# Decision Making Issues Related to Critical Infrastructures Interdependencies Management

Safa Attia, Abdelhak Boubetra, and Manel Saad Saoud

***Abstract*—In recent years, disaster management has become a new concern in decision making in most world countries. The main reason for this trend among world countries is the phenomenon of how to keep in safety critical infrastructures that can cause complex and difficult situations in the case of a failure problem or a catastrophic event. As a consequence the appearance of a large number of vulnerabilities and the increasing interdependence of economic and social activities put vital networks (lifelines) in a particular delicate position. However, these networks form critical infrastructures such that safety and security of each one of them depend on all the others. The more these critical infrastructures are interdependent, the more their failure can have catastrophic consequences on the whole. To strengthen and manage these infrastructures, and reduce their vulnerabilities, several research issues appeared in the past. This paper aims to present a modeling approach to solve problems related to the cause of failures of critical infrastructures. These issues are treated through agent based modeling and simulation by providing proactive solutions and take appropriate decisions by creating adaptive simulation scenarios.**

***Index Terms*—Critical infrastructure, interdependency, security, simulation, multi-agent systems.**

## I. Introduction

Critical infrastructures are constituted by all essential systems providing the life progress of communities as well as the social and economic well-being of their citizens such as the electricity and gas networks, water, telecommunications and transportation. Given the technological advancements, these infrastructures that were previously physically separated are becoming more and more interconnected creating interdependent infrastructure networks. These networks are characterized by an interdependency (that can be logical, geographical, physical or cybernetic) which offers many benefits for their proper functioning. However, a failure in one of them due for example to the unavailability or absence of a service can negatively influence on all the others.

The anticipation of solutions to the problem of production of these unwanted exceptional events can avoid or at least mitigate catastrophic arising situations. In this context, modeling and simulation appear as a first step to investigate and to deal with propagation of these failures. Simulation, and in particular, the multi-agent simulation allows us to represent the interdependence of these infrastructures, the diversity of their components (systems, sub-systems ....), their services and their interactions.

This research work seeks to identify issues related to the cause of failure of these infrastructures by modeling their functional aspects and conducting virtual simulation experiments to provide proactive solutions for decisions that must be taken in case of emergencies in the environment related to these infrastructures.

In the first part of this paper, the terms and concepts used in this manuscript are defined. In the second part, we present some existing studies and works that provide approaches that meet the needs and requirements of security for critical infrastructures. Finally, in the last section, issues about the proposed approach are given.

## II. Background

The USA Patriot Act of 2001 [1] defined critical infrastructures as "*systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters".* Secure and protected critical infrastructures like those indicated in Fig. 1 lead to a better living of citizens.

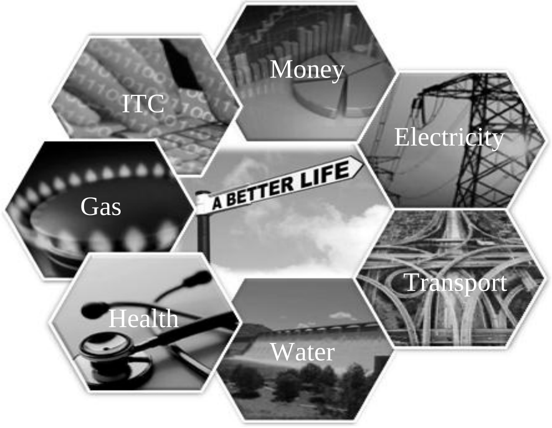

Fig. 1. Critical Infrastructures.

These Critical infrastructures cover a wide range of sectors, including the banking and financial sectors, transport and distribution, energy, health, supply and communications. Fig. 2 shows a classification of critical infrastructures. They are mainly belonging to four main sectors.

From this classification we can affirm that a failure in one critical infrastructure has serious repercussions on the others due to the interdependency between them. Rinaldi,

Manuscript received June 14, 2013; revised October 24, 2013.

Safa Attia, Abdelhak Boubetra, and Manel Saad Saoud are with the Department of Computer Science, University of Bordj Bou Arreridj, Algeria (e-mail: s.attia@univ-bba.dz, a.boubetra@univ-bba.dz, m.saadsaoud@univ-bba.dz).

DOI: 10.7763/JACN.2014.V2.70

Peerenboom, and Kelly [2] defined the interdependence of critical infrastructures as a bidirectional relationship between infrastructures such as the status of an infrastructure is affected by or correlated with the state of another. More specifically, we say that two infrastructures are interdependent if one depends upon the other and vice versa as shown in Fig. 3. Inside each infrastructure, there are dependencies between components. Likewise, these components can be in relationship with other components of another infrastructure.

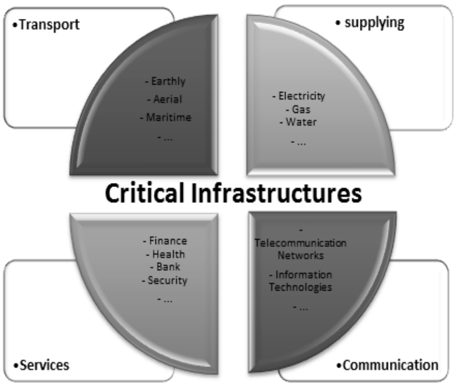

Fig.2 . Main critical infrastructure sectors.

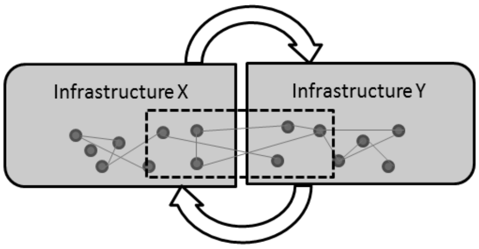

Fig. 3. Critical infrastructure interdependency.

These interdependencies can be of different types. Rinaldi, Peerenboom, and Kelly identified four classes of interdependencies: physical, cyber, geographic and logical [2]. This increased interdependency put critical infrastructures in a particularly delicate position and causes failure that can have catastrophic consequences on the whole. In [3] a failure is defined as "*a potentially damaging event that results from deficiencies in a system or in an external element on which the system depends. Failures may be due to results from software design errors, hardware degradation, human errors, or corrupted data.".* As an example, we can mention the interdependency between gas and electricity infrastructure due to the fact that several installations of gas infrastructure need electricity to function. A disturbance in the electrical system can affect the natural gas network, and the loss of natural gas can reduce the production of electricity.

Failures can arise from critical infrastructure weaknesses and vulnerabilities located at physical or logical components, and also from the interdependencies between the critical infrastructures. Whatever the origin, failures can easily spread out, affecting the operating safety and the security of all the infrastructures.

Securing the critical infrastructures means to defend them by preventing all failures and by well understanding the multi infrastructure systems and their interdependencies. To achieve this goal, modeling and simulation are used as basic elements in the process of system analysis and interdependencies. These latter became very widespread methods in different disciplines to understand, analyze and try to predict the behavior of complex systems. There are several different modeling and simulation methods to study the behavior of singular critical infrastructure; while the modeling of interdependencies between different infrastructures and the description of their complex behavior through simulation remain a challenging issue for many research works. As a result of the diversity of critical infrastructures, the interdependency existing between them and the multitude of arising failures, several modeling techniques have emerged. Currently, there is not a common and accurate classification of all proposed models. However, in [4] there are two main categories: analytical models and simulation techniques.

## III. Critical Infrastructures Modeling and Simulation

A survey dedicated to the field of modeling and simulation of critical infrastructures was prepared by the authors in [5] containing the state of the art of methodologies, applications and tools for critical infrastructure protection that appeared during the period from 1999 to 2010. From this survey, we can mention the different approaches used in this field, namely, as shown in the classification of Fig. 4, systems dynamics, multi-agent systems, decision trees, Monte Carlo methods and, continuous and discrete time-step. We focus in our paper on the modeling and simulation-based agents.

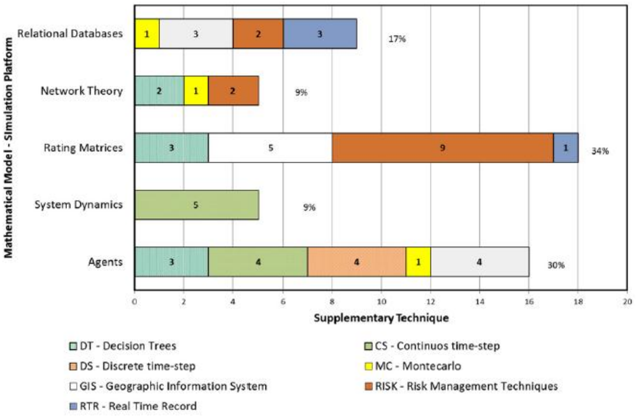

Fig. 4. Combinations of modeling techniques in the reviewed literature [5].

### A. *Agent Based Modeling and Simulation*

Agent based modeling and simulation (ABMS) is an approach using intelligent interconnected agents. This approach is widely used for the study of complex systems. However, in [2] critical infrastructures are defined as complex systems. Therefore, they can be processed by the ABMS.

### B. *Related Works*

Works to protect critical infrastructures and consolidate and reduce their vulnerabilities were initiated since 1996.

The leader in this field is the United States by the establishment of the Committee on Critical Infrastructure

Protection in 1996. Since then, taking into account the safety and security of critical infrastructures has become a great challenge and a research focus for many researchers in several laboratories. In what follows, we will mention some related works, most of which used the ABMS:

- **ASPEN (1996):** Researchers in the Sandia National Laboratories SNL [6] have developed a model of micro-simulation-based agents for the U.S. economy. ASPEN has the possibility to considerably improve the analysis capacity and the comparison of economic policies using a set of agents. SNL have extended this model by including rules and interactive agents representing the electric power, fuel and gas as the ASPEN-EE (Electricity Enhancement) [7]. This model simulates the effects of interdependent decisions and disturbances in the power system on other critical infrastructures in the U.S. economy.
- **CISIA (2004):** This simulator is described by Panzieri, Setola, and Ulivi [8] as a hybrid of two modeling approaches: interdependency analysis and system analysis. CISIA simulator is designed to analyze the short-term failure by modeling the behavior of a set of critical infrastructures using a modeling paradigm based interactive agents where each agent is a macro component of the modeled system and its behavior is described by fuzzy logic.
- **AIMS (2006): A** multi-agent system developed by the Laboratory of Intelligent and Adaptive systems at the University of Canada that models and simulates the interdependencies. AIMS can create critical infrastructure models and analyze the behavior of the system modeled by scenarios. One of the special features of AIMS is that it provides users with a set of pre-defined components (e.g. pipes, switches ...). In this paper [9], the authors focused on the AIMS approach and the Service Oriented Simulation to model services, routes and scenarios existing between the various components of interdependent critical infrastructures, such that each agent models one of these components and their behavior outlines the provided services.
- **CIMS (2006):** This simulation environment which is based on a discrete event agent was developed to provide decision makers with a powerful tool to assess infrastructure vulnerabilities and consider the various interactions and interdependencies between these infrastructures. CIMS is sponsored by IDAHO National Laboratory (INL) in its mission to protect critical infrastructures and civil protection. CIMS was presented in [10]; each infrastructure was plotted as a network consisting of a set of nodes and edges. The nodes indicate the different areas of influence in the infrastructure and each arc presents a direct level of dependency between two nodes. The architecture of CIMS uses an agent based approach to model the infrastructure elements, behaviors and existing relationships between its elements. Several models have been developed for some critical infrastructures such as power systems, transportation systems, computer networks, etc. In 2007, CIMS was combined with a genetic algorithm in a model proposed by Permann [11], in order to find optimal ways to protect critical infrastructures assets in cases of emergency.
- **DIESIS KBS (2009):** The general idea of the proposed approach [12] within the European EISAC project is to develop a knowledge based system (KBS) based on the ontology of different critical infrastructures (electricity infrastructure, telecommunications and transport) and on the rules on which the federated simulation environment DIESIS must rely.

### C. *Simulation Tools Interdependencies*

To develop simulation tools interdependencies of several infrastructures, two approaches are recently used: integration approach of models and federation approach of set simulators already developed and dedicated to study infrastructure singularly.

The first one called also "from-scratch approach" consists of developing new simulators based on the integration of different models of critical infrastructures in a single multi-infrastructure model representing the different critical infrastructures with their interdependencies. The federation approach combines two or more specific simulators of singular critical infrastructure in order to develop a unified and unique simulation environment of multi-infrastructures.

- **FedABMS** is a methodology that combines ABMS and Federated simulation to study the interdependencies of critical infrastructures. This implementation of the ABMS has been proposed by [13] under the project CRESCO of ROMA University. The authors have developed the first implementation of a simulator named Critical Infrastructure Agent Based Simulator (CIAB) with FedABMS architecture using a simple example of an information system for emergency management with UML as modeling language. The CIAB combines both e-AGORA (simulator grid) and OMNeT++ (a telecommunication network simulator) simulators.

## IV. The Targeted Issues

Today, most applications require the sharing and distribution of tasks between different autonomous entities in order to achieve their goals in an optimal way. Because traditional approaches are generally centralized, current applications are based on the use of multi-agent systems.

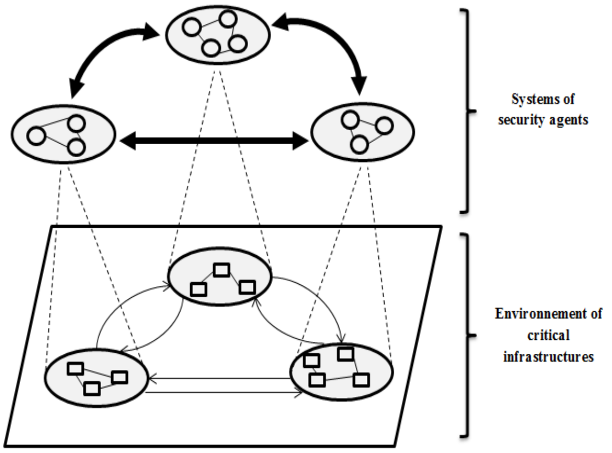
Systems of security agents
Environnement of critical infrastructures

Fig. 5. Propositional scheme.

The problem that arises in this paper relies on the study and analysis of various critical infrastructures with the existing interaction between them. For this reason, our proposition is to use multi-agent systems to simulate this problem that results from the interdependence of critical infrastructures. As shown in the propositional scheme presented in Fig. 4, we suggest creating for each infrastructure, a multi-agent system to ensure its protection. These systems consist of a set of security agents with different roles according to the state of security of the entire infrastructure.

Given that the security infrastructure is interdependent with the whole safety of the other infrastructures; we find that it is a necessity to have also a liaison between their multi-agent systems as shown in Fig. 5.

### A. *Security Agents*

The security agents have the task of ensuring a permanent, unique and instant security of the infrastructure to which they belong as well as of those who are directly or indirectly related to its protection. These agents are of two types:

- Physical Agents: act in the real world such as robots, surveillance cameras, sensors ... etc.
- Virtual Agents: such as software components, software modules ... etc.

The proposed diagram in Fig. 6 is based on three central concepts: *infrastructure*, *agent* and *role*. The infrastructure present the structuring element: it allows agents to know with whom they are interacting and what roles they should play. Roles indicate the different actions of agents in the infrastructure; such an agent must belong to a single infrastructure and have one or more roles where it will present its abilities.

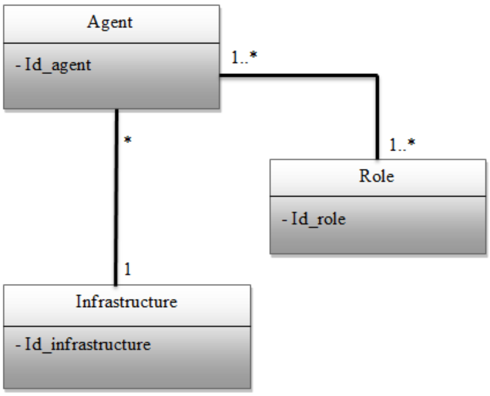

Fig. 6. Class diagram of the security system.

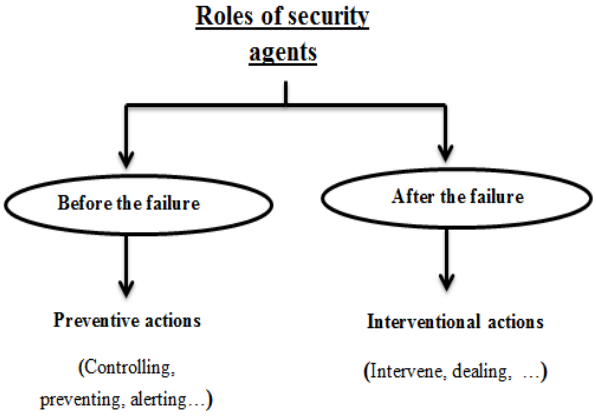

Fig. 7. Roles of security agents.

### B. *Roles of Security Agents*

As the Fig. 7 shown, we have two types of security agent's roles:

#### 1) *Before the failure*

In this section, the agent systems will make predictions about the existence or the probability of having an anomaly by monitoring and controlling the factors and reasons leading to this failure. Once the failure is detected, system of responsible agents will send alert messages to other multi-agent systems of the relevant critical infrastructure order to inform on the degree of risk in trying to limit its spread by creating adaptation scenarios.

#### 2) *After the failure*

In this step, the multi-agent systems should perform the starting from the blackout that occurred and the interventional action by applying adaptation scenarios already created in order to reduce the damage and consequences.

### C. *Types of Security Agents*

In each multi agents system, we distinguish four types of security agents as shown in Fig. 8.

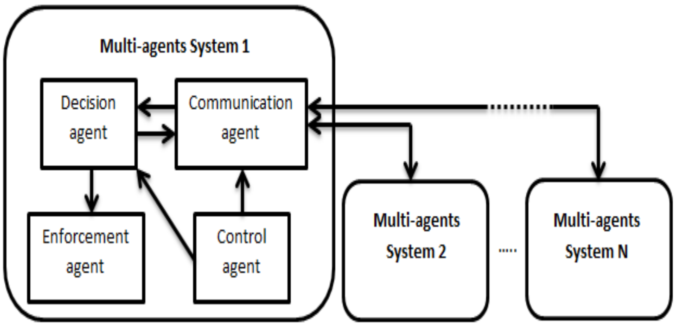

Fig. 8. Types of security agents.

- **Control agent:** When the control agent follows the factors and causes that lead to an anomaly, it states that there is an intrusion attempt to infrastructure; then an alert message will be sent to the communication agent.
- **Communication agent:** This agent is responsible for internal and external communication infrastructures by:
  • Reception of information or perception of alert messages from the control agent.
  • Sending and transmitting of these messages to the agents concerned.
- **Decision agent:** After it receives information, decision agent will provide appropriate decisions for the situation generated by creating adaptation scenarios.
- **Enforcement agent:** Receives the decision from the decision agent. The enforcement agent will conduct and apply adaptation scenarios already created.

Fig. 9 is a summary of all that we have mentioned previously. This conceptual scheme illustrates our proposed model and comprises three parts: the study area, the problematic and the proposed solution issues that we will be implemented in our future work.

- The study area: we will choose interdependent critical infrastructures.
- The problematic: present the problem of interdependence between the critical infrastructures which can be of several types that depend of critical infrastructures under study.

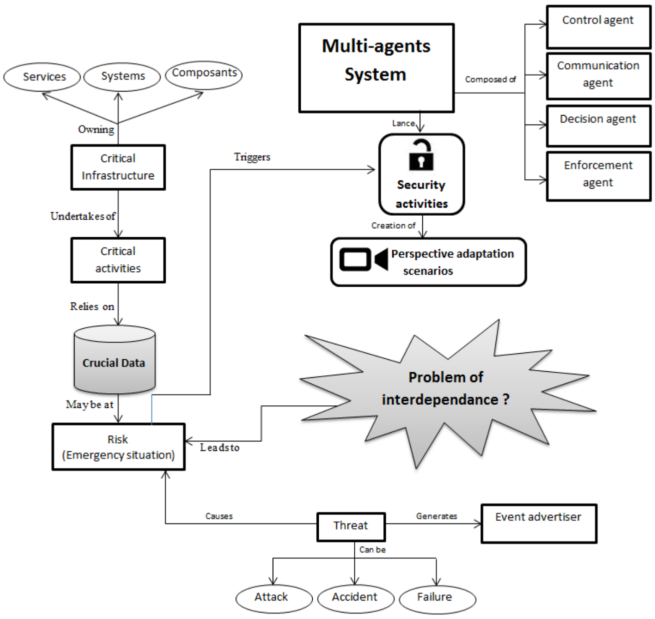

Fig. 9. Conceptual scheme.

## V. Conclusion and Perspective

Researches on the interdependencies between critical infrastructures are increasing more and more over recent years. This paper has suggested the use of multi agent security systems to resolve the problem of interdependent critical infrastructures.

The advantages of this approach over other methods are, on the one hand, the ability of these systems to formulate the dynamic and interrelated situation existing among critical infrastructures and on the other hand, these systems are more flexible and easily extensible.

As a perspective, we propose to develop this methodology in order to give an effective simulating tool.

## References

[1] U.S.A Patriot Act, "U.S.A Patriot Act: Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism," *Public Law 107-56*, October 26, 2001.

[2] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine*, pp. 11-25, 2001.

[3] R. J. Ellison, N. R. Mead, T. A. Longstaff, and R. C. Linger, "The Survivability Imperative: Protecting Critical Systems," *Defense Software Engineering*, 2000.

[4] E. Galli, "Agent Based Modeling and Simulation for critical and interdependent systems," Ph.D. thesis, Dept. Computer Systems and Production., Tor Vergata Univ., Rome, 2010.

[5] J. M. Yusta, G. J. Correa, and R. Lacal-Arantegui, "Methodologies and applications for critical infrastructure protection state-of-the-art," *Energy policy*, vol. 39, no. 10, pp. 6100-6119, 2011.

[6] N. Basu, R. J. Pryor, and T. Quint, *ASPEN: A microsimulation model of the economy*, SAND96-2459, Albuquerque, NM: Sandia National Laboratories, October 1996.

[7] D. C. Barton, K. L. Stamber, D. A. Schoenwald, K. L. Stamber, and R. K. Reinert, "An Agent-Based Microsimulation of Critical Infrastructure Systems," in *Proc. International Energy Foundation's ENERGEX 2000 Conf.*, 29 Mar 2000.

[8] S. Panzieri, R. Setola, and G. Ulivi, "An agent based simulator for critical interdependent infrastructures," *Securing Critical Infrastructures*, 2004.

[9] E. Bagheri, H. Baghi, and A. A. Ghorni, "An agent-based service-oriented simulation suite for critical infrastructure behaviour analysis," *International Journal of Business Process Integration and Management*, 2007.

[10] D. D. Dudenhoeffer, M. R. Permann, and M. Manic, "CIMS: A framework for infrastructure interdependency modeling and analysis," in *Proc. the 2006 Winter Simulation Conf.* , 2006.

[11] M. R. Permann, "Genetic algorithms for agent-based infrastructure interdependency modeling and analysis," *SpringSim 2007*, Mar. 2007.

[12] V. Masucci, F. Adinolfi, P. Servillo, G. Dipoppa, and A. Tofani, "Ontology-based critical infrastructure modeling and simulation," *Critical Infrastructure Protection III, IFIP Advances in Information and Communication Technology*, vol. 311, pp. 229-242, 2009.

[13] E. Casalicchio, E. Galli, and S. Tucci, "Federated Agent-based Modeling and Simulation Approach to Study Interdependencies in IT Critical Infrastructures," in *Proc. 11th IEEE International Symposium on Distributed Simulation and Real-Time Applications*, 2007, pp. 182-289.

**Safa Attia** was born in Setif, Algeria in 1989. She received her computer science bachelor degree from Bordj Bou Arreridj University (Algeria) in 2009. She received her Master's degree from Bordj Bou Arreridj University in 2011. Now she is a Phd student at the University of Bordj Bou Arreridj under the direction of Dr. A. Boubetra. Her research interests include Agent Based Modeling and Simulation.

**Abdelhak Boubetra** was born in Bordj Bou Arreridj Algeria in 1959. He is an associate professor and the Head Research Group of computer simulation in the computer Science department of the University of Bordj Bou Arreridj in Algeria. He received a computer science engineer degree from the University of Constantine (Algeria), a Master Philosophy degree from the University of Lancaster (U.K) and a Doctorat degree from the University of Setif (Algeria) in computer science. His research interests include data bases, software engineering, and green IT.

**Manel Saad Saoud** was born in Bordj Bou Arreridj, Algeria in 1988. She received her computer science bachelor degree from Bordj Bou Arreridj University in 2009. She received her Master's degree from Bordj Bou Arreridj University in 2011. Now she is a Phd student at the University of Bordj Bou Arreridj under the direction of Dr. A. Boubetra. Her research interests include Agent Based Modeling and Simulation.