programming. This framework uses $\mathcal{M}$OISE^{Inst}[13] Organizational Specification. In our case, we specify the responsibilities using $\mathcal{M}$OISE^{Inst} and deploy the underlying MAS with $\mathcal{U}$TOPIA.

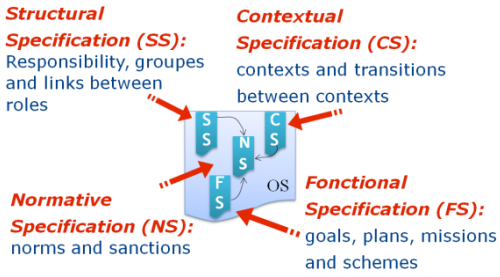

Figure 8. $\mathcal{M}$OISE^{Inst} organization

$\mathcal{M}$OISE^{Inst} (Fig. 8) is composed of four dimensions:

- Structural Specification (SS);
- Functional Specification (FS);
- Contextual Specification (CS);
- Normative Specification (NS).

NS	CS	SS	FS
N1	sMBP1/V	rMBP1	$mV = \{gV\}$
N2	sMBP2/TB	rMBP2	$mTV = \{gT \parallel gV\}$
N3	sMBP2/TBP	rMBP2	$mTBP = \{gT \parallel gB \parallel gP\}$
N4	sMBP3/TP	rMBP3	$mTP = \{gT \parallel gP\}$

Table III
SAMPLE OF ORGANIZATIONAL SPECIFICATION

The table III shows the Organizational Specification of our example. We focus on the responsibility assignment of three agents having the roles rMBP1, rMBP2 and rMBP3. The responsibilities are decomposed as following obligations: V

$$\alpha^{new}_{ACE1-ACE2} \; = \; g * \alpha_{ACE1-ACE2} \;\; and \;\; \beta^{new}_{ACE1-ACE2} \; = \; g * \beta_{ACE1-ACE2} \qquad (6)$$

$$Dis(ACE1, ACE2) \; = \; \sqrt{(R_{ACE1-ACE2} - R_{ACE2-ACE3})^2 + ... + (R_{ACE1-ACEn} - R_{ACE2-ACEn})^2} \qquad (9)$$

stands for monitoring a Voltmeter, T for the Temperature, B for a Barometer and P for Pressure.

We encode the obligations using contexts of the Contextual Specification, for instance sMBP3/TP is a context associated to the role rMPB3 and it is linked to the responsibility of monitoring the temperature and the pressure. The Fig 9 shows all the contexts described in Table III and the transitions. One can observe that transition are a way to reflect the capability aspect of the responsibility model, for instance the transition "/sMBP2/a" between TB and TB**P** means that MBP2 is capable of measuring **p**ressure.

$\mathcal{U}$TOPIA uses concrete actions, called goals, to influence the behavior of agents and these goals can be regrouped into missions. For instance the mission $mTV = \{gT \parallel gV\}$ means running in parallel the actions of probing into a thermometer and a voltmeter.

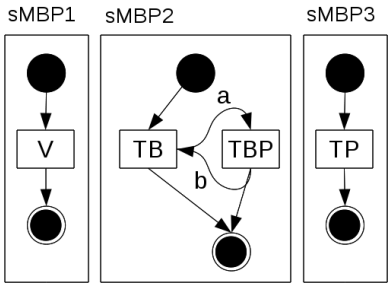

Figure 9. Contextual Specification

Finally the Norms make the link between Roles (SS), Contexts (CS) and Goals (FS) and allow to get this behavior:

- Initially MBP1 is in context V and N1 forces it to do gV. MBP2 is in TB and N2 forces it to do gT and gV in parallel. MBP3, through norm N4 monitors a Thermometer and the Pressure (TP).
- If the transition "/sMBP2/a" is sent, $\mathcal{U}$TOPIA will change the context to "/sMBP2/TBP" and the agent will have the additional responsibility to probe the pressure as the Norm N3 replace N2.

Using $\mathcal{U}$TOPIA make the dynamically assignment of responsibilities to agents simpler. In order to illustrate deeper the link between reputation and responsibility we reuse the values of reputation summarized into Table II.

1) Under a threshold of 0.5 the CRM considers that an agent is no longer trustworthy. According to Table II, the trust level of MBP3 is set to 0.16. Consequently the CRM is able to detect a problem with MBP3 and have to find a solution to dynamically transfer its responsability.
2) The CRM inspects the contextual state of the institution and detects that MBP2 has the capacity of taking MBP3's responsibility. In our simple case MBP2 is alone but if several agents have the capability to replace an agent, the hightest reputed is choosen. In order to transfer the responsability of MBP3 to MBP2, the CRM simply sends the transition "/sMBP2/a" and the final transition for MBP3.
   That allows $\mathcal{U}$TOPIA to reorganize the agents' responsibilities taking into consideration the agents' reputation. As consequence, MBP3 loses its access rights, is isolated and its responsibilities are transferred to the MBP2 which has a reputation of 0.9;
3) The agent MBP2 that receive the additional MBP3's responsibilities requests the underlying access rights to the CRM.

VI. Conclusions

Critical infrastructures are more and more present and needs to be seriously managed and monitored regarding the increasing amount of threats. This paper presents a solution to broadcast weather forecast alerts messages using a MAS based architecture. The system, initially developed based on static assignments of responsibilities to agents, has needs for more dynamism in order to keep aligned to the new arising risks.

This paper firstly addresses this new challenge by providing a framework for dynamically assigning responsibilities to agents depending on the crisis context. That contextualized responsibility assignment permits, *in fine*, to manage the agent access rights to critical information.

Secondly, the paper enhances this dynamic assignment by taking into account the trust and reputation between the agents during the assignment mechanism. Each agent is responsible to store and fuse different source of information. Information coming from prior direct experiences is represented by direct reputation and information coming from other is represented by indirect reputation.

The architecture we exploit to demonstrate the enhanced reaction mechanism, relies on the two main pillars ReD and $\mathcal{U}$TOPIA, which are being tested and currently produced in our labs. Practically ReD defines the structural bases for the weather broadcasting and $\mathcal{U}$TOPIA permits to deploy the responsibilities to agents. The paper is illustrated based on a use case that shows how the transfer of rights for a corrupted

MBP is performed during an evolution from normal to crisis situation.

ACKNOWLEDGMENT

This research was funded by the National Research Fund of Luxembourg in the context of TITAN (Trust-Assurance for Critical Infrastructures in Multi-Agents Environments, FNR CO/08/IS/21) project.

REFERENCES

[1] J. Bialek, "Recent blackouts in US, UK, Scandinavia and Italy: Is it contagious?" Powerpoint presentation, University of Edinburgh, Scotland, 2003.

[2] B. Carreras, V. Lynch, M. Sachtjen, I. Dobson, and D. Newman, "Modeling blackout dynamics in power transmission networks with simple structure," in hicss. Published by the IEEE Computer Society, 2001, p. 2018.

[3] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca et al., "Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance," Power Systems, IEEE Transactions on, vol. 20, no. 4, pp. 1922–1928, 2005.

[4] 2009. [Online]. Available: http://www.rte-france.com

[5] C. Feltus, D. Khadraoui, and C. Bonhomme, "Electric Blackout Prevention: Toward a Computer-Mediated Weather Alert Broadcasting Solution," 2010.

[6] F. Bellifemine, A. Poggi, and G. Rimassa, "JADE–A FIPA-compliant agent framework," in Proceedings of PAAM, vol. 99. Citeseer, 1999, pp. 97–108.

[7] C. Feltus, D. Khadraoui, and J. Aubert, "A Security Decision-Reaction Architecture for Heterogeneous Distributed Network," in Availability, Reliability, and Security, 2010. ARES'10 International Conference on. IEEE, 2010, pp. 1–8.

[8] C. Feltus and M. Petit, "Building a Responsibility Model Including Accountability, Capability and Commitment," in Availability, Reliability and Security, 2009. ARES'09. International Conference on. IEEE, 2009, pp. 412–419.

[9] B. Stahl, "Accountability and Reflective Responsibility in Information Systems," The Information Society: Emerging Landscapes, pp. 51–68, 2006.

[10] M. Singh, "Semantical considerations on dialectical and practical commitments," in Proceedings of the 23rd Conference on Artificial Intelligence (AAAI), 2008, pp. 176–181.

[11] M. Smith and M. Desjardins, "Learning to trust in the competence and commitment of agents," Autonomous Agents and Multi-Agent Systems, vol. 18, no. 1, pp. 36–82, 2009.

[12] J. Mehdi, M. Dastani, Z. Huang, and L. Van Der Torre, "Trust and Commitment in Dynamic Logic," in In Procs. of EurAsia ICT 2002, LNCS 2510. Citeseer, 2002.

[13] B. Gâteau, O. Boissier, D. Khadraoui, and E. Dubois, "Moiseinst: An organizational model for specifying rights and duties of autonomous agents," in Third European Workshop on Multi-Agent Systems (EUMAS 2005), 2005, pp. 484–485.

[14] J. Sabater and C. Sierra, "Review on computational trust and reputation models," Artificial Intelligence Review, vol. 24, no. 1, pp. 33–60, September 2005. [Online]. Available: http://portal.acm.org/citation.cfm?id=1057849.1057866

[15] C. Castelfranchi and R. Falcone, "Principles of trust for mas: Cognitive anatomy, social importance, and quantification." in ICMAS, Y. Demazeau, Ed. IEEE Computer Society, 1998, pp. 72–79.

[16] G. Vogiatzis, I. MacGillivray, and M. Chli, "A probabilistic model for trust and reputation," in Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: volume 1-Volume 1. International Foundation for Autonomous Agents and Multiagent Systems, 2010, pp. 225–232.

[17] J. Patel, W. T. L. Teacy, N. R. Jennings, and M. Luck, "A probabilistic trust model for handling inaccurate reputation sources." in iTrust, ser. Lecture Notes in Computer Science, P. Herrmann, V. Issarny, and S. Shiu, Eds., vol. 3477. Springer, 2005, pp. 193–209.

[18] L. Mui, M. Mohtashemi, C. Ang, P. Szolovits, and A. Halberstadt. (2001) Ratings in Distributed Systems: A Bayesian Approach.

[19] S. Buchegger and J.-Y. L. Boudec, "A Robust Reputation System for Peer-to-Peer and Mobile Ad-hoc Networks," P2PEcon 2004, Cambridge, MA, 4-5 June, 2004.

[20] A. Jsang and R. Ismail, "The beta reputation system," in Proceedings of the 15th Bled Electronic Commerce Conference, 2002, pp. 17–19.

[21] W. T. L. Teacy, J. Patel, N. R. Jennings, and M. Luck, "Travos: Trust and reputation in the context of inaccurate information sources." Autonomous Agents and Multi-Agent Systems, vol. 12, no. 2, pp. 183–198, 2006.

[22] P. Schmitt, C. Bonhomme, J. Aubert, and B. Gâteau, "Programming Electronic Institutions with Utopia," in Information Systems Evolution, ser. Lecture Notes in Business Information Processing, W. Aalst, J. Mylopoulos, N. M. Sadeh, M. J. Shaw, C. Szyperski, P. Soffer, and E. Proper, Eds. Springer Berlin Heidelberg, 2011, vol. 72, pp. 122–135.