ISSN:2231-0711



# Applying Ambient Intelligence to Industrial Storage

Dr K.R.R.Mohana Rao[1], Dr Syed Umar[1], Soma Ambedkar Borugadda[2]

[1]*Department of ECM,*
*KL University, A.P., INDIA.*

[2]*Department of IT,*
*CIT, Mothadaga, Guntur, A.P., INDIA.*

***Abstract*— Ambient Intelligence refers to an environment that is sensitive, adaptive, and responsive to the presence of people. Such an environment relies heavily on information from the numerous sensors monitoring the environment. The components of the ambient intelligence environment is pervasive, meaning all devices are connected to the personal, local, regional, national, and global network. The devices are also invisible, until they are needed.**

*Keywords*— **Ambient Intelligence, Intelligent Product, Cooperation, Security, WSN, Petri Nets, Castalia**

## 1. INTRODUCTION

Amongst the main constraints and objectives in industrial processes is the security issue. Especially, in industrial environment workers have to deal with unavoidable threats from products, resources and machines that are parts of work risks. Currently, many security systems depend on safety measurements that are taken by interacting devices eventually exposing people's lives to unpredictable situation as an example in storage and transport activities of hazardous chemical substances. Our research approach to study such fully distributed and discrete industrial environment which is based on communicating object's concept which represents a physical product equipped with perception, communication, actuation and decision making capabilities. The communicating object's approach has attracted the interest of several research projects as COBIS project (Collaborative Business Items) [1] that has developed a new approach to business processes involving physical entities such as goods and tools in enterprise. The intention is to embed business logic in the physical entities. Also, the computing department at Lancaster University [2] conceived cooperative products with perception, analysis and communication capacities that operated by information sharing principle. Also, [3] is considering the problem of Object Safety: how objects endowed with processing, communicating, 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. When the agent detects a threat, it seeks confirmation from its neighbors. Ambient intelligence and communication technologies bring new visions in creating reliable systems for security management where dangerous products can be turned into smart products to control, prevent and react to security threats in the ambient process. Each product plays the role of an active node of the overall security system by means of an embedded reactive model for the security assurance.

The aim of this work is to propose a Petri nets hierarchical modeling framework with internal cooperation model of intelligent products by using the High Level Petri Nets (HLPN) formalism. Conceptual modeling was validated by the software CPN-Tools from Aarhus University [4]. An internal model of an active product is implemented and then was validated by the simulation software Castalia based on the OMNET platform.

## 2. AMBIENT INTELLIGENCE(AMI)

Ambient Intelligence (AmI) [5-7] is growing fast as a multidisciplinary approach which can allow many areas of research to have a significant beneficial influence into our society. AmI has a decisive relation with many areas in computer science. The relevant areas are depicted in **Figure 1**. Here we must add that whilst AmI nourishes from all those areas, it should not be confused with any of those in particular.

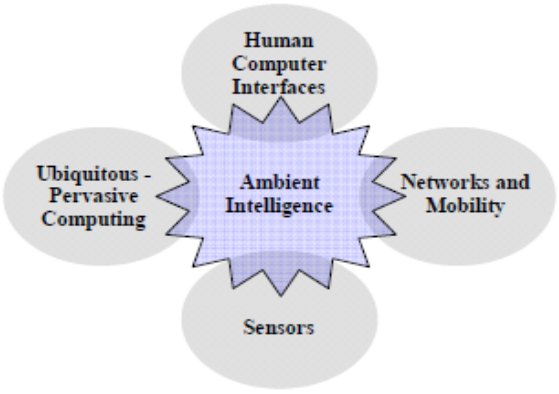


Figure 1. Relation between AmI and other areas.

Networks, sensors, interfaces, ubiquitous or pervasive computing and AI are all relevant but none of them conceptually covers AmI. It is AmI which puts together all these resources to provide flexible and intelligent services to users acting in their environments. As Raffler succinctly expressed [8], AmI can be defined as: A digital

environment that supports people in their daily lives in a nonintrusive way.

AmI is aligned with the concept of the disappearing computer [9,10]: the most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.

### 2.1. Intelligent Product

According to [11, 12], 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.

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 [13]. The latter is 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 [14], 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. The goal in this case is to record and update all information associated with a dynamic product (such as his statements, the operations he has endured). 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, [11] 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.

## 3. ACTIVE SECURITY MANAGEMENT SYSTEM

### 3.1. General Context

In order to present the general situation of subject, we have defined the elements which constitute the global framework of cooperation. A warehouse is an environment where we stoke dangerous chemicals products. In order to ensure the safety of these products, we will check only brightness, moisture and temperature. The follow-up of these variables can help to ensure the wellness of products. For example, starting from a value of temperature rather high one can note that the product in subject undergoes poor circumstances from where a critical condition is announced. Each containing chemicals must be equipped with a node of sensor containing: a temperature gauge, a sensor of moisture and a sensor of light, have fine to collect the variables of environment, the cycle of operation of each intelligent product is the following: to acquire the values of the sensors, to evaluate these values by consulting the clean knowledge base and decision making after having to compare the variables of environment with the critical variables. All intelligent products communicate with the manager who has the level higher (as shown in **Figure 2**).

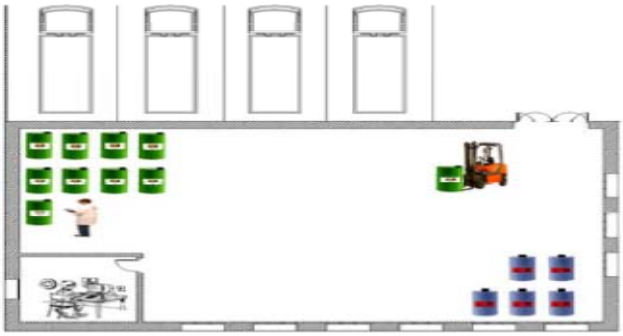

**Figure 2. Intelligent product interactions in an AmI environment.**

On the other hand, the objective consists with stage the mechanisms of interaction in which the intelligent product are able to communicate, acquire information, to decide and react to the stimuli and disturbances of its environment in order to make it possible that the product to deal with its intrinsic safety and total safety in its interactions with other products or people finally touching a decentralized aspect. But it is necessary to highlight which the decentralized aspect is not single, because, for example, the suitable knowledge base for have are sent by an administrator who also has like role of configured remotely these intelligent products. In made, our management system of active safety includes/understands a whole of product initially intelligent 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 intelligent product. Cooperation between intelligent products takes place by the exchange of messages.

### 3.2. Exchanged Messages

Communication between products works by using several types of messages which are sent by a broadcasting mode and classified according to their. Product's announcement in the products' community is of great importance for the overall security management. For this, we propose two types of messages: CTR (Control Timestamp Request): message which declares to the administrator the arrival of a new product. Ack_CTR: the acknowledgement message from the administrator.

After registration the product needs a setup configuration to allow it to interact within the community. This configuration concerns the type of product regarding its hazardous classification (safety symbols) and its static, dynamic and community related rules as well. When not configured, a product announces its status with three types of messages: NCF0: Product has no hazardous classification and no security rules configuration, NCF1: Product has only hazardous classification configuration and NCF2: Product has only security rules configuration. Then

the system administrator answers by an appropriate product configuration command message respectively: CMD1: Configuration of the product classification and CMD3: Configuration of the security rules.

Once the product is correctly configured; it becomes completely capable of surveying its neighborhood: it is now an effective Intelligent Product (IP). INA: this message carries the ambient sensors values embedded in the product. CFG: a message emitted by IP after an administrator request, contains the specific configuration in the IP. SER: a broadcast message containing the IP security rules values. ALE: an alert message to report to the administrator about a threat or a defective security state. The administrator participates in the communication part by specific command messages: CMD2: Administrator requires the configuration of the IP through this message, CMD4: Administrator asks for Security rules Configurations and CMD5: Administrator asks for specific ambient information of IPs.

### 3.3. Interaction Mechanism

#### 3.3.1. Centralized Tasks

Then in order to get through chemical community, any foreign product has to introduce itself to the community manager, this product has to be announced to the manager by sending a CTR message which is an empty message that affirms to the manager the product being into the network, this message is sent continuously in broadcast mode until the manager answers by a Ack_CTR message which represents the acknowledgment of the manager after the reception of the CTR message. After having to finish the phase d' inscription with the network, the product must ask for to the manager his rules and its symbols of safety by the sending of messages NCF. The manager in his turn already identified the product (by message CTR), can provide him these needs by consulting his database by sending CMD1 containing to him the symbols for safety or CMD3 containing the safety regulations. It is noticed that the two spots announcement and configuration obey centralized approaches because each time the IP must refer to the manager for s' to identify or to update its knowledge base. The second spot is the surveillance and communication where an IP must communicate with the products of vicinity. The communication between IPs is done by the greeting message GRE. As soon as an IP receives a message GRE it will transmit a Message RSSI (Received Signal Strength Indicator): The information of this type of message contains mainly the difference in power of the signal. This method of measurement is used to estimate compatibility with minimal distance between IPs.

#### 3.3.2. Ubiquitous Tasks

Equipped knowledge base (rules and symbols of safety) and of a capacity of collecting and decision, the IP can carry out two spot essence to be well as shown in **Figure 3**. The first spot is the internal monitoring where it becomes able to supervise its vicinity, whereas any modification of its environment, violating the individual or mutual safety regulations must be detected, analyzed and finally, following a difference between the variables of environment and those basic of knowledge, with the reactions are associated such as the sending of Rapp_D to the manager announcing a state of danger. The second spot is the monitoring and communication where an IP must communicate with the products of vicinity.

### 3.4. 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, Dynamic rules and Community rules.

## 4. MODELING BY PETRI NETS

Petri Nets are used for a long time as modeling tools of discrete events systems. Several works opted for the Petri Nets modeling in fields like communication systems, flow shop and logistic chain. [16] Proposed a model of TCP/IP communication behavior; [17] presented a model of a network controlled system. The major advantages that promote the use of Petri Nets are, first the possibility to verify the system behavior have good properties and to give specifications in formal way and to provide graphic of system, and then, the possibility to model and to simulate the system [18]. The objective of our work is to represent the behavior of the active product and the stream of messages through a wireless network in order to achieve interaction between products; CPN-Tools allow creating hierarchical models in order to simplify complex ones and divide it into other sub models. This means that in the Hierarchical Petri Net model certain transitions represent another Petri Net sub model.

### 4.1. Global Model

The model of cooperation is equipped with six elements (P1, P2, P3, manager (Administrator), Operator, Cart) which communicate between them, in order to form a community of wireless cooperation. Each element is represented by a transition (hierarchical) which presents the services and suitable task quoted in details in what follows. As the **Figure 4** shows, each node presents two places: Net Input and Net Output which respectively presents the output buffers of each element and input one. These aims of this buffers is to memorize the messages temporarily received from network before being treated (in the processing unit) and those emitted by the elements in the network.

### 4.2. Network Level

In this part, we will present the network's model where the sensor's nodes interact; firstly, we are going to model the hierarchical transition network which is represented by the **Figure 4** as a perfect network (without any disturbance) to evaluate the impact of progressive increasing of node's number existing in this network, and thereafter, we will create a disturbance in this network to check the robustness of allover the system. The **Figure 4** indicates the lower level of the Network: the higher places Net input indicate the output's buffers of the node where the messages are stored before being emitted in the network; these messages pass by a classification's stage which classify them according to their transmitting nodes before being stored in the place "message transmitted in network". The network presented to the **Figure5** defines a disturbed network where there is risk of loss of message. Each token (message), which is presented in the place ("message sent through

network") must cross the transition where it will be to assign to another place, in this moment this token will be lost or gone, after this passage (transition "gone"), this token enters a buffer of entry and afterwards enters a buffer of exit to be finally in the place "message received".

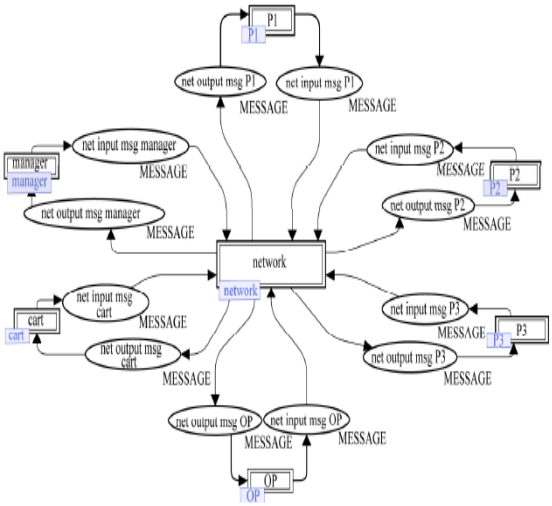


**Figure 4. Global cooperation model.**

For evaluation purposes we have implemented the IPs model into Castalia 2.0 a state of the art WSN simulator based on the OMNet++ platform.

## 5. CASTALIA SIMULATION

Castalia is a Wireless Sensor Network (WSN) simulator based on the OMNet++ platform that can be used by researchers and developers who wants to test their distributed algorithms and protocols within a realistic wireless channel and radio model.

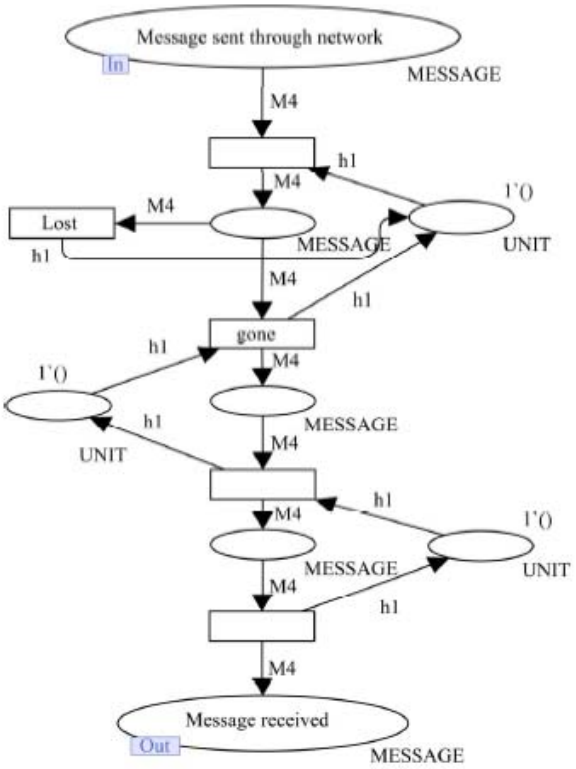


**Figure 5. Network model.**

### 5.1. Regulating of Reading Period Sensors

At first we changed the reading period of sensors and we were measured the responsiveness for each value system. To measure the responsiveness of the system, we have created a scenario. The following figure shows the effect of the reading period sensors on the relative error of system responsiveness. As it is shown in the **Figure 9**, the error on the reactivity of the system is minimal for a period of reading sensors equal to 0.5 seconds. On the other hand, we have studied the loss of packets based on number of intelligent products in a warehouse 25 m × 25 m surface and for each value of the reading period sensors during a simulation period equal 1000s. In the following we will fix the sensor reading period and the period of sending messages to 0.5 s. In our case, we fixed three aims for the simulation step that are: reactivity: The validation of all models proposed of supervision and communication, scalability: studying the model behavior in a large-scale network and energy consumption.

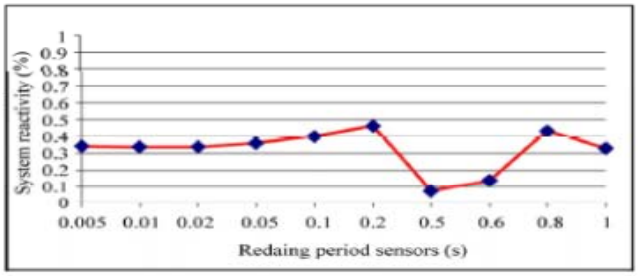


**Figure 9. Influence of the reading period sensors on the system reactivity.**

### 5.2. Studying Reactivity

When the IP is configured, and it has the security rules, it will start to send the salutation message (GRE). Value is the value captured by the sensor and VMax is threshold value for the sensor. (see **Figure 10**) 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 41.637 175 s this value reaches the threshold value (14), and in this case, it sent an ALE message on broadcast.

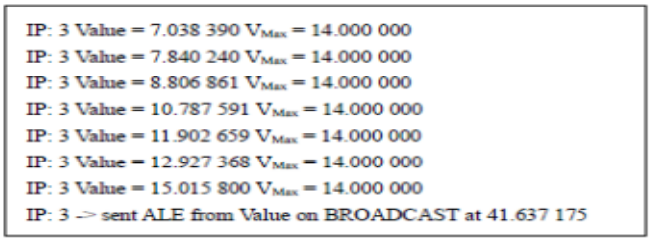


**Figure 10. Scenario of triggering alert.**

### 5.3. Studying Scalability

In order to verify the influence of the adding of the IPs model in the node application under Castalia, we run multiple simulations and in each simulation, we modify the IPs number. After that, we extract from each simulation the probability of lost packets. The histogram in **Figure 11** shows that the probability of lost packets exceeds 0.5 when the number of IPs in the warehouse surpasses the 278. In addition, it exceeds 0.2 when the number of IPs surpasses the 38.

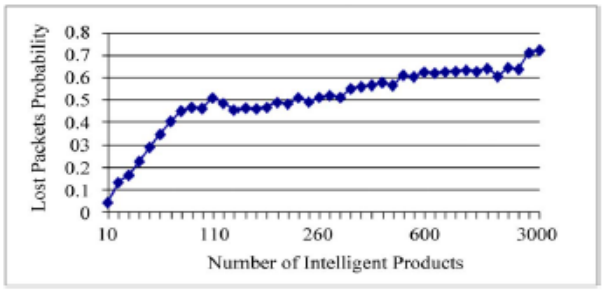


**Figure 11. Influence of the number of products on the lost packets probability.**

### 5.4. Energy Consumption

Resource management is of overriding importance for Wireless Sensor Networks 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 1** shows the value of the spent energy for each IP in the network. When we calculate the rate of the spent energy, we find that each IP consumes 0.85% of its initial energy (18720 joules) in a simulation time fixed to 1000s.

**Table 1. Spent energy for each state.**

| *Request* | *Spent energy (J)* |
|---|---|
| Initialisation(CTR/ACKCTR) | 0.011 764 |
| Configuration(NCF0/CMD1/CMD3) | 0.013 863 |
| Reading security rules (CMD4/SER) | 0.051 75 |
| Reading parameters(CMD2/CFG) | 0.051 75 |
| Reading ambiant information(CMD5/INA) | 0.051 75 |

## 6. CONCLUSIONS

In this work, we define a concept of an active security distributed management system, with modeling of IP's behavior dedicated to security management of hazardous products. We proposed an IP's behavior model represented by hierarchical colored Petri nets. This hierarchy includes sub-models where each one allows displaying the evolution of every state of the IP (registration, configuration, surveillance and communication and internal surveillance). With Petri. 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. As perspective of this work, one will develop an experimental platform in order to compare these simulation results of with the experimental results.

## REFERENCES

[1] Collaborative Business Items, European Community FP6 STREP Project, IST 004270, Technical Report, 2008. URL: www.cobis-online.de

[2] M. Strohbach, G. Kortuem and H. Gellersen, "Cooperative Arteifacts — A Framework for Embedding Knowledge in Real World Objects," International Workshop on Smart Object Systems at UbiComp, Tokyo, 11-14 September 2005, pp. 91-99.

[3] B. Quanz and C. Tsatsoulis, "Determining Object Safety Using a Multiagent Collaborative System," In ECOSOA, *Workshop at the 2nd IEEE International Conference on Self-Adaptive and Self-Organizing Systems*, Venice, 20-24 October 2008, pp. 25-30.

[4] A. V. Ratzer, L. Wells, H. M. Larsen, M. Laursen, J. F. Qvortrup, M. S. Stissing, M. Westergaard, S. Christensen and K. Jensen, "CPN-Tools for Editing, Simulating and Analysing Coloured Petri Net," *Proceedings of the* 24*th International Conference on Applications and Theory of Petri Nets*, Eindhoven, Vol. 2679, 23-27 June 2003, pp. 450-462.

[5] IST Advisory Group. The European Union Report, "Scenarios for Ambient Intelligence in 2010," 2001. URL: ftp://ftp.cordis.lu/pub/ist/docs/istagscenarios2010.pdf

[6] J. C. Augusto and D. Cook. "Ambient Intelligence: Applications in Society and Opportunities for AI," *Proceedings of the* 20*th International Joint Conference on Artificial Intelligence*, Hyderabad, 6-12 January 2007.

[7] J. C. Augusto, "Ambient Intelligence: The Confluence of Pervasive Computing and Artificial Intelligence," In: A. Schuster, Ed., *Intelligent Computing Everywhere*, Springer Verlag, Berlin, 2007, pp. 213-234.