Simulation of active products cooperation for active security management

Ahmed Zouinkhi, Amel Ltifi, Mohamed Ben Gayed, Naceur Abdelkrim, Eddy Bajic, Eric Rondeau

8th International Conference of Modeling and Simulation - MOSIM'10 - May 10-12, 2010 - Hammamet - Tunisia
"Evaluation and optimization of innovative production systems of goods and services"

SIMULATION OF ACTIVE PRODUCTS COOPERATION FOR ACTIVE SECURITY MANAGEMENT

Ahmed ZOUINKHI, Amel LTIFI, Mohamed BEN GAYED, Mohamed Naceur ABDELKRIM

MACS / ENIG
Unit of research MACS (Modelling, Analysis and Control of Systems), Ecole Nationale d'Ingénieurs de Gabès, Rue Omar Ibn Elkhattab, Zrig – Gabès 6029 - Tunisia
ahmed.zouinkhi@cran.uhp-nancy.fr

Eddy BAJIC, Eric RONDEAU

CRAN / Nancy University
Research Center for Automatic Control - CRAN - CNRS UMR 7039, Henri Poincaré University, Nancy, BP 239, 54506 Vandoeuvre-les-Nancy, France
eddy.bajic@cran.uhp-nancy.fr

ABSTRACT: *Wireless sensor networks (WSNs) are a new paradigm of telecommunication networks. WSNs are designed to perform efficient data collection and environment monitoring, among other applications. This article presents an approach of modelling and simulation of cooperation between active products that are equipped with a platform of sensor networks and ambient communication capabilities in order to increase their security, in a context of ambient intelligence of a deposit for chemical substances. The concept of active products supported by a model that we propose, offers the possibility for objects to interact between them in an autonomous, transparent and intelligent way, without any human help. Indeed, the model presented exploits the advantages offered by a network of sensors to generate active interactions between the products in order to guarantee active security, i.e., an interaction bilateral protected, transparent, autonomous and intelligent. We introduce the term of active security in industrial chemical storage sector, taken in charge directly by the active product subjugated by a constrained security level. The simulation of the model assembled with the Castalia-OMNET++ Tools language.*

KEYWORDS: *Active product, Cooperation, Castalia, OMNET++, WSN, Security.*

1 INTRODUCTION

In the sector of the chemical industry, the priority is granted to the protection and the safety of goods and people. It is for that besides that one seeks without cease to develop increasingly reliable means ensuring safety at the level storage and handling of the dangerous chemicals, from where the integration of the Wireless Sensor networks (WSN) in the systems design of security.
Currently, many security systems depend on safety measurements taken by others eventually exposing people lives to unpredictable environments as for examples storage and transport activities of hazardous chemical substances.
This subject attracted the interest of several research projects as the computing department at Lancaster University [Strohbach and al., 2005] conceived cooperative particles with perception, analysis and communication capacities that operate by information sharing principle.
Closely relative, a research work led by TecO lab from Karlsruhe University and MIT [Decker and al., 2004], announces the concept of Active physical documents for the management of integrity of written documents (files, notes, reports ...) to respect restricted accesses and keep the track of the document changes. This system bridges the gap between the status of electronic documents and their printed-out copies in the physical world. It introduces the DigiClip system that provides a solution to automatically enforce such consistency by converting passive paper documents to active physical documents.
CHAOS [Liu and al., 2000] project also leaned on the intelligent object approach to secure the exchange of information in distributed systems.
Recently, there are projects that address the safety of products, eg [Cobis, 2008], [Strohbach and al., 2004] [Strohbach and al., 2005] and [Brian and al., 2008].
COBIS project (Collaborative Business Items) [Strohbach and al., 2005] has developed a new approach to business processes involving physical entities such as goods and tools in enterprise. The intention is to apply advances in networked systems to embed business logic in the physical entities. COBIS project improved the networked systems to create finally cooperative products named particles, incorporated into various application contexts particularly for supervision dangerous products.
In this project, Sensor measurements are processed by the perception component that associates sensor data with meaning, and produces observational knowledge that is meaningful in terms of the applications domain.
This information is stored and maintained in a knowledge base (Knowledge base) which reflects current knowledge of the product on its environment, in which is structured into facts and rules. For example a product will need to know its content and a list of incompatible materials to detect a nearby product with a reactive chemical. Otherwise the local knowledge base will be used and in case of a negative result, the fact would first

be searched in the local knowledge base and then in the knowledge based of nearby products.
The detection of danger in COBIS is made by processing a knowledge base in which the rules of incompatibility, proximity and quantity are stored.
He applied his approach to product safety in a warehouse and takes into account data below as sources of threats;
- Storage of hazardous materials outside an approved area for longer than a predefined time interval.
- Storage of incompatible materials in proximity, in terms of predefined minimum distance.
- Storage of materials with others, all exceeding the critical mass in terms of predefined maximum amount.
This project does not include static rules and is not a classification level of dangerousness. Also the cooperation mechanism between products is decentralized among COBIS indeed the products share knowledge, i.e. the knowledge base of a product is available in the others. Therefore, if a threat is detected, products generate an alarm. In addition to his work in the existing knowledge is static since products will often be in the same situation.

Also, [Brian and al., 2008] is considering the problem of Object Safety: how objects endowed with processing, communication, and sensing capabilities can determine their safety. He assigned an agent to each object capable of looking out for its own self interests, while concurrently collaborating with its neighbors and learning / reinforcing its beliefs from them. Each product is represented by "an object safety agent", it deals with information from environmental sensors, in a known situation.
A base station is an entity that provides a description of scenarios, including its initial situation. When the agent detects a threat, it seeks confirmation from its neighbors. Upon confirmation, a base station is notified, and either confirms the threat and takes further action, or sends the agent a new situation description.
A situation is represented by attributes that describe the environment and the normal behavior of the agent in this situation. It is described by static rules that contain two types of parameters numerical and symbolic. The notion of threat here does not take account of community rules (compatibility,) or dynamic rules, because the dialogue between agents is done only by the sensor data. In addition there is no classification of the degree of dangerousness.
In addition, the confirmation of a threat, which is finally confirmed by a base station, led to a mechanism for cooperation among central.
Finally, in order to overcome the limitations of projects [Strohbach and al., 2005] and [Brian and al., 2008] above, we present our model in a security purpose. Our work involves transforming products with dangerous nature into communicating entities assuming the surveillance of its environment while collecting information from its surrounding. We present, as well, the relation with human operator in the monitored environment by controlling his abilities like mandatory professional authorizations.

In this paper, an internal model of an active product is implemented and then was validated by the simulation software Castalia based on the OMNET platform.

The rest of the paper is organized as follows: Section 2 presents the notion of intelligent product. Section 3 introduces the concept of active products for the security management. In Section 4 a functional model of an active Product is proposed. Section 5 presents the cooperation mechanisms between products based on messages exchanges. Section 6 exposes the internal model of active products behaviour. Section 7 presents the simulation results of the system. Finally Section 8 concludes the paper.

2 INTELLIGENT PRODUCT

According to [McFarlane and al., 2002] and [Bajic, 2009], an intelligent product is defined as a physical and informational representation of an object offering the following characteristics:
1. It possesses an unique identification;
2. It is capable to communicate effectively with its environment;
3. It can retain or store data about itself;
4. It deploys a language to display its features and its needs over its lifecycle;
5. It is capable of participating in or making decisions relevant to its own destiny;
6. It can survey and control its environment;
7. It can generate interaction by services offering: contextual, personal, reactive services.

Automatic identification involves automatically the identity of an object through an Auto-ID technology. For example, real-time access to the identity of a product through the automatic radio frequency identification to determine the presence of a product, and indirectly it is possible to determine its location [Finkenzeller, 2003]. It is important to note that in the definition of intelligent product it is possible to distinguish two levels of complexity: the product that contains the information in its environment and a product that supports decision-making mechanisms [Wong and al., 2002]. The latter is the more complex because in this case it must give the product decision-making mechanisms in implying that the product must have a capacity for integrated analysis to assess and make the best decision according to its condition and context. According to [Kärkkäinen and al., 2003], the concept of intelligent product is associated with the act of managing information of an individual product through its life cycle by integrating the flow of information and equipment to provide services in an Internet network.
As concrete example of applying the concept of intelligent product we quote the traceability [Vullers-Jansen and al., 2003] in its life cycle product Automatic identification of each individual product to link a product with its physical representation of information in a distributed information system. The goal in this case is to record and update all information associated with a dynamic prod-

uct (such as his statements, the operations he has endured ...) on an electronic tag, for example, or on one or more databases distant. Thanks to this, an actor in the supply chain can know at any time the detailed history of a product. Eventually, the information recorded on a label or on electronic databases may be used as input for a subsequent process to optimize a given transaction.
As another example, we mention the contribution of information stored on an intelligent product in a control process in a production system. In this case, the data captured is enriched with the contribution of the product information in making decision at the operational level through its memorization and communication. Indeed, the introduction of an automatic identification system allows the physical product to be recognized as providing the information to influence decisions and operations that a system performs with him. This involves assigning a more active role in a physical product. In this vein, [McFarlane and al, 2002] states that a product is an intelligent article of manufacture that has the ability to monitor, analyze and reason about its current or future, and if it is necessary to influence his destiny.

The availability of information on the product and the process leads to a visibility or observability [McFarlane and al, 2003] increased the changes of states of the products. Consequently the consideration of individual characteristics of a product immediately leads to a larger number of possible states.

3 ACTIVE PRODUCT

The concept of active product is said to provide a capability to communicate, inform, learn, decide and react to stimuli and perturbations of its environment, to allow the product to adapt, to influence, to cooperate and to transform the behavior of its environment [Zouinkhi and al., 07] [Dragos and al., 07]. The product is an intelligent player and proactive in its ambient environment with which it interacts via wireless communication. In the chemical industry, we can use this concept on an industrial product type container terminal for the safety of goods and people.
This object is composed of a drum containing a chemical substance which is attached to a microelectronic device which can communicate with other devices that are attached to other barrels. Thus a Product to Ambient Intelligence is able to "feel" its environment through sensors, to decide and make a choice of action / reaction according to specifications and / or share information in a collaborative environment to communicate with its environment. Microelectronic devices, called particles proposed in our work are "pParticle" marketed by "Teco", and from European research projects. If two particles are in the same field of communication, they communicate with each other through messages sent by radio frequency. Also, a particle can communicate with the supervisor in the same way. In addition, the particles can take advantage of services in the environment if they come near a Wbridge, the world without interfacing son to Ethernet / Internet.

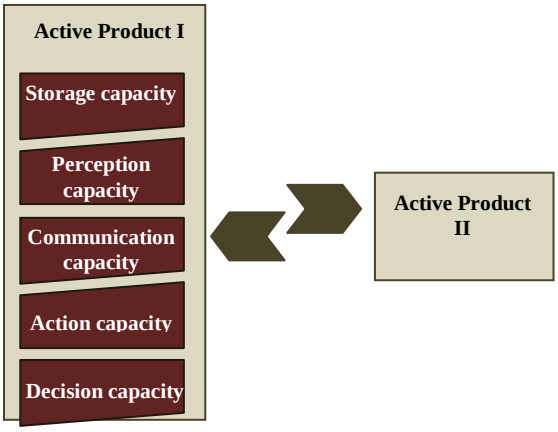

Figure 1: The capacities linked to an Active Product

4 FUNCTIONAL MODEL OF AP

Our model is depicted in Figure 2. A knowledge base processes the information of different sensors based on decision rules that reflect the current status of product. When a product detects a threat from the sensor information or services offered, the class on a level of dangerousness and depending on the value of the actuator is triggered.
Our model can handle the security of its environment by cooperating with the enclosures (PA, Op, Resources and Others).
A base station provides the current status of product, and then it allows the product to manage its intrinsic safety in cooperation with others.

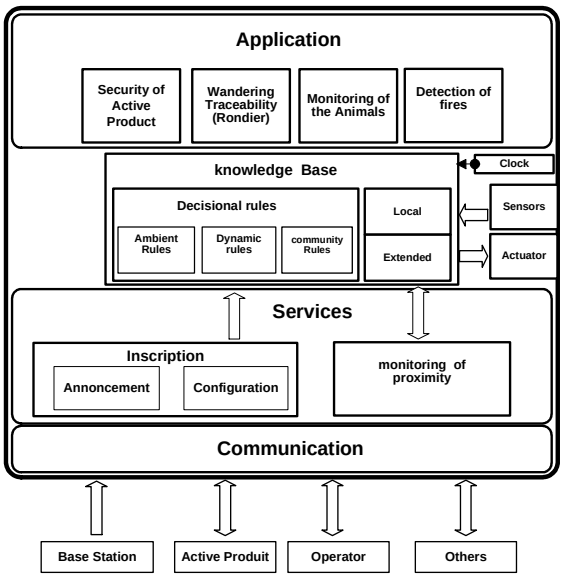

Figure 2: Functional model of AP

The knowledge base of a product can be represented by the following figure 6. We use a prolog style notation. The literal X refers to the others products.

Knowledge domain	*Product (product type, ID, Symbol)*
Static Rules	*D=Temperature (<LoLimit or > HiLimit)* *G=Temperature (in [LoLimit + ΔT, HiLimit - ΔT]* *A=Temperature (in [LoLimit, Lo-Limit + ΔT] or in[HiLimit -ΔT, HiLimit])* *……..*
Dynamic Rules	*Dangerous=Delay(A)>T_p*
Community Rules	*Dist=Distance (AP, X)* *Product Symbol * Tab compatibility P* *Product Symbol * Tab compatibility Op* *Product Symbol * Tab compatibility Others*
Actuators	*Message* *On :Incomp*(Dmin<Dist<Dmax)* *Alert On : (Dist<Dmin) * Incomp*

Figure 3: Knowledge base of an AP

Hazardous detection is done after data processing by the sensor knowledge base and depending on the application of decision rules. These rules are of three types namely, static, dynamic and community.
If a threat is detected an actuator will be activated and a base station will be announced.
The decision of a threat is made by applying a function that allows us to provide the level of security. The sources of threats are numerous: environment, proximity, compatibility between products, operators and resources.
In addition we have classified the threats according to their degree of danger that is threatening or bad.
We have introduced a security warehouse, taking into account resources and operators.
The cooperation mechanism integrates the two approaches later centralized administration and decentralized cooperation between products side active.
Active products worked together and they exchange information on the environment and the security level in real time by a product that can manage asset safety and security of its environment.

4.1 Security rules

To insure a good security surveillance of the product, three safety levels were established: (G) good level, (A) average level, (D) dangerous level. Determining security levels results after applying some security rules which are divided into three categories:
- *Static Rules:* these are rules that engage the product alone in its environment, This product measures some values defining its safety level such as temperature, humidity, shock, luminosity ... these can be used eg for fire detection. In order to keep itself in a stable sane state, these values should not exceed certain min or/and max limits.
- *Dynamic rules:* these are rules related to the product by itself considering its state evolution through time. For example some product could not be affected if they reach a certain temperature threshold but the fact of reaching it several times in a period of time can bring the product in an alarming state.
- *Community rules:* every product can have compatibility constraints with other ones of different nature. This incompatibility is established from the security symbols and also from risk and safety phrases according to the European directives 67/548/EEC. These rules can be used to detect some events such as chemical interaction. On the other hand, the manipulation of certain product requires an operator with specific fitness and aptitude; consequently, a product needs a well determined operator quality.

5 MECHANISMS OF INTERACTION

The organization of the autonomous systems rests on approaches arranging its informational structure; its approaches aim the aspect particularly controls and administration which ensures in fact the good management of the interactions circulating between the various elements constituting the autonomous system. Within the framework to show these interactions, we take the example suggested by [Garate and *Al*, 05] who developed a gathering network of the apparatuses house automations (TV, refrigerator, etc.) connected and managed by a central controller. The network gives to the user the advantage of communicating with these apparatuses and of being useful of their services and functionalities in natural language. However, this interaction an obligatory passage by the controller. The approach is thus centralized and does not integrate in the apparatuses house automations of self capacitance of interaction. Another example developed by [Rajeet and al., 05] which shows an application of pervasive technology RFID for the theft protection device of the bicycles in campus university spaces, a label RFID is placed on each bicycle and information is controlled by a PC located in a control room. The approach is thus centralized and in case of the dysfunction of the manager the system does not become functional any more.
The mechanism of co-operation at [Brian and Al, 2008] Texas is centralized because the confirmation of threat is done finally by confirmation of a basic station, which it will give to the product a new situation.
Indeed, the mechanism of co-operation between products at [Strohbach and Al, 2004], [Strohbach and Al, 2005] is decentralized the products share knowledge, i.e. the base of knowledge of a product is available in the others. Consequently, if a threat is detected, so the products set off an alarm.
On the other hand, the objective consists with stage the mechanisms of interaction in which the objects are able to communicate, to acquire information, to decide and react to the stimuli and disturbances of its environment

in order to make it possible the product to deal with its intrinsic safety and decentralized total safety in its interactions with other products or people touching an aspect finally

In fact, our system of active security management initially includes/understands a whole of product credits being the subject of the mutual interactions and sharing between them a flow of information and in second place a manager who undertakes to initialize and to gather the data coming from each active product. In this aspect immerses two forms which are exploited in this system: centralized approach related to the manager (aspect administration) who appears in the total collection of the data coming from all the community of the active products; it constitutes, in fact, the only source allowing the configuration and the acceptance of a new intruder. After the achievement of this stage, the system thus operates according to a decentralized approach distributed on the actors of the interaction.

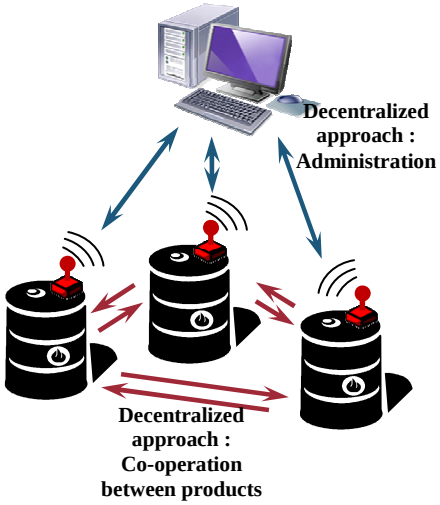

Figure 4: Existing approaches in the system of the security management proposed

6 INTERNAL MODEL OF THE ACTIVE PRODUCT

The objective of our work is to represent the behaviour of the active product and the stream of messages through a wireless network in order to achieve cooperation interaction between products.

To cross the product towards the Active state must be subjected to a strategy allowing him to get correctly to manage its own active security in a warehouse [Zouinkhi and al, 2009]. It passes inevitably in definite states to know registration, configuration, surveillance and communication and finally internal surveillance; as indicated in figure 5.

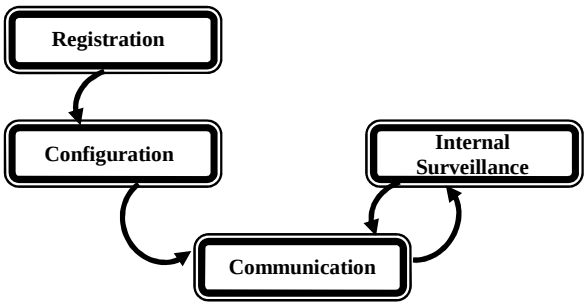

Figure 5: The states of an Active Product

6.1 Registration part

This part manages the registration of products that announce them self in the community by sending a discovery message detected by the administrator. As it is indicated in figure 6.

To achieve this action to register the product within the community, we proposed two types of messages:

- CTR message is an empty message to the manager and said the product introduction in the network, it is sent continuously broadcast by way of detection.

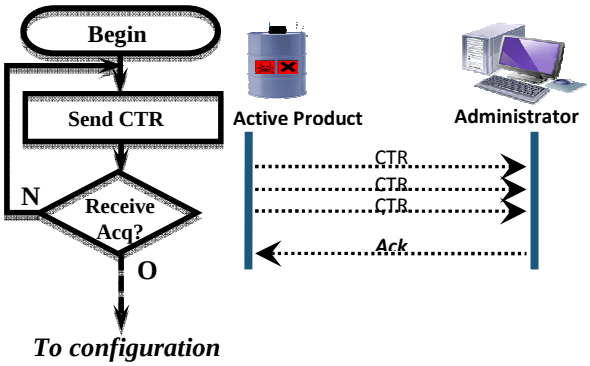

Figure 6: Sequence diagram and flow chart of the registration of an active product

6.2 Configuration model

After registration every product must evolve in its environment by identifying every other active product existing in surroundings. Identification is made by installing a configuration on every product allowing him to interact correctly in the community;

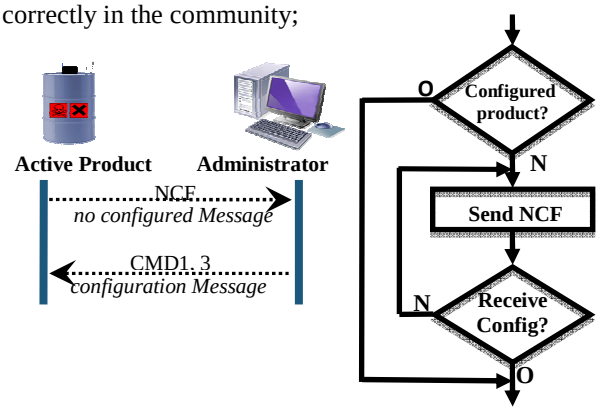

Figure 7: Sequence diagram and flow chart of the configuration of an Active product

The active product gets this information by sending specific messages to the administrator. In fact, the necessary configuration to the product depends on its initial state. The product can have a configuration already preinstalled in his memory; it can contain information about the symbols of product or security rules or both. According to this configuration we proposed three types of messages no configuration (NCF) issued since the product.
NCF0: If the product has neither the information symbols of security nor its security rules.
NCF1: If the product has only the information symbols of security.
NCF2: If the product has only configuration of its security rules.
These will be sent continuously in broadcast. Side of the administrator responds with the message type command respective configuration:
CMD1: message supporting the configuration of the product classification.
CMD3: message supporting the configuration of the various security rules.

6.3 Surveillance and communication model

Once the product is correctly configured; this last becomes absolutely able to supervise the neighbourhood.
Any modification of its environment infringing the rules of individual or mutual securities must be detected, to be diagnosed and must procreate external actions allowing to cover by actions or an information for surrounding environment on the actual level of security of the product.

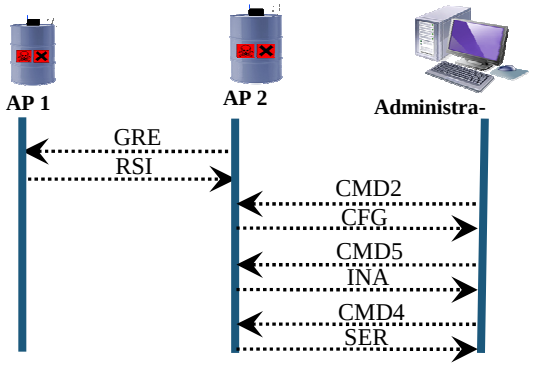

Figure 8: Sequence diagram of the surveillance and communication model

These correlations are made by means of the following messages:
Greeting message GRE : It is a message transmitted automatically and periodically between products in their normal state of functioning. It represents a message of salutation carrying information clean of the product (name, symbols of security), its actual level of security; and has a further role contributing to the calculation process of the distance separating two AP. The message of salutation is important for surveillance and communication between products because he notifies the state of the active product and transmits him his main characteristics. The structure of the greeting message is represented in figure 9.

Figure 9: Structure of the greeting message

Structure am composed of 5 parts whose first is called subject and includes the nature of the message; in that case (GRE: Greeting), the 3 following are the basic information of the product (name and security symbol) and the last contains the actual security level of the product.
RSI message: The information of this type of message contains in most cases the received signal strength indicator. It is used to estimate compatibility with minimal distance between active products.
In fact, this method of measure is based on equivalence between the received signal strength indicator and the value of the distance separating both products. This dependency is translated by a quasi linear curve represent in this figure.

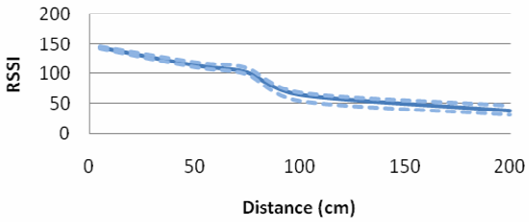

Figure 10: Dependence RSSI - Distance

After received a GRE message, the active product performs therefore its RSSI (Received Signal Strength Indicator) counting, then send result across the RSI message. The first active product accepting this message reads the value of RSSI, verify if the value of distance exceeded the allowable value or not. Here is the structure of the message RSI;

Figure 11: Structure of the RSI message

The first includes the subject of the message to know (RSI), the second (CIA) contains the value of measured distance.
- *INA Message:* this message carries the ambient sensors values embedded in the product. It is sent in fact having accepted a request since the administrator to provide him this information.
- *CFG message*: a message emitted by AP after an administrator request, contains the specific configuration in the AP.
- *SER message:* a broadcast message containing the AP security rules values, it is also sent after a request of the administrator.
The administrator participates in the communication part by specific command messages.
CMD2 : Administrator requires the configuration of the AP through this message.

CMD4 : Administrator asks for Security rules Configurations.
CMD5 : Administrator asks for specific ambient information of APs.
Theses messages have the same structure, they are composed of three parts: CMD indicates the subject of the message to know command; TYPE indicates the nature of command (2,4,5); and the last CAD includes the address of the product.

Figure 12: Structure of the CMD message

The figure 13 introduces the flowchart of surveillance and communication. It begins by finding the GRE message formed since the model of internal surveillance.
This last applies security rules to recovered surrounding data and determines the state of security which will be transmitted via the GRE message.
The model of surveillance and communication treats all accepted messages and proves if they are intended for the product or not; then according to the nature of the accepted message it performs appropriate action.

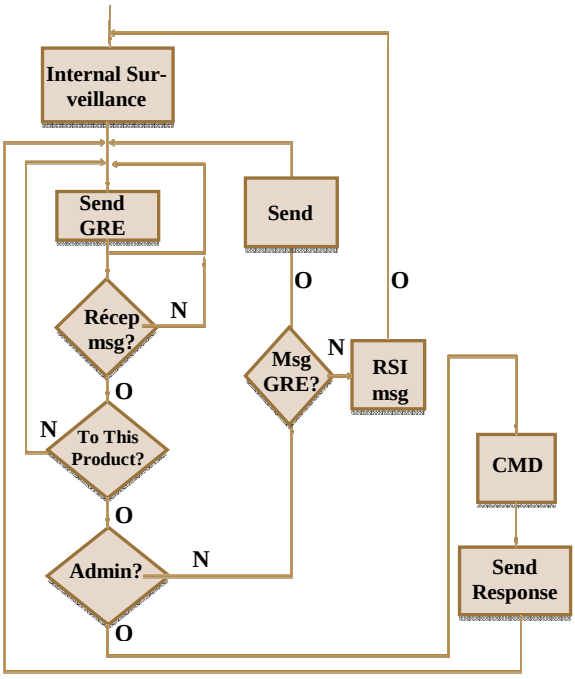

Figure 13: Flow chart of the surveillance and communication of an Active product

6.4 Internal surveillance model

Surveillance is procedure in which the product applies functions of its surrounding rules and begins treating measurements generated since its platform of sensors to decide on the common level of security finally. The messages that can issue in that case are the ALERT messages (ALE) announcing a state of threat and requiring an immediate intervention.

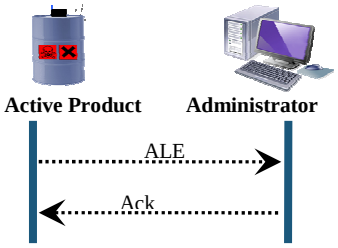

Figure 14 : Sequence diagram of the internal surveillance model

ALE message: it is sent in case of alert; this message puts back to the administrator the state of security faulty with the measurements which caused this state..
Static safety rules were performed by a function that locates the measured sensor value into its corresponding safety level. We give below an example of the temperature sensor static rule and cooresponding threats (D : Danger / A : Average / G: Good / : D=(T < LoLimit or T > HiLimit), A=(T < LoLimit+Delta or T > HiLimit-Delta), G= elsewhere.
This operates as follows: safety level is considered Dangerous if at least one (D) appears in the functions results, otherwise, safety level is considered Average if at least one (A) en appears in the functions results, if not safety level is considered Good. According to the final safety level appropriate messages will be transmitted with the necessary information about the ambient values which are GRE for (G) and (A) levels and ALE for (D) level.

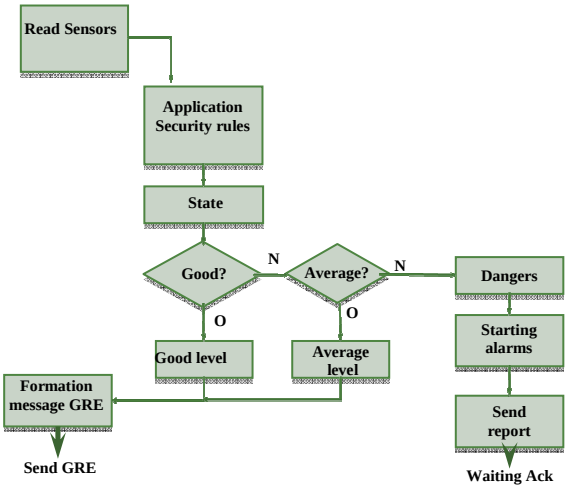

Figure 15: Flow chart of the internal surveillance

7 CASTALIA SIMULATION

Castalia is a Wireless Sensor Network (WSN) simulator based on the OMNet++ platform that can be used by researchers and developers who want to test their distributed algorithms and protocols within a realistic wireless channel and radio model which takes account of the physical characteristics of the radio [Hai and al, 07]. Castalia can also evaluate different platform characteristics for specific applications, since it is highly tunable, and can simulate a wide range of platforms.
The Castalia simulator is used for a long time as simulation tools of WSN systems.

Several works opted for the Castalia simulation in fields like communication systems.
[Andreas and al, 08] have used Castalia/OMNET++ to evaluate their solution for distributed node monitoring called DiMo (Distributed Node Monitoring in Wireless Sensor Networks), which consists of two functions: (i) Network topology maintenance, and (ii) Node health status monitoring. And they compared DiMo to existing state-of-the-art node monitoring solutions. So they implemented DiMo in Castalia 1.3. The simulations are performed for a network containing 80 nodes, arranged in a grid with a small Gaussian distributed displacement, representing an event detection system where nodes are usually not randomly deployed but rather evenly spread over the observed area. The characteristics of the Chipcon CC2420 are used to model the radio. 500 different topologies were analyzed.
In order to evaluate the Castalia Simulator, [Hai and al, 07] have compared simulation results with experience results. The first part was to reproduce the connectivity patterns seen at the real deployment by using the parameters in the channel/radio models. The network simulated contains 9 TelosB motes (radio CC2420) in indoor space 70mx90m. To monitor their behavior and generated results, they have programmed them such that they can receive commands wirelessly. The commands can change the node's MAC parameters (and thus MAC behavior), instruct the node to send packets, or acquire data from the nodes (e.g., link quality). A laptop with a TelosB node attached to a USB port was controlling the deployment by issuing of these commands. They noticed disagreements in the application results.
In our case, we fixed three aims for the simulation step that are:

- Reactivity: The validation of all models proposed of supervision and of communication,
- Scalability: studying the model behaviour in a large-scale network,
- Energy consumption.

For these evaluation purposes, we have implemented the active products model into Castalia 2.0 a state of the art WSN simulator based on the OMNet++ platform. We have created all the types of messages implicated in the model using files (.msg). The node behaviour when it receive a message was defined in the handleMessage() method. The figure 16 illustrates a part of the handleMessage Method.

```
case CTR:
{
 if (self != 0)
    printf("ERROR: CTR must be destinated only to the supervisor\n");
else
{
  if (ackCtrSent[atoi(msgSender.c_str())] == false)
  {
        send2NetworkACK(msgSender.c_str(), ACKCTR, 1);
       ackCtrSent[atoi(msgSender.c_str())] = true;
              }
        }
        break;
}
```

Figure 16: a part of the handleMessage() method

In addition, Castalia has a modular structure. Each one of the modules contains one or more parameters that affect its behavior. These parameters have types and so the user can only assign specific types of values to them either directly in the NED files or in the configuration file omnetpp.ini or in the .ini files in the Castlia/Simulations/Parameter_Include_Files directory. We modified some of these parameters like the nodes number in the network (9), its area (25mx25m) and the radio type (CC2420 used in TelosB motes).

7.1 Studying reactivity

Scénario1:
Each node should be configured before starting sensing data. First, to enter to the community, the node should send the CTR message to the supervisor and wait to be acquitted. When it receives the ACK message, it requests to be configured by sending the NCF message and it waits until it receives the CMD1 or the CMD3 messages (it depends on the type of NCF message sent (0, 1 or 2). After this step, the node is considered as configured.

```
node: 0 -> received APP_NODE_STARTUP at 0.000000
node: 1 -> received APP_NODE_STARTUP at 0.050996
                                                  ↓
node: 1 -> sent CTR to 0 at 0.050996        Initialization time
…                                             for node 1
node: 0 -> received APP_DATA_PACKET(CTR) from 1 at
0.190010
node: 0 -> sent ACK(1028) to 1 at 0.190010
node: 1 -> received APP_DATA_PACKET(ACKCTR) from 0
at 0.195583
node: 1 -> sent NCF(2) to 0 at 0.195583
…
node: 0 -> received APP_DATA_PACKET(NCF 0) from 1
node: 0 -> sent CMD1 to 1 at 0.404516
node: 1 -> received APP_DATA_PACKET(CMD1) from 0 at
0.414901
node: 1 -> sent ACK(1037) to 0 at 0.414901
node: 0 -> received  APP_DATA_PACKET(ACKCMD1)
from 1 at 0.423653
…
node: 1 -> sent ACK(1038) to 0 at 0.826218
…
node: 1 is now Configured and it has SecurityRules at
0.826218 ➡ Configuration time for node 1
```

Figure 17: Scenario of node configuring

In figure 17, node1 communicates with node0 (the supervisor) to be configured. It has started at 0.050996s when it has received the APP_NODE_STARTUP message sent by it self. In addition, it has configured at 0.826218s when it has received the reply of the NCF message from the supervisor.

Scenario 2:
When the particle is configured, and it has the security rules, it will start to send the salutation message (GRE) every period of GRE_DELAY, and the APP_2_SDM_SAMPLE_REQUEST every period of APP_SAMPLE_INTERVAL.
The scenario in the figure 18 shows the network reaction when a node is an alert case. For this purpose, we configured the node 3 in order to affect to its VMax parameter (the maximal value of the captured temperature al-

lowed) 14. The value captured by this node is 7 and this value will be increased by 2 every APP_SAMPLE_INTERVAL period.

```
node: 3 Value  = 7.038390 VMax = 14.000000
…
node: 3 Value = 7.840240  VMax  = 14.000000
…
node: 3 Value = 8.806861 VMax =  14.000000
…
node: 3 Value = 10.787591 VMax = 14.000000
…
node: 3 Value = 11.902659 VMax = 14.000000
…
node: 3 Value = 12.927368 VMax = 14.000000
…
node: 3 Value = 15.015800 VMax = 14.000000
node: 3 -> sent ALE from Value on BROADCAST at 41.637175
…
```

Figure 18: scenario of triggering alert

- Value: value captured by the sensor
- VMax: threshold value for the sensor

In the scenario of triggering alert, we simulate the sensed value as a value initialized by 7 and it would be after increased by 2 each sensing period. So, at 41.637175s this value reaches the threshold value (14), and in this case, it sent an ALE message on broadcast.

7.2 Studying scalability

In order to verify the influence of the adding of the active particles model in the node application under Castalia, we run multiple simulations and in each simulation, we modify the nodes number. After that, we extract from each simulation the probability of lost packets.

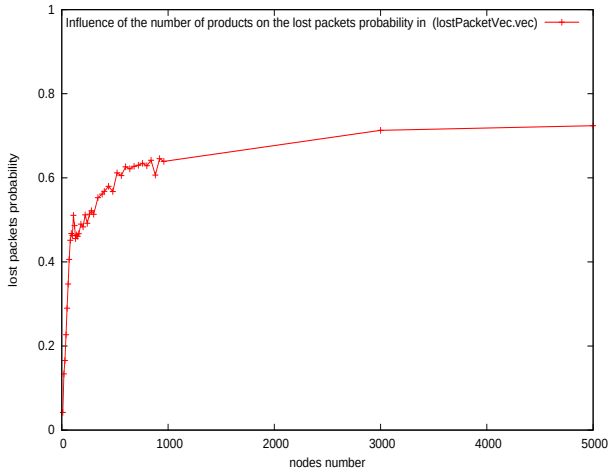

Figure 19: scalability histogram

The histogram in figure 19 shows that the probability of lost packets exceeds 0.5 when the number of nodes in the network surpasses the 278. In addition, it exceeds 0.2 when the number of nodes in the network surpasses the 38 nodes. On comparing with the same type of histogram done by an application of value propagation on the original version of Castalia (without any modification), it seems that the adding of the model has not a critical influence. Nevertheless, we should run an application with the same number of packets exchanged on Castalia simulator to do significant analyses.

7.3 Energy consumption

Resource management is of overriding importance for WSNs because the corresponding resource budgets need to be guaranteed in order to achieve certain requirements. This is particularly true for energy resources that are naturally limited. Our model should respect this particularity. The table of the figure 20 shows the value of the spent energy for each node in the network:

NODE	SPENT ENERGY (JOULES)
Node 0	161.989
Node 1	161.966
Node 2	161.966
Node 3	161.977
Node 4	161.966
Node 5	161.966
Node 6	161.967
Node 7	161.966
Node 8	161.966

Figure 20: spent energy for each node

When we calculate the rate of the spent energy, we find that each node consumes 0.85% of its initial energy (18720 joules) in a simulation time fixed to 1000s.
In Castalia, they are modeling a baseline power consumption (due to processor and other electronics running) which we can control in the parameters of the resource manager. In our case, we considered that it is equal to 0.1 joules each one second. Therefore, the baseline power consumption is 100 joules (0.1x1000). The radio module and the sensor device manager module consume the rest of spent energy.

We précised in the table of the figure 21 the spent energy value of each request in our model:

Request	Spent energy
Initialisation(CTR/ ACKCTR)	0.011764
Configuration(NCF0/ CMD1/ CMD3)	0,013863
Reading security rules (CMD4/SER)	0,05175
Reading configuration parameters(CMD2/CFG)	0,05175
Reading ambiant information(CMD5/INA)	0,05175

Figure 21: spent energy for each state

8 CONCLUSION

During this work, we define a concept of an active security distributed management system, with modeling of active product's behavior dedicated to security management of hazardous products. We proposed an active product's behavior model which was simulated the cooperation between products. Cooperation between active products is provided by exchanging of messages in order to manage and control dynamically in real-time their active security.

To implement our approach, we are using self-developed simulation test bed, designed using Castalia and OMNET++ simulators. We are currently implementing our approach in various real time scenarios to check its adaptiveness but the success and robustness of our model. Certainly, we only broke the surface of the problems associated with more realistic simulation and correspondence of real deployment data with simulation.
In future research, an adaptive algorithm will be developed to reduce the communication and computation overhead caused by the control packets.
As perspective of this work, one will develop an experimental platform in order to compare these simulation results of with the experimental results.

REFERENCES

Bajic E., 2009. A Service-Based Methodology for RFID-Smart Objects Interactions in Supply Chain, *International Journal of Multimedia and Ubiquitous Engineering, Vol. 4, No. 3, July, 2009.*

CoBIs, 2008. Collaborative business items. *European Community FP6 STREP Project, IST 004270, Technical report,* 2OO8. www.cobis-online.de.

Decker C., Beigl M., Eames A., and Kubach U., 2004. Digiclip : Activating physical documents. *ICDCSW' 04, 2004,* Tokyo, Japan.

Dobre D., Bajic E., 2007. Smart object design for active security management of hazardous products, *Ubicomp*, sbruck, Austria, Septembre 16-18, 2007.

Gárate A., Herrasti N., López A., 2005. GENIO: an Ambient Intelligence Application in Home Automation and Entertainment environment, *Joint Conference on Smart Objects and Ambient Intelligence*, 2005.

Kärkkäinen M., Holmström J., Främling K., Artto K., 2003. *Intelligent products – a step towards a more effective project delivery chain. Computer in Industry 50*, p. 141-151.

Liu D., Law K., and Wiederhold G., 2000. Chaos : An active security mediation system. *Conference on Advanced Information Systems Engineering*, 5-9 June 2000. Stockholm.

McFarlane D., Sarma S., Chirn Jin Lung, Wong C.Y., Ashton K., 2003. Auto ID systems and intelligent manufacturing control. *Engineering Applications of Artificial Intelligence*. *16*, p. 365-376.

McFarlane D., Sarma S., Chirn Jin Lung, Wong C.Y., Ashton K., 2002. The intelligent product in manufacturing control and management. *15th Triennial World Congress IFAC*, Barcelona, Spain.

Meier A., Motani M., Siquan H., and Künzli S., 2008. DiMo: Distributed Node Monitoring in Wireless Sensor Networks, , *MSWiM'08*, October 27–31, 2008, Vancouver, BC, Canada.

Pham H. N., Pediaditakis D., and Boulis A., 2007. From Simulation to Real Deployments in WSN and Back, *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM,2007*, 18-21 June 2007, Espoo, Finland, p. 1-6, (ISBN: 978-1-4244-0993-8).

Quanz B., Tsatsoulis C., 2008. Determining Object Safety using a Multiagent Collaborative System, *ECOSOA 2008, Workshop at Second IEEE International Conference on Self-Adaptive and Self-Organizing Systems*, Venice, Italy, October 20-24, 2008.

Rajeet Chatterjee C., Wolfe P., Park S., Choi J., 2005. Evaluation of using RFID passive tags for monitoring product location / *ownership*, Arizona State University USA.

Strohbach M., Kortuem G., and Gellersen H., 2005. Cooperative artefacts-a framework for embedding knowledge in real world objects. *International Workshop on Smart Object Systems, (UbiComp2005)*, Tokyo, Japan, p. 91–99.

Strohbach M., Gellersen H.-W., Kortuem G., and Kray C., 2004. Cooperative artefacts: Assessing real world situations with embedded technology. *In Proceedings of Sixth International Conference on Ubiquitous Computing*.

Wong C.Y., McFarlane D., Zaharudin A.A., Agarwal V., 2002. The Intelligent Product Driven Supply Chain. *IEEE International Conference on Systems, Man and Cybernetics*, Hammamet, Tunisia.

Zouinkhi A., Bajic E., Ben Gayed M. and Abdelkrim M. N., 2007. Modèle de Produits Actifs et Communication Ambiante pour la Gestion de la Sécurité de Produits Dangereux, *Huitième conférence internationale des Sciences et Techniques de l'Automatique (STA'2007)*, Monastir, Tunisie.

Zouinkhi A., Bajic E., ZIDI R., Ben Gayed M., RONDEAU E. and Abdelkrim M. N., 2009. Petri Net Modeling of active products cooperation for active security management. *Sixth IEEE International Multi-Conférence on System, Signals & Devices (SSD'09)*, 23-26 March – Djerba-Tunisia.